Cerințe fata de sistemul Mobile Devices Management

Cerințe generale a sistemului trebuie sa permită :

● gestionarea simultană a dispozitivelor mobile ale mai multor organizații, fără acces reciproc intre ele (multi-locație).
● disponibilitatea în calitate de serviciu, accesibil pentru contractorii dedicați echipamentelor contractante, găzduit în Uniunea Europeană.
● accesul la consola de sistem pe deplin web, de asemenea în limba rusă, engleză.
● suport minim pentru browser-ele: Internet Explorer și Mozilla Firefox.
● accesul la sistem pentru mulți utilizatori, împărțit în drepturi de acces la funcții individuale bazate pe roluri definite.
● capacitatea de a instala sistemul complet în infrastructura companiei.
● sistem fail-over (Disponibilitate ridicată).
● suport complet pentru sisteme și aplicații pe telefoane mobile în engleză.
● API disponibil pentru integrarea cu servicii / sisteme externe prin WebService.
● suport pentru sisteme de operare (minim) Android, Windows Mobile, iPhone, Windows Phone, Samsung KNOX.
● suport pentru API-urile extinse Samsung SAFE pentru platformele Android.
● Integrarea cu serverele Active Directory, LDAP, MS Exchange și RIM BES.
● suport pentru soluția Samsung KNOX.
● vizualizarea listei de dispozitive în consola care poate fi definită de utilizator, împreună cu vizualizarea alertelor pentru dispozitive individuale.
● sistemul oferă toate funcționalitățile de la o consolă de administrare centrala.
● toate funcționalitățile sistemului pot fi efectuate la distanță de la dispozitivele din consola de administrare.
● toate acțiunile efectuate asupra telefoanelor (inclusiv instalarea aplicațiilor, configurare, backup de date) pot fi efectuate pe un singur dispozitiv, sau simultan pe toate dispozitivele, sau pentru un grup specific (sau mai multe grupuri) de dispozitive - de la nivelul consolei sistemului administrativ.
● abilitatea de a accesa documente stocate pe serverele companiei din tablete cu iOS.
● disponibilitatea sistemului atât în modelul instalat în mediul intern, cât și ca soluție găzduită.
● Integrarea cu sistemele SNMP.
● Integrarea cu serverul BlackBerry Enteprise.
● Integrarea cu LDAP / AD.
● Integrarea cu soluția Cisco ISE, Extreme NAC.
● Producătorul trebuie sa dețină certificatele ISO - cel puțin ISO 9001 și ISO 27001.
● Producătorul de soluții trebuie să aibă o diviziune de protecție a informațiilor clasificate și un sistem de prelucrare a informațiilor clasificate.
● Licențiere: sistemul permite gestionarea completă a numărului de dispozitive specificate în licență, este posibil să se adauge în același timp dispozitive nelimitate.
● Licențiere: numărul de utilizatori ai sistemului trebuie să fie nelimitat de o licență.
● Soluția trebuie să aibă un client VPN încorporat pentru platforma Android care funcționează și în containerul KNOX, ceea ce va permite utilizarea autentificării cu doi factori la stabilirea unei conexiuni utilizând al doilea dispozitiv (de exemplu, cardul NFC, token hardware).
● suport pentru jetoanele hardware Yubico.

Cerințe pentru configurația la distanță trebuie sa suporte:
● configurare la distanță și înscriere fără intervenția utilizatorului (inclusiv Google Zero Touch, înregistrare KNOX Mobil, Configurare KNOX, Apple DEP).
● configurare de la distanță utilizând protocolul OMA DM.
● configurare de la distanță folosind protocolul CP OMA.

Digitally signed by Șarco Vasile
Date: 2018.11.29 13:00:32 EET
Reason: MoldSign Signature
Location: Moldova

● configurare de la distanță folosind protocolul SCEP.
● configurații de acces la rețea, inclusiv:
  ○ puncte de acces la internet.
  ○ setările punctelor de acces WiFi (bazate, de asemenea, pe EAP-TLS).
  ○ Setări VoIP / SIP.
  ○ configurarea e-mailului pe telefoanele mobile.
● capacitatea de a instala și configura aplicații de la părți terțe.
● capacitatea de a configura aplicațiile interne ale clientului prin integrarea dedicată cu sistemele de baze de date de comandă.
● sistemul trebuie să furnizeze un API Web Service care să permită verificarea configurației corecte a aplicației pe dispozitivele mobile achiziționate.
● generarea de rapoarte automate și disponibile la cerere privind activarea aplicațiilor mobile ale contractantului.
● gruparea configurației pentru sistemele de operare.
● combinarea configurației și instalării aplicațiilor în scripturile efectuate pe dispozitive, inclusiv logica încorporată în scripturi (abilitatea de a defini interdependența dintre elementele individuale ale scriptului).

Cerințe privind instalarea aplicației trebuie sa permită:
● instalarea în modul silențios (fără implicarea utilizatorului) pe dispozitive: orice dispozitiv cu sistem Android versiunea 6 sau mai mare (utilizând Profilul de lucru Android și proprietarul dispozitivului) și iOS (în modul supravegheat); suplimentar (fără modul WP și DO pe Samsung Android, Huawei Android, Zebra Android, LG Android, Lenovo Android).
● previzualizarea aplicațiilor instalate.
● crearea unei aplicații whitelist (permisă) din Magazin Google Play.
● capacitatea de a elimina în mod silențios aplicațiile nedorite.
● configurarea la distanță a e-mail clientului.
● instalarea aplicațiilor la distanță pe dispozitivele mobile.
● abilitatea de a crea un magazin intern cu aplicații "corporate appstore".
● capacitatea de a configura aplicații terțe.
● Mecanismul Whitelist si Blacklist de aplicații interzise și permise prin utilizarea semnăturii aplicației (semnături de aplicație) .
● abilitatea de a defini formate de fișiere de configurare - xml sau altele, permițând descărcarea de date din sistem și transferul acestora către aplicații mobile pe dispozitiv.

Cerințe de configurare a securității:
● configurarea politicilor pentru parole pe dispozitive mobile, inclusiv:
● definirea cerinței de introducere a parolei la pornirea dispozitivului,
● definirea complexității parolei (cerință de cifre, caractere speciale),
● definirea duratei de inactivitate, urmată de blocarea automată, forțând introducerea parolei,
● definirea numărului maxim de încercări de introducere a parolei urmate de ștergerea datelor de pe dispozitiv,
● stergerea datelor de la distanță de la dispozitiv în caz de pierdere,
● opțiunea de a bloca o resetare din fabrică pe o conexiune cu dispozitive mobile (hot-spot),
● blocarea la distanță a dispozitivului,
● afișarea unui mesaj către "căutător" în cazul blocării dispozitivului, reinițializarea dispozitivului la distanță,
● acces la distanta a ecranului și tastaturei dispozitivului,
● generarea ciclică a unei copii de rezervă a datelor,
● abilitatea de a bloca unele funcții ale telefonului (de ex. Camera, browser web, conectivitate bluetooth),

● blocarea capacității utilizatorului de a instala aplicații,
● definirea unei liste negre (black list) de aplicații care nu pot fi utilizate pe dispositive,
● blocarea capacității utilizatorilor de a edita setările telefonului,
● cooperarea cu o soluție antivirus pentru detectarea malware-ului pe dispozitivele mobile,
● integrarea cu Windows CA pentru a gestiona pe deplin ciclul de viață al certificatelor de pe dispozitivele mobile,
● Serverul CA integrat în soluție pentru a gestiona pe deplin ciclul de viață al certificatelor de pe dispozitivele mobile fără a fi nevoie de integrare externă,
● abilitatea de a configura și instala certificate de tip s / mime pe dispositive,
● integrarea cu soluția Samsung Enterprise FOTA pentru a controla versiunea de firmware pe dispozitivele mobile,
● gestionarea profilelor Bluetooth pentru dispozitivele Samsung,
● abilitatea de a schimba de la distanță codul PIN al cartelei SIM astfel încât utilizatorul să nu cunoască codul PIN (astfel încât atunci când este introdus într-un alt dispozitiv decât cel gestionat, cartela SIM este inutilizabilă),

Cerințe pentru separarea datelor companiei și ale utilizatorilor:
● suport pentru versiunea 2.0 a Samsung KNOX.
● suport pentru soluția Android Enteprise.
● suport pentru funcționalitatea dual APN care permite utilizarea punctelor separate de acces la Internet pentru datele companiei (container) și datele private.
● posibilitatea utilizării mai multor licențe KNOX în cadrul unei singure organizații.
● capacitatea de a bloca și de a debloca de la distanță containerul de date al companiei.
● abilitatea de a șterge de la distanță un container de date al companiei.

Cerințe pentru funcționalitățile geolocație:
● localizarea telefoanelor pe baza datelor GPS.
● localizarea telefoanelor utilizând ID-ul stației de bază a operatorului (BTS).
● sondaj pentru locație la cerere.
● sondaj pentru o locație într-un mod continuu, cu posibilitatea de a defini intervale în funcție de:
● schimbarea locațiilor pentru o anumită distanță,
● interval de timp configurabil,
● schimbarea ID-ului stației de bază în care se află telefonul mobil,
● vizualizarea datelor pe hartă,
● capacitatea de a exporta istoricul datelor de locație într-un fișier.

Cerințe pentru suportul de la distanță pentru telefoanele mobile:
● funcționalitatea accesului de la distanță la ecran și la tastatura telefonului, cel puțin pentru platformele Android, Symbian, Windows Mobile și RIM BlackBerry.
● capacitatea de a configura calitatea imaginii trimisă la server în timpul unei sesiuni de acces la distanță, pentru a ajusta cantitatea de date transferată în condițiile de rețea în care se află dispozitivul mobil.
● abilitatea de a vizualiza dispozitivul în modul live.
● capacitatea de a gestiona fișierele de pe un dispozitiv mobil.

Cerințe suplimentare:
● disponibilitatea portalului Self-Care pentru utilizatorii finali.
● posibilitatea instalării certificatului PKCS12 de către portalul utilizatorului pentru a configura criptarea poștei (SMIME) în containerul KNOX și containerul nativ iOS.
● Disponibilitatea API pentru integrarea soluțiilor terțe cu sistemul MDM.

● abilitatea de a opera într-un mediu complet închis (fără acces la Internet, în special la furnizorii de servicii Google, Amazon etc.).
● disponibilitatea procedurilor de audit al codului sursă al soluției (pentru a verifica securitatea soluției).
● Integrarea cu o soluție completă pentru backup și colaborare cu date.
● soluție care permite verificarea stării și gradului de respectare a politicilor de către un anumit dispozitiv mobil de către soluții terțe.