



## **Identity & Access Management (IAM)**

- Solution must provide two-factor authentication support out-of-the-box
- Two-factor authentication agent must be embedded in the UEM client
- Two-factor authentication must be implemented entirely on premises.

### **Two-factor authentication must support following methods:**

- ✓ Prompt Authentication
- ✓ Timed One Time Password (TOTP)
- ✓ Pre-authentication (Timed)
- ✓ Direct Authentication

- 2FA solution must support integration with physical tokens
- 2FA solution supports RADIUS and REST API
- Enterprise Identity solution supports SSO to cloud and standards-based services
- Identity Management integrates with any SAML-based authentication service for SSO
- Single identity for all cloud applications and in a simple way: in user's regular password, on any device
- Optional Zero Sign-On (ZSO) means applications can authenticate transparently when opened
- Mobile-based two-factor authentication with any service and without user hassle, key fobs or PINs
- Contextual authentication adjusts security based on risk, with optional advanced risk and geolocation policies