ELEKTROTEHNIČKI FAKULTET UNIVERZITETA U BEOGRADU

INTEGRACIJA MOBILNIH UREĐAJA U KORPORATIVNI SISTEM

–Master rad–

Kandidat:

Mladen Steljić 2012/3260

Mentor:

doc. dr Zoran Čiča

Beograd, Septembar 2015.

SADRŽAJ

1. UVOD

Živimo u eri mobilnih uređaja, bez kojih većina nas ne može da zamisli svakodnevicu. Svesni smo svih prednosti koje nam mobilnost donosi, pa tako želimo da te prednosti dobijemo i u poslovnom okruženju, ne samo u svakodnevnom privatnom životu. Mnoge kompanije uvidele su mogućnosti povećanja produktivnosti zaposlenih pa samim tim i povećanja zarade ako svojim zaposlenim omoguće fleksibilnost koju donosi mogućnost mobilnosti na poslu. Međutim, ovo nije jednostavan ni kratkotrajan postupak. Mora biti sproveden uz detaljan plan i koordinaciju različitih službi unutar jedne kompanije. Da bi omogućili korišćenje mobilnih uređaja u korporativnom okruženju neophodna je implementacija sistema poznatih kao EMM (Enterprise Mobility Management) rešenja.

Tema ovog rada je da pokaže neophodnost implementacije EMM rešenja u svakom okruženju gde će se mobilni uređaji koristiti za obavljanje poslovnih zadataka, tako što će se mobilnim uređajima pristupati IT resursima u internoj mreži kompanije. Poseban akcenat je stavljen na sigurnost korporativne infrastrukture, aplikacija kao i podataka. Kroz primer konkretne implementacije pokazaćemo načine rešavanja bezbednosnih i operativnih pitanja u vezi sa integracijom mobilnog u korporativni IT sistem.

Rad će biti organizovan u narednih 7 poglavlja, od kojih je prvo ovaj uvod. U drugom poglavlju biće predstavljene opšte poslovne potrebe za uvođenjem mobilnosti u poslovne okvire, zatim opis samih EMM rešenja, njihovih funkcionalnosti, arhitektura, strategija razvoja, kao i različitih scenarija zaštite korporativne mreže. U trećem poglavlju biće dat pregled najznačajnijih rešenja ove vrste na tržištu, analiza njihovih prednosti i nedostataka. Četvrto poglavlje, koje predstavlja centralno poglavlje ovog rada, daće detaljan opis implementacije funkcionalnosti EMM sistema u korporativnom okruženju. Opisaćemo detaljnu instalaciju rešenja u korporativnoj mreži, fizičku i logičku organizaciju pojedinačnih komponenti EMM rešenja, definiciju i primenjivanje različitih polisa kojima se obezbeđuje bezbednost IT sistema u kome se mobilni uređaji integrišu u korporativnu mrežu, kao i tehnika sigurne isporuke aplikacija na mobilne uređaje. U petom poglavlju predstavićemo rezultate testiranja implementiranog rešenja, gde se sa korisničke strane mogu videti uspešno implementirane funkcionalnosti EMM rešenja. Poseban osvrt na najčešće poslovne potrebe kao što su siguran pristup korporativnoj elektronskoj pošti, siguran pristup aplikacijama host-ovanim u internoj mreži kompanije kao i siguran pristup i deljenje korporativnih podataka i dokumenata. Šesto poglavlje predviđeno je za kratak osvrt na mogućnosti iskorišćenja EMM sistema u budućnosti i pravce daljeg razvoja ovih rešenja. U sedmom poglavlju iznećemo kratak zaključak, donesen na osnovu rada na ovoj temi.

2. PREGLED POSLOVNIH POTREBA I FUNKCIONALNOSTI EMM REŠENJA

2.1. Razlozi i poslovne potrebe uvođenja EMM rešenja

Trenutno svuda u svetu postoji ekspanzija korišćenja mobilnih uređaja različitih vrsta, funkcionalnosti i performansi. Napretkom tehnologije mobilni uređaji svakim danom dobijaju sve naprednije opcije i funkcionalnosti. Danas imamo smartfone i tablete koji poseduju takve mogućnosti i perfomanse da u većini situacija mogu zameniti tradicionalne personalne računare.

Brz tempo inovacija mobilnih uređaja kao i softvera kojim mogu raspolagati čini upravljanje njima izazovom. Sa druge strane, novi trendovi poslovanja očekuju ili čak zahtevaju sve veću mobilnost zaposlenih. Ova mobilnost, naravno, mora imati što manje ograničenja kada je u pitanju obavljanje radnih zadataka. Da bi zaposleni uopšte mogli da ispunjavaju svoje poslovne zadatke i obaveze potrebno je da imaju pristup korporativnim podacima i aplikacijama koji su im neophodni. U slučaju ovakvog poslovanja, poseban fokus mora biti stavljen na siguran pristup korporativnim aplikacijama i informacijama, kao i sprečavanju da korporativni podaci izađu iz okvira komapanije.

Da bi obezbedili što veću efkasnost i produktivnost svojih zaposlenih mnoge kompanije danas razmatraju implementaciju sistema koji bi omogućili zaposlenima korišćenje mobilnih uređaja za poslovne potrebe sa svim benefitima koje ova fleksibilnost može doneti.

Sistemi koji omogućavaju rešenje ovakvih potreba i problema na tržištu su poznati kao Enterprise Mobile Management (EMM) sistemi.

Enterprise Mobile Management (u daljem tekstu EMM) predstavlja sveobuhvatan pristup obezbeđivanju i omogućavanju poslovanja zaposlenih koji mogu koristiti mobilne uređaje u svakodnevnim poslovnim procesima eksploatišući na taj način sve pogodnosti i fleksibilnost koju im ovaj vid mobilnosti pruža. Dodatno, rešavajući sigurnosne probleme i pitanja, dobro definisana EMM strategija pomaže zaposlenima da budu produktivniji omogućavajući im pristup neophodnim alatima i podacima.

EMM je generalno kombinacija tri različite tehnologije čiji su fokus različiti delovi mobilnog sistema. I dok se Mobile Device Management (MDM) fokusira upravljanjem samim fizičkim mobilnim uređajima, Mobile Application Management (MAM) upravljanjem aplikacijama, dotle se Mobile Information Management (MIM) bavi pitanjima kontrole, upravljanja i sigurnosti samih korporativnih podataka. Više reči o ulozi različitih komponenti u EMM sistemu biće kasnije u ovom poglavlju [1].

Svaka od ovih tehnologija se bavi različitim pitanjima i problemima koje može izazvati korišćenje mobilnih uređaja u jednom korporativnom sistemu. Preklapanja funkcionalnosti ovakvih rešenja su minimalna. Rešavanje ovih pitanja predstavlja izazov kako u finansijskom, tako i u smislu ljudskih resursa koji su potrebni za implementaciju, a kasnije i za administraciju i upravljanje jednim ovakvim sistemom. Na svom samom početku razvoja EMM sistemi su sadržali samo MDM komponentu. Međutim, sa pojavom sve većeg broja kompanija koje usvajaju i implementiraju ovakva rešenja, i imajući u vidu potrebu za sve većim brojem funkcionalnosti

ovakvog sistema, EMM vendori su počeli sa razvojem MAM i MIM rešenja. Danas imamo jedinstvenu platformu EMM sistema koja se najčešće sastoji od ove tri komponente.

Koristeći sve tri komponente je najbolji i najproduktivniji način da se odgovori na sve zahteve koje određena kompanija može imati. Na kompaniji je da detaljnom analizom funkcionalnosti i performansi proizvoda dođe do rešenja koje će odgovoriti na sve njene potrebe. Svakako se mora imati na umu da se mora brinuti o obuci zaposlenih, kreiranju i sprovođenju pravila, kao i drugim kadrovskim pitanjima, bez obzira za koju se tehnologiju odlučimo.

Mobilni uređaji se sve češće integrišu u korporativne mreže i ovaj trend ne pokazuje znakove usporenja. Pošto mobilni uređaji postaju sve moćniji, pomerajući granicu onoga što kompjuteri zaista jesu, kompanije imaju potrebu da upravljaju ovakvim sistemima, kao i da obezbede da njihovo korišćenje bude potpuno sigurno u pogledu bezbednosti korporativne infrastrukture i podataka.

Sve veći priliv mobilnih uređaja u kompanije kao i sve veći broj proizvoda koji omogućava upravljanje tim uređajima podstakao je debatu o EMM-u – odnosno da li IT administratori treba da se fokusiraju na upravljanje mobilnim uređajima, ili aplikacijama i informacijama koji se na njima nalaze.

Sa više od 100 vendora EMM rešenja na tržištu danas, veliki je izazov odabrati proizvod koji će stvarno ispuniti sve zahteve jedne kompanije po pitanju EMM funkcionalnosti, koji će takođe omogućiti održivu i ekonomičnu IT strategiju po pitanju mobilnih uređaja. Možda se najveća pitanja odnose na zahtevani set funkcionalnosti za uspešno funkcionisanje mobilnih uređaja u korporativnoj mreži, i kako razviti i implementirati pravu kombinaciju proizvoda i servisa. Međutim, sa tako puno tehnologija i proizvoda koji se svakodnevno pojavljuju na tržištu, postoji opasnost da funkcionalna preklapanja i kompleksnost mogu potopiti čak i dobronamerne i dobro osmišljene procese. Jednostavnost je ključ uspeha, ali jednostavnost nikada ne dolazi od prvog dana.

Primenjujući na mobilne uređaje, kroz EMM posebno definisane sigurnosne polise, IT administratori mogu na primer, regulisati da se ovi uređaji mogu koristiti samo na način za koji kompanija smatra da je u skladu sa njenim sigurnosnim polisama. Ovo može smanjiti rizik od gubitka podataka, sprečiti instalaciju neodobrenih aplikacija i softvera, i izbeći neautorizovan pristup korporativnim podacima i mreži korišćenjem mobilnih uređaja.

Ovakvi sistemi, međutim, nisu namenjeni samo velikim kompanijama. Ovo pitanje treba da ozbiljno bude ozbiljno razmotreno u svim slučajevima, bez obira na veličinu kompanije.

2.2. Mogućnosti EMM rešenja

EMM pomaže kompanijama da integrišu mobilne uređaje u njihove sigurnosne okvire, sisteme i informacione tehnologije. Organizacije i kompanije koriste EMM da obezbede svojim korisnicima sledeće opšte funkcije:

- EMM omogućava konfigurisanje uređaja i aplikacija za potrebe korišćenja u korporativnom okruženju.
- Analizu, praćenje i izveštavanje: ova rešenja omogućavaju nadgledanje mobilnih uređaja sa ciljem praćenja usaglašenosti sa korporativnim polisama i pravilima. Oni takođe vode računa o softverima instaliranim na mobilnim uređajima, u cilju praćenja iskorišćenosti licenci pa samim tim troškova, i takođe imaju sposobnost praćenja i analize iskorišćenosti poslovnih servisa i aplikacija.

- Podršku: EMM pomaže IT zaposlenima u IT sektoru korporacije analiziranje i rešavanje problema na mobilnim uređajima omogućujući pozivanje akcije sa udaljene lokacije.
- Zaštitu mobilnog sistema na nivou uređaja, aplikacija i podataka.

Ovo je samo uopšteni pregled funkcionalnosti koje nude EMM rešenja, dok će detaljna analiza funkcionalnosti biti predstavljena u nastavku rada.

Pri odabiru EMM rešenja koje će biti implemntirano u sistem kompanije, treba obratiti pažnju da konkretno rešenje mora imati minimalno sledeće mogućnosti kako bi osnovna mobilna sigurnosna politika mogla biti formirana:

1) Primena PIN-a ili šifre. Slično kao šifra prilikom logovanja na računar na neki korisnički nalog i ovde se korporativnm polisom može zahtevati da korisnik ili administrator generiše PIN ili šifru kojom će se vršiti autentifikacija prilikom pristupa korporativnim resursima.
2) Enkripcija. Enkripcija na nivou „kontejnera" podataka, ili enkripcija na nivou celog uređaja. EMM proizvodi bi trebalo da omoguće sprovođenje enkripcije podataka na svakom od uređaja koji se nalazi pod njihovim pokroviteljstvom. O ovome će više reči biti u nekom od narednih odeljaka.
3) Daljinsko brisanje. Potrebno je da EMM rešenje poseduje ovu mogućnost kako bi se sprečila zloupotreba korporativnih podataka i aplikacija koji se nalaze na mobilnom uređaju a u slučaju da on bude izgubljen ili ukraden.
4) Zaštita podataka dok su oni pohranjeni na mobilnom uređaju kao i prilikom njihove tranzicije kroz sistem. Mogućnost zabrane kopiranja ili slanja određenih podataka dok se oni nalaze na određenom uređaju.
5) Detekcija *jailbroken* ili *rooted* mobilnih uređaja. *Jailbreak*-ovani *root*-ovani uređaji predstavljaju značajan rizik po korporativni sistem time što dozvoljavaju korisniku da instalira i koristi neodobrene softvere, kao i da pravi izmene na operativnom sistemu uređaja. Više reči o ovakvim uređajima biće kasnije u tekstu.

O svim navedenim karakteristikama EMM rešenja više reči će biti u nastavku teze, ovde su samo pomenute obavezne funkcionalnosti koje svako EMM rešenje mora posedovati.

Postoje naravno i dodatne EMM mogućnosti kao na primer GPS praćenje, VPN integracija, upravljanje sertifikatima, Wi-Fi polise, kreiranje belih (*white*) i crnih (*black*) listi, koje predstavljaju spisak dozvoljenih i nedozvoljenih mobilnih aplikacija, ograničavanja nekih funkcionalnosti na uređajima kao što su korišćenje kamere, proširenje memorije, funkcije slanja različitih izveštaja o dešavanjima u EMM sistemu, i mnoge druge. Ove mogućnosti su korisne, ali ne za sve kompanije. U najmanju ruku pet stavki navedenih gore trebaju biti potvrđene kada se radi o nabavci EMM rešenja. Takođe moramo biti sigurni da označeno EMM rešenje podržava sve platforme smartfona i tablet uređaja (iOS, Android, Windows Phone i druge) kojima kompanija namerava da upravlja i da ih štiti [2].

I dok se EMM fokusira na sigurnost i zaštitu mobilnih uređaja, korporativne infrastrukture, kao i korporativnih aplikacija i podataka, postoji nekoliko stvari kojima se EMM ne bavi. Za početnike, mnogi misle da je *Web filtering* obavezna funkcionalnost, ali činjenica je da se većina, ali ne svi, EMM vendori oslanjaju na odvojene sisteme koji obezbeđuju ovu funkcionalnost. Druga funkcionalnost za koju se možda može pretpostaviti da je EMM rešenja poseduju je *backup* podataka. EMM sistemi ne *backup*-uju podatke sa mobilnih uredjaja. Ako se podaci izgube na neki način, onda se ne mogu povratiti, osim ako ne postoje odvojeni *backup* sistemi sa kojih se podaci

mogu ponovo vratiti u sistem. Ovo je obično relizovano pomoću *third-party* aplikacija, ali ne prirodno kroz EMM proizvode.

2.3. Opis komponenti EMM sistema

Već smo rekli da funkcionalno postoje tri komponente EMM sistema čiji su fokus različiti delovi mobilnog sistema.

Mobile device management (MDM), Mobile Aplication Management (MAM) i Mobile information management čine sigurnosni trio koji štiti mobilne uređaje, korporativnu infrastrukturu i podatke u korporativnom mobilnom sistemu.

2.3.1. Mobile Device Management (MDM)

MDM (Mobile Device Management) je bio najraniji model za upravljenje i kontrolu mobilnim uređajima u korporativnom okruženju. Sada zajedno sa MAM (Mobile Aplication Management) i MIM (Mobile Information Management) čini EMM (Enterprise Mobile Management). Polise koje se kroz MDM sistem primenjuju su sigurnosne polise koje se odnose na same mobilne uređaje, ali su takođe i restriktivne u smislu da mogu onemogućiti neke funkcionalnosti mobilnih uređaja ili korišćenje pojedinih aplikacija. Neke od mogućih vrsta polisa koje IT administratori najčešće primenjuju kroz MDM kao deo EMM sistema:

- Polise koje se odnose na zahteve za enkripcijom uređaja
- Restrikcije za korišćenje pojedinih aplikacija
- Kontrola korišćenja nekih funkcionalnosti mobilnih uređaja kao što su kamera i bluetooth
- Zahtevi za postavljanjem PIN-a ili lozinke na uređaju
- Polise za blokiranje ili ograničenje korišćenja *root*-ovanih ili *jailbreak*-ovanih uređaja

MDM je komponenta koja je odgovorna za upravljanje samim fizičkim mobilnim uređajem. Teorijski uređaj bi trebalo biti konfigurisan prema korporativnim pravilima i specifikacijama, kako bi bio sigurnosno obezbeđen i upravljiv, kao i uređaji koji su u vlasništvu same kompanije. Upravljanje konfiguracijama i sprovođenje korporativnih pravila i politike (kao što su skeniranje na viruse ili korišćenje VPN-a) su neka od obeležja MDM-a, ali MDM softver može imati veliki broj funkcionalnosti. Mana je što MDM može imati uticaja na privatne podatlke na mobilnom uređaju.

Ključne funkcionalnosti MDM komponente EMM sistema su neke već pomenute u prethodnom odeljku, a to su primena polisa koje zahtevaju PIN ili šifru za „zaključavanje“ mobilnog uređaja, detekcija i mogućnost blokiranja *jailbreak*-ovanih i *root*-ovanih uređaja, daljinsko brisanje sadržaja na mobilnom uređaju, mogućnost lociranja uređaja, mogućnost otkrivanja softvera instaliranih na uređaju itd. Neke od ovih funkcionalnosti neophodne su za implementaciju funkcionalnosti MIM komponente sistema o čemu će više reči biti u odeljku koji se bavi opisom MIM komponente.

Postoji dosta paralela između MDM sistema i upravljanja i kontrole desktop sistemima. Pre svega se to odnosi na funkcionalnosti udaljenog pristupa i kontrole. Ovo uključuje ažuriranje softvera, menjanje kontrole pristupa ili daljinsko brisanje sadržaja sa administriranih uređaja.

Iako MDM ima tako puno da ponudi, menadžment alati koji daju potpunu kontrolu kompanija nad personalnim uređajima teško postižu neophodni balans između očekivanja zaposlenih kao korisnika mobilnih uređaja i u privatne i u poslovne svrhe, i potreba kompanije.

Jedan od načina da se balansiraju potrebe i interesi zaposlenih i kompanije je implementacija različitih delova EMM sistema koji imaju i različite sfere delovanja i kontrole. Potrebno je garantovati zaposlenima da mogu koristiti mobilne uređaje za potrebe izvršavanja poslovnih zadataka, ali da ti njihovi privatni podaci na uređaju neće biti pod stalnom kontrolom i upravljanjem kompanije, tj. samog poslodavca.

U isto vreme kompanija mora imati kontrolu nad tim gde njeni korporativni podaci idu, koliko dugo ostaju pohranjeni na mobilnim uređajima zaposlenih, da li ti podaci treba da budu enkriptovani dok su na mobilnim uređajima, kao i šta se sa podacima dešava dok se nalaze na mobilnim uređajima. Ovo je razlog uvođenja druge dve komponente EMM rešenja.

2.3.2. Mobile Aplication Management (MAM)

MAM funkcioniše oslanjajući se na teoriju da se sigurnost i integritet IT infrastrukture može obezbediti kroz primenu belih i crnih listi aplikacija. Gde će bela (*white*) lista biti sačinjena od aplikacija koje je dozvoljeno koristiti u poslovne svrhe, a crna (*black*) lista od nedozvoljenih aplikacija. Ova komponenta EMM-a se bavi upravljanjem mobilnim aplikacijama umesto samim mobilnim uređajima, kontrolišući koji korisnici mogu pristupati kojim aplikacijama i sa kojih mobilnih uređaja. Umesto da poslodavci imaju potpuni pristup samim personalnim uređajima, oni samo određuju koje aplikacije i podaci se mogu nalaziti na uređajima zaposlenih. Može se definisati koje aplikacije korisnici mogu imati instalirane na mobilnim uređajima, kao i komunikacija i razmena podataka između korporativnih aplikacija i onih koje korisnici koriste za privatne potrebe na svojim uređajima.

Ovo može imati veliku primenu ako su dozvoljene aplikacije ograničene na e-mail, deljenje dokumenata i druge često korišćene aplikacije. Prodavci aplikacija i softvera i MAM vendori imaju za cilj da obezbede sigurne verzije ovakvih aplikacija, ali takve verzije obično imaju manje opcija nego one verzije koje ne poseduju dodatne sigurnosne opcije.

Ključne funkcionalnosti MAM-a su pakovanje (*wrapping*) aplikacija i kontejnerizacija, postupci kojima se obezbeđuje logička razdvojenost aplikacija koje se koriste za poslovne potrebe i privatnih aplikacija na mobilnom uređaju.

MAM daje mogućnost granularne kontrole i izolovanja korporativnih aplikacija od oniih koje se koriste za lične potrebe, a dva glavna pristupa su gore pomenute kontejnerizacija mobilnih aplikacija na uređaju i postupak pakovanja aplikacija.

Sa ovim funkcionalnostima implementiranim kroz MAM komponentu EMM rešenja korisnici mogu da nastave da koriste njima familijarne aplikacije za lične potrebe bez uticaja na poslovne operacije. Osetljive aplikacije i podaci ostaju zaštićeni u, logički odvojenom, poslovnom delu mobilnog uređaja sa odvojenom kontrolom i višim nivoom sigurnosti.

Kod tzv. kodno bazirane kontejnerizacije programski kod mobilne aplikacije se integriše sa Software Development Kit (SDK) objavljenim od strane EMM vendora. SDK omogućava programerima aplikacija da, integrišući SDK u kod same aplikacije, u svoje aplikacije ugrade mogućnost kasnije kontejnerizacije, kada se te aplikacije nađu u EMM sistemu, povezane sa vendorskim upravljačkim platformama. Oni takođe mogu omogućiti međusobnu komunikaciju i razmenu podataka između aplikacija koje se interno razvijaju u okviru kompanije, a koje će se naći u upotrebi na mobilnim uređajima.

Integracija sa specifičnim vendorskim SDK može biti efikasna strategija ali ovakav pristup može ograničiti kompaniju na određeno EMM rešenje. Takođe kreira se segmentacija *third-party* aplikacija, zato što nezavisni softverski vendori ne žele da razvijaju različite verzije aplikacija

posebno za svakog EMM vendora i njegov SDK. Takođe, javlja se problem kod već razvijenih aplikacija, gde bi bilo potrebno menjati programski kod da bi im se implementirala mogućnost kontejnerizacije.

Dosta jednostavniji način za postizanje logičke razdvojenosti poslovnih od privatnih aplikacija je kroz postupak pakovanja (*wrapping*-a) aplikacija. U ovom pristupu, dinamičke biblioteke dobijene od EMM vendora se ugrađuju u binarne fajlove aplikacije, ali posle samog razvoja aplikacije. Programeri ne moraju u ovom slučaju da integrišu kod svoje aplikacije sa vendorskim SDK ili API-em. U stvari, u slučaju pakovanja aplikacija uopšte nije potrebno reprogramirati kod aplikacije. Administratori EMM sistema mogu ugraditi sigurnosne i kontrolne funkcionalnosti u aplikacije bez potrebe pristupa izvornom kodu, često sa samo par koraka kroz upravljačku konzolu EMM proizvoda.

Pakovanje aplikacija zamenjuje standardni sistem kontejnerizacije koji podrazumeva menjanje koda aplikacije, tako što dodaju novi sloj u aplikaciji sa ciljem zaštite i upravljanja istom, kada se ona nađe na mobilnom uređaju korisnika. Pakovanje aplikacija je odlično rešenje u slučaju kada nemamo pristup izvornom kodu aplikacije, kada imamo limitirane resurse za razvijanje aplikacija kao i kada imamo malo vremena za omogućavanje korišćenja konkretne aplikacije.

Pakovanje aplikacija ne podržava neke sofisticirane funkcionalnosti koje nudi princip kontejnerizacije, kao što je sposobnost korišćenja deljenih servisa. Postoji još jedno važno upozorenje, pakovati neku drugu aplikaciju osim onih interno razvijenih i prilagođenih korporativnim potrebama može biti donekle nezgodno u pogledu licenciranja i dozvole za korišćenje. Uprkos tome što pakovanje aplikacija nije nametljiv pristup, proces dodavanja novog sigurnosnog sloja može potencijalno prekršiti uslove korišćenja aplikacije. Takođe, ovo može biti u suprotnosti sa zakonima o autorskim pravima zato što je nelegalno menjati kod napisan i objavljen od strane drugih bez njihove dozvole.

Osim ako nemamo konkretnu potrebu za funkcionalnošću kontejnerizacije bazirane na promeni kod kao što je razmena dokumenata i podataka između aplikacija, verovatno je bolje da koristimo princip pakovanja. Ova tehnika ne zahteva rad programera i obezbeđuje lakši pristup sadržajima mobilnih aplikacija, dok u isto vreme nudi mnoge pogodnosti koje očekujemo od MAM proizvoda [4].

Rad sa interno razvijenim aplikacijama postavlja set drugih pitanja. Na primer, ako kompanija želi da svojim menadžerima isporuči interno razvijeni sistem izveštavanja, administratori će prvo morati da upakuju (wrapuju) u specifične softverske pakete definisane od strane MAM vendora. Pakovane aplikacije izvršavaju specifične MAM kodove na uređajima prilikom njihovog startovanja i isključivanja. Takve aplikacije mogu zahtevati drugačiji način njihovog korišćenja. Tako na primer mogu blokirati pristup resursima kompanije preko internet konekcije ukoliko to nije sigurna VPN konekcija.

Pored toga, programeri aplikacija mogu izabrati aplikativni programski interfejs (API) za implementaciju sigurnosnih kontrola. Ovo će verovatno značiti više posla prilikom razvijanja, testiranja i održavanja aplikacija. Ako se odlučimo da naš mobilni sistem koristi *sandboxing* (princip kontejnerizacije aplikacija na mobilnim uređajima) i druge sigurnosne mere, onda će biti manje potrebe za korišćenjem *wrapinga,* tj. pakovanja aplikacija ili specifičnih API-a.

Fokusiranje na upravljanje aplikacijama omogućava neke druge korisne kontrole. Na primer, polisa koja sprečava konkretnu aplikaciju da pristupi nekim korporativnim podacima može se lako zaobići ako korisnik te podatke može iskopirati iz neke autorizovane i dozvoljene aplikacije. MAM rešenja mogu sprečiti ovakvo nedozvoljeno kopiranje podataka iz odobrenih u neodobrene

aplikacije. Ovakva rešenja takođe omogućavaju kreiranje listi sa dozvoljenim i zabranjenim URL-ovima kako bi sveli na minimum rizik od posećivanja veb sajtova za krađu podataka, olakšavanje skidanja sadržaja, kao i sajtovi sa potencijalno štetnim sadržajima.

Kako kompanije nastavljaju da usvajaju SaaS (*Software as a Service*) kao model isporuke aplikacija na mobilne uređaje, tako će veći naglasak biti na kontroli informacija i podataka nego na kontroli samih mobilnih uređaja.

2.3.3. Mobile Information Management (MIM)

U idealnom svetu, oni koji su odgovorni za bezbednost informacija mogli bi da se fokusiraju na zaštitu samih podataka, bez fokusa na aplikacije ili same mobilne uređaje. Međutim, u realnosti imamo drugačiju sliku. Aplikacije i mobilni uređaji mogu biti mesta gde podaci „cure“, kao i mesta gde zlonameran sadržaj može ući u korporativnu mrežu. Pored standardne prevencije, detektovanja i brisanja zlonamernih sadržaja, MIM (Mobile Information management) je još jedan segment u razvoju EMM sistema koji upravljaju i kontrolišu mobilni korporativni sistem.

Ideja koja stoji iza MIM komponente EMM rešenja je zaštita korporativnih podataka na mobilnim uređajima koji koriste zaposleni, smatrajući da je zaštita korporativnih informacija ključ uspešnog korišćenja mobilnih uređaja u korporativne svrhe. MIM čuva podatke kreirajući sigurnosnu zaštitu oko osetljivih korporativnih podataka, čuvajući ih enkriptovane, i dozvoljavajući samo određenim odobrenim aplikacijama pristup i mogućnost slanja takvih podataka. Može se definisati pod kojim uslovima podaci mogu napustiti mobilni uređaj kao i kojim podacima smeju pristupati aplikacije korišćene za privatne potrebe.

Da bismo zaštitili podatke na mobilnim uređajiima neophodno je da imamo neku od metoda prevencije gubitka podataka (engl. *Data loss prevention* ili DLP). Ovo je osnovna funkcionalnost MIM komponente EMM rešenja, ali njena implementacija nije moguća bez prethodne implemantacije funkcionalnosti MDM komponente, što je već pomenuto.

Zaštita podataka na mobilnim uređajima je prvi korak ka sigurnosti u korporativnim mobilnim sistemima. Ali, čak i kada su primenjeni pravilna enkripcija uređaja i polise koje zahtevaju PIN ili šifru na mobilnom uređaju, IT osoblje mora biti svesno činjenice da mobilni uređaj može biti izgubljen ili ukraden, kao i da zaposleni nekad ne znajući mogu na uređaje preuzeti neki štetni sadržaj, koji može kompromitovati osetljive korporativne podatke.

Šta možemo uraditi u tom slučaju? Ovde ćemo analizirati funkcionalnost MIM komponente EMM sistema koja omogućava zaštitu od spoljnih pretnji.

Ako je uređaj, na kome su pohranjeni osetljivi korporativni podaci, izgubljen ili ukraden postoji velika opasnost da neko može zloupotrebiti podatke koji se na uređaju nalaze. Podaci na uređaju bi svakako trebali biti enkriptovani. Takođe, otključavanje uređaja pomoću PIN-a ili šifre bi trebalo biti aktivirano. Administratori mogu odbiti pretnju time što će primeniti funkcionalnost daljinskog brisanja podataka sa uređaja, što predstavlja funkcionalnost MDM komponente. Ovo se može uraditi na više načina.

Prvo, alati kao što su Microsoft's Exchange ActiveSync i IBM's Notes Traveler obezbeđuju mogućnost daljinskog brisanja. Ovo je, međutim, grub pristup jer kada je poslata komanda za brisanje sav saobraćaj uređaja će biti obrisan uključujući lične fotografije korisnika, muziku, aplikacije i ostale stavke u memoriji uređaja.

S obzirom da je uređaj sada u nepoznatim rukama korisnik će možda želeti da obriše sadržaj sa uređaja, a ukoliko podaci koji su se nalazili na uređaju postoje iskopirani još negde kao rezervna kopija (*backup*) korisnik ih može povratiti uz asistenciju administratora.

Drugi scenario koji plan uvođenja mobilnih uređaja u korporativno okruženje mora razmotriti je slučaj kada zaposleni napušta kompaniju. U ovom slučaju mogu se iskoristiti prednosti EMM sistem tako što će se obrisati samo korporativni podaci, dok će privatni ostati netaknuti (naravno, ovo u slučaju da bivši zaposleni zadržava uređaj, u slučaju da uređaj ostaje u kompaniji nema potrebe za brisanjem). Takođe, postoji i opcija brisanja svih stavki sa uređaja ako je to zahtevano.

Takođe, ako je EMM klijent na uređaju deinstaliran ili Exchange ili Notes Traveler deaktiviran, uređaj neće reagovati na komandu brisanja. Međutim, u većini slučajeva prilikom deinstalacije EMM klijenta ili deaktivacije email naloga svi podaci sa uređaja biće automatski obrisani.

Gubitak ili krađa uređaja su jedni od načina kada gubimo kontrolu nad korporativnim podacima, međutim, to nije jedina briga MIM komponente EMM rešenja. Korisnici se savetuju da uvek imaju rezervne kopije podataka koji se na uređaju nalaze, da bi u slučaju da sadržaj mora biti obrisan daljinski mogli povratiti podatke koji su na uređaju bili pohranjeni. Ovo se postiže prosleđivanjem elektronske pošte na privatne naloge i čuvanjem korporativnih dokumenata na javnim servisima za pohranu podataka kao što je DropBox. Ukoliko implementirano rešenje uključuje poseban cloud servis za pohranu podataka, kao što je Citrix-ov Share File StorageZone, svakako da bi korisnici svoje korporativne podatke trebalo da čuvaju na njemu. Ako u slučaju gubitka podataka nijedna tehnika njihovog povraćaja ne uspe, korisnik jednostavno može iskopirati podatke sa ovakvog jednog servisa.

Na sreću, EMM vendori su svesni ovakvih pretnji i razvili su metode da se izbore sa ovakvim problemima. Osnovni alat za rešavanje ovog problema je tzv. „sigurni kontejner“ ili „sandbox“ koji je u suštini region u memoriji uređaja koji je zaštićen šifrom i softverski definisan tako da čuva korporativne podatke logički odvojene od privatnih. Lako je primetiti analogiju sa MAM rešenjem koje na sličan način obezbeđuje logičku razdvojenost aplikacija. Ako je uređaj izgubljen, ukraden, ili zaposleni napušta kompaniju onda se „sigurni kontejner“ može izbrisati daljinskim putem.

Druga ključna funkcionalnost „sigurnog kontejnera“ je da svi podaci pohranjeni u njemu bivaju označeni na takav način da ne mogu biti prosleđeni van kontejnera. Email poruke i sadržaji koji su im pridruženi ne mogu biti ni prosleđeni niti kopirani, ukoliko to korporativnim polisama nije eksplicitno dozvoljeno.

„Sigurni kontejner“ može takođe sadržati druge korporativne aplikacije i njihov sadržaj takođe može biti prosleđen i korišćen od strane privatnih aplikacija samo ukoliko je to primenjenim polisama eksplicitno dozvoljeno. Kao što smo već pomenuli EMM proizvodi u svoju ponudu mogu takođe uključivati mogućnost sigurnog cloud servisa za smeštanje podataka (primer je Citrixov Share File Storage Zone o kom će više reči biti kasnije) kako bi se eliminisala potreba za korišćenjem servisa kao što je Dropbox.

Kao što vidimo, MIM kontroliše kretanje korporativnih podataka, kao i pravila koja određuju koje aplikacije mogu pristupati tim podacima. MIM rešenja predstavljaju veoma značajnu komponentu EMM platforme, posebno imajući u vidu sve veći trend korišćenja cloud servisa za pohranjivanje podataka, kao što su Dropbox, Box i One drive. Takođe, njegova uloga je i sinhronizacija podataka putem mobilnih uređaja [5].

2.3.4. Povezanost komponenti EMM sistema

MDM, MAM i MIM su blisko povezane tehnologije, koje čine segmente EMM sistema, zamišljene i dizajnirane da postignu ravnotežu između slobode i fleksibilnosti korišćenja mobilnih uređaja sa jedne strane i bezbednosti korporativnog informacionog sistema sa druge strane.

Preklapanje u funkcionalnostima između MDM-a, MAM-a i MIM-a je veoma malo. Ipak, testiranjem je potrebno potvrditi da različiti proizvodi neće ometati jedni druge, mada bi eventualni razvoj standarda trebao da pomogne u rešavanju ovog pitanja. Centralno pitanje u celoj priči, kada je u pitanju implementacija različitih komponenti EMM rešenja, je dodatni posao u administriranju sistema. Razlog tome je što svaka od komponenti može imati svoju konzolu za upravljanje, što zahteva veće napore administratora za održavanje pravilnog i kontinuiranog rada sistema. Ključni koraci za izbegavanje preklapanja funkcionalnosti različitih komponenti u EMM sistemu su sledeći:

- Izrada strategije korišćenja mobilnih uređaja u korporativne svrhe;
- Provera da li odabrano EMM rešenje odgovara razvijenoj strategiji;
- Voditi računa da implementacija i administracija odabranog rešenja bude što je moguće jednostavnija
- Redovna edukacija korisnika i preispitivanje proizvoda i servisa koji su u upotrebi.

Kako industrija EMM rešenja evoluira pojavljuju se i sve naprednija rešenja sa sve više funkcionalnosti, dok preklapanje funkcionalnosti različitih komponenti EMM proizvoda postaje sve manje, ali ova evolucija će potrajati.

Uz svaki novi uređaj uveden u mrežu preduzeća javljaju se nova sigurnosna pitanja, koja mogu biti od veoma jednostavnih do vrlo kompleksnih. Šta ako mobilni uređaj bude izgubljen? Da li se može obezbediti da korisnici pristupaju i koriste samo odobrene preporučene aplikacije? Kako se zaštititi od opasnosti da korporativni podaci dođu u pogrešne ruke?

Ironija je da sve sigurnosne mere primenjene na nivou aplikacija i podataka mogu biti bezvredne ako se sam fizički uređaj zarazi malcioznim sadržajem. Mobilne aplikacije su dostupne sa velikog broja različitih izvora i EMM vendori razvijaju veliki broj različitih pristupa kako da takve aplikacije testiraju pre nego dozvole njihovo preuzimanje, instaliranje i korišćenje na mobilnim uređajima integrisanim u korporativnu mrežu.

Izloženost štetnim uticajima se komplikuje ukoliko je uređaj *jailbreak*-ovan (termin za uređaje sa iOS operativnim sistemom) ili *root*-ovan (termin za uređaje sa Android operativnim sistemom). Ovo su nazivi za procese kojima se na mobilnim uređajima onemogućavaju sigurnosne mere, dozvoljavajući da aplikacije sa bilo kog izvora budu instalirane na uređaju. Softveri za *jailbreak*-ovanje i *root*-ovanje uređaja su slobodno dostupni na Internetu.

Detekcija ovakvih uređaja je, kao što smo rekli, obavezna funkcionalnost EMM proizvoda, tako da je sva EMM rešenja poseduju. Takvim uređajima zatim može biti blokiran pristup resursima u korporativnoj mreži ili korisnici samo mogu biti upozoreni, zavisno opet od sigurnosne politike kompanije. S obzirom na prirodu njihovog dizajna, ne postoji mogućnost izveštavanja o *jailbreak*-ovanim i *root*-ovanim Black Berry ili Windows Phone mobilnim uređajima, tako da je ova opcija ograničena na Apple iOS i Google Android mobilne uređaje.

Već je pomenuto da EMM sistemi takođe omogućavaju da administratori prave bele i crne liste aplikacija, gde definišu koje aplikacije se mogu koristiti na mobilnim uređajima, a koje ne. Zajedno sa korišćenjem nekog od prilagođenih antivirus softvera, infekcija mobilnih uređaja malicioznim sadržajima može se svesti na minimum.

Zbog strožije kontrole mobilnih aplikacija, neke kompanije kreiraju svoje sopstvene *app store*-ove. Mnogi EMM proizvodi poseduju funkcionalnosti kojima se ovo omogućava. Pored kontrolisanja, distribucije i ažuriranja aplikacija, ovakvi korporativni *app store*-ovi mogu upravljati bilo kojim softverom licenciranim od strane kompanije.

Mobile device management (MDM), Mobile Aplication Management (MAM) i Mobile information management (MIM) predstavljaju evoluciju u upravljanju i merama bezbednosti korporativnog mobilnog sistema. Evoluciju koja pokušava da nađe balans između potreba kompanije da zaštiti svoje korporativne podatke i zahteva zaposlenih, odnosno korisnika koji mobilne uređaje koriste. IT profesionalci moraju dobro razumeti višestruku prirodu mobilnog računarstva pre osmišljavanja i primene pravila i procedura korišćenja mobilnih uređaja u korporativne svrhe. Takođe moraju razumeti i razmotriti međusobnu povezanost uređaja aplikacija i podataka.

Kao što vidimo, svaka komponenta EMM sistema se fokusira na različit segment mobilnog sistema. Međutim, da bi se postigao zadovoljavajući nivo sigurnosti korporativne IT infrastrukture, aplikacija i podataka, sigurnosna pravila moraju biti jasno definisana, a zatim primenjena i na nivou aplikacija, operativnih sistema, kao i na samim hardverskim uređajima. Ovo zahteva ozbiljnu koordinaciju i standardizaciju prilikom implementacije jednog ovako bitnog sistema.

2.4. Strategije razvoja EMM sistema u korporativnom oruženju

Vremenom su se izdvojile dve osnovne strategija razvoja mobilnih sistema u okviru kompanija čija se osnovna razlika ogleda u tome ko polaže vlasništvo nad mobilnim uređajem. To su strategije nazvane *Bring Your Own Device* (BYOD) i *Corporate-Owned Personal Enabled* (COPE).

BYOD (*Bring Your Own Device*) je najnovija EMM strategija, strategija koja će kako vreme bude odmicalo biti sinonim za implementaciju EMM sistema, ali nije jedina na raspolaganju. Ona podrazumeva da zaposleni koriste svoje sopstvene mobilne uređaje u korporativne svrhe, tj. da pristupaju resursima u korporativnoj mreži pomoću svojih sopstvenih uređaja. Mobilni uređaji su sada sveprisutni, pošto su korisnici brzo prepoznali benefite koje ovi uređaji nude u svakodnevnom poslu. EMM podrazumeva razumevanje rizika koje BYOD nosi sa sobom i primenu odgovarajućih tehnologija kako bi se podaci i infrastruktura u vlasništvu kompanije zaštitili od bilo kakvog zlonamernog uticaja.

Model *Corporate-Owned, Personally Enabled* (COPE), je nešto starija strategija razvoja mobilnih sistema u okviru različitih kompanija. Predstavlja alternativu za organizacije u kojima BYOD trend nje zaživeo. COPE ima za cilj da obezbedi benefite korišćenja mobilnih uređaja za izvršavanje poslovnih zadataka, ali na način koji olakšava IT administratorima upravljanje tim uređajima. Osnovna razlika izmedju ove dve strategije je da za razliku od BYOD-a, COPE se oslanja na mobilne uređaje koji su nabavljeni i u vlasništvu su same kompanije, ali su dati na korišćenje zaposlenim i za izvršavanje poslovnih zadataka i za korišćenje u privatne svrhe.

Međutim, kao i BYOD, i COPE ima svoje dobre i loše strane, tako da nije pogodan za implementaciju u bilo kom informacionom okruženju. U nastavku ćemo obraditi prednosti i nedostatke i jedne i druge strategije. Na osnovu karakteristika oba pristupa, kao i konkretnih korporativnih zahteva treba odrediti strategiju razvoja EMM sistema u informacionom sistemu kompanije.

BYOD program je učinio da korišćenje personalnih smartfona i tableta na poslu doživi ekspanziju. IT administratori, neki brže nego drugi, su shvatili da mogu kvalitetnije i produktivnije

da iskoriste svoje vreme, nego u borbi da personalne uređaje zaposlenih drže podalje od korporativne mreže. Oni su preduzeli korake da integrišu mobilne uređaje u korporativnu mrežu i time odu korak napred u podsticanju produktivnosti svojih zaposlenih, pri tom na njihovo opšte zadovoljstvo. BYOD može doneti značajne benefite u pogledu produktivnosti zaposlenih, zato što današnji mobilni uređaji i aplikacije obezbeđuju daleko bolje korisničko iskustvo nego li tradicionalni PC računari i monolitni korporativni softverski alati. Fleksibilnost koja je ovim omogućena zaposlenima, kao i činjenica da više nisu vezani za svoje radna mesta može povoljno uticati na motivisanost a samim tim i produktivnost.

Neke kompanije mogu naći motiv za ulazak u BYOD program u uštedi finansijskih sredstava. Međutim, ovo je redak slučaj. Ako malo dublje analiziramo, dolazimo do zaključka da takvo razmišljanje i ne pije vodu kao što se na prvi pogled čini. Možda izgleda primamljivo to da kompanija ne mora da nabavlja mobilne uređaje za svoje zaposlene već da oni to učine sami, ali održavanje i podrška za EMM sistem koji bi morao biti implementiran u jednoj ovakvoj strategiji zahteva mnogo veća ulaganja i troškove od COPE strategije. Tako da se odabir strategije za razvoj mobilnog sistema u kompaniji mora detaljno i zrelo razmotriti, uzimajući u obzir dugoročne planove kompanije po ovom pitanju.

Osobina koja definiše BYOD je deljena odgovornost. Korisnici mobilnih uređaja očekuju određeni stepen privatnosti i slobode u korišćenju mobilnih uređaja, ali oni takođe moraju biti svesni potrebe za zaštitom korporativnih podataka, aplikacija i cele mreže. Ključ je edukacija korisnika o jasnim i primenjenim pravilima korišćenja mobilnih uređaja. Organizacije čije su delatnosti na primer finansije ili zdravstvo posebno su svesni osetljivosti svojih podataka.

BYOD može takođe ograničiti ono što IT sektor jedne organizacije želi da postigne implementacijom EMM rešenja. Treba imati u vidu da zaposleni možda neće biti voljni da dopuste punu kontrolu nad svojim uređajima, što uključuje mogućnosti kao što su daljinsko brisanje sadržaja na uređaju ili lociranja uređaja. I uopšte sve funkcionalnosti MDM komponente EMM rešenja kao što su zahtevanje PIN-a i šifre, zabrana korišćenja *root*-ovanih i *jailbreak*-ovanih uređaja može na korisnike, tj. zaposlene ostaviti utisak ograničenja.

Zaposleni će razumno očekivati da kompanija vrši kontrolu bezbednosti onih uređaja koji su u njenom vlasništvu, a dati su mu na korišćenje i za poslovne kao i za privatne potrebe. Međutim, kada zaposleni koriste svoje sopstvene uređaje oni očekuju da imaju kontrolu nad njim. Zapravo, mnoge kompanije možda ne žele da imaju kontrolu nad ličnim mobilnim uređajima svojih zaposlenih, ali svakako i dalje žele da zaštite svoje korporativne podatke.

Jedan od načina da se balansiraju potrebe i interesi zaposlenih i kompanije je implementacija različitih delova EMM sistema koji imaju i različite sfere delovanja i kontrole. U slučaju BYOD modela mobilnih sistema potrebno je garantovati zaposlenima da mogu koristiti svoje lične mobilne uređaje za potrebe izvršavanja poslovnih zadataka, ali da će integritet njihovih privatnih podataka ostati očuvan.

Za razliku od MDM komponente MAM komponenta EMM rešenja ima manje strog pristup, dajući IT administratorima kontrolu samo nad korporativnim delom mobilnog uređaja, što je za zaposlene dosta prihvatljivije. Ali ukoliko su MDM funkcionalnosti obavezne što je često slučaj, onda BYOD program možda nije najbolje rešenje.

Isto tako kada imamo personalne mobilne uređaje i korporativnu kontrolu nad njima dolazimo do pitanja privatnosti i legalnosti. Sa strane administratora u IT sektoru korporacije to što imaju pristup privatnim sadržajima na mobilnom uređaju zaposlenih ne znači da je dozvoljeno da to zloupotrebe. Sa strane korisnika ne postoji uvek jasna granica između operacija koje se na uređaju

izvršavaju iz privatnih a koje iz poslovnih razloga. Stroga i dobro definisana BYOD politika može pomoći da se ovakvi problemi izbegnu na zadovoljstvo obe strane.

COPE model se razlikuje od drugih korporativnih programa za podršku mobilnih uređaja, po tome što on prepoznaje da se mobilni uređaj koristi i u poslovne i u privatne svrhe. Onaj deo uređaja što treba da bude pod kontrolom osoblja IT sektora to i jeste, sve ono što treba da bude upravljivo i dostupno u uređaju to i jeste, a sva ostala podešavanja zavise od korisnika tj. zaposlenog. Zbog toga što se uređaj nalazi u vlasništvu kompanije, a ne samog zaposlenog IT može biti uporniji i detaljniji u sprovođenju kontrole, upravljanja i garantovanja sigurnosti nad uređajem.

COPE model je lakši za administraciju i podršku od strane administratora. Razlog za to je što administratori mogu podesiti unapređene i predefinisane procese registracije, konfiguracije i instalacije različitih aplikacija, ne čekajući da zaposleni donesu svoje vlastite uređaje koji će tek onda biti konfigurisani. Na ovaj način administratori imaju manji obim posla, i nemaju osećaj kao da treba da administriraju svaki uređaj na svetu kao što je slučaj sa BYOD programom.

Kompanije mogu imati razne finansijske olakšice koristeći COPE model. Nabavka mobilnih uređaja na veliko od strane raznih provajdera mobilnih usluga, otplaćujući uređaje kroz plaćanje servisa koji se koriste, može biti odličan način za uštedu finansijskih sredstava.

IT i dalje mora biti veoma pažljiv u pogledu kontrole i privatnosti korisnika mobilnih uređaja. Nejasna linija između poslovnih i ličnih podataka i aplikacija na mobilnom uređaju veoma je izražena kod primene COPE modela. Ako se korisnici budu osećali kao da ih neko svo vreme špijunira onda strategija razvoja EMM sistema neće uspeti [6].

2.5. Scenariji zaštite mobilnih korporativnih sistema

Kao što smo već rekli mobilni uređaji predstavljaju obavezne alate u današnjem poslovanju koje zahteva veliku mobilnost zaposlenih, brzi pristup podacima i informacijama sa različitih lokacija. I dok današnji smartfoni i tableti omogućavaju zaposlenima veliku fleksibilnost u izvršavanju njihovih radnih zadataka, oni istovremeno otvaraju pitanja koja moraju biti uzeta u razmatranje od strane kompanije, a tiču se sigurnosti i privatnosti korporativnih podataka. Implementacija EMM proizvoda omogućava sa jedne strane zaposlenima u kompaniji da koriste benefite koje pružaju mobilni uređaji, da efikasno i produktivno izvršavaju svoje radne zadatke, a sa druge strane pomaže IT osoblju kompanije da zaštiti korporativne podatke i infrastrukturu kao mobilne uređaje od zlonamernog pristupa.

Postoje tri glavna scenarija zaštite mobilnih sistema kroz EMM rešenja i to su:

- zaštita podataka na mobilnim uređajima
- zaštita samih mobilnih sistema
- zaštita podataka prilikom razmene između mobilnih uređaja i korporativne mreže.

Ovde ćemo razmotriti nekoliko različitih scenarija u implementaciji EMM rešenja, koji su dati kao priimeri, kako bi lakše shvatili logiku kojom se kompanije vode prilikom uvođenja EMM rešenja u informacioni sistem. U konkretnoj implementaciji može se koristiti neki od ovih scenarija, ali najčešće je u pitanju kombinacija više različitih scenarija, kako bi se dostigle željene performanse i funkcionalnosti sistema.

2.5.1. Scenario 1 - zaštita podataka

Kao što možemo pretpostaviti, najveći motiv implementacije EMM rešenja u jednom korporativnom IT sistemu u stvari i jeste zaštita podataka. Razlog tome je što su današnji mobilni

uređaji postali postali stvarni računari sa svojim moćnim procesorima i velikim memorijskim kapacitetima za čuvanje i obradu podataka, takvi da kada se koriste u korporativnom okruženju imaju pristup istim podacima i aplikacijama kao i standardni PC računari i laptopovi. Sa tim na umu, kompanije moraju proširiti zaštitu podataka, primenjenu na nivou kompanije, na ove uređaje bez ograničavanja njihovoe fleksibilnosti prilikom korišćenja u korporativnom okruženju.

S tim u vezi, EMM vendori su razvili dva pristupa zaštite podataka na mobilnim uređajima. Prvi zasnovan na principu smeštanja podataka u tzv. kontejnere, gde su korporativni podaci, posebnim tehnikama, o kojima će kasnije biti više reči, razdvojeni od privatnih koji se nalaze na mobilnom uređaju. Drugi pristup u kome ne postoji kontejnerizacija podataka, odnosno ovaj vid logičke razdvojenosti na privatni i poslovni deo mobilnog uređaja.

i) Princip kontejnerizacije

Proizvodi namenjeni sigurnosti mobilnih uređaja koji primenjuju princip kontejnerizacije, odrediće malu particiju u memoriji mobilnog uređaja, ograničavajući sve korporativne podatke, aplikacije, kao i korporativnu komunikaciju na ovaj deo uređaja, tj. kontejner. Svi podaci i aplikacije u korporativnom delu uređaja su enkriptovani, i ukoliko nije drugačije konfigurisano sprečena je komunikacija aplikacija iz privatnog dela mobilnog uređaja sa onim iz korporativnog dela. Na ovaj način postiže se logička razdvojenost privatnih od korporativnih podataka, dodajući na ovaj način još jedan nivo zaštite podataka.

Prednost ovakvog pristupa je da u slučaju gubitka ili krađe mobilnog uređaja, kao i napuštanja kompanije od strane zaposlenog, administratori, putem EMM sistema koji omogućava udaljeno brisanje podataka, mogu sa datog uređaja ukloniti sve korporativne podatke. Na ovaj način se može izbeći da podaci izađu iz okvira same kompanije, i potencijalno budu zloupotrebljeni.

Nedostatak ovakvog pristupa je da krajnji korisnici često nemaju mogućnost da koriste aplikacije koje su navikli, kompanije nemaju fleksibilnost korišćenja prilagođenih i interno razvijenih aplkacija ili softvera. Da bi ovo bilo moguće, potrebna je saradnja EMM vendora sa onim ko kreira aplikaciju, kako bi se postiglo da taj softver uđe u enkriptovani deo mobilnog uređaja, tj. kontejner. Ovo se postiže integracijom SDK programskih kodova u programski kod same aplikacije, ili procesom pakovanja aplikacije, o čemu je već bilo više reči. I dok mnogi EMM vendori sarađuju sa programerima koji razvijaju softvere treba imati na umu da nije svaka aplikacija kompatibilna da bi se moglo obezbediti njeno pojavljivanje u kontejneru na mobilnom uređaju.

ii) Princip bez kontejnerizacije

Pristup zasnovan na principu bez kontejnerizacije omogućava krajnjim korisnicima da koriste mobilne uređaje bez ograničenja sa mogućnošću korišćenja tradicionalnih aplikacija. Dakle ovaj metod obezbeđivanja sigurnosti za mobilne uređaje, za razliku od kontejnerizacije, pruža korisnicima fleksibilnost korišćenja aplikacija koje su njima familijarnije, i omogućava lakši pristup podacima iz nezavisnih (*third-party*) softvera nego što je to slučaj kod kontejnerizacije podataka na mobilnim uređajima. Ovo važi i za poslovne i za privatne podatke na uređaju. Zavisno od kreiranih korporativnih pravila i politike, konfiguracija uređaja može biti takva da obezbedi zaključavanje korporativnih aplikacija ali i/ili privatnih aplikacija.

Ovakav pristup, iako preuzima primat nad pristupom sa kontejnarizacijom, treba da bude detaljno razmotren od strane IT administratora.

Takođe postoje opcije za korišćenje alata koji sprečavaju gubitak podataka sa uređaja koji nisu podlegli kontejnerizaciji. Ovo omogućava proveru i zaštitu podataka pre nego što oni potencijalno napuste mobilni uređaj.

Zaštita podataka na mobilnim uređajima je od krucijalnog značaja. Samim tim treba da bude najvažniji uslov prilikom odluke o nabavci i implementaciji EMM rešenja.

2.5.2. Scenario 2 - zaštita samih mobilnih uređaja

Pored zaštite podataka važno je i pitanje zaštite samih hardverskih mobilnih uređaja, jer ako to nije slučaj može doći do raznih štetnih uticaja na samu mrežnu infrastrukturu kao i do kompromitovanja podataka u korporativnom sistemu.

i) Detekcija jailbreak-ovanih/root-ovanih uređaja

Većina EMM rešenja mogu upozoriti administratore ukoliko korisnik pokušava da koristi *jailbreak*-ovan/*root*-ovan smartfon ili tablet. Ovakvi uređaji omogućavaju korisnicima da u sistemu izvršavaju funkcije (kao što su pristup sa administratorskim pravima, skidanje i instalacija aplikacija sa spoljašnjih *app store*-ova, kao i mnoge druge) koje nisu predviđene od strane proizvođača ili odobrene sigurnosnom politikom kompanije. Ovo, naravno, ne mora uvek biti loše, ali ovakvi uređaji otvaraju nove rizike za sigurnost korporativne mreže, tako da je najbolje ne ostavljati mogućnost da korisnici *root*-uju svoje mobilne uređaje.

ii) Korišćenje PIN-a i lozinke

Prva linija zaštite koja je zahtevana za svaki uređaj je zaštita šifrom, tj. lozinkom. Postojanje EMM sigurnosne polise koja se primenjuje na uređaju, a zahteva postojanje PIN-a ili šifre je dobar način osiguravanja sistema od neautorizovanog pristupa osobe koja bi mogla da ukrade mobilni uređaj ili ga nađe ukoliko dođe do njegovog gubitka. Iako se ovo čini kao beznačajan doprinos sigurnosti, primena PIN-a ili lozinke na mobilnom uređaju bi trebalo da bude obavezna.

iii) Daljinsko brisanje

Opcija daljinskog brisanja sadržaja sa mobilnih uređaja može biti veoma značajna kada dođe do situacije da uređaj više nije u posedu zakonskog vlasnika. Ovo osigurava da ništa na mobilnom uređaju više nije dostupno, što ne predstavlja problem imajući u vidu da je vrednost korporativnih podataka mnogo veća od vrednosti samog hardverskog urđaja.

iv) Promene na operativnom sistemu i aplikacijama

Jednostavnim EMM polisama koje će biti primenjene na uređaje, administratori mogu ograničiti aplikacije koje mogu biti instalirane kao i promene na operativnom sistemu uređaja koje se mogu izvoditi od strane bilo korisnika telefona bilo nekog neatorizovanog pristupa. Primer je polisa koja dozvoljava instalaciju samo onih aplikacija koje se nalaze na beloj (*white*) listi, pazeći pri tom na uređajima na kojima imaju kamere one budu isključene. Ovo kompanijama garantuje da na mobilnim uređajima neće biti instalirane aplikacije koje mogu kompromitovati podatke na uređaju. Takođe čuva na mobilnim uređajima osnovne postavke operativnih sistema što olakšava upravljanje, održavanje i administraciju celog sistema mobilnih uređaja. Ovaj nivo kontrole aplikacija i operativnog sistema se mora imati kada je u pitanju distribucija mobilnih uređaja krajnjim korisnicima.

v) Enkripcija mobilnih uređaja

Kompanije bi trebale da enkriptuju sve mobilne uređaje koji sadrže važne korporativne podatke. EMM proizvod može pomoći da se ovo izvrši forsiranjem enkripcije na svim podržanim smartfonima i tabletima, slično načinu enkriptovanja celog diska što se radi za desktop i laptop računare. Enkripcija štiti sam mobilni uređaj kao i podatke koji se na njemu čuvaju. Važno je da se ova opcija omogući na svim uređajima, čak i u kompanijama koje imaju implementiran EMM proizvod zasnovan na principu kontejnerizacije mobilnih uređaja.

2.5.3. Scenario 3 – Zaštita konekcije mobilnih uređaja

Onda kada smo obezbedili zaštitu samih uređaja kao i podataka i aplikacija koji su na njima pohranjeni vreme je da se posvetimo i obezbeđivanju sigurne konekcije mobilnog uređaja. Ovde se razmatraju načini kako EMM rešenja mogu pomoći da se obezbedi sigurnost svih konekcija i sesija koje su uspostavljene između mobilnih uređaja i resursa u korporativnoj mreži.

Sa implementiranim EMM rešenjem kompanije mogu smanjiti rizik uspostavljanja nesigurne komunikacije i to sprečavajući nezavisno menjanje konfiguracije mobilnih uređaja čime bi se onemogućile neke sigurnosne funkcije uređaja, kao i omogućavanjem određenih funkcija samog rešenja, namenjenih za ovu svrhu. Jedna od funkcionalnosti je omogućavanje opcije VPN konekcije na mobilnim uređajima kako bi mogao da sigurno komunicira sa resursima u internoj mreži kompanije.

Dodatno postoji mnoštvo situacija u kojima je zaposlenima potreban pristup podacima ili servisima u internoj mreži kompanije. Umesto da dozvoli nesigurnu konekciju, EMM rešenja pružaju mogućnost da administratori zahtevaju pristup putem konekcije kroz sigurnu VPN konekciju.

Drugi metod za zaštitu pristupa korporativnoj mreži podrazumeva restrikciju nesigurnog pristupa ograničavanjem SSID-ova (*service set indentifier)* koje mobilni uređaji mogu koristiti. SSID je sekvenca karaktera koja jednoznačno određuje bežičnu lokalnu mrežu (WLAN). Tako, na primer, administratori mogu kreirati polisu koja će se primenjivati na mobilne uređaje, a zahtevaće da uvek kada se uređaj nalazi u korporativnoj bežičnoj mreži mora koristiti nju, umesto neke druge potencijalno nesigurne konekcije, bez obzira na kvalitet signala.

Mogućnost implementacije internih sertifikata u mobilnim uređajima, koji su izdati od strane korporativnog sertifikacionog tela, tj. servera je takođe preporučljivo i poželjno. Ovim putem se dobija još jedan dodatni nivo zaštite i autentifikacije u mobilnom sistemu.

Postoje i EMM opcije koje pružaju mogućnost ograničevanja pristupa određenim veb sajtovima. Naziv ove tehnologije je sigurno veb pretraživanje (*Secure Web browsing*). Ova tehnologija pruža korisnicima mogućnost internet pretraživanja tako što normalno uspostavlja konekciju sa veb proksi serverom u korporativnoj mreži, omogućujući sigurnu internet konekciju za mobilne uređaje. Na ovaj način, korisnik koristeći mobilni uređaj uspostavlja internet konekciju kao bilo koji drugi uređaj u internoj mreži kompanije. Drugim rečima, posmatrajući mobilne uređaje kao proširenje korporativne mreže, veoma je važno imati iste veb polise primenjene na njih kao i na ostale računare u korporativnoj mreži, što će omogućiti konzistentnu bezbednost kao i zadovoljstvo korisnika prilikom korišćenja internet servisa.

Na kraju, neka EMM rešenja uključuju u svoju ponudu funkcionalnost nazvanu *geofencing* koja dozvoljava moblnim uređajima konekciju ka korporativnoj mreži samo ako se nalaze okviru određene geografske lokacije. Ova opcija može biti veoma ograničavajuća za zaposlene koji puno putuju noseći sa sobom svoje mobilne uređaje, i primenu ove funkcionalnosti u ovom slučaju teba posebno detaljno razmotriti. Ali u slučaju uređaja koji ne bi trebalo da napuste određenu lokaciju, kao što su mobilni sistemi namenjeni mestima prodaje (*mobile POS*), ova funkcionalnost može biti veoma korisna. U slučaju da ovakav uređaj izađe iz okvira neke predefinisane lokacije, primenom korporativne polise, on će postati neupotrebljiv.

Mobilni uređaji su danas de fakto poslovni alat za skoro svakog zapslenog. Zbog ovog talasa popularnosti, kompanije moraju zaštiti svoje korporativne podatke, sistem i mrežu, a takođe i same mobilne uređaje kao i konekcije i sesije između tih uređaja i ostatka korporativne mreže. Ovim dolazimo do zaključka da je implementacija EMM rešenja, u svaku kompaniju koja ima ozbiljne

namere da omogući svojim zaposlenima prednosti korišćenja mobilnih uređaja i samim tim povećanje produktivnosti, apsolutno potrebna [7].

2.6. Integracija mobilnih aplikacija u EMM sistem

Kompanije isporučuju aplikacije na mobilne uređaje, sa ciljem da svojim zaposlenima omoguće punu fleksibilnost rada sa bilo koje lokacije na kojoj se trenutno nalaze. Ova mogućnost da se korisnicima omogući korišćenje CRM (*Customer Relationship Management*) aplikacija, posebnih aplikacija koje su razvijene interno u kompaniji, ili bilo koje aplikacije koju bi korisnici želeli da koriste je važno pitanje koje treba postaviti prilikom implementacije EMM rešenja kao i prilikom izbora nekog od rešenja sa tržišta.

Bilo koje implementirano EMM rešenje bi trebalo da omogući IT administratorima u kompaniji mogućnost upravljanja, integrisanja i primene korporativnih polisa na sve mobilne aplikacije koje se koriste unutar kompanije.

Na primer ako u okviru kompanije postoji prodajni tim nekog proizvoda kome je potreban pristup nekoj CRM aplikaciji, admisnistratori treba da imaju mogućnost da tu aplikaciju stave na tzv. belu (*white*) listu i zatim da je isporuče na mobilne uređaje članova ovog tima. Ovo će dalje omogućiti veću kontrolu nad uređajem kao i aplikacijom kojuće članovi tima koristiti.

Pojedini EMM vendori, međutim, imaju partnerstva sa velikim, svetskim firmama koje razvijaju aplikacije, tako da u međusobnoj saradnji, u svojim rešenjima nude veću fleksibilnost i sigurnost prilikom korišćenja takvih aplikacija. Ovakve aplikacije su kreirane tako da u EMM sistemu smanje sigurnosne rizike što je više moguće.

Ovde možemo imati aplikacije koje kompanije jednostavno ne žele da imaju na mobilnim uređajima svojih zaposlenih. EMM rešenja omogućavaju izveštaje sa svih mobilnih uređaja u EMM sistemu, o tome kojim sve mobilnim aplikacijama uređaji raspolažu. Takođe nude uvid da li na uređajima postoje neželjene, tj. nedozvoljene aplikacije čija se instalacija kosi sa korporativnim polisama i mobilnom politikom. Postoji opcija zabrane („zaključavanja“) onih aplikacija koje nisu poželjne na mobilnim uređajima, kao i pravljenja bele liste na kojoj će se nalaziti sve one aplikacije dozvoljene za insaliranje i korišćenje.

Mobilne aplikacije i jesu razlog rapidnog razvoja i korišćenja smartfona i tableta kao neopodnog poslovnog alata. Integracija poslovnih aplikacija u EMM rešenje ne samo da obezbeđuje isporuku ovih aplikacija na mobilne uređaje zaposlenih, već i njihovu sigurnu i efikasnu primenu prilikom obavljanja radnih zadataka.

2.7. Arhitektura EMM rešenja

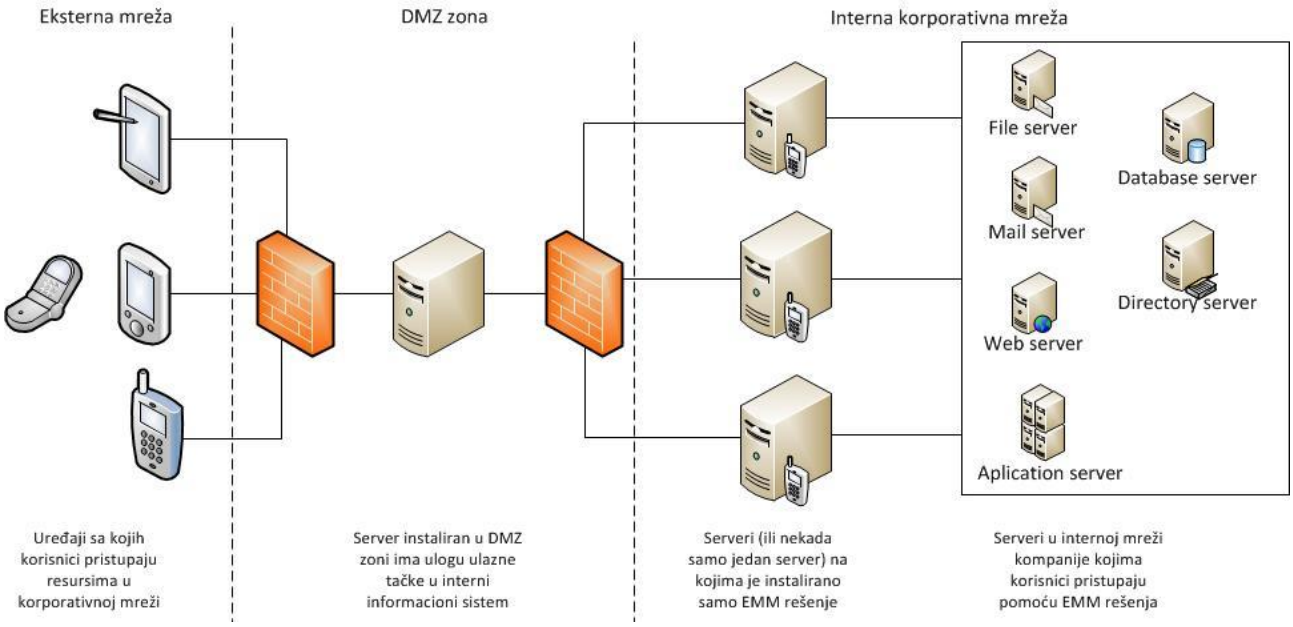
Arhitektura svih EMM rešenja prati određeni šablon. Komponente sistema su podeljene na tri vrste. One koje se nalaze u eksternoj mreži, tj. na korisničkim uređajima, zatim komponente koje se nalaze u *DeMilitarized Zone* (DMZ) zoni kompanije, i na kraju one koje se nalaze u internoj mreži kompanije.

Komponenta koja se nalazi na krajnjim korisničkim uređajima je obično agent aplikacija koju korisnik koristi prilikom pristupa resursima u internoj mreži kompanije.

Komponenta u DMZ zoni predstavlja ulaznu tačku mobilnih korisnika u korporativnu mrežu. Sa jedne strane ova komponenta mora biti javno objavljena i vidljiva sa Internet-a, dok sa druge strane mora imati privatne IP adrese koje pripadaju internoj mreži, i koje imaju pristup komponentama koje su instalirane u internoj zoni informacionog sistema.

Komponente u internoj mreži predstavljaju sama rešenja, koja pružaju MDM, MAM i MIM funkcionalnosti. Ovo su obično softveri koji se instaliraju ili na specifičnom hardveru ili na bilo kojem serveru u mreži kompanije. Instalacija može biti ili na postojećoj virtuelnoj infrastrukturi kompanije, ili na fizičkim serverima. Ove komponente komuniciraju, sa jedne strane sa komponentom u DMZ zoni, koja kao što smo rekli predstavlja gejtvej za mobilne korisnike, a sa druge strane komunicira sa raznim servisima u internoj mreži kao što su LDAP (*Lightweight Directory Access Protokol*) servis, DNS (*Domain Name Server*), sistemima za pohranu podataka, serverima elektronske pošte, aplikacijama koje su hostovane u internoj mreži i td.

Šematski prikaz opšte arhitekture EMM rešenja može se videti na Slici 2.8.1.



Slika 2.8.1. Arhitektura EMM rešenja u korporativnom okruženju

2.8. Implementacija EMM rešenja

Najčešći način implementacije EMM rešenja je instalacija odgovarajućeg sofvera na virtuelnoj infrastrukturi kompanije, ali će takođe skoro svi vendori ponuditi i hardverski bazirana rešenja ukoliko je to traženo ili jednostavno neophodno iz nekog razloga. Takođe sve veći broj vendora pruža ovaj servis kroz cloud.

Virtuelni imidži se obično isporučuju u obe varijante, OVA (*Open Virtual Appliance*) ili kao OVF (*Open Virtualization Format*), fajl formata, i ovo su potpuno podržani operativni sistemi tako da dozvoljavaju kompanijama da importuju softver u njihova već postojeća virtuena okruženja (Hyper-V, VMware, i drugi). Ovi virtuelni imidži omogućavaju veoma brzu, efikasnu i fleksibilnu instalaciju EMM softvera.

Postoje naravno EMM kupci koji nemaju instalirano virtuelno okruženje, ili žele da imaju EMM sistem koji radi na izolovanim hardverskim komponentama zbog pitanja performansi i sigurnosti sistema. U ovim slučajevima EMM vendori isporučuju specijalni EMM sistem kupcu sa detaljnim instrukcijama kako da se konfigurišu sve hardverske komponente sistema.

Implementacija EMM sistema na hardverskoj infrastrukturi može biti previše glomazna i zahtevna za neke kupce. Veliki broj EMM vendora počinje da nudi njihove proizvode na novi

način, *as software as a service* (SaaS) u cloudu. Ovakva razvojna opcija ima rastući trend, posebno među onim kompanijama koje žele EMM rešenje, ali imaju limitirane resurse.

Jednom kada je EMM proizvod instaliran u mreži, bilo na virtuelnom okruženju, na specifičnom hardveru ili u cloud-u, administratori moraju imati plan implementacije imajući u vidu tipove mobilnih uređaja koji će se u sistemu pojavljivati. Postupna implementacija rešenja kroz uređaje koji će participirati u EMM sistemu je pametan izbor, posebno imajući u vidu potrebnu edukaciju i korisnika, ali i administratora koji će koristiti novo rešenje.

Kako sva EMM rešenja omogućavaju korisnicima preuzimanje aplikacija bilo sa Google Play-a ili Apple App Store-a, kada se korisnik prvi put registruje u sistem, dobija mail ili tekstualnu poruku koja sadrži uputstva za instalaciju aplikacija. Kada zatim preuzme (*download*-uje) aplikaciju i autentifikuje se, najčešće kroz LDAP ili *one-time passphrase*, prekonfigurisane korporativne polise se primenjuju na mobilnom uređaju. Od ovog trenutka mobilni uređaj se nalazi pod kontrolom EMM sistema, i može biti administriran od strane osoblja IT sektora. Registracija uređaja u EMM sistem, primena različitih korporativnih polisa, kao i načini upravljanja i zaštite uređaja biće detaljno obrađeni prilikom opisa konkretne implementacije EMM rešenja.

Kao i kod implementacije ostalih bezbednosnih uređaja u korporativni informacioni sistem i kod EMM rešenja se u razmatranje moraju uzeti razni troškovi. Najveće troškove predstavljaju u stvari cena samog EMM rešenja, potencijalno specifični hardver na kom će rešenje biti instalirano, zatim inicijalna podrška vendora prilikom implementacije rešenja i testiranje rada rešenja. Manji troškovi odlaze na dodatnu podršku vendora posle implementacije sistema, a u slučaju njegovog nepravilnog rada ili nekih nepredviđenih incidenata. U obzir treba uzeti i edukaciju administratora koja je nekad poseban trošak, kao i moguću potrebu zaposlenja novih ljudi u cilju administriranja novog sistema u IT sistemu kompanije [8].

3. PREGLED NAJZNAČAJNIJIH REŠENJA

U ovom poglavlju napravićemo kratak pregled najznačajnijih EMM rešenja ponuđenih na tržištu. Kao referencu uzeli smo Gartnerov magični kvadrant. Gartner je svetski poznata i cenjena analitička kuća, koja se bavi analizom različitih rešenja iz oblasti informacionih i komunikacionih tehnologija. Mi ćemo ovde obraditi samo rešenja koja je Gartner prepoznao kao lidere među EMM proizvodima, tj. kao najznačajnije predstavnike ove tehnologije.

Pre nego što damo više reči o konkretnim EMM rešenjima sa osvrtom na njihove prednosti i mane, pomenućemo kriterijume po kojima su rešenja uopšte uključena u Gartnerov magični kvadrant.

3.1. Gartnerovi kriterijumi

S obzirom da više od 100 vendora nudi EMM funkcionalnosti, Gartner je definisao takozvane uključujuće kriterijume koje svaki vendor mora ispuniti da bi se našao u magičnom kvadrantu. Ovi kriterijumi predstavljaju kombinaciju poslovnih i tehničkih performansi. Ti kriterijumi su:

- Vendor mora imati najmanje 12 miliona američkih dolara prihoda od svog EMM rešenja
- Vendor mora imati najmanje pet referenci od organizacija koje koriste njegov EMM proizvod
- Vendorsko EMM rešenje mora pružati poršku za mobilne uređaje sa iOS, Android i Windows Phone operativnim sistemima
- Vendorsko rešenje mora uključivati funkcionalnosti MDM, MAM i MIM rešenja (zahteva da MAM rešenje poseduje funkcionalnost pakovanja aplikacija (*wrapping*), ne samo funkcionalnost kontejnerizacije)

Većina EMM proizvoda nudi još funkconalnosti pored ovih koje su već navedene. Neke od njih su razmotrene kao opcione i rešenja ih ne moraju posedovati da bi bila uključena u poređenje. Na primer:

- Napredne MAM funkcionalnosti koje obezbeđuju upravljanje PIM (*Personal Information Manager*)-ovima, brauzerima i drugim aplikacijama
- Podrška za MAC OS X i Windows operativne sisteme
- Analitiku mobilnog sistema što bi bilo od koristi prilikom razumevanja trendova iskorišćenosti sistema i olakšalo otklanjanje različitih incidentnih situacija
- Zaštitu podataka na nivou dokumenta, što bi omogućilo zaštitu podataka korišćenih ili kreiranih na mobilnim uređajima
- *Mobile identity* funkcionalnost, kao i mogućnost *single sign-on* (koja podrazumeva autentifikaciju na sistem samo prilikom prvog pristupa) na mobilnim uređajima, zatim autentifikacija prilikom pristupa korporativnoj mreži razmenom sertifikata, „kontekstulana autentifikacija“ na osnovu dinamičkih uslova kao što su vreme ili lokacija

Rešenja velikog broja vendora su razmatrana od strane Gartner-a, ali se nisu našli u magičnom kvadrantu, jer ne ispunjavaju neki od obaveznih kriterijuma, bilo poslovne ili tehničke prirode. Na slici 3.1.1 možemo videti grafički prikaz Gartnerovog magičnog kvadranta, a mi ćemo se, kao što smo već rekli, fokusirati na one vendore čija su rešenja označena kao lideri u EMM funkcionalnostima.

Slika 3.1.1. Gartnerov magični kvadrant

Kao što vidimo na slici 3.1.1 lideri među vendorima su Airwatch by VMware, Mobilelron, IBM, Good Tehnology i Citrix. Pogledajmo kratak pregled njihovih karakteristika, prednosti kao i nedostataka prepoznatih od strane Gartner-a.

3.2. Pregled rešenja

3.2.1. Airwatch by VMware

Posle nastanka Airwatch-a kao akvizicije VMware-a u februaru 2014, Airwatch postaje deo *End-User Computing* biznis jedinice, ali uglavnom posluje kao nezavisan entitet. Ovo počinje da se menja, kada Airwatch počinje da se integriše sa različitim VMware tehnologijama, najznačajniji među njima su WMware-ov pristupni menadžment i software-defined mrežni proizvodi. Airwatch-

ova ponuda ima veliki broj EMM funkcionalnosti, i kao rezultat toga Airwatch se često pojavljuje u Gartnerovim klijentskim listama gde se nalaze lideri među EMM vendorima. Ranije, Airwatch je bio zatvoren sistem sa ograničenom podrškom za *third-party* nezavisne softverske vendore (ISV-*Indepedent Software Vendor)* mobilnih aplikacija. Međutim, ovo se menja pod uticajem Vmware-a koji razvija veliki broj aplikacija koje su sada direktno integrisane u EMM rešenje. Gartner je svestan periodičnih problema u vezi kvaliteta Airwatch-ovog rešenja, ali ovo verovatno dolazi kao rezultat pokušaja da se brzo obezbedi široka paleta funkcionalnosti koje razne kompanije sve češće zahtevaju. Airwatch je podesan za organizacije koje zahtevaju implementaciju velikog broja EMM funkcionalnosti na velikom broju različitih platformi.

i) Prednosti rešenja

- Airwatch poseduje karakteristiku velike skalabilnosti i implementacije kroz različite platforme mobilnih uređaja (*most vertical markets).*
- Administrativna konzola, koja je jedna od najlakših za korišćenje i koja, poseduje ugrađene video instrukcije, linkove i wizarde kao pristup koji će, administratorima koji tek počinju da se bave ovom tehnologijom, omogućiti da u kratkom periodu savladaju korišćenje rešenja i samim tim dostignu što veću produktivnost.
- Airwatch nastavlja sa uvođenjem novih inovacija i podrškom za sve vrste operativnih sistema na mobilnim uređajima, kao i mnoge aplikacije sa javnih App Store-ova.

ii) Nedostaci rešenja

- Žalbe korisnika se odnose na nedostatke Inbox-a email aplikacije što uzrokuje da korisnici koriste *third-party* rešenja za *Personal Information Manager* (PIM). Airwatch radi na poboljšanju performansi Inbox-a svoje e-mail aplikacije kako bi se ovaj problem što pre prevazišao.
- Infrastrukturne komponente su bazirane na Windows-u, SQL Server-u i Linux-u, praveći na taj način dodatni posao administratorima koji je uporediv sa ostalim rešenjima ovog tipa.
- Stabilnost rešenja nastavlja da bude pitanje na kom treba raditi. Gartner-ovi klijenti su u poslednje vreme izveštavali o nekoliko problema i na strani administrativne konzole i na strani agenta na mobilnim uređajima.

3.2.2. Citrix

U Januaru 2015, Citrix je predstavio verziju 10 njihovog XenMobile proizvoda, što je predstavljalo značajan korak ka uprošćavanju arhitekture EMM rešenja, i unificiranje MDM i MAM konzole. Dodatno XenMobile sadrži i *self-service* portal kao i podršku za Android for Work. Share File, Citrix-ov MIM proizvod, ima sve funkcionalnosti EFSS (*Enterprise File Synchronization and Sharing*) proizvoda, uključen je u XenMobile Enterprise i smatra se jednim od boljih rešenja na tržištu. Citrix rešenje je pogodno za organizacije koje žele svojim zaposlenim i korisnicima da obezbede sigurno poslovno okruženje uključujući Windows, Web i mobilne aplikacije, kao i za organizacije koje koriste tehnologije kao što su XenApp, XenDesktop i NetScaler.

i) Prednosti rešenja

- Citrix dobija visoku ocenu za korisničko iskustvo i doživljaj. WorxMail (Citrix-ov sigurni PIM proizvod, tj. mail agent, aplikacija) sadrži kalendar sa nedeljnim pregledom, podržava zip fajlove i ostale nove funkcionalnosti uključene u verziju 10.
- Citrix-ov Share File ostaje jedan od najmoćnijih MIM rešenja među EMM vendorima.

- Citrix obezbeđuje integrisano korišćenje između virtuelnih Windows aplikacija i ostalih mobilnih aplikacija.

ii) Mane rešenja

- Iako se rešenje sa razlogom prodaje veoma dobro, Gartner još uvek nije pronašao dovoljan broj kupaca koji trenutno imaju velika okruženja (više od 10000 uređaja u sistemu), a koji bi poslužili kao referenca.
- XenMobile 10 konzola je odvojena od NetScaler-a i File Share-a. I dok NetScaler i File Share ne zahtevaju preveliki posao oko svakodnevne administracije, XenMobile administarcija je više zahtevna i manje prilagodljiva. Implementacija ovog rešenja je takođe mnogo zahtevniji projekat za kompanije koje imaju implementiran NetScaler.
- Citrix je razvio alat za *upgrade*, koji treba da pojednostavi migraciju sa verzije 9 na verziju 10, u aprilu 2015. Međutim, alat je namenjen samo za migraciju MDM instance EMM rešenja, dok je Citrix najavio razvoj sličnog alata za migraciju i za MAM i MDM-plus-MAM instance kasnije u 2015 godini.

3.2.3. IBM

IBM je rebrendirao MaaS360 u "MobileFirst Protect" 2015. godine da bi svrstao EMM u svoju IBM MobileFirst strategiju. MobileFirst Protect EMM može upravljati uređajima koji rade na tri popularna operativna sistema: iOS, Android i Windows phone sa dodatkom radnih stanica baziranih na Windows 7/8 i MAC OS X. MobileFirst Protect je deo "Secure and Manage" (Obezbedi i upravljaj) prakse, koja reprezentuje drugu od četiri oblasti prakse u MobileFirst portfoliu, ostali su "Build" alat za razvoj i testiranje mobilnih aplikacija, "Engage" alat za analiziranje i optimizovanje korisničkog interfejsa, i "Transform" alat za pomoć u kreiranju mobilnih biznis modela. MobileFirst Protect je odgovarajuće rešenje za organizacije koje traže rešenje koje je lako za implemntaciju, kao i za one koji su zainteresovani za širu primenu IBM MobileFirst strategije.

i) Prednosti

- IBM-ova razvijena multiprocesorska arhitektura je najbolja u klasi rešenja koja podrazumevaju implementaciju u cloud-u među svim rangiranim EMM vendorima. Ona podrazumeva lako razdvajanje pristupa za korisnike, kao i razdvajanje po različitim nivoima nadležnosti od administratora do Help Desk-a.
- Kupci koji su uzeti kao referenca pohvalili su rešenje kao veoma lako za implementaciju. Instalacija može biti unapred pripremljena kako bi se ispunile specifične potrebe kupca proizvoda, a postoje detaljni tutorijali koji su dostupni za individualne korisnike.
- MobileFirst Protect obezbeđuje robustan i obiman monitoring uređaja kao i sistem praćenja, koji uključuje mogućnost korišćenja selektivnog obaveštavanja u odnosu na geografsku poziciju.

ii) Mane

- Korišćenje MAM komponente ovog rešenja (koja uključuje pakovanje aplikacija kao I kontejnerizaciju aplikacija koristeći SDK), je retko po istraživanju Gartnera.
- Zapisi uređaja koji su izbačeni iz upotrebe ostaju neko vreme u sistemu, što može dovesti do problema u sinhronizaciji podataka između mobilnog gejtveja i MobileFirstProtect konzole.

- Ovo rešenje zaostaje za drugim proizvodima u nekim oblastima, posebno zbog nedostatka sertifikata za mobilne aplikacije (koji su trenutno u fazi razvijanja), nedostatka podrške za SAML, kao i limitiranih mogućnosti aplikativne analize.
- Interferencija je minimalna, ali korisnici imaju osećaj „ispadanja“ servisa.

3.2.4. Mobilelron

Mobilelron je jedan od nekoliko *stand-alone* EMM vendora, i on se suočava sa izazovom sve većih korporativnih IT infrastruktura. Kompanija nastavlja da beleži rast broja korisnika što prati sve veći nivo sofisticiranosti njenog EMM rešenja. Mobilelron-ova strategija je nastaviti sa omogućavanjem „otvorenog ekosistema“ mobilnih uređaja i mobilnih aplikacija dok se zaštita pristupa i zaštita informacija implementira sa serverske strane, odnosno sa strane korporativnog sistema, a ne uređaja. Ova strategija može izazvati dodatne troškove, kao i povećati kompleksnost za korisnike koji žele *single-vendor* rešenja za EMM zajedno sa ostalim relevantnim mobilnim proizvodima, kao što su EFSS (*Enterprise File Synchronization and Sharing*) i softveri koji štite mobilni sistem od štetnih sadržaja (antivirus i antimalware). Mobilelron nastavlja da dobija dobre ocene za performanse skalabilnosti, takvih da je moguće dodavati stotine pa čak i hiljade uređaja u sistem bez, ili sa veoma malim problemima u arhitekturi. Organizacije koje žele robusna i obimna EMM rešenja, posebno one sa željom da obezbede širok spektar mobilnih aplikacija, treba da razmotre mogućnost implementacije ovog rešenja.

i) Prednosti

- Mobilelron-ov MIM proizvod, Docs@Work, može enkriptovati i brisati fajlove, omogućavajući organizacijama da zaštite pojedinačne fajlove čak i kada se oni nalaze pohranjeni na memorijskim jedinicama koje nisu pod nadležnošću sistema.
- MobileIron-ov MAM product, AppConnect, ima dobru kompatibilnost sa širokom lepezom MADP (*Mobile Application Development Platform*) alata.
- Mobilelron ima veoma pozitivne reakcije svojih korisnika na mogućnosti njegovog sertifikacionog menadžmenta, podršku za veliki broj aplikacija koje se preuzimaju sa javnih *app store*-ova kao i mogućnost *single sign-on* prilikom pristupa u korporativni sistem.

ii) Mane

- MobileIron-ova infrastruktura je u stvari bazirana na hardveru, tj. ima svoj poseban hardver na kom je samo rešenje implementirano, pa je monitoring ovog sistema teže implementirati u odnosu na neke od njegovih konkurenata.
- MobileIron ima SaaS verziju rešenja (implementiranje u cloud-u) kao i *on-premises* (implementacija u data centru kompanije) verziju, i ne postoji mogućnost povezivanja ova dva načina implementacije.
- Izveštavanje je izazov kod ovog rešenja, naročito kreiranje izveštaja sa posebnim uslovima kao i njihovo vremensko zakazivanje.

3.2.5. Good Technology

Good Technology je izbacio Good Work, naslednika Good for Enterprise PIM klijenta, 2014. godine. Good Work je napravljen na Good Dynamics Secure Mobility Platform-i, nasledivši sigurnosne i funkcionalne performanse ove platforme, kao što su *single sign-on*, multifaktorska autentifikacija, kao i integraciju procesa rada. Izvedena tranzicija sa *legacy* Good for Enterprise i AppCentral proizvoda na trenutni Good Work and Good Dynamics proizvod, izazvala je zbunjenost

kod korisnika, najviše zbog toga što sadašnji proizvod još uvek ne podržava sve mogućnosti *legacy* proizvoda. U Oktobru 2014., Good je nabavio Macheen, aplikaciju smeštenu u cloud-u koja omogućuje povezivanje uređaja sa korporativnom mrežom, tj. predstavlja gejtvej za mobilne uređaje.

Good Technology EMM je odgovarajuće rešenje za organizacije sa strogim sigurnosnim zahtevima, kao na primer finansijske i zdravstvene institucije, ili pak one sa velikim planovima za razvijanje mobilnih aplikacija, koje mogu imati razne pogodnosti od širokog spektra mogućnosti koje garantuje Good Dynamics SDK.

i) Prednosti

- Good Tehnology PIM funkcionalnost je najnaprednija među rešenjima ovog tipa EMM vendora, uključuje funkcionalnosti kao što su: *mail push notifications*, za operativne sisteme iOS/Android/Windows, informacije o prisustvu uređaja u sistemu, napredna pretraživanja, ili istoriju kontakata.
- Ovo rešenja ima performanse servisnog menadžmenta među najboljim u svojoj klasi, sa moćnim alatima za izveštavanje koji u velikoj meri olakšavaju udaljenu podršku korisnicima.
- Good Dynamics platforma je evoulirala sa platforme čiji je fokus pomeren sa opštih sigurnosnih funkcionalnosti na prikupljanje SDK biblioteka koje će biti primamljive kompanijama koje razvijaju svoje sopstvene aplikacije. Mogućnosti razdvajanja podataka, koje nudi ovo rešenje, je obavezno za implementaciju u BYOD (*Bring Your Own Device*) okruženjima.

ii) Mane

- Good Work platforma je novo rešenje i ima veliki broj ograničenja za uređaje koji rade na Android, iOS i Windows Phone operativnim sistemima.
- Trenutni primarni mehanizam grupisanja je kroz grupe korisnika, međutim, ovo ne obezbeđuje kreiranje grupa na osnovu hardverskih ili softverskih karakteristika uređaja, što je svakako potrebno.
- Ovo rešenje zaostaje za konkurencijom u mnogim MDM funkcionalnostima za svaki od operativnih sistema na kojima rade mobilni uređaji, bilo da je to Android, bilo iOS ili Windows Phone operativni system [9].

4. PRIMER IMPLEMENTACIJE EMM REŠENJA

Predmet ovog dela master teze je da opiše EMM rešenje koje je implementirano u konkretnom korporativnom okruženju, međusobne veze komponenti sistema kao i način njihovog konfigurisanja.

Odabrano je Citrix-ovo rešenje kao primer jednog od vodećih EMM rešenja na tržištu, koje se našlo u magičnom Gartnerovom kvadrantu.

EMM rešenje za cilj ima pre svega povećanje zaštite korporativnih podataka na mobilnim uređajima. U konkretnom slučaju se koriste Android i iOS mobilni uređaji.

Ovaj deo master teze, koji u stvari predstavlja primer implementiranog EMM sistema, može se podeliti na više celina. Prva celina opisuje osnovne komponente implementiranog rešenja. U sledećih nekoliko celina je dat koncept realizacije fizičkih međuveza komponenti, sledi celina koja opisuje način konfigurisanja svake od komponenti sistema kako bi se obezbedile željene funkcionalnosti, i na kraju je opisan proces „pakovanja“ aplikacija u cilju obezbeđivanja isporuke i korišćenja ovih aplikacija.

4.1. Opis EMM rešenja

U ovom poglavlju dat je opis komponenti EMM sistema, njihovo mesto u mreži kao i kratak pregled arhitekture implementiranog rešenja.

Implementiran EMM sistem sastoji se iz Citrix XenMobile Enterprise rešenja i NetScaler VPX uređaja. Osnovna namena EMM sistema je da korisnicima omogući povećanu sigurnost nad korporativnim podacima na mobilnim uređajima kao i siguran pristup ka resursima koji se nalaze u internoj mreži kompanije. Korporativni podaci na mobilnim uređajima se nalaze u enkriptovanom kontejneru koji je izolovan od privatnog dela telefona čime se omogućava veća sigurnost.

Citrix XenMobile Enterprise rešenje se sastoji iz sledećih komponenti:

- XenMobile Device Manager
- XenMobile AppControler
- ShareFile Storage Zone Controller

4.1.1. XenMobile Device Manager

XenMobile Device Manager predstavlja robusno rešenje za upravljanje, konfigurisanje i nadgledanje mobilnih uređaja. Device Manager poseduje funkcionalnost udaljenog upravljanja, čime je moguće ostvariti selektivno ili potpuno brisanje podataka sa mobilnih uređaja. Device Manager takođe omogućava proveru da li je uređaj u skladu sa korporativnim polisama (*jailbreak*-ovan uređaj, obavezno zaključavanje *passcode* šifrom ...) kao i automatsku konfiguraciju uređaja. Poseduje integraciju sa LDAP bazom korisnika (u konkretnom slučaju za LDAP server se koristi Microsoft Active Directory, pa ćemo u daljem tekstu koristiti ovaj pojam) čime se omogućava primena različitih polisa u zavisnosti od pripadnosti korisnika različitim Active Directory grupama. Ova komponenta predstavlja MDM segment implementiranog EMM rešenja.

4.1.2. XenMobile AppControler

Predstavlja enterprise rešenje za menadžment mobilnih aplikacija. Omogućava sigurno korišćenje servisa elektronske pošte i internet pretraživanja kao i kreiranje personalizovanog korporativnog app store-a. Korišćenjem MDX (skraćenica MDX je nastala od *Mobile Device*, dok je slovo X dodato kao brend od XenMobile, Worx Home, Worx Web) tehnologije AppController omogućava specifična podešavanja aplikacija u skladu sa korporativnim polisama. Ima funkcionalnosti MAM rešenja u okviru ovog EMM rešenja.

4.1.3. ShareFile Storage Zone Controller

Predstavlja centralizovanu komponentu za sigurno čuvanje i deljenje dokumenata. Korporativnim administratorima je omogućen kompletan uvid u tokove razmene fajlova. Predstavlja MIM rešenje kojim se sami korporativni podaci čuvaju od zlonamernog uticaja.

4.1.4. NetScaler VPX uređaj

Komponenta koja omogućava korisnicima siguran pristup ka korporativnom delu mreže. Poseduje više funkcionalnosti i neke od njih su Load Balancing i Access Gateway koje su implementirane u ovom rešenju.

4.1.5. Arhitektura implementiranog rešenja

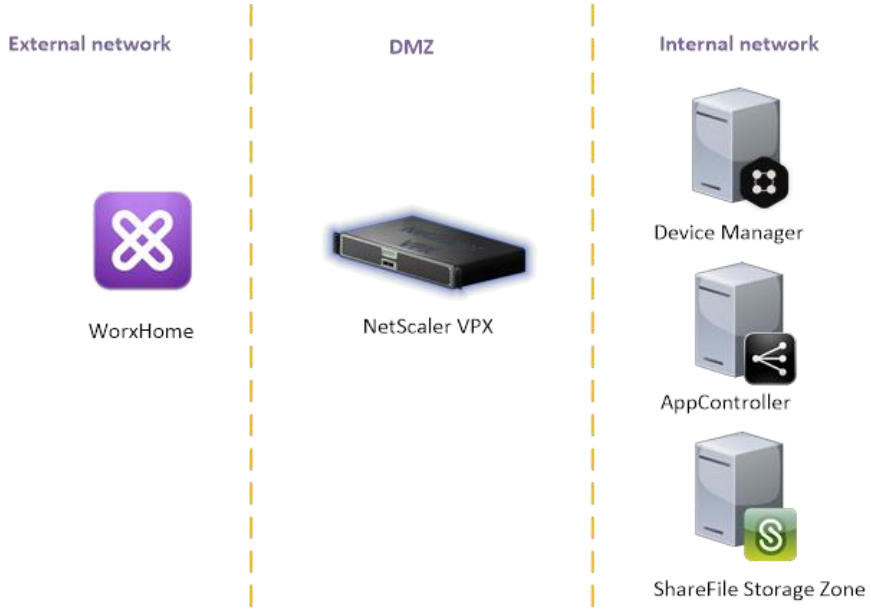
Komponente EMM sistema podeljene su u tri celine u zavisnosti od toga gde se nalaze u mrežnoj infrastrukturi i to na: komponentu eksternoj mreži, komponente u DMZ-u i komponente u internoj mreži.

Komponente u eksternoj mreži se nalaze na klijentskim mobilnim telefonima i tabletima. U ovom EMM sistemu predviđeno je da se na mobilnim uređajima koristi aplikacija Worx Home. Worx Home omogućava da se na mobilne uređaje primene odgovarajuća podedešavanja koja su u skladu sa korporativnim polisama. Ova funkcionalnost je ostvarena komuniciranjem Worx Home aplikacije sa Device Manager-om. Takođe, Worx Home omogućava korisnicima da pristupe svom personalizovanom korporativnom App Store-u, kao i primenu korporativnih polisa na mobilne aplikacije, što se postiže komunikacijom Worx Home sa App Controller-om.

Komponenta koja se nalazi u DMZ zoni je NetScaler. Njegova osnovna namena je da vrši granularnu kontrolu spoljašnjeg pristupa ka korporativnim resursima i komponentama Citrix XenMobile Enterprise rešenja.

Komponente koje se nalaze u internoj mreži su Device Manager, AppController i ShareFile. U implementiranom EMM sistemu uloga AppControllera je da korisnicima obezbedi potrebne korporativne mobilne aplikacije. Uloga Device Managera je da omogući potrebnu konfiguraciju mobilnih uređaja u skladu sa korporativnim polisama, a ShareFile-a da obezbedi jednostavan i siguran pristup podacima sa različitih uređaja.

Kratak prikaz arhitekture implementiranog EMM sistema dat je na Slici 4.1.1.



Slika 4.1.1. Kratakprikaz akhitekture EMM sistema

U DMZ zoni je instaliran NetScaler VPX uređaj koji predstavlja ulaznu tačku korisničkog saobraćaja ka komponentama implementiranog sistema. Ostale komponente EMM sistema su instalirane u internoj mreži.

4.2. Fizička i logička organizacija EMM rešenja

U ovom poglavlju dat je opis fizičke organizacije komponenti EMM sistema uključujući detaljan pregled povezivanja i FQDN-ova (*Fully Qualified Domain Name)* za sve komponente i implementirane servise.

U Tabeli 4.2.1 dat je detaljan pregled verzija komponenti EMM sistema koje su instalirane u data centru kompanije, a u Tabeli 4.2.2 je dat pregled FQDN-ova za komponente u internoj mreži. Tabeli 4.2.3 daje pregled FQDN-ova za implementirane servise na Net Scaler uređaju. Ovi FQDN-ovi će se u nastavku teksta koristiti umesto opisa određenih komponenti ili servisa implementiranih u sistemu.

Tabela 4.2.1. Prikaz verzija instaliranih komponenti

IME KOMPONENTE	VERZIJA SOFTVERA
DEVICE MANAGER	9.0
APPCONTROLER	9.0
SHAREFILE STORAGE ZONE	2.3
NETSCALER	NETSCALER NS10.5: BUILD 51.1017.E.NC

Komponente Citrix XenMobile Enterprise mogu biti instalirane na fizičkim serverima ili na virtuelnom okruženju kompanije, što je slučaj u ovom primeru, kojima su dodeljene odgovarajuće IP adrese koje nije potrebno navoditi u ovom slučaju. NetScaler uređaj se konfiguriše sa dve IP adrese na dve mrežne karte, a njihova uloga biće objašnjena u nastavku odeljka teze.

Tabela 4.2.2. Prikaz dodeljenih FQDN-ova za pojedine komponente

KOMPONENTA	NAMENA	FQDN
DEVICE MANAGER	REALAN SERVER	SRV-HQ-EMMDM.KORPDOMAIN
APPCONTROLLER	REALAN SERVER	SRV-HQ-EMMAPPC. KORPDOMAIN
SHAREFILE STORAGE ZONE	REALAN SERVER	SRV-HQ-EMMSF. KORPDOMAIN
NETSCALER	MGMT NSIP ADRESA	-
NETSCALER	SNIP ADRESA	-

Tabela 4.2.3. Prikaz dodeljenih FQDN-ova za implementirane servise na Net Scaler uređaju

KOMPONENTA	NAMENA	FQDN
NETSCALER AG VIP	PRISTUP KA APPCONTROLLERU-U	XENMOBILE.KORPDOMAIN
NETSCALER LB VIP	PRISTUP KA DEVICE MANAGER-U	ENROLL.KORPDOMAIN
NETSCALER SF VIP	PRISTUP KA SHAREFILE STORAGE ZONE-U	SHAREFILE.KORPDOMAIN

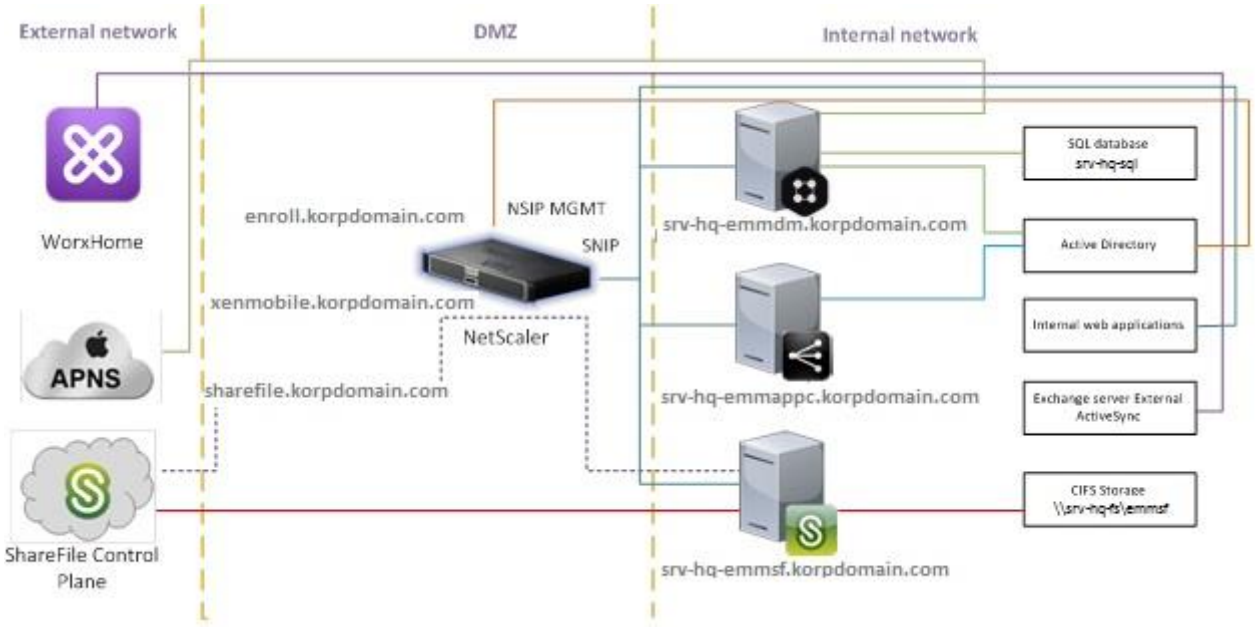
Servisi implementirani na NetScaler-u, koji je instaliran u DMZ zoni informacionog sistema kompanije, imaju svoje adrese koje se na internet ruteru ili Firewall-u NAT-uju *(Network Address Translation*). Na ovaj način se obezbeđuje da korisnici mogu pristupiti servisima preko Internet konekcije, iako su van korporativne mreže.

4.3. Fizička i logička organizacija komponenti EMM sistema

Sve komponente EMM sistema su instalirane na virtuelnoj infrastrukturi kompanije u data centru. NetScaler VPX je instaliran kao virtuelna mašina u DMZ zoni i predstavlja ulaznu tačku spoljašnjeg pristupa korisnika ka Citrix XenMobile Enterprise rešenju. NetScaler ostvaruje komunikaciju ka Device Manager, AppController i ShareFile Storage Zone komponentama instaliranim u internoj mreži data centra.

Net Scaler u stvari predstavlja gejtvej kada korisnik želi da ostvari pristup ka internim resursima kompanije. Korisnik sa svog mobilnog uređaja, zavisno od toga da li želi da se registruje na sistem, da li želi da preuzme neku aplikaciju ili dokument, pristupa nekom od servisa koji su objavljeni na Net Scaler uređaju sa javnim IP adresama. Zavisno od definisanih sigurnosnih polisa i sigurnosne grupe, u kojoj se korisnik koji ostvaruje konekciju nalazi, u Active Directory-ju, Net Scaler omogućava ili odbija pristup resursima u internoj mreži.

Na Slici 4.3.1 dat je detaljan prikaz arhitekture implementiranog EMM rešenja.



Slika 4.3.1. Detaljna arhitektura EMM sistema

U Tabeli 4.3.1 dati su parametri za pristup svim komponentama EMM rešenja. Vidimo da se komponentama može pristupati koristeći različite protokole, naravno samo oni korisnici koji imaju administratorska prava nad sistemom.

Tabela 4.3.1. Prikaz parametara pristupa ka komponentama EMM sistema

COMPONENT NAME		USER	PASSWORD
NETSCALER			
WEB ACCESS	HTTP://MGMT_NSIP_ADRESA	DOMAIN USER: IME.PREZIME	DOMAIN PASSWORD
SSH	MGMT_NSIP_ADRESA	DOMAIN USER: IME.PREZIME	DOMAIN USER
APPCONTROLLER			
WEB ACCESS	HTTPS://IP_ADRESA_APPCONTROLLER:4443/	ADMINISTRATOR	PASSWORD
SSH	IP_ADRESA_APPCONTROLLER	ADMIN; ADMINISTRATOR	PASSWORD
DEVICE MANAGER			
WEB ACCESS	HTTPS://IP_ADRESA_DEVICE_MANAGER/EMMBAZA/	DOMAIN USER: IME.PREZIME	DOMAIN PASSWORD
RDP	IP_ADRESA_DEVICE_MANAGER	EMMSERVICE	PASSWORD
SHAREFILE			
CONFIG WEB ACCESS ON THE SERVER	HTTP://LOCALHOST/CONFIGSERVICE/LOGIN.ASPX	ADMIN; ADMINISTRATOR	PASSWORD
RDP	IP_ADRESA_SHAREFILE_STORAGE_ZONE	EMMSERVICE	PASSWORD
CONTROL PLANE	HTTPS:// IMEKOMPANIJE.SHAREFILE.EU/	ADMIN; ADMINISTRATOR	PASSWORD
USER WEB ACCESS	HTTPS://IMEKOMPANIJE.SHAREFILE.EU/SAML/LOGIN	DOMAIN USER: IME.PREZIME	DOMAIN PASSWORD

4.4. Fizička i logička organizacija NetScaler VPX uređaja

NetScaler VPX uređaj je instaliran u DMZ zoni na postojećoj virtuelnoj infrastrukturi kompanije. Za povezivanje NetScaler-a definisana su dva NIC-a koja su povezana u DMZ deo mreže kompanije. NetScaler uređaj za potrebe administracije ima dodeljenu jednu IP adresu, tzv. Management IP adresu.

Na relevantnim mrežnim uređajima implementirano je odgovarajuće rutiranje i sigurnosne politike, tako da se može ostvariti sledeća komunikacija:

- Klijenti (i interni i eksterni) pristupaju javnim VIP IP adresama na NetScaler sistemu
- NetScaler pristupa svim XenMobile serverima, tu se misli na servere na kojima su instalirane Device Manager, AppControler i Share File Storage Zones. Za iniciranje ovih konekcija NetScaler koristi SNIP adresu kao source IP adresu. Ovu adresu NetScaler koristi i za pristup ka internim veb aplikacijama.
- NetScaler pristupa LDAP serveru za potrebe ostvarivanja AAA (*authentication, authorization, accounting*) funkcije. Za iniciranje ovih konekcija NetScaler koristi NSIP adresu kao source IP adresu.

U Tabeli 4.4.1 dat je pregled IP adresa koje je potrebno dodeliti NetScaler-u da bi se postigle sve njegove funkcionalnosti kao i njegova administracija. Tu su NSIP adresa koja se koristi kao source adresa prilikom slanja upita LDAP serveru, što će biti detaljnije objašnjeno u jednom od narednih pododeljaka. Ova adresa se ujedno koristi i za administraciju NetScaler uređaja. SNIP adresa se koristi kao source adresa prilikom upita koje NetScaler šalje aplikacijama i serverima u internoj mreži, VIP NS adrese su privatne adrese iz interne mreže dodeljene servisima koji su implementirani na uređaju, a VIP Public adrese javne adrese u koje su NAT-ovane privatne adrese servisa na nekom od relevantnih uređaja (internet ruteru ili internet firewall-u)

Tabela 4.4.1. Pregled IP adrese NetScaler-a

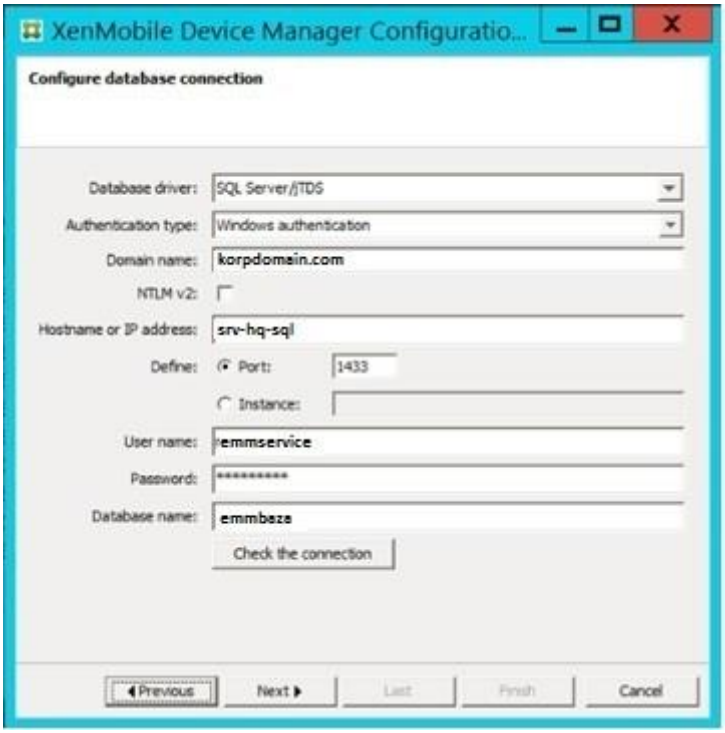
NS-HOSTNAME	NSIP	SNIP	VIP NS	VIP PUBLIC
NETSCALER	NSIP ADRESA ZA PRISTUP LDAP SERVERU	SNIP ADRESA ZA PRISTUP APLIKACIJAMA I SERVERIMA U INTERNOJ MREŽI	PRIVATNE ADRESE DODELJENE SERVISMA KOJI SU IMPLEMENTIRANI NA NETSCALERU	JAVNE (NAT-OVANE) ADRESE DODELJENE SERVISMA KOJI SU IMPLEMENTIRANI NA NETSCALERU

NetScaler je povezan sa LDAP serverom radi vršenja autentifikacije za krajnje korisnike i za vršenje autentifikacije za administratore sistema.

NetScaler je takođe povezan i sa DNS serverom.

4.5. Fizička i logička organizacija Device Manager servera

Device Manager komponenta verzije 9.0 je instalirana kao virtuelna mašina na postojećoj virtuelnoj infrastrukturi kompanije. Device Manager se nalazi u internoj mreži kompanije. Instaliranje je izvršeno nad Windows Server 2012 R2 Standard operativnim sistemom. Device Manager je prilikom instalacije potrebno povezati sa eksternom SQL bazom podataka kao što je prikazano na slici 4.5.1.



Slika 4.5.1. Povezivanje Device Manager-a sa eksternom SQL bazom

Takođe prilikom povezivanja sa eksternom SQL bazom potrebno je napraviti bazu podataka u kojoj će se nalaziti svi podaci Device Manager server-a. U ovom slučaju kreirana je baza podataka nazvana **emmbaza**. Podaci o samim uređajima, o definisanim polisama kao i o primenjenim polisama na određene mobilne uređaje biće smešteni u ovoj bazi.

Tokom instalacije Device Manager-a potrebno je izvršiti kreiranje i potrebnih sertifikata za pravilan rad komponente. Sertifikat za HTTPS konekciju je kreiran na FQDN virtuelnog servisa kreiranog na NetScaler-u koji glasi **enroll.korpdomain.com**. Na isti taj FQDN je izdat i APNS (*Apple Push Notification Service*) sertifikat potreban kako bi se omogućila konekcija iOS mobilnih uređaja ka Device Manager-u.

Tokom instalacije Device Manager-a potrebno je kreirati difolt administratorski nalog koji će posedovati sva prava nad sistemom.

Nakon inicijalne instalacije vrši se povezivanje Device Manager-a sa LDAP serverom. Primer je dat na slici 4.5.2, gde se može videti povezivanje sa Microsoft Active Directory.

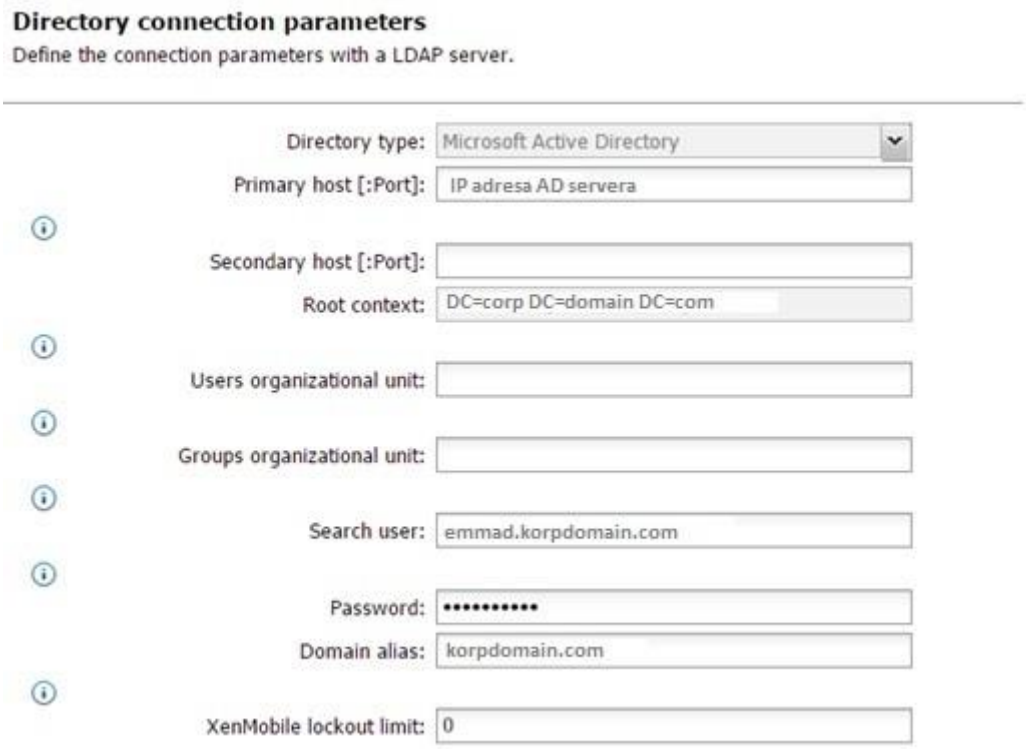
Nakon inicijalnog povezivanja vrši se dodavanje odgovarajućih korisničkih grupa u Device Manager server. Ovde samo navodimo primere mogućih korisničkih grupa koje mogu biti implementirane. Naravno, zavisno od konkretnih potreba kompanije, ove grupe se mogu organizovati na druge načine. Na LDAP serveru su kreirane sledeće grupe namenjene korisnicima sistema:

- G_EMM_Users
- G_EMM_VIP

Pored toga izvršeno je i dodavanje grupa namenjenih za administraciju Device Manager server-a:

- G_EMM_Admins

- G_EMM_Tehnicari



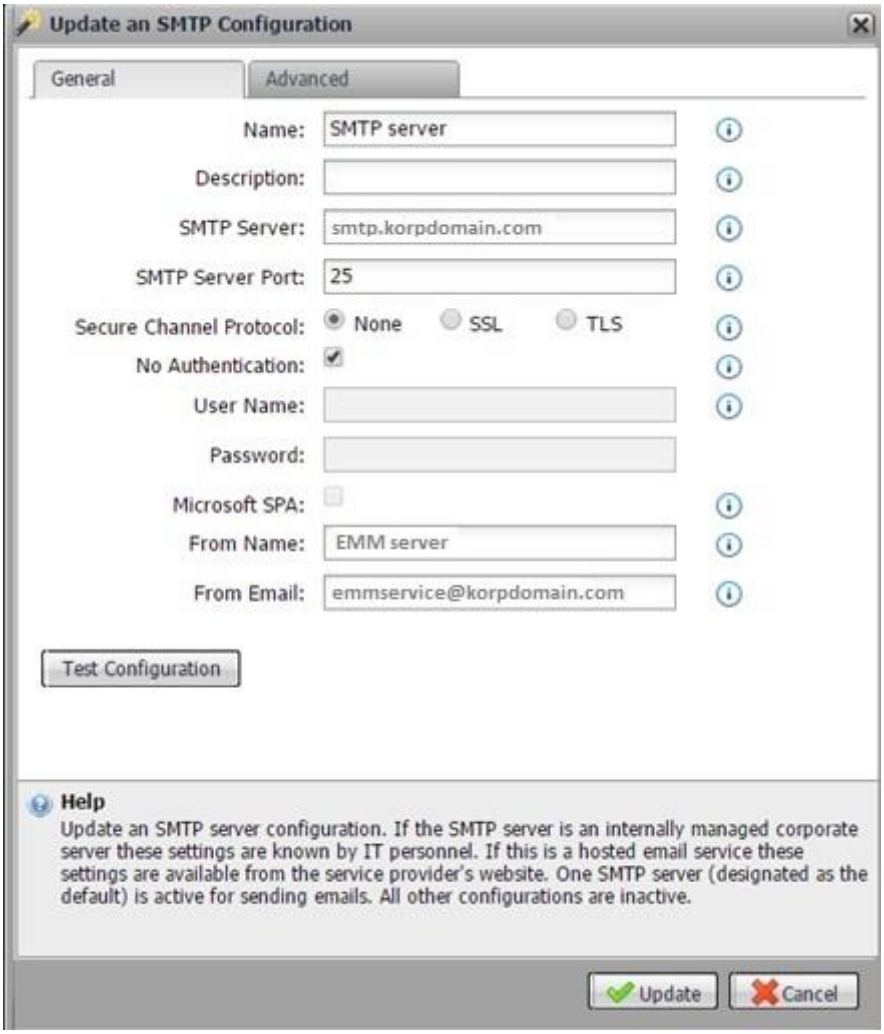
Slika 4.5.2. Povezivanje Device Manager-a sa Microsoft Active Directory-em

Kao što rekosmo ovo je samo primer implementiranog rešenja, grupe mogu biti drugačije organizovane .

G_EMM_Admins grupa ima ista admin prava kao i inicijalno kreirani lokalni admin account administrator. G_EMM_Tehnicari grupa ima prava da poziva nove korisnike u sistem, može da vidi informacije o korisničkim uređajima kao i da ih selektivno obriše.

Device Manager server može se povezati sa korporativnim SMTP serverom kako bi mogao da šalje poruke administratorima što je na ovom primeru i urađeno. Na slici 4.5.3 može se videti povezivanje Device Manager-a sa korporativnim SMTP serverom.

Kao email adresa sa koje šalje poruke koristi se **emmservice@korpdomain**.



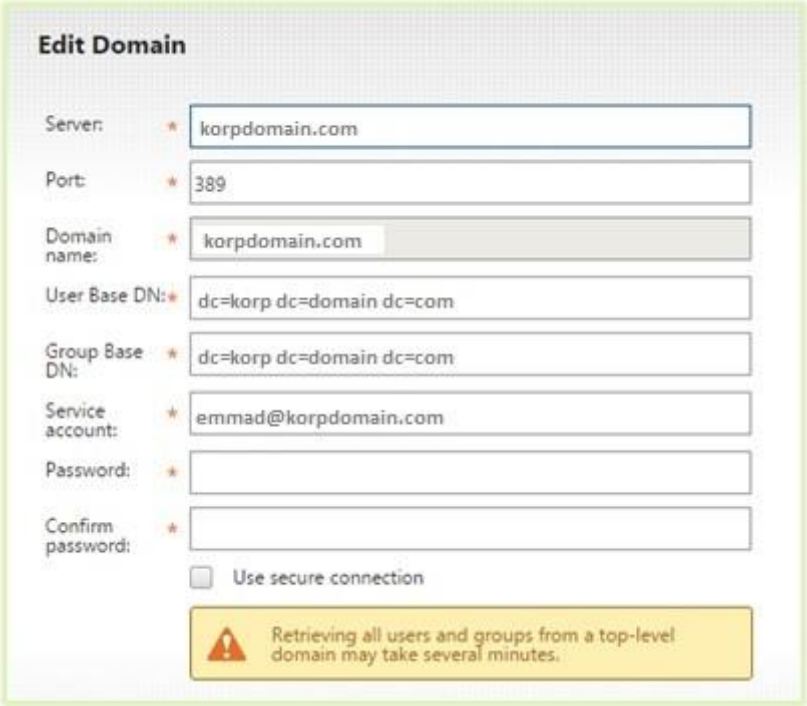
Slika 4.5.3. Povezivanje Device Manager-a sa SMTP serverom

4.6. Fizička i logička organizacija AppController servera

AppController komponenta verzije 9.0 instalirana je kao predefinisana virtuelna mašina na postojećoj virtualnoj infrastrukturi kompanije u internoj mreži. Tokom instalacije, potrebno je za AppController definisati IP adresu, subnet masku, difolt gejtvej, DNS i NTP server, kao neophodne parametre ovog server.

Nakon instalacije vrši se povezivanje AppController-a sa LDAP serverom.

Povezivanje AppController-a sa LDAP odnosno AD (*Active Directory*) serverom prikazano je na slici 4.6.1.



Slika 4.6.1. Povezivanje AppController-a sa LDAP serverom

Nakon izvršenog povezivanja sa LDAP serverom definisane su sledeće role koje su mapirane sa odgovarajućim grupama na LDAP-u datim u Tabeli 4.6.1 Role prestavljaju skup pravila koji će biti primenjen na određenu grupu korisnika, a tiče se polisa koje će biti primenjene na uređaje koje ti korisnici koriste. Primenjene polise će definisati prava pristupa resursima u internoj mreži kompanije, koje će korisnici, pripadnici pojedinh grupa imati, odnosno u skladu sa tim kojoj grupi pripadaju korisnici će imati određene nadležnosti, tj. role.

Tabela 4.6.1. Mapiranje AD grupa u Role

ROLE	LDAP GROUP
XENMOBILE_SHAREFILE_USERS	G_EMM_SHAREFILE
XENMOBILE_USERS	G_EMM_USERS
XENMOBILE_VIP_USERS	G_EMM_VIP

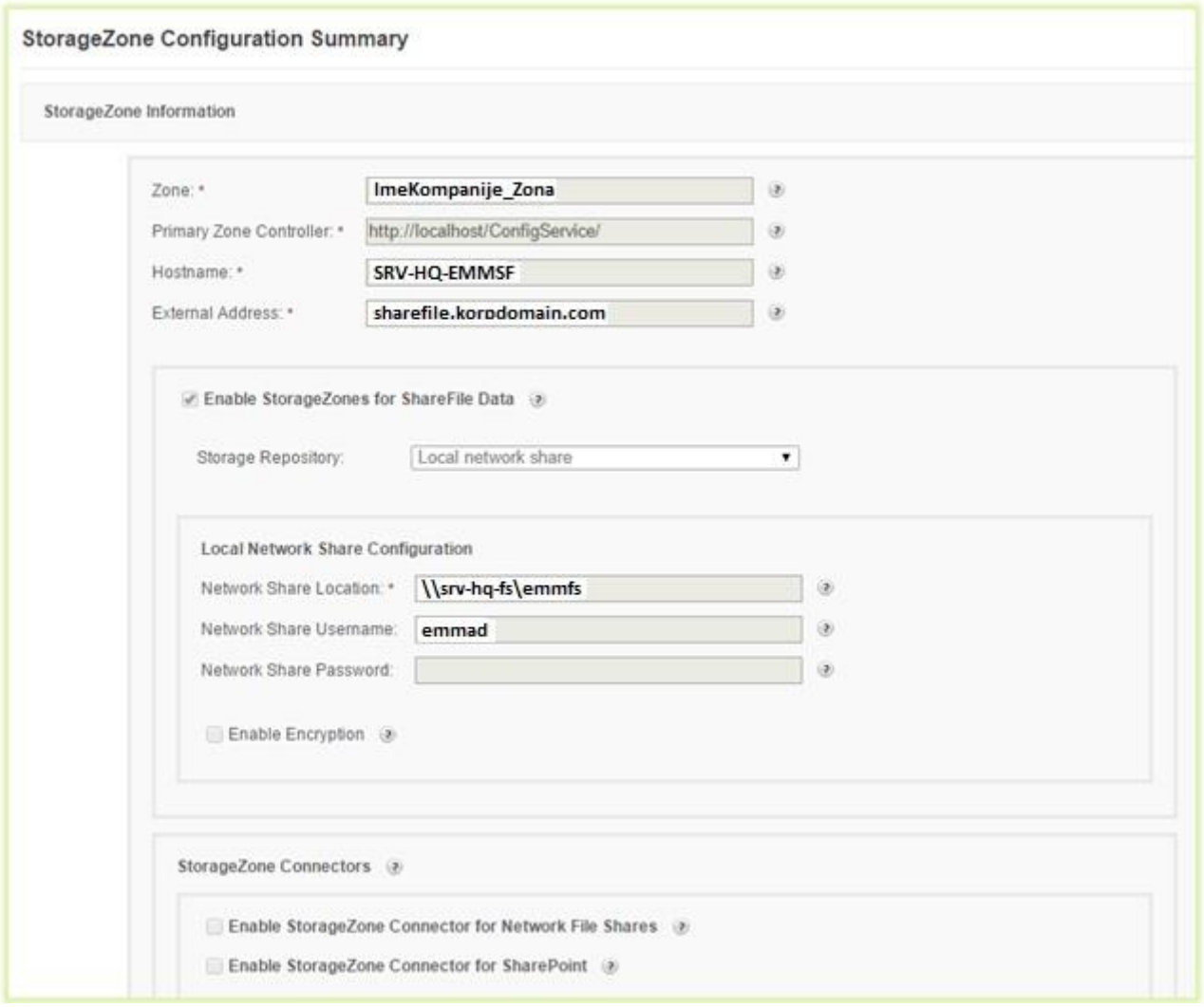
Na AppController su zatim instalirani odgovarajući *root*, *intermediate* i serverski sertifikati. Serverski sertifikat je izdat na FQDN AppController-a srv-hq-emmappc.korpdomain.com.

4.7. Fizička i logička organizacija ShareFile Storage Zone servera

ShareFile Storage Zone komponenta verzije 2.3 je instalirana kao virtuelna mašina na postojećoj virtuelnoj infrastrukturi kompanije. Instalirana je u internoj mreži. Instaliranje je izvršeno nad Windows Server 2012 R2 Standard operativnim sistemom.

Nakon instalacije izvršeno je kreiranje primarne zone ImeKompanije_Zona, koja je povezana sa CIFS-om (Citrix File Storage) na odgovarajućoj putanji (\\srv-hq-fs\emmsf). Kao hostname tokom konfiguracije Storage Zone-a naveden je SRV-HQ-EMMSF dok je kao eksterni URL naveden FQDN ShareFile virtuelnog servisa definisanog na NetScaler-u **sharefile.korpdomain.com.**

Konfiguracija ShareFile Storage Zone je data na Slici 4.7.1.



Slika 4.7.1 Konfiguracija ShareFile Storage Zone

Ova konfiguracija može se videti na SRV-HQ-EMMSF serveru odlaskom na http://localhost/configservice/login.aspx URL iz veb brauzera.

Nakon konfiguracije NetScaler-a, ImeKompanije_Zona je povezana sa ShareFile control plane-om u cloudu što se može videti u ShareFile control plane-u odlaskom na https://imekompanije.sharefile.eu/> Admin > Storage Zones.

Slika 4.7.2 prikazuje ShareFile Storage Zone u cloudu.

Slika 4.7.2. ShareFile Storage Zone u cloudu

4.8. Implementacija funkcionalnosti sistema za zaštitu i upravljanje mobilnim uređajima

EMM sistem pre svega ima za cilj povećanje sigurnosti korporativnih podataka na mobilnim uređajima. Kako bi se ostvario potreban nivo zaštite svi mobilni uređaji koji su pod kontrolom EMM sistema moraju imati "zaključavanje" ekrana telefona sa PIN-om. Ovi mobilni uređaji imaju mogućnost pristupa ka korporativnom AppStore-u sa kojeg korisnici mogu da preuzmu korporativne aplikacije namenjene za njih. Nad korporativnim aplikacijama koje se instaliraju na mobilne uređaje definisane su takve polise koje obezbeđuju kontejnerizaciju i enkripciju poslovnih podataka. Tim polisama se omogućava da samo korporativne aplikacije mogu međusobno da razmenjuju podatke dok je komunikacija između korporativnih i privatnih aplikacija instaliranih na mobilnom uređaju zabranjena. Svi podaci u korporativnim aplikacijama preuzetim sa korporativnog App Store-a su enkriptovani što ih čini nečitljivim za privatne aplikacije. Takođe, omogućeno je i potpuno ili delimično brisanje podataka sa mobilnih uređaja u slučaju da se za tako nečim ukaže potreba. Pored toga korisnicima je omogućen i siguran pristup ka internim veb aplikacijama sa mobilnih uređaja iz bilo koje 3G ili WiFi mreže. Kako bi se ostvarile sve definisane funkcionalnosti i na iOS i na Android mobilnim uređajima kreirane su odgovarajuće polise koje će biti opisane u nastavku ovog dela teze.

4.8.1. Implementacija funkcionalnosti MDM rešenja

i) Implementacija Enrollment-a mobilnih uređaja

Kako bi bilo moguće vršiti zaštitu i upravljanje nad mobilnim uređajima potrebno je da se mobilni uređaji povežu sa implementiranim EMM sistemom. Proces povezivanja uređaja sa sistemom se naziva *enrollment*. Kako bi se izvršilo povezivanje sa sistemom na mobilnim uređajima se instalira agent aplikacija koja se naziva WorxHome

Tokom procesa *enrollment*-a uspostavlja se veza između WorxHome aplikacije na mobilnom uređaju i Device Manager servera. Kada se uređaj prvi put obrati Device Manager serveru, server prvo izvršava proveru svih definisanih polisa i ukoliko je sve u redu vrši instalaciju jedinstvenog sertifikata na taj uređaj. Nakon ovog koraka uspostavljeno je poverenje između uređaja i Device Manager servera koji zatim primenjuje sve definisane korporativne polise na mobilni uređaj.

Nakon inicijalnog procesa *enrollment*-a veza sa Device Manager serverom se uspostavlja na drugačiji način za Android i iOS uređaje. Za Andriod uređaje komunikacija sa Device Manager serverom se vrši korišćenjem Schedule polise dok se komunikacija za iOS uređaje ostvaruje posredstvom Apple Push Notification APNS servisa.

Uloga APNS servisa je da "probudi" iOS uređaj koji se zatim konektuje sa Device Manager serverom kako bi preuzeo nove polise. Kada je potrebno da se izvrši neka izmena na iOS uređaju, Device Manager se prvo obraća APNS serveru koji zatim budi iOS uređaj koji se konektuje na Device Manager server. Ovim se omogućava da se sve polise koje se definišu na Device Manager serveru primenjuju u realnom vremenu na iOS mobilni uređaj. Za razliku od iOS uređaja, za koje se sve polise definisane na Device Manager serveru izvršavaju u skoro realnom vremenu, Android uređaji se konektuju na Device Manager server u predefinisanim vremenskim intervalima koji su dati u Schedule polisi. To znači da će se polise koje se definišu na Device Manager serveru izvršiti na Android uređaju sledeći put kada se on konektuje na server tako da će postojati izvesno zakašnjenje u njihovoj primeni na mobilnom uređaju.

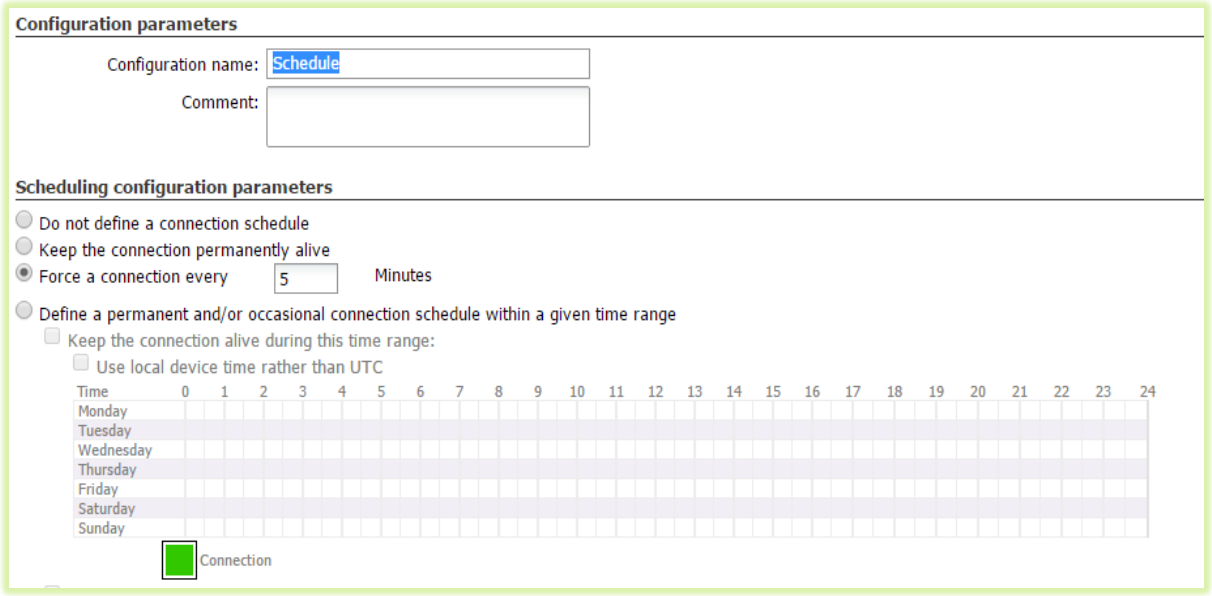
Kako bi se ostvario proces *enrollment*-a izvršeno je kreiranje potrebnog servisa na NetScaler uređaju, već pominjani enroll.korpdomain. Pored toga Device Manager server je instaliran sa sertifikatima koji su izdati na FQDN servisa kreiranog na NetScaler uređaju. Kako bi se ostvarila sigurna konekcija Device Manager servera sa Android mobilnim uređajima koristi se port 443 dok se za komunikaciju sa iOS uređajima koristi port 8443.

ii) Implementacija korporativnih polisa za mobilne uređaje

Nakon uspešnog procesa *enrollment*-a mobilnih uređaja vrši se instalacija definisanih polisa na mobilne uređaje kako bi oni bili u skladu sa korporativnim polisama. Kako bi se obezbedila sigurnost nad mobilnim uređajima izvršeno je definisanje polisa za iOS i Android uređaje.

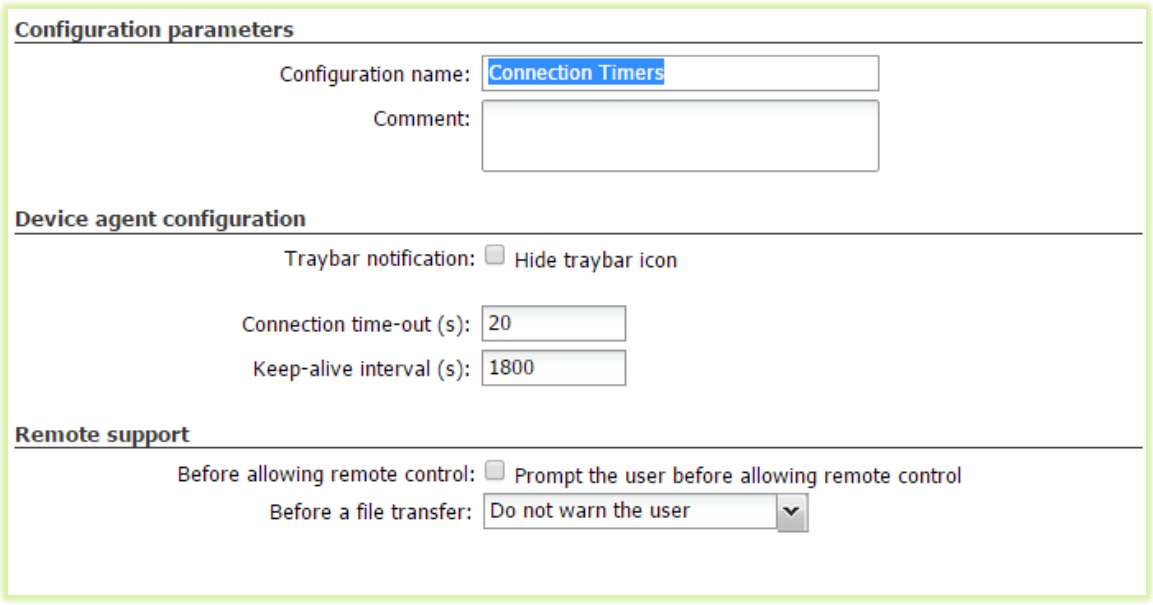
Schedule polisa daje instrukciju Android mobilnim uređajima koliko često je potrebno da se konektuju na Device Manager server. Kada se izvrši konektovanje uređaja na Device Manager server vrši se ažuriranje svih polisa definisanih za njega. Schedule polisom se omogućava da Device Manager ima uvek *up-to-date* (ažurne) informacije o uređaju. U sistemu za zaštitu i upravljanje nad mobilnim uređajima izvršeno je definisanje Schedule polise koja daje instrukciju da se Android uređaj konektuje na sistem svakih 5 minuta kako bi se izvršilo ažuriranje svih polisa.

Na slici 4.8.1 dat je primer konfigurisanja Schedule polise koja će se primenjivati na Android mobilne uređaje.



Slika 4.8.1. Konfiguracija Schedule polise

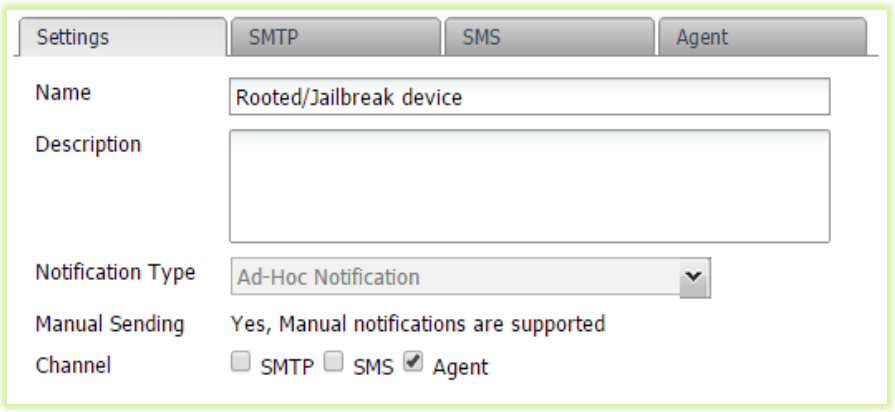
Connection Timers polisa omogućava definisanje *time-out* intervala za konekciju WorxHome agenta na Android mobilnom uređaju sa Device Manager serverom. Ukoliko istekne definisani *time-out* interval otkazaće se pokušaj konektovanja sa serverom. *Time-out* interval je definisan na 20 sekundi. Konfigurisanje Connection Timers polise je dato na Slici 4.8.2.



Slika 4.8.2. Konfiguracija Connection Timers polise

Software Inventory polisa omogućava Device Manager server potpuni uvid u sve aplikacije i softverske pakete instalirane na mobilnom uređaju. Ova polisa je predefinisana od strane Device Manager server-a i kao takva se sa ostalim polisama primenjuje na mobilne uređaje.

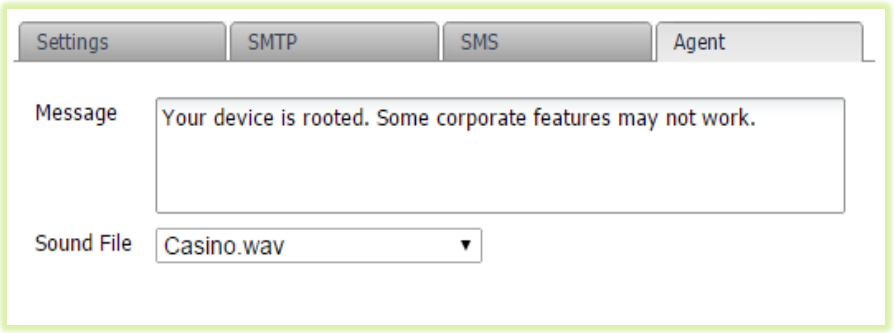
Rooted Device Notification polisa omogućava automatsko slanje notifikacije korisniku mobilnog uređaja čim Device Manager server detektuje da je uređaj *root*-ovan ili *jailbreak*-ovan. Polisa je konfigurisana tako da korisniku šalje notifikaciju. Kako bi se omogućilo automatsko slanje notifikacije čim Device Manager server detektuje uređaj koji je *root*-ovan ili *jailbreak*-ovan potrebno je da se prvo definiše Notification Template koji koristi Agenta kako bi obavestio korisnika o *root*-ovanom/*jailbreak*-ovanom uređaju. Korisniku telefona se kroz WorxHome agent pokazuje poruka *Your device is rooted. Some corporate features may not work.* Ovaj Notification Template se koristi u okviru Automated Action polise koja je zadužena za slanje automatske notifikacije čim Device Manager server detektuje da je uređaj *root*-ovan/*jailbreak*-ovan. Na slici 4.8.3 se može videti konfiguracija Notification Template-a.



Slika 4.8.3. Konfiguracija Notification Template-a

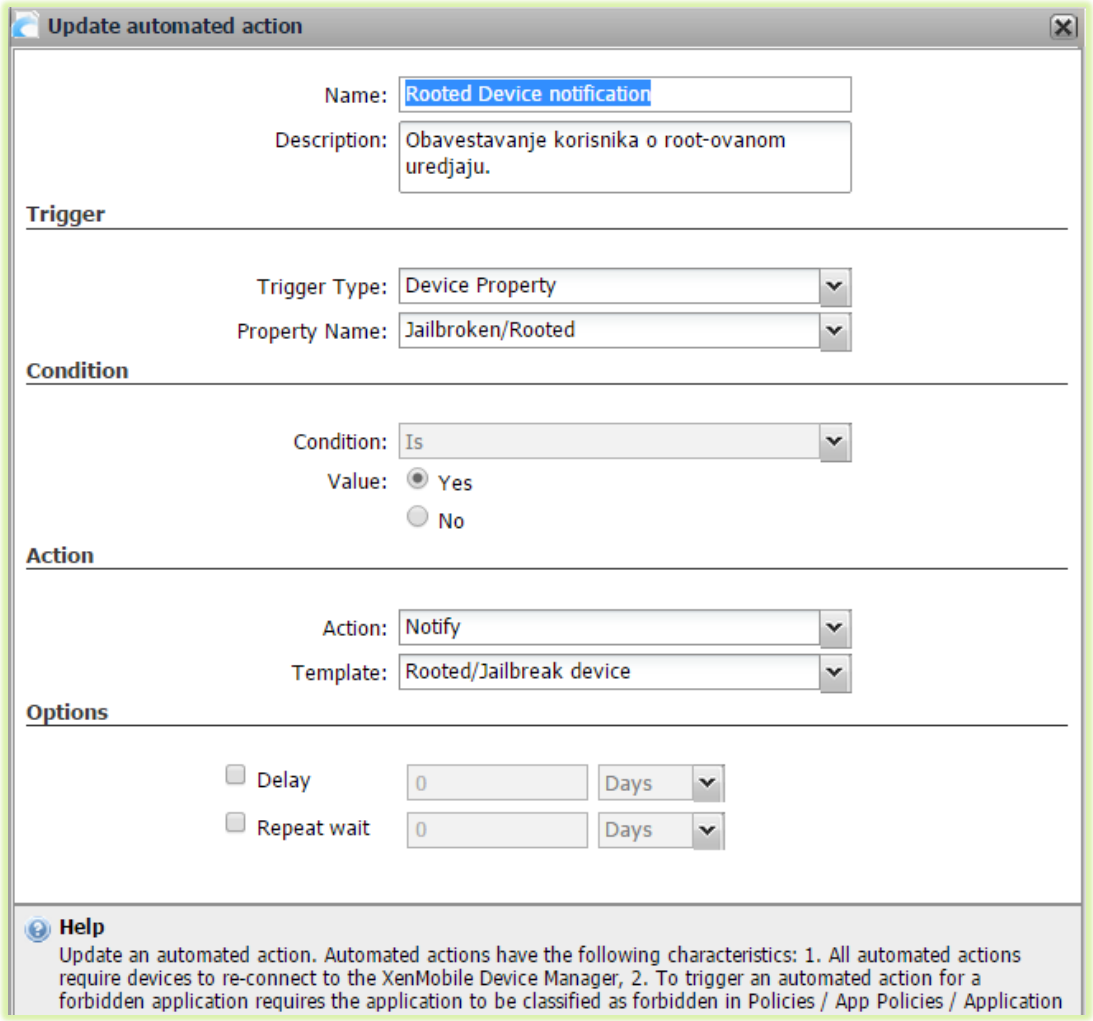
Na slici 4.8.4 se može videti konfiguracija agent notifikacije koja se šalje korisniku mobilnog uređaja.

.



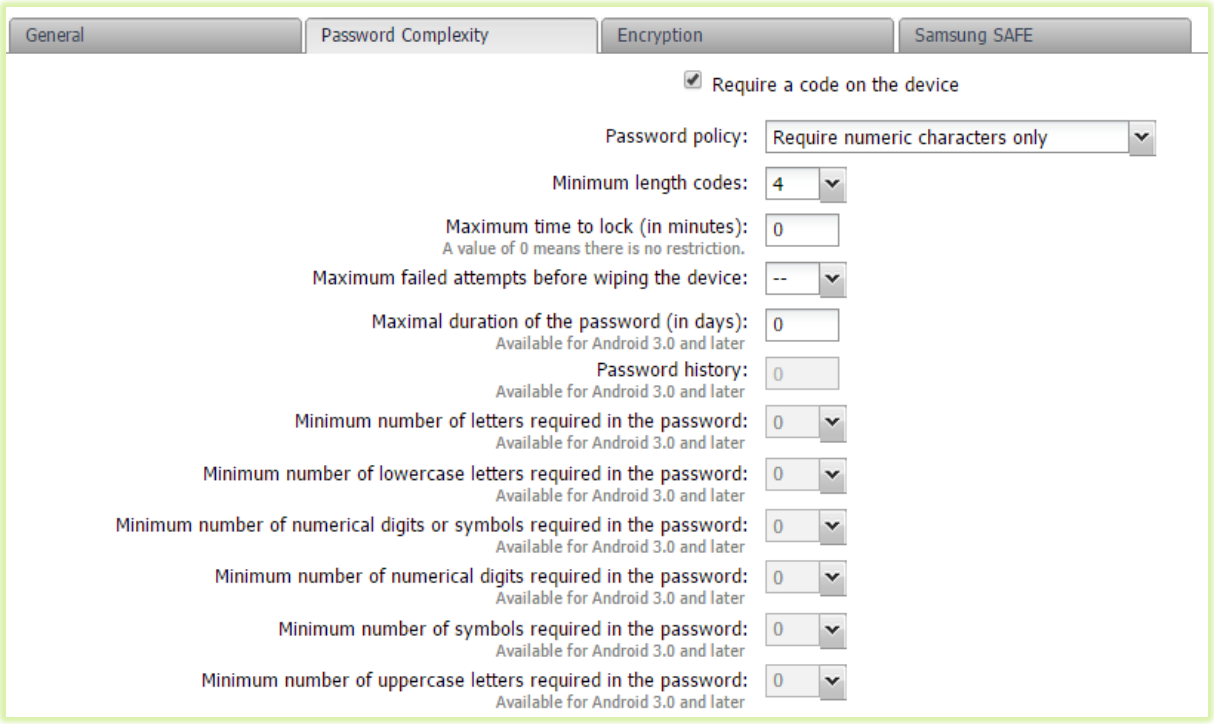
Slika 4.8.4. Konfiguracija agent notifikacije koja se šalje korisniku mobilnog uređaja

Na slici 4.8.5 se može videti konfiguracija Automated Action polise.



Slika 4.8.5. Konfiguracija Automated Action polise

Passcode polisa omogućava konfigurisanje zaključavanja mobilnog uređaja sa PIN-om kako bi se obezbedio veći nivo sigurnosti. Definisanom polisom je napravljeno ograničenje da PIN mora da se sastoji od minimum 4 karaktera. Na Slici 4.8.6 je dat prikaz konfigurisane passcode polise u konkretnom primeru:



Slika 4.8.6. Konfiguracija Passcode polise

iii) Primena korporativnih polisa na mobilne uređaje

Kako bi se definisane korporativne polise primenile na mobilnim uređajima potrebno je da se napravi paket na Device Manager serveru. Ovaj paket se naziva Deployment package i u njemu se smeštaju definisane polise koje želimo da primenimo na mobilni uređaj. Nakon što smestimo sve željene polise u Deployment package onda se ceo paket spušta na mobilni uređaj nakon čega se vrši konfiguracija uređaja u skladu sa polisama koje su kroz paket primenjene. Opet napominjem da ovde dajemo samo primer paketa koji mogu sadržati različite polise. Paketi mogu sadržati različite kombinacije polisa, zavisno od konkretne potrebe kao sigurnosne politike kompanije. Kako bi se primenile sve definisane polise nad Andorid i iOS uređajima u Device Manager serveru su definisani sledeći paketi:

Za Android mobilne uređaje:

- **Android Base Package** – u ovom paketu se na mobilne uređaje primenjuju polise:
    - Schedule
    - Connection Timers
    - Software Inventory
- **Android Passcode Package** – u ovom paketu se na mobilne uređaje primenjuje sledeća polisa:
    - Passcode
- **Device Rooted Notification** – u ovom paketu se na mobilne uređaje primenjuje sledeća polisa:

- Device Rooted Notification

Andorid Base Package i Passcode se primenjuju svaki put kada se korisnik konektuje na sistem dok se Device Rooted Notification paket primenjuje samo ukoliko već nije primenjivan na uređaj.

Na Slici 4.8.7 je prikazan konfigurisan Android Base Package paket, gde se mogu videti polise koje su uključene u njega. Drugačija oznaka ispred Software Inventory polise govori da je to predefinisana polisa za razliku od ostalih koje su eksplicitno konfigurisane.

Slika 4.8.7. Android Base Package

Na Slici 4.8.8 je prikazan konfigurisan Android Passcode Package paket. Jedina polisa u ovom paketu je ona kojom se zahteva da uređaj ima šifru kojom će se otključavati.

Slika 4.8.8. Android Passcode package

Na Slici 4.8.9 se može videti konfigurisan Device Rooted Notification paket, u koji je uključena polisa za notifikaciju korisnika koji koriste *root*-ovan ili *jailbreak*-van mobilni uređaj. Na ovoj kao i na prethodnim slikama na kojima je prikazana konfiguracija određenih paketa može se videti na koju grupu korisnika, koje su kreirane u Active Directory-ju, se paket primenjuje.

Slika 4.8.9. Device Rooted Notification

Za iOS uređaje konfigurisani su paketi:

- **iOS Base Package** – u ovom paketu na iOS uređaje primenjuje se polisa:
    - Software Inventory
- **iOS Passcode Package**– u ovom paketu na iOS uređaje primenjuje se polisa:
    - Passcode

Na Slici 4.8.10 može se videti konfigurisan iOS Base package, u koji je jedino uključena Software Inventory predefinisana polisa. U ovaj paket za mobilne uređaje sa iOS operativnim sistemom schedule polisa nije potrebna zbog načina na koji oni komuniciraju sa Device Manager-om, a o čemu je ranije bilo reči.

Slika 4.8.10. iOS Base Package

iOS Base Package se na uređaje primenjuje prilikom svake konekcije uređaja na Device Manager server.

Na slici 4.8.11 prikazan je konfigurisan iOS Passcode Package paket, koji je ekvivalentan Android Passcode Package.

Slika 4.8.11. iOS Passcode Package

4.8.2. Implementacija funkcionalnosti MAM rešenja

i) Implementacija povezivanja mobilnih uređaja sa korporativnim AppStore-om

Kako bi korisnici mobilnih uređaja mogli da preuzmu korporativne aplikacije potrebno je da se mobilnim uređajima obezbedi pristup ka korporativnom AppStore-u. Za kreiranje korporativnog AppStore-a zadužena je komponenta AppController. Povezivanjem Device Manager-a sa AppController-om se omogućava, da se nakon inicijalnog *enrollment*-a i primene korporativnih polisa na mobilnim uređajima, korisnicima omogući automatski pristup ka korporativnom AppStore-u bez potrebe da korisnik zna koja je adresa AppController servera. Kako bi se izvršilo povezivanje između Device Manager-a i AppController-a na Device Manager serveru su definisani AppController Host Name i Shared Key. Isti Shared Key je unet u AppController zajedno sa Host Name Device Manager servera. Komunikacija između ova dva servera se odvija po portu 80. Nakon inicijalnog *enrollment*-a i primene odgovarajućih polisa nad mobilnim uređajima, Device Manager server u WorxHome agent aplikaciju na mobilnom uređaju, putem NetScaler-a, prosleđuje potrebne parametre za pristup ka AppController serveru.

Na Slici 4.8.12 može se videti konfiguracija povezivanja Device Manager-a i AppController-a na Device Manager serveru:

Slika 4.8.12. Povezivanje Device Manager-a sa AppController-om na Device Manager-u

Na Slici 4.8.13 može se videti konfiguracija povezivanja Device Manager-a i AppController-a na AppController serveru:

Slika 4.8.13. Povezivanje AppController-a sa Device Manager serverom na AppController-u

ii) Primena korporativnih polisa nad aplikacijama

Kao što smo već rekli EMM sistem pored zaštite samih mobilnih uređaja obezbeđuje i zaštitu nad korporativnim aplikacijama i podacima. Dok se zaštita nad mobilnim uređajima ostvaruje korišćenjem Device Manager server-a, zaštita nad korporativnim aplikacijama i podacima se ostvaruje integracijom Device Manager-a sa AppController-om.

Kako bi se obezbedila zaštita nad korporativnim podacima, nad korporativnim aplikacijama su definisane odgovarajuće polise koje definišu interakciju između poslovnog i privatnog dela telefona, enkripciju nad korporativnim podacima kao i autentifikaciju kako bi se ka korporativnim podacima omogućio pristup. Sve ove polise se definišu u AppController-u za svaku od korporativnih aplikacija posebno. Primenom polisa nad korporativnim aplikacijama omogućava se željena "kontejnerizacija" poslovnih podataka.

Kako bi bilo moguće da se nad korporativnim aplikacijama primenjuju korporativne polise potrebno je prvo da se u aplikacije ubaci MDX logika procesom *wrapping*-a. Nakon što se korišćenjem Citrix wrapping tool-a u aplikacije umetne MDX logika ovako pripremljene aplikacije se ubacuju u AppController kako bi se definisale potrebne korporativne polise i izvršilo kreiranje korporativnog AppStore-a.

Kako bi se omogućila granularna kontrola pristupa ka korporativnim aplikacijama na LDAP-u su napravljene sledeće grupe koje su mapirane u odgovarajuće role na AppControlleru u Tabeli 4.8.1.

Tabela 4.8.1. Prikaz dodeljenih aplikacijama odgovarajućim AD grupama

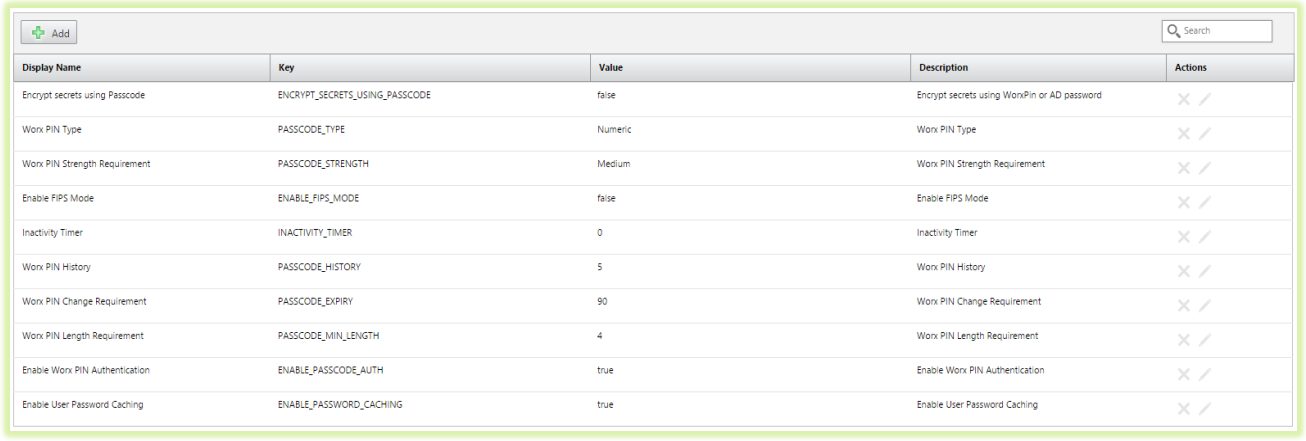
AD GRUPA	ROLA	MOBILNE APLIKACIJE
G_EMM_SHAREFILE	XENMOBILE_SHAREFILE_USERS	SHAREFILE_PHONE SHAREFILE_TABLET SHAREFILE_SAML_SP
G_EMM_USERS	XENMOBILE_USERS	WORXMAIL WORXEDIT ADOBE READER
G_EMM_VIP	XENMOBILE_VIP_USERS	WORXMAIL WORXEDIT

		ADOBE READER WORXWEB WORXWEB_SAMSUNGTAB3 FAST IMANGE VIEWER FREE

Kako bi se omogućio veći komfor prilikom pristupa ka resursima kroz WorxHome aplikaciju na mobilnim uređajima, na AppController-u je izvršeno definisanje logovanja korišćenjem PIN-a. Ovim se omogućava da korisnik samo nakon instalacije WorxHome aplikacije mora da unese svoj domenski *password* i da konfiguriše PIN. Svako naredno logovanje se ostvaruje korišćenjem PIN-a.

Polisama je definisano da PIN mora da budu 4 broja. Mora da se promeni na svakih 90 dana i istorija PIN-ova je 5 što znači da prilikom promene PIN-a ne može da se stavi PIN koji je već korišćen pre neke od prethodnih promena (tokom šeste promene PIN-a biće moguće ponovo staviti PIN koji je inicijalno korišćen).

Na Slici 4.8.14 je prikazana konfiguracija logovanja PIN-om.



Slika 4.8.14. Konfiguracija logovanja PIN-om nad WorxHome aplikacijom

Korporativne aplikacije koje su namenjene da se koriste u EMM sistemu su:

- **WorxMail** – predstavlja korporativnu mail aplikaciju koja je namenjena za primanje i slanje korporativnih mailova. Poseduje Push sinhronizaciju sa Exchange server-om kao i sinhronizaciju kalendara i kontakata. Kontakte je moguće sinhronizovati sa korporativnog Exchange server-a u kontakte na privatnom delu telefona.
- **WorxWeb** – predstavlja korporativni veb brauzer. Primarna funkcija mu je da omogući siguran pristup ka web aplikacijama u internoj mreži sa mobilnog uređaja kao i da otvara linkove primljene u mail-ovima WorxMail aplikacije.
- **ShareFile** – predstavlja aplikaciju za sigurno smeštanje priloga primljenih u mail-ovima WorxMail aplikacije kao i za sigurno deljenje korporativnim podataka.
- **WorxEdit** – predstavlja aplikaciju za sigurno pregledanje i menjanje Office dokumenata primljenih kao prilog u mail-ovima ili skladištenih u ShareFile aplikaciji.
- **Adobe Reader** – predstavlja aplikaciju za sigurno pregledanje pdf dokumenata primljenih kao prilog u mail-ovima ili skladištenih u ShareFile aplikaciji.
- **Fast Image viewer Free** – predstavlja aplikaciju namenjenu za sigurno gledanje slika.

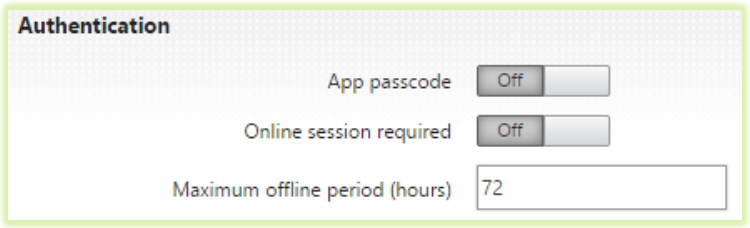
Korisnici EMM sistema na svojim mobilnim uređajima kroz korporativni AppStore preuzimaju korporativne aplikacije. WorxMail aplikacija se koristi za primanje i slanje korporativnih mail-ova dok se WorxWeb aplikacija koristiti za sigurno pregledanje linkova dobijenih u mail-ovima ili za siguran pristup ka internim veb aplikacijama. ShareFile aplikacija je namenjena za sigurno skladištenje i deljenje priloga dobijenih u mail-ovima kroz WorxMail aplikaciju i sigurno deljenje i pristupanje ka korporativnim dokumentima. Skladišteni dokumenti se dalje mogu sigurno deliti sa ostalim korisnicima sistema. Pored toga moguće je pregledati i vršiti izmene nad dokumentima korišćenjem WorxEdit aplikacije.

Kako bi se omogućila željena sigurnost nad korporativnim aplikacijama i podacima, nad korporativnim aplikacijama su konfigurisane polise koje su opisane u narednim poglavljima.

iii) Autentifikacija

Kako bi se obezbedio siguran pristup ka korporativnim aplikacijama i podacima kroz Device Manager server je izvršeno spuštanje passcode polise koja zahteva da na uređaju postoji PIN ili *pattern* za zaključavanje uređaja. Kako bi se omogućio što veći komfor u radu korisnika, za pristup svakoj od korporativnih aplikacija nije potrebno da se vrši dodatna autentifikacija. Samo u slučaju restarta mobilnog uređaja ili prilikom isteka korisničke sesije potrebno je da korisnik unese PIN za logovanje na WorxHome agent nakon čega je ponovo omogućen nesmetan pristup ka korporativnim aplikacijama. Maksimalno korišćenje aplikacija kada korisnik nema pristup internetu je 72 sata. Nakon što taj period istekne korisniku će biti onemogućen pristup ka korporativnim aplikacijama dok se ponovo ne uloguje na sistem putem mrežne internet konekcije.

Na Slici 4.8.15 je dat prikaz Authentication polise koja je konfigurisana nad svim iOS i Android korporativnim aplikacijama:

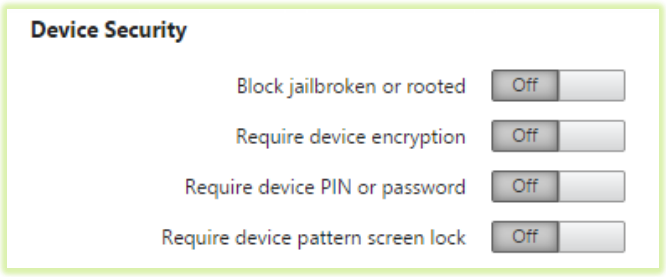


Slika 4.8.15. Authentication polisa nad korporativnim aplikacijama

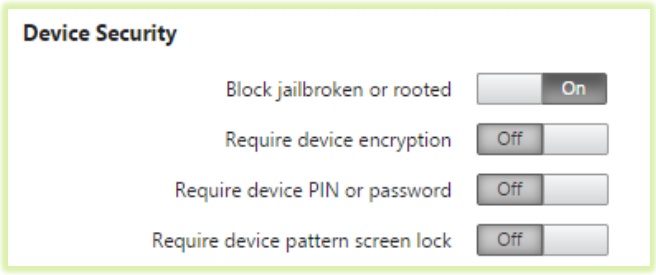
iv) Sigurnost mobilnih uređaja

S obzirom da je Passcode polisa primenjena za zaključavanje celog telefona korišćenjem Device Manager server-a nije potrebno vršiti dodatnu proveru postojanja PIN-a ili *pattern*-a prilikom pokretanja korporativne aplikacije zbog čega je ta provera isključena. Korporativne aplikacije je moguće koristiti i na *root*-ovanim i *jailbreak*-ovan uređajima osim WorxWeb i WorxMail aplikacije koje neće biti moguće startovati na *root*-ovanim/*jailbreak*-ovanim uređajima. Pošto se konfiguriše enkripcija samo nad korporativnim podacima nije potrebno da se dodatno zahteva enkripcija celog mobilnog uređaja kako bi se koristile korporativne aplikacije.

Na Slikama 4.8.16 i 4.8.17 je data konfiguracija polisa vezanih za sigurnost mobilnih uređaja prilikom izvršavanja korporativne aplikacije. Slika 4.8.16 se odnosi na sve aplikacije osim WorxWeb i WorxMail aplikacije, dok se Slika 4.8.17 odnosi na ove dve aplikacije.



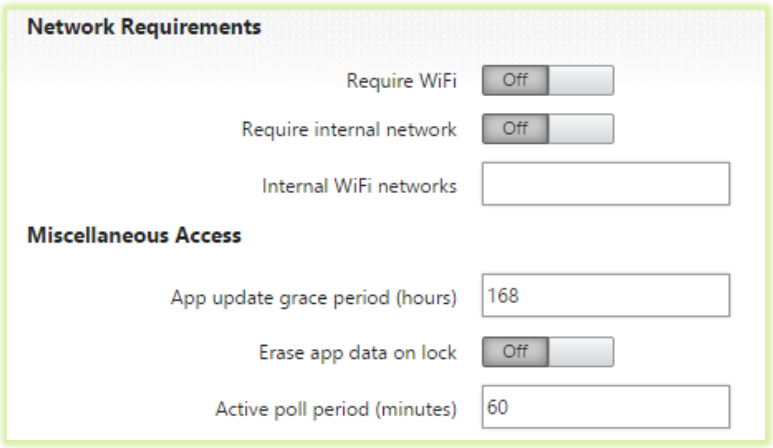
Slika 4.8.16. Device Security polise nad korporativnim aplikacijama



Slika 4.8.17. Device Security polise za WorxWeb i WorxMail aplikacije

v) Mreža i ažuriranje aplikacija

Polise koje se odnose na mrežu i ažuriranje aplikacija za cilj imaju definisanje da li je potrebno da uređaj bude konektovan na WiFi mrežu kako bi korporativna aplikacija mogla da se koristi. Pored toga, polisa definiše i ponašanje aplikacije nakon što se u sistem unese novija verzija aplikacije. Pošto smo u EMM sistemu definisali da je korisnicima omogućen pristup ka korporativnim resursima bez obzira gde se nalaze i da li pristup vrše putem WiFi ili 3G mreže, polisa koja zahteva da uređaj bude konektovan na WiFi mrežu kako bi aplikacija mogla da radi je isključena. Pored toga definisali smo da korisnici treba da izvrše ažuriranje aplikacije u periodu od 7 dana od kada se izvrši ubacivanje novije verzije aplikacije u sistem. Ukoliko se aplikacija ne ažurira za 7 dana, prilikom pokušaja startovanja javiće se greška koja ukazuje da mora da se uradi ažuriranje aplikacije kako bi mogla da se koristi i pristup ka aplikaciji će biti onemogućen sve dok se ne izvrši ažuriranje. Nakon ažuriranja sve će ponovo raditi, podaci u aplikaciji neće biti izgubljeni. Na Slika 4.8.18 je prikazana konfiguracija polisa koje se odnose na mrežu i ažuriranje aplikacija.

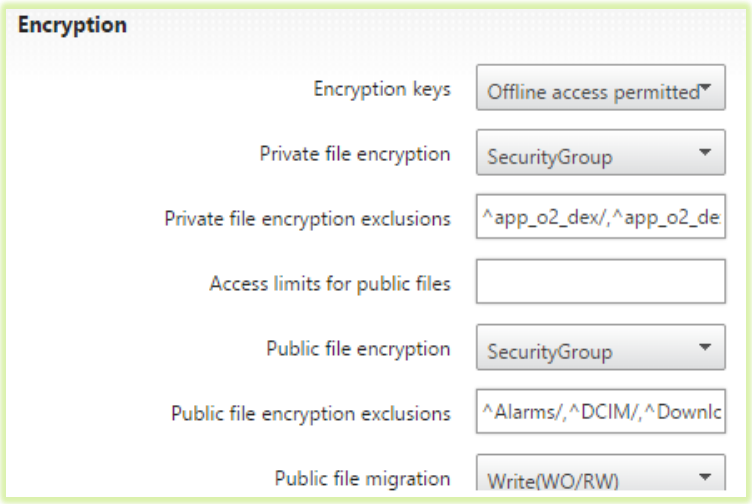


Slika 4.8.18. Network Requirements i Miscellaneous Access polise

vi) Enkripcija

Kako bi se obezbedila potpuna sigurnost nad korporativnim podacima potrebno je da oni budu enkriptovani. Enkripcija korporativnih podataka zajedno sa polisama za interakciju između aplikacija obezbeđuje željenu "kontejnerizaciju" nad korporativnim aplikacijama i podacima. U EMM sistemu definisana je enkripcija na nivou Security Grupe što znači da sve korporativne aplikacije dele isti enkripcioni ključ i mogu međusobno da čitaju korporativne podatke, dok su ti podaci za sve privatne aplikacije instalirane na mobilnom telefonu nečitljivi.

Na Slici 4.8.19 je dat prikaz konfigurisane polise za enkripciju podataka u okviru korporativnih aplikacija.



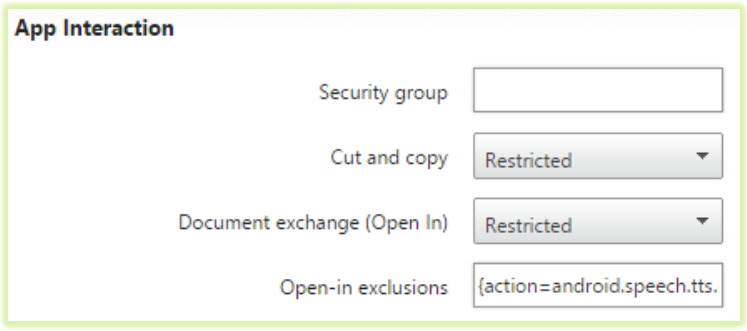
Slika 4.8.19. Encryption polisa

vii) Interakcija između aplikacija

Kako bi se obezbedila potpuna "kontejnerizacija" korporativnih podataka na mobilnim uređajima definisane su polise interakcije između aplikacija na takav način da samo korporativne aplikacije međusobno mogu da komuniciraju i razmenjuju korporativne podatke. Razmena podataka između korporativnih i privatnih aplikacija je zabranjena osim u sledećim slučajevima:

- Dozvoljena je sinhronizacija kontakata sa WorxMail aplikacije u kontakte privatnog dela telefona
- Dozvoljeno je upload-ovanje podataka iz privatnog dela telefona u WorxMail aplikaciju kako bi se isti poslali kao prilog u mailu.
- Dozvoljeno je upload-ovanje podataka iz privatnog dela telefona u ShareFile aplikaciju kako bi se isti mogli deliti sa ostalim korisnicima sistema.

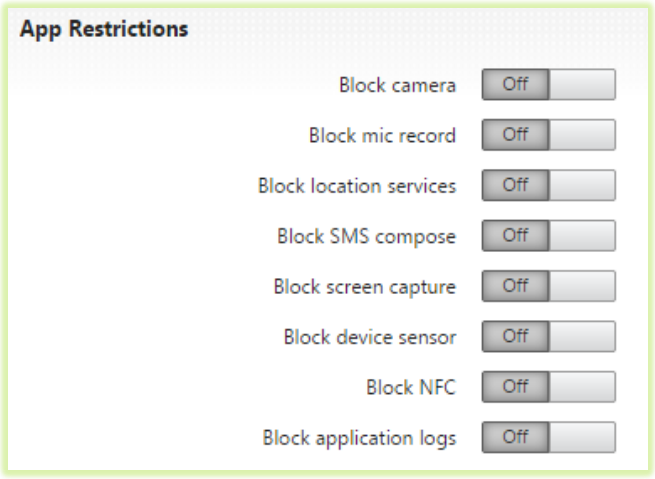
Na Slici 4.8.20 je dat prikat konfigurisane polise interakcije između aplikacija. Dozvoljeno je kopiranje podataka i razmena podataka samo između korporativnih aplikacija.



Slika 4.8.20. App Interaction polisa

viii)Ograničenja nad aplikacijama

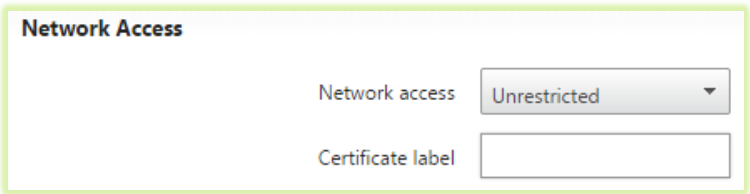
Radi ostvarivanja što većeg komfora prilikom korišćenja korporativnih aplikacija, nad aplikacijama nisu primenjene restriktivne polise poput blokiranja kamere, mikrofona ili GPS-a na mobilnom uređaju. Na Slici 4.8.21 se mogu videti konfigurisane polise.



Slika 4.8.21. App Restrictions polise

ix) Mrežni pristup za WorxWeb, ShareFile i WorxEdit aplikacije

Za nesmetan rad korporativnih aplikacija Network Access polisa je stavljena na Unrestricted što znači da će aplikacija moći da radi prilikom konekcije na bilo koju mrežu. Ova unrestricted polisa se odnosi na sve aplikacije osim WorxWeb. S obzirom da WorxWeb aplikacija omogućava pristup ka internim veb aplikacijama za nju je Network access polisa stavljena na Tunneled to the internal network što govori aplikaciji da mora da koristi micro vpn tehnologiju za pristup ka internim veb aplikacijama o čemu će biti više reči u nastavku ovog poglavlja. Slika 4.8.22 daje prikaz Network Access polisa za sve korporativne aplikacije osim za WorxWeb aplikaciju.



Slika 4.8.22. Network Access polisa

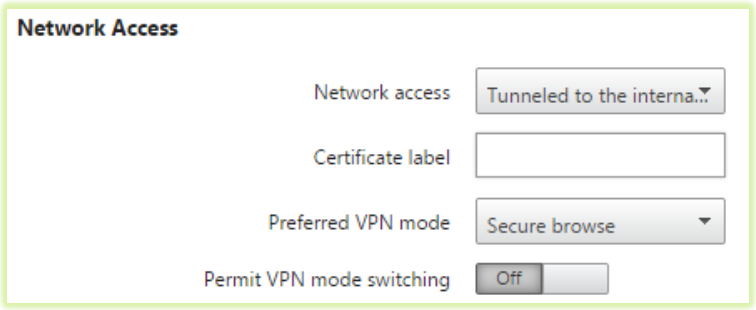
4.8.3. Implementacija Micro VPN funkcionalnosti i polisa za WorxWeb

WorxWeb aplikacija je namenjena za siguran pristup ka internim veb aplikacijama sa mobilnih uređaja kao i za sigurno otvaranje linkova primljenih u WorxMail aplikaciji. Kako bi se ostvarile ove funkcionalnosti izvršeno je implementiranje Micro VPN tehnologije.

Da bi se izvršila implementacija Micro VPN funkcionalnosti potrebna je odgovarajuća konfiguracija NetScaler uređaja koji predstavlja ulaznu tačku za mobilne uređaje koji pristupaju internoj mreži kompanije.

Zbog složenosti konfiguracije ona ovde neće biti prikazana.

Na mobilnoj WorxWeb aplikaciji izvršena je konfiguracija Network Access polise što je prikazano Slici 4.8.23.



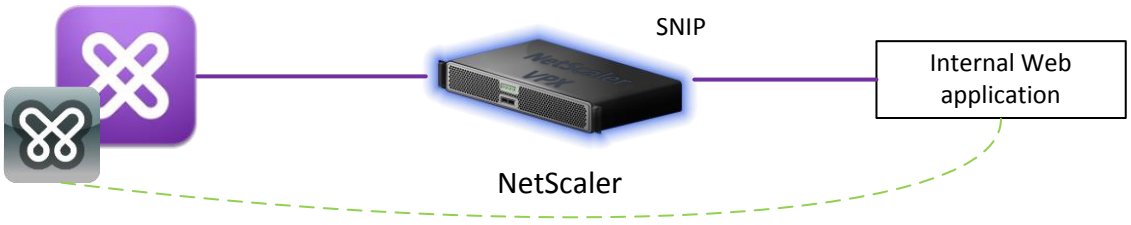
Slika 4.8.23. Network Access polisa za WorxWeb aplikaicju

Prilikom prvog startovanja WorxWeb aplikacija će proveriti definisane polise i Tunnel to the internal network polisa će joj reći da treba da uspostavi MicroVPN ka internim aplikacijama. WorxHome aplikacija će pokrenuti MicroVPN do NetScaler-a za WorxWeb aplikaciju. Kada se uspostavi MicroVPN tunel NetScaler na mobilni uređaj šalje konfiguraciju DNS-a. U NetScaler konfiguraciji je definisano da je -splitDns REMOTE što znači da će mobilni telefon sve DNS upite slati NetScaleru na razrešavanje.

MicroVPN može da se podeli na dva dela komunikacije:

- Komunikacija od WorxHome aplikacije do NetScaler uređaja
- Komunikaciju od SNIP adrese NetScaler uređaja do internih aplikacija.

Za krajnjeg korisnika MicroVPN izgleda kao da WorxWeb aplikacija direktno komunicira sa internim veb aplikacijama. MicroVPN je prikazan na Slici 4.8.24.

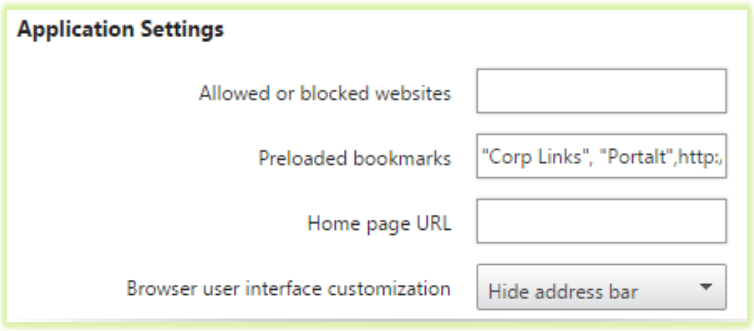


Slika 4.8.24. MicroVPN za pristup ka internim web aplikacijama

Kako bi se omogućilo da korisnici pristupaju iz WorxWeb aplikacije samo ka internim veb aplikacijama i ka linkovima primljenim u WorxMail aplikaciji, a da ne mogu da koriste WorxWeb aplikaciju za ostalo veb pretraživanje definisana je sledeća polisa:

Browser user interface customization – Hide address bar

Ova polisa je prikazana na Slici 4.8.25.



Slika 4.8.25. Prikaz Browser user interface customization polise

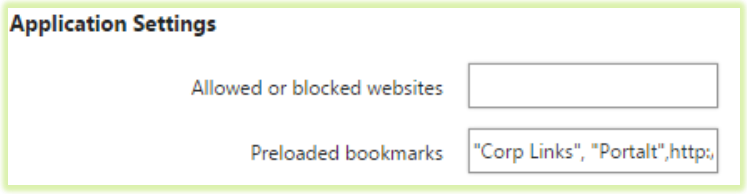
Ovom polisom je omogućeno da korisnici ne mogu u adresni bar WorxWeb aplikacije da ukucaju veb stranice kako bi ih pretraživali već mogu da otvore samo stranice koje su već predefinisane u Favorites delu aplikacije ili linkove primljene u email-u kroz WorxMail aplikaciju.

Polisa koja omogućava da se u WorxWeb aplikaciji nalaze predefinisane veb stranice ka internim veb aplikacijama je omogućena polisom Preloaded bookmarks.

Za dodavanje novih linkova potrebno je da se u već definisanu polisu doda novi link na sledeći način:

"Corp Links", “Ime”,https://link

Ova polisa je prikazana na Slici 4.8.26.



Slika 4.8.26. Polisa za definisanje Bookmarka u WorxWeb aplikaciji

4.8.4. Implementacija automatskog kreiranja korisničkih naloga u ShareFile cloudu i SSO funkcionalnosti za ShareFile

ShareFile se kao zaseban Citrix proizvod koristi za sigurno čuvanje i deljenje korporativnih podataka. On predstavlja korporativnu zamenu za DropBox i Google Drive rešenja. Postoje dva osnovna načina kako je moguće realizovatni ShareFile. Prvi način je da se korporativni podaci nalaze u Citrix cloudu dok je drugi način da se korporativni podaci nalaze u data centru korisnika dok se “control” saobraćaj nalazi u Citrix cloudu. Pored toga postoji više načina na koji korisnici mogu da se autentifikuju na ShareFile:

- Korisnički username i password se nalaze u control plane-u u Citrix cloudu i koriste se za autentifikaciju korisnika
- Korisnici se autentifikuju korišćenjem domenskog username-a i password-a na ShareFile

Kako bi korisnici mogli da se autentifikuju na ShareFile potrebno je da u “control plane-u” u Citrix cloudu postoje informacije o njima. Postoji više načina na koji je moguće obezbediti te informacije:

- Ručno kreiranje korisnika u ShareFile control plane-u u cloudu
- Korišćenjem Citrix User Management Tool-a (UMT) moguće je automatski kreirati korisnike iz LDAP-a u control plane-u ShareFile-a u cloud-u.
- AppController automatski može da kreira korisnike iz LDAP-a u control plane-u ShareFile-a u cloudu.

Prilikom automatskog kreiranja korisnika korišćenjem UMT-a ili AppController-a, u ShareFile control plane-u se iz LDAP-a dobijaju sledeće informacije: Ime, Prezime i email adresa. ShareFile control plane za svakog korisnika kreira nasumični *password* koji koristi za svoje interne provere. Korisnik može da promeni taj password i ukoliko nije konfiguirsano logovanje korišćenjem domenskih kredencijala onda se taj password koristi za logovanje na ShareFile.

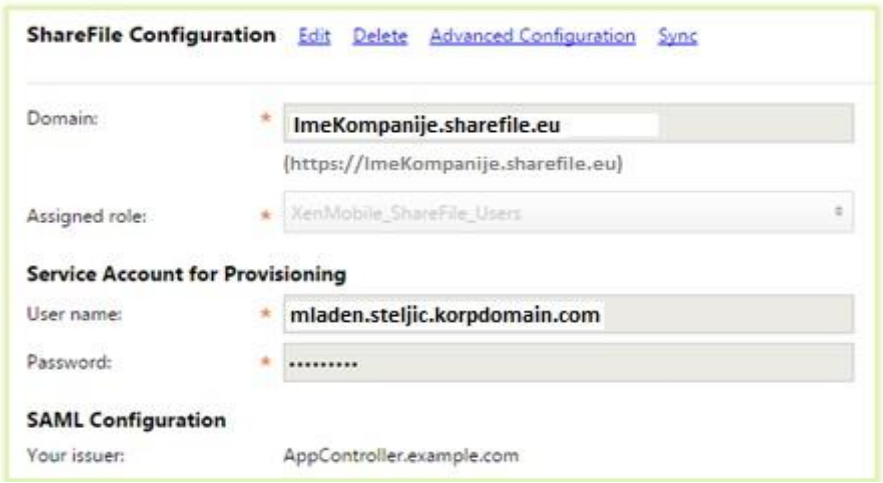
ShareFile kao proizvod podržava više mogućnosti pristupa ka korporativnim podacima kao što su pristup putem veb brauzera, instalacijom sync plug-in na Windows računarima, korišćenjem ShareFile aplikacije preuzete sa AppStore-a ili Play Store-a, kao i korišćenjem ShareFile aplikacije sa ubačenom MDX logikom.

U konkretnom EMM sistemu ShareFile je implementiran "on premise" što znači da se korporativni podaci nalaze u data centru kompanije dok se "control" saobraćaj nalazi u Citrix cloudu. Kreiranje korisnika u ShareFile control plane-u u cloudu se vrši korišćenjem AppController-a i autentifikacija korisnika je konfigurisana tako da se koriste domensko korissničko ime i šifra.

Kako bi se obezbedilo automatsko kreiranje korisničkih naloga u ShareFile control plane-u u cloud-u korišćenjem Appcontroller-a, izvršeno je povezivanje ShareFile control plane-a sa AppController-om. Od strane Citrix-a za kompaniju se pravi control plane **https://imekompanije.sharefile.eu/**

Konfiguracija za automatsko kreiranje korisnika u ShareFile control plane-u i za SSO (*Single Sign-On*) data je u nastavku.

Na AppController-u je izvršeno povezivanje sa ShareFile control plane-om u cloudu na sledeći način koji je prikazan na Slici 4.8.27.



Slika 4.8.27. Povezivanje AppController-a sa ShareFile control plane-om

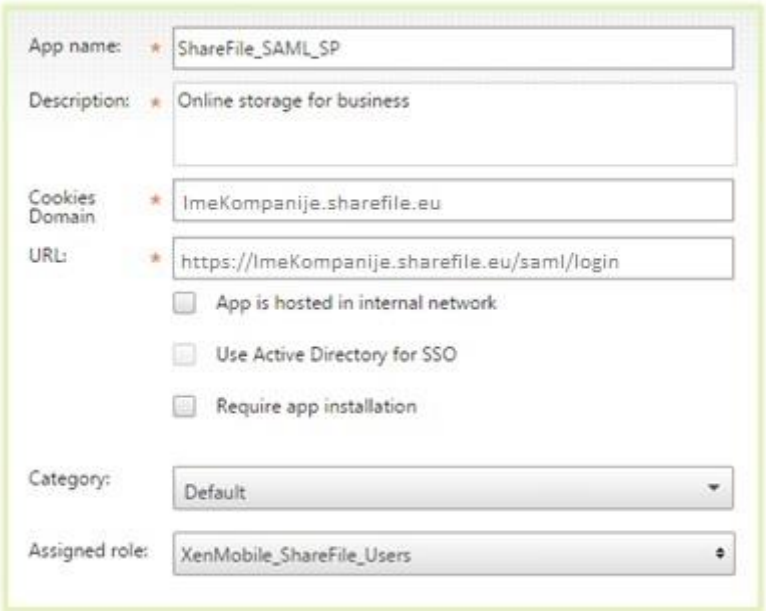
ShareFile aplikacija se koristi za sigurno čuvanje i deljenje korporativnih podataka.

U EMM sistemu namenjeno je da se za pristup ka korporativnim podacima koristi ShareFile veb aplikacija, Sync Tool za Windows i ShareFile mobilna aplikacija sa ubačenom MDX logikom.

Nakon povezivanja AppController-a sa ShareFile control plane-om u control plane-u će se pojaviti neophodne informacije za obezbeđivanje autentifikacije domenskim kredencijalima za pristup ka ShareFile dokumentima.

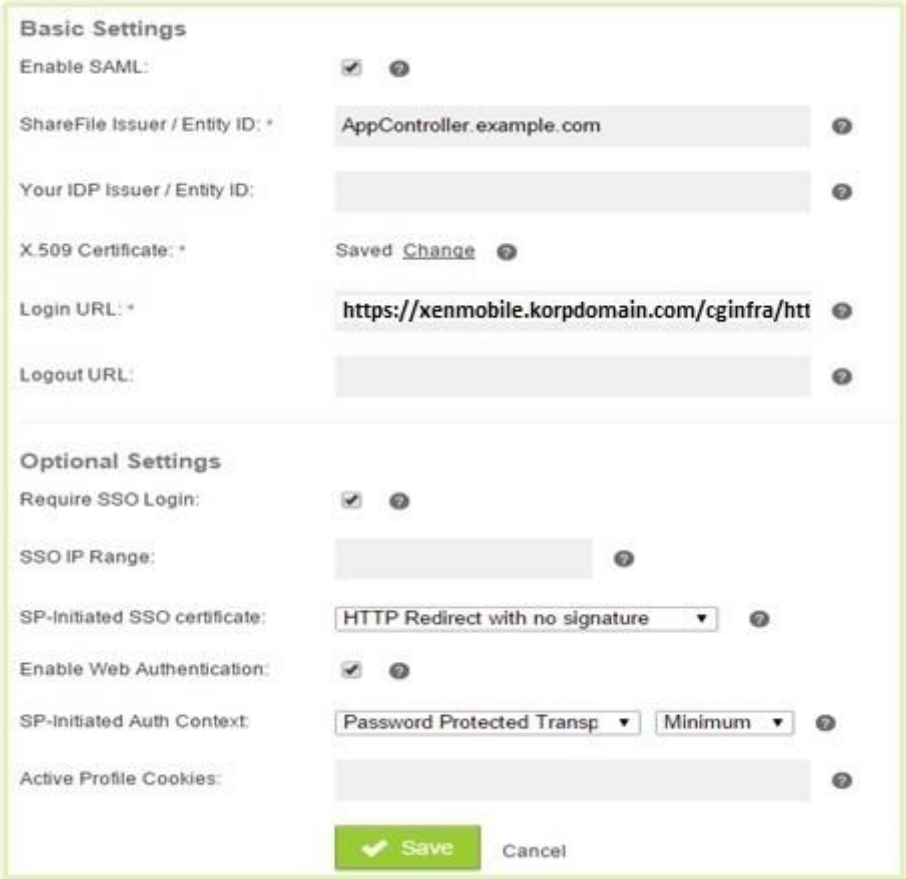
Nakon ovog povezivanja biće moguće pristupiti ka ShareFile dokumentima samo korišćenjem ShareFile mobilne MDX aplikacije. Kako bi se korisnicima omogućio pristup ka ShareFile dokumentima i iz veb brauzera i sa Windows Sync Tool-a potrebno je da se izvrši sledeća konfiguracija koja je opisana u nastavku.

U Web & SaaS tabu je konfigurisana aplikacija ShareFile_SAML_SP na sledeći način prikazan na Slici 4.8.28.



Slika 4.8.28. Konfiguracija ShareFile_SAML_SP aplikacije

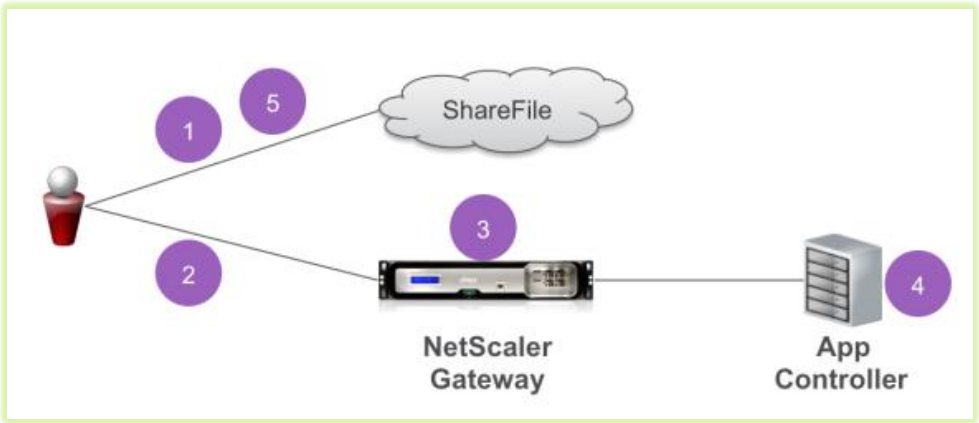
ShareFile control plane konfiguracija u Admin > Configure Single Sign-On i prikazana je na Slika 4.8.29.



Slika 4.8.29. SSO ShareFile konfiguracija u control plane-u

Gore navedenom konfiguracijom je omogućeno da korisnici mogu da pristupaju ka ShareFile dokumentima korišćenjem pristupa kroz veb brauzer, Windows Sync tool i ShareFile MDX mobilnu aplikaciju i da mogu da se autentifikuju sa domenskim kredencijalima.

Domensko logovanje funkcioniše na način prikazan na Slici 4.8.30.



Slika 4.8.30. SAML autentifikacija

1) Korisnik iz web browsera odlazi na stranicu https://imekompanije.sharefile.eu/saml/login
2) ShareFile control plane vrši redirekciju na https://xenmobile.imekompanije.com/vpn/index.html

3) Korsnik unosi svoj domenski username i password
4) Vrši se SSO na AppController-u koji korisniku vraća SAML token
5) SAML token se prosleđuje na https://imekompanije.sharefile.eu gde se završava autentifikacija i korisnicima se predstavljaju dokumenti smešteni na ShareFile-u

4.8.5. Implementacija pristupa dokumentima na ShareFile-u

Kako bi se omogućilo skladištenje ShareFile dokumenata na lokalnom CIFS share storage-u koji se nalazi u data centru kompanije potrebno je da se izvrši sledeća konfiguracija opisana u nastavku.

Izvršena je instalacija ShareFile Storage Zone komponente koja je povezana sa lokalnim CIFS file share-om koji se nalazi u data centru kompanije. Takođe je izvršeno povezivanje ShareFile storage zone-a sa ShareFile control plane-om u cloudu.

Na NetScaleru je izvršena potrebna konfiguracija SSL (*Secure Sockets Layer*) offloada za pristup ka ShareFile dokumentima smeštenim na lokalnom CIFS share-u.

U ShareFile control plane-u u cloudu se nakon instalacije ShareFile Storage Zone-a i konfiguracije NetScaler-a pojavljuju sledeće informacije prikazane na Slici 4.8.31.

Odlaskom na https://imekompanije.sharefile.eu/> Admin >StorageZone vide se sledeće informacije:

Slika 4.8.31. ShareFile Storage Zone informacije u Cloudu

4.9. Wrapping aplikacija

Funkcionalnosti MAM komponente EMM rešenja nam omogućavaju da sigurno upravljamo aplikacijama na mobilnim uređajima kao i da sigurno isporučujemo mobilne aplikacije na uređaje korisnika. Sa Citrix-ovim MDX Toolkit-om možemo pakovati (*wrapping*) iOS i Android aplikacije da bismo obezbedili siguran pristup aplikacijama koje su hostovane u internoj mreži kompanije i da bismo na lak način primenjivali i sprovodili polise.

U postupku *wrapping*-a, dinamičke biblioteke dobijene od EMM vendora se ugrađuju u binarne fajlove aplikacije, ali posle samog razvoja aplikacije. Pakovanje aplikacija zamenjuje standardni sistem kontejnerizacije koji podrazumeva menjanje koda aplikacije, tako što dodaju novi sloj u aplikaciji sa ciljem zaštite i upravljanja istom, kada se ona nađe na mobilnom uređaju

korisnika. Programeri ne moraju u ovom slučaju da integrišu kod svoje aplikacije sa nekim vendorskim kodom. Sve što je potrebno uraditi je da administratori EMM sistema kroz Citrix-ov MDX Toolkit "ugrade" sigurnosne i kontrolne funkcionalnosti. Ovako "upakovana" aplikacija se može na siguran način isporučiti na korisničke mobilne uređaje, a zatim na nju primeniti odgovarajuće definisane polise, što će omogućiti bezbedno korišćenje ovih aplikacija u skladu sa korporativnom sigurnosnom politikom.

Posle „pakovanja" aplikacije možemo je upload-ovati na App Controler koji smo već pominjali kao komponentu Citrix-ovog EMM rešenja, i konfigurisati MDX polise. Posle toga korisnici mogu preuzeti aplikaciju sa App Controller-a pomoću Worx Home. Zatim mogu otvoriti i koristiti aplikaciju na svojim mobilnim uređajima pristupajući resursima u internoj mreži kompanije, naravno sve u skladu sa sigurnosnom politikom kompanije.

4.9.1. Kako radi MDX toolkit

Citrix isporučuje MDX toolkit alat tako da obezbeđuje pakovanje aplikacija, za uređaje sa iOS i Android operativnim sistemima, sa Citrix-ovom logikom i polisama. Ovaj alat može pakovati aplikacije koje su interno razvijene u kompaniji, kao i druge aplikacije preuzete sa javnih app store-ova, na takav način da se one kasnije mogu sigurno instalirati i koristiti na mobilnim uređajima zaposlenih. Kada instaliramo MDX Toolkit u našem okruženju, Worx SDK biblioteka se takođe instalira i pojavljuje u MDX SDK folderima na radnoj stanici na kojoj se instalacija izvršava. MDX SDK folderi su obavezni da bi se obezbedila integracija pakovanih iOS mobilnih aplikacija sa Citrix Worx-om.

Posle pakovanja, aplikaciju možemo učitati na naš App Controller. Koristeći upravljačku konzolu konfigurišemo specifične performanse aplikacije kao i podešavanja polisa čije će izvršavanje biti realizovano tokom instalacije aplikacije na korisničkom mobilnom uređaju. Kada korisnik pristupi App Store-u na App Controler-u kroz Worx Home aplikaciju, upakovana aplikacija će se pojaviti sa mogućnošću preuzimanja, i instaliranja, posle čega će njeno korišćenje biti omogućeno u skladu sa polisama koje su definisane za datu aplikaciju [10].

4.9.2. Postupak wrapping-a

Ovde ćemo opisati sam postupak wrapping-a na primeru Andoid aplikacija u konkretnom slučaju.

Na MAC računaru su instaliran isporučeni MDX Toolkit alat kako bi se ostvario uspešan wrapping Android aplikacija.

Tokom wrapping-a Android aplikacija potrebno je da se izvrši njihovo potpisivanje. Za tu namenu je izvršeno kreiranje sertifikata sledećom komandom:

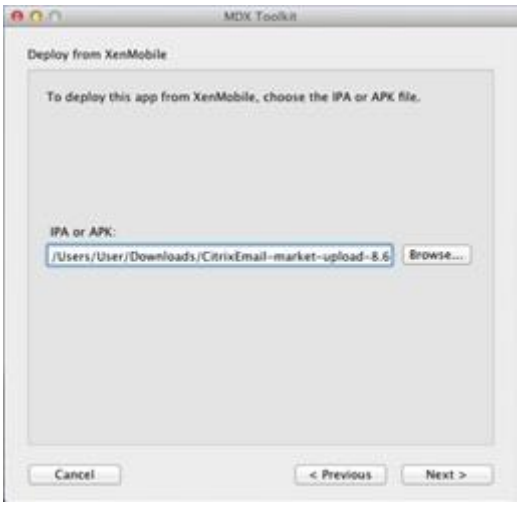
```
Keytool –genkey –keyalg DSA –alias mdm.keystore –storepass PASSWORD –
 keysize1024
```

Kreirani sertifikat se nalazi na sledećoj lokaciji na MAC računaru:

/Users/User/Downloads/emm.keystore

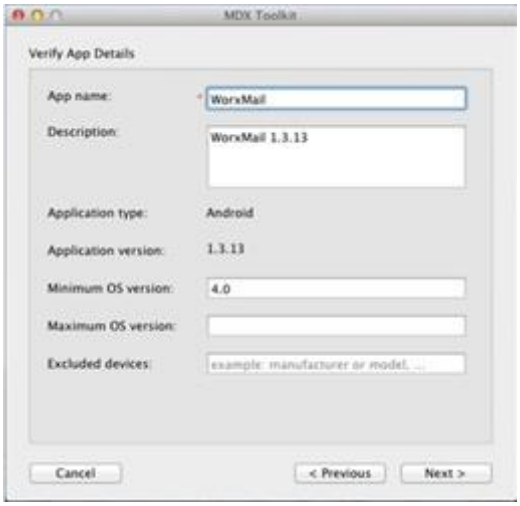
Prilikom pokretanja MDX Toolkit alata potrebno je da se izabere aplikacija u .ipa ili apk formatu. Na slici 4.9.1 prikazano je biranje aplikacije sa XenMobile komponente sistema, tj. u pitanju je korporativna aplikacija, a ne aplikacija sa nekog eksternog AppStore-a, dok na slici 4.9.2 vidimo učitavanje konkretne aplikacije u zahtevanom formatu.

Slika 4.9.1. Izbor lokacije odakle će biti učitana aplikacija



Slika 4.9.2. Učitavanje aplikacije u željenom formatu

Na Slici 4.9.3 je prikazan pimer aplikacije učitane u MDX Toolkit koja je sada spremna za pakovanje. U primeru je data aplikacija WorxMail.



Slika 4.9.3. Primer aplikacije učitane u MDX Toolkit

U Keystore selection opciji potrebno je izabrati putanju do sertifikata koja je u našem slučaju/Users/User/Downloads/emm.keystore. Ovo je prikazano na slici 4.9.4.

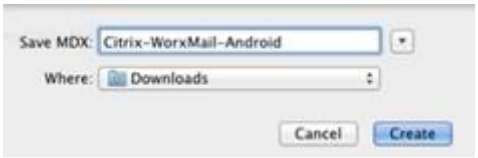
Slika 4.9.4. Biranje lokacije keystore-a

Zatim se pojavljuje prozor, kao na slici 4.9.5 za unos Keystore password-a. Ovde je potrebno uneti PASSWORD naveden u komandi prilikom kreiranja sertifikata.

Slika 4.9.5. Prozor za unos Keystore Password-a

U prozoru gde se bira alias trebalo bi da stoji keystore.mdm, a key alias password koji se zatim zahteva je isti onaj koji je unet prilikom kreiranja sertifikata.

Zatim se pojavljuje prozor gde je potrebno uneti naziv, sada upakovane aplikacije, kao i mesto na računaru gde će ona biti smeštena. Prikaz prozora na slici 4.9.6.



Slika 4.9.6. Unos naziva i mesto smeštanja pakovane aplikacije

Nakon ovog koraka trebalo bi da se pojavi prozor kao na slici 4.9.7 sa opcijom Show in Folder, čime je proces wrapping-a aplikacije završen. Posle ovoga aplikacija se može sigurno učitati na korporativni App Store na App Controller-u odakle dalje može biti distribuirana korisnicima na sigurno korišćenje.

Slika 4.9.7. Kraj procesa pakovanja aplikacije

5. PRIKAZ REZULTATA TESTIRANJA IMPLEMENTIRANOG REŠENJA

Kao što smo već opisali u poglavlju gde je govoreno o implementaciji konkretnog rešenja, namena EMMsistema je da obezbedi sigurnost nad korporativnim podacima koji se nalaze na mobilnim uređajima. U narednih nekoliko paragrafa ukratko je rečeno šta je sve postignuto implementiranim rešenjem i njegovim funkcionalnostima.

Sigurnost nad korporativnim podacima se obezbeđuje tako što se vrši izolacija poslovnog od privatnog dela mobilnog uređaja. Poslovni podaci bivaju zaštićeni enkripcijom dok privatni podaci na telefonu ostaju netaknuti tj. neizmenjeni.

Pored sigurnosti poslovnih podataka koji se nalaze na mobilnom uređaju EMM sistem omogućava i siguran pristup ka resursima u internoj mreži korišćenjem Micro VPN tehnologije. Ova tehnologija omogućava da bez podignutog globalnog VPN-a na mobilnom uređaju korisnik može sa interneta na siguran način da pristupi ka potrebnim resursima u internoj mreži Banke.

Takođe, EMM sistem omogućava i selektivno brisanje poslovnih podataka sa mobilnog uređaja u slučaju da je npr. telefon ukraden ili korisnik menja firmu pa više nema potrebe za čuvanjem poslovnih podataka na mobilnom uređaju.

Korisnicima čiji se mobilni uređaji nalaze pod kontrolom EMM sistema je omogućen pristup ka korporativnom AppStore-u odakle mogu da preuzmu aplikacije koje su za njih namenjene. Ovo praktično znači da različiti korisnici u korporativnom AppStore-u mogu da vide i preuzmu različite korporativne aplikacije.

5.1. Korišćene aplikacije

Korisnicima čiji se mobilni uređaji nalaze pod kontrolom EMM sistema je omogućen pristup ka korporativnom AppStore-u odakle mogu da preuzmu aplikacije koje su za njih namenjene. Ovo praktično znači da različiti korisnici u korporativnom AppStore-u mogu da vide i preuzmu različite korporativne aplikacije.

Korporativne aplikacije koje se koriste u konkretnom EMM sistemu su:

- **WorxMail** – korporativni mail klijent
- **WorxWeb** – brauzer za siguran pristup ka korporativnim web aplikacijama
- **WorxEdit** – aplikacija namenjena za gledanje i izmene office dokumenata
- **ShareFile** – sigurno smeštanje dokumenata na mobilnom uređaju

Korisnici će prilikom pristupa korporativnom AppStore-u videti ili neke od ove četiri aplikacije ili će videti sve četiri aplikacije. Odluka koje aplikacije će korisnik videti i moći da koristi je doneta na osnovu poslovnih potreba samog korisnika.

Kako bi se obezbedila dodatna zaštita nad korporativnim podacima svi telefoni koji se nalaze u EMM sistemu će morati da se zaključavaju korišćenjem PIN-a. Ovom polisom se obezbeđuje povećanje sigurnosti i nad privatnim podacima korisnika. Pored toga svi poslovni podaci se nalaze u okviru enkriptovanog kontejnera nad kojim takođe postoji definisana autentifikacija PIN-om. Ovaj PIN koji se definiše nad poslovnim podacima je u potpunosti nezavisan od PIN-a koji se definiše za globalno zaključavanje samog telefona. Ovo praktično znači da ova dva PIN-a mogu da se razlikuju. Takođe, ukoliko korisnik poseduje više mobilnih uređaja koji se nalaze u EMM sistemu, na svakom od njih može da ima drugačije PIN-ove za zaključavanje samog telefona i pristup ka kontejneru.

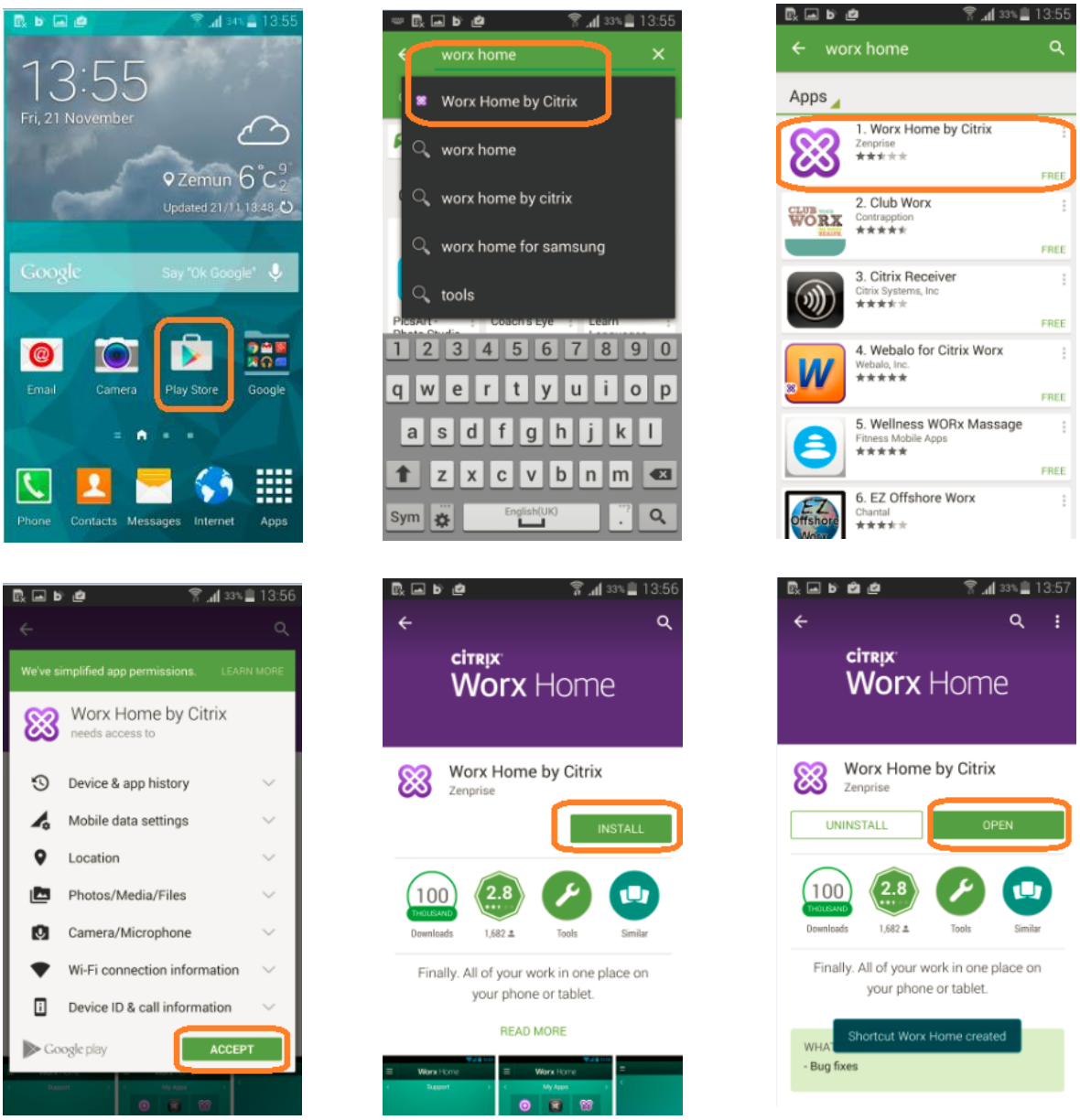
U ovom poglavlju ćemo, kroz konkretne poslovne potrebe, prikazati rezultate testiranja funkcionalnosti implementiranog EMM rešenja. Najčešća poslovna potreba zaposlenih su svakako siguran pristup elektronskoj pošti, siguran pristup aplikacijama hostovanim u internoj mreži kompanije i sigurno preuzimanje i deljenje korporativnih podataka i dokumenata. Šta je potrebno uraditi u sistemu da bi se ove funkcionalnosti korisnicima i omogućile biće opisano u narednim odeljcima.

5.1.1. Uvođenje uređaja u EMM sistem (enrollment)

Da bi se korisnicima uopšte obezbedio pristup korporativnom App Store-u, odakle će moći da preuzmu i instaliraju aplikacije koje će kasnije koristiti na svojim mobilnim uređajima, potrebno je da se prvo registruju u EMM korporativni sistem. Ubacivanje uređaja u EMM sistem je proces koji se naziva enrollment. Kako bi korisnik mogao da svoj mobilni uređaj ubaci u EMM sistem prvo je potrebno da mu se od strane administratora EMM sistema obezbede korisnička prava, što se postiže ubacivanjem korisnika u odgovarajuće grupe na AD-u. Nakon toga je potrebno da korisnik isprati sledeću proceduru datu u slikama kako bi uspešno mogao da doda svoj uređaj u EMM sistem.

Potrebno je da korisnik sa Google Play-ja preuzme i na svom uređaju instalira WorxHome aplikaciju.

Na slici 5.1.1 je prikazan postupak preuzimanja WorxHome aplikacije.



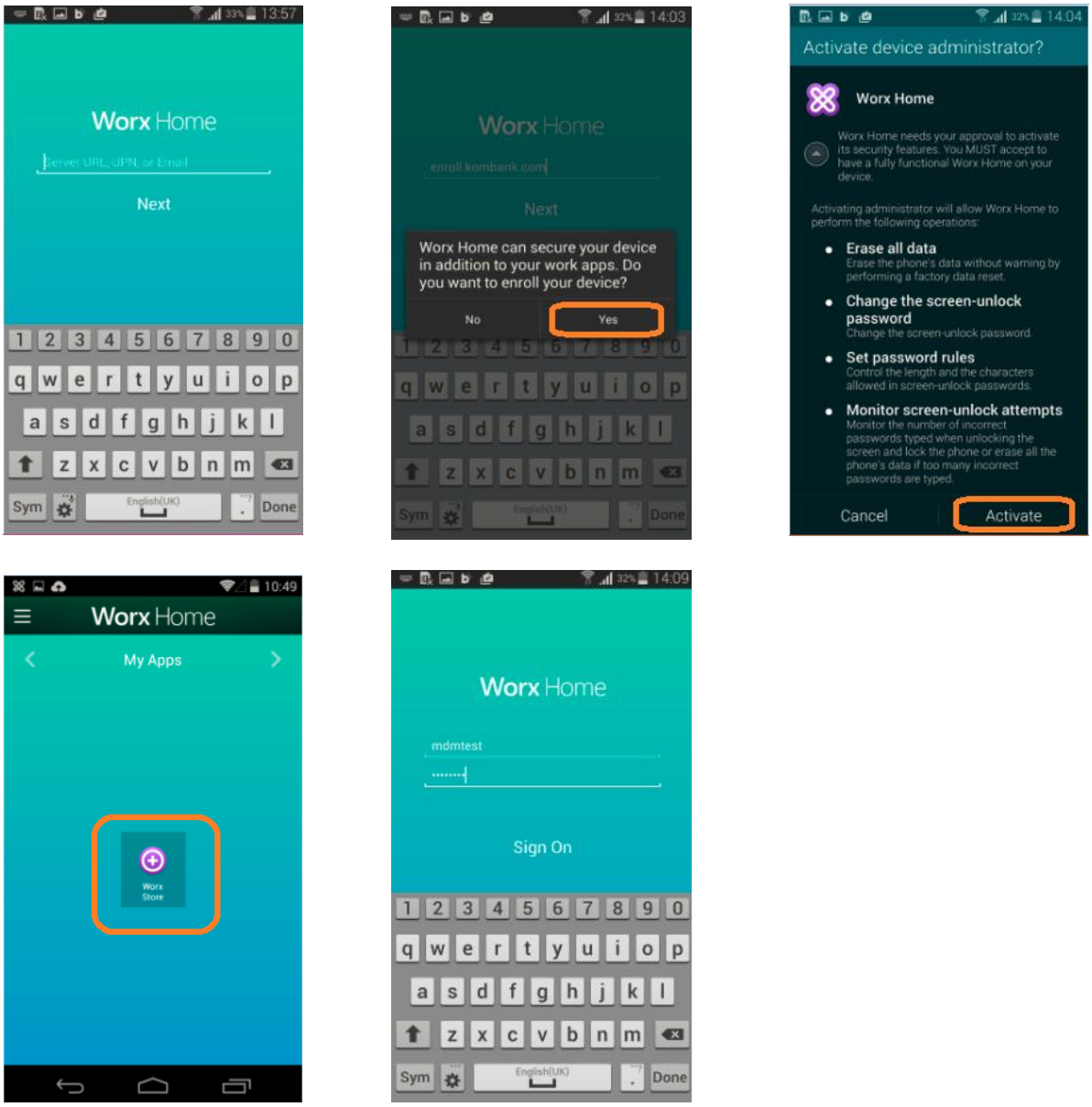
Slika 5.1.1. Preuzimanje WorxHome aplikacije

Prilikom prvog pokretanja aplikacije potrebno je da se kao adresa servera otkuca **enroll.imekompanije.com.**

Zatim je potrebno da se korisnik uloguje sa svojim domenskim kredencijalima, npr:

User: ime.prezime
Pass: ****

U ovom konkretnom slučaju napravljeno je testno korisničko ime mdmtest, koje je zatim ubačeno u odgovarajuću sigurnosnu grupu u Active Directory-ju. Na slici 5.1.2 su prikazani koraci koje je potrebno proći prilikom procesa registracije uređaja u sistem.



Slika 5.1.2. Proces enrollment-a mobilnih uređaja

Ovim je proces ubacivanja mobilnog uređaja u EMM sistem uspešno završen. Korisnici sada mogu da preuzmu korporativne aplikacije namenjene za njih, što je definisano polisama kroz MAM rešenje.

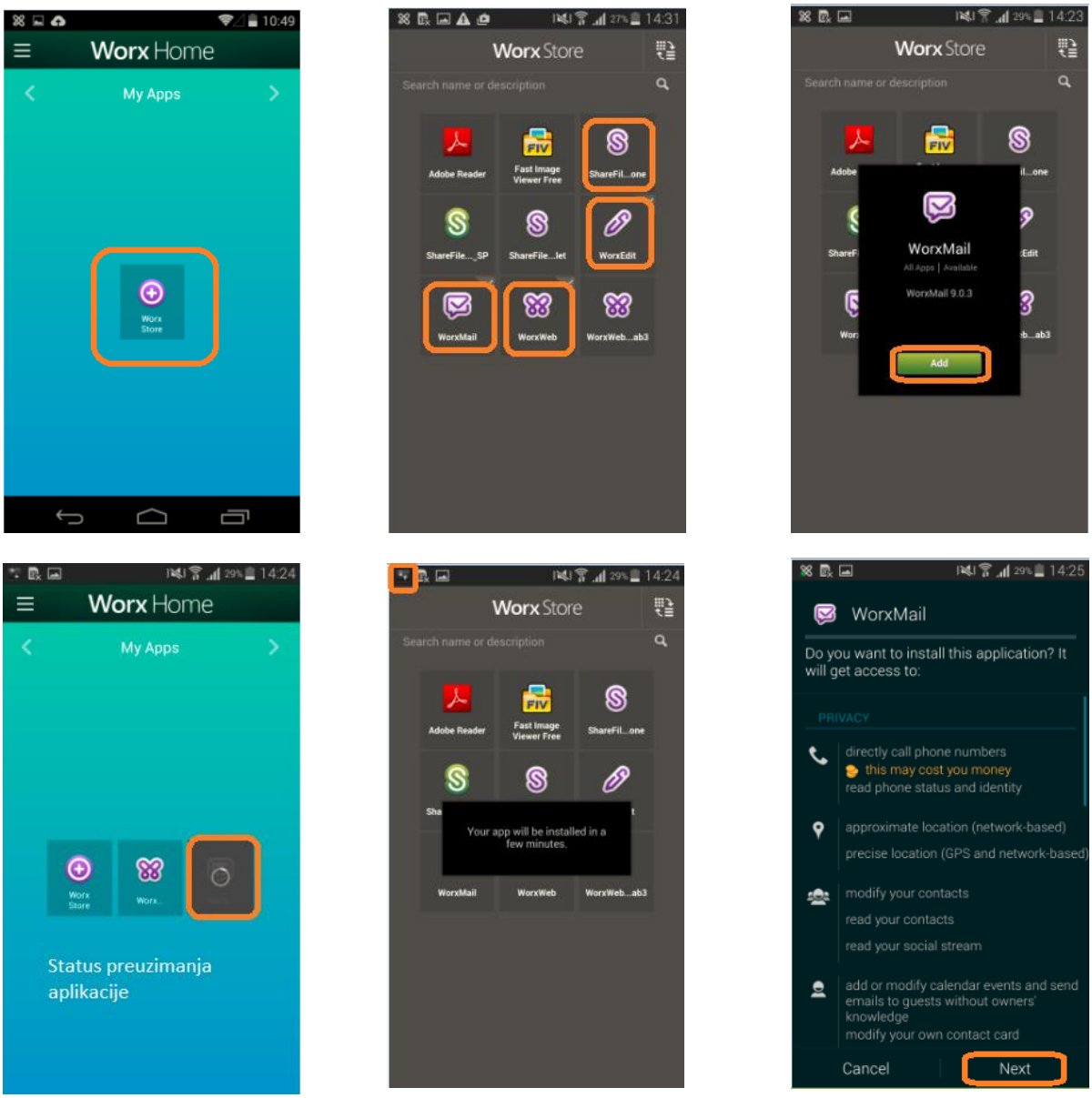
5.1.2. Preuzimanje aplikacija

Nakon što se telefon ubaci u EMM sistem sa njega je korisnicima omogućen pristup ka korporativnom AppStore-u sa kojeg mogu da se preuzimaju željene aplikacije. Sam proces preuzimanja je sledeći:

1) Potrebno je kliknuti na WorxStore ikonicu
2) Kliknuti na željenu aplikaciju
3) Odabrati add i ispratiti da se aplikacija uspešno preuzima na mobilni uređaj
4) Nakon preuzimanja potrebno je instalirati aplikaciju

5) Ovaj postupak je potrebno ponoviti za svaku aplikaciju koju korisnik želi da koristi.

Na slici 5.1.3 prikazan je postupak preuzimanja aplikacije sa korporativnog AppStore-a.



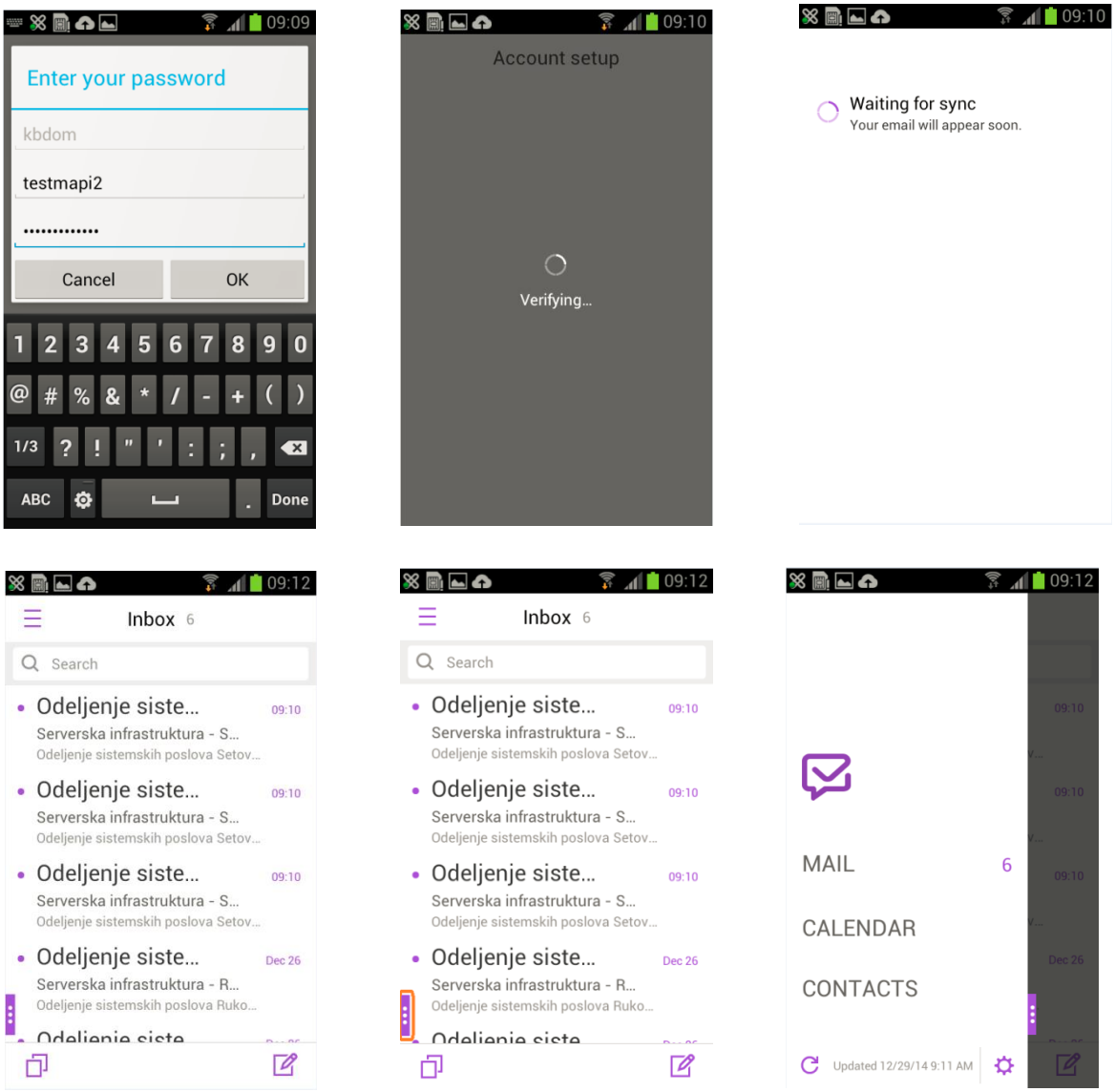
Slika 5.1.3. Postupak preuzimanja aplikacije sa korporativnog App Store-a

5.1.3. WorxMail

WorxMail aplikacija je namenjena za sigurnu sinhronizaciju korporativnih mail-ova, kontakata i kalendara. Svi podaci u okviru WorxMail aplikacije su enkriptovani i postoji mogućnost njihovog udaljenog brisanja u slučaju da se za tako nečim ukaže potreba.

Worx Mail aplikacija može da se preuzme samo sa korporativnog AppStore-a. Nakon instalacije na mobilnom uređaju prilikom prvog pokretanja aplikacije potrebno je da se unese domenska lozinka nakon čega će početi proces sinhronizacije mail-ova na mobilni uređaj.

Na Slici 5.1.4 može se videti kako izgleda Worx Mail aplikacija.

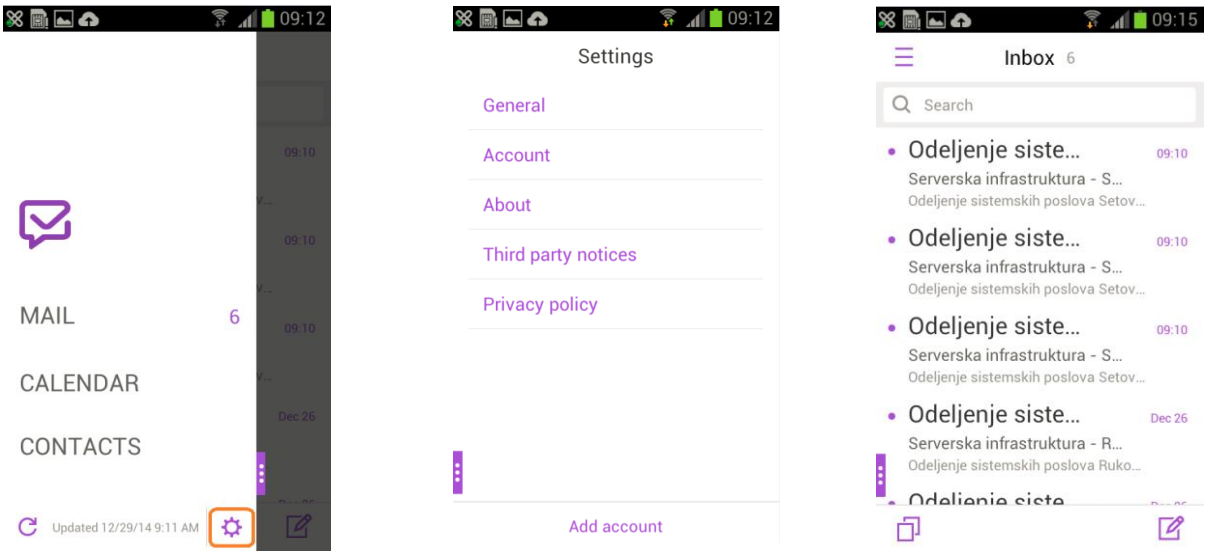


Slika 5.1.4. Prikaz rada Worx Mail aplikacije

Nakon što je proces sinhronizacije uspešno završen na mobilnom uređaju će se pojaviti korporativni mail-ovi. Klikom na ljubičasti pravougaonik u donjem levom uglu aplikacije moguće je pristupiti različitim opcijama u aplikaciji.

Klikom na settings ikonicu moguće je izvršiti dodatna podešavanja u okviru aplikacije po potrebama korisnika. U general settings delu nalaze se podešavanja vezana za pregled mail-ova i kalendara dok se u Account delu nalaze podešavanja poput: vremenskog intervala za sync mail-ova, da li želite da se kontakti sa exchange-a sinhronišu u lokalne kontakte na telefonu, Out of Office podešavanja.

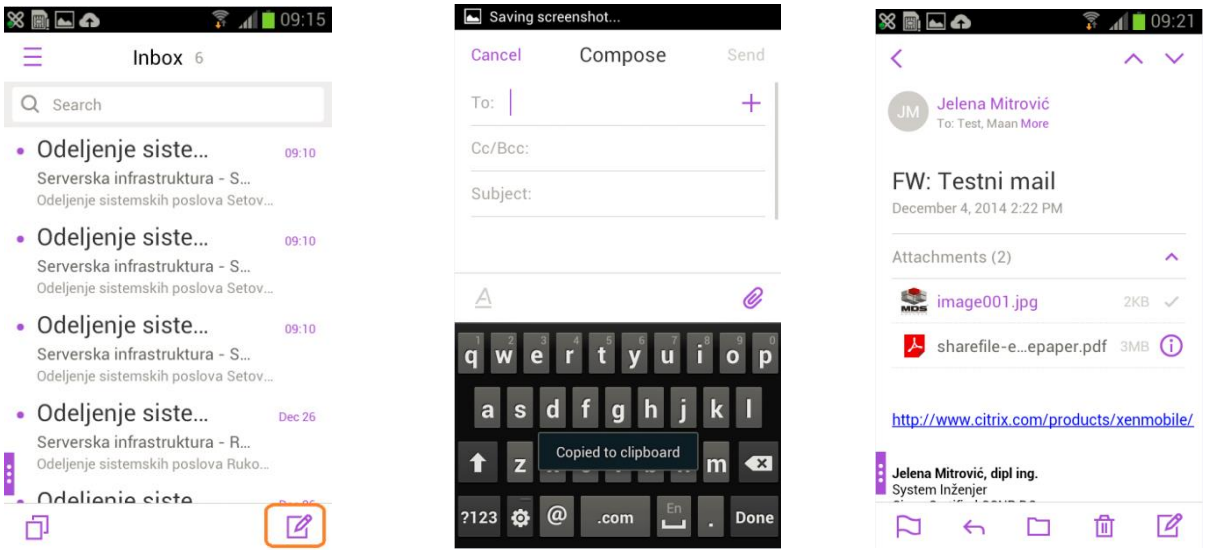
Na Slici 5.1.5 mogu se videti sve opcije koje je moguće podešavati u Worx Mail aplikaciji.



Slika 5.1.5. Podešavanja Worx Mail aplikacije

Za slanje novog maila potrebno je kliknuti na ikonicu sa olovkom nakon čega se standardno kreira mail i dodaju prilozi. Kada se primi mail, linkovi iz mail-a se automatski otvaraju u WorxWeb aplikaciji, a priloge je moguće videti u okviru WorxEdit aplikacije. Pored toga priloge je moguće trajno skladištiti na telefonu u okviru ShareFile aplikacije.

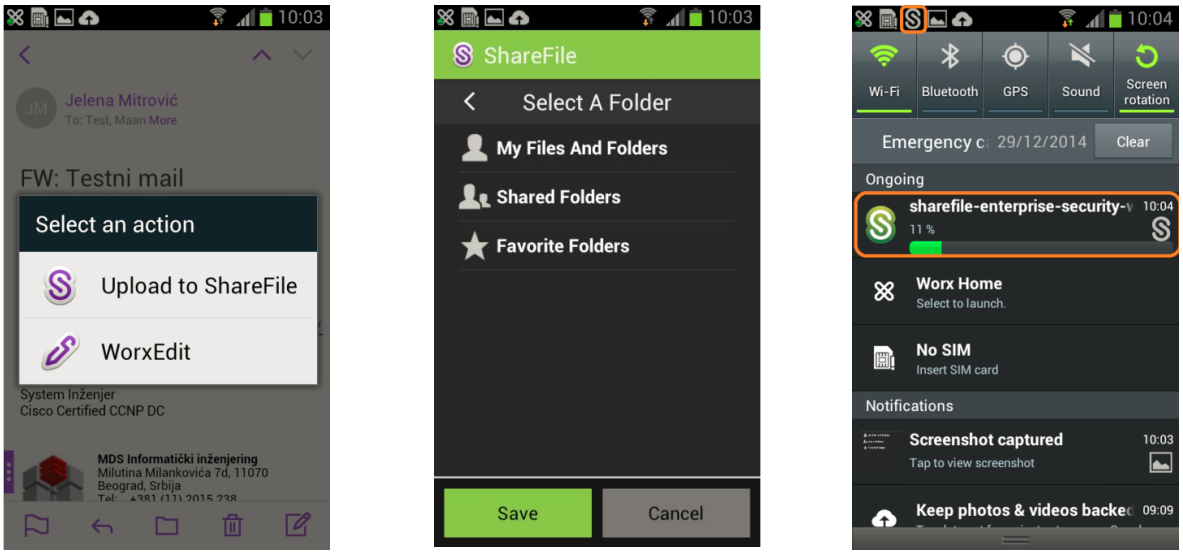
Na Slici 5.1.6 mogu se videti koraci kod slanja nove mail poruke pomoću Worx Mail aplikacije.



Slika 5.1.6. Slanje novog mail-a kroz mobilnu Worx Web aplikaciju

Ukoliko se izabere opcija Upload to ShareFile potrebno je da se izabere folder u koji će dokument biti snimljen kao npr. My Files And Folders. Nakon odabira foldera u gornjem levom delu ekrana pojaviće se ShareFile ikonica i moći će da se vidi upload proces. Dokument koji je postavljen na ShareFile će sada korisniku biti dostupan i prilikom pristupa kroz veb brauzer i prilikom pristupa kroz Sync Tool aplikaciju na Windows računaru.

Na Slici 5.1.7 vidi se postupak prilikom pohranjivanja podataka na ShareFile koji je takođe implementiran kao sastavni deo EMM rešenja.

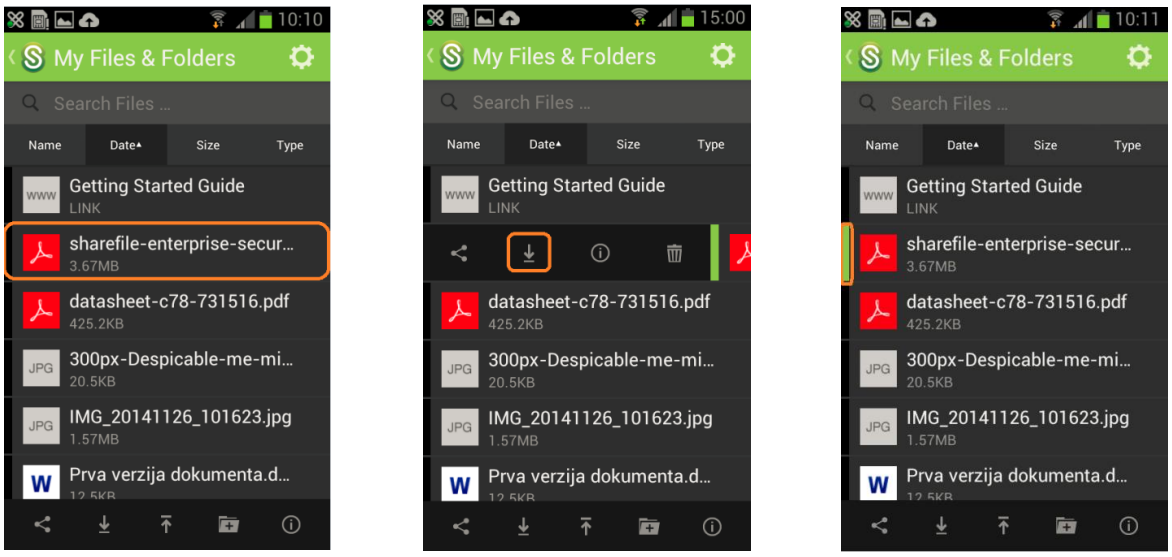


Slika 5.1.7. Čuvanje dokumenata iz priloga mail-a na korporativnom File Share-u

5.1.4. ShareFile

ShareFile je mobilna aplikacija koja je namenjena za sigurno čuvanje i deljene korporativnih podataka na mobilnim uređajima. Istim korporativnim podacima moguće je pristupiti i korišćenjem pristupa kroz veb brauzer kao i korišćenjem sync tool aplikacije na Windows računarima. ShareFile predstavlja zamenu za DropBox i Google Drive rešenja u korporacijama. Sve priloge koje korisnik primi u mail-u WorxMail aplikacije moguće je skladištiti kroz ShareFile mobilnu aplikaicju. Kada se dokument snimi, on se nalazi na storage-u u data centru kompanije. Dokument je moguće preuzeti za lokalno čuvanje na mobilnom uređaju.

Na Slici 5.1.8 vidimo postupak preuzimanja dokumenta sa korporativnog File Share-a za čuvanje na mobilnom uređaju.



Slika 5.1.8. Preuzimanje dokumenta sa File Share-a za čuvanje lokalno na uređaju

Postupak prikazan na prethodnoj slici se sastoji iz sledećih koraka:

1) Odabrati željeni dokument i prevući prstom sa leva na desno preko njega
2) Kliknuti na strelicu orijentisanu na dole
3) Ispratiti da se ispred dokumenta pojavio zeleni pravougaonik što označava da se dokument sada nalazi na lokalnom storage-u mobilnog telefona

Preuzeti dokument moguće je videti u okviru ShareFile aplikacije i korišćenjem WorxEdit aplikacije. Na Slici 5.1.9 prikazano otvaranje dokumenta pomoću Worx Edit aplikacije, iako je prikazana i opcija „Open with“, dokument je nemoguće pregledati ili menjati pomoću bilo kojeg drugog softvera instaliranog na uređaju sem pomenute mobilne aplikacije.

Slika 5.1.9. Korišćenje Worx Edit aplikacije za potrebe pregledanja i menjanja dokumenata

ShareFile dokumentima je moguće pristupiti i odlaskom na sledeću veb adresu https://imekompanije.sharefile.eu/saml/login

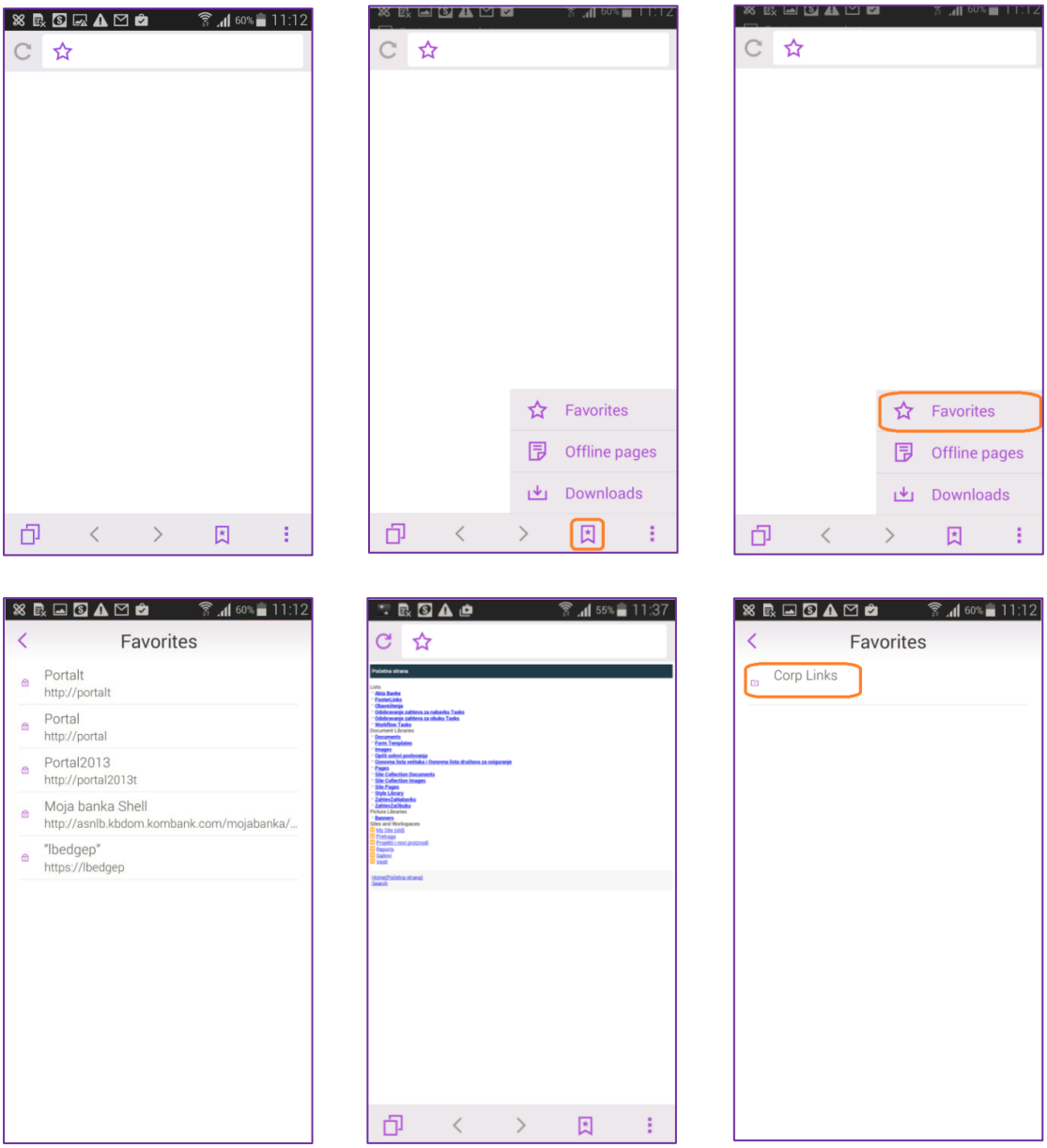
Potrebno je da se korisnik uloguje sa svojim domenskim kredencijalima nakon čega će mu biti omogućen pristup ka dokumentima skladištenim na ShareFile-u.

5.1.5. WorxWeb

WorxWeb aplikacija je namenjena za obezbeđivanje sigurnog pristupa ka veb aplikacijama koje se nalaze u internoj mreži kompanije. Pored toga namena joj je i da otvara veb linkove primljene u mail porukama WorxMail aplikacije. Kroz ovu aplikaciju nije moguće internet pretraživanje s obzirom da je search bar sakriven pa samim tim korisnicima nije omogućeno da sami unose željene veb stranice.

U favorites delu aplikacije se nalaze predefinisane adrese internih veb aplikacija ka kojima je omogućen pristup. Klikom na neku od njih otvara se željena veb aplikacija.

Na Slici 5.1.10 prikazan pristup predefinisanim linkovima, koji su u stvari adrese na kojima se nalaze hostovane aplikacije u internoj mreži kompanije, pomoću mobilne WorxWeb aplikacije.



Slika 5.1.10. Pristup aplikacijama hostovanim u internoj mreži kompanije

6. MOGUĆNOSTI ISKORIŠĆENJA ENTERPRISE MOBILITY REŠENJA I PRAVCI DALJEG RAZVOJA REŠENJA

Tržište rešenja, koja omogućuju integraciju mobilnih uređaja sa korporativnom infrastrukturom, je još uvek mlado. Kompanije imaju različite potrebe kao i različite strategije razvoja mobilnih sistema. Samo tržište se menja veoma brzo, i to je glavni razlog zašto su kompanije veoma obazrive u pogledu EMM rešenja. Mnoge promene će se neminovno desiti na ovom polju, posebno kada se uzme u razmatranje da mobilnost u budućnosti neće podrazumevati samo korišćenje tzv. pametnih telefona i tableta, već i takozvanih pametnih satova i naočara.

U prvom koraku koji kompanije prave prilikom integracije mobilnog sistema u korporativni informacioni sistem, obično se najviše vodi računa o sigurnosti i upravljanju uređajima, međutim sada mnoge kompanije tragaju za sveobuhvatnim rešenjima koji omogućavaju produktivnu, a u isto vreme i sigurnu integraciju.

EMM rešenja još uvek nisu dostigla svoje pune kapacitete. Strategija razvoja mobilnih sistema u korporativnim okruženjima i dalje se više zasnivaju na COPE nego na BYOD modelu. Ovo je naročito izraženo u zemljama sa nižim stepenom tehnološkog razvoja. Međutim, svi pokazatelji pokazuju da će BYOD strategija polako, ali sigurno preuzimati primat prilikom ulaska mobilnih uređaja u kompanije za potrebe realizovanja poslovnih zadataka.

Ovaj trend zahtevaće i evoluciju u funkcionalnostima EMM rešenja. I dok u COPE modelu mobilnog sistema imamo mobilne uređaje koji su u vlasništvu kompanije u BYOD (Bring Your Own device), kao što samo ime kaže, zaposleni koriste svoje lične mobilne telefone ili tablete. U prvom slučaju kompanija, legalno i očekivano, može imati veću kontrolu nad samim uređajem, pošto je u njenom vlasništvu. Međutim, kod BYOD modela logično je da zaposleni insistiraju na svojoj privatnosti. Sve ovo dovodi do toga da EMM rešenja moraju evoluirati u smeru što manjeg preklapanja funkcionalnosti različitih EMM komponenti. U tom smislu da kompanije mogu imati fleksibilnost i mogućnost izbora koju od komponenti EMM rešenja i njenih funkcionalnosti žele, a koju ne žele da implementiraju u svom okruženju. I dok je zadatak MDM komponente da kontroliše same hardverske mobilne uređaje, logično je da će sve manje njenih funkcionalnosti biti implementirano u kompanijama koje primenjuju BYOD model mobilnosti. U ovom slučaju fokus će biti na kontroli mobilnih korporativnih aplikacija i podataka kojima će zaposleni želeti da pristupaju, dok sam hardverski uređaj neće biti kontrolisan. Na ovaj način tražiće se balans između zahteva zaposlenog, koji sa jedne strane želi da eksploatiše prednosti koje mu donosi korišćenje mobilnog uređaja u poslovne svrhe, a sa druge želi da zaštiti svoju privatnost, i kompanije koja želi da svom zaposlenom omogući korišćenje mobilnog uređaja, ali koja mora garantovati za bezbednost svojih aplikacija i podataka.

Gartner procenjuje da prosečna kompanija ima između jedne i 15 aplikacija razvijenih interno u kompaniji, za potrebe njenih zaposlenih, i same poslovne potrebe. I dok se mobilna strategija ranije sastojala od obezbeđivanja pristupa osnovnim alatima za rad kao što su e-mail, kontakti i kalendar, sada imamo sve više aplikacija sa posebnim i specijalnim ulogama i funkcijama za zaposlenog kao i sa sve više kritičnih podataka i informacija koji bivaju pohranjeni ili učitani u mobilne uređaje zaposlenih. Kako ovaj trend uzima sve više maha, javlja se potreba za kontrolom

na aplikativnom nivou, mogućnošću izveštavanja o korišćenju korporativnih, interno razvijenih, aplikacija i podataka, kao i mogućnosti korišćenja sve većeg broja različitih tipova korporativnih sadržaja. Sve ovo predstavlja glavnu temu razvoja strategije korišćenja mobilnih uređaja za potrebe izvršavanja poslovnih zadataka. Alati koji upravljaju mobilnim uređajima nisu više dovoljni ako je jedina njihova svrha da upravljaju hardverskim funkcionalnostima mobilnih uređaja. Sposobnost da omoguće kontrolisani pristup podacima i aplikacijama, da iste isporuče na mobilni uređaj, kao i da upravljaju mobilnim aplikacijama postaju centralni zahtevi koje jedno EMM rešenje mora ispuniti.

Takođe, sve veći upliv BYOD strategije razvoja mobilnih sistema u korporativne mreže značiće neophodnu logičku podeljenost telefona na zone. Razdvojenost privatnog i poslovnog dela mobilnih uređaja u ovom slučaju mora biti još izraženije, a korporativni podaci zaštićeni dodatnim bezbednosnim nivoima. Jedna od teškoća u upravljanju aplikacijama je wrapping aplikacija. Kao što smo već rekli ovo je postupak kojim se u aplikaciju dodaje novi sigurnosni nivo za potrebe sigurne isporuke i korišćenja na mobilnim uređajima, i kako bi se omogućilo da samo određene aplikacije mogu razmenjivati podatke međusobno. Međutim, ovo može dovesti do određenih pravnih, a i tehničkih izazova. Za svaku aplikaciju i svaku njenu novu verziju neophodno je ponavljati proces pakovanja. Ovo može biti mukotrpan i dug posao. Takođe, retko koji vendor aplikacija će davati garancije, podršku i snositi odgovornost za aplikacije koje mi upakujemo radi korišćenja u našem korporativnim mobilnom sistemu. Zbog toga se kompanije sve više odlučuju na razvijanje sopstvenih internih aplikacija, sa kojima neće imati nikakvih pravnih problema ako požele da ih wrapp-uju i koriste na mobilnim uređajima. Kreiranje korporativnog App Store mora biti jedna od opcija u sistemu upravljanja korporativnim podacima.

Sa druge strane, korisnici žele da koriste aplikacije koje su im familijarne, kao na primer neke sa javnih App Store-ova. Za upravljanje ovakvim aplikacijama kompanije treba da favorizuju rešenja koja će omogućiti maksimalno iskorišćenje ovakvih aplikacija, ali i koja će omogućiti da ovakve aplikacije budu pod potpunom kontrolom.

Zaposleni u današnje vreme stalnog tehnološkog napretka, često menjaju svoje mobilne uređaje. Stalnim napretkom tehnologije, dolazimo do toga da imamo mobilne uređaje sa sve više mogućnosti i funkcionalnosti, što dovodi do toga da zaposleni u kompanijama žele da koriste svoje mobilne uređaje koriste kao deo BYOD programa. Na taj način oni imaju opciju da iskoriste sve benefite korišćenja mobilnih uređaja, koji im danas omogućavaju da izvrše gotovo sve radne zadatke. Kao rezultat toga postaje bitno da znamo ne samo ko je konektovan u korporativnu mrežu, nego i da li je taj neko konektovan koristeći autorizovan mobilni uređaj. Ovo je razlog zašto je identitet mobilnog uređaja prepoznat kao ključna stvar u razvoju EMM strategije.

I dok trenutna EMM rešenja kontrolu pristupa mreži zasnivaju na proveri da li korisnik koji pokušava da pristupi resursima sa specifičnog uređaja koji je već registrovan u sistemu, novi proizvodi će moći da pruže proveru dodatnih uslova, kao što su tip uređaja, geografska lokacija sa koje se konekcija inicira i drugi, za odlučivanje da li će pristup biti omogućen ili ne.

Bezbednost informacionog sistema je jedna od oblasti informatičkih tehologija gde posao nikad ne može biti do kraja završen, a verovatno nikad i neće. Možemo instalirati nove pristupne tačke, unaprediti naše upravljačke softvere, virtuelizovati servere i izmestiti aplikacije na razne cloud servise koji su danas široko rasprostranjeni, ali sigurnosni izazovi će biti pred nama svo vreme. Bezbednosne osnove, koje predstavljaju tehnike primene sigurnosnih polisa, zatim enkripcija podataka i autentifikacija korisnika, više nisu dovoljne da pokriju naše sigurnosne potrebe. Nažalost, uvođenje mobilnih sistema u korporativne okvire, bazirane na strategiji da svaki zaposleni koristi svoj lični uređaj (BYOD), ekstremno povećavaju sigurnosne rizike, zadajući administratorima IT sistema nove glavobolje.

Međutim, razloga za strah ne bi trebalo da bude. Istraživanja i unapređenja, koja su sprovedena u proteklih par godina, u oblasti kontrole pristupa mreži, autentifikacije (provere identiteta) i autorizacije (provere prava) donele su nove bezbednosne proizvode koji kontrolišu pristup korporativnim resursima na osnovu identiteta (*identity management*). Identity management najprostije rečeno definiše šta pojedini korisnici mogu uraditi u korporativnoj mreži koristeći specifične uređaje, i pod kojim uslovima. Ovo su rešenja čije će funkcionalnosti biti integrisane u EMM rešenja.

Ključne funkcionalnosti ovakvog sistema su definisanje polisa kojima se određuje kojim su uređajima i kojim korisnicima je pristup korporativnom sistemu dozvoljen, i šta oni mogu uraditi zavisno od vrste uređaja, lokacije sa koje pristupaju sistemu ili od drugih faktora. Svaka od ovih funkcionalnosti zavisi od karakteristika upravljačke konzole, uključujući definisanje polisa, izveštavanje, mogućih podešavanja alarma, i ostalih upravljačkih i operativnih zahteva. Alarm se, na primer, može podesiti da se javlja kada specifični korisnik pokuša da pristupi resursima za koje nema dozvolu. Može se podesiti i zakazati kreiranje izveštaja u željenom formatu.

Takođe, jasno je da će se sve više tražiti rešenja koja se lako mogu integrisati u postojeću infrastrukturu, gde se misli na postojeće Windows sisteme, uključujući primenjivanje polisa kroz Active Directory i sistem za pohranu podataka. Ovo podrazumeva da ne postoji paralelan sistem i da se vreme koje je potrebno za angažovanje IT administratora i dalje može planirati na sličan način kao pre implementacije novog sistema. Na ovaj način postižu se maksimalne pogodnosti za korisnike, što posledično donosi korist preduzeću, bez mnogo dodatnih troškova. Jednostavnost će u budućnosti biti najveći adut provajdera ovakvih rešenja.

Kao što smo već rekli BYOD strategija razvoja mobilnih sistema u korporativnom okruženju biće sve više zastupljena u budućnosti. S tim u vezi potrebne su automatske funkcionalnosti sistema, gde neće biti potrebno učešće IT osoblja u operacijama, kao što je automatska provera statusa uređaja, ili automatsko kreiranje izveštaja, zatim alarmiranje o pokušaju nedozvoljenog pristupa. Ovo su funkcionalnosti koje umnogome mogu smanjiti vreme potrebno za administriranje mobilnih sistema u korporativnom okruženju. S tim u vezi evolucija EMM sistema ide u smeru automatizovanja što je moguće više operacija koje administratori treba da obavljaju.

Još jedno važno pitanje koje će u budućnosti biti postavljeno pred kompanije je pitanje izmeštanja aplikacija i podataka na cloud servise. Iako javni cloud servisi za pohranu podataka, kao što su Box i Dropbox, imaju sve veću popularnost među korisnicima, kompanije će i dalje preferirati da korporativne poatke skladište u svojim data centrima umesto u cloud-u. Prosto svi su svesni da sigurnosni rizici u vezi sa cloud-om postoje. Drugi razlog je jednostavno potreba za što većom produktivnosti EMM sistema koji se obično integriše sa File sistemom, zatim sa Exchange serverima, nekad i sa backup sistemom i drugim. Ipak, postoji trend da neke kompanije hostuju aplikacije koje ne sadrže previše osetljive podatke u DMZ zoni iza firewall-a, a sve je više i onih koji „neosetljive“ aplikacije i podatke drže u cloud-u.

Osvrnuli bismo se još na budućnost mobilnosti u komapanijama u pogledu mobilnih uređaja sa različitim operativnim sistemima.

Od izlaska iOS 7 operativnog sistema Apple je bio neprikosnoven na vrhu po funkcionalnostima koje je nudio za integraciju uređaja u mobilnu mrežu. Pa iako su se Android mobilni uređaji koristili gotovo istom merom za ove namene, naročito u zemljama nižeg tehnološkog razvoja i napretka, jasno je da je na iOS 7 operativnom sistemu sve učinjeno kako bi ispunjavao sve sigurnosne i tehničke zahteve po pitanju integracije u korporativni informacioni sistem uz pomoć nekog od EMM rešenja. iOS 8 je nastavio ovaj trend sa još više interesantnih opcija po pitanju mobilnosti u poslovanju. Document Picker i Document Push su samo neke od

veoma važnih tačaka u kontekstu poslovne mobilnosti. iOS 8 pruža još više interesantnih biznis opcija, što će prouzrokovati nove trendove na tržištu. Pakovanje aplikacija, na koje su mnogi provajderi EMM rešenja tipovali, postaje zastareo način isporuke mobilnih aplikacija na uređaje. Kao što je ve' navedeno mobilni uređaji koji rade na iOS operativnim sistemima su trenutno najzreliji i najjednostavniji uređaji u pogledu integracije u poslovne IT sisteme, pa ne čudi što se većina kompanija oslanja upravo na iPhone telefone i iPad tablete. Kompanije će i u budućnosti sve više koristiti Open In Management sa iOS mobilnim uređajima. Ovo će omogućiti kompanijama da imaju kontrolu nad tim koje aplikacije mogu otvarati korporativne dokumente i menjati ih koristeći telefone i tablete sa iOS operativnim sistemom (iPad-i i iPhone-i). EMM rešenja moraju da poseduju ovu važnu sigurnosnu opciju kako bi se sprečio nekontrolisani pristup korporativnim podacima.

Ali svakako treba imati na umu da će Android postajati sve interesantniji kako Google bude unapređivao poslovne funkcije, hvatajući na taj način korak sa Apple-om. Android možda već ima svog keca u rukavu. Na konferenciji Google programera ove godine, Google je objavio svoj operativni sistem Android for Work. Ovaj operativni sistem direktno integriše dodatni sigurnosni nivo potreban za uvođenje mobilnih uređaja u korporativne okvire, praveći na ovaj način toliko pominjanu razdvojenost privatne i poslovne oblasti na mobilnom uređaju, što ga čini idealnim za BYOD program [11].

7. ZAKLJUČAK

S obzirom da smo svi svesni uloge koju mobilni uređaji zauzimaju u našem kako privatnom tako i poslovnom životu, svesni smo značaja i prednosti njihovog integrisanja u korporativni sistem. Na ovaj način omogućićemo iskorišćenje raznih benefita koje mobilnost u poslovnom okruženju donosi, unapređujući ukupnu produktivnost naše kompanije.

U ovom radu pokazali smo razna tehnička i sigurnosna pitanja koje ovakva integracija otvara, i probali da odgovorimo na njih. Probali smo da prikažemo razna sigurnosna pitanja koja se uvođenjem mobilnog sistema u IT sistem kompanije postavljaju pred administratore i inženjere koji taj sistem održavaju. Da bismo omogućili korišćenje mobilnih uređaja zaposlenih u cilju obavljanja poslovnih zadataka zahteva neophodna je implementacija određenog sistema za podršku, na tržištu poznatih pod nazivom Enterprise Mobility Management (EMM) rešenja.

Jasno je da sve kompanije koje žele da svojim zaposlenima pruže fleksibilnost korišćenja mobilnih uređaja moraju uzeti u razmatranje implementaciju nekog od EMM rešenja. Taj proces mora biti zrelo i detaljno isplaniran, uz koordinaciju svih relevantnih službi u okviru jedne kompanije, sagledavajući na pravi način sve funkcionalnosti koje su neophodne za implementaciju, kako bi se odgovorilo na sve konkretne poslovne potrebe kompanije.

Na primeru konkretne implementacije jednog EMM rešenja pokušali smo da približimo sve izazove koji u jednom ovakvom slučaju stoje pred IT osobljem kompanije, kao i kako se sa takvim izazovima izboriti. Poseban akcenat stavljen je na obezbeđivanje sigurnosti sistema. Cilj nam je bio da pokažemo kako dobro definisana sigurnosna politika kompanije, uz njihovu strogu primenu na svim nivoima može rešiti sve probleme koje uvođenje mobilnog sistema u korporativnu mrežu može izazvati. Rezultati testiranja implementiranog rešenja jasno pokazuju prednosti koje njegova implementacija donosi sa stanovišta zaposlenog tj. klijenta.

Na osnovu svega prikazanog, jasno je da su EMM sistemi budućnost svakog korporativnog okruženja, kao sastavni deo strategije postizanja što veće fleksibilnosti obavljanja poslovnih zadataka. Ovo bi za posledicu trebalo da ima veće zadovoljstvo zaposlenih, a u nekom dugoročnom planu i dostizanje maksimalne produktivnosti zaposlenih uz negovanje imidža kompanije, idući u korak sa tehnološkom revolucijom u oblasti mobilnih uređaja.

LITERATURA

[1] http://searchmobilecomputing.techtarget.com/definition/enterprise-mobility-management-EMM

[2] http://searchsecurity.techtarget.com/feature/Introduction-to-mobile-device-management-products - Matthew Pascucci

[3] http://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[4] http://searchmobilecomputing.techtarget.com/tip/Mobile-application-management-comparison-App-wrapping-vs-containerization - Robert Sheldon

[5] http://searchmobilecomputing.techtarget.com/tip/Top-techniques-for-mobile-data-loss-prevention - Michael Finneran

[6] http://searchmobilecomputing.techtarget.com/tip/BYOD-or-COPE-Which-enterprise-mobility-strategy-is-right-for-you - Colin Steele

[7] http://searchsecurity.techtarget.com/feature/Three-enterprise-scenarios-for-MDM-products- Matthew Pascucci

[8] http://searchsecurity.techtarget.com/feature/Introduction-to-mobile-device-management-products - Matthew Pascucci

[9] https://www.google.rs/search?q=gartner+magic+quadrant+enterprise+mobility+managemen&espv=2&biw=1280&bih=699&tbm=isch&tbo=u&source=univ&sa=X&ved=0CBsQsARqFQoTCIS1xMGE3scCFcY9GgodWlsDxA

[10] https://www.citrix.com/solutions/enterprise-mobility

[11] http://www.techradar.com/news/world-of-tech/the-future-of-enterprise-mobility-management-1272460/2 - Kristin Montag Product Manager for Cortado Corporate Server at Cortado AG