VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

# MDM systémy pre vzdialenú správu Windows zariadení

MDM systems for Remote Management of Windows Devices

Kevin Mikler

Bakalárska práca

Vedoucí práce : Ing. Lukáš Kapičák

Ostrava, 2021

# Poďakovanie

Rád by som poďakoval vedúcemu bakalárskej práce Ing. Lukášovi Kapičákovi za odbornú pomoc a konzultácie pri vytváraní tejto bakalárskej práce.

# Abstrakt

Táto bakalárska práca sa zaoberá zoznámením sa a porovnaním platforiem pre vzdialenú správu zariadení s operačným systémom Windows. Cieľom práce je porovnanie vybraných riešení z pohľadu efektivity, možností konfigurácie a administrácie. Úlohou teoretickej časti je zoznámiť čitateľa s problematikou vzdialenej správy zariadení. Ďalej nasleduje predstavenie niekoľkých platforiem použiteľných pre správu Windows zariadení ktorými sú SOTI MobiControl, Manageengine MDM, Samsung Knox, Miradore, Safetica a Hexnode MDM. V praktickej časti je popísaný poustup inštalácie, pridanie klientov a administrácia prostredí SOTI MobiControl a Manageengine MDM. Po dôkladnom otestovaní dvoch platforiem nasleduje stručný popis, vlastnosti, konfigurácia, metodika a jednotlivé testy. V závere sa ešte venujem subjektívnemu porovnaniu nástrojov použitých pre správu mobilných zariadení.



# Kľúčové slová

MDM; Windows; SOTI; Manageengine; Knox; Hexnode; Miradore; Safetica; Vzdialená kontrola; Distribúcia softvéru

# Abstract

This bachelor thesis deals with the acquitance and comparrison of platforms for remote device management for operating system Windows. The main goal of this thesis is comparison of selected solutions in terms of efficiency, configuration options and administration. The main purpose of the theoretical part is to introduce the reader to the topic of remote device management. The following is a introduction of several platforms usable for Windows management such as SOTI MobiContol, Manageengine MDM, Samsung Knox, Miradore, Safetica, and Hexnode MDM. The practical part describes the installation process, enrolling clients, and administrating platforms SOTI MobiControl and Manageengine MDM environments. After thorough testing of the two platforms follows a biref description, environment configuration, methodology of features and a few individual tests. At the end is a subjective comparison of tools used for mobile device management.



# Key words

MDM; Windows; SOTI; Manageengine; Knox; Hexnode; Miradore; Safetica; Remote control; Software distribution

# Obsah


Úvod ..... - 11 -

1 Úvod do MDM ..... - 12 -

1.1 Princíp fungovania MDM ..... - 12 -

1.2 Kontrola a ochrana údajov ..... - 12 -

1.3 Použitie MDM vo firemnom prostredí ..... - 12 -

1.4 Hlavné funkcie MDM pre Windows ..... - 13 -

1.4.1 Profily a skupiny zariadení ..... - 13 -

1.4.2 Blacklist a Whitelist ..... - 13 -

1.4.3 Sledovanie polohy ..... - 13 -

1.4.4 Vzdialené vymazanie, reštart a skenovanie ..... - 14 -

1.4.5 Distribúcia softvéru a súborov ..... - 14 -

1.4.6 Uzamknutie a kontrola ..... - 14 -

2 Implementácia MDM ..... - 15 -

2.1 Správa zariadení ..... - 15 -

2.2 Softvérové platformy ..... - 15 -

2.3 Cloud a On.premises riešenia ..... - 15 -

2.4 Kontajnerizácia ..... - 15 -

2.5 Zabezpečenie ..... - 16 -

2.5.1 Zabezpečený katalóg aplikácií ..... - 16 -

2.5.2 Zabezpečený prehliadač ..... - 16 -

2.5.3 Zabezpečený e-mail ..... - 16 -

2.5.4 Zabezpečené dokumenty ..... - 16 -

2.6 OTA Programovanie ..... - 16 -

3 Prehľad MDM riešení použiteľných pre systém Windows ..... - 17 -

3.1 Manageengine MDM ..... - 17 -

3.2 Hexnode MDM ..... - 18 -

3.3 Safetica ..... - 20 -

3.4 Knox Manage ..... - 21 -

3.5 Miradore MDM ..... - 22 -

3.6 SOTI MobiControl ..... - 23 -

3.7 Porovnanie služieb MDM prostredí ..... - 24 -

4 Testovanie prostredia SOTI MobiControl ..... - 25 -
4.1 Systémové požiadavky ..... - 25 -
4.2 Prerekvizity inštalácie ..... - 26 -
4.2.1 Microsoft .Net core ..... - 26 -
4.2.2 Java SE ..... - 27 -
4.2.3 Microsoft SQL server 2019 Express ..... - 27 -
4.3 Postup inštalácie ..... - 27 -
4.4 Zoznámenie sa s prostredím ..... - 30 -
4.5 Nasadenie prostredia na klientské počítače ..... - 32 -
4.6 Testovanie funkcií MDM prostredia na nasadených zariadeniach ..... - 33 -
4.6.1 Vzdialená kontrola nad zariadením ..... - 33 -
4.6.2 Odosielanie správ ..... - 34 -
4.6.3 Distribúcia Softvéru ..... - 35 -
4.6.4 Vzdialený reštart ..... - 36 -
4.6.5 BitLocker ..... - 36 -
4.7 Zhodnotenie testovania ..... - 37 -
5 Testovanie prostredia Manageengine MDM ..... - 38 -
5.1 Systémové požiadavky ..... - 38 -
5.2 Postup inštalácie ..... - 40 -
5.3 Zoznámenie sa s prostredím ..... - 42 -
5.3.1 Manageengine ServiceDesk Plus ..... - 42 -
5.3.2 Manageengine Desktop Central ..... - 43 -
5.3.3 Manageengine Mobile Device Manager Plus ..... - 45 -
5.4 Nasadenie prostredia na klientské počítače ..... - 46 -
5.5 Testovanie funkcií MDM na nasadených zariadeniach ..... - 47 -
5.5.1 Vzdialená kontrola nad zariadením ..... - 47 -
5.5.2 Blacklist a Whitelist ..... - 48 -
5.5.3 Chatové okno ..... - 49 -
5.5.4 Distribúcia softvéru ..... - 49 -
5.5.5 Vzdialený reštart ..... - 50 -
5.5.6 Systémový správca ..... - 51 -
5.6 Zhodnotenie testovania ..... - 52 -
6 Porovnanie testovaných MDM prostredí ..... - 53 -

6.1 Systémové požiadavky ..... - 53 -
6.2 Zložitosť správy MDM ..... - 53 -
6.3 Odozva pri vykonaní zmien ..... - 53 -
6.4 Výhody a nevýhody testovaných prostredí ..... - 54 -
Záver ..... - 55 -
Použitá literatúra ..... - 56 -

# Zoznam použitých skratiek

| Zkratka | Význam |
|---|---|
| **MDM** | Mobile Device Management |
| **EMM** | Mobile Device Management |
| **UEM** | Unified Endpoint Management |
| **IOT** | Internet of things |
| **POS** | Point of sale |
| **BYOD** | Bring your own device |
| **OTA** | Over the air |
| **IT** | Information Technologies |
| **IMEI** | International Mobile Equipment Identify |
| **IMSI** | International Mobile Subscriber Identify |
| **APP** | Application |
| **SaaS** | Software as a Service |
| **VPN** | Virtual private network |
| **DLP** | Data loss protection |
| **AD** | Active Directory |
| **RDP** | Remote Desktop Protocol |
| **VM** | Virtual Machine |
| **OS** | Operation Systém |
| **HTTP** | Hypertext Transfer Ptotocol |
| **HTTPS** | Hypertext Transfer Ptotocol Secure |
| **CLI** | Command Line Input |
| **SDK** | Software Development Kit |
| **SD** | Secure Digital |
| **URL** | Uniform Resource Locator |
| **AES** | Advanced Encryption Standard |

# Zoznam obrázkov

*Obrázok 1: Registračný formulár- 27 -*
*Obrázok 2: Zoznam sofvéru na stiahnutie - 27 -*
*Obrázok 3: Ponuka súčastí při inštalácií - 27 -*
*Obrázok 4: Výber SQL serveru - 27 -*
*Obrázok 5: Zadanie licenčného kódu - 30 -*
*Obrázok 6: Prihlasovací formulár - 30 -*
*Obrázok 7: Prehľadová obrazovka SOTI MobiControl - 30 -*
*Obrázok 8: Nahrávanie balíčkov na server - 30 -*
*Obrázok 9: Výber balíčkov pri nahrávaní - 30 -*
*Obrázok 10: Vytvorenie pravidla při nasadení - 32 -*
*Obrázok 11: Vytvorenie inštalačného súboru - 32 -*
*Obrázok 12: Výber metódy nasadenia - 32 -*
*Obrázok 13: Špecifikácia balíčkov pri nasadení - 32 -*
*Obrázok 14: Ponuka akcií vykonateľných na zariadení - 33 -*
*Obrázok 15: Okno vzdialenej kontroly and zariadením prostredia SOTI MobiControl - 34 -*
*Obrázok 16: Formulár na odosielanie správ - 34 -*
*Obrázok 17: Výpis správy na spravovanom zariadení - 34 -*
*Obrázok 18: Vytvorenie balíčku - 35 -*
*Obrázok 19: Nahranie inšatalčného súboru do balíčku - 35 -*
*Obrázok 20: Priradenie profilu pre distribúciu softvéru - 35 -*
*Obrázok 21: Dotaz k inštalácií softvéru na spravovanom zariadení - 36 -*
*Obrázok 22: Kiosk obrazovka v administrátorskom režime - 36 -*
*Obrázok 23: Kiosk obrazovka v používateľskom režime - 36 -*
*Obrázok 24: Výber verzie platformy - 40 -*
*Obrázok 25: Výber portu - 40 -*
*Obrázok 26: Ponuka inštalácie a konfigurácie Mobile Device Manager - 40 -*
*Obrázok 27: Ponuka inštalácie a konfigurácie Desktop Cenral - 40 -*
*Obrázok 28: Generácia API kľúča - 42 -*
*Obrázok 29: Synchronizácia Desktop Central aplikácie so ServiceDesk - 42 -*
*Obrázok 30: náhľad úvodnej obrazovky a záložiek ServiceDesk Plus - 42 -*
*Obrázok 31: Úvodná obrazovka aplikácie Desktop Central - 43 -*
*Obrázok 32: Rozhranie Inventory Desktop Central - 43 -*
*Obrázok 33: Rozhranie inventory MDM plus - 45 -*
*Obrázok 34: Ponuka stiahnutia inštalačného súboru - 46 -*
*Obrázok 35: Hláška po úspešnom nasadení prostredia - 46 -*
*Obrázok 36: Okno vzdialenej kontroly nad zariadením - 47 -*
*Obrázok 37: Rozhrane pre aplikáciu Blacklistu a Whitelistu - 47 -*
*Obrázok 38: Hlásenie zablokovane aplikácie - 47 -*
*Obrázek 39: Chatové okno medzi používateľom a administrátorom - 49 -*
*Obrázok 40: Vytvorenie balíčku v Desktop Central - 49 -*
*Obrázok 41: Vytvorenie a nasadenie konfihurácie - 49 -*

*Obrázok 42: Rozhranie pre sledovanie pre sledovanie stavu konfigurácií - 49 -*
*Obrázok 43: Vytvorenie príkazu na reštart - 50 -*
*Obrázok 44: Varovné okno pred reštartom - 50 -*
*Obrázok 45: Rozhranie pre správu systému - 51 -*

# Zoznam tabuliek

*Tabuľka 1: porovnávacia tabuľka MDM prostredí - 24 -*
*Tabuľka 2: Systémové požiadavky SOTI MobiControl pre administrátorský počítač - 25 -*
*Tabuľka 3: Systémové požiadavky SOTI MobiControl pre klientský počítač - 25 -*
*Tabuľka 4: Zoznam portov potrebných pre komunikáciu SOTI MobiControl - 25 -*
*Tabuľka 5: Systémové požiadavky Manegeengine MDM pre klienský počítač - 38 -*
*Tabuľka 6: Systémové požiadavky Manageengine MDM pre administrátorský počítač - 38 -*
*Tabuľka 7: Zoznam portov potrebných pre komunikáciu Manageengine MDM - 38 -*

# Úvod

V posledných rokoch sa potreba využitia informačných technológií vo firemnom prostredí výrazne zvýšila. S touto potrebou bolo nutné vyriešiť problém so správou neustále narasatúceho počtu zariadení vo firmách a zároveň zachovať bezpečnosť firemných dát. Vzhľadom na aktuálnu situáciu a povinnosť zamestnancov pracovať z domu je využitie vzdialenej správy mobilných zariadení v mnohých prípadoch nevynutné.

Bakalárska práca je zameraná na uvedenie čiateľa do problematiky vzdialenej správy zariadení s operačným systémom Windows, predstavenie niekoľkých platforiem podporujúcich tento operačný systém, demonštrácia ich inštalácie, konfigurácie a ich využitia v praxi.

Prvá kapitola obsahuje teoretický popis princípu fungovania prostredí pre vzdialenú správu mobilných zariadení a funkciách, ktoré tieto prostredia poskytujú. Ďalej je v tejto kapitole objasnený princíp nasadenia prostredia na súkromné zariadenia zamestnancov a ich kontroly.

Druhá kapitola obsahuje popis princípu vzdialenej správy zariadení, rozdielov medzi miestnym alebo cloudovým serverom, zabezpečením firemných údajov a postupom zablokovania a vymazania v prípade odcudzenia zariadenia obsahujúceho firemné údaje.

Tretia kapitola obsahuje predstavenie šiestich platforiem vhodných pre systém Windows. Pri každom systéme sú uvedené služby, ktoré poskytuje. Na konci kapitoly sa nachádza tabuľka obsahujúca porovnanie funkcií poskytovaných jednotlivými prostrediami.

Štvrtá kapitola obsahuje postup inštalácie, konfugirácie a použitia prvého testovanéno prostredia pre správu mobilných zariadení SOTI MobiControl zahŕňajúca systémové požiadavky, dokumentáciu inštalácie a nasadenia prostredia na spravované zariadenie a návod na použitie jeho základných funkcií.

Piata kapitola obsahuje postup inštalácie, konfigurácie a použitia druhého testovaného prostredia pre správu mobilných zariadení Manageengine MDM zahŕňajúca systémové požiadavky, dokumentáciu inštalácie a nasadenia prostredia na spravované zariadenie a návod na použitie jeho základných funkcií.

Šiesta kapitola obsahuje porovnanie poznatkov zistených pri testovaní dvoch MDM prostredí z hľadiska zložitosti administrácie prostredia, náročnosti na systémové požiadavky a ich využiteľnosť v praxi.

Záver obsahuje zhodnotenie dosiahnutých výsledkov a poznatkov, získaných počas testnovania jednotlivých MDM prostredí.

# 1 Úvod do MDM

Mobile device management alebo MDM je priemyselný názov pre správu mobilných zariadení, ako sú napríklad smartfóny, tablety a notebooky. MDM je zvyčajne implementované prostredníctvom predpripraveného prostredia, ktoré obsahuje funkcie správy pre produkty konkrétnych dodávateľov mobilných zariadení. MDM úzko súvisí so správou podnikovej mobility (EMM) a jednotnou správou koncových bodov (UEM). Na rozdiel od MDM, EMM poskytuje správu mobilných informácií, správu mobilných aplikácií a správu mobilného obsahu. UEM poskytuje správu koncových zariadení ako sú desktopy, IoT (Internet Of Things) zariadenia, tlačiarne a podobne[1].

## 1.1 Princíp fungovania MDM

Účelom MDM je nahradiť fyzickú prítomnosť administrátora pri každom spravovanom zariadení a umožniť mu nasadzovať a konfigurovať aplikácie na všetkých spravované zariadeniach súčasne. Tento proces tiež odstraňuje možnosť ľudskej chyby pri inštalácií. V moderných firemných IT prostrediach, samotný počet a rozmanitosť spravovaných zariadení motivoval vývojárov MDM prostredí k vytvoreniu aplikácií, ktoré umožňujú správu zariadení konzistentným a škálovateľným spôsobom. Celkovou úlohou MDM je zvýšiť podporu a zabezpečenie podnikových zariadení bez výrazného obmedzenia činností zamestnancov pri vykonávaní inštalácií a konfigurácií.

## 1.2 Kontrola a ochrana údajov

Kontrolou a ochranou údajov a konfiguračných nastavení všetkých mobilných v sieti môže MDM znížiť náklady na podporu a riziká stráty firemných dát[2]. Zámerom MDM je optimalizovať funkčnosť a bezpečnosť mobilnej komunikačnej siete pri minimalizácií nákladov. Vďaka flexibilite mobilných zariadení a rastúcemu počtu aplikácií na trhu rastie dôležitosť monitorovania mobilných zariadení. Kontrola zariadení sa vykonáva v reálnom čase pomocou simulácie akcií používateľov, monitorovaním ich aktivity, zisťovaním a opravovaním chýb v aplikáciách.

## 1.3 Použitie MDM vo firemnom prostredí

Funkcionalita MDM môže zahŕňať bezdrôtovú distribúciu aplikácií, údajov a konfiguračných nastavení pre všetky typy mobilných zariadení vrátane mobilných telefónov, smartfónov, tabletov, notebookov, mobilných POS(Point of Sale) zariadení, prenosných tlačiarní a mnoho ďalších[2]. Notebooky a stolné počítače boli pridané do zoznamu podporovaných systémov, pretože správa mobilných zariadení sa stáva viac založená na samotnej správe zariadení a menej na mobilnej platforme. Nástroje MDM sú využívané pre zariadenia vlastnené firmou aj jej zamestnancami v celom podniku alebo pre zariadenia vlastnené zamestnancami. Dopyt používateľov po možnosti použitia vlastného zariadenia (BYOD) na pracovné účely si vyžaduje väčšie úsilie v oblasti vzdialenej správy a zvýšené zabezpečenie zariadení aj sietí, ku ktorým sa pripájajú. Deje sa to preto, lebo zamestnávatelia a zamestnanci majú odlišné predstavy týkajúce sa druhov obmedzení, ktoré sa uplatňujú na mobilné zariadenia[3].

## 1.4 Hlavné funkcie MDM pre Windows

Mnoho organizácií spravuje všetky zariadenia a aplikácie práve pomocou MDM produktov alebo služieb. MDM sa primárne stará o segregáciu (triedenie) podnikových údajov, zabezpečením e-mailov, zabezpečením podnikových dokumentov, kontrolou podnikových pravidiel a integráciou a správou mobilných zariadení. Implementácie MDM môžu byť riešené miestnym alebo cloudovým spôsobom.

MDM nám umožňuje nasledujúce operácie:

- Zaistenie konfigurácie zariadenia na konzistentný a podporovaný súbor aplikácií a funkcií,
- aktualizácia zariadenia, aplikácií a funkcií škálovateľným spôsobom,
- zaistenie toho, aby používatelia používali aplikácie bezpečným spôsobom
- monitorovanie a sledovanie zariadenia (poloha, stav, aktivita),
- schopnosť efektívne diagnostikovať a odstraňovať problémy so zariadením na diaľku.

Časté funkcie ponúkané MDM prostrediami :

- App Catalogue,
- jailbreak (umožnenie prístupu k informáciam administrátora),
- vzdialené odstránenie firemných údajov,
- vzdialené vymazanie celého zariadenia,
- vzdialené uzamknutie zariadenia,
- blacklist a whitelist.

### 1.4.1 Profily a skupiny zariadení

Väčšina dnešných MDM prostredí umožňuje administrátorom vytvárať používateľské profily ku ktorým sú následne priradené spravované zariadenia. Táto možnosť je veľmi výhodná pokiaľ jeden zamestnanec používa viac ako jedno zo spravovaných zariadení. Administrátor môže prostredníctvom profilov rýchlo a efektívne spravovať vybrané zariadenia.

### 1.4.2 Blacklist a Whitelist

Po nasadení MDM prostredia na zariadenie získa administrátor všetky informácie o zariadení vrátane zoznamu nainštalovaných aplikácií. To umožňuje administrátorovi roztriediť aplikácie do takzvaného blacklistu a whitelistu. Blacklist alebo čierna listina je zoznam aplikácií, ku ktorým nebude mať používateľ prístup a to aj napriek tomu, že sú na danom zariadení nainštalované. Whitelist je naopak zoznam aplikácií, ktorých použitie administrátor vyhodnotí ako bezpečné a potrebné vo firemnom prostredí.

### 1.4.3 Sledovanie polohy

Lokalizácia zariadenia je veľmi dôležitá z hľadiska bezpečnosti spravovaných zariadení. MDM poskytuje metódy vynútenia prístupu k polohe zariadenia. To v praxi znamená, že používateľ nebude schopný vypnúť prístup k polohe na spravovanom zariadení. Vďaka tejto funkcií môže administrátor sledovať zariadenie v reálnom čase a taktiež uchovávať históriu pohybu zariadenia.

### 1.4.4 **Vzdialené vymazanie, reštart a skenovanie**

Skenovanie spravovaných zariadení poskytuje administrátorovi aktuálne informácie o zariadení a jeho aplikáciách a hardvéri. V prípade potreby je možné naplánovať vypnutie alebo reštart zariadenia na určitý čas a dátum. Pri odchode zamestnanca z firmy je možné vykonať takzvaný *Corporate Wipe*, teda vymazanie všetkých súborov a aplikácií nainštalovaných prostredníctvom prostredia MDM bez zásahu do súkromných údajov zamestnanca. Pri strate alebo krádeži je tiež možné kompletné vymazanie údajov a uvedenie zariadenia do továrneho nastavenia.

### 1.4.5 **Distribúcia softvéru a súborov**

Často nastáva situácia, kedy administrátor potrebuje nainštalovať alebo aktualizovať aplikácie na veľkom počte zariadení. MDM prostredia poskytujú efektívne metódy hromadnej inštalácie aplikácií na diaľku. Inštalácia softvéru často prebieha po pozadí a vďaka tomu nedochádza k narušeniu pracovnej činnosti zamestnanca. Administrátor môže tiež distribuovať a premiestňovať súbory na úložisko spravovaného zariadenia.

### 1.4.6 **Uzamknutie a kontrola**

V prípade neprítomnosti zamestnanca alebo administrátora vo firemnom prostredí, MDM prostredia umožňujú administrátorovi vzdialene prevziať kontrolu nad celým zariadením. Vďaka tejto funkcií môže administrátor alebo technik vykonávať zmeny, ktoré MDM prostredie priamo neposkytuje. Počas tejto aktivity je často prístup k zariadeniu na strane zamestnanca zablokovaný. Vzdialená kontrola je tiež veľmi užitočná pri krádeži zariadenia. Administrátor je schopný zabrániť odcudzeniu citlivých firemných údajov. Vzdialené zablokovanie alebo vymazanie je tiež možné vykonať priamo v prostredí MDM.

# 2 Implementácia MDM

MDM riešenia väčšinou zahŕňajú serverový komponent, ktorý odosiela príkazy na správu do mobilných zariadení a klientský komponent, ktorý je spustený na spravovanom zariadení a má na starosti príjem a implementáciu príkazov na správu zariadenia. V niektorých prípadoch poskytuje predajca server aj klient, zatiaľ čo v iných prípadoch pochádzajú klient aj server z rôznych zdrojov[24].

## 2.1 Správa zariadení

Správa mobilných zariadení sa postupom času vyvíjala. Spočiatku bolo potrebné nainštalovať aplikácie v potrebnom poradí aby boli možné vykonávať zmeny a aktualizácie. Jedným z ďalších krokov bolo povolenie aktualizácie iniciovanej klientom, podobne jako keď používateľ spustí službu *Windows Update*. Ďalším krokom je centrálna vzdialená správa, ktorá odosiela príkazy bezdrôtovo. Administrátor podnikového dátového centra IT môže pomocou administratívnej konzoly aktualizovať a nakonfigurovať ľubovoľné zariadenie alebo skupinu zariadení. Tento krok poskytuje potrebnú mieru škálovateľnosti, ktorá je potrebná na správu veľkého počtu rozdielnych zariadení.

## 2.2 Softvérové platformy

Softvérové platformy na správu zariadení zabezpečujú, aby koncoví užívatelia mohli využívať služby „plug and play" pre akékoľvek zariadenie, ktoré používajú. Takáto platforma dokáže automaticky detekovať zariadenia v sieti a odosielať im konfigurácie pre okamžitú a nepretržitú použiteľnosť[2].

Tento proces je plne automatizovaný, uchováva históriu použitých zariadení a odosiela nastavenia iba k pripojeným zariadeniam, ktoré neboli predtým nastavené. Tieto MDM systémy dosahujú rýchlosti 50 súborov s aktualizáciou za sekundu.

## 2.3 Cloud a On.premises riešenia

Dnešné MDM ponúkajú riešenia ako SaaS (cloudové riešenie) alebo On-premises (lokálne riešenie). V rýchlo rozvíjajúcom sa priemysle, ako je napríklad mobilný, je systém SaaS (cloudový) výhodnejší, pretože poskytuje jednoduché a rýchle nastavenie a nízkonákladové aktualizácie. Lokálne riešenia vyžadujú na svoju údržbu hardvér alebo virtuálne prostredie, čo môže byť finančne náročné, ale na druhú stranu poskytujú administrátorovi lepšiu kontrolu nad MDM serverom a tiež nad spravovanými zariadeniami.

## 2.4 Kontajnerizácia

Takmer všetky MDM produkty sú postavené na myšlienke takzvanej kontajnerizácie. MDM kontajner musí byť zabezpečený pomocou kryptografických techník (napr. AES-256)[2]. Firemné údaje, ako sú e-maily, dokumenty a podnikové aplikácie sú šifrované a spracované vo vnútri kontajnera. To zaisťuje, že podnikové údaje sú oddelené od osobných údajov používateľa v zariadení. Ďalej je možné vynútiť šifrovanie celého zariadenia alebo karty SD v závislosti od možností MDM softvéru.

## 2.5 Zabezpečenie

Jedným z hlavných dôvodov vzniku MDM bolo zabezpečenie firemných zariadení a to aj mimo firemného prostredia. Táto funkcia umožňuje zamestnancom bezpečne používať firemné aj vlastné zariadenia bez potreby prítomnosti vo firme alebo pripojenia na firemnú sieť. *Mobile Security Management* (MSM) umožňuje administrátorovi povoliť alebo obmedziť definovanú úroveň nastavení v závislosti na prostredí, v ktorom sa zariadenie aktuálne nachádza[24].

### 2.5.1 Zabezpečený katalóg aplikácií

Podniky a organizácie môže spravovať a inovovať aplikácie v zariadení zamestnanca pomocou *App Catalogue* ( katalóg aplikácií ). To umožňuje aplikáciám aby boli nainštalované na používateľove zariadenie priamo z *App Store* alebo cez *App Catalogue*. V app catalogue je tiež možné zakázať inštaláciu aplikácií z neznámich alebo nedôveryhodných zdrojov. V prípade potreby poskytuje MDM prostredie administrátorovi možnosť spustenia zariadení v Kiosk Mode (kioskový režim) alebo Lock-Down Mode (uzamknutý alebo núdzový režim).

### 2.5.2 Zabezpečený prehliadač

Používanie zabezpečeného prehliadača môže používateľa ochrániť pred mnohými potenciálnymi bezpečnostnými rizikami. Mnoho MDM prostredí má integrovaný vlastný prehliadač. Administrátor môže zablokovať pôvodné prehliadače, aby prinútil používateľov používať prehliadač v kontajneri MDM. Tiež je možné vynútiť filtrovanie URL adries za cieľom zvýšenia bezpečnosti prehliadania.

### 2.5.3 Zabezpečený e-mail

Produkty MDM umožňujú organizáciám integrovať svoje existujúce nastavenie a preferencie do prostredia MDM. Takmer všetky MDM prostredia podporujú integráciu so servermi *Office365, Exchange server, Lotus Notes, BlackBerry Enterprise Server (BES)* a ďalšími. To poskytuje flexibilitu pri konfigurácií e-mailu na diaľku.

### 2.5.4 Zabezpečené dokumenty

Zamestnanci často kopírujú prílohy stiahnuté z podnikového e-mailu do svojich osobných zariadení a potom ich zneužívajú. MDM dokáže obmedziť alebo zakázať prístup do alebo z schránky zabezpečeného kontajnera, obmedziť preposielanie príloh na externé domény alebo zabrániť ich uloženiu na SD kartu. Táto funkcia pomáha zabezpečiť firemné údaje pred ich zneužitím.[25]

## 2.6 OTA Programovanie

Schopnosti *Over-the-air programming* (OTA) sú jednou z hlavných súčastí operátora mobilných sietí a podnikového softvéru na správu mobilných zariadení. Medzi ne patrí schopnosť vzdialene konfigurovať jedno alebo viac zariadení, vybranú skupinu mobilných zariadení, posielať aktualizácie softvéru a operačného systému, vzdialene uzamknúť alebo vymazať zariadenie, čím je možné chrániť dáta v zariadení pri strate alebo krádeži a tiež vzdialene riešiť iné problémy so zariadením. Príkazy OTA sú odosielané ako binárne SMS správy, ktoré obsahujú údaje potrebné na vykonanie zmien[23]. Podniky, ktoré využívajú OTA SMS ako súčasť svojej infraštruktúry požadujú pri odosielaní OTA správ vysokú kvalitu, čo vyžaduje od poskytovateľov SMS brán vysoké požiadavky na kvalitu a spoľahlivosť ich služieb.

# 3 Prehľad MDM riešení použiteľných pre systém Windows

Táto kapitola sa zaoberá predstavením šiestich MDM prostredí vhodných pre správu zariadení s operačným systémom Windows. Jej cieľom je uľahčiť prípradnému záujemcovi výber vhodného MDM prostredia na základe jeho požiadaviek na funkcie prostredia.

## 3.1 Manageengine MDM

Manageengine MDM poskytuje rozsiahle možnosti správy zariadení so systémom Windows s verziami 8, 8.1 a 10. Prostredie umožňuje administrátorom monitorovať, spravovať, kontrolovať a zabezpečiť údaje na firemných zariadeniach [4]. Manageengine Mobile device Manager plus poskytuje prehľadnú ponuku funkcií pre správu zariadení s operačným systémom Windows, Android, macOS, iOS a Chrome OS. Manageengine ponúka miestne (On premise) aj cloudové riešenie.
Hlavné Funkcie Manageengine MDM pre Windows sú:
1.Application management:

- Vytvorenie vlastného App catalogue,
- správa interných aplikácií a aplikácií tretích strán,
- distribúcia aplikácií a dokumentov,
- blacklist a whitelist.

2.Security management:

- Uzamknutie na diaľku,
- sledovanie zariadenia v reálnom čase,
- kompletné vymazanie údajov zo zariadenia,
- vymazanie firemných údajov zo zariadenia (často používané v BYOD zariadeniach).

3.Profile management:

- Konfigurácia zariadenia a profilu používateľa podľa firemných potrieb,
- obmedzenie používania určitých aplikácií (Facebook, YouTube, Fotoaparát a pod.),
- vytvorenie logickej skupiny zariadení na základe oddelenie alebo umiestnenia,
- rozlíšenie podnikových a súkromných (BYOD) zariadení,
- možnosť hromadnej distribúcie aplikácií.

4.Mobile content management:

- Vytvorenie úložiska pre ukladanie firemných dokumentov,
- distribúcia dokumentov v rôznych formátoch (docx, PDF, pptx apod.),
- obmedzenie zdieľania dokumentov.

5.E-mail management

- Vzdialené zabezpečenie e-mailu,
- obmedzenie používateľov v úprave alebo odstránení ich e-mailového účtu,
- vzdialené vymazanie účtu.

6.Audit/Report:

- Sledovanie a analýza informácií v zariadení,
- skenovanie zariadenia za účelom kontroly bezpečnosti,
- podrobné informácie o spustených a spravovaných zariadeniach[5].

## 3.2 Hexnode MDM

Hexnode MDM ponúka cloudové riešenie a podporuje počítače a telefóny so systémom Android, iOS, Windows, macOS a tvOS. Hexnode MDM má najväčší podiel zamerania spoločnosti. Umožňuje centralizovanú správu zariadení, tvorbu reštrikcií a obmedzení funkcií zariadenia[6]. Ďalej umožňuje uzamknutie zariadení do kiosk mode, ktorý povolí použitie len vybraných aplikácií. Aplikácia Hexnode, ktorá beží na zariadeniach obsahuje rôzne možnosti zabezpečenia, ako je kiosk prehliadač, prístup k povoleniu Wi-Fi, filtrácia URL adries a mnoho ďalších. Medzi ďalšie funkcie patrí správa obsahu, správa výdavkov, FileVault (zabezpečená zložka súborov), vzdialené prehliadanie a kontrola zariadenia, BitLocker (zabezpečenie dát pre Windows OS), správa aplikácií, filtrovanie webu a Hexnode messenger. Hlavné funkcie Hexnode MDM pre Windows sú:

1.Password management:

- Vzdialená konfigurácia silných hesiel na ochranu podnikových údajov,
- umožnenie správcom presne definovať podmienky hesla,
- možnosť prednastaviť podmienky na automatické uzamknutie zariadenia.

2.Device restrictions enforcement:

- Získanie úplnej kontroly nad všetkými zariadeniami, ktoré sú pripojené na firemnú sieť,
- konfigurácia obmedzení v prístupe k aplikáciám nepotrebným vo firemnom prostredí (môže byť riešené cez Geofence),
- správca môže zamedziť prístup k Wi-Fi, Bluetooth, prehliadač, zdieľanie internetu a ďalším funkciám zariadenia.

3.Network settings configuration:

- Vzdialená konfigurácia sieťových nastavení,
- vzdialené nastavenie e-mailu na všetkých podnikových zariadeniach,
- vzdialené vymazanie všetkých firemných nastavení zo zariadenia bez zásahu do súkromných údajov (pri odchode zamestnanca z podniku),
- vzdialené nastavenie a konfigurácia Exchange ActiveSync do zariadenia a jeho synchronizácia (e-maily, prílohy, kalendár, kontakty) medzi zariadením a serverom.

4.Application management:

- Jednoduchá vzdialená inštalácia aplikácií na zariadenia s Windows OS,
- definovanie aplikácií ako povinných zabezpečuje, že používatelia majú nainštalované všetky potrebné aplikácie na svojich zariadeniach (v prípade zistenia ich absencie je možné zariadenie zablokovať),
- blacklist a whitelist.

5.Device Audition:

- Pravidelná generácia správ zahŕňajúcich zabezpečenie a súlad s predpismi,
- monitorovanie údajov používateľa, štatistík aplikácií a narušení bezpečnosti,
- export prehľadu za účelom dokumentácie.

6.Security management:

- Úplné zablokovanie zariadenia na diaľku,
- sledovanie zariadenia v reálnom čase,
- vyžiadanie povolenie od administrátora pri inštalácií aplikácie na podnikové zariadenie,
- obmedzenie synchronizácie údajov s neoverenými cloud službami,
- vzdialené vymazanie podnikových údajov zo zariadenia,
- URL blacklisting,
- konfigurácia VPN pre jednotlivé aplikácie,
- prepracovaná kontajnerizácia dát,
- nasadenie BitLocker (aj vynútenie zablokovania disku).

7.Remote Control:

- Hexnode messenger,
- zdieľanie obrazovky,
- prevzatie kontroly nad zariadením,
- inštalácia aplikácií,
- bezpečné zdieľanie súborov[7].

## 3.3 Safetica

Safetica je cloudový MDM nástroj, ktorý je zameraný na zabezpečenie dát na mobilných zariadeniach. Jeho funkcie sú zamerané na obranu dát (DLP) a prácu s nimi. Vzhľadom na účel väčšiny dnešných IT zariadení je táto funkcia v MDM najdôležitejšia. Aplikácia býva nasadzovaná spolu s ďalšími systémami a aplikáciami slúžiacimi na samotnú správu a evidenciu zariadení (napr. Active Directory). AD nie je bežne využívaná pre mobilné zariadenia s operačným systémom Android a iOS, preto safetica nie je vhodné riešenie pre tieto zariadenia[8].

Samotné využitie aplikácie spočíva v podrobnejšej správe pripojených zariadení (ktorý USB kľúč môže byť pripojený, ktorý nie), kde je možné na úrovni jednotlivých zariadení blokovať alebo povoliť jednotlivé prístupové kanály k dátam (email, web, Bluetooth).

Reportovanie je nastavba MDM, ktorá monitoruje systém a dokáže detekovať podozrivú aktivitu a pokusy o použitie nepovolených zariadení a prístupových kanálov. Safetica je platený MDM systém a neposkytuje žiadny typ dočasnej testovacej verzie.

Hlavné funkcie Safetica pre Windows sú:

1.Security:

- Prevencia úniku dát,
- rozlíšenie aktívneho a neaktívneho času,
- podrobné monitorovanie akejkoľvek aktivity,
- monitoruje a zabezpečuje všetky potenciálne cesty prenosu dát,
- monitorovanie nezvyklej aktivity,
- pravidlá pre fungovanie aplikácií v závislosti od aktuálneho času a bezpečnosti prostredia,
- kontrola tlačových výstupov,
- blokovanie pripájania neoprávnených zariadení,
- vynútenie šifrovania interných aj externých zariadení,
- monitorovanie a uchovanie informácie o destinácií odoslaných dát,
- filtrovanie dopredu vybraných kategórií a kľúčových slov,
- nastavenia limitov pre jednotlivých používateľov aj pre celé oddelenia,
- integrovanie ochrany firemných dát, reportovanie a politiky blokovania,
- nie je nutné zakúpiť žiadne dodatočné bezpečnostné zariadenia.

2. Reporting and blocking:

- Blacklist a Whitelist,
- obmedzenie operácií so súbormi,
- sledovanie odchýlok v aktivite (dlhodobé aj krátkodobé),
- história návštev webových stránok a e-mailovej komunikácie,
- sledovanie vyhľadávaných kľúčových slov,
- posielanie správ,
- sledovanie aplikácií vrátane sledovania aktívneho a neaktívneho času,
- tlačové výstupy,
- aktivita obrazovky,
- keylogging[9].

## 3.4 Knox Manage

Knox manage je súčasťou produktu Knox spoločnosti Samsung, ktorý bol pôvodne iba zabezpečovacou vrstvou pre Samsung produkty. Knox manage sa vďaka svojej úspešnosti rozšíril na často používané platformy ako Windows, Android (nie iba Samsung produkty) a prekvapivo aj konkurenčné iOS[10].

Knox manage cloudové centrum umožňuje správcom IT vzdialene spravovať a konfigurovať nastavenie zariadení. Nevyžaduje žiadnu systémovú integráciu, čo umožňuje veľmi rýchle a ľahké nastavenie podnikového prostredia. Pomocou služby Samsung Knox Manage automatickej inštalácie a registrácie klienta sa výrazne znižuje čas nasadenia. Jeho vstavané funkcie pomáhajú používateľom nastaviť a spravovať zariadenia v kioskovom režime bez väčších zásahov zo strany správcov.

Hlavné funkcie Knox Manage pre Windows sú:

1.Device management:

- Obmedzenie komunikačných aplikácií a snímania obrazovky,
- vynútenie pravidiel nastavenia pripojenia a prehliadača,
- vzdialené vypnutie a vymazanie,
- režim vývojára (Developer mode),
- bezpečný a núdzový režim,
- vytváranie profilov s skupín zariadení.

2. Application management:

- Vzdialená distribúcia firemných súborov,
- blacklist a whitelist,
- distribúcia aplikácií,
- aktualizácia aplikácií,
- znemožnenie odinštalovania kľúčových aplikácií,
- zakázanie štahovania a inštalácie aplikácií z neoverených zdrojov.

3. Event based management:

- Sady pravidiel nastaviteľné na určitý dátum a čas,
- geofencing,
- pravidlá vzťahujúce sa na firemnú sieť alebo VPN.

4. Remote device support:

- Vzdialené ovládanie zariadenia,
- prenos súborov medzi administrátorským a používateľským zariadením,
- odosielanie správ o chybách,
- skenovanie podozrivej aktivity.

5. Compliance check:

- Monitorovanie stavu zariadenia,
- získanie podrobných informácií o zariadení,
- sledovanie polohy v reálnom čase,
- plánované kontroly zariadenia[11].

## 3.5 Miradore MDM

Miradore MDM je veľmi populárne MDM riešenie vďaka svojej jednoduchosti bezplatnej verzii cloudového riešenia bez časového obmedzenia. Miradore MDM umožnuje administrátorovi zabezpečiť a ovládať mobilné zariadenia a spravovať ich nastavenia na diaľku. Bezplatná verzia sa dá vždy dá zmeniť na vyššiu platenú verziu[12].

Široká ponuka funkcií umožňuje zabezpečiť spravované zariadenia, automatizovať množstvo úloh, ako je konfigurácia e-mailových účtov, nastavenia Wi-Fi, prehľad používaných a inštalovaných aplikácií, poloha, zablokovanie zariadenia a mnoho ďalších.

Miradore pomáha zaistiť bezpečnosť zariadení a údajov, ako aj jednotnosť údajov v celej organizácii. Umožňuje šifrovanie všetkých dôverných údajov, oddelenie firemného a súkromného použitia, vynútenie bezpečných prístupových kódov, zámky obrazovky a zabrániť použitiu nežiaducich aplikácií. Hlavné funckie Miradore MDM pre Windows sú:

1. Application management:
    - Nasadenie a správa aplikácií,
    - vytváranie profilov a skupín zariadení,
    - inventár nainštalovaného softvéru,
    - vzdialený reštart a vymazanie,
    - blacklist a whitelist.
2. Security:
    - Vytváranie zabezpečených kontajnerov aplikácií,
    - vynútenie vytvorenia silného hesla s preddefinovanými požiadavkami,
    - selektívne vymazanie údajov,
    - vzdialené uzamknutie obrazovky alebo celého zariadenia,
    - kódovanie citlivých súborov.
3. Patch management:
    - Implementácia opráv na pridružených zariadeniach,
    - aktualizácie programov a OS,
    - detekcia slabých miest v zariadení,
    - optimalizácia výkonu a spotreby batérie.
4. Automation:
    - Automatizácia pravidelných úkonov v MDM prostredí,
    - plánovanie kontrol a aktualizácií,
    - zber dát,
    - zníženie rizika chýb na strane človeka[13].

## 3.6 SOTI MobiControl

SOTI MobiControl je riešenie správy mobilných zariadení, ktoré zvláda mnohé aspekty mobilných zariadení od ich nasadenia až po vyradenie z prevádzky. Podporuje zariadenia s operačným systémom macOS, iOS, Android a Windows s cieľom eliminovať komplikácie pri správe programov podnikovej mobility pre viacúčelové aplikácie, aplikácie od viacerých dodávateľov a pre rôzne operačné systémy. SOTI MobiControl poskytuje úkony ako je zabezpečenie zariadení aj údajov v nich, sledovanie jeho aktivít, vzdialená podpora zariadení a správa aplikácií a obsahu[14].

Hlavné funckie SOTI MobiControl pre Windows sú:

1.Device management:

- Získanie informácií o zariadení a jeho aplikáciach,
- nasadenie balíčkov aplikácií,
- vytváranie profilov a špecifikácia ich oprávnení,
- vzdialený reštart a vymazanie,
- odosielanie správ používatľskému zariadeniu,
- vzdialené uzamknutie zariadenia.

2. Remote Control:

- Vzdialené prevzatie kontroly nad zariadením,
- prístup na lokálny disk používateľského zariadenia,
- možnosť výmeny súborov medzi zariadeniami,
- spávca úloh je súčasťou okna pre vzdialenú kontrolu.

3.Rules:

- Generácia inštalačných programov pre nasadenie klientských zariadení,
- špecifikácia podmienok pre nasadenie,
- možnosť zberu podrobných dát o zariadení,
- varovné spávy pri podozrivej aktivite.

4.Profiles and packages:

- Vytváranie profilov pre jednotlivé zariadenia,
- možnosť vytvorenia kiosk obrazovky s presnou špecifikáciou povolených aplikácií,
- vytvátranie vlastných balíčkov pre distribúciu v programe Package Studio,
- definícia podmienok postupu inštalácie balíčku[15].

## 3.7 **Porovnanie služieb MDM prostredí**

V tabľke č.1 vidíme, že všetky uvedené MDM prostredia poskytujú veľmi podobné funkcie pre správu zariadení. Jediný väčší rozdiel nastal v možnosti *On-premise* implementácie MDM prostredia.

*Tabuľka 1: Povorvnávacia tabuľka MDM prostredí*

| **Typ Služby** | **SOTI** | **Manageengine** | **Hexnode** | **Safetica** | **Knox Man.** | **Miradore** |
|---|---|---|---|---|---|---|
| Správa aplikácií | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO |
| Zabezpečenie | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO |
| Vytváranie skupín | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO |
| Zablokovanie | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO |
| Správa výdavkov | NIE | NIE | NIE | NIE | NIE | NIE |
| Nahlasovanie chýb | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO |
| Režim Kiosk | ÁNO | NIE | ÁNO | NIE | ÁNO | NIE |
| Lokálny klient | ÁNO | ÁNO | NIE | NIE | NIE | ÁNO |
| Cloudový klient | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO | ÁNO |

# 4 Testovanie prostredia SOTI MobiControl

V tejto kapitole som sa zaoberal inštaláciou a konfiguráciou SOTI MobiControl a jej testovaním na zariadeniach s operačným systémom Windows. Z dôvodu pandémie a nutnosti dištančnej výuky som musel na testovanie MDM prostredia použiť virtuálne počítače vytvorené v prostredí *VMware*. Na simuláciu administrátora MDM som použil virtuálny počítač so systémom Windows 10, ktorý ako jediný z rodiny WindowsOS dokáže pracovať ako samostatný server. Na simuláciu klientov som použil tri virtuálne počítače so systémami Windows 10, Windows 8 a Windows 7, ktorého podpora zo strany spoločnosti Microsoft už síce skončila ale SOTI MobiControl je s ním kompatibilný. Pre prístup k virtuálnym počítačom som použil aplikáciu Remote Desktop, ktorá je súčasťou systému Windows 10 už pri jeho inštalácií a používa protokol vzdialenej plochy (RDP).

## 4.1 Systémové požiadavky

Pre úspešnú inštaláciu a následné použitie SOTI MobiControl prostredia musia byť splnené hardvérové aj softvérové požiadavky. Pri inštalácií som zistil, že systémové požiadavky uvádzané na stránkach spoločnosti SOTI nie sú aktuálne. Taktiež je nutné zaistiť, aby rozhranie *Windows Defender Firewall*, ktoré má na starosti zabezpečenie systému Windows nebránilo prostrediu SOTI MobiControl prístup ku komunikačným portom (rozhraniam), ktoré toto MDM prostredie používa. Problém s povolením portov nastal iba na strane administrátora. Prehľad portov a systémových požiadaviek SOTI MobiControl môžeme vidieť v nasledujúcich tabuľkách.

*Tabuľka 2: Systémové požiadavky SOTI MobiControl pre administrátorský počítač*[16]

| **Komponent** | **Odporúčané parametre** |
|---|---|
| Operačný systém | Windows 10<br>Microsoft Windows Server 2016 |
| Operačná pamäť | 1 až 500 klientov - 4 GB<br>500 až 1000 klientov - 6 GB<br>1000 a viac klientov - 8 GB |
| Výkon procesora | 1 až 500 klientov - 2 GHz dual-core<br>500 až 1000 klientov – 3 GHz dual-core<br>1000 a viac klientov – 3 GHz quad-core |
| Voľný priestor na disku | 15 GB |
| Webový prehliadač | Google Chrome<br>Microsoft Edge<br>Mozilla Firefox |

*Tabuľka 3: Systémové požiadavky SOTI MobiControl pre administrátorský počítač*[16]

| **Komponent** | **Odporúčané parametre** |
|---|---|
| Operačný systém | Windows 10<br>Windows 8<br>Windows 7 |
| Operačná pamäť | 4 GB |
| Výkon procesora | 2,5 GHz single core |
| Voľný priestor na disku | 2 GB |
| Webový prehliadač | Google Chrome<br>Microsoft Edge<br>Mozilla Firefox |

*Tabuľka 4: Zoznam portov potrebných pre komunikáciu SOTI MobiControl*[17]

| **Číslo portu** | **Protokol** | **Účel portu** |
|---|---|---|
| 3389 | RDP | Prevádzka porotokolu vzdialenej plochy |
| 443 | HTTPS | Komunikácia s klientskými zariadeniami |
| 5494/5495 | Binary | Prevádzka SOTI MobiControl serveru |
| 80/443 | HTTP/S | Windows notification service |
| 1433 | Binary | Komunikácia Microsoft SQL serveru |
| 9200/9300 | HTTPS | Vyhľadávanie SOTI MobiControl služby |

## 4.2 Prerekvizity inštalácie

Pred samotnou inštaláciou je nutné nainštalovať niekoľko aplikácií a uistiť sa, že k ním SOTI MobiControl má prístup. V prípade ich neprítomnosti sa inštalácia ukončí chybovou hláškou a požiada vás o inštaláciu komponentov. Podobne ako pri systémových požiadavkách sa aplikácie líšia od požiadaviek uvedených spoločnosťou SOTI, avšak jedná sa len o novšie potrebných aplikácií. Pre úspešné dokončenie inštalácie musia byť na administrátorskom počítači prítomné nasledujúce aplikácie:

- Balíček dotnet-sdk-3.1.407,
- Java SE 8,
- Microsoft SQL server 2019.

### 4.2.1 Microsoft .Net core

Microsoft .Net core je nástupca dnes už nepoužívaného Microsoft .Net Framework. Jeho hlavný účel je zvýšiť kompatibilitu aplikácií vytvorených v programovacích jazykoch *C#, C++, CLI a Visual Basic* s rôznymi operačnými systémami. Jeho význam pre MDM prostredie je umožniť distribúciu aplikácií na spravované zariadenia, ktoré nemajú rovnaký operačný systém ako administrátorský počítač. Microsoft .Net core zahrnutý v balíčku Microsoft *.Net Software Development Kit (SDK)* [18].

### 4.2.2 **Java SE**

Java Platform Standard Edition alebo Java SE poskyuje základ pre budovanie a nasadzovanie sieťových aplikácií od stolného počítača až po server pracovnej skupiny. Java SE je zahrnutá v balíčku *Java Software Development Kit (SDK)* [19].

### 4.2.3 **Microsoft SQL server 2019 Express**

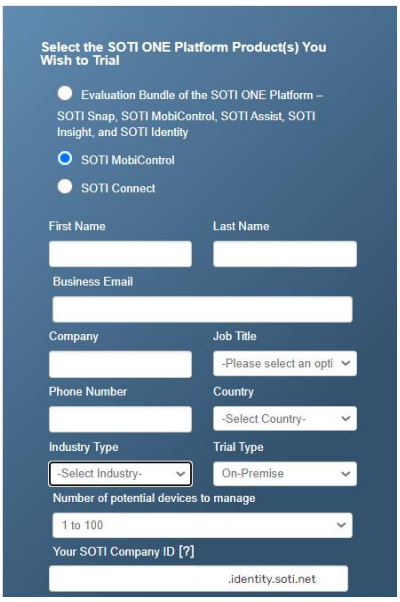
Microsoft SQL server je systém pre správu relačných databáz. Ako databázový server sa jedná o produkt s primárnou funkciou ukladania a načítania údajov podľa požiadaviek iných softvérových aplikácií, ktoré môžu pracovať na rovnakom počítači alebo inom počítači v sieti. Pre prostredie SOTI MobiControl to reprezentuje zoznam zariadení a informácií o nich, ktoré MDM prostrediu umožňujú identifikovať zariadenia pridané do systému. V mojom prípade bola použitá bezplatná verzia Express, ktorá poskytuje databázu s veľkosťou do 10 GB s nízkym výkonom. Táto verzia je vhodná pre malé alebo začínajúce spoločnosti[20].

## 4.3 **Postup inštalácie**

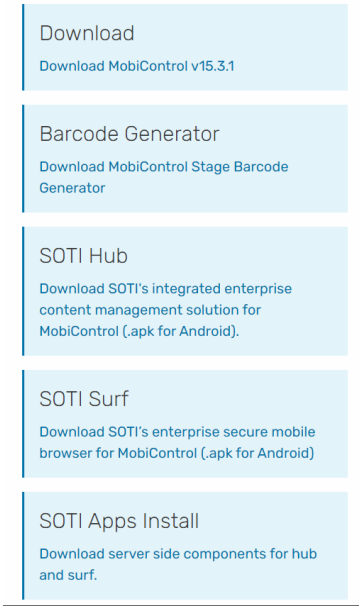
Na testovacie prostredia SOTI MobiControl som použil bezplatnú skúšobnú verziu s platnosťou 30 dní. Jedná sa o verziu On-premise, čo znamená že management server vytvára a spravuje administrátor firemnej siete.

Ako prvé je som muselo skúšobnú licenciu na stránkach spoločnosti SOTI. Pre jej udelenie je nutné vyplniť formulár obsahujúci základné údaje o používateľovi a registračný email. Po niekoľkých hodinách som obdržal email obsahujúci odkaz na stiahnutie inštalačného súboru SOTI MobiControl a registračný kód s platnosťou 30dní. Po otvorení odkazu som bol presmerovaný na stránky SOTI a stiahol som si inštalačný súbor *MobiControl v15.3.1*.

*Obrázok 1: Registračný formulár*




*Obrázok 2: Zoznam sofvéru na stiahnutie*

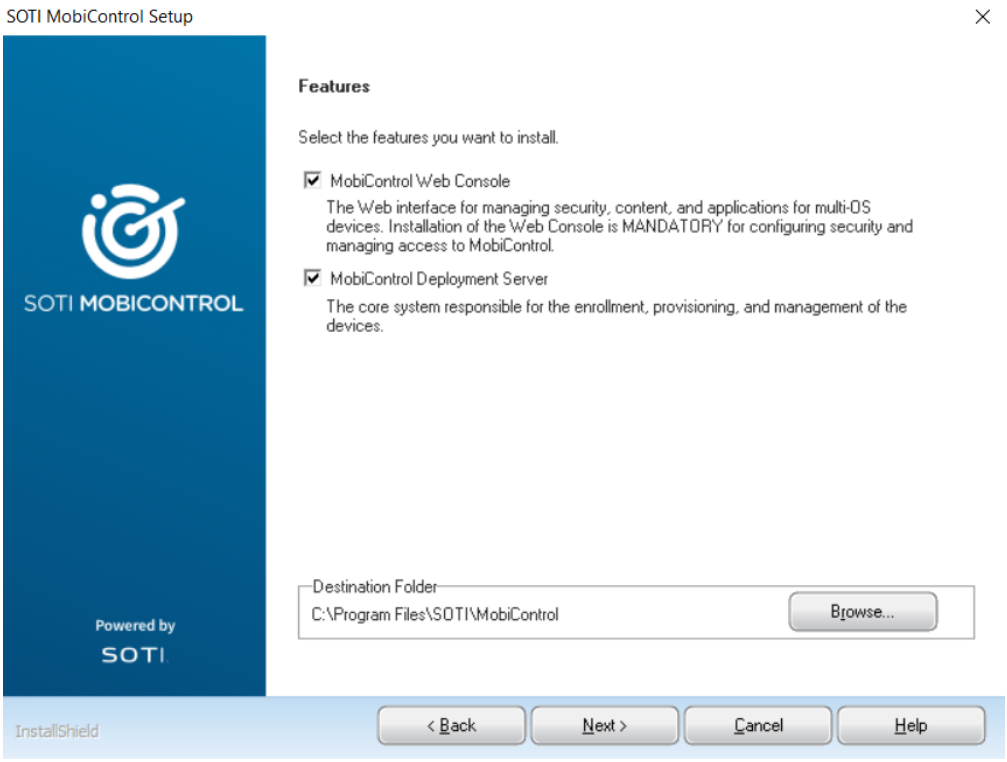



Po stiahnutí som spustil inštalačný súbor ako administrátor. Nasledoval výber jazyka. Keďže nebola možnosť výberu slovenského ani českého jazyka, zvolil som anglický jazyk. Ďalej som musel odsúhlasiť licenčné podmienky pre použitie softvéru stanovené spoločnosťou SOTI pre použitie softvéru.

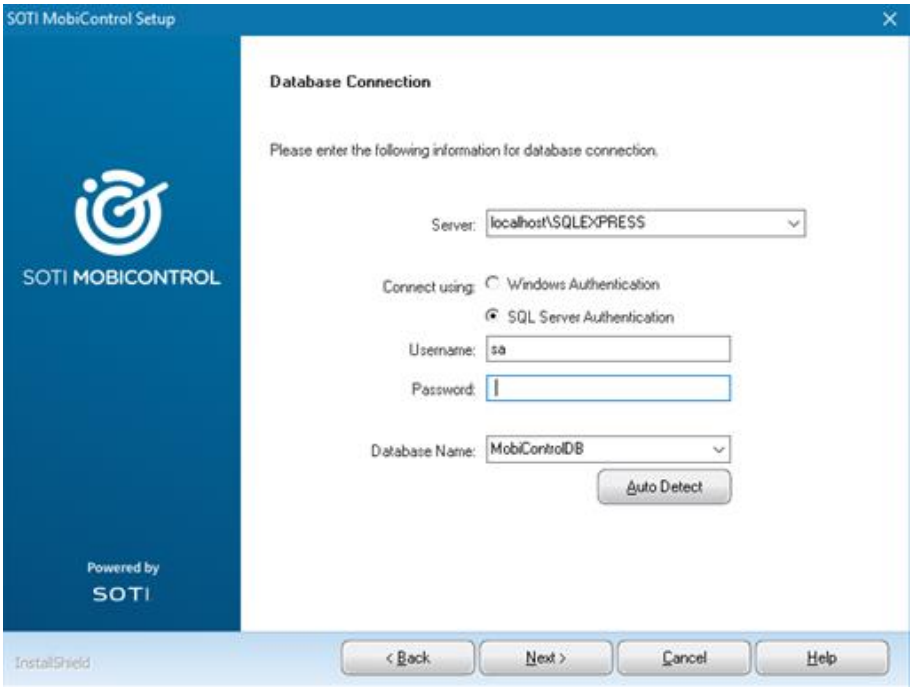
Nasledujúca časť sa líši od štandardného postupu inštalácie. Inštalačný sprievodca SOTI MobiControl mi pri inštalácií ponúkol možnosť inštalácie programu Microsoft SQL Server 2014 Express, ktorý má v MDM prostredí slúžiť na zber dát. Pri pokuse nainštalovať prostredie touto cestou sa inštalácia skončila neúspechom a chybová hláška mi oznámila, že nebolo možné vytvoriť SQL databázu. Po niekoľkých pokusoch o opakovanie inštalácie a rovnakým výstupom som sa rozhodol samostatne nainštalovať program *Microsoft SQL server 2019*. SQL server som nainštaloval s predvolenými nastaveniami a prihlasovanie do neho som ponechal v hybridnom režime. Pre prístup aplikácie k databáze som ponechal predvoleného užívateľa ,,*sa*''. Pre reálne použitie je však vhodné zvoliť iného užívateľa z hľadiska bezpečnosti a tiež v závislosti od iných aplikácií používajúcich danú databázu.

Pri opätovnom spustení inštalácie mi už nebola ponúknutá inštalácia programu *Microsoft SQL Server 2014 Express* a ani formulár na vytvorenie databáze a inštalácia sa úspešne dokončila.

*Obrázok 3: Ponuka súčastí při inštalácií*



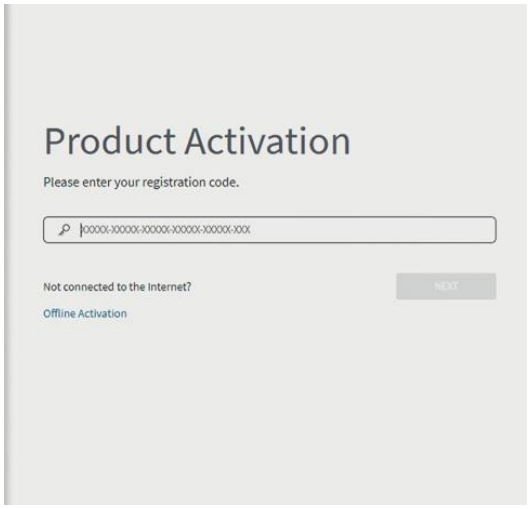
*Obrázok 4: Výber SQL serveru*



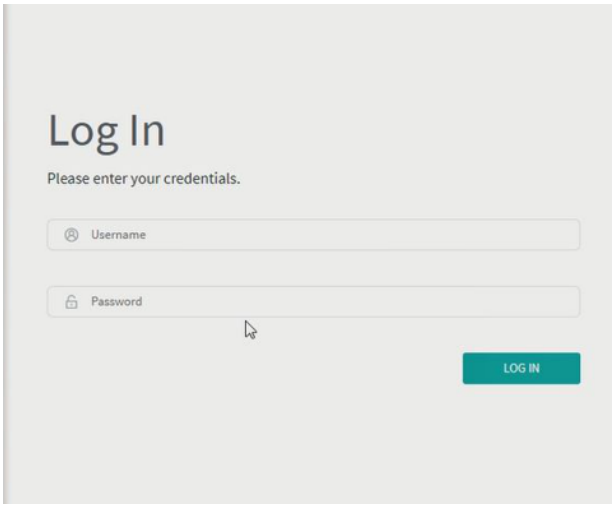

Po ukončení inštalácie a spustení SOTI MobiControl sa mi otvoril predvolený prehliadač (v mojom prípade Microsoft Edge) a požadoval môj registračný kód. Registračný kód je použiteľný 30 dní a je funkčný aj pri opätovnej inštalácií softvéru, no jeho platnosť sa nepredĺži. Po zadaní platného registračného kódu sa mi zobrazila ponuka prihlásenia do systému. Ako používateľské meno (Username) je treba použiť výraz *„Administrator“* a heslo (Password) je potrebné použiť heslo k databázy vytvorenej pri inštalácií.

Po úspešnom prihlásení je systém SOTI MobiControl pripravený na pridanie nových zariadení a ich správu.

*Obrázok 5: Zadanie licenčného kódu*



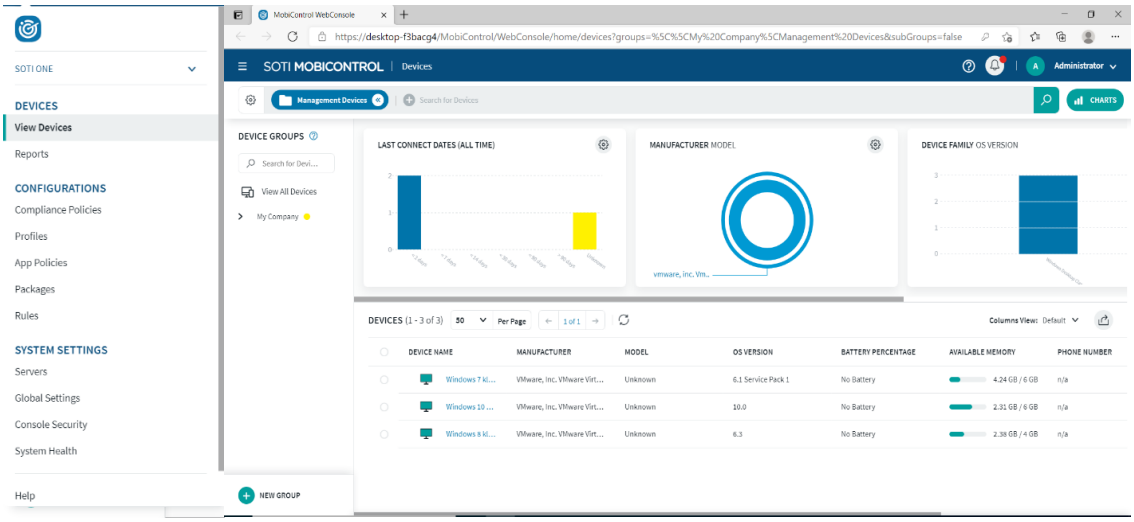

*Obrázok 6: Prihlasovací formulár*



## 4.4 Zoznámenie sa s prostredím

Administrátorské rozhranie systému SOTI MobiControl je k dispozícii cez webový prehliadač. Pri inštalácii prostredia bol tiež automaticky nainštalovaný program MobiControl Administration Utility, ktorý umožňuje administrátorovi upravovať samotný MDM server (reštart, zmena portu, zmena databázy a pod.). Po prihlásení sa zobrazí prehľadová obrazovka na ktorej môžeme vidieť niekoľko prehľadových grafov, ktoré poskytujú administrátorovi prehľad o nedávnych pripojeniach, pomer pripojených zariadení na základe operačného systému (v našom prípade iba Windows zariadenia) a verzie operačných systémov spravovaných zariadení. V nastaveniach je možné vytvoriť si vlastné grafy, ktoré sa budú na úvodnej obrazovke zobrazovať.

*Obrázok 7: Prehľadová obrazovka SOTI MobiControl*




Po kliknutí na ikonu v ľavom hornom rohu sa zobrazí lišta obsahujúca záložky (viz obrázok 7), ktoré po kliknutí presunú administrátora do iného rozhrania MDM prostredia.

Záložka *View Devices* je zobrazená automaticky po prihlásení do MDM systému. Obsahuje zoznam všetkých zariadení a poskytuje administrátorovi možnosť vytvárať skupiny zariadení podľa jeho potreby. Obsahuje tiež niekoľko možností vyhľadávania zariadení podľa operačného systému, skupiny v ktorej je zaradené a aj štandardné vyhľadávanie podľa názvu zariadenia.

Záložka *Reports* ma presunula do rozhrania v ktorom môžeme generovať podrobné hlásenia o vybraných oblastiach spravovaných zariadení. Medzi hlavné oblasti hlásení patria:

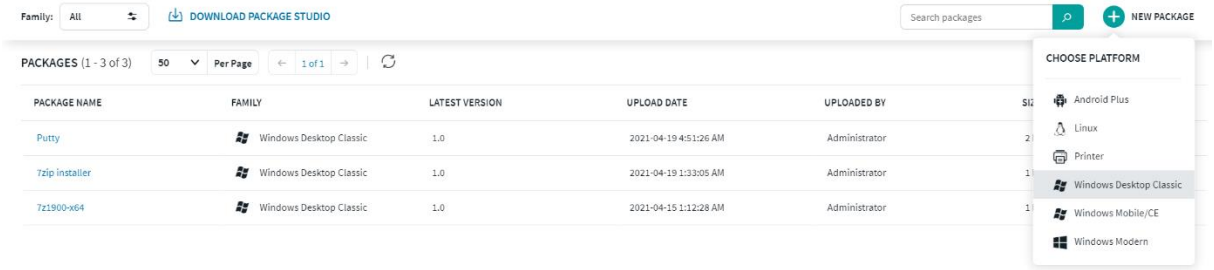
- Informácie o všetkých pripojeniach,
- súhrn všetkých systémových informácií,
- zoznam nainštalovaných aplikácií,
- informácie o polohe zariadenia,
- informácie o stave batérie, využitie operačnej pamäte a voľnom mieste na disku.

Zo záložkou *Compliance Policies* som sa veľmi nezaoberal pretože jej funkcie sú aplikovateľné iba na operačné systémy Linux, Android a iOS, ktoré v tejto práci nepoužívam. Z môjho pozorovania by mala táto záložka obsahovať možnosť vytvorenia pravidiel, ktoré budú aplikované hneď po nasadení na spravované zariadenie.

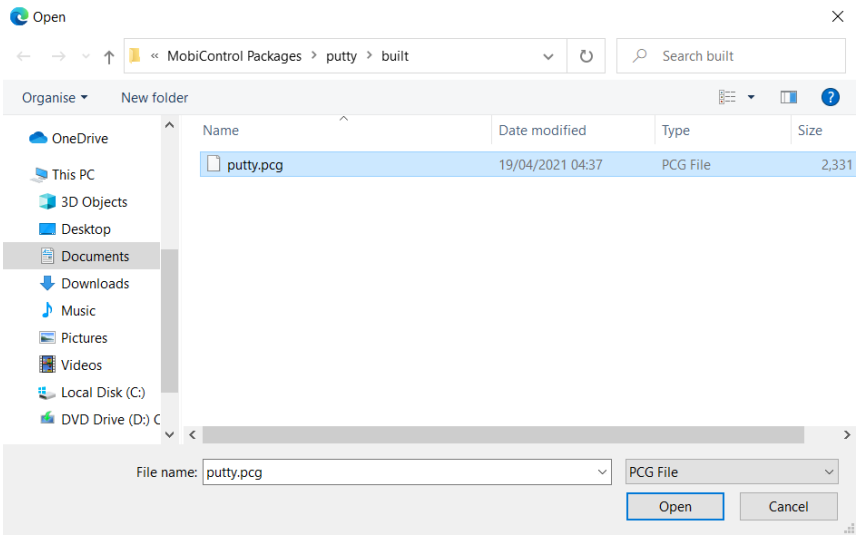
Záložka *Rules* presmeruje administrátora do rozhrania, ktoré slúži hlavne na pridanie nových zariadení do systému. Pri pridávaní nového nového zariadenia vytvorí administrátor nové pravidlo (rule), v ktorom špecifikuje názov zariadenia, operačný systém a skupinu do ktorej má byť zariadenie pridané. Na základe týchto špecifikácií je následne vygenerovaný inštalačný súbor, ktorý je nutné prekopírovať a spustiť na novom zariadení.

V záložke *Packages* môže administrátor nahrávať na server takzvané balíčky (packages). Tieto balíčky obsahujú inštalačný súbor aplikácie a preddefinované parametre pre jej inštaláciu. Balíčky sú ďalej vkladané do profilov a distribuované na spravované zariadenia.

*Obrázok 8: Nahrávanie balíčkov na server*




*Obrázok 9: Výber balíčkov pri nahrávaní*




Záložka *Profiles* slúži na vytvorenie konfigurácií, ktoré sú následne aplikované na spravované zariadenia. Do tejto konfigurácie je možné pridať balíčky aplikácií a obmedzenia pre zariadenia, na ktoré je profil aplikovaný.

Po rozkliknutí konkrétneho zariadenia v záložke *View Devices* sa nám zobrazí okno s nasledujúcimi záložkami:

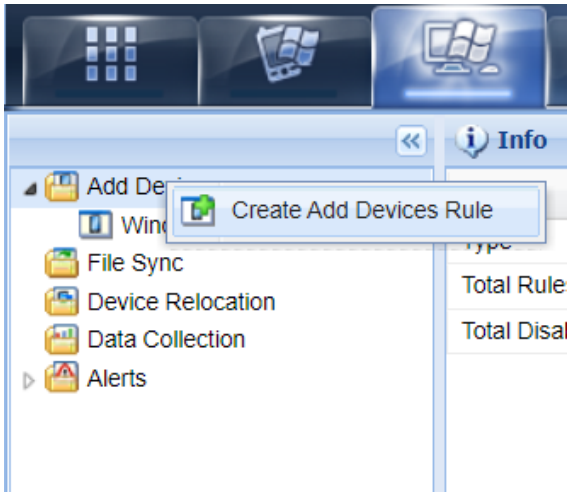
- Device details,
- configurations,
- applications,
- location,
- security.

V tomto okne môžeme vykonávať operácie ako vzdialená kontrola nad zariadením, načítanie informácií o zariadení, vzdialený reštart, odosielanie správ a podobne.

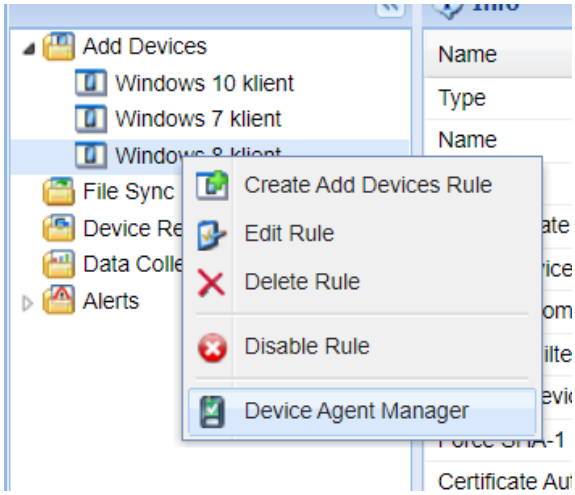
## 4.5 Nasadenie prostredia na klientské počítače

Pre nasadenie nového zariadenia sa musí administrátor presunúť do záložky Rules a vytvoriť nové pravidlo pre nasadenie na nové zariadenie. Pri vytváraní pravidla musí administrátor presne špecifikovať operačný systém, názov zariadenia, počiatočné pravidlá a skupinu do ktorej bude zariadenie pridané.

*Obrázok 10: Vytvorenie pravidla při nasadení*

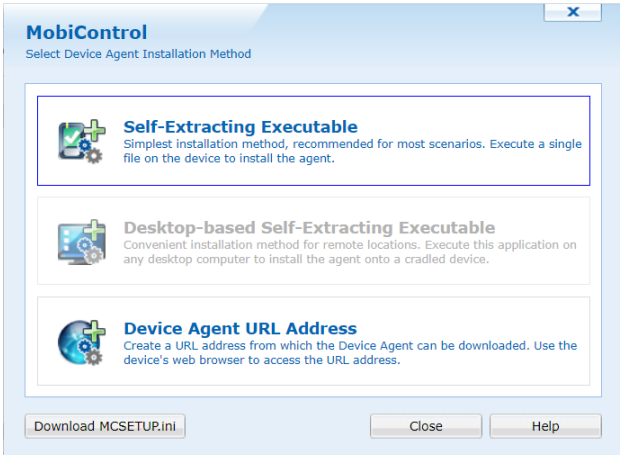



*Obrázok 11: Vytvorenie inštalačného súboru*

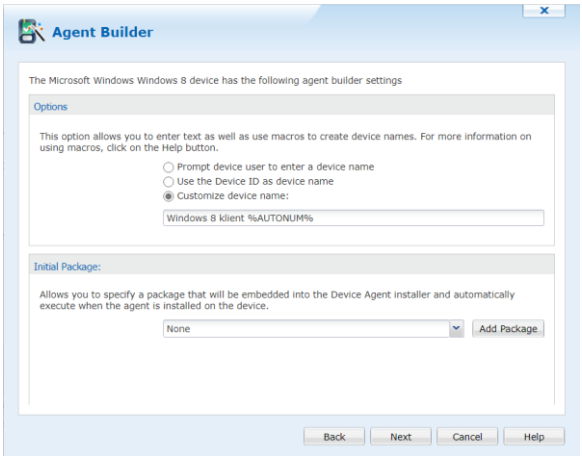



Ďalej je potrebné v prostredí Device Agent Manager vytvoriť súbor pre nasadenie, ktorý prekopírujeme a spustíme na zariadení, ktoré chceme pridať do systému MDM. V tomto prostredí je nutné presne špecifikovať typ a verziu operačného systému nového zariadenia a tiež je tu možnosť pridať balíčky, ktoré budú pri nasadení automaticky nainštalované. Na koniec si vyberieme metódu nasadenia. Osobne som zvolil metódu *Self-Extracting Executable*, ktorá mi prišla ako najspoľahlivejšia.

*Obrázok 12: Výber metódy nasadenia*




*Obrázok 13: Špecifikácia balíčkov pri nasadení*

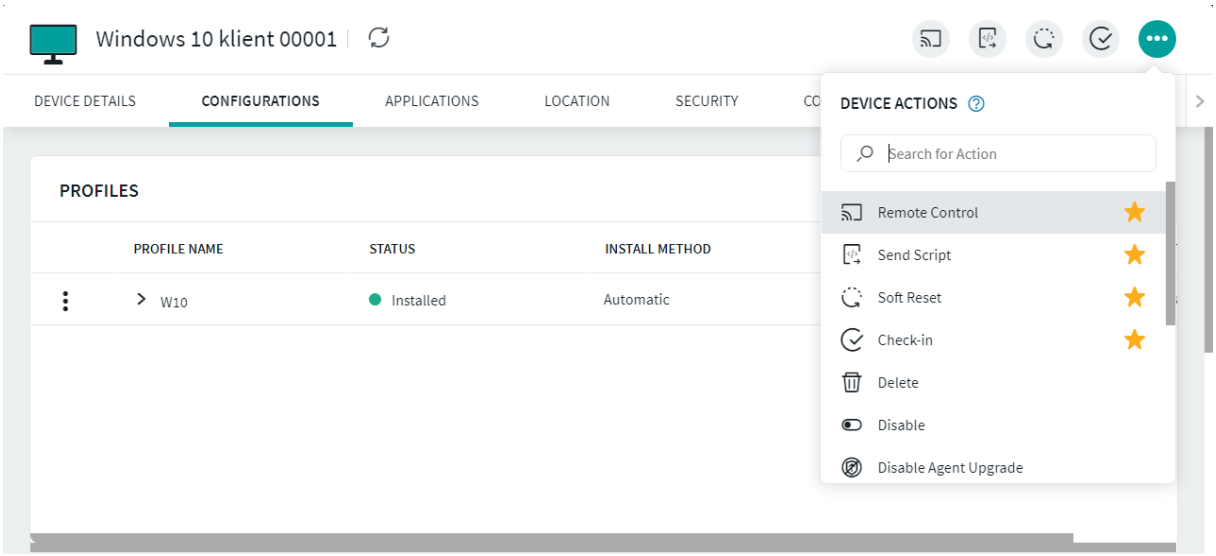


Po prekopírovaní na nové zariadenie jednoducho spustíme inštalačný súbor. Ak sme pri vytváraní súbor správne špecifikovali, do jeden minúty bude zariadenie pridané do MDM prostredia a pripravené na použitie.

## 4.6 Testovanie funkcií MDM prostredia na nasadených zariadeniach

Po každej inštalácií aplikácie je vhodné si overiť jej funkčnosť. Pri nasledujúcich testoch som si overil funkčnosť najdôležitejších funkcií MDM prostredia pre operačný systém Windows ako je vzdialená kontrola nad zariadením, distribúcia softvéru, vzdialený reštart a odosielanie správ. Pred každou operáciou je doporučené spustiť funkciu *Check-in*, ktorá načíta aktuálne informácie o zariadení a jeho dostupnosti.

*Obrázok 14: Ponuka akcií vykonateľných na zariadení*




### 4.6.1 Vzdialená kontrola nad zariadením

Prevzatie kontroly nad spravovaným zariadením je podľa môjho názoru najdôležitejšia funkcia MDM prostredia pre Windows. Po aktivácií tejto funkcie je administrátor presunutý do okna ktoré je rozdelené na 3 časti:

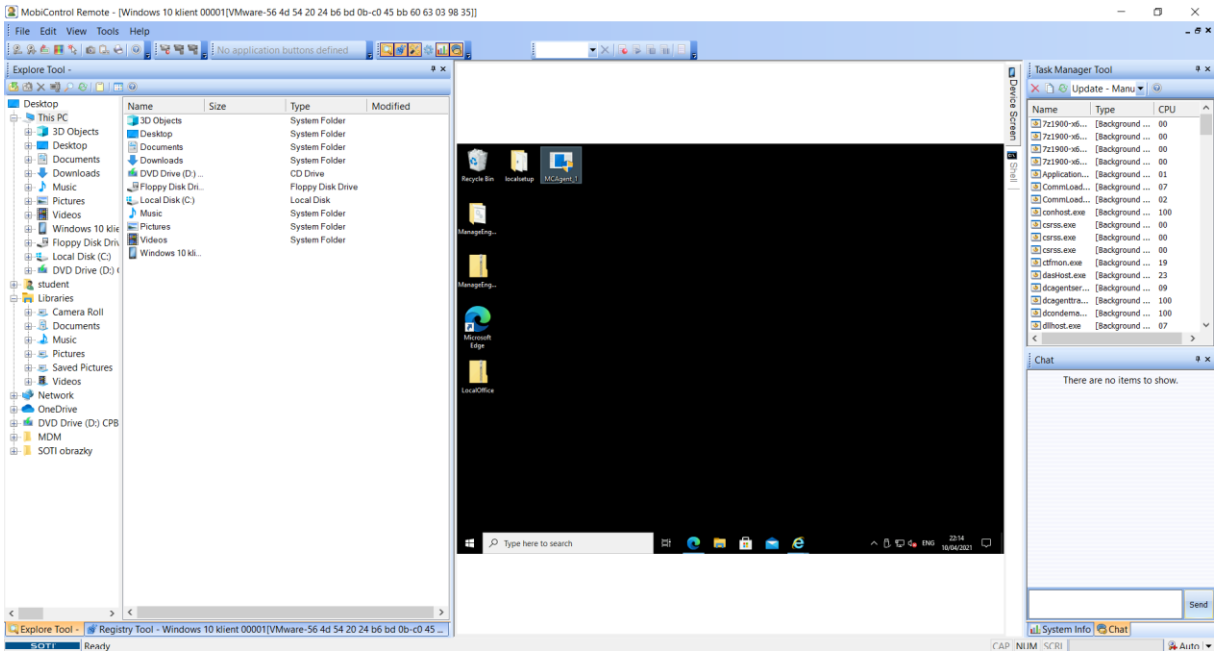
- Pracovná plocha spravovaného zariadenia,
- správca súborov administrátorského aj spravovaného počítača,
- správca úloh spravovaného zariadenia.

Po aktivácií funkcie je používateľovi spravovaného zariadenia znemožnená akákoľvek manipulácia so zariadením. Administrátor má teda plnú kontrolu and počítačom a môže bezpečne vykonávať zmeny.

Pri testovaní na tejto funkcie na virtuálnom počítači ale nastáva drobná komplikácia. SOTI MobiControl podobne ako mnoho ďalších MDM prostredí využíva protokol vzdialenej plochy (RDP). Pomocou toho istého protokolu som sa však pripájal k virtuálnym počítačom, ktoré simulujú MDM administrátora a spravované zariadenia. Z tohto dôvodu som bol na strane môjho osobného počítača odpojený od virtuálneho stroja.

Vzdialená kontrola and zariadením na strane administrátora aj napriek kolízií fungovala bez problémov. Po ukončení vzdialenej kontroly som sa bezproblémovo pripojil k virtuálnemu stroju s môjho osobného počítača.

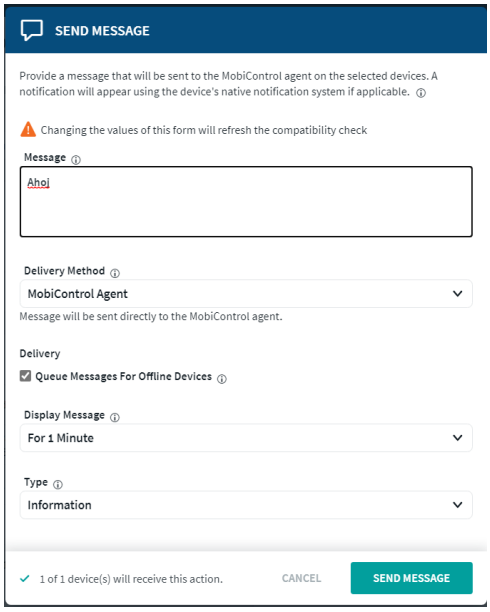
*Obrázok 15: Okno vzdialenej kontroly and zariadením prostredia SOTI MobiControl*



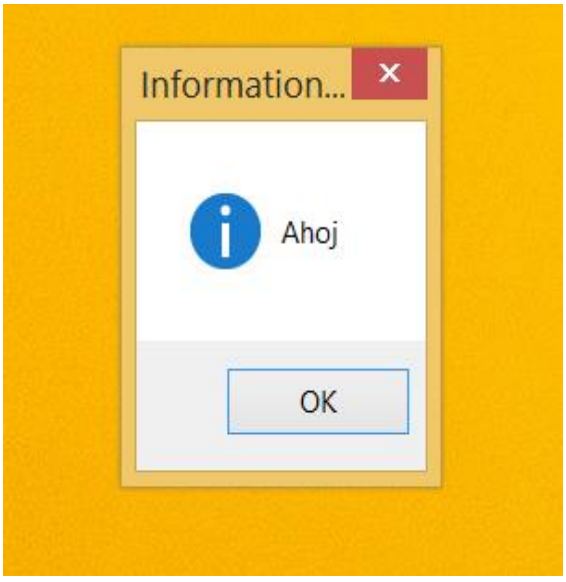

## 4.6.2 **Odosielanie správ**

Odosielanie správ je asi najjednoduchšia funkcia každého MDM prostredia. Administrátor vyplní formulár s textom, ktorý chce používateľovi odoslať. Používateľovi sa správa zobrazí ako výstražné okno, ktoré prekryje všetky spustené aplikácie.

*Obrázok 16:* F*ormulár na odosielanie správ*




*Obrázok 17:* V*ýpis správy na spravovanom zariadení*

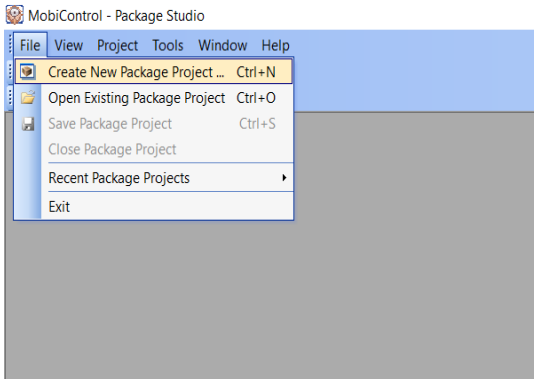


### 4.6.3 **Distribúcia Softvéru**

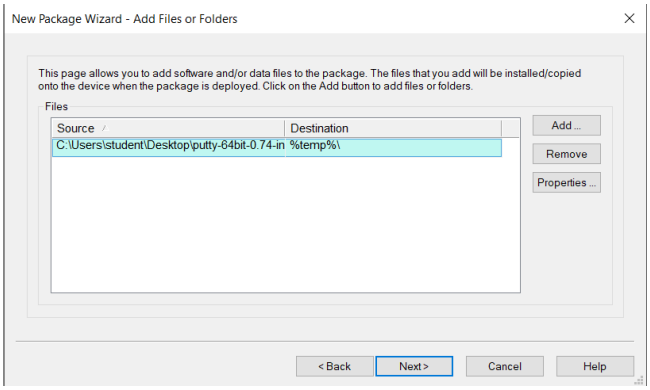
Vzdialená inštalácia softvéru na viac zariadení naraz je ideálna cesta pre spoločnosti s viacerými pobočkami a veľkým počtom spravovaných zariadení. V prostredí SOTI MobiControl táto funkcia prebieha skrz vytváranie profilov a ich následné prideľovanie na zariadenia alebo skupiny.

Ako prvé je treba vytvoriť už niekoľko krát spomínaný balíček (package) v programe MobiControl Package Studio. Jeho stiahnutie je administrátorovi automaticky ponúknuté v záložke Packages. Do tohto prostredia administrátor nahrá inštalačný súbor a špecifikuje zariadenia a podmienky, za ktorých inštalácia prebehne. Po vytvorení je balíček potrebné skompilovať a následne nahrať na server SOTI MobiControl. Pri nahrávaní je treba vybrať súbor s príponou *pcg*.

*Obrázok 18:* Vytvorenie balíčku

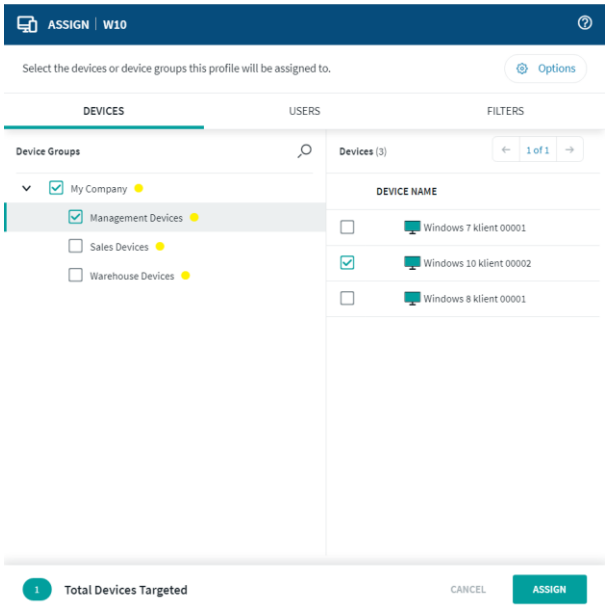



*Obrázok 19:* Nahranie inšatalčného súboru do balíčku

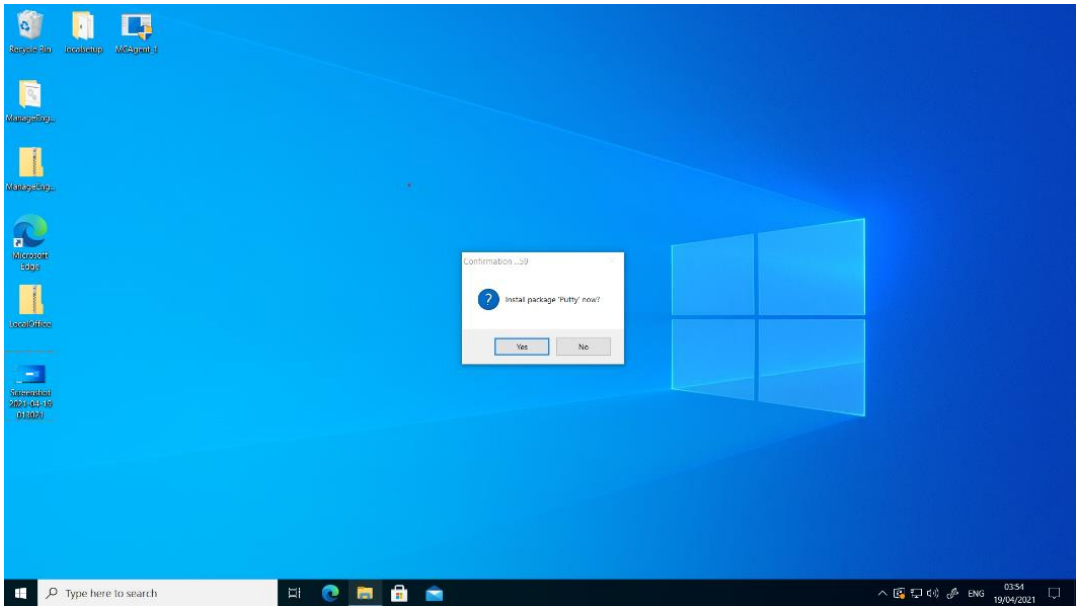



S pripravenými balíčkami prejde administrátor do záložky Profiles kde vytvorí profil (konfiguráciu), do ktorého následne nahrá potrebné balíčky. V profile je tiež možné nadefinovať obmedzenia pre vybrané zariadenia. Po potvorení profilu administrátor ho administrátor uloží a vyberie zariadenia (save and assign), na ktoré bude aplikovaný. Po úspešnom dokončení budú požadované aplikácie nainštalované na všetky zvolené zariadenia.

*Obrázok 20: Priradenie profilu pre distribúciu softvéru*



*Obrázok 21: Dotaz k inštalácií softvéru na spravovanom zariadení*




### 4.6.4 **Vzdialený reštart**

Reštart zariadenia je po inštalácií softvéru vždy doporučený. Pomocou MDM prostredia ho môže administrátor vykonať na diaľku. Jeho funkčnosť som bohužiaľ nebol schopný graficky zdokumentovať, pretože prostredie SOTI MobiControl túto funkciu aplikuje okamžite a bez výstrahy.

### 4.6.5 **BitLocker**

*BitLocker* alebo *kiosk* obrazovka umožní administrátorovi obmedziť používateľovi prístup k určitým aplikáciám. Administrátor presne nadefinuje, ktoré aplikácie môžu byť použité. Zvyšné aplikácie sú zblokované až do vypnutia kiosk obrazovky administrátorom.

Pre aktiváciu tejto funkcie musí byť na spravovanom zariadení nasadený profil (rovnako ako pri distribúcií softvéru), v ktorom je povolená a nadefinovaná funkcia *lockdown*. Po pridelení profilu sa spravované zariadenie reštartuje a zostane úplne uzamknuté. Podobne ako pri vzdialenom ovládaní som bol s virtuálneho počítača odpojený a keďže bolo zablokované, nebol som schopný sa pripojiť späť.

Po aktivácií funkcie *Enable Kiosk Screen* mi bolo umožnené sa pripojiť na spravované zariadenia pomocou vzdialenej plochy (RDP) v obmedzenom režime. Kiosková obrazovka má dva režimy, administrátorský (Administrator lockdown) a používateľský (User lockdown).

V administrátorskom režime má používateľ prístup k ovládaciemu panelu, správcovi úloh a správcovi súborov, pomocou ktorého je schopný spustiť ďalšie aplikácie nainštalované v počítači. V administrátorskom režime je tiež možné vypnúť funkciu *Kiosk Screen*. V používateľskom režime je možné využívať iba aplikácie povolené v profile nasadenom na zariadení.

*Obrázok 22: Kiosk obrazovka v administrátorskom režime*


*Obrázok 23: Kiosk obrazovka v používateľskom režime*


## 4.7 Zhodnotenie testovania

Inštalácia prostredia môže byť pomerne komplikovaná, pretože spoločnosť SOTI na svojich stránkach neuvádza problém s inštaláciou aplikácie *Microsoft SQL server 2014 Express* a tiež zastaralé verzie aplikácií, ktorých prítomnosť je požadovaná pred započatím inštalácie samotného MDM prostredia. Odhliadnuc od tohto problému prebehla inštalácia bez ďalších problémov.

Samotné prostredie MDM je podľa mňa prijateľne spracované. Každá testovaná funkcia bola aplikovaná takmer okamžite a bez problémov. Prostredie pre nasadenie zariadení je prispôsobené pre pridanie veľkého počtu zariadení pomocou jedného inštalačného súboru.

Za nedostatky tohto prostredia považujem absenciu funkcie kompletného vymazania zariadení pri krádeži a tiež funkcie B*lacklist* a W*hitelist*. Pri distribúcií softvéru by som privítal zjednotenie celého procesu do jedného rozhrania.

# 5 Testovanie prostredia Manageengine MDM

V tejto kapitole som sa zaoberal inštaláciou a konfiguráciou systému Manageengine MDM. Rovnako ako pri systéme SOTI MobiControl som musel na testovanie MDM prostredia použiť virtuálne počítače a protokol vzdialenej plochy. Manageengine však podporuje iba zariadenia s operačným systémom Windows 10. Na stránkach spoločnosti Manageengine je síce uvedené, že podporuje zariadenia so systémom Windows 8, pri pokuse o nasadenie na tento operačný systém sa proces ukončil chybovou hláškou. Napriek tomu, že bol súbor pre nasadenie zariadenia vygenerovaný priamo v Manageengine MDM prostredí mi chybová hláška oznámila, že môj operačný systém je zastaralý a pre nasadenie potrebujem mať nainštalovaný systém Windows 10. Z tohto dôvodu som na simuláciu klientského počítača použil iba jeden virtuálny počítač.

## 5.1 Systémové požiadavky

Rovnako ako pri systéme SOTI MobiControl a každom inom programe je nutné, aby boli splnené požiadavky pre správne fungovanie MDM prostredia. Pred započatím inštalácie nie je potrebná inštalácia žiadnych ďalších programov alebo súčastí. Ako už bolo spomenuté, technické požiadavky uvedené na stránkach spoločnosti Manageengine sú značne zastaralé a preto som ich na základe testovania musel upraviť. Nižšie uvedené požiadavky by mali byť považované za absolútne minimum, ktoré musí byť k dispozícií pre správnu funkciu prostredia. Ďalej je nutné povoliť MDM prostrediu prístup ku komunikačným portom v aplikácií *Windows Defender Firewall*. Pri inštalácií prostredia je však administrátorovi umožnený výber portov pre komunikáciu a preto je nutné tomu prispôsobiť nastavenie Firewallu. Pri výbere portov je však potrebné brať na vedomie, že všetky súčasti prostredia Manageengine MDM komunikujú výhradne prostredníctvom lepšie zabezpečeného prenosu (HTTPS).

Prehľad portov a systémových požiadaviek Manageengine MDM môžeme vidieť v nasledujúcich tabuľkách.

*Tabuľka 5: Systémové požiadavky Manegeengine MDM pre klienský počítač[21]*

| **Komponent** | **Odporúčané parametre** |
|---|---|
| Operačný systém | Windows 10 |
| Operačná pamäť | 4 GB |
| Výkon procesora | 2,5 GHz single core |
| Voľný priestor na disku | 2 GB |
| Webový prehliadač | Google Chrome<br>Microsoft Edge<br>Mozilla Firefox |

*Tabuľka 6: Systémové požiadavky Manageengine MDM pre administrátorský počítač[21]*

| **Komponent** | **Odporúčané parametre** |
|---|---|
| Operačný systém | Windows 10<br>Microsoft Windows Server 2016<br>Microsoft Windows Server 2019 |
| Operačná pamäť | 1 až 250 klientov - 6 GB<br>250 až 1000 klientov - 8 GB<br>1000 až 3000 klientov - 12 GB<br>3000 až 10000 klientov - 16 GB<br>10000 a viac klientov - 32 GB |
| Výkon procesora | 1 až 250 klientov - 2.4 GHz dual-core<br>250 až 1000 klientov – 2.9 GHz dual-core<br>1000 až 3000 klientov – 2.5 GHz quad-core<br>3000 až 10000 klientov – 2.6 GHz eight-core<br>10000 a viac klientov – 2.7 twelve-core |
| Voľný priestor na disku | 1 až 250 klientov - 5 GB<br>250 až 1000 klientov - 20 GB<br>1000 až 3000 klientov - 30 GB<br>3000 až 10000 klientov - 60 GB<br>10000 a viac klientov - 120 GB |
| Webový prehliadač | Google Chrome<br>Microsoft Edge<br>Mozilla Firefox |

*Tabuľka 7: Zoznam portov potrebných pre komunikáciu Manageengine MDM[22]*

| **Číslo portu** | **Protokol** | **Účel portu** |
|---|---|---|
| 3389 | RDP | Prevádzka protokolu vzdialenej plochy |
| 443 | HTTPS | Komunikácia s klientskými zariadeniami |
| 8080 | HTTP | Prevádzka Manageengine ServiceDesk plus |
| 9020 | HTTP | Prevádzka Manageengine Mobile Device Manager |
| 9383 | HTTPS | Komunikácia Manageengine Mobile Device Manager |
| 8020 | HTTP | Prevádzka Manageengine Desktop Central |
| 8383 | HTTPS | Komunikácia Manageengine Desktop Central |
| 445 | TCP | správa Windows zariadení bez agenta |

## 5.2 Postup inštalácie

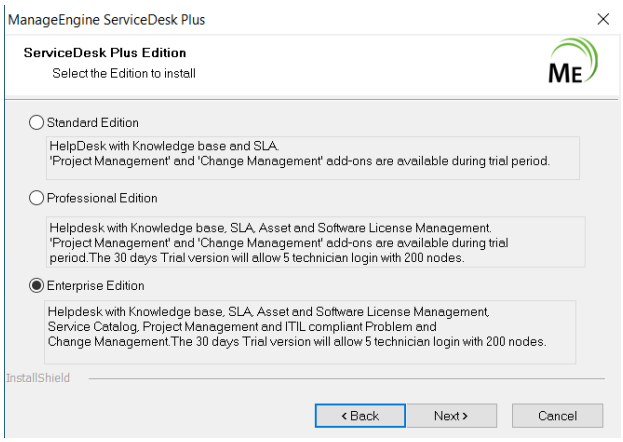
Na testovanie prostredia Manageengine MDM som použil voľne prístupnú skúšobnú verziu s platnosťou 30 dní od prvej inštalácie. Rovnako ako pri prostredí SOTI MobiControl sa jedná o verziu On-premise. Pre využitie všetkých funkcií MDM prostredia Manageengine je nutné nainštalovať a synchronizovať si nasledujúce aplikácie:

- Manageengine ServiceDesk plus,
- Manageengine Mobile Device Manager,
- Manageengine Desktop Central.

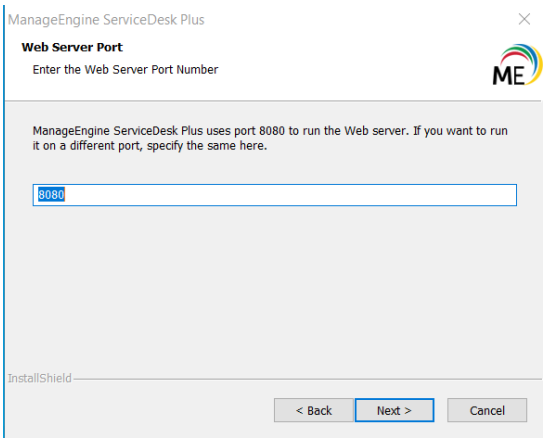
Ako prvé je nutné nainštalovať si aplikáciu Manageengine ServiceDesk plus, ktorá slúži ako centrála všetkých funkcií a komponentov (plug-in). Aplikácia je prístupná bez akejkoľvek registrácie na stránkach spoločnosti Manageengine a vyplnenie formulára s údajmi o používateľovi je dobrovoľné.

Po stiahnutí a spustení inštalačného súboru som zvolil verziu *Enterprise*, ktorá mi počas trvania skúšobnej verzie poskytla prístup ku všetkým komponentom. Nižšia verzia Standard neposkytuje prístup ku komponentom pre MDM prostredie. Ďalej treba špecifikovať port na ktorom bude pracovať webový server (localhost) tejto aplikácie, ktorý som ponechal na porte číslo 8080. Registrácia pre technickú podporu nie je povinná a je možné ju preskočiť.

*Obrázok 24: Výber verzie platformy*



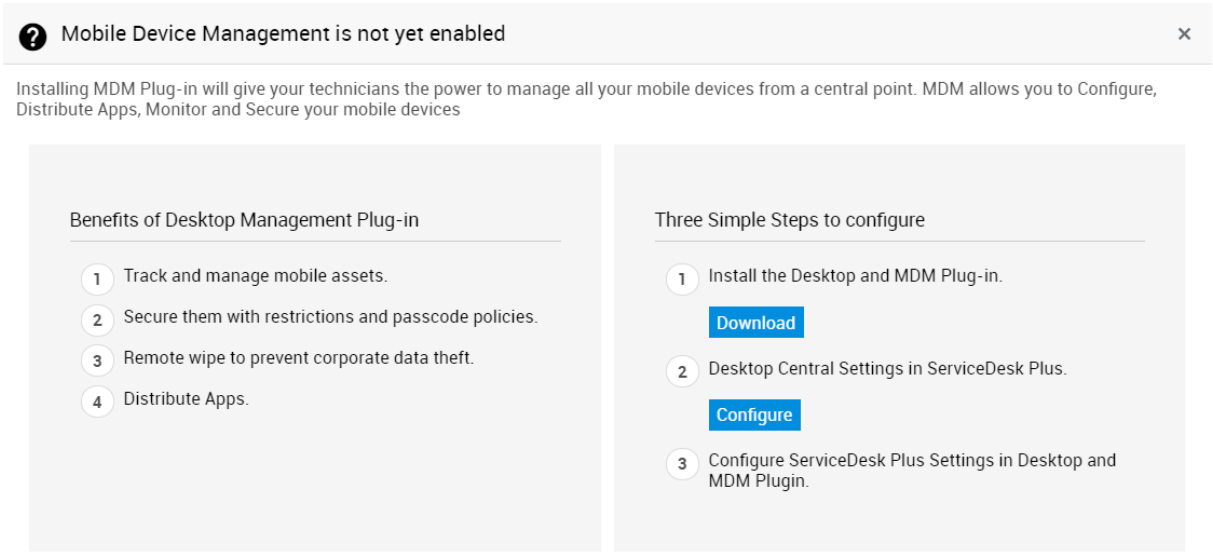

*Obrázok 25: Výber portu*




Po ukončení inštalácie a spustení webového serveru sa automaticky spustí webový prehliadač na adrese *localhost:8080*. Prednastavené prihlasovacie údaju sú používateľské meno *Administrator* a heslo *administrator*. Pre bezpečnú prevádzku je doporučená zmena hesla.

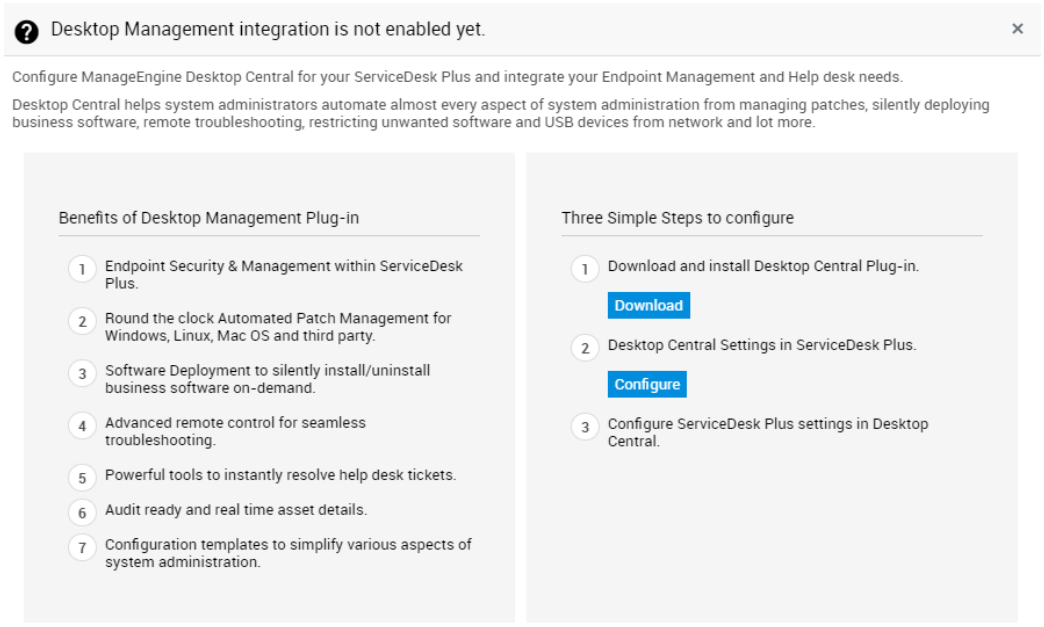
Ako ďalší krok je potrebné si stiahnuť prídavné komponenty (plug-in) Mobile Device Manager a Desktop Centra. Prostredie ServiceDesk Plus ma presmerovalo na stránky, kde mi bolo ponúknuté ich stiahnutie. Postup inštalácie týchto dvoch komponentov je takmer identický s inštaláciou ServiceDesk Plus. Jediná odlišnosť nastala v tom, že komponenty pracujú na samostatných portoch.

*Obrázok 26: Ponuka inštalácie a konfigurácie Mobile Device Manager*

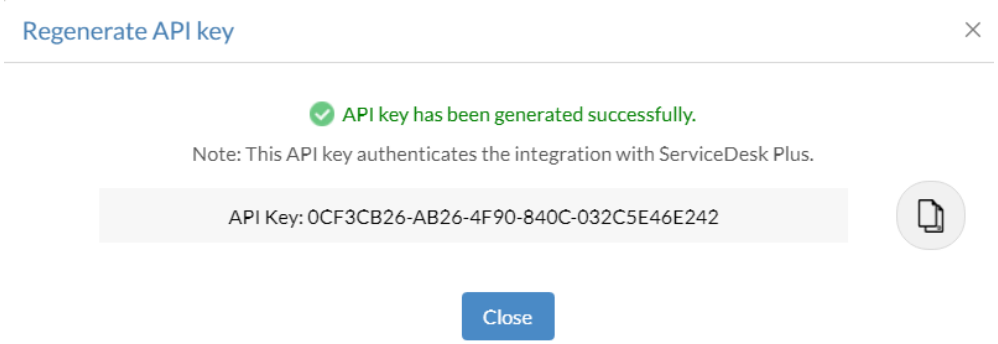



Po nainštalovaní a spustení troch webových serverov je potrebne zaistiť komunikáciu medzi nimi. K tomuto účelu slúži v prostredí Manageengine takzvaný kľúč *API*. Tento som musel vygenerovať na *plug-in* aplikáciach. Po kliknutí na možnosť *Configure* (obrázok č.24 a 25) som bol presmerovaný na rozhranie v ktorom je potrené zadať názov serveru (v našom prípade localhost), číslo portu na ktorom je webový server spustený a kľúč *API* vygenerovaný na *plug-in* aplikácií. Po správnom zadaní potrebných údajov a kliknutí na odkaz otestovať spojenie a uložiť (test connection and save) sa ServiceDesk úspešne synchronizoval s *plug-in* aplikáciou. V aplikácií Mobile Device Manager je nutné nastaviť porty pre komunikáciu aplikácie so spravovanými zariadeniami. V mojom prípade sa jednalo len o potvrdenie predvolených nastavení.

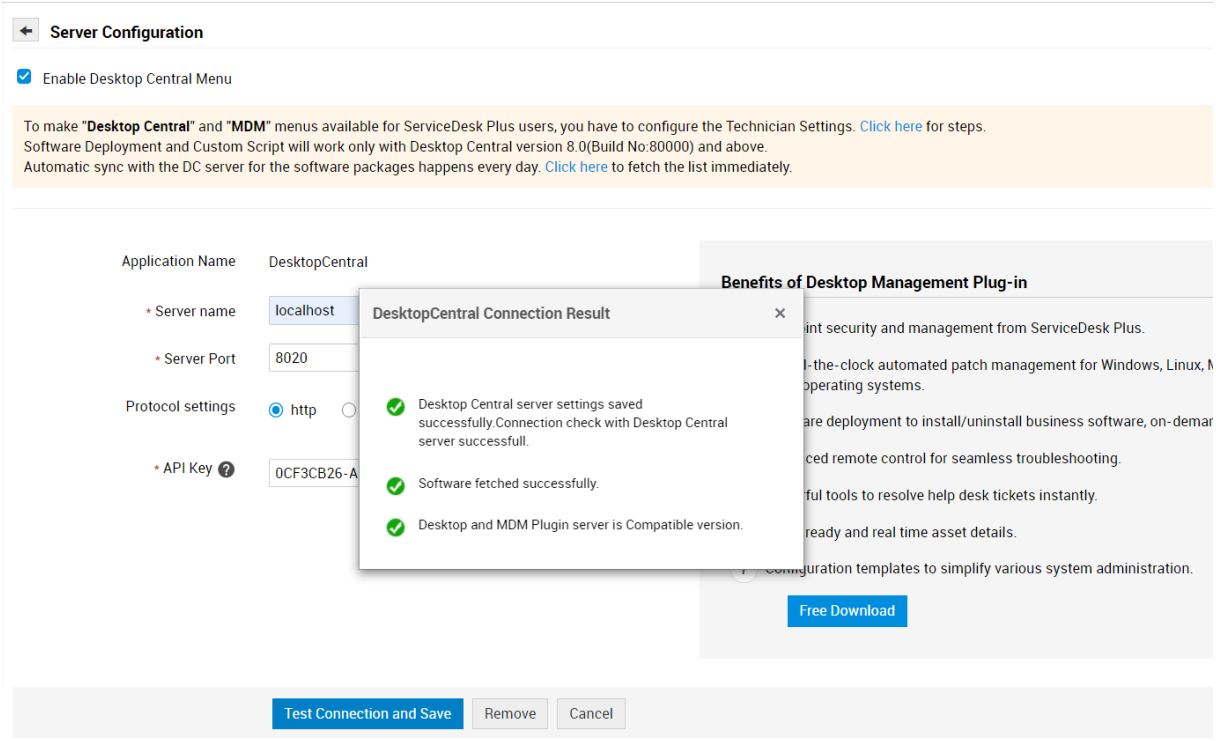
*Obrázok 27: Ponuka inštalácie a konfigurácie Desktop Cenral*



*Obrázok 28: Generácia API kľúča*




*Obrázok 29: Synchronizácia Desktop Central aplikácie so ServiceDesk*




Po vykonaní všetkých vyššie uvedených krokov je prostredie Manageengine MDM pripravené na nasadenie nových zariadení a ich následnú správu.

## 5.3 Zoznámenie sa s prostredím

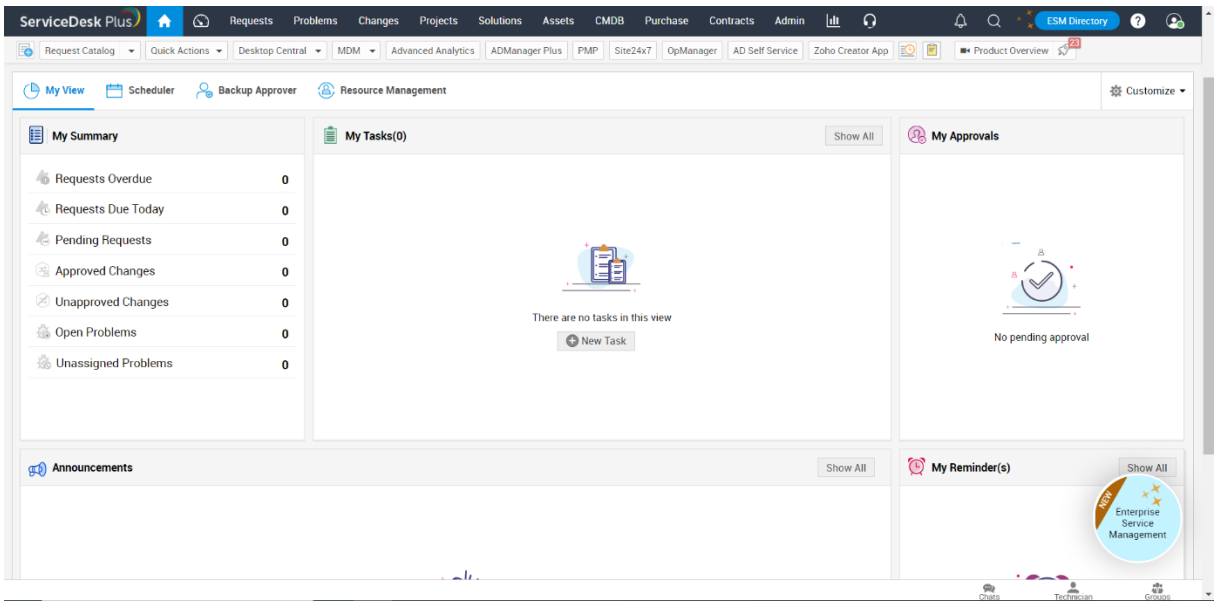
Administrátorské rozhranie systému Manageengine MDM je k dispozícií cez webový prehliadač a tri serverové aplikácie, ktorými sú hlavná aplikácia ServiceDesk Plus a dve *plug-in* aplikácie Mobile Device Manager a Desktop Central. Ako už bolo spomínané pri inštalácií, obe *plug-in* aplikácie musia byť prepojené s centrálnou aplikáciou ServiceDesk Plus pre ich správne fungovanie.

### 5.3.1 Manageengine ServiceDesk Plus

ServiceDesk plus slúži ako centrum pre synchronizáciu všetkých služieb ponúkaných spoločnosťou Manageengine. V mojom prípade ide o centrálu, zabezpečujúci výmenu dát medzi *plug-in* aplikáciami Mobile Device Manager a Desktop Central, ktoré používam na vzdialenú správu Windows zariadení.

V záložkách MDM a Desktop Central sa nachádzajú odkazy na stiahnutie a synchronizáciu *plug-in* aplikácií. Po úspešnej synchronizácií sa v záložkách budú nachádzať odkazy na jednotlivé funkcie *plug-in* aplikácií. Tieto odkazy však z neznámeho dôvodu nie sú funkčné a k funkciám *plug-in* aplikácií sa musí pristupovať cez adresy webových serverov (localhost), na ktorých sú spustené.

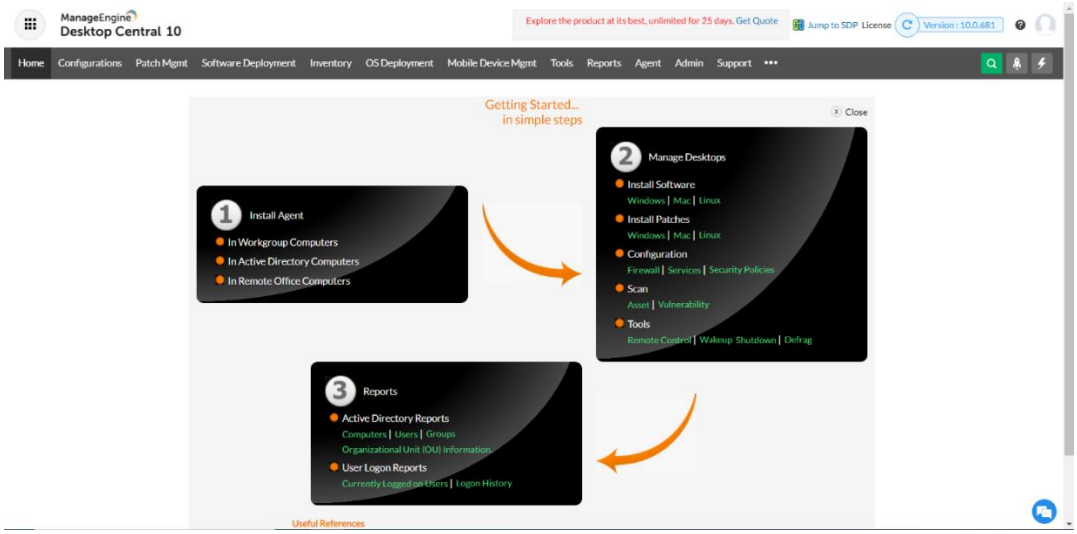
*Obrázok 30: náhľad úvodnej obrazovky a záložiek ServiceDesk Plus*




### 5.3.2 **Manageengine Desktop Central**

Desktop Central je webová *plug-in* aplikácia určená na správu stolných počítačov a notebookov s operačným systémov Windows, Linux a Mac. Poskytuje administrátorovi vykonávanie MDM funkcií ako je distribúcia softvéru, inštalácia a odinštalácia programov, vzdialená kontrola nad zariadením, chatové okno s používateľom spravovaného zariadenia a mnoho ďalších. Desktop Central je spustená na porte číslo 8020 a komunikuje cez port číslo 8383. Pre prihlásenie je potrebné zadať adresu webového serveru, čo je v mojom prípade adresa *localhost:8020*.

*Obrázok 31: Úvodná obrazovka aplikácie Desktop Central*



Po prihlásení sa administrátorovi zobrazí úvodná obrazovka spolu s lištou záložiek a niekoľkými odkazmi na funkcie MDM prostredia.

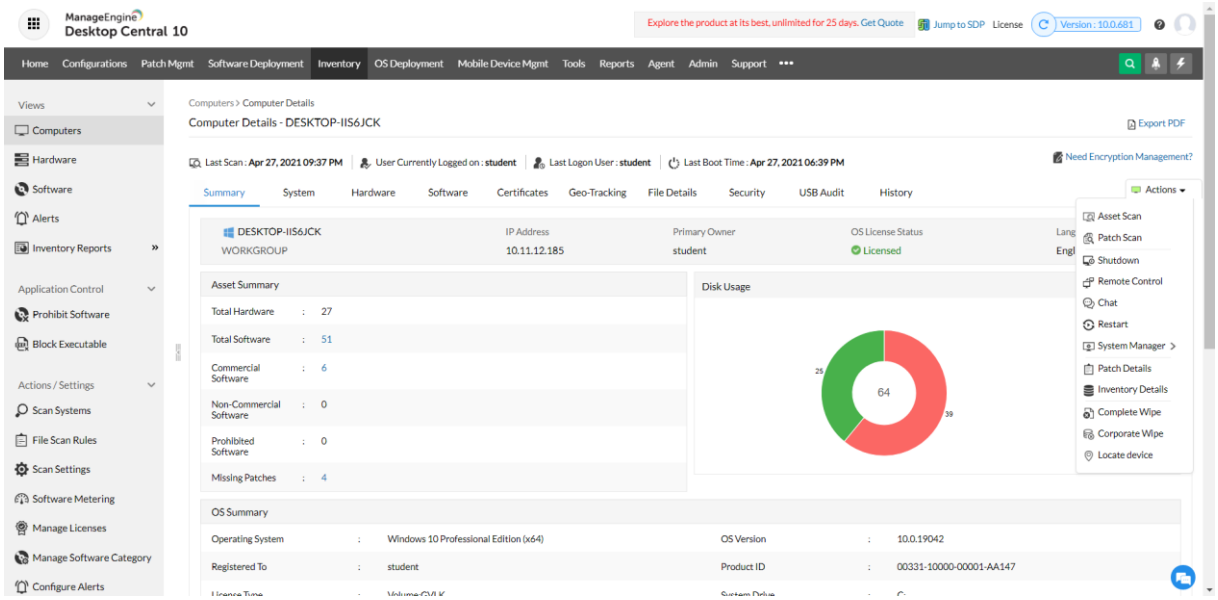
V záložke *Configurations* môže administrátor vytvárať pravidlá a obmedzenia pre spravované zariadenia. Medzi hlavné funkcie patrí špecifikácia *Wi-Fi* pripojenia, obmedzenia webových prehliadačov a stránok, zakázanie prístupu k určitým zložkám a súborom, vynútenie skenovania novo pripojených USB zariadení a mnoho ďalších.

Záložka *Patch Mgmt* slúži na správu aktualizácií pre spravované zariadenie. Prostredie monitoruje úspešné aj neúspešné inštalácie a administrátor má vďaka tomu prehľad o aktualizáciách inštalovaných na zariadenia. Prostredie tiež umožňuje administrátorovi distribuovať vlastné aktualizácie.

V záložke *Software Deployment* môže administrátor vykonávať distribúciu softvéru na spravované zariadenia. Administrátor vytvorí balíček (package) obsahujúci inštalačný súbor a podmienky inštalácie. Distribúcia prebieha v pozadí spravovaného zariadenia a nie je vyžadovaný žiadny zásah zo strany používateľa spravovaného zariadenia.

V záložke *Inventory* má administrátor prístup k zoznamu používaného hardvéru a nainštalovaných aplikácií. V tejto záložke je možné vykonávať pokročilé funkcie MDM ako je vzdialená kontrola nad zariadením, chatové okno, vzdialený reštart alebo vypnutie, skenovanie, vymazanie MDM prostredia alebo všetkých dát a lokalizácia zariadenia.

*Obrázok 32: Rozhranie Inventory Desktop Central*




Záložka *OS Deployment* obsahuje možnosti pre správu a aktualizáciu operačných systémov na spravovaných zariadeniach. Tiež tu môže administrátor vytvárať zálohy používateľských profilov a inštalovať ovládače.

V záložke *Mobile Device Mgmt* sa nachádzajú funkcie pre správu zariadení, ktoré nevyžadujú prítomnosť klienta aplikácie Desktop Central. Zvláštne je, že mnohé funkcie sú identické s funkciami v záložke Inventory. Záložka poskytuje funkcie ako čierna listina aplikácií (blacklist), skenovanie zariadení, automatizácia aktualizácií, distribúcia dokumentov a nasadenie nových zariadení. Ostatné funkcie sú zhodné s funkciami v záložke *Inventory*.

Záložka *Tools* opať obsahuje funkcie na správu zariadení. Duplicitu odkazov na tieto funkcie v prostredí som nebol schopný objasniť.

### 5.3.3 Manageengine Mobile Device Manager Plus

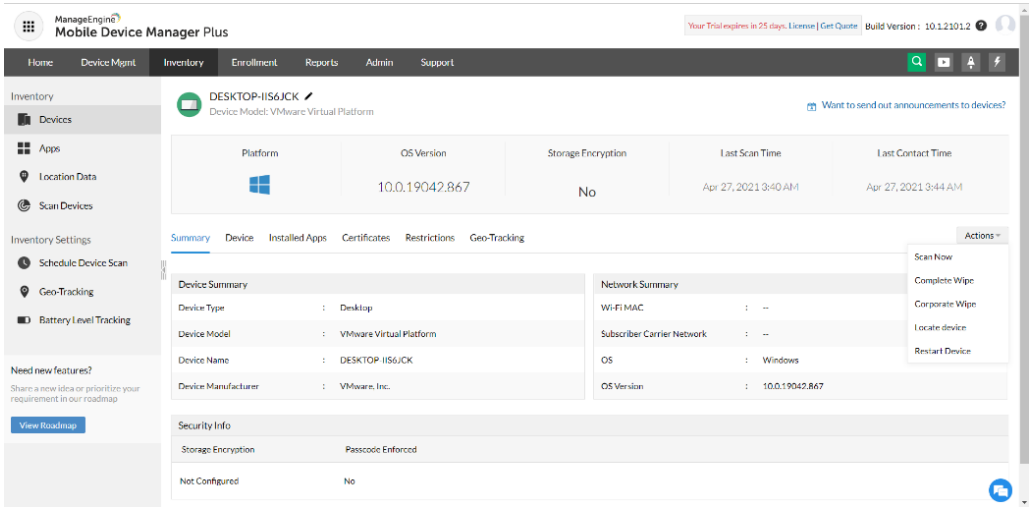
Mobile Device Manager Plus obsahuje väčšinu funkcií určených pre správu mobilných zariadení, ako sú smartfóny a tablety. Umožňuje aj správu stolných počítačov a notebookov, ale keďže nepracuje pomocou klienta, obsahuje menej funkcií pre správu stolných zariadení ako Desktop Central. Pre prihlásenie do aplikácie je potrebné zadať do webového prehliadača adresu webového serveru, v mojom prípade je to adresa localhost:9020. Aplikácia je spustená na porte číslo 9020 a komunikuje pomocou portu číslo 9383. Mobile Device Manager nie je potrebný pokiaľ spravované zariadenie pozostávajú iba z stolných počítačov a notebookov (stačí Desktop Central).

Po prihlásení sa administrátorovi zobrazí rozhranie úvodnej stránky, na ktorom môžeme vidieť niekoľko grafov obsahujúcich informácie o spravovaných zariadenia, okno obsahujúce výsledky pravidelného skenovania zariadení a panel so záložkami odkazujúcimi na ďalšie rozhrania pre správu zariadení.

Záložka *Device Mgmt* presmeruje administrátora do zohrania v ktorom môžem vytvárať profily a skupiny používateľov, ku ktorým sú neskôr priradené nasadené zariadenia. Ďalej sa v záložke nachádzajú funkcie na vytvorenie pravidiel a plánov pre aktualizáciu aplikácií a operačného systému. Prostredníctvom tejto záložky je tiež možné distribuovať dokumenty na spravované zariadenia.

V záložke *Inventory* má administrátor prístup k zoznamu všetkých spravovaných zariadení a informácií o nich vrátane zoznamu nainštalovaných aplikácií, ktoré môže pridať na čiernu listinu (blacklist) a tým znemožniť spravovaným zariadeniam ich spustenie. Ďalej tu môže administrátor vykonávať akcie ako skenovanie zariadení, vzdialený reštart, vymazanie všetkých MDM prvkov zo zariadenia, kompletné vymazanie dát zo zariadenia spojené s uvedením do továrneho nastavenia a lokalizáciu zariadenia.

*Obrázok 33: Rozhranie inventory MDM PLUS*



Záložka *Enrollment* slúži k nasadeniu nových zariadení do MDM prostredia. Nasadenie je realizované pomocou vygenerovaného inštalačného súboru ktorého priebeh je preddefinovaný v súbore bat. V tejto záložke je tiež možné špecifikovať podmienky, za ktorých bude zariadenia pridané do MDM prostredia.

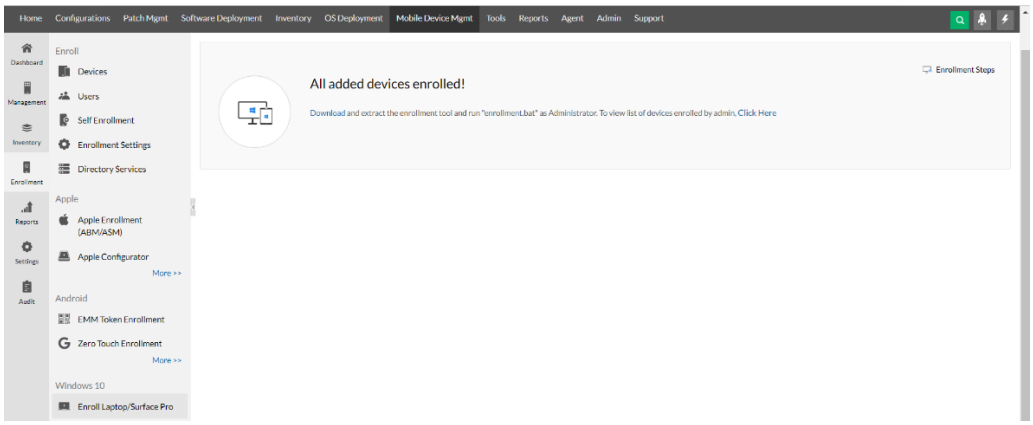
V záložke *Reports* sa nachádza široký zoznam správ obsahujúcich informácie o zariadeniach, aplikáciách a tiež niekoľko možností zoradenia zariadení podľa zvolených parametrov. V záložke je tiež možné naplánovať vytváranie správ podľa potreby Administrátora.

V záložke *Admin* je možné meniť nastavenia MDM prostredia podľa potreby administrátora a tiež bližšie špecifikovať spôsob komunikácie so zariadeniami (adresy, porty a podobne).

## 5.4 Nasadenie prostredia na klientské počítače

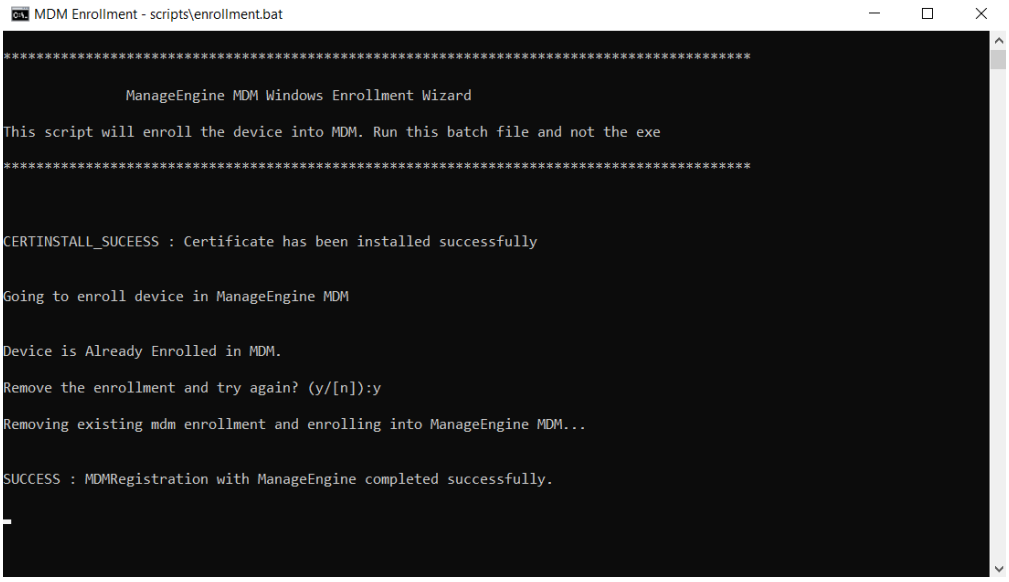
Pre nasadenie nových zariadení do prostredia Manageengine MDM je potrebné vytvoriť inštalačný súbor. Keďže som na používal virtuálne stroje simulujúce stolné počítače, inštalačný súbor je potrebné vygenerovať v prostredí Desktop Central. V záložke *Mobile Device Mgmt* je potrebné prejsť na odkaz *Enrollment* a následne stiahnuť inštalačný súbor a prekopírovať ho na zariadenie, ktoré chceme pridať do MDM prostredia.

*Obrázok 34: Ponuka stiahnutia inštalačného súboru*




Po presunutí inštalačného súboru na používateľské zariadenie je potrebné ho rozbaliť a spustiť program enrollment.bat ako administrátor. Po spustení program nainštaluje klienta prostredia Desktop Central a pridá zariadenie do MDM prostredia. Po úspešnom dokončení tohto kroku je zariadenie pripravené na správu pomocou MDM.

*Obrázok 35: Hláška po úspešnom nasadení prostredia*




## 5.5 Testovanie funkcií MDM na nasadených zariadeniach

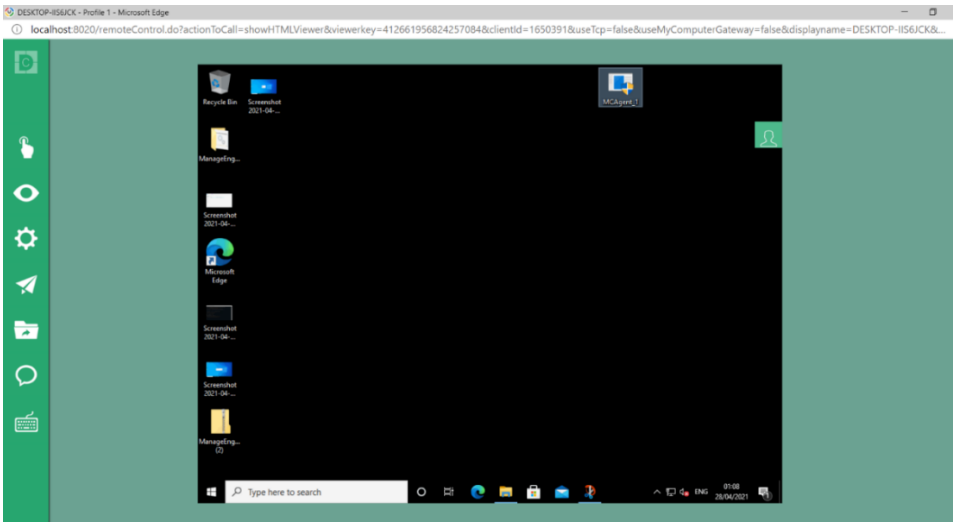
V nasledujúcich testoch som si overil si overil funkčnosť prostredia Manageengine MDM. Keďže na testovanie používal stolné počítače, všetky funkcie MDM som aplikoval prostredníctvom prostredia Desktop Central. V tomto testovaní som demonštroval funkcie ako vzdialená kontrola nad zariadením, *Blacklist* a *Whitelist*, chatové okno, vzdialený reštart, distribúciu softvéru a systémového správcu.

### 5.5.1 Vzdialená kontrola nad zariadením

V záložke *Inventory* je možné funkciu vzdialenej kontroly. Po zahájení sa používateľovi spravovaného zariadenia zobrazí okno s dôvodom prevzatia kontroly nad jeho zariadením a bude mu zablokovaný prístup ku vstupným zariadeniam (klávesnica a myš).

Rovnako ako pri prostredí SOTI MobiControl využíva Desktop Central protokol vzdialenej plochy (RDP) a prevzatí kontroly som bol odpojený od vzdialenej plochy a pripojiť sa mi podarilo až po ukončení vzdialenej kontroly zariadenia.

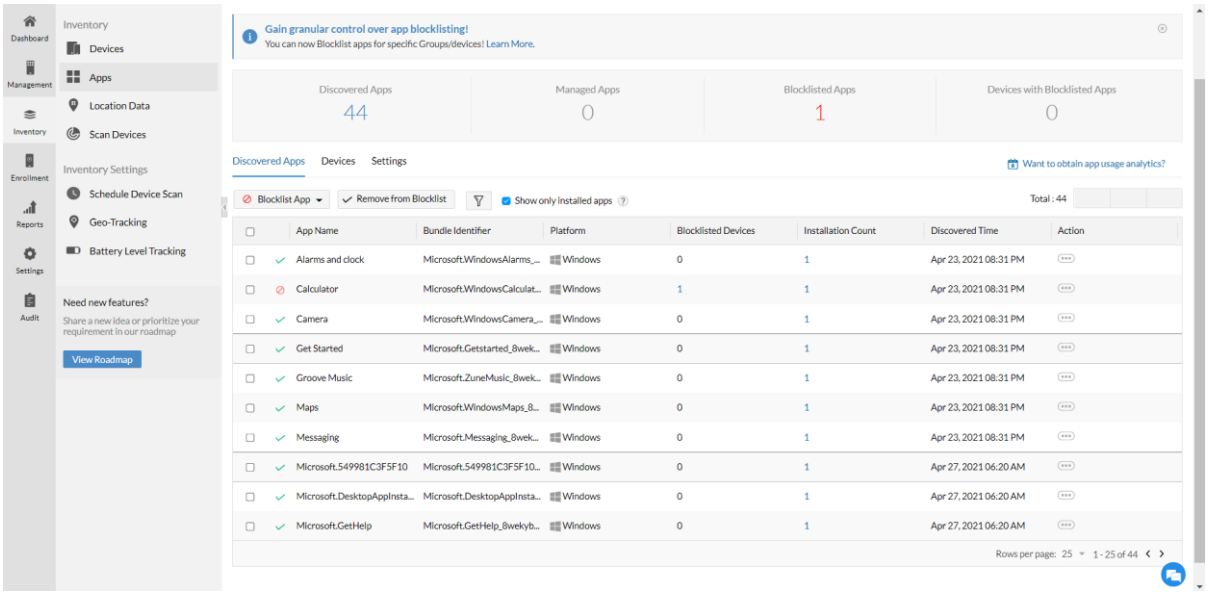
*Obrázok 36: Okno vzdialenej kontroly nad zariadením*



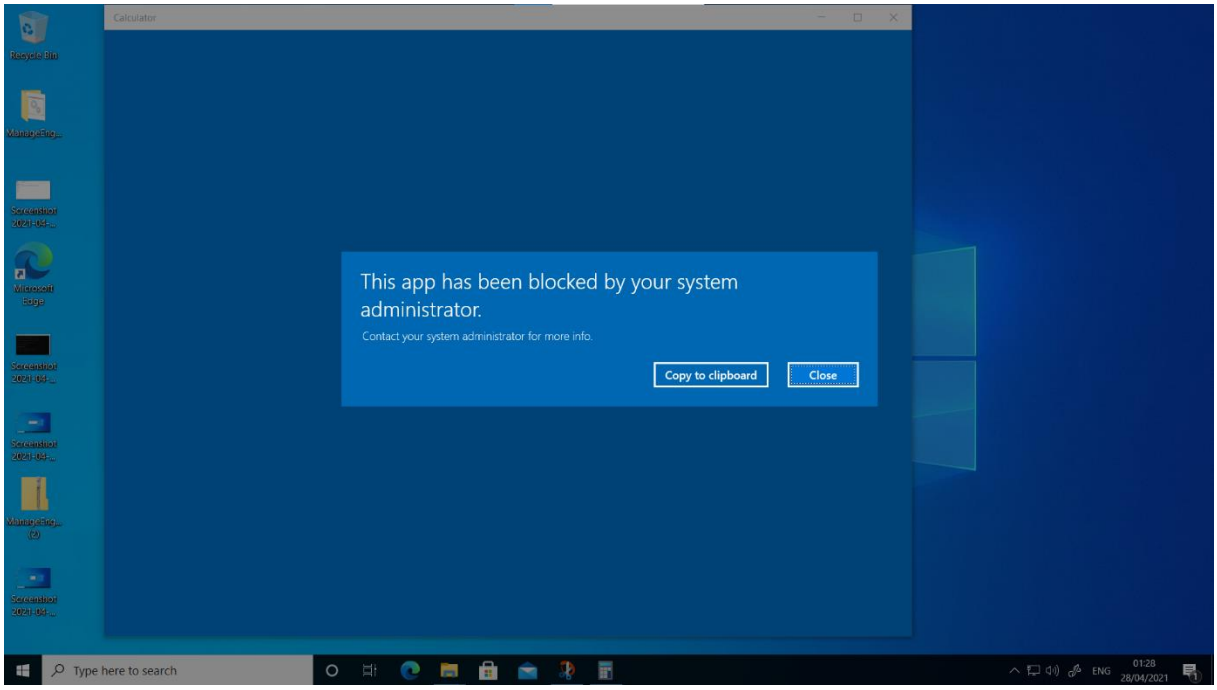
### 5.5.2 **Blacklist a Whitelist**

Z hľadiska bezpečnosti je niekedy potrebné zabrániť používateľom použitie niektorých aplikácií. K tomuto slúži takzvaná čierna listina (Blacklist), na ktorú administrátor umiestni zoznam aplikácií ktoré budú po jeho potvrdení zablokované. Túto funkciu nájdeme v záložke Mobile Device Mgmt pod kartou APPS. Pre demonštráciu funkčnosti som zablokoval aplikáciu kalkulačka.

*Obrázok 37: Rozhrane pre aplikáciu Blacklistu a Whitelistu*



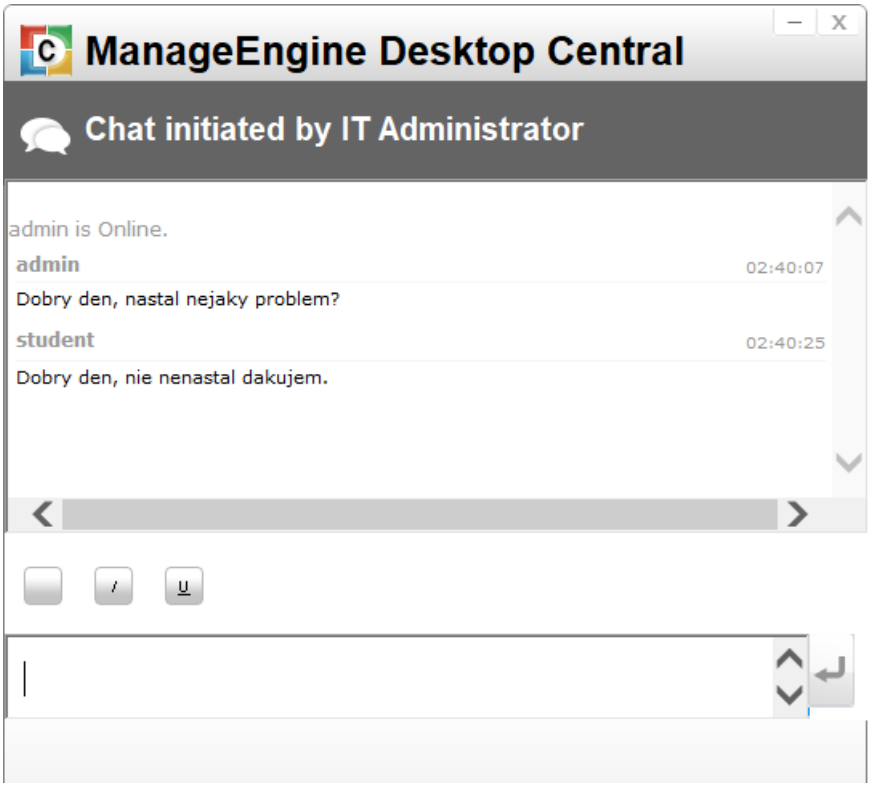

*Obrázok 38: Hlásenie zablokovane aplikácie*



### 5.5.3 **Chatové okno**

Administrátor môže v prípade potreby komunikovať a riešiť technické problémy s používateľom prostredníctvom chatového okna. Toto okno nejak nenarušuje používateľov prístup k počítaču.

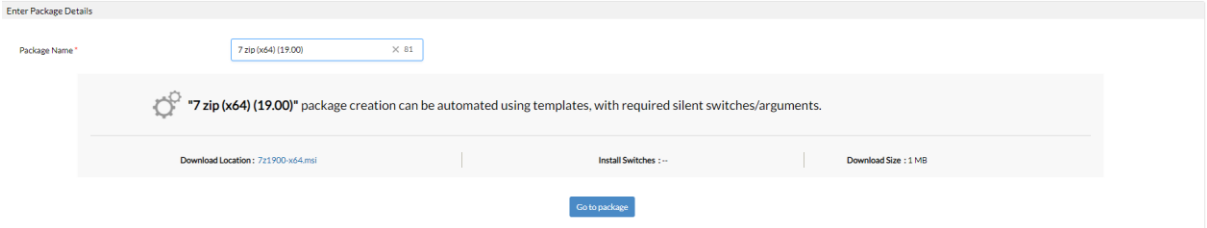
*Obrázek 39: Chatové okno medzi používateľom a administrátorom*



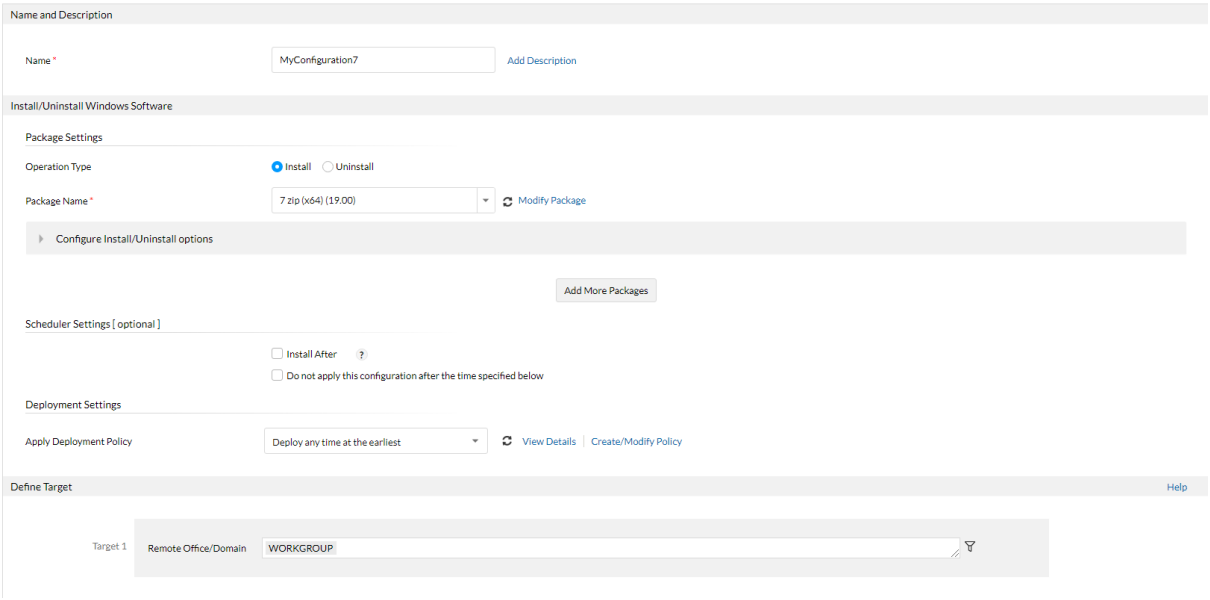

### 5.5.4 **Distribúcia softvéru**

Prostredie Desktop Central poskytuje veľmi jednoduchú cestu pre vzdialenú distribúciu a inštaláciu softvéru. V záložke Software Deployment je najprv potrebné vytvoriť balíček, do ktorého administrátor nahrá inštalačný súbor. Po zvolení súboru mi prostredie ponúklo možnosť automatického vytvorenie balíčku, ktorú som aj využil. Po vytvorení balíčkov si administrátor pomocou príkazu Install software vytvorí konfiguráciu v ktorej pridá balíčky špecifikuje podmienky inštalácie a tiež zvolí zariadenia alebo skupiny, na ktoré bude konfigurácia aplikovaná. Osobne som pri distribúcií používal metódu Deploy Immiediately.

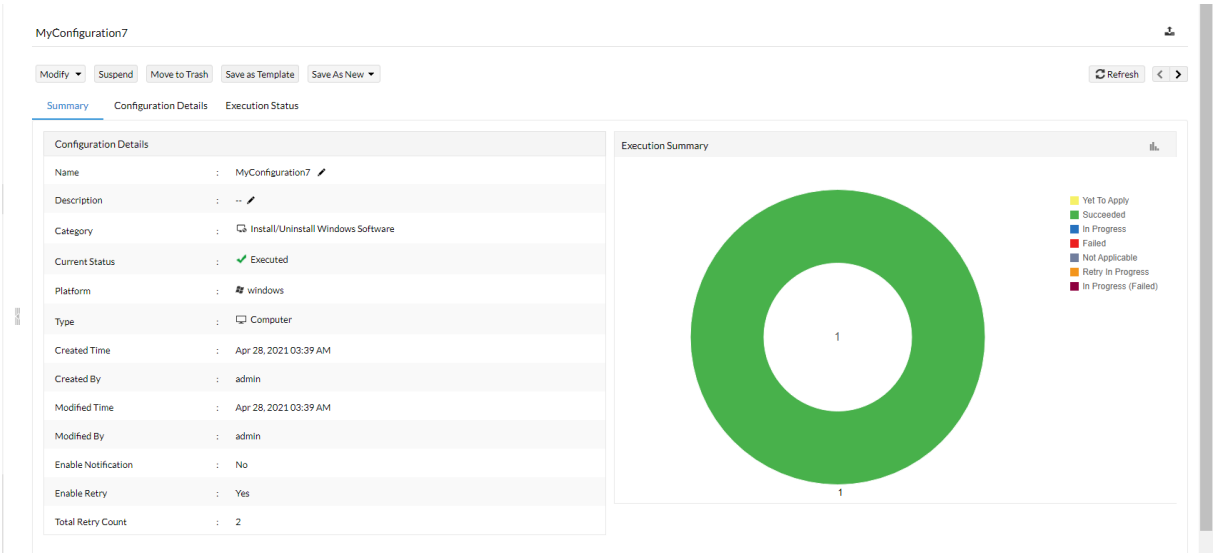
*Obrázok 40: Vytvorenie balíčku* v Desktop Central



*Obrázok 41: Vytvorenie a nasadenie konfigurácie*




*Obrázok 42: Rozhranie pre sledovanie pre sledovanie stavu konfigurácií*

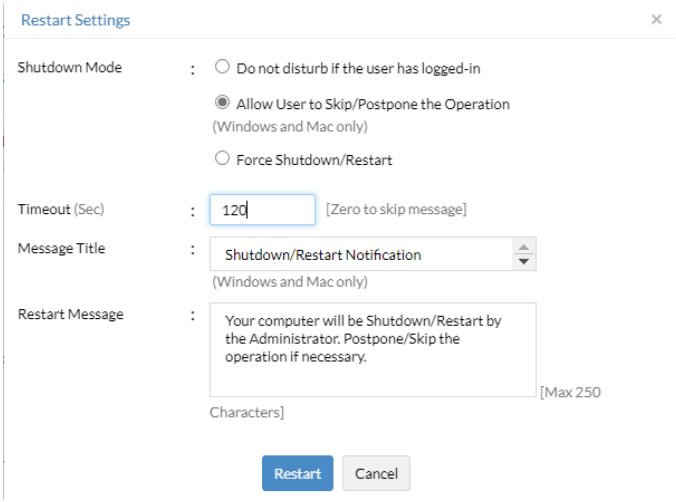



Pre otestovanie tejto funkcie som použil inštalačné súbory pre aplikácie *Putty* a *7-Zip*. Distribúcia a inštalácia a inštalácia trvala približne jednu až dve minúty. Po potvrdení príkazu na distribúciu je možné sledovať jej priebeh v okne *View Configurations*. Keďže celá inštalácia prebieha v pozadí a bez upozornenia, nemohol som ju na klientskom počítači zdokumentovať.

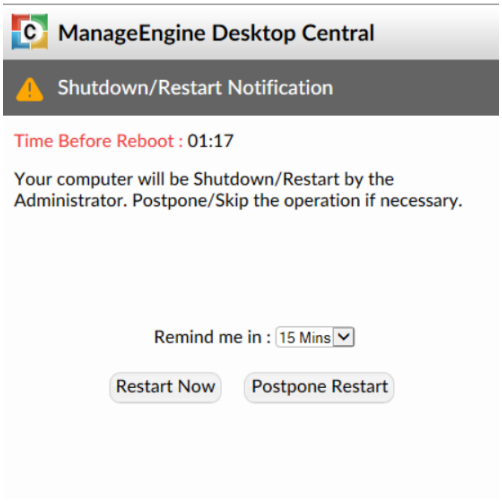
### 5.5.5 **Vzdialený reštart**

Po aktivovaní funkcie vzdialený reštart si administrátor vyberie či chce reštart vynútiť, dovoliť používateľovi ho odložiť alebo v prípade aktívnosti používateľa reštart zrušiť. Tiež zadá čas, za ktorý sa reštart vykoná. Používateľovi sa zobrazí varovanie o pláne reštartu.

*Obrázok 43: Vytvorenie príkazu na reštart*




*Obrázok 44: Varovné okno pred reštartom*

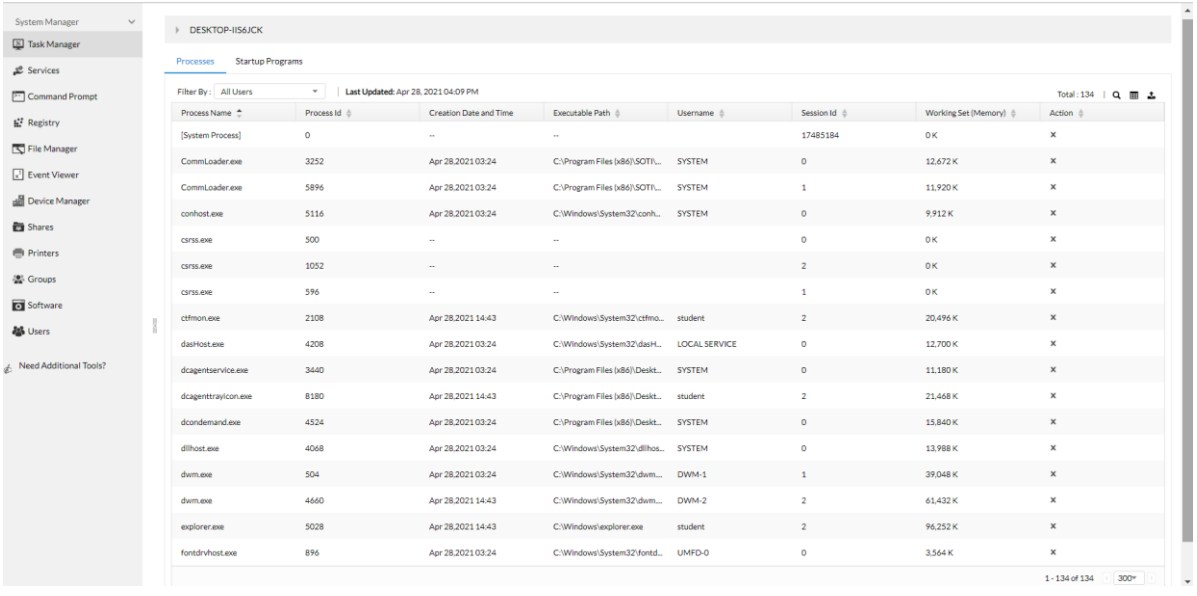



### 5.5.6 **Systémový správca**

Desktop Central poskytuje administrátorovi prístup k systémovému správcovi na spravovaných zariadeniach. V tomto prostredí je možné spravovať dôležité procesy, hardvér, ovládače, registre a mnoho ďalších bez akéhokoľvek zásahu do činností používateľa. Toto prostredie poskytuje prístup k nasledujúcim funkciám:

- Správca úloh,
- služby,
- príkazový riadok,
- zoznam registrov,
- prehliadač súborov,
- správca zariadení,
- správca nainštalovaného softvéru.

*Obrázok 45: Rozhranie pre správu systému*



## 5.6 Zhodnotenie testovania

Inštalácia a konfigurácia prebehla bezproblémovo. Technické parametre virtuálneho počítača, na ktorom som prostredie testoval sú takmer zhodné s minimálnymi požiadavkami uvedenými v tabuľke 6. Pri týchto parametroch trvala inštalácia jednotlivých súčastí pomerne dlho. Počas inštalácie boli prostriedky počítača využité takmer na plný výkon a kompletná inštalácia zabrala vyše hodinu času. Vo firemnom prostredí by som počítač s minimálnymi požiadavkami na hardvér odporučil iba na správu MDM prostredia.

Pre správu zariadení som používal hlavne prostredie Desktop Central. Prostredie je podľa mňa výborne spracované a jednoduché na obsluhu. Ďalšou veľkou výhodou je výborná synchronizácia a výmena údajov medzi prostrediami Desktop Central a Mobile Device Manager Plus. Testované funkcie prebehli bezproblémovo a ich obsluha je intuitívne spracovaná, čo je veľkou výhodou pre správcov ktorý s MDM prostredím ešte nepracovali.

Za nedostatky prostredia považujem vysokú náročnosť na technické parametre administrátorského počítača, odkaz na rovnakú funkciu prostredia s viacerých záložiek v prostredí a neprítomnosť funkcie BitLocker, ktorá sa však dá nahradiť zablokovaním jednotlivých funkcií a programov.

# 6 Porovnanie testovaných MDM prostredí

V tejto kapitole som sa zoberal porovnaním funkcií prostredí Manageengine MDM a SOTI MobiControl z hľadiska zložitosti použitia, odozvy pri vykonávaní zmien, poskytovaných funkcií, náročnosti na systémové požiadavky a ich využiteľnosť v praxi. Oboje použité prostredia sú implementované prostredníctvom verzie On-premise, ktorá umožňuje administrátorovi spravovať server služby MDM.

## 6.1 Systémové požiadavky

Z hľadiska náročnosti na systémové požiadavky je systém SOTI MobiControl veľmi výhodný. Jeho náročnosť na výkon je veľmi nízka pretože pre svoju prevádzku používa iba jeden webový server.

Pokiaľ chceme v prostredí Manageengine MDM spravovať mobilné telefóny aj stolné počítače, je nutná inštalácia niekoľkých webových serverov, čo sa odráža na vysokej náročnosti na operačnú pamäť administrátorského zariadenia.

## 6.2 Zložitosť správy MDM

Osobne sa mi lepšie pracovali s prostredím Manageengine, pretože je podľa môjho názoru spracovaný jednoducho a intuitívne. Funkcie pre distribúciu softvéru sú zjednotené do jedného rozhrania a jednoduché na pochopenie. Jediné čo mi na prostredí prekážalo bola duplicita odkazov na funkcie MDM.

Práca s prostredím SOTI MobiControl je pomerne zložitá. Už pri nasadení zariadenia musí administrátor absolvovať zdĺhavý proces vytvárania pravidiel pre nasadenie a vytvorenie inštalačného súboru. Pri distribúcií softvéru a vzdialenej kontrole zariadení je nutná inštalácia a použitie osobitných programov. Osobne sa mi s prostredím SOTI MobiControl pracovalo horšie ako s prostredím Manageengine MDM.

## 6.3 Odozva pri vykonaní zmien

Časová odozva pri vykonávaní zmien pomocou prostredí MDM závisí od niekoľkých faktorov:

- Rýchlosť internetového pripojenia administrátorského aj používateľského počítača,
- veľkosť prenesených dát a zložitosť inštalácie pri distribúcií softvéru,
- výkon a aktuálne vyťaženie spravovaného počítača.

Testované prostredia mali pomerne zhodnú odozvu. Keďže boli testované virtuálne počítače pripojené do školskej siete Eduroam, odozva po použití funkcií MDM bola veľmi malá. Väčšina MDM funkcií bola aplikovaná do niekoľkých sekúnd. Pri distribúcií softvéru proces zahral jednu až dve minúty.

## 6.4 Výhody a nevýhody testovaných prostredí

Na záver porovnania by som rád zdôraznil hlavné klady a zápory prostredí Manageenigne MDM a SOTI MobiControl, ktoré som spozoroval pri inštalácií a testovaní.

Výhody prostredia Manageengine:

- Jednoduché a intuitívne použitie,
- funkcie prostredia sú centralizované a prehľadné,
- výborné spracovanie distribúcie softvéru,
- poskytuje väčei množstvo funkcií ako SOTI MobiControl.

Nevýhody prostredia Manageengine:

- Vysoká náročnosť na systémové požiadavky,
- neprítomnosť funkcie BitLocker,
- pri nasadení je potrebné priradiť zariadenie ku profilu a skupine,
- duplicita odkazov na funkcie.

Výhody prostredia SOTI MobiControl:

- Nízka náročnosť na systémové požiadavky,
- lepšie spracované rozhranie pre vzdialenú kontrolu nad zariadeniami ako Manageengine MDM,
- automatické priradenie profilu a skupiny pri nasadení.

Nevýhody prostredia SOTI MobiControl:

- Neprítomnosť funkcií Blacklist a Bitlocker,
- proces distribúcie softvéru je veľmi zložitý,
- inštaláciu SQL serveru je nitné vykonať samostatne.

# Záver

V tejto bakalárskej práci som snažil čitateľovi čo najviac priblížiť, predstaviť a porovnať platformy pre vzdialenú správu zariadení s operačným systémom Windows. Spomunté platformy boli Manageengine MDM, hexnode MDM, Safetica, Knox Manage, Miradore a SOTI MobiControl. MDM systémy sú v dnešnej dobe veľmi populárne keďže v súčastnej dobe je nariadená dištančná forma vzdelávania a práca z domu(home office).

Teoretická časť bola venovaná popisu fungovania a implementácie MDM prostredí a porovnanie už spomenutých šiestich MDM prostredí. Pri každej s popisovaných platforiem sa nachádza stručný popis prostredia a zoznam funkcií, ktoré poskytuje.

Praktická časť bola venovaná inštalácií, konfigurácií, administrácií a porovnaniu prostredí Manageengine MDM a SOTI MobiControl. Pri každej platforme sa nachádza popis inštalácie, postup nasadenia prostredia na nové zariadenia, postup testovania a tiež obsahuje návody na použitie ich základných funkcií. Obe prostredia sú implementované pomocou lokálneho serveru (On-premise) a zároveň sú to jediné dve prostredia, ktoré poskytujú bezplatnú testovaciu verziu pre tento typ implementácie.

Z dôvodu nutnosti dištančnej výuky som nebol schopný testovať prostredia až na piatich rôznych zariadeniach a musel som použiť virtuálne počítače vytvorené pomocou prostredia VMware. Problémom tiež bolo, že v dnešnej dobe existujú iba dve verzie operačného systému Windows(8 a 10) podporované aktualizáciami spoločnosti Microsoft.

Prostredie SOTI MobiControl sa ukázalo ako veľmi užitočné pre správu zariadení so zastaralým operačným systémom. Všetky nasadené zariadenia so systémom Windows spadajú pri ich správe do kategórie *Widnows Desktop Classic*, čo znamená že postup ich správy je jednotný. Z hľadiska obtiažnosti obsluhy mi systém prišiel v niektorých oblastiach až príliš zložitý, najmä pri Vzdialenej kontrole zariadení a distrubúcií softvéru. Prostredie by som teda odporučil administrátorom, ktorý už majú s MDM prostredím skúsenosti.

Prostredie Manageengine MDM mi napriek potrebe inštalácie niekoľkých webových serverov pripadalo podstatne jednoduchšie z hľadiska orientácie a zložitosti použitia. Na správu stolných počítačov a notebookov administrátorovi stačí prostredie *Desktop Central*. Výborná synchronizácia s prostredím ServiceDesk plus umožňuje administrátorovi spojiť MDM funckie s ďalšími produktami spoločnosti Manageengine, kedykoľvek uzná za vhodné. Za jediný nedostatok prostredia považujem vysoké nároky MDM prostredia na systémové požiadavky administrátorského počítača. Toto prostredie je vhodné pre menej skúsených administrátorov MDM prostredí.

Nie je možné určiť jedno ideálne MDM prostredie. Výber prostredia závisí na preferenciách firiem a systémových administrátorov. Keďže všetky spomenuté MDM prostredia sú platené služby, je na každej firme aby zvážila, či je potrebné implementovať MDM do firemného prostredia.

Pevne verím, že táto bakalárska práca prinesie každému čitateľovi užitočné informácie v tejto oblasti a prípadne pomôže pri výbere a konfigurácií platformy pre správu mobilných zariadení.

# Použitá literatúra


[1] What's the difference between MDM, MAM, EMM and UEM? [online]. Lucas Mearian, 2017 [cit. 2021-4-28]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[2] Mobile device management (MDM) [online]. Erica Mixon, 2020 [cit. 2021-4-27]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[3] BYOD Requires Mobile Device Management [online]. McKinsey & Company, 2012 [cit. 2021-4-28]. Dostupné z: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/High%20Tech/PDFs/BYOD_means_so_long_to_company-issued_devices_March_2012.ashx

[4] Mobile Device Management (MDM) software [online]. [cit. 2021-4-28]. Dostupné z: https://www.manageengine.com/mobile-device-management

[5] Manage Apple, Android, Windows, & Chrome Devices [online]. [cit. 2021-4-28]. Dostupné z: https://www.manageengine.com/mobile-device-management/features.html

[6] Manage any platform and any device [online]. [cit. 2021-4-28]. Dostupné z: https://www.hexnode.com/mobile-device-management/

[7] Hexnode [online]. [cit.2021-4-28]. Dostupné z: https://en.wikipedia.org/wiki/Hexnode#:~:text=Hexnode%20MDM%20enables%20centralized%20device,down%20devices%20into%20kiosk%20mode.

[8] Safetica Mobile [online]. [cit.2021-4-28]. Dostupné z: https://www.safetica.com/products/safetica-mobile

[9] Choose the right solution for your business [online]. [cit. 2021-4-28]. Dostupné z: https://www.safetica.com/products/products-features

[10] Mobile management made easy [online]. [cit. 2021-4-28]. Dostupné z: https://www.samsungknox.com/en/solutions/it-solutions/knox-manage

[11] Windows [online]. [cit. 2021-4-28]. Dostupné z: https://docs.samsungknox.com/admin/knox-manage/configure-windows.htm

[12] The smarter way to manage devices [online]. [cit. 2021-4-28]. Dostupné z: https://www.miradore.com/

[13] Miradore makes device management easy [online]. [cit. 2021-4-28]. Dostupné z: https://www.miradore.com/product/?utm_medium=ppc&utm_campaign=%5BSearch%5D%5BGL%5D%5BEN%5D+Brand&utm_source=adwords&utm_term=%2Bmiradore&hsa_src=g&hsa_ver=3&hsa_grp=113710734931&hsa_kw=%2Bmiradore&hsa_acc=3191970914&hsa_mt=b&hsa_tgt=aud-353220343347:kwd-372614913064&hsa_ad=460752251021&hsa_cam=11002184147&hsa_net=adwords&gclid=CjwKCAjwj6SEBhAOEiwAvFRuKGEx1JhcshqTac_NH9k-Pn3I3pSNgbFuhOif_JvWU3N3rIxNcRLy7xoCPcQQAvD_BwE

[14] Manage Your Devices Securely with SOTI MobiControl [online]. [cit. 2021-4-28]. Dostupné z: https://www.soti.net/products/soti-mobicontrol/

[15] What is SOTI MobiControl? [online]. [cit. 2021-4-28]. Dostupné z: https://comparecamp.com/soti-mobicontrol-review-pricing-pros-cons-features/

[16] System Requirements [online]. [cit. 2021-4-28]. Dostupné z: https://www.soti.net/mc/help/v14.2/en/setup/installing/system_requirements.html
[17] Network Ports [online]. [cit. 2021-4-28]. Dostupné z: https://www.soti.net/mc/help/v14.0/en/setup/installing/network_ports.html
[18] .NET Core [online]. [cit. 2021-4-28]. Dostupné z: https://www.soti.net/mc/help/v14.0/en/setup/installing/network_ports.html
[19] Java SE and Java EE applications [online]. [cit. 2021-4-28]. Dostupné z: https://www.ibm.com/docs/en/odm/8.8.1?topic=application-java-se-java-ee-applications
[20] Microsoft SQL Server [online]. [cit. 2021-4-28]. Dostupné z: https://en.wikipedia.org/wiki/Microsoft_SQL_Server
[21] System Requirements for Mobile Device Manager Plus [online]. [cit. 2021-4-28]. Dostupné z: https://www.manageengine.com/mobile-device-management/system-requirements.html
[22] Mobile Device Manager Plus (MDM) Architecture [online]. [cit. 2021-4-28]. Dostupné z: https://www.manageengine.com/mobile-device-management/mobile-device-manager-plus-architecture.html
[23] [online]. [cit. 2021-4-29]. Dostupné z: https://web.archive.org/web/20160801184227/http://www.sms-wiki.org/p_65-binary-sms.html
[24] BYOD Demand and Information Security [online]. Glenn Ford, 2014 [cit. 2021-4-29]. Dostupné z: http://cybersecurity-hq.blogspot.com/2014/02/byod-consumer-demand-and-information.html
[25] Mobile device management [online]. [cit. 2021-4-29]. Dostupné z: https://en.wikipedia.org/wiki/Mobile_device_management