IMPLEMENTACIJE RJEŠENJA ZA UPRAVLJANJE SIGURNOSNIM ASPEKTIMA MOBILNIH UREĐAJA S CILJEM IDENTIFIKACIJA NAJBOLJIH PRAKSI

Čorluka, Ivan

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

Implementacije rješenja za upravljanje sigurnosnim aspektima mobilnih uređaja s ciljem identifikacija najboljih praksi

Ivan Čorluka

Zagreb, veljača 2023.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".

U Zagrebu, 22.02.2023.

Predgovor

Ovim završnim radom htio bi se zahvaliti svim profesorima koji su mi predavali tijekom studija na Algebri, posebno mentoru profesoru Zlatanu Moriću na pomoći pri izradi završnog rada. Posebno se želim zahvaliti svojoj obitelji i djevojci Nataši koji su u svim teškim trenucima bili uz mene i bodrili me tijekom cijelog studiranja.

Sažetak

U ovim završnom radom bavit ću se usporedbom i analizom dva mobilna rješenja Samsung Knox i Workspace ONE, istražit ću prednosti i mane oba sustava. MDM (mobile device managment) rješenja pružaju sustav upravljanja, konfiguracije i zaštite svih mobilnih uređaja i podataka koje oni sadrže, s naglasnom na njihovu zaštitu. Osim sigurnosti također bavit ću procjenom troškova implementacije, razvojem sigurnosnih politika te krajnjim iskustvom korisnika na nekoliko tipova upravljanja uređajima. Svrha ovog završno rada je da istraživanjem kojem opisujem i analiziram sustave pomogne organizacijama koje pokušavaju odabrati pravo rješenje za upravljanje mobilnim uređajima za svoju tvrtku.

Ključne riječi: MDM, upravljanje, sigurnost, Samsung Knox, Workspace ONE, implementacija, analiza.

In this final work I will deal with the comparison and analysis of two mobile solutions Samsung Knox and Workspace ONE, I will explore the pros and cons of both systems. MDM (mobile device management) solutions provide a system of management, configuration and protection of all mobile devices and the data they contain, with emphasis on their protection. In addition to security, I will also deal with the assessment of implementation costs, the development of security policies and the end experience of users on several types of device management. The purpose of this final work is to use research to describe and analyze systems to help organizations that are trying to choose the right mobile device management solution for their company.

Keywords: MDM, management, security, Samsung Knox, Workspace ONE, implementation, analysis.

Sadržaj

1. Uvod

1.1. Definicija upravljanja mobilnim uređajima

U velikim organizacijama, ali i u malim poduzećima za upravljanje nadzor i osiguranje mobilnih uređaja kao što su pametni telefoni, tableti i prijenosna računala koristimo alate koji se zovu upravljanje mobilnim uređajima (eng. MDM - Mobile Device Managment). Cilj MDM-a je osigurati da se mobilni uređaji koriste na siguran i kontroliran način, uz zadržavanje privatnosti podataka pohranjenih na tim uređajima. Takva rješenja omogućuju organizacijama da provode pravila za sigurnost uređaja, zaštitu podataka i upravljanje aplikacijama, kao i daljinsko praćenje i upravljanje uređajima. Implementacijom MDM rješenja organizacije mogu poboljšati sigurnost svojih mobilnih uređaja, smanjiti složenost i troškove upravljanja tim uređajima te povećati učinkovitost svojih zaposlenika.[1]

1.2. Važnost MDM-a u današnjem poslovnom okruženju

Rasprostranjena upotreba mobilnih uređaja u suvremenom poslovnom okruženju donijela je brojne izazove za organizacije koje žele osigurati svoje podatke i zadržati kontrolu nad svojim mobilnim uređajima. Upravljanje mobilnim uređajima (MDM) postalo je ključna komponenta cjelokupne IT strategije organizacije jer pruža način upravljanja, praćenja i zaštite mobilnih uređaja na centraliziran i učinkovit način. Važnost MDMa u današnjem poslovnom okruženju potaknuta je nizom čimbenika, uključujući kao što su sigurnost, usklađenost, ušteda troškova i poboljšana učinkovitost. Pružajući način upravljanja i zaštite mobilnih uređaja, organizacije mogu smanjiti rizik od kršenja podataka, udovoljiti regulatornim zahtjevima, smanjiti troškove i poboljšati učinkovitost svoje mobilne radne snage.

2. Vrste rješenja za upravljanje mobilnim uređajima

Razumijevanje različitih vrsta dostupnih MDM rješenja ključno je za organizacije koje žele učinkovito upravljati i osigurati svoje mobilne uređaje. U ovom odjeljku istražit ćemo različite vrste MDM rješenja, uključujući potpuni MDM, kontejnerizacija, hibrid i samostalni MDM. Razumijevanjem prednosti i slabosti svakog rješenja organizacije mogu donijeti informiranu odluku o tome koja vrsta MDM rješenja najbolje odgovara njihovim potrebama.

2.1. Potpuni MDM

Ovim tipom upravljanja mobilnim uređajima mislimo na potpuno upravljanje odnosno na sveobuhvatno rješenje unutar neke tvrtke na vlastitoj infrastrukturi, sa minimalnom asistencijom odnosno nabavkom resursa od treće strane. Takva rješenja obično uključuju značajke kao što su nabavka uređaja, upravljanje aplikacijama, provedba internih sigurnosnih pravila i na koncu daljinsko upravljanje mobilnim uređajima. Takav način koriste velike tvrtke sa velikim brojem zaposlenika, jer ovakav model rješenja nudi opsežan skup značajki za upravljanje i osiguranje mobilnih uređaja. Prednost ovakvog rješenja uključuje sljedeće: centralizirano upravljanje, visoku implementaciju sigurnosti i poboljšanu produktivnost, te podršku informatičkog tima unutar tvrtke.[2]

2.2. Kontejnerizacija MDM-a

Implementacija MDM tehnologije s kontejnerizacijom daje mogućnost provođenja upotrebe jake autentifikacije i šifriranja te selektivnog brisanja korporativnih podataka s izgubljenih ili ugroženih uređaja, da osobni podaci ostaju netaknuti. Enterprise brisanje također dobro dođe kada zaposlenik koji radi sa svojim osobnim uređajem napusti organizaciju, a organizacija želi ukloniti podatke iz poslovnog spremnika bez uništavanja resursa koji su prisutni u osobnom profilu koju je vlasnik uređaja pohranio na svom uređaju. Dakle, administratori mogu spriječiti osobnim aplikacijama pristup korporativnim podacima i aplikacijama, a korisnici mogu biti sigurni da organizacija neće pristupiti osobnim podacima koje pohranjuju na uređaju izvan profila. [3]

2.3. Hibrid

Hibridna rješenja za upravljanje mobilnim uređajima kombiniraju prednosti potpunog MDMa i kontejnerizacijska rješenja. U hibridnom MDM rješenju uređajem se upravlja i na razini uređaja i na razini aplikacije, pružajući sveobuhvatnije i sigurnije rješenje.[4]

Prednosti hibridnih MDM rješenja uključuju:

- Povećana sigurnost: Hibridna MDM rješenja pružaju višu razinu sigurnosti, jer se i uređajem i aplikacijama upravlja i osigurava.
- Poboljšano korisničko iskustvo: Hibridna MDM rješenja mogu pružiti bolje korisničko iskustvo, jer korisnici imaju pristup svim svojim aplikacijama i podacima vezanim uz posao, dok IT odjeli još uvijek mogu upravljati i osigurati informacije.
- Povećana učinkovitost: Hibridna MDM rješenja mogu povećati učinkovitost, jer IT odjeli imaju sveobuhvatniji pogled na uređaj i aplikacije, što olakšava upravljanje i zaštitu informacija.

2.4. Samostalni MDM

Samostalna rješenja za upravljanje mobilnim uređajima ne zahtijevaju integraciju sa vlastitom infrastrukturom, aplikacijama ili platformama. Ova rješenja pružaju osnovne mogućnosti upravljanjem uređajima kao što su postavljanje lozinki i brisanje uređaja. Ovakva opcija vrlo je isplativa za mala poduzeća i tvrtke sa malim brojem zaposlenika koje imaju ograničene potrebe za upravljanjem mobilnim uređajima. [5]

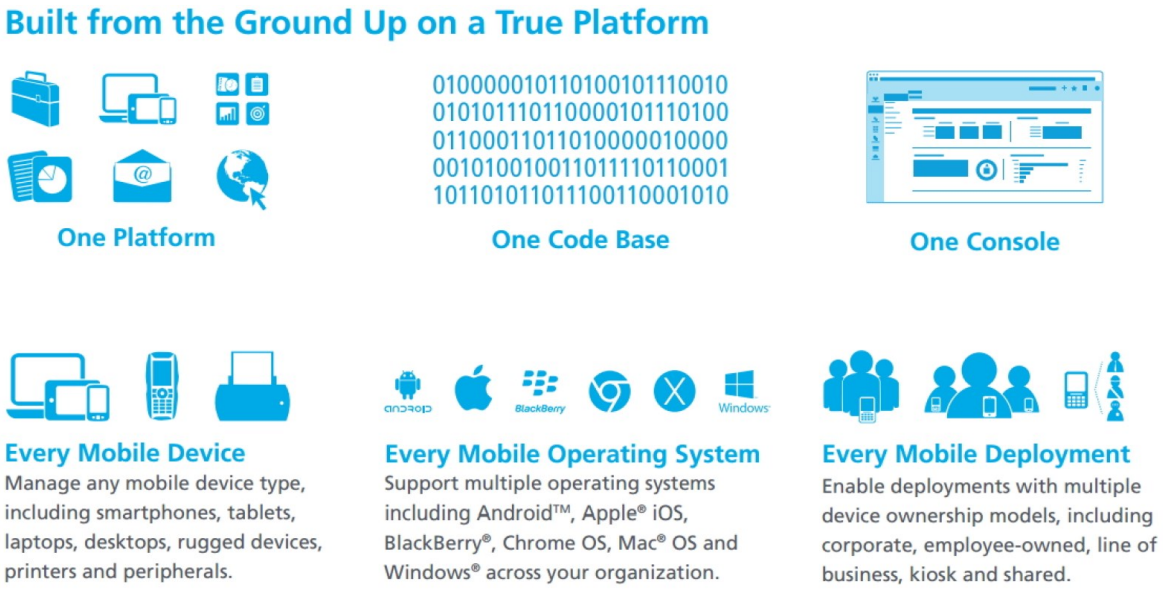
3. Implementacija sustava Samsung Knox i VMware Workspace ONE

Ovim završnim radom obradit ćemo proces implementacije i integracije rješenja za upravljanje mobilnim uređajima Samsung Knox i VMware Workspace ONE na vlastitoj infrastrukturi. Rješenje za upravljanje mobilnim uređajima temelji se na visoko dostupnim sustavima. Implementacija Samsung Knox sustava zahtjeva pravilno planiranje i konfiguraciju mobilnih uređaja kako bi se osigurala njegova učinkovita uporaba u upravljanju i osiguravanju mobilnih uređaja unutar organizacije. Pokazat ćemo mogućnosti kao što su registracija uređaja, upravljanje aplikacijama, te provedba sigurnosnih pravila.

Ovaj sustav bazira se na rješenjima temeljena na oblaku, koja će nam omogućiti prilagodbu i automatizaciju upisa uređaja koji su kupljeni od strane jednog proizvođača, ovo iskustvo izvan kutije, će nam omogućiti širok raspon opcija konfiguracije.

Drugo rješenje koje ćemo opisivati će biti VMware Workspace ONE, ono je sveobuhvatno rješenje za upravljanje poslovnom mobilnošću koje nudi upravljanje mobilnim uređajima. Implementaciju ćemo raditi na fizičkoj infrastrukturi koja će uključivati integraciju različitih komponenti kao što su upravljanje uređajima, upravljanje aplikacijama i sigurnost. Postupak također zahtjeva pažljivo planiranje i izvršenje kako bi se osiguralo učinkovito uvođenje i korištenje rješenja.

Ukratko, u praktičnom dijelu prikazat ćemo koje je preduvjete potrebno osigurati kako bismo uspješno izvršili on-premise implementaciju VMware Workspace ONE rješenja, usputno ćemo prikazati i opisati cloud rješenje Samsung Knox, kako ispravno konfigurirati sustav da bi smo ga mogli koristiti. Svi testovi koje ću izvršavati biti će testirani u korporativnom okruženju, sa malo manje od 2000 korisnika mobilnih uređaja.



Slika 3. High-level funkcionalnosti

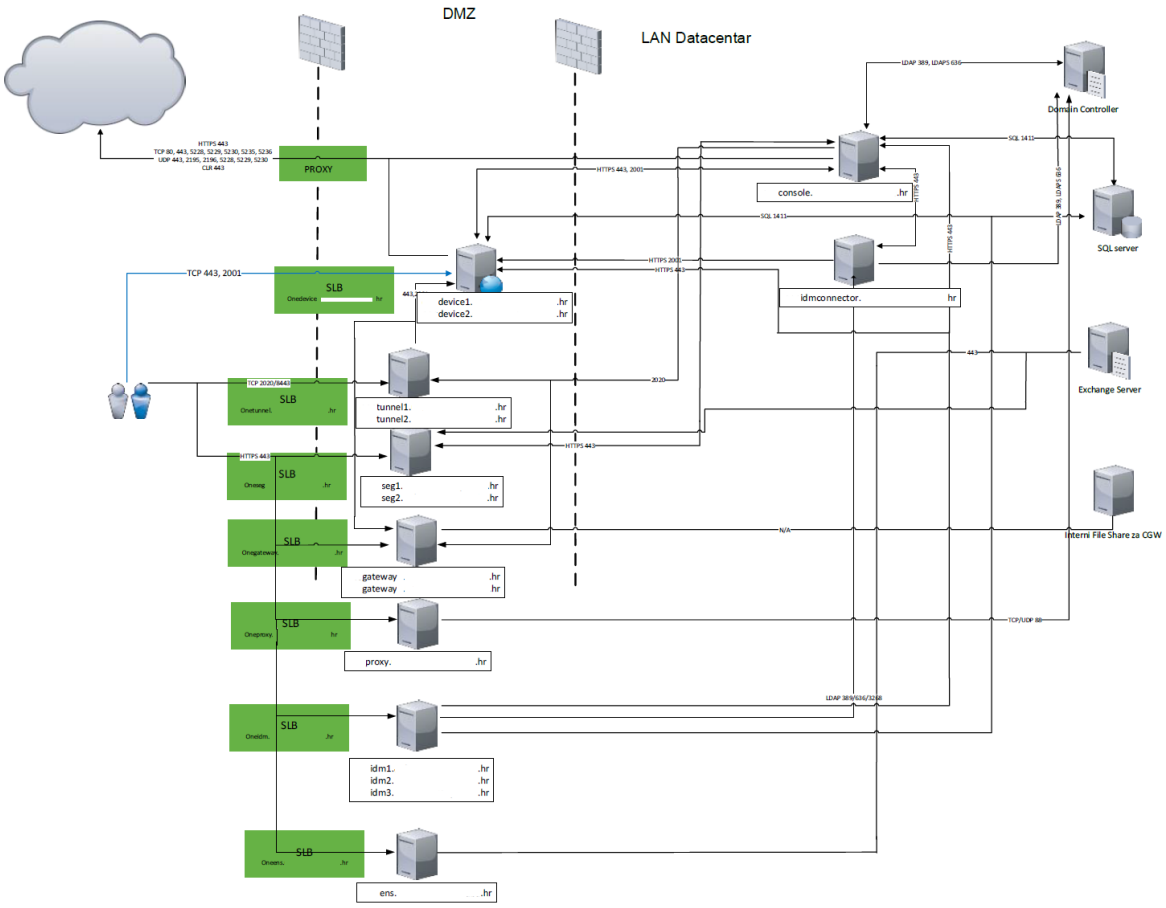
Slika iznad Enterprise Mobility pruža korisnicima isto iskustvo na svim platformama, pružajući tako sigurno digitalno radno mjesto za kritične poslovne aplikacije, sigurno omogućujući BYOD i uspostavljajući platformu koja se prilagođava potrebama korporacije kako bi se omogućila podrška za rad s mobilnih uređaja. EMA+ pruža jedinstvenu platformu za upravljanje uređajima.

3.1. Instalacija konzole i sigurnosnih politika

Preduvjeti koje je potrebno ispuniti da bismo implementirali VMware Workspace ONE produkcijsku okolinu u svome poduzeću su sljedeći:

- Korisnički račun sa administratorskim pravima na Windows poslužiteljima i appliance-ima
- Instalirani Windows virtualni poslužitelj za Device Services (DS) rolu (2 komada)
- Instaliran Windows virtualni poslužitelj za Console (UEM) rolu (1 komad)
- Instalirani Linux virtualni appliance za Identity Manager (IDM) komponentu (3 komada)
- Instaliran Windows virtualni poslužitelj za Email Notification Service (ENS) komponentu (1 komad)
- Importani Unified Access Gateway (UAG) appliance-i za Tunnel, Secure Email Gateway (SEG) i Web Reverse Proxy (WRP)

- Instaliran Notepad++ na EMA+ Windows poslužiteljima
- Instaliran Chrome i Firefox na EM+ Windows poslužiteljima
- Sve dostupne Microsoft nadogradnje na Windows serverima.
- Licenciran Windows Server OS sa Microsoft licencama
- Osigurani servisni računi za autentikaciju na backend sustave
- Testni uređaji (Apple/Android)
- Korporativni Google račun
- Korporativni AppleID
- Definirane IP adrese za poslužitelje, dostupne za komunikaciju preko Interneta (javni DNS i interni DNS zapisi)
- Osiguran javno vjerovni certifikati u .pfx formatu (preporuka Digicert zajedno s root i intermediate certifikatima za komponente Admin console, Device services, Secure Email Gateway, Tunnel, Access, Web Reverse Proxy)
- Konfigurirana mrežna propuštanja i osigurana mrežna povezivost između komponenti sustava (specifično za ACC komponentu i backend korisničku infrastrukturu prema SEG, Tunnel, WRP, ENS i IDM komponentu koje trebaju imati pristup internim resursima)
- Instalirana IIS rola na Windows poslužiteljima (UEM i DS poslužitelji)
- Instalirani feature-i: .NET Framework 3.5.1, Message Queuing: Message Queuing Server, Telnet Client na EMA+ Windows poslužiteljima
- Certifikat povezan na port 443 na DS i UEM poslužitelju
- Instaliran .NET Framework 4.0 (for Windows 2008) ili 4.5 (for Windows 2012) na EMA+ Windows poslužiteljima
- Instaliran database server – MS SQL 2008 R2 ili noviji
- Kreirana AirWatch baza podataka
- SQL collation postavljen na SQL_Latin1_General_CP1_Cl_AS
- Servisni account ima db_owner prava na EMA+ baze podataka
- Full-Text search je instaliran na SQL bazi podataka
- Osiguran load balanser (LB) za osiguravanje visoke dostupnosti rješenja i raspoređivanja mrežnog opterećenja za visoko dostupne komponente sustava
- Ispravna komunikacija kroz Proxy, LB i ostale mrežne komponente

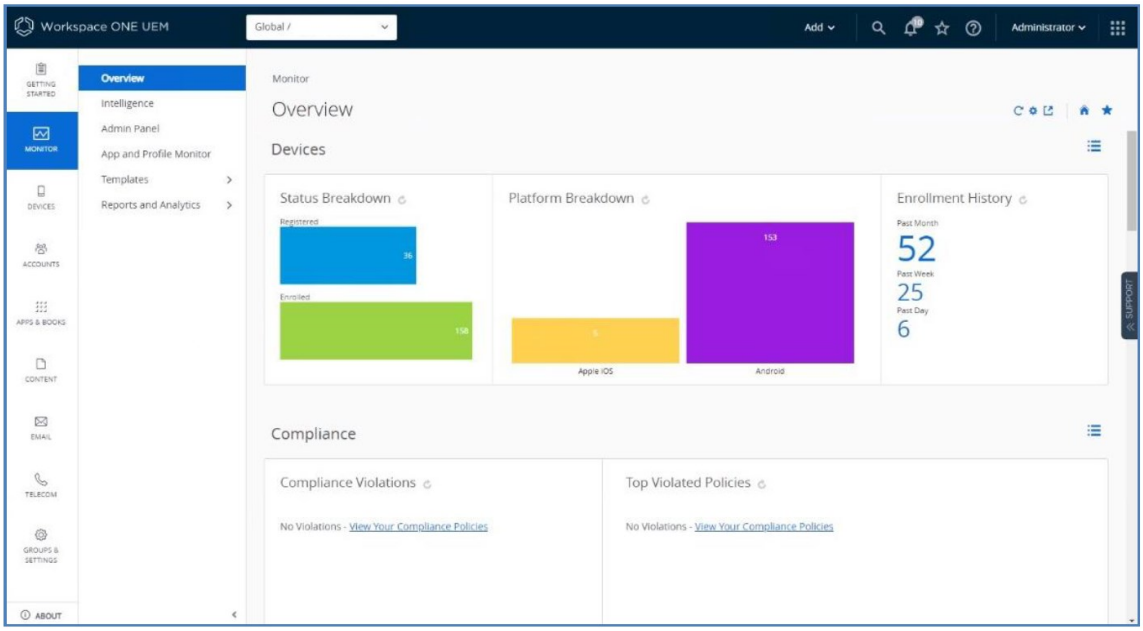


Slika 3.1 Shema implementiranog rješenja

U shemi iznad smo prikazali kompletnu infrastrukturu koju jedna organizacija treba pripremiti kako bi rješenje za upravljanje mobilnim rješenjima funkcioniralo sa sigurnosnog tako i aspekta visoke dostupnosti.

Također je potrebno imati aktivnu konfiguraciju mrežnih komponenti poput Load Balancera (LB), postavljenog Proxy servera i Firewalla, potrebno je izvesti ispravna mrežna propuštanja kako bi cijeli sustav ispravno radio.

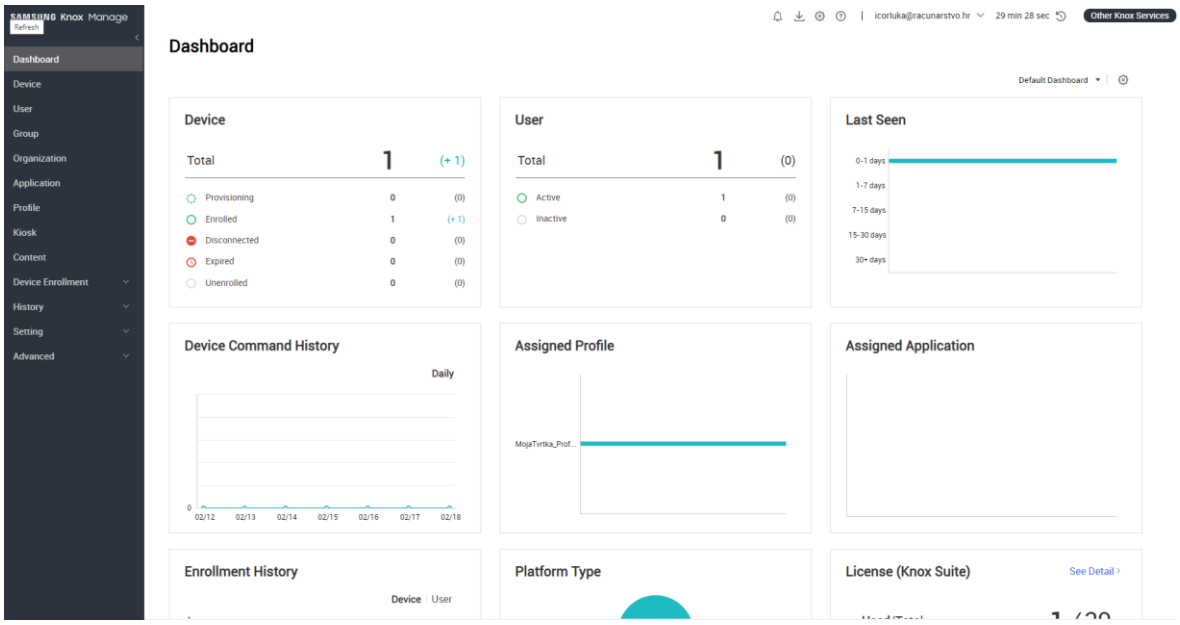
Unified endpoint management (UEM) poslužitelji mogu se konfigurirati preko tvrtkinog Proxy servera, no Apple uređaji ne mogu se propustiti preko klasičnog HTTP prometa već se mora izravno pustiti na Internet.



Slika 3.2 Konzola VMware Workspace ONE

U slici iznad možemo vidjeti početnu stranicu VMware konzole za upravljanje mobilnim uređajima sa svim popratnim značajkama.

Sustav Samsung Knox također može biti implementiran na način da se gnijezdi u vlastitu infrastrukturu.

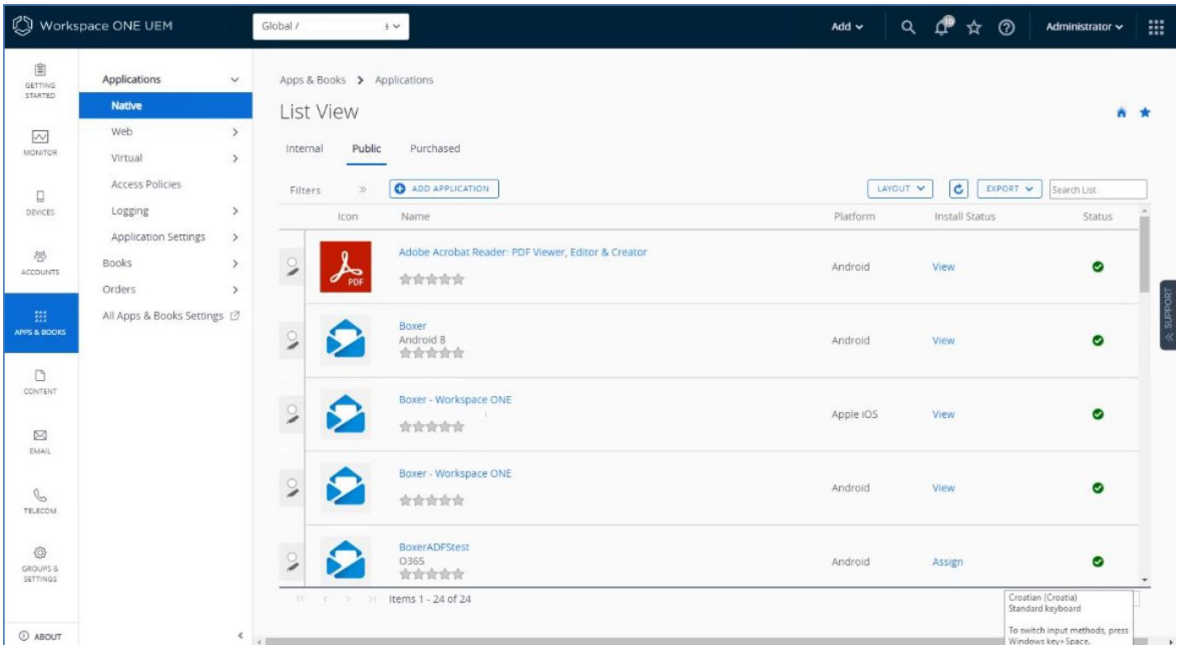


Slika 3.3 Konzola Samsung Knox Manage

No, ovo rješenje je više bazirano na cloud rješenju na Samsungovoj infrastrukturi samim time postavljanje ne zahtjeva više od korisničkog računa, koji će postati glavni administrator konzole. Što možemo vidjeti na slici iznad.

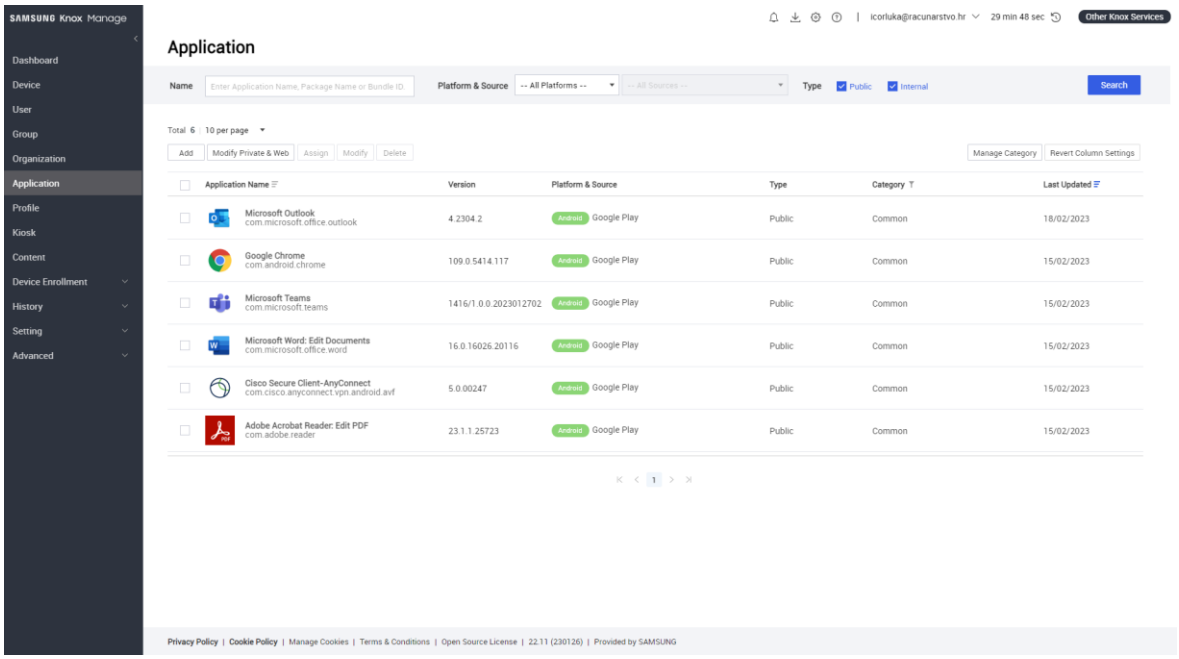
3.2. Konfiguracija aplikacija

Odabirom poslovnih aplikacija koje će se instalirati na mobilne uređaje određuje sama tvrtka, odnosno njeni administratori. Odabirom aplikacija moramo voditi računa što je bitno za tvrtku, da li su te aplikacije neophodne i kako će se one koristiti. Sve odabrane aplikacije se stavljaju u katalog koji se preuzima prilikom početnog postavljanja uređaja.



Slika 3.4 Aplikacije iz Google Play Store na Workspace ONE

Na isti način smo postavili aplikacije i preko administratorske konzole Samsung Knox, gdje smo odabrali aplikacije koje će se moći koristiti.

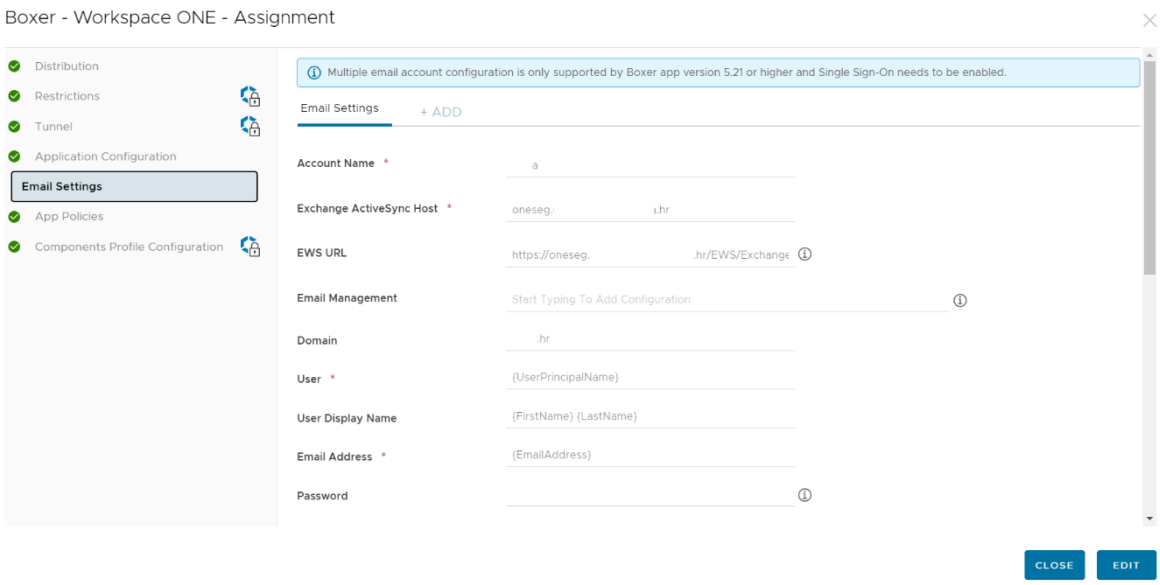


Slika 3.5 Aplikacije iz Google Play Store na Samsung Knox

Također u oba MDM sustava dodajemo aplikacije iz Google Play Store i iOS App Store kako bi smo aplikacije mogli koristiti na dvije mobilne platforme Android i iOS.

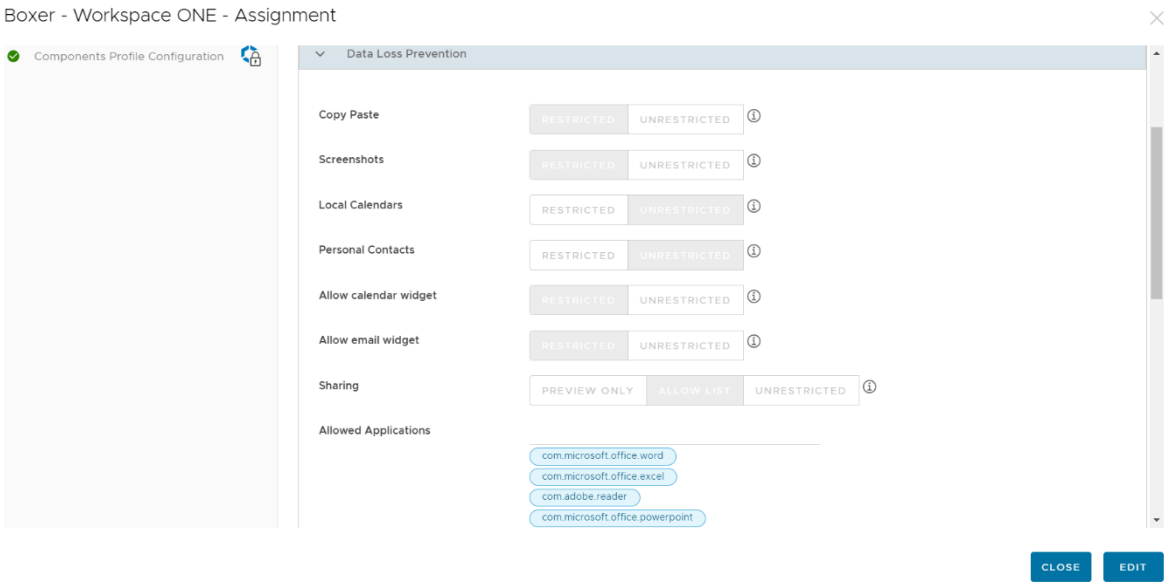
Nakon što smo dodali aplikacije koje će biti ponuđene prilikom postavljanja, također je bitno određenim aplikacijama kao mail zadati konfiguraciju kako ne bi imali dodatnog posla nakon postavljanja uređaja nego da sve ide automatizmom.

Uzet ćemo na primjer aplikaciju za čitanje i slanje pošte. Konfigurirat ćemo je tako da ćemo je povezati na tvrtkin mail server, preko kojega ćemo dobivati mailove.



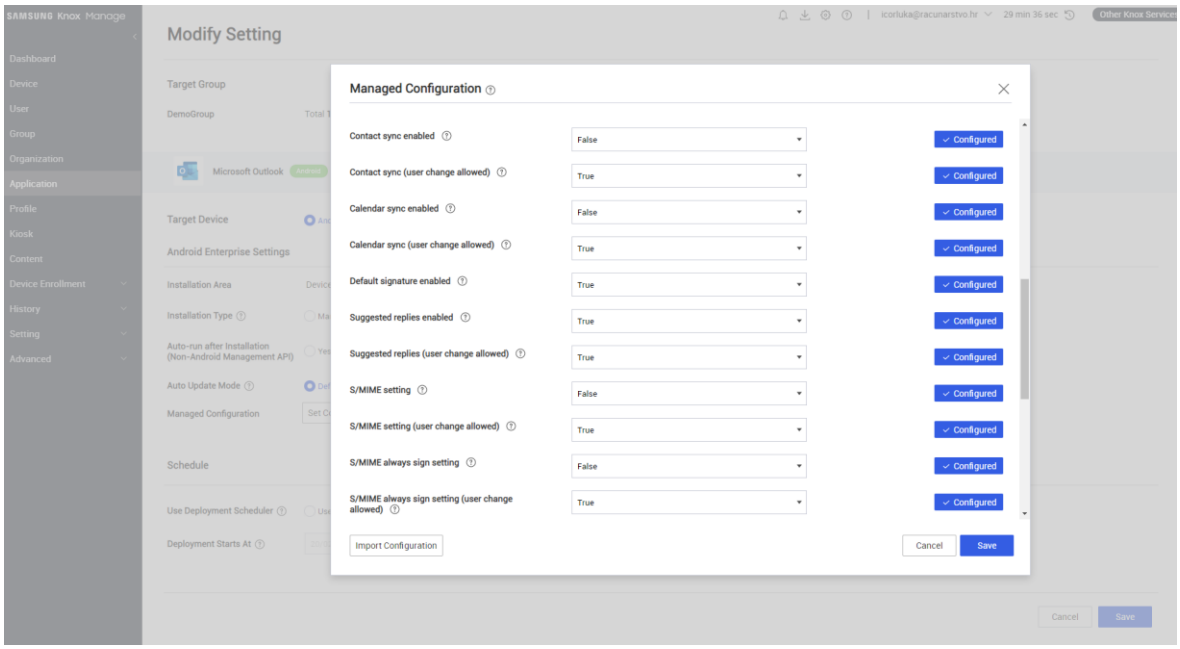
Slika 3.6 Povezivanje Boxer aplikacije sa mail serverom

Postavljamo određene restrikcije kako zaposlenici ne bi mogli raditi kopiranje sadržaja van poslovnog profila, također zabranili smo snimku zaslona uređaja i dopustili smo da se privici mogu otvarati sa Office aplikacijama.



Slika 3.7 Postavljanje restrikcija u Boxer aplikaciji

Samsung ima puno manje mogućnosti restrikcija mail računa, koje smo postavili za aplikaciju Boxer.



Slika 3.8 Postavljanje restrikcija u Outlook aplikaciji za Knox

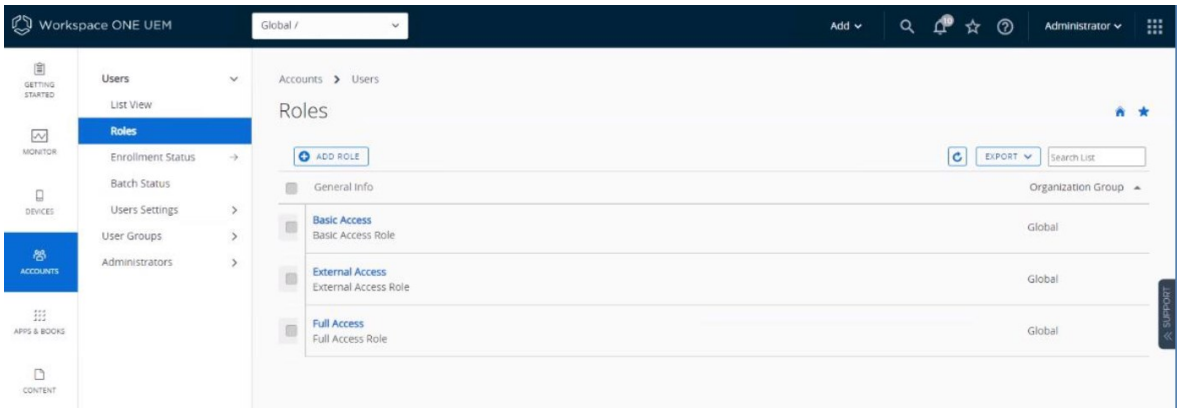
Postavljanje restrikcija vrši se također kroz konzolu gdje adimistrator klikanjem odobrava ili zabranjuje određene postavke.

3.3. Administracija korisnika i uređaja

Koristimo dva različita sustava za upravljanje mobilnim uređajima, ali oba mogu biti povezana sa internim AD (*eng. Active Directory*) ili možemo ručno dodavati korisnike. Dakako ova druga opcija nije poželjna ukoliko imamo veliku tvrtku sa puno zaposlenih, gdje bi ručno dodavanje uzelo puno vremena.

Kako svi zaposlenici nisu jednako rangirani po funkcijama, potrebno je napraviti određene grupe uloga u koje ćemo zaposlenika svrstati kako bi imali određene dozvole. Tako imamo tri grupe:

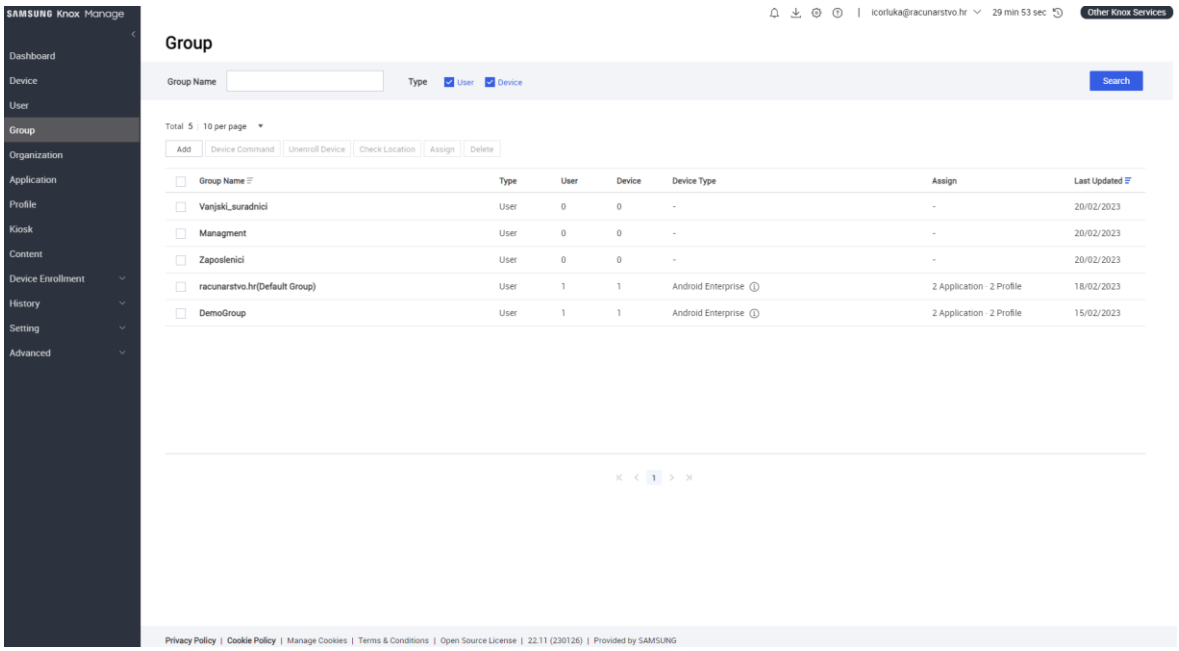
- grupa administratora,
- grupa zaposlenika, te
- grupa vanjskih suradnika.



Slika 3.9 Prikaz kreiranih korisničkih grupa Workspace ONE

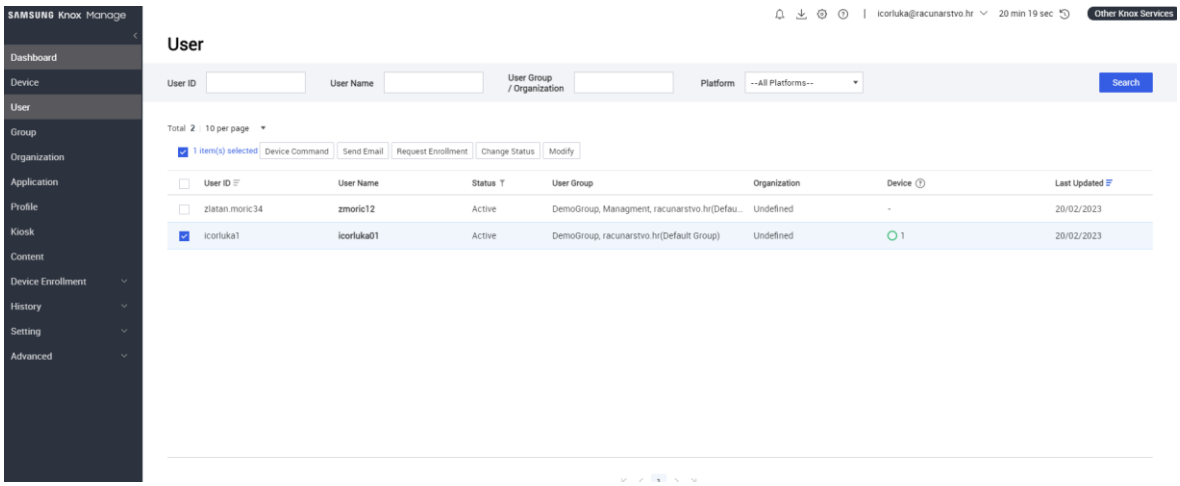
Kada se šalje aktivacijski token, odnosno jednokratna šifra za postavljanje mobilnog uređaja, odabire se funkcija koju će taj korisnik imati. U kategoriju Basic access spadaju svi zaposlenici, External access spadaju vanjski korisnici koji je potreban mail i Full acess spada visoki menadžment.

Identičnu stvar pruža i Samsung Knox, gdje u slici ispod možemo vidjeti dodavanje organizacijskih jedinica u grupe koje svaka ima svoja ograničenja.



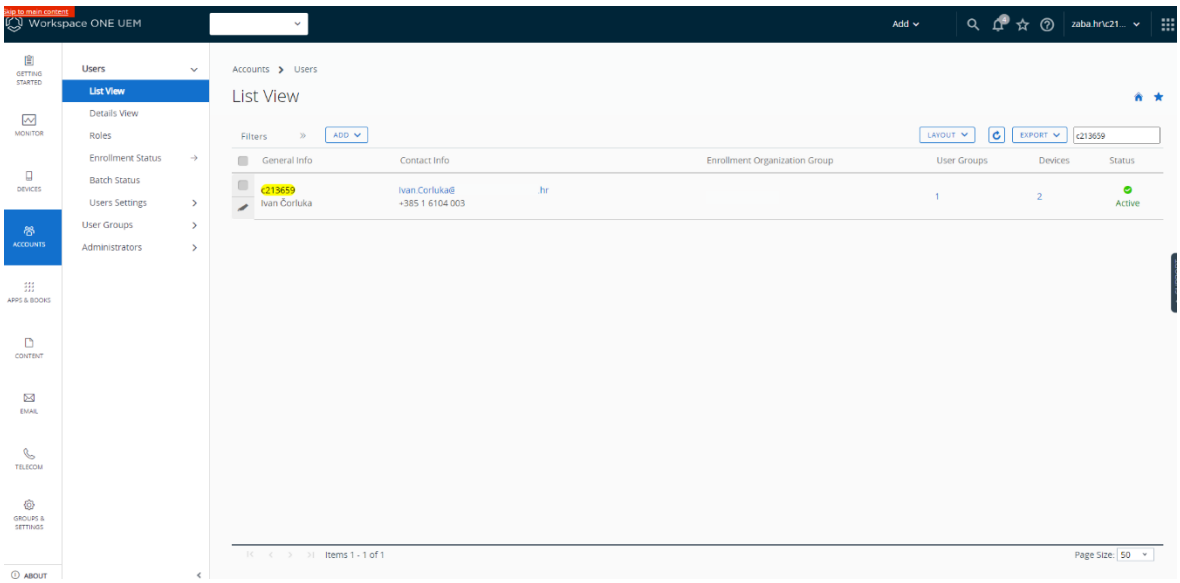
Slika 3.10 Prikaz korisničkih grupa Samsung Knox

Nakon što su korisnici dodani u sustav, bilo ručno ili putem AD (eng. Active Directory) oni se mogu pretraživati po broju radnika, imenu i prezimenu i čak po imenu uređaja kojeg koriste.



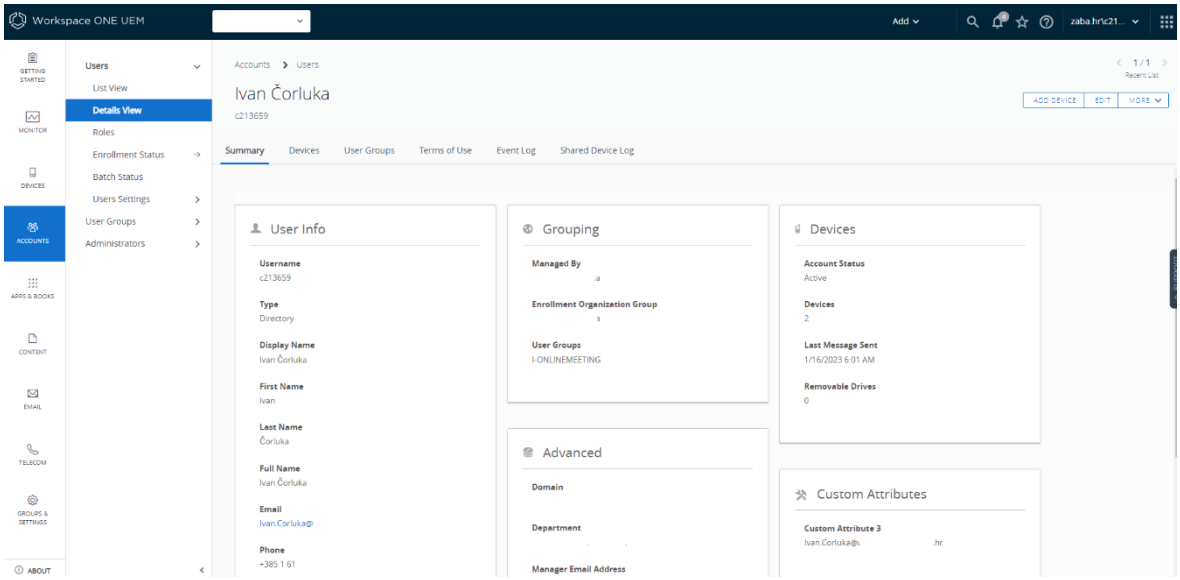
Slika 3.11 Pretraživanje korisnika Samsung Knox

Na slici ispod možemo vidjeti da sam pretraživao usera po broju radnika, no u Workspace ONE konzoli također mogu pretraživati po IMEI broju uređaja, serijskom broju itd.



Slika 3.12 Pretraživanje korisnika Workspace ONE

Ukoliko je konzola spojena sa Active Directory, odnosno domenom, možemo vidjeti sve informacije o zaposleniku.



Slika 3.13 Detaljne informacije o korisniku

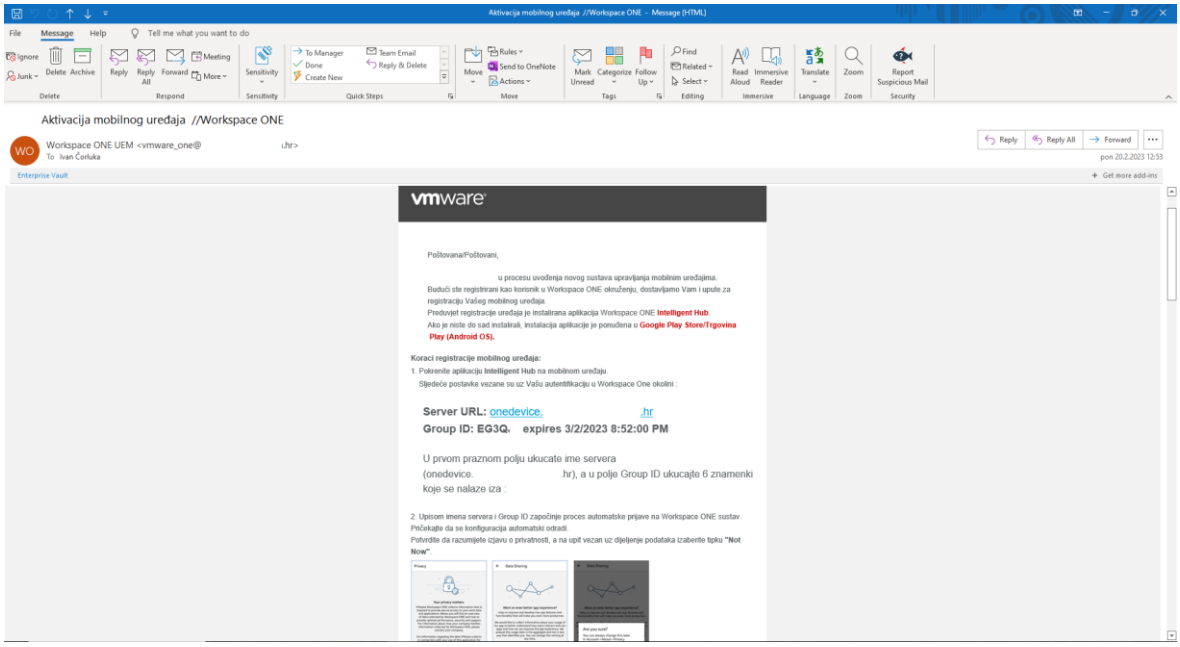
To nam dakako olakšava stvar da ne bi trebali dodavati korisnika svakog pojedinačno, a kada se izbriše iz domene također nestaje i u konzoli.

4. Ključne značajke MDM rješenja

Mobilni uređaji koje zaposlenici zadužuju služe kako bi u bilo kojem trenutku bili dostupni odraditi zadatak vezan za posao, bez obzira gdje se nalaze. U prijašnjim poglavljima smo opisali što je sve potrebno kako bi se cijeli sustav postavio, a sada ćemo pokazati kako se on implementira na same mobilne uređaje i kako se ono koristi.

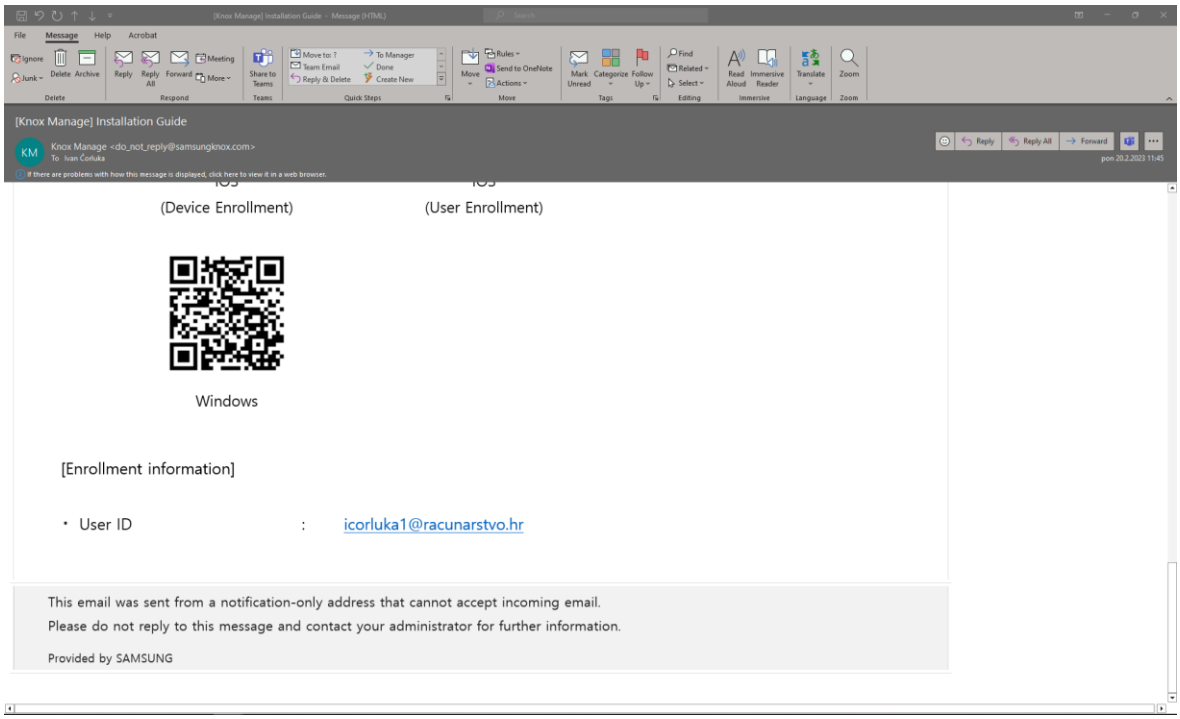
4.1. Postavljanje uređaja

Sama instalacija ne zahtjeva preveliko tehničko znanje kako bi se uređaj postavio u korporativno okruženje. Da bi se smanjila asistencija administratora sustava, prilikom slanja aktivacijskih tokena putem maila dolaze i upute pomoću kojih zaposlenik sam postavlja mobilno rješenje na svoj korporativni mobitel/uređaj.



Slika 4.1 Aktivacijski mail Workspace ONE

Kod sustava Workspace ONE dobiva se server URL (*eng. Uniform Resource Locator*) i upisuje se šesteroznamenkasti jednokratni token koji sam pokreće instalaciju.

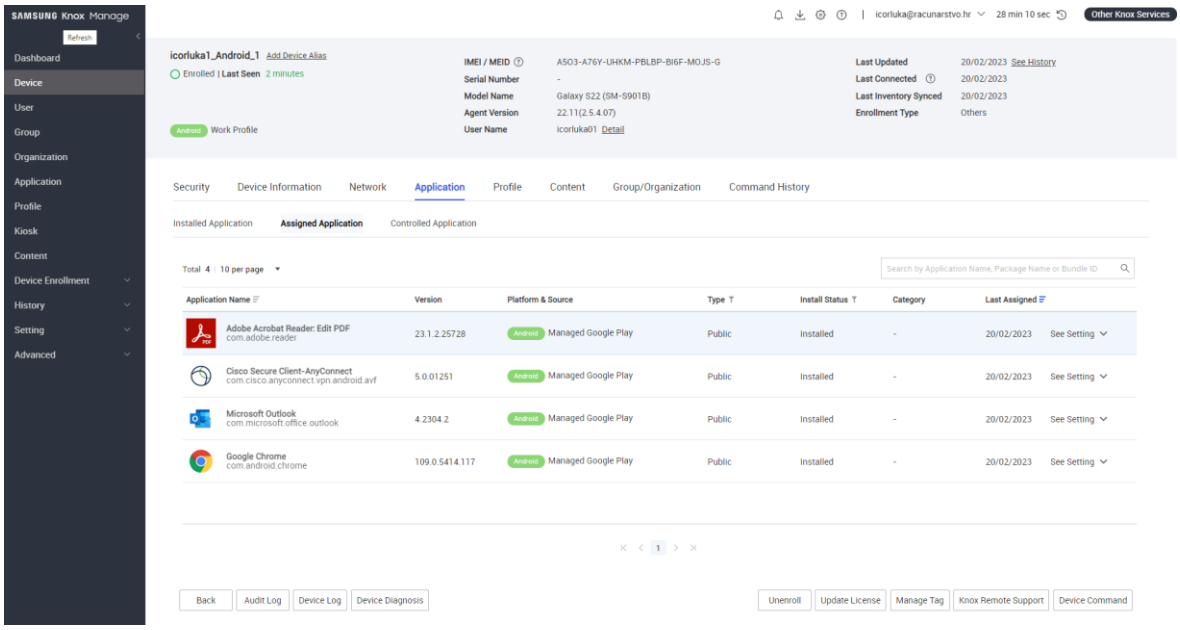


Slika 4.2 Aktivacijski mail Samsung Knox

Samsung Knox ima slično rješenje postavljanja mobilnog maila gdje u uputama dostavlja QR kod pomoću kojega se preuzima aplikacija Knox Manage Agent te se u njemu upisuju kredencije koje su postavljene od strane administratora.

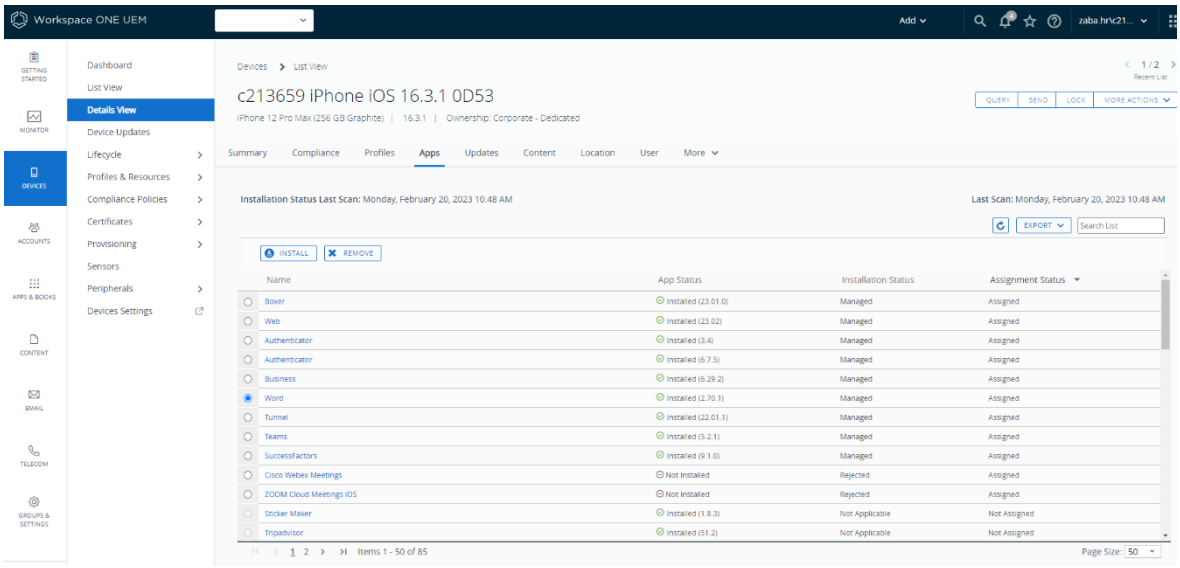
4.2. Upravljanje mobilnim aplikacijama

Kod implementacije smo postavili da se pojedine aplikacije automatski instaliraju, na primjer aplikacija za VPN (*eng. Virtual Private Network*), za mobilni mail, pdf čitači ili neke korporativne interne aplikacije. No također, nekim zaposlenicima nisu potrebne sve aplikacije, stoga će ona biti dostupne za preuzimanje u Google Play Store ili u iOS App Store kako ne bi nepotrebno trošili resurse memorije na uređaju.



Slika 4.3 Brisanje aplikacije preko konzole Samsung Knox

Preko konzole Knoxa ili Workspace ONE moguće je dodavanje ili brisanje pojedinih aplikacija na mobilnim uređajima koje bi mogle kompromitirati sami uređaj.

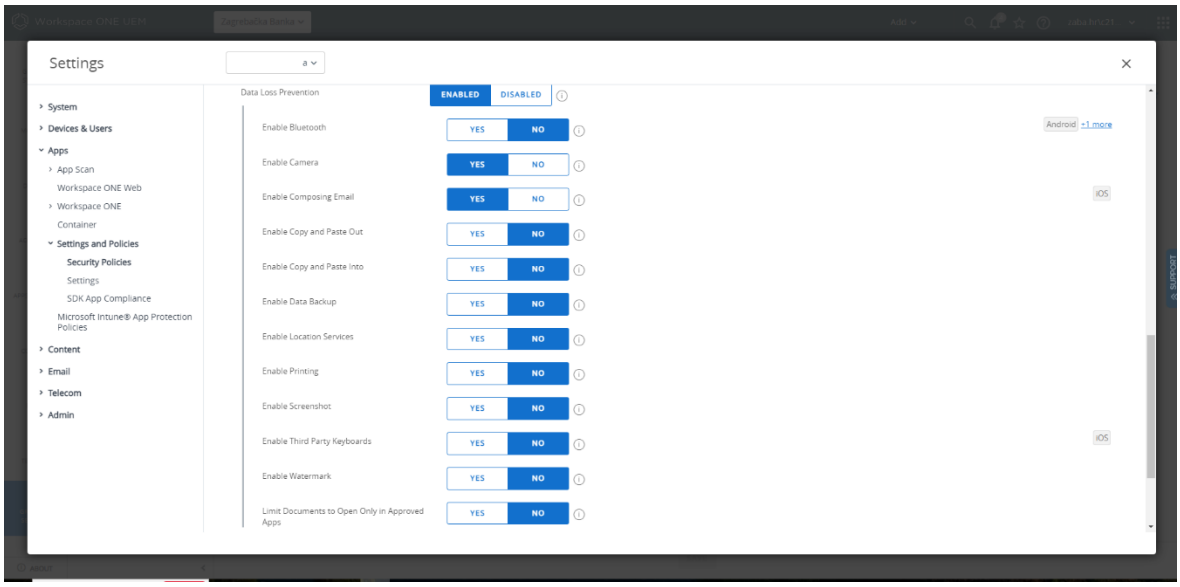


Slika 4.4 Brisanje aplikacije preko konzole Workspace ONE

Aplikacije se momentalno brišu sa uređaja, ukoliko je uređaj dostupan na mobilnoj mreži ili putem bežične veze.

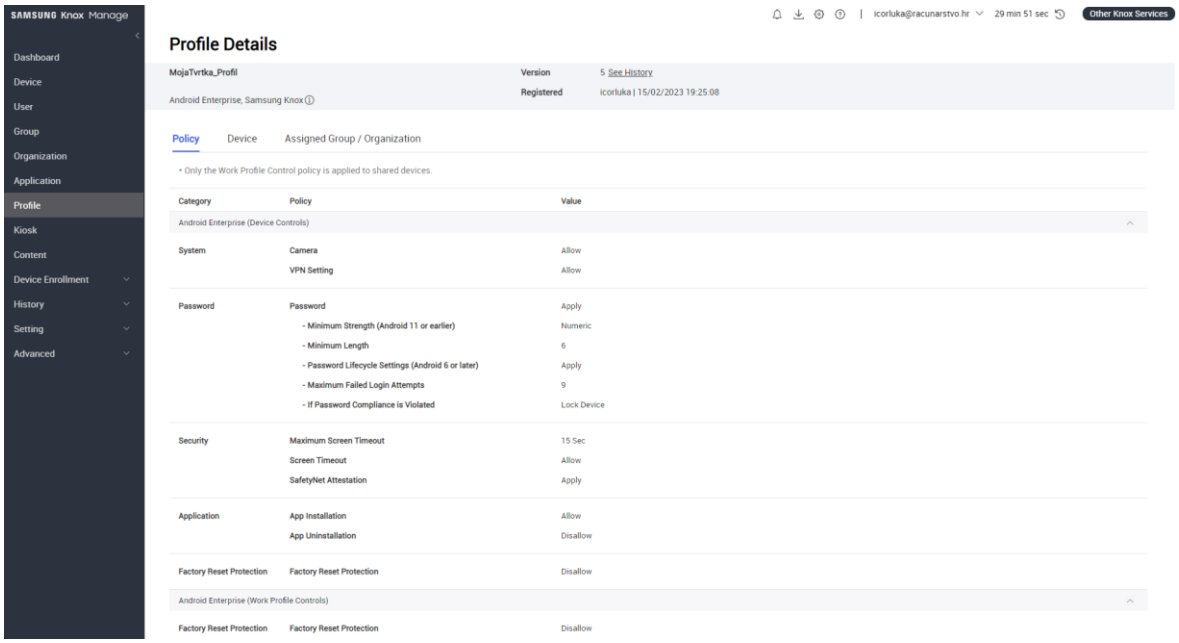
4.3. Konfiguracija sigurnosnih politika na mobilne uređaje

Kroz samu implementaciju morali smo postaviti kolekciju postavki kako bi se sve nužne prilikom postavljanja uređaja spustile na mobilne uređaje. Postavke koje smo naučili koristiti na privatnim mobitelima i koje nam olakšavaju stvari u svakodnevnom životu, u na poslovnim uređajima se moraju ograničiti. Razlog leži u tome kako bi zaštitili podatke i informacije koje bi eventualno treća strana mogla zlouporabiti.



Slika 4.5 Restrikcije mobilnih uređaja Workspace ONE

Tako smo ograničili postavke poput kopiranja i lijepljenja sadržaja maila izvan aplikacije, onemogućen je backup na servise trećih strana, zabranili smo print dokumenata i privitci iz maila se otvaraju u samo izabranim aplikacijama.



Slika 4.6 Restrikcije mobilnih uređaja Samsung Knox

Lako je primijetiti da su postavke politika zabrane jako slične na oba sustava imaju generičke predefinirane postavke kako bi olakšale administratorima da jednim klikom naprave zabranu.

5. Beneficije implementacije MDMa

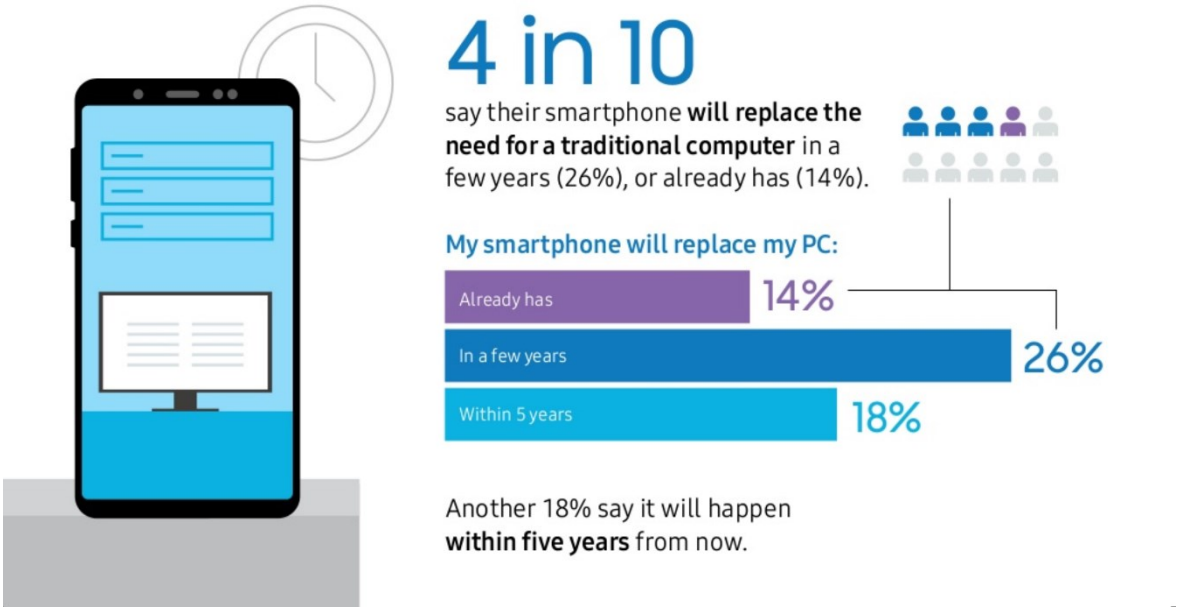
Implementacija sustava za upravljanje i nadziranje mobilnih uređaja u tvrtkama donosi brojne prednosti pretežito u području sigurnosti. Današnja sva rješenja za upravljanje mobilnim uređajima su gotovo identična, odnosno pružaju slične postavke upravljanja i zaštite mobilnim uređajima. Odabir ispravnog sustava je stvar potrebe tvrtke za takvim rješenjima, gdje se prije svega gleda cijena i da li je rješenje u skladu sa politikama tvrtke. To znači da tvrtka ako se bavi uslužnim djelatnostima kao na primjer usluge restorana, zasigurno im ne treba visoka sigurnost podataka u mobilnim uređajima, već samo dostupnost prema određenim aplikacijama i mail rješenju kao što je Outlook.

5.1. Poboljšana sigurnost

Rješenja koja opisujem u ovom završnom radu Samsung Knox i VMware Workspace One dostavljaju opsežne sigurnosne politike za korporativnu mail infrastrukturu. Ovim sustavima tvrtke mogu kontrolirati koji mobilni uređaji mogu pristupiti elektroničkoj pošti, spriječiti gubitak podataka, kriptirati osjetljive podatke i postaviti naprede politike. Aplikacija Browser za pretraživanje interneta pruža tvrtkama prilagođenu konfiguraciju postavki kako bi osigurali zahtjeve poslovanja i krajnjih korisnika. Također oba sustava imaju prilagođen File Content Manager koji osigurava distribuciju dokumenata i omogućava kolaboraciju na dokumentima u bilo koje vrijeme. Sve aplikacije distribuirane putem ova dva mobilna rješenja nalaze se u tako zvanim kontejnerima, oni pružaju separaciju korporativnih i osobnih podataka na mobilnom uređaju, time osigurava korporativne resurse i omogućava privatnost korisnika.

5.2. Povećana produktivnost

U post COVID-19 vremenu gdje smo se već svi navikli raditi od kuće, vrlo nam je bitno da oprema koju koristimo bude pouzdana i softverski ažurna, kako ne bi utjecala na našu produktivnost. Sustavi poput ovih koje sam opisivao u ovome radu služe da se sve razine organizacijskog odjela u tvrtki lakše i brže razmjenjuju informacije bilo putem elektroničke pošte, lokalnog Intraneta ili kolaboracijskih aplikacija poput Teams, Skype i slično. Zapravo ključ implementacije MDM rješenja svodi se na to da IT odjel cjelokupnim sustavom automatizira postavljane uređaja kako bi uštedjeli novac i vrijeme pogotovo ako se radi o velikoj količini uređaja koje treba postaviti, bez potrebe za dodatnim zapošljavanjima. Takav automatizirani sustav olakšava posao sebi na način da krajnjem korisniku isporuči aktivacijski mail sa uputama, bez potrebe dolaska na lokaciju tvrtke.

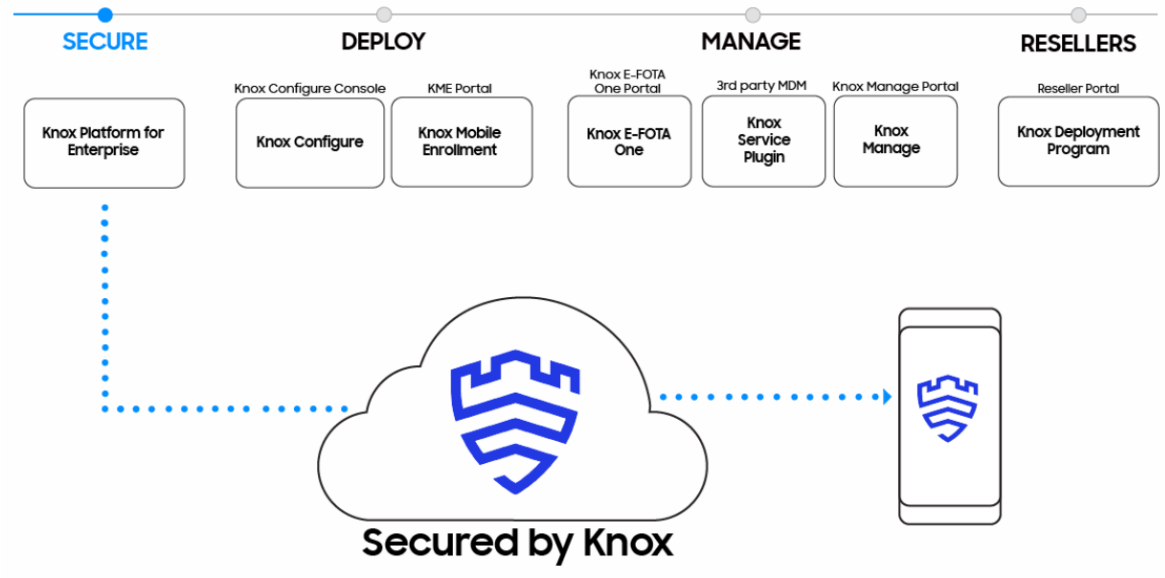


Slika 5.1 Anketa ispitanika vezano za uporabu mobilnih uređaja u poslovne svrhe

Jedna anketa na web stranici[6] je pokazala kako 40% zaposlenika kaže da mobilni uređaj može zamijeniti konvencionalno računalo, te da sve svoje svakodnevne zadatke mogu riješiti putem mobitela, što se može vidjeti na slici iznad.

5.3. Usporedba troškova sustava Knox i Workspace ONE

Kada krenemo uspoređivati cijene ova dva sustava, teško je naći neki zajednički jezik kolika je cijena za provedbu. Samsung ima jedu zanimljivost koju nudi sa svojim mobilnim rješenjem, a to je da svi mobilni uređaji Samsung po defaultu imaju ugrađen Knox sustav u svoje uređaje. To znači ako preko lokalnog dobavljača nabavljate Samsung mobitele za svoju tvrtku imate pravo besplatno korištenje cloud sustava za upravljanje mobilnim uređajima do 90 dana za 30 uređaja. Zapravo cijela ideja tvrtke Samsung se bazira na ideji Knox Ecosystem, to jest da sve možete obaviti na jednom mjestu, od kupnje uređaja i održavanju do implementacije MDMa i na kraju da se mobitel jednostavno dodijeli krajnjem korisniku, zaposleniku.



Slika 5.2 Samsungov ecosustav Knox[7]

Dok Samsung i VMware nude različite varijante za pretplatu kao, uređaj po godini ili uređaj po mjesecu, trebalo bi uzeti u obzir bitne faktore kao što su broj uređaja, funkcionalnost, podrška i usluga koje će se koristiti. Sa financijske strane treba uzeti aspekt da troškovi nisu povezani samo sa odabirom i implementacijom MDM rješenja, već je važno napomenuti da usporedba troškova ova dva rješenja nije jednostavna i ovisi o različitim čimbenicima kao što su potrebe organizacije, broj uređaja i metoda implementacije. Stoga se preporuča procijeniti troškove i koristi svakog rješenja prije donošenja odluke.

5.4. Korisničko iskustvo

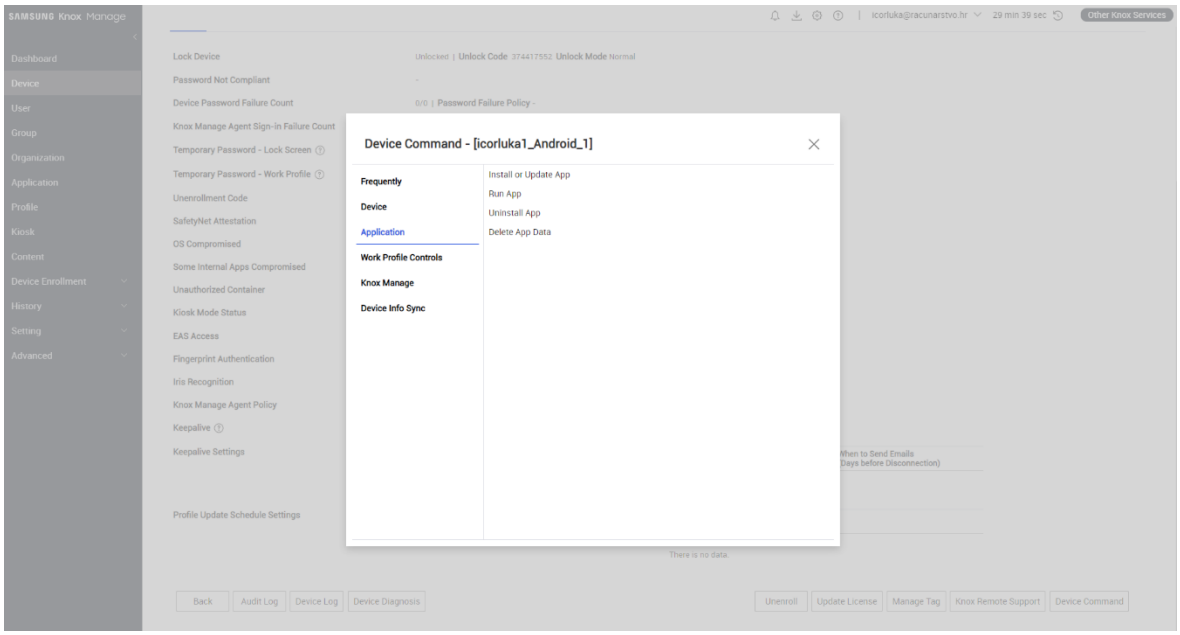
Analizirajući obje platforme za mobilna rješenja došao sam do zaključka da ono može biti učinkovito ovisno o potrebama tvrtke i njenih zaposlenika. Važno je procijeniti specifičnosti i mogućnosti svakog rješenja kako bi se utvrdilo koje će najbolje zadovoljiti potrebe tvrtke. Oba rješenja nude najbolje što se na tržištu trenutno može ponuditi, a da je krajnji cilj pružiti stabilno i sigurno iskustvo zaposlenicima koji pristupaju korporativnim resursima na mobilnim uređajima. Samsung Knox nudi vlastito iskustvo za Samsung uređaje, dok Workspace ONE nudi pristup koji može raditi na širem rasponu uređaja i operativnih sustava. To može biti posebno korisno za organizacije s različitim flotama uređaja ili politikom donesite vlastiti uređaj (BYOD). Međutim, korisničko iskustvo također može biti složenije ili manje integrirano za neke korisnike u usporedbi s izvornim rješenjem poput Samsung Knoxa. U poglavlju vezano za produktivnost može se vidjeti slika 5.1. ankete gdje korisnici kažu da većinu osnovnih zadaća mogu odraditi na svome uređaju.

6. Sigurnost mobilnih uređaja

U ovom poglavlju ćemo objasniti sigurnost uređaja koji su pod nadzorom neke organizacije ili tvrtke koja je odlučila u svojim politikama da svi podaci na poslovnom djelu uređaja moraju biti zaštićeni. Pokazat ćemo daljinsko brisanje uređaja, kako je uređaj povezan na korporativnu mrežu, što to zapravo znači za privatnost zaposlenika sa korporativnim upravljanjem mobitela.

6.1. Daljinsko brisanje

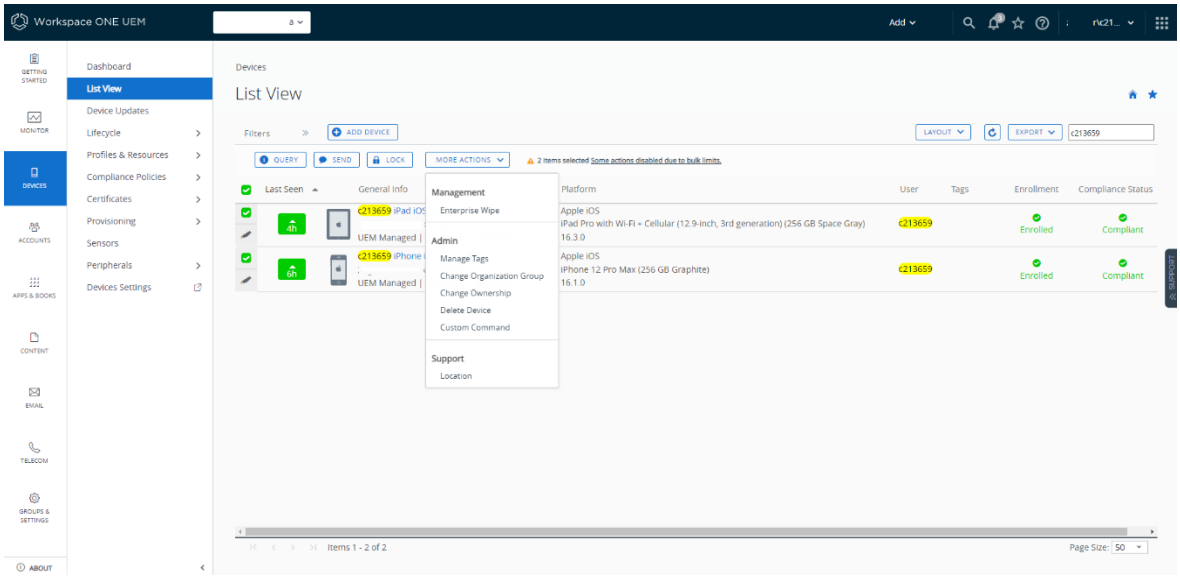
Ova vrlo korisna značajka u MDM sustavu koja administratorima omogućuje daljinsko brisanje podataka na upravljanom uređaju u slučaju da uređaj izgube, bude ukraden ili kada zaposlenik napusti tvrtku. Ova je značajka važna za organizacije jer pomaže u zaštiti osjetljivih podataka i intelektualnog vlasništva sprječavajući neovlašteni pristup uređaju i podacima. Ova je značajka posebno korisna za organizacije koje se bave osjetljivim podacima kao što su financijske institucije, zdravstvene ustanove i vladine organizacije.



Slika 6.1 Samsung Knox enterprise wipe

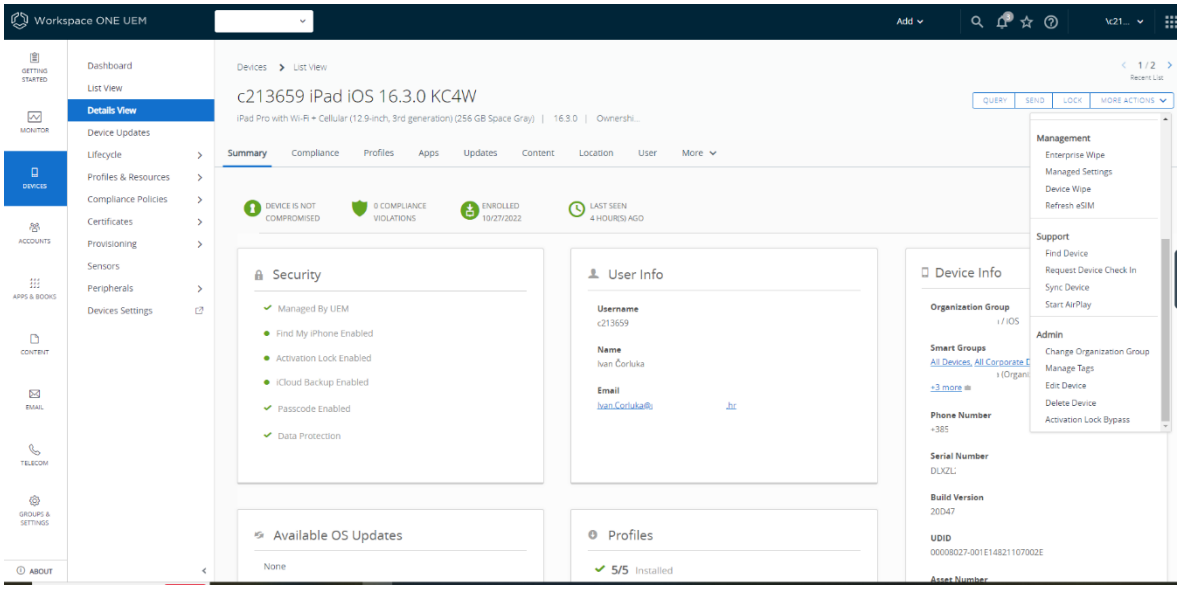
Prilikom kreiranja profila i politika u Samsung Knox Manage postavili smo da se ne briše cijeli uređaj, već samo poslovni profil. No, kod Workspace ONE imamo potpunu kontrolu nad uređajem i tu ćemo obrisati cijeli uređaj, odnosno možemo ga postaviti na tvorničke

postavke. To znači da će uređaj biti obrisan u potpunosti, ali opet prilikom pokretanja tražiti će da se upiše ispavan AppleID račun kako bi se uređaj mogao pokrenuti. Bez unosa ispravnog računa za prijavu, uređaj je totalno beskoristan.



Slika 6.2 Prikaz svih uređaja od zaposlenika

Ukoliko zaposlenik ima više uređaja, mogu se označiti svi te se grupno izbrisati.

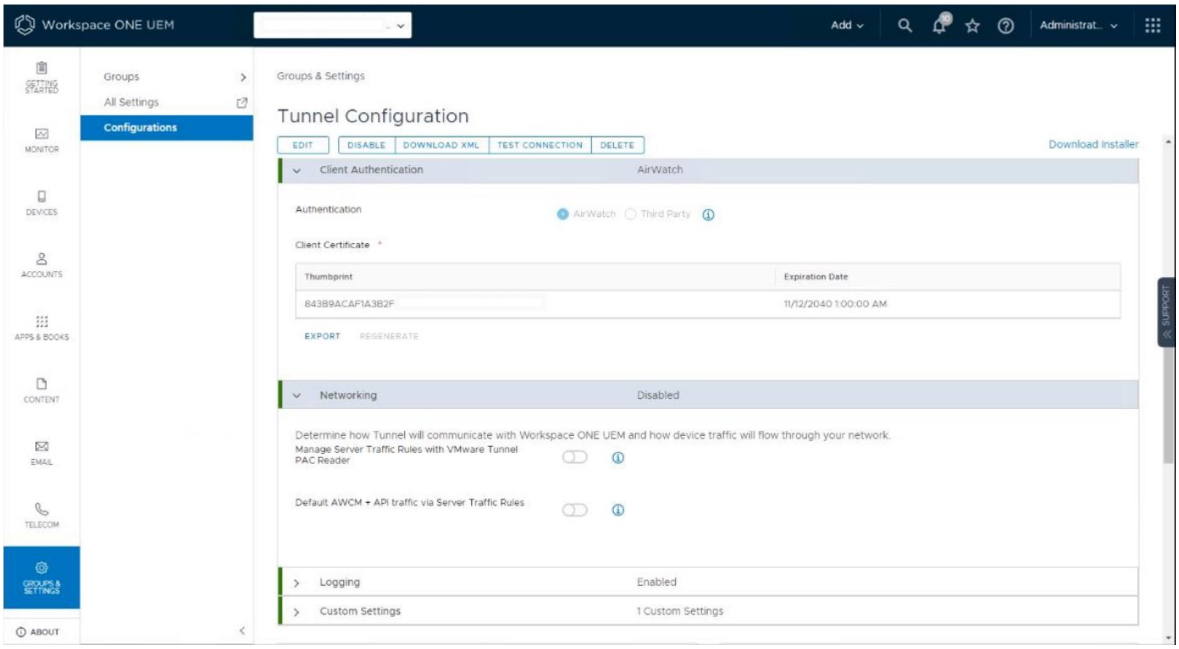


Slika 6.3 Brisanje uređaja

Također Workspace one nudi mogućnost brisanja samo poslovnog profila na uređaju, koji može poslužiti ukoliko je zaposlenik otišao iz tvrtke, te nije potrebno brisanje cijelog uređaja.

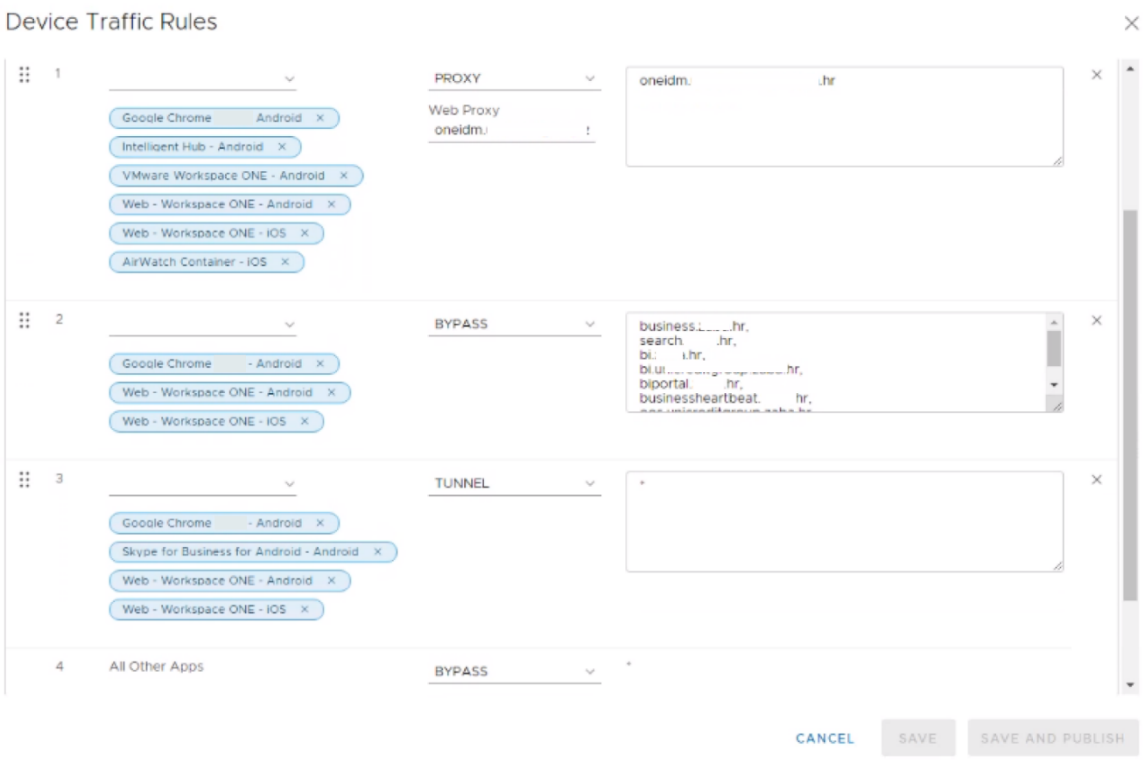
6.2. Enkripcija uređaja

Najvažniji aspekt upravljanja mobilnim uređajima je enkripcija podataka kako na samom uređaju tako je potrebno osigurati i kriptiranu vezu prema udaljenim podacima, odnosno pristupu podacima na unutar naše tvrtke. Workspace ONE nudi rješenje za end-to-end enkripciju putem aplikacije Tunnel, ona pruža sigurnu vezu između uređaja i internih resursa, omogućavajući siguran pristup korporativnim podacima. Takva enkripcija se ostvaruje putem protokola SSL (eng. Secure Sockets Layer) koja se ostvaruje između klijenta i pristupnog servera, za sav promet koji ide preko Interneta. Nakon što smo kreirali popis sigurnih aplikacija korporativnom pristupu putem aplikacije Tunnel, potrebno je implementirati jedinstveni X.509 certifikat za enrollane uređaje. Takav certifikat ćemo koristiti za međusobnu provjeru autentičnosti i enkripciju između aplikacije i aplikacije Tunnel.



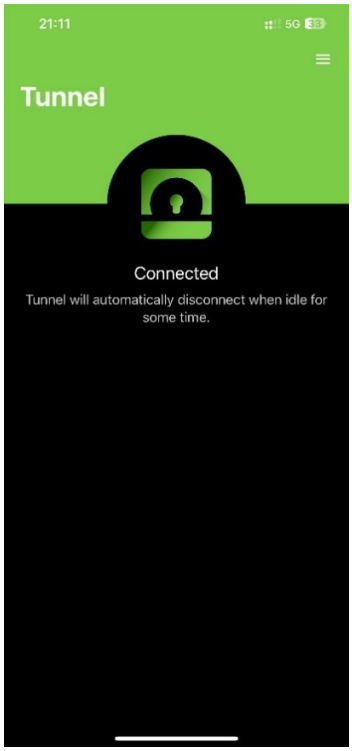
Slika 6.4 Postavljenje klijentskog certifikata Tunnel

Nakon što smo postavili certifikat potrebno je postaviti pravilima i aplikacije koje će koristiti siguran promet kroz aplikaciju Tunnel.

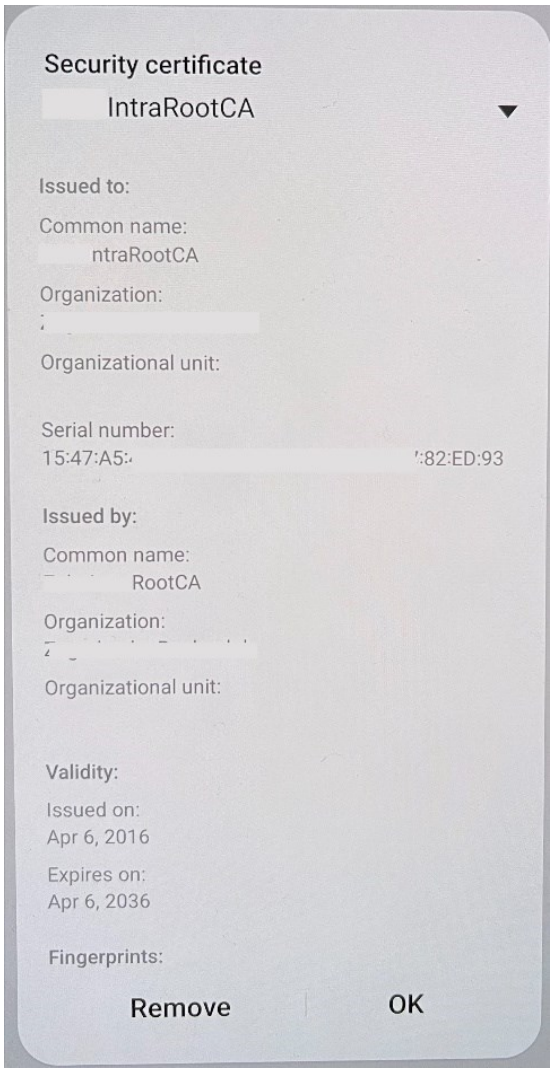


Slika 6.5 Popis aplikacije koje će koristiti Tunnel kao sigurnu vezu

Na slici ispod se može vidjeti kako je VPN konekcija između mobilnog uređaja i sustava aktivna, no ta konekcija nije stalna nego se tunel uspostavlja pri potrebi.

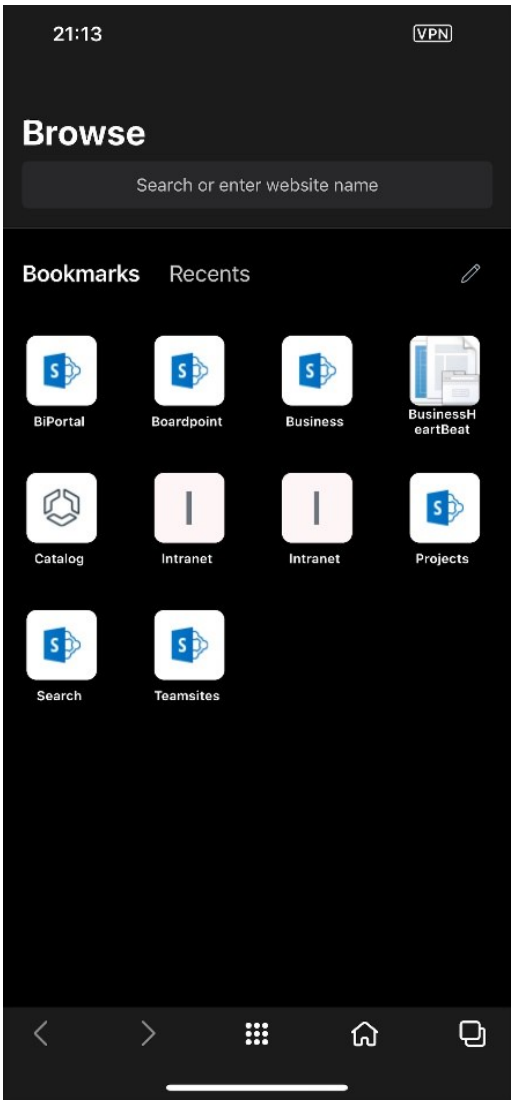


Slika 6.6 Aktivna konekcija VPN-a preko aplikacije Tunnel



Slika 6.7 Certifikat klijenta na mobilnom uređaju

Na mobilnom uređaju nije potrebno upisivati nikakve kredencije za uspostavu VPN konekcije, ona se vrši već spomenutim certifikatom koji je implementiran prilikom postavljanja uređaja.



Slika 6.8 Uspostava VPN-a prilikom otvaranja aplikacije koja zahtjeva sigurnu vezu

Samsung Knox sustav također ima sličan sustav, no on koristi aplikacije trećih strana poput Cisco AnyConnect aplikacije za uspostavu sigurnije veze. No Samsung koristi još neka rješenja na svojim uređajima poput Sensitive Data Protection (SDP) koji služi da se podacima pristupi tek nakon provjere autentičnosti korisnika, te potom na taj način dešifrira datoteke i podatke na uređaju. I noviji sustav DualDAR koji pruža dva odvojena sloja šifriranja i generiranja ključeva, kako bi se pristupilo podacima koji su smješteni unutar radnog profila, a ne i privatnog dijela. Time se postiže visoka zaštita podataka.

6.3. Privatnost korisnika

Upravljanje mobilnim uređajima je dovelo do visoke sigurnosti mobilnih uređaja, no poneki zaposlenici bi mogli izazvati zabrinutost prilikom prihvaćanja uvjeta korištenja MDMa kako na korporativnim tako i na privatnim uređajima ako je tamo implementirano. Korporacije i tvrtke koje implementiraju takva rješenja moraju uspostaviti jasne politike i smjernice za upotrebu koje balansiraju sigurnosne potrebe s pravom zaposlenika na privatnost, osiguravajući transparentnost o tome koje podatke prikupljaju, tko ima pristup i kako ih se koristi. Ukoliko se zaposlenici ne slažu sa nekim od politika, potrebno im je dati mogućnost isključivanja MDMa sa uređaja koje koriste, kao i mogućnost pregleda i brisanja prikupljenih podataka. Takvim proaktivnim pristupom i edukacijom zaposlenika, korporacije i tvrtke moraju uspostaviti povjerenje zaposlenika u sustav i održavati usklađenost s propisima o privatnosti podataka.

7. Financijski izazovi i ograničenja

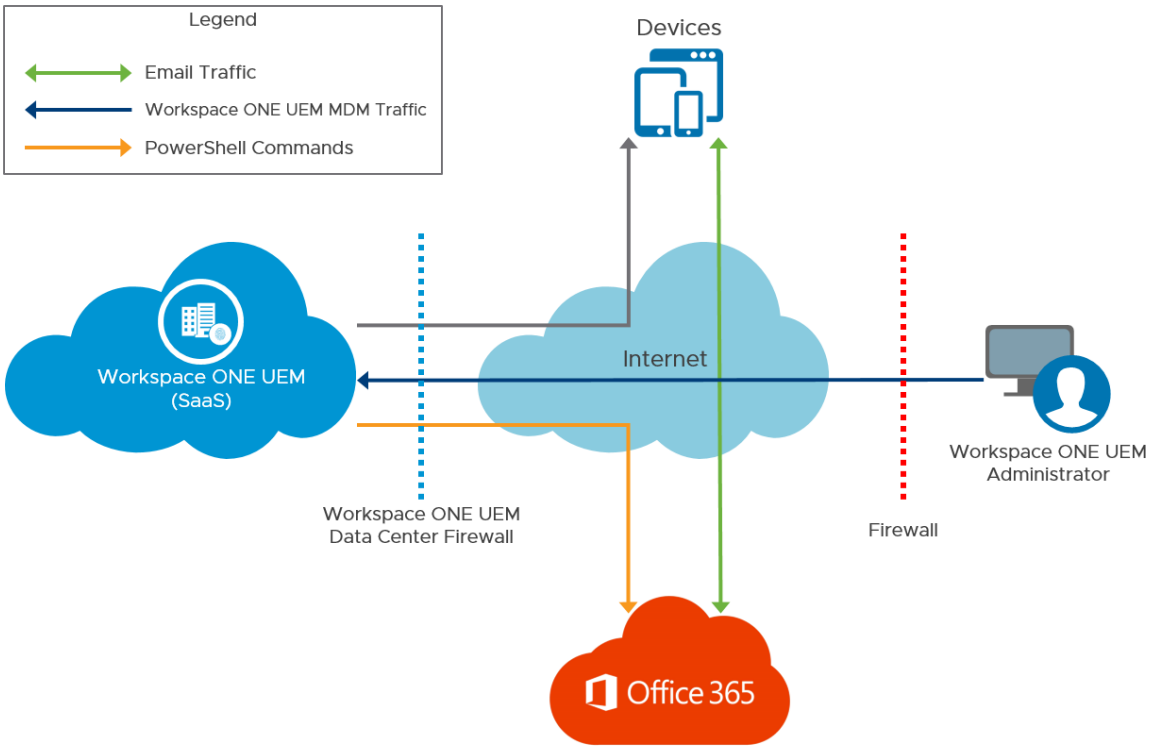
Kada se stvori poslovna potreba korporacije za MDM rješenjima sama implementacija može predstavljati određene financijske, organizacijske i tehnološke izazove. Kao prvo bi izdvojio kompatibilnost uređaja koje koristi neka tvrtka, ukoliko koristi starije modele mobilnih uređaja što može ograničiti opseg i učinkovitost sustava. U poglavlju prije sam spomenuo da se može naići na otpor korisnika koji jednostavno ne žele da su njihovi mobiteli pod kontrolom tvrtke jer su zabrinuti zbog svoje privatnosti praćenja aktivnosti. Na koncu uvijek govorimo o financijama, a sami troškovi implementacije i održavanja zahtijevaju značajna ulaganja u smislu hardvera, softvera i obuke IT osoblja koji će cijeli sustav održavati.

7.1. Integracija sa naslijeđenim sustavima

Sama integracija novog MDM rješenja sa naslijeđenim sustavima može zadati glavobolje svakom IT menadžeru koji dobije takav zadatak, glavni uvjeti uglavnom su da bude brzo i jeftino. No, nije svaka tvrtka tehnološki div da ima najnovije sustave hardvera i softvera, kako bi implementacija MDM rješenja prošla glatko. Prije razmatranja implementacije potrebno je paziti na kompatibilnost sustava i tehnologije koja tvrtka koristi, svakako je možda i najvažnije dobro isplanirati migraciju podataka i uvidjeti kakvi su sigurnosni procesi unutar firme, kako bi sustav bio otporan na kibernetičke prijetnje. Potrebno je paziti da naslijeđeni sustavi nemaju zastarjele sigurnosne protokole ili ne podržavaju najnovije softverske i hardverske zahtjeve. Bilo koje MDM rješenje da se izabere potrebno je da imamo odličnu komunikaciju sa tehničkom podrškom davatelja takve usluge kako bi plan integracije bio prilagođen i uspješno izvršen.

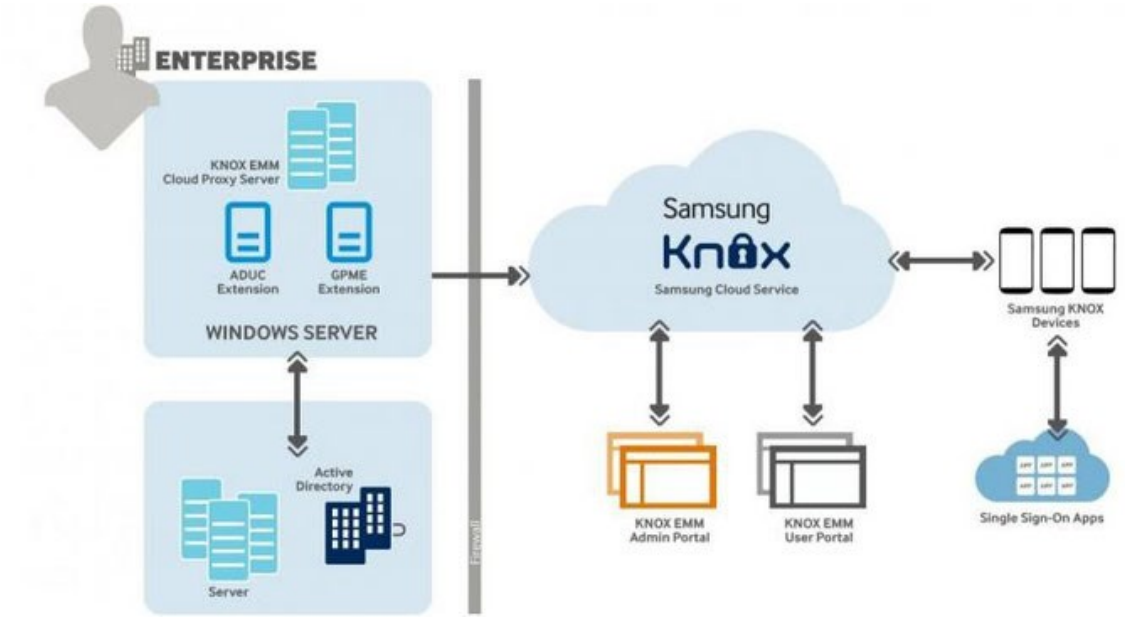
7.2. Upravljanje ekosustavom mobilnih uređaja

Praksa nadgledanja i kontrole cijelog spektra mobilnih uređaja u organizaciji odnosi se na oba MDM rješenja koja opisujemo. Oba rješenja nude slične značajke koje uključuju registraciju uređaja, upravljanje konfiguracijom, praćenje usklađenosti politika i upravljanje sigurnosnim politikama. Workspace ONE rješenje nudi mogućnost da korporacija upravlja i štiti uređaje s jedne konzole, vrlo je fleksibilan sa naslijeđenim sustavima i omogućuje spektar mogućnosti upravljanjem uređaja koji ne moraju biti od jednog proizvođača.



Slika 7.1 Arhitektura Workspece ONE [8]

Sa druge strane imamo Samsung Knox ekosustav, koji pruža tvrtkama rješenja upravljanja cijelim životnim ciklusom uređaja, implementacije platforme, sigurnosti, i održavanjem. Nije uvjet ali cijeli sustav je dizajniran prvenstveno za Samsung uređaje, što naravno ne isključuje druge proizvođače da koriste ovo rješenje. Zapravo oba ekosustava su jako slična no odabir ispravnog je stvar potrebe tvrtke.



Slika 7.2 Arhitektura Samsung Knox[9]

7.3. Visoki troškovi provedbe

Ukoliko se korporacija ili tvrtka odluči krenuti u implementaciju MDM rješenja, svakako najbitnije pitanje je koliko će to koštati? Troškovi se razlikuju ovisno o veličini tvrtke, broju zaposlenika i brojem uređaja koji će se koristiti. Treba naglasiti da sve značajke koje smo u poglavljima prije naveli podižu trošak samog rješenja.

Workspace ONE	Cijena	Značajka	Cloud/on-premise
Standard	6.52$/korisnik	Siguran pristup aplikacijama i upravljanje uređajima	Obje mogučnosti
Advanced	10.90$/korisnik	Cjelokupno rješenje UEM i sigurnost mobilnim aplikacijama	Obje mogučnosti
Enterprise	15$/korisnik	konzola za nadzor	Obje mogučnosti
Enterprise for VDI	25$/korisnik	konzola za nadzor	Cloud
Samsung Knox	Cijena	Značajka	Cloud/on-premise
Knox manage	1.60€/uređaj	konzola za nadzor cijelog sustava	Obje mogučnosti
Knox platform	uključeno sa uređajem	postoji u svakom Samsung uređaju	Obje mogučnosti
Knox enrollment	uključeno sa uređajem	postoji u svakom Samsung uređaju	Obje mogučnosti
Knox E-FOTA One	1.85€/uređaj	za nadzor OS verzija	Obje mogučnosti
Knox configure	0.62€/uređaj	servis za automatsko postavljaje uređaja	Cloud

Tablica 1 Usporedba cijene MDM rješenja

U tablici iznad možemo vidjeti cijene Workspace ONE i Samsung Knox rješenja, sam investitor mora procijeniti koji je model najbolji za njega i što mu je zapravo potrebno.

8. Najbolje prakse za implementaciju MDMa

Odabirom jednog od ova dva sustava uključuje razvoj jasnih politika i smjernica za korištenje mobilnih uređaja temelji se na potrebama organizacije i prijeko potrebno testiranje prije same implementacije. Potrebno je napraviti detaljan plan projekta, koji uključuje sve potrebne IT odjele u jednoj tvrtki, kako bi se sve ključne odluke donosile zajednički u cilju pružanja sveobuhvatnog osposobljavanja i podrške krajnjim korisnicima. Vrlo je bitno redovito dokumentirati, ocjenjivati sva ažuriranja kako bi rješenje pružalo učinkoviti sustav za upravljanje mobilnim uređajima.

8.1. Određivanje poslovne prakse

Tvrtka može maksimizirati učinkovitost implementiranog MDM rješenja sljedeći ove nekoliko od sljedećih rješenja:

- Definiranjem jasnih ciljeva koje su u skladu sa strategijom tvrtke
- Plan implementacije koji opisuje sve potrebne korake, vremenske rokove i ljudske resurse
- Uključenost zaposlenika kako bi primili na znanje i bili upućeni u proces implementacije
- Izrada sigurnosnih politika koja uključuje snažnu zaštitu podataka i obranu od kibernetičkih napada
- Jasne upute u kojima se navodi kako bi se mobilni uređaji trebali upotrebljavati, održavati i osiguravati
- Redovito ažuriranje aplikacija i nadogradnja operativnih sustava
- Kontinuirano uvođenje poboljšanja i praćenje zahtjeva krajnjih korisnika kako bi MDM bio u skladu sa poslovnim ciljevima.

Slika 8.1 Zašto nam je potreban MDM?[10]

Slika iznad zapravo pokazuje šturi hodogram kako bi se jedno poduzeće trebalo postaviti prije odabira implementacije sustava za upravljanje mobilnim uređajima.

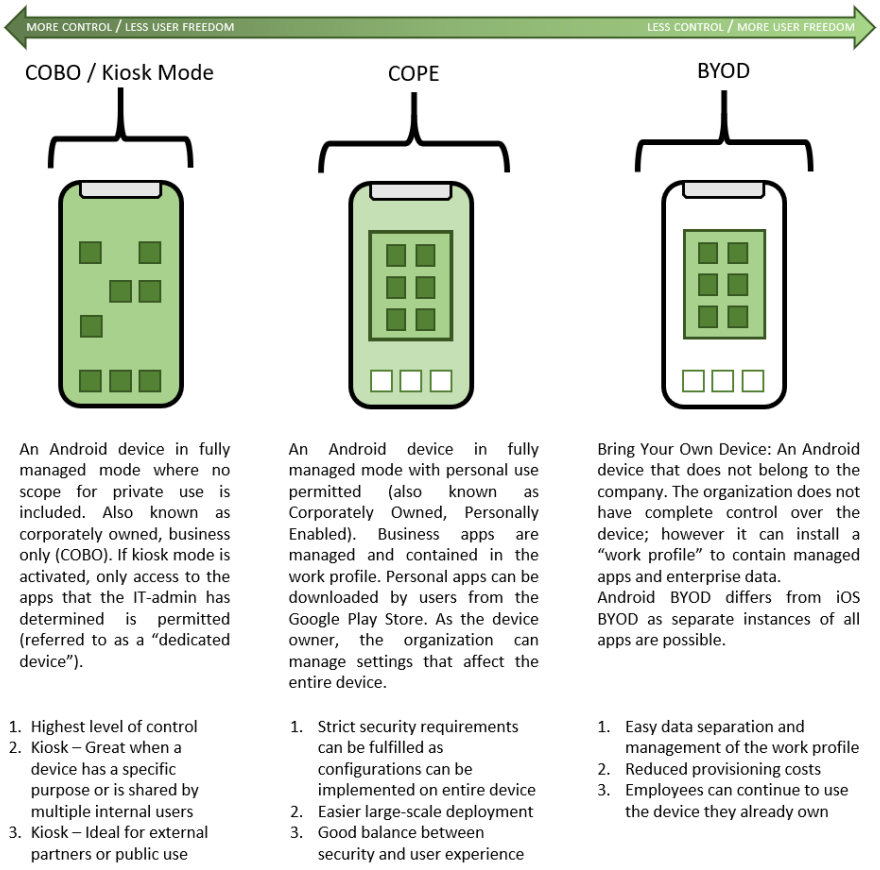
8.2. Pristupi upravljanja mobilnim uređajima

Postoje tri vrste pristupa upravljanjem mobilnim uređajima, svaki od tih modela ima svoje prednosti i određene mane. Bitno je korisnicima pružiti jasna pravila i smjernice korištenja uređaja, kako bi provedba sigurnosnih pravila bila u skladu sa politikama korporacije.

COBO (Corporate-Owned, Business-Only) uređaje kupuje tvrtka koja zaposlenicima daje uređaje kako bi ih koristili kako samo za potrebe obavljanja posla i ona njima u potpunosti upravlja. Značajna je kontrola nad uređajima, samim time i sigurnost.

COPE (Corporate-Owned, Personally Enabled) su uređaji koje također nabavlja tvrtka no osim za potrebe posla, uređaji se mogu koristiti i za osobne aktivnosti, no potrebno je voditi računa koje politike i zabrane implementirati jer korisnici na istom uređaju imaju i osobne podatke.

BYOD (Bring Your Own Device) ovaj pristup izrazito smanjuje troškove tvrtke vezano za kupnju uređaja, no ovaj model pristupa predstavlja najveću prijetnju sigurnosti sustava, jer tvrtka ima najmanju kontrolu nad uređajem i podacima pohranjenim na njemu.



Slika 8.2 Ilustracije prakse za upravljanje mobilnim uređajima[11]

U slici iznad možemo vidjeti različite tipove, odnosno pristupe MDM rješenja. Koje je odabrati najbolje, to je subjektivno pitanje koje mora odlučiti menadžment tvrtke koja će rješenje implementirati. Osobnog sam mišljenja da tvrtka koja osigurava svojim zaposlenicima mobilne uređaje koristi COPE mode, da se zaposlenicima ipak ostavi prostora da rastave privatni i poslovni dio mobitela, da je uređaj pod nadzorom tvrtke ali samo poslovni profil dok je privatni od korisnika. To smatram čisto iz praktičnog razloga jer neki zaposlenici ne žele stalno nositi dva uređaja, nego privatni i poslovni koriste u jednom.

Zaključak

Upotreba mobilnih uređaja u poslovne svrhe značajno se povećala posljednjih godina, a upravljanje tim uređajima postalo je iznimno važno. Organizacije imaju važan zadatak implementirati rješenja za upravljanje mobilnim uređajima kako bi pružila zaštitu podataka i imovine koje će njezini zaposlenici koristiti. Ovim završnim radom opisivali smo Samsung Knox i Workspace ONE rješenja, no i mnoga druga imaju vrlo slična značajke za provedbu sigurnosti i implementacije. Neke od najbitnijih značajki su šifriranje, siguran pristup aplikacijama, mogućnost daljinskog brisanja uređaja i sadržaja na njemu. Najkritičniji čimbenik implementacije MDM rješenja je osigurati da korisničko iskustvo ne bude negativno pogođeno. To znači da je potrebna komunikacija i edukacija zaposlenika, odnosno korisnika kako ispravno koristiti uređaje, kako bi bile zadovoljne politike tvrtke i kako bi bila osigurana maksimalna privatnost korisnika korištenjem uređaja koji je pod upravljanjem od strane tvrtke.

Sama implementacija može biti skupa i vrlo izazovna ako se ne zadovolje svi kriteriji odabranog rješenja, stoga je prije same implementacije potrebno provesti plan implementacije da li tvrtka može odabrano rješenje implementirati na vlastitu opremu ili će koristiti rješenje u oblaku. Takvim pristupom tvrtke mogu podići razinu poslovanja na višu razinu jer će zadovoljiti sve sigurnosne kriterije, zadovoljstvo zaposlenika i na koncu bržu i jednostavniju komunikaciju.

Popis kratica

MDM	*Mobile Device Managment*	Upravljanje mobilnim uređajima
EEM	*Enterprise Mobility Managment*	Sustav za upravljanje mobilnošću poduzeća
VPN	*Virtual Private Network*	Virtualna privatna mreža
LB	*Load Balancer*	Sustav za balansiranje mrežnog prometa
UEM	*Unified Endpoint Management*	Sustav za objedinjeno upravljanje
COBO	*Corporate-Owned, Business-Only*	Uređaj u vlasništvu poduzeća, samo za posao
COPE	*Corporate-Owned, Personally Enabled*	Uređaj u vlasništvu poduzeća, korištenje u osobne svrhe
BYOD	*Bring Your Own Device*	Korištenje vlastitog uređaja u poslovne svrhe
IMEI	International Mobile Equipment Identity	Međunarodni mobilni identitet opreme

Popis slika

Popis tablica

Literatura

[1] https://www.bmc.com/blogs/mdm-mobile-device-management/20.02.2023.

[2] https://www.techtarget.com/searchmobilecomputing/definition/COPE-corporate-owned-personally-enabled/ 20.02.2023.

[3] https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/ 20.02.2023.

[4] https://learn.microsoft.com/en-us/mem/intune/user-help/what-happens-when-you-create-a-work-profile-android/ 20.02.2023.

[5] https://softwarekeep.com/blog/office-365-mobile-device-management/ 20.02.2023.

[6] https://emteria.com/learn/what-is-device-management/ 21.02.2023.

[7] https://docs.samsungknox.com/admin/fundamentals/welcome.htm 21.02.2023.

[8] https://techzone.vmware.com/resource/workspace-one-uem-architecture#direct-powershell-model 21.2.2023.

[9] https://www.isec7.com/deutsch/emm/samsung-knox/ 21.02.2023.

[10] https://www.appknox.com/blog/what-is-mobile-device-management 21.02.2023.

[11] https://blog.cortado.com/de/android-enterprise/ 22.02.2023.

[12] https://docs.samsungknox.com/admin/fundamentals/welcome.html 18.2.2023.

[13] https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html; https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/rn/Workspace-ONE-UEM-Archived-documentation.html

[14] Omelchenko, T. A., Nikishova, A. V., Umnitsyn, M. Y., Omelchenko, I. A., & Umnitsyn, Y. P. (2020). Information security management of enterprise mobile device. Journal of Physics: Conference Series, 1661, 012008.

[15] Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications. Digital Business, 1(1), 100001.

[16] Batool, H., & Masood, A. (2020). Enterprise Mobile Device Management Requirements and Features. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).
[17] Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19.
[18] Pierer, M. (2016). MDM evaluation for small and medium sized enterprises. Mobile Device Management
[19] Dorjmyagmar, M., Kim, M., & Kim, H. (2017). Security analysis of Samsung Knox. 2017 19th International Conference on Advanced Communication Technology (ICACT).