ANALIZA FUNKCIONALNOSTI APLIKACIJA ZA UPRAVLJANJE MOBILNIM UREĐAJIMA

Lovrić, Hrvoje

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

ANALIZA FUNKCIONALNOSTI APLIKACIJA ZA UPRAVLJANJE MOBILNIM UREĐAJIMA

Hrvoje Lovrić

Zagreb, lipanj 2019.

Predgovor

Zahvaljujem se mentoru Zlatanu Moriću na doprinosu i pomoći pri izradi diplomskog rada, a najviše svojoj obitelji na podršci i razumijevanju bez kojih moje studiranje kao i ovaj diplomski rad ne bi bili mogući.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

U ovom radu obradit ću temu sustava za upravljanje mobilnim uređajima (*Mobile Device Managementa*) odnosno, fokusirat ću se na rješenje MobileIron kao jedno od mnogih softvera za *Mobile Device Management*. Dat ću kratki povijesni pregled, objasniti *Mobile Device Management* kao sustav, što je, kako se koristi, zašto bi ga uopće koristili te detaljnije objasniti aplikacije, funkcionalnost samog MobileIrona. Usporedit ću MobileIron s ostalim softverskim rješenjima za *Mobile Device Management* te objasniti najveće razlike, prednosti i mane različitih softvera. Svrha je pokazati prednost korištenja i implementacije *Mobile Device Managementa* u firmu/e što je pokazano u praktičnom dijelu ovog diplomskog rada.

Ključne riječi: mobilni uređaji, *Mobile Device Management*, MobileIron, softver, implementacija.

Sadržaj

1. Uvod 1

2. Povijesni pregled 2

3. O sustavima za upravljanje mobilnim uređajima 3

3.1 Zašto je sustav za upravljanje mobilnim aplikacijama koristan? 4

3.2 Ponesi svoj uređaj (BYOD) 4

4. Najpopularniji sustavi za upravljanje mobilnih uređaja 6

4.1 Intune 6

4.2 IBM MaaS360 7

4.3 Cisco Meraki 8

4.4 SAP Mobile Secure 9

5. MobileIron 11

6. Implementacija MobileIrona u radno okruženje 13

6.1 Sigurnosne politike 14

6.1.1 App Blacklist 15

6.1.2 Compromised devices 16

6.1.3 MI Client Out of Contact 17

6.1.4 Data protection/Encryption disabled 18

6.1.5 MDM / Device Adiministration Disabled 19

6.2. Konfiguracije 20

6.2.1 Katalog aplikacija 20

6.2.2 Pristup aplikacijama iz kataloga 21

6.2.3 Autorizacija i prevencija od gubitka podataka 22

6.2.4 Sigurnosne konfiguracije 23

6.3 Aplikacije i njihove konfiguracije 25
6.3.1 Email+ 25
6.3.2 Docs@Work 27
6.3.3 Web@Work 28
6.4 Administracija korisnika/uređaja 30
6.4.1 Korisnici 31
6.4.2 Uređaji 33
6.5 Shematski prikaz 36
7. Testiranje funkcionalnosti aplikacija MobileIron-a 38
8. Usporedba MobileIron-a s drugim sustavima za upravljanje mobilnim uređajima 42
8.1 Usporedba Intune-a i MobileIron-a u upravljanju podacima i uređajima 42
8.2 Tablica usporedbi rješenja 43
8.3 Gledajući u budućnost 44
9. Budućnost MDM-a 46
10. Zaključak 47
Popis kratica 48
Popis slika 49
Popis kôdova 52
Literatura 53

1. Uvod

Sustav za upravljanje mobilnim uređajima (*Mobile Device Management*) je sigurnosni softver koji IT odjelima omogućuje primjenu pravila koja osiguravaju, nadziru i upravljaju mobilnim uređajima krajnjih korisnika. Ovo ne uključuje samo pametne telefone, već se može proširiti i na tablete, prijenosna računala, pa čak i na IoT uređaje. MDM osigurava sigurnost korporativne mreže, a korisnicima omogućuje korištenje vlastitih uređaja i učinkovitije funkcioniranje.[1]

MDM je obično implementacija kombinacije aplikacija i konfiguracija na uređaju, korporativnih pravila te pozadinske infrastrukture, u svrhu pojednostavljenja i poboljšanja IT upravljanja krajnjih korisničkih uređaja. U modernim korporativnim IT okruženjima, brojnost i raznolikost upravljanih uređaja (i ponašanja korisnika) motivirali su rješenja MDM-a koja omogućuju upravljanje uređajima i korisnicima na dosljedan i skalabilan način. Glavna uloga MDM-a je povećati mogućnost podrške za uređaje, sigurnost i korporativnu funkcionalnost uz održavanje određene fleksibilnosti korisnika. MDM se prvenstveno bavi segregacijom poslovnih podataka, osiguravanjem e-pošte, osiguravanjem korporativnih dokumenata na uređajima, provedbom korporativnih politika, integriranjem i upravljanjem mobilnim uređajima, uključujući prijenosna računala i ručna računala različitih kategorija. MDM implementacije mogu biti na lokalnoj razini ili u oblaku.[2]

2. Povijesni pregled

Područje upravljanja mobilnim uređajima nastavlja se razvijati kako sve više profesionalaca koristi prijenosna računala i pametne telefone za rad. To je povećalo potrebu za rješenjima koja zaposlenicima omogućuju pristup informacijama gdje god se nalazili i u bilo kojem trenutku. Rana rješenja usmjerena isključivo na uređaje, kojima je nedostajalo upravljanje aplikacijama i sadržajem; danas, oni prerastaju u šira rješenja kako bi bolje obuhvatili sve mobilne mogućnosti.[3] Ovo je područje značajno evoluiralo tijekom posljednjih nekoliko godina. Danas imamo posebne uloge u upravljanju mobilnim okruženjima, uz posvećene timove za mobilnost (i sigurnost) poduzeća. Početni opseg MDM-a prvenstveno je bio vezan uz uređaje u stilu telefona i tableta, točnije za iOS i Android uređaje s podrškom za Windows Mobile, Blackberry i druge mobilne platforme. Danas, s izlaskom sustava Windows 10 i dodatnom funkcionalnošću za korištenje MDM mogućnosti, krajolik upravljanja uređajem se promijenio. Ono što je nekad bilo jasno razlikovanje između primjene uređaja s računalima / prijenosnim računalima i upravljanje uređajem s telefonima / tabletima spojilo se u jednu funkciju. To pruža mogućnost za promjenu načina upravljanja i implementacije uređaja. Sada kada se telefon / tablet i računalo / prijenosno računalo može upravljati unutar jedne funkcije i potencijalno jednim skupom alata, možemo početi mijenjati dinamiku uvođenja i upravljanja uređajima. Imamo priliku udaljiti se od naslijeđene metode snimanja uređaja i omogućiti učinkovitiju implementaciju koju pokreću potrošači. S predinstaliranim OS-om na uređaju, možemo gurnuti MDM agent na uređaj, što će nam zauzvrat omogućiti implementaciju aplikacija, konfiguracija i sigurnosnih zahtjeva za uređaje.[4]

3. O sustavima za upravljanje mobilnim uređajima

Upravljanje mobilnim uređajima razvijalo se tijekom vremena. Skalabilnost je u početku bila problem, ali centralno daljinsko upravljanje eliminiralo je zastarjele korake poput ažuriranja SIM kartice i klijenta. Moderni MDM softver može automatski detektirati nove uređaje priključene na korporativnu mrežu i primijeniti postavke za pojednostavljenu provedbu politike.

MDM može uključivati distribuciju aplikacija, podataka i konfiguracija za sve vrste mobilnih uređaja, uključujući mobilne telefone, pametne telefone, tablet računala, mobilna računala, mobilne pisače, mobilne POS uređaje itd. Kontrolom i zaštitom podataka i konfiguracijskih postavki svih mobilnih uređaja u mreži MDM može smanjiti troškove podrške i poslovne rizike. Namjera MDM-a je optimizacija funkcionalnosti i sigurnosti mobilne komunikacijske mreže uz minimiziranje troškova i zastoja.

Neke od osnovnih funkcija MDM-a uključuju:

- Osiguravanje konfiguriranja raznolike korisničke opreme na dosljedan standardni / podržani skup aplikacija, funkcija ili korporativnih pravila
- Ažuriranje opreme, aplikacija, funkcija ili pravila na skalabilan način
- Osigurati da korisnici koriste aplikacije na dosljedan i podržavan način
- Oprema za praćenje (npr. lokacija, status, vlasništvo, aktivnost)
- Biti u stanju učinkovito daljinski dijagnosticirati i otkloniti poteškoće s opremom

Upravljanje mobilnim uređajima zahtijeva dvije komponente u podatkovnom centru:

- Komponenta poslužitelja - gdje IT administratori konfiguriraju i šalju politike putem upravljačke konzole.
- Komponenta klijenta - koja prima i implementira naredbe na mobilnim uređajima krajnjeg korisnika. [5]

3.1 Zašto je sustav za upravljanje mobilnim aplikacijama koristan?

Postoji jako puno razloga zašto bi implementirali neku vrstu MDM-a u naše radno okruženje. Svaka firma koja brine o sigurnosti podataka koji su ključ svakog uspješnog poslovanja trebala bi imati pojačanu sigurnost i na mobilnim uređajima jer baš od gubitka istih prijeti najveća opasnost.

Daljinsko upravljanje jedna je od najočitijih prednosti MDM-a. Jamči povećanu sigurnost svakog mobilnog uređaja spojenog na mrežu, istodobno stvarajući mogućnost daljinskog onemogućavanja neovlaštenih korisnika i aplikacija. Korisnici se lako mogu osigurati od ukradenih i izgubljenih uređaja, a na organizacije je manje vjerojatno da će utjecati raniji zaposlenici koji imaju pristup osjetljivim podacima tvrtke. Pomoću MDM-a se lako mogu izbrisati povjerljive podatke s bilo kojeg uređaja.

MDM stvara centraliziranu kontrolu za korisnike koji trebaju instalirati aplikacije na svoje uređaje, a centralizirani sustav upravljanja stvara višestruke prednosti poput upravljanja pristupom temeljenom na ulogama i mogućnosti onemogućavanja aplikacija. Suvremena usklađenost s propisima trebala bi uključivati zakone koji sprječavaju neovlaštene uređaje da ugroze sigurnost vaše tvrtke. Osim toga, mogućnosti izvješćivanja MDM-a trebale bi omogućiti potvrdu integriteta mreže. S MDM-om, inicijative za poštovanje pravila pomno se prate kroz centraliziranu konzolu.

3.2 Ponesi svoj uređaj (BYOD)

Sve veća potrošnja u IT-u dovela je do toga da više zaposlenika dovodi svoje osobne uređaje na radno mjesto, a s tim nastaje i potreba za njihovim praćenjem i upravljanjem. BYOD ima mnoge prednosti, uključujući smanjenje troškova opreme i uštedu vremena IT odjelima (budući da će zaposlenici upravljati vlastitim uređajima), ali mogu uvesti sigurnosne rizike ako se uređaji ne prate na odgovarajući način.[1]

Upravljanje mobilnim uređajima ključno je za snažnu BYOD politiku, omogućavajući zaposlenicima da koriste vlastite uređaje, a istovremeno pokrivaju sve moguće sigurnosne praznine. Ovisno o poslovanju, kulturi, zakonskim i regulativnim odredbama, kao i načinu

upravljanja rizikom, organizacija će odrediti način na koji će sustav biti implementiran. Naravno, ako je procijenjeni rizik prevelik, organizacija može u potpunosti zabraniti korištenje vlastitih uređaja, ali sustav nadzora bi i u tom slučaju trebao biti postavljen. [6]

Korištenje BYOD definitivno predstavlja rizik za poslovanje, najčešće prisutan kao rizik od krađe podataka, neovlaštenog pristupa aplikacijama i sustavima organizacije, gubitku reputacije i sl. Ako smo utvrdili da korisnici trebaju koristiti vlastite uređaje, iste moramo zaštiti na odgovarajući način, gdje u priču opet dolazi MDM koji je apsolutno nužan kod BYOD uređaja ukoliko želimo zaštiti poslovne podatke.

4. Najpopularniji sustavi za upravljanje mobilnih uređaja

Koje značajke treba potražiti u softveru za upravljanje mobilnim uređajima? Prije svega, trebao bi biti u mogućnosti podržati širok raspon mobilnih uređaja koje zaposlenici koriste na radnom mjestu. Drugo, trebalo bi imati osnovne mogućnosti koje će vam pomoći upravljati tri ključna područja - inventar uređaja, pravila uređaja i sigurnost uređaja. Treće, mora biti u mogućnosti pružiti nadzor i izvješćivanje u stvarnom vremenu.

Mogu postojati i druge značajke i mogućnosti, ovisno o proizvodu i dobavljaču. MDM je paket kao cjeloviti softver koji se sastoji od nekoliko alata. Softver se obično koristi zajedno s dodatnim alatima kao što je upravljanje mobilnom aplikacijom (MAM) kako bi se došlo do potpunog sigurnosnog rješenja za upravljanje mobilnošću u poduzeću (EMM). Postoji nekoliko desetaka MDM rješenja, u ovom radu ću spomenuti najpopularnije, odnosno najkorištenije te njihove glavne značajke. MobileIron, koji je glavna tema ovog rada bit će razrađen u posebnom poglavlju.

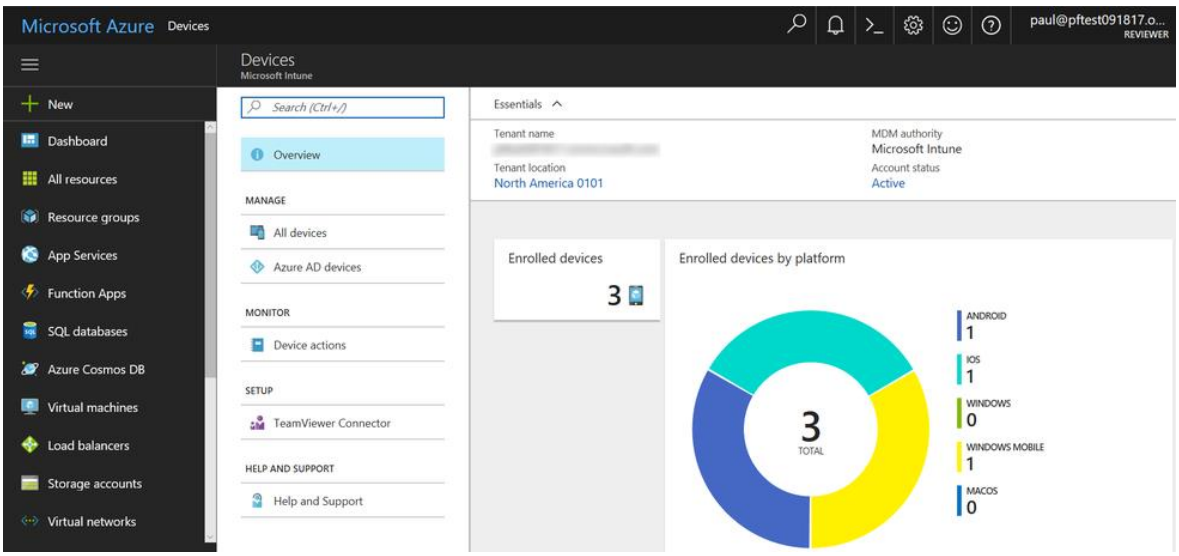
4.1 Intune

Intune Enterprise Mobility + Security je proizvod tvrtke Microsoft. On se kombinira s raznim rješenjima za sigurnost i upravljanje identitetima Microsoft Azure-a. Omogućuje definiranje strategije upravljanja mobilnim uređajima koje odgovara potrebama različitih organizacija te primjenjuje fleksibilne upravljačke programe za mobilne uređaje i aplikacije. Intune je dizajniran da podrži raznolik mobilni ekosustav, omogućujući vam da sigurno upravljate iOS, Android, Windows i MacOS uređajima iz jednog jedinstvenog mobilnog rješenja. Također pomaže u očuvanju podataka tvrtke s ili bez prijave uređaja stvaranjem pravila o zaštiti aplikacija, kao i postizanja IT učinkovitosti u oblaku tako da ne morate održavati poslužitelje na lokaciji.

Glavne značajke:

- Upravljanje mobilnim uređajima i aplikacijama

- Napredna zaštita podataka sustava Microsoft Office 365
- Integrirano upravljanje računalom
- Integrirano lokalno upravljanje
- Upravljanje identitetom i pristupom
- Zaštita podataka
- Sigurnost temeljena na identitetu



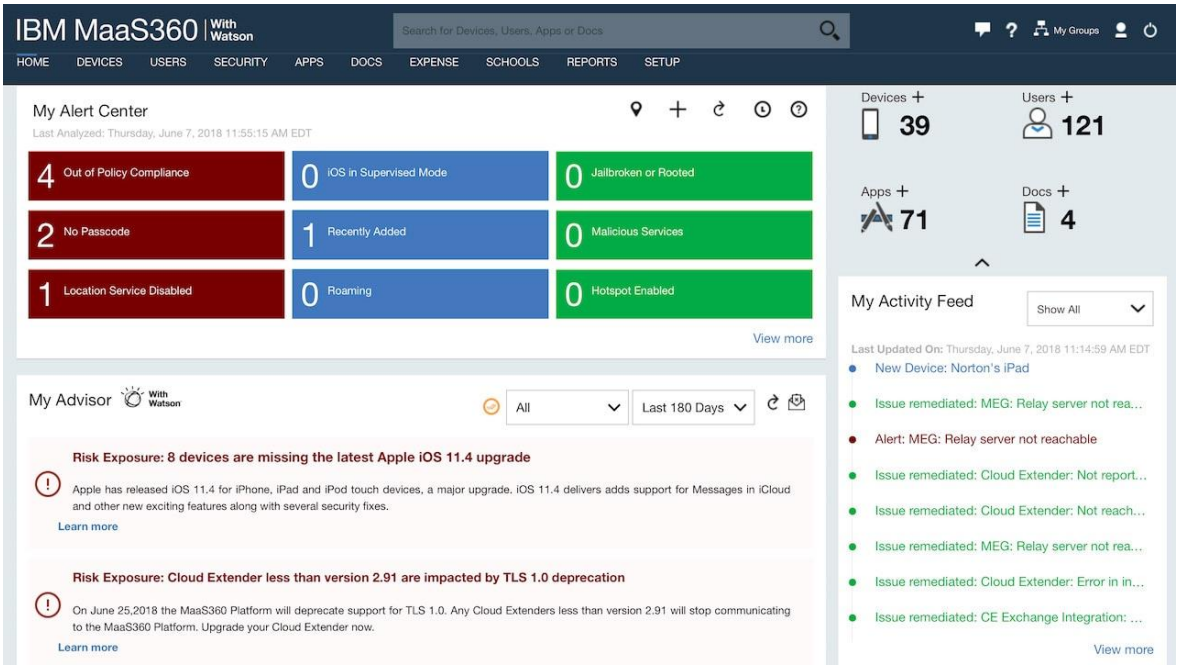
Slika 4.1 Microsoft Intune

4.2 IBM MaaS360

IBM-ov MaaS360 s Watsonom daje vidljivost i kontrolu iOS, macOS, Android i Windows uređaja putem intuitivnog portala. Posjeduje prednost prijavljivanja OTA uređaja, tako da se može brzo i jednostavno upravljati uređajima bez instaliranja hardvera. Uz MaaS360 dobije se višestruka podrška OS-a iz jedne konzole što omogućuje da sigurno i produktivno pokrijete krajnje točke bez obzira na to je li riječ o uređajima Apple, Android ili Windows OS-a. On može zaštititi uređaje izvan njihovih izvornih mogućnosti dajući krajnjim korisnicima sve što im je potrebno bez ugrožavanja sigurnosti. Podržava i IoT uređaje koji koriste API-je za upravljanje, štiteći uređaje istovremeno prikupljajući podatke.

Glavne značajke:

- Pokreće ga Watson engine
- Multi OS i sigurnost platforme
- Podržava IoT uređaje
- Pruža siguran spremnik za pohranu korporativnog sadržaja



Slika 4.2 IBM Maas360

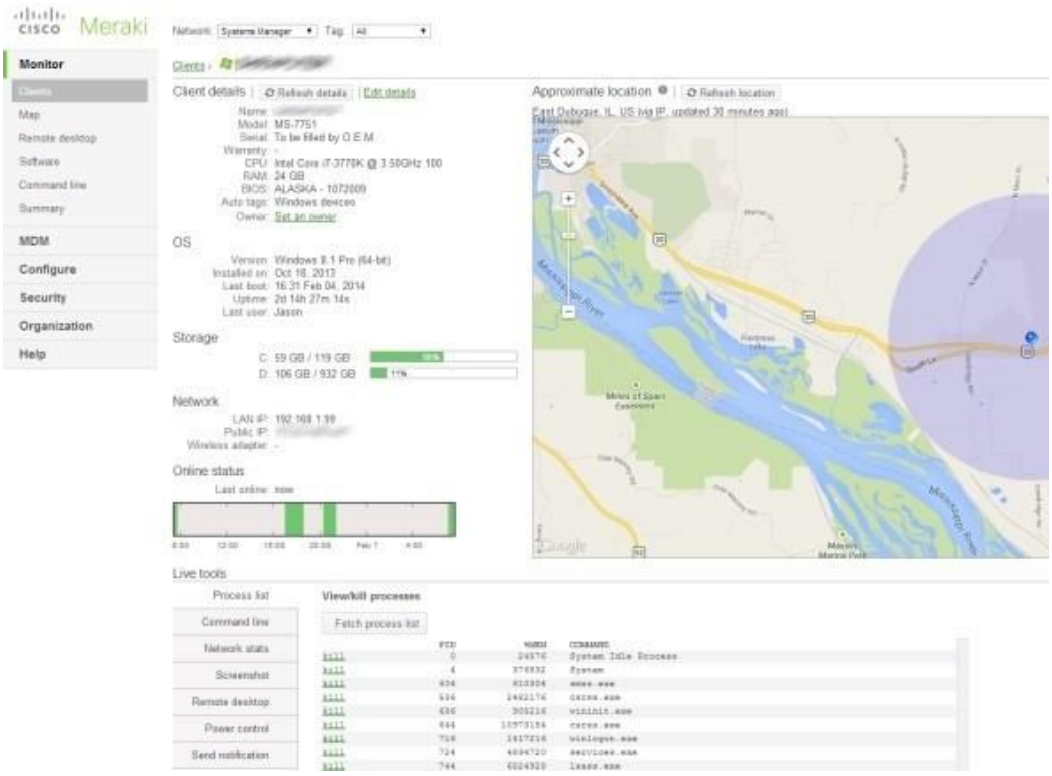
4.3 Cisco Meraki

Cisco Meraki osigurava jedinstveno upravljanje mobilnim uređajima, Macovima, računalima i cijelom mrežom s centralizirane nadzorne ploče. Daje mogućnost za provođenje pravila o sigurnosti uređaja, implementaciju softvera i aplikacija te izvođenje daljinskog otklanjanja poteškoća uživo na tisućama upravljanih uređaja. Jedinstvena platforma za upravljanje višestrukim uređajima pruža OTA centralizirano upravljanje, dijagnostiku i nadzor za mobilne uređaje kojima upravlja organizacija. Upravitelj sustava nadzire svaki uređaj organizacije, prikazujući korisne podatke kao što su hardver / softver klijenta i nedavna lokacija. Nudeći robusnu provedbu sigurnosnih pravila na svim mobilnim uređajima kojima upravlja vaša organizacija, ona je u stanju zaštititi uređaje i

njihove podatke, kontrolirati njihovu upotrebu te ograničiti pristup trgovini aplikacija, igranju i sadržaju.

Glavne značajke:

- Skalabilna konfiguracija krajnje točke
- Upravljanje sadržajem na uređaju
- Sigurna podrška za BYOD inicijative
- Automatska klasifikacija uređaja
- Automatska primjena pravila mreže prema vrsti uređaja
- Analiziranje mrežne aktivnosti pomoću automatskog izvješćivanja



Slika 4.3 Cisco Meraki

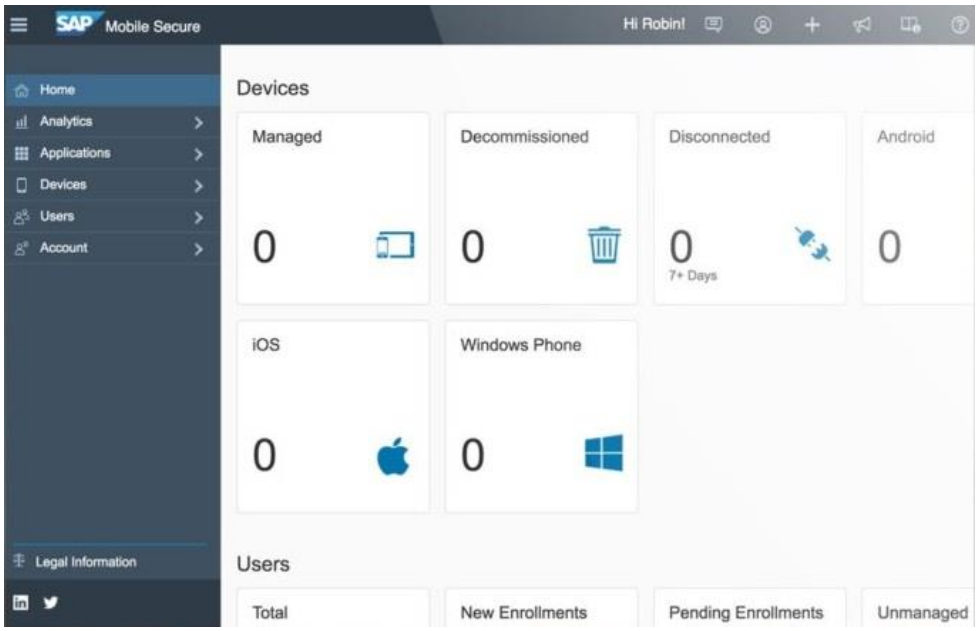
4.4 SAP Mobile Secure

SAP Mobile Secure omogućuje izlaženje iz okvira MDM-a pomoću rješenja za upravljanje mobilnošću u poduzeću (EMM) u oblaku, što vam omogućuje zaštitu i upravljanje mobilnim

uređajima i aplikacijama tvrtke. EMM platforma temeljena na oblaku nudi integrirane alate za MDM, BYOD sigurnost, upravljanje mobilnim aplikacijama (MAM), itd. Može se upravljati sigurnošću mobilnih uređaja s jedne SaaS platforme pa čak i postaviti vlastitu poslovnu trgovinu aplikacijama. Pomoću SAP Mobile Secure-a osiguravate mobilne uređaje i aplikacije svoje organizacije bez ugrožavanja korisničkog iskustva. Mogu se uspostaviti detaljna sigurnosna pravila za uređaje i na razini aplikacija; minimizirajući BYOD sigurnosne rizike i štiteći podatke tvrtke te također konfigurirati mobilne aplikacije, koristiti uslugu otkrivanja aplikacija i riješiti sve moguće sigurnosne praznine.

Glavne značajke:

- Jednostavno samoposluživanje
- Trgovina aplikacija tvrtke
- Pojednostavljena implementacija i prilagodba aplikacija
- Mobilno korisničko iskustvo bez komplikacija. [7]



Slika 4.4 SAP Mobile Secure

5. MobileIron

MobileIron je tvrtka koja nudi softver za upravljanje i sigurnost mobilnih uređaja (aplikacije). Navedeni cilj tvrtke MobileIron je učiniti mobilne uređaje, operativne sustave i aplikacije primarnim računalnim platformama za sve organizacije - što je poznato kao pristup koji se temelji na mobilnosti.[8] MobileIron stvara sigurnosni kontejner na uređaju koji sprječava miješanje poslovnih podataka s privatnim podacima. Privatni podaci ostaju privatni jer MDM rješenje ne može vidjeti vašu povijest poziva, SMS komunikaciju, fotografije, videozapise, osobne račune e-pošte, lokaciju uređaja, aktivnosti preglednika weba itd. Proizvodi tvrtke MobileIron dostupni su i kao lokalni softver i kao usluga u oblaku. Ponude MobileIron-a uključuju:

- MobileIron platforma: MobileIron-ov EMM softver osigurava MDM, upravljanje mobilnim aplikacijama i mogućnosti upravljanja mobilnim sadržajem.
- Pristup za MobileIron: Ovaj proizvod omogućuje organizacijama da osiguraju i kontroliraju pristup aplikacijama u oblaku na mobilnim uređajima.
- MobileIron Bridge: Ova značajka ima za cilj ujediniti mobilni uređaj i Windows 10 PC upravljanje, pristup poznat kao jedinstveno upravljanje krajnjim točkama.
- Aplikacije: MobileIron nudi dug popis aplikacija koje organizacije mogu implementirati korisnicima kako bi omogućile pristup odobrenim uslugama i sadržaju tvrtke. [8]

MobileIron omogućuje daljinsko upravljanje uređajima - od životnog ciklusa uređaja i implementacije politike do nadzora i povlačenja - sve bez ugrožavanja sigurnosti. To rasterećuje IT odjel dopuštajući korisnicima da se sami povežu sa sustavom putem samouslužnog portala. Kada se jednom poveže, IT može provoditi sigurnosne postavke na uređajima kako bi spriječio provalu i druge aktivnosti koje nisu u skladu sa sigurnosnim politikama organizacije omogućavajući zaposlenicima fleksibilnost i slobodu izbora. Svaki mobilni uređaj s pristupom podacima tvrtke bit će podložan sigurnosnim pravilima.

Sigurnosna politika definira različite sigurnosne zahtjeve koji se primjenjuju na uređaj, kao što su:

- zaključavanje zaslona (jedan za uređaj, odvojeno za radno područje tvrtke)
- enkripcija mobilnih uređaja (gdje je podržano)
- dopuštene aplikacije samo iz službenih trgovina aplikacija

S MobileIron-om, mobilni uređaji imat će sljedeće aplikacije instalirane na svom uređaju:

- E-mail + - siguran klijent za primanje / slanje e-mailova tvrtke.

- Web @ Work - siguran web preglednik (s bookmarsima na neke interne web stranice)

- Docs @ Work - sigurno skladište dokumenata (prilozi iz mailova)

MobileIron prodaje svoj EMM proizvod u tri paketa - gold, silver i platinum - koji nude različite značajke. Organizacije mogu kupiti licence za te pakete na temelju uređaja ili korisnika.

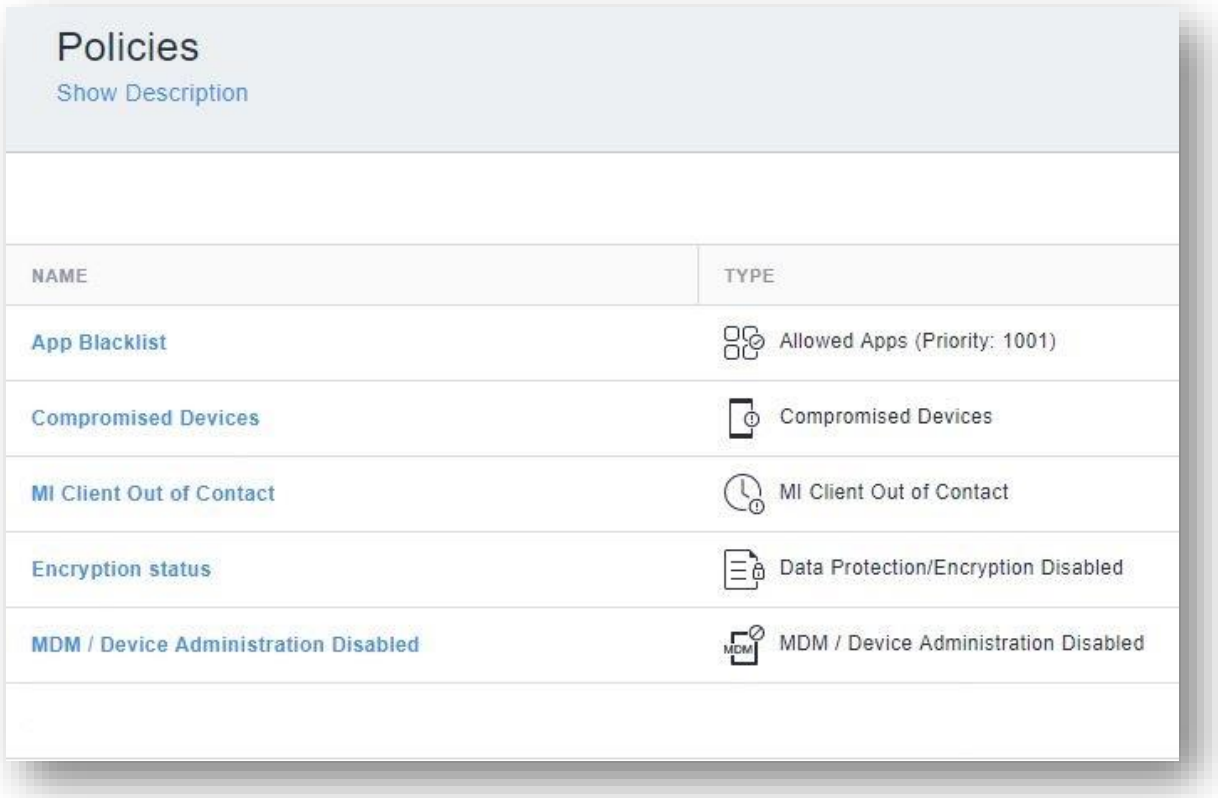
6. Implementacija MobileIrona u radno okruženje

U praktičnom dijelu pokazati ću implementaciju MobileIrona, odnosno, složit ću konfiguracije, sigurnosne politike, kontejnere s aplikacijama, te ću pokazati samu administraciju sustava za mobilne uređaje. Pokazat ću i opisati kako izgleda komunikacija između mobilnog uređaja i sustava (koji je u cloudu), odnosno, što se događa kada mobilni uređaj pristupa poslovnim resursima kroz MobileIron. Testirat će se funkcionalnost instaliranih aplikacija te će se usporediti s nekim drugim MDM rješenjem, Praktični rad je testiran u radnom okruženju, u organizaciji u kojoj radim te je imala preko 400 testnih korisnika.

6.1 Sigurnosne politike

Politike definiraju sigurnosne kriterije za odlučivanje kada uređaji nisu u skladu s istima i radnje koje treba poduzeti za kršenje uređaja. Uređaji koji krše pravila bit će označeni kao neskladni, a protiv uređaja će se poduzeti radnje povezane s pravilima.

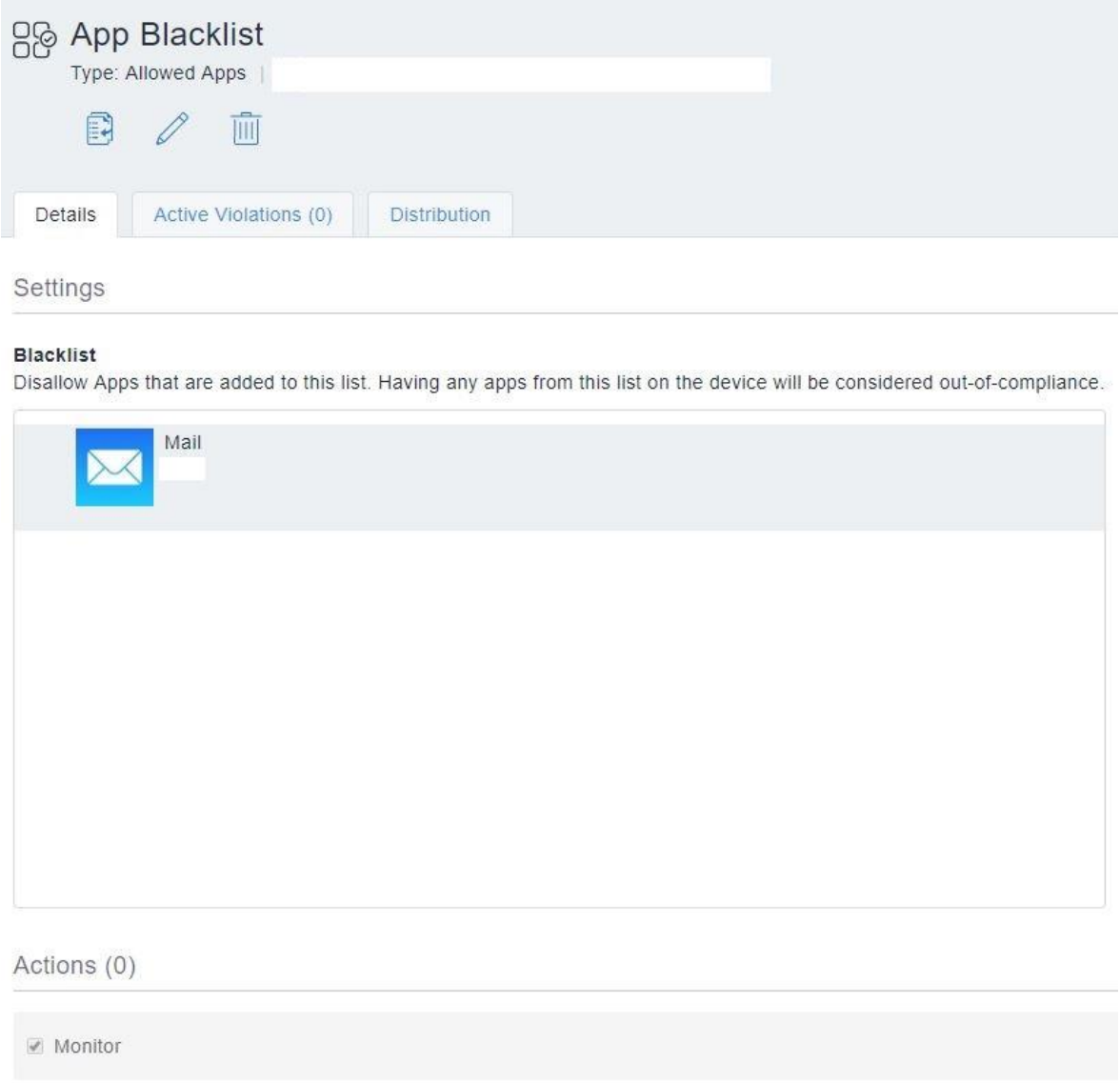
Postoji nekoliko sigurnosnih politika koje su definirane i distribuirane na sve korporativne uređaje, a to su: blacklistane aplikacije, kompromitirani uređaji, klijenti koji su izvan dosega, status enkripcije te onemogućena administracija.



Slika 6.1 Politike

6.1.1 App Blacklist

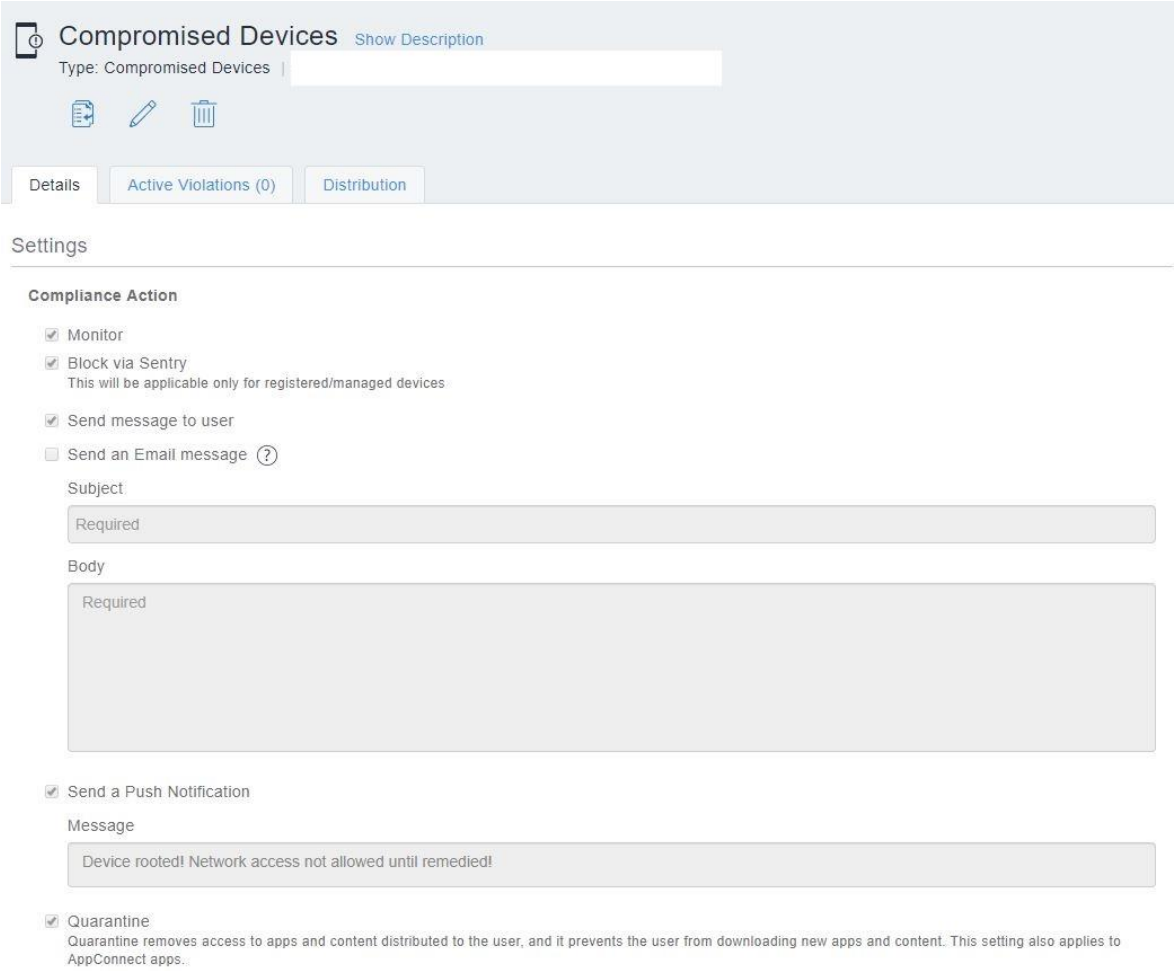
Onemogućuje aplikacije koje su dodane na ovaj popis. Ako se bilo koje aplikacije s ovog popisa nađu na uređaju smatraju se neskladnim, odnosno, ukoliko se poslovnim resursima pokušava pristupiti preko ugrađene “Mail“ aplikacije, a ne preko sigurnosnih aplikacija MobileIrona. Ovdje bi svakako trebalo blacklistati ugrađene mail aplikacije kako bismo primorali korisnike da koriste MDM rješenje za čitanje i slanje mailova.



Slika 6.2 Blacklistane aplikacije

6.1.2 Compromised devices

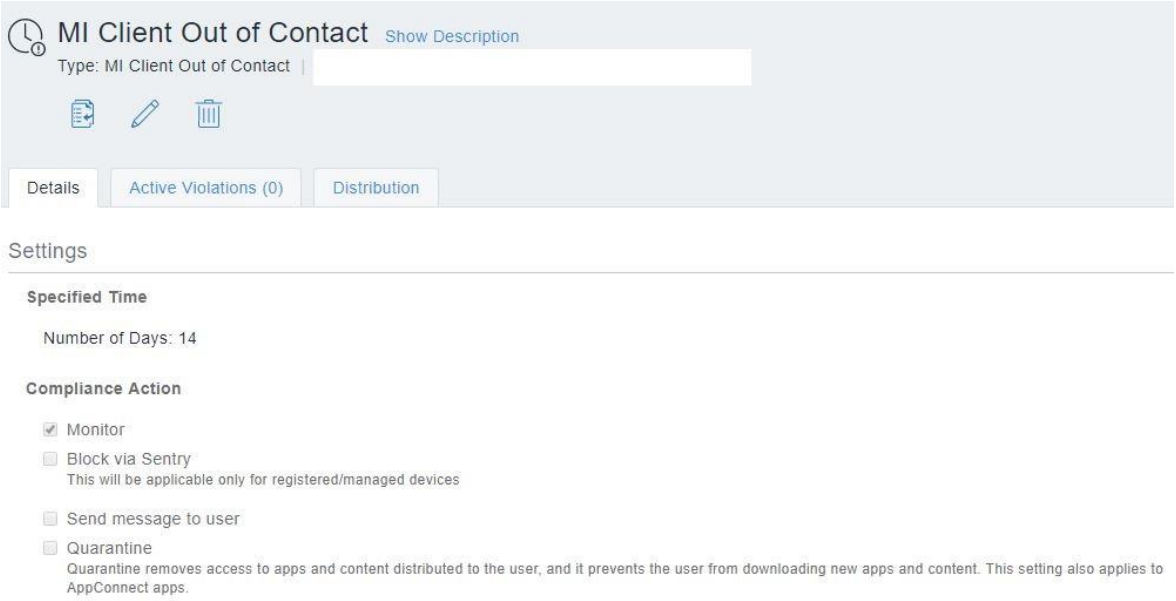
Ova sigurnosna politika provjerava je li uređaj "root-an" ili "jailbroke-an". Ukoliko provjera pokaže da je neki uređaj ugrožen, istog trenutka mu se blokira pristup do MobileIron Sentry-a te korisnik dobije notifikaciju da je uređaj ugrožen te ga stavlja u karantenu (korisnik, odnosno, uređaj ne može pristupiti MobileIron aplikacijama niti ih ponovno skinuti). Preporuka je nadgledati uređaje te ih blokirati ukoliko se primijeti da je uređaj na neki način kompromitiran.



Slika 6.3 Kompromitirani uređaji

6.1.3 MI Client Out of Contact

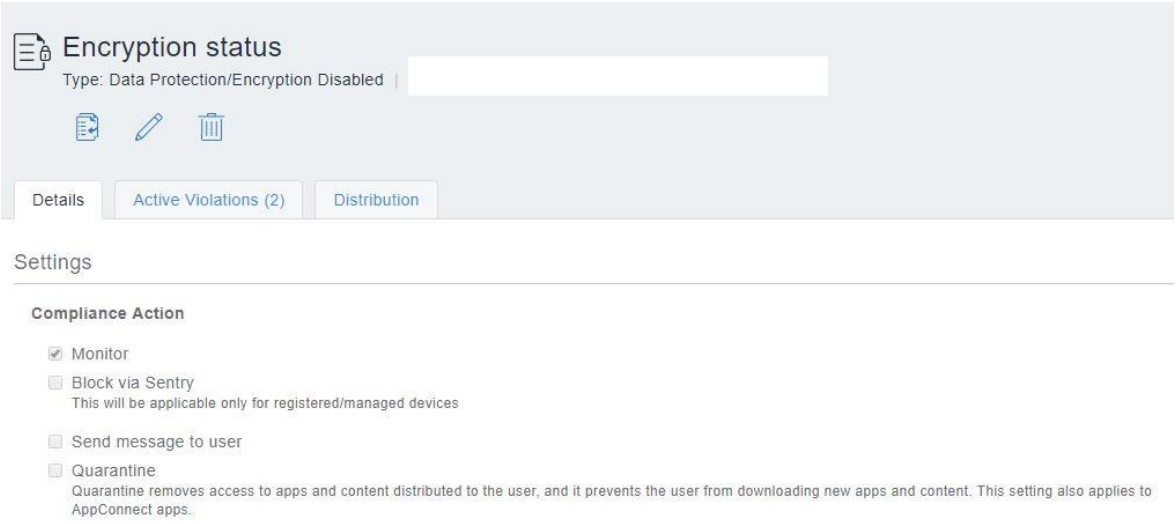
Provjerava se postoje li klijenti koji ne komuniciraju s centralnom konzolom, odnosno sa sentry-em 14 ili više dana. Ovdje se ne poduzimaju nikakve posebne akcije (jer npr. korisnik može biti na godišnjem odmoru) osim samog nadgledanja, ukoliko posumnjamo na nešto uvijek možemo blokirati pristup sentry-u za taj uređaj ili poslati poruku useru da provjeri zašto nema valjane komunikacije. Ovdje ne trebamo poduzimati nikakve drastične mjere pošto korisnik može biti na godišnjem odmoru, bolovanju i sl. Stoga je preporuka uključiti samo nadgledanje pa onda intervenirati prema potrebi.



Slika 6.4 Klijenti koji su izvan dosega

6.1.4 Data protection/Encryption disabled

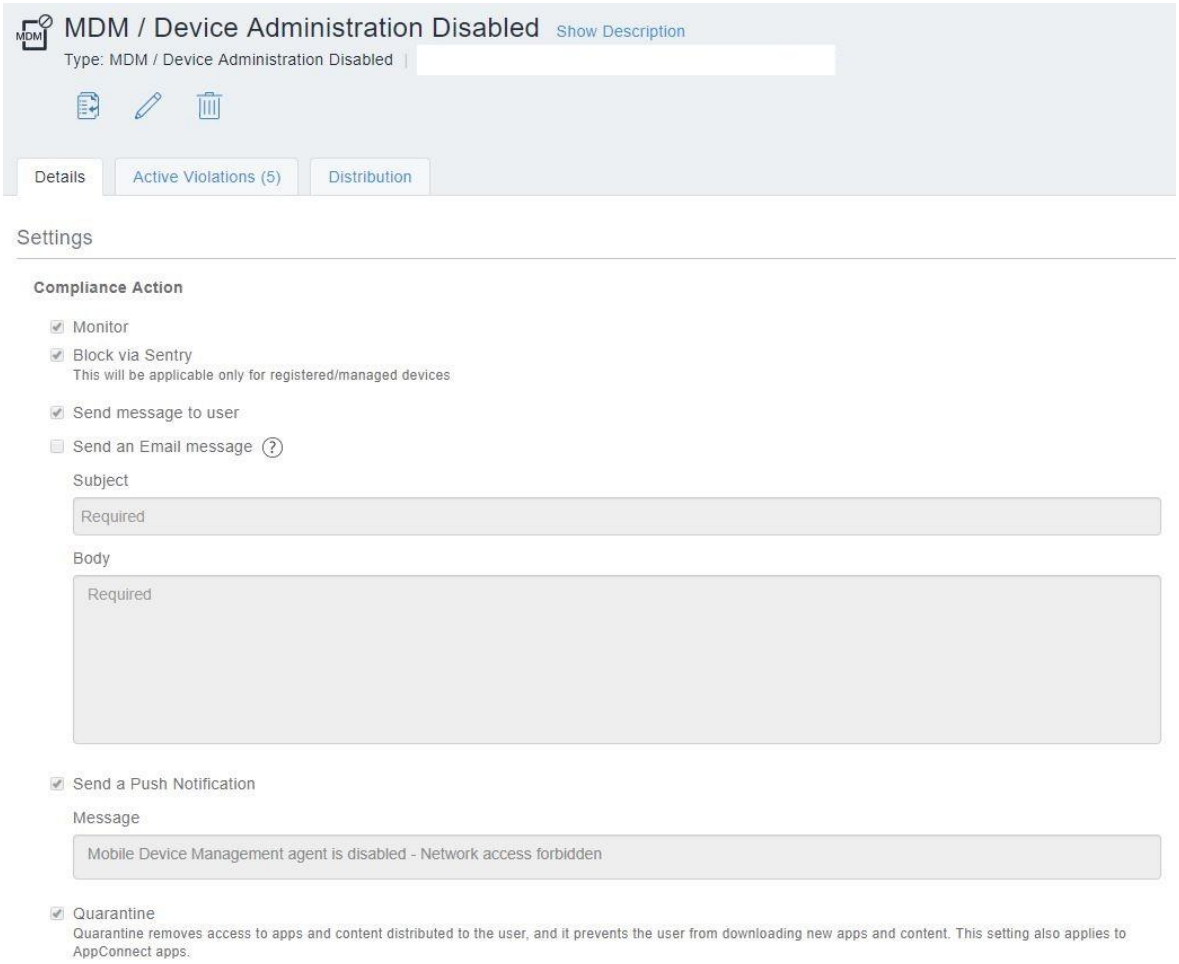
Provjerava se je li enkripcija uređaja omogućena, odnosno, napravljena. To znači da će za dešifriranje uređaja svaki put kada uključite telefon trebati ili numerički pin ili lozinka. Jedini način za ulazak u telefon je kodiranje šifriranim ključem što znači da će podaci biti sigurni, ukoliko dođe do gubitka uređaja što je svakako krucijalno za firmu – da podaci budu zaštićeni. Ovdje se ne poduzimaju nikakve posebne akcije osim samog nadgledanja, ukoliko vidimo da uređaj nije enkriptiran možemo kontaktirati korisnika da napravi enkripciju ili u krajnjem slučaju blokirati mu pristup aplikacijama dok ne napravi enkripciju. Ovo je vrlo bitna stavka jer uređaj mora biti zaštićen od neovlaštenog pristupa stoga je potrebno nadgledati uređaje koji potencijalno mogu predstavljati sigurnosni problem.



Slika 6.5 Status enkripcije

6.1.5 MDM / Device Adiministration Disabled

Provjeravaju se uređaji koji nemaju uključenu MDM/Device administraciju što znači da se s njima ne može upravljati iz centralne konzole (ne dobivaju konfiguracije, nove politike, aplikacije, itd.). Ovo je jedna od ključnih politika stoga su ovdje akcije stroge. Takvim uređajima se blokira komunikacija sa Sentry-em, šalje mu se poruka i notifikacija da je MDM agent onemogućen te se uređaj stavlja u karantenu dok se administracija ne omogući. Preporuka je postaviti što strože politike jer je upravo ovo ključna politika – ukoliko je administracija onemogućena uređaj nije niti vidljiv u centralnoj konzoli.



Slika 6.6 Onemogućena administracija

6.2. Konfiguracije

Konfiguracije su kolekcije postavki koje se šalju na mobilne uređaje. U ovom radu će se proći kroz konfiguracije koje su nužne da bi uređaji dobili potrebne aplikacije MobileIrona za pristup poslovnim resursima koji naravno za pristup iziskuju nekakvu metodu autentikacije.

6.2.1 Katalog aplikacija

Katalog aplikacija sadrži aplikacije MobileIrona koje će se instalirati na uređaj, o njima ću detaljnije u sljedećem poglavlju. Ova konfiguracija omogućava pristup vlastitom, modificiranom katalogu aplikacija u koji možemo staviti aplikacije koje god želimo. Bitno je omogućiti aplikaciju na uređajima i onemogućiti brisanje kataloga jer onda korisnici neće biti u mogućnosti instalirati iste.

```
cloneable: false
cloneableAcrossSpace: false
clonedFromDefaultSpace: false
configurationMutable: false
deletable: false
description: Access the App Catalog on mobile devices.
distributionChannelType: null
distributionMutable: false
dmPartitionDistributionType: ALL
dmPartitionId: 31864
enabled: true
modifiedAt: !!timestamp '26-06-19 19:40:23:148 +0000'
modifiedBy: Hrvoje Lovric - Admin
name: App Catalog for mobile devices
policyId: 253892
policyType: APPCATALOG
policyVariables: null
priority: null
priorityMutable: false
replaceConfigurationId: null
systemName: AppCatalog
uuid: 8938760a-cbeb-4300-961f-860d515abb7a
```

Kod 1 Konfiguracija kataloga aplikacija

6.2.2 Pristup aplikacijama iz kataloga

U ovoj konfiguraciji postavljamo lozinku odnosno metodu autentikacije korisnika za pristup aplikacijama iz kataloga aplikacija. U kodu možemo vidjeti da se omogućuje čak i biometrijska metoda – otisak prsta, naravno, ukoliko sam uređaj ima mogućnost skeniranja otiska prsta. Maksimalan broj pokušaja za ulazak je 10, a minimalna dužina je četiri znamenke. Naravno, ovo se može modificirati po željama i sigurnosnim pravilima firme. Preporuka je svakako forsirati neku metodu autentikacije za pristup te nakon određenog broja neuspješnih pokušaja blokirati pristup aplikacijama kako bi i na taj način bili zaštićeni od neovlaštenog pristupa.

```
allowSimple: true
changeAtNextAuth: false
cloneable: true
cloneableAcrossSpace: true
clonedFromDefaultSpace: false
configurationMutable: true
deletable: true
description: null
distributionChannelType: null
distributionMutable: true
dmPartitionDistributionType: NONE
dmPartitionId: 31864
enableAnyLockMethod: true
enableFingerprint: true
enableLockScreenNotificationsForWorkManagedDevice: true
enableSmartlock: true
enableUnredactedLockScreenNotificationsForWorkProfile: true
enabled: true
forcePIN: true
maxFailedAttempts: 10
maxGracePeriod: 5
maxInactivity: 5
maxPINAgeInDays: 180
minComplexChars: null
minLength: 4
modifiedAt: !!timestamp '87-07-19 16:44:32:678 +0000'
modifiedBy: Hrvoje Lovric - Admin
name: Common Password-PIN configuration
pinHistory: 5
policyId: 260533
policyType: PASSCODE
policyVariables: null
priority: 1002
priorityMutable: true
replaceConfigurationId: null
requireAlphanumeric: false
systemName: null
```

```
uuid: f464ad9b-938b-40e9-b08c-db99003192c4
```

Kod 2 Konfiguracija pristupa katalogu

6.2.3 Autorizacija i prevencija od gubitka podataka

U sljedećoj konfiguraciji možemo vidjeti da se nakon 3600 sekundi (neaktivnosti) korisnika odjavljuje iz svih aplikacija unutar MobileIrona te će se morati ponovno autenticirati kako bi pristupio podacima. Nadalje, možemo vidjeti da se unutar MobileIron aplikacija ne može koristiti privatna galerija slika, kamera, pristup web stranicama kao niti uzimanje screenshot-ova. Sve to, kako bi se maksimalizirala sigurnost i prevencija od gubitka/curenja podataka. Preporuka je zabraniti bilo kakve aktivnosti unutar samih aplikacija – screenshotove, snimanje, slikanje, itd. Isto tako ključna je stavka da se nakon određenog vremena korisnik automatski odjavi iz aplikacija.

```
appAuthorizationSettings:
    checkinIntervalSeconds: 3600
    configVariables: null
    id: 0
    outOfTouchRetireMinutes: 0
    uuid: null
    wipeAppOnCompromisedDevice: null
    wipeAppOnUSBDebugMode: null
cloneable: true
cloneableAcrossSpace: false
clonedFromDefaultSpace: false
configurationMutable: true
dataLossPreventionSettings:
    allowCamera: false
    allowGallery: false
    allowMediaPlayer: false
    allowOpenIn: null
    allowPrinting: null
    allowScreenCapture: false
    allowUnsecureWebUrlsInsideContainer: false
    allowWebUrlsOutsideContainer: false
    clipboardPolicy: ALLOW_ALL
    configVariables: null
    documentInteractionPolicy: null
    id: 0
    uuid: null
modifiedAt: !!timestamp '24-07-19 11:10:17:665 +0000'
modifiedBy: Hrvoje Lovric - Admin
```

Kod 3 Konfiguracija za prevenciju od gubitka podataka

6.2.4 Sigurnosne konfiguracije

Što se tiče konfiguracija samog uređaja koji je dan korisniku od firme na korištenje možemo vidjeti da se ništa drastično nije dogodilo. Zabranjen je tek bluetooth tethering i instalacija aplikacija s nepoznatih izvora (.apk paketi koji se importaju na mobilni uređaj ili se direktno skidaju na mobitel). Dozvoljena je instalacija svih aplikacija koje se nalaze na provjerenim trgovinama (Google Play, App store, itd.) te naravno instalacija iz kataloga aplikacija koje smo sami kreirali. Ključna stvar kod ove konfiguracije je zabraniti instalaciju aplikacija s nepoznatih izvora pogotovo ukoliko se aplikacije skidaju s neprovjerenih web stranica i importaju na uređaj.

```
---
cloneable: true
cloneableAcrossSpace: false
clonedFromDefaultSpace: false
configurationMutable: true
deletable: true
description: null
disableAdminPrivilegesRemoval: false
disableBluetooth: false
disableBluetoothExceptAudio: false
disableBluetoothTethering: true
disableCamera: false
disableCopyPaste: false
disableDataRoaming: false
disableFactoryReset: false
disableGps: false
disableMicrophone: false
disableMobileData: false
disableNFC: false
disableNativeBrowser: false
disableOTAUpgrade: false
disablePhoneDialer: false
disableSDCard: false
disableScreenCapture: false
disableSettingsChange: false
disableUSBMassStorage: false
disableUSBMediaPlayer: false
disableUSBTethering: false
disableUnknownSources: true
disableVoiceRoaming: false
disableWifi: false
disableWifiTethering: false
disableYouTube: false
distributionChannelType: null
distributionMutable: true
dmPartitionDistributionType: NONE
dmPartitionId: 31864
```

```
enabled: true
kioskConfiguration:
    allowUserToSelectLanguage: true
    allowedAppDetailList:
    -   bundleIdentifier: com.mobileiron.kiosk.settings
        forceReinstall: false
        hideLauncherIcon: false
    disableQuickSettings: true
    enableLockTaskMode: true
    enabled: false
    enterKioskAutomatically: false
    exitPinCode: null
    kioskSharedDeviceConfiguration: null
    locationSetting: ENABLED
    userControllableBluetooth: false
    userControllableBrightnessAndAutoRotate: false
    userControllableDateTime: false
    userControllableDelayedAppUpdates: false
    userControllableLocationSettings: false
    userControllableMobileNetworks: false
    userControllableWifi: false
modifiedAt: !!timestamp '07-07-19 16:32:34:135 +0000'
modifiedBy: Hrvoje Lovric - Admin
```

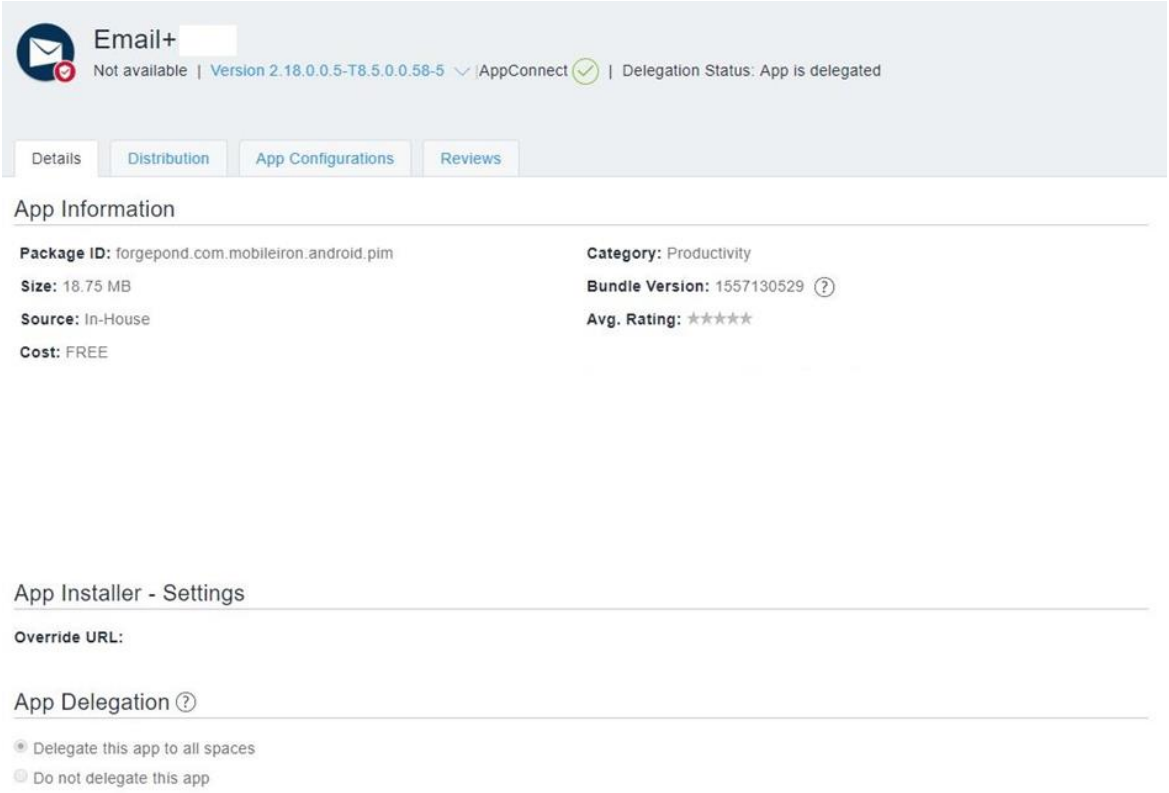
Kod 4 Konfiguracije sigurnosnih postavki

6.3 Aplikacije i njihove konfiguracije

Aplikacije MobileIron-a služe za pristup poslovnim resursima – pošti, dokumentima i internim web stranicama. Stavljaju se u već spomenuti katalog aplikacija koji smo sami kreirali kako bi ih korisnici instalirali na svoje mobilne uređaje. Funkcionalnosti aplikacija bit će pokazane u posebnom poglavlju gdje će se demonstrirati rad svake od aplikacija.

6.3.1 Email+

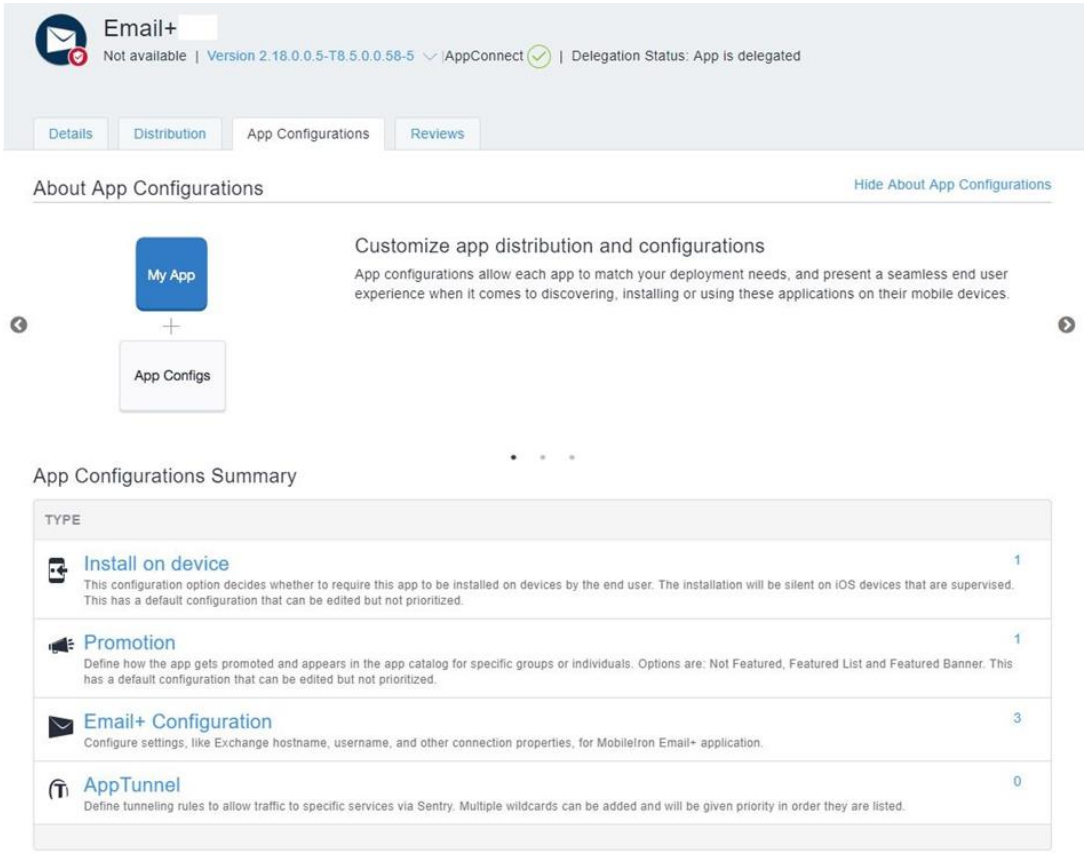
Aplikacija za čitanje i slanje mailova unutar i izvan poslovne organizacije. Možemo vidjeti veličinu aplikacije, verziju i ostale informacije vezane uz samu aplikaciju (Slika 7).



Slika 6.7 Detalji Email+ aplikacije

Što se tiče distribucije nju možemo preskočiti jer je ista za sve aplikacije – primijenjena je na sve uređaje firme. Konfiguracija aplikacije je malo složenija, postoji nekoliko stvari koje se mogu (trebaju) konfigurirati:

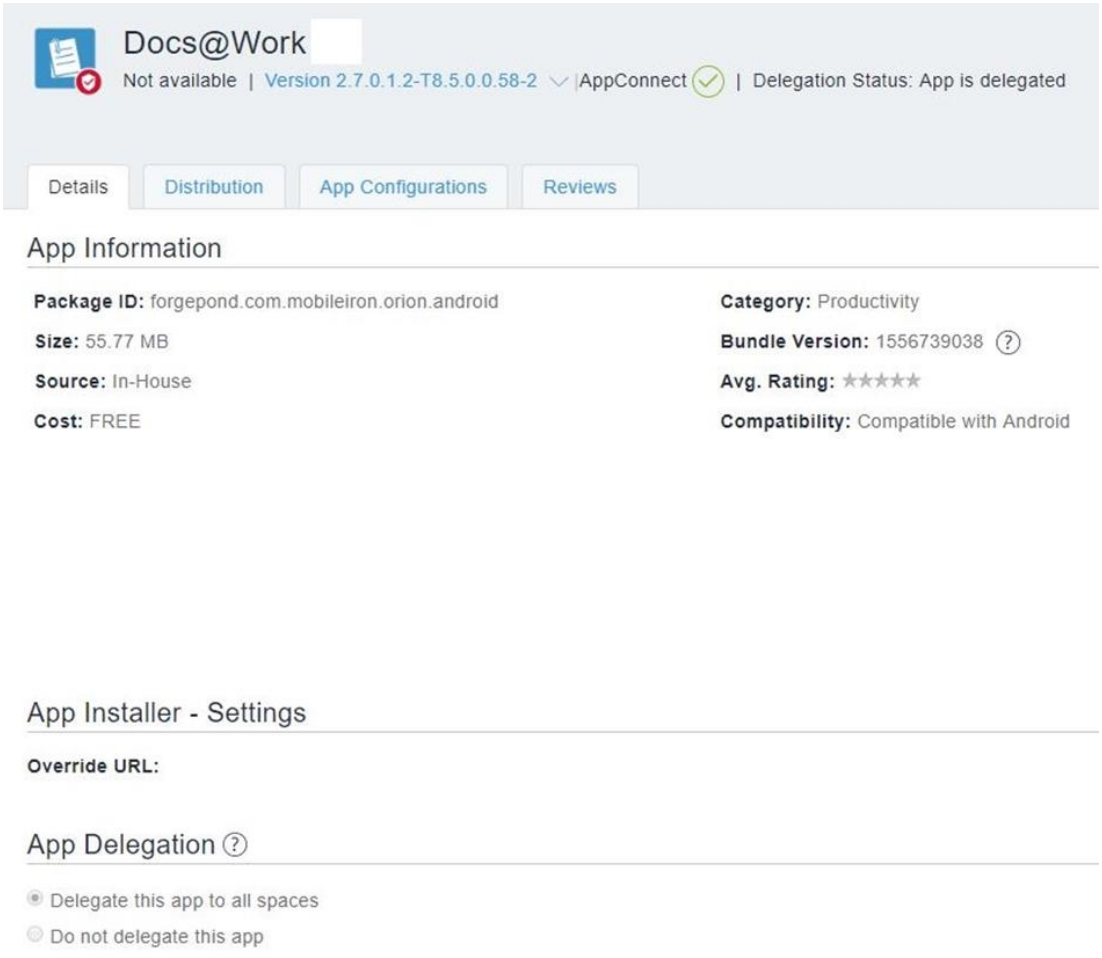
- “Install on device“ - ova opcija konfiguracije odlučuje da li će ovu aplikaciju krajnji korisnik moći instalirati na svoj mobilni uređaj. Ovo je zadana konfiguraciju koja se može uređivati. Preporuka je uključiti ovu opciju globalno za sve uređaje kako kasnije ne bi imali problema.
- “Promotion“- određuje kako se aplikacija promovira i prikazuje li se u katalogu aplikacija za određene grupe ili pojedince. Također ima zadanu konfiguraciju koja se može uređivati.
- „Email+ configuration“ – ovdje se konfiguriraju postavke kao što su Exchange, korisničko ime i ostali potrebni podaci koji su potrebni kako bi se pristupilo mailu firme. Ovo je ključna stavka te ju je nužno konfigurirati kako bi aplikacija imala komunikaciju prema Exchange serveru.
- “App Tunnel“ – definiraju se pravila tuneliranja kako bismo omogućili promet do određenih usluga putem Sentryja. Ovdje, kod Email+ aplikacije to se neće koristiti.



Slika 6.8 Konfiguracija Email+ aplikacije

6.3.2 Docs@Work

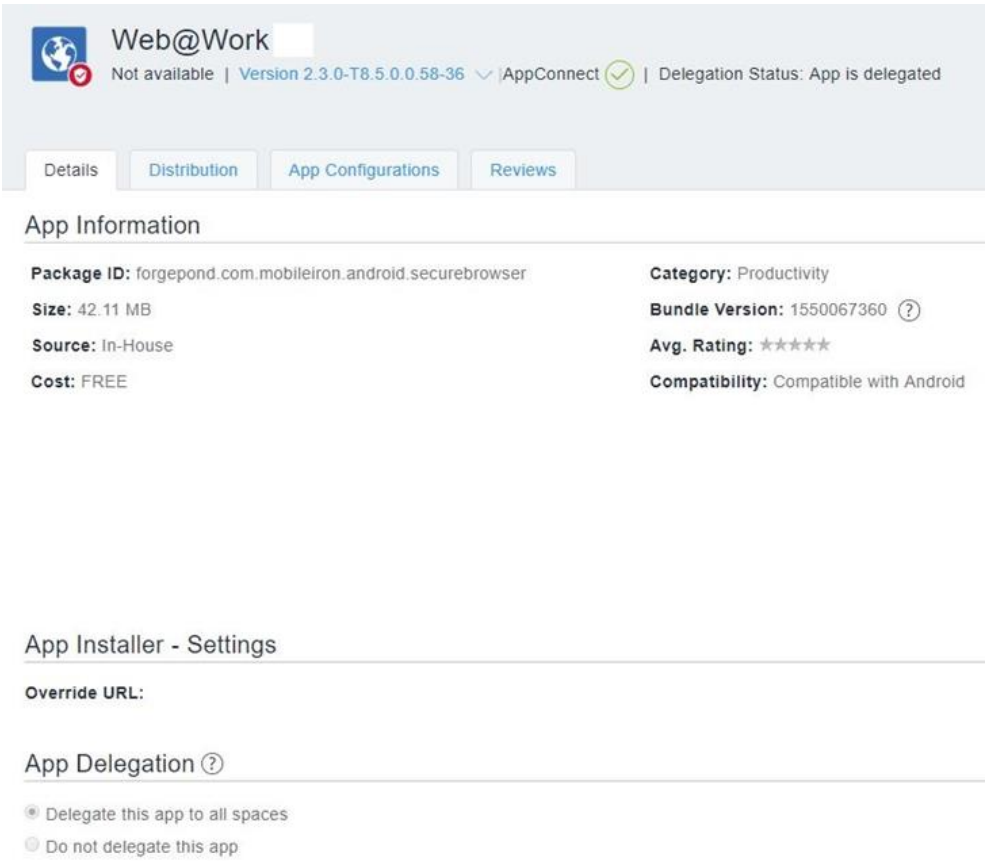
Ova aplikacija služi za pregledavanje (slanje) dokumenata svih formata koje smo prethodno skinuli preko aplikacije Email+. Svi prilozi koje želimo spremiti iz naših mailova (preko Email+ aplikacije) spremaju se u ovu aplikaciju koje onda možemo slati dalje. Prilozi se ne spremaju u internu memoriju telefona kao svi ostali dokumenti koje skidamo (obično idu u mapu "Preuzimanja") nego u odvojeni kontejner zvan "Docs@Work". Bitno je naglasiti da se dokumenti mogu dijeliti iz kontejnera samo preko Email+ aplikacije, ukoliko se pokuša podijeliti preko nekih drugih aplikacija, dobit će se poruka da je to zabranjeno te upravo je ovo najvažnije kod ove aplikacije. Preporuka je preusmjeriti, odnosno, forsirati spremanje datoteka iz Email+ aplikacije isključivo u Docs@Work aplikaciju.



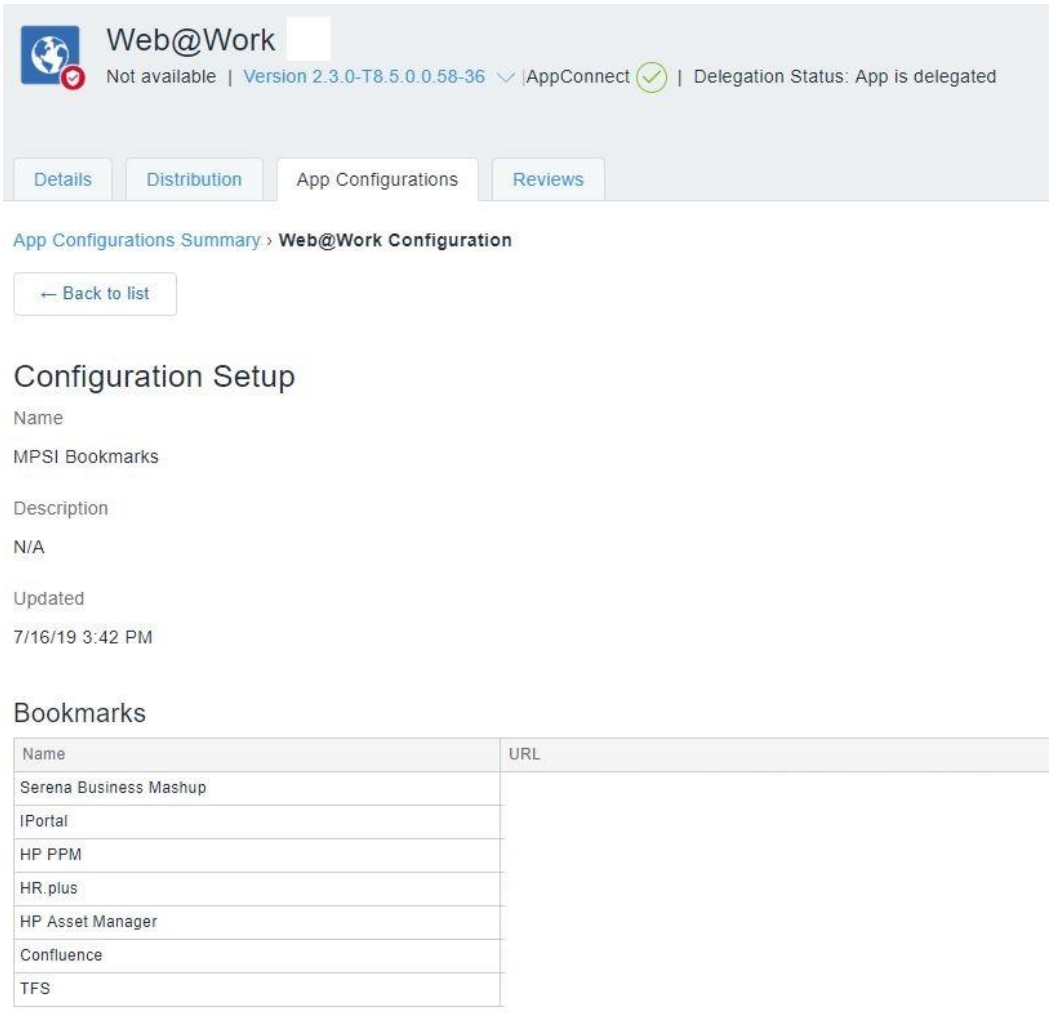
Slika 6.9 Detalji Docs@Work aplikacije

6.3.3 Web@Work

Aplikacija preko koje se pristupa internim web stranicama firme, npr. stranica s aktualnim događanjima, stranica za upis radnih sati, pregled plaća, itd. Postoje nekoliko razlika u konfiguraciji u odnosu na prethodne dvije aplikacije. Dodane su oznake za interne web stranice na koje se onda jednostavnim klikom pristupi bez potrebe da se upisuje cijeli URL. Nadalje, konfiguriran je tzv. "App Tunnel" odnosno, postavljeno je da se pristupa stranicama preko firminog internog web proxya. Kod ove aplikacije može biti vrlo korisno ukoliko dodamo oznake koje će pojednostaviti korisnicima pristupanje internim web stranicama (umjesto da pišu cijeli URL).



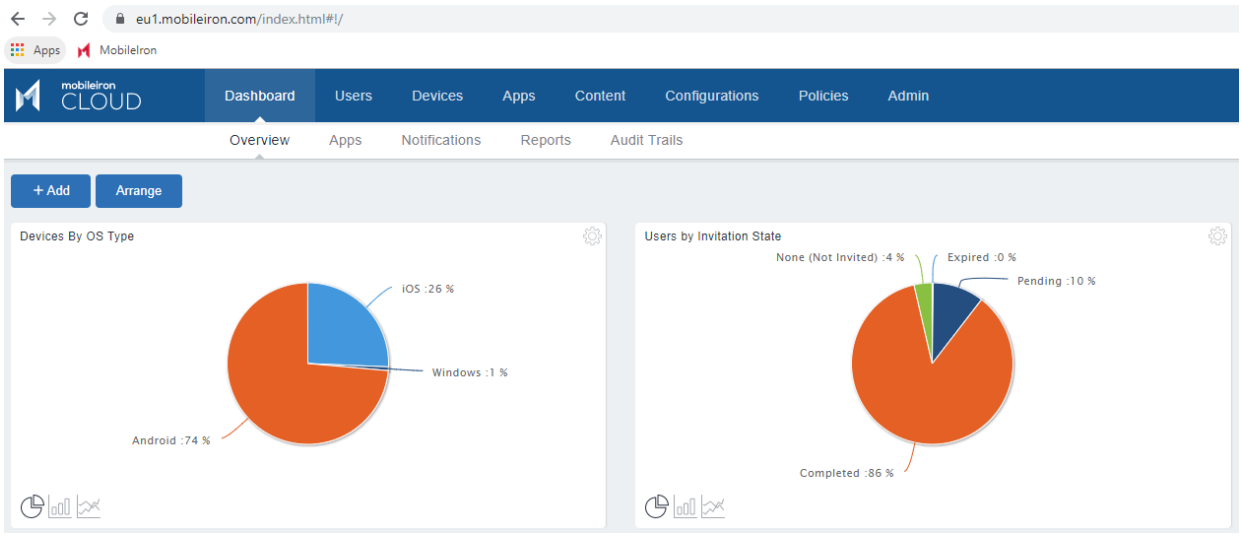
Slika 6.10 Detalji Web@Work aplikacije



Slika 6.11 Oznake u Web@Work aplikaciji

6.4 Administracija korisnika/uređaja

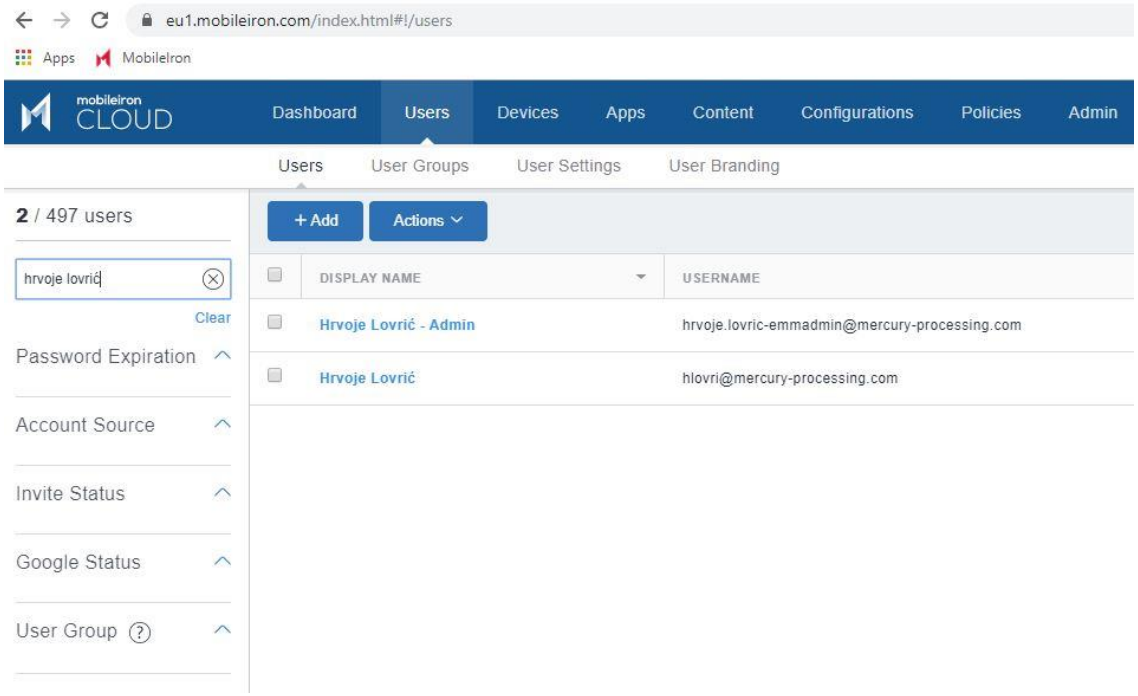
Administracija korisnika/uređaja radi se preko MobileIron administracijskog portala https://eu1.mobileiron.com/. Na početnoj stranici možemo vidjeti dva dijagrama koji pokazuju zastupljenost uređaja po operacijskom sustavu te stanje korisnika u firmi. Naravno, dijagrami se mogu dodavati/modificirati po želji. Aplikacije, konfiguracije i sigurnosne politike su objašnjene u prethodnim poglavljima pa ću se ovdje fokusirati isključivo na korisnike i uređaje te administraciju istih.



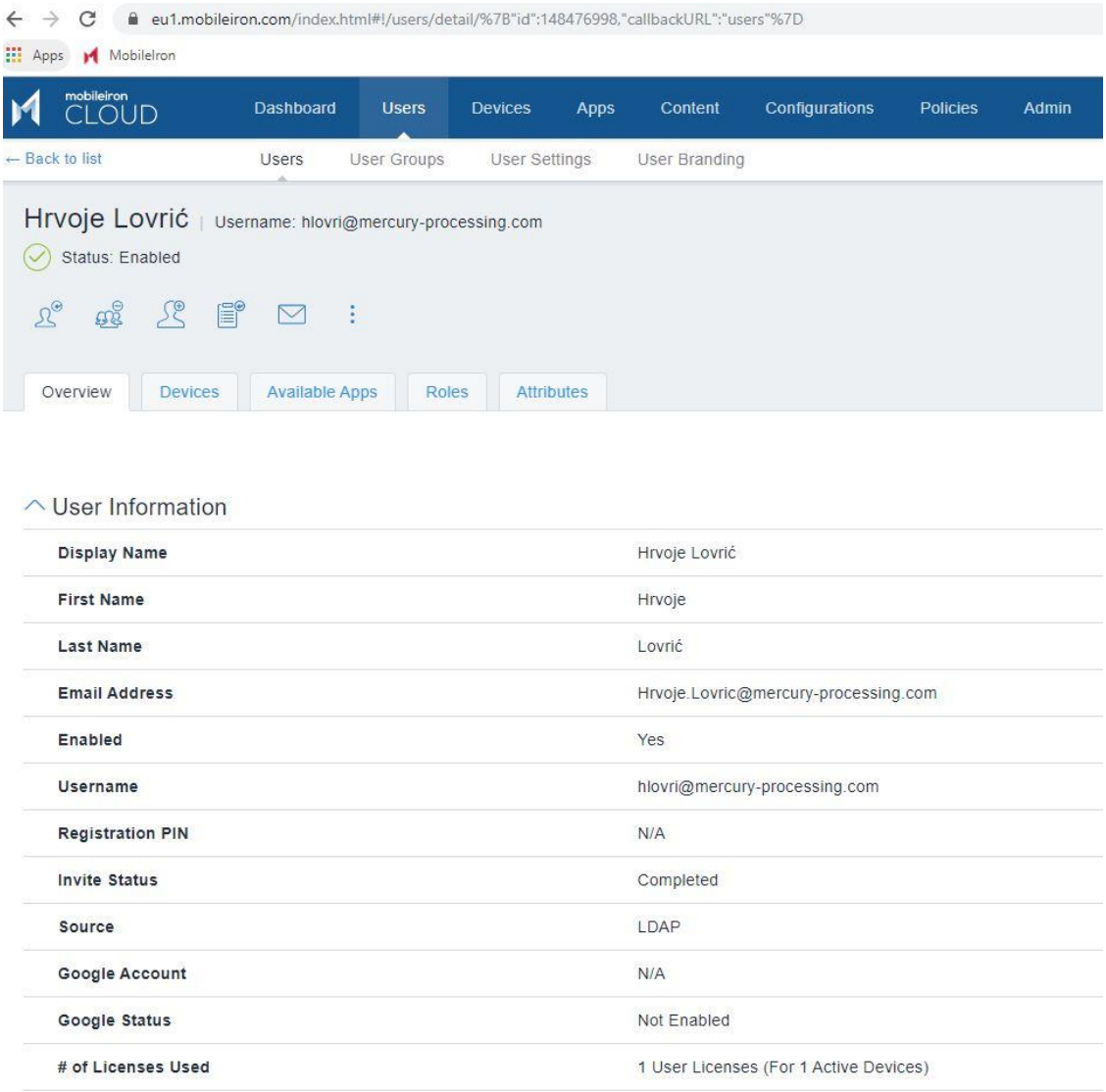
Slika 6.12 Početna stranica MobileIron centralne konzole

6.4.1 Korisnici

Korisnike lako možemo pretraživati po imenu i prezimenu, što je puno lakše nego tražiti korisnike ili njihove uređaje preko “Devices“ iz razloga što moramo upisati IMEI ili nešto jedinstveno za svaki od uređaja. Kada uđemo na korisnika vidljive su osnovne informacije – ime, prezime, email adresa, korisničko ime, status korisnika te koliko licenci koristi. Ispod status možemo vidjeti nekoliko ikonica – dodavanje korisnika u grupu, brisanje iz grupe, slanje poruke, itd. Pod „“Available Apps“ nalaze se aplikacije koje smo stavili u katalog aplikacija, a u “Attributes“ mogu se koristiti atributi korisničkog računa kako bi se korisnicima pridružili dodatna svojstva. Ova svojstva mogu se zatim koristiti za izradu grupa ili distribuciju konfiguracija.



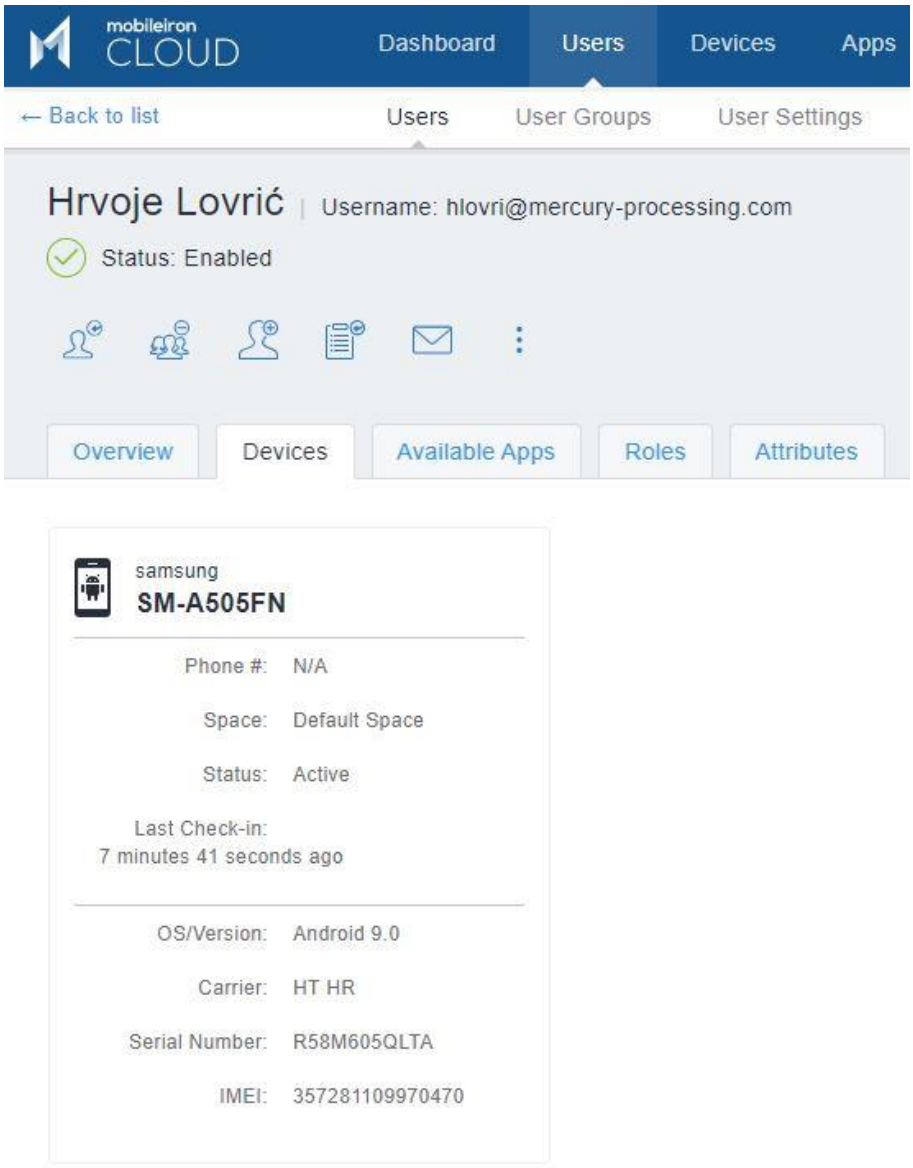
Slika 6.13 Pretraživanje korisnika po imenu i prezimenu



Slika 6.14 Informacije o korisniku

6.4.2 Uređaji

Na uređaje možemo doći iz korisničkog profila stisnuvši na “Devices“ ili otići na Devices tab u gornjem izborniku pa tražiti uređaj po jedinstvenom obilježju što je daleko kompliciranije. Možemo vidjeti neke osnovne informacije o uređaju, model, status, zadnja upotreba aplikacija, verzija operacijskog sustava, mobilni operater te serijski broj i IMEI.

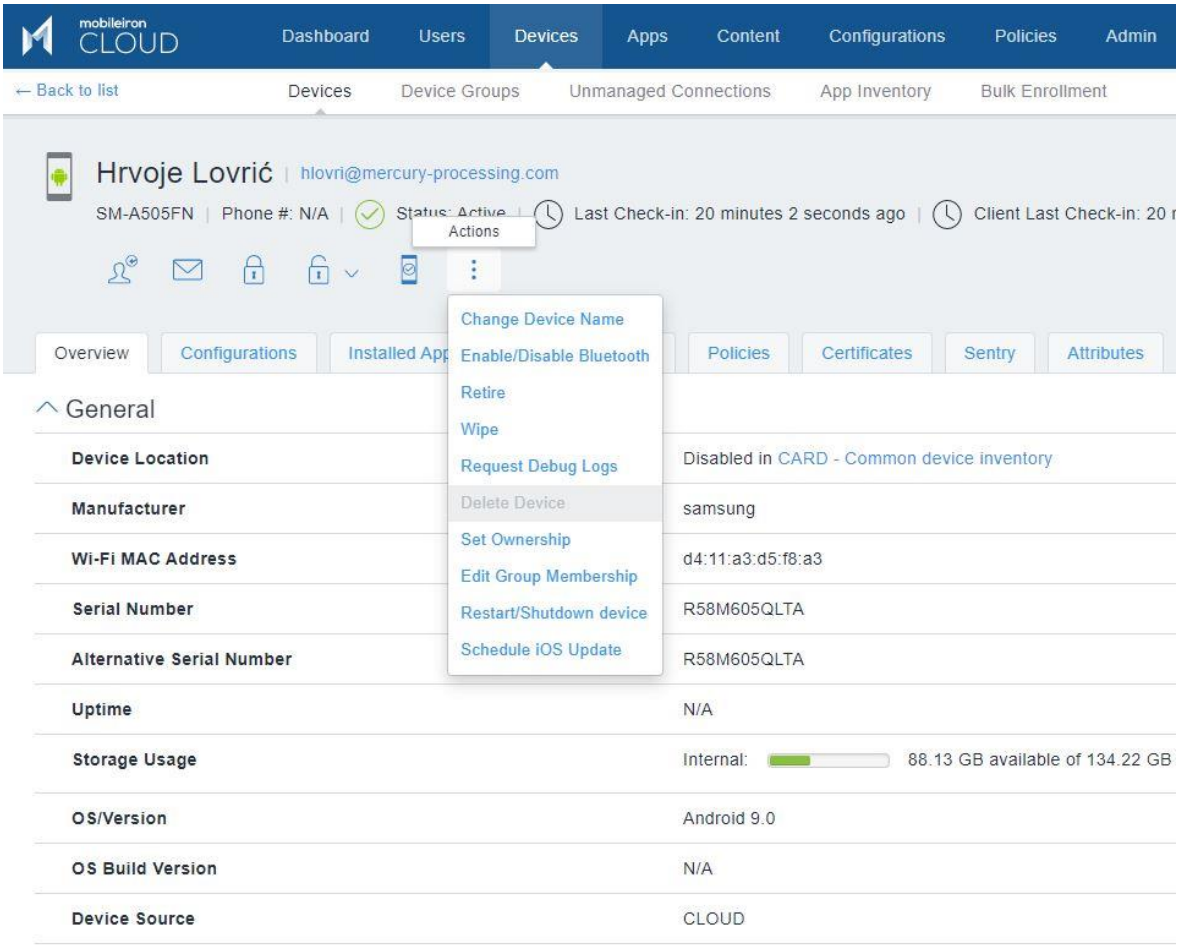


Slika 6.15 Uređaji korisnika

Kada uđemo na uređaj, može vidjeti slične informacije koje su bile na prošloj slici, dodatno, može se vidjeti koliko prostora je slobodno te wi-fi MAC adresa. Pomoću ikonica možemo

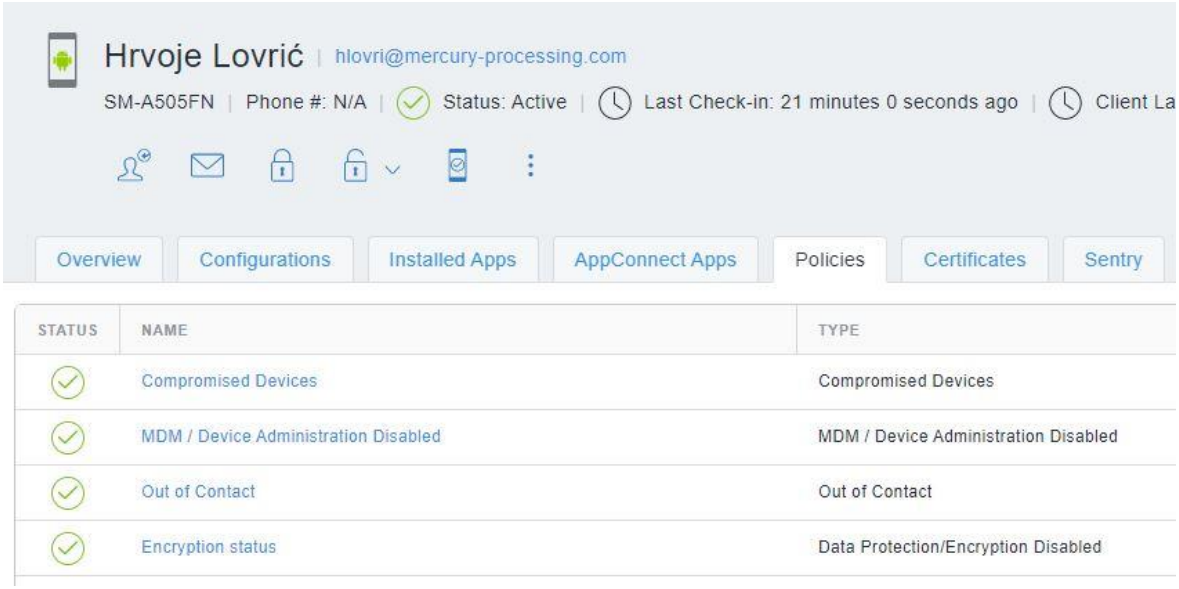
zaključati ili otključati uređaj ukoliko je PIN zaboravljen, a pod "Actions" postoji par opcija pomoću kojih možemo upravljati uređajima:

- Promijeniti ime uređaja radi lakšeg pretraživanja
- Omogućiti/onemogućiti bluetooth
- Umiroviti uređaj – na uređaju se brišu samo aplikacije MobileIron-a, vezane uz poslovni dio, sve ostalo ostaje. Ovo je odlična opcija ukoliko dođe do gubitka ili krađe uređaja, naime, umirovljenjem uređaja firma se osigurala od gubitka poslovnih podataka.
- Vratiti uređaj na tvorničke postavke – ukoliko korisnik to zahtjeva ili postoji neki drugi razlog – brišu se svi podaci s uređaja (poslovni i privatni)
- Izbrisati uređaj (iz MobileIron administracije) možemo tek kada ga umirovimo
- Isto tako, možemo uzeti logove uređaja, modificirati grupe te resetirati ili ugasiti uređaj.



Slika 6.16 Akcije koje se mogu napraviti

Pod konfiguracijama, politikama, aplikacijama nalaze se stvari koje su pokazane u prethodnim poglavljima.



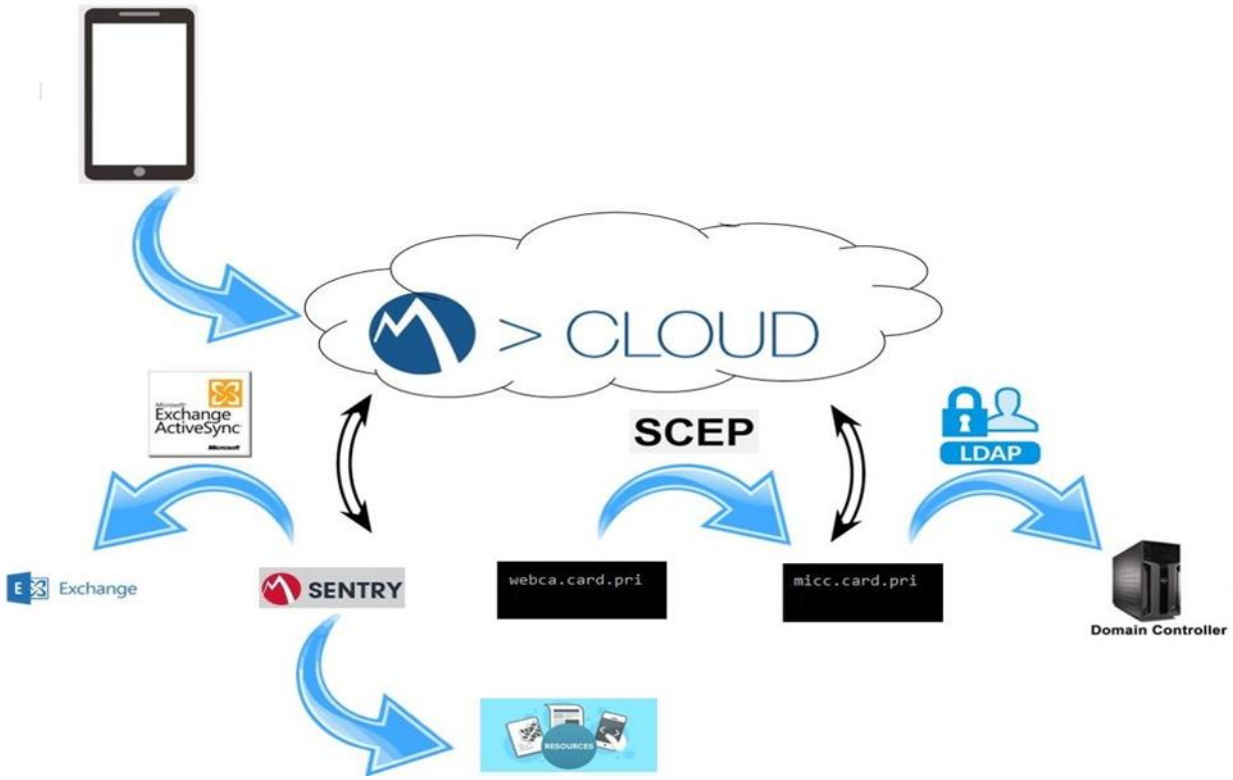
Slika 6.17 Primjer politika koje smo konfigurirali

6.5 Shematski prikaz

Postoji nekoliko komponenata koji su ključni za uspješno ostvarivanje komunikacije između mobilnog uređaja i MobileIrona:

- MobileIron Cloud – centralna komponenta koja omogućuje zaposlenicima da pristupe sigurnosnim aplikacijama i poslovnim resursima na mobilnim uređajima
- Sentry – ključna komponenta MobileIron-a, gatekeeper (određuje tko može čemu pristupiti) koji upravlja i osigurava promet između mobilnih uređaja i poslovnih sustava
- Web CA - izdaje digitalne potvrde, koje su datoteke podataka koje se koriste za kriptografsko povezivanje subjekta s javnim ključem. Izdaju SSL certifikate koje web preglednici koriste za provjeru autentičnosti sadržaja poslanog s web poslužitelja.
- MICC – konektor između CA i LDAP-a
- LDAP - aplikacijski protokol za čitanje i pisanje imenika preko IP mreže. Imenik je u LDAP-u datoteka ili skupina podataka koji su organizirani slično kao telefonski imenik, koji sadrže podatke o korisnicima, datotekama i aplikacijama, kao i njihove sigurnosne postavke.
- DC – poslužitelj na kojem se nalazi baza AD-a, kontroler domene
- Exchange (ActiveSync) - Microsoftov protokol za (uglavnom) mobilne aplikacije s Exchangeom.

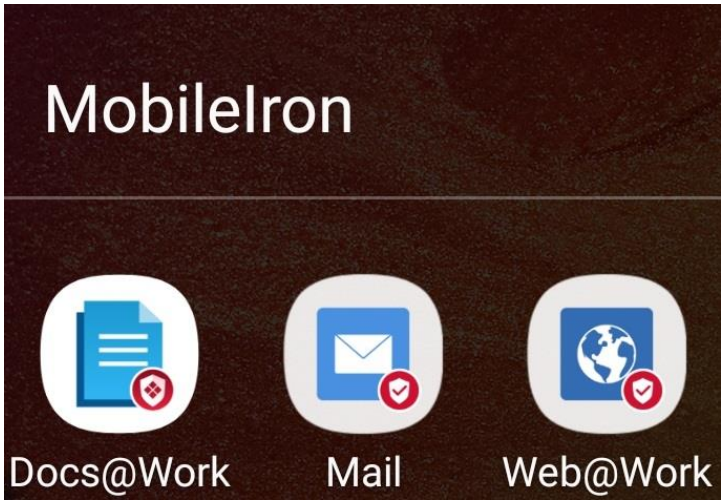
Na slici je prikazan shematski prikaz kako funkcionira prijava na MobileIron platformu te komunikacija između potrebnih komponenata. Centralna komponenta se nalazi u cloudu. Svi mobiteli se za inicijalnu konfiguraciju spajaju na (MobileIron) cloud, registriraju se preko clouda sa svojim domenskim korisničkim imenom i lozinkom te nakon ostvarene komunikacije instaliraju se aplikacije i konfiguracije MobileIron-a na uređaj. Nakon toga, da bi se uređaj uopće mogao spojiti na sentry mora dobiti certifikat kojim se uređaj autenticira (izdan od strane webca). Micc dolazi do internog certificate authoritya preko SCEP protokola, a onda pristupa preko LDAP-a DC-u kako bi mogao izvući podatke o korisnicima. Nakon toga, uređaj se spaja na sentry kako bi pristupio internim resursima firme. I na kraju, sentry komunicira preko Active Sync-a - s Exchangeom, kako bi na uređaj dobili pristup na Email+, Docs@Work i Web@Work.



Slika 6.18 Shematski prikaz komponenata

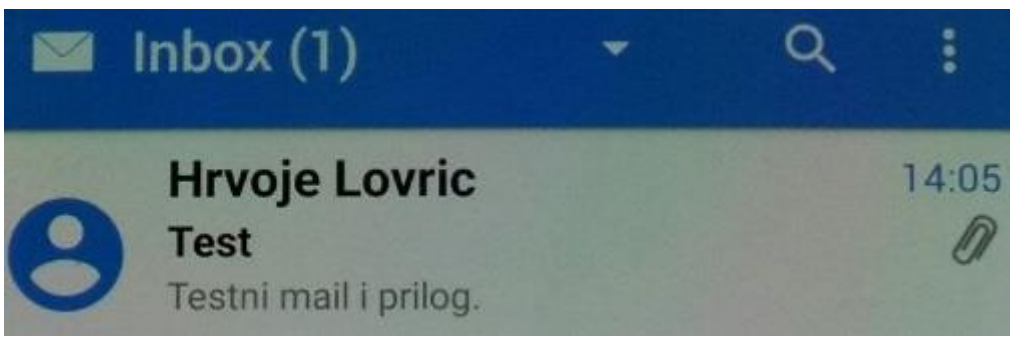
7. Testiranje funkcionalnosti aplikacija MobileIron-a

Kada smo instalirali aplikacije MobileIron-a na mobilni uređaj možemo ih početi koristiti. Nakon instalacije one se nalaze na našem uređaju zajedno sa svim ostalim aplikacijama, ali za potrebe ovog diplomskog rada svrstane se u poseban folder.

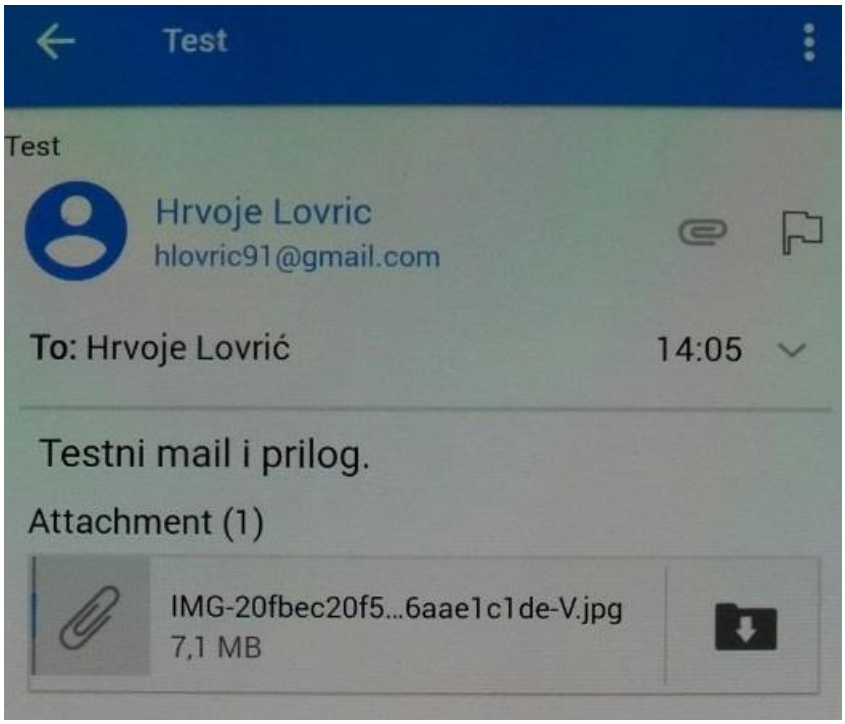


Slika 7.1 Instalirane aplikacije na uređaju

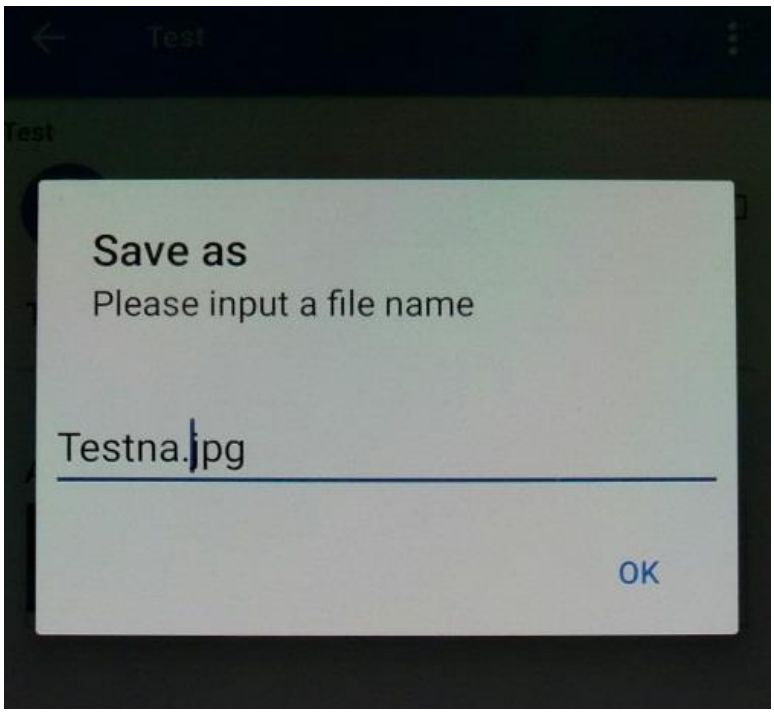
Za testiranje funkcionalnosti aplikacija poslat ćemo jedan mail s prilogom s Gmail-a. Mail će nam doći u Mail aplikaciju, a onda ćemo prilog koji smo dobili spremiti te će biti vidljiv u Docs@Work aplikaciji. Prilog, odnosno, sliku ćemo spremiti pod nazivom Testna.jpg.



Slika 7.2 Testni mail

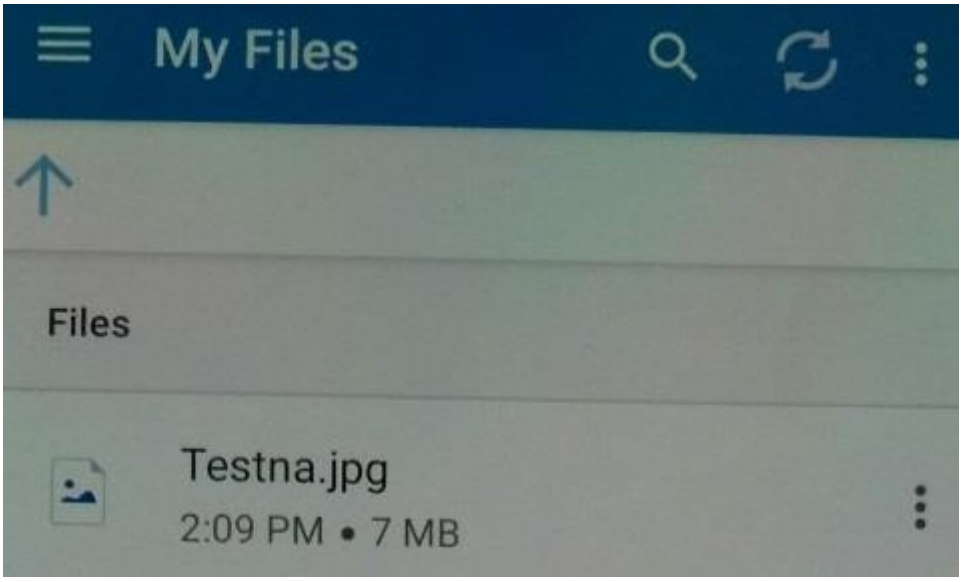


Slika 7.3 Testni mail s prilogom



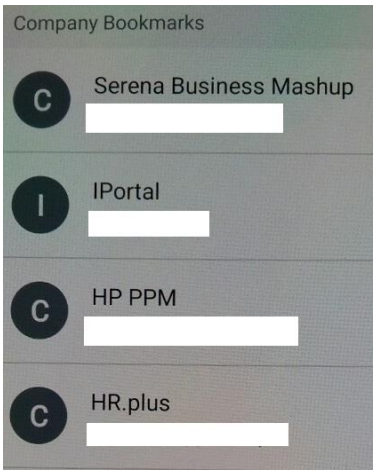
Slika 7.4 Spremanje priloga

Sada kada otvorimo Docs@Work aplikaciju možemo vidjeti da se navedena datoteka nalazi tamo te je ubuduće možemo koristiti za slanje, ali samo preko Mail aplikacije od MobileIrona.



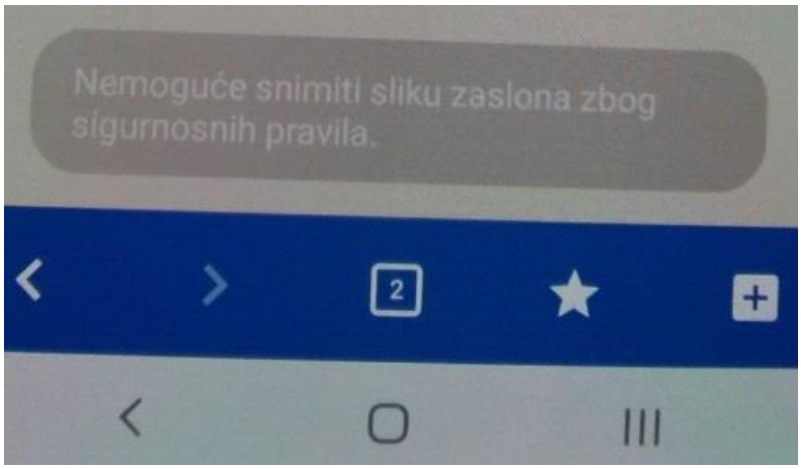
Slika 7.5 Spremljeni prilog u Docs@Work

Što se tiče Web@Work aplikacije, možemo vidjeti da se u njoj nalaze oznake koje smo kreirali. Pritiskom na jednu od tih oznaka otići ćemo na internu web stranicu na kojoj onda možemo raditi kao da smo spojeni u LAN mrežu na našem PC-u na radnom mjestu. Isto tako, možemo vidjeti da ne možemo uzeti screenshot unutar MobileIron aplikacija što smo i postavili konfiguracijom sigurnosnih pravila.



Slika 7.6 Oznake koje su kreirane u Web@Work

Slika 7.7 Otvaranje stranice Serena u Web@Work



Slika 7.8 Nemogućnost uzimanja screenshot-ova

8. Usporedba MobileIron-a s drugim sustavima za upravljanje mobilnim uređajima

Pošto je MobileIron vrlo sličan već spomenutim MDM rješenjima: SAP-u, Cisco Meraki-ju i IBM-om MaaS-u, napravit ću proširenu usporedbu s Microsoftovim Intune-om jer upravo on se najviše razlikuje od MobileIrona. Intune je Microsoftov proizvod što mu svakako već u startu daje bolju poziciju. Može ga se dobiti u paketu s nekim drugim Microsoft proizvodima pa ukoliko smo korisnik Microsoft Azure-a vjerojatno ćemo se odlučiti za Intune.

U prošlosti su tvrtke koristile rješenja za upravljanje uređajima kako bi utvrdile strogu kontrolu nad uređajima prije nego što im odobre pristup. Danas, sve više ljudi koristi osobne uređaje kako bi pristupili poslovnim resursima. Naravno, možemo odlučiti blokirati te uređaje, ali to znači da će tim korisnicima trebati omogućiti (kupiti) uređaje za daljinski rad. Čak i u tom scenariju, većina ljudi radije ne bi nosila osobni uređaj i poslovni uređaj. Moderna rješenja za upravljanje uzimaju to u obzir i omogućavaju kontrolu podataka na razini aplikacije, bez obzira na uređaje na kojima se nalaze. Ovdje dolaze do izražaja rješenja poput Intune-a i MobileIron-a koji omogućuju sigurnost da podaci koje postavljate na određeni uređaj ostaju na tom uređaju. Možemo postaviti šifriranje podataka te osigurati da se podaci ne mogu premjestiti na neupravljanu lokaciju. Kao administrator možemo učinkovito ukloniti poslovne podatke s upravljanog uređaja kada je to potrebno.

8.1 Usporedba Intune-a i MobileIron-a u upravljanju podacima i uređajima

Možemo usporediti Intune-a i MobileIron-a kada je u pitanju upravljanje podacima na uređajima krajnjeg korisnika. Oba rješenja ovdje nude izvrsnu funkcionalnost; pružaju mogućnost osigurati da vaši podaci ne napuste aplikaciju koju su pokrenuli: zabraniti copy/paste, spremanje na uređaj (u oblak), screenshotanje, itd.

Problem je što oba rješenja zahtijevaju da koristite njihovog klijenta (Outlook, OneDrive, Apps, Docs ili Email +). MobileIron za razliku od Intune-a zahtjeva registraciju uređaja kako bismo zapravo dobili potrebne aplikacije. Stvari poput zadanih mail aplikacija u ne dolaze u obzir zbog nedostatka podrške za SDK (Software Development Kit) i kod jednog i kod drugog riješenja.

Microsoftov Intune omogućava upravljanje aplikacijama bez registracije uređaja. Jednostavno se može koristiti Outlook aplikacija (ili OneDrive, SharePoint, Box, Dropbox itd.) i prijaviti se s bilo kojeg uređaja kao što bi to obično radili kako bismo pristupili svojim podacima. U tom se trenutku pravila kreirana od strane administratora primjenjuju se na samoj aplikaciji, a ne na uređaju. To je najveća razlika između MobileIron-a i Intune-a.

Što se tiče upravljanja uređajima i Intune i MobileIron izvrsne su opcije ako ćete zahtijevati da se svi uređaji upisuju i upravljaju centralno, stvar je u tome da Intune to ne zahtjeva dok je kod MobileIron-a to nužno. Potreba da određene aplikacije na uređaju pristupe podacima lako se rješava jednostavnim guranjem potrebne aplikacije (konfiguracije) na uređaj. Problem je ukoliko koristimo BYOD. Neće svaki krajnji korisnik biti sretan s odlukom da mora registrirati vlastiti uređaj.

8.2 Tablica usporedbi rješenja

U tablici ispod možemo vidjeti kratku usporedbu sustava za upravljanje mobilnim uređajima što se tiče najbolje značajke, cloud ili on-premise dostupnosti te cijene. Glavne značajke rješenja pokazane su u poglavljima prije, no ovdje su izdvojena po jedna od svake koja je karakteristična za pojedino rješenje te ona koja ih razlikuje od drugih rješenja. Što se tiče dostupnosti; MobileIron i SAP mogu biti u cloudu te kao on-premise rješenje što je svakako prednost ukoliko planiramo imati servere u našim sistem salama. Manje firme će prije tražiti rješenja u cloudu, što zbog jednostavnosti implementacije (održavanja), što zbog cijene.

Kada pogledamo cijene, možemo vidjeti da je SAP Mobile Secure najjeftiniji, ali možda i najmanje zastupljen od ostalih rješenja pa stoga i ova cijena. Cijena MobileIron-a je ovisna o pretplati koju uzmemo. MobileIron prodaje svoj proizvod u tri paketa - gold, silver i platinum - koji nude različite značajke. Organizacije mogu kupiti licence za te pakete na temelju uređaja ili korisnika što je opet prednost jer ostala rješenja eksplicitno kažu je li

pretplata po korisniku ili uređaju. MobileIron nam od svih rješenja daje najviše slobode da sami sastavimo paket i opcije koje želimo te je idealan i za male i za velike firme.

Naziv rješenja:	Najbolja značajka:	Cloud/On-premise:	Cijena:
MobileIron	Napredna autentikacija	Obje opcije moguće	Ovisi o pretplati
Microsoft Intune	Integracija s Microsoft Azure-om	Cloud	40 kuna po korisniku mjesečno
IBM Maas360	Watson engine	Cloud	25 kuna po uređaju mjesečno
Cisco Meraki	Vidljivost potencijalnih ranjivosti	Cloud	20 kuna po uređaju mjesečno
SAP Mobile Secure	Jednostavan samouslužni portal	Obje opcije moguće	10 kuna po uređaju mjesečno

Tablica 1 Usporedba rješenja

8.3 Gledajući u budućnost

Iako je MobileIron danas možda dobra opcija za upravljanje mobilnim uređajima, postoje određena ograničenja koja se trebaju riješiti. Naime, MobileIron nema mogućnost integriranja uređaja koji rade na Windows OS-u. Intune je već izgrađen s Azure Active Directory-om jer je okosnica za pružanje uvjetnog pristupa, multifaktorske provjere autentičnosti i sve analitike i telemetrije koja vam je potrebna da biste saznali tko se prijavio, koliko puta i odakle. Sve ovo ne znači da MobileIron (ili bilo koje drugo trenutno rješenje) nije odličan odgovor na problem osiguravanja podataka na mobilnim uređajima no pitanje je zašto bi u budućnosti netko odabrao MobileIron s obzirom na način na koji se Microsoft

pozicionirao - da u budućnosti svi korisnici Azure-a (kojih će biti jako puno) iskoriste i Intune kao MDM rješenje.

9. Budućnost MDM-a

S mobilnim uređajima koji postaju sveprisutni i aplikacije koje preplavljuju tržište, mobilni nadzor postaje sve važniji. Korištenje upravljanja mobilnim uređajima nastavlja rasti stalnim tempom i vjerojatno će godišnja stopa porasti od gotovo 23% do 2028. S.A.D. će i dalje biti najveće tržište za upravljanje mobilnim uređajima na globalnoj razini. Mobilni uređaji i aplikacije su sveprisutni u današnjem okruženju. Njihova stalna prisutnost i uporaba i dalje će imati veliku prisutnost u svim našim životima. I, kao što je već spomenuto, sve ove okolnosti zajedno daju neizbježan rast mobilnog praćenja i softverskih rješenja koja podržavaju taj zahtjev.

Sljedećih nekoliko godina bit će uzbudljivo kada je u pitanju upravljanje uređajima. Mogućnost prelaska s naslijeđenog modela za obradu uređaja na model upravljanja uređajem za sve krajnje točke je realna i moguća. Naravno, bit će izazova i rasprava oko slučajeva upotrebe i može li se navedeno usvojiti na svim uređajima. U početku će možda biti smisleno ciljati neke manje grupe sa više mobilnih specifičnih zahtjeva, a zatim graditi dalje. Također, implementacija će biti lakša jer prave, fizičke podatkovne centre polako sve više zamjenjuje cloud. Potrebno je pojednostaviti novi model uklanjanjem i prelaskom s modela pokretanja mikro upravljanog uređaja na prirodnije iskustvo s kojim je korisnik već upoznat. Moramo razmišljati o implementaciji kao većem broju usluga. To omogućava korisnicima da se brže prilagode. Nadalje, IoT nadilazi objedinjavanje mobilnih i PC / prijenosnih računala. Trenutno je na tržištu eksplozija takvih uređaja i do danas ne postoje standardi oko upravljanja i sigurnosti. Samo je pitanje vremena kad će se i to promijeniti.[4]

10. Zaključak

Mobilni uređaji i aplikacije su sveprisutni u današnjem okruženju. Njihova stalna prisutnost i uporaba i dalje će imati veliku prisutnost u svim našim životima. I, kao što je već spomenuto, sve ove okolnosti zajedno daju neizbježan rast mobilnog praćenja i softverskih rješenja koja podržavaju taj zahtjev. Kako se sve više poslovanje okreće mobilnom svijetu svakako postoji potreba za zaštitu podataka i na mobilnim uređajima. Isto tako, mobilni uređaji predstavljaju upravo najveći problem gubitka podataka, često budu izgubljeni i ukradeni. Postoji sve više rješenja kako zaštiti podatke na mobilnim uređaja. Po potrebama firme potrebno je odabrati najbolje rješenje u skladu s financijskim mogućnostima, kompleksnosti sustava, broja ljudi, itd. Mnoge tvrtke imaju i još mnogo njih će na kraju zaključiti da je rizik poslovanja bez odgovarajuće MDM rješenja prevelik i puno veći od troškova instalacije ovog softvera.

Popis kratica

IoT	*Internet of Things*	povezivanje uređaja putem interneta
MDM	*Mobile Device Management*	sustav za upravljanje mob. uređajima
OS	*Operating System*	softver za upravljanje računalom
SIM	*Subscriber Identity Module*	modul za identifikaciju pretplatnika
POS	*Point-of-sale*	uređaj za el. plaćanje roba i usluga
BYOD	*Bring Your Own Device*	korištenje vl. uređaja za posl. potrebe
MAM	*Mobile Application Management*	upravljanje mobilnim aplikacijama
EMM	*Enterprise Mobility Management*	upravljanje mobilnošću poduzeća
OTA	*Over-the-air*	skidanje aplikacija bežičnim putem

Popis slika

Slika 4.1 Microsoft Intune 7

Slika 4.2 IBM Maas360 8

Slika 4.3 Cisco Meraki 9

Slika 4.4 SAP Mobile Secure 10

Slika 6.1 Politike 14

Slika 6.2 Blacklistane aplikacije 15

Slika 6.3 Kompromitirani uređaji 16

Slika 6.4 Klijenti koji su izvan dosega 17

Slika 6.5 Status enkripcije 18

Slika 6.6 Onemogućena administracija 19

Slika 6.7 Detalji Email+ aplikacije 25

Slika 6.8 Konfiguracija Email+ aplikacije 26

Slika 6.9 Detalji Docs@Work aplikacije 27

Slika 6.10 Detalji Web@Work aplikacije 28

Slika 6.11 Oznake u Web@Work aplikaciji 29

Slika 6.12 Početna stranica MobileIron centralne konzole 30

Slika 6.13 Pretraživanje korisnika po imenu i prezimenu 31

Slika 6.14 Informacije o korisniku 32

Slika 6.15 Uređaji korisnika 33

Slika 6.16 Akcije koje se mogu napraviti 34

Slika 6.17 Primjer politika koje smo konfigurirali 35

Slika 6.18 Shematski prikaz komponenata 37

Slika 7.1 Instalirane aplikacije na uređaju 38

Slika 7.2 Testni mail 38

Slika 7.3 Testni mail s prilogom 39
Slika 7.4 Spremanje priloga 39
Slika 7.5 Spremljeni prilog u Docs@Work 40
Slika 7.6 Oznake koje su kreirane u Web@Work 40
Slika 7.7 Otvaranje stranice Serena u Web@Work 41
Slika 7.8 Nemogućnost uzimanja screenshot-ova 41

Popis tablica

Tablica 1 Usporedba rješenja 44

Popis kôdova

Kod 1 Konfiguracija kataloga aplikacija 20

Kod 2 Konfiguracija pristupa katalogu 22

Kod 3 Konfiguracija za prevenciju od gubitka podataka 22

Kod 4 Konfiguracije sigurnosnih postavki 24

Literatura

[1] FORCEPOINT, https://www.forcepoint.com/cyber-edu/mobile-device-management-mdm, lipanj 2019.

[2] TECHTARGET, https://searchmobilecomputing.techtarget.com/definition/mobile-device-management, rujan 2019.

[3] COONTINUM, https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm, lipanj 2019.

[4] ENTERPRISE-CIO, https://www.enterprise-cio.com/news/2016/jul/13/the-evolution-of-device-management/, lipanj 2006.

[5] DEVICE MANAGEMENT, http://www.devicemanagement.org/content/view/20754/152/, kolovoz 2019.

[6] CARNET, https://sysportal.carnet.hr/node/1235, kolovoz 2019.

[7] FINANCES ONLINE. https://financesonline.com/mobile-device-management/, kolovoz 2019.

[8] TECHTARGET, https://searchmobilecomputing.techtarget.com/definition/MobileIron, rujan 2019.

Student vlastoručno potpisuje diplomski rad iza zaključka s datumom i oznakom mjesta završetka rada te naznakom:

„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, datum.

Ime Prezime