



Samsung SDS Enterprise Mobility Management (EMM) Proven Security for Classified Mobile Communication

Tactical law enforcement and military agencies rely on mobile devices to exchange classified data and mission-critical voice calls. In order to manage these devices they need to control access and keep sensitive data secure using an independently verified solution. Samsung SDS Enterprise Mobility Management (EMM) for on-premise is the first and only government-grade EMM solution validated for the highest level of security to manage mobile devices and prevent critical data leaks.

DESIGNED FOR SECURITY

- All Data in Transit (DIT) between the EMM server and device is protected via a secure TLS 1.2 channel
- Supporting RSA 2048 or ECDSA p256/p384 up to SHA384
- All encryption and decryption is done using FIPS 140-2 validated cryptographic kernels
- Samsung SDS EMM has the ability to use “triggers” in an offline capacity to apply different IT policies based on different network or application conditions
- Provision multiple secure containers for connection to different back end systems and networks

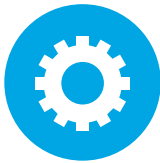
Samsung SDS EMM is designed from the ground up to be able to work in a completely offline environment, with no connectivity to the outside world. There is also no need, after provisioning, for the devices to “phone home” to the EMM, making this a perfect solution for tactical or CSFC/Classified deployments where internet connection may be in question or untrusted.



SUPPORTS THE LATEST SAMSUNG KNOX ENTERPRISE SECURITY SOLUTION FOR SMARTPHONES

Samsung SDS EMM offers deep integration with Samsung KNOX APIs, including the Knox Workspace Secure Container, to present an end-to-end security solution using the Samsung Galaxy series for enterprise mobility. Samsung SDS EMM offers powerful control over these devices by supporting the latest KNOX API features designed specifically for them. Our rapid development methodology adds API support on an ongoing basis.

Samsung SDS EMM solution supports your agency in building a secure mobile work environment by offering seamless, convenient inventory management, self-service device management and an enterprise app store for greater control.



Convenient Inventory Management

Agencies can provision and manage a wide range of mobile devices and servers from a remote location; protect enterprise data systematically by applying role-based security policies; disable features that can infiltrate data; and monitor app, device and OS-level threats.



Secure Self-service

When someone loses a device, data on it is vulnerable until that device can be wiped and secured. Self-service capabilities improve security by allowing the user to wipe the lost device immediately, rather than waiting for the help desk to open. In addition to the immediate protection this offers, agencies get an added benefit: you can reduce costs because you no longer have to staff a help desk 24x7.



Proprietary App Store/Catalog

Government agencies need to verify that mobile apps meet policy, security and procurement requirements before allowing distribution to end users. Samsung SDS EMM enables agencies to host their own app store, ensuring that end users download only vetted apps in a safe and timely manner.

ABOUT SAMSUNG SDS AMERICA, INC.

Samsung SDS America (SDSA) is the U.S. subsidiary of Samsung SDS, a global IT solutions company. SDSA provides purpose-built technology solutions in the areas of enterprise mobility, security, advanced analytics, mobile sales productivity, and training. We enable our customers in the public sector, finance, retail and other industries to achieve greater freedom, operational efficiency and smarter decision making as the driving force for their competitive advantage. SDSA is headquartered in Ridgefield Park, NJ, with offices in Herndon, VA and San Jose, CA.

CONTACT US

To learn more about our EMM solution visit www.samsungsdsa.com or email us at bd.sdsa@samsung.com.