Extend Identity Management to Mobile Devices

Due to popular trends like Bring Your Own Device, or BYOD, IT organizations across the world are under pressure to allow those personal devices to access sensitive corporate assets to increase workforce productivity. The potential benefit is significant, with some studies estimating enabling smartphones can add up to 2 more hours of productivity per day. But this also increases the number of devices IT is expected to support and can introduce security concerns into the workplace.

Extend IdentityIQ centralized identity management to include mobile devices

Many organizations have already taken the step of implementing a Mobile Device Management (MDM) solution to secure and manage personal devices that access corporate resources. But these mobile devices can’t be managed in a silo – they need to be integrated into the organization’s broader identity management strategy. SailPoint IdentityIQ MDM Integration Modules provide an out-of-box integration with the most popular Mobile Device Management solutions to give organizations better visibility and control, and its pre-built connectivity options make it easy to deploy for faster return on your investment.

The IdentityIQ MDM Integration Modules deliver centralized visibility into the devices employees are using to access corporate resources, and the applications that are on them. This information is critical to maintaining the security of your corporate data.

The MDM Integration modules can also increase control of personal mobile devices and the policies that govern them. It integrates mobile devices into existing IdentityIQ audit control processes, including automated access certifications, and provides an automated process for reviewing and documenting changes to mobile policies.

Finally, the MDM Integration modules can reduce mobile device administration costs by automating support processes, like provisioning/deprovisioning of the device.

IdentityIQ MDM Integration modules increase the visibility and control of mobile devices while decreasing administration costs through support process automation.
Integrated Capabilities with IdentityIQ and MDM solutions

Incorporates mobile device and app data with corporate identity

Without the visibility to what mobile devices are on your corporate networks and what applications are on those devices, it’s impossible to have a complete picture of user access. The Integration Modules import this information from the MDM solution to maintain a centralized corporate identity source.

Provides unlock for mobile devices and/or containers

In order to access corporate resources, employees are often required to use a PIN or password on their device or corporate container. As with any password, many times it’s forgotten. With the MDM Integration Module, the help desk can use IdentityIQ to unlock mobile devices as well, eliminating the need for MDM access for this group and getting the user back online faster.

Enables partial or full wipe of mobile devices

Personal mobile devices are a potential source of leaked data when an employee leaves an organization. With the MDM Integration Modules, IdentityIQ can automatically trigger a full or partial wipe of the mobile device as part of terminating a user’s access, protecting valuable corporate resources.

Automates Compliance Controls

A critical part of identity and access management is ensuring the right policy is applied to the right user. With the integration modules, this control can be extended to mobile devices to avoid audit gaps. It also incorporates mobile devices and policies into regular access reviews as part of the organizations overall governance program.

Delivers a self-service mobile device registration portal

With certain MDMs, IdentityIQ can also provide self-service registration for new employee devices. Registering the device will trigger the MDM to create a new account and then automatically send the user instructions on how to complete the registration, simplifying the mobile device set up process.

About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of the world’s largest organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company’s innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information about SailPoint, please visit www.sailpoint.com.

© 2014 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo and all techniques are trademarks or registered trademarks of SailPoint Technologies, Inc. in the U.S. and/or other countries. All other products or services are trademarks of their respective companies. 0614-4255