

NetIQ's Mobile IAM Solutions

In virtually every organization, employees are walking around with powerful mobile devices in their pockets, and so are their partners and customers. Now, all sorts of businesses—from large to small—are investing in mobile, not only for their workforce in field and sales services but also as an important way to interact with their customers. Whether the objective is to move business processes faster and make them easier or to raise the level of customer touch, organizations understand that mobile app development is strategically smart. In fact, almost 8 out of 10 enterprises¹ have made elevating mobile interaction a critical or high priority.

¹ Forrester—Latest IT Trends for Secure Mobile Collaboration

Table of Contents

page

The Challenge of Mobile Apps.....	1
Mobile-Enable Your Whole Environment—Avoid Piecemeal	3
Four Tips for Updating Your IAM for Mobile	4
Does Your Solution Match Your Problem?	5
NetIQ Mobile IAM Is Powerful.....	6
IAM-Enable Your Mobile Apps	8
Need Quick Wins?	8
Next Steps	10

The Challenge of Mobile Apps

The challenge is that usually mobile apps don't provide value as a standalone application. They need to fetch data from services that are somewhere else, either from the cloud or internal backend systems in which they are dependent. So while the intent of these new mobile initiatives is to interact with and enable workforce groups and partners, the complexity to connecting to back-end engines and data repositories hasn't gone away.

This means that your mobile app team building these applications face the same complexities of securely accessing these various systems as the web app teams of yesteryear. In fact, today's mobile app teams face additional challenges such as accessing external cloud-based systems that aren't integrated with existing identity and access management systems. Whatever the configuration, the same common challenges exist: keeping credentials and, ultimately, access to the private information available to those credentials secure, so that mobile convenience doesn't become a liability to the business.



NetIQ makes it easier for development teams to secure access across the services that support them.

Fig. 1

Regardless of the mobile application strategy the organization is pursuing, NetIQ® makes it easier for development teams to secure access across the services that support them. NetIQ also gives organizations options to quickly leverage past investments that accelerate their mobile expansion. This white paper reviews the authentication complexities that mobile app developers face as they secure integration points. It also suggests how corporations can limit the added risk that these applications impose.

The path to becoming a “mobile first” enterprise is unclear at best and perhaps confusing. This lack of clarity matters because at some point, the pitfalls of a tactical approach of allowing disjointed pockets of mobile development to occur will become clear.

Mobile-Enable Your Whole Environment—Avoid Piecemeal

While enterprises know that mobility presents an unprecedented opportunity to transform their business, the best way to get there is still elusive. The path to becoming a “mobile first” enterprise is unclear at best and perhaps confusing. This lack of clarity matters because at some point, the pitfalls of a tactical approach of allowing disjointed pockets of mobile development to occur will become clear. The consequence is more impactful than an inconsistent look and feel across the corporation’s mix of applications. A bottoms-up approach to authentication to backend systems introduces inconsistent and uneven security. Extending user access to mobile users already increases the organization’s exposure due to unauthorized use and stolen devices, and abandoning proven identity and access infrastructure broadens that exposure further.

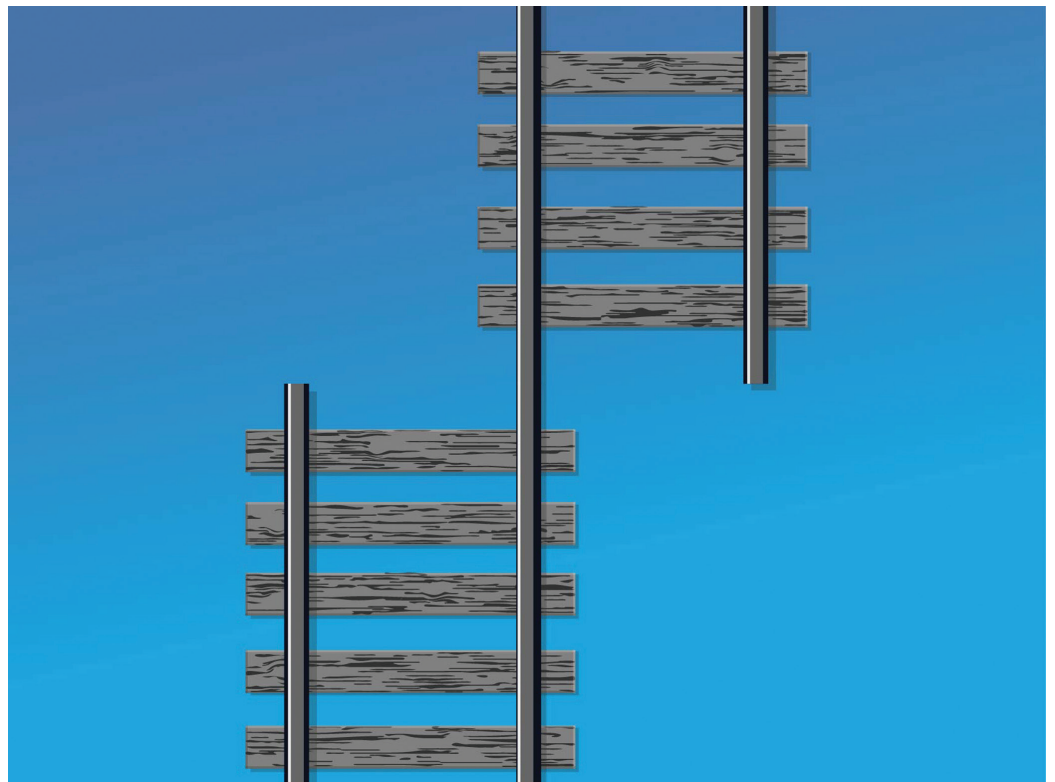


Fig. 2

The reality is that the same business drivers that prompted the need to establish an identity and access management (IAM) infrastructure years ago still apply and have expanded even more. Not only is there a wider range of devices and access situations that need to be secured, SaaS vendors often provide the required services to support these mobile apps and host them in the cloud. So whether your top IAM business drivers have been to secure your intranet, improve value chain efficiency, or personalize interaction with customers, leveraging what you have already invested in to secure your mobile apps only makes sense. Here's a list of IAM recommendations that will keep it central.

Whether your top IAM business drivers have been to secure your intranet, improve value chain efficiency, or personalize interaction with customers, leveraging what you have already invested in to secure your mobile apps only makes sense.

Four Tips for Updating Your IAM for Mobile

1. Don't let your organization allow mobile app projects to start in silos or as one-off projects. Instead, balance the need for quick wins with an eye toward maintaining a single set of IAM-controlled services to be leveraged by all.
2. Since mobile apps introduce a higher level of risk to your business, you will need to update your security policies to account for them. As you assess your tolerance for risk, balanced with internal objectives, keep in mind that convenience is paramount to app usage. As you do this, balance convenience against potential financial loss and even customer trust. There is a good chance that a number of your policies haven't been updated to account for SaaS services, so now is a good time to include them because mobile apps will commonly consume them.
3. Assess current manual identity processes to see if any need to be updated or automated for mobile usage, and ensure that manual processes are solid and accurate. Otherwise, simply automating failing processes will result in a failed automated process.
4. Don't bite off more than you can chew. As long as you have a good idea of how mobile fits within your IAM infrastructure, use the business case of each mobile app project to extend it as necessary. Quick wins are often essential to ensure development success.

Organizations use mobile application management (MAM) solutions to apply policy controls to and provision mobile applications. This level of control is available primarily for internally developed apps.

Does Your Solution Match Your Problem?

Based on the amount of confusion found in many organizations, it's worth taking a moment to clarify the particulars across today's mobile management platforms and frameworks.

Mobile device management (MDM) consists of configuration and policy management tools. MDM solutions are device-specific to the mobile operating system's application programming interfaces (APIs), such as Apple and Google, to control and manage mobile devices. The typical hardware and application inventory found in MDM solutions include:

- *Enforced security policies such as allowed passwords, device encryption, WiFi settings, detection of jailbroken devices, and so forth.*
- *Execution of actions such as partial or remote wipe, remote lock, device location mapping, and passcode clearing*
- *Access to self-service portals to enable users to protect personal and enterprise data*

Organizations use mobile application management (MAM) solutions to apply policy controls to and provision mobile applications. This level of control is available primarily for internally developed apps. MAM solutions usually have an enterprise app store that enables application control and delivery to mobile devices. MAM solutions are commonly used to provide control over mobile applications by incorporating a software development kit (SDK), but it's also possible by incorporating a wrapper. The wrapper approach also allows the management of commercial apps found in Google Play and the Apple App Store, but the SDK allows developers to integrate additional security and configuration features.

Enterprise mobile management (EMM) is assumed to include MDM and MAM capabilities, plus a container that enables corporate data to be secured. With that background, it's important to point out that although these technologies do a good job of securing mobile devices and their applications, they don't address the need for those applications to access and authenticate to the systems they rely on. Take, for example, a mobile CRM application that requires access to information about customer care and order history, internal relationships mapping across the businesses, and product configuration. Or consider a mobile ERP app that is dependent on authenticated access to its distributed datastores for various BI information. This is simply out of scope for today's EMM technology.

NetIQ Mobile IAM Is Powerful

Because MDM and MAM technologies don't secure services beyond the device itself, perhaps some might think that the smartest approach is to have each mobile app team bridge their mobile IAM gap on their own. At first blush, this piecemeal tact might seem like the most practical way to deliver mobile capability to your organization; however, the complexity of mobile integration and security aren't much different from traditional platforms. To do it right requires an environment-wide solution. In fact, Gartner has observed that integration is often the largest portion of a mobile app project. And considering where the focus is for most mobile development teams, it's no surprise that they typically underestimate the time and resources it takes to securely bring it all together².

Gartner notes that even today, mobile apps continue to trickle out of IT at a surprisingly slow rate and that integration complexity continues to be one of the dominant causes. Gartner even observed a surprising number of enterprise mobility projects that still haven't delivered any of their targeted mobile apps². A fundamental flaw observed from this trend is the common practice of mobile projects originating as islands of initiatives, lacking any type of common practice of implementation and the inability to leverage existing infrastructure. There is little planning around solving the difficulties of adhering to security practices established over the years to protect the organization from intruders, all of which takes time to sort out.

Mobile app teams shouldn't waste time solving IAM-related problems. The vast majority of these mobile team members aren't security experts, so such challenges become time sinks that generally result in higher risks to the business.

When teams choose to take on access control themselves, they are (or should be) forced to deal with proper credential and token security, as well as federation. They have the overhead of figuring out what to do when credentials aren't current or when users forget their password. Is this really the best use of your mobile team's time?

Mobile app convenience starts with single sign-on (SSO), meaning that once users have authenticated into the app, they're not bothered anymore with authentication requests. It just works. The users should never be aware of all the moving parts in the background that make it work. NetIQ has a rich set of SSO technologies that span the entire spectrum of systems that users access.

Considering where the focus is for most mobile development teams, it's no surprise that they typically underestimate the time and resources it takes to securely bring it all together.

² Gartner press release June 16, 2015

NetIQ's risk-based authentication allows you to evaluate a set of contextual factors related to an access request. You can then use those factors to determine the type of authentication experience that meets your business needs.

If two-factor authentication is required to meet security requirements, NetIQ's mobile capable IAM solutions provide an array of second-factor technologies that span smart cards, OTP, biometrics, tokens, and more. IT administrators have the freedom to choose from a wide range of strong-authentication devices, or leverage what they already have.

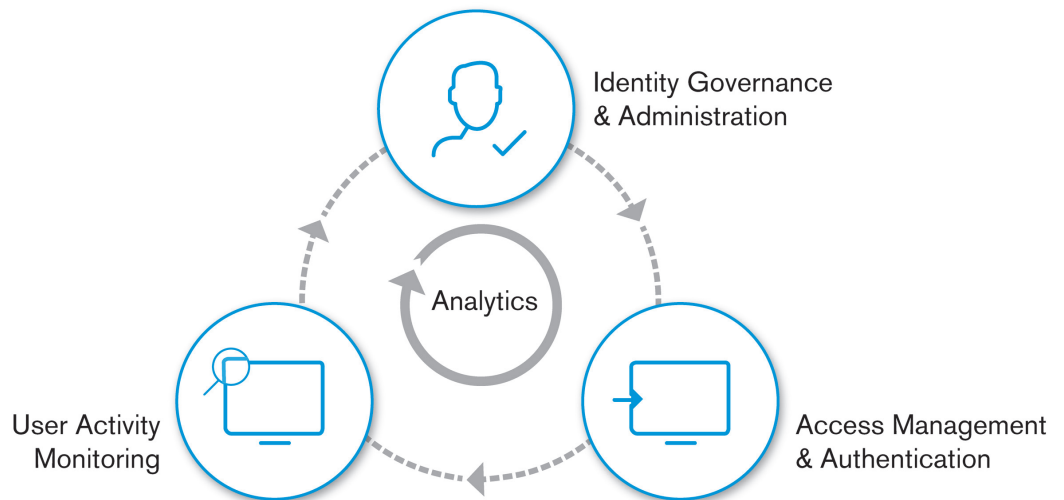


Fig. 3

Today, context is increasingly becoming an important factor in determining a user's authentication requirements, even more so in situations involving mobile users.

Because of the growing threat of being targeted by criminals and the consequences when they are successful, it is essential that you decide on the level of risk introduced from mobile users that is acceptable for your business. NetIQ's risk-based authentication allows you to evaluate a set of contextual factors related to an access request. You can then use those factors to determine the type of authentication experience that meets your business needs. When a user requests access to private information using a familiar context, there is a good probability that the user is indeed who he or she claims to be, and the authentication can be adapted accordingly. Access requests that fall outside of a context defined to be safe can be adjusted accordingly. Combined with NetIQ's advanced authentication, mobile development teams

are able to provide a user experience that is far more convenient and secure than they could create on their own. And because NetIQ supports centralized authentication policies, backdoors created by inconsistent policies are avoided.

Mobile access life cycle management includes being able to remove user access in a timely manner so they no longer have access to corporate applications (many of which are likely in the cloud). NetIQ's automated provisioning and account management is an important component of enabling and securing mobile access, whether the user is an employee, partner, or customer.

NetIQ's automated provisioning and account management is an important component of enabling and securing mobile access, whether the user is an employee, partner, or customer.

IAM-Enable Your Mobile Apps

Developers consuming NetIQ's mobile SDK have two options: OAuth/OpenID Connect and NetIQ's native iOS SDK. For teams that have a cross-platform view of application development, NetIQ's tested OpenID Connect SDK is likely the best fit. It accommodates cross-platform coding while supporting the full-stack of the OAuth 2.0 protocol. It also gives you full integration with NetIQ's role-based access control and advanced authentication framework.

For teams developing native iOS applications specifically, they will find it faster and much easier to use Access Manager's iOS SDK. This SDK obscures the complexity of proper credential and token management and protection, raising the level of security for the whole application. Of course, in addition to any direct authentication required by the application, the SDK provides direct access to all of Access Manager's SSO, advanced authentication, and authorization policies. And soon, Android developers will have the same ease.

Need Quick Wins?

Even with simplified identity and access management, mobile projects aren't completing fast enough. In fact, Gartner predicts that by the end of 2017, demand for mobile apps will outstrip development capacity by more than five to one.

Organizations implementing hybrid applications for their mobile users have the option of simply dropping them into MobileAccess and enabling them for SSO to other systems, or using OpenID Connect SDK.

Speaking ahead of the Gartner Application Architecture, Development & Integration Summit, Gartner principal research analyst Adrian Leow said enterprises find it difficult to develop, deploy, and maintain mobile apps fast enough to meet demand, “resulting in their mobile apps becoming tactical, rather than strategic.” Mr. Leow goes on to say that organizations must find ways to respond³. Much of the demand that Leow refers to is a result of needing to extend web apps to mobile devices, often natively. The challenge for those working away from their desk is that mobile devices still have limited screen real estate and there is rarely a physical keyboard handy. In fact, mobile users are often standing while they work. What might be effortless on a laptop can be much harder on a tablet or smartphone.

The NetIQ MobileAccess App (published for iOS and Android) provides a secure, single-touch launch point for both hybrid and web apps. This means that mobile teams have several options beyond just creating native mobile applications and NetIQ has a solution.

- **Web apps, unmodified**—*MobileAccess is able to create single-touch launch points from an icon to specific functions within the web app, enabling the user to complete a business process on his or her mobile device. Multiple icons (launch points) can be created for each application. Users see the application icons that they have access to and with a single touch they're in. No time-consuming or onerous hoops to jump through, just convenient access.*
- **Mobile friendly web apps**—*Applications that have been updated to render pages to fit on the mobile form factor can be instantly IAM-enabled, providing SSO as well as enforcing all the appropriate policies regarding authentication and authorizations. The users experience the same level of convenient access on the device.*
- **Hybrid Apps**—*Development teams covering their portable platform requirements using hybrid app technology can IAM-enable them by simply adding them to MobileAccess. Once added, MobileAccess will secure its token and integrate it into Access Manager™.*

As shown, any organization with a native iOS or Android strategy has tactical options today to quickly optimize their existing web apps, solving their near-term mobile requirements. Organizations implementing hybrid applications for their mobile users have the option of simply dropping them into MobileAccess and enabling them for SSO to other systems, or using OpenID Connect SDK. Either way, organizations have multiple options to quickly IAM-enable their mobile applications. When they do so, they gain the value of Access Manager today:

- *Mobile users gain the speed and convenience of single sign-on.*
- *Existing, as well as new access policies in Access Manager are enforced.*

³ Gartner press release June 16, 2015

- Administration for device administration can be configured to include self-service device registration capabilities to use when a device is lost or stolen, lowering help desk administration costs.
- Using Access Manager, organizations can configure adaptive authentication levels to match the authentication type to match the level of risk right for their business.
- Organizations have access to NetIQ's Advanced Authentication Framework to meet any two-factor or multi-factor authentication need.

Although NetIQ is known by the IT administration and infrastructure teams for their powerful IAM solutions, it doesn't occur to them how easy it is to port that capability to mobile devices. The environments that currently have Access Manager deployed, it is a trivial to create appmarks that provide one icon touch access to smart phone users. All you need to extend Access Manager's application to mobile users is to have them download the MobileAccess application and register it into your environment. From there, the hardest part is to decide what icon you want your mobile users to see for each application.

Next Steps

Each business or organization has their own specific needs around mobility, and that's why NetIQ has multiple options. In most cases, organizations that allow a bottom's up approach to mobility will pay the price of rework, less secure products, and often less powerful products. Using Access Manager to IAM-enable mobile environments in the same way that it has done for years on desktop and web environments makes sense. It allows organizations to extend what they have, rather than rebuild. It reduces development time, increases security, and delivers sought-after convenience from users. It gives IT organizations the ability to focus their mobile teams on what they do best while managing their risks.

To learn more about Micro Focus mobile single sign on and access control, go to:
www.netiq.com/accessmanager

www.netiq.com



Worldwide Headquarters

515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

For a complete list of our offices

in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit: www.netiq.com/contacts