# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Features and Enhancements</td>
<td>17</td>
</tr>
<tr>
<td>Introducing MobileIron Access</td>
<td>18</td>
</tr>
<tr>
<td>MobileIron Access overview</td>
<td>18</td>
</tr>
<tr>
<td>Deployment modes</td>
<td>18</td>
</tr>
<tr>
<td>Naming convention</td>
<td>19</td>
</tr>
<tr>
<td>User interface</td>
<td>19</td>
</tr>
<tr>
<td>Support and compatibility</td>
<td>20</td>
</tr>
<tr>
<td>Component interaction</td>
<td>20</td>
</tr>
<tr>
<td>MobileIron UEM compliance actions and policies</td>
<td>21</td>
</tr>
<tr>
<td>Authentication flow with Access</td>
<td>22</td>
</tr>
<tr>
<td>Managed non-AppConnect app using Tunnel</td>
<td>22</td>
</tr>
<tr>
<td>AppConnect apps with Access enabled (Core only)</td>
<td>24</td>
</tr>
<tr>
<td>Authentication flow with Access + Standalone Sentry</td>
<td>24</td>
</tr>
<tr>
<td>Managed non-AppConnect app using Tunnel and Standalone Sentry</td>
<td>24</td>
</tr>
<tr>
<td>AppConnect apps using AppTunnel with Access + Standalone Sentry</td>
<td>25</td>
</tr>
<tr>
<td>After the user is authenticated in an Access deployment</td>
<td>25</td>
</tr>
<tr>
<td>Accessing the cloud service from a desktop, laptop, or an unmanaged device</td>
<td>25</td>
</tr>
<tr>
<td>Setup overview for MobileIron Access</td>
<td>26</td>
</tr>
<tr>
<td>Before you configure MobileIron Access</td>
<td>26</td>
</tr>
<tr>
<td>Overview of steps to set up MobileIron Access</td>
<td>27</td>
</tr>
<tr>
<td>Basic configuration</td>
<td>27</td>
</tr>
<tr>
<td>Advanced configuration</td>
<td>27</td>
</tr>
<tr>
<td>Split tunneling configuration</td>
<td>28</td>
</tr>
<tr>
<td>Delegated IdP</td>
<td>28</td>
</tr>
<tr>
<td>Authentication options</td>
<td>28</td>
</tr>
</tbody>
</table>
### Contents

**Getting Started with MobileIron Access** ................................................................. 30

Before you set up MobileIron Access ................................................................. 30

Deployment Type ................................................................................................. 30

Federated authentication ...................................................................................... 31

MobileIron Access credentials ........................................................................... 31

Standalone Sentry information ........................................................................... 31

Certificates for Access + Standalone Sentry ................................................... 32

SSL certificate for MobileIron Access .............................................................. 32

Generating an SSL certificate (PKCS12 file) for MobileIron Access ................. 32

Signing certificate ............................................................................................... 32

Working with MobileIron Access administrative portal .................................. 33

Changing the password ...................................................................................... 38

  Password requirements ................................................................................. 38

Resetting the password recovery key ............................................................. 38

Resetting your password ............................................................................... 39

Configuring 2-step verification ......................................................................... 40

Disabling 2-Step Verification ........................................................................... 42

Signing out of the MobileIron Access administrative portal ........................... 43

Working with MobileIron Access in Cloud administrative portal ...................... 43

Account settings ............................................................................................... 46

Changing the Password for Cloud portal ...................................................... 47

Admins ............................................................................................................... 48

MobileIron Access Global Dashboard ............................................................ 49

GeoIP Map ......................................................................................................... 51

  Viewing details for allow, block, or warn requests ........................................ 51

**Set up Access with MobileIron UEM** ................................................................. 53

Overview of configuration with MobileIron Cloud ......................................... 53

Configuring Access in MobileIron Cloud ......................................................... 53

Configuring MobileIron Tunnel in MobileIron Cloud ....................................... 55
# Contents

- Configuring MobileIron Cloud in Access ................................................................. 57
- Overview of configuration with MobileIron Core ....................................................... 59
- Configuring Access in MobileIron Core ........................................................................ 59
- Configuring MobileIron Tunnel in MobileIron Core .................................................... 61
- Configuring MobileIron Core in Access ......................................................................... 63
- Deregistering Access from UEM .................................................................................... 64
- **Set up Access + Standalone Sentry** ........................................................................... 66
  - Overview of steps to set up Access + Standalone Sentry ............................................ 66
  - Adding a profile ......................................................................................................... 66
    - Error conditions for SSL certificate ..................................................................... 69
  - Registering a Standalone Sentry ............................................................................... 69
    - Example of Standalone Sentry registration to MobileIron Access ..................... 70
  - Viewing Standalone Sentry information .................................................................... 71
  - Standalone Sentry actions ....................................................................................... 72
    - Assigning Standalone Sentry to a profile ......................................................... 72
    - Unassigning Standalone Sentry from a profile ................................................ 73
    - Deleting a Standalone Sentry .............................................................................. 73
  - Profile overview ...................................................................................................... 73
    - Editing the profile ................................................................................................. 74
- **Federated Pairs** ......................................................................................................... 75
  - Configuring federated pairs ...................................................................................... 75
  - Use Cases for distinctive deployments .................................................................... 77
    - Jabber and Access ................................................................................................. 77
  - Signing certificates .................................................................................................. 78
    - Adding a signing certificate in MobileIron Access .............................................. 78
    - Generating a signing certificate in MobileIron Access ....................................... 78
  - Service provider (SP) metadata ............................................................................... 79
    - Assertion Consumer Service (ACS) URLs ......................................................... 80
    - Metadata for G Suite ............................................................................................. 80
Configuring Access as the delegated IdP ........................................................................... 101
PowerShell commands for ADFS ....................................................................................... 107
  Running the PowerShell script to set up Access as the delegated IdP in ADFS .................. 107
  Using the PowerShell script to create a new Access theme in ADFS for iPadOS 13 upgrades .................................................................................................................. 108

**Conditional Access** ........................................................................................................ 110
Conditional policies ............................................................................................................... 110
  Adding a new conditional policy ....................................................................................... 110
Conditional rules .................................................................................................................. 111
  Adding a conditional rule ................................................................................................. 111
Predefined conditional rules ............................................................................................... 111
Customizable conditional rules ........................................................................................... 112
  Tunnel rule ...................................................................................................................... 113
  User Info Rule ................................................................................................................ 113
  Network Rule .................................................................................................................. 114
  App Rule ......................................................................................................................... 115
  Advanced Network Rule ................................................................................................. 116
Multi-factor Authentication ................................................................................................. 118
  Zero Sign-on Rule .......................................................................................................... 119
  Desktop Trust Rule ......................................................................................................... 119
  Request Header Rule ...................................................................................................... 119
Policy chaining ...................................................................................................................... 121
Example setup with conditional rules .................................................................................. 122
  Setup with conditional ..................................................................................................... 122
  Expected behavior with the example setup ..................................................................... 122
Managing policies and rules ............................................................................................... 122
  Applying a conditional policy to a federated pair ............................................................ 123
  Editing a conditional policy ............................................................................................ 123
  Deleting a conditional policy .......................................................................................... 123
  Editing a rule .................................................................................................................. 123
Disabling, enabling, or deleting a rule ................................................................. 123
Enabling the compliance remediation page ..................................................... 124
**Configuring Mobile App Single Sign-on (SSO)** .............................................. 125

**Split Tunneling** .......................................................................................... 128
Split tunneling in an Access + Standalone Sentry deployment ........................ 128
Split tunneling in an Access deployment ....................................................... 129
Split tunneling for Android ........................................................................... 130
Split tunneling for iOS and macOS ............................................................... 130
Overview of steps for configuring split tunneling in Access ....................... 130
Enabling split tunneling .............................................................................. 130
Adding domains for split tunneling ............................................................. 131

**Branding** .................................................................................................. 133
Branding overview ....................................................................................... 133
Adding a remediation page ......................................................................... 137
Redirecting device users to a URL ............................................................... 137
Creating a customized message .................................................................. 138
Creating a customized warning message .................................................... 138

**Session Revocation** ................................................................................ 140
About session revocation ........................................................................... 140
Configuring Session Revocation ................................................................ 142
Session revocation report .......................................................................... 143
What users see if session revocation is configured .................................... 144

**Fast Identity Online (FIDO2) or Zero Sign-on with MobileIron Access** ..... 145
Overview .................................................................................................... 145
Key features ............................................................................................... 145
Use cases ................................................................................................... 146
Deployment use cases .............................................................................. 146
Required MobileIron components ............................................................ 148
Supported devices ..................................................................................... 149
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported browsers</td>
</tr>
<tr>
<td>Authentication flow types</td>
</tr>
</tbody>
</table>

Configuring Zero Sign-on in MobileIron Cloud | 150
Creating a Zero Sign-On configuration in MobileIron Cloud | 150
Syncing the Zero Sign-On configuration with MobileIron Access | 150

Configuring Zero Sign-on in MobileIron Core | 151
Creating a Zero Sign-on policy in MobileIron Core | 151
Syncing the Zero Sign-on policy with MobileIron Access | 152

Configuring Zero Sign-on in MobileIron Access | 152
Setting Zero Sign-on security and user experience | 152
Set the session timeout duration | 153
Registering with MobileIron Authenticate | 153
Unlocking the desktop | 154
Authentication for service providers | 155
FIDO Key | 155

Passwordless authentication to service providers on unmanaged devices | 157
Password-less login from unmanaged devices | 157
Enabling Password-less Authentication on MobileIron Go and Mobile@Work | 158
Adding a Zero Sign-on Rule in the Policies | 159
Configuring branding for Zero Sign-on | 162
Publishing the changes | 162

Password less login to cloud services for managed desktops | 162
Password-less log in to desktops | 163
Required MobileIron components | 163
Supported devices | 163
Supported browsers | 163
Password-less log in to cloud services from MobileIron managed desktops | 163
Use cases | 163
Required MobileIron components | 164
Supported devices ........................................................................................................ 164
Supported browsers ................................................................................................. 164
Password-less login from MobileIron managed devices ........................................... 164
Deploying MobileIron Authenticate using UEM ......................................................... 164
Review Registration Settings .................................................................................... 165
Enabling Password-less Authentication on MobileIron Go and Mobile@Work .............. 166
Adding a Zero Sign-on Rule in the Policies ............................................................... 167
Configuring branding for Zero Sign-on ..................................................................... 170
Publishing the changes ............................................................................................. 171
Zero Sign-on from desktops managed by JAMF ........................................................ 171
Use cases .................................................................................................................. 171
Authentication flow from desktops ............................................................................ 172
Required MobileIron components ............................................................................ 172
Supported devices ..................................................................................................... 172
Supported browsers .................................................................................................. 172
Configuring UEM with JAMF in MobileIron Access .................................................. 173
What users see for FIDO2 .......................................................................................... 176
Workflow for registered browsers .............................................................................. 176
Workflow for non-registered browsers ....................................................................... 177
Workflow on Android devices .................................................................................... 180
Unlocking a desktop on Android devices .................................................................. 181
Unlocking a Windows desktop ................................................................................... 181
Unlocking a Mac desktop ........................................................................................... 182
Activating a password-less sign-in on Android device .............................................. 182
Deactivating a password-less sign-in on Android device .......................................... 183
Ending a browser session ........................................................................................ 183
Workflow on iOS devices .......................................................................................... 184
Unlocking a desktop on iOS devices ........................................................................ 184
Activating password-less sign-in on iOS device ....................................................... 186
Deactivating password-less sign-in on iOS device ......................................................... 187
Ending a browser session on an iOS device ................................................................. 188
Workflow for Desktop login ....................................................................................... 188
MobileIron Authenticate ............................................................................................. 189
Configuring MobileIron Authenticate on MobileIron Cloud ........................................ 190
Adding and distributing a macOS application for MobileIron Authenticate .................... 193
Adding and distributing a Windows application for MobileIron Authenticate .................. 197
Configuring MobileIron Authenticate on JAMF .......................................................... 201
What users see for MobileIron Authenticate ................................................................ 203
Workflow on Windows desktop .................................................................................... 203
Workflow on macOS desktop ....................................................................................... 206
Client Registration Settings ...................................................................................... 208
Authenticator Only with MobileIron Access ................................................................. 210
About Authenticator Only with MobileIron Access ...................................................... 210
Required components for Authenticator Only ............................................................. 210
Use cases for Authenticator Only ............................................................................. 211
Authentication flow for Authenticator Only ............................................................... 211
Device actions and policies for Authenticator Only ..................................................... 212
Administrator actions (Cloud) .................................................................................... 213
Administrator actions (Core) ..................................................................................... 213
Device user actions .................................................................................................... 213
Compliance polices and actions (Cloud) .................................................................... 213
Polices and actions (Core) ........................................................................................ 214
Android enterprise and Authenticator Only ............................................................... 214
Configuring Authenticator Only on MobileIron Cloud ............................................... 214
Adding an Authenticator Only configuration on MobileIron Cloud ......................... 215
Syncing with MobileIron Access ............................................................................... 216
Viewing Authenticator Only on MobileIron Cloud .................................................... 217
Devices list ................................................................................................................. 217
Activate MobileIron Authenticator ......................................................... 252
Access cloud services ........................................................................... 252
Custom service provider ...................................................................... 253
Authenticator settings ........................................................................ 253

**Access Certificates** ......................................................................... 254
Certificates .......................................................................................... 254
Actions you can take .......................................................................... 254

User Certificates .................................................................................. 254
Adding a certificate ............................................................................. 255
Actions you can take .......................................................................... 256
User Certificate Details ........................................................................ 256

Certificate expiry notifications ............................................................ 257
Notification in Profile > Federation .................................................... 258
Notifications after a certificate expires .............................................. 258
Notification when you edit a federated pair or delegated IdP ............ 259

Updating certificates for an SP or IdP .................................................. 260
Certificate update if you uploaded metadata .................................... 260
Certificate update if you added metadata ........................................... 262
Certificate update if you entered a metadata URL .............................. 263

**Reports** .......................................................................................... 266
About reports ....................................................................................... 266
Access reports .................................................................................... 267
Delegated IdP field in Access reports .............................................. 268
authnRequestID field in Access reports .......................................... 268
Search Access reports ........................................................................ 269
Flexible Query .................................................................................... 270
Query Examples .................................................................................. 270
Display exceptions in reports ............................................................. 271
Filtering report data ........................................................................... 272
Configuring LDAP in MobileIron Cloud for session revocation .................................................. 292
Configuring LDAP in MobileIron Core for session revocation .................................................. 293
Customizing certificates for single sign-on in Access ................................................................. 294
  Configuring SAML assertion fields ......................................................................................... 294
  Language to generate values from certificate fields ............................................................. 294
  Selection pattern description ................................................................................................. 296
Back up and restore Office 365 settings .................................................................................... 297
  Back up Office 365 settings .................................................................................................. 297
  Restore Office 365 settings ................................................................................................. 297
Configuring MobileIron Access Splunk application .................................................................... 298
  Splunk dashboard ................................................................................................................ 301
New Features and Enhancements

This guide documents 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 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**: You can now select "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.
Introducing MobileIron Access

MobileIron Access is a cloud service which secures access to enterprise content in business cloud services such as Box, G Suite, Office 365, Dropbox, and Salesforce. MobileIron Access secures access based on the following:

- device identity
- user identity
- app identity

MobileIron Access overview

MobileIron Access allows access to enterprise cloud resources based on user and device posture, and whether apps are managed or not. Non-AppConnect managed apps and AppConnect apps are supported. Authentication traffic for managed apps uses MobileIron Tunnel and for AppConnect apps uses AppTunnel. In addition, conditional rules can be configured to allow access for unmanaged applications, as well as, manage access from mobile devices, laptops, and desktops.

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).

MobileIron Access in either deployment provides the following features:

- Integration with business cloud service providers (SP).
- Integration with identity providers (IdP). Conditional rules to allow, block, and warn Access.
- Secure access to enterprise cloud based services.
- Federated authentication with SAML or WS-Fed.
- Visibility into users, devices, and apps accessing cloud services.
- Prevention of unauthorized devices and apps from accessing cloud based services.

**Naming convention**

Unless otherwise noted, MobileIron Access refers to both Access and Access + Standalone Sentry deployments.

**User interface**

MobileIron Access is available in the Access administrative portal or in the MobileIron Cloud portal. To work with either of these instances, use one of the following options:

- If your Access deployment does not integrate with MobileIron Cloud, then Access features are available in the Access administrative portal. For more information, see Working with MobileIron Access administrative portal.

- If your Access deployment integrates with MobileIron Cloud, then the Access features are available in MobileIron Cloud in the left navigation pane. The Cloud and Access tabs are available in one console in MobileIron Cloud. For more information about this user experience, see Working with MobileIron Access in Cloud administrative portal.
Support and compatibility

For information on support and compatibility, see the MobileIron Access Release Notes.

Component interaction

This section provides an overview of how the various components in a MobileIron Access deployment interact with each other. The following table describes how various components interact with MobileIron Access.

<table>
<thead>
<tr>
<th>MobileIron component</th>
<th>Access</th>
<th>Access + Standalone Sentry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access administrative portal</td>
<td>All Access related configurations, monitoring, reporting are done in the Access administrative portal.</td>
<td>All Access related configurations, monitoring, reporting are done in the Access administrative portal.</td>
</tr>
<tr>
<td>UEM</td>
<td>Managed apps which use Tunnel, the Tunnel app, and configurations are pushed from UEM. Access gets device posture information from UEM.</td>
<td>Managed apps which use Tunnel, the Tunnel app, and configurations are pushed from UEM.</td>
</tr>
</tbody>
</table>
**TABLE 1. MOBILEIRON COMPONENT INTERACTION WITH MOBILEIRON ACCESS (CONT.)**

<table>
<thead>
<tr>
<th>MobileIron component</th>
<th>Access</th>
<th>Access + Standalone Sentry</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>authentication traffic to Access goes through Tunnel. To trigger Tunnel, apply the Tunnel VPN configuration to the managed apps and AppConnect apps.</td>
<td>authentication traffic to Access goes through Tunnel. To trigger Tunnel, apply the Tunnel VPN configuration to the managed apps and AppConnect apps.</td>
</tr>
<tr>
<td>Standalone Sentry</td>
<td>Not applicable.</td>
<td>Access gets device posture information from Standalone Sentry.</td>
</tr>
</tbody>
</table>

Standalone Sentry:  
- Gets the following from the MobileIron Access administrative portal  
  - SP and IdP federated pairings  
  - conditional rules for access control  
  - SSL certificates and signing certificates (X.509 certificate and corresponding private key)  
- Captures information on which users, devices, and apps authenticate to enterprise cloud service. This information is reported in the Access administrative portal.

Standalone Sentry Communicates with the MobileIron Access administrative portal on port 443.

Standalone Sentry syncs up with MobileIron Access at 15-minute intervals. To force update the configuration changes to Standalone Sentry, use the following CLI command in CONFIG mode: `accs config-fetch update`

---

**MobileIron UEM compliance actions and policies**

Policies configured in a MobileIron UEM define the checks on device posture and compliance actions if the device in non compliant. Access does the following if devices are out of compliance:

- **Access blocks connection to cloud service** if devices are non compliant (violate an UEM policy) and also have a blocking action set up against the corresponding policy. If there is a non blocking action (such as
email, monitor, notify) for a policy violation, Access does not take any action.

- For MobileIron Core and Connected Cloud, Access quarantines connection to cloud service if the devices are non compliant (violate an UEM policy) and also have a quarantine action set up against the corresponding policy.
  However, for MobileIron Cloud, Access does not take any action against a corresponding quarantine policy.

In addition, you can configure Access to revoke a session token if a device is non compliant. For more information on device compliance for session revocation, see About session revocation.

For more information on UEM compliance actions and policies, see the respective MobileIron Core or MobileIron Cloud guides.

Authentication flow with Access

The following describe the authentication flow with MobileIron Access.

- Managed non-AppConnect app using Tunnel
- AppConnect apps with Access enabled (Core only)

NOTE: This section is not applicable if you are deploying Access + Standalone Sentry.

Managed non-AppConnect app using Tunnel

The following describes the authentication flow when a managed non-AppConnect app accesses a enterprise cloud service.
1. A managed app triggers Tunnel.

2. If the device is in compliance, Tunnel establishes a secure connection with Access.

3. The managed app connects to the service provider (SP) through Tunnel.
   Split Tunneling is enabled: If split tunneling is enabled, and the split tunneling does not require tunneled connection to the service provider, the app connects directly with the service provider.

4. If the managed app does not have a valid session token, the SP issues a SAML 2.0 AuthN Request to the app and redirects the app to MobileIron Access.

5. MobileIron Access issues a secondary SAML AuthN Request based on the AuthN Request in step 4. The AuthN Request is issued via SAML and points the user to the identity provider (IdP).

6. If the user does not have a current valid session token, the identity provider (IdP) requests the user’s credentials. If the credentials match, the IdP issues a SAML Assertion to the user. The SAML Assertion identifies the user and redirects the user to MobileIron Access.

7. The user presents the SAML Assertion to MobileIron Access. If conditional rules for access control allow, MobileIron Access issues a secondary SAML Assertion to the user. The secondary SAML Assertion identifies the user and redirects the user to the cloud service (SP).

8. The user presents the secondary SAML Assertion to the cloud service (SP). The SP verifies the secondary SAML Assertion and creates a session token to the app. The session token gives the user access to the SP.
AppConnect apps with Access enabled (Core only)

AppConnect apps with Access enabled automatically use HTTP tunnel to MobileIron Access.

Authentication flow with Access + Standalone Sentry

The following describe the authentication flow in an Access + Standalone Sentry deployment.

- Managed non-AppConnect app using Tunnel and Standalone Sentry
- AppConnect apps using AppTunnel with Access + Standalone Sentry

Managed non-AppConnect app using Tunnel and Standalone Sentry

The following describes the authentication flow when a managed non-AppConnect app accesses an enterprise cloud service in an Access + Standalone Sentry deployment.

**Figure 2. Authentication Flow for a Managed Non-AppConnect App**

1. A managed app triggers Tunnel.
2. If the device is in compliance, Tunnel establishes a secure connection with Standalone Sentry.
3. The managed app connects to the service provider (SP) through Tunnel.
Split Tunneling is enabled: If split tunneling is enabled, and the split tunneling does not require tunneled connection to the service provider, the app connects directly with the service provider.

4. If the managed app does not have a valid session token, the SP issues a SAML 2.0 AuthN Request to the app and redirects the app to MobileIron Access on Standalone Sentry.

5. MobileIron Access issues a secondary SAML AuthN Request based on the AuthN Request in step 4. The AuthN Request is issued via SAML and points the user to the identity provider (IdP).

6. If the user does not have a current valid session token, the identity provider (IdP) requests the user’s credentials. If the credentials match, the IdP issues a SAML Assertion to the user. The SAML Assertion identifies the user and redirects the user to MobileIron Access.

7. The user presents the SAML Assertion to MobileIron Access on Standalone Sentry. If conditional rules for access control allow, MobileIron Access issues a secondary SAML Assertion to the user. The secondary SAML Assertion identifies the user and redirects the user to the cloud service (SP).

8. The user presents the secondary SAML Assertion to the cloud service (SP). The SP verifies the secondary SAML Assertion and creates a session token to the app. The session token gives the user access to the SP.

**AppConnect apps using AppTunnel with Access + Standalone Sentry**

Authentication traffic for managed apps goes to MobileIron Tunnel. For AppConnect apps that use AppTunnel, authentication traffic automatically goes through MobileIron Access. By default, AppTunnel traffic is trusted by MobileIron Access.

**After the user is authenticated in an Access deployment**

After a session token is created, data between the managed app or AppConnect app and the cloud service continues to flow through Tunnel and AppTunnel. Data does not flow through MobileIron Access. The user will have to authenticate again only after the expiration of the session token. The length of the session token is configured on the cloud service.

**Accessing the cloud service from a desktop, laptop, or an unmanaged device**

Conditional rules configured in Access can be used to define which apps and devices can authenticate with the cloud service provider (SP). You can configure a conditional rule to allow an unmanaged app to access the SP. By default, conditional rules are not applied to managed apps using Tunnel and to AppConnect apps using Tunnel or AppTunnel. The default conditional rule can be set to allow, block, or warn apps and devices if conditional rules do not match. If the default conditional rule is set to Allow when all other conditional rules do not match, authentication traffic will be allowed through Access. In this setup, the app will be able to authenticate with the IdP.

Access provides a set of predefined and customizable rules. For more information about conditional rules, see Conditional Access.
Setup overview for MobileIron Access

This section provides an overview of the setup required for implementing access control to cloud services using MobileIron Access and contains the following:

- Before you configure MobileIron Access
- Overview of steps to set up MobileIron Access
- Authentication options

Before you configure MobileIron Access

Before you start configuring MobileIron Access the following infrastructure setup is required:

- **Federated authentication**
  MobileIron Access supports federated authentication using SAML and WS-Fed. Refer to the documentation provided by your SP and IdP for information on how to set up federated authentication using SAML or WS-Fed.

- **Standalone Sentry enabled for AppTunnel**
  By default, MobileIron Access trusts all AppTunnel traffic.
  
  NOTE: Required only for a MobileIron Access + Standalone Sentry deployment.

- **MobileIron Tunnel or AppConnect**
  
  NOTE: AppTunnel is supported only with an Access + Standalone Sentry deployment.

- **App distribution**
  Managed apps are distributed through MobileIron Core or MobileIron Cloud.

For related documentation, see the following:

- **MobileIron Core documentation**
  For information on how to set up AppTunnel, AppConnect, Tunnel, and app distribution see the following documents: at:
  
  - For information on how to setup AppTunnel see the MobileIron Sentry Guide at [MobileIron Sentry Product Documentation](https://docs.mobileiron.com/miserv/.
  
  - For information on how to configure MobileIron Tunnel see MobileIron Tunnel Guide for Administrators at [MobileIron Tunnel for Android Product Documentation](https://docs.mobileiron.com/miserv/.
  
  [MobileIron Tunnel for iOS Product Documentation](https://docs.mobileiron.com/miserv/.
  
  [MobileIron Tunnel for macOS Product Documentation](https://docs.mobileiron.com/miserv/.

  - For information on how to set up an AppConnect app and how to distribute managed apps using MobileIron Core, see the following at MobileIron Core Product Documentation: AppConnect and AppTunnel Guide Apps@Work Guide

  Ensure that the MobileIron Tunnel (iOS) VPN setting is selected in the app configuration for non-AppConnect apps.
Overview of steps to set up MobileIron Access

The setup for MobileIron Access is done in the MobileIron Access administrative portal.

**Basic configuration**

1. Get started with the set up.
   See [Getting Started with MobileIron Access](#).
2. If your deployment uses Standalone Sentry, then register and assign Standalone Sentry to MobileIron Access.
   See [Set up Access + Standalone Sentry](#).
   OR
   If your deployment is Access (without Standalone Sentry), set up integration with MobileIron UEM.
   See [Set up Access with MobileIron UEM](#).
3. Set up a cloud service provider (SP) and identity provider (IdP) federated pair.
   See [Federated Pairs](#).
4. Upload Proxy metadata to the cloud service and identity provider.
   See [Uploading proxy metadata](#).
5. Publish the profile.
   See [Publishing a profile](#).
6. Verify traffic flow.
   See [Verifying traffic flow](#).

**Advanced configuration**

1. Set up conditional rules for access control. Conditional rules allow you to define which applications and IP network ranges can access a cloud resource.
   See [Conditional Access](#).
2. Set up session revocation, which allows you to terminate or revoke the session token if a device is out of compliance and the compliance action is blocked or a device is retired.
   See [Session Revocation](#).
3. Set up mobile app single sign-on (SSO) to allow users to access enterprise cloud services from their managed mobile devices without having to enter passwords. See Configuring Mobile App Single Sign-on (SSO).

4. Set up Zero Sign-on to allow users access to enterprise cloud services from their unmanaged devices without having to enter passwords. See Fast Identity Online (FIDO2) or Zero Sign-on with MobileIron Access.

5. Set up multi-factor authentication using the UEM client to allow users to access their enterprise cloud services from an unmanaged device using multi-factor authentication in addition to their enterprise credentials. See Multi-factor Authentication with MobileIron UEM Client.


Split tunneling configuration

In a MobileIron Access deployment, all authentication traffic for the federated pairs configured in MobileIron Access goes through MobileIron Access using MobileIron Tunnel VPN. Depending on the type of MobileIron Access deployment, all other traffic through Tunnel VPN goes directly to the destination server or through Standalone Sentry. Split tunneling allows you to control which traffic goes through Standalone Sentry to on-premise enterprise resources and which traffic goes directly to the destination.

For information about configuring Access as the delegated IdP, see Split Tunneling.

Delegated IdP

In most cases, MobileIron Access is deployed as an intermediary between the service provider (SP) and the identity provider (IdP). In such a deployment, MobileIron Access acts as a proxy to the IdP and all federated SP traffic goes through MobileIron Access. In some cases, you may want to retain the existing SP-IdP federated setup, but deploy MobileIron Access to federate a sub set of the traffic, such as traffic from mobile devices. In such cases MobileIron Access can be deployed as a delegated IdP rather than as a proxy to the IdP.

For information about configuring split tunneling, see Delegated IdP.

Authentication options

With a basic Access setup, when users initially attempt to log in to an enterprise cloud service from their managed device, they are prompted for their username and password. In addition, Access allows you to set up various authentication options to allow your users ease of access from both managed and unmanaged devices to enterprise cloud services. The following table describes these options. See Advanced configuration for information on how to set up the various authentication options.
## Table 2. Authentication Options

<table>
<thead>
<tr>
<th>Feature</th>
<th>Purpose</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile app single sign-on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Native mobile application single sign-on (SSO)</td>
<td>Password less access from managed device.</td>
<td>Users do not need to enter their username and password.</td>
</tr>
<tr>
<td>SaaS sign-on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zero Sign-on</td>
<td>Password less access from managed device.</td>
<td>Users do not need to enter their username and password.</td>
</tr>
<tr>
<td></td>
<td>Password less access from unmanaged devices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A QR code is presented to users attempting to access a cloud service from their unmanaged device. Scanning the QR code with their managed device authenticates the user and allows access from the unmanaged device. Users have the option to enable push notifications or one-time passcode (OTP). If enabled, a push notification is sent to the managed device on subsequent logins from the unmanaged device. Alternately, users can use OTP. Users do not need to enter their username and password.</td>
<td></td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>Access from unmanaged devices.</td>
<td>Two factor authentication allows users to access cloud services from unmanaged devices. Users enter their username and password on the unmanaged device. If accepted, users can access the cloud service from their unmanaged device. Alternately, users can use OTP.</td>
</tr>
<tr>
<td>Desktop trust agent</td>
<td></td>
<td>The MobileIron desktop trust agent verifies and establishes trust for unmanaged Windows 7 and Windows 10 desktops, thus allowing access to cloud services</td>
</tr>
</tbody>
</table>
Getting Started with MobileIron Access

The following topics let you configure MobileIron Access:

- Before you set up MobileIron Access
- Working with MobileIron Access administrative portal
  - Changing the password
  - Resetting the password recovery key
  - Configuring 2-step verification
- Working with MobileIron Access in Cloud administrative portal
  - Changing the Password for Cloud portal
  - Admins
- MobileIron Access Global Dashboard

Before you set up MobileIron Access

Verify that you have the following items before configuring MobileIron Access.

- Deployment Type
- Federated authentication
- MobileIron Access credentials
- Standalone Sentry information
  Gather Standalone Sentry information if you plan to have Standalone Sentry in your MobileIron Access deployment.
- Certificates for Access + Standalone Sentry
- Signing certificate

Deployment Type

MobileIron Access supports deployment with Standalone Sentry or Access (as a service). Before you begin with MobileIron Access, ensure that you understand the deployment types.

For more information, see MobileIron Access overview.
Federated authentication

MobileIron Access supports federated authentication using SAML and WS-Federation.

Before you begin with MobileIron Access, ensure that you are able to login to every service provider you intend to use with Access using federated identity from your identity provider(s).

NOTE: Federated authentication setup is not required for implementing certificate-based SSO with MobileIron Access.

MobileIron Access credentials

When you sign up for MobileIron Access, an email is forwarded to you by your sales representative.

The email contains the following important information that you will need for accessing the system:

- URL for the MobileIron Access administrative portal
- Local administrator login credentials

Be sure to retrieve the information in the email before proceeding.

Root Admin credentials lets you perform the following tasks:

- Sign in to MobileIron Access administrative portal
- Create cloud service provider (SP) and identity provider (IdP) federated pairs
- Set up access control rules
- User management
- Activate or deactivate admins
- Self Serve
- Configuration Management
- Analytics and Dashboard
- Register Standalone Sentry
- View reports

Standalone Sentry information

If your deployment is Access + Standalone Sentry, add a secondary hostname to the Standalone Sentry you use for access control. The primary DNS FQDN is reserved for Standalone Sentry for AppTunnel. The secondary hostname will be reserved for the MobileIron Access module on the Standalone Sentry. You will use the second hostname when you first log in to the MobileIron Access administrative portal and go through the setup wizard.
Certificates for Access + Standalone Sentry

Ensure that you have an SSL certificate to use with MobileIron Access. You will also require signing certificates when you set up a cloud service provider (SP) and identity provider (IdP) federated pair.

SSL certificate for MobileIron Access

The SSL certificate must be in PKCS 12 format and issued by a publicly trusted certificate authority (CA). The issuer can be an intermediate or root CA. The common name (CN) in the certificate must be exactly the same name as the second hostname reserved for the MobileIron Access module on Standalone Sentry. You will upload this certificate when you go through the setup wizard.

Generating an SSL certificate (PKCS12 file) for MobileIron Access

If you don’t already have a PKCS12 file, you can use OpenSSL to generate a PKCS12 file. Ignore this section if you already have a PKCS12 file.

Execute the following commands to generate a PKCS12 file:

1. Generate a certificate signing request (CSR) to submit to a certificate authority (CA). Enter the following command in OpenSSL:

   ```bash
   openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key
   ```

2. Forward the CSR.csr file to the CA for signing. The CA returns a .crt (example: certificate.crt) file.

3. Combine the certificate and private keys into a PKCS12 file.
   To combine the certificate and private keys into a PKCS12 file, enter the following OpenSSL command:

   ```bash
   openssl pkcs12 -export -out certificate.p12 -inkey privateKey.key -in certificate.crt -certfile CA_Cert.crt
   ```

   - CACert.crt contains the CA’s cert chain that signed certificate.crt.
   - You will be asked for an export password. You will use the export password when you upload the certificate in MobileIron Access.

Signing certificate

MobileIron Access uses signing certificates to sign authentication requests and SAML assertions. A default signing certificate specific to your Access instance is automatically provided. When you set up a federated pair in the MobileIron Access administrative portal, you are also provided with the option to either generate a new signing certificate or upload a certificate of your choosing. If you do not want to use the default certificate, you can use the option to generate or upload a new certificate. For more information, see Federated Pairs.

NOTE: The SSL certificate should not be used in lieu of a signing certificate.
Working with MobileIron Access administrative portal

You can access the MobileIron Access administrative portal from a web browser. Use the credentials provided in the welcome email to sign in to the MobileIron Access administrative portal.

If you wish to use the new user interface, see Working with MobileIron Access in Cloud administrative portal.

**Procedure**

1. In a supported browser, enter the MobileIron Access URL provided in the welcome email. 
   Example: https://access-na1.mobileiron.com
   The URL may vary depending on the region.
   
   **NOTE:** Administrator accounts lock temporarily for a short period after multiple consecutive invalid password attempts on initial log in.

2. For **Username**, enter the email address provided in the Welcome email.
3. For **Password**, enter the password provided in the Welcome email.
4. Click **Sign In**. The **Change Password** window displays.
5. For **Current Password**, enter the password provided in the Welcome email.

6. For **New Password**, enter a new password.

7. For **Confirm New Password**, re-enter the same password that was used for **New Password** and click **Done**. The log in screen appears. Enter the new credentials to log in to MobileIron Access.

8. Enter the new password to log in to MobileIron Access.
   - The **Password Recovery Key** window displays, which provides options for receiving the password recovery the key.
9. Enter the **New Password** in the text box.

10. Select one of the following options to backup your Recovery Key.

   - **Email Recovery key**: This option lets you email the Password Recovery Key to your administrator email address.
   
   - **Copy Recovery key**: This option lets you copy the Password Recovery Key to a file in your local drive. A warning to receive an email for recovery key appears when you click Copy Recovery Key option.

### Figure 6. WARNING FOR PASSWORD RECOVERY KEY

A Password Recovery Key is generated which is needed in the event the admin forgets their password. Without the Recovery Key you will not be able to reset your forgotten password and MobileIron will have to reset your tenant by deleting your tenant data.

You must copy the Recovery Key on the next screen and take a screenshot.

After login, if you forget your password, click **Account Settings > Change Password**. The window to change your password opens. You must use the password recovery key to change your password.

**IMPORTANT**: If you forget your password and lose your password recovery key, you will not have access to the Access administrative portal. Contact the Root Admin or the Super Admin to reset the password. If the Root Admin forgets the password, contact MobileIron Support.

11. Click **OK > Generate Key**.
12. **Click Continue to get started with the setup wizard.**

**FIGURE 7. SETUP WIZARD**

13. **Click Get Started to select the preferred deployment type.**
   
The screen to select **Access** or **Access + Standalone Sentry** appears.

   **IMPORTANT:** Once you select the deployment type and click **Done**, you will not have the option to change your selection.

**FIGURE 8. SELECT DEPLOYMENT TYPE**
14. Click **Done**.

15. Click **人事** to start configuring account settings.

The email for the administrator account and the Tenant GUID is visible.

**Figure 9. Account Settings**

Next steps

- For an Access (without Standalone Sentry) deployment, see Set up Access with MobileIron UEM.
- For an Access + Standalone Sentry deployment, see Set up Access + Standalone Sentry.

Related topics

- Changing the password
- Resetting the password recovery key
- Configuring 2-step verification
- MobileIron Access Global Dashboard
Changing the password

After you initially sign in to the MobileIron Access administrative portal using the credentials provided by MobileIron, you may want to change the password. Your enterprise security policies may require you to change your password periodically.

When you attempt to enter a password for more than six times, the account is locked. You must wait for sometime to log in again.

NOTE: After login, if you forget your password, click Account Settings > Change Password. The window to change your password opens. You must use the password recovery key to change your password.

Procedure
1. In the MobileIron Access administrative portal, click Account Settings > Change Password. The Change Password dialog appears.
2. For Current Password, enter the current password.
3. For New Password, enter the new password.
4. For Confirm New Password, re-enter the new password.
5. Click Done.

Password requirements

A new password must match the following requirements:
• Password length should be between 8 and 32 characters
• No spaces
• Not more than 2 identical characters in a row (For example: 111 not allowed)
• Sequential characters are not allowed (For example: 123 or abcde)
• At least one lower case letter (a-z)
• At least one upper case letter (A-Z)
• At least one number (0-9)
• At least one symbol [~ ! @ $ % ^ & * ( ) _ + : ; < > ? { ] ]

Resetting the password recovery key

You can change the password recovery key in the MobileIron Access administrative portal.

Procedure
1. In the MobileIron Access administrative portal, click Account Settings > Reset Password Recovery Key. The Password Recovery Key dialog appears.
2. Enter your password in the text box.
3. Select one of the following options to backup your Recovery Key.
   - **Email Recovery Key**: This option emails the Password Recovery Key to your admin email address.
   - **Copy Recovery Key**: This option lets you copy the Password Recovery Key to a file in your local drive.
     You can use this key to recover your password in case you forget the password.
4. Click **Generate Key**.

**NOTE**: If you forget your password and lose your password recovery key, you will not have access to the Access administrative portal.

**Resetting your password**

The password recovery key is required to reset the password from the log in screen. However, when a tenant logs in, recovery key is not required to reset the password. You cannot reuse the last three passwords including the current password when you reset a password.

**Procedure**

1. On the MobileIron Access Log in page, click **Reset Password**. You will be prompted to create a new password.
2. For **Username**, enter your username.
3. For **Recovery Key**, enter your password recovery key. You can copy and paste the key.
4. For **New Password**, enter a new password.
5. For **Confirm New Password**, re-enter the new password.
6. Click on **Reset Password**. You will be returned to the Sign In dialog.
7. Enter the new password to sign in to the Access administrative portal.
Resetting your password can sometimes fail for the following reasons. Ensure that you check the error and verify the reason.

- Invalid recovery credentials
- Account could be in either ‘Deactivated’ or ‘Require Password Change’ state

Configuring 2-step verification

2-Step verification adds another layer of security that requires not only a password and user name but also a verification code to sign in to the MobileIron Access administrative portal. The verification code is generated by either MobileIron Authenticator or Google Authenticator. You configure 2-step verification in the MobileIron Access administrative portal.

You can enable 2-step verification only for your account. You cannot enable 2-step verification for other administrators or vice versa. If 2-step verification is enabled, you are prompted to enter your credentials and the verification code to access MobileIron Access account. If the verification code is not available, you cannot sign in to the Access administrative portal.

Note The Following:
- 2-Step verification with Google Authenticator is supported on iOS and Android devices. 2-Step verification with MobileIron Authenticator is supported only on iOS devices.
- If 2-Step verification fails, verify if your device is in sync with the local time

Before you begin
- Verify that you have created a MobileIron Access account.
• For iOS devices, verify that you have downloaded the MobileIron Authenticator app or Google Authenticator app from iOS App Store.
  OR
For Android devices, verify that you have downloaded the Google Authenticator app from Android Google Play Store.

Procedure
1. In the MobileIron Access administrative portal, click **Account Settings > 2-Step Verification**.
2. Click the **Off** toggle.
   A **Warning** is displayed.
3. To configure 2-step verification, click **Continue**, then **Next**.
   A QR code is displayed.

**FIGURE 10. QR CODE FOR 2-STEP VERIFICATION**

--- Back to list

<table>
<thead>
<tr>
<th>2-Step Verification</th>
<th>Cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Authenticator</td>
<td></td>
</tr>
<tr>
<td>Setup Authenticator</td>
<td></td>
</tr>
<tr>
<td>Enable 2-Step Verification</td>
<td></td>
</tr>
</tbody>
</table>

**Setup Authenticator app**
Scan the QR below
Once in the Authenticator app scan the QR with your phone camera.

![QR Code]

*Can't scan the QR Code? Enter Time based Secret Key*

**Secret Key**

QF2XOZM5KFFLYK6G3U62DPL0DEUQ5G

4. On your device, launch the authenticator app.
5. From the authenticator app, scan the **QR code** displayed in MobileIron Access.
   
   Alternately, for Google Authenticator only, click the **Enter Time based Secret Key** link to generate a secret key. Enter the generated secret key in Google Authenticator. The secret key is unique to every verification. A 6-digit code is generated in the authenticator app.
6. In the Access administrative portal, click **Next** to enter the 6-digit code.
7. In **Enable 2-Step Verification** enter the 6-digit code.

8. Click **Done**.

To verify whether 2-step verification is on or off, in MobileIron Access, go to **Settings > Admins**. The **2-Step Verification** column displays the status.

To generate a verification code for 2-step verification for signing in to MobileIron Access:
- If you are using Google Authenticator, launch the app.
- If you are using MobileIron Authenticator, launch the app, and go to **Settings > Admin OTP**.

**Disabling 2-Step Verification**

Administrators can disable 2-step verification for their own account only. However, a **Super Admin** can disable 2-step verification for an **Admin** or **Read Only Admin**. If an administrator with **Admin** or **Read Only Admin** role loses their phone or has issues with 2-step verification, they can contact their Access **Super Admin** to reset 2-step verification for their account. If a **Super Admin** is not available, contact MobileIron Support. An email notification is sent to the administrator if a Super Admin or MobileIron Support disables 2-step verification for an account. However, email notification is not sent when administrators disable the 2-Step Verification for their own account. For more information about administrator roles, see **Admins**.

2-Step verification can be disabled from **Account Settings > 2-Step Verification** in the admin portal.

**Before you begin**
- Verify that 2-Step Verification is enabled.

**Procedure1**
1. In the MobileIron Access administrative portal, go to **Account Settings > 2-Step Verification**.
2. Click the toggle to change the setting to **OFF**.

**Procedure2**
1. In the MobileIron Access administrative portal, click **Settings > Admins**.
2. Click the toggle in the 2-Step Verification column for your account to change the setting to **OFF**.

**NOTE:** This method is not available to administrators with Read-only permission.
Signing out of the MobileIron Access administrative portal

If you do not sign out, the session will timeout in 30 minutes.

Procedure
1. In the MobileIron Access administrative portal, click Account Settings > Sign Out.

When you sign in to Access again, launch an authenticator app and generate a verification code. You will be prompted to enter the verification code in addition to your username and password.

Working with MobileIron Access in Cloud administrative portal

You can access the MobileIron Access administrative portal from a web browser. If your MobileIron deployment uses MobileIron Cloud, sign in with your MobileIron Cloud credentials. If your MobileIron deployment uses MobileIron Core, use the credentials provided in the welcome email to sign in to the MobileIron Access administrative portal.

The features such as resetting the password recovery key and configuring 2-step verification are not supported for Access in the Cloud administrative portal.

Procedure
1. In a supported browser, enter the URL for your MobileIron Cloud tenant.
   Example: https://na2.mobileiron.com/login.html
   For Access: login.mobileiron.com
   The URL will vary depending on your region.
2. Enter your Cloud administrator account.

3. Click **Sign In** and enter the Password.
4. Click **Sign In** again.
   The MobileIron Cloud portal opens.
5. Click the **Access** tab to view the admin portal.
6. Click **Get Started** to select the preferred deployment type.
   The screen to select **Access** or **Access + Standalone Sentry** appears.
   **IMPORTANT:** Once you select the deployment type and click **Done**, you will not have the option to change your selection.

7. Select the deployment type as **Access** or **Access + Standalone Sentry**.
Access is configured and the Access admin portal opens.

8. Click 🔄 to start configuring account settings.
   The email for the administrator account and the Tenant GUID is visible.
- For an Access (without Standalone Sentry) deployment, see Set up Access with MobileIron UEM.
- For an Access + Standalone Sentry deployment, see Set up Access + Standalone Sentry.

**Account settings**

Click **Access > Account** to view the links to documentation, support, your Access tenant GUID, your administrator account information, and links to change your password and sign out.

![ACCOUNT SETTINGS](image.png)
Changing the Password for Cloud portal

After you initially sign in to the MobileIron Cloud administrative portal using the credentials provided by MobileIron, you may want to change the password. Your enterprise security policies may require you to change your password periodically.

When you attempt to enter a password for more than six times, the account is locked. You must wait for sometime to log in again.

NOTE: If you forget your password, click Forgot Password in the log in page. An email is sent to the user associated with the username with instructions to reset the password.

Procedure
1. In the MobileIron Access administrative portal, click Account Settings > Change Password. The Change Password dialog appears.

2. For Current Password, enter the current password. The password requirements are listed when you click to enter the password.
3. For New Password, enter the new password.
4. For Confirm New Password, re-enter the new password.
5. Click Done.

Related topics
- Changing the Password for Cloud portal
**Admins**

The **Admins** tab lets you create and delete profiles for administrators to manage the Access portal. It also lets you activate and deactivate (enable or disable) the administrators.

**NOTE:** The Reset Password and 2-Step verification is not available for Admins with Access Cloud portal.

When a new Admin is created, you will receive an email with an activation link to reset the password.

Admins added in the Access tab will not have any Cloud role. They will only see the Access tab. Admins added in the Cloud tab may have Access roles as well as Cloud roles depending on what they are assigned.

The following options are not available in the Cloud portal:

- The Status column is not available for the Admin created.
- The reset admin password option is also removed in Cloud portal.
For more information on Adding an administrator, creating and deleting profiles, see Admins.

MobileIron Access Global Dashboard

The MobileIron Access Global Dashboard is designed to support data management. The dashboard is categorized into sections such as Authenticated Users, Authentication Requests, Secured Cloud Services, Secured Mobile Apps, Authenticated Users & Authentication Requests, Top Secured Services, Top Services By Authenticated Users, Mobile Apps Blocked, and Block & Allow Requests.

You can view the dashboard data for any preferred period. The dashboard displays real time data when the reports are submitted to MobileIron Access by Sentry. It takes about 15 minutes to refresh the data.

You can click on the trend graphs to fetch the overlay card for a preferred date. The overlay card displays the report for the appropriate date you selected. To view the complete report, click View All Data. The Reports tab displays the complete report.

Each data set on the dashboard can be viewed in multiple different graphical formats, such as a bar graph, line graph, pie graph, or in a tabular format. The tabular form also displays the time that the data is aggregated by Coordinated Universal Time (UTC).
## Table 3. Data Description

<table>
<thead>
<tr>
<th>Sections</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated Users</td>
<td>Provides the number of allowed or blocked users that are authenticated by the identity providers.</td>
</tr>
<tr>
<td>Authentication Requests</td>
<td>Provides the number of allowed or blocked requests that are targeting the cloud services. It also provides information about the requests that have processing exceptions.</td>
</tr>
<tr>
<td>Secured Cloud Services</td>
<td>Provides information about Federated Pairs. Each active Federated Pair is a service.</td>
</tr>
<tr>
<td>Secured Mobile Apps</td>
<td>Provides the number of unique applications that are accessed by the user.</td>
</tr>
<tr>
<td>MobileIron Authenticate Registered</td>
<td>Provides the number of MobileIron Authenticate registered desktops. It helps the admin view the percentage of desktops they intend to have registered and then accordingly admin can register more desktops.</td>
</tr>
<tr>
<td>Authenticated Users &amp; Authentication Requests</td>
<td>Provides a graphical representation for the authenticated users and requests trends.</td>
</tr>
<tr>
<td>Top Secured Services</td>
<td>Provides the number of blocked requests based on the top secured services.</td>
</tr>
<tr>
<td>Top Services By Authenticated Users</td>
<td>Provides the number of authenticated users for every service.</td>
</tr>
<tr>
<td>Mobile Apps Blocked</td>
<td>Provides a graphical representation about the blocked services.</td>
</tr>
<tr>
<td>Allow, Block &amp; Warn Requests</td>
<td>Provides a graphical representation about the allowed and blocked hits based on any appropriate combination such as Rule, SAML pair, and policies. It also provides information about the warn requests to secured cloud services using specific policies and rules.</td>
</tr>
<tr>
<td>Authentication by OS Platforms</td>
<td>Provides a graphical representation about the Service Provider actions by aggregate OS such as iOS, Android, Windows, Macintosh, Linux, and other unknown platforms.</td>
</tr>
<tr>
<td>Authentication by Managed Apps</td>
<td>Provides a graphical representation about the list of Managed Apps that are accessing the Service Provider.</td>
</tr>
</tbody>
</table>

**NOTE:** When a managed app that is not available in MobileIron Access database is accessed, a bar named Unknown is displayed in the graph. These apps will be monitored and added to the database in the future releases.
GeolP Map

The Allow, block, and warn requests data to secured cloud services is available based on geolocation. In the Allow, Block, and Warn Requests section of the dashboard, click ⌁ to view geolocation.

GeoIP identifies the location and other characteristics such as overlay card displaying IP address, username, time stamp of MobileIron end users for a wide range of applications including content personalization, fraud detection, traffic analysis, and compliance. The GeoIP map provides the following features:

- Count of Allow/Block/Warn requests
- Zoom in and Zoom out to have better precision of the data
- Horizontal scrolling to view a particular section of the map
- Filters to narrow down the data set
- Checkboxes to select Allow, Block, or Warn requests

Note The Following:
- The geolocation data in some cases may not provide the exact location.
- To see individual Rule Action, select only one check box.
- Some activity dots may appear off the continental maps. Zoom in for accurate locations.

FIGURE 13. GELOCATION FOR ALLOW, BLOCK, AND WARN REQUESTS

Viewing details for allow, block, or warn requests

The Allow, Block, or Warn requests are displayed on the GeoIP map at various locations. You can determine the users logged in from a specific location to assess and mitigate the risks. Clarity is provided through reverse lookup. When you mouse over the Geo bubble, the callout which appears, displays the count of Allow, Block, and Warn requests.

Procedure
1. On the GeoIP map, click the Geo Bubble for Allow, Block, or Warn request.
The Allow Requests, Block Requests, or Warn Requests window displays based on your selection.

**Figure 14. Request Details**

### Allow Requests

<table>
<thead>
<tr>
<th>TIMESTAMP</th>
<th>POLICY</th>
<th>RULE</th>
<th>SOURCE IP</th>
<th>USERNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017/11/28</td>
<td>Policy 1</td>
<td>General Bypass</td>
<td>9e938b3100a</td>
<td><a href="mailto:2a133c51441@example.com">2a133c51441@example.com</a></td>
</tr>
<tr>
<td>2017/11/28</td>
<td>Policy 1</td>
<td>General Bypass</td>
<td>8a93a024ac3a</td>
<td><a href="mailto:cb56ed033b@example.com">cb56ed033b@example.com</a></td>
</tr>
<tr>
<td>2017/11/28</td>
<td>Policy 1</td>
<td>General Bypass</td>
<td>32ef563958c</td>
<td><a href="mailto:cc176ba1cd8@example.com">cc176ba1cd8@example.com</a></td>
</tr>
<tr>
<td>2017/11/28</td>
<td>Policy 1</td>
<td>General Bypass</td>
<td>81009533165</td>
<td><a href="mailto:980a1e2a84@example.com">980a1e2a84@example.com</a></td>
</tr>
<tr>
<td>2017/11/28</td>
<td>Policy 1</td>
<td>General Bypass</td>
<td>da8583e36c2</td>
<td><a href="mailto:9d8943de6@example.com">9d8943de6@example.com</a></td>
</tr>
<tr>
<td>2017/11/28</td>
<td>Policy 1</td>
<td>General Bypass</td>
<td>79bf9c8539e</td>
<td><a href="mailto:60238380cc8@example.com">60238380cc8@example.com</a></td>
</tr>
</tbody>
</table>

2. **Click View All Data.**

   The Reports page opens to display the Geolocation details.
Set up Access with MobileIron UEM

MobileIron Access integrates with a MobileIron unified endpoint management (UEM) platform to get device posture and compliance information. To set up the integration, you configure MobileIron Access integration in the MobileIron UEM and verify the integration in MobileIron Access. The MobileIron UEM are:

- MobileIron Core
- MobileIron Cloud
- MobileIron Connected Cloud

You can integrate up to six MobileIron Cloud instances, multiple MobileIron Core servers (no limit), and multiple MobileIron Connected Cloud instances (no limit) in your deployment.

Unless otherwise noted, the documentation for MobileIron Core generally applies for Connected Cloud as well. For the most recent documentation available for Connected Cloud, see Previous Versions from MobileIron Core Documentation.

NOTE: The configuration with UEM described in these sections only apply to Access (without Standalone Sentry) deployments.

Overview of configuration with MobileIron Cloud

Complete the following tasks to set up MobileIron Cloud integration with Access:

1. Configuring Access in MobileIron Cloud
2. Configuring MobileIron Cloud in Access
3. Configuring MobileIron Tunnel in MobileIron Cloud

Configuring Access in MobileIron Cloud

Set up Access on MobileIron Cloud.

Before you begin

- Make a note of the URL for your Access instance, and the Access administrator username and password. The URL for your Access instance is one of the following:
  - https://access-na1.mobileiron.com
  - https://access-eu1.mobileiron.com
- Ensure that you have Manage MobileIron Access Integration role in MobileIron Cloud.
- You have the credentials for the Access administrator account you will use to set up Access in MobileIron Cloud. MobileIron recommends creating a separate administrator account in Access that is specifically used for UEM integration with Access. Ensure that the account does not have 2-step verification enabled.
Procedure

1. In MobileIron Cloud, go to Admin > Access.

**Figure 15. Configure access on MobileIron Cloud**

![Configuration interface for MobileIron Access](image)

2. Enter the following:
   - **Access Admin URL**: URL for Access
   - **Access Admin Username**: User name for the Access administrator account you created for Access integration.
   - **Access Admin Password

3. Click **Register**.

   Access is registered with MobileIron Cloud and the following displays:

**Figure 16. MobileIron Access Registration**

![Registration confirmation](image)

**Next steps**

Configuring MobileIron Cloud in Access.
Related topics
See the MobileIron Cloud Administrator Guide for information about setting roles.

Configuring MobileIron Tunnel in MobileIron Cloud

MobileIron Tunnel creates a secure connection between the managed device and MobileIron Access for authenticating users accessing enterprise cloud resources.

Before you begin

- Add a Certificate Authority and create an Identity Certificate setting in MobileIron Cloud.
  - Add the Certificate Authority in Admin > Certificate Authority.
  - Create an Identity Certificate setting in Configuration > Add > Identity Certificate. For Certificate Distribution, select Dynamically Generated and for Source, select the certificate you configured in Admin > Certificate Authority.
- If you were using a Sentry profile to configure Access in MobileIron Cloud, reconfigure your setup to use an Access profile before deploying MobileIron Tunnel 3.1.0 for iOS through the most recently released version as supported by MobileIron. To set up an Access profile, see Configuring Access in MobileIron Cloud.
- For Android enterprise, app configuration is done when adding the app to the UEM for distribution. The following procedure applies to all supported OS except Android enterprise. However, configuration information provided in this procedure also applies when you configure Android enterprise. For information on how to add MobileIron Tunnel for Android enterprise to MobileIron Cloud, see the relevant section in the MobileIron Tunnel Guide for Administrators.
  
  NOTE: If you are configuring Tunnel for Android enterprise and using MobileIron Access Profile only, MobileIron recommends adding configuring AllowedAppList to specify the apps for which authentication traffic goes through Tunnel.

Procedure

1. In MobileIron Cloud, go to Configurations > +Add.
2. Search for MobileIron Tunnel and click MobileIron Tunnel.
3. Select the OS type for the configuration.
4. Create a separate Tunnel configuration for each OS type.
5. Enter a name for the configuration.
6. Select one of the following:
   a. MobileIron Access Profile Only - Select if Tunnel traffic goes only to Access.
   b. MobileIron Sentry + Access Profile - Select if Tunnel VPN supports both traffic to Access for authentication to enterprise cloud resources and through Standalone Sentry to on-premise enterprise resources. This option is available for iOS and Android only.
Figure 17. Profile mode selection

Configuration Setup

| iOS 7+ & macOS 10.13+ |

Profile selection mode to use for this configuration:

- MobileIron Sentry Profile Only
- MobileIron Access Profile Only
- MobileIron Sentry + Access Profile

Note: Changes to profile selection mode will clear any existing Sentry, Access and SCEP selections. This will result in needing to reconfigure the settings again.

7. If you selected MobileIron Sentry + Access Profile for profile mode, select the Sentry profile and the iOS or Android service you created in the Sentry profile.

8. For a Tunnel for Android configuration, do the following:
   a. For Client Cert. Alias, for Tunnel for Android only, select the same certificate configuration you select for SCEP Identity.
   b. For SCEP Identity, select the Identity Certificate configuration you created for Tunnel.

9. For a Tunnel for Windows 10 configuration, do the following:
   a. For SCEP Identity, select the Identity Certificate configuration you created for Tunnel.
   b. For Define Tunnel App Settings, select Advanced.
   c. Enter the following key-value pairs:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
</table>
| AppTriggerList/0/App/Id     | App Id that will trigger Tunnel. Example:
                              | %PROGRAMFILES%(x86)\Google\Chrome\Application\chrome.exe             |
| TrafficFilterList/0/App/Id  | App Id that will tunnel traffic through Tunnel. Example:
                              | %PROGRAMFILES%(x86)\Google\Chrome\Application\chrome.exe             |
| RouteList/0/Address         | If your Cloud tenant is *.access-na1.mobileiron.com enter:
                              | 18.232.253.154                                                        |
                              | If your Cloud tenant is *.access-eu1.mobileiron.com enter:
                              | 18.194.253.44                                                         |
### Key Value

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RouteList/0/PrefixSize</td>
<td>32</td>
</tr>
<tr>
<td>TrafficFilterList/0/RoutingPolicyType</td>
<td>SplitTunnel</td>
</tr>
<tr>
<td>RouteList/1/Address</td>
<td>If your Cloud tenant is *.access-na1.mobileiron.com enter: 18.232.30.29</td>
</tr>
<tr>
<td></td>
<td>If your Cloud tenant is *.access-eu1.mobileiron.com enter: 18.194.99.243</td>
</tr>
<tr>
<td>RouteList/1/PrefixSize</td>
<td>32</td>
</tr>
</tbody>
</table>

10. Leave all defaults as is and click **Next**.

**NOTE:** If you are configuring Tunnel for Android enterprise and using *MobileIron Access Profile only*, MobileIron recommends adding configuring **AllowedAppList** to specify the apps for which authentication traffic goes through Tunnel.

11. Select the distribution for the configuration and click **Done**.

12. In MobileIron Access,
   a. Navigate to the **UEM** tab.
   b. Select the Cloud UEM and click the **Sync UEM** button.
   c. Enter the credentials and click **Verify** and **Done**.

   This step is required to pull the Tunnel certificates from the UEM and established trust between Tunnel and Access.

**Next steps**

1. Add MobileIron Tunnel to MobileIron Cloud. For information on how to add MobileIron Tunnel to MobileIron Cloud, see the relevant section in the *MobileIron Tunnel Guide for Administrators* for the device OS.
2. Set up SP and IdP federated pairs.
   See [Service provider (SP) metadata](#) and [Identity provider (IdP) metadata](#).

**Related topics**

For more information about configuring and distributing MobileIron Tunnel see the *MobileIron Tunnel Guide for Administrators* for the OS.

### Configuring MobileIron Cloud in Access

You configure your Access tenant in MobileIron Cloud and verify the integration in Access in the **UEM** tab.

**Before you begin**

Ensure the following:
Your Access tenant is configured in MobileIron Cloud. See Configuring Access in MobileIron Cloud.

You have the credentials for the MobileIron Cloud administrator account you will use to verify the connection from Access to Cloud. MobileIron recommends creating a separate administrator account in MobileIron Cloud that is specifically used for UEM integration with Access. Ensure that the account,

- is a single user, not an API user.
- has Access administrator, Common Platform Service (CPS), and Device Read Only roles.

**Procedure**

1. Click **UEM** on the left navigation pane in Access.

![Figure 18. UEM Tab](image)

2. In MobileIron UEMs tab, click **Connect to Verify** to complete the UEM registration process. The Verify UEM Tenant window appears.

![Figure 19. Verify UEM Tenant](image)

3. Enter the following:

   - **UEM Username**: User name for the MobileIron Cloud administrator account you created for Access integration.
• **UEM Password**: Password for the administrator account.

The following status displays in MobileIron Access based on the connection:

Table 4. UEM Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Access and Cloud are connected.</td>
</tr>
<tr>
<td>Not Verified</td>
<td>The Cloud Credentials are not verified by Access. Enter the credentials to complete the workflow.</td>
</tr>
<tr>
<td>Deregistered</td>
<td>Access is deregistered.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Server is unable to connect to MobileIron Cloud.</td>
</tr>
<tr>
<td>Incorrect Password or Permissions</td>
<td>The UEM permissions or password is incorrect.</td>
</tr>
</tbody>
</table>

4. Click **Verify**.
5. Click **Done**.
6. Select the host added and click **Sync UEM** in the right-pane.
   This action fetches the Tunnel profiles from UEM and pushes to gateway.

**Next steps**

**Overview of configuration with MobileIron Core**

Set up MobileIron Core integration with Access configuration in the following order:
• Configuring Access in MobileIron Core
• Configuring MobileIron Tunnel in MobileIron Core
• Configuring MobileIron Core in Access

**NOTE:** Unless otherwise noted, the instructions for MobileIron Core generally apply for Connected Cloud as well.

**Configuring Access in MobileIron Core**

Configure Access in MobileIron Core.

**Before you begin**
• Add a **Certificate Enrollment** setting in MobileIron Core. You will upload the associated CA certificate in Access to establish trust between Tunnel and Access.
  For more information about **Certificate Enrollment** settings, see the MobileIron Core Device Management Guide for your device operating system. For Android enterprise, see the MobileIron Core Device Management Guide for Android.
• Ensure that you have **Manage MobileIron Access Integration** and **Common Platform Services (CPS)** roles enabled in MobileIron Core. To enable roles, in the MobileIron Core Admin Portal, go to **Admin > Admins > select the administrator > click Actions > Edit Roles**.

**NOTE:** After updating roles, sign out and then sign in again to the MobileIron Core Admin Portal for the changes to take effect.

• Ensure that 2-step verification is turned off for the administrator in Access.

• Make a note of the URL for your Access instance, and the Access administrator username and password. The URL for your Access instance is one of the following:
  - https://access-na1.mobileiron.com
  - https://access-eu1.mobileiron.com

**Figure 20. Adding roles in MobileIron Core**

**Procedure**

1. In the MobileIron Core Admin Portal, go to **Services > Access**.
2. Enter the following:
   - **Access Admin URL**: URL for Access.
   - **Access Admin Username**: Username for an Access administrator.
   - **Access Admin Password**.

3. Click **Register**.
   Access is registered with MobileIron Core.

**Next steps**


**Configuring MobileIron Tunnel in MobileIron Core**

MobileIron Tunnel creates a secure connection between the managed device and Access for authenticating users accessing enterprise cloud resources.

**Before you begin**

- Ensure that you have registered Access with MobileIron Core.
- Ensure that you have added MobileIron Tunnel to MobileIron Core.
For information on how to add MobileIron Tunnel to MobileIron Core, see the relevant section in the MobileIron Tunnel Guide for Administrators for the device OS.

Procedure
1. In MobileIron Core, go to Polices & Configs > Configurations.
2. Click Add New > VPN.

3. For Connect Type, select the MobileIron Tunnel or MobileIron Tunnel (Android).
   Create a separate Tunnel configuration for each OS type.
4. Enter a name for the configuration.
5. Select the check box for Enable MobileIron Access.
6. For Identity Certificate, select the Certificate Enrollment configuration you created earlier to establish trust between Tunnel and Access.
7. Click Save.

Note The Following:
• The Enable MobileIron Access setting is also available in the AppConnect App Configuration and Web@Work configuration. The setting allows these apps to direct authentication traffic to Access. The setting is available only if Services > Access is configured in the MobileIron Core Admin Portal. Otherwise, the setting is grayed out.
• Federated traffic from Docs@Work through Access is only supported with Tunnel. However, using Tunnel to CIFs services will fail. Federated traffic through AppTunnel and an Access (without Standalone Sentry) deployment is not supported for Docs@Work. Selecting **Enable MobileIron Access** in the Docs@Work configuration does not have an impact.
• Google Apps (GApps) require Chrome to direct authentication traffic through Access.

**Next steps**
Configure Access in MobileIron Core. See [Configuring MobileIron Core in Access](#).

**Configuring MobileIron Core in Access**

The MobileIron Core with which Access integrates is configured in the **UEM** tab in Access.

**NOTE:** When CORE is in maintenance, you must configure the load balancers to return 503, Service Unavailable.

**Before you begin**
• Ensure that you have completed the steps detailed in the following:
  - Configuring Access in MobileIron Core
  - Configuring MobileIron Tunnel in MobileIron Core
• Make a note of the following:
  - FQDN for MobileIron Core.
  - The username and password for an administrator with Common Platform Services (CPS) and Device Read Only roles in Core.
  - MobileIron recommends creating a separate administrator account in MobileIron Core that is specifically used for UEM integration with Access.

**Procedure**
1. Click **UEM** on the left navigation pane in the Access administrative portal. The UEM panel with the host details appears.
2. Click **Connect to Verify** either in the **UEM Username** column or in the right hand panel. The **Verify UEM Tenant** window appears.

**FIGURE 24. VERIFY UEM TENANT**
3. Enter the following details:
   - **Host URL**: The fully qualified domain name (FQDN) of MobileIron Core.
     The field is automatically populated and not editable.
   - **UEM Username**: A user with Common Platform Services (CPS) and Device Read Only roles assigned in Core.
   - **UEM Password**

   The following status is displayed in Access based on the connection:

   **Table 5. UEM Status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Access and Core are connected.</td>
</tr>
<tr>
<td>Not Verified</td>
<td>The Core Credentials are not verified by Access. Enter the credentials to complete the workflow.</td>
</tr>
<tr>
<td>Deregistered</td>
<td>Access is deregistered.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Server is unable to connect to MobileIron Core.</td>
</tr>
<tr>
<td>Incorrect Password or Permissions</td>
<td>The UEM permissions or password is incorrect.</td>
</tr>
</tbody>
</table>

4. Click **Verify**.
   The Tunnel certificate is pulled and establishes trust between Tunnel and Access.

5. Click **Done**.

**Next steps**
Set up SP and IdP federated pairs. See **Federated Pairs**.

**Deregistering Access from UEM**

To stop using Access with MobileIron UEM, deregister the Access profile configured in the UEM and delete the UEM in Access.

**NOTE**: Deregistering the Access profile in MobileIron UEM and deleting the UEM in Access can be done in any order. It is, however, important to do both.

**Before you begin**
- Ensure that the Access profile in MobileIron UEM is no longer in use and that there is no data associated with the profile. This means that **Enable MobileIron Access** is disabled in any Tunnel VPN profile, AppConnect App Configuration, Docs@Work, or Web@Work configuration.

**Procedure**

1. In the MobileIron UEM, navigate to the Access profile.
   - In the MobileIron Core Admin Portal, go to **Services > Access**.
   - In MobileIron Cloud, go to **Admin > Infrastructure > Access**.

2. Click **Deregister** to remove the Access profile.
A Deregister Access Profile window displays.

3. Depending on your UEM, click Confirm or Deregister Access Profile to deregister.
   Enter the Access Admin Username and Password to deregister.

4. In the Access administrative portal, click UEM.

5. Click Delete in the right panel to remove UEM.
   The Delete UEM window appears.

6. Click Delete UEM.
   UEM is removed from Access.
Set up Access + Standalone Sentry

In Access + Standalone Sentry deployment, MobileIron Access gets device posture and compliance information from Standalone Sentry. To make Standalone Sentry known to MobileIron Access, register Standalone Sentry to MobileIron Access, then assign the Sentry to the MobileIron Access profile.

Overview of steps to set up Access + Standalone Sentry

The following describe the tasks to set up Access + Standalone Sentry:
• Adding a profile
• Registering a Standalone Sentry
• Assigning Standalone Sentry to a profile

Adding a profile

If you selected Access + Standalone Sentry, the Add Profile screen appears. Use the Profile page to create a profile for MobileIron Access and set up Access + Standalone Sentry.

Before you begin

• The certificate must be signed by a trusted third-party CA, and must have its associated private key as part of the PKCS 12 file.
• The certificate must comply with security requirements. See Error conditions for SSL certificate. For more information about error conditions, see Adding a profile. If the SSL certificate does not comply with the security requirements, then the following error displays.
• Associate the SSL certificate with the Sentry second hostname.

**Procedure**

1. For **Hostname**, enter the second hostname for the Standalone Sentry. The second hostname will be associated with MobileIron Access.

**Figure 25. Configure Hostname**

2. Click on **Next**.

**Figure 26. Configure Certificate**

3. Click **Add new certificate** to upload the SSL certificate associated with the second hostname.
4. For **Certificate Name**, enter a name by which you can identify the certificate.
5. For **Certificate Password**, enter the password required to open the certificate.
6. Click **Choose File** to navigate to the location of the certificate file or drag and drop the certificate file.
7. Click **Add SSL Certificate** to complete the process of adding the certificate.
8. Click **Done** to complete the profile setup.

**Figure 28. Complete profile setup**

9. Click **Continue** to view the profile in the **Overview** page.
You will now have created a profile. You can now add a cloud service provider (SP) and identity provider (IdP) federated pair to this profile.

Next steps
Register a Standalone Sentry to MobileIron Access. See Registering a Standalone Sentry.

Related topics
See Federated Pairs for information about adding an SP and an IdP federated pair.

Error conditions for SSL certificate

The SSL certificate you upload to the Sentry profile must meet the security requirements from Apple. If the certificate does not meet the security requirements the system displays error messages. Access checks for the following error conditions:

- SHA-1 server certificate or issuing authority detected.
- Server certificate or issuing authority contains RSA key size less than 2048 bits.
- Server certificate does not contain DNS name of the server in the Subject Alternative Name extension.

The following conditions are applicable only if the server certificate is issued after July 1, 2019 as indicated in the certificate. For more information, see the requirements provided by Apple: https://support.apple.com/en-us/HT210176

- Server certificate does not contain an ExtendedKeyUsage (EKU) extension containing the id-kp-serverAuth OID.
- TLS server certificates have validity period of more than 825 days.

Registering a Standalone Sentry

Use the Standalone Sentry command line interface (CLI) to register Standalone Sentry to MobileIron Access.

Procedure
1. SSH to Standalone Sentry.
2. Log in as an administrator.
3. Enter the following commands:
   a. Enable
   b. Configure terminal
   c. accs registration <tenant url> <user>.
      <tenant url>: The tenant URL you received in the welcome email.
      Do not use /cms in the tenant url.
      <user>: The local admin email for MobileIron Access you received in the welcome email.
      You will be prompted to enter the tenant admin password. This is the admin password your received in the welcome email.
   d. End
Example of Standalone Sentry registration to MobileIron Access

The following example shows the CLI and output for registering Standalone Sentry to MobileIron Access.

```
Last login: Fri Feb 19 16:58:43 2016 from 10.10.15.2
******************************************************************************
* MobileIron Sentry CLI *
* *
******************************************************************************
Welcome miadmin it is Tue Feb 23 22:24:51 UTC 2016
sentry@mycompany.com> enable
Password:
sentry@mycompany.com# configure terminal
Enter configuration commands, one per line.
sentry@mycompany.com/config# accs registration https://access-na1.mobileiron.com
foo@example.com
Enter password for user "foo@example.com":
Registration succeeded. Details:

    "tenantURL" : "https://access-na1.mobileiron.com",
    "tenantUsername" : "foo@example.com",
    "registrationTimeMs" : 1456267371581,
    "crtUuid" : "17592186044416",
    "crtUsername" : "17592186044416"
}
sentry@mycompany.com/config# end
sentry@mycompany.com# show accs registration
{
    "tenantURL" : "https://access-na1.mobileiron.com",
    "tenantUsername" : "foo@example.com",
    "registrationTimeMs" : 1456267371581,
    "crtUuid" : "17592186044416",
    "crtUsername" : "17592186044416"
}sentry@mycompany.com#
```

Next steps
Assign the Standalone Sentry to a profile. See Assigning Standalone Sentry to a profile.

Related topics
Example of Standalone Sentry registration to MobileIron Access
Viewing Standalone Sentry information

You can view the Standalone Sentry information that you have added in MobileIron Access. The registered Standalone Sentry checks-in every fifteen minutes to MobileIron Access. When Sentry does not check-in, authentication failures to cloud service providers might occur. When Sentry does not check-in for an hour, MobileIron Access displays an alert in the Sentry tab to resolve the issues. The administrator is also notified with an email every 30 minutes for 24 hours to diagnose the issues and resolve the check-in issue. The email notification is stopped after 24 hours.

NOTE: If the Standalone Sentry that was registered to MobileIron Access is no longer in use, unassign the Standalone Sentry from the profile to stop getting alerts.

Procedure
1. Click **Sentry** in the left navigation pane of MobileIron Access administrative portal after you have registered the Standalone Sentry.
   
   You can now assign the Standalone Sentry to a profile.
   
   The Supported versions of Standalone Sentry are also listed on this page.
2. Enter the administrator's password to assign the Standalone Sentry to a profile.
3. To view the detailed report of the Standalone Sentry that you have added, select the appropriate Sentry. The detailed report displays on the right pane.

**Figure 29. Standalone Sentry Report**
### TABLE 6. STANDALONE SENTRY INFORMATION

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>The Overview section provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• ID</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Last Activity Time</td>
</tr>
<tr>
<td></td>
<td>• Registration Time</td>
</tr>
<tr>
<td>Inventory</td>
<td>The Inventory report provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• Hostname</td>
</tr>
<tr>
<td></td>
<td>• Machine Size</td>
</tr>
<tr>
<td></td>
<td>• Product Version</td>
</tr>
<tr>
<td></td>
<td>• Fips Enabled</td>
</tr>
<tr>
<td></td>
<td>• Portal Url</td>
</tr>
<tr>
<td></td>
<td>• Service Start Time</td>
</tr>
<tr>
<td></td>
<td>• UEM Hostname</td>
</tr>
<tr>
<td></td>
<td>• UEM Server Type</td>
</tr>
<tr>
<td>Configuration</td>
<td>The Configuration report provides information about the status of the Sentry configuration.</td>
</tr>
<tr>
<td>Registration</td>
<td>The Registration report provides information about the status of Sentry registration.</td>
</tr>
</tbody>
</table>

### Standalone Sentry actions

You can take the following actions on a Standalone Sentry:

- **Assign** the Standalone Sentry to a profile.
- **Unassign** the Standalone Sentry to a profile.
- **Delete** the Standalone Sentry.

### Assigning Standalone Sentry to a profile

Assigning Standalone Sentry to MobileIron Access profile allows MobileIron Access to get device posture and compliance information from that Standalone Sentry.

**Procedure**

1. In the **Sentry** page, select the Standalone Sentry.
2. Click **Actions > Assign** to assign the Standalone Sentry to the profile.
   
   The Standalone Sentry **Status** displays as **Profile Assigned**.
Unassigning Standalone Sentry from a profile

Unassign Standalone Sentry if it is no longer in use.

Procedure
1. In the Sentry page, select the Standalone Sentry.
2. Click Actions > Unassign to unassign the Standalone Sentry to the profile.
   - The Standalone Sentry Status displays as Profile Unassigned.

Deleting a Standalone Sentry

When you delete a Standalone Sentry, it will be unregistered when the Standalone Sentry syncs with the MobileIron Access administrative portal.

Before you begin

Unassign the Standalone Sentry from an Access profile. See Unassigning Standalone Sentry from a profile.

Procedure
1. In the Sentry page, select the Standalone Sentry.
2. Click Actions > Delete.
3. Click on Delete Sentry.
   - The Standalone Sentry will no longer be listed in the Sentry page.

NOTE: The Standalone Sentry will be unregistered when it next syncs with the MobileIron Access administrative portal.

Profile overview

The Profile > Overview page provides an overview of the steps to enable access control for cloud services.

If you have an Access + Standalone Sentry deployment, the page also provides a snapshot of Standalone Sentry under Profile Details. You can edit the hostname and SSL certificates from the Overview page.
A profile is a set of configurations that can be assigned to a Standalone Sentry. It consists of a single hostname and its SSL configuration, IdP and SP proxy pairs, and conditional rules that control access to the IdP and SP proxy pairs. You can have multiple IdP and SP proxy pairs and conditional rules in the profile.

NOTE: For MobileIron Access + Standalone Sentry, you can assign a profile to multiple Standalone Sentry.

**Editing the profile**

The edit function allows you to update the Standalone Sentry second hostname and SSL certificate for MobileIron Access.

**Procedure**

1. In **Profile Details**, click the text box to edit the details.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The second hostname for Standalone Sentry. The second hostname is associated with MobileIron Access on Standalone Sentry.</td>
<td>Hostname entered during initial setup.</td>
</tr>
<tr>
<td>SSL Certificate Alias</td>
<td>The SSL certificate for MobileIron Access. Select from the drop down list.</td>
<td>Certificate uploaded during initial setup</td>
</tr>
<tr>
<td>Add new certificate</td>
<td>Click to add a new SSL certificate.</td>
<td></td>
</tr>
</tbody>
</table>

2. Click ✔️ to save the changes or ✗ to cancel.

The changes are applied when the Standalone Sentry syncs with the MobileIron Access administrative portal.
Federated Pairs

MobileIron Access acts as a proxy between the service provider (SP) and identity provider (IdP). In a federated pair set up, MobileIron Access appears as a service provider (SP) to your identity provider (IdP) and as an IdP to your SP. A federated pair is the original IdP and SP pair for which MobileIron Access is used as the proxy.

Configuring federated pairs

A federated pair is the identity provider (IdP) and service provider (SP) pair for which MobileIron Access is used as the intermediary. Federated pairs are configured in Federated Pairs. The Federated Pairs link in the left navigation pane changes to Federation if delegated IdP is enabled.

Before you begin
Before you configure a federated pair, ensure the following:

1. You have an existing federated authentication setup, using SAML or WS-Fed, between the cloud service provider (SP) and the identity provider (IdP).
2. The existing federated authentication setup between the SP and IdP works without MobileIron Access in the path.
3. You have the SP and IdP metadata.
   - For instructions on getting cloud service provider (SP) metadata see the following Knowledge Base article How do I access Service Provider (SP) metadata?
   - For instructions on getting identity provider metadata see the Knowledge Base article at How do I access Identity Provider (IdP) metadata?

Note The Following:

- Microsoft Azure Active Directory as an IdP is qualified only with Salesforce (SP) and G Suite (SP).
- Microsoft Azure Active Directory as an IdP is not supported with Office 365 (SP).
- G Suite as an IdP is qualified only with Salesforce (SP) and Facebook Workplace (SP).
- G Suite as an IdP is not supported with Office 365 (SP).
- OneLogin as an IdP is not supported with Office 365 (SP).
- WebEx as an SP is qualified only with Microsoft ADFS (IdP) and Okta (IdP).
- For Office 365 Using WS-Federation only the following IdP are supported: Microsoft ADFS and Ping Identity.
Procedure

1. In the MobileIron Access administration portal, go to Profile > Federated Pairs.
2. Click +Add New Pair. The set of supported cloud service providers displays.
3. Click the appropriate service provider to configure service provider settings. To add a service provider that is not listed, select either Custom SAML Service Provider or Custom WS-Federation Service Provider.

   NOTE: Concur is a compatible app. Concur as a service provider is tested only with Okta and Microsoft ADFS.

4. Enter the requested information for the service provider. The requested information includes the signing certificate, encryption certificate for SAML assertions, service provider metadata, checkbox to validate signature for authentication requests sent by service provider, and the option to configure single sign-on (SSO).

   TIP: If you had previously uploaded signing certificates, select the certificate from the Signing Certificate drop-down list. MobileIron also provides a default signing certificate, which is also available in the drop-down list.

Note The Following:

- Previously, the service provider signing certificates existed but were not validated and user could log in to the service provider regardless of the signing certificate status. Now, a checkbox is introduced to validate the service provider signature and log an error in the Reports > Access. For the existing federated pairs, the checkbox is disabled and for the new federated pairs, it is enabled by default. This field is supported for Salesforce and Custom SAML service provider only.

- When configuring a Federated Pair, the checkbox 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.

5. Click Next. The set of supported identity providers displays.

6. Click the appropriate identity provider to configure identity provider settings.

7. Enter the requested information. The requested information includes the signing certificate and the identity provider metadata.

8. Click Done to complete the federated pair configuration.

9. Click OK in the Federated Pairs Setup is Complete message. The new pair is displayed on the Federated Pairs tab in MobileIron Access.

IMPORTANT: You can also edit a federated pair. On the Federation page, click for the federated pair that you want to edit. When editing a federated pair, you can switch from add metadata URL to upload metadata or vice versa or only provide the metadata URL for the federated pair.
Use Cases for distinctive deployments

Some customers have distinctive deployment scenarios with custom service provider and identity providers. This section lists some of the use cases that are distinctive and can serve a requirement in other deployments.

Jabber and Access

A MobileIron Core user can leverage Access to provide Zero Sign-on or conditional access for a Jabber client. Jabber can be used to protect messaging and calling voice data requirements. This deployment uses MI Packet Tunnel for Jabber (service provider) and Ping Federate (identity provider) with MobileIron Access.

For more information on MI Packet Tunnel and Access deployment, see the [KB article](#).
Signing certificates

MobileIron Access uses standard PKI to sign authentication requests and assertions used for federation. A default signing certificate is created for every MobileIron Access instance. If you do not want to use the default certificate, you can generate a new signing certificate in the Access administrative portal or add a PKCS 12 file containing a certificate and private key to use for signing federation messages.

- Adding a signing certificate in MobileIron Access
- Generating a signing certificate in MobileIron Access

Note The Following:
- SSL certificates should not be used in lieu of the signing certificate. This use case is not supported.
- You can use the same signing certificate for the SP as well as the IdP.

Adding a signing certificate in MobileIron Access

The following provides the steps for adding a signing certificate in MobileIron Access.

Before you begin
- Ensure that you have a PKCS 12 format file (.PFX or .P12) that contains your signing certificate and corresponding private key.

Procedure
1. In the service provider or identity provider configuration, click Advanced Options.
2. Click Add a new certificate.
3. Enter the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Name</td>
<td>Enter an identifying name for the signing certificate.</td>
</tr>
<tr>
<td>Certificate Password</td>
<td>Enter the password for the signing certificate.</td>
</tr>
<tr>
<td>Choose File</td>
<td>Click to navigate to the location of the certificate or drag and drop the certificate to this location.</td>
</tr>
</tbody>
</table>

4. Click Add Signing Certificate to add the signing certificates.
   The certificate is available to select from the Signing Certificate drop-down list.
   The certificate is also listed in the Access Certificates tab.

Generating a signing certificate in MobileIron Access

The following provides the steps for generating a signing certificate in MobileIron Access.

Procedure
1. In the service provider or identity provider configuration, click Advanced Options.
2. Click Generate certificate to generate and add the signing certificate.
3. For Certificate Name, enter a name to identify the signing certificate.
4. Click **Generate Signing Certificate**.
   The Certificate Name displays in the **Signing Certificate** drop-down list.
   The certificate is also listed in the **Access Certificates** tab.

**Service provider (SP) metadata**

When a federated pair uses SP metadata URL, metadata is monitored. Access monitors SP metadata present in the system with the metadata at the URL. Metadata monitoring occurs every 24 hours. The fields such as Entity ID, ACS URL, and Signing cert pem are monitored and evaluated for changes.

Use one of the options described in the following table to upload SP metadata to MobileIron Access. When any changes are detected across any of these fields between metadata present in the system and the metadata at the URL, Access raises an alert with an email to all the administrators. It also displays an alert in the Access portal. The administrator then uses the sync metadata option to update the federated pair with these changes.

**NOTE:** MobileIron Access verifies the validity of the service provider metadata certificate file and sends email notifications. For more information, see **Certificate expiry notifications**.

If the SP certificate expires, your device end users will not be able to authenticate and access corporate services federated through MobileIron Access admin portal.

The following table describes the options for uploading service provider (SP) metadata.

**Table 7. Options for uploading SP metadata**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload Metadata</td>
<td>Click <strong>Choose File</strong> to navigate to the metadata file to add or drag and drop the file. The metadata file automatically populates the data MobileIron Access.</td>
</tr>
</tbody>
</table>
| Add Metadata   | Enter the following information:
   • Entity ID
   • Assertion Consumer Service URL
   Click **Add New** to add multiple Assertion Consumer Service (ACS) URLs. The option to add multiple ACS URLs is available for **Custom SAML SP and Custom WS-Fed SP** only. For more information about multiple ACS URLs, see **Assertion Consumer Service (ACS) URLs**.
   Select **Auth requests signed** to enter a Base64 Encoded Cert.
   **NOTE:** Use the **Add Metadata** option to add metadata for G Suite. For more information, see **Metadata for G Suite**.                                                                                                                                                     |
| Metadata URL   | Enter the metadata URL. If there are changes to the metadata on the SP at the configured URL, Access sends an email notification to the Access administrator.                                                                                                                     |
### TABLE 7. OPTIONS FOR UPLOADING SP METADATA (CONT.)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In <strong>Access &gt; Federated Pairs</strong>, the following alert message displays for the federated pair:</td>
</tr>
<tr>
<td></td>
<td><strong>SP metadata has changed.</strong></td>
</tr>
<tr>
<td></td>
<td>For the federated pair, click <strong>Actions &gt; Sync SP metadata</strong> to update the metadata file in Access.</td>
</tr>
<tr>
<td></td>
<td>An email notification is sent to the Access administrator after the sync.</td>
</tr>
</tbody>
</table>

## Assertion Consumer Service (ACS) URLs

Configure Assertion Consumer Service (ACS) URLs if you want to configure multiple destinations for the service provider (SP). For example, you may want your sales and customer support teams to go to separate locations on the service. Based on the intended destination, the SP encodes a different ACS URL in the authentication request. Access directs traffic to the ACS URL in the Authentication Request if it matches the ACS URL configured in Access. If an ACS URL is not provided in the Authentication Request or the ACS URL does not match the ACS URL configured in Access, the traffic goes to the default destination.

The option to add multiple ACS URLs is available for only for **Custom SAML SP** and **Custom WS-Fed SP** only.

### Metadata for G Suite

G-Suite does not provide a metadata file, therefore, for G Suite, select the Add Metadata option to add the service provider metadata to MobileIron Access. Enter the following:

- **Entity ID**: `google.com/a/{yourcompany.com}`
- **Assertion Consumer Service URL**: `https://www.google.com/a/{yourcompany.com}/acs`

For PingIdentity only, select the check box for **Auth requests signed**. In the **Base 64 Encoded Cert** text box, paste the Base 64 Encoded Cert from PingIdentity.

See also, the Knowledge Base article at [https://community.mobileiron.com/docs/DOC-4097](https://community.mobileiron.com/docs/DOC-4097)

## IdP initiated login

The Enable IdP initiated login for this SP option is available for configuration for custom service providers (SP) only. However, the option is enabled by default for Concur SP. The option is disabled for all other SPs.

Select the Enable IDP initiated login for this SP option if your service provider redirects to the IdP login page, instead of sending a SAML AuthnRequest to the IdP.
Enabling IdP initiated login lets MobileIron Access expose an IdP URL that generates a SAML request to the original IdP. However, if the Use Tunnel Certificate for SSO option is also enabled, MobileIron Access generates a SAML response to the SP based on the user’s Tunnel certificate.

**SAML response signature**

The ability to choose the SAML response signature is available for custom service providers (SP) only.

This option is available for service providers that require the SAML Response to be signed instead of signing the SAML Assertion inside the SAML Response.

The **Sign Assertion** option is selected by default. You can select the **Sign Response** option if appropriate.

*NOTE:* SAML Responses received by MobileIron Access must always have the Assertion signed. However, the Response must not be signed.

**Encrypting SAML assertions**

Enabling encryption of SAML assertions adds another layer of security. Enable this feature in a mobile app single sign-on setup if the SP supports SAML assertion decryption. The SAML assertions are encrypted such that the assertions can be decrypted only with the private keys held by the service provider.

**Note The Following:**

- Encryption of SAML assertions is disabled by default.
- Responses can be signed while carrying a signed encrypted Assertion, but the Response itself is not encrypted.
- Do not use the signing certificate for encrypting SAML assertions and vice-versa.
- The following service providers (SP) support encryption of SAML assertions:
  - Salesforce
  - Custom SAML Service Provider
  - Custom WS-Federation Service Provider
- A default certificate for encryption is automatically available in your MobileIron Access tenant.
- Enabling SAML assertion encryption, enables additional options for **Native Mobile Application Single Sign-On (SSO)**. These options allow you to select the data encryption algorithm and the key transport algorithm for single sign-on.

**Before you begin**

See Configuring Mobile App Single Sign-on (SSO) for information about setting up single sign-on.
Procedure

1. In the service provider configuration for Salesforce, Custom WS-Federation Service Provider or for Custom SAML Service Provider, go to Encryption Certificate.
2. Click the check box for Encrypt SAML assertion.
   The default encryption certificate is automatically selected.
3. (Optional) To use a different certificate than the default certificate, do one of the following:
   - select a certificate from the drop-down list.
   - click Generate certificate or Add new certificate.

Adding a new certificate for SAML assertion encryption

The following provides the steps for adding a new certificate for SAML assertion encryption.

Before you begin

- Ensure that you have a PKCS 12 format file (.PFX or .P12) that contains the certificate and corresponding private key.

Procedure

1. In the service provider (SP) configuration, in the Encryption Certificate section, click Add new certificate.
2. Enter the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Name</td>
<td>Enter an identifying name for the encryption certificate.</td>
</tr>
<tr>
<td>Certificate Password</td>
<td>Enter the password for the encryption certificate.</td>
</tr>
<tr>
<td>Choose File</td>
<td>Click to navigate to the location of the encryption certificate or drag and drop the certificate to this location.</td>
</tr>
</tbody>
</table>
3. Click Add Encryption Certificate to add the new certificate.
   The certificate is now available to select from the drop-down list.
   The certificate is also listed in Profile > Access Certificates.

Generating a certificate for SAML assertion encryption

The following provides the steps for generating a certificate for SAML assertion encryption.

Procedure

1. In the service provider (SP) configuration, in the Encryption Certificate section, click Generate certificate.
2. For Certificate Name, enter a name to identify the certificate.
3. Click Generate Encryption Certificate.
   The certificate is now available to select from the drop-down list.
   The certificate is also listed in Profile > Access Certificates.
Related topics
• Adding a new certificate for SAML assertion encryption
• Generating a certificate for SAML assertion encryption

Identity provider (IdP) metadata

When a federated pair uses IdP metadata URL, metadata is monitored. Access monitors IdP metadata present in the system with the metadata at the URL. Metadata monitoring occurs every 24 hours. The fields such as Entity ID, Redirect SSO URL, Post SSO URL, and Signing cert pem are monitored and evaluated for changes.

Use one of the options described in the following table to upload IdP metadata to MobileIron Access. When any changes are detected across any of these fields between metadata present in the system and the metadata at the URL, Access raises an alert with an email to all the administrators. It also displays an alert in the Access portal. The administrator then uses the sync metadata option to update the federated pair with these changes.

Use one of the options described in the following table to upload IdP metadata to MobileIron Access.

NOTE: MobileIron Access verifies the validity of the identity provider metadata certificate file and sends email notifications. For more information, see Certificate expiry notifications.

If the IdP certificate expires, your device end users will not be able to authenticate and access corporate services federated through MobileIron Access admin portal.

### TABLE 8. OPTIONS FOR UPLOADING IDP METADATA

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload Metadata</td>
<td>Click <strong>Choose File</strong> to navigate to the metadata file to add or drag and drop the file. The metadata file automatically populates the data in MobileIron Access.</td>
</tr>
</tbody>
</table>
| Add Metadata     | Enter the following information:  
|                  | • Entity ID  
|                  | • Post SSO URL  
|                  | • Redirect SSO URL  
|                  | • Base64 Encoded Cert                                                                                                                                   |
| Metadata URL     | Enter the metadata URL. For ADFS, enter the metadata URL for the ADFS server in the following format: https://<ADFS DOMAIN NAME>/FederationMetadata/2007-06/FederationMetadata.xml.  
|                  | NOTE: If the ADFS server is internal, expose the URL through the firewall. If there are changes to the metadata on the IDP at the configured URL, Access sends an email notification to the Access administrator. |
**Table 8. Options for uploading IDP metadata (cont.)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In <strong>Access &gt; Federated Pairs</strong>, the following alert message displays for the federated pair:</td>
<td></td>
</tr>
<tr>
<td><strong>IDP metadata has changed.</strong></td>
<td></td>
</tr>
<tr>
<td>For the federated pair, click <strong>Actions &gt; Sync IDP metadata</strong> to update the metadata file in Access.</td>
<td></td>
</tr>
<tr>
<td>An email notification is sent to the Access administrator after the sync.</td>
<td></td>
</tr>
</tbody>
</table>

**About Microsoft ADFS metadata**

For a SAML pair configured with Microsoft ADFS, you can upload the metadata, configure a metadata URL, or add the metadata. Changing the initial configuration of the metadata to a different form depends on how you configured the metadata initially. The following table describes the initially configured form and the forms to which it can be modified.

**Table 9. Modify Microsoft ADFS metadata**

<table>
<thead>
<tr>
<th>Initial SAML pair configuration using</th>
<th>Can be modified to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload metadata</td>
<td>Metadata URL.</td>
</tr>
<tr>
<td></td>
<td>However, it cannot be modified to Add Metadata.</td>
</tr>
<tr>
<td>Metadata URL</td>
<td>Upload Metadata.</td>
</tr>
<tr>
<td></td>
<td>The existing URL configuration is overridden by the uploaded metadata, and the URL is no longer tracked.</td>
</tr>
<tr>
<td></td>
<td>The metadata configuration cannot be modified to Add Metadata.</td>
</tr>
<tr>
<td>Add Metadata</td>
<td>Cannot be modified to other options.</td>
</tr>
</tbody>
</table>

**Office 365 settings**

Office 365 is configured using either WS-Federation or SAML federation authentication protocols. Select one of the following service provider options in the **Choose Service Provider** page to configure Office 365 settings:

- Office 365 Using SAML
- Office 365 Using WS-Federation
Figure 31. Choose Service Provider

Choose Service Provider

The following describes the settings specific to Office 365 as the service provider:

- Office 365 settings using SAML authentication
- Office 365 settings using WS-Federation authentication
- PowerShell commands for Office 365
- Backup and restore Office 365 federation settings
- Multi-domain issuer
- Active Logon Policy for Office 365

Office 365 settings using SAML authentication

The following describes the additional Office 365 settings available for configuration if your service provider is Office 365 Using SAML. These settings are available in the IdP configuration page:

- **ECP Backend Type**: Select from the drop-down list. Specifies the ECP backend type to connect to the IdP.
- **Federated Domain**: Enter the value for Office 365. Example: mycompany.com.
- **Active Logon Settings**: Enter the Active Logon URL in the text box for Original IDP Active Logon URL. The Active Logon URL varies depending on the ECP backend type and the IdP. If your IdP is
Microsoft ADFS, the Original IDP Active Logon URL text box is pre-populated with the Active Logon URL. Update the URL with the correct ADFS domain.

- Example for ADFS using ECP WS-Trust 1.3: https://<FQDN of the ADFS server>/adfs/services/trust/13/useamemixed.

**Office 365 settings using WS-Federation authentication**

The following describes the additional Office 365 settings available for configuration if your service provider is **Office 365 Using WS-Federation**.

The option to enable multiple federated domains is available in the Office 365 service provider configuration page.

- **Support Multiple Domains**: Select the check box to enable multiple federated domains to use the same federated pair in MobileIron Access.

The options to configure MEX metadata and the Active Logon URL are available in the IdP configuration page. MEX metadata and Active Logon URL expose SOAP Web Service endpoints and define how other endpoints interact with the SOAP Web Service endpoints. MobileIron Access publishes MEX metadata based on the MEX metadata configuration provided by the original IdP. Access only exposes the endpoints that are supported and configured in the MEX metadata of the original IdP. Only WS-Trust 1.3 and WS-Trust 2005 protocols for useamemixed are supported. Configuring MEX metadata allows for support for applications such as Microsoft Dynamics 365 and Microsoft SQL Server. In addition, Windows Transport endpoint is supported with Access + Standalone Sentry deployments only.

For more information about enabling Windows Transport endpoints see Azure Hybrid Domain-Join with MobileIron Access.

Select one of the following methods to provide the MEX metadata configuration from the original IdP:
- **Enable Mex Metadata**: Select the check box to provide metadata configuration from the original IdP. Choose one of the following:
  - **MEX metadata URL**: Enter the URL for the MEX metadata for the original IdP. Example for ADFS MEX Metadata URL: https://<FQDN of the ADFS server>/adfs/services/trust/mex
    - **Note**: Federation metadata import through URL might fail if the server does not present certificate chain issued by trusted certificate authorities. For the MEX metadata URL, the corresponding server must present full certificate chain issued by trusted certificate authority.
  - **Upload MEX metadata**: Upload the MEX metadata file from the original IdP. Deselect the check box to disable MEX metadata.

- **Enable Active Logon URL**: Select the check box to enable Active Logon URL. Enter the Active Authentication URL for the original IdP. You enable Active Logon URL to handle Active Auth traffic. This is required for applications, such as some email applications, that support only active authentication. MobileIron Access exposes only WS-Trust 2005 usemamemixed endpoints. If your IdP is Microsoft ADFS, the Original IDP Active Logon URL text box is pre-populated with the Active Logon URL. Update the URL with the correct ADFS domain.
  - **Example**: https://<FQDN of the ADFS server>/adfs/services/trust/2005/usemamemixed
  - Deselect the check box to disable Active Logon URL.

**NOTE**: Native iOS clients, Android email clients, and MobileIron Email+ use active authentication.

See also [Active Logon Policy for Office 365](#).
Authentication with Microsoft PowerShell commands

Access supports the use of Microsoft PowerShell commands, such as Connect-MsolService and Connect-SPOSService, to get authorization tokens to authenticate endpoints with Azure ID. This support allows administrators to set up authentication for service provider (SP) accounts that belong to a federated domain.

Note the following:

- **PowerShell commands**, such as Connect-MsolService and Connect-SPOSService, are ActiveAuth transactions. Therefore, ensure that an Active Logon Policy is applied. Otherwise, the ActiveAuth traffic is bypassed and no rules are evaluated.

- Ensure that the latest version of MSOnline PowerShell module is installed when running PowerShell scripts from Access pair for setting up Office 365. If older version of this module are used, it prompts a login with Basic Auth which will be deprecated by Microsoft in October.

For Access + Standalone Sentry deployments, the feature is not enabled by default. The feature is enabled using command line interface (CLI) commands in Standalone Sentry. The commands are available in Standalone Sentry 9.6.0 through the latest version as supported by MobileIron.
WARNING: Do not enable the feature on a Standalone Sentry that is configured for ActiveSync. The feature is not supported on a Standalone Sentry that is configured for ActiveSync.

To enable the feature in Access + Standalone Sentry deployments, enter the following command in Standalone Sentry command line interface (CLI) in CONFIG mode:

```
config# debug sentry ignore-line-breaks true
```

To disable the feature in Access + Standalone Sentry deployments, enter the following command in Standalone Sentry command line interface (CLI) in CONFIG mode:

```
config# debug sentry ignore-line-breaks false
```

Restart the Standalone Sentry service for the configuration changes to take effect. To restart Standalone Sentry service, enter the following command in EXEC PRIVELEGEX mode:

```
sentry# service tomcat restart
The 'service tomcat restart' may impact traffic.
Would you like to proceed? [yes][no] : yes
```

To view whether the feature is enabled or not in Standalone Sentry, enter the following show command in EXEC PRIVELEGEX mode:

```
sentry# show sentry ignore-line-breaks
org.apache.xml.security.ignoreLineBreaks: false
```

- **False** indicates that the feature is disabled.
- **True** indicates that the feature is enabled.

### PowerShell commands for Office 365

The commands to federate Azure AD with MobileIron Access are provided as a PowerShell batch script, which can be downloaded from the MobileIron Access administrative portal. After you create a federated pair with Office 365 in MobileIron Access, the link to download the PowerShell batch script becomes available in the federated pair listing in **Profile > Federated pairs**.

NOTE: Ensure that the latest version of MSOnline PowerShell module is installed when running PowerShell scripts from Access pair for setting up Office 365. If older version of this module is used, it prompts a login with Basic Auth which will be deprecated by Microsoft in October.

To use the PowerShell commands, download the PowerShell script and run the script in PowerShell with the following command:

```
script_name.ps1 -domain mydomain.com
```

In the above command:

- **script_name** is the name of the downloaded PowerShell script.
- **mydomain.com** is the Microsoft Azure AD domain.

Ensure that you have PowerShell Administrator permissions.
Backup and restore Office 365 federation settings

To backup and restore the Office 365 federation settings, see Back up and restore Office 365 settings.

Multi-domain issuer

If you are federating using the WS-Federation protocol, you can use the same federated pair for multiple AD domains suffixes that federate with the same Office 365 tenant.

In cases where multi-domain issuer is enabled, Access composes the multi-domain issuer from the domain in the UPN. If the UPN domain is the sub domain, the issuer will not match with the root domain issuer in Azure AD. Configure the attribute AzureDomain in the ADFS, if you have a domain forest (multiple ADs joined in the forest). In such cases, the issuer URI suffix is derived from the value of the attribute name AzureDomain in the assertion from the original IdP.

For ADFS 3.0, to add the AzureDomain attribute, add the following claim rules to the relying party trust:

- Query DistinguishedName from AD
  
  ```
  c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
  ```
Active Logon Policy for Office 365

A passive logon policy (passive or modern authentication) is configured by default for Office 365 federated pairs. If your Office 365 email application does not support passive authentication, use the **Active Logon Policy** option to assign a separate conditional policy to authenticate the active authentication (ActiveAuth) traffic for the Office 365 federated pair. The **Active Logon Policy** option becomes available after the Office 365 federated pair is created.

Passive authentication is based on a browser-based connection to Office 365, which supports redirects. The following describe the federated authentication flow with passive authentication:

1. The user-agent (browser) connects to Office 365.
2. Office 365 responds with a 301 redirect to the identity provider.
3. The user-agent follows the redirect to the identity provider.
4. The identity provider presents a login form for end users to enter their credentials.
   
   **NOTE:** The credentials can be in the form of user name and password, certificate, or another alternative method.
5. The identity provider generates a response that contains an authentication Assertion and a browser-based mechanism, either redirect or JavaScript, to auto-submit the Assertion to Office 365.
6. The user-agent uses the browser-based mechanism to submit the Assertion to Office 365.

7. Office 365 validates the Assertion, thus allowing the user to log in.

Active authentication does not support browser-based connection to Office 365. Therefore, it does not

- support 301 redirects
- render HTML or form-based entry
- do JavaScript-based automatic form submission.

The federated authentication flow for active authentication is as follows:

1. Users enter their account credentials in the email application.
2. The email application sends the user credentials to Office 365.
3. Office 365 forwards the user credentials to the identity provider.
4. The identity provider returns an Assertion in the response to Office 365.
5. Office 365 validates the Assertion allowing the user to log in.

For an Office 365 federated pair configured in Access, if there are no policies assigned to ActiveAuth traffic, the ActiveAuth traffic is bypassed and no rules are evaluated. If you are using email applications that support only active authentication, to allow these applications to authenticate with Office 365, assign an Active Logon policy to the Office 365 federated pair. See Office 365 settings.

NOTE: Native iOS clients, Android email clients, and MobileIron Email+ use active authentication.

When you assign a policy from the Active Logon Policy drop-down, the conditional rules in the assigned policy are evaluated for ActiveAuth traffic. The following conditional rules are not applicable to ActiveAuth traffic:

- Trusted App and Device Rule
- Tunnel Rule
- Multi-Factor Authentication
- Android for Work Registration
- iOS Native Email OAuth
- Desktop Trust Rule

Assigning an active logon policy

The option to assign a policy for active logon is available in Profile > Federated Pairs, in the listing for the Office 365 federated pair.

Before you begin

Ensure that you have created a separate conditional policy to use for ActiveAuth traffic. When you create a conditional policy, the policy becomes available in the Active Logon Policy drop down when you are assigning the policy. To create a conditional policy, see Conditional Access.

NOTE: MobileIron recommends that you configure a separate conditional policy for Active Logon.
Procedure

1. In MobileIron Access, go to Profile > Federated Pairs.

2. In the listing for the Office 365 federated pair, click .
   The Assign Policy window opens.

   ![Assign Policy Window](image)

   **Figure 35. Assign Logon Policy**

   **Assign Policy Window**

   - **Passive Policy**
     - Default Policy

   - **Active Logon Policy**
     - Best practice is to configure a separate policy for Active Logon.
     - Office 365 Active Logon policies:
       1. Conditional Access Rules with "Warn" action will behave as an "Allow" action.
       2. Conditional Access Rules for Trusted App and Device and Tunnel Rule are not applicable for Active Logon.

   - **Active Logon Policy**
     - None

3. Select the policy from the following options:
   a. **Passive Policy**: Select the Passive policy from the drop-down list for browser-based solution.
   b. **Active Logon Policy**: Select the Active Logon policy from the drop-down list for client-based solution.
      Select None from Active Logon drop down list, if you do not want Active Authentication traffic to evaluate any policy’s rule condition.

4. Click Assign.

Publishing a profile

Publishing the profile makes the changes available. In an Access (without Standalone Sentry) deployment, publishing the profile makes the changes live. Typically, it takes less than two minutes for the changes to take effect.

In a deployment with Access + Standalone Sentry, the changes are made available to the Standalone Sentry paired with the profile. Standalone Sentry picks up the changes when it next syncs. If there are any changes, Standalone Sentry consumes the changes.

Standalone Sentry syncs every 15 minutes with the MobileIron Access administrative portal. Therefore, it might take up to 15 minutes for the changes to take effect. However, you can force an update from the Standalone Sentry command line.
If there is a delay of fifteen minutes for Sentry to be updated, then to manually force an update, use Sentry CLI 
\texttt{accs config-fetch\{update\|force-update\}}.

The following changes cause Standalone Sentry to restart:
• Fetching updates for the first time
• Access hostname changes
• Access SSL cert changes
• Access port changes

\textbf{Before you begin}
Under the menu options, click \textbf{View Changes} to verify the changes.

\textbf{NOTE:} The profile Publish button is hidden when there is no change in the profile since the last publish. 
The Publish button is enabled only when the profile is modified since the last publish. Whenever the changes to configuration are reverted, the publish button disappears. It disappears if there is no actual change to the profile, since the last publish.

\textbf{Procedure}
1. In the MobileIron Access administrative portal, go to \textbf{Profile > Overview}.
2. Click \textbf{Publish}.
   \textbf{Publish} is only available if a pair has been created.
3. Click \textbf{OK}.

\textbf{Azure Hybrid Domain-Join with MobileIron Access}

Azure AD Join Configuration allows an administrator to enable Windows Transport endpoint for Windows device registration with Azure AD.

For more information, see the KB article at \url{https://community.mobileiron.com/docs/DOC-7533}.

\textbf{View federated pairs}

You can view the list of configured federated pairs in the MobileIron Access administration portal in \textbf{Profile > Federated Pairs}.
• Information and metadata for a SP and IdP pair
• Assigning a policy to a federated pair
• Editing a federated pair
• Deleting a federated pair

\textbf{Information and metadata for a SP and IdP pair}

For information and metadata for a federated pair, expand the row for the federated pair or click on the icons under \textbf{Actions}. 
FIGURE 36. FEDERATED PAIRS DETAILS

TABLE 10. FEDERATED PAIRS DETAILS

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name you entered for the federated pair.</td>
</tr>
<tr>
<td>Policy</td>
<td>Name of the conditional policy applied to the federated pair. For an Office 365 federated pair, the Passive Policy name is displayed.</td>
</tr>
<tr>
<td>Certificate SSO</td>
<td>Indicates whether certificate-based single sign-on is configured for the pair.</td>
</tr>
</tbody>
</table>
| Access SP Metadata (Upload to IdP) | MobileIron Access generates proxy metadata by combining the service provider metadata and the signing certificate. You upload the Access (SP) metadata to the IdP.  
  • Click Download to download the MobileIron Access proxy metadata for the SP.  
  • Click View to view the MobileIron Access proxy metadata for the SP.  
  • Click Copy URL to copy the proxy metadata and upload to IdP. |
| Access IDP Metadata (Upload to SP) | MobileIron Access generates proxy metadata by combining the IdP metadata and the signing certificate. You upload the Access (IdP) proxy metadata to the cloud service provider.  
  • Click the Download to download the MobileIron Access proxy metadata for the IdP.  
  • Click the View to view the MobileIron Access proxy metadata for the IdP.  
  • Click Copy URL to copy the proxy metadata and upload to SP. |
<p>| Actions                            |             |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign policy icon</td>
<td>Click to assign a conditional policy. For an Office 365 federated pair, you can choose a passive policy or an active logon policy.</td>
</tr>
<tr>
<td>Edit icon</td>
<td>Click to edit the settings for the federated pair.</td>
</tr>
<tr>
<td>Vertical three dots</td>
<td>Click for additional actions available for the federated pair:</td>
</tr>
<tr>
<td></td>
<td>• Delete: Click to delete the federated pair</td>
</tr>
<tr>
<td></td>
<td>• View SP Metadata: Click to view the metadata you uploaded for the cloud service provider (SP).</td>
</tr>
<tr>
<td></td>
<td>• View IDP Metadata: Click to view the metadata you uploaded for the identity provider (IdP).</td>
</tr>
<tr>
<td></td>
<td>• Download PowerShell Commands for ADFS: Click to download the PowerShell script to run the commands.</td>
</tr>
<tr>
<td></td>
<td>• Download PowerShell Commands for Office 365: Click to download the PowerShell script to run the commands.</td>
</tr>
</tbody>
</table>

### Assigning a policy to a federated pair

If a policy is not applied to a federated pair, the default policy is applied.

**NOTE:** During the initial setup, MobileIron recommends that you do not make changes to the default policy.

**Procedure**

1. In the MobileIron Access administration portal, go to **Profile > Federated Pairs**.
2. For the federated pair, click 📜.
3. In the Assign Policy dialog, from the Policy drop down list select a policy.
4. Click **Assign**.
5. Click **Publish**.

   If you do not **Publish** the changes, the updates are not applied.

**Related topics**

- Office 365 settings.
- Conditional Access.

### Editing a federated pair

If you make changes to a federated pair, change the metadata file, or the signing certificate, you must upload an updated proxy metadata file to the service provider and the IdP.

**Procedure**

1. In the MobileIron Access administration portal, go to **Profile > Federated Pairs**.
2. For the federated pair, click **Actions > Edit**.
3. After editing, click **Publish**.
   If you do not **Publish** the changes, the updates are not applied.

## Deleting a federated pair

The following provides the steps for deleting a federated pair.

**Procedure**

1. In the MobileIron Access administration portal, go to **Profile > Federated Pairs**.
2. For the federated pair, click **Actions > Delete**.
3. In the pop-up box, click **Delete**.
4. After deleting, click **Publish**.
   If you do not **Publish** the changes, the updates are not applied.

**NOTE:** Delete, removes the Federated pair from Access. However, to also remove Access from the federated login path to the service provider, you must establish or restore the direct federation between your service provider and identity provider.

## Renewing the SSL certificate

The following describes the steps to add a new SSL certificate when the current SSL certificate expires.

**Procedure**

1. Login to the MobileIron Access with administrator credentials.
2. In the **Overview** tab, scroll down to **Profile Details**.
3. Click the certificate in the **SSL Certificate Alias** field.
4. Click **Add new certificate**. The **Add SSL Certificate** windows displays.
5. Enter the **Certificate Name** and **Certificate Password**.
6. Under **SSL Certificate Upload**, click **Choose File**.
7. Upload the new SSL certificate to renew the certificate.
8. Click **Add SSL Certificate**.
   The SSL certificate is now renewed.

## Uploading proxy metadata

MobileIron Access generates proxy metadata by combining the cloud service provider (SP) or the identity provider (IdP) metadata and the signing certificate. The proxy meta data is automatically generated when you configure the SP and IdP in the MobileIron Access administrative portal.

You upload the proxy meta data to the SP and the IdP. When you upload the proxy meta data to the (SP) and the (IdP), you establish a three-way trust between the SP, IdP, and MobileIron Access. All authentication traffic now goes through MobileIron Access.
Before you begin
If your deployment is Access + Standalone Sentry:
- Ensure that a Standalone Sentry is registered on the MobileIron Access administrative portal.
- The Standalone Sentry is assigned to the profile.
- The profile with configured federated pair is published to Standalone Sentry.

Procedure
1. Get the proxy metadata from the MobileIron Access administrative portal:
   a. Go to Profile > Federated Pairs.
   b. Expand the row for the federated pair.
   c. For the Access service provider proxy metadata, click the Download link adjacent to Access(SP) Metadata.
      You will upload the Access(SP) Metadata file to the identity provider (IdP).
   d. For the Access identity provider proxy metadata, click the Download link adjacent to Access(IDP) Metadata.
      You will upload the Access(IDP) Metadata file to the cloud service provider (SP).
2. Upload the proxy metadata to cloud service provider (SP).
3. Upload the proxy metadata to identity provider (IdP).

Related topics
- For instructions on uploading the IdP proxy metadata to an SP, see the Knowledge Base article at https://community.mobileiron.com/docs/DOC-4099
- For instructions on uploading the SP proxy metadata to an IdP, see the Knowledge Base article at https://community.mobileiron.com/docs/DOC-4254

Verifying traffic flow
After you upload proxy metadata to the cloud service provider (SP) and identity provider (IdP), traffic will flow through MobileIron Access and Standalone Sentry. You can verify that authentication and access to the cloud service is working.

Procedure
1. On a mobile device use the service provider’s app to access the cloud service. You should be able to access the cloud service successfully.
2. On a desktop, access the cloud service. You should be able to access the cloud service successfully.
   The Reports > Access page displays the authentication traffic to which the default rule is applied. Standalone Sentry syncs with the MobileIron Access administrative portal every 15 minutes. It may take up to 15 minutes for the authentication traffic to display in Reports > Access.
4. Use the `debug accs check-in access-report` CLI command that forces Sentry to sync MobileIron Access reports to the cloud console.

Next steps
- Set up conditional rules.
  See Conditional Access.
Delegated IdP

The following provide more information about setting up Access as a delegated IdP:

- Delegated IdP overview
- Authentication flow with Access as the delegated IdP
- Configuring Access as the delegated IdP

Delegated IdP overview

In most cases MobileIron Access is deployed as a proxy between the service provider (SP) and the identity provider (IdP). In such a deployment, all federated SP traffic goes through MobileIron Access. In some cases, you may want to retain the existing SP-IdP federated setup, but deploy MobileIron Access to federate a sub set of the traffic, such as traffic from mobile devices. In such cases, MobileIron Access can be deployed as a delegated IdP rather than as a proxy to the IdP. If MobileIron Access is deployed as a delegated IdP, the original IdP is seen as an SP by MobileIron Access.

**Figure 37. Access as the IdP proxy**

**Figure 38. Access as the delegated IdP**

Access can be deployed as the delegated IdP only for the following IdPs:

- Idaptive
- Microsoft ADFS
- Okta
- PingFederate

In an Access configured as a delegated IdP:
To authenticate managed devices, configure certificate single sign-on (SSO) in the MobileIron UEM.

To authenticate unmanaged devices, you have the option to enable Unmanaged Device Authentication in Access. If authentication for unmanaged devices is enabled, the unmanaged device is redirected to the original IdP for forms-based authentication.

Authentication flow with Access as the delegated IdP

The following graphic provides the authentication flow with Access as delegated IdP for managed devices:

1. Users access a service provider (SP) from a managed app. The managed app triggers MobileIron Tunnel.
2. If the app does not have a valid session token, the SP issues an authentication request to the app and redirects the app to the identity provider (IdP).
3. The IdP issues a secondary authentication request based on the authentication request in step 2 and points the user to MobileIron Access (delegated IdP).
4. Access identifies the user based on the certificate used to establish the Tunnel VPN. Based on the information provided in the Tunnel certificate, Access generates an authentication response to the app and redirects to the original identity provider (IdP). Access determines the contents of the authentication response based on the Native Mobile Application Single Sign-On (SSO) configuration in Access, which includes the user identifying information that the SP expects.
5. The original IdP generates an authentication response to the app based on the authentication response in step 4 and redirects to the original SP.
6. The SP verifies the user information and creates a session token to the app. The session token gives the user access to the SP.
Configuring Access as the delegated IdP

Setting up MobileIron Access as the delegated IdP requires configuration in MobileIron UEM, Access, and in the IdP as well. Access supports delegation for the following IdPs: Idaptive, Microsoft ADFS, Okta, and PingFederate.

NOTE: Only authentication from managed devices is allowed for Delegated IDP with Idaptive pair.

The setup described here does not apply to an Access + Standalone Sentry deployment. If your deployment is Access + Standalone Sentry, see the following KB article: Access as Delegated IDP.

Overview of tasks

1. In MobileIron UEM, configure certificates for single sign-on. If single sign-on is configured, Access authenticates the user. Otherwise, the user is redirected to the original IdP for forms-based authentication.
2. In Access, enable Delegated IdP in Settings > Tenant Settings.
3. In Access, and set up the original IdP in Profile > Federation > Add Pair > Delegated IdP.
4. In the original IdP, set up delegation to Access.

Before you begin

Ensure the following:

- You have an existing federated authentication set up between the cloud service provider (SP) and the supported identity provider (IdP).
- In a delegated IdP setup, Access sees the IdP as an SP. Therefore, download the SP metadata from the IdP. If you are enabling authentication for unmanaged devices, also download the IdP metadata from the IdP. The following table provides links to instructions on how to get the metadata for your IdP.

<table>
<thead>
<tr>
<th>IdP</th>
<th>For instructions on how to get the metadata go to</th>
<th>Supported methods for providing metadata in Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idaptive</td>
<td>Download the metadata. See the Cookbook for Idaptive.</td>
<td>Upload metadata</td>
</tr>
<tr>
<td>ADFS</td>
<td>Download metadata from https://&lt;YourADFS&gt;/FederationMetadata/2007-06/FederationMetadata.xml</td>
<td>Upload metadata</td>
</tr>
<tr>
<td>Okta (Manual Setup)</td>
<td><a href="https://community.mobileiron.com/docs/DOC-8295">https://community.mobileiron.com/docs/DOC-8295</a>.](<a href="https://community.mobileiron.com/docs/DOC-8295">https://community.mobileiron.com/docs/DOC-8295</a>). See the &quot;How to get Metadata from Okta as SP for Access&quot;</td>
<td>Upload metadata</td>
</tr>
<tr>
<td>IdP</td>
<td>For instructions on how to get the metadata go to</td>
<td>Supported methods for providing metadata in Access</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Okta (Automated Setup)</td>
<td>section for instructions on downloading the SP metadata from Okta. See the “How to get Metadata from Okta as IdP for Access” section for instructions on downloading the IdP metadata from Okta. Required only for enabling authentication for unmanaged devices.</td>
<td>Enter metadata URL</td>
</tr>
<tr>
<td>PingFederate</td>
<td>Cookbook for configuring Okta as delegated IDP See “Step 1: Creating an application and download the metadata for Okta” section for instructions on downloading the metadata from Okta.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: If the okta admin wants to unhide the Access application created from the automated workflow, they can do so by from Okta console. For more information, see the cookbook.</td>
<td></td>
</tr>
</tbody>
</table>

- If single sign-on is configured in MobileIron UEM, SCEP obtains user information from LDAP. Therefore, ensure that the LDAP settings in MobileIron UEM fetch the appropriate attributes from LDAP. The Tunnel certificate is setup to include the mapping to a certificate field for certificate native mobile application single sign-on (SSO). The following tables describe the certificate field mapping for MobileIron Cloud and MobileIron Core.

### TABLE 12. MOBILEIRON TUNNEL CERTIFICATE FIELD MAPPING IN MOBILEIRON CLOUD

<table>
<thead>
<tr>
<th>LDAP for MobileIron Cloud deployments</th>
<th>Certificate</th>
<th>SAN Type in SCEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idaptive</td>
<td>${userEmailAddress}</td>
<td>RFC 822 Name</td>
</tr>
<tr>
<td>ADFS</td>
<td>${userEmailAddress}</td>
<td>RFC 822 Name</td>
</tr>
</tbody>
</table>
To make it easier to configure mobile application single sign-on, upload a sample Tunnel certificate and assign user friendly names to each field in the certificate. For more information, see User Certificates.

**Procedure**

1. In MobileIron Access, go to **Settings > Tenant Settings**.
2. For **Delegated IDP**, click the toggle to **ON** to enable delegated IdP.
3. Navigate to Profile > Federation.

![Federation Profile]

**FIGURE 40. FEDERATION PROFILE**

4. Click Add Pair and select Delegated IdP.

![Select IDP for Delegation]

**FIGURE 41. SELECT IDP FOR DELEGATION**

5. Click the appropriate IdP to configure identity provider settings.
   Select Custom Identity Provider for any other provider other than the available identity providers.

6. Select the signing certificate.
   A default signing certificate is selected. You can select a different signing certificate from the drop-down list.

7. Select "Validate signature for authentication requests sent by the service provider". For backward compatibility, this option is unchecked for the existing pairs. Ensure that the SP/IdP metadata is updated and enable the checkbox.

8. (Optional) Select the check box for Encrypt SAML assertions.

9. Upload the service provider (SP) metadata from the original identity provider (IdP).
10. For mobile app single sign-on do the following:
   a. From the Reference Client Certificate drop-down list, select the sample Tunnel certificate.
   b. In the SAML Subject Configuration section:
      - For Type:
        - If your IdP is Idaptive, select Email.
        - If your IdP is ADFS, select Persistent.
        - If your IdP is Okta, select Email.
        - If your IdP is PingFederate, select Email.
      - For Get Value From, select SAN of type rfc822Name.
        The instance maps to the order it is listed in the certificate configuration in UEM.
   c. (Only if your IdP is ADFS) In the SAML Attribute Configuration section:
      NOTE: SAML Attribute Configuration is not needed for Okta and PingFederate, irrespective of the SP.

<table>
<thead>
<tr>
<th>Name</th>
<th>Get Value from</th>
<th>Additional transforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserID</td>
<td>SAN of type rfc822Name</td>
<td>-</td>
</tr>
<tr>
<td>UserDomain</td>
<td>SAN of type directoryName:</td>
<td>dn:domain</td>
</tr>
<tr>
<td></td>
<td>Instance 1</td>
<td></td>
</tr>
</tbody>
</table>

   d. If you selected Encrypt SAML assertions, select the encryption algorithms.
      The options for encryption algorithms are only visible if you selected Encrypt SAML assertions.

11. Click Next.

12. (Optional for Okta Manual Setup) For Unmanaged Device Authentication, check Enable policy and configurations for handling authentication of Unmanaged Mobile Devices via IdP.
   Enabling the option directs authentication traffic from unmanaged devices to the original IdP for forms-based authentication.
   If the original IdP is Okta or PingFederate, the option to upload IdP metadata becomes available.
   This option is not available for ADFS because the metadata for ADFS, uploaded earlier in the configuration, includes both SP and IdP metadata.

   NOTE: This set up is for Okta manual setup only. Follow the Cookbook for Okta automated setup for automated setup.
13. (Optional) For Okta or PingFederate, if you enabled **Unmanaged Device Authentication**, upload the IdP metadata downloaded from the respective IdP.

14. Click **Done** to complete the configuration.

15. In **Profile > Federation**, click on the IdP listed in **Delegated IdP** and download the **Access IdP Metadata**. If **Unmanaged Device Authentication** is enabled, you will also see **Access SP Metadata**. Download the Access SP metadata as well.

16. (Optional) If your IdP is ADFS, click **Download the Powershell Command for ADFS**.

**NOTE:** If there are changes to the SP or delegated IDP metadata, Access detects these changes and notifies the administrator via email. The following alert message also displays for the federated pair in **Access > Delegated IDP**: **SP/Application metadata (IDP) has changes**. For the delegated IDP, click **Actions > Sync SP/Application metadata (IDP)** to update the metadata file in Access. An email notification is sent to the Access administrator after the sync.

**Next steps**

- Set up the IdP for delegation to Access. This includes uploading the Access IdP, and the Access SP, if applicable, metadata to the IdP. Upload the Access IdP metadata in the IdP where delegations are configured. Upload the Access SP metadata in the IdP where service providers are configured. Do one of the following:
  - If your IdP is ADFS, run the PowerShell script in ADFS. This is the same PowerShell script you downloaded from Access. The PowerShell script contains the commands to setup delegation to Access.
    See **PowerShell commands for ADFS**.
    See also **Using Access as a Delegated IdP for ADFS**.
  - If your IdP is Okta, see Okta as Delegated IdP (Manual Setup) and Okta as Delegated IdP
Automated Setup).
  - If you IdP is PingFederate, see Access as Delegated IdP for PingFederate

- If you enabled unmanaged device authentication, ensure that the conditional policies applied to the Delegated IdP configuration does not block unmanaged devices.

Related topics
  - Signing certificates
  - Identity provider (IdP) metadata
  - Encrypting SAML assertions
  - Conditional policies

PowerShell commands for ADFS

MobileIron Access provides PowerShell scripts for the following:

- Set up Access as the delegated IdP in ADFS
- Create a new Access theme in ADFS for iPads running iOS 13

The PowerShell scripts eliminate the need to copy and paste the commands. The PowerShell scripts can be downloaded from Profile > Federation and run on your machine.

The following describes how to use the PowerShell scripts:

- Running the PowerShell script to set up Access as the delegated IdP in ADFS
- Using the PowerShell script to create a new Access theme in ADFS for iPadOS 13 upgrades

Running the PowerShell script to set up Access as the delegated IdP in ADFS

The commands to set up Access as the delegated IdP in ADFS are provided as a PowerShell batch script that can be downloaded and run on your machine. After you create a delegation for ADFS in Access, the link to download the PowerShell batch script becomes available in the listing for the delegated IdP in Profile > Federation.

Running the script as described allows you to set up Access as a Claims Provider Trust in ADFS. When Access presents its claims to ADFS, ADFS serves the corresponding Relying Party, such as Office 365 or Salesforce, and allows the user to authenticate to the Relying Party. The Relying Party, such as Office 365 or Salesforce, must also be configured in ADFS.

If authentication of unmanaged devices is enabled in the delegated IdP configuration in Access, the PowerShell script also adds Access as a Relying Party with all required claims in ADFS.
Before you begin

- Ensure that you have PowerShell Administrator permissions.
- Depending on your ADFS version, run one of the following commands to get the Active Directory identifier:
  - For ADFS 4.0: `(Get-AdfsClaimsProviderTrust -Name "Active Directory").Identifier`
  - For ADFS 3.0: `Get-ADFSProperties`
    Look for the value for `Identifier`.

Procedure

1. Download the PowerShell script.
   a. In Access, go to Profile > Federation.
   b. For the ADFS listed, click the three vertical dots in Actions.
   c. Click Download Powershell Commands for ADFS to download the script.

2. Run the following command in PowerShell:

   ```bash
   .\MICROSOFT_ADFS_SP_WSFSFED-script.ps1 -activeDirectoryIdentifier "ActiveDirectoryIdentifier" -sourceAdfsWebThemeName default -targetAccessWebThemeName "AccessThemeName"
   ```

   You will be prompted to enter values specific to your environment.

   For `ActiveDirectoryIdentifier`, enter your enterprise Active Directory identifier.

   For `AccessThemeName`, enter any name. This the web theme name for Access. ADFS automatically creates the web theme name based on the name you enter.

Using the PowerShell script to create a new Access theme in ADFS for iPadOS 13 upgrades

The iPadOS 13 upgrade PowerShell script creates a new Access theme in ADFS so that authentication traffic from iPads running iPadOS 13 is redirected to Access.

Note The Following:

- The iPadOS 13 upgrade PowerShell script becomes available only if you have an existing delegated IdP setup with ADFS. If you are creating a new delegated IdP setup with ADFS, follow the procedure in Running the PowerShell script to set up Access as the delegated IdP in ADFS.
- The upgrade script does not overwrite or delete any existing web theme in your environment. It creates a new theme from an existing source theme that you specify.

Before you begin

Ensure that you have PowerShell Administrator permissions.
Procedure

1. Download the PowerShell script.
   a. In Access, go to **Profile > Federation**.

   ![Figure 43. iPadOS 13 update script](image)

   - **IDP**: Microsoft
   - **Name**: msentry11
   - **Policy**: Default Policy
   - **Created On**: 2019/06/06 4:45 PM

   **Access IDP Metadata (Upload to IDP)**: View | Download | Copy URL
   **Access SP Metadata (Upload to IDP)**: View | Download | Copy URL

   Safari 
   **iPadOS 13 Upgrade PowerShell Script**: Download

   b. For the ADFS listed, for **iPadOS 13 Upgrade PowerShell Script**, click **Download**.

2. Run the following command in PowerShell:
   
   `MICROSOFT_ADFS_SP-iPadOS13-upgrade-script.ps1`

3. Enter values that are specific to your environment.
   - **ActiveDirectoryIdentifier**: enter your enterprise Active Directory identifier.
   
   Run one of the following commands to get the Active Directory identifier based on the version of ADFS:
   
   - For ADFS 4.0: `(Get-AdfsClaimsProviderTrust -Name "Active Directory").Identifier`
   - For ADFS 3.0: `Get-ADFSProperties
     Locate the value for Identifier`.

4. Enter the source web theme name from which to create the new web theme.
   
   **TIP**: Enter the existing Access web theme name. A duplicate of the Access web theme is created.

5. Enter a new target web theme name for the new web theme.
   
   ADFS automatically creates a new web theme name based on the name you enter.
   
   If you provide an existing web theme name, the script prompts you to enter a new name.

After the new web theme is created, you are presented with the following options:

- **Apply customized ADFS web theme to all Relying Party Trusts**: Select this option to apply the new web theme to all Relying Party Trusts.

- **Do not apply ADFS web theme now. Exit**: Select this option to save the web theme and exit PowerShell without applying to any Relying Party Trusts. If you need to apply the new web theme to only some Relying Party trusts in your environment, contact your ADFS administrator.
Conditional Access

MobileIron Access allows you to define which applications and IP network ranges can access a cloud resource. You define the apps and IP network ranges that can access the cloud resource in conditional policies and rules in Access.

Conditional policies

A conditional policy is a set of conditional rules, which can be applied to a federated pair. A conditional policy can contain multiple conditional rules.

A default policy is automatically created when you do the initial setup through the setup wizard. The default policy is automatically applied to a federated pair if no other policy is applied. You cannot delete the default policy, you can only edit it. The default policy automatically includes a set of predefined rules. You can create additional policies. However, only one policy can be applied to a federated pair with the exception of the Active Logon policy, which can be applied in addition to another policy.

You can do the following in a policy:
• Add or delete rules.
• Move rules up or down in the list.
• Change the action on a rule.
• Disable rules.

Adding a new conditional policy

To add a new conditional policy in MobileIron Access, go to Profile > Conditional Access.

Before you begin

Before you create conditional access policies and rules, verify that traffic is flowing as expected between MobileIron Access, the identity provider (IdP), and the cloud service provider (SP). See Verifying traffic flow

Procedure

1. In the MobileIron Access administrative portal, go to Profile > Conditional Access.
2. Click +Add Conditional Policy to add a new conditional policy. The new policy is created.
3. Edit this policy appropriately. You can enter a name and description for the policy.

NOTE: The General Bypass rule is created by default when you add a new policy.
4. Click Publish to make the changes available.
Conditional rules

Conditional rules define which app, devices, or users are allowed or blocked access to the service provider. Conditional rules are contained in a policy. The rules are applied in the order they are listed in the policy. The top row is evaluated first. If the rule condition is not met, the next rule is evaluated. If rule condition is met, the action associated with the rule is taken and all other rules are skipped. You can change the order of the rules by moving the rule either up or down in the list.

Conditional rules allow or block access to a cloud resource based on the following:

- Tunnel information
- User information
- IP network range
  
  You can limit traffic to allow only the configured IP network range, or block traffic from the configured IP network range.

TIP: Go to **Reports > Access** to view the source IP for the authentication traffic.

- Source IP or headers added by a HTTP proxy or load balancer.
- User agent (app) accessing the cloud service
  
  The user agent is a short string provided by the app accessing the cloud service. The user agent string identifies the app.

TIP: Go to **Reports > Access** to view the user agent string for the authentication traffic.

Adding a conditional rule

You add a conditional rule to a conditional policy.

**Procedure**

1. In the MobileIron Access administrative portal, go to **Profile > Conditional Access**.
2. Expand the policy row to which you want to add the conditional rule.
3. Click **+Add Rule** to add a new conditional rule.
4. Click a predefined or customizable rule.
5. Complete the requested fields for the rule.
6. Click **Done** to save the rule.
   
   The rule appears at top of the list. To reorder the list, select the rule and move it to the preferred position in the list.
7. Click **Publish** to make the changes available.

**Related topics**

- Predefined conditional rules
- Customizable conditional rules

Predefined conditional rules

MobileIron Access provides a set of predefined conditional rules. These rules are automatically added to the default policy when the default policy is created. You cannot change a predefined rule. You can do the following to a predefined rule:
The General Bypass rule is a special predefined rule that is automatically added to all new policies and it is the last rule in the policy. The rule cannot be moved up in the list or be disabled. You can only change the action on the rule.

<table>
<thead>
<tr>
<th>Rule name</th>
<th>Description</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted App and Device</td>
<td>Determines whether conditional access rules are applied to apps that use AppTunnel. These apps are AppConnect apps that use AppTunnel and managed apps that use Tunnel.</td>
<td>Allow</td>
</tr>
<tr>
<td>Untrusted Apps on iPad</td>
<td>Determines if unmanaged apps on an iPad are allowed or blocked.</td>
<td>Block</td>
</tr>
<tr>
<td>Untrusted Apps on iPhone</td>
<td>Determines if unmanaged apps on an iPhone are allowed or blocked.</td>
<td>Block</td>
</tr>
<tr>
<td>Untrusted Apps on Android</td>
<td>Determines if unmanaged apps on Android are allowed or blocked.</td>
<td>Block</td>
</tr>
<tr>
<td>Untrusted Apps on Windows 10</td>
<td>Determines if unmanaged apps on Windows 10 are allowed or blocked.</td>
<td>Block</td>
</tr>
<tr>
<td>Android for Work Registration</td>
<td>Determines whether the untrusted devices are enabled to register for Android for work.</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>NOTE: If your deployment is Access + Standalone Sentry, ensure that your Standalone Sentry version is 8.5.0 through the most recent version as supported by MobileIron.</td>
<td></td>
</tr>
<tr>
<td>iOS Native Email OAuth</td>
<td>Controls (allow/block) access to the IdP from iOS 10.3 native email client using OAuth.</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>NOTE: This rule is not automatically added to the default policy.</td>
<td></td>
</tr>
<tr>
<td>General Bypass</td>
<td>Determines if unmanaged apps on devices are allowed or blocked. This rule cannot be deleted, disabled, or moved up in the list. You can only edit this rule.</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Customizable conditional rules

You can customize the following set of conditional rules:
- **Tunnel Rule.** For more information, see Tunnel rule.
• **User Info Rule.** For more information, see [User Info Rule](#).
• **Network Rule.** For more information, see [Network Rule](#).
• **App Rule.** For more information, see [App Rule](#).
• **Advanced Network Rule.** For more information, see [Advanced Network Rule](#).
• **Multi-Factor Authentication:** For more information, see [Multi-factor Authentication](#).
• **Request Header Rule:** For more information, see [Request Header Rule](#).
• **Desktop Trust Rule.** For information, see [Desktop Trust Rule](#).

### Tunnel rule

Add a Tunnelled rule to control access for tunneled apps. The following describes the fields in the Tunnel Rule.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text for the rule.</td>
</tr>
<tr>
<td>Action</td>
<td>From the drop down menu, select one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Allow:</strong> Allows traffic from the specified Tunneled application.</td>
</tr>
<tr>
<td></td>
<td><strong>Block:</strong> Blocks traffic from the specified Tunneled application.</td>
</tr>
<tr>
<td></td>
<td><strong>Warn:</strong> Warns traffic from the specified Tunneled application.</td>
</tr>
<tr>
<td></td>
<td><strong>Follow Policy:</strong> Applies the conditional policy that you choose from the existing list.</td>
</tr>
</tbody>
</table>

### User Info Rule

Add a User Info Rule to control access for an user or an user group. By default, all the fields in the SAML assertion, including subject and any attributes are matched against the values specified in this rule.

- Add attribute names in this rule if you want to match the values specified in this rule only to the attribute you specify here.
- If you want the values specified in this rule to match all attributes, use the attribute name ".*". Values can be user IDs or group IDs. If you configure your Identity Provider to include a group ID to match against, it enables you to configure a small list of group IDs instead of a large list of individual user IDs.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text for the rule.</td>
</tr>
<tr>
<td>SAML Assertion Field</td>
<td>Select the <strong>SAML Subject</strong> checkbox if you want the UserInfoRule to match the SAML Subject. The default option is set to true.</td>
</tr>
</tbody>
</table>
### Table 16. User Info Rule Field Description (Cont.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Match With** | From the drop-down menu, select one of the following:  
• **Add**: Lets you add users to the list to configure the rule.  
• **Upload to Append**: Lets you upload a text file with one user or group per line.  
• **Upload to Replace**: Lets you replace the existing list of users with a new list of users in a new text file.  
NOTE: MobileIron recommends to use .txt format files to upload the users. The file must contain only one user per line. |
| **Action** | From the drop-down menu, select one of the following:  
• **Allow**: Allows traffic from the specified User or User group.  
• **Block**: Blocks traffic from the specified User or User group.  
• **Warn**: Warns traffic from the specified User or User group.  
• **Follow Policy**: Applies the conditional policy that you choose from the existing list. |

### Network Rule

Add a Network Rule to control access from an IP network range. The following describes the fields in a Network Rule.

**Table 17. Network Rule Field Description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter descriptive text for the rule.</td>
</tr>
</tbody>
</table>
| **Action** | From the drop-down menu, select one of the following:  
• **Allow**: Allows traffic from the specified IP address range.  
• **Block**: Blocks traffic from the specified IP address range.  
• **Warn**: Warns traffic from the specified IP address range.  
• **Follow Policy**: Applies the conditional policy that you choose from the existing list. |
TABLE 17. NETWORK RULE FIELD DESCRIPTION (CONT.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start IP Mask or CIDR</td>
<td>Enter the start address for the IP address range.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The IP address can be in the form of an IPv4 address or CIDR.</td>
</tr>
<tr>
<td>End IP Mask or CIDR Network Address</td>
<td>Enter the end address for the IP range.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The IP address can be in the form of an IPv4 address or CIDR.</td>
</tr>
</tbody>
</table>

App Rule

Add an App Rule for an app or device platform to allow or block the app or device platform. The following describes the fields in an App Rule.

TABLE 18. APP RULE FIELD DESCRIPTION

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the conditional rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text for the conditional rule.</td>
</tr>
<tr>
<td>Action</td>
<td>From the drop down menu, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>Allow: Allows traffic from the specified Application.</td>
</tr>
<tr>
<td></td>
<td>Block: Blocks traffic from the specified Application.</td>
</tr>
<tr>
<td></td>
<td>Warn: Warns traffic from the specified Application.</td>
</tr>
<tr>
<td>Follow Policy</td>
<td>Applies the conditional policy that you choose from the existing list.</td>
</tr>
<tr>
<td>Matching Algorithm</td>
<td>From the drop down menu, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>Regex: Select if you plan to use a regular expression for the user agent.</td>
</tr>
<tr>
<td></td>
<td>Wildcard: Select if you plan to use wildcard for the user agent</td>
</tr>
<tr>
<td></td>
<td>Literal: Select if the rule should exactly match the configured expression.</td>
</tr>
<tr>
<td>Expression</td>
<td>Enter an expression for the app, based on the matching algorithm you selected.</td>
</tr>
<tr>
<td>TIP</td>
<td>Check the Reports view to see the user agents in the traffic for authentication.</td>
</tr>
<tr>
<td>Case Sensitive</td>
<td>Select if the rule should consider the case configured in the expression.</td>
</tr>
<tr>
<td>Partial Match</td>
<td>Select if the rule can be applied to a partial match of the configured expression.</td>
</tr>
</tbody>
</table>
Advanced Network Rule

Add an advanced network conditional rule to control access based on source IP and/or headers added by an HTTP proxy or load balancer. For more information, see https://community.mobileiron.com/docs/DOC-7127.

**Figure 44. Adding Advanced Network Rule**

Create Advanced Network Rule

Rule to control access based on source IP or headers added by an HTTP proxy or load balancer.

How do I configure rules?

**Source IP Setting**

- **Source IP Ranges**
  
  This action is applied only if source IP address belongs to any of the following IP addresses or ranges.

- **Excluded Source IP Ranges**
  
  This action is not applied if source IP address matches any of the following IP addresses or ranges. Use to exclude certain sub IP ranges.

**IPv4 or CIDR Network Address(es)**

- **IPv4 or CIDR Network Address(es)**

  0 Item(s)

  Add New

**Configure Header Rule**

- **Header Rule Configuration**

  - **HTTP Header**
    
    Select the HTTP header containing client IP addresses.

  - **X.Forwarded.For**

  
  - **Header IP Ranges**
    
    This action is applied only if the configured HTTP header contains a client IP address belonging to any of the following IP addresses or ranges.

  - **Ignored Header IP Ranges**

    If the configured HTTP header contains an IP address belonging to any of the following IP addresses or ranges, that IP address in the HTTP header is ignored.

**IPv4 or CIDR Network Address(es)**

- **IPv4 or CIDR Network Address(es)**

  0 Item(s)

  Add New

**Rule Action**

- **Select Action**

The following describes the fields in an Advanced Network Rule.
### TABLE 19. ADVANCED NETWORK RULE FIELD DESCRIPTION

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the conditional rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text for the conditional rule.</td>
</tr>
<tr>
<td><strong>Source IP Setting</strong></td>
<td></td>
</tr>
<tr>
<td>Source IP Ranges</td>
<td>• Click <strong>Add New</strong> to add the IP address manually. Enter the Source IP address range that must be IPv4 or CIDR Network Address. For example: 192.168.0.1 or 192.168.0.0/24</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Upload to Append</strong> to upload a fine and append the IP addresses to the existing IP address. Select <strong>Upload to Replace</strong> to replace all the IP address with the IP address from the uploaded file. Upload a text file containing the IP addresses in CIDR format or the normal IP Address format. The maximum number of allowed entries of IP address(es) in the text file is 1000 for successful upload of IP address(es).</td>
</tr>
<tr>
<td>Excluded Source IP Ranges</td>
<td>Exclude Source IP range is required when you have a large IP range that to configure for source IP and exclude subsets of that range from the consideration. For example: The rule must be configured for the range 192.168.0.0 – 192.168.0.255. However, you might not want IP ranges from this set. The IP ranges to be excluded are 192.168.0.0 – 192.168.0.3 and 192.168.0.8 – 192.168.0.11.</td>
</tr>
<tr>
<td></td>
<td>a. Configure the source IP range as 192.168.0.0/24.</td>
</tr>
<tr>
<td></td>
<td>b. In exclude IP range, add 192.168.0.0/30 and 192.168.0.8/30.</td>
</tr>
<tr>
<td>Procedure</td>
<td>• Click <strong>Add New</strong> to enter the sub IP address range that you wish to exclude from the Source IP ranges. For example: 192.168.0.1 or 192.168.0.0/24</td>
</tr>
<tr>
<td></td>
<td>• Use the drop-down list to <strong>Upload to Append</strong> or <strong>Upload to Replace</strong> an IP address range. You must upload a plain text file with each line containing an IP address or a CIDR network. The maximum number of IP range entries supported is 1000.</td>
</tr>
<tr>
<td><strong>Configure Header Rule</strong></td>
<td>Select the check-box to configure the Header Rule. By default, this checkbox is enabled. Deselect the checkbox to create a rule without headers.</td>
</tr>
<tr>
<td><strong>Header Rule Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>HTTP Header</td>
<td>Select one of the HTTP header types containing client IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• X-Forwarted-For</td>
</tr>
<tr>
<td></td>
<td>• X-MS-Forwarded-Client-IP</td>
</tr>
<tr>
<td>Header IP Ranges</td>
<td>• Click <strong>Add New</strong> to enter the Header IP range that contains a client IP address. For example: 192.168.0.1 or 192.168.0.0/24</td>
</tr>
</tbody>
</table>
TABLE 19. ADVANCED NETWORK RULE FIELD DESCRIPTION (CONT.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Setting</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Configure Header Rule</td>
<td>X-Forwarded-For and upload a .txt file (including the static IP)</td>
</tr>
<tr>
<td>Rule action: Allow</td>
<td></td>
</tr>
<tr>
<td>Set the General bypass rule</td>
<td>to Block.</td>
</tr>
</tbody>
</table>

All the source IPs are valid unless the IP matches, it is blocked by General bypass rule.

Multi-factor Authentication

For information about adding the multi-factor authentication rule, see Multi-factor Authentication with MobileIron Authenticator.
Zero Sign-on Rule

For more information about adding the Zero Sign-on rule, see Fast Identity Online (FIDO2) or Zero Sign-on with MobileIron Access

Desktop Trust Rule

For information about adding a desktop trust rule, see the MobileIron Access Desktop Trust Agent Guide.

Request Header Rule

Add the Request Header Rule to match the value of a HTTP request header with a specified pattern. The Request Header rule is very similar to the App rule; however, you can select any header name other than just the User-Agent.

Use case: When the user has MobileIron Access federated with Microsoft ADFS and Office 365 and then tries to register a device, it gets blocked by the untrusted Apps on Windows 10 rule. If you use the Azure Domain integration, then the actual MDM registration is also done by Azure.

Due to the current policies, there is no option to allow device registrations on these Windows 10 devices except from allowing Edge.

The new Request Header Rule thus helps to match the value of any HTTP request header with a specified pattern.
Figure 45. Request Header Rule

The following table lists the fields in a Request Header Rule:

Table 20. Request Header Rule Field Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the conditional rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text for the conditional rule.</td>
</tr>
<tr>
<td>Request Header Name</td>
<td>Enter any appropriate header name such as User-Agent.</td>
</tr>
<tr>
<td>Matching Algorithm</td>
<td>From the drop-down menu, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>Regex: Select if you plan to use a regular expression the header name.</td>
</tr>
</tbody>
</table>
TABLE 20. REQUEST HEADER RULE FIELD DESCRIPTION (CONT.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wildcard: Select if you plan to use wildcard for the header name. Literal: Select if the rule should exactly match the configured expression.</td>
<td></td>
</tr>
<tr>
<td>Expression</td>
<td>Enter an expression for the app, based on the matching algorithm you selected.</td>
</tr>
<tr>
<td>TIP: Check the Reports view to see the header name that you mentioned in the traffic for authentication.</td>
<td></td>
</tr>
<tr>
<td>Case Sensitive Select if the rule should consider the case configured in the expression.</td>
<td></td>
</tr>
<tr>
<td>Partial Match Select if the rule can be applied to a partial match of the configured expression.</td>
<td></td>
</tr>
<tr>
<td>Remember decision across requests of a single login Select this checkbox to remember the action for the first request and to apply the same action for the rest of the requests. This action skips the rule evaluation for the remaining requests of SP login.</td>
<td></td>
</tr>
<tr>
<td>Action From the drop down menu, select one of the following: Allow: Allows traffic from the specified Application. Block: Blocks traffic from the specified Application. Warn: Wams traffic from the specified Application. Follow Policy: Applies the conditional policy that you choose from the existing list.</td>
<td></td>
</tr>
</tbody>
</table>

Policy chaining

You can chain a conditional policy to a conditional rule in another policy. When the conditional rule is evaluated and the conditions in the rule are met, the conditional rules in the chained policy are also evaluated. This allows you to configure additional conditionals rules to be evaluated for the original rule. This is called policy chaining and allows additional flexibility in evaluating which apps and IP network ranges can access a cloud resource. You can choose a policy from the existing list of policies for a rule to follow. You can chain only one policy to a rule.
Example setup with conditional rules

In the setup described in this section, traffic from managed apps using AppTunnel (AppConnect apps using AppTunnel and managed apps using Tunnel) on an iPhone or iPad, and all traffic from laptops, desktops, and Android and Windows 10 mobile devices flows through MobileIron Access.

- Setup with conditional
- Expected behavior with the example setup

Setup with conditional

The following outlines the example setup with conditional rules:

- Configure Salesforce service provider and related IdP in Federated Pairs.
- Apply Tunnel VPN to the Salesforce app.
- Configure the following rules in Conditional Access:

<table>
<thead>
<tr>
<th>Conditional rule name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted App and Device on iOS</td>
<td>Allow</td>
</tr>
<tr>
<td>Untrusted Apps on iPhone</td>
<td>Block</td>
</tr>
<tr>
<td>Untrusted Apps on iPad</td>
<td>Block</td>
</tr>
<tr>
<td>General Bypass</td>
<td>Allow</td>
</tr>
</tbody>
</table>

NOTE: The order of the rules matters. Rules are evaluated in the order they appear.

Expected behavior with the example setup

The following outlines the expected behavior with the example setup:

- Traffic from the managed Salesforce app on an iPhone and on an iPad will be allowed through MobileIron Access. This setup allows apps such as Web@Work that use AppTunnel to also authenticate to Salesforce.
- All other traffic from iPhone and iPad will not be allowed through MobileIron Access.
- Therefore, on an iPad or iPhone, only traffic from the managed Salesforce app and any apps that use AppTunnel will have access to Salesforce.
- This setup allows users on other devices to continue to access Salesforce. Other devices include desktops, laptops, and Windows 10 and Android mobile devices.

For additional examples, see https://community.mobileiron.com/docs/DOC-4100.

Managing policies and rules

You can take the following actions on a conditional policy or rule:

- Disable: Disables the conditional rule. The rule is no longer applied.
• Delete: Deletes the conditional rule or policy. You cannot delete a policy that is applied to a federated pair, however you can delete conditional rules in that policy.
• Edit: Allows you to edit the settings in a policy or a rule.
• Reorder: Allows you to reorder the position of the conditional rule.

Applying a conditional policy to a federated pair

See Assigning a policy to a federated pair.

Editing a conditional policy

Procedure
1. In the MobileIron Access administrative portal, go to Profile > Conditional Access.
2. To edit the name of a conditional policy, click on the edit icon next to the policy name.
3. To edit the description for a policy, click on the edit icon next to the descriptive text.
4. To make changes to the conditional rules in a policy, click on the directional arrow to expand the policy. See Editing a rule.
5. Click Publish to push the changes associated with the Profile.

Deleting a conditional policy

Procedure
1. In the MobileIron Access administrative portal, go to Profile > Conditional Access.
2. Click on the trash icon next to the policy name you want to delete.
3. In the pop up window, click Delete Policy.
4. Click Publish to update the changes associated with the Profile.

 Editing a rule

Procedure
1. In the MobileIron Access administrative portal, go to Profile > Conditional Access.
2. Click on the directional arrow to expand the policy you want to edit.
3. Click on the Edit icon for the conditional rule you want to edit. For a description of the fields, see Customizable conditional rules.
4. Click Done to save the changes.
5. Click Publish to update the changes associated with the Profile.

Disabling, enabling, or deleting a rule

Procedure
1. In the MobileIron Access administrative portal, go to Profile > Conditional Access.
2. Click on the directional arrow to expand the profile you want to edit.
3. For each conditional rule you can do the following:
   - Disable: The rule is no longer applied.
   - Enable: Enables the conditional rule. The rule is applied in the order in which it is listed.
   - Edit: Modifies the conditional rule.
- Delete: Deletes the conditional rule.
- Reorder: Move the conditional rule higher or lower in the list.

4. Click **Publish** to update the changes associated with the Profile.

## Enabling the compliance remediation page

If a device is not in compliance, authentication traffic to Access is blocked and the user is presented with an Internet unavailable error. The error is logged in Access in **Reports > Errors**.

Enabling Compliance Remediation Page allows you to specify a customized remediation page to the device user.

**Note The Following:**

- This feature is not available for Access + Standalone Sentry deployments.
- If split tunneling is configured, only authentication traffic is blocked. All other traffic is allowed to destination.

**Before you begin**

Ensure that you have created a remediation page to present to users from non-compliant devices. For information on creating a custom remediation page, see **Adding a remediation page**.

### Procedure

1. In MobileIron Access, navigate to **Profile > Conditional Access**.
2. For **Compliance Remediation Page**, slide the toggle to **ON**.

3. From the drop-down list, select a remediation page.
   The remediation page is presented to users attempting to access a cloud service from a non-compliant device.
4. Click **Save** and publish the changes.
Configuring Mobile App Single Sign-on (SSO)

In an Access deployment, single sign-on (SSO) allows users access to enterprise cloud services from the apps on their mobile devices without having to enter passwords. Single sign-on is available only for managed apps, including the Safari browser, on managed devices using MobileIron Tunnel. Access identifies the user based on the certificate used to establish the VPN tunnel. Based on the information provided in the certificate, Access generates a federation response to the service provider (SP) without redirecting the user to the original identity provider (IdP). Access determines the contents of the federation response based on the Native Mobile Application Single Sign-On (SSO) configuration in Access, which includes the user identifying information that the SP expects.

The user identifying information that the SP expects is typically available in the enterprise LDAP directory. The UEM SCEP that Tunnel uses captures the user information from LDAP and makes the information available in the Tunnel certificate. The Native Mobile Application Single Sign-On (SSO) configuration uses the information from the Tunnel certificate in the federation response to the SP.

This feature is also referred to as certificate-based single sign-on.

Before you begin

- Ensure that the user identifying information that the service provider (SP) expects is available in the Tunnel certificate.
  
  The following are examples of user identifying information:
  
  - Email address
  - Immutable ID

- Configure the subject alternative names in the SCEP setting for the Tunnel certificate in the UEM.
  
  Example: If you are using the email address and immutable ID as the user identifying information, configure the following in the subject alternative name:

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 822 Name</td>
<td>$EMAIL$</td>
</tr>
<tr>
<td>NT Principal Name (Required only for Office 365, holds the unique immutable ID)</td>
<td>$USER_CUSTOM1$</td>
</tr>
</tbody>
</table>

- SCEP obtains users information from LDAP. Therefore, ensure that the LDAP settings in MobileIron UEM fetch the appropriate attributes from LDAP. If you are using email and immutable ID as the user identifying information, ensure that the following values are available in LDAP settings in MobileIron UEM:

  - Email: userPrincipalName
  - Custom 1: ObjectGUID
For more information, see Appendix, Configuring MobileIron Cloud for SSO certificates, and Customizing certificates for single sign-on in Access.

To make it easier to configure mobile application single sign-on, upload a sample Tunnel certificate and assign user friendly names to each field in the certificate. For more information, see User Certificates.

Procedure

1. In MobileIron Access, go to Profile > Federated Pairs.
2. Click +Add New Pair or edit an existing pair.
3. In the service provider (SP) configuration page, scroll down to the Native Mobile Application single Sign-On (SSO) section.

4. Select Use Tunnel Certificates for SSO.
5. Expand Advanced Options.
6. From the Reference Client Certificate drop-down list, select the sample Tunnel certificate.
7. In the **SAML Subject Configuration** section, for **Type**, select
   - **Unspecified** for SAML
   - the type the service provider expects for WS-Fed.

8. For **Get Value From**, select the certificate field from which to get the value.
   You created the user-friendly names when you added the sample Tunnel certificate to Access in the **User Certificates** tab.

9. (Optional) For **Additional Transforms**: Enter the required transforms if the SP expects values that are derived from the value provided in the certificate.

10. (Optional) SAML Attribute Configuration. The SAML attribute configuration populates the Attribute and value section of the federation response from Access. Configure this if the SP expects such attributes. Click **New** to add each new attribute.

11. (Optional) For **Encryption Algorithms**, select the data encryption algorithm and the key transport algorithm.
    The encryption options are available only if **Encrypt SAML assertions** is enabled.

12. (Optional) Click the **View SAML Assertion Example Based on Specifications Below** link to verify that the SAML assertion contains the required user-identifying information.

**Related topics**
- For information about configuring the assertion fields in a federation response, see [Customizing certificates for single sign-on in Access](#).
- For information about encrypting SAML assertions, see [Encrypting SAML assertions](#)
Split Tunneling

In a MobileIron Access deployment, all authentication traffic for the federated pairs configured in MobileIron Access goes through Access using MobileIron Tunnel VPN. Depending on the type of MobileIron Access deployment, all other traffic through Tunnel VPN goes directly to the destination server or through Standalone Sentry. Split tunneling allows you to control which traffic goes through Standalone Sentry to on-premise enterprise resources and which traffic goes directly to the destination.

For example, you may need to configure split tunneling if your deployment uses Tunnel VPN:
- to authenticate to a service provider (SP), such as Salesforce, via Access.
- to access an internal SharePoint server such as sharepoint.mycompany.com via Standalone Sentry.

In the example, federated authentication traffic to Salesforce goes through Access, traffic to the SharePoint server goes through Standalone Sentry, and data traffic to Salesforce goes directly to the destination.

Split tunneling is supported for both Access and Access + Standalone Sentry deployments.

The following topics provide additional information about split tunneling:

- Split tunneling in an Access + Standalone Sentry deployment
- Split tunneling in an Access deployment
- Split tunneling for Android
- Split tunneling for iOS and macOS
- Overview of steps for configuring split tunneling in Access

Split tunneling in an Access + Standalone Sentry deployment

In an Access + Standalone Sentry deployment, all authentication traffic for the federated pairs configured in MobileIron Access goes to Access. All other Tunnel VPN traffic goes through Standalone Sentry. Split tunneling allows you to specify how the traffic that is not federated through Access is handled. You can specify whether the traffic goes through Standalone Sentry or directly to the destination.

NOTE: Split Tunneling is disabled if all the Sentry profiles from VPN are removed from all the registered EMMs.
Split tunneling in an Access deployment

In an Access deployment, by default, all authentication traffic for the federated pairs configured in Access goes to Access. All other traffic goes directly to the destination. However, you may require that some traffic go through Standalone Sentry to access on-premise enterprise resources. In such cases, you configure split tunneling to do the following:

- Authentication traffic for federated pairs configured in Access goes through Access.
- Traffic to on-premise enterprise resources goes through Standalone Sentry.
- All other traffic goes directly to destination.
Split tunneling for Android

For Android apps, split tunneling is configured in the Tunnel VPN configuration for Android or in the Tunnel for Android enterprise configuration. Split tunneling using Tunnel for Android native and Android enterprise is handled in the Tunnel configuration for those devices. See the MobileIron Tunnel for Android Guide for Administrators for information about setting up split domains and routes lists.

NOTE: In an Access deployment, tunneling to both enterprise cloud services and to on-premise enterprise resources is not supported with Tunnel for Samsung Knox Workspace.

Split tunneling for iOS and macOS

For iOS apps and macOS, split tunneling is configured in MobileIron Access in Profile > Split Tunneling. The split tunneling configuration in MobileIron Access is only applicable to Tunnel for iOS and macOS.

Overview of steps for configuring split tunneling in Access

The following is an overview of steps for configuring split tunneling in Access:

1. Enabling split tunneling
2. Adding domains for split tunneling

Enabling split tunneling

The split tunneling feature is disabled by default.
To configure split tunneling for iOS devices, enable split tunneling and configure the domains to go to Standalone Sentry or direct to destination.

Deleting a Standalone Sentry configuration from an UEM and performing a sync removes the Standalone Sentry data from Access. This also disables split tunneling. To stop traffic from being redirected, Publish the changes in Access.

**Before you begin**

- To access on-premise enterprise resources through Standalone Sentry, ensure that you have deployed Standalone Sentry and that the Standalone Sentry is selected in the Tunnel VPN configuration.
- In an Access + Standalone Sentry deployment, ensure that you have an SP and IdP pair configured. An Access profile is created only if an SP-IdP pair is configured. Assign Standalone Sentry to the profile. Assigning the Standalone Sentry to an Access profile, allows Standalone Sentry to pull the Access configurations, which includes the split tunneling configuration. The SP-IdP pair can be an SP-IdP pair with dummy data.

**Procedure**

1. In MobileIron Access, go to **Profile > Split Tunneling**. The **Split Tunneling Configuration** page displays.
2. For **Enable Split Tunneling**, move the toggle to **On**. By default, traffic that does not go to Access goes directly to destination.
3. To change the default behavior, click the link next to **Default Action**.

**Related topics**

For more information, see [https://community.mobileiron.com/docs/DOC-6117](https://community.mobileiron.com/docs/DOC-6117).

**NOTE:** When you enable split tunneling, the Tunnel authentication traffic to Access rule is added by default. This rule is the default domain to which traffic is sent. The rule cannot be edited.

**Adding domains for split tunneling**

Add destination domains to configure which domains go directly to the destination and which domains go via Standalone Sentry.

**Before you begin**

- Verify that the Tunnel-enabled apps and Safari are tested before deploying to production. This is because enabling or disabling split tunneling in Access impacts the traffic through Tunnel.
- Verify that split tunneling is enabled in MobileIron Access. See [Enabling split tunneling](#).

**Procedure**

1. In MobileIron Access, go to **Profile > Split Tunneling**. The **Split Tunneling Configuration** page displays.
2. Click **Add Domain**.
3. In the **Add Split Tunneling Rule** pane, enter the name for the rule.
4. (Optional) Enter a description for the domain.
5. In the **Split Tunnel Config** section, enter the destination domain.
Examples: login.example.com or *.example.com

6. In the **Action** drop-down, select the appropriate action.
   - **Send to destination via Sentry**: Traffic destined to the domain is sent to Standalone Sentry.
   - **Send directly to destination**: Traffic destined to the domain goes directly to the destination.

7. Click **Done**. The domain rule is added to the table and is enabled by default.

8. Click **Publish** to make the changes available.
Branding

The Branding page allows you to customize what users see if an app on a device cannot access a cloud resource.

Branding overview

You configure branding in Profile > Branding. MobileIron Access provides the following options to customize the branding and messaging that users see in the interaction pages on their device.

**Figure 50. Branding Options**

- **Company Logo**: Upload your company logo to customize what device users see in interaction pages for Zero Sign-on and Authenticator. See, Configuring branding for Zero Sign-on.

- **Remediation Page**: Use this page to customize the message that device users see if a conditional rule blocks access to an application. You can redirect device users to a URL or create a custom error page. You can add a different remediation page for each conditional rule to block access to an application. See, Adding a remediation page.

- **Service Unavailable Page**: Use this page to customize the message that the device users see if an application cannot access the cloud service or any other reason. For example, the service may not be available due to network issues. You can redirect device users to a URL or create a custom error page.

- **Warning Page**: Use this page to customize the message that device users see when conditional access rule has the action set to warn. You can allow users to continue through this warning.

The following default interaction pages are available:
- Interaction page when access to cloud application is blocked on desktop and Mobile
- Interaction page when the service is unavailable on desktop and mobile
- Interaction page when access to cloud application is blocked on desktop and Mobile

**Figure 51. Interaction page when access to cloud application is blocked on desktop and Mobile**
FIGURE 52. INTERACTION PAGE WHEN THE SERVICE IS UNAVAILABLE ON DESKTOP AND MOBILE

We have encountered an issue that prevents access to your application.

Please try again. If the issue persists, contact your administrator.
Figure 53. Interaction page with a warning for security reasons

WARNING

Your access to this Cloud Application is blocked for security reasons

WARNING !!

Device must be registered with MobileIron Security and this application must be downloaded from MobileIron Apps@Work for continued access to it. Failure to conform will deny access to this application. Please follow instructions below to conform with our company security policy.

Continue

Powered by MobileIron
Adding a remediation page

A remediation page is presented to device users if a conditional rule blocks access to a cloud service. You can customize the default remediation page that is provided or you can create a new remediation page. You can create separate remediation pages for each conditional rule to customize the remediation actions that device users see.

After you create a remediation page, navigate to Profile > Conditional Access to associate the remediation page with the conditional rule.

Before you begin

- If your deployment is Access + Standalone Sentry, verify that you have installed Sentry 9.1.2 through the most recently released version as supported by MobileIron.
- Verify that you have a working federated pair before enabling this feature.

Procedure

1. Navigate to Profile > Branding.
2. Click Add Remediation Page in the Remediation Page Branding panel. The new Remediation page is added below the default remediation page.
3. Customize and preview the remediation page.
4. (Optional) The administrator can choose to associate an appropriate Remediation page with the rule.
5. Click Publish to apply the conditional rule with the profile.

NOTE: In a Access + Standalone Sentry deployment, there is a delay of fifteen minutes for Sentry to be updated.

You can customize what the user sees in one of the following ways. If the branding is not customized, the default message is displayed to the device user.

- Redirecting device users to a URL
- Creating a customized message

Redirecting device users to a URL

If an application is blocked or the connection fails for any reason, you can redirect the device users to a specified URL.

Procedure

1. In the MobileIron Access, go to Profile > Branding > Remediation Page or Service Unavailable Page.
2. In Page Options, select I want to redirect users to my website URL.
3. Enter the redirect URL in the text box for Redirect URL. The redirect URL must include http:// or https://.
4. Click Save Changes to save the settings.
   - If a redirect URL is configured in the Remediation Page, device users are directed to the redirect URL if an application is blocked.
If a redirect URL is configured in the Service Unavailable Page, device users are directed to the redirect URL if the cloud service is unavailable. For example, a 503 error.

 Creating a customized message

If an application is blocked or the connection fails for any other reason, you can customize the error message presented to the device user. You can customize the error message by adding your company logo, company name, custom text, and a Help link.

Procedure
1. In the MobileIron Access administrative portal, go to Profile > Branding > Remediation Page or Service Unavailable Page.
2. In Page Options, select I want to customize the page presented to users.
3. In Customization Settings, click Choose File to navigate to the location of your company logo.
   The graphic must be no more than 300 pixels wide and 50 pixels high.
   If you do not want to upload a graphic, select Remove logo.
4. Enter a Message describing why users have encountered the issue.
   You can enter up to 255 characters.
5. Enter a Help message describing how users can access help or report the issue. You can enter up to 255 characters.
6. Enter the Help Link. Choose http:// or https://, and enter the URL in the text box.
7. Enter the Help Link Text that the device users see instead of the URL.
8. Click Save Changes to save the settings.
   The Preview section displays the customized message.

Device users are now presented with the customized message.

NOTE: Use Reset to Default option, in the Remediation page or Service Unavailable page to restore the default values when the profile was created.

 Creating a customized warning message

You can customize the warning messages to device users when a Conditional Access Rule is set to warn.

Procedure
1. In the MobileIron Access administrative portal, go to Profile > Branding > Warning Page.
2. In Customization Settings, click Choose File to navigate to the location of your company logo.
   The graphic must be no more than 300 pixels wide and 50 pixels high.
   If you do not want to upload a graphic, select Remove logo.
3. Enter a Warning Message about the issue.
   You can enter up to 255 characters.
4. Enter a Help message describing how users can access help or report the issue. You can enter up to 255 characters.
5. Enter the Help Link. Choose http:// or https://, and enter the URL in the text box.
6. Enter the Help Link Text that device users see instead of the URL.
7. Enter the Continue Button Text that the users see to click and proceed.
8. Click **Save Changes** to save the settings.
   The **Preview** section displays the customized message.
   Device users are now presented with the customized message.

**NOTE:** Use the **Reset to Default** option, in the Warning page to restore the default values when the profile was created.
Session Revocation

Access provides authentication assertions, based on the SAML or WS-Federation protocols, to cloud services. As a result of the authentication, the app gets a session token from the cloud service. This token is stored on the device and allows the app to access the cloud service without having to reenter user credentials. The session token expires after a certain length of time, after which the user is prompted to authenticate again.

The following topics provide more information about session revocation:

- About session revocation
- Configuring Session Revocation
- Session revocation report
- What users see if session revocation is configured

About session revocation

Session revocation allows administrators to terminate or revoke the session token if a device is out of compliance and the UEM policy action is blocked or a device is retired. The revocation prevents out of compliance and retired devices from continuing to use a session token on the device to access the cloud service. Session revocation impacts the sessions of the managed applications (service provider) on all the devices that the user uses to access the cloud service. After a session token is revoked, the user has to re-authenticate with the service provider through Access to get a new session token. When the user tries to re-authenticate, Access enforces conditional policies and unblocks the app.

NOTE: You can update the compliance policies in MobileIron Core > Policies & Configs > Compliance Policies.

Compliance policy

- Support for policy action based Session revocation
- MobileIron Access Session revocation service (SRS) workflows are improved to consider UEM (MobileIron Core) policy action configurations
- Session revocation is triggered only for those devices which are non compliant and also have a blocking action setup against the corresponding policy
- Session revocation actions is also triggered for other device states such as quarantine, wipe, and retire
• For all other cases of violation, if there is a non blocking action (such as email, monitor, notify, etc) no action will be taken by Access.

Session revocation is supported for Access deployments for Office 365 using the Azure Graph API and G Suite using Google API console. However, the session revocation feature is not supported for Access + Standalone Sentry deployments.

Note The Following:

• Session revocation is not supported with MobileIron Connected Cloud.

• To start session revocation, MobileIron Access verifies the compliance action configured on MobileIron UEM when the device goes out of compliance and the actions configured against them. For MobileIron Cloud or Core deployments, session revocation is triggered if the device is out of compliance and the compliance action is either block or quarantine. Session revocation is also triggered if the device is Wiped or Retired.

• To start session revocation, MobileIron Access verifies the compliance action configured on MobileIron UEM when the device goes out of compliance and the actions configured against them. For MobileIron Core deployments, session revocation is triggered if the device is out of compliance and the compliance action is block. Session revocation is not triggered if the action is SendAlert.
Configuring Session Revocation

Session revocation is configured in MobileIron Access.

Before you begin

- Verify the following before configuring session revocation:
  - You have an Access deployment with a MobileIron UEM.
  - The MobileIron Access administrator has Common Platform Services (CPS) role in MobileIron UEM.
    MobileIron Cloud: For information on assigning roles, see “Assigning Roles to Users” in the MobileIron Cloud Administrator Guide or click Help in the MobileIron Cloud administrative portal.
    MobileIron Core: For information on assigning roles, see the MobileIron Core Delegated Administration Guide.
  - Common Platform Services Notifications is enabled in MobileIron UEM.
    MobileIron Cloud: Go to Admin > Common Platform Services Notifications, and enable Common Platform Services Notifications.
    MobileIron Core: From the MobileIron Core command line interface (CLI), enter the following command in CONFIG mode - activemq
  - Session tokens are revoked if the device state is retired or non-compliant as reported by the UEM to Access.
    For information about configuring compliance polices, see your MobileIron UEM documentation.
    MobileIron Core: See the MobileIron Core Device Management Guide.
  - Users are registered LDAP users with custom attribute of userPrincipalName and objectGUID in a MobileIron UEM.
    MobileIron Core: See Configuring LDAP in MobileIron Core for session revocation.
  - Port 8883 in the firewall is open to allow Access to pick up queued up events.

- For Office 365
  - A federated pair with Office 365 and ADFS configured in Access
  - An app registration for the Access revocation service in Microsoft Azure. This set up provides Access permission to revoke session tokens for Office 365.
    For information about creating an app registration for the Access session revocation service, see the knowledge base article Configuring an application in Azure for the session revocation service (SRS) for Office 365 (Azure AD). Make a note of the Azure directory ID, application ID, and the secret key.
- For G Suite
  - A federated pair with G Suite and any appropriate IdP configured in Access.
  - Generate a service account key file using Google API console. This set up provides Access permission to revoke session tokens from G Suite.
    For more information about creating the service account key file, see the knowledge base article Configuring G Suite for the session revocation service (SRS). Make a note of the G Suite service account key.

**Procedure**

1. In MobileIron Access, go to Profile > Session Revocation. The Service Provider Configuration page displays.
2. In the Service Provider Configuration page, click +Add Configuration.
3. For service provider, click Office 365 or G Suite appropriately.
4. Enter the following information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the configuration.</td>
</tr>
<tr>
<td>Add Description</td>
<td>Add a description for the configuration.</td>
</tr>
<tr>
<td><strong>Configuration for Office 365</strong></td>
<td></td>
</tr>
<tr>
<td>Azure Directory ID</td>
<td>Enter the Azure directory ID.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Enter the application ID from the app registration you created for the Access session revocation service in Azure.</td>
</tr>
<tr>
<td>Secret key</td>
<td>Enter the Azure secret key from the app registration you created for the Access session revocation service in Azure.</td>
</tr>
<tr>
<td><strong>Configuration for G Suite</strong></td>
<td></td>
</tr>
<tr>
<td>G Suite Service Account Key</td>
<td>Service account key file in JSON format.</td>
</tr>
<tr>
<td></td>
<td>To obtain this file, follow KB article:</td>
</tr>
<tr>
<td>G Suite administrator Email ID</td>
<td>Enter the Super Admin email ID.</td>
</tr>
</tbody>
</table>

5. Click Save.

**Session revocation report**

For information on which user and service provider (SP) a revocation action was performed, see Reports > Session Revocation in the Access administrative portal.

The report provides status information on whether the revocation was successful or not and the context for the revocation.
What users see if session revocation is configured

If the session token is revoked, users are prompted to log in to the cloud service. Based on conditional policies, Access evaluates whether the user on the device has access to the cloud service. If access is denied, a message is presented to the user stating that they are blocked by the administrator from accessing the service.
Fast Identity Online (FIDO2) or Zero Sign-on with MobileIron Access

With Fast Identity Online (FIDO2) or extended Zero Sign-on solution, MobileIron provides ease of access to enterprise resources within a highly secure framework. Users access enterprise cloud resources from either unmanaged or managed devices without the requirement of having to enter their username and password.

The following provides information about FIDO2 or extended Zero Sign-on with MobileIron Access:

- Overview
- Configuring Zero Sign-on in MobileIron Cloud
- Configuring Zero Sign-on in MobileIron Core
- Configuring Zero Sign-on in MobileIron Access
- MobileIron Authenticate
- What users see for FIDO2
- Client Registration Settings

Overview

Using Fast Identity Online (FIDO2) secure authentication protocols, MobileIron extends the MobileIron Zero Sign-on solution to third-party managed devices. FIDO2 is the industry standard that replaces passwords with a login experience that is passwordless, fast, and secure across websites and apps.

For information about the FIDO2 standard, see https://fidoalliance.org.

Key features

- FIDO2 standard provides Secure, Phishing-proof, and convenient methods of authentication.
- Users never need to enter username.
- Users never need to enter passwords.
- FIDO2 uses biometric authentication.
- FIDO2 has standard around no username authentication too.
Use cases

FIDO2 is supported on desktops managed by MobileIron Cloud, JAMF and SCCM.

NOTE: MobileIron Zero Sign-on with FIDO2 solution is for managed desktops only and not for mobiles. MobileIron Authenticate must be installed on your desktop for this solution to function.

Deployment use cases

The following use cases are supported for FIDO2 or Zero Sign-on solution:
## Table 22. Use Cases

<table>
<thead>
<tr>
<th>Deployment Use cases</th>
<th>Notifications</th>
<th>Interaction Use case</th>
</tr>
</thead>
</table>
| Passwordless login to cloud services from MobileIron Cloud managed desktops | - Biometrics on the desktop, or  
- Push notifications to a MobileIron managed device or a MobileIron Auth-only device. | User verification (Step Up Authentication) is disabled for 3rd party managed UEM desktops along with device authentication  
- only device authentication is done using FIDO2 client on desktop  
Block unmanaged traffic from unmanaged devices which are not 3rd party UEM managed  
- block the access if FIDO2 authentication cannot be performed  
Block 3rd party UEM managed desktops which are non compliant where device posture is not correct |
| Passwordless login to cloud services from JAMF managed desktops | - Biometrics on the desktop, or  
- Push notifications to a MobileIron managed device or a MobileIron Auth-only device. | - Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct  
- Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct  
- User verification is enabled for 3rd party managed UEM desktops along with device authentication  
  - Along with device authentication, user verification must be done which can be performed either using biometrics of desktops or mobile devices or using username or password authentication with |
### TABLE 22. USE CASES (CONT.)

<table>
<thead>
<tr>
<th>Deployment Use cases</th>
<th>Notifications</th>
<th>Interaction Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passwordless login to cloud services from SCCM managed desktops</strong></td>
<td>• Biometrics on the desktop, or</td>
<td>• Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct</td>
</tr>
<tr>
<td></td>
<td>• Push notifications to a MobileIron managed device or a MobileIron Auth-only device.</td>
<td>• Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct</td>
</tr>
<tr>
<td><strong>Passwordless login to a desktop</strong></td>
<td>• Push notifications to a MobileIron managed device or a MobileIron Auth-only device</td>
<td>User verification is disabled for 3rd party managed UEM desktops along with device authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• only device authentication is done using MobileIron Authenticate on desktop</td>
</tr>
<tr>
<td><strong>Passwordless login from unmanaged devices</strong></td>
<td>• QR code</td>
<td>• Allow unmanaged traffic from unmanaged devices which are not 3rd party UEM managed.</td>
</tr>
<tr>
<td></td>
<td>• Push notifications to a MobileIron managed device or a MobileIron Auth-only device</td>
<td>• Block unmanaged traffic from unmanaged devices which are not 3rd party UEM managed.</td>
</tr>
<tr>
<td></td>
<td>• administrator mandates compliance check to be performed for these devices and block if they are non compliant</td>
<td></td>
</tr>
</tbody>
</table>

### Required MobileIron components

- MobileIron Access
- MobileIron Cloud deployment
- MobileIron Authenticate for macOS and Windows 10
- If FIDO2 is not enabled, then the following components are required in an Access deployment:
  - MobileIron Tunnel configuration with Access enabled.
  - MobileIron Tunnel deployed to devices.
  - NOTE: MobileIron tunnel only works with Mobileiron managed desktops and does not work for other 3rd party managed devices.
Supported devices

- macOS devices managed by MobileIron Cloud
- Windows 10 devices managed by MobileIron Cloud

Supported browsers

- macOS: Safari, Chrome
- Windows 10: Edge, Chrome, Firefox

Authentication flow types

The following flow types lists the authentication workflow in a FIDO2 solution:

- MobileIron Managed flow
- Unmanaged flow
- Other managed flow
Configuring Zero Sign-on in MobileIron Cloud

Create a Zero Sign-on configuration in MobileIron Cloud and sync with MobileIron Access.

Before you begin

Ensure that you have set up Access with MobileIron Cloud. See Overview of configuration with MobileIron Cloud.

Procedure: Overview of steps

1. Creating a Zero Sign-On configuration in MobileIron Cloud
2. Syncing the Zero Sign-On configuration with MobileIron Access

Creating a Zero Sign-On configuration in MobileIron Cloud

In MobileIron Cloud, create a Zero Sign-on configuration.

Before you begin

Ensure that you have configured Zero Sign-on in Access.

Procedure

1. In MobileIron Cloud, go to Configurations > + Add > Saas Sign-On.
2. In the Name field, enter a name for the configuration.
3. (Optional) Expand + Add Description, to add a description for the configuration.
4. For SCEP Identity, select the identity certificate you created for Tunnel. The Tunnel certificate is the same certificate you used to set up mobile app single sign-on in Access.
5. Turn on the Enable FIDO toggle switch to enable FIDO 2 authentication.
6. Select a distribution option. The configuration is distributed to the devices in the selected option.
7. Click Done.

Related topics

- For more information about configuring mobile app single sign-on (SSO):
  - For a federated pair, see Configuring Mobile App Single Sign-on (SSO).
  - For delegated IdP, see Configuring Access as the delegated IdP.

Syncing the Zero Sign-On configuration with MobileIron Access

Sync with MobileIron Access to pull the Zero Sign-on configuration from the UEM.
Procedure

1. In MobileIron Access, navigate to the UEM tab.
2. Select the Cloud UEM and click the Sync UEM icon.
3. Enter the UEM administrator credentials.
4. Enter the credentials and click Verify.
5. Click Done.
   The SaaS Sign-on configuration and MobileIron Authenticate configuration is now synced with Access.

Configuring Zero Sign-on in MobileIron Core

Create a Zero Sign-on configuration in MobileIron Core and sync with MobileIron Access.

Before you begin

You have set up Access with MobileIron Core. See Overview of configuration with MobileIron Core.

Procedure: Overview of steps

1. Creating a Zero Sign-on policy in MobileIron Core
2. Syncing the Zero Sign-on policy with MobileIron Access

Creating a Zero Sign-on policy in MobileIron Core

In MobileIron Core, create a Zero Sign-on policy.

Before you begin

Ensure that you have configured Zero Sign-on in Access.

Procedure

1. In MobileIron Core, go to Policies &Configs > Policies > Add New > SaaS Sign-on.
2. In the Name field, enter a name for the configuration.
3. For Status, select Active.
   Active is default status.
4. (Optional) Add a description for the policy.
5. For Identity Certificate, select the certificate enrollment setting you created for Tunnel.
   The Tunnel certificate is the same certificate you used to set up mobile app single sign-on in Access.
6. Turn on the Enable FIDO toggle switch to enable FIDO authentication.
7. Click Save.
8. Apply the policy to a label.
   a. Select the SaaS sign-on policy.
   b. Click Actions > Apply To Label.
   c. Select the labels to apply and click Apply.

Related topics

- For more information about configuring mobile app single sign-on (SSO):
  - For a federated pair, see Configuring Mobile App Single Sign-on (SSO).
  - For delegated IdP, see Configuring Access as the delegated IdP.

Syncing the Zero Sign-on policy with MobileIron Access

Sync with MobileIron Access to pull the Zero Sign-on configuration from the UEM.

Procedure

1. In MobileIron Access, navigate to the UEM tab.
2. Select the Core UEM and click the Sync UEM icon.
3. Enter the credentials and click Verify.
4. Click Done.

Configuring Zero Sign-on in MobileIron Access

This section provides information for the following scenarios:

- Setting Zero Sign-on security and user experience
- Passwordless authentication to service providers on unmanaged devices
- Passwordless login to cloud services for managed desktops
- Zero Sign-on from desktops managed by JAMF

Setting Zero Sign-on security and user experience

Users can customize the security and user experience of Zero Sign-on. You can find the settings in Profile > Zero Sign-on > Zero Sign-on Settings. It lists the following configuration options:

- General: Setting the session timeout duration
- MobileIron Authenticate: Registering with MobileIron Authenticate
Setting the session timeout duration

Use the Zero Sign-on configuration, Profile > Zero Sign-on, to do the following:

- Set the session timeout duration after users authenticate using Zero Sign-on.
  Once user authenticates on their managed or personal device, they don't have to sign-in next time while they are within the signed-in session duration. Except if the policy associated to the Service Provider requires Step-Up Authentication, then user would be prompted for it. Session is terminated by closing the browser.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Click Zero Sign-on Settings > General to update the number of hours, if needed, for Enable Signed In Session.

   ![Zero Sign-On Settings](image)

3. By default, the option is enabled and the number of hours is set at 12. The option sets the session timeout that is applied when users select the Yes, this is my personal computer option in the Zero Sign-on interaction page.
4. Click Save.

Registering with MobileIron Authenticate

After an automatic installation, MobileIron Authenticate connects with Access to register to the desktop to the appropriate user.
You can register in one of the following methods:

- **Silent**: Registration is done by fetching the username from the desktop identity certificate.
- **Require QR code scan to register**: User must open MobileIron Authenticate application and scan the QR code using MobileIron Go app. The username is then obtained from the mobile device identity certificate.

**Unlocking the desktop**

Desktop unlock is a secure and convenient method of unlocking user's desktop using a phone. The MobileIron Authenticate application on the desktop works in conjunction with Access to send a push notification to the user's activated mobile phone to authenticate and unlock the desktop. Keep the toggle on in **Profile > Zero Sign-on > Zero Sign-on Settings > MobileIron Authenticate** to enable the feature.
Authentication for service providers

The toggle switch "Show users the option to sign-in with MobileIron Authenticate when they perform Zero Sign-On authentication" is disabled by default. When this option is enabled, this option lets the users sign-in to MobileIron Authenticate on the desktops.

Even with this option disabled, users can use the other authentication options such as QR code, Push and Password.

Provide a customized description for Sign-in using MobileIron Authenticate. This description helps the users decide to select the "Sign-in using MobileIron Authenticate " when using a desktop browser that is not FIDO registered with MobileIron Authenticate.

FIDO Key

FIDO keys are used for stronger authentication. During registration with an online service, the user's client device creates a new key pair. The client's private keys can be used only after they are unlocked locally on the device by the user. The user can manage the settings of the FIDO key in Access after registering.

NOTE: MobileIron recommends that the admin does not need to change the settings. However, the admin should discuss with MobileIron before enabling or disabling the settings.
Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Click Zero Sign-on Settings > FIDO Key.

3. Update the following fields to enhance the feature as required:
   - **Rotation Period for FIDO Key**: Specify the duration required to generate a new FIDO key.
   - **Grace period to rotate the FIDO Key before expiry**: Specify the grace period to generate a FIDO key if it was not during the Rotation period.
   - **FIDO key storage**: Specify the Trusted Platform Module version supported to store the FIDO key.
   - **Allow storing in iOS keychain**: Turn on option iOS user.
- **Allow storing in Windows Certificate Store**: Specify if the FIDO key can be stored in Certificate Store.
- **Allow storing in MacOS keychain**: Turn on the option for MacOS user.
- **Allow storing in Android key store**: Turn on the option for Android user.
- **Desktop Password Encryption**: Specify the RSA key size for Mobile devices or for desktops.
- **Public Key Algorithms**: Select the public key algorithms and specify the order that they must be applied.
- **MobileIron Authenticate as a FIDO key**: Select the option to authenticate with FIDO key on the website. MobileIron Authenticate is automatically invoked and prompts the user to authenticate with a push notification.

4. Click **Add New** to add the relying parties that accept FIDO keys to use MobileIron Authenticate to sign-in.
5. Click **Save**.

---

**Passwordless authentication to service providers on unmanaged devices**

This section contains the following sections:

- Password-less login from unmanaged devices

**Password-less login from unmanaged devices**

The following describes the configuration in Access for Zero Sign-on.

**Before you begin**

- Ensure that you have an Access deployment with MobileIron UEM.
  See [Overview of configuration with MobileIron Cloud](#).
  OR
  See [Overview of configuration with MobileIron Core](#)
- Ensure that mobile app single sign-on (SSO) is configured for the service provider (SP).
  For a federated pair, see [Configuring Mobile App Single Sign-on (SSO)](#).
  For delegated IdP, see [Configuring Access as the delegated IdP](#).
Procedure: Overview of steps

- Enabling Password-less Authentication on MobileIron Go and Mobile@Work
- Adding a Zero Sign-on Rule in the Policies

NOTE: A green tick displays when these steps are configured correctly. This shows that the authentication is configured correctly.

Enabling Password-less Authentication on MobileIron Go and Mobile@Work

Before you begin

- Configure the user information for Zero Sign-on.
  - To configure the user information, map the fields in the certificate from which Access gets user identifying information. This is the identity certificate used for setting up the configuration. Configuring the user information enables password-less authentication.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand Enable Password-less Authentication on MobileIron Go and Mobile@Work.
3. Click **See Details** to view the existing configuration details for the devices.

![Zero Sign-On](image)

4. To enable more devices follow the steps i) and ii) as shown above.
   a. Deploy SaaS Sign-On on managed mobile devices.
   b. Sync UEM.

### Adding a Zero Sign-on Rule in the Policies

In the policy associated with the SAML pair for which Zero Sign-on is required, add a **Zero Sign-on Rule** conditional rule. If the rule is added, users accessing the cloud service from an unmanaged device see an interaction page. The interaction page contains a QR code, which device users can scan from a managed device to authenticate to the cloud service. Alternately, the interaction page also contains a link to authenticate with username and password.

### Before you begin

- Ensure that mobile app single sign-on is configured for the federated pair or delegated IdP to which you want to assign the Zero Sign-on Rule. If mobile app single sign-on is not configured, you will see errors when creating or assigning the **Zero Sign-on Rule**.
Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.

![Add Zero Sign-On Rule in the Policies](image)

3. Click See Details to view the existing UEMs with SaaS on configuration created and synced with Access.
4. Verify that the rule is configured.
   Else add a rule in Profile > Conditional Policies.
5. In MobileIron Access, go to Profile > Conditional Access.
6. Expand Default Policy.
   If you want Zero Sign-on only for some federated pairs or delegated IdP, create a new policy.
   The Zero Sign-on rule can be added to any policy. Adding the Zero Sign-on rule to the default policy makes it available to all pairs to which the default policy is applied. Add the Zero Sign-on rule to another policy if you want to apply the rule to only some federated pairs or delegated IdP.
7. Click +Add Rule > Zero Sign-on Rule to add the conditional rule for Zero Sign-on.
8. Enter a name and description for the rule.

9. Configure the rule for one of the following devices.

   a. **For unmanaged devices**: Enable the toggle switch to allow access on unmanaged devices. Users are authenticated with one of the following methods: QR code, Push notification, One Time Password (OTP).
b. **Step-Up Authentication**: Enable the toggle switch to step-up authentication such as Push notifications or biometric for managed desktops.

10. For **Rule Action**, select **Allow**.

11. Click **Done** to save the policy and rule.

**IMPORTANT:** The order of the conditional rules matters. When you create a **Zero Sign-on Rule**, Access automatically orders the rules such that the **Zero Sign-on Rule** follows the **Trusted App and Device** rule. The order of rules, if they are configured, is as follows: **Trusted App and Device** rule, **Zero Sign-on Rule**, **Multi-Factor Authentication** rule. However, the rules can be manually reordered. Ensure that the order of the rules matches the order stated in this note.

**Configuring branding for Zero Sign-on**

Customize the user experience for your enterprise users by uploading your company logo to Access. The user notification screen as well as the interaction page with the QR code are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

**Procedure**

1. In Access, go to **Profile > Branding**.
2. In the **Company Logo** section, drag and drop your company logo or click **Choose** to navigate to the location of the file and add.

**Next steps**

Publish the updates. See **Publishing the changes**.

**Publishing the changes**

Publish the changes to make the updates available. In the Access administrative portal, a publish banner appears in any of the **Profile** tabs when there are configuration changes.

**Procedure**

1. In the Access, go to **Profile > Overview**.
2. Click **Publish**.
3. Click **OK**.

**Password less login to cloud services for managed desktops**

This chapter contains the following sections:
• Password-less log in to cloud services from MobileIron managed desktops
• Password-less login from MobileIron managed devices

**Password-less log in to desktops**

• Passwordless login to desktops with push notifications to a MobileIron managed device.
• Users signing into their desktops get push notification to their MobileIron managed device. Users do not need to enter their username and password.

**Required MobileIron components**

• MobileIron Cloud deployment
• MobileIron Authenticate for Windows 10
• MobileIron FIDO2 cloud instance

**Supported devices**

• macOS devices managed by MobileIron Cloud
• Windows 10 devices managed by MobileIron Cloud

**Supported browsers**

• macOS: Safari, Chrome
• Windows 10: Edge, Chrome, Firefox

**Password-less log in to cloud services from MobileIron managed desktops**

The MobileIron FIDO2 solution is based on FIDO2 standards and extends the passwordless experience to desktops with TouchID.

**Use cases**

The following use cases are supported for passwordless log in:

• Log in to cloud services from MobileIron managed desktops.
  Users are automatically authenticated using macOS TouchID if the device supports TouchID. Entering their username and password is not required. The biometric option is also available and is turned off by default.

• Log in to cloud services from unmanaged desktops using push notifications.
  Users are prompted to allow the access from a push notification sent to a MobileIron managed or Auth-only mobile device. Entering their username and password is not required.

• Log in to a desktop using push notifications.
Users are prompted to allow the access from a push notification sent to a MobileIron managed or Auth-only mobile device. Entering their username and password is not required. This use case requires that you also have a MobileIron Cloud deployment.

**Required MobileIron components**

- MobileIron Cloud deployment
- MobileIron Authenticate for macOS
- MobileIron Authenticate for Windows 10
- MobileIron FIDO2 cloud instance

**Supported devices**

- macOS devices managed by MobileIron Cloud
- Windows 10 devices managed by MobileIron Cloud

**Supported browsers**

- macOS: Safari, Chrome
- Windows 10: Edge, Chrome, Firefox

**Password-less login from MobileIron managed devices**

The following describes the configuration in Access for Zero Sign-on.

- Deploying MobileIron Authenticate using UEM
- Review Registration Settings
- Enabling Password-less Authentication on MobileIron Go and Mobile@Work
- Adding a Zero Sign-on Rule in the Policies

**Deploying MobileIron Authenticate using UEM**

You can connect UEM with Access and distribute MobileIron Authenticate to user desktops.

**Procedure**

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Under Steps for deploy, expand Deploy MobileIron Authenticate using UEM.
3. For desktops managed by:
   a. **3rd Party UEM**: In MobileIron Access, go to **UEM > 3rd Party UEM** tab. Click **Connect UEM** and follow steps.
   b. **MobileIron Cloud**: Go to **UEM**. Select the Cloud UEM and follow steps in the MobileIron Authenticate section.

**Review Registration Settings**

The Registration settings are used by clients such as MobileIron Go to register user’s device with Access.

**Procedure**

1. In MobileIron Access, go to **Profile > Zero Sign-on**.
2. Under Steps to deploy, expand **Review Registration Settings**.
   Verify the certificate mapping.
3. Click **View Template** to view the default client certificate.

4. Click **Edit** to modify the registration.

   
   **Client Registration Settings**
   
   MobileIron clients such as MobileIron Go and MobileIron Authenticate send the device identity certificate to Access. The setting below is used to determine the username from the certificate and register device. **Learn More**

   **Note:** This setting is also available via Profile > Client Registration Settings

   The identity certificate of the devices (mobile or desktop) registering with Access must follow the same template as the one used in Certificate based Single Sign-On (Profile > Federation).

<table>
<thead>
<tr>
<th>Identity Certificate Template</th>
<th>Username Maps To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Client Certificate</td>
<td>SAN of type mDNS</td>
</tr>
<tr>
<td>View certificate template</td>
<td>Additional transform</td>
</tr>
</tbody>
</table>

   **Cancel**  **Save**

5. Select the username mapping in the certificate appropriately and click **Save**. For more information, see **Client Registration Settings**.

**Related topics**
For information about MiTra expressions, see **Language to generate values from certificate fields**.

**Enabling Password-less Authentication on MobileIron Go and Mobile@Work**

**Before you begin**

- Configure the user information for Zero Sign-on.
  - To configure the user information, map the fields in the certificate from which Access gets user identifying information. This is the identity certificate used for setting up configuration. Configuring the user information enables passwordless authentication.
Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand Enable Password-less Authentication on MobileIron Go and Mobile@Work.

3. Click See Details to view the existing configuration details for the devices.
4. To enable more devices follow the steps i) and ii) as shown above.
   i. Deploy SaaS Sign-On on managed mobile devices.
   ii. Sync UEM.

Adding a Zero Sign-on Rule in the Policies

In the policy associated with the saml pair for which Zero Sign-on is required, add a Zero Sign-on Rule conditional rule. If the rule is added, users accessing the cloud service from an unmanaged device see an interaction page. The interaction page contains a QR code, which device users can scan from a managed device to authenticate to the cloud service. Alternately, the interaction page also contains a link to authenticate with username and password.
Before you begin

- Ensure that mobile app single sign-on is configured for the federated pair or delegated IdP to which you want to assign the Zero Sign-on Rule. If mobile app single sign-on is not configured, you will see errors when creating or assigning the Zero Sign-on Rule.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.

3. Verify that the rule is configured.
   Else add a rule in Profile > Conditional Policies.
5. Expand Default Policy.
   If you want Zero Sign-on only for some federated pairs or delegated IdP, create a new policy. The Zero Sign-on rule can be added to any policy. Adding the Zero Sign-on rule to the default policy makes it available to all pairs to which the default policy is applied. Add the Zero Sign-on rule to another policy if you want to apply the rule to only some federated pairs or delegated IdP.
6. Click **+Add Rule > Zero Sign-on Rule** to add the conditional rule for Zero Sign-on.

   ![Zero Sign-on Rule Configuration](image)

   - **Create Zero-sign-on Rule**
     - Enable password-less authentication to service providers, on non-failed browser and apps.
     - **Name**
     - **Add Description**

   - **How does the Zero Sign-on rule work?**
     - **For managed desktops**
       - **Enabled**
     - **For unmanaged devices**
       - **Enabled**
     - **Step-Up Authentication**
     - **Disabled**

   - **Sign-in Session is disabled.** So users will be prompted to authenticate every time they try to access associated service providers.
     - For details, visit the Zero Sign-On Settings page under Profile > Zero Sign-On.
     - During authentication, users also have the option to alternatively sign-in using username and password.

   - **Rule Action**
     - **Selected Action**

7. **Enter a Name and Description** for the rule.

8. Configure the rule for one of the following devices.

   a. **For managed desktops:** Users device is automatically authenticated using MobileIron Authenticate and FIDO2 protocol. Enable the toggle switch to select this configuration.

   ![For managed desktops](image)

   - **User's device is automatically authenticated using MobileIron Authenticate and FIDO protocol.**
   - **Allow access only on desktops that meet the compliance criteria for the UEM**
   - **Remediation message for blocked access:** Default Remediation Page

   b. **For unmanaged devices:** Enable the toggle switch to allow access on unmanaged devices. Users are authenticated with one of the following methods: QR code, Push notification, One Time Password
c. **Step-Up Authentication**: Enable the toggle switch to step-up authentication such as Push notifications or biometric for managed desktops.

9. For **Rule Action**, select **Allow**.
10. Click **Done** to save the policy and rule.

**IMPORTANT**: The order of the conditional rules matters. When you create a Zero Sign-on Rule, Access automatically orders the rules such that the Zero Sign-on Rule follows the Trusted App and Device rule. The order of rules, if they are configured, is as follows: Trusted App and Device rule, Zero Sign-on Rule, Multi-Factor Authentication rule. However, the rules can be manually reordered. Ensure that the order of the rules matches the order stated in this note.

### Configuring branding for Zero Sign-on

Customize the user experience for your enterprise users by uploading your company logo to Access. The user notification screen as well as the interaction page with the QR code are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

**Procedure**

1. In Access, go to **Profile > Branding**.
2. In the **Company Logo** section, drag and drop your company logo or click **Choose** to navigate to the location of the file and add.

**Next steps**

Publish the updates. See [Publishing the changes](#).
**Publishing the changes**

Publish the changes to make the updates available. In the Access administrative portal, a publish banner appears in any of the Profile tabs when there are configuration changes.

**Procedure**

1. In the Access, go to Profile > Overview.
2. Click Publish.
3. Click OK.

**Zero Sign-on from desktops managed by JAMF**

The MobileIron FIDO2 Zero Sign-on solution allows you to provide a password less log in experience from your JAMF managed desktops.

**Use cases**

The following use cases are supported for passwordless log in:

- Log in to cloud services from desktops managed by JAMF on the desktop.
  Users are automatically authenticated using macOS TouchID if the device supports TouchID. Entering their username and password is not required.
  This use case does not require that you also have a MobileIron Cloud deployment.
  This configuration is optional and it is turned off by default.

- Log in to cloud services from desktops managed by JAMF using push notifications.
  Users are prompted to allow the access from a push notification sent to a MobileIron managed or Auth-only mobile device. Entering their username and password is not required.
  This use case requires that you also have a MobileIron Cloud deployment.

- Log in to a desktop using push notifications.
  Users are prompted to allow the access from a push notification sent to a MobileIron managed or Auth-only mobile device. Entering their username and password is not required.
  This use case requires that you also have a MobileIron Cloud deployment.
Authentication flow from desktops

**Figure 54. Authentication flow from JAMF managed desktops**

1. User requests access to a cloud service from a JAMF desktop.
2. The cloud service redirects user to the configured identity provider (IdP) to authenticate. Since Access is the configured IdP, the request is redirected to Access.
3. Access generates a new SAML response to redirect to the original SP. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

**Required MobileIron components**

- MobileIron Authenticate for macOS
- MobileIron FIDO2 cloud instance (Access in the EAP cluster with configured SP+IdP federated pairs)
- MobileIron Cloud deployment if push notifications to a MobileIron managed device is needed.

**Supported devices**

- macOS devices managed by JAMF

**Supported browsers**

- macOS: Safari, Chrome
Configuring UEM with JAMF in MobileIron Access

MobileIron Access integrates with JAMF (UEM vendor) to provide Zero Sign-on capability for desktops or laptops managed by them.

Before you begin

- Verify that you provide the CA signer certificate from the 3rd party UEM used for the identity certificate in the managed desktops.
- Verify that you have the Desktop Identity Certificate CA referenced in Certificate based Single Sign On (Profile > Federation).
- Download the PKG file from MobileIron support site.

Procedure

1. Login to Access > UEM > 3rd Party UEMs.
2. Click Connect UEM.
3. Select JAMF.
4. Enter the following details:
   a. Enter a Name.
   b. Click Add Certificate under Desktop Identity Certificate CA.
5. Enter the Certificate Name and add the certificate.
   Or
   Paste the certificate.
   Only PEM and CER file types are allowed.
6. Click **Done**.

7. Click **Next**.

8. (Optional) Enter the **Management Check** details.
   Check whether desktop is registered to JAMF and check compliance if smart group is provided.
   - Enable to toggle for **"Verify desktop is managed by JAMF and limit access to only managed desktops"**. Enabling this option performs a check during MobileIron Authenticate registration and authentication to service providers.
   - Enter the **Tenant URL**.
   - Username
   - Password
9. (Optional) Enter the compliance criteria using Smart Group to enable restricted access to service providers. 
   Use the Zero Sign-on rule to enforce that only desktops compliant with this criteria are able to access the service providers governed by the policy.

10. Click Done.

11. Under UEM > 3rd Party UEMs, the JAMF instance is created.

12. Click Download Plist and save the XML as a .plist file to upload in JAMF.
Next steps

- Configuring MobileIron Authenticate on JAMF

What users see for FIDO2

FIDO2 is a feature available with the MobileIron UEM client. The MobileIron UEM clients are: MobileIron Go or Mobile@Work, and MobileIron Authenticate.

If FIDO2 solution is configured, users can authenticate and access enterprise cloud services from third party managed devices with MobileIron Authenticate installed.

When a user tries to log in, a push notification is sent to all active devices. When the user allows push notification on any appropriate device, access is granted for the session. However, on all other devices, the sessions become invalid and deactivating on this device does not deactivate on other devices.

The following provide information about the user experience with FIDO2:

- Workflow for registered browsers
- Workflow for non-registered browsers
- Workflow on Android devices
- Workflow on iOS devices
- Workflow for Desktop login

Workflow for registered browsers

A browser that launches after a successful MobileIron Authenticate registration, is a registered browser.

For a registered browser, when user tries to open the service provider, Access automatically invokes MobileIron Authenticate and authenticates the user using FIDO2.

If step up authentication is configured, user is prompted to either present biometrics or approve a push notification sent to MobileIron registered mobile device.

The following provides an example of the authentication workflow with a registered browser:
Workflow for non-registered browsers

Non-registered browser are browsers that are not default browsers and other browsers that are not registered with MobileIron Authenticate.

The non-registered browsers must authenticate using either MobileIron Authenticate, QR Code, or with Passwords.

The following provides an example to login using MobileIron Authenticate:
The following provides an example to login using QR Code:
The following provides an example to login using username and password credentials:
Workflow on Android devices

This section provides information for the various end user interactions on Android devices.
Unlocking a desktop on Android devices

To unlock a FIDO2 windows or mac desktop, you must authenticate from your device.

Unlocking a Windows desktop

The following provides an example to authenticate on a device using MobileIron Go, when a user tries to unlock his FIDO2 enabled Windows desktop:
Unlocking a Mac desktop

The following provides an example to authenticate on a device using MobileIron Go, when a user tries to unlock his FIDO2 enabled Mac desktop:

Activating a password-less sign-in on Android device

To activate a FIDO2 Android device, (If it is not already done during enrollment) go to MobileIron Go > Menu > Settings > Authenticate and turn on the toggle button. Follow authentication as shown below:
Deactivating a password-less sign-in on Android device

To deactivate an Android FIDO2 device, turn off the toggle button in **MobileIron Go > Menu > Settings > Authenticate**.

**Ending a browser session**

You can end a browser session from **MobileIron Go > Menu > Settings > Authenticate > End Browser Session**. Ending a browser session automatically signs you out of the company websites on the browsers.

**NOTE:** This option is available only if the user has active browser sessions running.
Workflow on iOS devices

This section provides information for the various end user interactions on iOS devices.

- Unlocking a desktop on iOS devices
- Activating password-less sign-in on iOS device
- Deactivating password-less sign-in on iOS device
- Ending a browser session on an iOS device

Unlocking a desktop on iOS devices

To unlock a desktop on an unlocked mobile, go to **MobileIron Go > Menu > Settings > Authenticate.**
To unlock a desktop on a locked mobile, go to MobileIron Go > Menu > Settings > Authenticate.
Activating password-less sign-in on iOS device

To activate a FIDO2 iOS device, go to MobileIron Go > Menu > Settings > Authenticate and turn on the toggle button. Follow authentication as shown below:
Deactivating password-less sign-in on iOS device

To deactivate an iOS FIDO2 device, turn off the toggle button in MobileIron Go > Menu > Settings > Authenticate.
## Ending a browser session on an iOS device

You can end a browser session from **MobileIron Go > Menu > Settings > Authenticate > End Browser Session**. Ending a browser session automatically signs you out of the company websites on the browsers.

### Workflow for Desktop login

You must login to a desktop and approve the push notification on your mobile device.
MobileIron Authenticate

MobileIron Authenticate is a Fast Identity Online (FIDO2) solution that simplifies the user experience while reducing the risk of data breaches. Authenticate ensures that only verified users can access business applications and it prevents the misuse of an employee's corporate credentials in case they are stolen.
Authenticate eliminates risky password-based security on desktop endpoints by providing a trust model for MobileIron-secured devices.

This authentication is done by requesting the user to present multiple factors to confirm their identity. Users gain instant approval through mobile push. Intelligent authentication flows adapt to the type of device, app, network, user location, and more.

MobileIron Authenticate leverages a user’s smartphone so the user no longer have to carry (and potentially misplace) cumbersome key fobs. Authenticate sends push notifications that enable quick access for convenient authentication based on the user’s needs.

### Configuring MobileIron Authenticate on MobileIron Cloud

Configure the FIDO2 Desktop Agent to provide password less authentication for cloud services and desktop login.

**Before you begin**

- Verify that you have configured MobileIron Cloud.
- Verify that you have uploaded the desktop identity certificate in MobileIron Access > UEM.
  - Download the certificate from MobileIron Cloud > Admin > Infrastructure > Certificate Management.

**Procedure**

1. On MobileIron Cloud, click Configurations > Add.
2. In the Search Configurations field, enter MobileIron Authenticate.
4. Enter the following details:
   a. Name
   b. Description

5. Under Configuration Setup, select the following:
   a. Select the Desktop Identity Certificate from the drop-down.
   b. Select the Operating System, macOS or Windows or both.

6. Select Windows and click Done to complete the Authentication.
   Windows does not require distribution.

OR
7. **Select macOS** and enter the **Key** and **Value** for **Custom Data**. Click **Next**.

   ![Image of MobileIron Authenticate Configuration page]

   **a. Select the devices to which the configuration is applied and click **Done** to complete the authentication.**

   ![Image of device selection page]
8. **Under Configurations**, select the MobileIron Authenticate configuration created and click **Details**.

9. Click **Copy Command Line Text** to distribute the app.

---

**Next steps**

**Adding and distributing a macOS application for MobileIron Authenticate**

After configuring MobileIron Authenticate for an appropriate operating system, the user adds the MobileIron Authenticate application in MobileIron Cloud.

**Before you begin**

- Download the PKG file for MobileIron Authenticate from the MobileIron support site.
Procedure

1. In MobileIron Cloud, click **Apps > App Catalog > Add**.

2. Select **In-House** from the drop-down.

3. Click **Choose File** and upload the PKG file appropriately. Click **Next**.
4. Enter the appropriate **Category** in the description page.

5. (Optional) **Add Screenshots** appropriately.
6. (Optional) Delegate this application if it should be inherited by newly created spaces.

   **App Delegation**

   Define whether this app should be inherited by newly created spaces.
   - Delegate this app to all spaces
   - Do not delegate this app

7. Choose any option to distribute the app between the appropriate users and click **Next**.
   a. **Everyone**
   b. **No One**
   c. **Custom**: Select **Users** or **User Groups**, **Distribution Filter** and view the **App Distribution Summary**.

   **Choose one of these options**

   - **Everyone**: All users will see this application in the app catalog.
   - **No One**: No user will see this app.
   - **Custom**: Define specifically who will see the app in the app catalog.

   **Select below to distribute this app**

   - **Users**
   - **User Groups**

   **App Distribution Summary**

   This app will be sent to:
   - **Individual Users**
   - **User Groups**

   **Distribution Filter**

   - **Name**: Mac Only Apps
   - **Description**: A default filter that limits app distribution to Mac devices only.
   - **Result**: Devices

   Other Distribution Filter Options
   - **Search Existing Distribution Filters...**
   - **Add Distribution Filter**

8. In **App Configurations**, configure the application as desired.
   a. **Install on device**: Allows specifying install settings for an application.
   b. **Promotion**: Defines how the app gets promoted and appears in the app catalog for specific groups or individuals.
   c. **Per App VPN**: Enables Per App VPN for the application such that it connects to enterprise services
through native iOS/macOS capabilities or using Tunnel app.

9. Click Done.

Adding and distributing a Windows application for MobileIron Authenticate

After configuring MobileIron Authenticate for an appropriate operating system, the user adds the Windows MobileIron Authenticate application in MobileIron Cloud.

Before you begin

- Download the MSI file for MobileIron Authenticate from the MobileIron support site.

Procedure

1. In MobileIron Cloud, click Apps > App Catalog > Add.

2. Select In-House from the drop-down.
3. Click **Choose File** and upload the MSI file appropriately. Click **Next**.

4. Enter the appropriate **Category** in the description page.

6. **(Optional)** **Add Screenshots** appropriately.

![Add Screenshots](image)

6. (Optional) **Add Screenshots** appropriately.

7. **(Optional)** Delegate this application if it should be inherited by newly created spaces.

![Delegate](image)

7. **(Optional)** Delegate this application if it should be inherited by newly created spaces.

8. Choose any option to distribute the app between the appropriate users and click **Next**.
   
a. **Everyone**

b. **No One**

c. **Custom**: Select **Users** or **User Groups**, **Distribution Filter** and view the **App**
9. **In App Configurations**, configure the application as desired.

   a. **Install on device**: Allows specifying install settings for an application.

   b. **Promotion**: Defines how the app gets promoted and appears in the app catalog for specific groups or individuals.

   c. **Per App VPN**: Enables Per App VPN for the application such that it connects to enterprise services through native iOS/macOS capabilities or using Tunnel app.

10. **Click Done**.
Configuring MobileIron Authenticate on JAMF

MobileIron Access integrates with JAMF (UEM vendors) to provide Zero Sign-On capability for desktops or laptops managed by them.

Before you begin

- Verify that you have the JAMF credentials and account to log in.
- Verify that you have downloaded the PKG package file from MobileIron Support site.
- Verify that you have configured JAMF in MobileIron Access. See Configuring UEM with JAMF in MobileIron Access.
- Verify that you have the .plist file that you saved when configuring JAMF in MobileIron Access. See Configuring UEM with JAMF in MobileIron Access.

Procedure

1. Login to JAMF account with admin credentials.
2. Click Computers> Configuration Profiles.
3. Click Upload > Choose File > Upload.
4. Click **Management Settings > Packages > New.**

![Image of Management Settings]

5. Enter the **Display Name** and select the **Category** to add the package to.

![Image of New Package]

6. Click **Upload Package File** to upload the PKG package file downloaded from the MobileIron Support site.

7. Click **Save.**
8. Click Policies > New > Display Name.

![Policy Configuration Screen]

9. Click Packages > Configure.

10. Add the PKG package file that was uploaded in Management Settings.

11. Click Save.

**What users see for MobileIron Authenticate**

After configuring MobileIron Authenticate on UEM, Windows or macOS desktops get notification to authenticate and register MobileIron Authenticate.

A silent registration is enabled by default for MobileIron Authenticate.

The following provide information about the user experience with MobileIron Authenticate:

- **Workflow on Windows desktop**
- **Workflow on macOS desktop**

**Workflow on Windows desktop**

**Workflow for Silent Registration**
Workflow on Windows desktop

Workflow for QR Code

Workflow for QR Code and password
Registration Status

Lock pass initiated on a Windows lock screen
Workflow on macOS desktop

Silent Registration
Workflow on a macOS light mode

Registration Status
Client Registration Settings

The Client Registration Settings is used to register Zero Sign-on clients such as MobileIron Go and MobileIron Authenticate with Access. MobileIron clients send the device identity certificate to Access for Zero Sign-on registration.

The device identity certificates used by MobileIron clients must follow the same schema as the certificate used in Certificate SSO, under Federation. Use the following setting to determine the username from the certificate and register.

Procedure

1. In MobileIron Access, go to Profile > Client Registration Settings.
2. For User Certificate, select the user certificate from which to get the user identification information such as the username.
The user certificate is the Tunnel sample certificate you uploaded to Access.

3. For **Field Name**, select the field from which the MobileIron UEM client gets user identifying information.

4. (Optional) For **Additional transforms**, enter a MiTra expression.
   Configure a MiTra expression if the value in the certificate does not map directly to the user identifying information.
   Example: select:X509:SubjectAltName:rfc822Name

5. Click **Save Registration**.

**Next steps**
- Configuring Zero Sign-on in MobileIron Access
- Configuring multi-factor authentication in Access

**Related topics**
For information about MiTra expressions, see Language to generate values from certificate fields.
Authenticator Only with MobileIron Access

Authenticator Only allows employees to use their unmanaged mobile device as their identity and authentication factor. Using their mobile device as their identity allows employees to take advantage of Zero Sign-on features, which allow passwordless access to SaaS applications and other business services.

- About Authenticator Only with MobileIron Access
- Configuring Authenticator Only on MobileIron Cloud
- Viewing Authenticator Only on MobileIron Cloud
- Configuring Authenticator Only on MobileIron Core
- Viewing Authenticator Only on MobileIron Core
- What users see for Authenticator Only

About Authenticator Only with MobileIron Access

In an Authenticator Only deployment, employees register their device with a MobileIron unified endpoint management (UEM) platform in Authenticator Only mode. A device that is registered with MobileIron in Authenticator Only mode is not managed by MobileIron. This means that mobile device management policies and configurations such as mobile threat defense, password requirements, Wi-Fi, VPN are not applied to the device. However, the Authenticator Only device checks in with the MobileIron UEM periodically and registers the posture of the device. If the Authenticator Only device is in compliance, users can continue to use it as their identity and authentication factor.

The following provides additional information about Authenticator Only with MobileIron Access:

- Required components for Authenticator Only
- Use cases for Authenticator Only
- Authentication flow for Authenticator Only
- Device actions and policies for Authenticator Only
- Android enterprise and Authenticator Only

Required components for Authenticator Only

Deploying Authenticator Only requires that the following components are set up:

- MobileIron Access deployment with a MobileIron unified endpoint management (UEM) platform. The MobileIron UEM platforms are:
Use cases for Authenticator Only

The following describes the authentication use case enabled with Authenticator Only devices:

- **Password less access from unmanaged devices**: Users accessing an enterprise cloud service provider (SP) from an unmanaged device are presented with a QR code. Scanning the QR code with their Authenticator Only device authenticates the user and allows access from the unmanaged device. Users scan the QR code using the MobileIron client and the native camera on the Authenticator Only device. Users do not need to enter their username and password. Users have the following additional options for subsequent log in:
  - Enable push notifications. If enabled, a push notification is sent to the managed device on subsequent log in from the unmanaged device.
  - Alternately, users can use the MobileIron client on their managed device to generate a one-time passcode (OTP). OTP allows users to access cloud services from the unmanaged device even when the MobileIron client does not have access to the Internet.

The following table describes the passwordless features with Authenticator Only devices:

<table>
<thead>
<tr>
<th>MobileIron UEM</th>
<th>MobileIron Client</th>
<th>Feature supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron Cloud</td>
<td>MobileIron Go for iOS</td>
<td>QR code, push notifications, OTP</td>
</tr>
<tr>
<td>MobileIron Core</td>
<td>Mobile@Work for iOS</td>
<td>QR code, push notifications, OTP</td>
</tr>
<tr>
<td>MobileIron Cloud</td>
<td>MobileIron Go for Android and Android enterprise</td>
<td>QR code, push notifications, OTP</td>
</tr>
<tr>
<td>MobileIron Core</td>
<td>Mobile@Work for Android and Android enterprise</td>
<td>QR code, push notifications, OTP</td>
</tr>
</tbody>
</table>

Authentication flow for Authenticator Only

The following describes the authentication flow from an Authenticator Only device using passwordless authentication.
1. User requests access to a cloud service from an unmanaged device, such as a desktop.
2. The cloud service redirects user to the configured identity provider (IdP) to authenticate. Since Access is the configured IdP, the request is redirected to Access.
3. Access generates and presents a QR code to the user.
4. The user scans the QR code with the mobile device in Authenticator Only mode to approve the login.
5. Access generates a new SAML response to redirect to the original SP. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

**Device actions and policies for Authenticator Only**

A device in Authenticator Only mode is not managed by MobileIron UEM. Device and app management policies and features are not available on a device in Authenticator Only mode. To view the device’s security posture, the following devices actions and policies are available and applied to Authenticator Only devices.

- Administrator actions (Cloud)
- Administrator actions (Core)
- Device user actions
- Compliance polices and actions (Cloud)
- Polices and actions (Core)
Administrator actions (Cloud)

Administrators can take the following actions on Authenticator Only devices on MobileIron Cloud:

- Retire: The Retire action removes the SaaS configuration (Cloud) or policy (Core) from the device and retires the device.
- Add to Group: Select or change the device group.
- Assign Custom Attributes
- Remove Custom Attributes
- Assign to user
- Force Check-in
- Set Ownership

Administrator actions (Core)

Administrators can take the following actions on Authenticator Only devices on MobileIron Core:

- Retire: The Retire action removes the SaaS policy from the device and retires the device.
- Apply to Label
- Remove from Label
- Set Custom Attributes: Set or clear custom attributes.

Device user actions

The following lists the actions device users can take on the User portal:

- Retire Device
- Send invitation

Compliance polices and actions (Cloud)

The following compliance policy is applied to Authenticator Only devices on Cloud:

- Compromised Devices policy: MobileIron Go checks in with the MobileIron Cloud and reports if the device is compromised. The device status is displayed in the listing for the device in Device > Device on MobileIron Cloud. The following compliance actions are applied on Authenticator Only devices:
  - Retire: Removes the SaaS configuration from the device and retires the device.
  - Quarantine: Uninstalls the SaaS only configuration and associated certificates.
Polices and actions (Core)

The following policies and compliance actions are applied to Authenticator Only devices on Core:

- Security policy: The default policy is applied.
- Sync policy: The default policy is applied.
- Privacy policy: The default policy applied.
- Compliance actions:
  - Quarantine: The SaaS policy is removed.

See "Managing Compliance" in the [Undefined variable GlobalBookTitles.DDAG]]

Android enterprise and Authenticator Only

If the MobileIron UEM supports both Work Profile for device management (MDM), as well as Authenticator Only, the Work Profile policies and configurations take priority.

Therefore, MobileIron recommends creating separate user groups for Android enterprise and for Authenticator Only. Do the following:

- Apply the Authenticator Only devices to the Authenticator Only user group.
- Do not apply Android enterprise devices, polices, and configurations, to the Authenticator Only user group. The Android enterprise configurations are:
  - Android enterprise: Work Profile (Android for Work)
  - Android enterprise: Work Managed Device (Android for Work)
  - Android enterprise: Managed Device with Work Profile

Configuring Authenticator Only on MobileIron Cloud

An Authenticator Only deployment requires an Access deployment with MobileIron UEM, as well as additional configurations for Zero Sign-on in Access and in the MobileIron UEM. The configurations for Authenticator Only are done in MobileIron UEM. The following steps provide an overview of the configuration steps for deploying Authenticator Only and pointers to the relevant content in the MobileIron Cloud Administrator Guide.

Before you begin

- Ensure that you have an MobileIron Access deployment with MobileIron UEM.
  See Overview of configuration with MobileIron Cloud.
- Ensure that Zero Sign-on is configured.
  See "Zero Sign-on" in the Access Guide.
Procedure: Overview of steps

1. Create a user group to deploy Authenticator Only and manually add users to the group.
   See "Creating a manually managed user group" in the MobileIron Cloud Administrator Guide.

2. Create a dynamically managed device group with the rule "user group," which equals to the user group created for Authenticator Only.
   See "Adding a device group" in the MobileIron Cloud Administrator Guide.
   NOTE: If devices had been previously enrolled in a Cloud tenant, users will not be able to register with the same Cloud tenant using Authenticator Only. Delete the devices from the Cloud tenant, then register again with the same Cloud tenant using Authenticator Only.

3. Create an Authenticator Only configuration and assign it to the dynamically managed device group created for Authenticator Only.
   See Adding an Authenticator Only configuration on MobileIron Cloud.

   See Syncing with MobileIron Access

5. Download and register MobileIron Go.
   If Always require client registration is enabled in Users > User Settings > Device Registration Setting in MobileIron Cloud, users automatically get emails for registering their device using MobileIron Go. Device users download MobileIron Go to their device directly from the Apple App Store or from Google Play Store.
   See What users see for Authenticator Only for information about how device users can register their devices to your MobileIron Cloud instance.

Related topics

- About Authenticator Only with MobileIron Access
- What users see for Authenticator Only

Adding an Authenticator Only configuration on MobileIron Cloud

Create an Authenticator Only configuration on MobileIron Cloud.

Before you begin

You can create the Authenticator Only configuration only if a SaaS Sign on configuration is available. Therefore, verify that a SaaS Sign on configuration has been created. The SaaS Sign on configuration is created for a Zero Sign-on deployment. See "Zero Sign-on" in the Access Guide.
Procedure

1. In MobileIron Cloud, go to Configurations > + Add > Authenticator Only.

2. In the Name field, enter a name for the configuration.

3. (Optional) Expand + Add Description, to add a description for the configuration.

4. For SaaS Sign-On config, select a SaaS sign on configuration.
   The selected SaaS Sign-On configuration is pushed to the device. MobileIron Access uses the SaaS sign-on configuration to authenticate the device.

5. Click Next.

6. Verify that the the check box for Enable this configuration is selected.
   The option is selected by default.

7. Select the distribution group created for Authenticator Only.
   The configuration is distributed to the devices in the selected option.

8. Click Done.

Next steps
Syncing with MobileIron Access

Syncing with MobileIron Access

Sync with MobileIron Access to pull the UEM configurations.

Procedure

1. In MobileIron Access, navigate to the UEM tab.
2. Select the Cloud UEM and click the Sync UEM icon.
3. Enter the UEM administrator credentials and click Verify.
4. Click Done.

Next steps
See Registration workflow for Authenticator Only devices
Viewing Authenticator Only on MobileIron Cloud

After a device registers with MobileIron Cloud in Authenticator Only mode, device information and status is available on MobileIron Cloud.

- Devices list
- Device details

Devices list

A device in Authenticator Only mode is listed with all other devices registered with MobileIron Cloud. To view device listings, on MobileIron Cloud, go to **Devices > Devices**. Go to the Settings icon and select the check box for **Authenticator Only**. Selecting the option makes the **Authenticator Only** column visible in **Devices > Devices**. The Settings icon is visible on the top right corner of **Devices** listing page.

The value for **Authenticator Only** displays as **Yes** if the device is registered as an Authenticator Only device.

**Figure 57. Authenticator only column in devices list**

Device details

The **Authenticator Only device** label is seen for devices when you click on the device listing for more details.

**Tip:** The label is also visible in the user portal for an Authenticator Only device.
Configuring Authenticator Only on MobileIron Core

An Authenticator Only deployment requires an Access deployment with MobileIron UEM, as well as additional configurations for Zero Sign-on in Access and in the MobileIron UEM. The configurations for Authenticator Only are done in MobileIron UEM. The following steps provide an overview of the configuration steps for deploying Authenticator Only and pointers to the relevant content in the Getting Started with Core guide.
Before you begin

- You have set up MobileIron Access with MobileIron Core.
  See Overview of configuration with MobileIron Core.
- Ensure that Zero Sign-on is configured.
  See "Zero Sign-on" in the Access Guide.

Procedure: Overview of steps

1. Create an LDAP group for Authenticator Only deployment and configure the group in MobileIron Core.
   See "Managing LDAP users" in the Getting Started with Core guide.
   Alternately, you can add local users.
   See "Adding local users" in the Getting Started with Core guide.

2. Assign the Enable Authenticator Only Role user role to the Authenticator Only LDAP group or local user in MobileIron Core.
   When you assign the Enable Authenticator Only Role to a user, the Retire Device and Register Device User Portal roles are selected by default. The Retire Device and Register Device roles are the only User Portal roles available for Authenticator Only users. All other User Portal roles are grayed out.
   See "Assigning and removing device user roles" in the Getting Started with Core guide.

   NOTE: If a user is assigned the Enable Authenticator Only Role, then the user can register their device in Authenticator Only mode. This does not impact any devices that the user has already registered.

   FIGURE 60. ENABLE AUTHENTICATOR ONLY ROLE ON MOBILEIRON CORE

   See Syncing with MobileIron Access

4. Download and register Mobile@Work.
   In-app registration is supported. Users will need to use their enterprise credentials and know the Core server address to register. Device users download Mobile@Work to their device directly from the Apple App Store or from Google Play. See "In-app registration for iOS and Android" in the [[[Undefined variable GlobalBookTitles.DDAG]]].
Also see What users see for Authenticator Only for information about how device users can register their devices to MobileIron Core.

Syncing with MobileIron Access

Sync with MobileIron Access to pull the SaaS sign-on configuration from the UEM.

Procedure

1. In MobileIron Access, navigate to the UEM tab.
2. Select the Core UEM and click the Sync UEM icon.
3. Enter the UEM administrator credentials and click Verify.
4. Click Done.

Next steps

See Registration workflow for Authenticator Only devices

Viewing Authenticator Only on MobileIron Core

After a device registers with MobileIron Core in Authenticator Only mode, device information and status is available on MobileIron Core.

- Devices list
- Device details

Devices list

A device in Authenticator Only mode is listed with all other devices registered with MobileIron Core. To view device listings, on MobileIron Core Admin Portal, go to Devices & Users > Devices.

The value for Authenticator Only displays as Yes if the device is registered as an Authenticator Only device.

![Figure 61. Authenticator Only column in devices list](image)

Device details

The Authenticator Only device label is seen for devices when you click on the device listing for more details.
What users see for Authenticator Only

Authenticator Only is a feature available with the MobileIron UEM client. If Authenticator Only is configured, users can register their unmanaged device in Authenticator Only mode. The device can now serve as the user’s identity and authentication factor, allowing users to authenticate and access enterprise cloud services from an unmanaged device without having to use their user name and password.

The following provide information about the user experience with Authenticator Only:

- Registration workflow for Authenticator Only devices
- Log in to cloud services
- Zero Sign-on with QR code - Android Authenticator Only devices
- Zero Sign-on with QR code - iOS Authenticator Only devices
- Zero Sign-on with push notifications or OTP
- Device out of compliance
- Deactivate Authenticator Only on the device

Registration workflow for Authenticator Only devices

To register their devices with MobileIron UEM in Authenticator Only mode, users can download the MobileIron UEM client (MobileIron Go or Mobile@Work) from the Apple App Store or from Google Play Store.
IMPORTANT: Only in-app registration is supported.

- Authenticator Only registration workflow on Android devices
- Authenticator Only registration workflow on iOS devices

Authenticator Only registration workflow on Android devices

To register their unmanaged device in Authenticator Only mode, users download the MobileIron UEM client from the Google Play Store. The following picture illustrates the Authenticator Only registration workflow using MobileIron Go on Android devices.

**Figure 63. Authenticator Only registration workflow on MobileIron Go for Android**

Users are prompted to grant permission for MobileIron Go to access the camera. Access to the camera is needed to scan the QR code for passwordless authentication. If biometrics is configured on the UEM, device users are prompted to set up biometrics after they have registered.

Authenticator Only registration workflow on iOS devices

To register their unmanaged device in Authenticator Only mode, users download the MobileIron UEM client from the Apple App Store. The following picture illustrates the Authenticator Only registration workflow using MobileIron Go on iOS devices.
If biometrics is configured on the UEM, device users are prompted to set up biometrics after they have registered.

Log in to cloud services

When users attempt to access an enterprise cloud service on an unmanaged device, such as their desktop, they are presented with an interaction page.

The interaction page contains a QR code and the following options, which are provided for additional security and ease of use:

- **Yes, this is my personal computer**
  - By selecting this option, users indicate that the device is trusted.

- **No, this is a shared computer**
  - By selecting this option, users indicate that the device is publicly available.
Users scan the QR code with the MobileIron UEM client, MobileIron Go or Mobile@Work, on their mobile device to sign on to the enterprise cloud service. To scan the QR code, device users,

1. Tap the MobileIron UEM client on their mobile device.
2. Tap **Authenticate**.
3. Authenticate with pass code or biometrics.
   
The authentication method depends on the setup of the device and the MobileIron UEM client.

**NOTE:** The Authenticator Only device used to scan the QR code automatically becomes the primary device for passwordless authentication. Push notifications are sent to the primary device.

**Subsequent login attempts**

If users select the **Yes, this is my personal computer** option on the interaction page when scanning the QR code, the user ID is remembered on the browser for 30 days. For subsequent login attempts to the enterprise cloud services set up on Access:

- Login is seamless. Users are not prompted to sign in for the session timeout duration set by the administrator in Profile > SaaS Sign on.
- For login attempts after the session timeout duration, a push notification is automatically sent to their managed device. Users have the option to either enter an OTP or scan a QR code.
- At the end of 30 days, the user ID is no longer remembered in the browser, and users are once again prompted to scan a QR code.

If users select **No, this is a shared computer** the session management settings in the cloud service are applied.

**Zero Sign-on with QR code - Android Authenticator Only devices**

The following figure provides an example of the workflow on an Android Authenticator Only device when using passwordless authentication.

**FIGURE 66. SCANNING THE QR CODE - WORKFLOW ON ANDROID AUTHENTICATOR ONLY DEVICE**
Zero Sign-on with QR code - iOS Authenticator Only devices

The following figure provides an example of the workflow on an iOS Authenticator Only device when using passwordless authentication.

**FIGURE 67. SCANNING THE QR CODE - WORKFLOW ON iOS AUTHENTICATOR ONLY DEVICE**

*Figure 67.* Scanning the QR Code workflow on iOS Authenticator Only device

Zero Sign-on with push notifications or OTP

Push notifications are sent to the Authenticator Only device that was used to scan the QR code. Accepting the push notification on the Authenticator Only device completes the sign-on to the enterprise cloud service.

Users also have the option to generate and use a one-time passcode (OTP) instead of using a push notification. Generate the OTP on the Authenticator Only device, then click the OTP option on the unmanaged device to enter the passcode.

**FIGURE 68. LOGIN MESSAGE IF A PUSH NOTIFICATION IS SENT**

*Figure 68.* Login message if a push notification is sent
The following illustrates an example of the OTP workflow on an Android device using MobileIron Go.

**Figure 69. OTP Option on an Android Authenticator Only Device**

The following illustrates an example of the OTP workflow on an iOS device using MobileIron Go.

**Figure 70. OTP Option on an iOS Auth-only Device**

**Device out of compliance**

In a Authenticator Only deployment, if users scan the QR code with an Authenticator Only device that is out of compliance, an out of compliance message is presented. Access to the enterprise cloud service is not granted. A new QR code is presented to the user. Users can switch to a compliant Authenticator Only device to authenticate.

Users see the non-compliance message in the following cases:

- Initial login by user, however the Authenticator Only device is not in compliance.
- Subsequent login by user, however the push notification sent to the Authenticator Only device is not in compliance.
Deactivate Authenticator Only on the device

Users can deactivate Authenticator Only on their device. Users may want to deactivate Authenticator Only on a device if they want to use another Authenticator Only device to scan the QR code and receive push notifications on the new device. The device used to scan the QR code automatically becomes the primary device for Authenticator Only and receives push notifications if the user enabled the feature when scanning the QR code. Deactivating Authenticator Only on the device stops the device from receiving push notifications.

To deactivate Authenticator Only in the UEM client for Android, open the menu and tap **Settings > Sign Out.**
When users sign out, the device is unregistered from the UEM. However, the MobileIron UEM client app remains on the device. To register once again, launch the MobileIron UEM client app on the device and enter the username and password.

On iOS devices, users deactivate Authenticator Only by removing the MobileIron UEM client from the device. To use the device as user's identity and authentication factor, device users can install and register the MobileIron UEM client for iOS in Authenticator Only mode.
Multi-factor Authentication with MobileIron UEM Client

Multi-factor authentication with the MobileIron UEM client allows device users to use their managed mobile device for second-factor authentication.

IMPORTANT: The reference to multi-factor authentication in device settings is removed from Access user interface. Use the Client Registration Settings to register clients such as MobileIron Go and MobileIron Authenticate with Access. For more information about configuring, see Configuring multi-factor authentication in Access.

The multi-factor authentication feature is not supported with Access + Standalone Sentry deployments.

The following provide more information about multi-factor authentication:

- About multi-factor authentication with MobileIron UEM client
- Overview of configuring multi-factor authentication with MobileIron UEM client
- Configuring multi-factor authentication in Access
- What users see for multi-factor authentication in UEM client

About multi-factor authentication with MobileIron UEM client

All approval notifications are sent to the primary device. Users also have the option to generate one-time passcode (OTP).

- Required components for multi-factor authentication with MobileIron UEM client
- Use cases for multi-factor authentication
- One-time passcode (OTP)
- About multi-factor authentication with MobileIron UEM client

Required components for multi-factor authentication with MobileIron UEM client

Deploying multi-factor authentication with MobileIron Access requires that the following components are set up:

- MobileIron Access deployment.
- MobileIron UEM client.

See the MobileIron Access Release Notes for supported versions.
Use cases for multi-factor authentication

- Two-factor authentication to enterprise cloud services with push notification. Users accessing an enterprise cloud service confirm their identity by:
  - Providing their user credentials, typically the name and password, to the identity provider.
  - Accepting the push notification on their managed device.
- Two-factor authentication to enterprise cloud services with one-time passcode (OTP). Users accessing an enterprise cloud service confirm their identity by:
  - Providing their user credentials, typically the name and password, to the identity provider.
  - Generating a one-time passcode (OTP) using their MobileIron UEM client, and entering the OTP in addition to their user credentials.
- In addition, administrators can configure conditional rules to define when multi-factor authentication is triggered.
  Example: Create a User Info Rule to trigger multi-factor authentication for only a certain set of users or groups, a Network Rule to trigger multi-factor authentication if the user is outside the enterprise IP range.

One-time passcode (OTP)

Device users have the option of generating a one-time passcode (OTP) in the MobileIron UEM client, which they can use instead of using push notification. OTP provides users another option to control access to enterprise cloud services from another managed device. It also provides an option to control access to enterprise cloud services even when the MobileIron client does not have access to the Internet.

The OTP for multi-factor authentication is displayed when the MobileIron UEM client is launched.

Multi-factor authentication flow

The following describes the authentication flow with multi-factor authentication.
**Figure 73. Multi-factor authentication flow**

1. User requests access to a cloud service.
2. The cloud service redirects user to the configured identity provider (IdP) to authenticate. Since Access is the configured IdP, the request is redirected to Access.
3. Access redirects the request to the original IdP.
4. The original IdP challenges the user for a user name and password.
5. The user enters the user name and password and posts to the IdP.
6. Access obtains the user identity from the SAML response, and sends a push notification to the managed device registered to receive authentication push notifications for that user. If one-time passcode (OTP) is enabled, users have the option to generate an OTP in the UEM client. See One-time passcode workflow.
7. The user receives the push notification and launches the UEM client to respond. If the user approves the transaction, the UEM client authenticates to Access.
8. If Access verifies the user identity received from the UEM client to be the same as the user identity received in the SAML response, Access generates a new SAML response to redirect to the original SP.
9. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

**One-time passcode workflow**

Device users can generate a one-time passcode (OTP) in the UEM client. A progress value indicates for how long the OTP is valid.
The following describes the OTP workflow when users access a cloud service provider (SP) from a browser or an unmanaged app or device:

1. Users are redirected to an interaction page to enter their credentials. They have the option to click on the Enter one-time password link to enter the OTP obtained from the UEM client.
2. Access validates the passcode entered by the user against the passcode generated by the MobileIron UEM client. A match completes the second-factor authentication of the user.
3. Access verifies and retrieves the user identity from the activated device and generates a new SAML response to redirect to the original SP.
4. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

Overview of configuring multi-factor authentication with MobileIron UEM client

Multi-factor authentication requires configurations in Access as well as in the MobileIron UEM.

Before you begin
• Ensure that you have an Access deployment.
  See Set up Access with MobileIron UEM.

Procedure: Overview of steps

1. Configure multi-factor authentication in MobileIron Access
  See Configuring multi-factor authentication in Access
2. Configure SasS sign-on in MobileIron UEM.
  See Configuring Zero Sign-on in MobileIron Cloud.
  OR
  See Configuring Zero Sign-on in MobileIron Core

Related topics
• About multi-factor authentication with MobileIron UEM client

Configuring multi-factor authentication in Access

The following describes the multi-factor authentication configuration in Access.

Procedure: Overview of steps

  See Configuring user ID for multi-factor authentication.
2. Add a conditional rule in Access for enabling multi-factor authentication, which triggers authentication using the MobileIron UEM client.
   See Adding a conditional rule for multi-factor authentication.
3. Configure your company branding. Users see the branding on the messages on the device from which they attempt to access cloud services.
   See Configuring branding for multi-factor authentication in Access.
4. Publish the changes.
   See Publishing the changes.

Configuring user ID for multi-factor authentication

Enable multi-factor authentication in MobileIron Access in Profile > Client Registration Settings. You will also map the fields from which the MobileIron UEM client gets user identifying information.

Before you begin
Upload a sample Tunnel certificate in Profile > User Certificates. For more information, see User Certificates.

Procedure

1. In MobileIron Access, go to Profile > Client Registration Settings.
2. For User Certificate, select the user certificate from which to get the user identification information.
   The user certificate is the Tunnel sample certificate you uploaded to Access.
3. For Field Name, select the field from which the MobileIron UEM client gets user identifying information.
4. (Optional) For Additional transforms, enter a MiTra expression.
   Configure a MiTra expression if the value in the certificate does not map directly to the user identifying information.
Example: select:X509:SubjectAltName:rfc822Name
5. Click Save.

NOTE: One time pass code (OTP) is enabled by default.

Next steps
Add a conditional rule for multi-factor authentication. See Adding a conditional rule for multi-factor authentication.

Related topics
For information about MiTra expressions, see Language to generate values from certificate fields.

Adding a conditional rule for multi-factor authentication

In the default policy in MobileIron Access, add a Multi-Factor Authentication conditional rule. The rule triggers multi-factor authentication.

Procedure

1. In MobileIron Access, go to Profile > Conditional Access.
2. Expand Default Policy.
3. Click +Add Rule > Multi-Factor Authentication to add the conditional rule.
4. Complete the requested fields.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the multi-factor authentication rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive text for the rule.</td>
</tr>
</tbody>
</table>
| Map the Identity Provider (IDP) user ID to Authenticator user ID | Select one of the following:  
• SAML Subject (Default)  
• SAML Attribute |
| Additional transforms | (Optional) Enter a MiTra expression.  
Configure a MiTra expression, if the value in the federation response does not map directly to the user identifying information.  
Example: The certificate contains the base-64 representation of the user ID, however you need the hex representation. Enter the following:  
decode:Base64 |
| Rule Action | From the drop down menu, select Allow. |

5. Click Done to save the policy and rule.  
The rule appears at top of the list in the policy.

6. Ensure that the Trusted App and Device rule is enabled and the rule is moved to the top of the list.

7. Edit the General Bypass rule, and set the Action for the rule to Block.
NOTE: You can create additional conditional rules to further define how multi-factor authentication is triggered. For example, you can create an **User Info Rule** to trigger multi-factor authentication for only a certain set of users or groups.

**Next steps**

**Related topics**
For information about MiTra expressions, see Language to generate values from certificate fields.

**Configuring branding for multi-factor authentication in Access**

Customize the user experience for your enterprise users by uploading your company logo to Access. The user notification screens are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

**Procedure**
1. In Access, go to **Profile > Branding**.
2. In the **Company Logo** section, drag and drop your company logo or click **Choose** to navigate to the location of the file and add.

**Next steps**
Publish the updates. See Publishing the changes.

**Publishing the changes**

Publish the changes to make the updates available.

**Procedure**
1. In the Access administrative portal, go to **Profile > Overview**.
2. Click **Publish**.
   - Publish is only available if a federated pair has been created.
3. Click **OK**.

**Next steps**
Configure SaaS sign-on in MobileIron UEM.

- See Configuring Zero Sign-on in MobileIron Cloud.
- OR
- See Configuring Zero Sign-on in MobileIron Core

**Related topics**
Publishing a profile
What users see for multi-factor authentication in UEM client

If multi-factor authentication is configured, device users can authenticate and access enterprise cloud services from an unmanaged device. Users see the **Authenticate** option in the MobileIron UEM client on their managed device.

![Authenticate option in MobileIron UEM client](image)

The following topics provide information about multi-factor authentication on the MobileIron UEM client:

- Access cloud services
- Custom service provider
- Generating one-time passcode (OTP)

Access cloud services

When users attempt to access an enterprise cloud service from an unmanaged device, they are prompted to enter their user name and then prompted to confirm the request on the managed device that has the UEM client.

**NOTE:** The configured IdP challenges users for their credentials. MobileIron Access does not ask users for their credentials.

A prompt appears on the managed device alerting the user to the access request. If users accept the prompt, they are allowed access from the unmanaged device. If users decline the prompt, they see an authentication failed message on the device and the authentication request from the device is blocked.
**Custom service provider**

The interaction pages and push notification for two-factor authentication display the service provider (SP) name and logo. For a custom service provider, if a name is not configured, the interaction pages and push notifications display **Custom Service Provider** for the SP name. If a logo is not configured for the custom SP, the name of SP is seen where the logo would have been displayed.

**Generating one-time passcode (OTP)**

Device users can generate a one-time passcode in the MobileIron UEM client. Users may want to generate an OTP if the managed device does not have access to the Internet.

**Procedure**

1. Launch the MobileIron UEM client.
2. Tap **Authenticate** > **One-Time PIN**.
Figure 76. One-time PIN

Generating one-time passcode (OTP)
Multi-factor Authentication with MobileIron Authenticator

Multi-factor authentication with MobileIron Authenticator allows device users to use their managed mobile device, which has the MobileIron Authenticator app, for second-factor authentication. The managed device on which the Authenticator app is installed is the primary device.

The multi-factor authentication feature is not supported with Access + Standalone Sentry deployments.

The following provide more information about multi-factor authentication:
- About multi-factor authentication with MobileIron Authenticator
- Configuring multi-factor authentication in Access for Authenticator
- What users see for multi-factor authentication

About multi-factor authentication with MobileIron Authenticator

For multi-factor authentication, there can be only one primary device. The managed device on which the Authenticator app is installed is the primary device. All approval notifications are sent to the primary device. If multiple managed devices have Authenticator installed, the latest managed device on which Authenticator is activated is considered the primary device. If enabled, users also have the option to generate one-time passcode (OTP).

- Required components for multi-factor authentication with MobileIron Authenticator
- Use cases for multi-factor authentication with MobileIron Authenticator
- One-time passcode (OTP) with Authenticator
- Multi-factor authentication flow
- One-time passcode workflow
- Authenticator app features

Required components for multi-factor authentication with MobileIron Authenticator

Deploying multi-factor authentication with MobileIron Access requires that the following components are set up:

- Access deployment
- MobileIron Tunnel
- MobileIron Authenticator app on a managed mobile device.
  The managed device can be either an iOS, Android, or Android enterprise device.
See the *MobileIron Access Release Notes* for supported versions.

**Use cases for multi-factor authentication with MobileIron Authenticator**

- MobileIron Authenticator provides two-factor authentication to enterprise cloud services. Users accessing an enterprise cloud service confirm their identity by:
  - Providing their user credentials, typically the name and password, to the identity provider.
  - Accepting the Authenticator notification on their managed device.
- In addition, administrators can configure conditional rules to define when multi-factor authentication with the Authenticator app is triggered. Example: Create a *User Info Rule* to trigger multi-factor authentication for only a certain set of users or groups, a *Network Rule* to trigger multi-factor authentication if the user is outside the enterprise IP range.

**One-time passcode (OTP) with Authenticator**

Device users have the option of generating a one-time passcode (OTP) in Authenticator, which they can use instead of using push notification. OTP provides users another option to control access to enterprise cloud services from another managed device. It also provides an option to control access to enterprise cloud services even when Authenticator does not have access to the Internet.

The OTP for multi-factor authentication is displayed when the application is launched.

**Multi-factor authentication flow**

The following describes the authentication flow with multi-factor authentication.
Figure 77. Multi-factor authentication flow

1. User requests access to a cloud service.
2. The cloud service redirects user to the configured identity provider (IdP) to authenticate. Since Access is the configured IdP, the request is redirected to Access.
3. Access redirects the request to the original IdP.
4. The original IdP challenges the user for a user name and password.
5. The user enters the user name and password and posts to the IdP.
6. The IdP verifies the user identity, generates a SAML Response containing the user identity and sends it to the configured service provider (SP) via a redirect. Since Access is the configured SP in the IdP, Access receives the redirect.
7. Access obtains the user identity from the SAML response, and sends a push notification to the managed device registered to receive authentication push notifications for that user. If one-time passcode (OTP) is enabled, users have the option to generate an OTP in Authenticator. See One-time passcode workflow.
8. The user receives the push notification and launches the Authenticator to respond. If the user approves the transaction, the Authenticator authenticates to Access using Tunnel.
9. If Access verifies the user identity received from Authenticator to be the same as the user identity received in the SAML response, Access generates a new SAML response to redirect to the original SP.
10. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.
One-time passcode workflow

The Authenticator app automatically generates and displays a one-time passcode (OTP) when device users launch the app. A progress value indicates for how long the OTP is valid.

The following describes the OTP workflow when users access a cloud service provider (SP) from a browser or an unmanaged app or device:

1. Users are redirected to an interaction page to enter their credentials. They have the option to click on the Enter one-time password link to enter the OTP obtained from Authenticator.
2. Access validates the OTP entered by the user against the OTP generated by Access for the activated device for that user. A match completes the second-factor authentication of the user.
3. Access verifies and retrieves the user identity from the activated device and generates a new SAML response to redirect to the original SP.
4. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

Authenticator app features

The Authenticator app provides the following features:

- The Authenticator app is easy to activate or deactivate on users' managed devices.
- Device users can either allow or block access to requests. They may want to deny access if an unknown user attempts to access an enterprise cloud service.
- If a request is not allowed or blocked within 5 minutes, the request expires and the authentication attempt from the device is blocked.
- Device users have the option to generate a one-time passcode (OTP) instead of using push notifications.
- If the managed device is locked, a notification is presented. Users unlock the device to view the request in Authenticator.
- Authenticator provides information about the service being accessed and device information and location.
- Administrators can add their company branding to the Authenticator app.

Configuring multi-factor authentication in Access for Authenticator

Multi-factor authentication requires a Access deployment, as well as additional configurations for multi-factor authentication in Access.

Before you begin

- Ensure that you have an Access deployment.
  See Set up Access with MobileIron UEM.
Procedure: Overview of steps

   See Configuring user ID for multi-factor authentication
2. Add a conditional rule in Access for enabling multi-factor authentication, which triggers authentication using the Authenticator app.
   See Adding a conditional rule for the Authenticator app.
3. Configure the user identifying information to use with the Authenticator app. Authenticator extracts the user identifying information from the certificate associated with MobileIron Tunnel.
4. Configure your company branding. Users see the branding on the messages on the device from which they attempt to access cloud services and on the Authenticator app.
   See Configuring branding for multi-factor authentication in Access.
5. Publish the changes.
   See Publishing the changes.
6. Add the Authenticator app to MobileIron EMM for distribution to managed devices.
   See the following:
   - Adding the Authenticator app to MobileIron Cloud
   - Adding the Authenticator app to MobileIron Core.

Configuring user ID for multi-factor authentication

Enable multi-factor authentication in MobileIron Access in Profile > SaaS Sign-on. You will also map the fields from which Authenticator gets user identifying information.

Before you begin
Upload a sample Tunnel certificate in Profile > User Certificates. For more information, see User Certificates.

Procedure

1. In MobileIron Access, go to Profile > Client Registration Settings.
2. For User Certificate, select the user certificate from which to get the user identification information.
   The user certificate is the Tunnel sample certificate you uploaded to Access.
3. For Field Name, select the field from which Authenticator gets user identifying information.
4. (Optional) For Additional transforms, enter a MiTra expression.
   Configure a MiTra expression if the value in the certificate does not map directly to the user identifying information.
   Example: select:X509:SubjectAltName:rfc822Name
5. Click Save Registration.

NOTE: One time pass code (OTP) is enabled by default.

Next steps
Add a conditional rule for the Authenticator app. See Adding a conditional rule for the Authenticator app.
**Related topics**
For information about MiTra expressions, see Language to generate values from certificate fields.

**Adding a conditional rule for the Authenticator app**

In the default policy in MobileIron Access, add a **Multi-Factor Authentication** conditional rule. The rule triggers multi-factor authentication using the Authenticator app.

**Procedure**

1. In MobileIron Access, go to **Profile > Conditional Access**.
2. Expand **Default Policy**.
3. Click **+Add Rule > Multi-Factor Authentication** to add the conditional rule for the Authenticator app.
4. Complete the requested fields.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the multi-factor authentication rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive text for the rule.</td>
</tr>
</tbody>
</table>
| Map the Identity Provider (IDP) user ID to Authenticator user ID | Select one of the following:  
- SAML Subject (Default)  
- SAML Attribute |
| Additional transforms | (Optional) Enter a MiTra expression.  
Configure a MiTra expression, if the value in the federation response does not map directly to the user identifying information.  
Example: The certificate contains the base-64 representation of the user ID, however you need the hex representation. Enter the following:  
decode:Base64 |
| Rule Action | From the drop down menu, select **Allow**. |

5. Click **Done** to save the policy and rule.  
The rule appears at top of the list in the policy.

6. Ensure that the **Trusted App and Device** rule is enabled and move the **Trusted App and Device** rule to the top of the list.

7. Edit the **General Bypass** rule, and set the **Action** for the rule to **Block**.

**NOTE:** You can create additional conditional rules to further define how the Authenticator app is triggered. For example, you can create an **User Info Rule** to trigger multi-factor authentication for only a certain set of users or groups.

**Next steps**
Related topics
For information about MiTra expressions, see Language to generate values from certificate fields.

Configuring branding for multi-factor authentication in Access

Customize the user experience for your enterprise users by uploading your company logo to Access. The user notification screen as well as the Authenticator app are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

Procedure
1. In Access, go to Profile > Branding.
2. In the Authenticator section, drag and drop your company logo or click Choose to navigate to the location of the file and add.

Next steps
Publish the updates. See Publishing the changes.

Publishing the changes

Publish the changes to make the updates available.

Procedure
1. In the Access administrative portal, go to Profile > Overview.
2. Click Publish.
   - Publish is only available if a federated pair has been created.
3. Click OK.

Next steps
Add the Authenticator app to MobileIron Cloud for distribution to managed devices. See the following:
- Adding the Authenticator app to MobileIron Cloud
- Adding the Authenticator app to MobileIron Core

Related topics
Publishing a profile

Adding the Authenticator app to MobileIron Core

Adding the Authenticator app to MobileIron Core makes the app available to distribute to managed devices.
- Adding the Authenticator app for iOS to MobileIron Core
- Adding Authenticator for Android AppConnect to MobileIron Core
- Adding Authenticator for Android enterprise to MobileIron Core
Adding the Authenticator app for iOS to MobileIron Core

Device users can download Authenticator for iOS directly from the Apple App Store. You can also distribute the app as a recommended app through Apps@Work.

Procedure

1. In MobileIron Core, go to Apps > App Catalog.
2. From the Quick Import drop-down list, select iOS.
3. Enter MobileIron Authenticator in the Application Name text box.
4. Click Search.
5. Select the app from the list that is displayed.
6. For MobileIron Authenticator, click Import.
7. Click OK on the pop-up message, and close the Quick Import dialog.
   MobileIron Authenticator is now listed in the App Catalog. Information included in the app, such as the name, is automatically configured. All other settings, such as the App Category and whether the app is a free app, are set to default settings.
   TIP: To view and edit the settings for the app, click on the app name in the App Catalog.
8. Apply the Tunnel VPN configuration to the app:
   a. Click on the app name in the App Catalog to edit the app settings.
   b. In the Per App VPN Settings, apply the Tunnel VPN setting to the app.
   c. Click Save.
9. Select the app to and apply to a label:
   a. Click Actions > Apply to Label.
   b. Select the label that represents the iOS devices for which you want the selected app to be displayed.
   c. Click Apply

Next steps
Create a managed app setting for the Authenticator app. See Creating a managed app setting for the Authenticator app for iOS.

Related topics
For more information about adding iOS apps to MobileIron Core for distribution, see the MobileIron Core Apps@Work Guide.

Creating a managed app setting for the Authenticator app for iOS

Create a managed app configuration for the Authenticator app to provide additional configurations for the device.

Before you begin
- Make a note of the bundle ID for Authenticator. The bundle ID is com.mobileiron.efa.distribution.mica
- Create a plist file with the following content:
Adding Authenticator for Android AppConnect to MobileIron Core

Upload the MobileIron Authenticator app to MobileIron Core as an in-house app and configure the app to make it available to Android devices.

Before you begin

- Ensure that Secure Apps Manager is also installed on MobileIron Core. For the supported Secure Apps Manager (SAM) version for Authenticator, see the MobileIron Access Release Notes.
- This section provides basic information about how to add and configure the Authenticator app for Android AppConnect. For information about AppConnect apps, see the MobileIiron Core AppConnect and AppTunnel Guide.

Procedure

1. In the MobileIron Core Admin Portal, go to Apps > App Catalog > Add+ > In-House. (Prior to MobileIron Core 8.0 go to Apps > App Distribution Library, and select Add App).
2. Add the apps just as you would any in-house app.
3. Add Secure Apps Manager (SAM) if you have not already uploaded it to support other secure apps.
4. After adding the apps, apply the apps to appropriate labels so that they are available to the required devices.

**Next steps**
Edit the AppConnect app configuration for Authenticator. See Configuring an AppConnect app configuration for Email+ in MobileIron Core.

**Related topics**
- For information on adding in-house apps for Android, see “Working with Apps for Android devices” in the MobileIron Core Apps@Work Guide.

**Configuring an AppConnect app configuration for Email+ in MobileIron Core**

When you add Authenticator for Android AppConnect, an AppConnect app configuration is automatically created for Authenticator. Edit the automatically-created AppConnect app configuration to add app specific configurations.

**WARNING:** Make sure only one AppConnect app configuration for Authenticator is applied to each device.

**Procedure**
1. In the MobileIron Core Admin Portal, go to Policy & Configs > Configurations.
2. Select the automatically-created AppConnect app configuration for Authenticator for Android, and click Edit.
4. In App-specific Configurations, add the following key-value pairs:
   - **Key:** ACC_URL
   - YourAccessCluster is either access-na1 or access-eu1.
   - Example: https://access.access-na1.mobileiron.com
5. Click Save.
   - The automatically-created app configuration has the same labels you applied to the app. You do not need to apply the automatically-created app configuration to a label.

**Adding Authenticator for Android enterprise to MobileIron Core**

Upload the MobileIron Authenticator app to MobileIron Cloud from the Google Play Store and configure the app to make it available to Android enterprise devices.

**Before you begin**
Ensure that your MobileIron Unified Endpoint Management (UEM) platform is set up for Android enterprise. Your MobileIron UEM is either MobileIron Cloud or MobileIron Core.
   - MobileIron Cloud: See the MobileIron Cloud online help documentation.

**Procedure**
1. In MobileIron Core, go to Apps > App Catalog > +Add.
2. Select Google Play from the drop-down menu next to the search box.
3. In the search box, enter MobileIron Authenticator.
4. Click **MobileIron Authenticator** to select the app.
5. Click **Next and then Next**.
6. Choose a distribution option for the app and click **Next**.
7. Update the settings in **App Configurations** as follows:
   a. In **Install on device**, enable **Install on Device**.
      This is the recommended setup. **Install on Device** silently installs the app on the devices in the selected distribution option.
   b. In **Promotion**, update the promotion settings as needed.
   c. For **Managed Configurations for Android**, click +.
      Enter a name for the configuration.
      In the **Managed Configurations** section:
      YourAccessCluster is either access-na1 or access-eu1.
      Example: https://access.access-na1.mobileiron.com
8. Click **Done**.
9. If necessary, update the Tunnel VPN configuration for Android to tunnel authentication traffic from MobileIron Authenticator to MobileIron Access.
   The Tunnel VPN configuration for Android is listed in MobileIron Cloud in **Configurations**.

**Related topics**
- See the MobileIron Core Apps@Work Guide for more information about adding Android enterprise apps to the MobileIron Core app catalog.

## Adding the Authenticator app to MobileIron Cloud

Adding the Authenticator app to MobileIron Cloud makes the app available to distribute to managed devices.

- Adding the Authenticator app for iOS to MobileIron Cloud
- Adding Authenticator for Android AppConnect to MobileIron Cloud
- Adding Authenticator for Android enterprise to MobileIron Cloud

### Adding the Authenticator app for iOS to MobileIron Cloud

Upload the MobileIron Authenticator app to MobileIron Cloud from the Apple AppStore and configure the app to make it available to iOS devices.

**Procedure**
1. In MobileIron Cloud, go to **Apps >App Catalog > +Add**.
2. Select the icon for AppStore from the drop down list.
3. Enter MobileIron Authenticator in the search text box.
4. Select **MobileIron Authenticator** from the search results and click **Next**.
5. Make updates as necessary and click **Next**
   You can change the category and add a description.
6. Choose a distribution option for the app and click **Next**.
7. Update the settings in **App Configurations** as follows:
   a. In **Install on device**, enable **Install on Device**.
This is the recommended setup. **Install on Device** silently installs the app on the devices in the selected distribution option.

b. In **iOS Managed App Configuration**, click +Add.
   For **Key**, enter ACC_URL.
   YourAccessCluster is either access-na1 or access-eu1.
   Example: https://access.access-na1.mobileiron.com

c. In **Per App VPN**, click + to add a per app VPN configuration.
   Select **Enable Per-App VPN for this app**.
   From the drop-down list, select the Per-App VPN configuration for Tunnel.

8. Click **Done**.

**Related topics**
See the **MobileIron Cloud Guide** or **Help** for more information on adding apps to the MobileIron Cloud app catalog.

**Adding Authenticator for Android AppConnect to MobileIron Cloud**

Upload the MobileIron Authenticator app to MobileIron Cloud as an in-house app and configure the app to make it available to Android devices.

**Before you begin**
- Ensure that Secure Apps Manager is also installed on MobileIron Cloud. For the supported Secure Apps Manager version for Authenticator, see the **MobileIron Access Release Notes**.

**Procedure**
1. In MobileIron Cloud, go to **Apps >App Catalog > +Add > In-House**
   Add the app just as would any in-house app.

2. Choose a distribution option for the app and click **Next**.

3. Update the settings in **App Configurations** as follows:
   a. In **Install on device**, enable **Install on Device**.
      This is the recommended setup. **Install on Device** silently installs the app on the devices in the selected distribution option.

   b. In **Promotion**, update the promotion settings as needed.

      Enter a name for the configuration.
      In the **AppConnect Custom Configuration** section:
      For **Key**, enter ACC_URL.
      YourAccessCluster is either access-na1 or access-eu1.
      Example: https://access.access-na1.mobileiron.com

4. Click **Done**.

5. If necessary, update the Tunnel VPN configuration for Android to tunnel authentication traffic from MobileIron Authenticator to MobileIron Access.
   The Tunnel VPN configuration for Android is listed in MobileIron Cloud in **Configurations**.
Related topics

- See the MobileIron Cloud Guide or MobileIron Cloud Help for more information on adding Android AppConnect apps to the MobileIron Cloud app catalog.
- See the MobileIron Tunnel for Android Guide for Administrators for information on configuring the Tunnel VPN configuration for Android.

Adding Authenticator for Android enterprise to MobileIron Cloud

Upload the MobileIron Authenticator app to MobileIron Cloud from the Google Play Store and configure the app to make it available to Android enterprise devices.

Procedure

1. In MobileIron Cloud, go to Apps > App Catalog > +Add.
2. Select Google Play from the drop-down menu next to the search box.
3. In the search box, enter MobileIron Authenticator. <is this what we are calling the app in Google play?>
4. Click MobileIron Authenticator to select the app.
5. Click Next and then Next.
6. Choose a distribution option for the app and click Next.
7. Update the settings in App Configurations as follows:
   a. In Install on device, enable Install on Device. This is the recommended setup. Install on Device silently installs the app on the devices in the selected distribution option.
   b. In Promotion, update the promotion settings as needed.
   c. For Managed Configurations for Android, click +. Enter a name for the configuration.
      In the Managed Configurations section:
      For ACC_URL, enter https://access. YourAccessCluster. mobileiron.com. YourAccessCluster is either access-na1 or access-eu1.
      Example: https://access.access-na1. mobileiron.com
8. Click Done.
9. If necessary, update the Tunnel VPN configuration for Android to tunnel authentication traffic from MobileIron Authenticator to MobileIron Access.
   The Tunnel VPN configuration for Android is listed in MobileIron Cloud in Configurations.

Related topics

- See the MobileIron Cloud Guide or MobileIron Cloud Help for more information on adding Android enterprise apps to the MobileIron Cloud app catalog.
- See the MobileIron Tunnel for Android Guide for Administrators for information on configuring the Tunnel VPN configuration for Android.

What users see for multi-factor authentication

MobileIron Authenticator provides secure login to your enterprise cloud services. If you have configured the app to be installed silently, which is recommended for a seamless user experience, the app is installed on managed devices when the device checks in with MobileIron Cloud.
NOTE: If a device user has already launched Authenticator for iOS as a standalone trial app, the device user must uninstall and reinstall the app to use it as a managed app.

The following topics provide information about multi-factor authentication:

- Activate MobileIron Authenticator
- Access cloud services
- Custom service provider
- Authenticator settings

**Activate MobileIron Authenticator**

To activate MobileIron Authenticator, users simply launch the app after it is installed.

**Figure 78. Launch Authenticator**

**Access cloud services**

When users attempt to access an enterprise cloud service, they are prompted to enter their user name and then prompted to confirm the request on the managed device that has the activated Authenticator app.

A prompt appears from the Authenticator app on the managed device alerting the user to the access request. If users accept the prompt, they are allowed access. If users decline the Authenticator prompt, they see an authentication failed message on the device and the authentication request from the device is blocked.

NOTE: The configured IdP challenges users for their credentials. MobileIron Access does not ask users for their credentials.
Custom service provider

The interaction pages and push notification for two-factor authentication display the service provider (SP) name and logo. For a custom service provider, if a name is not configured, the interaction pages and push notifications display Custom Service Provider for the SP name. If a logo is not configured for the custom SP, the name of SP is seen where the logo would have been displayed.

Authenticator settings

The following table describes the information available in Settings in the Authenticator app.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About</td>
<td>Tap to view version and license information.</td>
</tr>
<tr>
<td>Debug Logging</td>
<td>Disabled by default. Device users can enable debug logging if necessary.</td>
</tr>
<tr>
<td>Email Debug Log</td>
<td>Tap to enter an email address to send the debug logs.</td>
</tr>
<tr>
<td>Deactivate</td>
<td>Tap to deactivate the Authenticator app.</td>
</tr>
</tbody>
</table>
Access Certificates

The Certificates page lists the SSL certificates and signing certificates that have been uploaded to the MobileIron Access administrative portal.

Certificates

By default at least one SSL certificate and an Access Signing Certificate are always available. These certificates are not editable.

**Figure 80. SSL and signing certificates**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>sf_Signing</td>
<td>Generated Signing Cert</td>
<td>![icon] ![icon] ![icon]</td>
</tr>
<tr>
<td>Access Signing Certificate</td>
<td>Generated Signing Cert</td>
<td>![icon] ![icon] ![icon]</td>
</tr>
<tr>
<td>sslCert</td>
<td>Server Cert</td>
<td>![icon] ![icon] ![icon]</td>
</tr>
</tbody>
</table>

**Actions you can take**

You can take the following actions on a certificate:

- ![icon]: Click to view certificate details.
- ![icon]: Click to download the certificate.
- ![icon]: Click to delete the certificate.

**Note:** Only the X509 certificate is available for viewing or downloading. Private keys are not available for viewing or downloading.

**User Certificates**

The User Certificates page lists the client certificates that are uploaded to the MobileIron Access administrative portal. The Default Client Certificate is created by default. The Default Client Certificate can be used as a
Adding a certificate reference certificate and cannot be deleted.

**FIGURE 81. DEFAULT CLIENT CERTIFICATE**

Adding your own user certificate enables you to easily map fields from the certificate into federation responses generated by Access in Certificate based Single Sign-on. You can add a sample certificate used by your Tunnel VPN profile that is assigned to mobile applications that use cloud services federated with MobileIron Access.

**Before you begin**

Verify that you have created a certificate of your choice using the default certificate as a reference.

**Procedure**

1. In MobileIron Access, go to Profile > User Certificates, click **Add Certificate** to import a User Certificate.
2. Enter a **Certificate Name**.
3. Under **Upload Certificate**, click **Choose File** and browse to select the appropriate PEM certificate.
4. Click **Add Certificate**.
   The user certificate is added.
## Figure 82. User Certificate

### User Certificates

List of User Certificates. Click on 'Add Certificate' to import a User Certificate.

### Add Certificate

<table>
<thead>
<tr>
<th>NAME</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>jan_test_cert</td>
<td><img src="icon" alt="View Details" /> <img src="icon" alt="Delete" /></td>
</tr>
<tr>
<td>test1_cert</td>
<td><img src="icon" alt="View Details" /> <img src="icon" alt="Delete" /></td>
</tr>
<tr>
<td>test2_cert</td>
<td><img src="icon" alt="View Details" /> <img src="icon" alt="Delete" /></td>
</tr>
</tbody>
</table>

## Actions you can take

You can take the following actions on a certificate:

- ![View Details](icon): Click to view certificate details.
- ![Delete](icon): Click to delete the certificate.

**NOTE:** You cannot delete a certificate that is configured in a federated pair for single sign-on. In order to remove a certificate, you must first edit and associate the certificate with another certificate (during enabling cert SSO). This disassociates the older certificate. You can then remove the older certificate.

## User Certificate Details

The Client Certificate consists of **Certificate Details** and **Fields available for SSO configuration**. The Certificate Details lists the Issuer, Serial No, Validity and Version of the Certificate.

The **Fields available for SSO configuration** enable you to view and provide friendly names to fields populated in the User Certificate that you uploaded. These friendly names match the MiTra expression for a field used for SSO configuration.
Certificate expiry notifications

MobileIron Access periodically verifies the validity of the metadata for a service provider (SP) and identity provider (IdP) federated pair. A scheduled job runs every 24 hours to check the federated pairs metadata files. Any issues found during the scheduled job display as notifications in the administration portal in Profile > Federated Pair.

The verification includes checking the expiration date of the certificate embedded in the metadata. MobileIron Access sends email notifications to Access administrators on the 30th, 15th, and 7th day before the expiry of the certificate. Starting on the 7th day before the certificate is set to expire, an email notification is sent every day till the expiration date. Once the certificate expires, an email is sent to confirm that the certificate has expired.

IMPORTANT: Update the certificate before expiry to ensure that the most current certificates are available in Access. If the certificate in Access does not match the certificate in the SP or IdP, authentication will fail for device users accessing the federated cloud service through MobileIron Access. Authentication will continue to work as expected if the certificate in Access and in the SP or IdP are the same, irrespective of whether the certificates are expired or not.

In addition to email notifications, the following notifications are also provided in the MobileIron Access user interface:
- Notification in Profile > Federation
- Notification when you edit a federated pair or delegated IdP
- Notifications after a certificate expires

**Notification in Profile > Federation**

A notification displays in Profile > Federation. The notification includes the number of days remaining before the certificate expires. The row for the delegated IdP or federated pair with certificates that have warnings expands by default.

**Figure 84. Certificate expiration notification**

Notifications after a certificate expires

The following figure shows the notifications after the certificate expires for the delegated IdP or federated pair.
**Figure 85. Notification after certificate expires**

Notification when you edit a federated pair or delegated IdP

A notification displays when you edit the federated pair or delegated IdP. The notification includes the number of days remaining before the certificate expires. The following figures show notifications 30 days and one day prior to certificate expiration.

**Figure 86. 30 days before certificate expires**

<table>
<thead>
<tr>
<th>Edit federated pair</th>
<th>Cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Service Provider</td>
<td></td>
</tr>
<tr>
<td>Configure Service Provider</td>
<td>2</td>
</tr>
<tr>
<td>Choose Identity Provider</td>
<td>3</td>
</tr>
<tr>
<td>Configure Identity Provider</td>
<td>4</td>
</tr>
</tbody>
</table>

Salesforce

Conditional access control for the Salesforce mobile app and the ecosystem of applications that access Salesforce.com

Encryption Certificate

- Encrypt SAML assertions

Service Provider Metadata

Use the Help link for instructions on getting your Service Provider metadata

- Upload Metadata
- Add Metadata
- Metadata URL

No Metadata selected

Certification expires on: April 3, 2019 (30 days)

Native Mobile Application Single Sign-On (SSO)
 Updating certificates for an SP or IdP

Occasionally, you may need to update the service provider (SP) or identity provider (IdP) certificates for the federated pairs configured in Access. You must update the certificates if the service provider or identity provider certificate is about to expire or has expired. Access then provides notifications if the certificate expiration date is upcoming. The administrator can then update the certificate by providing the updated metadata. For information about certificate expiration notifications, see Certificate expiry notifications.

NOTE: MobileIron recommends to update certificates for uninterrupted services.

Certificate information is available in the service provider or identity provider metadata you upload to Access. Depending on whether you uploaded metadata, added metadata, or entered a metadata URL when configuring the federated pair, do one of the following to update the certificate:

- Certificate update if you uploaded metadata
- Certificate update if you entered a metadata URL
- Certificate update if you entered a metadata URL

NOTE: Access only consumes the information in the metadata. If the metadata references an expired certificate or soon-to-expire certificate, Access will continue to show the certificate expiration notifications.

Certificate update if you uploaded metadata

Do the following if you uploaded metadata from the service provider (SP) or identity provider (IdP) when configuring the federated pair.
Procedure

1. Get the metadata from the affected SP or IdP. See MobileIron Access Cookbooks for more details.

2. Go to Profile > Federation.

3. Click Update beside the warning message to update the certificate for the SP or IdP. The Update IDP metadata screen displays.
Certificate update if you added metadata

Do the following if you added a metadata when configuring the federated pair.

Procedure

1. Go to Profile > Federation.
2. Click Update beside the warning message to update the certificate for the SP or IdP. The Update IDP metadata screen displays.

Related topics

- For information about getting metadata from the SP or IdP, see "Before you begin" in Configuring federated pairs.
- For information about editing a federated pair, see Editing a federated pair.
- For information about downloading the Access proxy metadata and uploading the proxy metadata to the SP or IdP, see Uploading proxy metadata.
a. Update the certificate.
   If a valid certificate is updated, a confirmation message displays that the update is successful.

b. (Optional) Click Edit to change metadata to provide URL or Upload Metadata instead of Add Metadata.

Certificate update if you entered a metadata URL

Do the following if you entered a metadata URL when configuring the federated pair.

Procedure

1. Go to Profile > Federation.
2. Perform one of the following actions based on the changes:

a. **Update link for Metadata expired or expiring**: The Update IDP metadata window opens sync option is available. Click **Sync metadata** to complete the update. However, the modified attributes are not listed.

b. **Update link for change in metadata**: The Update IDP metadata window opens and the modified attributes are listed along with a sync button. Click **Sync metadata** to complete the update.

c. **Update SP or IDP metadata via menu option**: This is a one-click sync operation link. Clicking on the menu option syncs the metadata automatically and the quick update window displays the
attributes that are modified.

3. (Optional) Click **Edit** to **Upload** or **Add Metadata** instead of **Metadata URL**.
4. Click **Sync metadata > Close**.
   A sync completed successfully confirmation message displays.

**NOTE:** For Office 365 and Microsoft ADFS, when the Office 365 domain is federated with Access and Access is federated with ADFS, ADFS metadata is uploaded in Access or it can provided using metadata URL.

ADFS has certificate rollover functionality where it provides both primary and secondary signing certificates in the metadata. When the primary is about to expire, ADFS switches to secondary certificate. Access also uses the certificate which has later expiry date and monitors that certificate. This does not break the authentication.

However whenever the certificate is updated on ADFS side, it must either be uploaded in Access by providing new ADFS metadata or can also be synced using “Sync IdP Metadata” if ADFS metadata is provided using url.

**Related topics**

- View federated pairs
- Service provider (SP) metadata
- Identity provider (IdP) metadata
Reports

You can generate reports in the MobileIron Access administrative portal that provide information about authentication, errors, and certain audit actions.

About reports

The following types of reports are available in the Access administrative portal:

- **Access Reports**: Authentication traffic that goes through Access is captured and displayed in Reports > Access.
- **Session Revocation**: Session revocation report provides status information whether the user and service provider (SP) revocation action was successful or not and the context for the revocation. The report is displayed in Reports > Session Revocation. For more information, see Session Revocation.
- **Error Reports**: Whenever a device connection to gateway fails, an error report is generated and displayed in Reports > Errors.
- **Audit Log**: Actions taken by the Access local administrator in the Access administrative portal are displayed in Reports > Audit.
- **Authenticator**: The Authenticator report provides debugging and activity tracking logs for the multi-factor authentication activity from the Authenticator app in Reports > SaaS Sign-on.

Reports data is retained for 90 days.

You can download a report by clicking on Export. The report is downloaded as a CSV file. The export action is captured in the Audit log. If the download fails, a failure message is also captured in the Audit log.
**Figure 88. Access reports**

<table>
<thead>
<tr>
<th>ACTION</th>
<th>STATUS</th>
<th>SOURCE IP</th>
<th>TIMESTAMP</th>
<th>RESOURCE TYPE</th>
<th>USER AGENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloaded</td>
<td>Success</td>
<td>172.18.0.15</td>
<td>2019/01/16 1:57 PM</td>
<td>User</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36</td>
<td>Access report downloaded successfully</td>
</tr>
<tr>
<td>Login</td>
<td>Success</td>
<td>172.18.0.15</td>
<td>2019/01/16 1:57 PM</td>
<td>User</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36</td>
<td>User</td>
</tr>
<tr>
<td>Downloaded</td>
<td>Success</td>
<td>172.18.0.15</td>
<td>2019/01/16 1:57 PM</td>
<td>User</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36</td>
<td>Access report downloaded successfully</td>
</tr>
<tr>
<td>Login</td>
<td>Success</td>
<td>172.18.0.15</td>
<td>2019/01/16 1:57 PM</td>
<td>User</td>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36</td>
<td>User</td>
</tr>
</tbody>
</table>

Access reports

Authentication traffic that goes through Access is captured and displayed in Access Reports. Each IdP or SP proxy request to Access is logged and displayed as a separate row. For a single authentication instance, there may be up to two log entries.

Each row provides visibility into users, devices, and apps accessing cloud services.

You can do the following with the report data displayed in Access Reports:

- Filter the reported instances to view a subset.
- View details for the reported instances.
- Export the reported instances that are displayed.
- Search for reports in the search bar with advanced and flexible query search to filter desired report data.
- Access Report now displays the **Client IP** or the **Device IP** in the Access Reports.
Delegated IdP field in Access reports

MobileIron Access displays the persisting Delegated IDP field in Access reports that help users identify the log entries for delegated IdP.

authnRequestID field in Access reports

The authnRequestID field for SP proxy and IdP proxy in Access Reports allows administrators to correlate entries for the IdP proxy and SP proxy that are part of the same pair. The authnRequestID for SpProxy and IdpProxy is now visible in Access Reports which lets you relate between the two entries. Export the report to a .csv file to do the correlation.

NOTE: The authnRequestID is not searchable through flexible search.
Search Access reports

Access reports includes a search option that allows you to do advanced and flexible queries to filter the desired data and customize the report in Reports > Access.

The screen displays the advanced query that you can use to search the report. A maximum or 1024 characters is supported in a query.

The following query words are searched in the Search bar:

- Source IP
- UserAgent
- Username
- Exception
- Service Name
- Request Class
- Assertion Attributes
Flexible Query

The following flexible query types are supported. If more than one word (except boolean operators) is specified, the select condition is composed by operators.

Note the Following:

- An exception is thrown for any word (except boolean operators) with wildcard (*, ?) having length less than three characters. For example: ab*, a?b, etc results in an exception, while abc*, abc? will not result in exception.
- Searching is not case sensitive.

<table>
<thead>
<tr>
<th>Type</th>
<th>Supported Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators</td>
<td>AND</td>
</tr>
<tr>
<td>Unsupported characters</td>
<td>All characters except the invisible control characters and unused code points are supported.</td>
</tr>
<tr>
<td>Wildcards</td>
<td>* and ?</td>
</tr>
</tbody>
</table>

Query Examples

The following table provides examples of search queries.

<table>
<thead>
<tr>
<th>Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND Operator</td>
<td>To search for records having IP Address as 10.11.12.13 and Chrome as the User agent:</td>
</tr>
<tr>
<td></td>
<td>• 10.11.12.13 AND chrome</td>
</tr>
<tr>
<td>OR Operator</td>
<td>To search for records having IP Address as 10.11.12.13 or Chrome:</td>
</tr>
<tr>
<td></td>
<td>• 10.11.12.13 OR chrome</td>
</tr>
</tbody>
</table>

Difference between AND and OR.

A AND B means both A and B must be present in the record.
A OR B means either A or B should be present in the record.
Table 26. Search Query Examples (Cont.)

<table>
<thead>
<tr>
<th>Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOT Operator</td>
<td>NOT operator is used to exclude certain terms from the result.</td>
</tr>
<tr>
<td></td>
<td>For example, the below query returns all records that do not contain</td>
</tr>
<tr>
<td></td>
<td>chrome and 10.11.12.13</td>
</tr>
<tr>
<td></td>
<td>• NOT chrome AND NOT 10.11.12.13</td>
</tr>
<tr>
<td>Wildcard</td>
<td>If the details are partially unknown, use wildcards to fetch the results:</td>
</tr>
<tr>
<td></td>
<td>• 10.11.* AND chro*</td>
</tr>
<tr>
<td>Using Quotes (*)</td>
<td>1. Double quotes are used around search words to get the exact match.</td>
</tr>
<tr>
<td></td>
<td>For example: To fetch the results with chrome version, use the below query:</td>
</tr>
<tr>
<td></td>
<td>• “Chrome/60.0.3112.113”</td>
</tr>
<tr>
<td></td>
<td>This query returns the records that have chrome version, 60.0.3112.113</td>
</tr>
<tr>
<td></td>
<td>2. If two words are separated by a space, then by default OR operator is used.</td>
</tr>
<tr>
<td></td>
<td>For example, a search query, Intel Mac os x is interpreted as Intel OR Mac OR os OR x.</td>
</tr>
<tr>
<td></td>
<td>3. To search for space separated words as an exact string, apply double quotes around the whole string.</td>
</tr>
<tr>
<td></td>
<td>For example: &quot;Intel Mac os x&quot;</td>
</tr>
<tr>
<td></td>
<td>This query returns the records with complete string Intel Mac os x.</td>
</tr>
<tr>
<td>Grouping</td>
<td>Multiple Operators along with parenthesis can be used for searching.</td>
</tr>
<tr>
<td></td>
<td>For example, (chrome AND (10.11.12.13 OR 10.11.12.14))</td>
</tr>
<tr>
<td></td>
<td>This query returns all the records with chrome and IP Address as either 10.11.12.13 or 10.11.12.14.</td>
</tr>
<tr>
<td></td>
<td>NOTE: It is recommended to include parenthesis in the query as it provides grouping. For example, the above example without parenthesis might be interpreted differently by the system and desired results might not be obtained.</td>
</tr>
</tbody>
</table>

**Best Practice:** If the search word contains a special character, MobileIron recommends to use double quotes around the searched word.

For example: While searching for username joe@domain.com, it is recommended to use quotes around the username for better results - “joe@domain.com”.

Display exceptions in reports

When there is an Access Report with error, by expanding Report Details an exception message is displayed. When you click More, stack trace is also displayed. Also, the default message has the error code and message.
### Filtering report data

To filter report data, do one or a combination of the following in the left panel:

- Enter a **Start Date & Time** and **End Date & Time**.
- Select the data type to view a subset of the reported data.

**NOTE:** The report data is always sorted by timestamp in descending order. By default, the filter for time is set from 12 AM to 12 AM.

### Data available for filtering

The following fields are available to filter the report data. When you run a report, the active federated pairs, policies, and rules are listed on top of the list. The deleted items are structured at the bottom of the list.

**TABLE 27. DATA FOR FILTERING**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Date &amp; Time</strong></td>
<td>Enter a start date and time to filter the data.</td>
</tr>
<tr>
<td><strong>End Date &amp; Time</strong></td>
<td>Enter an end date and time to filter the data.</td>
</tr>
<tr>
<td><strong>Federated Pair</strong></td>
<td>Select the federated pair for which you want to see data.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Allow</td>
</tr>
<tr>
<td></td>
<td>• Block</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Warn</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td>Select the conditional access policy for which you want to see data.</td>
</tr>
<tr>
<td><strong>Rule</strong></td>
<td>Select the conditional access rule for which you want to see data. Only the rules in the selected policy are available for selection. If a policy is not selected, rules will not be available for selection.</td>
</tr>
</tbody>
</table>

### Viewing details

To view additional details for a report entry, click on one of the following options:
• **Show Detail**: Click on Show Detail to see the details for all rows.

• Click on the three dots (…) adjacent to each row to view details for that log entry.

**Figure 94. Report Details**

### Exporting Report Data

The **Export** feature allows you to download Access report data as a CSV file. You can then import the .csv file to a reporting tool and generate custom views and reports.

When you export report data, only the rows in the **Reports > Access** view will be downloaded. You cannot customize the fields for exporting.

**Procedure**

1. In the Access administrative portal, go to **Reports > Access**.
2. Click on **Export**. The Export Reports window appears that displays the size of the report file.

**Figure 95. Export Reports**

You are about to export 171 record(s). The expected report file size is 150.29 KB. To reduce the file size please select new or modify existing filter criteria.

3. Click **Export** if the size is appropriate.

A CSV file containing the report data is downloaded.

**Note The Following:**

• When a report is exported, there is an appropriate entry in the Audit reports.

• Use the left navigation filter to select appropriate records such as files that are larger in size. Only the filtered records are then exported in the file and can help in reducing file sizes.

### Errors Report

Whenever a device connection to MobileIron Access fails, an error report is generated and displayed in MobileIron Access. Each row provides visibility into Source IP, Tunnel Type, Error Domain, and Error Code.
To view the Errors report in MobileIron Access, click Reports > Errors. Reports are generated for the following error domains:

- **SSL_AUTH**: Errors related to authentication. For example, an invalid certificate.
- **COMPLIANCE**: Errors related to device reported in a non-compliant state.
- **CONFIGURATION**: Error in reading or processing tenant configuration update from MobileIron Access, or issues with local configuration of UEM.
- **CONNECTION**: Errors while attempting to connect to MobileIron Access.

**Figure 96. Error Report**

You can filter the Error report data displayed in Access Reports based on the following error domain:

- **SSL_AUTH**
- **COMPLIANCE**

For more information on search field, see Search in Access reports.

**Export error report**

Export the error report to a .csv file for correlation.

**Procedure**

1. In MobileIron Access, navigate to Reports > Errors. The Error report displays.
2. Click Export at the right hand top corner. The Export Reports window appears.
FIGURE 97. EXPORT REPORTS

Export Reports

The approximate file size of the report is 2.05 KB. Click on Export to download the report.

3. Click Export to confirm.
The report is exported to your local drive.

Audit Log

Actions taken by the MobileIron Access local administrator are captured in logs and displayed in Reports > Audit.

The Audit log displays audit trail information such as Actions, Status, SourceIP, Timestamp and so on.

The Description field now provides the following information about

- The policy update that displays the federated pair it belongs to.
- The rule update that displays the policy it belongs to.
You can do the following with the audit report data:

- Filter the reported instances to view a subset.

### Filtering audit report data

To filter audit report data, do the following the following in the left panel:

- Enter a **Start Date** and **End Date**.

### Audit report data available for filtering

The following fields are available to filter the report data:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>Enter a start date to filter the data.</td>
</tr>
<tr>
<td>End Date</td>
<td>Enter an end date to filter the data.</td>
</tr>
</tbody>
</table>

### Actions

Local administrator actions logged and reported in **Reports > Audit** include:
### Table 29. Administrator Actions Report in Audit

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Local administrator signs in to the Access administrative portal (User).</td>
</tr>
<tr>
<td>Logout</td>
<td>Local administrator signs out of the Access administrative portal (User).</td>
</tr>
<tr>
<td>Password Changed</td>
<td>The local administrator password is changed (User).</td>
</tr>
<tr>
<td>Password Reset</td>
<td>Password recovery key is reset.</td>
</tr>
<tr>
<td>Created</td>
<td>The following are created or added:</td>
</tr>
<tr>
<td></td>
<td>• Profile.</td>
</tr>
<tr>
<td></td>
<td>• Certificate.</td>
</tr>
<tr>
<td></td>
<td>• Service provider (SP) and identity provider (IdP) pair (SAML_Pair).</td>
</tr>
<tr>
<td></td>
<td>• Policy. A policy is automatically created when you click Continue in the App and Device Identity Trust screen in the Getting Started Wizard.</td>
</tr>
<tr>
<td></td>
<td>• Conditional rule for a IP address range (Source_IP_Rule).</td>
</tr>
<tr>
<td></td>
<td>• Conditional rule for an app or device platform (User-Agent_Rule).</td>
</tr>
<tr>
<td>Updated</td>
<td>The following are edited and saved:</td>
</tr>
<tr>
<td></td>
<td>• Profile is edited and saved.</td>
</tr>
<tr>
<td></td>
<td>• Service provider (SP) and identity provider (IdP) pair.</td>
</tr>
<tr>
<td></td>
<td>• Profile details are updated. (Policy).</td>
</tr>
<tr>
<td></td>
<td>• Conditional rule for a IP address range (Source_IP_Rule).</td>
</tr>
<tr>
<td></td>
<td>• Conditional rule for an app or device platform (User-Agent_Rule).</td>
</tr>
<tr>
<td></td>
<td>• Remediation page.</td>
</tr>
<tr>
<td>Deleted</td>
<td>The following are deleted:</td>
</tr>
<tr>
<td></td>
<td>• Service provider (SP) and identity provider (IdP) pair.</td>
</tr>
<tr>
<td></td>
<td>• Conditional rule for a IP address range (Source_IP_Rule).</td>
</tr>
<tr>
<td></td>
<td>• Conditional rule for an app or device platform (User-Agent_Rule).</td>
</tr>
<tr>
<td></td>
<td>• Standalone Sentry is deleted (CRT).</td>
</tr>
<tr>
<td>Rules_Reordered</td>
<td>Conditional rules are reordered (Policy).</td>
</tr>
<tr>
<td>Registered</td>
<td>A Standalone Sentry is registered to MobileIron Access (CRT).</td>
</tr>
<tr>
<td>Assigned</td>
<td>Standalone Sentry is assigned to the profile (CRT).</td>
</tr>
<tr>
<td>Unassigned</td>
<td>Standalone Sentry is unassigned from the profile (CRT).</td>
</tr>
<tr>
<td>Recovery Key Generated</td>
<td>A Recovery Key is generated for the Access administrator account.</td>
</tr>
<tr>
<td>EmailId</td>
<td>An Email ID is associated with Access.</td>
</tr>
</tbody>
</table>

Status provided for an action include:

- **Success:** The action was successful.
- **Failure:** The action was unsuccessful.
The description column provides a description of the action taken.

- Successful example: Saml pair SP-Box-IDP-PingIdentity created
- Failed example: Saml pair SP-Box-IDP-PingIdentity updated (failed)

## SaaS Sign-on

The SaaS Sign-on report provides debugging and activity tracking logs for the multi-factor authentication and single sign-on activity. The **Export** feature allows you to download SaaS sign-on report data as a CSV file. The SaaS sign-on reports have a retention period of 90 days.

Select the Service Provider, Auth Modes (Zero Sign-on or Multi Factor Authentication), Auth Methods (OTP, Push, QR Code, IDP Login), and the Status appropriately to fetch the desired report. The Auth Method that you select displays the appropriate Status for that method. Select the Status that is applicable to the method from the list.

**TIP:** For UserID, enter a partial or complete UserID in the query search bar.

**Figure 99. SaaS sign-on report**

The following table provides the multi-factor authentication actions logged and reported in **Reports > SaaS Sign-on**.

**Table 30. Actions reported for SaaS Sign-on**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Status</strong></td>
<td></td>
</tr>
<tr>
<td>Activated device</td>
<td>User activates the client app. The client app is either MobileIron Go or Authenticator.</td>
</tr>
<tr>
<td>Deactivated device</td>
<td>User deactivates the client app. The client app is either MobileIron Go or Authenticator.</td>
</tr>
<tr>
<td>No activated device</td>
<td>User tries to log in through the client app but has not activated the client app on a device.</td>
</tr>
<tr>
<td>Non Compliant Device</td>
<td>The users device does not meet the compliance policy.</td>
</tr>
</tbody>
</table>
### Table 30. Actions Reported for SaaS Sign-on (Cont.)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Status</strong></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>Push notification could not be sent.</td>
</tr>
<tr>
<td>IDP Login Attempted</td>
<td>User logs in using identity provider instead of SaaS Sign-on.</td>
</tr>
<tr>
<td>OTP incorrect</td>
<td>User uses an incorrect one-time passcode (OTP).</td>
</tr>
<tr>
<td>OTP successful</td>
<td>User uses one-time passcode (OTP) to approve the transaction and is successful.</td>
</tr>
<tr>
<td>Push rejected</td>
<td>Firebase or APNS returned an error, therefore a push notification was not sent.</td>
</tr>
<tr>
<td>Push successful</td>
<td>Push is successfully sent to the Firebase or APNS service.</td>
</tr>
<tr>
<td>QR code scanned</td>
<td>Allows the user to view only logs for authentication to the service provider done using QR code.</td>
</tr>
<tr>
<td>Sign-In requested</td>
<td>A sign-in request is received by notification or QR scan.</td>
</tr>
<tr>
<td><strong>SaaS Sign-on Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Invalid transforms</td>
<td>Configuration for SaaS sign-on in MobileIron Access in Profile &gt; SaaS Sign-on is incorrect. An incorrect configuration results in an exception during evaluation of the MiTra against the Tunnel certificate.</td>
</tr>
</tbody>
</table>
Settings

Use the Settings tab to perform the following tasks:

- Create administrators from the Admins tab. See Admins.
- Create Test IDPs from the Test IDP tab. See Working with Test IDP
- Create Test SPs from the Test SP tab. See Working with Test SP.
- Enable or disable account-level features, such as delegated IdP, from the Tenant Settings tab. See Delegated IdP.

Admins

The Admins tab lets you create, delete, reset password, and manage 2-Step Verification for administrators to manage the Access portal. It also lets you activate and deactivate (enable or disable) the administrators.

NOTE: The Reset Password and 2-Step verification is not available with Access Cloud portal.

Admins added in the Access tab will not have any Cloud role. They will only see the Access tab. Admins added in the Cloud tab may have Access roles as well as Cloud roles depending on what they are assigned.

FIGURE 100. ADMINS TAB

An administrator can perform tasks such as reset password, create Federated Pairs, create rules with conditional policies, and so on based on his role. These tasks are grouped as Configuration, Self Service, User Management, and viewing Analytics and Dashboard only tasks.
TABLE 31. ADMINISTRATOR TASK DETAILS

<table>
<thead>
<tr>
<th>Dashboard and Reports</th>
<th>Configuration</th>
<th>User Management</th>
</tr>
</thead>
</table>
| Viewing Dashboard and Reports only. | • Create a new profile  
• Create, Edit, and Delete federated pairs  
• Create, Edit, and Delete conditional access policies  
• Configure split tunneling  
• Manage branding  
• Manage certificates | • Create admin  
• Delete admin  
• Reset admin (not Applicable for Access Cloud portal)  
• Enable and Disable administrators  
• Change administrator role  
• Disable 2-Step Verification (not Applicable for Access Cloud portal) |

The administrator task details are provided in the following table:

TABLE 32. ADMINISTRATOR ROLES

<table>
<thead>
<tr>
<th>Role</th>
<th>Tasks based on Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Admin</td>
<td>A Root Admin is created by the tenant provisioning process. A Root Admin has all the permissions and can perform all the tasks as mentioned in the above table. The Root Admin cannot be disabled or deleted.</td>
</tr>
</tbody>
</table>
| Super Admin     | A Super Admin can perform Read-only, Configuration, and User Management tasks.  
A Super Admin can delete all other admins, except Root Admin. |
| Admin           | An Admin can perform Read-only and Configuration tasks.  
An Admin cannot delete any other admins. |
| Read-only Admin | A Read-only Admin can perform Read-only tasks only.  
A read-only Admin cannot delete any other admins. |

Adding an administrator

A Root Admin and a Super Admin can add multiple role-based administrators.

NOTE: When adding an Admin, do not use mobileiron.com as the domain.

Before you begin
• Verify that you have understood the various Admin Roles available in Access. See Admins.
• Verify that you have the correct password to authorize the Admin creation.
**Procedure**

1. Navigate to **Settings > Admins** and click **+ Add Admin**. The **Add New Admin** window opens.
2. In the **Admin details** panel, enter the following information in appropriate fields:
   - First name
   - Last name
   - Email
   - Display name
3. In the **Admin Roles** panel, select one of the following roles for the administrator:
   - Super Admin
   - Admin
   - Read-only Admin
4. Click **Save**. The new Admin is created.

**Deleting an administrator**

You can delete an admin based on your role.
- A Root Admin cannot be deleted.
- A Root Admin can delete other administrators.
- A Super Admin can delete all other administrators, except administrators with Root Admin role.
- The Admin and Read-only Admin cannot delete any administrators.
- The Admin role cannot delete their own account.

**Before you begin**

- Verify that you have understood the various Admin Roles available in Access. See **Admins**.
- Verify that you have the correct password to authorize the Admin deletion.

**Procedure**

1. Navigate to **Settings > Admins**. All the available administrators are displayed.
2. Click in the **Actions** column of the admin you wish to delete.
3. The admin is deleted successfully.

**NOTE:** You must always provide your login password to manage the administrators created.

**Resetting password for an Access administrator**

**NOTE:** Resetting the password for an Access administrator is not applicable for Access Cloud portal.

Administrators can reset the password of another administrator based on their role. The Audit log captures who reset the password. Self-reset password is not allowed as ‘Change Password’ is the specified option. Password reset is not allowed on a deactivated account.

The permission matrix for the roles to reset the password is as below:
TABLE 33. PERMISSION MATRIX

<table>
<thead>
<tr>
<th>Performs Action</th>
<th>Root Admin</th>
<th>Super Admin</th>
<th>Admin</th>
<th>Read-only Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Admin</td>
<td>x</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Super Admin</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Admin</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Read-only Admin</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Before you begin**

- Verify that you have understood the various Admin Roles available in Access. See [Admins](#).
- Verify that you have the correct password to authorize the password reset.

**Procedure**

1. Navigate to **Settings > Admins**. All the available administrators are displayed.
2. Click in the **Actions** column for the administrator you wish to reset the password.
   The password is reset and the affected administrator is emailed with the details to reset the password.

**Working with Test IDP**

The Test IDP tab lets you test IdP’s in your environment before using the identity provider in your production deployment. It is provided only for testing purposes. You must use only commercial IdPs such as Microsoft ADFS, Okta, OneLogin, or PingIdentity. You can add up to 5 test IdP users in your environment.

**Before you begin**

- Verify that you have downloaded the metadata file available on **Settings > Test IDP > Applications > Download Test IDP Metadata file**.
- Create a federated pair with your service provider metadata file and the Test IDP metadata file that you downloaded. For example, Salesforce metadata and Test IDP metadata.

**Procedure**

1. Navigate to **Settings > Test IDP** and click **Add Test IDP User**. The Add Test IDP User window opens.
2. Enter the **First name**, **Last name**, **Username**, **Email** and **New Password** for the IdP user.
3. Click **Done**. The IdP user is created.
4. On the **Applications** tab, click **Add Application** and enter the **App Name**.
5. Select **Add Metadata** or **Upload Metadata** to upload the Access SP Metadata file that you downloaded when creating a Federated Pair OR select **Metadata URL** and enter the URL for metadata details. For example, the Salesforce metadata file used to create the test federated pair.
6. Click **Done**.
7. The **Test IDP Reports** tab displays the report after being authenticated by test IdP, success or failure. Use this report to assess the IdP use in your deployment.
Working with Test SP

The Test SP tab lets you test SP’s in your environment before using the service provider in your production deployment. You can add up to 5 test SP users in your environment.

Before you begin

• Verify that you have the metadata (Entity ID) details for the test SP.

Procedure

1. Navigate to Settings > Test SP Users and click + Add Test SP User. The Add Test SP User window opens.
2. Enter the First name, Last name, Username, and Email for the SP user.
3. Click Done. The SP user is created.
4. On the Linked IDP tab, click + Add IDP Details and enter the IDP Name. Choose from one of the following options to login to the service provider:
   • Login to SP: Click this link to log in to the service provider.
   • Copy Login URL: Click this link to copy the SP login URL to use on a different browser.
5. Select Upload Metadata and upload the metadata file that you downloaded OR select Add Metadata and enter the details in the following table OR select Metadata URL and enter the URL for metadata details.

NOTE: When you upload the IDP metadata file, the details are populated by default.

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDP Name</td>
<td>Test IDP name.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Entity ID from the metadata file.</td>
</tr>
<tr>
<td>NameId Format</td>
<td>Supported values:</td>
</tr>
<tr>
<td></td>
<td>• EMAIL</td>
</tr>
<tr>
<td></td>
<td>• PERSISTENT</td>
</tr>
<tr>
<td></td>
<td>• TRANSIENT</td>
</tr>
<tr>
<td></td>
<td>• ENTITY</td>
</tr>
<tr>
<td>Auth Request Signed</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Assertion Signed</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Response Signed</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default IDP</td>
<td>Yes or No</td>
</tr>
<tr>
<td></td>
<td>If the default IDP value is set to True,</td>
</tr>
<tr>
<td>Binding Type</td>
<td>• REDIRECT</td>
</tr>
<tr>
<td></td>
<td>• POST</td>
</tr>
<tr>
<td>Redirect Location</td>
<td>Enter the data from the metadata file.</td>
</tr>
<tr>
<td>Field</td>
<td>Values</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Post Location</td>
<td>Enter the data from the metadata file.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>RSA_SHA1</td>
</tr>
<tr>
<td></td>
<td>RSA_SHA256</td>
</tr>
</tbody>
</table>

6. Click **Done**. The IDP details are added.
7. Click **Login to SP** to verify redirection.
   Login to SP redirects to Test IDP and after providing credentials and successful authentication, it redirects to Test SP.
Troubleshooting

The following topics help you troubleshoot:

- Password is not prompted by Email+ application when using Access for Office 365
- Salesforce from Web@Work does not display authentication page
- Salesforce produces incorrect metadata with invalid Entity ID

Password is not prompted by Email+ application when using Access for Office 365

**Problem:** Password does not prompt for Email+ configuration before using Access for Office 365.

**Cause:** The prompt for email password option is not set to true in the Email+ configuration.

**Solution:**

- For MiCloud, in App Configuration setup, set the *Prompt for Password Before Connecting to Server* to true in Email+ configuration.
- For Core, in AppConnect App Configuration, add *prompt_email_password* property and set the value to true.

Salesforce from Web@Work does not display authentication page

**Problem:** If your setup uses MobileIron Core, and you are using Okta as the IdP to access Salesforce, accessing Salesforce from Web@Work does not display the authentication page.

**Solution:** In the Standalone Sentry System Manager, in **Settings > Services > Sentry > Outgoing SSL**

**Configuration:** check **Enable SNI** and remove **SSLv2Hello** from Selected protocols.

Salesforce produces incorrect metadata with invalid Entity ID


**Solution:** MobileIron Access displays a warning message as follows:

You might have uploaded incorrect metadata. The EntityID in the uploaded metadata is saml.salesforce.com. However, it must be customdomain.my.salesforce.com.
When you upload the MobileIron Access metadata to Salesforce, download the Salesforce metadata again for the Access IDP and upload it again. Alternatively, edit the Salesforce metadata file and provide the correct Entity ID. Upload the modified metadata file again to MobileIron Access.
Appendix

This chapter provides more information about MobileIron Access features.

Configuring MobileIron Cloud for SSO certificates

Simple Certificate Enrollment Protocol (SCEP) must be configured in MobileIron Cloud to generate certificates from CAs configured within Cloud. To create the fields in user or device certificates, you must define SCEP. In order to define SCEP, it must obtain information from LDAP source.

LDAP source configuration

For the SCEP to request user certificates from CA, it must obtain the user information from the LDAP source. For example, Active Directory as an LDAP Source. You must configure two important attributes:

- User’s email address obtained from Active Directory. userPrincipalName is the LDAP attribute populated in the email field.
- User’s unique ID in the Active Directory. ObjectGUID is obtained and set as the attribute Custom 1.

After updating LDAP, you must sync LDAP. On the User’s tab, value of the custom attribute objectGUID is as below:

Figure 101. LDAP source configuration
SCEP configuration

The SCEP configuration must be updated in two locations in MobileIron Cloud:

- Admin > Certificate Authority
- Configurations > Add > Identity Certificate

After the LDAP configuration, to obtain the fields for certificates, define the SCEP. Add two sub-fields in the Subject Alternative Name field of the certificate.

- The sub-field of type RFC 822 Name holds the email address. As shown in the LDAP configuration, this corresponds to the $EMAIL$ directory attribute.
- The sub-field of type NT Principal Name (required only for Office 365) holds the unique immutable Id. This configuration corresponds to the objectGUID custom attribute.
  
  You must enter "fn:replace('ldap.objectGUID','\','""') manually in this field value.

If you are using a local user instead of LDAP, then you can hardcore the value of RFC 822 name to EmailID of the user.

For Office 365, you can get the immutable ID by executing the following command in ADFS Windows server PowerShell.

    Get-MsolUser -UserPrincipalName <username> | select ImmutableId

NOTE: Convert Immutable Id value from Base64 to Hex and then add it in the SCEP profile. Both the Subject Alt Names must be present in the SCEP profile for SSO to work.

**Figure 102. Identity certificate configuration**
### Configuring MobileIron Core for SSO certificates

Simple Certificate Enrollment Protocol (SCEP) must be configured in MobileIron Core to generate certificates from CAs configured in Core. To create the fields in user or device certificates, you must define SCEP.

- **LDAP source configuration**
- **SCEP configuration**

#### LDAP source configuration

For the SCEP to request user certificates from CA, it must obtain the user information from the LDAP source. For example, Active Directory as an LDAP Source. You must configure two important attributes:

- User’s email address obtained from Active Directory. `userPrincipalName` is the LDAP attribute populated in the email field.
- User’s unique ID in the Active Directory. `ObjectGUID` is obtained and set as the attribute Custom 1.
SCEP configuration

After the LDAP configuration to obtain the fields for certificates, you must define the SCEP. Add two sub-fields in the Subject Alternative Name field of the certificate.

- The sub-field of type RFC 822 Name holds the email address. As shown in the LDAP configuration, this corresponds to the $EMAIL$ directory attribute.
- The sub-field of type NT Principal Name (required only for Office 365) holds the unique immutable Id. As shown in the LDAP configuration, this corresponds to the User Custom 1 attribute.

NOTE: UI displays a drop-down list of values for this attribute that does not contain the User Custom 1 option. You must enter $USER_CUSTOM1$ manually in this field value.
Configuring LDAP in MobileIron Cloud for session revocation

Configure one or all of the following custom attributes in the LDAP configuration in MobileIron Core:

- userPrincipalName
- objectGUID

Procedure

1. In the MobileIron Cloud, go to Admin > LDAP.
2. Select an LDAP server and click the Edit icon.
3. Click Test Connection and Continue.
4. In the Configure LDAP Server page, scroll down to Set Custom Attribute.

**Figure 105. Edit LDAP Server**

5. Click + Add Custom Attribute.
6. Enter one or both of the following custom attributes:
   - userPrincipalName
   - objectGUID
7. Click Done.

Related topics

- For information about configuring LDAP in MobileIron Cloud, see "Admin > LDAP" in the MobileIron Cloud Administrator Guide or click Help in the MobileIron Cloud administrative portal.
- Configuring Session Revocation

Configuring LDAP in MobileIron Core for session revocation

Configure one or all of the following custom attributes in the LDAP configuration in MobileIron Core:

- userPrincipalName
- objectGUID

Procedure

1. In the MobileIron Core Admin Portal, go to Services > LDAP.
2. Select an LDAP server and click the Edit icon.

   ![Figure 106. Edit LDAP server](image)

3. In the Modifying LDAP Setting page, scroll down to Custom Attributes.
4. Enter one or both of the following custom attributes:
   - userPrincipalName
   - objectGUID
Use an available custom field or click **Create New Custom Attribute** to add a new custom field.

5. Click **Save**.

**Related topics**

- For information about configuring LDAP in MobileIron Core, see "Configuring LDAP servers" in the *Getting Started with Core Guide*.
- Configuring Session Revocation

**Customizing certificates for single sign-on in Access**

Certificate single sign-on lets you login to cloud services from managed apps on their devices without passwords. You can customize the certificates for single sign-on by selecting SAML Assertions with your SP. The SP requires additional information other than the email address in SAML Assertion’s Subject field.

If you are authenticating an original Identity Provider, the SAML message that Access obtains from the original IdP is relayed to the SP with minimal modifications. However, when the user is being authenticated using the Cert SSO, Access must construct the SAML message, and put the appropriate user identifying values from the certificate into the SAML assertion in that message. To provide flexibility in choosing and transforming values from the certificate and putting them in the SAML, MobileIron Access provides a flexible customization capability.

Currently, this capability is offered only when you choose the **Custom SP**.

- Configuring SAML assertion fields
- Language to generate values from certificate fields

**Configuring SAML assertion fields**

The MobileIron Access UI enabled you to choose the Certificate SAN rfc822Name and NTPrincipalName type values and add them into the SAML Subject or in SAML attributes. However, this might not be sufficient for all issues. For advanced configuration, select Custom and enter the values.

For more information, see [Configuring Mobile App Single Sign-on (SSO)](https://mobileiron.accessguide.com/).

**Language to generate values from certificate fields**

The values for either the subject or the attributes can be defined using **MobileIron Transform expressions** or **MiTra expressions**. The MiTra expressions are a comma-separated list of double-quoted strings. Each String in this list is called a specification. Each specification has a verb, a format and a format-specific pattern. The verb, format, and pattern are all separated by the ":" character. Evaluation of MiTra expressions is left-to-right, with the output of the preceding expression on the left is used as the input to the expression on the right. The first specification must be either a X509 format expression or a Literal format expression, so that values are either derived from the Tunnel certificate or a constant string.

The grammar for MiTra expressions is as follows:
The verb is a general description of the operation to be performed. The `encode` and `decode` verbs do not take any arguments. The `select` verb takes the `pattern` argument. The pattern specifies the selector within the format. For example, in X509, the pattern can be `Subject` or `SubjectAltName:rfc822Name`.

An example of a multi-expression specification is as follows:

```plaintext
select:X509:SubjectAltName:ntPrincipalName,decode:Hex,encode:Base64
```

The above expression sequence is used in constructing a SAML Subject for Office 365 from a cert that contains an ObjectGUID from an Active Directory. The following formats are supported by MiTra expressions:

| Format   | Description                               | Operations Supported | Notes                                                          |
|----------|-------------------------------------------|----------------------|                                                               |
| X509     | X.509 Certificates                        | select               |                                                                 |
| Literal  | Constants                                 | select               | Selection pattern is output verbatim.                         |
| RFC2253  | LDAP name simple text representation      | select               |                                                                 |
| URL      | URL-encoded data                          | select, encode, decode| Selection pattern is parameter name.                         |
| Hex      | Hex-encoded data                          | encode, decode       |                                                                 |
| HTML     | HTML format string                        | select               | Selection pattern is in CSS syntax.                          |
| HTTP     | HTTP request stream                       | select               | Selection pattern is either header name or `Content` to select the content. |
| Base64   | Base64 encoded data                       | encode, decode       |                                                                 |

**TABLE 34. MiTra Expressions**
TABLE 34. MITrA EXPRESSIONS (CONT.)

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Operations Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompressedBase64</td>
<td>Deflate encoded Base64</td>
<td>encode, decode</td>
<td></td>
</tr>
<tr>
<td>Deflate</td>
<td>Deflate encoded data</td>
<td>encode, decode</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td>XML-encoded data</td>
<td>select, decode</td>
<td>Selection pattern is XPath spec. Decode results in pretty-printed XML.</td>
</tr>
</tbody>
</table>

Selection pattern description

The selection pattern that appears in a MiTra expression after the second ":"., is dependent on the format on which that expression applies. The following is the syntax of the pattern for each format:

- **X509 Pattern Syntax**

```
X509pattern = ( "Subject" / sanPattern )
sanPattern = "SubjectAltName:" sub-type [ ":" occurence ]
sub-type = ( "otherName"/ "ntPrincipalName"/ "rfc822Name"/ "dnsName"/ "x400Address"/ "directoryName"/ "ediPartyName"/ "uniformResourceIdentifier"/ "ipAddress"/ "registeredId" )
occurence = *DIGIT ; ordinal number starting with 1 for the first occurrence.
```

To select the second SAN extension of type rfc822Name, you must specify the following string:

```
select:X509:SubjectAltName:rfc822Name:2
```

- **Literal**
  The pattern is any string that is selected in its entirety.

- **RFC 2253**
  RFC2253 is the string representation of LDAP names. A certificate's subject or subjectAltName:directoryName might result in a value of type RFC2253 name. To choose a specific value from an RFC2253 name, the pattern specifies the DN component name and optionally its occurrence from the right. For example, a MiTra expression of the form

```
select:RFC2253:DC:2
```

from the string

"CN=testuser2521, OU=contacts, DC=mobileiron, DC=com"

results in getting the value mobileiron.
Back up and restore Office 365 settings

Back up Office 365 settings
- Open the PowerShell command window and enter the following command to connect to the Office 365 tenant:

  PS c:\>Connect-MsolService

- Enter the following command to back up the current domain federation settings into a file:

  PS C:\Users\Administrator>Get-MsolDomainFederationSettings -DomainName <federated-domain> | Export-Clixml <xml-file-path>

  For example:
  Enter the following command to back up the current domain federation setting for the federated domain orange.com to an xml file c:\orange.com-original-settings.xml.

  PS C:\Users\Administrator>Get-MsolDomainFederationSettings -DomainName orange.com | Export-Clixml c:\orange.com-original-settings.xml

Restore Office 365 settings

Perform the following tasks to restore Office 365 settings from an existing saved file:
1. Load the configuration into a variable.

  PS C:\Users\Administrator>$original = Import-Clixml <xml-file-path>

  For example:
  load config from file c:\orange.com-original-settings.xml into variable $original

  PS C:\Users\Administrator>$original = Import-Clixml c:\orange.com-original-settings.xml

2. Enter the following command to unfederate the domain if the domain is federated.

  PS C:\Users\Administrator>Set-MsolDomainAuthentication -DomainName <federated-domain> -Authentication Managed

  For example:
  unfederate the orange.com domain

  PS C:\Users\Administrator>Set-MsolDomainAuthentication -DomainName <federated-domain> -Authentication Managed

3. Enter the following command to restore the configuration from the variable.

  PS C:\Users\Administrator>Set-MsolDomainAuthentication -DomainName <federated-domain> -FederationBrandName $original.FederationBrandName -Authentication Federated -PassiveLogOnUri

For example:
The restore federation settings for orange.com domain using WsFed protocol:

```
```

NOTE: The value of the federation-protocol depends if you used SAML or WS-Federation earlier. The acceptable values are SAMLP or WSFED.

**Configuring MobileIron Access Splunk application**

Splunk fetches Audit logs and Access reports for a tenant everyday from MobileIron Access. You must configure MobileIron Access Splunk application for this activity. Splunk v8.0.1 and MobileIron Access Splunk app v5.0 is now supported.

**Before you begin**
- Verify that you have installed Java 8 (JRE and JDK).
- Verify that before you upgrade, delete the configured data input for Access if any.

**Procedure**
1. Copy the app distribution .spl file (miaccess_splunk_ap.spl) to the Splunk machine.
   The .spl file is available at [MobileIron Product Documentation Page](#).
2. Login to Splunk > Apps.
   Click Install app from file and select miaccess_splunk_app.spl file. The Upload an app window opens.

![Figure 107. Splunk App](#)
3. Click **Choose file** and select `miaccess_splunk_app.spl`.
4. Select **Upgrade app. Check this will overwrite the app if it already exists.**

**NOTE:** If you do not have the miaccess-splunk app already installed, then deselect this box.

5. Click **Upload**.
   
   Once the upload completes, configure the data inputs.

6. Click **Settings > Data inputs.**

The `miaccess_splunk_app` entry is now listed in local **Data inputs.**
7. Click **New** in `miaccessSplunkApp` to configure the file.
   The data input screen appears.

8. Enter the following details:

   **NOTE:** You must not modify the data inputs when the job is running. However, you can modify the data inputs when the job is not running.
   
   - **MobileIron Access Splunk app Configuration:** Enter any name for the input configuration.
   - **MobileIron Access Read-only admin username** and **MobileIron Access Read-only admin password:** Enter the MobileIron Access username and password.

   **NOTE:** Use MobileIron Access read-only user.
   
   - **MobileIron Access admin url:** Enter the MobileIron Access admin URL such as `https://access-na1.mobileiron.com` or `https://access-eu1.mobileiron.com`.

   **NOTE:** If you do not see the app listed in local Data inputs, then restart Splunk.
- **MobileIron Access Read-only admin username**: Enter the MobileIron Access username.
- **MobileIron Access Read-only admin password**: Enter the password for MobileIron Access. The password is now masked.
- **Splunk user role username**: Enter the Splunk username with minimum user having edit_tcp role.
- **Splunk user role password**: Enter the Splunk user role password.
- **Splunk management port**: Enter the management port such as 8089.
- **Polling interval in hours**: Enter the frequency in number of hours to pull data from MobileIron Access.
- **Click Save.**

You can now monitor the fetching of audit logs and access reports in `splunkd.log` file. Use the following indexes to search for the reports after the Access Reports are available in Splunk:

- `index="miaccess_report_index"`
- `index="miaccess_audit_log_index"`

**Note The Following:**
- After importing the .spl file, if the app is not visible, then restart Splunk.
- When you configure Splunk for the first time, it pulls data for past 90 days which can take a few minutes.

**Splunk dashboard**

After adding and configuring the .spl file, the MiAccess application is available on the homepage. Click the application to view the dashboards for the application.

**Figure 112. Splunk dashboard**

The graphs are prepopulated for AuditLogs and AccessReports. There is one graph for AuditLogs and four graphs for AccessReports.

**Figure 113. Audit Logs**
**Figure 114. Access Reports Platforms**

**Figure 115. Access Reports Actions**
**Figure 116. Access reports Geodata**

![Access reports Geodata]

**Figure 117. Access reports Country name**

![Access reports Country name]

**Figure 118. Access reports Derived Useragents**

![Access reports Derived Useragents]