

Secure Container Feature Overview



This document provides an overview about the Secure Container Workspace supported by Silverback

MOBILE OS & ACTIVESYNC SUPPORT

| | |
|---|----|
| Android and iOS tablet support | ✓ |
| Android 5.x + support | ✓ |
| Apple iOS 9 + support* | ✓ |
| Microsoft Office365 cloud service | ✓ |
| On Premise support for Microsoft Exchange 2010+ | ✓ |
| Supports caller ID for secure enterprise contacts | ✓* |
| Policy driven support of limited personal / enterprise calendar integration | ✓ |

DEVICE ENROLLMENT

| | |
|---|---|
| Enrollment by end-user (Zero touch for IT) | ✓ |
| QR code automated enrollment process for device provisioning | ✓ |
| IT Policy for simple end user "one step" PIM Active Sync provisioning | ✓ |
| Integrated enrollment templates for group or user based provisioning instructions | ✓ |
| Organization & user based policy engine limiting or enabling feature access | ✓ |

ENTERPRISE DATA SECURITY

| | |
|---|---|
| Complex Passcode policy with lock/unlock, clear & reset passcode | ✓ |
| Supports biometric and multi-factor authentication into secure container | ✓ |
| Secure container AES 256 bit encryption - FIPS140-2 certified encryption | ✓ |
| Secure container wipe removes only enterprise data from the device | ✓ |
| "Time Bomb" secure container feature wipes enterprise data from an offline device | ✓ |

ENTERPRISE DIRECTORY INTEGRATION

| | |
|--|---|
| Support for single-sign on & local authentication | ✓ |
| Supports something you "have" and something you "know" multi-factor authentication | ✓ |

IT SERVICES

| | |
|--|---|
| Supports integrated iOS and Android notifications | ✓ |
| Integrated secure container administrator messaging tool | ✓ |
| Supports Wi-Fi / enterprise Wi-Fi and cellular SIM connectivity | ✓ |
| Policy based GPS location tracking services for secure container | ✓ |
| User self service portal allowing limited access to management console | ✓ |

SECURE CONTAINER ENTERPRISE APPLICATIONS

| | |
|--|---|
| PIM (Email, Calendar, Contacts, Tasks & Notes) | ✓ |
| Secure Camera and Images Gallery (Separated from Device Camera Roll) | ✓ |
| Secure File Manager to save and manage files on device | ✓ |
| Secure Browser for accessing online resources | ✓ |

APPLICATION MANAGEMENT

| | |
|--|---|
| Supports framework integration of native or hybrid iOS or Android applications | ✓ |
| Policy driven application access for enterprise, organization or individual user | ✓ |
| Support for complex application policy based on time of day | ✓ |
| Administrator Web clip feature allowing URL to be added as an application icon | ✓ |

PRODUCT ARCHITECTURE (ON PREMISE)

| | |
|---|---|
| Standard Windows Server based | ✓ |
| IIS based application | ✓ |
| Microsoft SQL Server 2008, 2012 | ✓ |
| Use existing Windows, SQL Backup & Recovery processes | ✓ |
| Use of existing firewalls and proxies | ✓ |
| Architecture supports HA and failover services for service redundancy | ✓ |

REMARKS

Some feature's availability varies dependent on mobile OS and Cloud vs. On Premise Deployment. Contact Matrix42 to get more information for your specific project requirements.

✓* = Apple iOS version 10 required to support integrated CallKit to view incoming call ID for enterprise contacts

** = Productivity applications can be licensed via request to Matrix42 sales department

RECOMMENDED SECURE CONTAINER SERVER CONFIGURATION FOR 1000 DEVICES

Windows 2008 R2 SP1, Windows 2012 R1, IIS 7.5, .NET 4.6.2

Separate, existing Microsoft SQL 2008 R2 /2012 and higher, Standard Edition and higher

Transport / Management Console Server: 64 Bit Quad Core CPU, 2.66 GHz Xeon or faster, 8 GB RAM, 80 GB disk space, 1 GB network interface card

Relay / RelayQue Server: 64 Bit Quad Core CPU, 2.66 GHz Xeon or faster, 8 GB RAM, 60 GB disk space, 1 GB network interface card

Virtual Machine Support: VMware ESXi, Microsoft Hyper V

Customer specific design will be finalized during project implementation phase

DATA LOSS PROTECTION

| | |
|---|---|
| Public App Store application provisioning | ✓ |
| Jailbreak detection (will not install, auto deletion of data if device is jailbroken) | ✓ |
| Copy and paste of data restriction enforced | ✓ |
| Enterprise data cannot be saved outside of container | ✓ |

COMPLIANCE

| | |
|--|---|
| Console supports audit of administrator actions on users | ✓ |
| Disclaimer user policy requires user validation of "terms of use" of enterprise data | ✓ |
| Customizable email disclaimer to assist with regulatory compliance | ✓ |
| GDPR compliance by physical separation of enterprise and personal data | ✓ |

ADMINISTRATOR UI

| | |
|--|---|
| Language support for English & German | ✓ |
| Web-browser Admin UI & End user Self-Service Portal | ✓ |
| Multi-level predefined granular administrator roles and access permissions | ✓ |

CLOUD SERVICE

| | |
|--|---|
| Securely hosted in Microsoft Azure data center physically located in Germany | ✓ |
| SaaS service or private cloud capable implementation options | ✓ |
| Ability to restrict access based on, department or geographic access rights | ✓ |

APIs

| | |
|--|---|
| REST based API for easy integration into Matrix42 Service Store | ✓ |
| Manage organizations, groups, users, devices, apps, enrollments, policies | ✓ |
| Secure Container device actions like lock, Clear passcode, (enterprise) wipe | ✓ |

PRODUCTIVITY APPLICATIONS**

| | |
|--|---|
| Smart Office - create new, edit, rename MS Office files (.docx, .xlsx, .pptx) | ✓ |
| Briefcase - granular, role based push of enterprise documentation to mobile users | ✓ |
| One Drive - access, download and post One Drive files securely | ✓ |
| Skype for Business, Lync, Communicator & Google Talk secured communications | ✓ |
| SharePoint - secure mobile sync and control of files on enterprise SharePoint site | ✓ |