Napredna organizacijska rješenja usluge nadzora mobilnih uređaja i aplikacija putem oblaka, na primjeru koncepta „Mobile Device Management-Intune“

Drgestin, Martin

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **The University of Applied Sciences Baltazar Zaprešić / Veleučilište s pravom javnosti Baltazar Zaprešić**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:129:452319

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij Informacijskih tehnologija

MARTIN DRGESTIN

Napredna organizacijska rješenja usluge nadzora mobilnih uređaja i aplikacija putem oblaka, na primjeru koncepta „Mobile Device Management-Intune“

PREDDIPLOMSKI ZAVRŠNI RAD

Zaprešić, rujan 2022. godine

VELEUČILIŠTE
BALTAZAR
ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij Informacijskih tehnologija

PREDDIPLOMSKI ZAVRŠNI RAD

Napredna organizacijska rješenja usluge nadzora mobilnih uređaja i aplikacija putem oblaka, na primjeru koncepta „Mobile Device Management-Intune“

Mentor:
Prof. dr. sc. Vladimir Šimović

Student:
Martin Drgestin

Naziv kolegija:
Poslovna inteligencija

JMBAG studenta:
0234059434

SADRŽAJ

SAŽETAK 4
ABSTRACT 5
1. UVOD 6
2. SERVIS 7
2.1 Microsoft Intune 7
2.2 MDM 7
2.3 Zašto MDM ? 8
2.4 MAM 8
2.5 Zašto MAM ? 9
2.6 Certifikati, licence i vrste mobilnih uređaja 9
3. PROFILI 10
3.1 Android Profili 10
3.2 IOS profil 10
3.3 Fully Managed, dedicated, and corporate work profile 11
3.3.1 Personally Owned – Work profile 12
3.3.2 Corporate -OWNED Dedicated device 12
3.3.3 Enrollment Proces Android Fully Managed Devices 13
3.3.4 Android CP 18
3.3.5 Ios Enrollment 20
4. ZAKLJUČAK 26
5. IZJAVA 27
6. POPIS LITERATURE 28
a. KNJIGE; ČLANCI 28
b. INTERNETSKI IZVORI 28
7. POPIS SLIKA 29
8. ŽIVOTOPIS 30

SAŽETAK

Informacijske tehnologije i informacijski sustavi u današnjem svijetu imaju abnormalan rast i pružaju rješenja za razne tipove automatizacija, tako da ih je jako potrebno pratiti i prilagodljivo aplicirati kako bih kompanije mogle opstati na tržištu. jer se gotovo svi automatizirani tokovi odvijaju kroz informacijske sustave ili njihove podsustave ili dijelove, kao što su to napredna organizacijska rješenja usluge nadzora mobilnih uređaja i aplikacija putem oblaka, a na primjeru koncepta „Mobile Device Management-Intune (Šimović, 2010; Šimović, Ružić-Baf, 2013) Svaka srednja i veća kompanija ima poveći broj mobilnih i statičkih uređaja, stoga im je potreban pristup informacijskim sustavima putem istih uređaja, a posebno zbog sigurnosti sustava i lakše administracije.

Tema ovog rada je organizacijsko rješenje nadzora i upravljanja mobilnim uređajima unutar srednjih i većih kompanija. Cilj rada je objasniti Microsoft Intune platformu, svrhu nadzora uređaja, kreiranje politika i profila prema uvjetima koje organizacija zahtjeva, te mogućnosti koje Microsoft Intune nudi za upravljanje aplikacijama i uređajima.

Ključne riječi: Administrator, upravljanje uređajima, korisnici, organizacija, Microsoft Intune, Mobile Device Management

Title in English:

Advanced organizational solutions for the monitoring of mobile devices and applications via the cloud, on the example of the concept "Mobile Device Management-Intune

ABSTRACT

Information technologies and information systems in today's world have abnormal growth and provide solutions for various types of automation, so it is very necessary to monitor them and apply them adaptively so that companies can survive in the market. because almost all automated flows take place through information systems or their subsystems or parts, such as advanced organizational solutions for the monitoring of mobile devices and applications via the cloud, and on the example of the "Mobile Device Management-Intune" concept (Šimović, 2010; Šimović, Ružić -Baf, 2013) Every medium and large company has a large number of mobile and static devices, therefore they need access to information systems through the same devices, especially for system security and easier administration.

The topic of this paper is the organizational solution for monitoring and managing mobile devices within medium and large companies. The paper aims to explain the Microsoft Intune platform, the purpose of device monitoring, the creation of policies and profiles according to the conditions required by the organization, and the possibilities that Microsoft Intune offers for managing applications and devices.

Keywords: Administrator, Device management, Users, Organization, Microsoft Intune, Mobile Device Management

1. UVOD

Za uspješno poslovanje i rad svakog radnika potrebno je imati adekvatnu opremu što podrazumijeva mobilni uređaj i računalo. Svaki radnik kada dođe u kompaniju dobije „Welcome letter“ u kojemu može pronaći sve bitne stavke za početak rada, kao što su korisnički podaci, broj mobitela, pristup resursima kompanije i kontakt za podršku. Prema ITIL-u[1] za IT administratora bitno je da je oprema konkretno zavedena, da je računalo u domeni, da su instalirani svi korporativni servisi i pristupi koje svaki djelatnik treba imati za sami početak rada. Kako se do nekoliko godina unazad Microsoftva platforma dodatno razvila i stvorila dodatne mogućnosti tako je omogućila uz korištenje EMS licence korištenje Intune-a. Microsoft Intune omogućuje isto kao dosadašnji SCCM pristup resursima koje se nalaze unutar kompanije, bilo riječ o mobilnim uređajima ili računalima, najbitnije od svega je što je „cloud“ rješenje i takvo ima dodatne prednosti vezane za integraciju istog. IT administratorima je stvar dodatno olakšana zbog nadzora prema opremi, a korisniku zbog pristupa resursima koji su „in house“ rješenja.

[1] ITIL Foundation, SCCM konzola za nadzor sustava.

2. SERVIS

2.1 Microsoft Intune

Microsoft Intune je „cloud“ servis koji nam omogućuje nadzor mobilnih uređaja, laptopa, računala i tableta. Nadzor i upravljanje mobilnim uređajima radimo kroz MDM sustav, dok upravljanje aplikacijama radimo kroz isti sustav zvan MAM. On je integriran zajedno sa Azure[2] Active Directory-em. AAD je također „cloud“ rješenje od strane Microsofta koje nam nudi jako puno mogućnosti koje nam običan AD ne nudi. Za IT administratore AAD nam omogućuje pristup resursima aplikacija kompanije, vlastitim aplikacijama koje korisnik koristi, puno manja je latencija unutar kreiranja distribucijskih i sigurnosnih grupa, nudi nam 2-faktornu autentifikaciju korisnika što pokazuje sigurnost pristupa korporativnim servisima, zatim omogućuje pristup domeni bez kontrolera i možemo raditi analize, izvještaje bez dodatnih alata kao što smo morali na „starom“ AD-u.

2.2 MDM

Svaka organizacija može naići na problem kada govorimo o financijskom budžetu za IT opremu u koliko se ne radi dobra evidencija opreme koju korisnici zadužuju i koriste u službene svrhe. Svaka organizacija prema standardima koje propisuje ITIL (Information Tehnology Infrastructure Library) treba imati nekakav „asset management“ za IT opremu, te prema internim standardima propisani vijek trajanja opreme u svrhu zamjene iste. Kada se ne vodi adekvatna evidencija o opremi dobivamo loš „feedback“ od strane korisnika, same kolege iz IT-a ne mogu provjeriti točno stanje opreme korisnika što može doći također do problema kod razduživanja opreme kada korisnik odlazi iz kompanije, te najbitnija stvar o kojoj sve ovisi LTP (Long term planing). U koliko prema lošoj evidenciji se napravi LTP postoji mogućnost da odjel će imati manjak robe ili višak, što može izazvati jako lošu reakciju na poslovanje. Organizacije bih trebale imate takva adekvatna rješenja implementirana u sustave bez obzira što financijski implementacija je skupa za takve sustave u srednjim kompanijama, ali donosi velike benefite i djelatnici mogu biti fokusirani na konkretnije projekte i slično. Jedni od takvih alata su HPSM,Gira,SharePoint i sami MDM.

[2] Microsoft Azure, Klijentska podrška, Intune konzola.

Mobile Device Management je alat koji služi za upravljanje svih tipova mobilnih i statičnih uređaja unutar organizacije. Danas imamo jako puno alata koji se mogu implementirati u sustave kompanija i pružiti im razne benefite. Mobile Device Management je jedan od vodećih „cloud“ rješenja koja pruža tu mogućnost.

2.3 Zašto MDM ?

Uređaj kada izvrši određeni proces prijave na sustav pomoću procesa „Enrollment“ javlja se sustavu i sustav MDM ga bilježi na platformi sa korisničkim podacima. Kada je uređaj vidljiv na platformi mi možemo vidjeti serijski broj uređaja, IMEI, status uređaja, koji operativni sustav ima, verziju, memoriju, apsolutno sve vezano za uređaj osim privatnih podataka kao što su slike, razgovori i pozivi.

Organizacijsko gledano rješenje pruža veliku sigurnost jer se može nadzirati promet koji se radi na uređaju, kada korisnik izgubi ili mu se ukrade uređaj „remote“ se može sa konzole uređaj obrisati, zaključati ili spojiti na njega. Kada se uređaj obriše on u roku od 10 sekundi odlazi na tvorničke postavke i brišu sve svi podaci sa njega. Ovaj servis omogućuje adekvatno praćenje opreme od strane korisnika i mogu se raditi analize i izvještaji koji IT administratorima omogućuje olakšan rad i fokus na bitnije stavke. Za korisnike MDM pruža mogućnost pristupa korporativnim servisima što je ujedno olakšano korištenje poslova koji možda traju par minuta, a djelatnicima oduzimaju vrijeme dok dođu za radno mjesto.

2.4 MAM

MAM (Microsoft Application Management) je funkcija vezana za MDM koja omogućuje da se na organizacijskim uređajima instaliraju, ažuriraju i brišu klijentske i korporativne aplikacije putem servisa kojim upravlja IT administrator. Od strane svakog administratora bitno je korisnicima omogućiti pristup korporativnim aplikacijama kojima se služe. MAM nam pruža opcije da se ograniče pristupi aplikacijama na način da ako uređaj se primjerice nije javio sustavu određeno vrijeme kojeg se unutar politika prepiše, te aplikacija neće raditi. U tom slučaju korisnik je dužan napraviti ponovnu prijavu kroz Intune kako bih aplikacija bila moguća za korištenje. Servis nam omogućuje nadzor i mogućnost instalacija aplikacija za sve tipove uređaja koji su pristupni organizaciji.

2.5 Zašto MAM ?

Tvrtke imaju većinom razvijen Intranet za pristup korporativnim servisima i obavijestima koji se zbivaju unutar kompanije. MAM nam omogućuje da kreiramo aplikaciju prema našim uvjetima i okruženjima koje zahtijevamo te samim time djelatnicima omogućimo pristup HRnet-u, Intranetu, SharePoint servisima i svemu što može olakšati djelatnicima rad. Aplikacije se mogu spuštati na uređaje preko grupa koji su kreirani na o365 platformi i pojedinačno na korisnika ili uređaj. One se mogu omogućiti na svim tipovima uređaja u „store-u“ i korisnik sam može instalirati aplikaciju koju koristi ili direktno bez odobrenja spustiti na uređaj. Kao i sami centralni servis „Endpoint“ možemo vidjeti verzije aplikacija koje se nalaze na uređajima, prema potrebni ih ažurirati ili postaviti automatiku.

2.6 Certifikati, licence i vrste mobilnih uređaja

Licenca ima određene mogućnosti za broj uređaja koji može pristupiti platformi kako to organizacija ili ustanova propiše. One mogu biti postavljene preko AAD-a za registraciju ili preko procesa Intune Enrollment-a. EMS licenca omogućuje da korisnik ima 15 maksimalnih uređaja u svom korištenju, kojeg se može i umanjiti preko portala. Certifikat vezan za servis dolazi sa korištenjem i plaćanjem licence koju organizacija kupi od ključnog kupca. Prema korištenju aplikacijskog servisa na platformi potrebno je obnavljati certifikate koji s besplatni za Android i IOS uređaje i vezane za web servis play store-a i app store-a. Korporativna aplikacija koja se omogućuje korisnicima kroz platformu također treba certifikat koji je potrebno obnavljati određeni period. Kada se rade promjene na takvim aplikacijama potrebno je novi apk. priložiti na platformu i sinkronizirati sa svim uređajima kako bih dobili ispravnu verziju iste. Istekom valjanog certifikata dolazi obavijest osobi zaduženoj za servis koja mora isti obnoviti kako bih aplikacije mogle nesmetano raditi, ako se certifikati ne obnove aplikacije će raditi ali se neće update-ati na novu verziju korisnicima koji ih koriste. Platforma nam omogućuje da imamo više tipova uređaja koji mogu biti vezani za korisnika i mogu biti upravljivi sa konzolom koju rabimo.
Vrste tih uređaja su :

- Android OS (Mobiteli, tableti)
- IOS OS (Mobiteli, tableti)
- MacOS
- Windows 10 – Računala
- Windows 11 – Računala

3. PROFILI

3.1 Android Profili

Prije nego uređaj se postavi u nadzor i sustav kompanije potrebno je na platformi kreirati profile sa određenim politikama koje trebaju biti odrađene kako bih uređaj uopće mogao pristupiti korporativnim servisima i biti vidljiv sustavu. Samim time potrebno je prvenstveno prilikom kreiranja profila odabrati „Profile type“ koji zadovoljava naše potrebe. U ponudi se za Android profile nudi opcija „Fully managed, dedicated , and corporate work profile“ Što predstavlja uređaj koji kompletno pripada organizaciji i organizacija ima uvid u sve resurse i izmjene koje napravi dešavaju se odmah na uređaju, te imamo „Personally- owned work profile“ što predstavlja drugačiji tip profila koji ima razdvojen „Work/Personal“ dio na uređaju, te u personalnom djelu ima uvid u osobne podatke dok u „work“ djelu samo korporativne aplikacije. Nakon odabira profila dolazimo do „Compliance“ postavki koje moramo odrediti minimalnu OS verziju uređaja, koji tip passworda se bude koristio na tim uređajima i što se dešava sa uređajima koji se ne javljaju sustavu. Kada se postavi profil mi moramo kreirati grupu korisnika na o365 konzoli i primijeniti na koju grupu ljudi/ uređaja te profile želimo primijeniti. Prilikom primjenjivanja ove politike na korisnike možemo na nadzornoj ploči pratiti u kojem je statusu koja instalacija i vidjeti zašto nije uspjela. Imamo mogućnost također kreiranja profila pod opcijom KIOSK što predstavlja restrikcije koje ne doživljavaju korištenje resursa na uređaju koje administrator ne želi da se koriste. Profil se kreira na način da se ograniči pristup svim resursima s uređaja i kreira zaseban profil koji prikazuje ono što je zamišljeno da se rabi. U ovom radu mi ćemo konkretno vidjeti kako funkcioniraju „Fully Managed i Personal/Work“ profili. Android je doista razvijen u ovom segmentu i nudi nam jako puno vrsta profila koje možemo koristiti. AOSP (Android Open Source Project) nije povezan sa Google servisima, nudi dobru mogućnost dijeljenja podataka između više osoba koji sudjeluju na nekom projektu.

3.2 IOS profil

IOS nije razvijen u velikim opcijama za Intune platformu. Nudi nam samo jedan tip profila kojeg možemo kreirati i postaviti za korištenje, samim time je puno jednostavniji za „setup“ od androida koji nudi jako puno opcija. Profil je osmišljen da bude kao „Fully Managed“, ali radi na principu „Work/Personal“ tako da korisnici su zadovoljni jer je jednostavnije za koristiti. Također je potrebno restrikcije postaviti i zahtjeve koji reguliraju mogućnosti spajanja na sustav. Najbitnije stavke su : PIN, vremenski zaključavanje

zaslona, jednostavne lozinke, verzija IOS-a i grupe korisnika. Slučaj kada se politika primjeni na korisnika koji nije u toj skupini uređaja nema posljedica jer ga smatra ne podržanim i samim time neće se moći pristupiti.

3.3 Fully Managed, dedicated, and corporate work profile

Ovaj tip profila nam govori da je poštuje samo prava svoje organizacije, odnosno da pripada svojoj organizaciji te da organizacija kompletno upravlja tim uređajem. Administrator u ovom slučaju kada pobriše uređaj sa konzole uređaj se briše na tvorničke postavke, dakle ima veći pristup resursima nego „Work/Personal profil“. Također uvjeti za „enrollment“ su minimalna verzija OS je 8.0 za 5 bitnih stavki putem kojih se može odraditi „Enrollment“ :

- NFC
- Token entry
- QR Code
- Zero Touch
- Knox Enrollment

Većina korisnika je više zadovoljnija sa ovim tipom profila jer vizualno ne predstavlja nikakvu promjenu na uređaju da osoba ima dodatan posao, nego naprotiv daje mogučnosti korisnicima na uvid korporativne stvari , a potom i privatne. Ovaj profil upravljanja poznat je kao i osobni profil u vlasništvu tvrtke, dakle značajna razlika u odnosu na osobni uređaj s radnim profilom je vlasništvo. Kada korisnik koristi ovaj uređaj sa ovim profilom, uređaj je u vlasništvu tvrtke.
Prednosti Fully Managed, profila :

- Potrebne aplikacije se instaliraju bez interakcije krajnjeg korisnika
- Sve od podataka je pohranjeno u ranom profilu
- Kontakti tvrtke se mogu pretraživati kroz Outlook aplikaciju, a dolazni brojevi se prepoznaju
- Prilikom nestanka uređaja od strane korisnika uređaj se može na daljinu obrisati na tvorničke postavke

3.3.1 Personally Owned – Work profile

Osobno – poslovni profil predstavlja uređaj u osobnom vlasništvu sa radnim performansama za upravljanje korporativnim podacima aplikacijama na Android uređajima u vlasništvu korisnika. Prema zadatim postavkama omogućena je registracija uređaja sa radnim profilom u osobnom vlasništvu pa nisu potrebne nikakve daljnje radnje. Da bih se konfiguriralo ograničenje platforme i dodijelilo ih se određenim grupama korisnika pristupa se resursu ograničenja upisa i blokiraju se upisi administratora. „Enrollment“ se odrađuje na način da se iz Trg. Play aplikacije skine „Company Portal“ i prijavi se na aplikaciju. Na osobnom uređaju nakon „Enrollmenta“ se pojavljuje posebni kružić pod nazivom radni profil gdje se pristupa svim radnim informacijama. Unutar radnog profila pohranjuju se sve poslovne informacije. Sve izvan radnog profila nije vidljivo platformi. Opseg između radnog i privatnog djela može se konfigurirati do određene razine.

Prednosti ovog profila su :

- Prilikom brisanja uređaja sa konzole samo nestaje radni profil
- Pravila zaštite aplikacija nisu potrebna, ali se mogu zaštititi
- Svi kontakti, podaci i aplikacije tvrtke su pohranjeni u radnom djelu
- Aplikacije se mogu instalirati bez interakcije krajnjeg korisnika

Nedostaci profila :

- Jedan radni profil se može izraditi po uređaju
- Kontakti iz Outlook aplikacije se ne mogu sinkronizirati sa osobnim kontaktima
- Komunikacija kroz Outlook aplikaciju zahtjeva puno interakcije korisnika za slanje privitaka
- Uređaji se često smrzavaju zbog promjene profila
- Feedback nije učinkovit

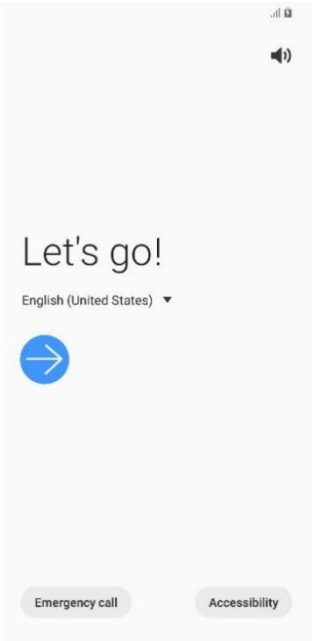
3.3.2 Corporate -OWNED Dedicated device

Android profil koji se sastoji od konfiguracije sa multi kiosk mogućnosti sa aplikacijom za udaljeno povezivanje. Korištenjem namjenskog profila djelatnici ne mogu sami dodavati aplikacije, mijenjati postavke, slikati niti ući u aplikaciju ako im nije pristup dozvoljen. Uređaji koji su kreirani sa ovim tipom profila nisu povezani sa korisnikom, tako da je za administraciju teže dokučiti tko ga koristiti, pa samim

time nisu namijenjeni za korištenje s aplikacijama za osobnu upotrebu. Ovaj profil je više namijenjen za uređaje koji se koriste sa aplikacijama koje nisu integrirane s načinom dijeljenog uređaja AAD-a kako bi se omogućila jednokratna prijava i odjava između korisnika i aplikacije. Kiosk uređaji se više koriste za ankete, ili pristupe samo jednom tipu resursa koji korisnik treba odrađivati.

3.3.3 Enrollment Proces Android Fully Managed Devices

- Uređaj mora biti na tvorničkim postavkama.
- 7 puta je potrebno taknuti sa prstom na bijelu površinu.

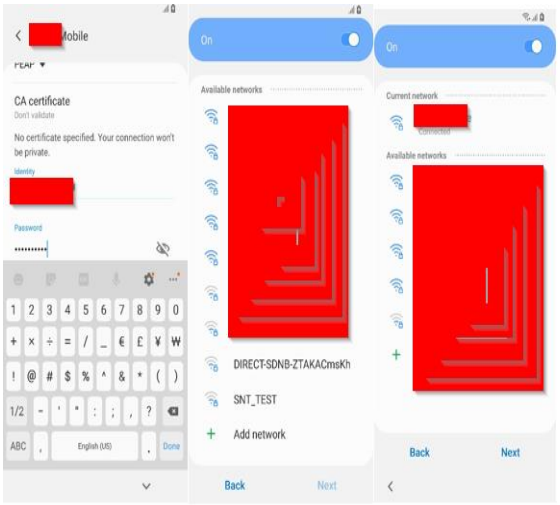


Slika 1. Početni zaslon

- Skenirati QR kod.

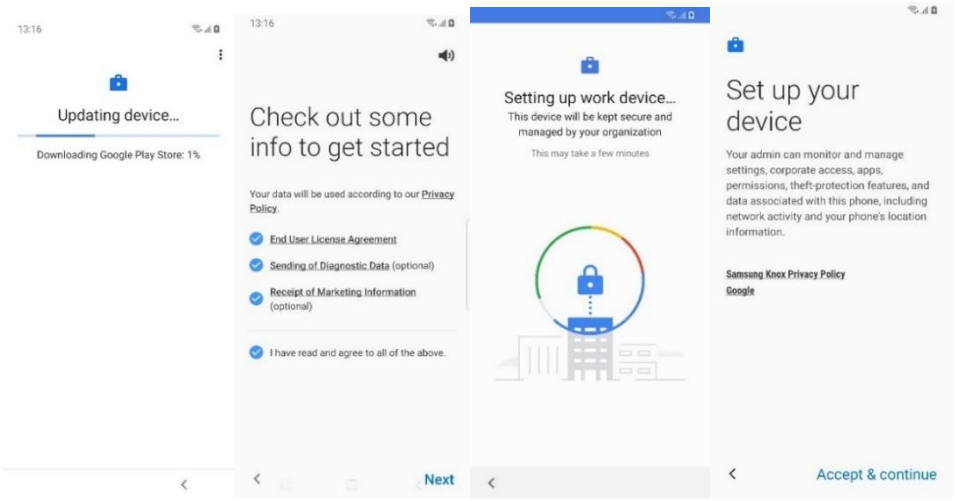
Slika 2. QR kod za skeniranje

- Odabrati mrežu za spajanje na Internet.



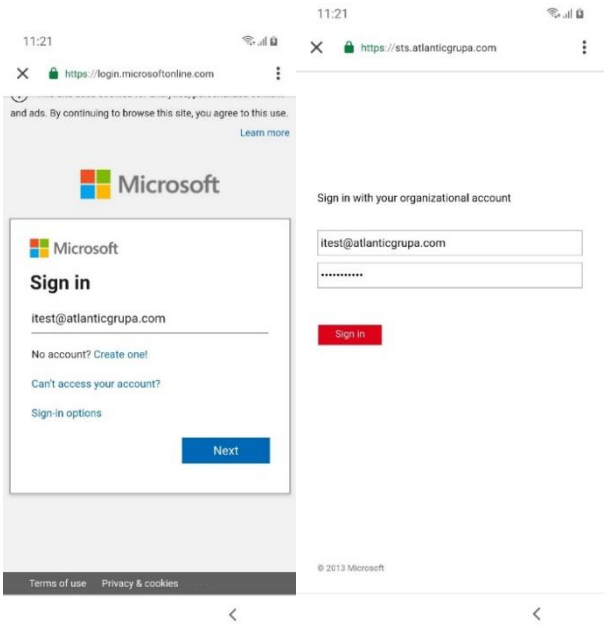
Slika 3. Pristup Wifi

- Ažurirati Google servis, prihvatiti odredbe za početak korištenja uređaja i krenuti u postavljanje poslovnog profila.



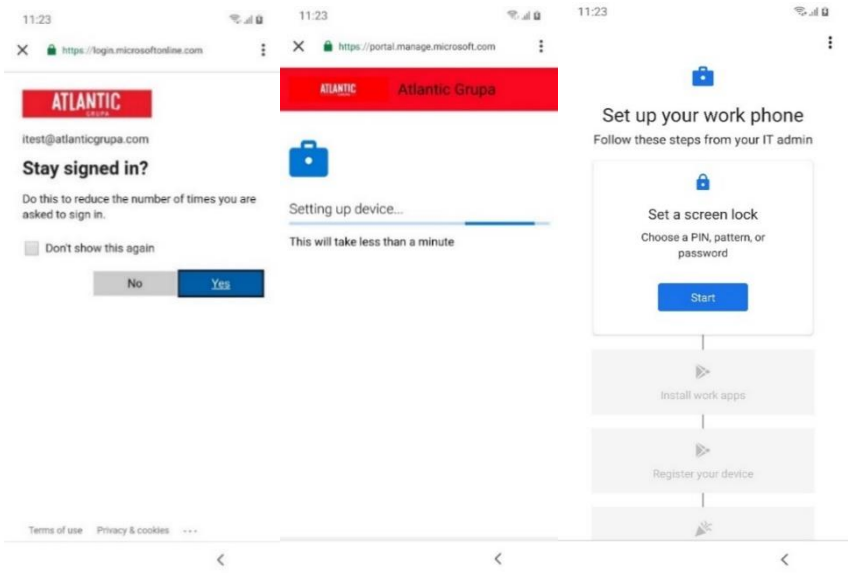
Slika 4. Google značajke

- Upisati korisničke podatke za prijavu.



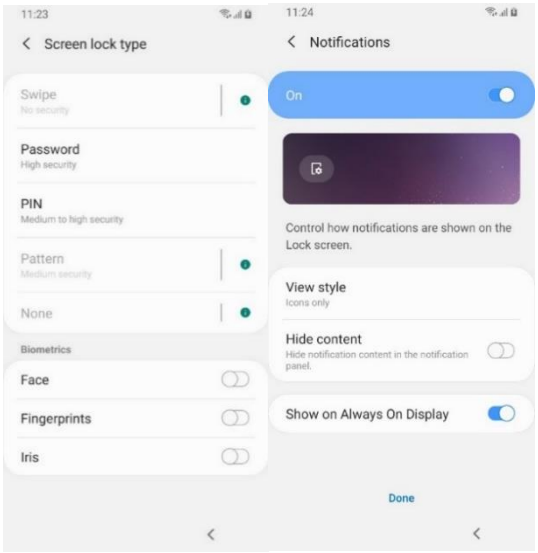
Slika 5. Upis korisničkih podataka

- Kliknuti na „Yes“ , pritisnuti „Start“ i „Enrollment“ proces se pokreče sa provedbom korporativnih pravila.



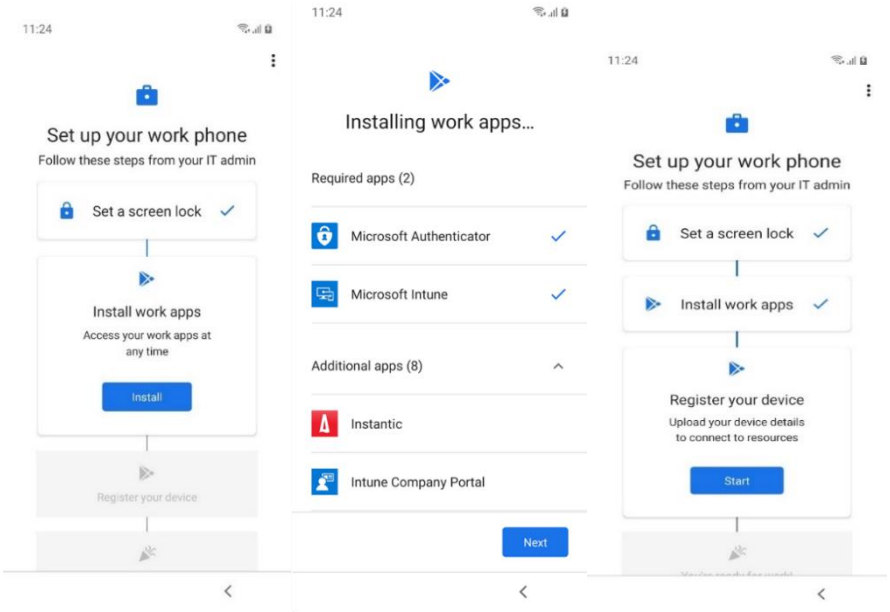
Slika 6. Postavke poslovnog profila

- Korisniku će se putanja preusmjeriti za postavljanje PIN-a, lozinke ili neke druge autentifikacije.



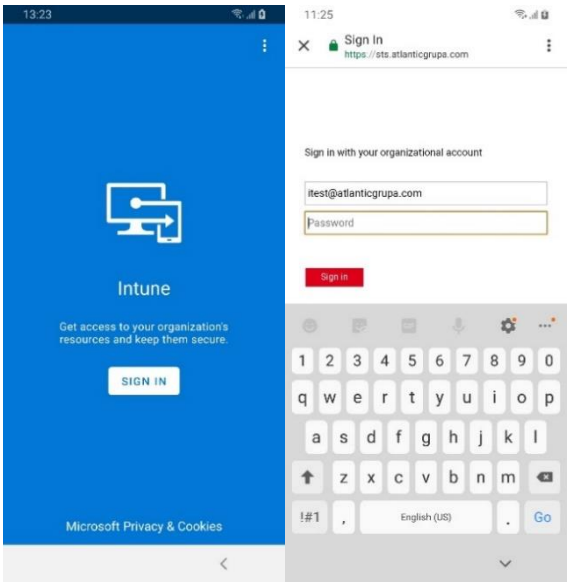
Slika 7. Postavljanje lozinke

- Instaliranjem službenog djela profila, omogućen je uvid u organizacijske aplikacije. Pritisnuti „Start opciju za registraciju uređaja.



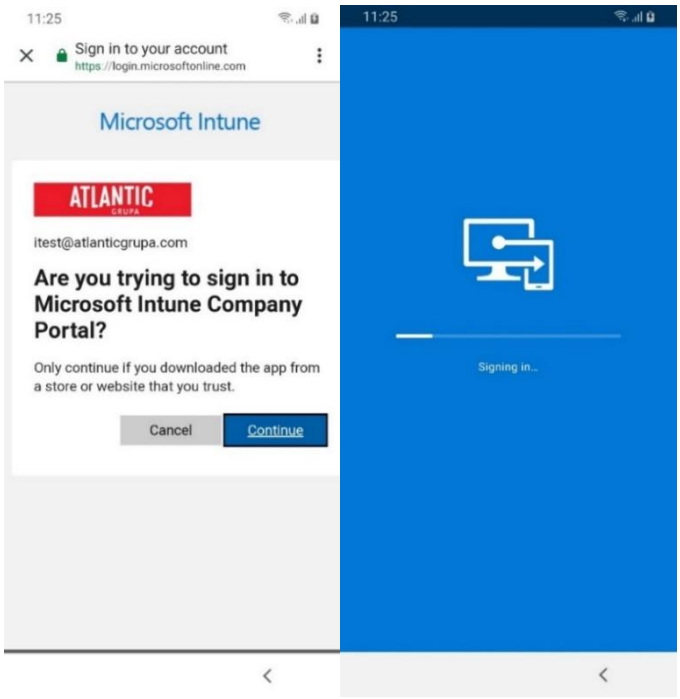
Slika 8. Instalacija poslovnih aplikacija

- Pristupi Intune konzoli sa korisničkim podacima.



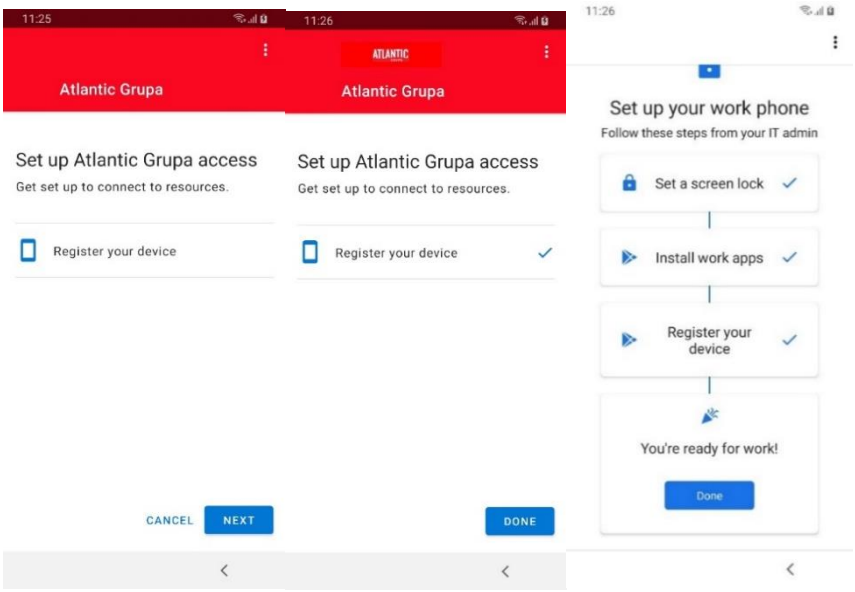
Slika 9. Autentifikacija

- Odabrati „Continue“ za pristup i prijavu na sustav.



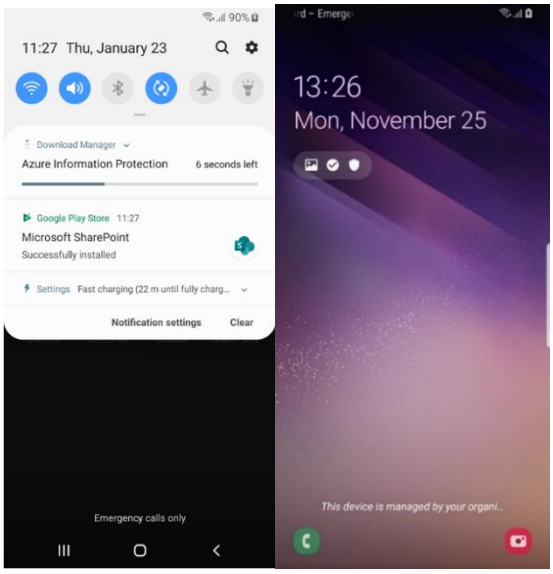
Slika 10. Pristup Intune portalu

- Odraditi registraciju uređaja „Next“ & „Done“.



Slika 11. Potvrda spajanja

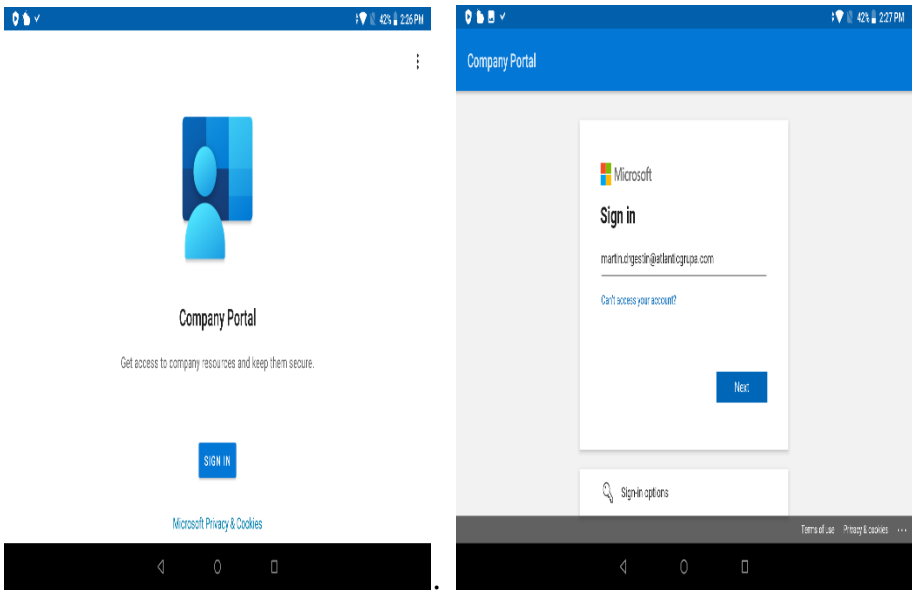
- Nakon instalacije poslovnog profila, instalirati će se sve aplikacije koje je organizacija omogućila. Korisnik može primjetiti na dnu ekrana da tvrtka upravlja uređajem nakon procesa koji je odrađen.



Slika 12. Gotovo

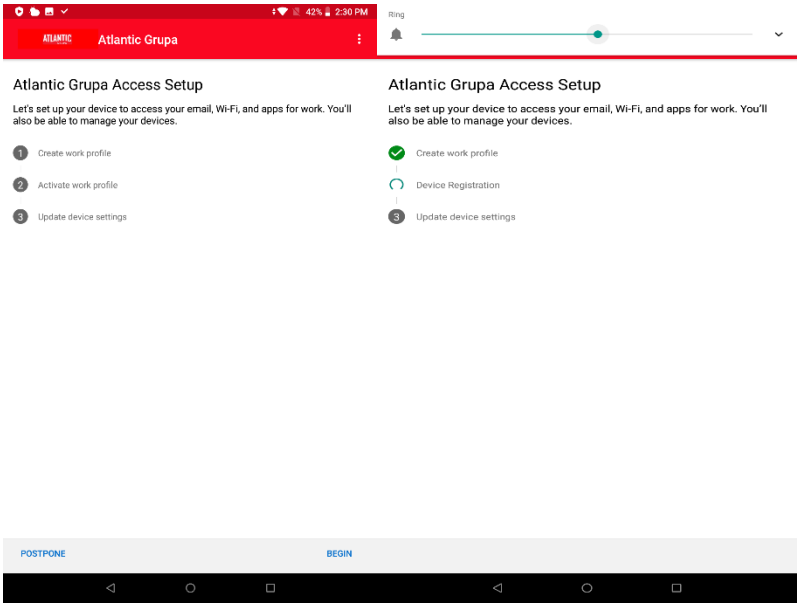
3.3.4 Android CP

- Potrebno je pristupiti na Trgovini Play i preuzeti aplikaciju „Company Portal“, zatim se ulogirati sa korisničkim podacima u aplikaciju.



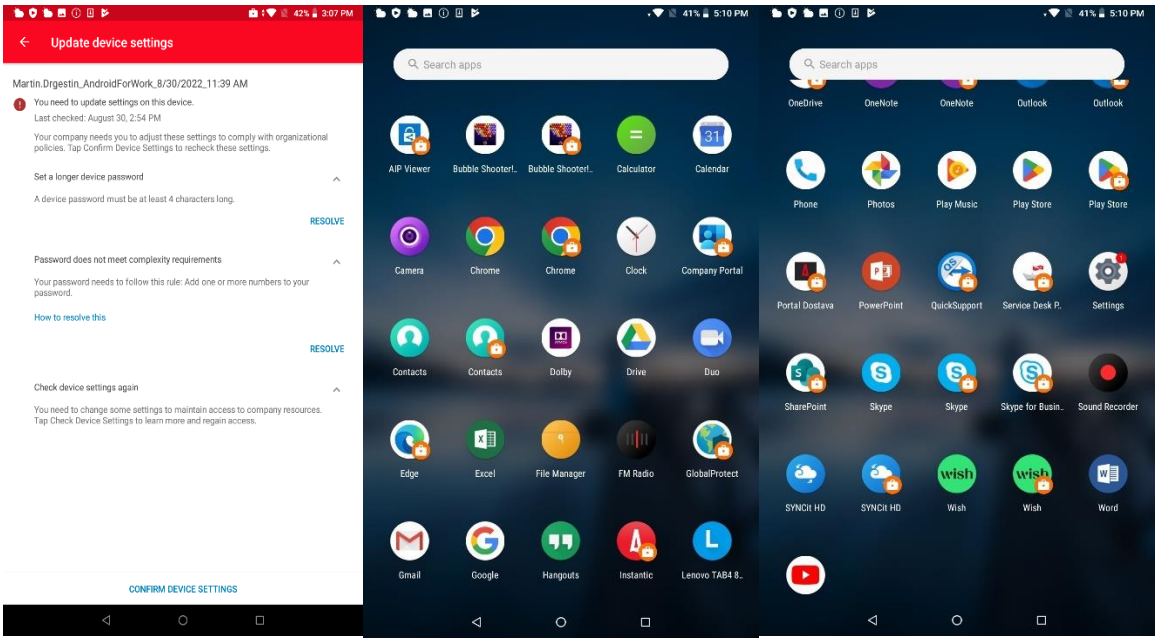
Slika 13. Pristup Konzoli

- Pokrenuti instalaciju službenog profila na uređaj, instalirati certifikat koji se nudi za preuzimanje.



Slika 14. Uvid u značajke sustava

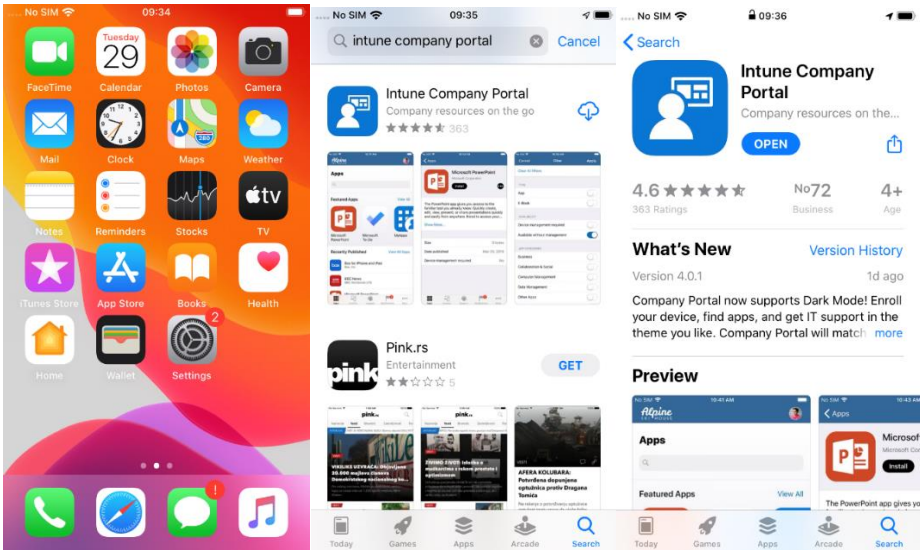
- Postaviti PIN za zaključavanje zaslona, registrirati se korisničkim podacima i ažurirati postavke uređaja za spajanje na sustav. Nakon obavljenog „Enrollment-a“ počinju se spuštati ikone sa „koferom“ koja označava da je aplikacija službeno instalirana na uređaju.



Slika 15. Izgled CP

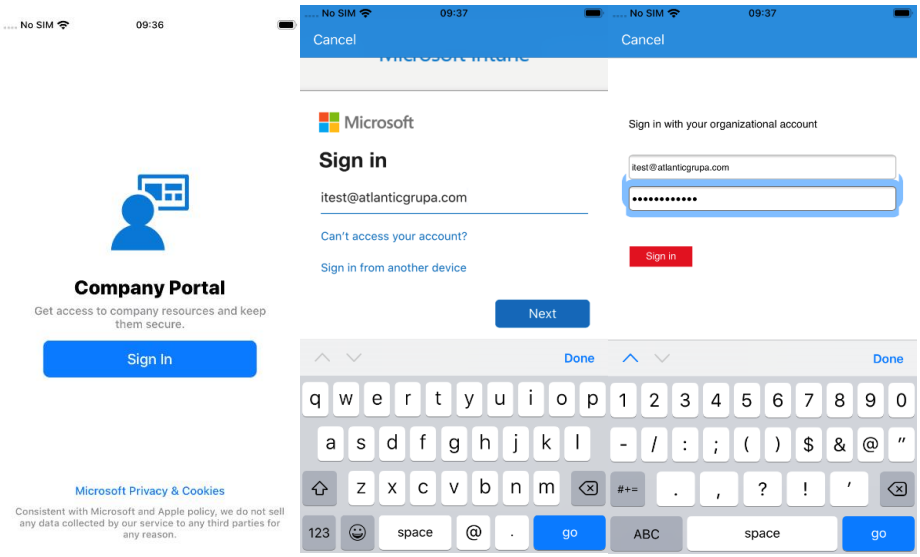
3.3.5 Ios Enrollment

- Instalirati u „App Store-u“ Intune Company Portal aplikaciju.



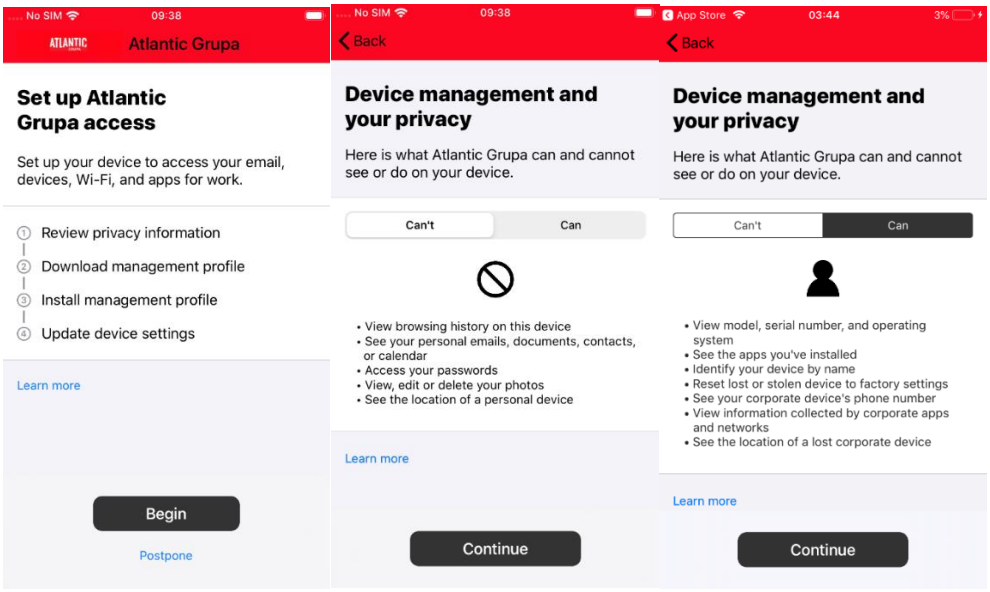
Slika 16. Instalacija aplikacije

- Prijaviti se u aplikaciju sa korisničkim podacima



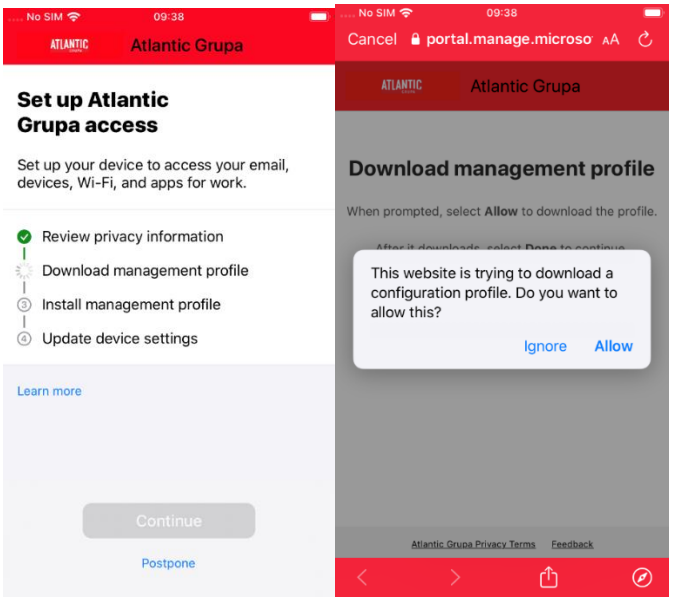
Slika 17. Pristup konzoli

- Krenuti u pripremu profila i stisnuti „Begin“.
- Provjeriti sve što tvrtka ima uvid u telefonu kada se profil instalira.



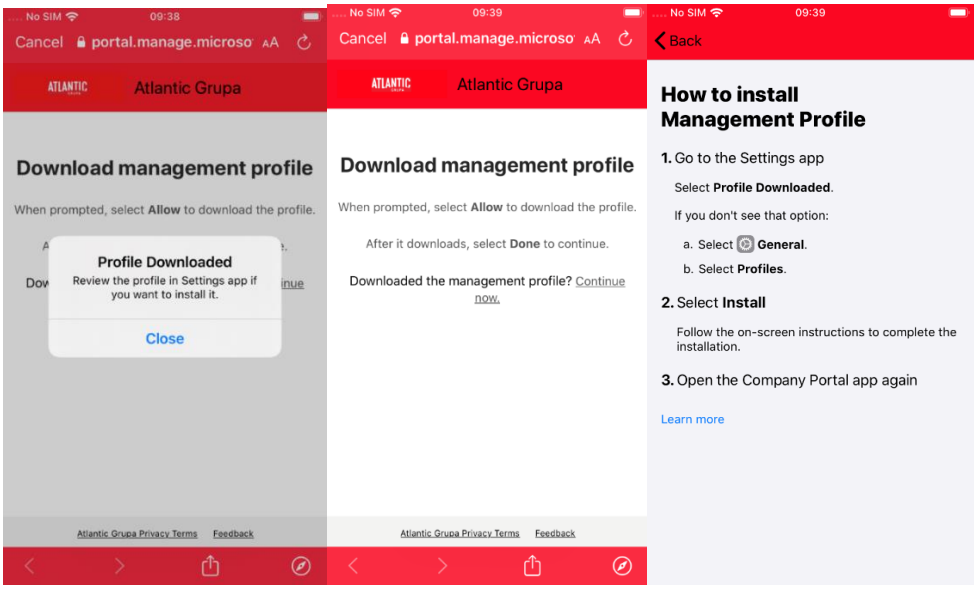
Slika 18. Uvid u značajke sustava

- Instalirati „Management Profil“

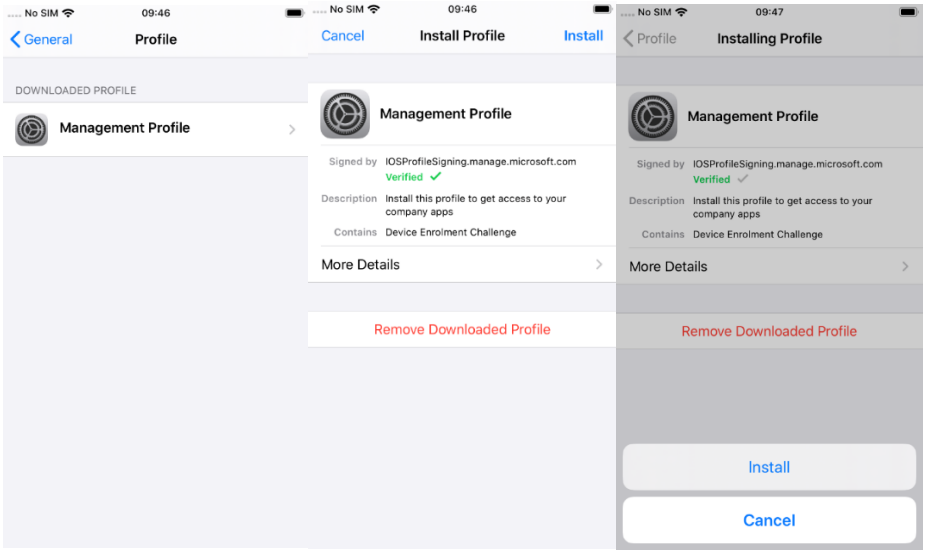


Slika 19. Instalacija profila

- Odabrati opciju zatvori, skinuti navedeni profil i instalirati ga.

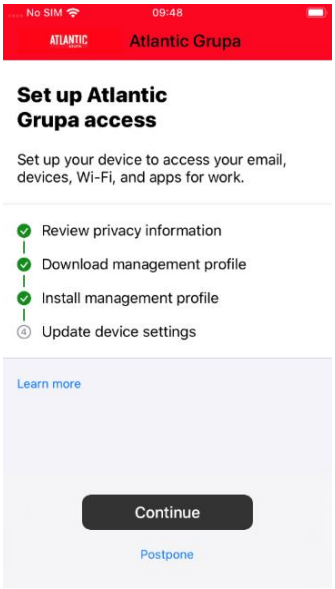


Slika 20. Skidanje i potvrđivanje profila



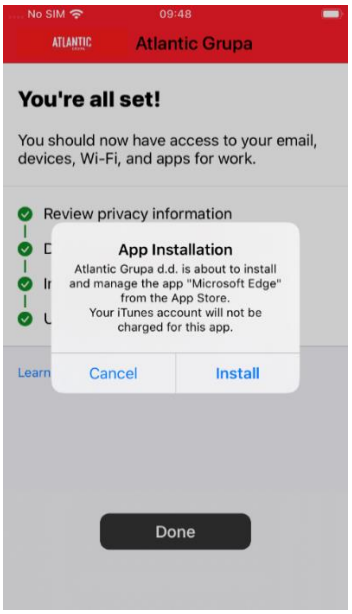
Slika 21. Instalacija M. profila

- „Continue“



Slika 22. Pristup korporativnim resursima

- Dozvoliti instalaciju aplikacija koje organizacija spušta na uređaj.



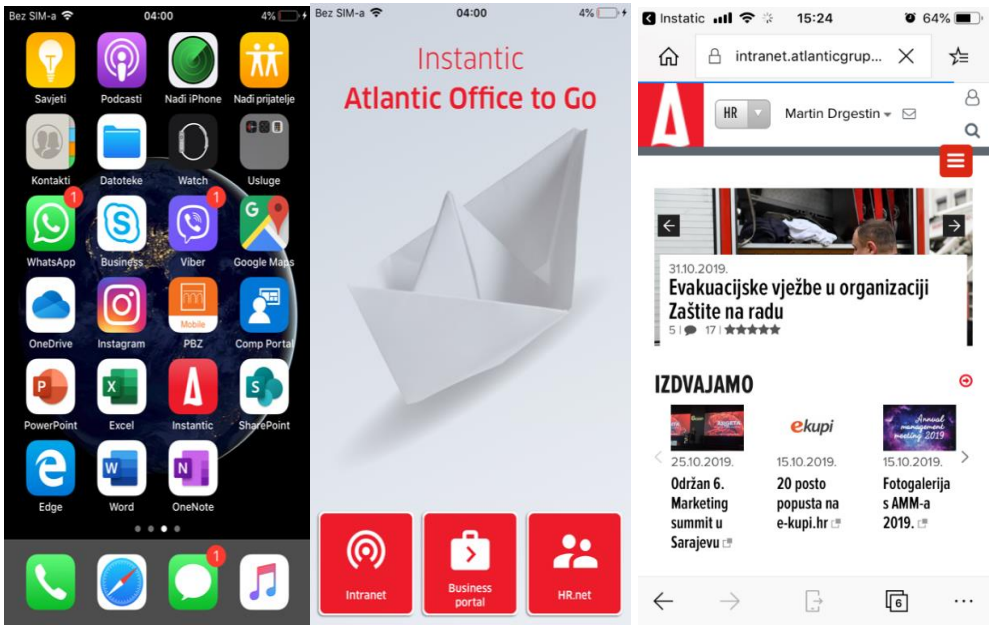
Slika 23. Instalacija aplikacija

- Postaviti lozinku na uređaj

Slika 24.Unos lozinke

- Instantic Aplikacije

Korisnici mogu pristupiti korporativnim aplikacijama koje smo omogućili kroz „Instantic“ sa svojim korisničkim podacima.



Slika 25. Pristup korporativnim aplikacijama

4. ZAKLJUČAK

Sigurnost informacijskih sustava za svaku kompaniju je vrlo važna kako ne bih došlo do krađe dokumenata što osobnih i poslovnih, te sprečavanje mogućih napada na informacijske sustave. Financijskom analizom kroz određeni period korištenja MDM sustava može se primijetiti benefiti koje doprinosi. Jedni od tih su veći angažman korisnika u svom svakodnevnom radu, što daje veću fokusiranost osobe na svoj posao, sigurnost od krađe identiteta sa primjenom sigurnosnih aplikacija, smanjenje troškova uređaja sa primjenom 2u1 uređaj i administratorski benefit koji daje samom administratoru mogućnost fokusa na konkretne stvari. Alat nudi još puno performansi za ostali tip uređaja koji može omogućiti vidljivost potrošnju resursa na računalu, udaljenu podršku, broj aplikacija, spuštanje aplikacija i praćenje statusa ažuriranja. Imamo mogućnost slaganja profila koji se služi za projekte i komunikaciju između projektnog tima. Praćenjem noviteta primijećeno je da ovakav alat se sve više počinje koristiti tako da sami vanjski partneri unapređuju i ažuriraju mogućnosti rada u istom. Proces „Enrollment-a“ po korisniku traje 10 do 20 minuta sa naknadnim spuštanjem aplikacija.

Prema svemu sudeći ovakav tip rješenja za bilo koju tvrtku je dobar i može samo doprinijeti veću sigurnost samih korisnika i organizacije. Danas već proizvođači nude „zaštićene telefone“ koje je samo potrebno aktivirati sa organizacijskim podacima korisnika.

Atlantic Grupa je prva u nizu kompanija sa ovih područja koja je implementirala ovo rješenje koje je doprinijelo značajan pomak u praćenju informacijskih tehnologija i daljnjem razvijanju istih.

Organizacije koje su u rastu broja zaposlenih bih svakako trebali gledati nova rješenja koja se nude jer se tehnologije razvijaju i tvrtke koje ne prate razvoj mogu vrlo brzo propasti, jer samom automatizacijom tvrtke postižu veći fokus na konkretne stvari i traženju boljih rješenja za poslovne procese koje su im „core“. Tvrtke koje ne prate razvoj dođu u situaciju da imaju previše troškova zbog gubljenja vremena i radnih snaga na procese koji su manje bitni, a iziskuju puno vremena.

Stoga svakako je bitno pratiti tržišta i razvoj kako bih opstali i nastavili poslovanje sa širenjem distribucije, prodaje i proizvodnje. Ulaganjem u poslovne inteligencije i ljude, tvrtke rastu i razvijaju se što doprinosi zadovoljstvo svima.

5. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Martin Drgestin

Matični broj studenta: 0234059434

Naslov rada: Napredna organizacijska rješenja usluge nadzora mobilnih uređaja i aplikacija putem oblaka, na primjeru koncepta „Mobile Device Management-Intune“

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem i plagiranjem sadržaja. Prilikom izrade rada koristio sam materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio. 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.
Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum	Potpis studenta
_____	_____

6. POPIS LITERATURE

a. KNJIGE; ČLANCI

1. Šimović, V. (2010) *Uvod u informacijske sustave, 2. dopunjeno i izmijenjeno izdanje*. Zagreb: Tehnička knjiga.
2. Šimović, Vladimir, Maja Ružić-Baf, *Suvremeni informacijski sustavi*, Sveučilište Jurja Dobrile u Puli, Pula, 2013.

b. INTERNETSKI IZVORI

3. Microsoft Intune :https://docs.microsoft.com/en-us/mem/intune/
4. Endpoint Manager: https://www.techtarget.com/searchitchannel/definition/Microsoft-Intune
5. Device administration preuzeto https://query.prod.cms.rt.microsoft.com/cms/api/am/binary
6. Korporativni izvori

7. POPIS SLIKA

Slika 1. Početni zaslon 13
Slika 2. QR kod za skeniranje 13
Slika 3. Pristup Wifi 14
Slika 4. Google značajke 14
Slika 5. Upis korisničkih podataka 15
Slika 6. Postavke poslovnog profila 15
Slika 7. Postavljanje lozinke 16
Slika 8. Instalacija poslovnih aplikacija 16
Slika 9. Autentifikacija 17
Slika 10. Pristup Intune portalu 17
Slika 11. Potvrda spajanja 18
Slika 12. Gotovo 18
Slika 13. Pristup Konzoli 19
Slika 14. Uvid u značajke sustava 19
Slika 15. Izgled CP 20
Slika 16. Instalacija aplikacije 20
Slika 17. Pristup konzoli 21
Slika 18. Uvid u značajke sustava 21
Slika 19. Instalacija profila 22
Slika 20. Skidanje i potvrđivanje profila 22
Slika 21. Instalacija M. profila 23
Slika 22. Pristup korporativnim resursima 23
Slika 23. Instalacija aplikacija 24
Slika 24. Unos lozinke 24

8. ŽIVOTOPIS

Europass

Osobni podaci

Ime / Prezime	**Martin Drgestin**
Adresa	Savska Opatovina 22, Zagreb
Telefonski broj	Mob: +385 912413275
E-mail	Shpzgb2@gmail.com
Državljanstvo	Hrvatsko
Datum rođenja	11. Prosinac 1995, Zagreb
Spol	Muški

Radno iskustvo

Datumi	2.3.2015 – trenutno zaposlen
Zanimanje ili radno mjesto	IT Administrator
Glavni poslovi i odgovornosti	- Konfiguracija mrežne opreme - Izrada plana zamjene korisničke opreme - Zamjena korisničke opreme starije od 5 godina - Zamjena skladišne opreme - Konfiguriranje SCCM-a
Naziv poslodavca	Atlantic Grupa d.d.
Vrsta djelatnosti ili sektor	Distribucija, Prozvodnja

Obrazovanje i osposobljavanje

Datumi	2010 g. – 2014. g
Naziv dodijeljene kvalifikacije / zvanje	Elektrotehničar
Glavni predmeti / stečene profesionalne vještine	Stečene vještine na području računalstva i elektrotehnike
Naziv i vrsta ustanove pružatelja obrazovanja i osposobljavanja	Elektrotehnička Škola Zagreb, Konavoska 2

Razina prema nacionalnoj ili međunarodnoj klasifikaciji	Srednja stručna sprema
Datumi	Rujan 2010. – Lipanj 2014.
Naziv dodijeljene kvalifikacije / zvanje	Elektrotehnika/ Cisco
Glavni predmeti / stečene profesionalne vještine	Uvod u mrežne tehnologije CISCO Elektrotehnička škola konavoska 2.
Naziv i vrsta ustanove pružatelja Obrazovanja i osposobljavanja	Cisco Akademija
Razina prema nacionalnoj ili međunarodnoj klasifikaciji	

Osobne vještine i kompetencije

Rad na računalu

Napredni rada na računalu

Materinski jezik **Hrvatski**

Drugi jezik(ci) **Engleski**

Samoprocjena	**Razumijevanje**		**Govor**		**Pisanje**
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
Engleski jezik	Odlično	Odlično	Odlično	Odlično	Odlično

Napomena

Nakon završetka srednje škole u kojoj sam pohađao Cisco akademiju za mreže , završio sam edukaciju za IT administratora u Algebra veleučilištu. Trenutno studiram na Veleučilištu Baltazar smjer informacijske tehnologije i radim u Atlantic Grupi kao IT administrator sa dodatnim mrežnim provedbama unutar kompanije. Završio sam unutar osnovnog obrazovanja 7. stupanj SOVA programa za učenje stranog jezika. U sklopu rada u trenutnoj kompaniji položio sam ITIL certifikate za poslovanje, Microsoft Azure certifikat za upravljanje portalom i Powershell administraciju.