onelogin

WHITEPAPER

# NAPPS: A Game-Changer for Mobile Single Sign-On (SSO)

## INTRODUCTION

### The proliferation of mobile applications, including mobile apps custom to an organization, makes the need for an SSO solution critical.

Some interesting data points to illustrate the challenges facing mobile users and organizations:

- **SHADOW IT** The average enterprise has over 500 cloud applications in use, however less than 15% are enterprise ready
- **MOBILE ACCESS** Nearly half of all cloud app activities occur on mobile devices

Mobile applications are an increasingly important application delivery channel however most don't support SAML (Security Assertion Markup Language) for SSO, and tiny keyboards are incompatible with passwords. For those mobile apps that do support SAML, the user's authentication experience is poor and security is weakened since user sessions are not frequently revalidated. Forcing users to constantly enter passwords degrades usability and hinders their productivity.

The industry is moving to solve this problem with the introduction of NAPPS or Native Applications, a standard protocol to provide SSO for users on mobile devices through a "token agent" which will enable native mobile applications to authenticate users more easily. As is the case with SAML and SCIM (System for Cross-domain Identity Management) for web applications, the promotion of NAPPS to mobile application developers will be imperative in order to provide a more secure and integrated user experience. With a mobile identity and authentication infrastructure tied to native mobile apps,  both the user experience as well as the security and compliance challenges are addressed.

## STANDARDS ARE A TIDE THAT LIFTS ALL BOATS

Until the SAML standard came together in 2003, single sign-on projects were expensive, complex and locked the customer to a particular vendor's solution forever. At first, the adoption of SAML was slow, but as the migration to the cloud has accelerated, so has the adoption of SAML. OneLogin's catalog of 4,000+ applications now has more than 600 that support SAML and the trend is accelerating. Figure 1 shows the growth in OneLogin's SAML connectors since 2010.

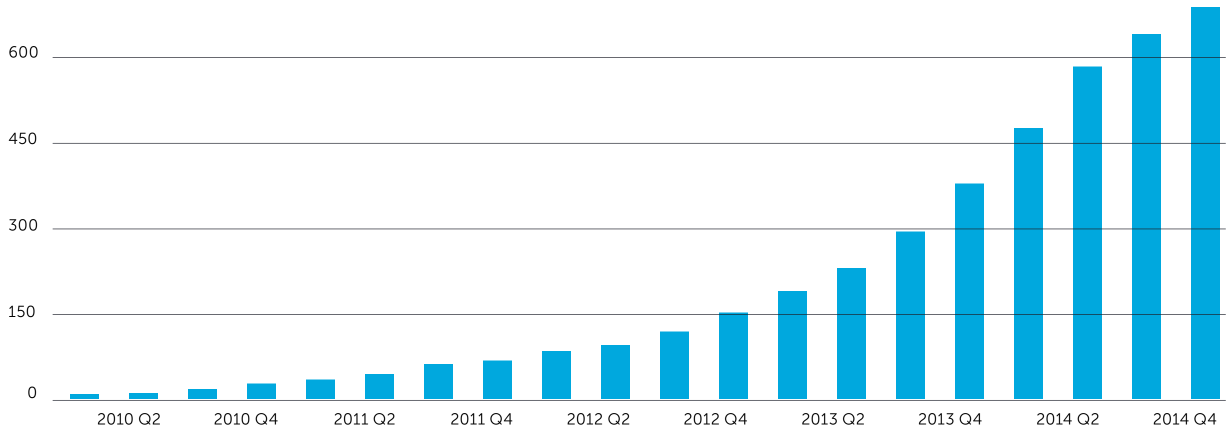


FIGURE 1. GROWTH OF SAML-ENABLED APPS IN ONELOGIN'S CATALOG

The state of user provisioning is similar to where SAML was in 2010. Most applications have their own proprietary user management API, but new cloud startups have jumped on the emerging SCIM standard that allows them to integrate to any identity provider who supports the standard.

Time has proven over and over again that standards are good for industries, and drive innovation. Standards reduce vendor lock-in, which gives customers choice and enables ecosystems to flourish and further accelerate the growth of an industry. For example, the relational database industry exploded once SQL became a standard, and all the world's information is now linked together online because of HTML. Giant industries have arisen around both standards to the benefit of vendors and customers alike.

## NAPPS AND MDM

The mobile ecosystem is dominated by MDM (Mobile Device Management) vendors like VMware/AirWatch, Citrix/Zenprise, MobileIron, and Good Technologies. Current MDM solutions solve the problem of managing end-users' devices, and pushing and removing applications to and from those devices. Similarly, MAM (Mobile Application Management) solutions are coming online to help differentiate consumer and enterprise apps.

However, both MDM and MAM solutions don't address the security problem of managing user identity and authentication. With MDM and MAM, users still have to manually sign into each individual application using passwords. NAPPS addresses this challenge. In other words, MDM, MAM and NAPPS are complementary, and the industry is viewing this collectively as Enterprise Mobility Management (EMM).

| MOBILE DOMAIN | CAPABILITIES |
|---|---|
| **MOBILE IDENTITY MANAGEMENT** | NAPPS is an emerging authentication standard focused on providing SSO for native mobile applications, either supplementing or replacing the traditional web browser channel often serviced by SAML. |
| **MAM** | Segment focused on application management, providing a higher level of control over applications, and includes the provisioning, delivery, security, and retirement of mobile apps, monitoring of application performance and usage, containerizing or wrapping corporate apps from personal apps, and remotely wiping data from managed applications.<br>With these capabilities, IT can manage the entire application life cycle and potentially make the applications available to employees through a private enterprise app store. |
| **MDM** | Segment focused on controlling and protecting the data and configuration settings for all mobile devices in the network, and includes capabilities such as provisioning enterprise settings such as Wi-Fi and VPN to provide end-users with secure access to corporate services e.g. email. If a device should fall out of compliance, IT can define remediation actions that will either notify the user of policy violations or selectively wipe corporate information without touching any personal data. |

FIGURE 2. COMPONENTS OF ENTERPRISE MOBILITY MANAGEMENT

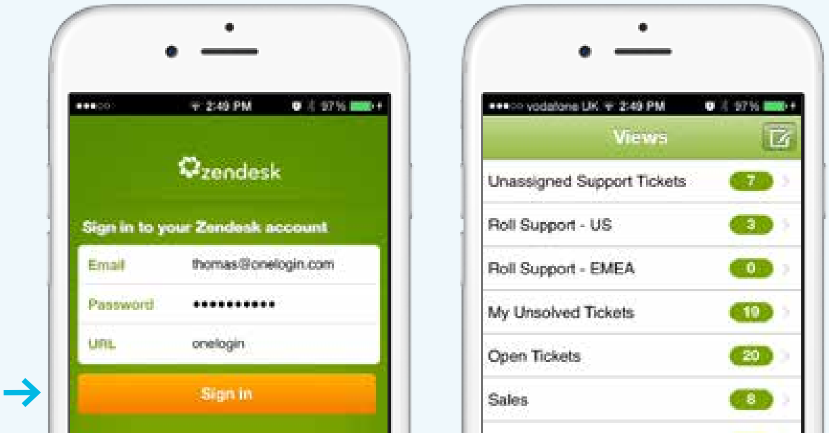
## THE CURRENT STATE OF IDENTITY & SSO ON MOBILE

Mobile devices are rapidly outnumbering desktops and notebooks in the workforce. More cloud vendors now have mobile versions of their applications optimized to work in these environments. Many vendors support SAML in their web application and some of them even support SAML in their mobile application. But a large number of vendors do neither and still require users to sign in using a password. These vendors fall into three different groups.

| SSO SUPPORT | SUPPORT SAML IN WEB APP | SUPPORT SAML IN MOBILE APP |
|---|---|---|
| No SSO | NO | NO |
| Partial SSO | YES | NO |
| Full SSO | YES | YES |

FIGURE 3. DEGREES OF SAML SUPPORT ACROSS VENDORS

To better illustrate what end-users have to deal with in mobile applications, let's look at a couple of real world examples. Figure 4 shows how users sign into Zendesk's mobile application.



Sign in to your Zendesk account

Email thomas@onelogin.com
Password ••••••••••
URL onelogin

| | |
|---|---|
| Unassigned Support Tickets | 7 |
| Roll Support - US | 3 |
| Roll Support - EMEA | 0 |
| My Unsolved Tickets | 19 |
| Open Tickets | 20 |
| Sales | 8 |

FIGURE 4. MANUAL AUTHENTICATION IN ZENDESK

Although Zendesk's web interface supports SAML, users still have to sign into the mobile app using a password. This  provides an inconsistent user experience and adds administrative complexity because passwords have to be synchronized from the corporate directory or must be managed manually.

Figure 5 shows how Box has made SAML work in their mobile application.

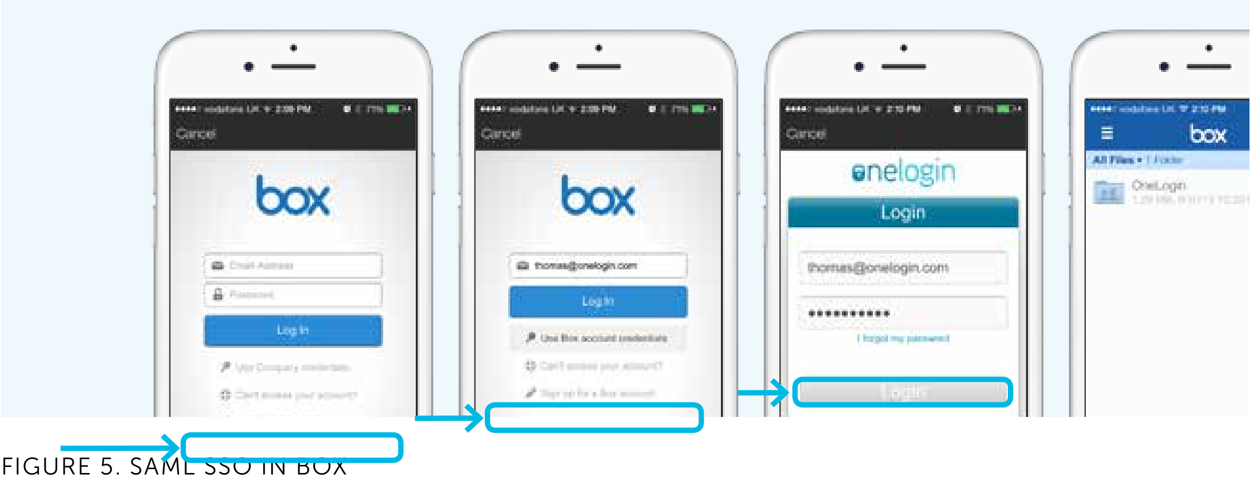


FIGURE 5. SAML SSO IN BOX

First, the user chooses to sign in with their company credentials and the enters their email address. This allows Box to discover the identity provider and then redirect to the identity provider's mobile login page (in this case, OneLogin), which is now embedded in a browser object inside the native Box app. The user then enters their company credentials, gets authenticated and is signed into Box's web app using SAML. Box's web app now exchanges an API token with the native app, and the user is finally signed in.

This approach is an improvement over Zendesk's approach because the user can sign-in with their corporate identity and doesn't have to remember a separate password. But it has a few drawbacks. The sign-in process is overly complicated and has to be repeated for every app on the phone that supports SAML. There is no way to easily federate mobile apps using SAML.

The second problem is that because of the complicated sign-in process, the native app needs to keep the session valid for a very long time as to not inconvenience the user with signing in too often. Long-lasting sessions increase exposure.

The industry is quickly recognizing that the right security posture to minimize risk is to transition away from passwords to a federated sign-in process.

## HOW NAPPS WORKS

The NAPPS specification is part of the OpenID Foundation and is defined by the Native

Applications Working Group. NAPPS was specifically designed to handle single sign-on for native, mobile applications and is based on the OpenID Connect and OAuth 2.0 standards.

NAPPS addresses the main issues illustrated in the Box example: user experience and security exposure. It provides a seamless sign-in experience where an identity provider can federate access across numerous applications, and sessions can be validated repeatedly without degrading the user experience.

Figure 6 shows the various components involved in NAPPS single sign-on.

FIGURE 6. NAPPS PROTOCOL FLOW

On the left you have a mobile phone with an identity provider's agent and a native mobile app, and on the right you have their respective cloud-based backends such as an Identity Provider (IdP).

The end-user only authenticates with the identity provider on the mobile device and it is up to the identity provider how and when a user authenticates. Mobile applications invoke the identity provider when they don't know who the user is or when a previous session has expired.

The identity provider app will obtain an OAuth token from its backend and use this to fetch secondary tokens that can be used to sign the user into the mobile application via OpenID Connect. When the mobile application receives a secondary token, it will validate it against its own backend, which in turn will validate it against the identity provider.

The NAPPS steps are a bit more involved than with SAML, but they ensure that a user will be signed out of the mobile applications when the secondary token is no longer valid.

## DEPROVISIONING DEVICES

Another benefit of NAPPS is that the identity provider issues one primary OAuth token per user per device. So if a user accesses a NAPPS-enabled app on both their iPad and iPhone, it will be done with different OAuth tokens. In the event that a user loses their iPhone, the IT department can invalidate that device and its tokens, while allowing the user continued access to the app via the iPad.

## COEXISTENCE WITH PASSWORD-BASED LOGIN

Supporting NAPPS can be done without affecting the experience for users who sign in with username and password. When the mobile application renders its login page it can easily detect whether a NAPPS-compliant identity provider agent is installed on the phone and display a sign-in button that says “Sign in with Acme, Inc. credentials” or similar. If a NAPPS identity provider agent is not present, the mobile application can just render username and password fields as usual.

## HOW TO GET STARTED WITH NAPPS

As part of OneLogin's commitment to standards, we have developed NAPPS toolkits for iOS, Android and JavaScript, which can be used today. The toolkits come with a mock token agent that can be used to make testing easier.

**OneLogin NAPPS Server documentation**
http://resources.onelogin.com/d/8h1gq/NAPPS-Server-Documentation

**OneLogin NAPPS SKD for iOS documentation**
http://resources.onelogin.com/d/v73rL/OneLogin-NAPPs-SDK-iOS

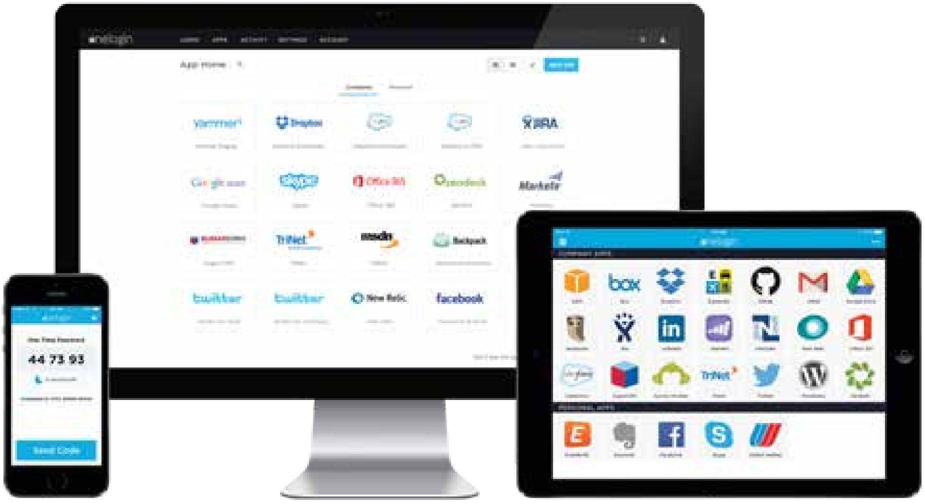
**OneLogin NAPPS SDK for Android documentation**
http://resources.onelogin.com/d/d58pQ/OneLogin-NAPPs-SDK-Android

Cancel
box
Email Address
Log In
Use Box account credentials
Can't access your account?
Sign up for a Box account
elogin

# ABOUT ONELOGIN

OneLogin is the innovator in enterprise identity management and provides the industry's fastest, easiest and most secure solution for managing internal and external users across all devices and applications.

The only Challenger in Gartner's IDaaS MQ, considered a "Major Player" in IAM by IDC, and Ranked #1 in Network World Magazine's review of SSO tools, OneLogin's cloud identity management platform provides secure single sign-on, multi-factor authentication, integration with common directory infrastructures such as Active Directory and LDAP, user provisioning and more. OneLogin is SAML-enabled and pre-integrated with thousands of applications commonly used by today's enterprises, including Microsoft Office 365, Asure Software, BMC Remedyforce, Coupa, Box, Clarizen, DocuSign, Dropbox, Egnyte, EMC Syncplicity, EchoSign, Google Apps, Jive, Innotas, LotusLive, NetSuite, Oracle CRM On-Demand, Parature, Salesforce.com, SuccessFactors, WebEx, Workday, Yammer, ServiceNow, Zscaler and Zendesk. OneLogin, Inc. is backed by CRV and The Social+Capital Partnership.



onelogin

150 Spear Street, Suite 1400 San Francisco, CA 94105 ☎ 877 979 0411 onelogin onelogin.com