



**Deliver Secure, User-Friendly
Access to Mobile Business Apps**



The Best-Run Businesses Run SAP®

Promote app security for enterprise safety

Promote app security for enterprise safety

Whether your enterprise is deploying third-party mobile apps or developing them internally, they must be locked down tight. The SAP® Mobile App Protection solution by Mocana helps you to apply advanced authentication protocols while simplifying the logon process and providing an intuitive user experience. As a result, you can **access business information quickly and securely.**

Today, new mobile app security methods are removing dependence on hardware. “App wrapping” separates security from the development process and provides precise usage and security policies in mobile apps.

By “wrapping” security into each app, SAP Mobile App Protection helps you meet security needs for deploying internal or third-party software. Available either on premise or in the cloud, the solution helps you to apply rigorous security protocols to both native and Web-based mobile apps. Meanwhile, one-touch

access to enterprise apps improves the user experience and accelerates the speed at which you can do business.

Companies with strict security requirements and those in highly regulated industries – such as financial services, healthcare, retail, and government – are realizing that app wrapping adds flexibility in bring-your-own-device (BYOD) environments. App wrapping can also speed the development process for business-to-business or business-to-employee apps.



Automate security to meet compliance and audit requirements

Automate security to meet compliance and audit requirements

Accelerate your mobile initiatives

Secure mobile communications and prevent data loss

Improve user experience through streamlined connectivity

SAP Mobile App Protection helps you accelerate mobile initiatives by automating app security. You can apply consistent, replicable controls across all your enterprise apps without writing any code, and you can secure business and confidential data on managed or unmanaged corporate devices.

You can also secure Web-based apps or apps on devices that you don't control or are not on your network – including those of partners, contractors, or employees. Just choose an app or group of apps, select the related

security policies, and add functions for encryption, data protection, authentication, and virtual private networks (VPNs).

SAP Mobile App Protection also helps you fulfill compliance and audit requirements, such as those for the Health Insurance Portability and Accountability Act (HIPAA), regulations for the payment card industry (PCI), and other industry rules. You can readily integrate security policies that suit your organization and industry into an existing IT environment.



Apply meaningful security policies across all your enterprise apps – from partners, contractors, or employees.



Automate security to meet compliance and audit requirements

Accelerate your mobile initiatives

Secure mobile communications and prevent data loss

Improve user experience through streamlined connectivity

Accelerate your mobile initiatives

By streamlining the process of making apps more secure, SAP Mobile App Protection helps keep mobile projects on track. By quickly adding security features to both native and Web-based apps, you can reduce the time required for app development and deployment phases by days and weeks.

In addition to app-level encryption, data protection, authentication, and VPN, you can choose from a variety of security policies, including:

- User authentication
- Data loss prevention
- Secure data transfer between wrapped apps
- Data-at-rest encryption with cryptography certified by Federal Information Processing Standard (FIPS) 140-2
- “Jailbreaking” or “rooting” detection
- 256-bit encrypted VPN tunnel for each app
- Contextual usage
- Controls for cut, copy, and paste



Quickly protect valuable corporate app data with your choice of security functions and policies.



Secure mobile communications and prevent data loss

Automate security to meet compliance and audit requirements

Accelerate your mobile initiatives

Secure mobile communications and prevent data loss

Improve user experience through streamlined connectivity

SAP Mobile App Protection empowers you to lock down mobile apps so you can confidently make business activities mobile, knowing you are delivering the highest possible level of security.

By requiring user-authentication passwords or multifactor authentication to access, SAP Mobile App Protection helps ensure that data is quickly made inaccessible when devices are lost or stolen. The application helps prevent unauthorized data leakage by securing cut-copy-paste functionality and funneling data only to authorized e-mail clients for sharing sensitive information.

Smart firewall policies let you block potentially unsecure network traffic from apps to keep your network safe. You can set an expiration

date on an app to create time-limited access. And you can rapidly disable an app to prevent access to it, or even wipe stored data from it if a device is compromised by:

- Jailbreaking – Overriding security settings in Apple-based operating systems
- Rooting – Overriding security settings in Android-based operating systems
- Failed authentication – Too many failed authentication attempts

SAP Mobile App Protection keeps data in motion safe by communicating with an app over an encrypted VPN tunnel for each app. This encryption prevents potential rogue applications and malware from accessing your enterprise network even if the device is compromised.



Improve user experience through streamlined connectivity

Automate security to meet compliance and audit requirements

Accelerate your mobile initiatives

Secure mobile communications and prevent data loss

Improve user experience through streamlined connectivity

Powered by the SAP HANA® platform, SAP Business Suite applications help you connect different parts of the enterprise in real time, analyze complex data to support decision making, and streamline processes.

The ability to offer staff fast mobile access to these applications can boost productivity, accelerate time to market, and drive efficiency improvements. However, multilevel security authorizations and connectivity requirements of mobile apps can slow down processes and put users off.

Paired with the Mocana Atlas platform, SAP Mobile App Protection enables you to provide secure and smooth mobile access to SAP mobile apps including the SAP Fiori® user experience (UX). SAP Fiori UX connects your staff to SAP Business Suite applications and provides a modern user experience – simple, responsive, and personalized.

Using the Mocana Atlas platform and SAP Mobile App Protection, you can secure apps with robust authentication, encryption, and data security protocols. Instead of negotiating numerous authentication screens, users need only sign on once to access the information they need.



Cut out complexity with single-touch access to enterprise software with SAP Mobile App Protection paired with the Mocana Atlas platform.



Make mobile apps safe with an exceptional user experience

Make mobile apps safe with an exceptional user experience

The pressure for mobile business processes comes from all over the enterprise. Executives and other users want the convenience of mobile apps. Enterprise mobility helps organizations like yours respond more quickly to customers, partners, and employees. More organizations are realizing that mobile apps increase productivity, improve efficiency, and speed time to market.

With SAP Mobile App Protection, your business processes can become mobile and safe from misuse, even when devices and apps are used by partners, contractors, and customers. If security concerns have sidelined your mobile app deployments, let the automated security from app wrapping put your project

back on track. The solution adds robust security to business apps in seconds and helps protect your enterprise from risk while providing your users with a high-quality mobile experience.

Users can interact with mobile apps in familiar ways without installing an additional client or separating their business and personal apps. Authentication merely requires a user name and passcode.

Assisted passcode recovery is available. Once authenticated, users can connect to enterprise servers through a VPN tunnel, which is maintained and autoconnected even if a user moves from one network to another.



Objectives

Solution

Benefits

Quick Facts

Summary

The SAP® Mobile App Protection solution by Mocana speeds up mobile initiatives by helping to eliminate security problems that add bottlenecks to the development and deployment of enterprise apps. SAP Mobile App Protection “wraps” data protection and access control features around an app – without any manual changes or coding. Your enterprise can gain robust security for mobile apps in seconds.

Objectives

- Add security to mobile apps without writing code
- Enable bring-your-own-device (BYOD) environments with safe, secure communications
- Speed app deployment and development
- Provide simple and secure mobile access to enterprise applications
- Meet industry compliance and auditing requirements, including Health Insurance Portability and Accountability Act (HIPAA) and regulations for the payment card industry (PCI)

Solution

- Consistent, repeatable security controls
 - Assisted passcode recovery and rapid authentication
 - Secure, user-friendly access to SAP Business Suite applications, using the SAP Fiori® user experience (UX) paired with the Mocana Atlas platform
 - On-premise or cloud-based deployment
-

Benefits

- Secure apps and data across all native and Web-based apps
 - Customized security that aligns with users and business requirements
 - Compliance with industry requirements
 - Decreased liability from exposure to corporate data breaches
 - Improved adoption of enterprise apps
-

Learn more

To find out more, call your SAP representative today or visit us online at www.sap.com/mobile-app-protection.



© 2014 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.



The Best-Run Businesses Run SAP®