

# Fixmo SafeZone

Part of Fixmo's portfolio of Mobile Risk Management Solutions

CRADA  
PREVIEW



## Mobile Risk Management (MRM)

MRM is a holistic approach to identifying, mitigating and managing the risks associated with mobile devices. It focuses on risk mitigation and enablement, helping organizations deploy corporate and personal-liable devices while protecting private data and maintaining compliance.

Mobility deployments introduce unique and complex risks that go beyond the devices themselves. Organizations must take into account the integrity and security of mobile infrastructure, devices and apps as well as the risks associated with end-users, device loss and situational context.

## Manage Your Risks

Fixmo MRM solutions continuously verify the configuration and integrity of mobile devices, protect them from data loss, track regulatory compliance and enable you to prove it. Fixmo helps you manage your risk so you can be confident while enabling the full potential of mobility.

**Verify. Protect. Comply. Prove.**

## Fixmo SafeZone Foundation

### Secure and Contained

Managed "Secure Container" for corporate data in-transit and at-rest

### Reliable and Manageable

IT controlled and managed, does not rely on any external relay or NOC

### Built for User Experience

Full delineation of personal and corporate data and apps

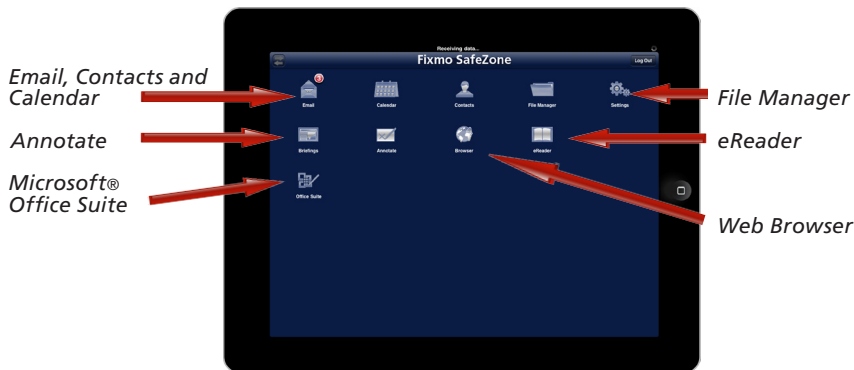
### Extensible and Customizable

Email, PIM, documents, files, web plus deploy your own custom apps

## Data Protection and Security to Enable Corporate and Personal-Liable (BYOD) Mobility Deployments

Fixmo SafeZone™ is a powerful solution to manage the risks associated with allowing employees to access and store private corporate data on personal-liable or corporate-liable smartphones and tablets.

Fixmo SafeZone provides a "Secure Container" solution for iOS and Android® devices that keeps corporate data completely separated from personal data and apps on the device. It provides advanced encryption and access controls for corporate data in-transit and at-rest including email, PIM, documents, files, web content and more while enabling end-users to safely create and edit documents and annotate PDF files. Organizations can also deploy custom applications and 3rd party apps into Fixmo SafeZone using the Fixmo SafeZone SDK. Fixmo SafeZone ensures that private corporate data remains protected and contained on both personal-liable and corporate-liable devices, helping organizations mitigate the risk of data loss and prove regulatory compliance. Fixmo SafeZone provides 256-bit AES encryption for corporate data in-transit and at-rest and has achieved FIPS 140-2 certification.



## Key Benefits of Fixmo SafeZone

Fixmo SafeZone helps organizations protect their private data while empowering employees to get the most out of their device of choice:

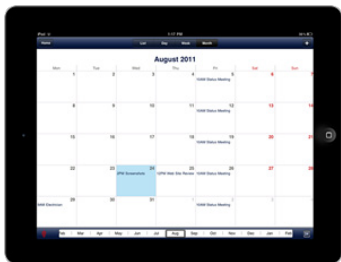
- Complete delineation between corporate and personal data means Enterprises control corporate data and apps while Employees control their personal data and services
- Secure and contained access to email, PIM, and Microsoft Office, Document creation and editing, intranet web content and more
- Deploy custom enterprise applications into Fixmo SafeZone to access enterprise workflow and other custom or legacy apps
- Support for iPhone®, iPad® and Android-based devices
- No-NOC architecture means enterprises maintain control

# Fixmo SafeZone

## Full Suite of Enterprise Apps and Secure Browsing for iOS and Android Devices: In One Secure and Managed Container

Fixmo SafeZone enables employees to use the mobile devices of their choice while ensuring they can access the corporate applications and data they need in a secure, protected and compliant environment. It offers full delineation from personal applications and content, ensuring corporate data and apps are not accessible to the personal apps and services running on the device. Fixmo SafeZone includes a suite of built-in applications and services that enable the seamless extension of your existing corporate applications and data stores to both corporate and personal-liable iOS and Android devices, including:

- **Microsoft Exchange®:** Full support for corporate email and attachments, calendar and contacts.
- **Microsoft Office:** View, edit, create and manage Microsoft Word®, Excel® and PowerPoint® documents
- **Document Annotation:** Annotate PDF documents, Microsoft Office documents, briefings and more
- **Corporate Web Browser:** Securely access intranet-based web content from Fixmo SafeZone browser
- **Custom and 3rd Party Apps:** Fixmo SafeZone SDK enables deployment of custom and 3rd party apps



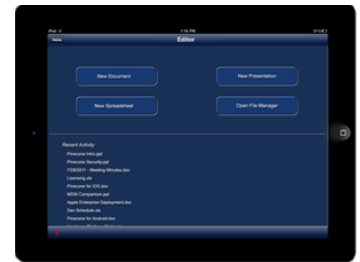
Calendar



Contacts



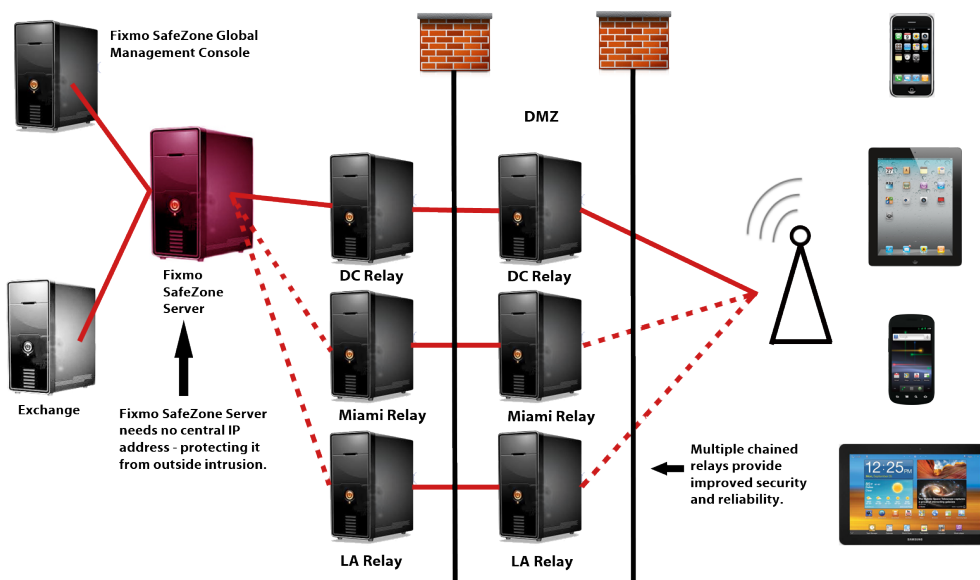
Create and extract ZIP files



Create and edit Microsoft Documents

## System Architecture to meet your Security, Reliability and Manageability Needs

Fixmo SafeZone provides end-to-end secure messaging and access to corporate applications without relying on a centralized NOC. The messaging relay is deployed inside your organization's network, giving you complete control over your data and infrastructure while ensuring there is no need for dual authentication. Any installation can be configured for hot-failover to an alternate computing facility, giving you the control and manageability you need to meet your security and service level requirements.



## Architecture Highlights

- No NOC required
- Messaging relay behind your firewall
- Scales with global deployments
- Support hot-failover and redundancy
- One system for iOS and Android devices
- FIPS 140-2 certified AES encryption

For more information on Fixmo, please contact [sales@fixmo.com](mailto:sales@fixmo.com) or visit us at [www.fixmo.com](http://www.fixmo.com).