



EMM

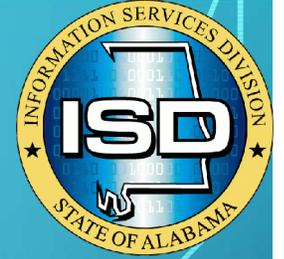
# ENTERPRISE MOBILITY MANAGEMENT

ISD BUSINESS SERVICE

ALABAMA DEPARTMENT OF FINANCE, INFORMATION SERVICES DIVISION (ISD)

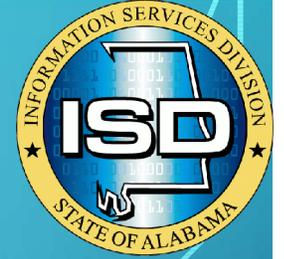
PROJECT MANAGER: MIKE VANHOOK

JUNE 23, 2016



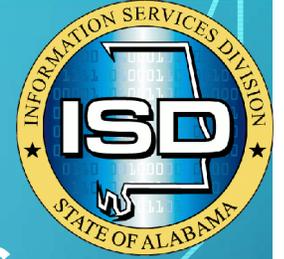
# SYSTEMS ADMINISTRATION

- Cloud based solution that provides multi-tenant hosting
  - Agencies will be provided options to:
    - manage a tenant group and admin
    - enroll devices into the default policies
  - Synchronized Active Directory groups to manage enrollments
    - Utilizing current account provisioning and directory services
  - State baseline policies delivered upon enrollment of device



# ENROLLMENT REQUIREMENTS

- Any devices connecting to the State email system will be required to be enrolled in EMM services.
- All devices will be placed in quarantine upon access request by client application unless the user has been provisioned for device enrollment



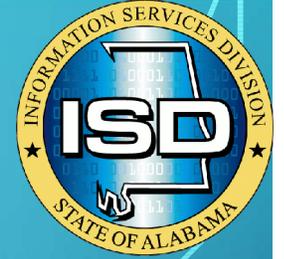
# AGENCY REPORTING REQUIREMENTS

- Use device agreements must be kept on record
  - Personal Electronic Device user agreement (320 F1)
    - OIT policy 320 and use form: <http://oit.alabama.gov/library.aspx>
  - Agency owned portable device user agreement (662-S2)
    - [http://cybersecurity.alabama.gov/documents/forms/Portable\\_Device\\_User\\_Agreement.pdf](http://cybersecurity.alabama.gov/documents/forms/Portable_Device_User_Agreement.pdf)



# AGENCY REQUESTS FOR SERVICE

- Agencies will need to contact the ISD Help Desk
  - Specify the following per distinguished user:
    - Device Type (Agency-owned, Personal)
    - EMM Subscription Type (BYOD, MDM, MTM)
    - Device user agreement
  - Specify the following per agency for tenant admins:
    - Active Directory synchronization group
- Contact ISD Help Desk ([help.desk@isd.Alabama.gov](mailto:help.desk@isd.Alabama.gov), 242-2222)



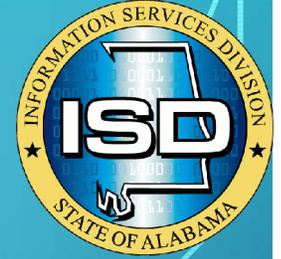
# AVAILABILITY

- EMM Services are available to all State Agencies and ISD Clients.
- Agencies that are not included in the State Active Directory Forest can be configured to synchronize devices with the MaaS360 Extender to provide tenant access.



# EMM SUBSCRIPTION OPTION TYPES

- **Secure Productivity Suite** – containerization and productivity suite for BYOD.
  - Suite/Bundle of products including MaaS360 Secure Mobile Mail, MaaS360 Mobile Application Management, MaaS360 Mobile Application Security, MaaS360 Mobile Content Management, and MaaS360 Secure Mobile Browser.
- **Advanced Mobility Management Bundle** – full MDM functionality.
  - The core mobility device management (MDM) features includes device enrollment, configuration, security policy management and device actions, such as send message, locate, lock, and wipe. The Advanced MDM features include automated compliance rules, bring your own device (BYOD) privacy settings, and Mobility Intelligence dashboards and reporting.
- **Mobile Threat Management (MTM)** – Option per device for BYOD and MDM
  - MaaS360 Mobile Threat Management provides enhanced mobile security with mobile malware detection and advanced jailbreak/root detection. With MaaS360 Mobile Threat Management, Client will be able to set and manage compliance policies around detected malware and other security vulnerabilities.
- Subscriptions may be combined for additional management and security requirements



# SUBSCRIPTION PRICING

- **Subscriptions per single device and distinguished user**
- **BYOD – Encrypted Container, Select Wipe**
  - **\$5.00** - Secure Productivity Suite (Device), MPSBD
- **MDM – Full Device Management, Full Wipe**
  - **\$5.00** - Advanced Mobility Management Bundle (Device), MMSZD
- **MTM – Enhanced Mobile Security and Malware Detection**
  - **\$2.00**- Mobile Threat Management (Device), MMTMD