Simple and smart security for the enterprise cloud

MobileIron ACCESS

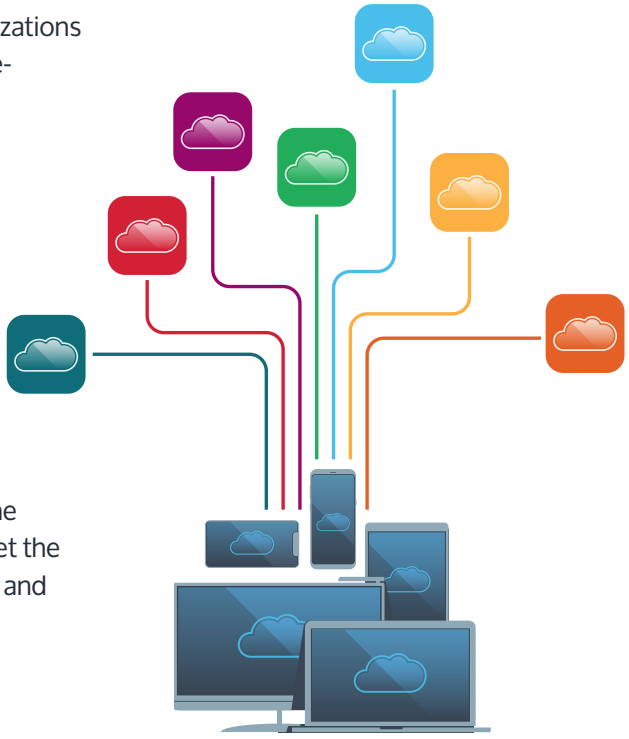
Protecting your mobile and cloud resources from unauthorized or malicious access is one of the biggest challenges organizations face today — and password-only security is no longer up to the task. In fact, in 2018, stolen user credentials are the top cause of enterprise data breaches.[1]

In the PC era, employees operated from within a well defined enterprise IT perimeter and passwords were sufficient to establish user trust. However, in today's mobile-cloud environment, the enterprise perimeter has dissolved and business information is available to users on a variety of endpoints, apps, services, networks, locations. In this dynamic access environment, organizations need a different approach to security that is able to:

- Establish user trust using multiple factor authentication
- Correlate user trust with other factors such as endpoint, app, network, and more
- Apply adaptive, risk-based policies that match the user's environment

MobileIron Access provides this new security framework so organizations can confidently adopt mobile-cloud technologies to drive user productivity while reducing the risk of data breaches.

With capabilities such as multi-factor authentication (MFA), seamless single sign-on (SSO), and an advanced policy engine, organizations have the right security platform to meet the growing information security and compliance requirements.



Key benefits
MobileIron Access provides standards-based security for the mobile-cloud world so that business information is only available to verified users on authorized endpoints, apps, and cloud services.

Simple
With capabilities such as one-touch enrollment for multi-factor authentication and passwordless sign-on for mobile apps, Access provides users with the best possible user experience.

Smart
Access enforces adaptive, risk-based policies that account for the type of endpoint, app, network, user location, and more. Security matches the risk on the user's environment and reduces the threat of data breaches.

MobileIron

About MobileIron
MobileIron provides the secure foundation for modern work to companies of all sizes around the world. For additional information about MobileIron Access, visit www.mobileiron.com/Access or contact your MobileIron sales representative.

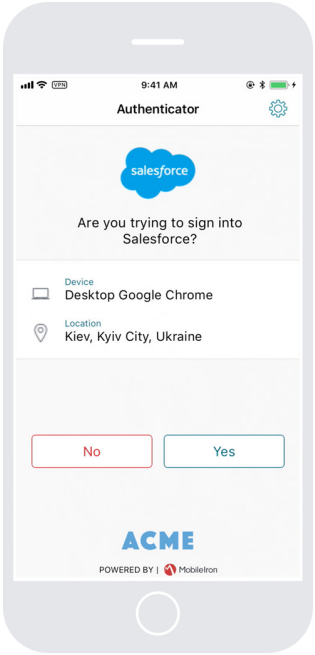
1 Verizon, 2018 Data Breach Investigations Report

Capabilities

Multi-factor authentication with MobileIron Authenticator

Simple MFA app that replaces cumbersome and expensive hard tokens with a secure mobile MFA solution that's easy to use and cost-efficient.

- **One-touch setup**
  Setup and configuration is automated through the MobileIron platform. The user only has to launch the Authenticator app for one-touch activation. Once activation is complete, the user is ready to verify login attempts on their configured smartphone.
- **Push notifications**
  MobileIron Authenticator sends instant notifications to users on their mobile phones, which gives them a quick and easy method to start approving login attempts.
- **Adaptive authentication**
  MobileIron Authenticator provides intelligent authentication flows that adapt based on a variety of feeds including endpoint posture, app, network, and user location.



Native sign-on experience for modern endpoints

Provide a native mobile sign-on experience that users are most familiar with. With a native mobile SSO experience users securely connect to business services via native mobile apps without having to first authenticate via a different SSO app or portal.

- **Seamless single sign-on**
  Adaptive policies provide users with passwordless authentication when users connect via authorized apps and endpoints.
- **Intelligent sign-on**
  SSO that in context-aware and prevents users from connecting to business services from unmanaged apps or unauthorized services.

Trust engine for smart policies

Make smart access control decisions that go beyond user identity and include device, app, service, user location, network and so on.

- **Intuitive remediation workflows**
  Customizable and easy-to-follow steps that allow users to self-remediate when using non-compliant devices, saving them time and the trouble of opening help desk tickets.
- **Standards-based security**
  Secure any cloud service using a standards-based approach to scale your security framework to meet growing business needs.