Cloud and mobile apps are quickly forcing their way into the enterprise, facilitating employee productivity, while exposing business-critical data. Cloud apps, and the mobile devices that can access app data, are often outside of IT control.

**MANAGING ACCESS IS THE ISSUE:**

**Too many locks – too many keys**
Managing and securing access to each individual cloud app and mobile device means managing unique accounts, passwords, and policies across hundreds – often thousands – of endpoints and apps. With so many disparate systems and devices, IT needs a single solution from which to provision users and manage access policies across all across all apps, from any devices, regardless of location.

**Password sprawl wastes time for IT and users**
With growing application access, users are resorting to password sharing and reuse, exposing corporate data to attacks based on compromised credentials. Compounding this issue is an exponential increase in helpdesk calls and tickets for password resets – reducing IT productivity and user satisfaction.

**User productivity leads to IT inefficiency**
With dozens – or hundreds – of apps in use, controlling which users have access to specific apps becomes unmanageable. Staying on top of account provisioning is not only cumbersome, but leads to security holes and failed compliance audits if terminated employees have access to corporate apps and data after they leave.

**IDENTITY IS THE SOLUTION**

**Integrated cloud app and mobile management**
IAM uniquely unifies cloud app and mobile management into an enterprise cloud service. Samsung SDS America leverages identity to secure and manage users’ access to application from any device, regardless of location.

By leveraging a single identity across cloud, mobile and onsite apps, users get a single username and password across all the apps they use for work, and IT can enforce consistent access policies based on user identity.

IAM provides a single, simple cloud portal for app management. Users get one-click access to all their apps from any device, and IT gets policy-based control, automated provision, and account management.
IDENTITY AND ACCESS MANAGEMENT: THE BENEFITS OF INTEGRATED IDENTITY MANAGEMENT

Samsung SDS America IAM provides security, simplicity and control. IT gets one place to manage all accounts and devices. Users get single sign-on across cloud and mobile apps from any device.

Security:
• Eliminate the security risk of simple, reused and or improperly managed passwords
• Control cloud and mobile app with identity-based policy across apps and devices
• Enable secure, remote access to on-premise apps – without the risks and hassles of VPNs
• Implement a secure BYOD policy with SDSA’s integrated mobile device management. Secure apps on mobile devices by unlocking with NFC, PIN, passcode or fingerprint

Simplicity:
• Automate account provisioning/deprovisioning and licensing entitlements for business apps
• Eliminate separate policy silos with integrated management of cloud, mobile and onsite apps
• Reduce helpdesk tickets for password resets, app requests, and device management with user self-service and automated workflows

Control:
• Prove ROI and show compliance with granular app and device reporting
• Enforce user policy from a single authoritative source, applied across devices, apps and locations
• Control access using existing on-site Active Directory. LDAP, cloud director or any combination

FLEXIBLE SUBSCRIPTION OPTIONS:

<table>
<thead>
<tr>
<th>Identity and Access Management</th>
<th>App</th>
<th>App+</th>
</tr>
</thead>
<tbody>
<tr>
<td>SINGLE SIGN ON: Turnkey support for 2500+ cloud, mobile and on-premise apps, or add your own.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ENTERPRISE MOBILITY MANAGEMENT: Integrated mobile device and app management. Device certificate management for KPI.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDENTITY FROM ANYWHERE: Internal: Active directory or LDAP External: Cloud directory or external users User self-services and password resets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USER ACCOUNT PROVISIONING: Full lifecycle management of cloud and on-premise apps and devices based on role: access, authorization, SSO, and revocation.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WORKFLOW: Automated workflows for managing app request, approval and provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ON-PREMISE APP GATEWAY: Secure access to on-premise apps without VPN. Single cloud connector across multiple apps. No additional infrastructure required.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contact: email: bd.sdsa@samsung.com  |  samsungsdsa.com