



Safetica Technologies

Produktová dokumentace

Safetica Discovery

Safetica Protection

Microsoft Bitlocker

Verze 9.9.x

Jan Strnad, AUTOCONT

OBSAH

OBSAH	2
1. POPIS SAFETICA TECHNOLOGIES.....	6
1.1. Ochrana dat	6
1.2. Soulad s normami a zákony	6
1.3. způsoby, jak se citlivé dokumenty mohou dostat mimo kontrolu	6
1.4. Přehled o fungování firmy	6
1.5. Dohled nad produktivitou.....	7
1.6. Zvýšení efektivity personálních nákladů	7
1.7. Kontrola připojovaných zařízení	7
2. ARCHITEKTURA SAFETICA.....	8
2.1. Server	9
2.2. Konzole.....	9
2.3. WebSafetica	9
2.4. Safetica Agent	10
2.5. Klient	10
2.6. Databáze	10
3. HW A SW POŽADAVKY NA INSTALACI SAFETICA.....	11
3.1. Požadavky na infrastrukturu	11
3.2. HW a SW požadavky	12
3.2.1. Požadavky na klientské systémy	12
3.2.2. Požadavky na management server Safetica	12
4. ZPŮSOB ZAJIŠTĚNÍ KOORDINACE REALIZACE PŘEDMĚTU PLNĚNÍ S BĚŽNÝM PROVOZEM	13
5. ZÁKLADNÍ KONFIGURACE SAFETICA MANAGEMENT SERVERU	14
5.1. Základní konfigurace Safetica management serveru.....	15
6. NASTAVENÍ DISCOVERY	16
6.1. Nastavení a uložení filtrů	18
7. NASTAVENÍ POLITIKY SUPERVISORU.....	23
7.1. Správa webů.....	23
7.2. Správa aplikací	26
7.3. Reportování blokovanych webů a aplikací	28
8. NASTAVENÍ PROTECTION (DLP)	29

8.1. Datové kategorie.....	30
8.1.1. Obsahová klasifikace dat.....	31
8.1.2. Kontextová klasifikace dat	34
8.1.2.1 Nastavení aplikačního pravidla:	34
8.1.2.2 Nastavení webového pravidla	36
8.1.2.3 Nastavení pravidla umístění	37
8.1.3. Vizualizace zobrazuje výsledek klasifikace dat:	39
8.2. DLP politiky	40
8.2.1. Obecná pravidla	41
8.2.2. Datová pravidla	43
8.2.3. Aplikační pravidla	47
8.3. DLP záznamy	50
8.4. Zóny.....	51
8.5. Hlídní disků.....	53
8.6. Správce zařízení	54
8.6.1. Definice zón	54
8.6.2. Nastavení portů počítače.....	55
8.7. Bitlocker zařízení.....	56
8.8. Bitlocker Disky.....	58
8.8.1. Nastavení šifrovací politiky počítače.....	59
9. NASTAVENÍ SPRÁVCŮ A PŘÍSTUPOVÝCH PRÁV K MGMT KONZOLI	62
9.1. Definice uživatele Safetica	63
9.2. Nastavení práv uživatele	64
9.2.1. Výběr uživatele,	65
9.2.2. Výběr skupiny.....	65
9.2.3. Nastavení přístupu	66
9.2.3.1 Položka „Název“	66
9.2.3.2 Položka „Nastavení“	68
9.2.3.3 Položka „Záznamy“	69
9.3. Příklad nastavení pro uživatele User 2.....	70
10. ÚDRŽBA.....	72
10.1. Přehled koncových stanic	73
10.2. Aktualizace a nasazení	74

10.3. Deaktivace koncových stanic	77
10.4. Nastavení integrace	79
10.4.1. Integrovaný režim	79
10.4.2. Integrace aplikací	80
10.4.3. Důvěryhodné servery	81
10.4.4. Problematická zařízení	81
10.5. Nastavení koncových stanic	82
10.6. Sběr informací	83
10.7. Správa databáze	85
10.8. Správa přístupů	86
10.9. Správa Licencí	86
10.10. Kategorie	87
10.10.1. Kategorie aplikací	87
10.10.2. Kategorie webů	89
10.10.3. Kategorie přípon	91
10.11. Využití počítačů	92
11. INSTALACE KLIENTSKÉHO SOFTWARE	93
11.1. Instalace Safetica Agentů	93
11.2. Kontrola instalace agentů	94
11.3. Instalace klienta	95
11.4. Kontrola instalace klienta	96
11.5. Odinstalace klienta	97
11.6. Kontrola odinstalace klienta	98
12. PROFIL	100
13. PŘEHLEDY	102
14. REPORTY	103
15. VAROVÁNÍ – NOTIFIKACE	106
16. WEBSAFETICA	108
17. SPRÁVA MOBILNÍCH ZAŘÍZENÍ	111
17.1. Seznam spravovaných mobilních zařízení	112
17.2. Politiky Safetica Mobile	116
17.2.1. Zásady hesel	116
17.2.2. Wifi	117

17.2.3. Omezení.....	118
17.2.4. Řízené aplikace.....	121
17.2.5. integrace Safetica Mobile s Android a iOS prostředím.....	123

1. POPIS SAFETICA TECHNOLOGIES

1.1. OCHRANA DAT

Každá organizace má důležité dokumenty, které v případě úniku mohou způsobit finanční ztráty, vznik konkurence, poškození pověsti anebo jiné škody.

Safetica zabezpečuje klíčová firemní data a získává kontrolu nad tím, kdo k nim přistupuje:

- Smlouvy
- Strategické plány
- Osobní údaje Výrobní výkresy a návrhy
- Know-how
- Databáze zákazníků
- Obchodní informace

1.2. SOULAD S NORMAMI A ZÁKONY

Řešení Safetica zkontroluje, kdo s dokumenty přichází do styku, a nastavuje, co konkrétní uživatelé a oddělení mohou s daty dělat. Provedete interní bezpečnostní audit a v případě externí kontroly budou k dispozici detailní záznamy operací se soubory.

Řešení Safetica bylo navrženo pro použití v souladu se zákony chránícími soukromí zaměstnanců. Zákazník proto i získá návod, jak používat řešení Safetica dle platné legislativy.

1.3. ZPŮSOBY, JAK SE CITLIVÉ DOKUMENTY MOHOU DOSTAT MIMO KONTROLU

Safetica pozná, kdo s jakým dokumentem pracuje, a podle nastavených pravidel zablokuje zakázanou činnost, informuje administrátora, anebo poučí zaměstnance o bezpečnostní směrnici. Pokud dokument opouští firmu (například na USB flash disku)

1.4. PŘEHLED O FUNGOVÁNÍ FIRMY

Safetica pomáhá odhalit problémy ve fungování společnosti. Zákazník rychle získá ucelený přehled o všech o aktivitách uvnitř firmy. Díky tomu bude moci řídit svou společnost informovaně a lépe.

Objevuje problémy v interních procesech a zjišťuje, co se děje uvnitř společnosti

Víte co se opravdu děje uvnitř vaší organizace?

Jaké máte problémy v interních procesech?

Jak nakládají zaměstnanci s důležitými dokumenty?

1.5. DOHLED NAD PRODUKTIVITOU

Safetica pomáhá ušetřit provozní náklady a zjistit kde lze omezit plýtvání. K dispozici budou například informace o využití drahých licencí, vytížení internetové sítě, času kdy běžely počítače naprázdno, anebo přehled barevného a nadměrného tisku. Uspořené finance tak bude moci investovat do toho, co se dlouho odkládalo - například na firemní teambuilding či lepší počítače.

Pomocí dohledu se zjistí:

- kolik % nákladů společnosti na IT a HR je efektivně vynaloženo.
- kolik času tráví zaměstnanci společnosti neproduktivní činností v pracovní době.
- které drahé softwarové licence společnost nevyužívá

1.6. ZVÝŠENÍ EFEKTIVITY PERSONÁLNÍCH NÁKLADŮ

Dává přehled o tom, co zaměstnanci dělají v pracovní době.

Safetica vám dá kompletní informace o tom, kolik času stráví zaměstnanci na webu, sociálních sítích či v pracovních programech. Takže budete moci dělat informovaná rozhodnutí na základě reálného stavu produktivity zaměstnanců. K dispozici budete mít přesné statistiky o jednotlivcích i srovnání v rámci oddělení. Navíc, v případě podezřelých aktivit a změn chování budete okamžitě upozorněni a situaci tak můžete řešit bez prodlení.

1.7. KONTROLA PŘIPOJOVANÝCH ZAŘÍZENÍ

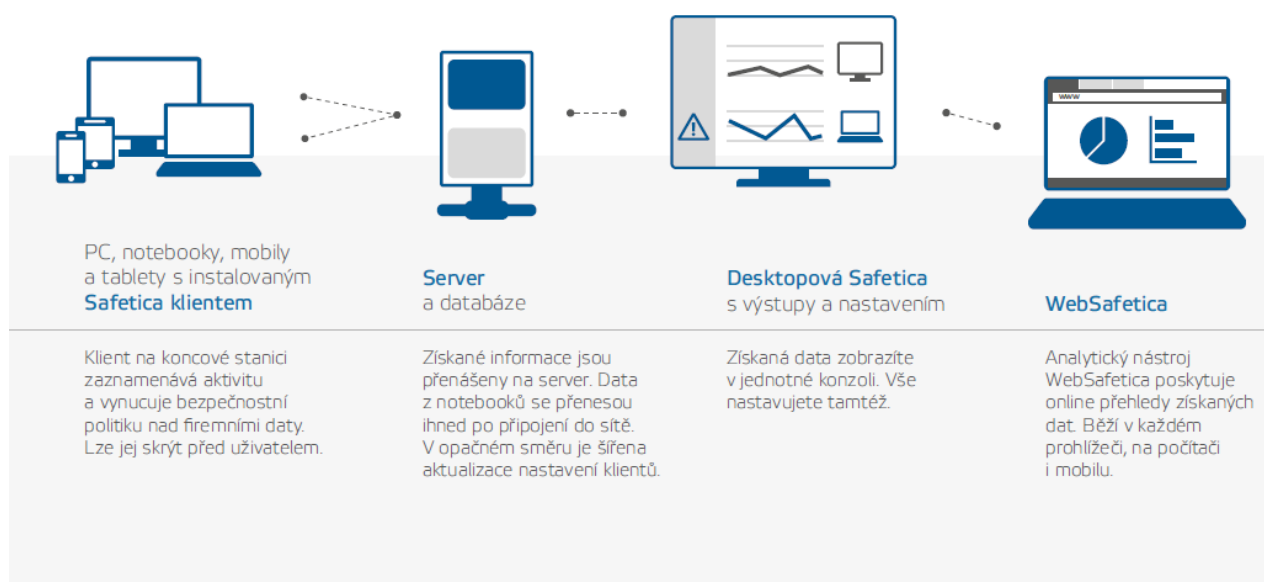
Určuje, která přenosná zařízení se smí používat a zabraňuje v připojování neautorizovaných medií

Se Safetica se snižuje možnost zanesení škodlivého malware do firemní sítě tím, že omezí připojování neautorizovaných zařízení. Definuje, která zařízení může kdo připojovat, co s nimi lze dělat anebo jaká data na ně lze nahrávat.

2. ARCHITEKTURA SAFETICA

Produkt Safetica je založen na architektuře klient-server – On-Premis řešení. Na koncových stanicích je nainstalován Safetica klient, který komunikuje se Safetica serverem. Spolu se klientem běží na koncové stanici také downloader agent, který je určený pro instalaci, aktualizaci a další správu klientské součásti. Ke správě, nastavení a zobrazení získaných dat slouží konzole nebo WebSafetica. Data získána z jednotlivých koncových stanic jsou ukládána na databázový server. V databázi je také uloženo nastavení všech komponent Safetica.

ARCHITEKTURA

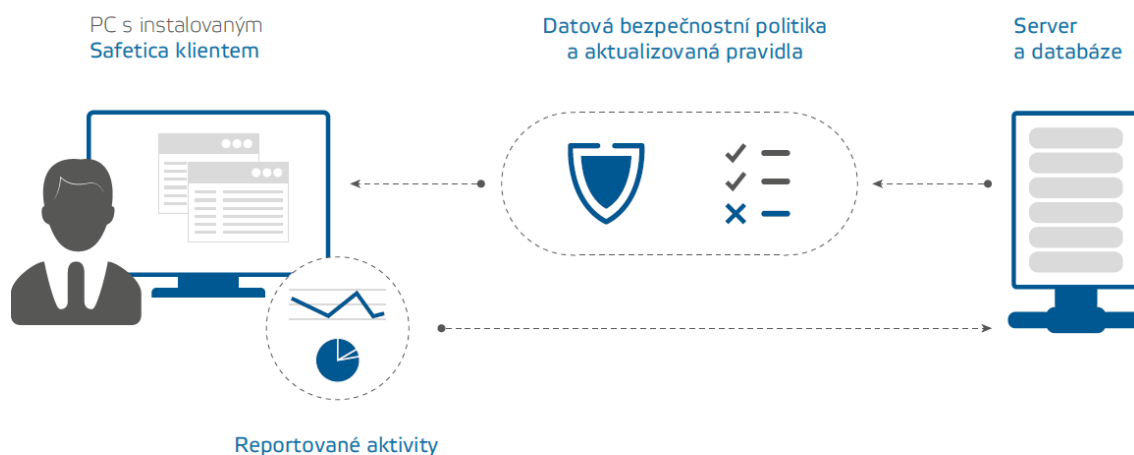


Komunikace klienta se serverem:

Komunikace mezi klientem a serverem je vedena bezpečným šifrovaným komunikačním kanálem

Tímto kanálem jsou přenášeny jak bezpečnostní politiky DLP, nová pravidla a nastavení, ale také události detekované na klientské stanici.

V případě, že je pro klienta nedostupný management server, klient události shromažďuje u sebe a po opětovném připojení k management serveru veškeré nashromážděné události preposílá. Zároveň aktualizuje bezpečnostní politiku z management serveru.



2.1. SERVER

Safetica server běží jako služba na vyhrazeném serveru, zajišťuje propojení mezi databází a ostatními součástmi Safetica a umožňuje jejich vzdálenou správu.

Instalace bude provedena na dedikovaném serveru Microsoft Windows server 2016.

2.2. KONZOLE

Konzole slouží pro nastavení a správu klientu a downloader agentu na koncových počítačích, serverové služby (serveru), databáze a pro nastavení všech funkcí Safetica na koncových stanicích. Dále zobrazuje výstupy získaných dat, statistiky a grafy. Muže běžet kdekoliv, odkud bude mít spojení na spravovaný server. Instalace bude provedena na serveru centrální správy Safetica

2.3. WEBSAFETICA

WebSafetica je webová konzole pro správu Safetica a zobrazení záznamu získaných z koncových stanic. Přístup k WebSafetica je možný z jakékoliv stanice společnosti pomocí webového browseru.

2.4. SAFETICA AGENT

Safetica agent je součástí Safetica pro správu Safetica klienta na koncových počítačích. Umožňuje jeho vzdálenou instalaci, aktualizaci a další správu. Jedná se o základní SW na klientské stanici, který je možné instalovat jak vzdáleně, například přes GPO, tak pomocí logon scriptu nebo spuštěním instalátoru na klientské stanici. Jedná se o MSI balíček.

2.5. KLIENT

Klient zajišťuje na koncových stanicích veškeré bezpečnostní a monitorovací funkce Safetica. Spouští se vždy při startu operačního systému a zajišťuje monitorování, vynucování bezpečnostní politiky a komunikaci s databází a serverem. Klientská služba zajišťuje na koncových stanicích funkci modulu Auditor, DLP a Supervisor. Instaluje se se vzdáleně ze Safetica management konzole pomocí Safetica Agent

2.6. DATABÁZE

Centrální databáze slouží k uložení nastavení a získaných záznamu ze všech součástí Safetica. Každý server potřebuje tři vyhrazené databáze pro uložení záznamu, nastavení a kategorií aplikací, webu a přípon. Pro uložení databází můžete použít Microsoft SQL Server 2008 a vyšší verze včetně Express edicí. Při použití WebSafetica je podporovaný Microsoft SQL Server 2012 a vyšší včetně Express edicí. Pro instalaci centrální správy Safetica se využije stávající SQL server zákazníka.

Safetica podporuje instalaci management komponent jak na fyzické servery, tak na virtualizované servery.

Centrální správa Safetica je nainstalována do stávající infrastruktury, na dedikovaný server Microsoft Windows server 2016 dle specifikace do virtualizovaného VMware vSphere prostředí zákazníka.

3. HW A SW POŽADAVKY NA INSTALACI SAFETICA

Systém Safetica nebude zasahovat do stávající infrastruktury a nebude vyžadovat zásadní změny v konfiguraci infrastruktury a systémů.

V následující tabule je přehled požadovaných systémů a konfiguračních změn, které vyžaduje systém Safetica jak na straně centrální správy, tak na straně klientských stanic.

3.1. POŽADAVKY NA INFRASTRUKTURU

Přístup	Možnost lokálního nebo vzdáleného přístupu k serveru a klientským stanicím.
Databáze	Připravenou databázi v podporované verzi - MS SQL 2016 Nutná je instalace .NET framework 3.5.
Síť	Koncové stanice musí mít dostupné síťové spojení na serverovou službu a databázi. Serverová služba musí mít na firewallu výjimku pro porty: 1433 (SMS – DB, odchozí), 4438 (SMS – SEC, příchozí), 4441 (SMS – SMC, příchozí) a 4442 (update, příchozí). Pro zasílání automatických upozornění je nutno vytvořit poštovní účet pro tyto účely. Strukturu v Microsoft® Active Directory® (preference bez duplicit ve více skupinách).
Klientské stanice	Zajistit možnost restartu koncových stanic. Mít možnost lokálně deaktivovat antivir pro instalaci, či ladění kompatibility. Nutná je instalace .NET framework 3.5 (kromě .NET 4.5.1) a dostupných aktualizací operačního systému.
Emailový klient	Pro možnost sledování komunikace je nutné, aby emailoví klienti byli konfigurováni nešifrovaně nebo pomocí TLS/SSL. Sledování komunikace přes StartTLS není podporováno.

3.2. HW A SW POŽADAVKY

Systém Safetica pracuje jako server-klient řešení. Pro správu systému je nutné nainstalovat Safetica server, který zajišťuje centrální správu klientských systémů.

SW Safetica bude zalicencován licencí vydanou společností Safetica Technologies pro zadavatele.

3.2.1. POŽADAVKY NA KLIENTSKÉ SYSTÉMY

Na každou pracovní stanici nebo server, které budou ve správě systému Safetica, se bude instalovat Safetica agent a Safetica klient. Požadavky na instalaci jsou:

HW konfigurace	Procesor: 2,4 GHz 32-bit (x86) nebo 64-bit(x64) dvoujádrový procesor RAM: 2 GB Požadavky na místo na disku: 10 GB vyhrazeného místa
Operační systém	Windows 7, 8.1, 10 (x86 nebo x64), Windows Server 2008 R2, 2012, 2012 R2 a vyšší, Microsoft Terminal Server a Citrix XenApp.

3.2.2. POŽADAVKY NA MANAGEMENT SERVER SAFETICA

Pro instalaci je požadován virtuální Microsoft Windows server 2016 s požadavky:

HW konfigurace	8 jader procesoru 16 GB RAM 250 GB volného místa na disku SQL serveru (databáze + zálohy) a 20 GB vyhrazeného místa pro serverovou komponentu
Operační systém/y	Windows Server 2012, případně vyšší (x86 nebo x64), ideálně Windows Server 2016, včetně IIS 7.5 nebo novější
Typ databázového serveru a verze	MS SQL Server 2012, případně vyšší, ideálně MS SQL Server 2016

4. ZPŮSOB ZAJIŠTĚNÍ KOORDINACE REALIZACE PŘEDMĚTU PLNĚNÍ S BĚŽNÝM PROVOZEM

K hladkému průběhu jednotlivých kroků nasazení je vyžadována určitá minimální součinnost ze strany zákazníka. Jedná se o:

- Seznam klientských stanic vybraných k instalaci
- Vzdálený přístup na server, kde bude nainstalována Safetica Management Service
- Vzdálený přístup na server, kde bude nainstalována Safetica Management Console (může se jednat o stanici shodnou s předchozí)
- Prostředek lokální nebo vzdálené instalace klientské komponenty Safetica Agent (např. Group Policy Microsoft® Active Directory®)
- Možnost zadání výjimek do antivirového řešení, firewallu a VPN
- Vzdálený přístup na server se Safetica Management Console na týdenní bázi pro kontrolu korektního průběhu sběru dat
- Aplikaci pro správu použité databáze (např. SQL Server Management Studio v případě použití MS SQL databáze)
- Na požádání dodavatele zajistit spolupráci a součinnost všech osob podílejících se na realizaci

Pozn.: Pro zajištění vzdáleného přístupu je možné využít ISL Online, Microsoft Remote Desktop nebo TeamViewer 11.

5. ZÁKLADNÍ KONFIGURACE SAFETICA MANAGEMENT SERVERU

Management server instaluje tyto komponenty Safetica Instalace:

Safetica Management Service

Safetica Management Console

Safetica Web Console

Součástí instalace Management Service jsou i Safetica Agent a Safetica Klient – vyžadují customizaci při instalaci. Doporučení je stáhnout customizovaného agenta v běžící management konzoli.

Stažení poslední dostupné verze Safetica:

http://downloads.safetica.com/partner/safetica_setup.exe

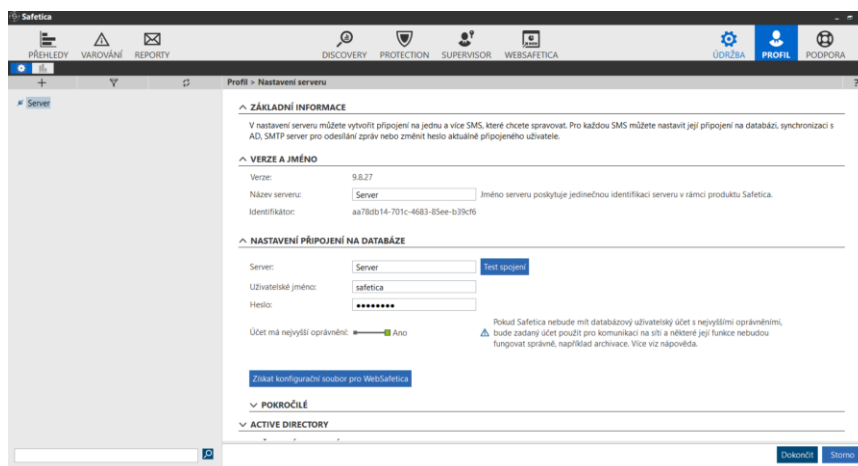
Instalace management konzole Safetica probíhá z instalačního balíku, který je dostupný na portále společnosti Safetica. Instalace obsahuje výše zmíněné komponenty, které je možné instalovat jako jeden celek v případě použití MS SQL Express, který je součástí instalačního balíčku.

V případě použití externího SQL serveru, nebo stávajícího SQL serveru na stejném serveru, kam se instaluje Safetica management konzole, je nutné každou komponentu instalovat samostatně.

Safetica management service – vlastní management server

Safetica management console – konzole pro správu systému. Konzoli je možné nainstalovat i na další počítače správců, tak aby bylo možné spravovat systém vzdáleně

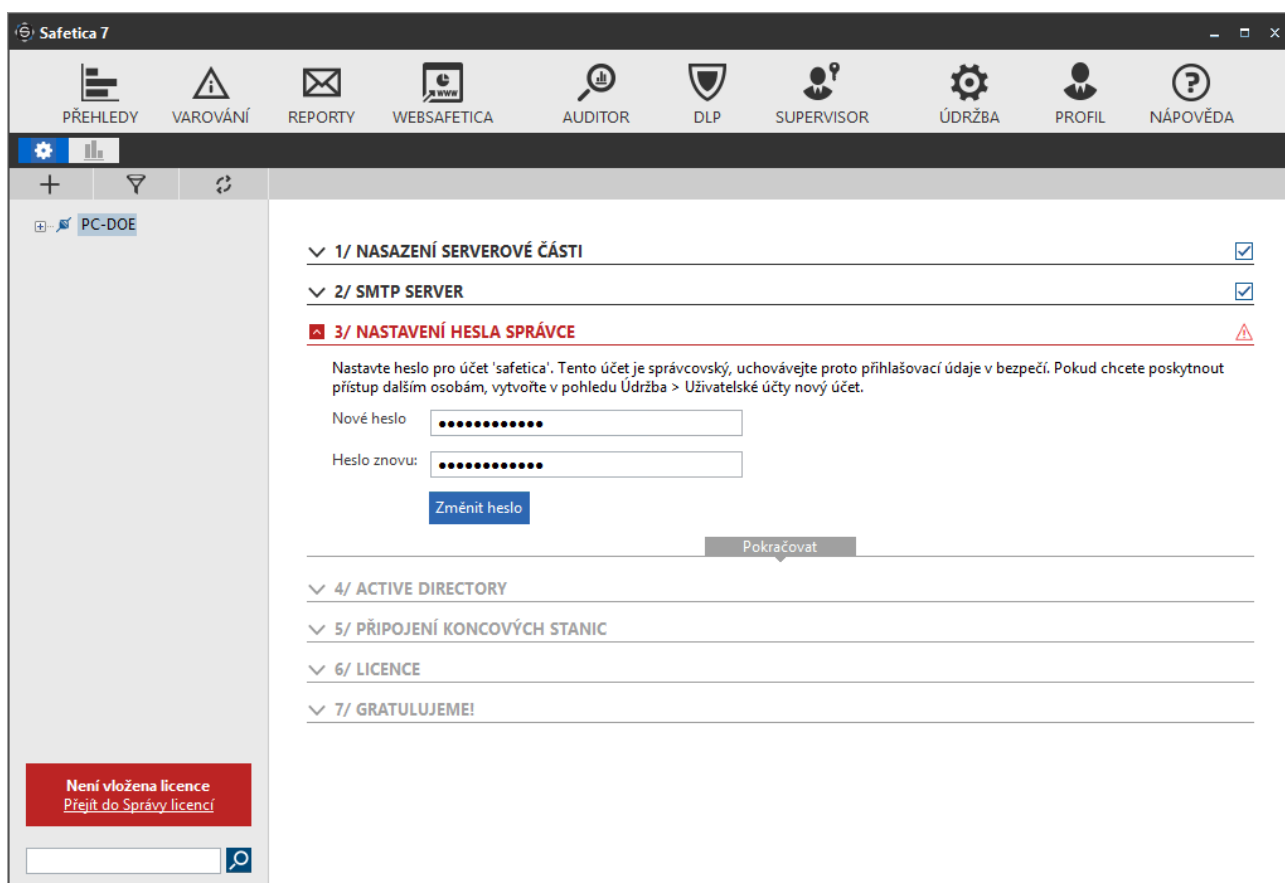
Safetica Web Console – instaluje komponenty do Microsoft IIS pro reporting a základní konfiguraci systému přes webový prohlížeč. Pro úspěšnou instalaci je nutné z management konzole získat konfigurační soubor pro připojení, na který se následně instalace Web konzole odkazuje. Konfigurační soubor je možné stáhnout z položky „Profil“ v nastavení „Připojení“ kliknutím na „Nastavení“ u serveru. A následně kliknutím na tlačítko „Získat konfigurační soubor pro Websafetica“



5.1. ZÁKLADNÍ KONFIGURACE SAFETICA MANAGEMENT SERVERU

Po instalaci management serveru se provede základní konfigurace, která obsahuje:

- Definice SMTP serveru pro odesílání notifikací
- Nastavení hesla správce
- Aktivace synchronizace Active Directory
- Možnost připojení koncových stanic – stažení MSI balíčku Safetica agenta
- Zadání platné licence



Většinu nastavení v průvodci je nutné vyplnit, aby bylo možné pokračovat dále.

Ke všem nastavením je možné se kdykoliv v management konzoli vrátit a systém přenastavit.

6. NASTAVENÍ DISCOVERY

Nastavení Discovery se provádí pod tlačítkem Discovery v horní liště management konzole. V rámci nasazení jsou zvoleny následující funkce a aktivity, které bude auditor sledovat u všech spravovaných stanic a serverů.

- Aplikace (vč. rozlišení aktivního času a rozložení během dne)
- Zařízení - Externí zařízení a disky
- Webové stránky (vč. rozlišení aktivního času a rozložení během dne)
- Tisk (síťové i virtuální tiskárny s detaily o dokumentech)
- Síťový provoz - využití sítě (vč. rozpadu na aplikace)
- Trendy - dlouhodobé trendy, krátkodobé odchylky v aktivitách
- E-maily (informace o přílohách)
- Operace se soubory, i na připojených cloudových discích a Office 365








Nastavení Discovery je možné kdykoliv změnit přesunutím šoupátka na pozici vypnuto.

^ ZÁKLADNÍ INFORMACE

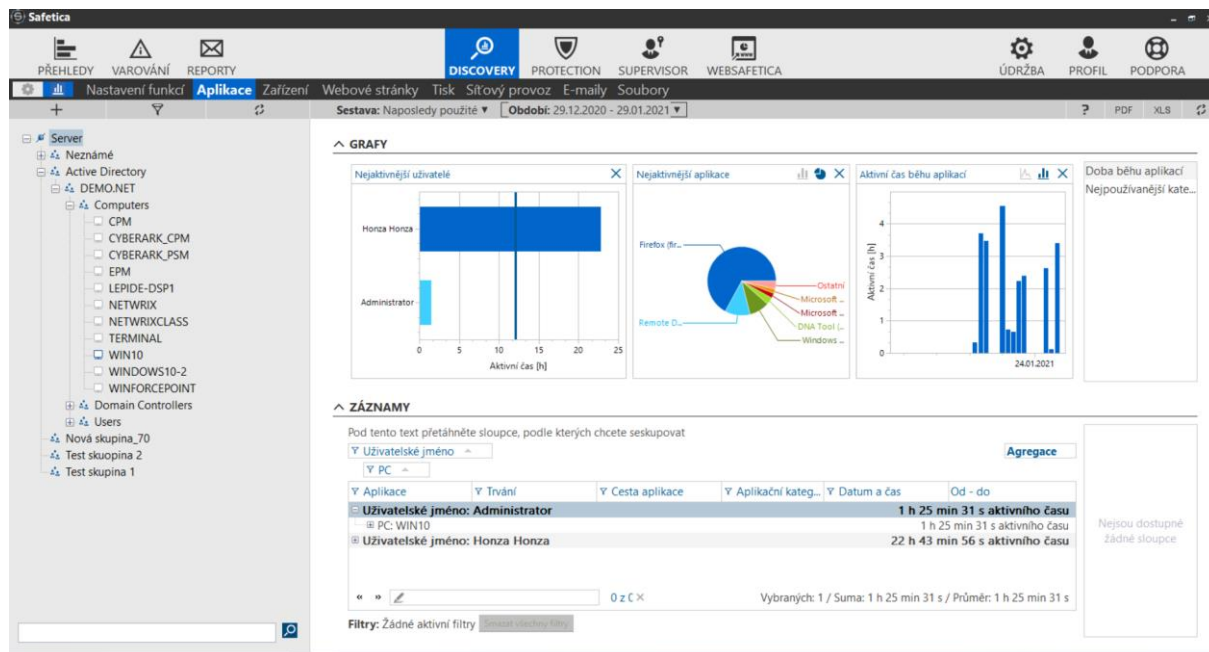
Zde můžete zapnout nebo vypnout monitorovací funkce Safetica. Nezapomeňte vždy ve stromě vlevo zkontrolovat uživatele, na které se toto nastavení vztahuje.

⚠ Data měřená modulem Síťový provoz mohou být na systémech Windows 7 u některých aplikací nepřesná.

UŽIVATELSKÉ NASTAVENÍ

	<input checked="" type="checkbox"/> Zapnuto	
Aplikace		
	<input checked="" type="checkbox"/> Zapnuto	
Zařízení		
	<input checked="" type="checkbox"/> Zapnuto	
Webové stránky		
	<input checked="" type="checkbox"/> Zapnuto	» Zobrazit rozšířená nastavení
Tisk		
	<input checked="" type="checkbox"/> Zapnuto	
Síťový provoz		
	<input checked="" type="checkbox"/> Zapnuto	
E-maily		
	<input checked="" type="checkbox"/> Zapnuto	» Zobrazit rozšířená nastavení
Soubory		

Výstupem Discovery jsou grafy a záznamy pro jednotlivé monitorované kategorie.



Systém umožňuje sledovat jak celou síť globálně, tak je možné sledovat aktivity jednotlivých počítačů nebo uživatelů. Systém podporuje napojení na Active Directory, kde je možné sledovat aktivitu podle skupin počítačů a uživatelů.

Je možné zobrazovat aktivitu se soubory, přístup na webové servery, připojená externí zařízení apod.

Je možné i filtrovat na určité časové období – minimálně jeden den, popřípadě vybrat konkrétní okno až v minutách.

Zobrazuje nastavení jednotlivých politik na systémy a uživatele v rámci celého systémového stromu

Poskytuje detailní přehled, odkud je jaké nastavení děděno a kde došlo k přerušení dědění.

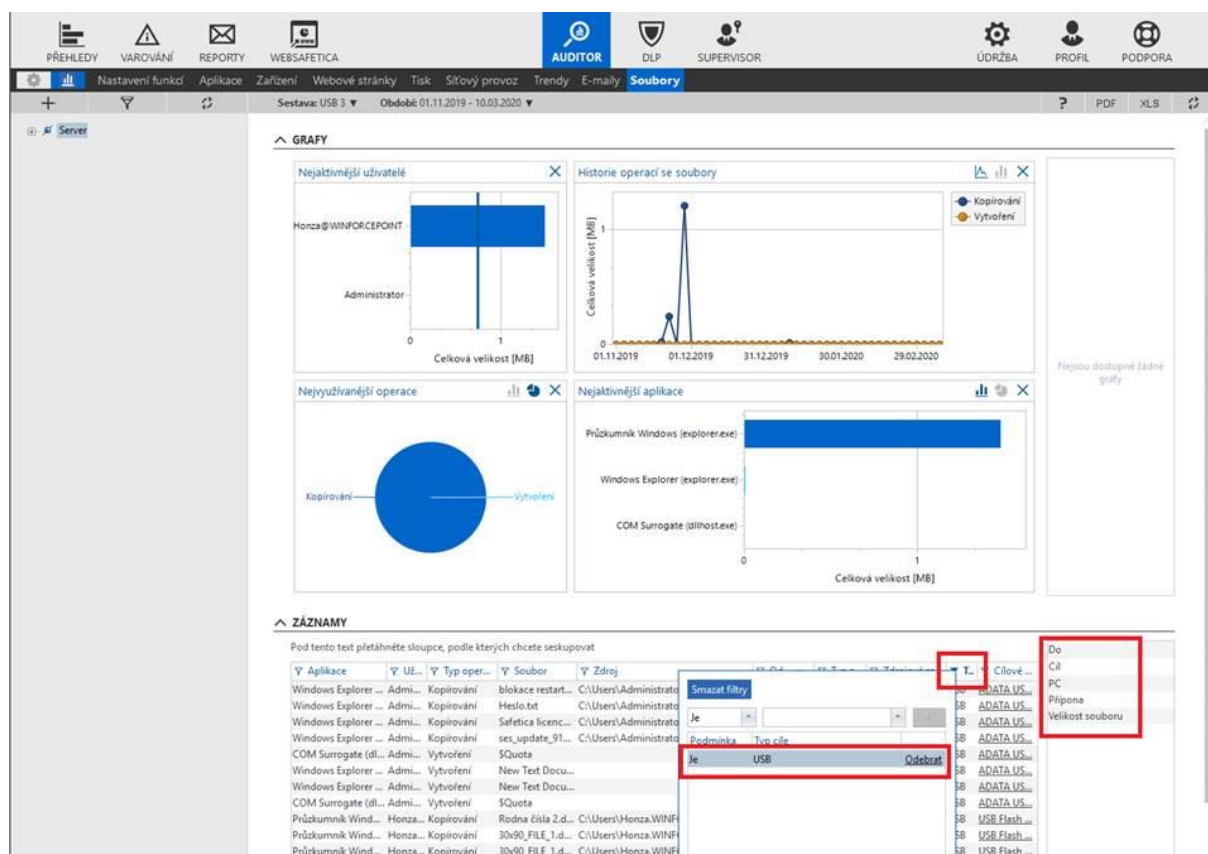
Užitečná pomůcka při hledání problémů, kdy například systém nepracuje tak, jak by se předpokládalo.

6.1. NASTAVENÍ A ULOŽENÍ FILTRŮ

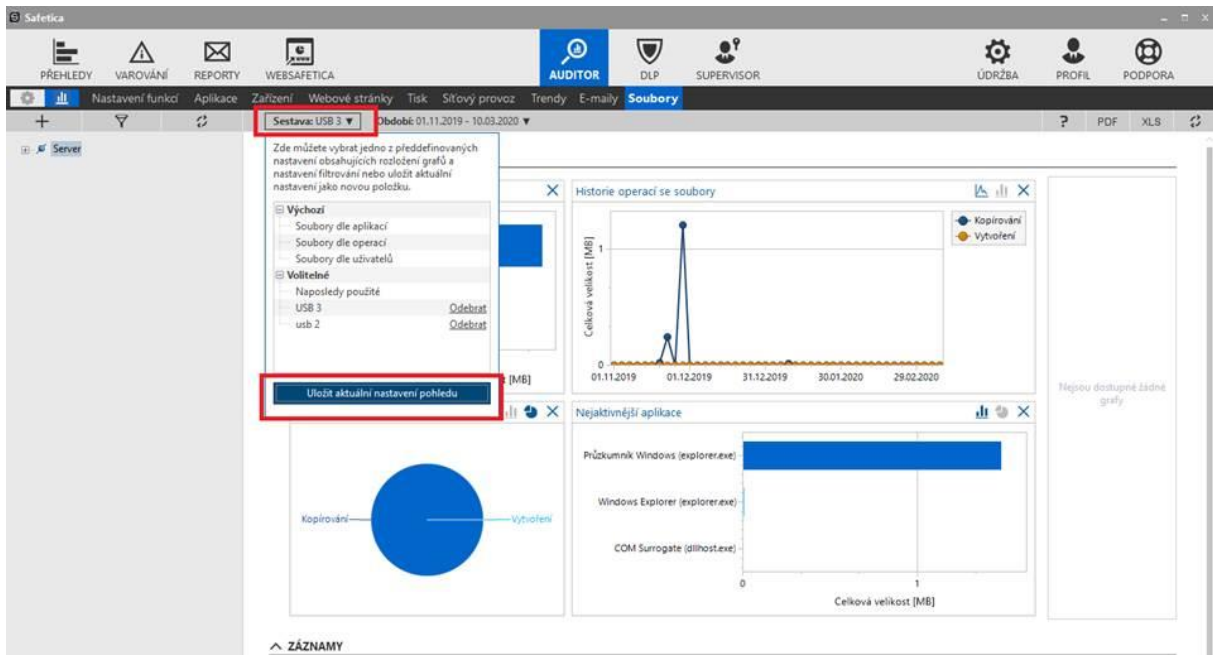
Safetica umožňuje vytvoření a uložení filtrů pro detekované události a grafy.

Umožňují správci velice rychle vyfiltrovat události, které ho pravidelně zajímají a vytvářet automatizované reporty.

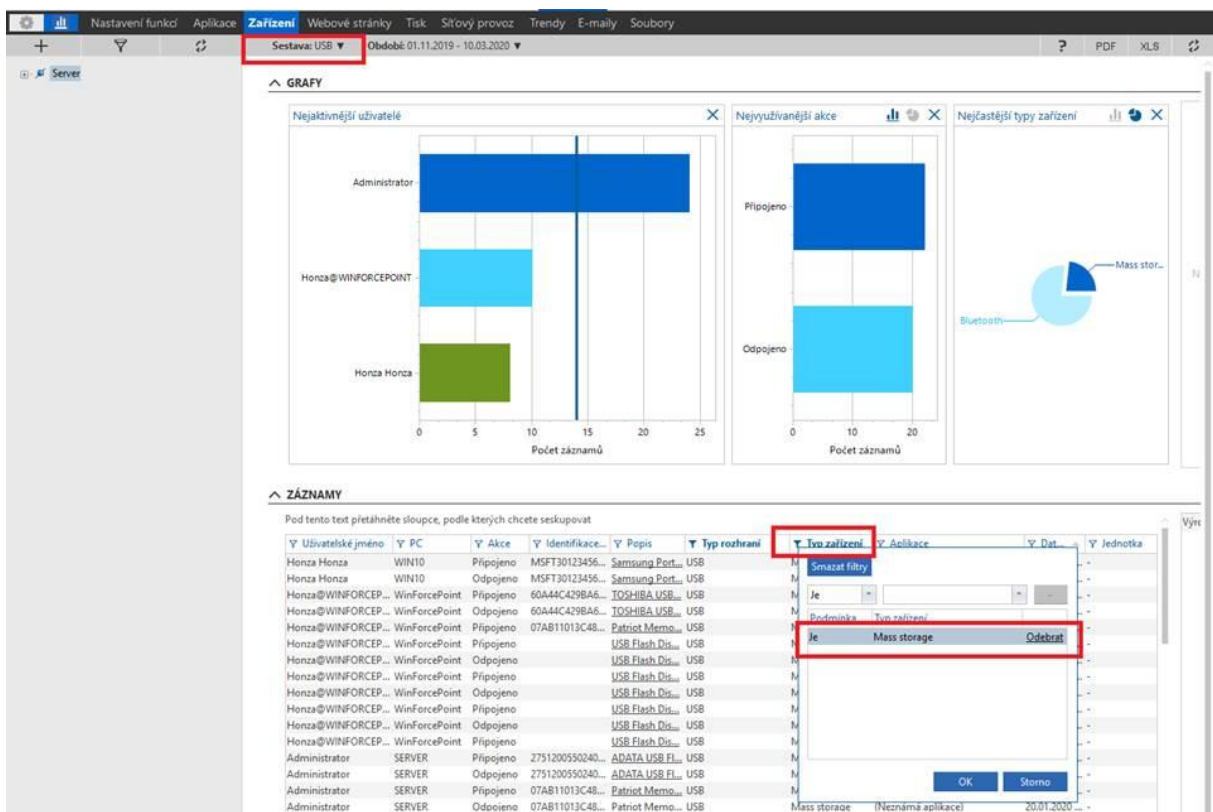
1. Je nutné v rámci správy vytvořit sestavu, ze které se bude generovat vlastní report – například práce se soubory na USB
 Zvolit si grafy, které se budou zobrazovat v reportu PDF a filtr na záznamy, které budou zobrazeny v XLS reportu



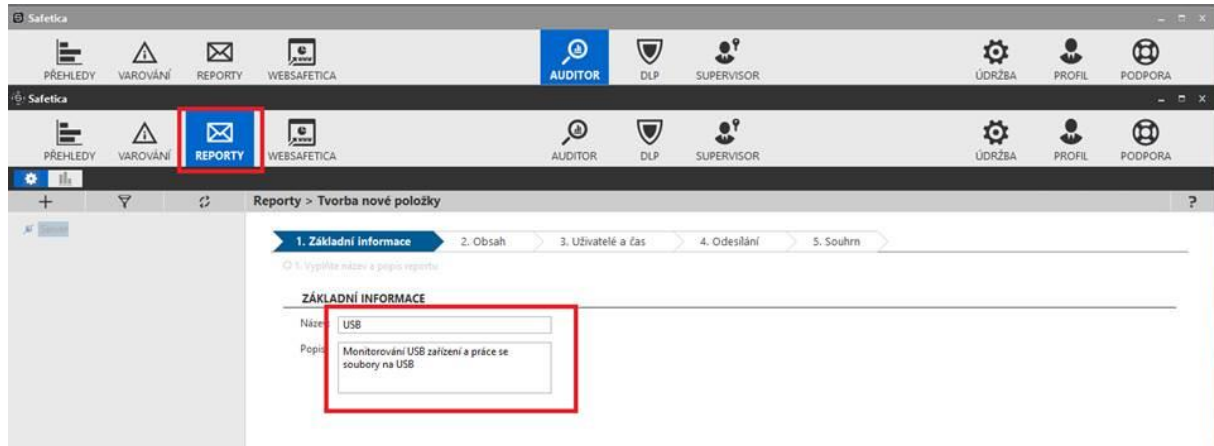
Následně sestavu uložit:



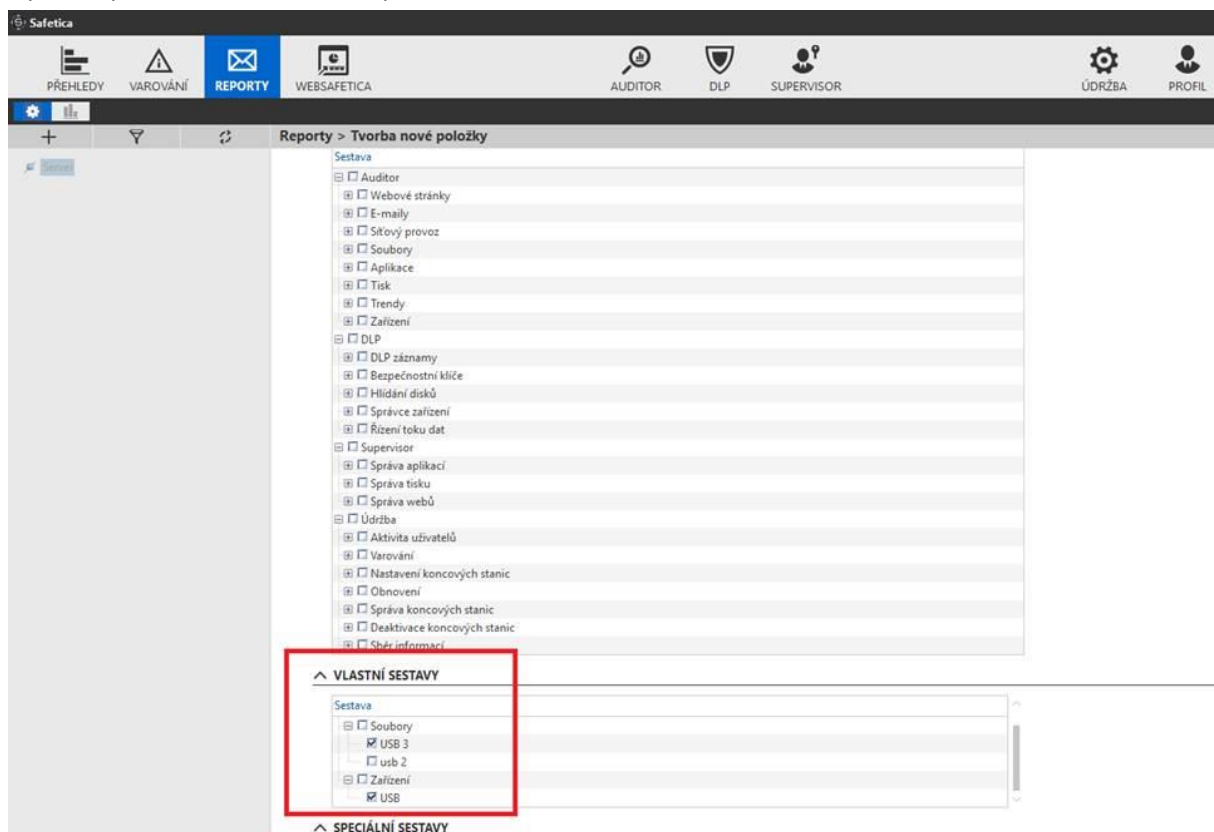
To samé je potřeba udělat pro reporty na zařízení:



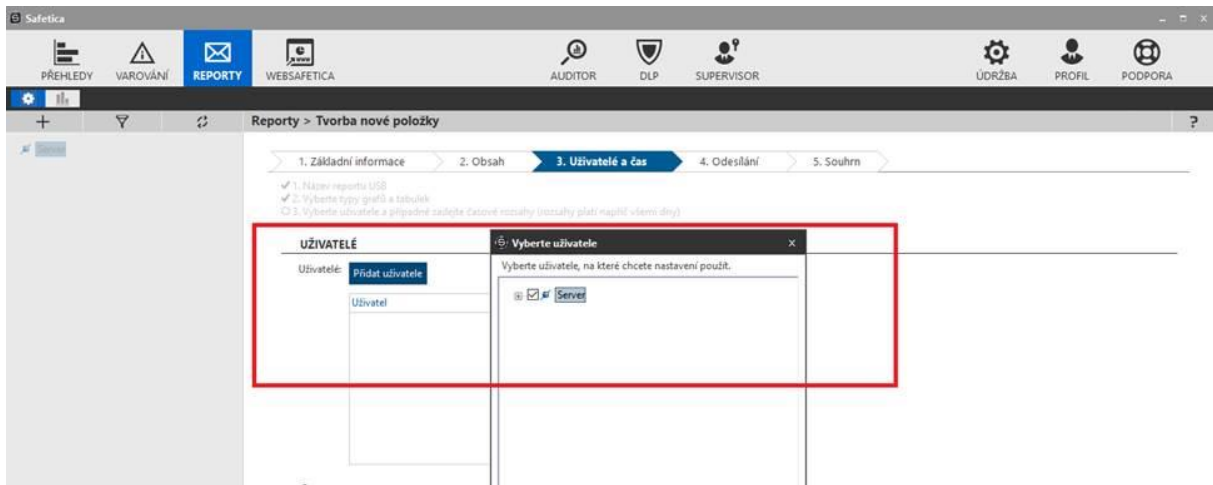
Nastavení reportů:



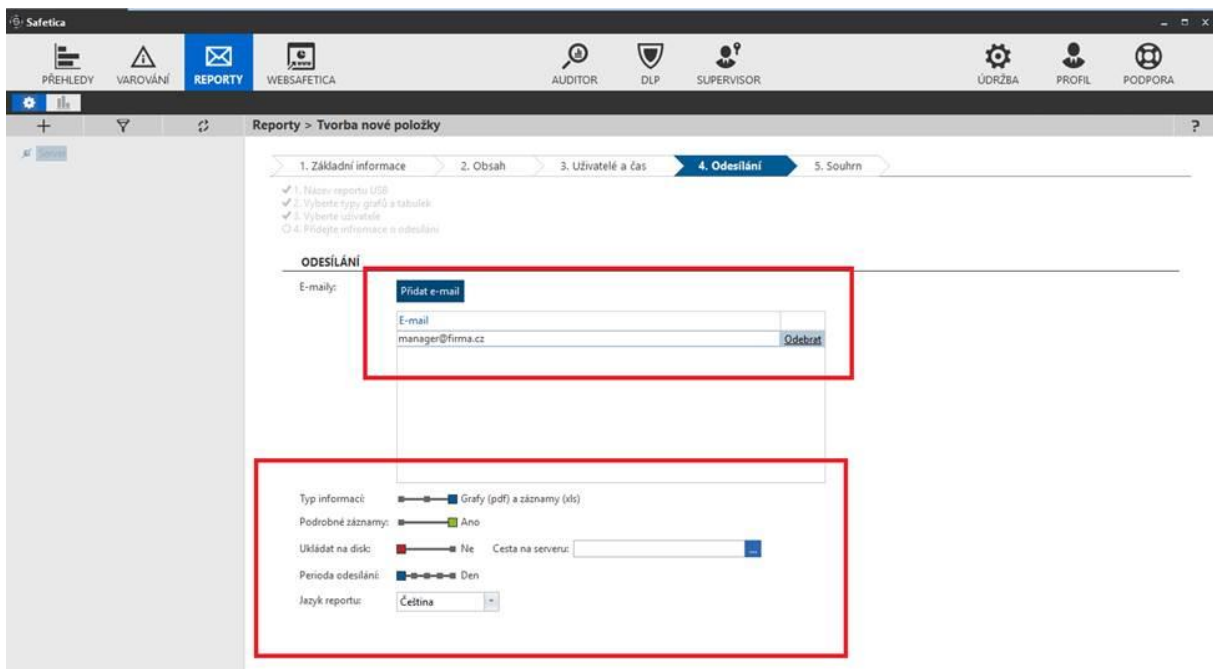
Vybrat vytvořené vlastní sestavy:



Vybrat uživatele/zařízení, pro které se bude generovat report:



Vybrat typ reportu a adresu příjemce:



Po uložení bude report ve zvolené periodě generován, nebo je možné report vygenerovat manuálně:

ZÁKLADNÍ INFORMACE

Pomocí automatických reportů můžete být pravidelně informováni o situaci ve vaší firmě. Můžete si nechat zasílat přehledy aktivit pro jednotlivé zaměstnance, skupiny nebo celé pobočky. Můžete si také vyžádat vlastní reporty. Pro každý report lze zvolit, co bude obsahovat, kterých uživatelů, skupin nebo počítačů se bude týkat a komu se bude zasílat. Při exportu dat dbějte na legislativní podmínky pro uchování dat, přístup, soukromí a další, které se mohou týkat dat odchozích ze Safetica databáze. Doporučujeme skontrolovat tyto podmínky před nastavením reportů a/nebo exportem jakýchkoli dat.

Nové pravidlo

Název	Vytvořil		
Denní report	safetica	Upravit	Odebrat
Report akti...	safetica	Upravit	Odebrat
Report udiz...	safetica	Upravit	Odebrat
test report	safetica	Upravit	Odebrat
USB	safetica	Upravit	Odebrat

INFORMACE O REPORTU

Název: USB

Popis: Monitorování USB zařízení a práce se soubory...

Naposledy generováno: -

Generovat nyní

OBSAH

Výchozí sestavy: (Žádné položky)

Vlastní sestavy:

- Auditor
- Soubory
- USB 3
- Zařízení
- USB

Speciální sestavy: (Žádné položky)

UŽIVATELÉ A ČAS

7. NASTAVENÍ POLITIKY SUPERVISORU

Zvyšuje efektivitu procesů uvnitř firmy. Zajistí, že aktivity zaměstnanců budou v souladu s interními bezpečnostními pravidly.

Nastavení Auditoru se provádí pod tlačítkem Supervisor v horní liště management konzole.

Supervisor umožňuje nastavovat tři komponenty:

- Správa webů
- Správa Aplikací

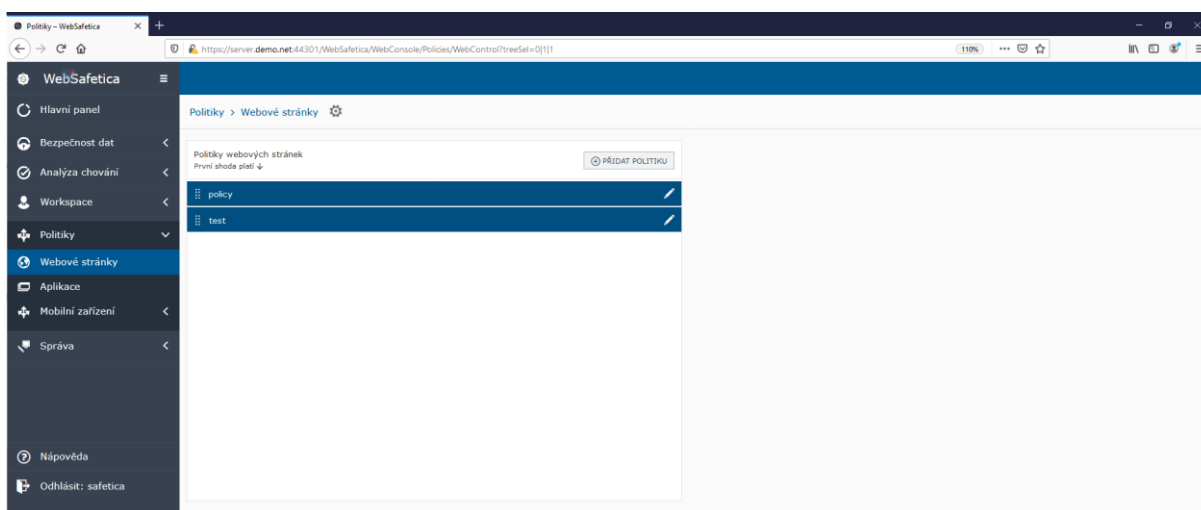
Supervisor je od verze Safetica 9.6 součástí Websafetica, není dostupný ve standardní konzoli Safetica.

7.1. SPRÁVA WEBŮ

URL filtr s kategorizací webových serverů. Obsahuje 28 přednastavených kategorií, nebo je možné definovat vlastní URL adresy nebo IP adresy, které mají být systémem monitorované nebo blokové.

Je možné i přesměrovat uživatele na definovanou webovou stránku v případě blokace.

Ukázka konzole pro nastavení URL filtru:



Doporučené nastavení blokace webových stránek

- Games – blokování herních webových stránek
- Illegal – blokování nelegálních webových stránek
- Malware – blokování webových stránek s malware
- Pornography – blokování webových stránek s pornografickým materiálem
- Proxy web – blokování využívání proxy serverů

Ukázka nastavení politiky blokace webových stránek:

The screenshot shows the 'Detail politiky' (Policy Details) configuration page. At the top, the breadcrumb navigation reads 'Politiky > Webové stránky > Detail politiky'. The main form contains the following elements:

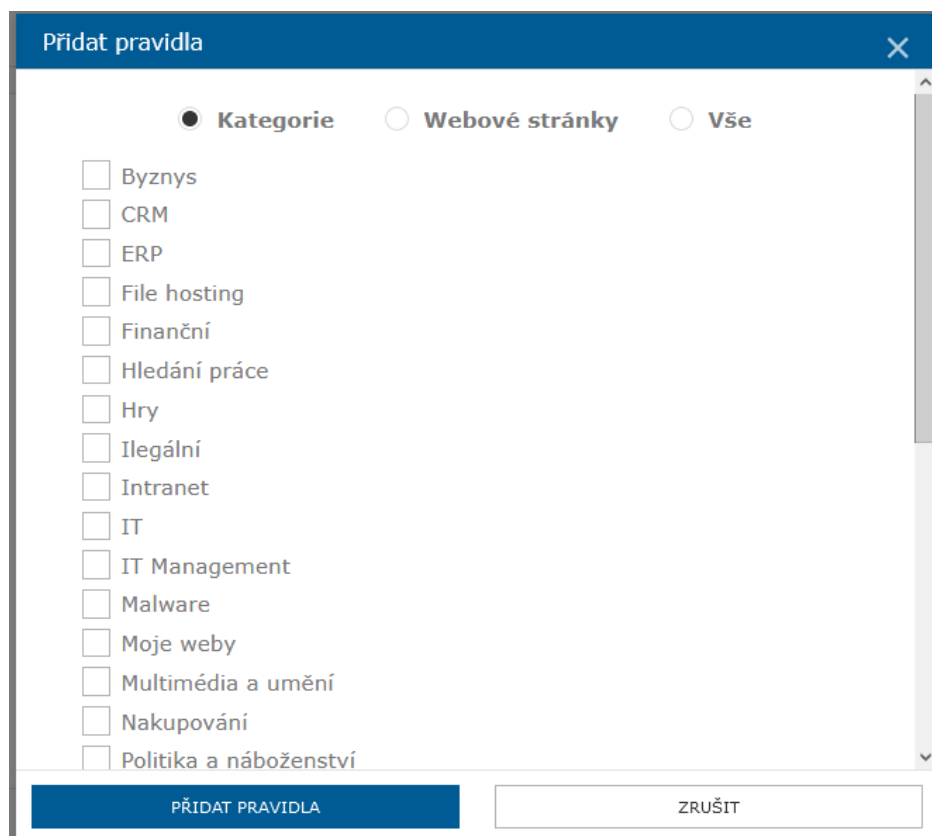
- Název** (Name): A text input field containing the word 'policy'.
- Stav** (Status): A checkbox labeled 'Politika je aktivní' (Policy is active), which is checked.
- POUŽITA NA** (Used on): A section with a 'PŘIDAT UZLY' (Add nodes) button and a list box containing the email address 'Honza@WIN103 X'.
- PRAVIDLA POLITIKY** (Policy Rules): A section with a 'PŘIDAT PRAVIDLA' (Add rules) button and a dropdown menu set to 'První shoda platí' (First match applies). Below this is a table of rules:

Action	Category	Remove
Blokovat	Pornografie	🗑️
Blokovat	Malware	🗑️
Blokovat	Ilegální	🗑️

At the bottom of the form, there are icons for deleting and copying, and two buttons: 'ULOŽIT POLITIKU' (Save policy) and 'ZRUŠIT' (Cancel).

Pomocí tlačítka Přidat pravidla je možné přidat další kategorie nebo URL adresy, která budou pomocí politiky blokována. V rámci definice pravidla je možné přidávat jak konkrétní URL adresy, tak přednastavené kategorie od výrobce.

Definice kategorií webových stránek



The screenshot shows a dialog box titled "Přidat pravidla" (Add rules) with a close button (X) in the top right corner. It features three radio buttons for selection: "Kategorie" (selected), "Webové stránky" (unselected), and "Vše" (unselected). Below these are 17 categories, each with an unchecked checkbox: Byznys, CRM, ERP, File hosting, Finanční, Hledání práce, Hry, Ilegální, Intranet, IT, IT Management, Malware, Moje weby, Multimédia a umění, Nakupování, and Politika a náboženství. At the bottom, there are two buttons: "PŘIDAT PRAVIDLA" (Add rules) and "ZRUŠIT" (Cancel).

Příklad manuálního přidání URL adresy:



The screenshot shows the same "Přidat pravidla" dialog box, but with the "Webové stránky" (Web pages) radio button selected. A text input field labeled "Adresa webu" (Website address) contains the text "www.seznam.cz". Below the input field, there is a note: "Pokud zadáte pouze server.com, budou blokovány všechny podúrovně domény (m, www, img, ...)." (If you enter only server.com, all subdomains will be blocked (m, www, img, ...)). At the bottom, the "PŘIDAT PRAVIDLA" and "ZRUŠIT" buttons are visible.

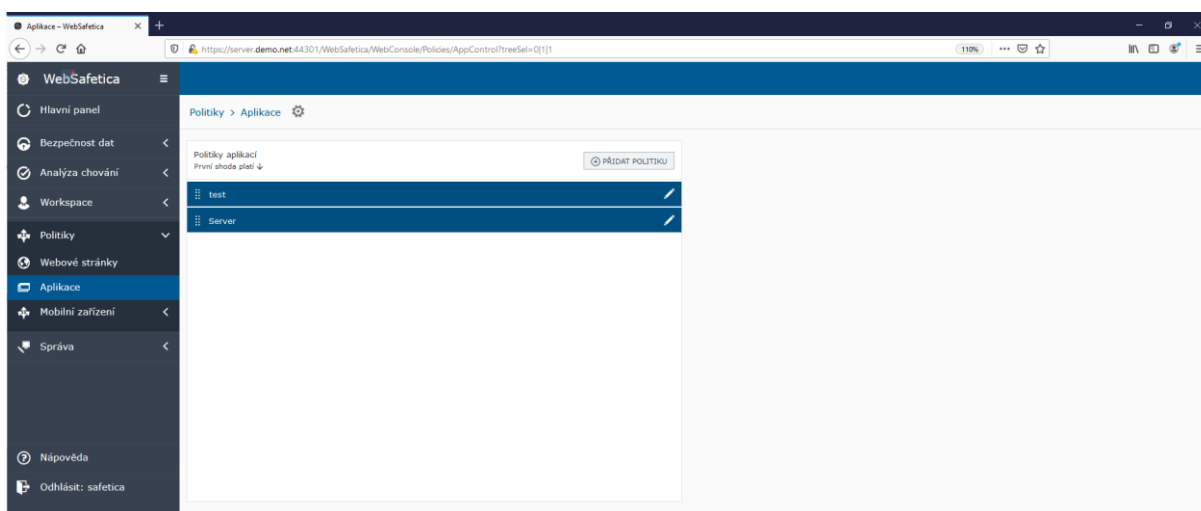
Nastavení Správy Webů je možné kdykoliv rozšířit o další kategorie, nebo definovat své vlastní kategorie s webových serverů, které budou povoleny nebo zakázány.

Politiky je možné nastavovat globálně pro všechny uživatele ve správě, nebo konkrétně zvolením skupiny počítačů nebo uživatelů ve stromu management konzole.

7.2. SPRÁVA APLIKACÍ

Správa aplikací obsahuje 39 přednastavených aplikačních kategorií, které je možné uživateli povolit nebo zakázat. Je možné zvolit i vlastní aplikaci. Safetica klient zároveň načítá veškeré spuštěné aplikace na koncových zařízeních a následně je možné tyto aplikace přidávat do stávajících kategorií, nebo vytvořit novou kategorii.

Správa aplikací je od verze Safetica 9.6 dostupná pouze ve Websafetica.



V rámci nasazení je možné využít přednastavené politiky pro blokaci závadných aplikací, nebo vytvořit vlastní politiku.

Doporučeno je blokovat tyto aplikační kategorie:

- Keylogger – blokace spuštění aplikace odchyťující klávesy uživatele
- Games – blokace herních aplikací
- Miners – blokace aplikací těžících kryptoměny
- File sharing – blokace aplikací umožňující sdílení souborů přes internet

Nastavení politiky pro blokaci aplikací

Politiky > Aplikace > Detail politiky

Název

Stav Politika je aktivní

POUŽITA NA ➕ PŘIDAT UZLY

PRAVIDLA POLITIKY ➕ PŘIDAT PRAVIDLA

První shoda platí ↓

<input type="checkbox"/>	Blokovat ▼	<input type="checkbox"/> Keylogger	<input type="checkbox"/>
<input type="checkbox"/>	Blokovat ▼	<input type="checkbox"/> Hry	<input type="checkbox"/>

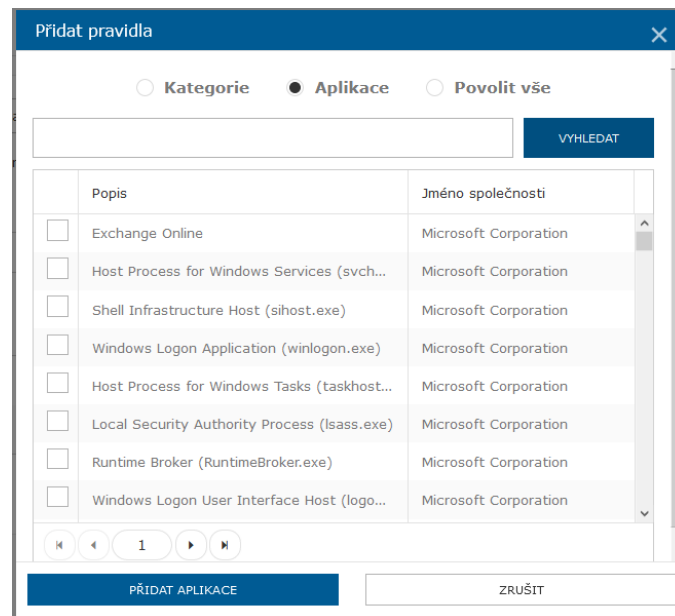
Pomocí tlačítka „Přidat pravidla“ je možné přidat další přednastavené kategorie

Přidat pravidla

Kategorie Aplikace Povolit vše

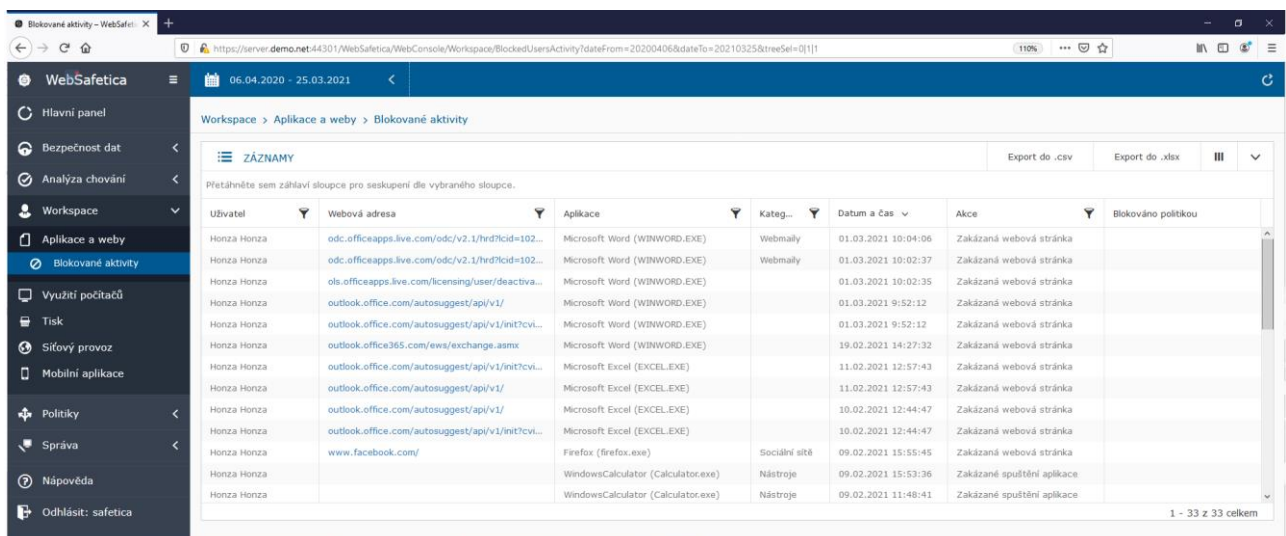
- 3D designový software
- Alternativní webové prohlížeče
- Antivir
- Archivační software
- CAD software
- Cestování
- CRM
- Databáze
- Ekonomický software
- E-mailový klient
- ERP
- Forcepoint
- FTP klienti
- Hry
- Keylogger
- Manažer souborů

Nebo je možné zvolit aplikace ze seznamu načtených aplikací pomocí Discovery modulu



7.3. REPORTOVÁNÍ BLOKOVANÝCH WEBŮ A APLIKACÍ

Události o blokování přístupu na webové stránky, nebo blokování aplikací jsou následně zobrazovány ve Websafetica konzoli Workspace / Aplikace a Weby / Blokování aktivit

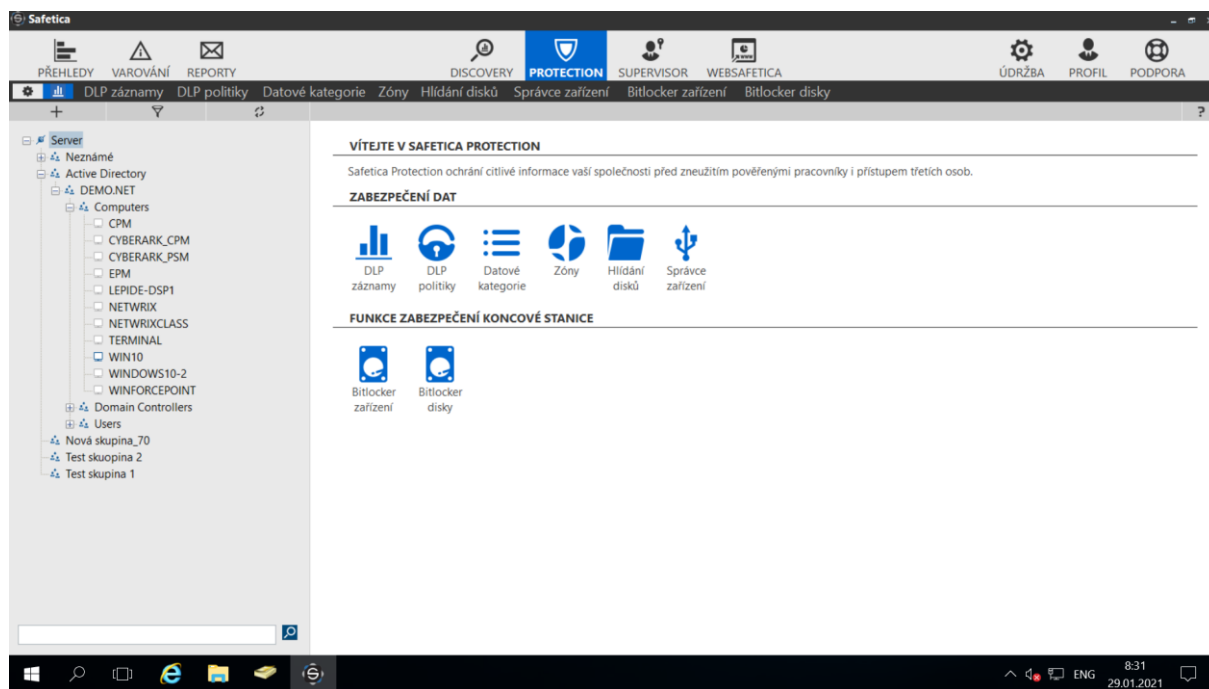


Uživatel	Webová adresa	Aplikace	Kateg...	Datum a čas	Akce	Blokováno politikou
Honza Honza	odc.officeapps.live.com/odc/v2.1/hrd?cid=102...	Microsoft Word (WINWORD.EXE)	Webmaily	01.03.2021 10:04:06	Zakázaná webová stránka	
Honza Honza	odc.officeapps.live.com/odc/v2.1/hrd?cid=102...	Microsoft Word (WINWORD.EXE)		01.03.2021 10:02:35	Zakázaná webová stránka	
Honza Honza	outlook.office.com/autosuggest/api/v1/	Microsoft Word (WINWORD.EXE)		01.03.2021 9:52:12	Zakázaná webová stránka	
Honza Honza	outlook.office.com/autosuggest/api/v1/init?cv...	Microsoft Word (WINWORD.EXE)		01.03.2021 9:52:12	Zakázaná webová stránka	
Honza Honza	outlook.office365.com/ews/exchange.asmx	Microsoft Word (WINWORD.EXE)		19.02.2021 14:27:32	Zakázaná webová stránka	
Honza Honza	outlook.office.com/autosuggest/api/v1/init?cv...	Microsoft Excel (EXCEL.EXE)		11.02.2021 12:57:43	Zakázaná webová stránka	
Honza Honza	outlook.office.com/autosuggest/api/v1/	Microsoft Excel (EXCEL.EXE)		11.02.2021 12:57:43	Zakázaná webová stránka	
Honza Honza	outlook.office.com/autosuggest/api/v1/	Microsoft Excel (EXCEL.EXE)		10.02.2021 12:44:47	Zakázaná webová stránka	
Honza Honza	outlook.office.com/autosuggest/api/v1/init?cv...	Microsoft Excel (EXCEL.EXE)		10.02.2021 12:44:47	Zakázaná webová stránka	
Honza Honza	www.facebook.com/	Firefox (firefox.exe)	Sociální sítě	09.02.2021 15:55:45	Zakázaná webová stránka	
Honza Honza		WindowsCalculator (Calculator.exe)	Nástroje	09.02.2021 15:53:36	Zakázané spuštění aplikace	
Honza Honza		WindowsCalculator (Calculator.exe)	Nástroje	09.02.2021 11:48:41	Zakázané spuštění aplikace	

8. NASTAVENÍ PROTECTION (DLP)

Nastavení Protection (DLP) se provádí pod tlačítkem „Protection“ v horní liště management konzole.

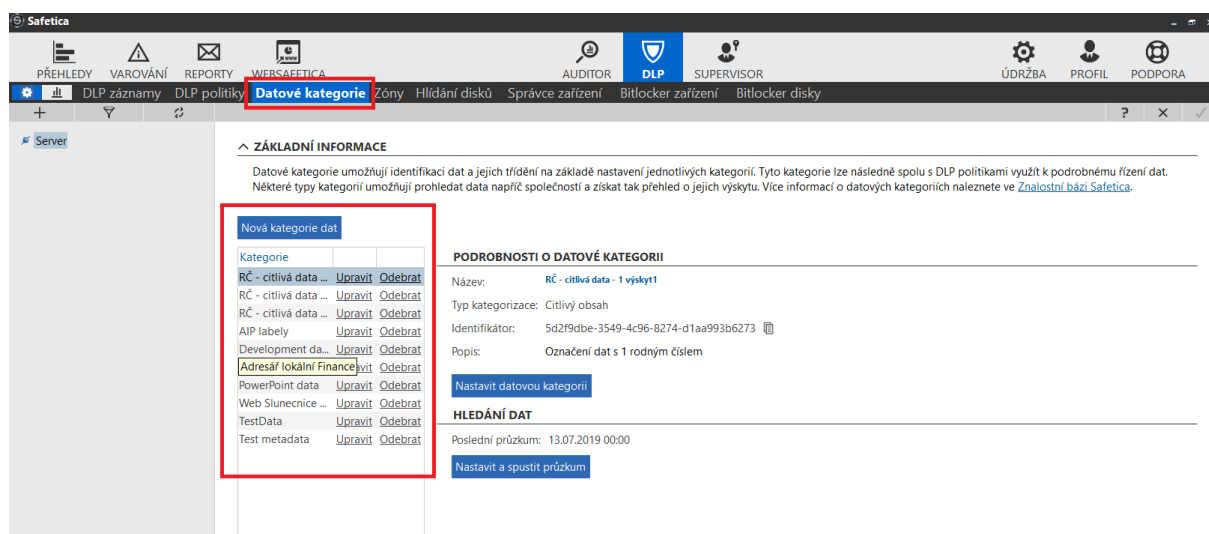
DLP je nejobsáhlejší část Safetica řešení. Umožňuje nastavení klasifikace dat a následná pravidla pro monitoring a blokaci citlivých údajů nebo klasifikovaných souborů.



8.1. DATOVÉ KATEGORIE

Datové kategorie umožňují definici klasifikátorů pro vyhledávání citlivých dat v dokumentech a datech.

Pomocí tlačítka Nová kategorie dat je možné nastavit klasifikátory dat pomocí RegEx výrazů nebo definicí slov. Systém nabízí jak přednastavené klasifikátory, tak možnost definovat vlastní klasifikátory.



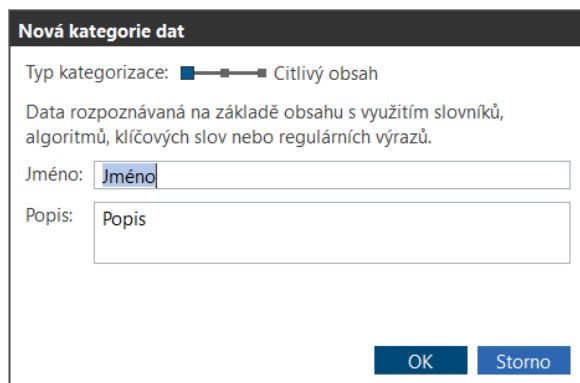
The screenshot shows the Safetica web interface. The top navigation bar includes 'PŘEHLEDY', 'VAROVÁNÍ', 'REPORTY', 'WEBSAFETICA', 'AUDITOR', 'DLP', and 'SUPERVISOR'. The main menu includes 'DLP záznamy', 'DLP politiky', 'Datové kategorie', 'Zóny', 'Hlídaní disků', 'Správce zařízení', 'Bitlocker zařízení', and 'Bitlocker disky'. The 'Datové kategorie' menu item is highlighted with a red box. Below the navigation, there is a section for 'ZÁKLADNÍ INFORMACE' (Basic Information) and 'PODROBNOSTI O DATOVÉ KATEGORII' (Details of Data Category). The 'Nová kategorie dat' button is also highlighted with a red box.

Klasifikaci dat v DLP Safetica je možné provádět několika způsoby.

- **Citlivý obsah** – možnost vyhledávat citlivá podle definovaného slovníku, nebo pomocí RegEx výrazů. Systém klasifikuje data v on-line režimu při práci uživatele
- **Kontextová pravidla (expertní)** – umožňuje klasifikovat data na základě kontextu. DLP agent přidává tzv. TAG – identifikátor dat, do extended atributů NTFS partition.

Tímto způsobem je možné označovat soubory na základě:

- dat vytvořených aplikací
- dat uložených na definovaném úložišti
- dat vygenerovaných webovou aplikací
- **Existující klasifikace (metadata)** – DLP Safetica vyhledává klasifikátory třetích stran, které jsou uloženy v metadatech souborů, například klasifikace pomocí Microsoft AIP, nebo AEC DocTag.



Nová kategorie dat

Typ kategorizace: Citlivý obsah

Data rozpoznávána na základě obsahu s využitím slovníků, algoritmů, klíčových slov nebo regulárních výrazů.

Jméno:

Popis:

OK Storno

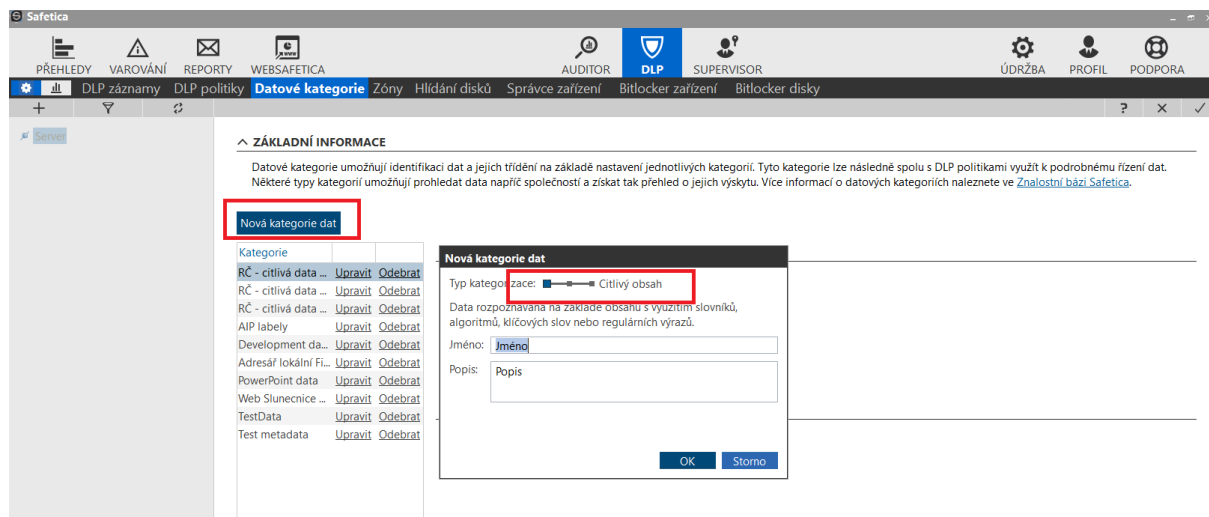
Je možné definovat pro každou definici samostatné pravidlo, nebo je možné kombinovat klasifikátory například data vytvořená aplikací a uložena na definované úložiště.

8.1.1. OBSAHOVÁ KLASIFIKACE DAT

Umožňuje definovat slova nebo RegEx výrazy, které jsou citlivé.

A následně data, která tyto výrazy obsahují, je nutné DLP systémem monitorovat nebo chránit.

Příklad vytvoření nového klasifikačního pravidla pro citlivá data:



Safetica

PŘEHLEDY VAROVÁNÍ REPORTY WEBSAFETICA AUDITOR DLP SUPERVISOR ÚDRŽBA PROFIL PODPORA

DLP záznamy DLP politiky **Datové kategorie** Zóny Hlídaní disků Správce zařízení Bitlocker zařízení Bitlocker disky

Nová kategorie dat

Nová kategorie dat

Typ kategorizace: Citlivý obsah

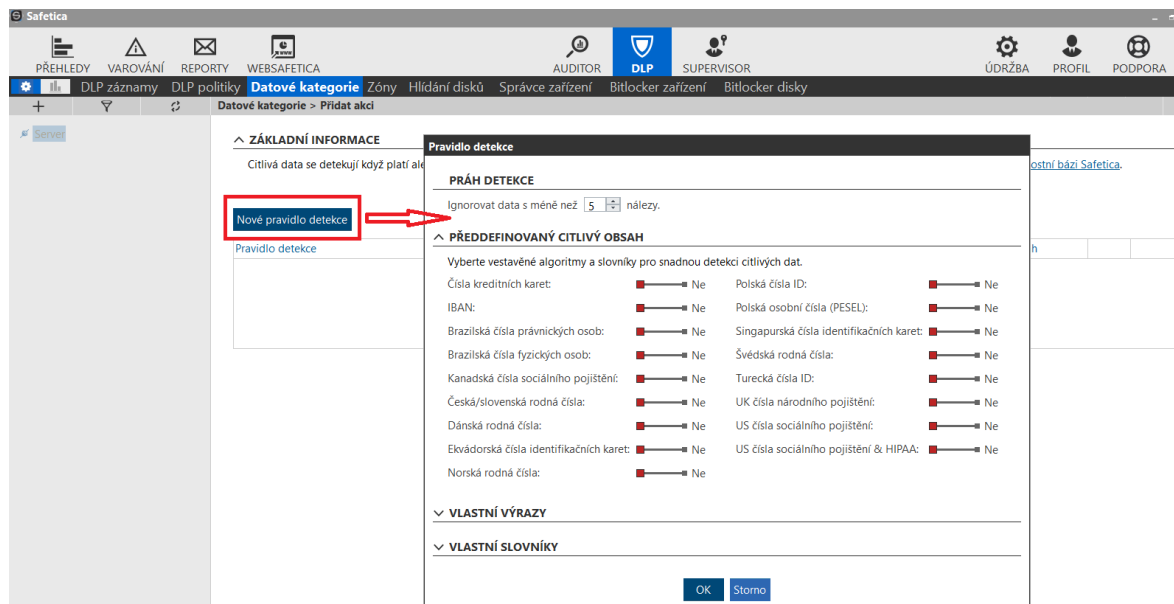
Data rozpoznávána na základě obsahu s využitím slovníků, algoritmů, klíčových slov nebo regulárních výrazů.

Jméno:

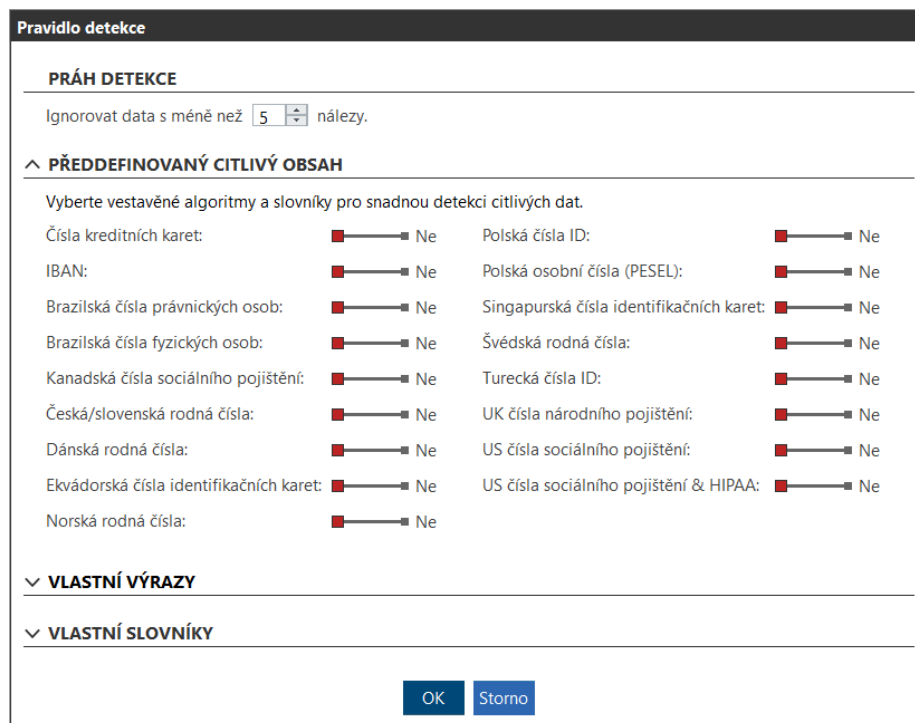
Popis:

OK Storno

Definice pravidla pro citlivá data. Pomocí tlačítka „Nová kategorie dat“ je možné přidat nové pravidlo. Pravidla detekce je možné skládat, mezi pravidly platí operand „OR“.



Safetica nabízí volby z přednastavených klasifikátorů, kde je možné zvolit například „Česká/slovenská rodná čísla“, nebo „Čísla kreditních karet“ a zároveň definovat „Práh detekce“ – počet výskytů citlivých údajů, kdy dojde ke klasifikaci dat.



Dále je možné specifikovat vlastní výrazy – slova, a RegEx výrazy, popřípadě slovníky – možnost importu slovníku ze souboru. Příklad – slovo „tajné“

Pravidlo detekce

PRÁH DETEKCE

Ignorovat data s méně než nálezy.

∨ **PŘEDDEFINOVANÝ CITLIVÝ OBSAH**

∧ **VLASTNÍ VÝRAZY**

Zadejte vlastní regulární výrazy a klíčová slova pro detekci citlivých dat.

[Nový výraz](#)

Výraz	RegEx	
tajné	<input type="checkbox"/>	Odebrat

∨ **VLASTNÍ SLOVNÍKY**

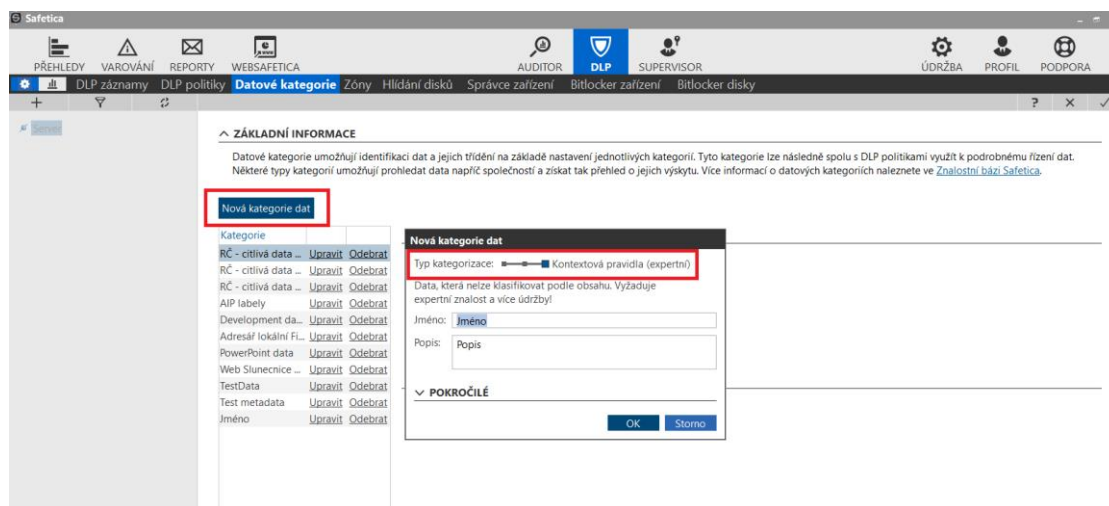
8.1.2. KONTEXTOVÁ KLASIFIKACE DAT

Kontextová klasifikace označuje soubory tagem na úložštích. Tag je uložen v extended attributech NTFS partition.

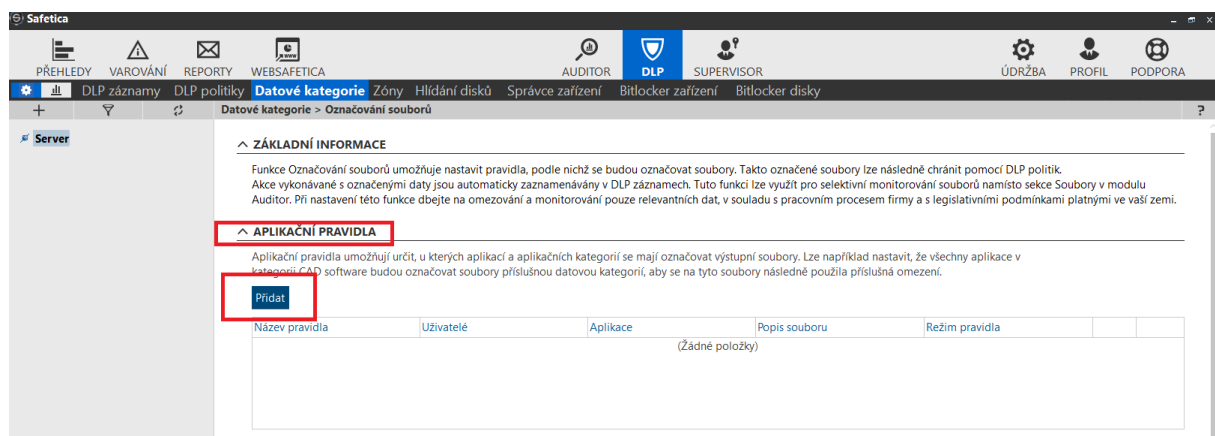
Kontextová klasifikace umožňují klasifikovat data na základě pravidel:

- Aplikační pravidla – data vygenerovaná definovanou aplikací – například Ginis
- Webová pravidla – data stažená z webového portálu – například CRM nebo HR systém
- Pravidla umístění – citlivá data uložená na úložštích – lokální nebo sdílené adresáře/disky

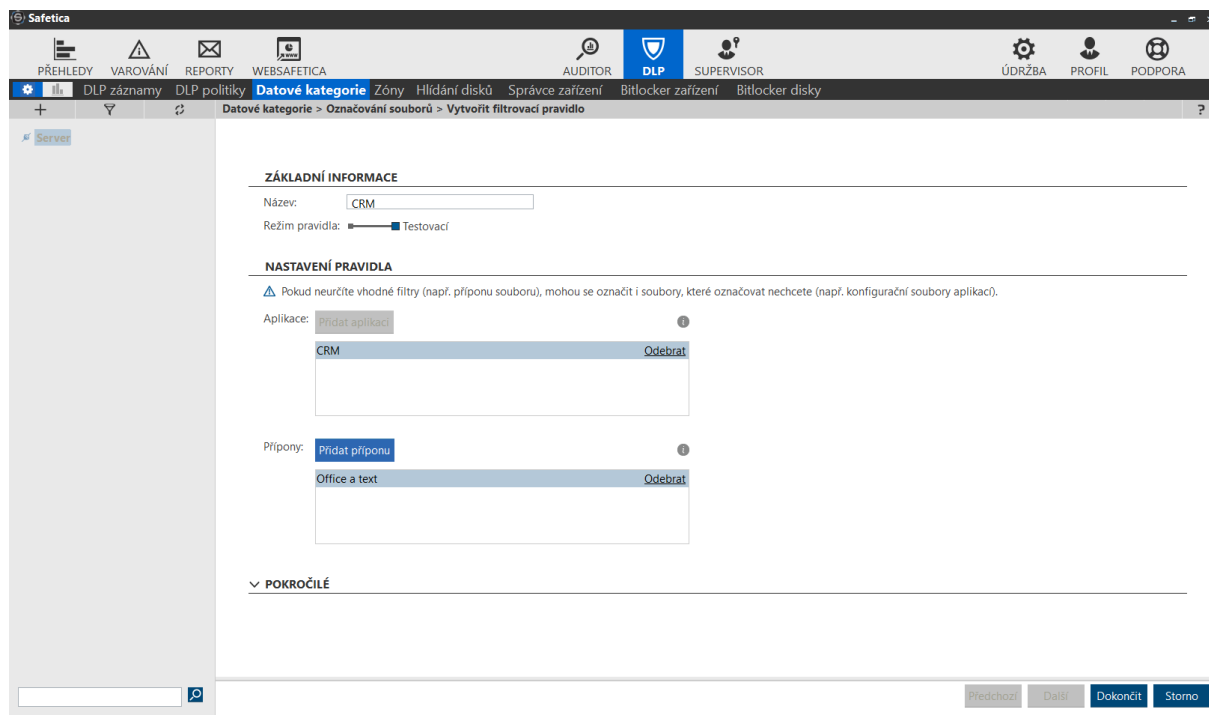
Příklad vytvoření kontextové klasifikace:



8.1.2.1 Nastavení aplikačního pravidla:



Definice aplikačního pravidla – výběr aplikace a souborů ,které budou klasifikovány tagem.
Příklad – aplikace skupiny CRM a soubory s příponami Office a text:



V tomto konkrétním případě budou kontextovou značkou označeny všechny soubory, které budou vytvořeny aplikacemi z aplikační skupiny „CRM“ a příponou ze skupiny „Office a text“.

Skupiny aplikací a přípon se definují v sekci Údržba/Kategorie/Kategorie aplikací nebo přípon, viz kapitola Údržba – Kategorie

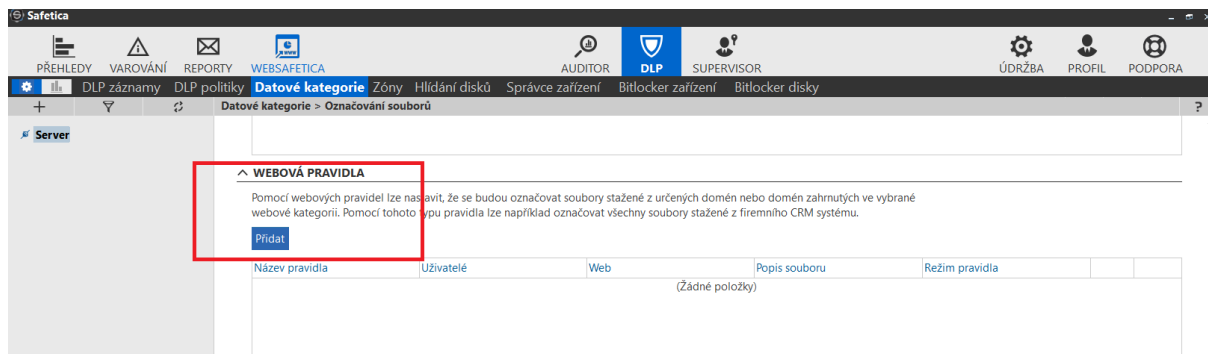
Klasifikaci dat je možné rozšířit a pokročilé nastavení, kde je možné definovat obsah, který bude při klasifikaci vyhledáván v souborech.



Tímto způsobem je možné označit pouze data, která byla vygenerována aplikací ze skupiny „CRM“ a měla příponu ze skupiny „Office a text“ a zároveň obsahovala slovo „tajně“.

Doporučení: Aplikovat pouze na textové dokumenty, ne na obrázky, grafiku nebo výkresy.

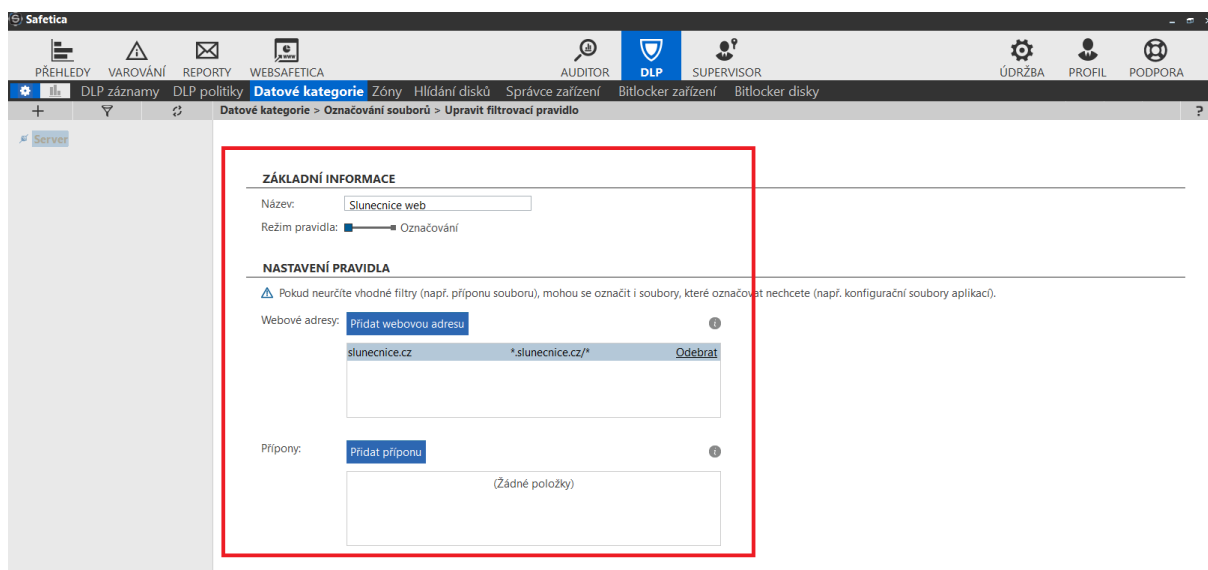
8.1.2.2 Nastavení webového pravidla



Definice webového pravidla – definice URL adresy a přípony stahovaných souborů.

Je možné vybrat skupinu webových serverů z přednastavených kategorií nebo definovat konkrétní URL adresu a příponu souborů.

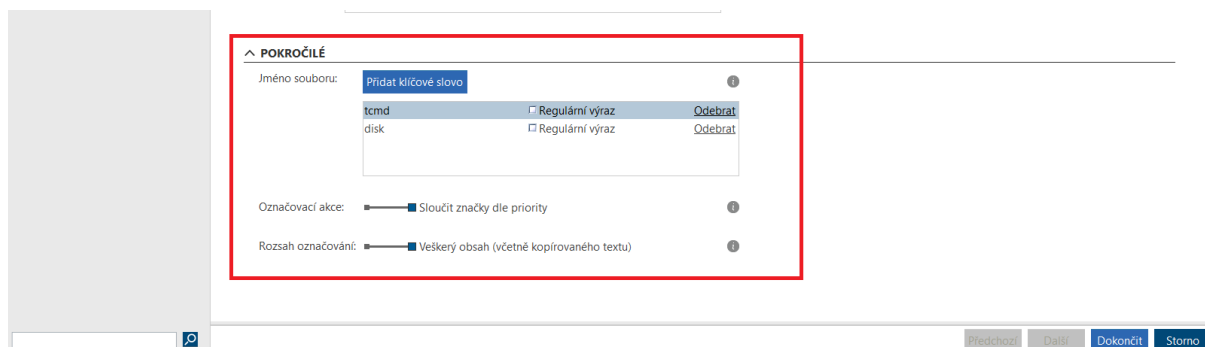
Soubory stažené z definované URL adresy s definovanou příponou budou označeny kontextovou značkou.



V tomto konkrétním případě budou kontextovou značkou označeny všechny soubory, které budou staženy z webové stránky „slunecnice.cz“ bez ohledu na příponu souboru.

Skupiny webových kategorií a přípon se definují v sekci Údržba/Kategorie/Kategorie webů nebo přípon, viz kapitola Údržba – Kategorie

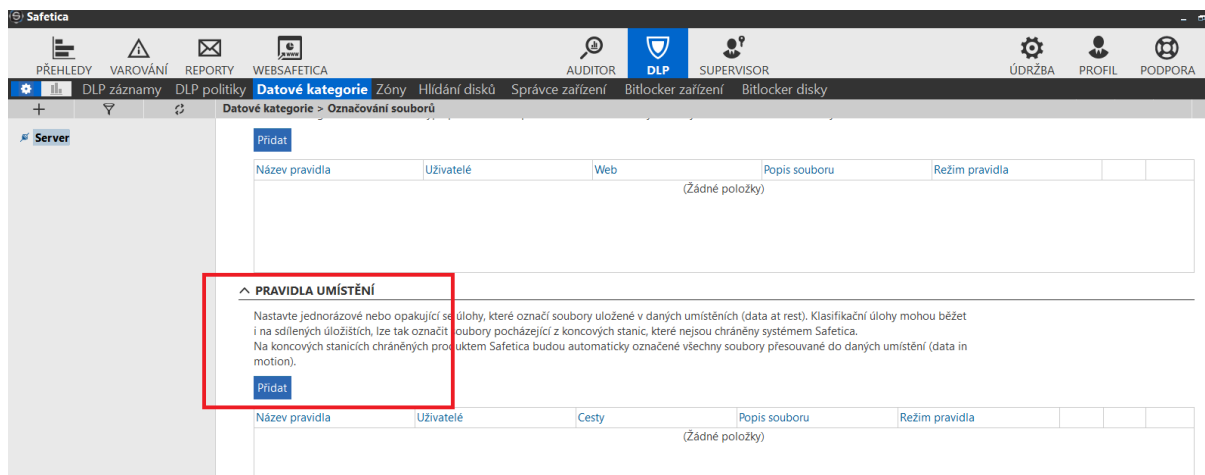
Klasifikaci dat je možné rozšířit a pokročilé nastavení, kde je možné definovat obsah, který bude při klasifikaci vyhledáván v souborech.



Tímto způsobem je možné označit pouze data, která byla stažena z webové stránky „slunecnice.cz“ a zároveň obsahovala slovo „TCMD“ a „DISK“.

Doporučení: Aplikovat pouze na textové dokumenty, ne na obrázky, grafiku nebo výkresy.

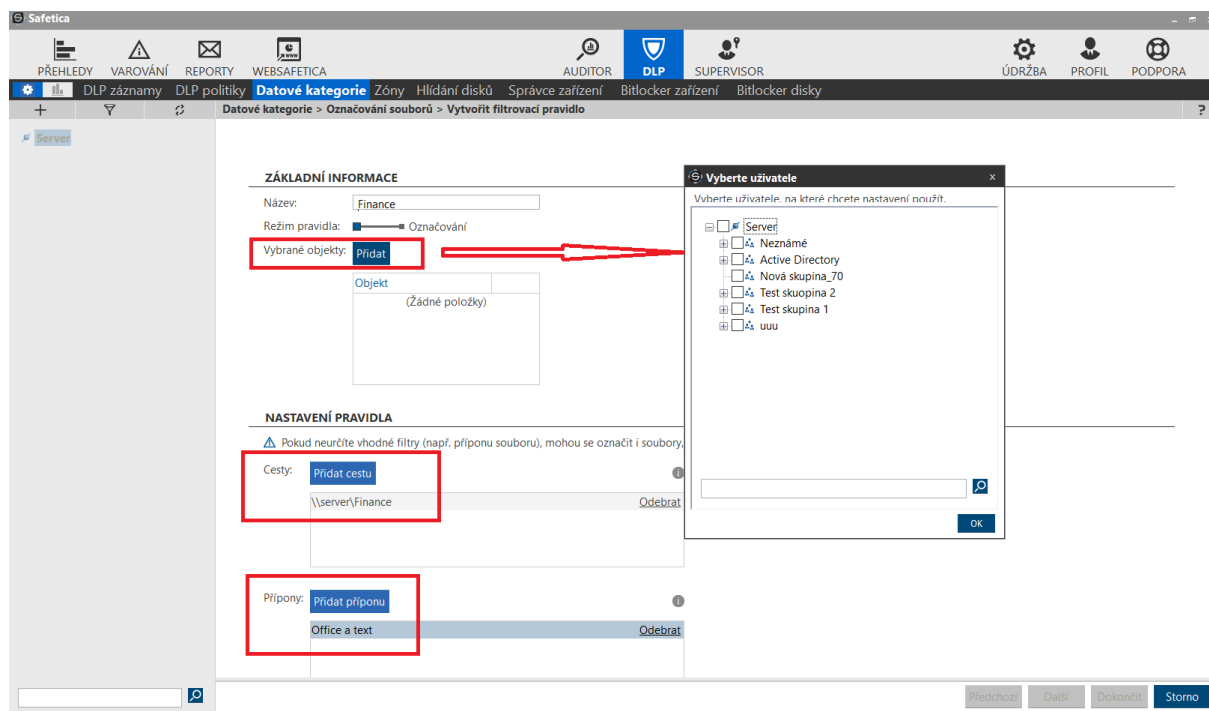
8.1.2.3 Nastavení pravidla umístění



Definice pravidla umístění – definice adresáře/disku, na kterých budou data označena tagem.

Je možné vybrat objekty, na které bude toto pravidlo uplatněno – počítače nebo uživatelé, kteří budou aktivně klasifikovat data na úložištích.

Dále se definuje adresář/disk/síťová cesta, kde budou data klasifikována a je možné vybrat i příponu, pro kterou budou data klasifikována tagem.



V tomto konkrétním případě budou kontextovou značkou označeny všechny soubory, které se uloží na sdílený adresář [\\server\finance](#) s příponou ze skupiny „Office a text“.

Skupiny přípon se definují v sekci Údržba/Kategorie/Kategorie přípon, viz kapitola Údržba – Kategorie

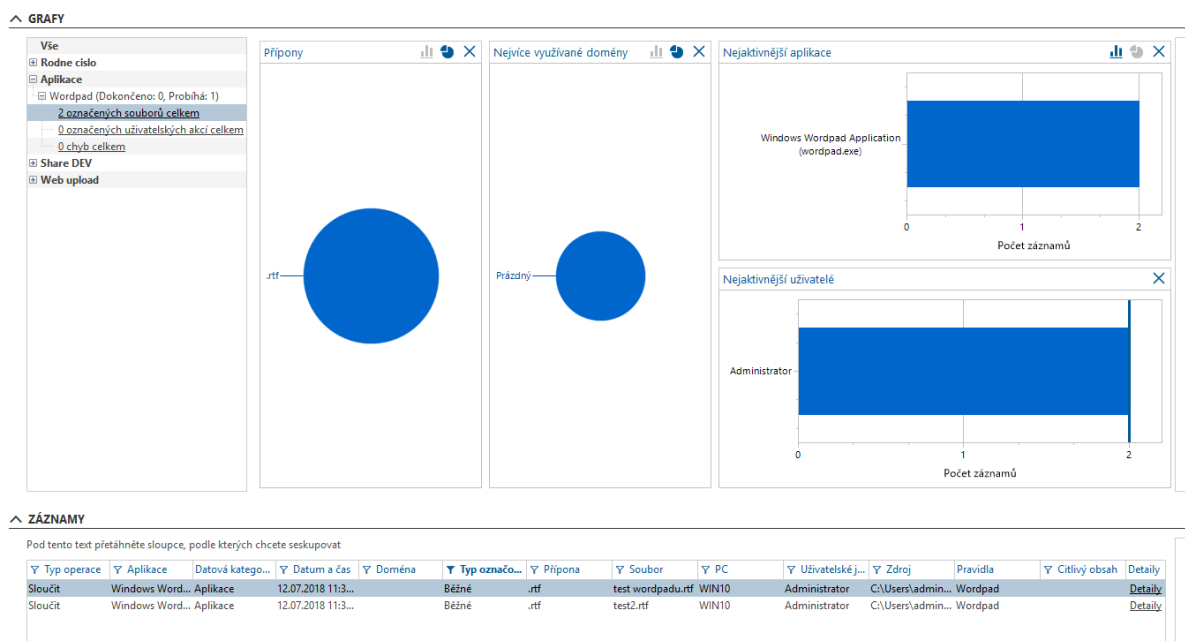
8.1.3. VIZUALIZACE ZOBRAZUJE VÝSLEDEK KLASIFIKACE DAT:

Vizualizace zobrazuje stav označování dokumentů.

Jsou zde zobrazené klasifikované soubory pomocí kontextové klasifikace dat - tagu:

- Aplikační pravidla
- Webová pravidla
- Pravidla umístění

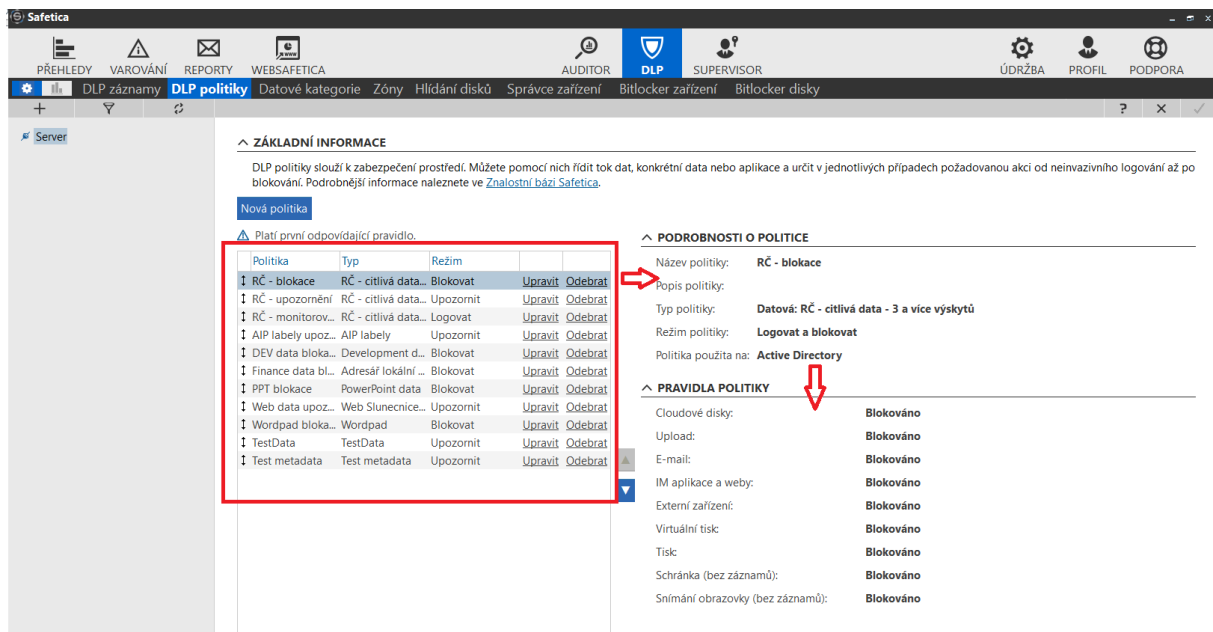
Citlivá data v seznamu nejsou – neoznačují se tagem, ale v případě detekce citlivého obsahu ve zpracovávaných datech si značku udržuje DLP engine v operační paměti a není uložena se souborem.



8.2. DLP POLITIKY

Politiky uplatňují bezpečnostní pravidla na obecné, datové nebo aplikační kategorie.

Politika definuje, jak se bude DLP agent chovat ke klasifikovaným datům pro jednotlivé komunikační kanály.



Server

ZÁKLADNÍ INFORMACE

DLP politiky slouží k zabezpečení prostředí. Můžete pomocí nich řídit tok dat, konkrétní data nebo aplikace a určit v jednotlivých případech požadovanou akci od neinvazivního logování až po blokování. Podrobnější informace naleznete ve [Znalostní bázi Safetica](#).

Nová politika

Platí první odpovídající pravidlo.

Politika	Typ	Režim		
RC - blokace	RC - citlivá data...	Blokovat	Upravit	Odebrat
RC - upozornění	RC - citlivá data...	Upozornit	Upravit	Odebrat
RC - monitorov...	RC - citlivá data...	Logovat	Upravit	Odebrat
AIP labely upoz...	AIP labely	Upozornit	Upravit	Odebrat
DEV data bloka...	Development d...	Blokovat	Upravit	Odebrat
Finance data bl...	Adresář lokální ...	Blokovat	Upravit	Odebrat
PPT blokace	PowerPoint data	Blokovat	Upravit	Odebrat
Web data upoz...	Web Služnice...	Upozornit	Upravit	Odebrat
Wordpad bloka...	Wordpad	Blokovat	Upravit	Odebrat
TestData	TestData	Upozornit	Upravit	Odebrat
Test metadata	Test metadata	Upozornit	Upravit	Odebrat

PODROBNOSTI O POLITICE

Název politiky: **RC - blokace**

Popis politiky:

Typ politiky: **Datová: RC - citlivá data - 3 a více výskytů**

Režim politiky: **Logovat a blokovat**

Politika použita na: **Active Directory**

PRAVIDLA POLITIKY

Cloudové disky:	Blokováno
Upload:	Blokováno
E-mail:	Blokováno
IM aplikace a weby:	Blokováno
Externí zařízení:	Blokováno
Virtuální tisk:	Blokováno
Tisk:	Blokováno
Schránka (bez záznamů):	Blokováno
Snímání obrazovky (bez záznamů):	Blokováno

DLP pravidla je možné nastavovat ve více kategoriích:

- Obecná pravidla
- Datová pravidla
- Aplikační pravidla

8.2.1. OBECNÁ PRAVIDLA

Obecná pravidla ovlivňují a řídí veškeré komunikační kanály bez ohledu na klasifikaci dat. Je možné monitorovat/blokovat jednotlivé komunikační kanály, přes která tečou data – například všechny e-mailové zprávy, uploady, externí zařízení atd.

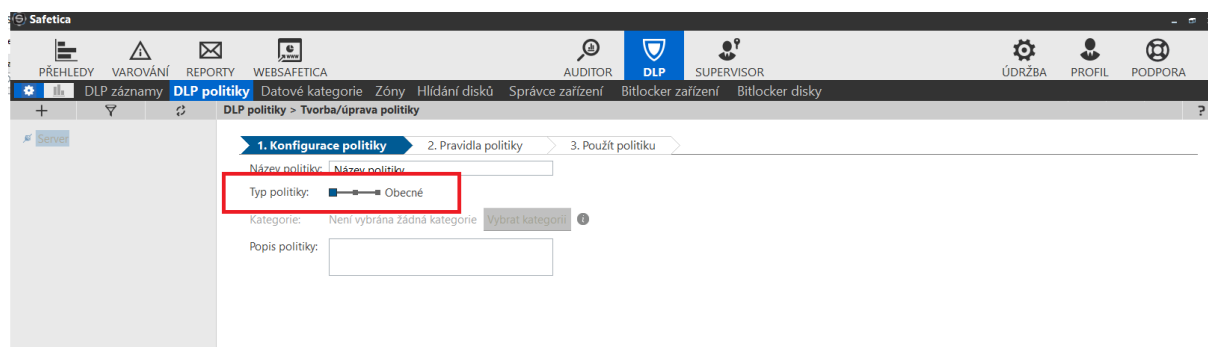
Obecné politiky jsou vhodné pro nastavení všeobecných podmínek toho, co je a co není povoleno, a je nejlepší je zařadit na konec seznamu DLP politik.

Doporučení: obecné pravidlo nastavit na logování. Při blokaci by byla veškerá data, na která nebyla uplatněna předchozí pravidla DLP politiky, blokována.

Obecná pravidla už nemají v současné verzi DLP Safetica velké opodstatnění.

Vytvoření obecného pravidla:

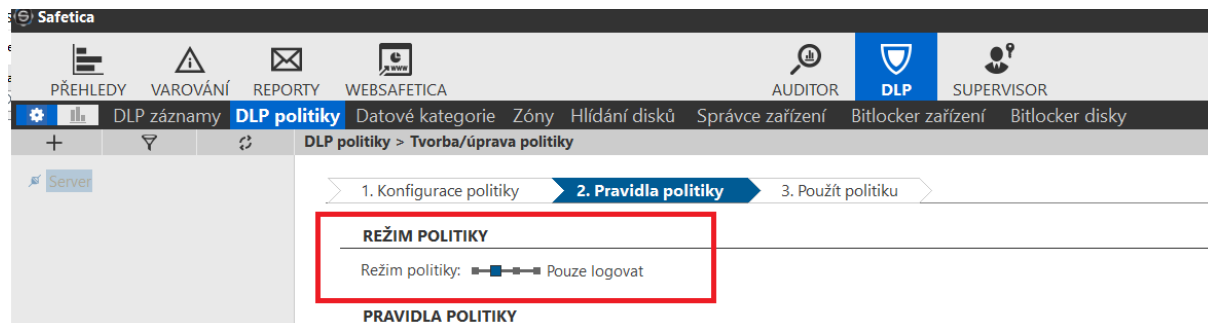
Konfigurace politiky - definuje název a Typ politiky – Obecné



Pravidla politiky – definuje chování politiky pro jednotlivé komunikační kanály.

Režim politiky

- Vypnuto – politika je vypnutá
- Pouze logovat – logují se události
- Logovat a upozornit – Safetica klient zobrazí okno, kde uživatel povolí nebo zakáže akci
- Logovat a blokovat – akce bude zakázána a logována

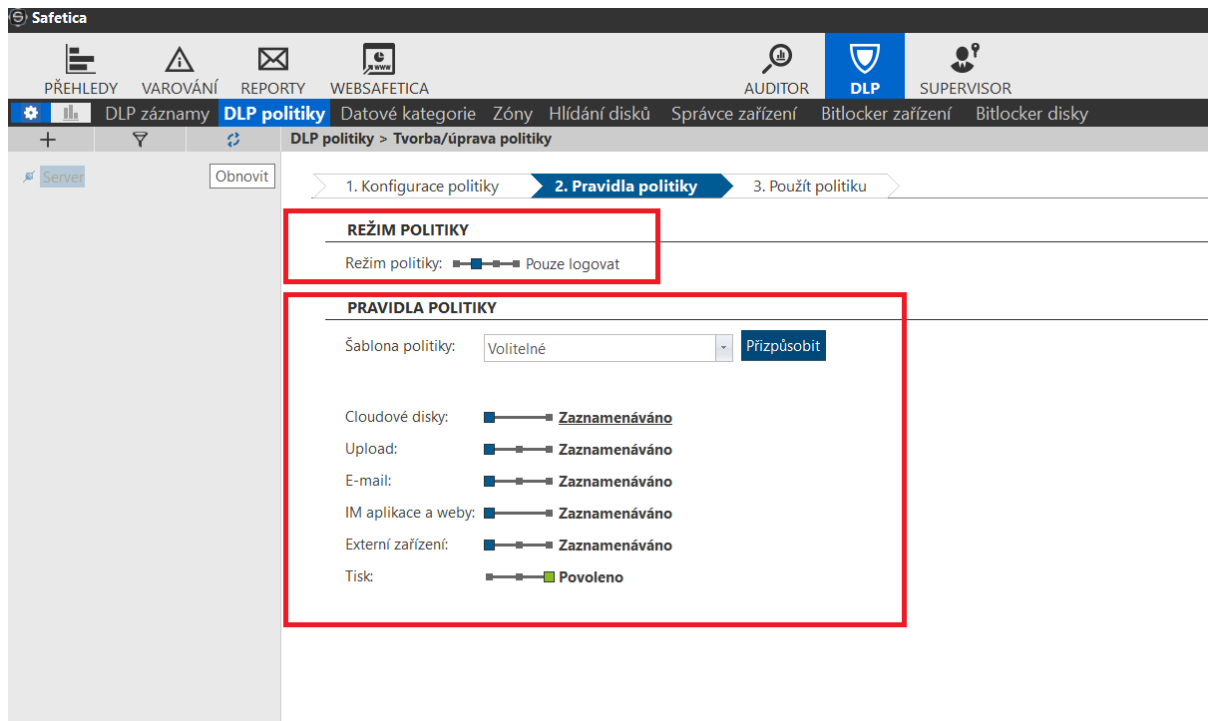


Pravidla politiky

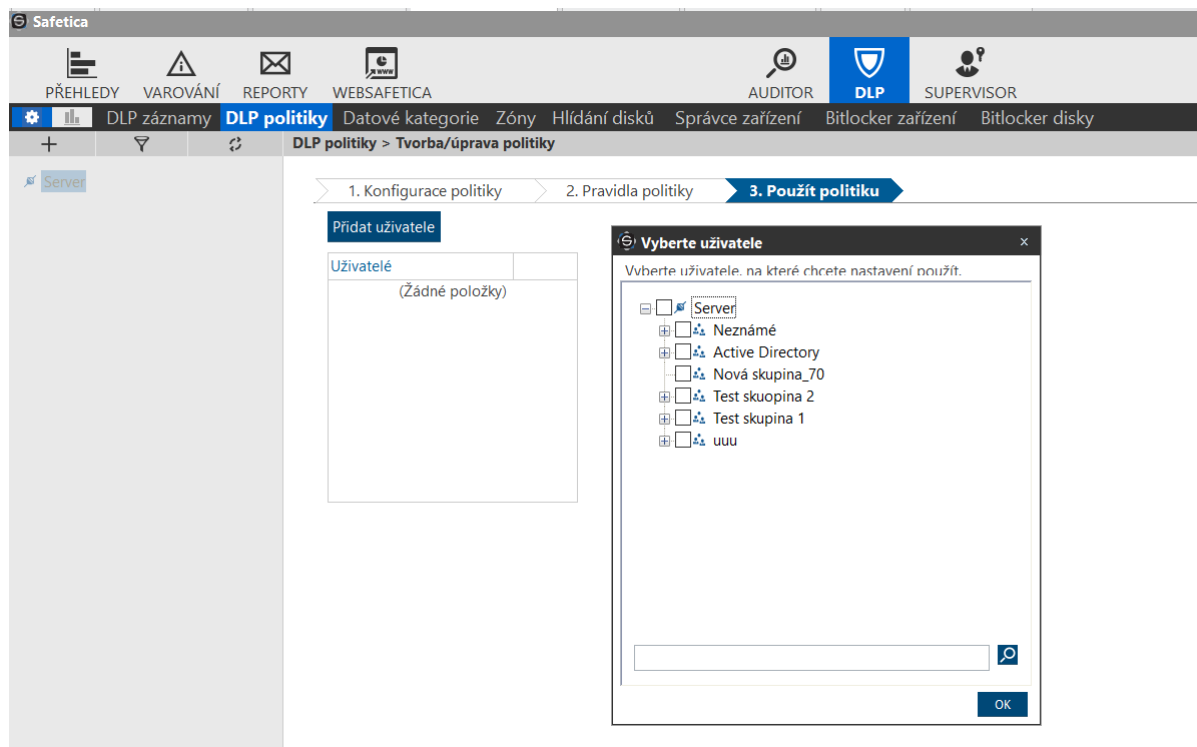
Definuje se chování DLP pravidla pro jednotlivé komunikační kanály – email, web, externí zařízení....

V závislosti na režimu politiky se nastavuje konkrétní akce pro jednotlivé komunikační kanály.

Na příkladu níže, režim politiky povoluje tisk, ostatní komunikační kanály budou povoleny a aktivita bude zaznamenána.



Použít politiku – definice, kde se bude politika uplatňovat – celá organizace, konkrétní uživatel, skupina nebo počítač:



8.2.2. DATOVÁ PRAVIDLA

Datová politika definuje a chrání citlivá data podle klasifikace dat vytvořené v datových kategoriích.

Datová pravidla mohou chránit:

- Data z oblasti dodržování předpisů, jako jsou osobní identifikační čísla, čísla kreditních karet, podmínky související s HIPAA atd – přednastavené klasifikátory
- Vlastní klíčová slova nebo regulární výrazy – klasifikátory definované správcem DLP
- Klasifikovaná data např. soubory označené jako "Interní", "Citlivé" atd – data klasifikovaná jiným klasifikačním nástrojem – Microsoft AIP, Titus, Boldon James, AEC DocTag
- Data klasifikovaná kontextovou klasifikací Safetica, např. soubory uložené ve sdíleném síťovém umístění, stažené soubory z intranetu, exporty CRM atd.

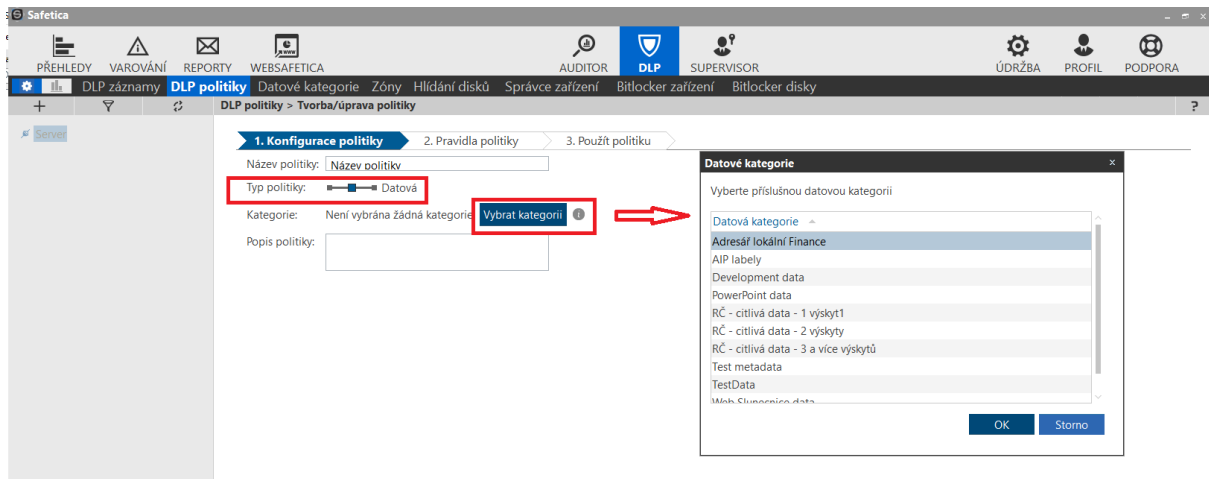
Datovou DLP politiku umísťujte do horní části seznamu politik, tak aby se uplatnila prioritně před obecnou politikou.

Vytvoření DLP datového pravidla:

Konfigurace politiky - definuje název

Typ politiky – Datová

Vybrat kategorii - Ze seznamu se vybere klasifikace dat – nastavená klasifikační pravidla v Datových kategoriích:



Pravidla politiky – definuje chování politiky pro jednotlivé komunikační kanály.

Režim politiky

- Vypnuto – politika je vypnutá
- Pouze logovat – logují se události
- Logovat a upozornit – Safetica klient zobrazí okno, kde uživatel povolí nebo zakáže akci
- Logovat a blokovat – akce bude zakázána a logována

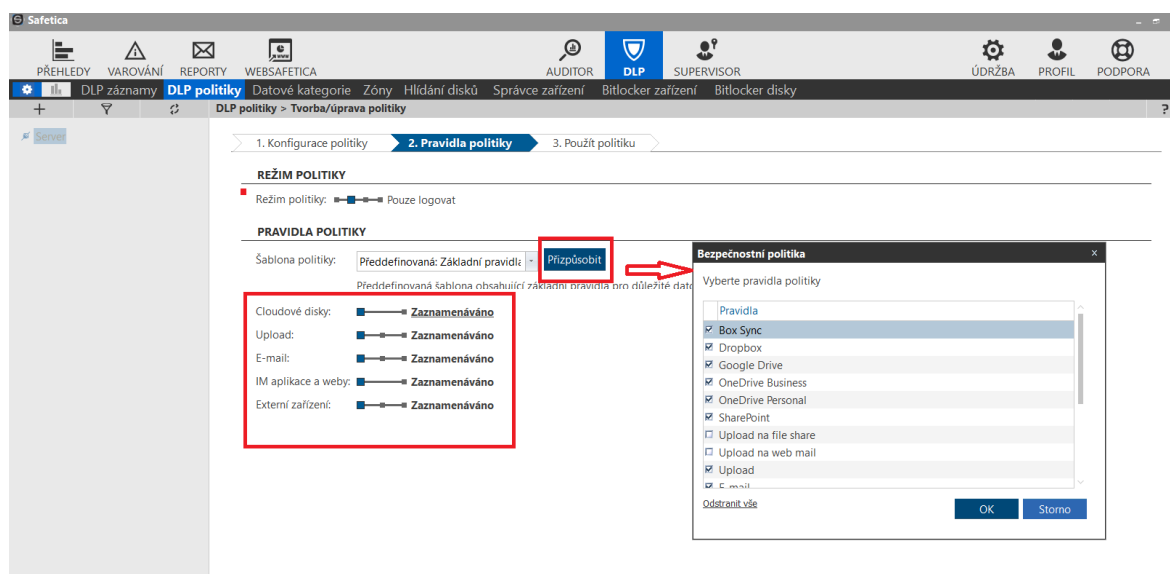


Pravidla politiky

Definuje se chování DLP pravidla pro jednotlivé komunikační kanály – email, web, externí zařízení....

V závislosti na režimu politiky se nastavuje konkrétní akce pro jednotlivé komunikační kanály.

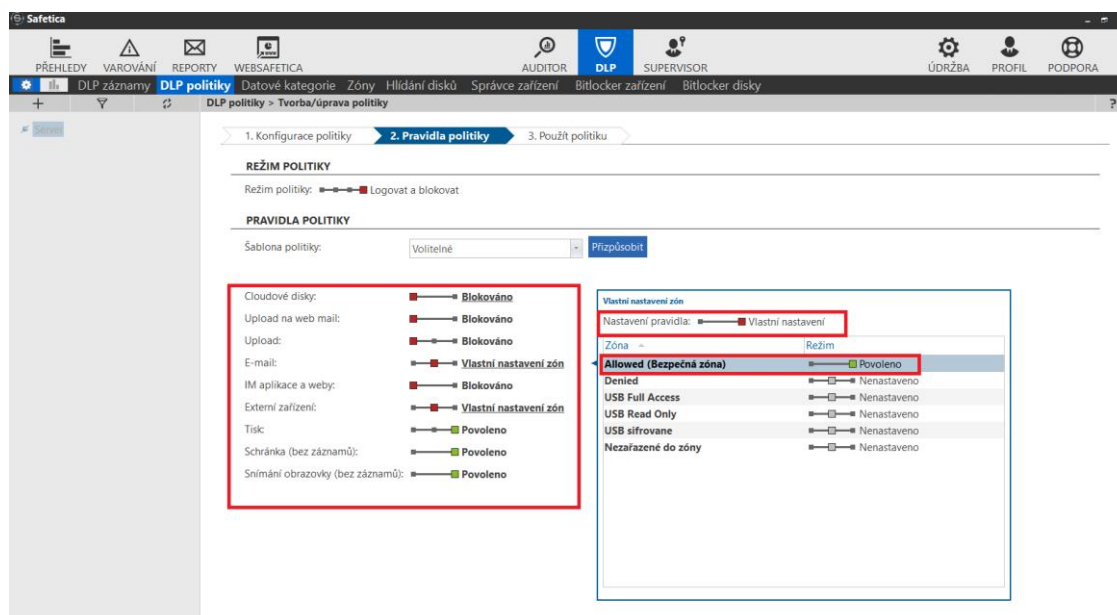
Při definici pravidla jsou výrobcem nabídnuty standardní komunikační kanály. Pomocí tlačítka „Přizpůsobit“ je možné zvolit další komunikační kanály, které budou v tomto DLP pravidle sledovány.



Na základě výběru komunikačních kanálů pro DLP pravidlo je poté možné každému pravidlu nastavit akci – v případě blokování – blokaci nebo povolení.

Na příkladu níže, režim politiky loguje a upozorňuje tisk dat, copy/paste a printscreen

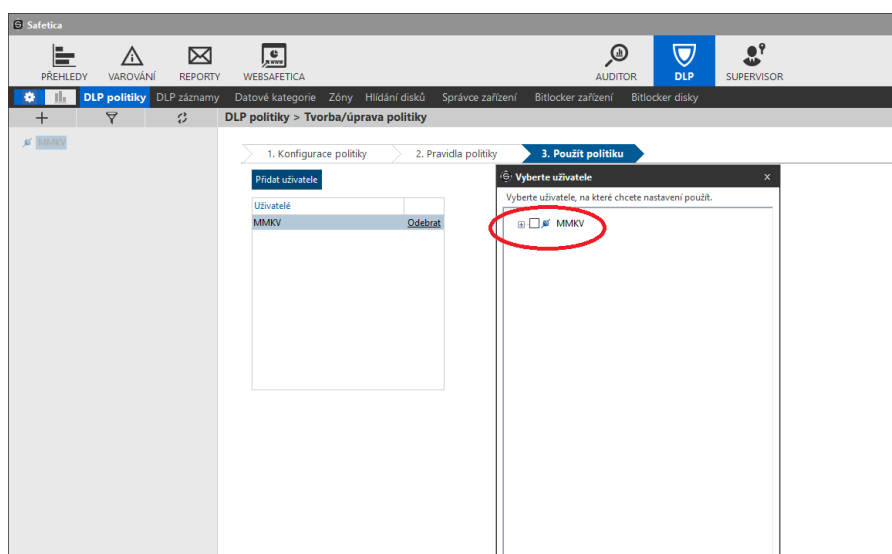
Odchod dat přes ostatní definované komunikační kanály je blokován



Pro určité komunikační kanály je možné zvolit „Vlastní nastavení“ – například email, nebo externí zařízení. Tím lze dosáhnout toho, že například emaily mimo společnost budou blokovány, ale v rámci tzv. Allowed zón, kde bude nastavena lokální emailová doména, budou emaily pouze logovány a uživatelé si data mohou předávat.

Definice zón a jejich vlastnosti je popsáno v kapitole Údržba / Zóny.

Použití politiku – definice, kde se bude politika uplatňovat – celá organizace, konkrétní uživatel, skupina nebo počítač:



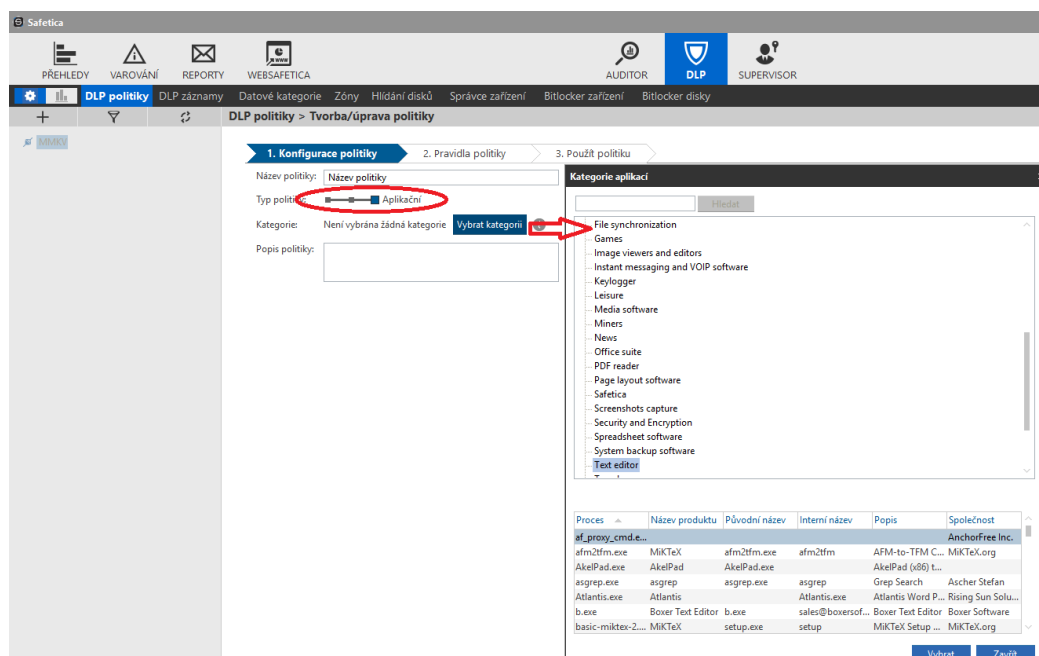
8.2.3. APLIKAČNÍ PRAVIDLA

Aplikační pravidla upravují způsob práce s aplikacemi. Jsou aplikovány na kategorie aplikací.

Aplikační DLP politiku umístíte do horní části seznamu politik spolu s datovými politikami, kde je seřadíte podle vaší upřednostňované priority.

Konfigurace politiky - definuje název a Typ politiky – Aplikační

Ze seznamu se vybere kategorii aplikací



Pravidla politiky – definuje chování politiky pro jednotlivé komunikační kanály.

Režim politiky

- Vypnuto – politika je vypnutá
- Pouze logovat – logují se události
- Logovat a upozornit – Safetica klient zobrazí okno, kde uživatel povolí nebo zakáže akci
- Logovat a blokovat – akce bude zakázána a logována

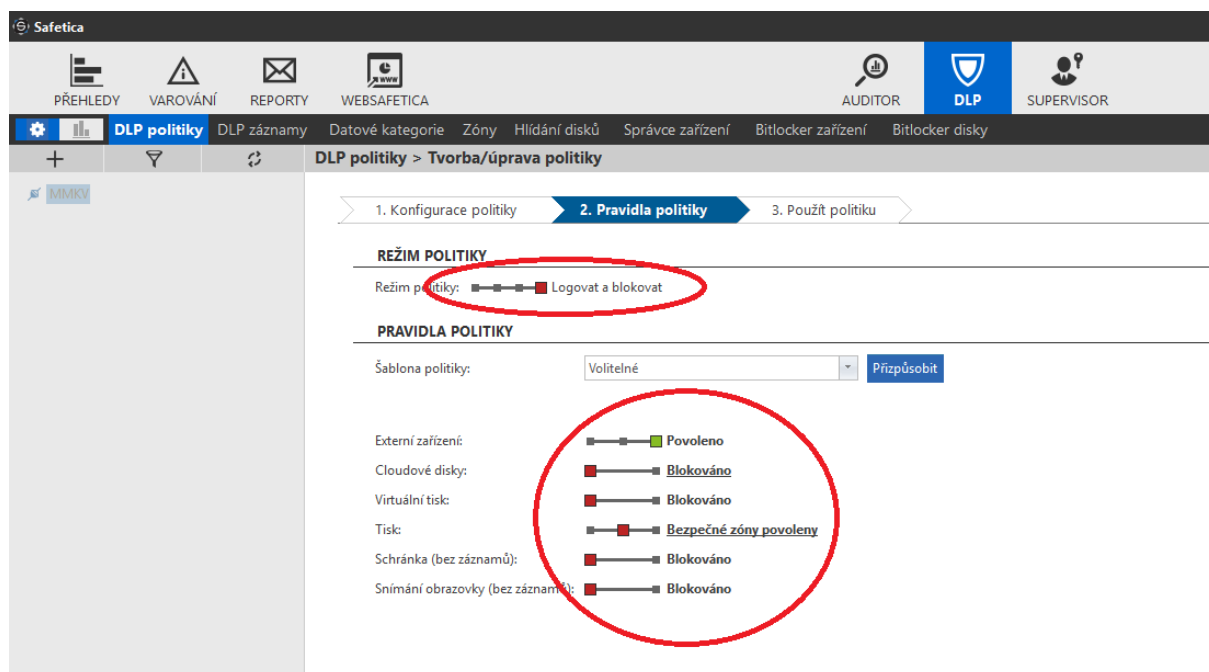


Pravidla politiky

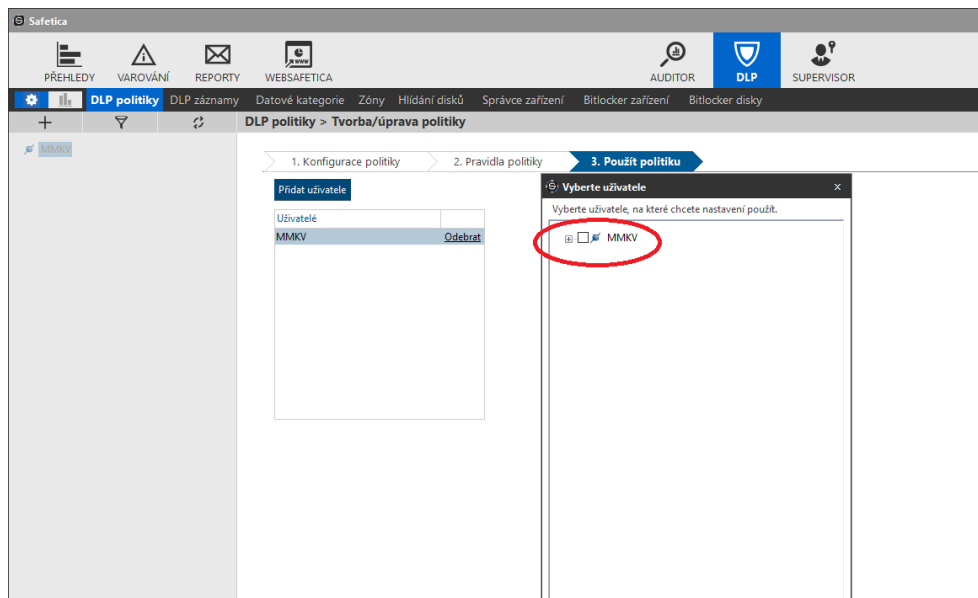
Definuje, jak budou moci nastavené aplikace komunikovat přes jednotlivé komunikační kanály – email, web, externí zařízení....

V závislosti na režimu politiky se nastavuje konkrétní akce pro jednotlivé komunikační kanály.

Na příkladu níže, režim politiky blokuje a loguje aplikace pro všechny komunikační kanály kromě Externích zařízení, které pouze loguje



Použít politiku – definice, kde se bude politika uplatňovat – celá organizace, konkrétní uživatel, skupina nebo počítač:



8.3. DLP ZÁZNAMY

Zobrazuje grafy a záznamy o detekovaných událostech na jednotlivých zařízeních. Je možné filtrovat jak na časové období – dny, tak na uživatele, typ operace, počítač apod.

The screenshot displays the Safetica DLP interface with several components:

- Left Panel:** A tree view showing the server structure, including 'Server', 'Active Directory', 'Users', and 'Administrator'.
- Top Charts:**
 - Nejaktivnější uživatelé:** A horizontal bar chart showing 'Administrator' as the most active user with a total size of approximately 160 KB.
 - Nejaktivnější aplikace:** A horizontal bar chart showing 'Microsoft Outlook (outlook.exe)' as the most active application with a total size of approximately 120 KB.
- Middle Charts:**
 - Nejvyužívanější akce:** A pie chart showing the most used actions: 'Zakázat' (blue), 'Povolit' (green), and 'Upozornění' (red).
 - Nejvyužívanější operace:** A pie chart showing the most used operations: 'E-mail' (blue), 'Otevření souboru' (red), 'Kopírování souboru' (green), 'Upload na web' (yellow), and 'Snímky obrazovky' (purple).
- Bottom Section:** A table titled 'ZÁZNAMY' (Records) with columns for 'Typ operace', 'Uživatelové jméno', 'Akce', 'Soubor', 'Aplikace', 'Od', 'Typ zdroje', 'Zdrojové za...', 'PC', 'Zdroj', 'Typ cíle', 'Cílové zařízení', 'Dat...', 'Velikost s...', 'Detaily', and 'Moduly'. The table lists several records, including actions like 'Upload na web', 'E-mail', and 'Snímky obrazovky' performed by 'Administrator'.

This section provides a closer look at the two pie charts:

- Nejvyužívanější akce:** A pie chart where 'Povolit' (green) is the dominant category, representing the majority of the data.
- Nejvyužívanější operace:** A pie chart with three main categories: 'Upload na web' (blue), 'Tisk' (red), and 'E-mail' (green).

The 'ZÁZNAMY' table shows the following records:

Uživatelové jméno	Typ	Typ ...	S...	Apl...	O...	T...	Z...	...	Cit...	Dato...	Cílov...	Velikost...	Detaily	Moduly
Politika: (Prázdný) Celková velikost: 45 B														
Politika: Channel control - MMKV - All data - default action Celková velikost: 41.08 MB														
Politika: Channel control - MMKV - Sensitive data - default action Celková velikost: 680.56 KB														

8.4. ZÓNY

Pomocí zón lze vytvářet pojmenované sady externích zařízení, tiskáren, IP adres, síťových cest a e-mailů, na které se lze odkazovat jako na celek. Vytvořené zóny se využívají v DLP politikách. Safetica umožňuje definovat zóny, které mohou obsahovat:

- Definice IP adres – lokální síť
- Definice emailových adres – lokální doména
- Definice webových adres – lokální webové servery
- Definice zařízení – USB flash disky, Bluetooth zařízení..

^ ZÁKLADNÍ INFORMACE

Zóny umožňují vytvářet skupiny zařízení, domén a síťových cest, které lze hromadně řídit různými DLP funkcemi. Zóny označené jako bezpečné lze také využít pro nastavení důvěryhodného fire [politikách](#).

Obsah zóny Nezařazené položky

V této části naleznete všechny existující zóny. Můžete si zde prohlížet jejich obsah a přidávat další zařízení.

[Přidat zónu](#)

Název zóny		
Allowed	Upravit	Odebrat
Denied	Upravit	Odebrat
USB block	Upravit	Odebrat
USB Full Access	Upravit	Odebrat
USB Read Only	Upravit	Odebrat

INFORMACE O ZÓNĚ

Název zóny: Allowed (Bezpečná zóna)

Popis: -

[Přidat položku](#)

Obsah zóny:

<ul style="list-style-type: none"> USB <ul style="list-style-type: none"> Mass storage <ul style="list-style-type: none"> (Žádné položky) Ostatní (není zahrnuto v DLP politikách) <ul style="list-style-type: none"> (Žádné položky) Tiskárny <ul style="list-style-type: none"> Fyzické tiskárny <ul style="list-style-type: none"> (Žádné položky) Síťové tiskárny <ul style="list-style-type: none"> (Žádné položky) Síť <ul style="list-style-type: none"> Síťové cesty <ul style="list-style-type: none"> (Žádné položky) IP adresy <ul style="list-style-type: none"> (Žádné položky)
--

Příklad definice dalších zón, které je možné následně využít v nastavení

- USB Read Only
- USB Full Access
- USB Block

Zóny jsou v prázdné, bez definovaných zařízení. V budoucnu je možné do zón přiřadit jednotlivé parametry a zajistit tak správu externích zařízení, nebo zóny využít v DLP pravidlech pro detailnější nastavení.

ZÁKLADNÍ INFORMACE

V pohledu Zóny můžete vytvářet zóny, do kterých lze zařadit externí zařízení, tiskárny, IP adresy, síťové cesty, e-mailové adresy a webové adresy. Zóny využívají funkce [DLP pravidla](#) a Bezpečného firemního prostředí, pro které můžete nastavit výjimky v [Řízení toku dat](#).

Obsah zóny Nezařazené položky (3)

V této části naleznete všechny existující zóny. Můžete si zde prohlédnout jejich obsah a přidávat další zařízení.

Přidat zónu

Název zóny		
Allowed (Bezpečná zóna)	Upravit	
Denied	Upravit	Odebrat
USB Read Only	Upravit	Odebrat
USB Full Access	Upravit	Odebrat

INFORMACE O ZÓNĚ

Název zóny: USB Full Access
 Popis: -

Přidat položku

Obsah zóny:

- USB
 - Mass storage
 - Kingston DTR30G2 USB Device [Detaily](#) [Upravit](#) [Odebrat](#)
 - Patriot Memory USB Device [Detaily](#) [Upravit](#) [Odebrat](#)
 - Ostatní (není zahrnuto v DLP pravidlech)
 - (Žádné položky)
 - Tiskárny
 - Fyzické tiskárny
 - (Žádné položky)
 - Síťové tiskárny
 - (Žádné položky)
 - Síť
 - Síťové cesty
 - (Žádné položky)
 - IP adresy
 - (Žádné položky)
 - Webové adresy
 - (Žádné položky)
 - E-maily
 - (Žádné položky)
 - Přenosná zařízení systému Windows (není zahrnuto ...)
 - (Žádné položky)

Nezařazené položky – detekovaná zařízení, například USB Flash disky mohou být přesunuty do přednastavených zón.

Přiřazení zařízení je možné přetažením zařízení z nezařazených položek do konkrétní zóny

ROZDĚLOVÁNÍ POLOŽEK

Název zóny: Allowed (Bezpečná zóna)

Položky, které nejsou přiřazeny do žádné zóny:

Název zóny		
Allowed	Upravit	Odebrat
Denied	Upravit	Odebrat
USB block	Upravit	Odebrat
USB Full Access	Upravit	Odebrat
USB Read Only	Upravit	Odebrat

Nezařazené položky

- USB
 - Mass storage (posledních 30 dnů)
 - ADATA USB Flash Drive USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - ADATA USB Flash Drive USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Disková jednotka [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Disková jednotka (Garmin VYA3 Flash USB Devi... [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Generic Flash Disk USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Generic Flash Disk USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - CHIPSBNK v3.3.9.1 USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Kingston DataTraveler 2.0 USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Kingston DT 101 G2 USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Patriot Memory USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Samsung Digital Camera USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - UFD 2.0 Silicon-Power30G USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - USB DISK 2.0 USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - WD Elements 1078 USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - WD My Passport 0748 USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)
 - Ostatní (není zahrnuto v DLP politikách)
 - Generic-Multi-Card USB Device [Detaily](#) [Upravit](#) [Přidat](#) [Odebrat](#)

8.5. HLÍDÁNÍ DISKŮ

Pomocí hlídání disků je možné jednoduchými pravidly nastavit uživatelům oprávnění k přístupu k souborovému systému. Například zvolit disky, na které budou mít přístup, nebo ze kterých mohou jenom číst popřípadě zvolit přímo jednotlivé cesty respektive složky

Hlídání disků umožňuje definovat právo přístupu nebo blokovat přístup nebo povolit pouze čtení k:

- lokálním adresářům
- sdíleným adresářům
- lokálním diskům
- cloudovým službám

Příklad nastavení definice přístupu na lokální, síťové a Cloudové disky u konkrétních jednotlivců nebo skupin počítačů.

- Definice lokálních cest – lokální disk – povolit vše
- Definice síťových cest – sdílené disky – povolit vše
- Definice cloudových disků – povolit vše


^ ZÁKLADNÍ INFORMACE

Pomocí funkce Hlídání disků můžete zakázat přístup k diskovým jednotkám, lokálním nebo síťovým cestám. Přístupy k diskům nebo cestám mohou být zaznamenávány.

^ NASTAVENÍ ZAZNAMENÁVÁNÍ

Zaznamenávání: Zastaveno Zapnuto

CESTY

 Zákaz systémového disku může způsobit nefunkčnost důležitých programů. Takové nastavení bude na klientské stanici ignorováno.

Cesta	Přístup	
Lokální cesty		
(Žádné položky)		
Síťové cesty		
(Žádné položky)	<input type="checkbox"/> Zdědit	
Jednotky		
Cloudové disky		
OneDrive Personal	<input checked="" type="checkbox"/> Povolit	0 koncových stanic
OneDrive Business	<input checked="" type="checkbox"/> Povolit	0 koncových stanic
SharePoint	<input checked="" type="checkbox"/> Povolit	0 koncových stanic
Google Drive	<input checked="" type="checkbox"/> Povolit	0 koncových stanic
Dropbox	<input checked="" type="checkbox"/> Povolit	0 koncových stanic
Box Sync	<input checked="" type="checkbox"/> Povolit	0 koncových stanic

8.6. SPRÁVCE ZAŘÍZENÍ

Pomocí správce zařízení je možné povolit nebo zakázat používání a přístup k různým druhům externích zařízení. Přístup k USB, Bluetooth, FireWire zařízením a přenosným zařízením systému Windows můžete řídit pomocí zón.

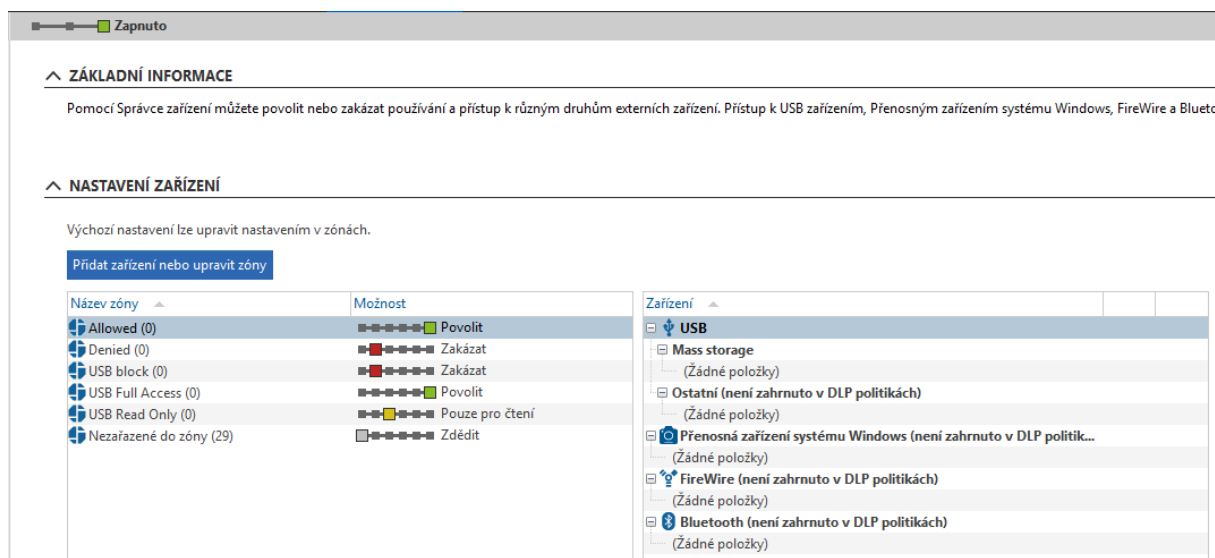
Je možné definovat globální pravidla pro jednotlivé typy portů, nebo nastavit detailní konfiguraci pro konkrétní zařízení, které bylo historicky připojeno k počítači s DLP agentem a je načteno nezařazených zařízeních – Nastavení Zóny.

System umožňuje vytvářet velice detailní pravidla jak pro globální chování, tak pravidla pro uživatele, počítače a skupiny.

8.6.1. DEFINICE ZÓN

Pro definované zóny jsou nastavena pravidla chování ve správci zařízení

- Allowed zóna povolena
- Denied zóna blokována
- USB Read Only zóna povolena pouze pro čtení
- USB Full access zóna povolena
- USB Block zóna blokována



The screenshot shows the 'Správce zařízení' (Device Manager) interface. At the top, there is a status bar with a green indicator and the text 'Zapnuto'. Below this, there are two main sections: 'ZÁKLADNÍ INFORMACE' and 'NASTAVENÍ ZAŘÍZENÍ'.

ZÁKLADNÍ INFORMACE
 Pomocí Správce zařízení můžete povolit nebo zakázat používání a přístup k různým druhům externích zařízení. Přístup k USB zařízením, Přenosným zařízením systému Windows, FireWire a Blueto

NASTAVENÍ ZAŘÍZENÍ
 Výchozí nastavení lze upravit nastavením v zónách.
 Přidat zařízení nebo upravit zóny

Název zóny	Možnost
Allowed (0)	Povolit
Denied (0)	Zakázat
USB block (0)	Zakázat
USB Full Access (0)	Povolit
USB Read Only (0)	Pouze pro čtení
Nezařazené do zóny (29)	Zdědit

Zařízení

- USB
 - Mass storage (Žádné položky)
 - Ostatní (není zahrnuto v DLP politikách) (Žádné položky)
 - Přenosná zařízení systému Windows (není zahrnuto v DLP politik... (Žádné položky)
 - FireWire (není zahrnuto v DLP politikách) (Žádné položky)
 - Bluetooth (není zahrnuto v DLP politikách) (Žádné položky)

Pro každou zónu je možné v budoucnu pomocí šoupátka upravit jednotlivá nastavení jak globálně, tak například pro určitý počítač nebo skupinu uživatelů, popřípadě konkrétního uživatele.

8.6.2. NASTAVENÍ PORTŮ POČÍTAČE

V této části je možné globálně upřesnit možnost přístupu k jednotlivým typům zařízení nebo jiným

souborovým systémům než NTFS. Například FAT32, ext3, ext4 apod.

V rámci nasazení je provedena definice správy portů u konkrétních jednotlivců nebo skupin počítačů, zvolen je Testovací režim

- USB
- Čtečka karet
- Přenosná zařízení systému Windows
- CD/DVD
- FireWire
- IrDA
- Bluetooth
- COM
- LPT

^ POKROČILÁ NASTAVENÍ

Jiné souborové systémy než NTFS: Povolit

Nastavení portů

USB: Testovací režim

Čtečka karet: Testovací režim

Přenosná zařízení systému Windows: Testovací režim

CD/DVD: Testovací režim

FireWire: Testovací režim

IrDA: Testovací režim

Bluetooth: Testovací režim

COM: Testovací režim

LPT: Testovací režim

Pokročilé nastavení je možné v budoucnu pomocí šoupátka upravit jak globálně, tak například pro určitý počítač nebo skupinu uživatelů, popřípadě konkrétního uživatele.

8.7. BITLOCKER ZAŘÍZENÍ

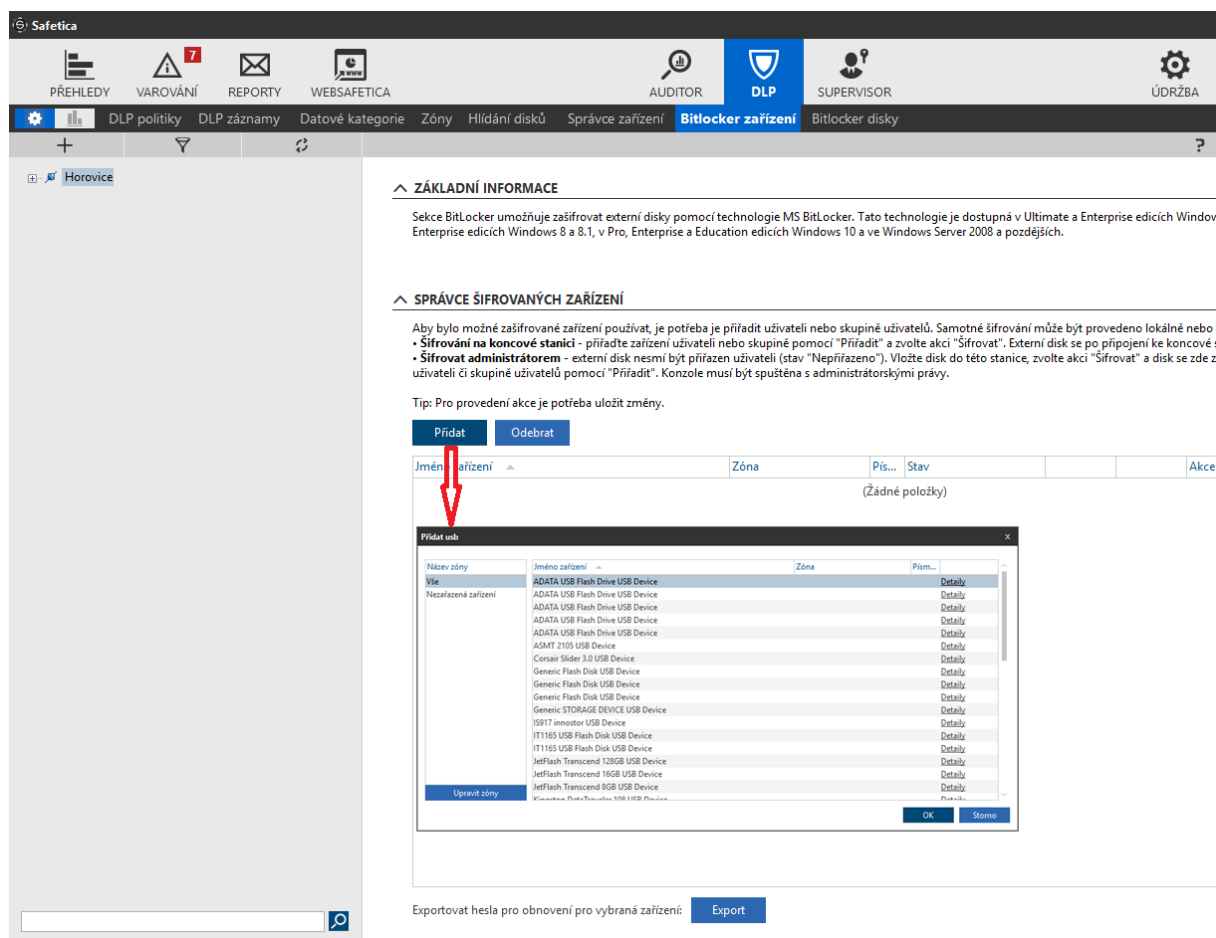
Tato funkce umožňuje šifrovat externí disky pomocí nástroje BitLocker od společnosti Microsoft. Přístup k zašifrovaným zařízením lze přiřazovat jednotlivým uživatelům, počítačům nebo skupinám.

Zašifrování USB flash disků lze provést na počítači, na kterém je nainstalována konzole nebo na počítači s klientem, ke kterému je flash disk připojen..

Je možné selektivně vybírat uživatele, nebo počítače, kterým bude zašifrovaná USB disk přístupný.

Tlačítkem „Přidat“ je možné vybrat zařízení, které má být pomocí technologie Bitlocker šifrováno.

Seznam zobrazí veškerá USB zařízení, která byla k systémům se Safetica klientem v minulosti připojena.



Safetica

PŘEHLEDY VAROVÁNÍ REPORTY WEBSAFETICA AUDITOR DLP SUPERVISOR ÚDRŽBA

DLP politiky DLP záznamy Datové kategorie Zóny Hlídaní disků Správce zařízení **Bitlocker zařízení** Bitlocker disky

Horovice

ZÁKLADNÍ INFORMACE

Sekke BitLocker umožňuje zašifrovat externí disky pomocí technologie MS BitLocker. Tato technologie je dostupná v Ultimate a Enterprise edicích Windows Enterprise edicích Windows 8 a 8.1, v Pro, Enterprise a Education edicích Windows 10 a ve Windows Server 2008 a pozdějších.

SPRÁVCE ŠIFROVANÝCH ZAŘÍZENÍ

Aby bylo možné zašifrované zařízení používat, je potřeba je přiřadit uživateli nebo skupině uživatelů. Samotné šifrování může být provedeno lokálně nebo v.

- Šifrování na koncové stanici** - přiřadíte zařízení uživateli nebo skupině pomocí "Přiřadit" a zvolíte akci "Šifrovat". Externí disk se po připojení ke koncové s
- Šifrovat administrátorem** - externí disk nesmí být přiřazen uživateli (stav "Nepřiřazeno"). Vložíte disk do této stanice, zvolíte akci "Šifrovat" a disk se zde za uživateli či skupině uživatelů pomocí "Přiřadit". Konzole musí být spuštěna s administrátorskými právy.

Tip: Pro provedení akce je potřeba uložit změny.

Přidat **Odebrat**

Jméno zařízení	Zóna	Přím...	Stav	Akce
(Žádné položky)				

Přidat usb

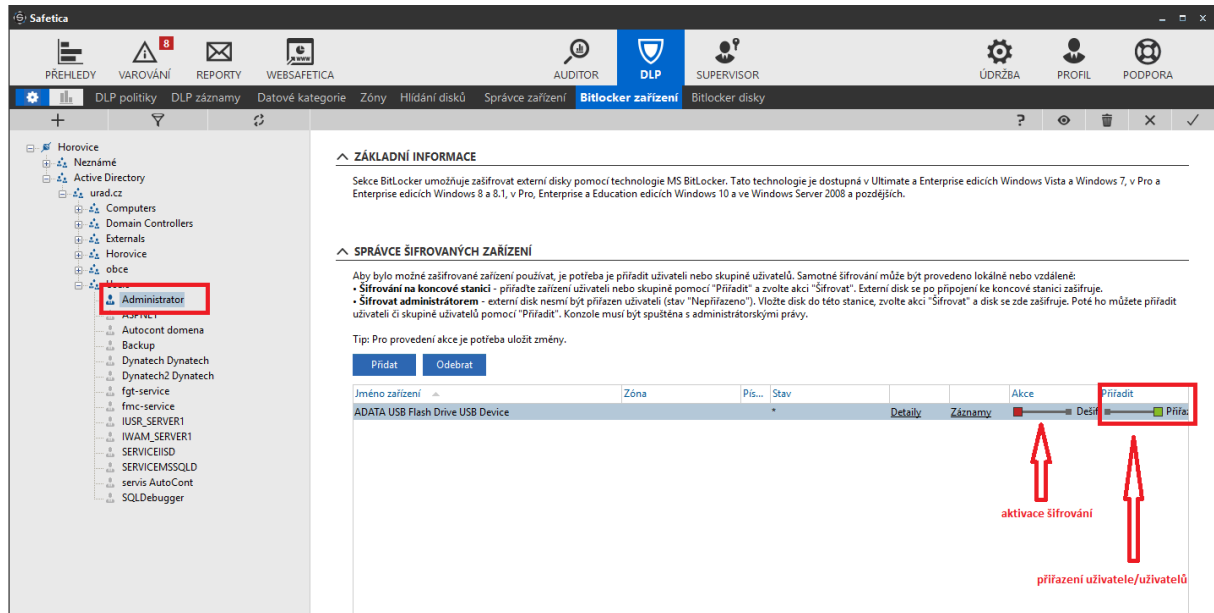
Název zóny	Jméno zařízení	Zóna	Přím...	Akce
Vše	ADATA USB Flash Drive USB Device		Detaily	
Nerealizovaná zařízení	ADATA USB Flash Drive USB Device		Detaily	
	ADATA USB Flash Drive USB Device		Detaily	
	ADATA USB Flash Drive USB Device		Detaily	
	ADATA USB Flash Drive USB Device		Detaily	
	ASMT 2103 USB Device		Detaily	
	Corstar Slider 3.0 USB Device		Detaily	
	Generic Flash Disk USB Device		Detaily	
	Generic Flash Disk USB Device		Detaily	
	Generic STORAGE DEVICE USB Device		Detaily	
	GS17 Innovator USB Device		Detaily	
	IT1165 USB Flash Disk USB Device		Detaily	
	IT1165 USB Flash Disk USB Device		Detaily	
	JetFlash Transcend 128GB USB Device		Detaily	
	JetFlash Transcend 16GB USB Device		Detaily	
	JetFlash Transcend 8GB USB Device		Detaily	
	Verbatim Disk Transcend 1GB USB Device		Detaily	

Upravit zóny **OK** **Storno**

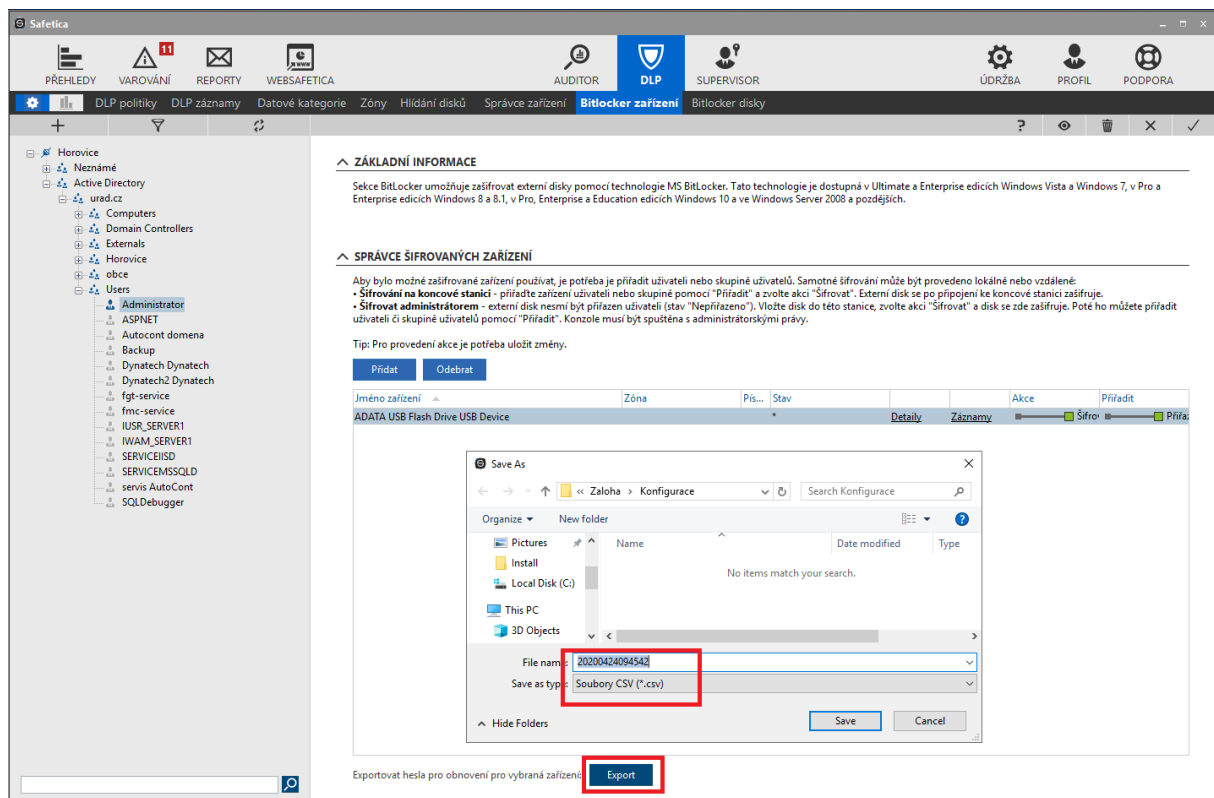
Exportovat hesla pro obnovení pro vybraná zařízení: **Export**

Po vybrání USB zařízení se nastavuje šifrování USB disku a přiřazení USB disku uživatelům, nebo počítačům, kterým bude tento USB disk transparentně přístupný po vložení do počítače.

Otevření šifrovaného USB disku vyžaduje Safetica klienta a přihlášeného uživatele nebo zvolený počítač, který je k USB disku přiřazen.



Tlačítkem „Export“ je možné zálohovat šifrovací klíče USB zařízení do CSV souboru



8.8. BITLOCKER DISKY

BitLocker Drive Encryption slouží pro fyzické šifrování systémových i nesystémových disků na počítačích pomocí nástroje Microsoft.

Safetica klient zajišťuje aktivaci šifrování BitLockerem na koncových počítačích uživatelů, volbu disků, které budou šifrovány, synchronizaci klíčů s Microsoft Active Directory a export klíčů do souboru – záloha.

Ne každý počítač ve společnosti bude šifrován, proto je doporučení NENASTAVOVAT šifrování v globální politice – na celý strom počítačů, ale specifikovat skupinu nebo konkrétní počítače, kde bude šifrování disků aktivováno.

Pohled na globální nastavení pro celou strukturu Safetica managementu zobrazuje jak politiku nastavení – nedoporučuje se měnit na „šifrovat“, tak aktuální stav jednotlivých počítačů ve správě.

Zobrazuje se, zda je počítač šifrován, jaká je podpora TPM čipu, v jakém stavu daný počítač je.

Kliknutím na odkaz „Detaily“ se zobrazí podrobné informace u zvoleného počítače.

Šifrovací politika: Dešifrovat

Dostupné možnosti pro vybranou politiku:

Systémový disk: TPM

Heslo jako alternativa: Ne

USB klíč jako alternativa: Ne

Převzít: Ne

PC	USB klíč k dis...	Heslo k dispozici	TPM k dispoz...	TPM s pinem...	Datové disky...	Cíl	Stav	Detaily	Vyjimky	Akce	Obnovení
SERVER	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Dešifrovat	Dešifrováno	Detaily	<input type="checkbox"/>	Zdědit	
WIN10		Bez GPO	-	-	Základní	Dešifrovat	Dešifrováno	Detaily	<input type="checkbox"/>	Zdědit	
FPMGMT	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Dešifrovat	Chyba	Detaily	<input type="checkbox"/>	Zdědit	<input type="checkbox"/> Opa...
Win10_1		Bez GPO	-	-	Základní	Dešifrovat	Dešifrováno	Detaily	<input type="checkbox"/>	Zdědit	
WIN101		Bez GPO	-	-	Základní	Dešifrovat	Dešifrováno	Detaily	<input type="checkbox"/>	Zdědit	
WinForcePoint		Bez GPO	-	-	Základní	Dešifrovat	Dešifrováno	Detaily	<input type="checkbox"/>	Zdědit	
CPM	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Bez Bitlockeru	Dešifrovat	Chyba	Detaily	<input type="checkbox"/>	Zdědit	<input type="checkbox"/> Opa...

ZÁLOHOVÁNÍ OBNOVOVACÍCH INFORMACÍ BITLOCKERU

Uložit informace k obnovení do Active Directory: Ne

Exportovat informace k obnovení:

8.8.1. NASTAVENÍ ŠIFROVACÍ POLITIKY POČÍTAČE

V případě aktivace šifrování disků počítače se nejprve zvolí počítač, u kterého se budou šifrovat pevné disky ve stromové struktuře Safetica management konzole

Následně se provede nastavení šifrování disků zvoleného počítače v položce „Šifrovací politika“

Je možné vybrat z následujících možností:

- **Dešifrovat** – dešifruje systémový disk a všechny datové disky.
- **Zašifrovat všechny disky** – zašifruje systémový disk pomocí zvolené metody (popsáno níže) a datový disk zašifruje pomocí náhodně vygenerovaných klíčů. Datové disky budou odemčeny automaticky po odemčení systémového disku.
- **Zašifrovat datové disky** – zašifrují se pouze datové disky.

Na základě zvolené politiky je možné upravit některou z následujících možností:

- **Systémový disk** – nastavení způsobu odemykání systémového disku:
 - **Heslo** – při startu počítače bude uživatel požádán o zadání přístupového heslo, které si nastaví při aplikování politiky.
 - **TPM** – systémový disk se při startu odemkne automaticky. Heslo je uloženo v bezpečnostním TPM čipu.
 - **TPM+Pin** – Heslo je uloženo v bezpečnostním TPM čipu chráněném pinem. Při startu počítače bude uživatel požádán o zadání pinu, který si nastaví při aplikování politiky.
- **Heslo jako alternativa** – jako další alternativní metoda odemknutí systémového disku bude nastaveno heslo. Lze nastavit pouze při zvolení odemykacích metod TPM a TPM+Pin.
- **USB klíč jako alternativa** – jako další alternativní metoda odemknutí systémového disku bude nastaven klíč uložený na USB disku.
- **Převzít** – Safetica převezme správu na disky, které byly dříve zašifrovány přímo BitLockerem bez použití Safetica. Staré přístupové údaje a obnovovací klíče budou vymazány a nahrazeny novými, které budou kompatibilní s nastavenou politikou.

^ BITLOCKER SPRÁVA

Šifrovací politika: Šifrovat všechny disky ?

Dostupné možnosti pro vybranou politiku:

Systémový disk: TPM+Pin ?

Heslo jako alternativa: Ano ?

USB klíč jako alternativa: Ano ?

Převzít: Ano ?

PC	USB klíč k dis...	Heslo k dispozici	TPM k dispoz...	TPM s pinem ...	Datové disky ...	Cíl	Stav	Detaily	Vyjímky	Akce
WIN10	-	Bez GPO	-	-	Základní	Dešifrovat	Dešifrováno	Detaily	<input type="checkbox"/>	Zdědit

Šifrovací klíče je možné synchronizovat s Microsoft Active Directory ve volbě „Uložit informace k obnovení do Active Directory“ popřípadě vyexportovat do CSV souboru.

^ ZÁLOHOVÁNÍ OBNOVOVACÍCH INFORMACÍ BITLOCKERU

Uložit informace k obnovení do Active Directory: Ne

Exportovat informace k obnovení: [Exportovat](#) ?

Stav šifrování je možné sledovat kliknutím na „Detaily“ pro zvolený počítač

WIN10

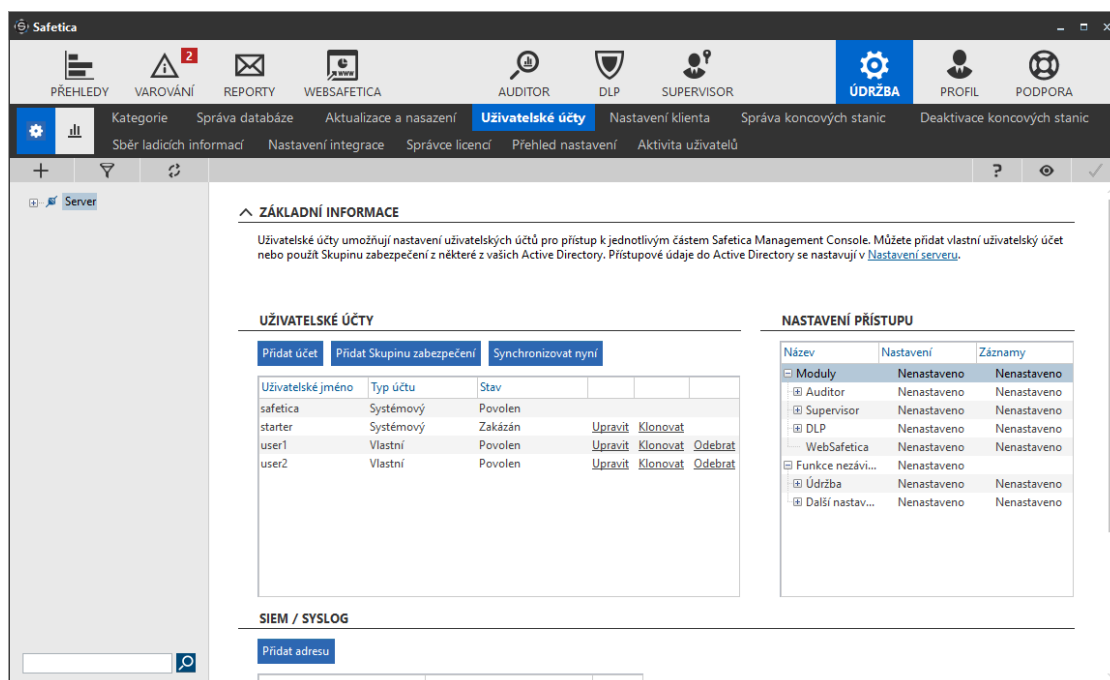
Bitlocker:	
Cíl:	Dešifrovat
Stav:	Dešifrováno
Přehled:	
Systémový disk:	C:\
Svazek:	\\?\Volume{39a85bf5-fccc-4591-8d56-006b1704baee}\
Stav:	Dešifrováno
Možnosti:	
USB klíč:	-
Heslo:	Bez GPO
TPM:	-
TPM + Pin:	-
Heslo k datovým ...	Základní
Informace o PC:	
Operační systém:	Windows 10 Enterprise 64-bit 10.0.17763
TPM čip:	Chybí
GPO nastavení:	
Systémové dí...	
USB klíč:	Ne
Heslo (Mini...	Ne (8, Ne)
TPM:	Ano
TPM + Pin (...	Ne (6, Ne)
Datové disky:	
USB klíč:	Ano
Heslo (Mini...	Ano (8, Ne)

OK

9. NASTAVENÍ SPRÁVCŮ A PŘÍSTUPOVÝCH PRÁV K MGMT KONZOLI

V rámci nastavení je možné definovat správce Safetica management konzole a jejich práva pro Správu

Definice se uživatele se nastavuje v záložce Údržba / Uživatelské účty



UŽIVATELSKÉ ÚČTY

Přidat účet | Přidat Skupinu zabezpečení | Synchronizovat nyní

Uživatelské jméno	Typ účtu	Stav			
safetica	Systémový	Povoleno			
starter	Systémový	Zakázán	Upravit	Klonovat	
user1	Vlastní	Povoleno	Upravit	Klonovat	Odebrat
user2	Vlastní	Povoleno	Upravit	Klonovat	Odebrat

NASTAVENÍ PŘÍSTUPU

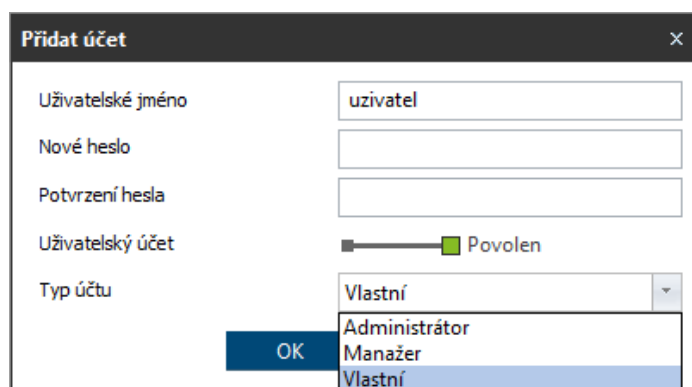
Název	Nastavení	Záznamy
Moduly	Nenastaveno	Nenastaveno
Auditor	Nenastaveno	Nenastaveno
Supervisor	Nenastaveno	Nenastaveno
DLP	Nenastaveno	Nenastaveno
WebSafetica	Nenastaveno	Nenastaveno
Funkce nezávi...	Nenastaveno	Nenastaveno
Údržba	Nenastaveno	Nenastaveno
Další nastav...	Nenastaveno	Nenastaveno

SIEM / SYSLOG

[Přidat adresu](#)

9.1. DEFINICE UŽIVATELE SAFETICA

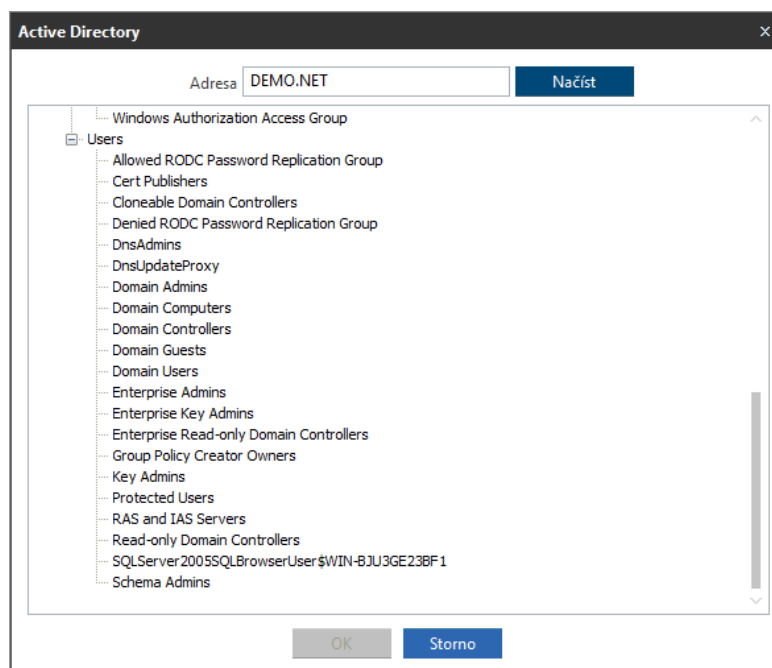
Pomocí tlačítka „Přidat uživatele“ se definuje uživatel systému Safetica



Definuje se jméno, heslo a typ účtu. Jsou přednastavené dva profily – Manažer a Administrátor. Pokud je třeba definovat konkrétní nastavení pro definovaného uživatele, je třeba zvolit typ účtu „Vlastní“

Pomocí tlačítka „Přidat skupinu zabezpečení“ je možné přidat uživatelskou skupinu z Active Directory.

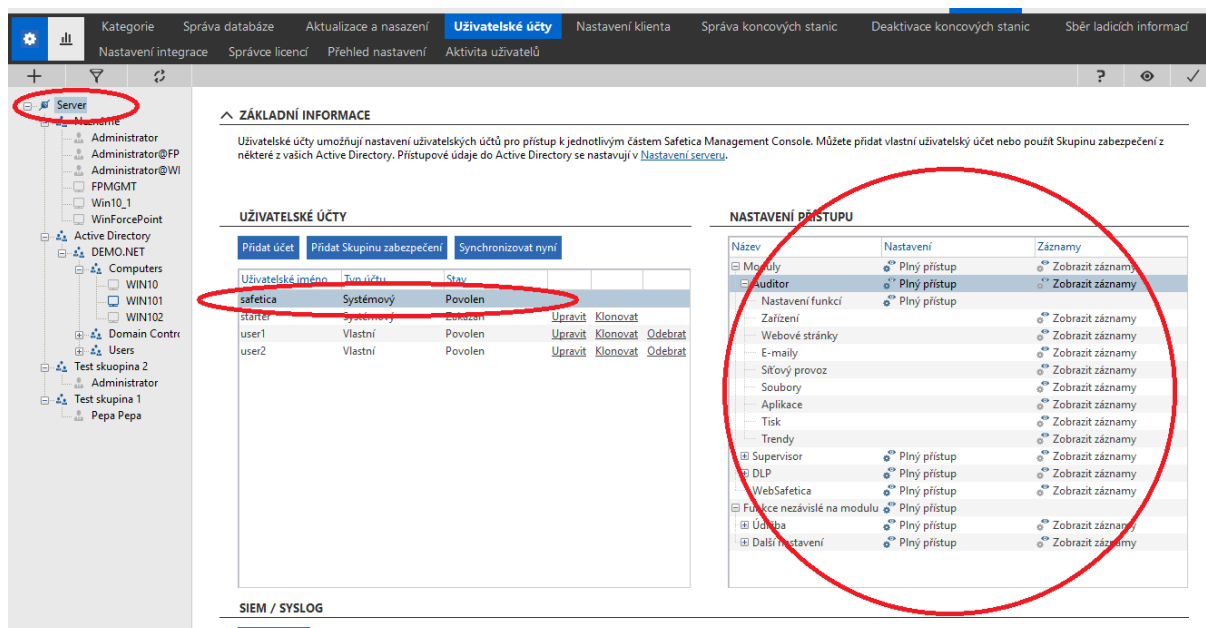
Pokud se přidá skupina z AD, všichni členové skupiny budou mít stejná práva přístupu ke správě systému Safetica.



9.2. NASTAVENÍ PRÁV UŽIVATELE

Pro nastavení práv na uživatele je nutné označit uživatele nebo skupinu, na kterých se budou práva nastavovat.

Dále ve struktuře skupin zvolit skupinu, pro kterou se budou práva nastavovat a následně je možné v tabulce „Nastavení přístupu“ definovat jednotlivá oprávnění



The screenshot displays the 'Uživatelé' (Users) section of the Safetica Management Console. The left sidebar shows a tree view of the network structure, with 'Server' and 'Active Directory' expanded. The main area is divided into two sections: 'ZÁKLADNÍ INFORMACE' (Basic Information) and 'UŽIVATELSKÉ ÚČTY' (User Accounts).

The 'UŽIVATELSKÉ ÚČTY' section contains a table of user accounts. The 'safetica' user is highlighted with a red circle. The 'NASTAVENÍ PŘÍSTUPU' (Access Settings) section contains a table of permissions for various modules and functions, also highlighted with a red circle.

Uživatel	Typ účtu	Stav	Upravit	Klonovat	Odebrat
saftetica	Systémový	Povoleno			
startel	Systémový	Zakázáno	Upravit	Klonovat	Odebrat
user1	Vlastní	Povoleno	Upravit	Klonovat	Odebrat
user2	Vlastní	Povoleno	Upravit	Klonovat	Odebrat

Název	Nastavení	Záznamy
Moduly	Plný přístup	Zobrazit záznamy
Auditor	Plný přístup	Zobrazit záznamy
Nastavení funkcí	Plný přístup	
Zařízení		Zobrazit záznamy
Webové stránky		Zobrazit záznamy
E-mail		Zobrazit záznamy
Sítový provoz		Zobrazit záznamy
Soubory		Zobrazit záznamy
Aplikace		Zobrazit záznamy
Tisk		Zobrazit záznamy
Trendy		Zobrazit záznamy
Supervisor	Plný přístup	Zobrazit záznamy
DLP	Plný přístup	Zobrazit záznamy
WebSafetica	Plný přístup	Zobrazit záznamy
Funkce nezávislé na modulu	Plný přístup	Zobrazit záznamy
Údoba	Plný přístup	Zobrazit záznamy
Další nastavení	Plný přístup	Zobrazit záznamy

9.2.1. VÝBĚR UŽIVATELE,

Výběr skupiny, kde se budou nastavovat oprávnění

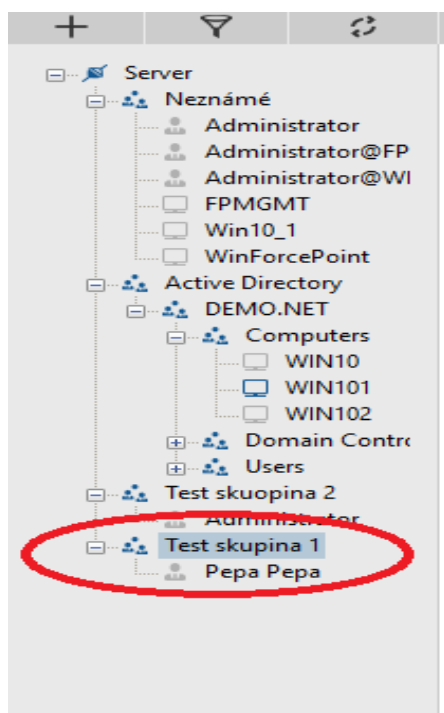
UŽIVATELSKÉ ÚČTY

Přidat účet Přidat Skupinu zabezpečení Synchronizovat nyní

Uživatelské jméno	Typ účtu	Stav			
safetica	Systémový	Povolen			
starter	Systémový	Zakázán	Upravit	Klonovat	
user1	Vlastní	Povolen	Upravit	Klonovat	Odebrat
user2	Vlastní	Povolen	Upravit	Klonovat	Odebrat

9.2.2. VÝBĚR SKUPINY

Výběr skupiny, kde se budou nastavovat oprávnění – je možné zvolit skupinu počítačů, uživatelů, nebo konkrétní počítač a uživatele.



9.2.3. NASTAVENÍ PŘÍSTUPU

Definují se jednotlivá práva přístupu k systému Safetica.

NASTAVENÍ PŘÍSTUPU

Název	Nastavení	Záznamy
[-] Moduly	⚙ Zakázat vše	📄 Zobrazit záznamy
[-] Auditor	⚙ Zakázat vše	📄 Zobrazit záznamy
..... Nastavení funkcí	⚙ Zakázat vše	
..... Zařízení		📄 Zobrazit záznamy
..... Webové stránky		📄 Zobrazit záznamy
..... E-maily		📄 Zobrazit záznamy
..... Síťový provoz		📄 Zobrazit záznamy
..... Soubory		📄 Zobrazit záznamy
..... Aplikace		📄 Zobrazit záznamy
..... Tisk		📄 Zobrazit záznamy
..... Trendy		📄 Zobrazit záznamy
[+] Supervisor	⚙ Zakázat vše	📄 Zobrazit záznamy
[+] DLP	⚙ Zakázat vše	📄 Zobrazit záznamy
..... WebSafetica	⚙ Zakázat vše	📄 Zobrazit záznamy
[-] Funkce nezávislé na modulu	⚙ Zakázat vše	
[+] Údržba	⚙ Zakázat vše	📄 Zobrazit záznamy
[+] Další nastavení	⚙ Zakázat vše	📄 Zobrazit záznamy

9.2.3.1 Položka „Název“

Seznam jednotlivých modulů Safetica systému

Moduly

- Auditor – práva na modul Auditor
- Supervisor – práva na modul Supervisor

DLP – práva na modul Supervisor

Funkce nezávislé na modulu

- Údržba
- Další nastavení

V rámci tohoto nastavení je možné definovat práva pro jednotlivé části modulů

NASTAVENÍ PŘÍSTUPU

Název	Nastavení	Záznamy
[-] Moduly	Nenastaveno	Nenastaveno
[-] Auditor	Nenastaveno	Nenastaveno
... Nastavení funkcí	Nenastaveno	
... Zařízení		Nenastaveno
... Webové stránky		Nenastaveno
... E-maily		Nenastaveno
... Síťový provoz		Nenastaveno
... Soubory		Nenastaveno
... Aplikace		Nenastaveno
... Tisk		Nenastaveno
... Trendy		Nenastaveno
[-] Supervisor	Nenastaveno	Nenastaveno
... Správa webů	Nenastaveno	Nenastaveno
... Správa aplikací	Nenastaveno	Nenastaveno
... Správa tisku	Nenastaveno	Nenastaveno
[+] DLP	Nenastaveno	Nenastaveno
... WebSafetica	Nenastaveno	Nenastaveno
[-] Funkce nezávislé na mod	Nenastaveno	
[-] Údržba	Nenastaveno	Nenastaveno

9.2.3.2 Položka „Nastavení“

Umožňuje definovat práva na nastavení systému, co bude smět uživatel nastavovat.

Je možné vybrat jednotlivé položku modulů nebo celý modul

NASTAVENÍ PŘÍSTUPU

Název	Nastavení	Záznamy
Sítový provoz		Zobrazit záznamy
Soubory		Zobrazit záznamy
Aplikace		Zobrazit záznamy
Tisk		Zobrazit záznamy
Trendy		Zobrazit záznamy
[-] Supervisor	Zakázat vše	Zobrazit záznamy
Správa webů	Zakázat vše	Zobrazit záznamy
Správa aplikací	Zakázat vše	Zobrazit záznamy
Správa tisku	Zakázat vše	Zobrazit záznamy
[-] DLP	Zakázat vše	Zobrazit záznamy
Datové kategorie	Zakázat vše	Zobrazit záznamy
DLP pravidla	Zakázat vše	
DLP protokol		Zobrazit záznamy
Zóny	Zakázat vše	
Hlídnání disků	Zakázat vše	Zobrazit záznamy
Správce zařízení	Zakázat vše	Zobrazit záznamy
Šifrované disky	Zakázat vše	
Bitlocker zařízení	Zakázat vše	
Bitlocker disky	Zakázat vše	

A následně definovat práva uživatele pro „Nastavení“

NASTAVENÍ PŘÍSTUPU

Název	Nastavení	Záznamy
Sítový provoz		Zobrazit záznamy
Soubory		Zobrazit záznamy
Aplikace		Zobrazit záznamy
Tisk		Zobrazit záznamy
Trendy		Zobrazit záznamy
[-] Supervisor	Zakázat vše	Zobrazit záznamy
Správa webů	Zakázat vše	Zobrazit záznamy
Správa aplikací	Zakázat vše	Zobrazit záznamy
Správa tisku	Zakázat vše	Zobrazit záznamy
[-] DLP	Zakázat vše	Zobrazit záznamy
Datové kategorie	Nenastaveno	Zobrazit záznamy
DLP pravidla	Zakázat vše	
DLP protokol	Zobrazit nastavení	Zobrazit záznamy
Zóny	Zakázat vše	
Hlídnání disků	Zakázat vše	Zobrazit záznamy
Správce zařízení	Zakázat vše	Zobrazit záznamy
Šifrované disky	Zakázat vše	
Bitlocker zařízení	Zakázat vše	
Bitlocker disky	Zakázat vše	

9.2.3.3 Položka „Záznamy“

Umožňuje definovat práva na logové záznamy systému, jaké logy, a grafy bude smět uživatel sledovat.

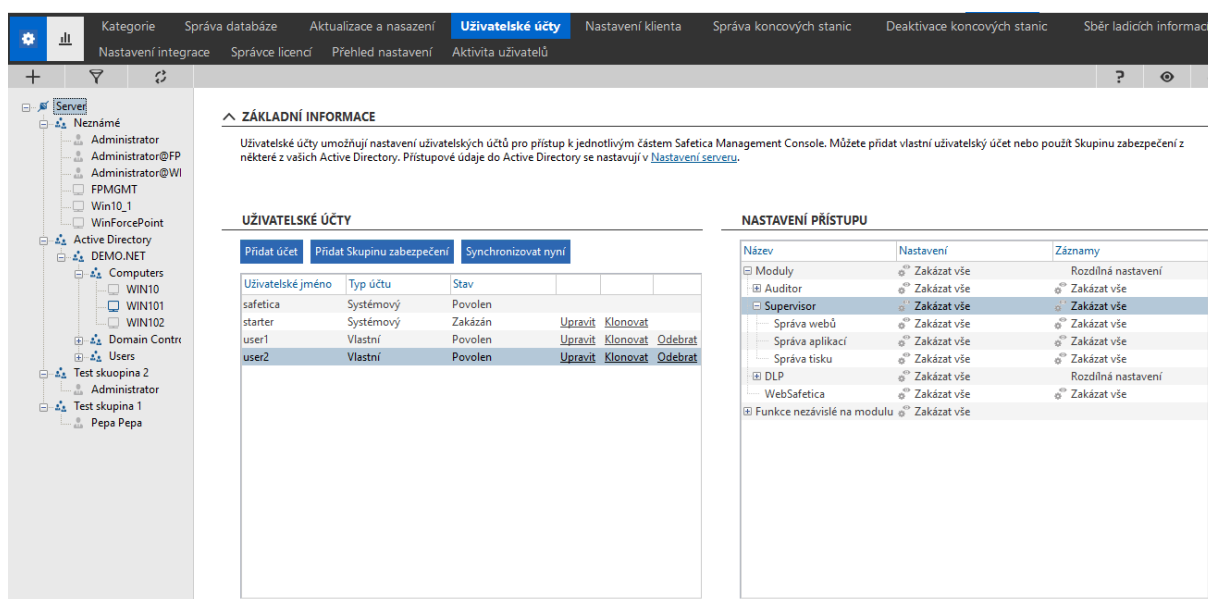
NASTAVENÍ PŘÍSTUPU

Název	Nastavení	Záznamy
..... Síťový provoz		⚙️ Zobrazit záznamy
..... Soubory		⚙️ Zobrazit záznamy
..... Aplikace		⚙️ Zobrazit záznamy
..... Tisk		⚙️ Zobrazit záznamy
..... Trendy		⚙️ Zobrazit záznamy
☑ Supervisor	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
..... Správa webů	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
..... Správa aplikací	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
Správa tisku	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
☑ DLP	⚙️ Zakázat vše	⚙️ Nenastaveno
..... Datové kategorie	⚙️ Zakázat vše	⚙️ Zakázat vše
..... DLP pravidla	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
..... DLP protokol		⚙️ Zobrazit záznamy
..... Zóny	⚙️ Zakázat vše	
..... Hlídní disků	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
..... Správce zařízení	⚙️ Zakázat vše	⚙️ Zobrazit záznamy
..... Šifrované disky	⚙️ Zakázat vše	
..... Bitlocker zařízení	⚙️ Zakázat vše	
..... Bitlocker disky	⚙️ Zakázat vše	

9.3. PŘÍKLAD NASTAVENÍ PRO UŽIVATELE USER 2

Uživatel má právo pouze na skupinu „Test skupin 1“ a to pouze na prohlížení logů

Přístup na celou společnost je zakázán



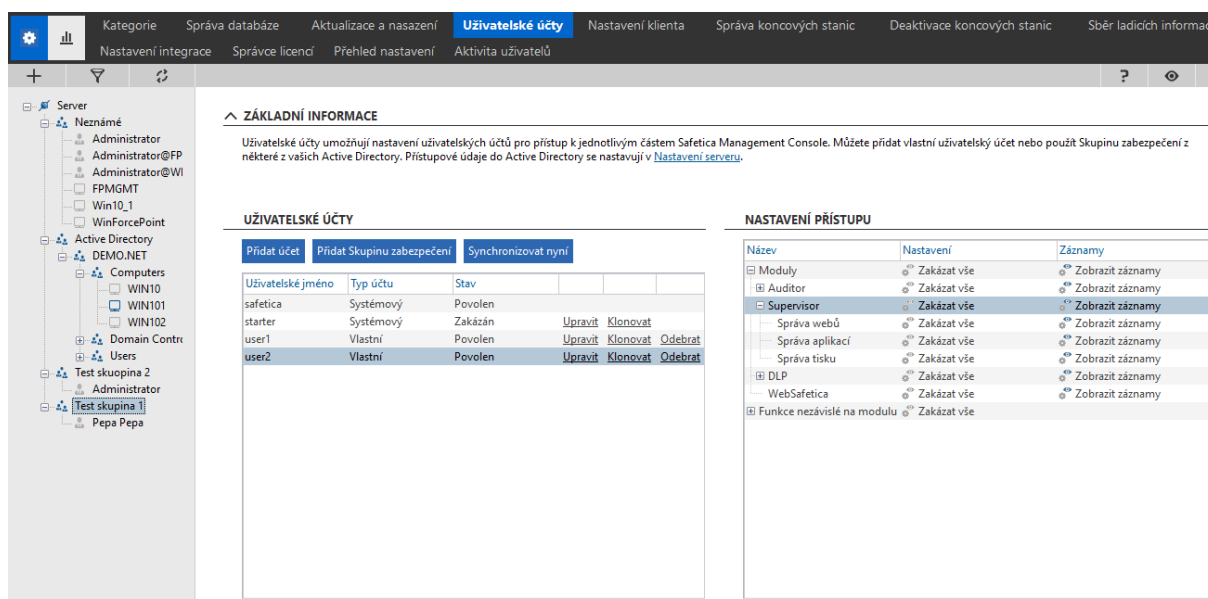
The screenshot shows the 'Uživatelé' (Users) configuration page in Safetica Management Console. The left sidebar shows a tree view of the Active Directory structure, including 'Test skupina 1' and 'Test skupina 2'. The main content area is divided into three sections:

- ZÁKLADNÍ INFORMACE**: A brief description of user accounts and a link to 'Nastavení serveru'.
- UŽIVATELSKÉ ÚČTY**: A table listing user accounts. The 'user2' account is highlighted in blue.

Uživatelé jméno	Typ účtu	Stav			
safetica	Systémový	Povoleno			
starter	Systémový	Zakázáno	Upravit	Klonovat	
user1	Vlastní	Povoleno	Upravit	Klonovat	Odebrat
user2	Vlastní	Povoleno	Upravit	Klonovat	Odebrat
- NASTAVENÍ PŘÍSTUPU**: A table showing access permissions for various modules. The 'Supervisor' module is highlighted in blue.

Název	Nastavení	Záznamy
Moduly	<input type="radio"/> Zakázat vše	<input type="radio"/> Rozdílná nastavení
Auditor	<input type="radio"/> Zakázat vše	<input type="radio"/> Zakázat vše
Supervisor	<input type="radio"/> Zakázat vše	<input type="radio"/> Zakázat vše
Správa webů	<input type="radio"/> Zakázat vše	<input type="radio"/> Zakázat vše
Správa aplikací	<input type="radio"/> Zakázat vše	<input type="radio"/> Zakázat vše
Správa tisku	<input type="radio"/> Zakázat vše	<input type="radio"/> Zakázat vše
DLP	<input type="radio"/> Zakázat vše	<input type="radio"/> Rozdílná nastavení
WebSafetica	<input type="radio"/> Zakázat vše	<input type="radio"/> Zakázat vše
Funkce nezávislé na modulu	<input type="radio"/> Zakázat vše	

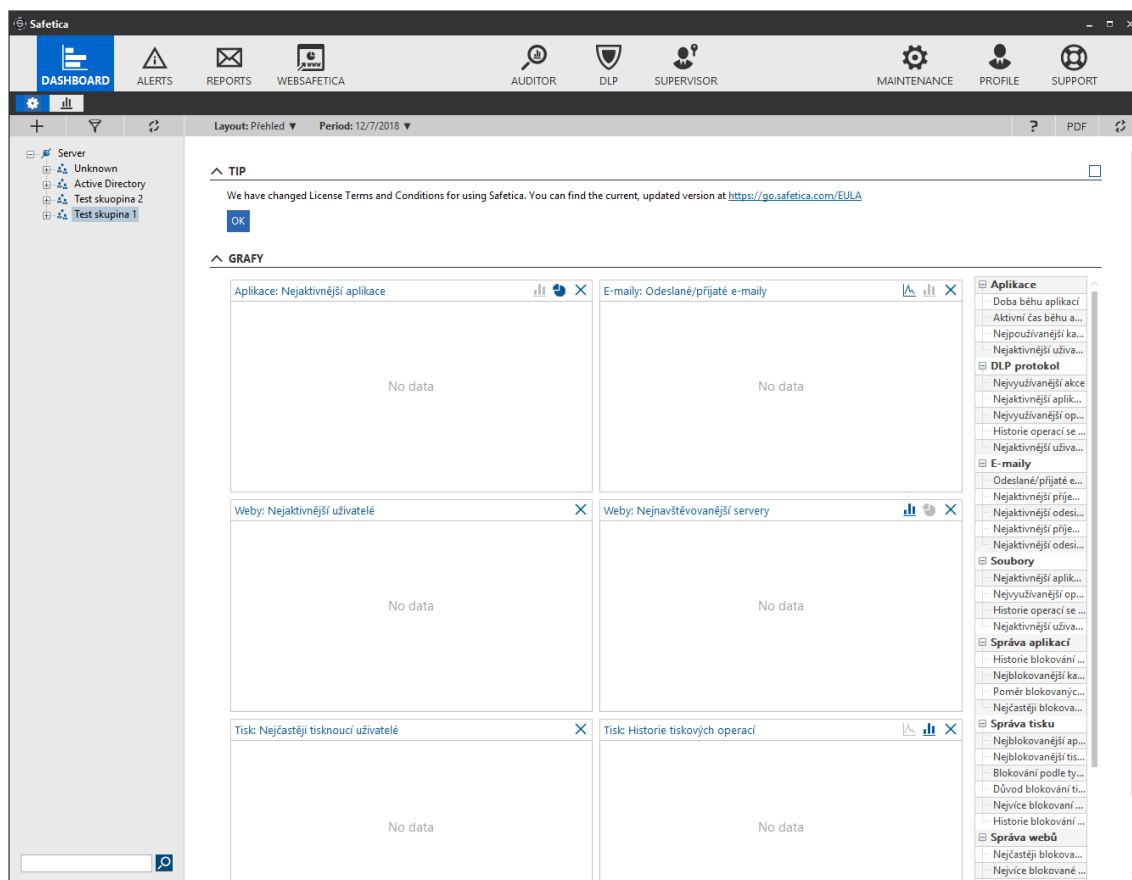
Přístup na skupinu „Test skupina 1“ je povolen pouze na zobrazení logů



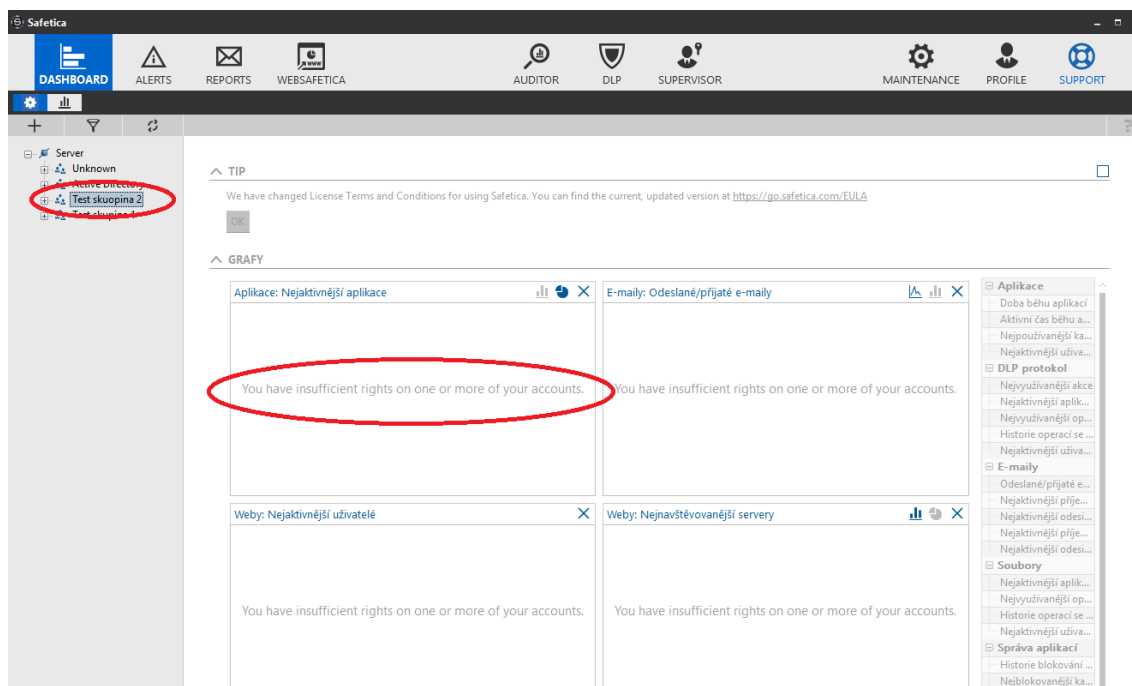
This screenshot is identical to the previous one, but with the 'Test skupina 1' group selected in the left sidebar. The 'NASTAVENÍ PŘÍSTUPU' table shows that the 'Záznamy' (Logs) column for the 'Supervisor' module is now set to 'Zobrazit záznamy' (Show logs) instead of 'Zakázat vše' (Deny all).

Název	Nastavení	Záznamy
Moduly	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
Auditor	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
Supervisor	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
Správa webů	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
Správa aplikací	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
Správa tisku	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
DLP	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
WebSafetica	<input type="radio"/> Zakázat vše	<input type="radio"/> Zobrazit záznamy
Funkce nezávislé na modulu	<input type="radio"/> Zakázat vše	

Po přihlášení uživatel vidí pouze záznamy ze skupiny „Test skupina 1“



Do ostatních skupin a celé nastavení nemá právo přístupu a možnosti nastavení

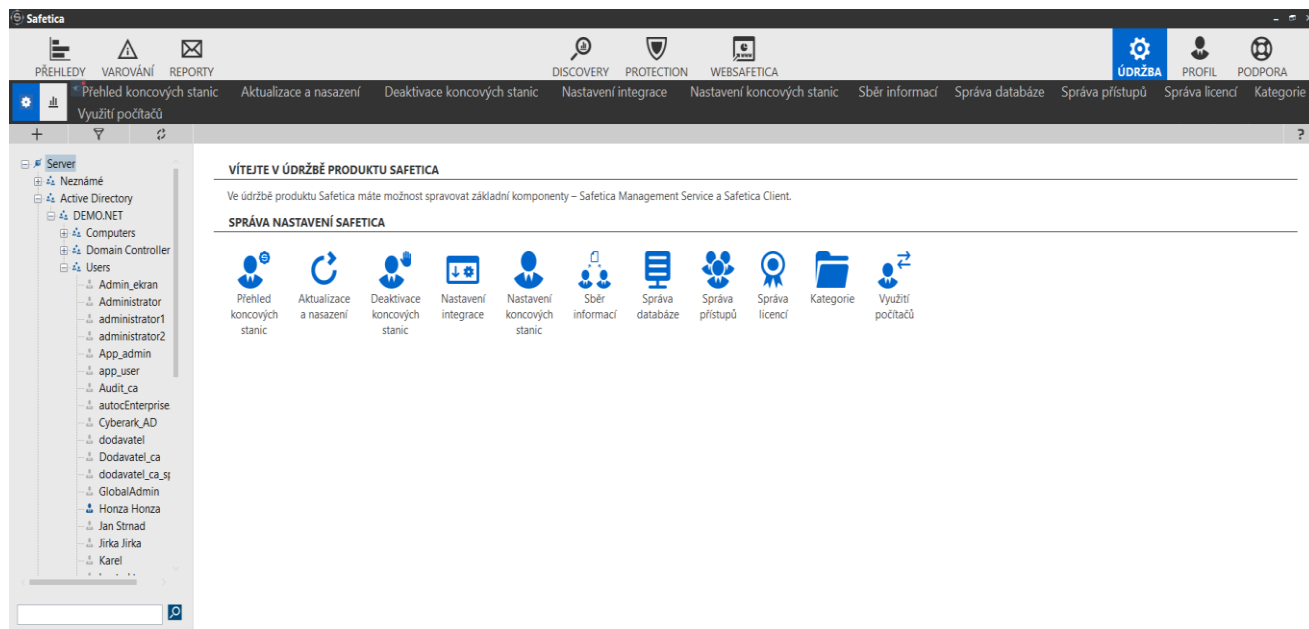


10. ÚDRŽBA

Umožňuje provádět základní nastavení management konzole. Zajišťuje instalaci, deaktivaci a správu koncových zařízení, nastavení klienta, definici kategorií pro webové servery a aplikace, správu licencí aktualizaci pod.

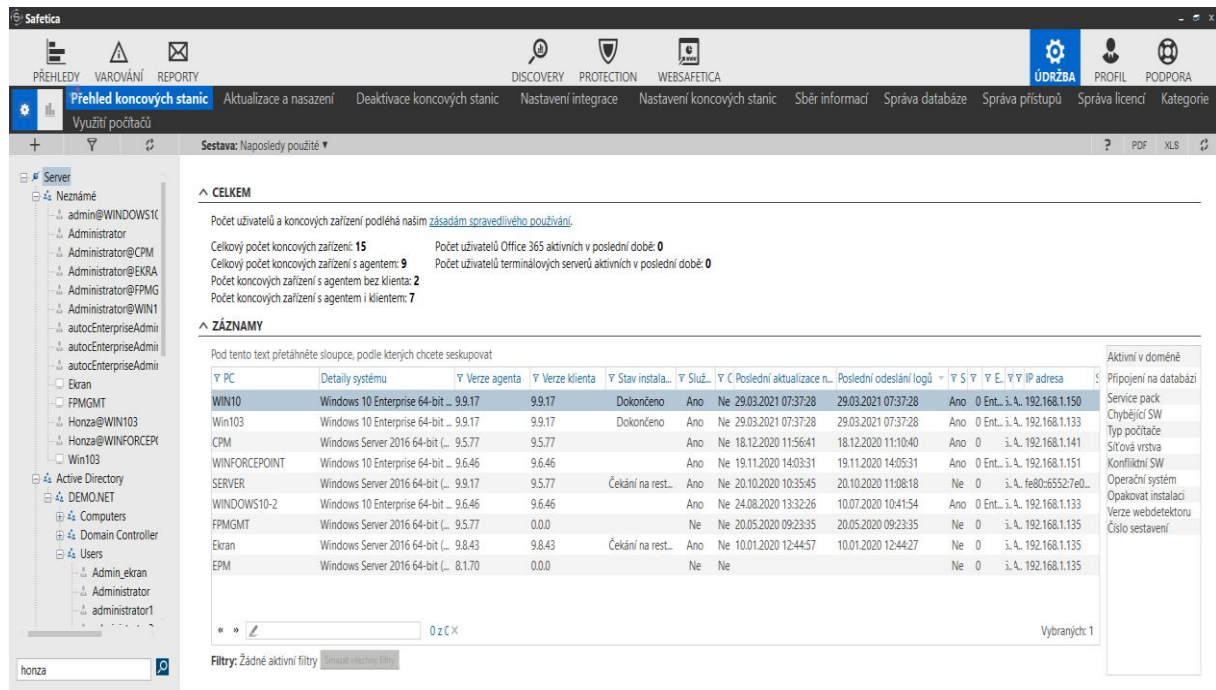
Údržba obsahuje tyto kategorie

- Přehled koncových stanic
- Aktualizace a nasazení
- Deaktivace koncových stanic
- Nastavení integrace
- Nastavení koncových stanic
- Sběr informací
- Správa databáze
- Správa přístupů
- Správce licencí
- Kategorie
- Využití počítačů



10.1. PŘEHLED KONCOVÝCH STANIC

Přehled koncových stanic zobrazuje seznam všech systémů, které jsou ve správě Safetica management konzole a v jakém stavu se nachází – instalované verze agenta a klienta apod.



CELKEM

Počet uživatelů a koncových zařízení podle našim [základním spravedlivého používání](#).

Celkový počet koncových zařízení: **15** Počet uživatelů Office 365 aktivních v poslední době: **0**
 Celkový počet koncových zařízení s agentem: **9** Počet uživatelů terminalových serverů aktivních v poslední době: **0**
 Počet koncových zařízení s agentem bez klienta: **2**
 Počet koncových zařízení s agentem i klientem: **7**

ZÁZNAMY

Pod tento text přetáhněte sloupce, podle kterých chcete seskupovat

PC	Detaily systému	Verze agenta	Verze klienta	Stav instalace	Služ.	Poslední aktualizace n.	Poslední odeslání logů	S	E	IP adresa	Aktivní v doméně
WIN10	Windows 10 Enterprise 64-bit ...	9.9.17	9.9.17	Dokončeno	Ano	Ne 29.03.2021 07:37:28	29.03.2021 07:37:28	Ano	0	Ent...i.A., 192.168.1.150	Připojení na databázi
Win103	Windows 10 Enterprise 64-bit ...	9.5.77	9.5.77		Ano	Ne 18.12.2020 11:56:41	18.12.2020 11:10:40	Ano	0	Ent...i.A., 192.168.1.133	Service pack
CPM	Windows Server 2016 64-bit ...	9.6.46	9.6.46		Ano	Ne 19.11.2020 14:03:31	19.11.2020 14:05:31	Ano	0	Ent...i.A., 192.168.1.141	Chybějící SW
WINFORCEPOINT	Windows 10 Enterprise 64-bit ...	9.6.46	9.6.46		Ano	Ne 19.11.2020 14:03:31	19.11.2020 14:05:31	Ano	0	Ent...i.A., 192.168.1.151	Typ počítače
SERVER	Windows Server 2016 64-bit ...	9.5.77	9.5.77	Čekání na rest...	Ano	Ne 20.10.2020 10:35:45	20.10.2020 11:08:18	Ne	0	i.A., fe80::65527e0...	Síťová vrstva
WINDOWS10-2	Windows 10 Enterprise 64-bit ...	9.6.46	9.6.46		Ano	Ne 24.08.2020 13:32:26	10.07.2020 10:41:54	Ano	0	Ent...i.A., 192.168.1.133	Konfliktní SW
FPMGMT	Windows Server 2016 64-bit ...	9.5.77	0.0.0		Ne	Ne 20.05.2020 09:23:35	20.05.2020 09:23:35	Ne	0	i.A., 192.168.1.135	Operační systém
Ekran	Windows Server 2016 64-bit ...	9.8.43	9.8.43	Čekání na rest...	Ano	Ne 10.01.2020 12:44:57	10.01.2020 12:44:27	Ne	0	i.A., 192.168.1.135	Opakovat instalaci
EPM	Windows Server 2016 64-bit ...	8.1.70	0.0.0		Ne	Ne		Ne	0	i.A., 192.168.1.135	Verze webdetektoru
											Číslo sestavení

0 z 15

Wybraných: 1

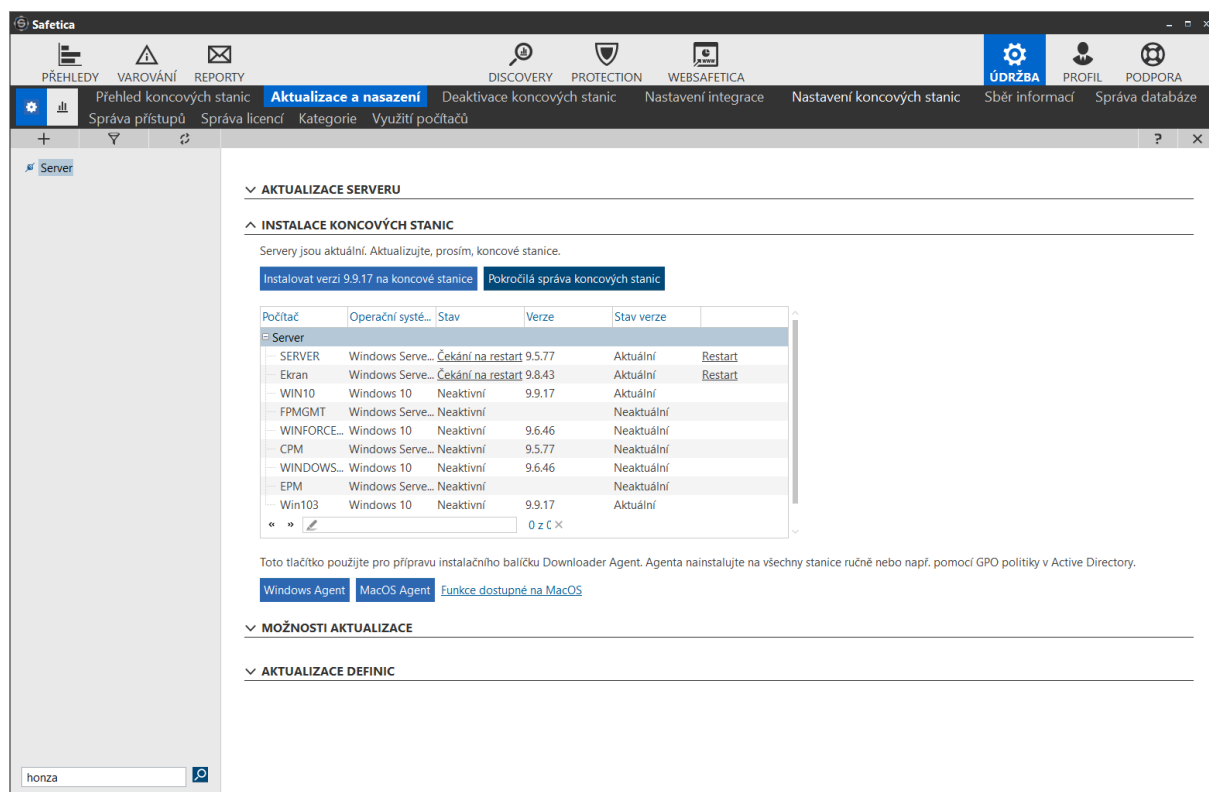
Filtery: Žádné aktivní filtry

10.2. AKTUALIZACE A NAsAZENÍ

Nastavení aktualizace systému a nasazení

Umožňuje stáhnout a nainstalovat aktualizaci management konzole nebo koncových zařízení. Zobrazuje seznam spravovaných zařízení a možnost vytvářet úlohy na instalaci Safetica agent a klienta.

Tlačítkem „Instalovat verzi xxx na koncové stanice“ je možné vytvořit globální úlohu, která umožňuje instalaci klientů a upgrade agenta a klienta na koncových zařízeních.



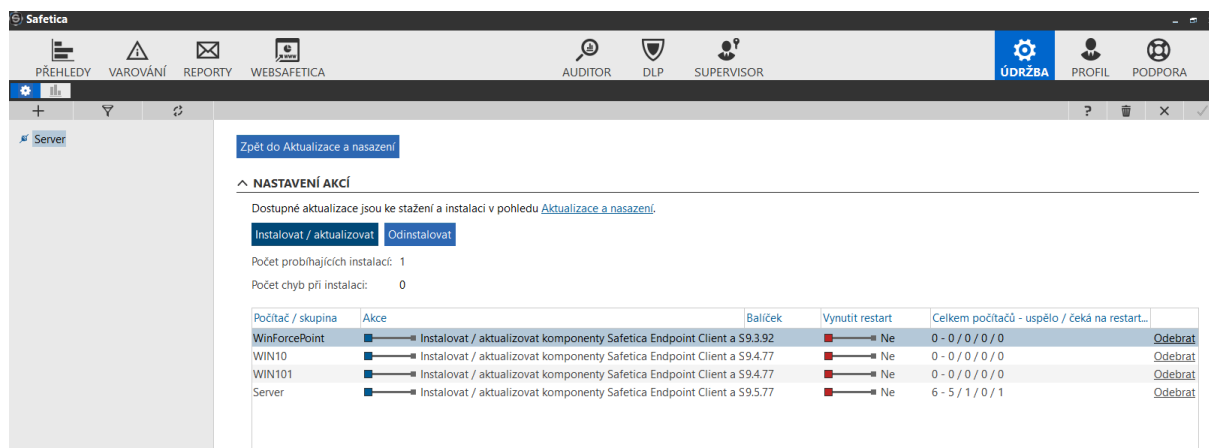
The screenshot displays the Safetica management console interface. The main content area is titled 'AKTUALIZACE KONCOVÝCH STANIC' (Update Endpoints) and contains the following information:

- Buttons: [Instalovat verzi 9.9.17 na koncové stanice](#) and [Pokročilá správa koncových stanic](#)
- Table of devices:

Počítač	Operační systé...	Stav	Verze	Stav verze	
SERVER	Windows Serve...	Čekání na restart	9.5.77	Aktuální	Restart
Ekran	Windows Serve...	Čekání na restart	9.8.43	Aktuální	Restart
WIN10	Windows 10	Neaktivní	9.9.17	Aktuální	
FPMGMT	Windows Serve...	Neaktivní		Neaktuální	
WINFORCE...	Windows 10	Neaktivní	9.6.46	Neaktuální	
CPM	Windows Serve...	Neaktivní	9.5.77	Neaktuální	
WINDOWS...	Windows 10	Neaktivní	9.6.46	Neaktuální	
EPM	Windows Serve...	Neaktivní		Neaktuální	
Win103	Windows 10	Neaktivní	9.9.17	Aktuální	

Below the table, there is a note: 'Toto tlačítko použijte pro přípravu instalačního balíčku Downloader Agent. Agentu nainstalujte na všechny stanice ručně nebo např. pomocí GPO politiky v Active Directory.' Below this note are links for [Windows Agent](#), [MacOS Agent](#), and [Funkce dostupné na MacOS](#).

Tlačítko „Pokročilá správa koncových stanic“ umožňuje definovat granulární instalaci a odinstalaci klienta nebo agenta z a na koncové stanice.

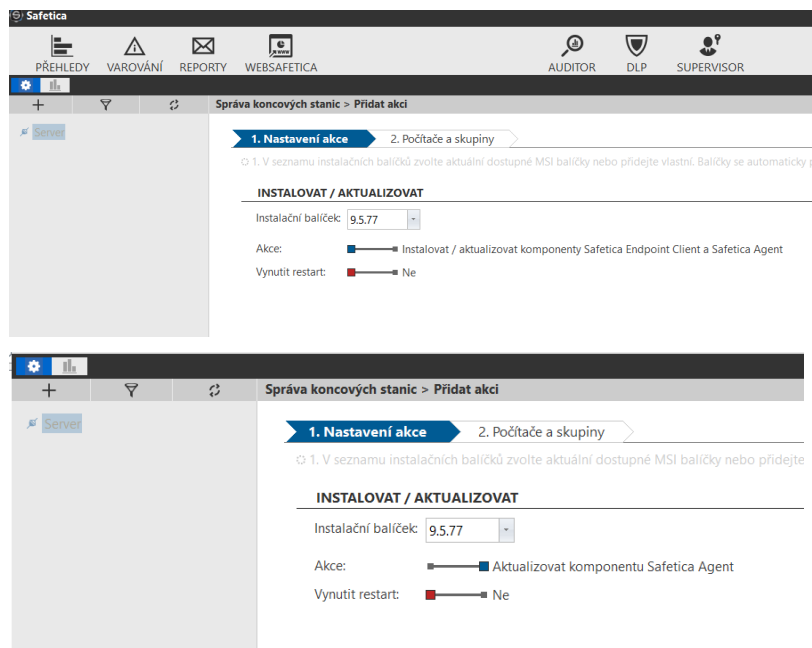


Správa koncových stanic umožňuje instalovat / upgradovat koncová zařízení, nebo odinstalovat Safetice SW z koncových stanic

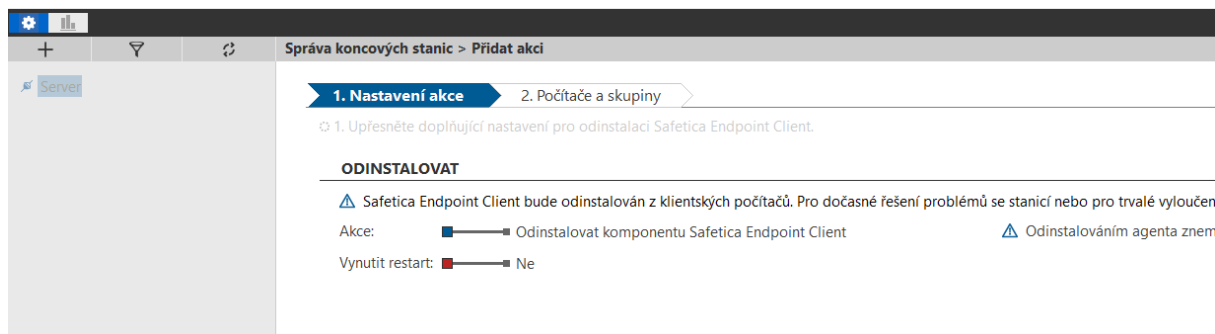
System umožňuje vytvořit úlohy:

- Instalovat nebo aktualizovat Safetice agenta a klienta
- Odinstalovat Safetice klienta a agenta

Instalace nebo aktualizace komponent Safetice – agent, klient



Odinstalace komponent Safetica – klient a agent



Součástí je i tlačítko „Windows agent“ a „MacOS agent“ – stáhne Safetica Agent, který se jako první instaluje na koncová zařízení – detail v sekci instalace Safetica agenta.

Možnosti aktualizace – umožňuje manuální aktualizaci/upgrade Safetica management konzole a agentů. Kliknutím na tlačítko „Vybrat“ je možné načíst instalační balíček a provést manuální aktualizaci všech komponent Safetica.

Aktualizace definic je nastavena na automatickou od výrobce, je možné ověřit aktuálnost verze používaných definic, popřípadě nové definice stáhnout tlačítkem „Aktualizace“

^ MOŽNOSTI AKTUALIZACE

Použít dočasnou URL: Používat Obnovit výchozí

Aktualizovat ze souboru: Vherte Safetica Universal instalátor.

^ AKTUALIZACE DEFINIC

Aktualizace definic zahrnují kategorie, nastavení integrace a detektor webových aktivit.

Verze: Definice jsou aktuální (verze 9.5.80.2)

Datum: -

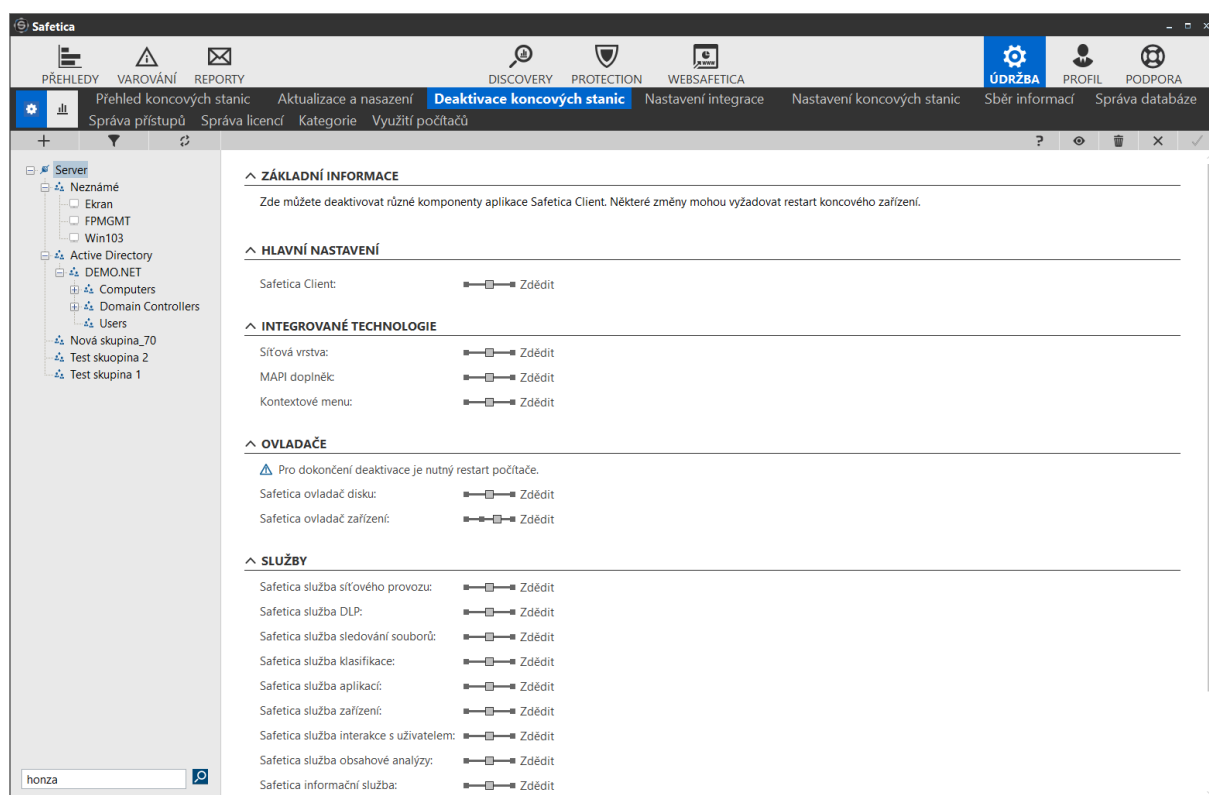
Automatická aktualizace: Zapnuto

10.3. DEAKTIVACE KONCOVÝCH STANIC

V případě problémů s během Safetica klienta, nebo nekompatibilitou, je možné využít funkce deaktivace koncových stanic.

Systém nabízí jak deaktivaci celého SW klienta Safetica, tak jeho jednotlivých modulů a ovladačů.

Tímto způsobem je velice jednoduché zjistit, zda klient Safetica nebo jeho komponenta způsobuje vzniklý problém.



Systém nabízí jak deaktivaci kompletního Safetica klienta – zastavení všech jeho funkcí, tak jeho modulů.

Deaktivace některých modulů vyžaduje restart stanice z důvodu aktivace/deaktivace ovladačů na OS.

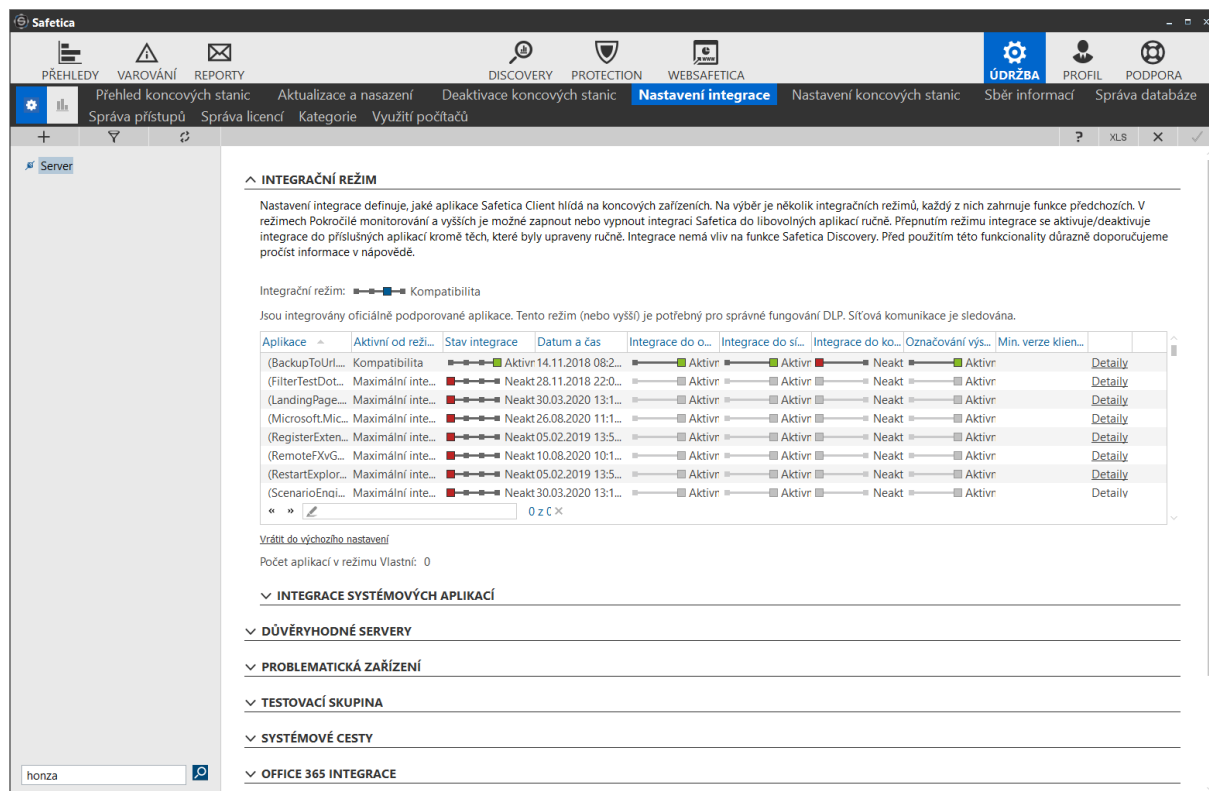
Vizualizace zobrazuje stav aktivních a deaktivovaných stanic

The screenshot shows the Safetica management console. The main window displays a summary and a table of endpoint devices. The summary indicates 15 total devices, 0 deactivated, and 3 partially deactivated. The table lists various devices including WIN10, FPMGMT, WINFORCEPOINT, SERVER, CPM, Ekran, WINDOWS10-2, EPM, and Win103, along with their operating systems and current status (Aktivováno or Částečně dea...).

PC	Detaily systému	Stav	Deaktivované části	Safetica sl...	MAP...
WIN10	Windows 10 Enterprise...	Aktivováno		Aktivováno	Aktivov...
FPMGMT	Windows Server 2016 ...	Částečně dea...	Safetica služba obsahové analýzy	Aktivováno	Aktivov...
WINFORCEPOINT	Windows 10 Enterprise...	Aktivováno		Aktivováno	Aktivov...
SERVER	Windows Server 2016 ...	Částečně dea...	Kontextové menu	Aktivováno	Aktivov...
CPM	Windows Server 2016 ...	Aktivováno		Aktivováno	Aktivov...
Ekran	Windows Server 2016 ...	Částečně dea...	Síťová vrstva, Safetica ovladač disku, Safetica ovladač zařízení	Aktivováno	Aktivov...
WINDOWS10-2	Windows 10 Enterprise...	Aktivováno		Aktivováno	Aktivov...
EPM	Windows Server 2016 ...	Aktivováno		Aktivováno	Aktivov...
Win103	Windows 10 Enterprise...	Aktivováno		Aktivováno	Aktivov...

10.4. NASTAVENÍ INTEGRACE

Nastavení integrace definuje chování Safetica klienta na koncových stanicích.



INTEGRAČNÍ REŽIM

Nastavení integrace definuje, jaké aplikace Safetica Client hledá na koncových zařízeních. Na výběr je několik integračních režimů, každý z nich zahrnuje funkce předchozích. V režimech Pokročilé monitorování a vyšších je možné zapnout nebo vypnout integraci Safetica do libovolných aplikací ručně. Přepnutím režimu integrace se aktivuje/deaktivuje integrace do příslušných aplikací kromě těch, které byly upraveny ručně. Integrace nemá vliv na funkce Safetica Discovery. Před použitím této funkcionality důrazně doporučujeme pročíst informace v nápovědě.

Integrační režim: Kompatibilita

Jsou integrovány oficiálně podporované aplikace. Tento režim (nebo vyšší) je potřebný pro správné fungování DLP. Síťová komunikace je sledována.

Aplikační	Aktivní od režimů	Stav integrace	Datum a čas	Integrace do o...	Integrace do sí...	Integrace do ko...	Označování výs...	Min. verze klien...	
(BackupToUrI...	Kompatibilita	<input checked="" type="checkbox"/>	Aktiv 14.11.2018 08:2...	<input checked="" type="checkbox"/> Aktiv	<input checked="" type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(FilterTestDot...	Maximální inte...	<input type="checkbox"/>	Neakt 28.11.2018 22:0...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(LandingPage...	Maximální inte...	<input type="checkbox"/>	Neakt 30.03.2020 13:1...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(Microsoft.Mic...	Maximální inte...	<input type="checkbox"/>	Neakt 26.08.2020 11:1...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(RegisterExten...	Maximální inte...	<input type="checkbox"/>	Neakt 05.02.2019 13:5...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(RemoteFXVG...	Maximální inte...	<input type="checkbox"/>	Neakt 10.08.2020 10:1...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(RestartExplor...	Maximální inte...	<input type="checkbox"/>	Neakt 05.02.2019 13:5...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily
(ScenarioEndi...	Maximální inte...	<input type="checkbox"/>	Neakt 30.03.2020 13:1...	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Aktiv	<input type="checkbox"/> Neakt	<input checked="" type="checkbox"/> Aktiv		Detaily

Vrátit do výchozího nastavení

Počet aplikací v režimu Vlastní: 0

INTEGRACE SYSTÉMOVÝCH APLIKACÍ
 DŮVĚRYHODNÉ SERVERY
 PROBLEMATICKÁ ZAŘÍZENÍ
 TESTOVACÍ SKUPINA
 SYSTÉMOVÉ CESTY
 OFFICE 365 INTEGRACE

10.4.1. INTEGRAČNÍ REŽIM

Na výběr je několik integračních režimů, kde každý na vyšší úrovni zahrnuje funkce předchozích režimů na nižší úrovni. Na nejnižší úrovni je režim Bez integrace a na nejvyšší je Maximální integrace. Přepnutím režimu integrace se aktivují nebo deaktivují potřebné aplikace kromě těch, které byly upraveny ručně. Integrace nemá vliv na funkce Discovery a na funkci Správa aplikací.

Přednastavené profily integrace aplikací

- Bez integrace – aplikace nejsou integrovány.
- Pokročilé monitorování – jsou integrovány aplikace, které umožňují sledovat souborové operace a získávat tak lepší výstupy pro funkci Soubory. Síťová komunikace není ovlivňována.
- Kompatibilita – jsou integrovány oficiálně podporované aplikace. Tento režim (nebo vyšší) je potřebný pro správné fungování DLP. Síťová komunikace je sledována.

- Maximální integrace – jsou integrovány všechny aplikace kromě známých nekompatibilních aplikací, jako jsou například antiviry. Tento režim může mít zásadní vliv na funkčnost pracovního prostředí. Síťová komunikace je sledována.

Doporučení: zachovat defaultní nastavení Kompatibilita. V případě potřeby manuálně integrovat aplikaci, která má být DLP systémem sledována

10.4.2. INTEGRACE APLIKACÍ

Seznam všech spuštěných aplikací na koncových systémech a jejich integrace se Safetica klientem.

Vytváří se dynamicky, tak jak se aplikace spouští na klientských počítačích a Safetica klient je eviduje do seznamu.

Integrací se rozumí vřazení Safetica klienta do komunikace jednotlivých aplikací.

Safetica klient se chová jako „man in middle“, vstupuje do komunikace aplikace. Je možné integrovat klienta i do šifrované SSL/TLS komunikace pro webové prohlížeče a emailové klienty.

Integrace pro běžně používané aplikace je nastavena výrobcem, pro ostatní aplikace je možné integraci nastavit manuálně.

^ ZÁKLADNÍ INFORMACE

Nastavení integrace definuje chování Safetica Endpoint Client na koncových stanicích. Na výběr je několik integračních režimů, každý z nich zahrnuje funkce předchozích. V režimech Správní a vyšší je možné zapnout nebo vypnout libovolné aplikace ručně. Přepnutím režimu integrace se aktivují/deaktivují potřebné aplikace kromě těch, které byly upraveny ručně. Integrace nemá vliv na funkce Safetica Auditor a na funkci Správa aplikací v Safetica Supervisor. Před použitím této funkce důrazně doporučujeme pročíst informace v nápovědě.

INTEGRAČNÍ REŽIM


































































Integrační režim: Kompatibilita

Jsou integrovány oficiálně podporované aplikace. Tento režim (nebo vyšší) je potřebný pro správné fungování DLP. Síťová komunikace je sledována.

Počet aplikací v režimu Vlastní: 0

^ INTEGRACE APLIKACÍ

Vrátit do výchozího nastavení

Aplikace	Aktivní od režimu	Stav integrace	Datum a čas	Integrace do opera...	Integrace do síťov...	Integrace do komu...	Označování výstup...	Min. verze klienta	
(BackupToUrl.exe)	Kompatibilita	 Aktivní	14.11.2018 08:23:30	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
(FilterTestDotNet...	Maximální integrace	 Neaktivní	28.11.2018 22:00:16	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
7-Zip Standalone C...	Maximální integrace	 Neaktivní	28.11.2018 22:00:16	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Acquire License Fr...	Maximální integrace	 Neaktivní	18.09.2018 10:38:58	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
AcroTextExtractor (...)	Maximální integrace	 Neaktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
ADeLRCP Dynamic ...	Maximální integrace	 Neaktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Adobe Acrobat Rea...	Kompatibilita	 Aktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Aktivní	 Aktivní		Detaily
Adobe Acrobat Rea...	Maximální integrace	 Neaktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Adobe Acrobat Spe...	Maximální integrace	 Neaktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Adobe Acrobat Up...	Maximální integrace	 Neaktivní	17.07.2018 14:22:36	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Adobe AIR Redistri...	Maximální integrace	 Neaktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Adobe Collaborati...	Maximální integrace	 Neaktivní	18.07.2018 12:49:11	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily
Adobe Collaborati...	Maximální integrace	 Neaktivní	28.11.2018 22:00:16	 Aktivní	 Aktivní	 Neaktivní	 Aktivní		Detaily

^ INTEGRACE SYSTÉMOVÝCH APLIKACÍ

Integraci aplikací je často nutné použít pro aplikace, která nejsou defaultně od výrobce nastaveny. **Vždy je nutné nově integrovanou aplikaci otestovat.**

10.4.3. DŮVĚRYHODNÉ SERVERY

V případě, že je Safetica klient integrován do webové komunikace a je sledován SSL/TLS provoz, může nastat problém s připojením na webové servery, které vyžadují klientský certifikát nebo jiný způsob ověření spojený přímo s prohlížečem uživatele. Důvodem je fakt, že Safetica klient vstupuje jako „man in middle“ do této komunikace, přerušuje přímou komunikaci klienta a webového serveru a využívá svůj self signed certifikát.

Pro tyto případy je nutné tyto servery – bankovní servery, servery státní správy apod. definovat do seznamu důvěryhodných serverů.

Zápis těchto serverů je na základě domény, bez zpětných lomítek a dalších zástupných znaků.

^ DŮVĚRYHODNÉ SERVERY

Zabezpečení integrace do SSL/TLS komunikace můžete zvýšit tím, že v pohledu [Nastavení serveru](#) vložíte vlastní kořenový certifikát pro generování důvěryhodných certifikátů.

Můžete nastavit webové domény, pro které neproběhne integrace do SSL/TLS komunikace (např. *.office.com, *.facebook.com, maps.google.com) nebo můžete zvolit IP adresy, které budou z hlídání na síti zcela vyjmuty. IP adresy je možné zadávat jednotlivě (např. 192.168.10.10) nebo jako rozsah v CIDR formátu (např. 192.168.0.0/24).

Pro hromadné přidání adres použijte tlačítko Import. Vybraný soubor musí obsahovat na každém řádku jednu adresu ve formátu uvedeném výše.

Přidat adresu	Import
Adresa	
czechpoint.cz	Odebrat
10.1.1.2	Odebrat
« »	0 z C X

10.4.4. PROBLEMATICKÁ ZAŘÍZENÍ

Seznam USB zařízení, které způsobují nekompatibilitu se Safetica klientem.

Pokud se vyskytne problém s připojením USB zařízení, je možné ho vyjmout z kontroly Safetica klientem zařazením do tohoto seznamu.

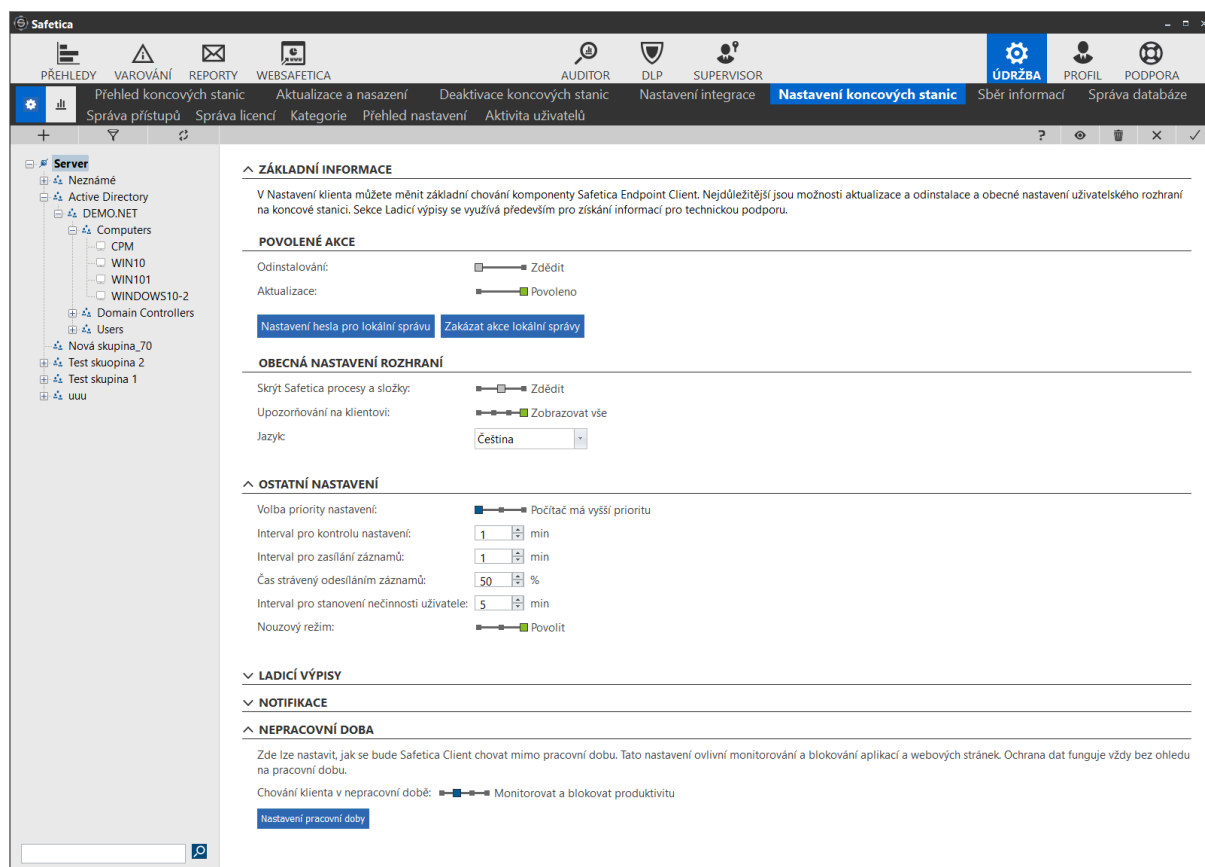
Příkladem mohou být čtečky karet.

10.5. NASTAVENÍ KONCOVÝCH STANIC

Definice nastavení Safetica klienta – povolené akce na klientovi, komunikace klienta, obecná nastavení

Doporučené nastavení klienta:

- **Odinstalace** – Zdědit – nedovolí odinstalovat klienta
- **Aktualizace** – Povolené – umožňuje aktualizovat klienta na nové verze
- **Skrýt Safetica procesy a služby** – Zdědit – procesy a služby budou uživateli skryty
- **Upozorňování na klientovi** – Povolené – uživateli se budou zobrazovat notifikace o blokaci nebo potvrzení akce v DLP politice
- **Volba priority nastavení** – počítač/uživatel – uplatní se přednostně politika zvoleného nastavení



Safetica

PŘEHLEDY VAROVÁNÍ REPORTY WEBSAFETICA AUDITOR DLP SUPERVISOR ÚDRŽBA PROFIL PODPORA

Přehled koncových stanic Aktualizace a nasazení Deaktivace koncových stanic Nastavení integrace **Nastavení koncových stanic** Sběr informací Správa databáze

Správa přístupů Správa licencí Kategorie Přehled nastavení Aktivita uživatelů

Server

- Neznámé
- Active Directory
- DEMONET
- Computers
 - CPM
 - WIN10
 - WIN101
 - WINDOWS10-2
- Domain Controllers
- Users
- Nová skupina_70
- Test skupina 2
- Test skupina 1
- uuu

^ ZÁKLADNÍ INFORMACE

V Nastavení klienta můžete měnit základní chování komponenty Safetica Endpoint Client. Nejdůležitější jsou možnosti aktualizace a odinstalace a obecné nastavení uživatelského rozhraní na koncové stanicích. Sekce Ladicí výpisy se využívá především pro získání informací pro technickou podporu.

POVOLENÉ AKCE

Odinstalování: Zdědit

Aktualizace: Povoleno

[Nastavení hesla pro lokální správu](#) [Zakázat akce lokální správy](#)

OBEČNÁ NASTAVENÍ ROZHRAŇÍ

Skrýt Safetica procesy a složky: Zdědit

Upozorňování na klientovi: Zobrazovat vše

Jazyk:

^ OSTATNÍ NASTAVENÍ

Volba priority nastavení: Počítač má vyšší prioritu

Interval pro kontrolu nastavení: min

Interval pro zaslání záznamů: min

Čas strávený odesláním záznamů: %

Interval pro stanovení nečinnosti uživatele: min

Nouzový režim: Povolit

^ LADICÍ VÝPISY

^ NOTIFIKACE

^ NEPRACOVNÍ DOBA

Zde lze nastavit, jak se bude Safetica Client chovat mimo pracovní dobu. Tato nastavení ovlivní monitorování a blokování aplikací a webových stránek. Ochrana dat funguje vždy bez ohledu na pracovní dobu.

Chování klienta v nepracovní době: Monitorovat a blokovat produktivitu

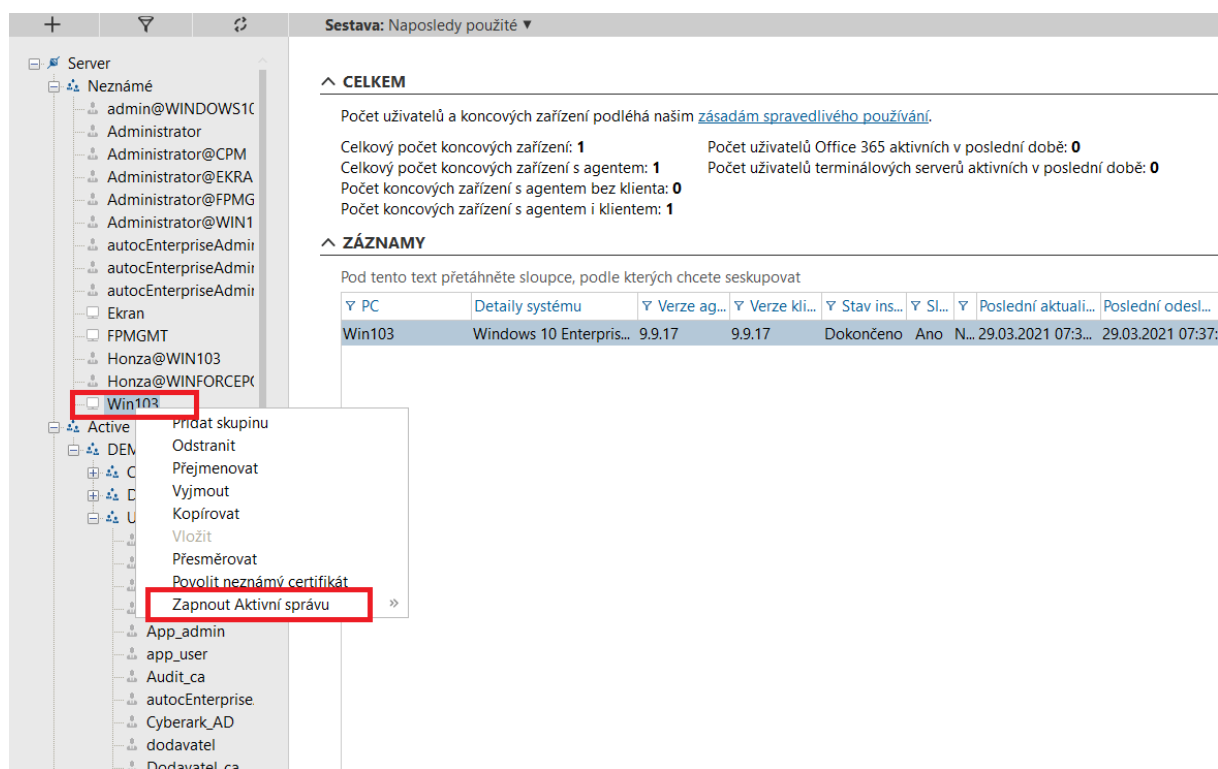
[Nastavení pracovní doby](#)

10.6. SBĚR INFORMACÍ

V případě problémů s během nebo funkčností Safetica klienta je možné vygenerovat ladící výpis, který je možné následně přiložit servisnímu tiketu na společnost Safetica.

Spuštění sběru informací z koncové stanice je možné v jaémkoliv nastavení, kde je k dipozici strom spravovaných systémů – například v Přehledu koncových stanic.

V kontextovém menu pro každou spravovanou stanici nebo server je k dispozici několik voleb, přičemž poslední volba je „Zapnout aktivní správu“



The screenshot shows the Safetica interface with a tree view on the left and a summary table on the right. The tree view shows a hierarchy of servers, with 'Win103' selected. A context menu is open over 'Win103', showing options like 'Přidat skupinu', 'Odstranit', 'Přejmenovat', 'Vymout', 'Kopírovat', 'Vložit', 'Přesměrovat', 'Povolit neznámý certifikát', and 'Zapnout Aktivní správu'. The 'Zapnout Aktivní správu' option is highlighted with a red box. The summary table on the right shows the following data:

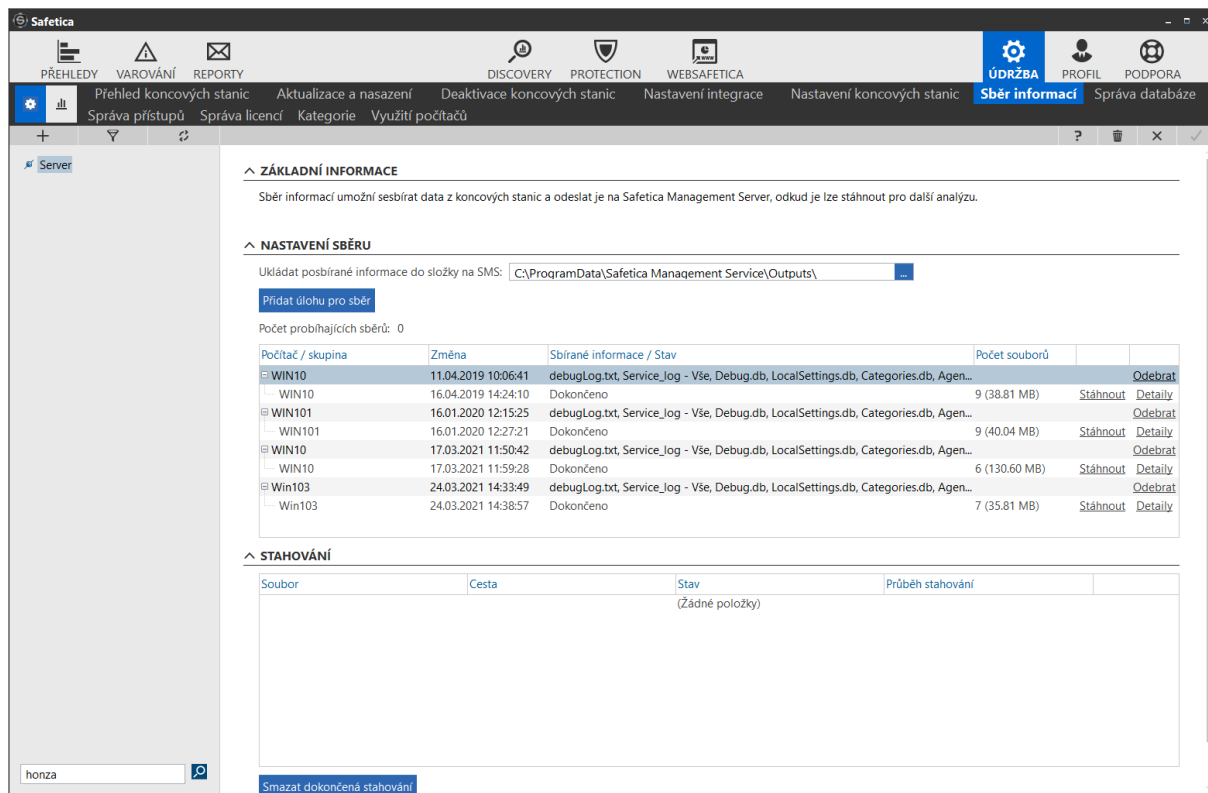
PC	Detaily systému	Verze ag...	Verze kli...	Stav ins...	SI...	Poslední aktuali...	Poslední odesl...
Win103	Windows 10 Enterpris...	9.9.17	9.9.17	Dokončeno	Ano	N... 29.03.2021 07:3...	29.03.2021 07:37:

Zapnutím aktivní správy dojde na pracovní stanici k zapnutí detailního logování.

Je možné v této fázi simulovat problém a veškeré informace s zaznamenají do logu.

Aktivní logování je možné opět v kontextovém menu následně vypnout.

Veškeré logové informace jsou následně na pracovní stanici shromážděny a zaslány na management konzoli, odkud je možné tyto informace stáhnout a odeslat výrobci na hloubkovou analýzu.



The screenshot displays the Safetica Management Server web interface. The top navigation bar includes sections for 'PŘEHLEDY', 'VAROVÁNÍ', 'REPORTY', 'DISCOVERY', 'PROTECTION', and 'WEBSAFETICA'. The main menu contains 'Přehled koncových stanic', 'Aktualizace a nasazení', 'Deaktivace koncových stanic', 'Nastavení integrace', 'Nastavení koncových stanic', 'Sběr informací', and 'Správa databáze'. The 'Sběr informací' section is active, showing 'ZÁKLADNÍ INFORMACE' and 'NASTAVENÍ SBĚRU'. The 'NASTAVENÍ SBĚRU' section includes a text input for the SMS path: 'C:\ProgramData\Safetica Management Service\Outputs\'. Below this, a table lists collected logs with columns for 'Počítač / skupina', 'Změna', 'Sbírané informace / Stav', and 'Počet souborů'. The table contains seven rows of log entries with 'Odebrat' and 'Stáhnout' links. At the bottom, there is a 'STAHOVÁNÍ' section with a table for download progress, currently showing '(Žádné položky)'. A search bar with the text 'honza' is visible in the bottom left corner.

Server

^ ZÁKLADNÍ INFORMACE
Sběr informací umožní sesbírat data z koncových stanic a odeslat je na Safetica Management Server, odkud je lze stáhnout pro další analýzu.

^ NASTAVENÍ SBĚRU
Ukládat posbírané informace do složky na SMS:
[Přidat úlohu pro sběr](#)
Počet probíhajících sběrů: 0

Počítač / skupina	Změna	Sbírané informace / Stav	Počet souborů	
WIN10	11.04.2019 10:06:41	debugLog.txt, Service_log - Vše, Debug.db, LocalSettings.db, Categories.db, Agen...		Odebrat
WIN10	16.04.2019 14:24:10	Dokončeno	9 (38.81 MB)	Stáhnout Detaily
WIN101	16.01.2020 12:15:25	debugLog.txt, Service_log - Vše, Debug.db, LocalSettings.db, Categories.db, Agen...		Odebrat
WIN101	16.01.2020 12:27:21	Dokončeno	9 (40.04 MB)	Stáhnout Detaily
WIN10	17.03.2021 11:50:42	debugLog.txt, Service_log - Vše, Debug.db, LocalSettings.db, Categories.db, Agen...		Odebrat
WIN10	17.03.2021 11:59:28	Dokončeno	6 (130.60 MB)	Stáhnout Detaily
Win103	24.03.2021 14:33:49	debugLog.txt, Service_log - Vše, Debug.db, LocalSettings.db, Categories.db, Agen...		Odebrat
Win103	24.03.2021 14:38:57	Dokončeno	7 (35.81 MB)	Stáhnout Detaily

^ STAHOVÁNÍ

Soubor	Cesta	Stav	Průběh stahování
(Žádné položky)			

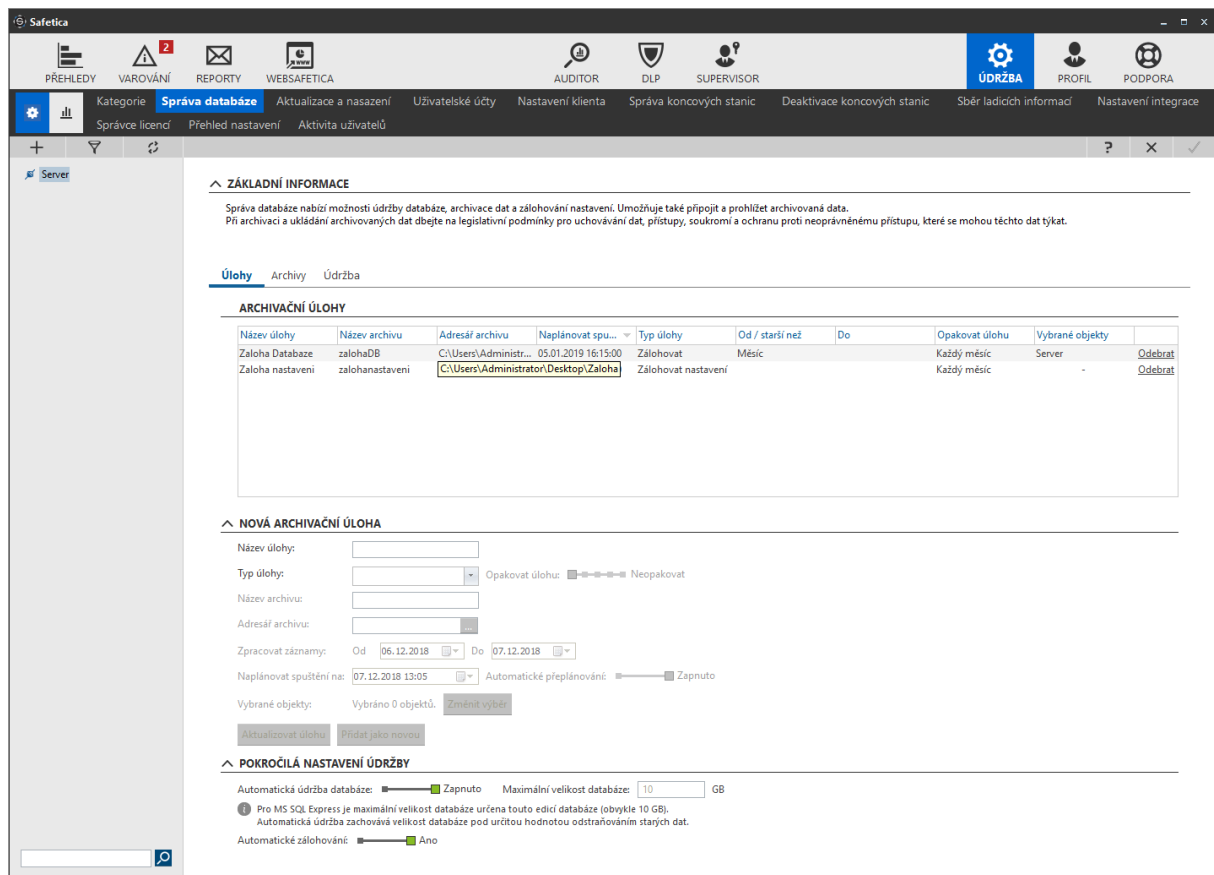
honza

[Smazat dokončená stahování](#)

10.7. SPRÁVA DATABÁZE

Správa databáze umožňuje definovat úlohy pro

- Zálohu databáze
- Odstranění dat z databáze
- Zálohu konfigurace



ZÁKLADNÍ INFORMACE

Správa databáze nabízí možnosti údržby databáze, archivace dat a zálohování nastavení. Umožňuje také připojit a prohlížet archivovaná data. Při archivaci a ukládání archivovaných dat dbejte na legislativní podmínky pro uchování dat, přístupy, soukromí a ochranu proti neoprávněnému přístupu, které se mohou těchto dat týkat.

Úlohy Archivy Údržba

ARCHIVAČNÍ ÚLOHY

Název úlohy	Název archivu	Adresář archivu	Naplánovat spu...	Typ úlohy	Od / starší než	Do	Opakovat úlohu	Vybrané objekty	
Zaloha Databáze	zalohaDB	C:\Users\Administr...	05.01.2019 16:15:00	Zálohovat	Měsíc		Každý měsíc	Server	Odebrat
Zaloha nastavení	zalohanastaveni	C:\Users\Administrator\Desktop\Zaloha		Zálohovat nastavení			Každý měsíc	-	Odebrat

NOVÁ ARCHIVAČNÍ ÚLOHA

Název úlohy:

Typ úlohy: Opakovat úlohu: Neopakovat

Název archivu:

Adresář archivu:

Zpracovat záznamy: Od Do

Naplánovat spuštění na: Automatické přepínání: Zapnuto

Vybrané objekty: Vybráno 0 objektů.

POKROČILÁ NASTAVENÍ ÚDRŽBY

Automatická údržba databáze: Zapnuto Maximální velikost databáze: GB

Pro MS SQL Express je maximální velikost databáze určena touto edicí databáze (obvykle 10 GB).
Automatická údržba zachovává velikost databáze pod určitou hodnotou odstraňováním starých dat.

Automatické zálohování: Ano

Dále je možné definovat archivaci databáze a její údržbu

10.8. SPRÁVA PŘÍSTUPŮ

Umožňuje definovat uživatele Safetica management konzole.

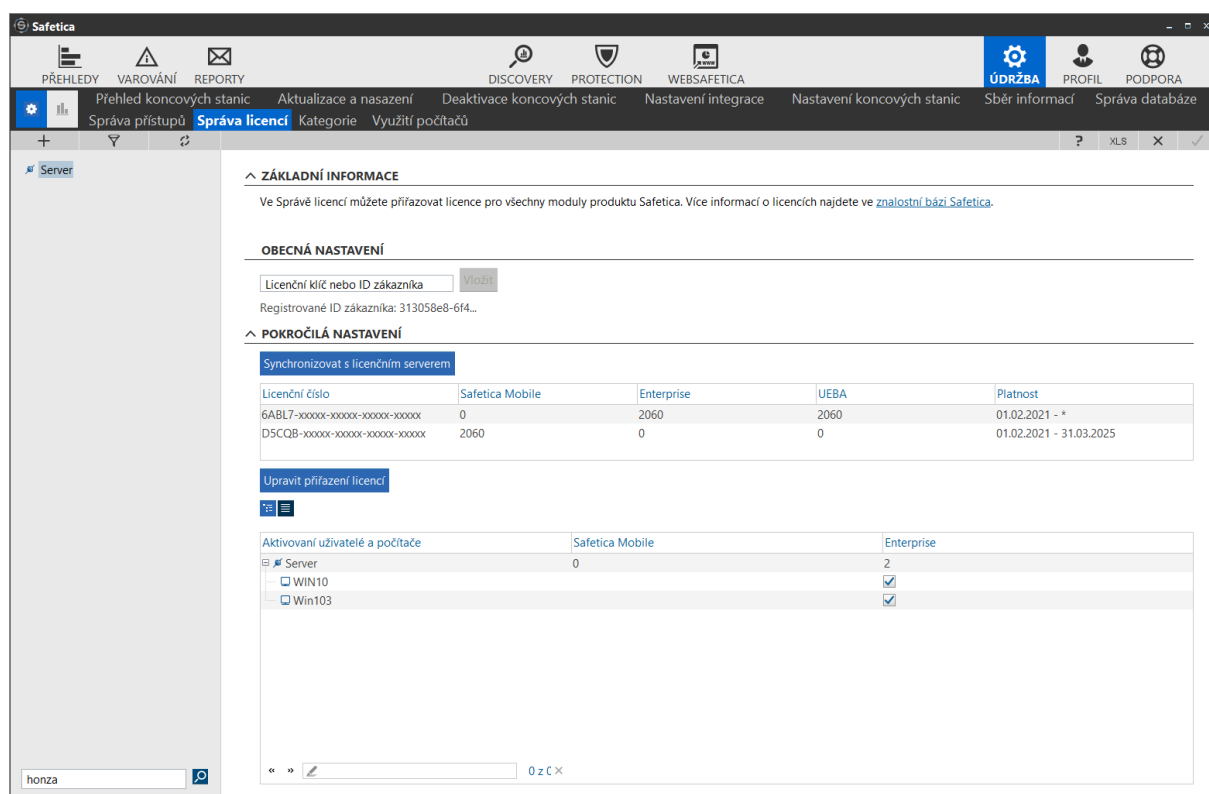
Detailní nastavení je v kapitole 8

10.9. SPRÁVA LICENCÍ

Umožňuje spravovat zakoupené licence.

Licence jsou plovoucí, přidělují se uživateli při přihlášení Safetica agenta k management konzoli a ruší se o půlnoci.

V přehledu licencí je zobrazen seznam všech aktuálních aktivních klientů za poslední den.



ZÁKLADNÍ INFORMACE

Ve Správě licencí můžete přiřazovat licence pro všechny moduly produktu Safetica. Více informací o licencích najdete ve [znalostní bázi Safetica](#).

OBEČNÁ NASTAVENÍ

Licenční klíč nebo ID zákazníka

Registrované ID zákazníka: 313058e8-6f4...

POKROČILÁ NASTAVENÍ

Licenční číslo	Safetica Mobile	Enterprise	UEBA	Platnost
6ABL7-xxxxx-xxxxx-xxxxx-xxxxx	0	2060	2060	01.02.2021 - *
D5CQB-xxxxx-xxxxx-xxxxx-xxxxx	2060	0	0	01.02.2021 - 31.03.2025

Aktivování uživatelé a počítače	Safetica Mobile	Enterprise
Server	0	2
<input type="checkbox"/> WIN10		<input checked="" type="checkbox"/>
<input type="checkbox"/> Win103		<input checked="" type="checkbox"/>

honza

10.10. KATEGORIE

Umožňuje definovat kategorie aplikací webových serverů, aplikací a přípon, které se následně využívají v definicích Supervisoru a DLP

10.10.1. KATEGORIE APLIKACÍ

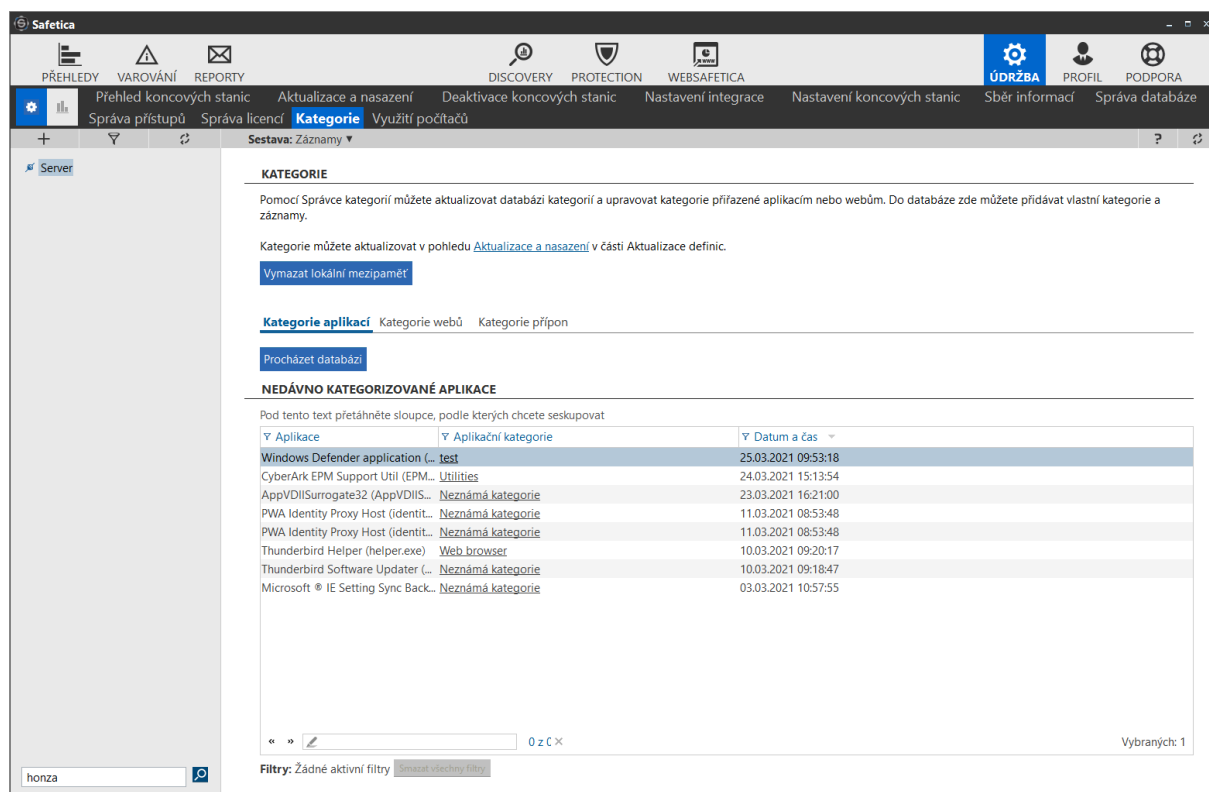
Zobrazuje seznam aplikací a jejich kategorizaci.

V seznamu jsou zobrazeny všechny aplikace, které byly uživateli spuštěny na všech počítačích s instalovaným Safetica klientem.

Pokud je aplikace kategorizována výrobcem Safetica, bude zobrazena její kategorie. Pokud se jedná o Safetice neznámou aplikaci, bude označena jako „neznámá kategorie“

Každou neznámou aplikaci je možné manuálně kategorizovat do již stávajících kategorií, nebo do vlastní kategorie.

Základní nastavení kategorií aplikací



KATEGORIE

Pomocí Správce kategorií můžete aktualizovat databázi kategorií a upravovat kategorie přiřazené aplikacím nebo webům. Do databáze zde můžete přidávat vlastní kategorie a záznamy.

Kategorie můžete aktualizovat v pohledu [Aktualizace a nasazení](#) v části Aktualizace definic.

[Vymazat lokální mezipaměť](#)

Kategorie aplikací Kategorie webů Kategorie přípon

[Procházet databázi](#)

NEDÁVNO KATEGORIZOVANÉ APLIKACE

Pod tento text přetáhněte sloupce, podle kterých chcete seskupovat

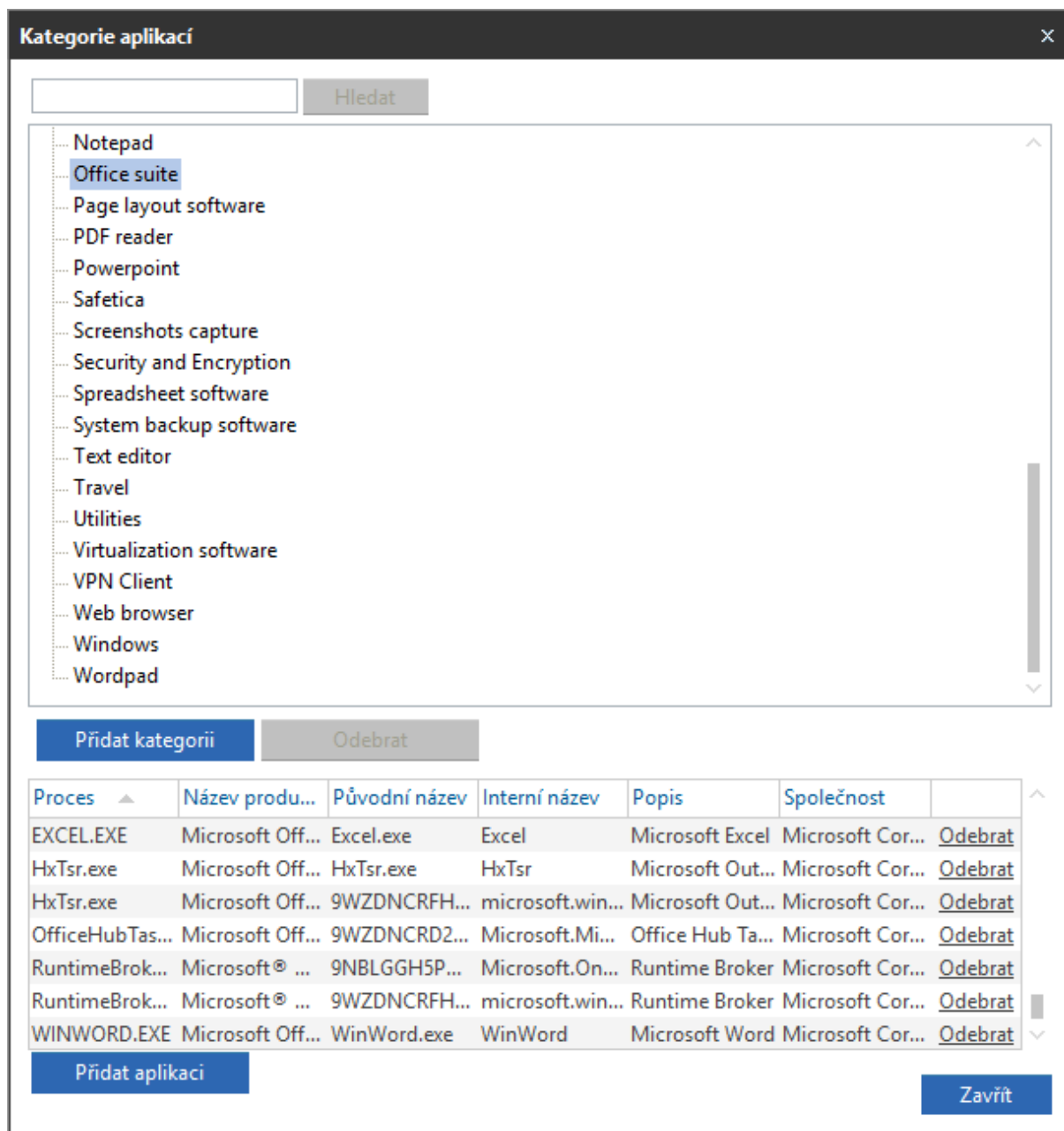
Applikace	Applikační kategorie	Datum a čas
Windows Defender application (... test)		25.03.2021 09:53:18
CyberArk EPM Support Util (EPM... Utilities)		24.03.2021 15:13:54
AppVDIISurrogate32 (AppVDIIS...	Neznámá kategorie	23.03.2021 16:21:00
PWA Identity Proxy Host (identit...	Neznámá kategorie	11.03.2021 08:53:48
PWA Identity Proxy Host (identit...	Neznámá kategorie	11.03.2021 08:53:48
Thunderbird Helper (helper.exe)	Web browser	10.03.2021 09:20:17
Thunderbird Software Updater (...)	Neznámá kategorie	10.03.2021 09:18:47
Microsoft ® IE Setting Sync Back...	Neznámá kategorie	03.03.2021 10:57:55

« » 0 z 0 x Vybranych: 1

Filtery: Žádné aktivní filtry [Smazat všechny filtry](#)

Databáze kategorií aplikací.

Zobrazuje seznam kategorií aplikací, které jsou definovány společností Safetica pod tlačítkem „Procházet databází“



Kategorie aplikací

Hledat

- Notepad
- Office suite**
- Page layout software
- PDF reader
- Powerpoint
- Safetica
- Screenshots capture
- Security and Encryption
- Spreadsheet software
- System backup software
- Text editor
- Travel
- Utilities
- Virtualization software
- VPN Client
- Web browser
- Windows
- Wordpad

Přidat kategorii Odebrat

Proces	Název produ...	Původní název	Interní název	Popis	Společnost	
EXCEL.EXE	Microsoft Off...	Excel.exe	Excel	Microsoft Excel	Microsoft Cor...	Odebrat
HxTsr.exe	Microsoft Off...	HxTsr.exe	HxTsr	Microsoft Out...	Microsoft Cor...	Odebrat
HxTsr.exe	Microsoft Off...	9WZDNCRFH...	microsoft.win...	Microsoft Out...	Microsoft Cor...	Odebrat
OfficeHubTas...	Microsoft Off...	9WZDNCRD2...	Microsoft.Mi...	Office Hub Ta...	Microsoft Cor...	Odebrat
RuntimeBrok...	Microsoft® ...	9NBLGGH5P...	Microsoft.On...	Runtime Broker	Microsoft Cor...	Odebrat
RuntimeBrok...	Microsoft® ...	9WZDNCRFH...	microsoft.win...	Runtime Broker	Microsoft Cor...	Odebrat
WINWORD.EXE	Microsoft Off...	WinWord.exe	WinWord	Microsoft Word	Microsoft Cor...	Odebrat

Přidat aplikaci Zavřít

10.10.2. KATEGORIE WEBŮ

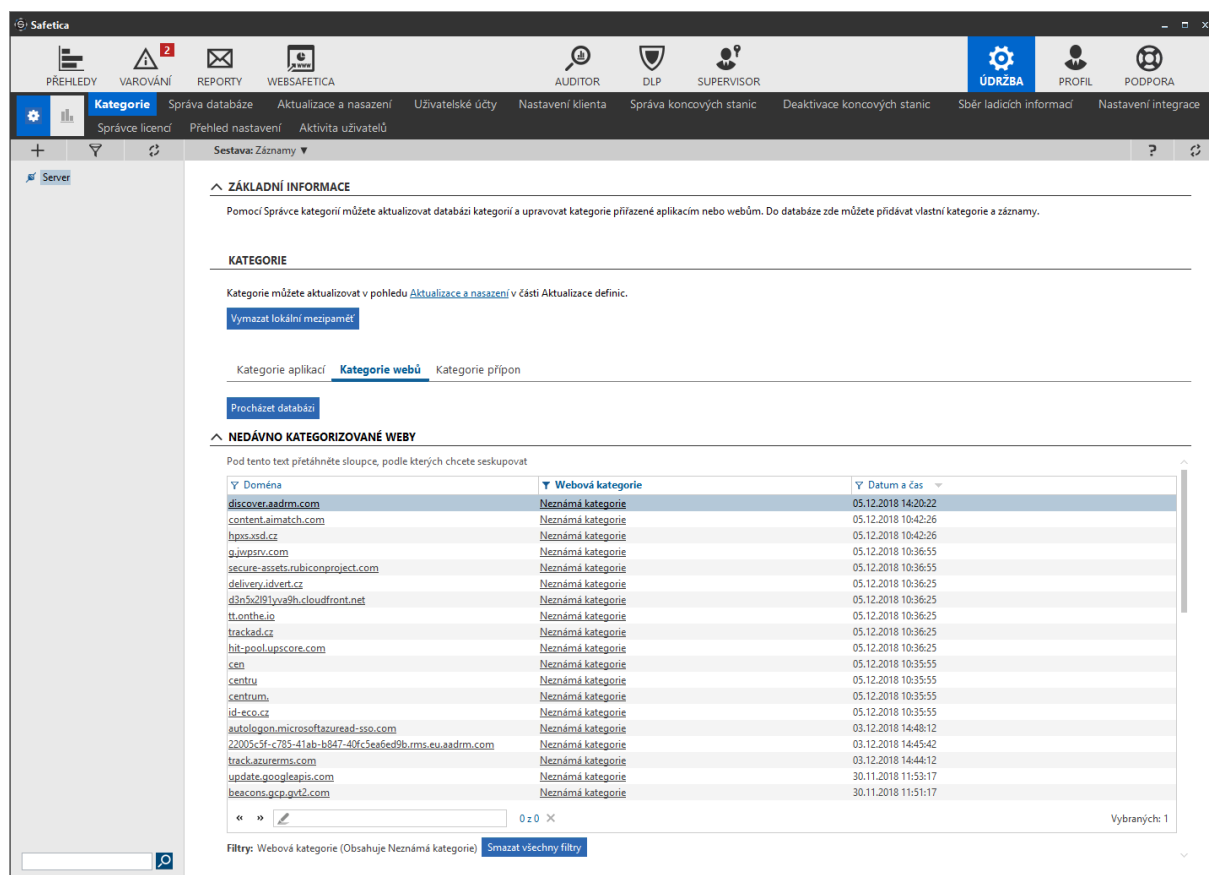
Zobrazuje seznam webů a jejich kategorizaci.

V seznamu jsou zobrazeny všechny webové servery, které byly uživateli navštíveny na všech počítačích s instalovaným Safetica klientem.

Pokud je web kategorizována výrobcem Safetica, bude zobrazena jeho kategorie. Pokud se jedná o Safetice neznámý web, bude označena jako „neznámá kategorie“

Každý neznámý web je možné manuálně kategorizovat do již stávajících kategorií, nebo do vlastní kategorie.

Základní nastavení kategorií webů



ZÁKLADNÍ INFORMACE

Pomocí Správce kategorií můžete aktualizovat databázi kategorií a upravovat kategorie přiřazené aplikacím nebo webům. Do databáze zde můžete přidávat vlastní kategorie a záznamy.

KATEGORIE

Kategorie můžete aktualizovat v pohledu [Aktualizace a nasazení](#) v části Aktualizace definic.

[Vymazat lokální mezipaměť](#)

Kategorie aplikací [Kategorie webů](#) Kategorie přípon

[Procházet databázi](#)

NEDÁVNO KATEGORIZOVANÉ WEBY

Pod tento text přetáhněte sloupce, podle kterých chcete seskupovat

Doména	Webová kategorie	Datum a čas
discover.aadrm.com	Neznámá kategorie	05.12.2018 14:20:22
content.aimatch.com	Neznámá kategorie	05.12.2018 10:42:26
hpxs.vsd.cz	Neznámá kategorie	05.12.2018 10:42:26
g.wpsrv.com	Neznámá kategorie	05.12.2018 10:36:55
secure-assets.rubiconproject.com	Neznámá kategorie	05.12.2018 10:36:55
delivery.idvert.cz	Neznámá kategorie	05.12.2018 10:36:25
d3n5y2l91yva9h.cloudfront.net	Neznámá kategorie	05.12.2018 10:36:25
tt.onthe.io	Neznámá kategorie	05.12.2018 10:36:25
trackad.cz	Neznámá kategorie	05.12.2018 10:36:25
hit-poolupscore.com	Neznámá kategorie	05.12.2018 10:36:25
cen	Neznámá kategorie	05.12.2018 10:35:55
centru	Neznámá kategorie	05.12.2018 10:35:55
centrum	Neznámá kategorie	05.12.2018 10:35:55
id-eco.cz	Neznámá kategorie	05.12.2018 10:35:55
autologon.microsoftazuread-ss0.com	Neznámá kategorie	03.12.2018 14:48:12
22005-c5f-c785-41ab-b847-40fc5ea6ed9b.rms.euaadrm.com	Neznámá kategorie	03.12.2018 14:45:42
track.azureads.com	Neznámá kategorie	03.12.2018 14:44:12
update.googleapis.com	Neznámá kategorie	30.11.2018 11:53:17
beacons.gcp.gvt2.com	Neznámá kategorie	30.11.2018 11:53:17

« » 0 z 0 X Vybraných: 1

Filtrovat: Webová kategorie (Obsahuje Neznámá kategorie) [Smazat všechny filtry](#)

Databáze kategorií webů

Zobrazuje seznam kategorií webů, které jsou definovány společností Safetica pod tlačítkem „Procházet databází“

Kategorie webů

Hledat

- Instant Messaging Web Applications
- Intranet
- IT
- Job search
- Leisure
- Malware
- Moje weby
- Multimedia and art
- News
- Pornography
- Proxy web
- Science and education
- Search engines
- Shopping
- Social networks
- Sport
- Web mails
- Web portals

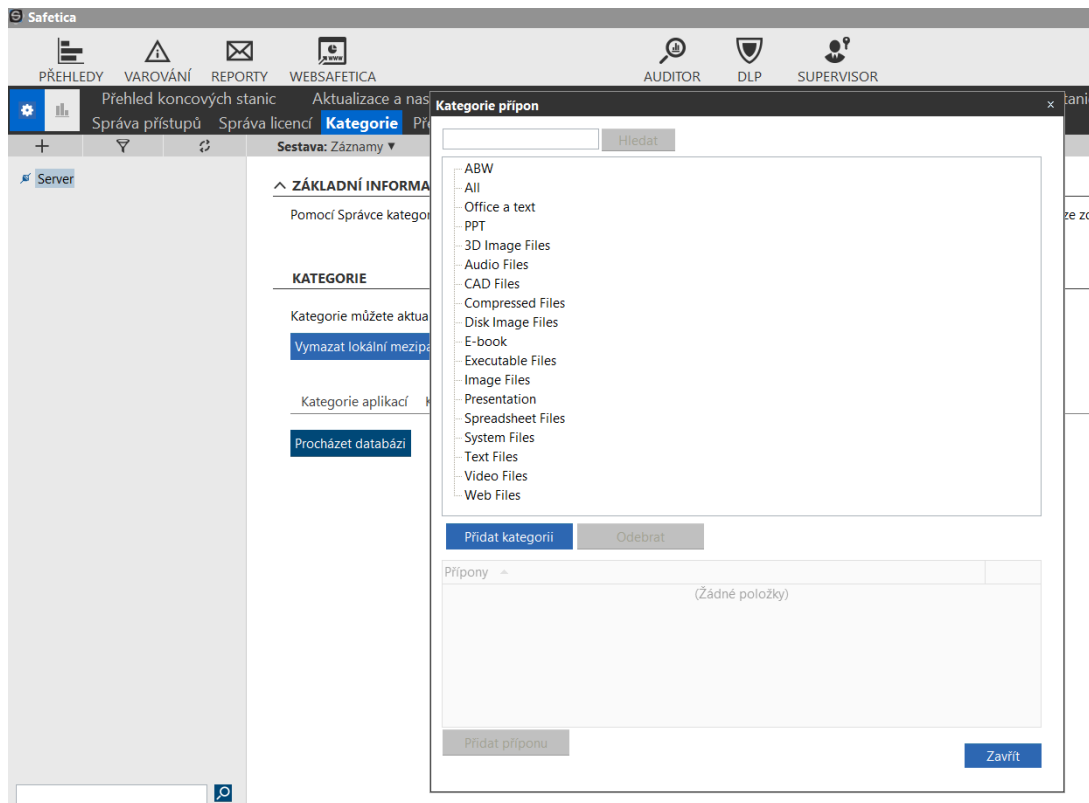
Přidat kategorii Odebrat

Adresa serveru	Odebrat
alertonline.org	Odebrat
alfadate.uv.ro	Odebrat
all.bg	Odebrat
alleferiecentre.dk	Odebrat
allesider.no	Odebrat
allforfashiondesign.com	Odebrat
allportal.ro	Odebrat

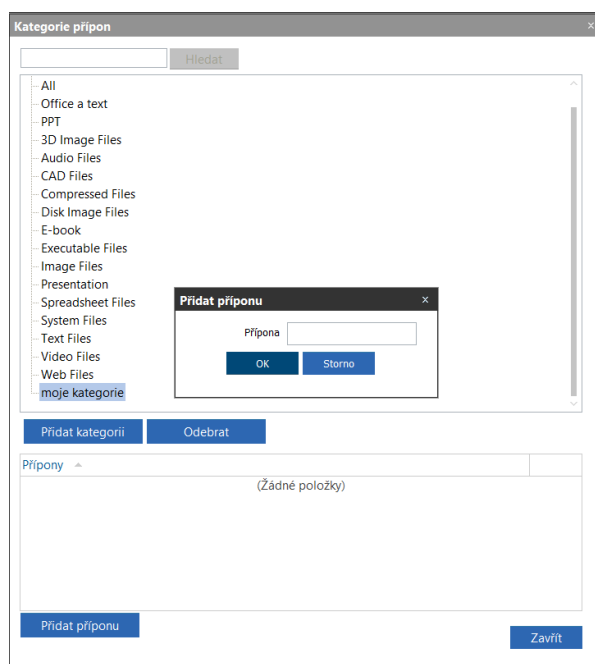
Přidat web Zavřít

10.10.3. KATEGORIE PŘÍPON

Zobrazuje seznam přednastavených kategorií přípon.

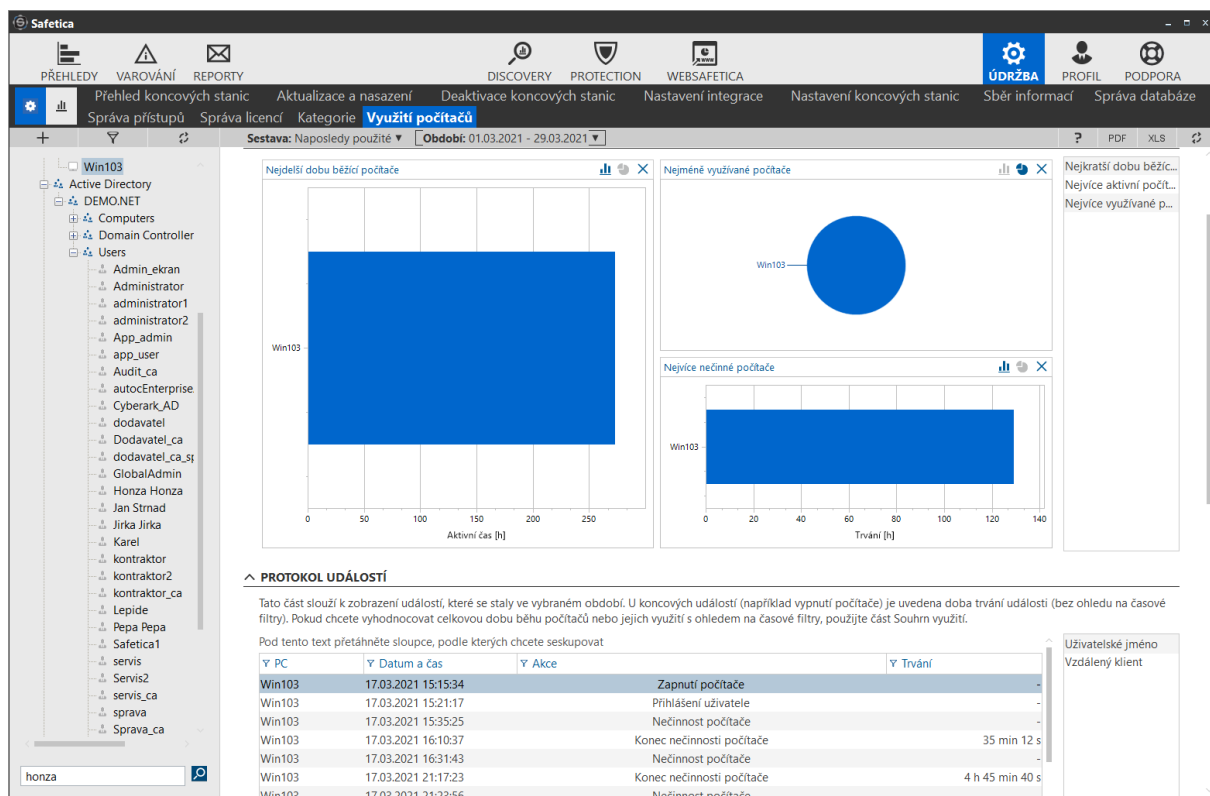


Systém umožňuje vytvářet vlastní kategorie přípon, do kterých se následně definují vlastní přípony souborů



10.11. VYUŽITÍ POČÍTAČŮ

Zobrazuje aktivitu uživatelů včetně spuštění, vypnutí počítače nebo doby spuštění počítače. Zobrazují se informace za poslední den, logové informace a přepočítávají každý den o půlnoci.



Intuitivnější přehled o aktivitě uživatelů nabízí WebSafetica

11. INSTALACE KLIENTSKÉHO SOFTWARE

Klientský software se skládá ze dvou částí

- Agent - Umožňuje jeho vzdálenou instalaci, aktualizaci a další správu. Jedná se o základní SW na klientské stanici, který je možné instalovat jak vzdáleně, například přes GPO, tak pomocí logon scriptu nebo spuštěním instalátoru na klientské stanici. Instalátor je MSI balíček.
- Klient - Klient zajišťuje na koncových stanicích veškeré bezpečnostní a monitorovací funkce. Instaluje se se vzdáleně ze Safetica management konzole pomocí Safetica Agent, nevyžaduje další distribuční software.

11.1. INSTALACE SAFETICA AGENTA

Instalace agenta může být provedena na všechny klientské systémy v síti, kde bude v konečné fázi Instalovaný klient Safetica. Tento SW není intruzivní, neprovádí žádné blokační ani monitorovací funkce, které by mohli zapříčinit nedostupnost služeb nebo znemožnit práci uživatelů. Slouží ke komunikaci mezi klientem a Safetica management serverem.

Instalace se provádí pomocí MSI balíčku, který je dostupný na management konzoli v záložce Údržba, Aktualizace a Nasazení

Instalovat verzi 8.3.85 na koncové stanice Pokročilá správa je dostupná v pohledu [Správa koncových stanic](#)

Počítač	Operační systém	Stav	Verze	Stav verze	
Server					
FPMGMT	Windows Server 2016	Čekání na restart	8.3.85	Aktuální	Restart
SERVER					
WIN10	Windows 10	Neaktivní	8.3.85	Aktuální	
WIN102	Windows 10				
Win10_1	Windows 10	Neaktivní	8.3.84	Neaktuální	
WIN101	Windows 10	Neaktivní	8.3.85	Aktuální	

« » 0 z 0 X

Toto MS Office produkt je pro přípravu instalačního balíčku Downloader Agent. Agentu nainstalujte na všechny stanice ručně nebo např. pomocí GPO politiky v Active Directory.

Získat Downloader Agent

Instalaci je možné provést přes Group policy. Detailní postup instalace je popsán Instalačním manuálem, na straně 18. Je možné provést instalaci agenta ručně nebo pomocí jiné služby na distribuci MSI balíčků

Odkaz na instalační manuál - https://cdn.safetica.com/help/Safetica_Installation_Manual_CZ.pdf

Příklady možností instalace agenta Safetica:

Distribuce instalačního balíčku pomocí ESET ERA

Návod pro distribuci přes ERA

<https://support.safetica.com/index.php?/Knowledgebase/Article/View/229/0/how-to-deploy-safetica-downloader-agent-using-eset-remote-administrator-era>

Distribuce instalačního balíčku pomocí Microsoft GPO

Návod pro distribuci přes GPO

<https://support.safetica.com/index.php?/Knowledgebase/Article/View/319/0/hromadna-instalace-safetica-instalatoru-pomoci-gpo>

Pro instalaci agenta je dobré zvýšit oprávnění. Zde bych doporučil provést nastavení z bodu č.10.

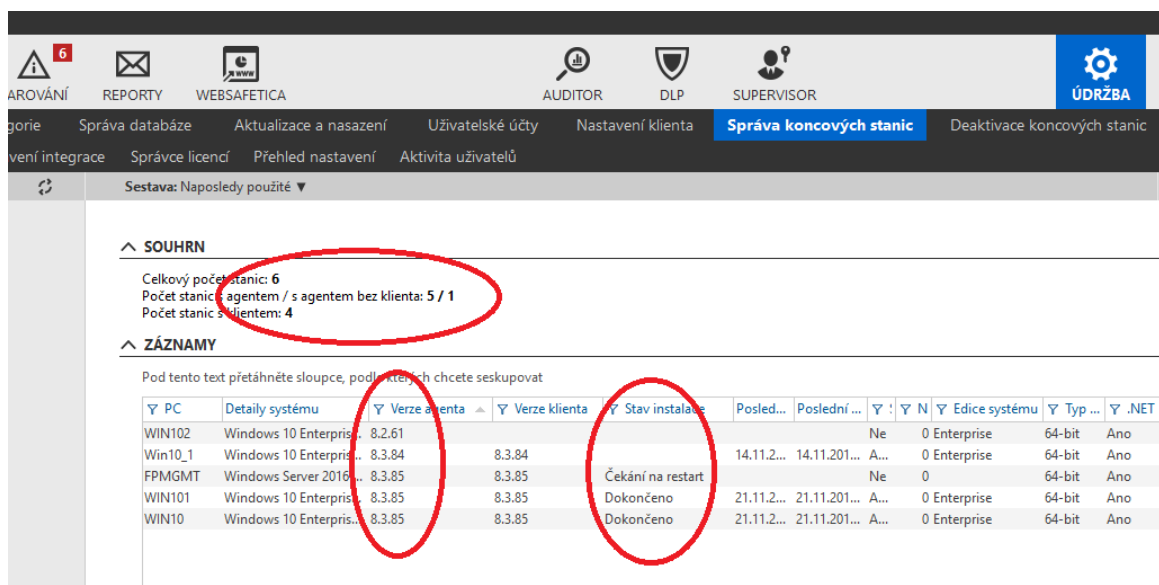
11.2. KONTROLA INSTALACE AGENTA

Po instalaci je potřeba provést kontrolu, kde se Safetica agent úspěšně nainstaloval a na kterých klientských počítačích instalace selhala.

Kontrola se provádí v záložce Údržba, Správa koncových zařízení.

V souhrnu je vidět počet systémů z AD a počet systémů, kde je Agent nainstalovaný

V záznamech je zobrazen seznam všech klientských systémů s verzí instalovaného agenta i stav instalace.



SOUHRN

Celkový počet stanic: 6
 Počet stanic s agentem / s agentem bez klienta: 5 / 1
 Počet stanic s klientem: 4

ZÁZNAMY

Pod tento text přetáhněte sloupce, pod kterými chcete seskupovat

PC	Detaily systému	Verze agenta	Verze klienta	Stav instalace	Posled...	Poslední ...	Y	N	Y	Edice systému	TypNET
WIN102	Windows 10 Enterpris...	8.2.61					Ne	0	Enterprise	64-bit	Ano	
Win10_1	Windows 10 Enterpris...	8.3.84	8.3.84		14.11.2...	14.11.201...	A...	0	Enterprise	64-bit	Ano	
FPMGMT	Windows Server 2016...	8.3.85	8.3.85	Čekání na restart			Ne	0		64-bit	Ano	
WIN101	Windows 10 Enterpris...	8.3.85	8.3.85	Dokončeno	21.11.2...	21.11.201...	A...	0	Enterprise	64-bit	Ano	
WIN10	Windows 10 Enterpris...	8.3.85	8.3.85	Dokončeno	21.11.2...	21.11.201...	A...	0	Enterprise	64-bit	Ano	

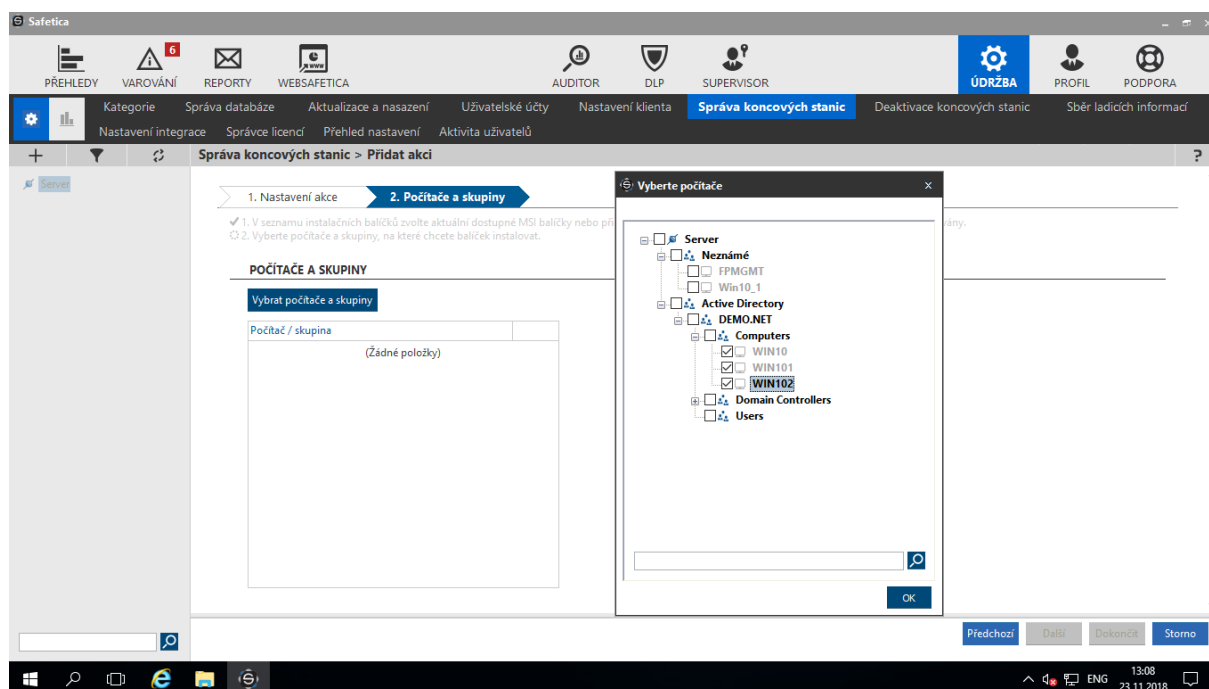
11.3. INSTALACE KLIENTA

Klientský SW již podle definované politiky DLP aktivně monitoruje/blokuje zpracovávaná dat uživatelem, externí zařízení, webové stránky, aplikace apod.

Z důvodu hladkého průběhu začlenění DLP systému do infrastruktury zákazníka bude provedena pilotní instalace Safetica klienta na 10-20 klientských systémů. Budou vybrány klientské systémy z různých oddělení zákazníka, tak aby bylo možné v pilotní fázi nasazení ověřit funkčnost DLP systému a zároveň nasbírat co nejvíce informací, které budou po ukončení pilotní fáze sloužit jak k doporučení, tak následné úpravě bezpečnostní politiky DLP systému.

V rámci nasazení bude provedena instalace na zvolené klientské systémy a aplikována politika nastavená v předcházejících krocích.

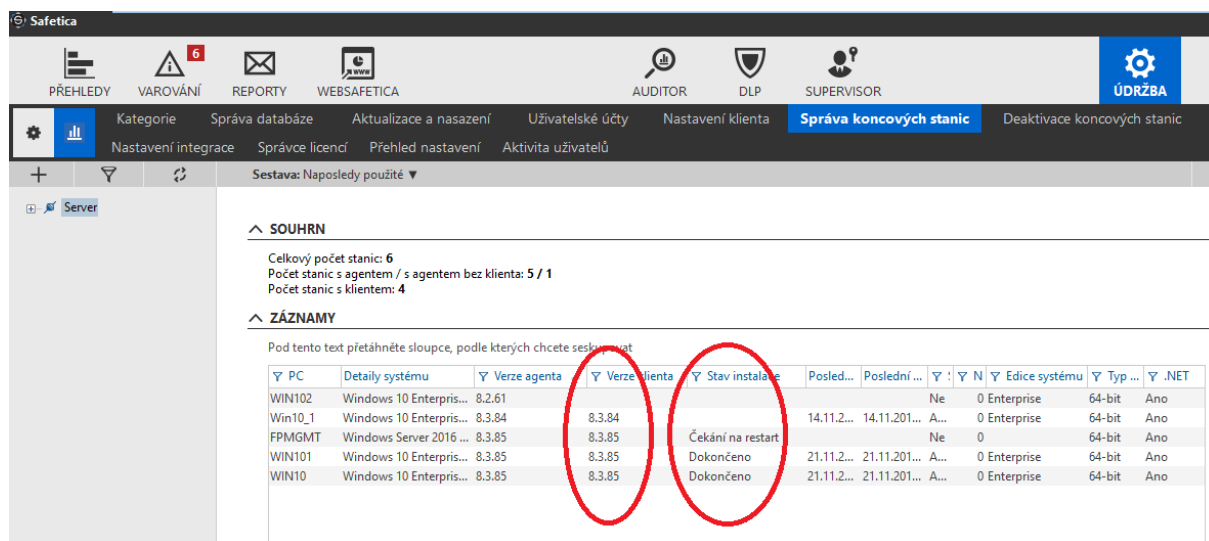
Instalace se provede z management konzole Safetica serveru v Údržba, Správa koncových stanic spuštěním průvodce instalací Instalovat / Aktualizovat. Budou zvoleny klientské stanice definované v předchozím kroku, viz příklad:



11.4. KONTROLA INSTALACE KLIENTA

Po instalaci je potřeba provést kontrolu, zda se Safetica klient úspěšně nainstaloval, popřípadě na kterých klientských počítačích instalace selhala.

Aktivní klienty je možné kontrolovat na management konzoli v Údržba, Správa koncových zařízení ve sloupcích instalovaná verze klienta, stav instalace a datum a čas poslední komunikace s management serverem.



SOUHRN

Celkový počet stanic: 6
 Počet stanic s agentem / s agentem bez klienta: 5 / 1
 Počet stanic s klientem: 4

ZÁZNAMY

Pod tento text přetáhněte sloupce, podle kterých chcete seskupovat

PC	Detaily systému	Verze agenta	Verze klienta	Stav instalace	Posled...	Poslední ...	Y	N	Edice systému	TypNET
WIN102	Windows 10 Enterpris...	8.2.61					Ne	0	Enterprise	64-bit	Ano
Win10_1	Windows 10 Enterpris...	8.3.84	8.3.84		14.11.2...	14.11.201...	A...	0	Enterprise	64-bit	Ano
FPMGMT	Windows Server 2016 ...	8.3.85	8.3.85	Čekání na restart			Ne	0		64-bit	Ano
WIN101	Windows 10 Enterpris...	8.3.85	8.3.85	Dokončeno	21.11.2...	21.11.201...	A...	0	Enterprise	64-bit	Ano
WIN10	Windows 10 Enterpris...	8.3.85	8.3.85	Dokončeno	21.11.2...	21.11.201...	A...	0	Enterprise	64-bit	Ano

11.5. ODINSTALACE KLIENTA

V případě nutnosti odinstalace klient je možné využít úlohu, která zajistí odebrání Safetica klienta popřípadě Safetica klienta i agenta z konkrétního počítače, nebo hromadně z více definovaných zařízení.

Odinstalace se provede z management konzole Safetica serveru v Údržba, Správa koncových stanic spuštěním průvodce instalací „odinstalovat“.

Volba možností odinstalace – odinstalace klienta

Správa koncových stanic > Přidat akci

1. Nastavení akce 2. Počítače a skupiny

1. Uprávněte doplňující nastavení pro odinstalaci Safetica Endpoint Client.

ODINSTALOVAT

⚠ Safetica Endpoint Client bude odinstalován z klientských počítačů. Pro dočasné řešení problémů se stanicí nebo pro trvalé vyloučení stanice použijte akci [Deaktivace koncových stanic](#).

Akce: Odinstalovat komponentu Safetica Endpoint Client Odinstalováním agenta znemožníte vzdálenou instalaci a správu koncové stanice.

Vynutit restart: Ne

Volba možností odinstalace – kompletní odinstalace klienta i agenta

Správa koncových stanic > Přidat akci

1. Nastavení akce 2. Počítače a skupiny

1. Uprávněte doplňující nastavení pro odinstalaci Safetica Endpoint Client.

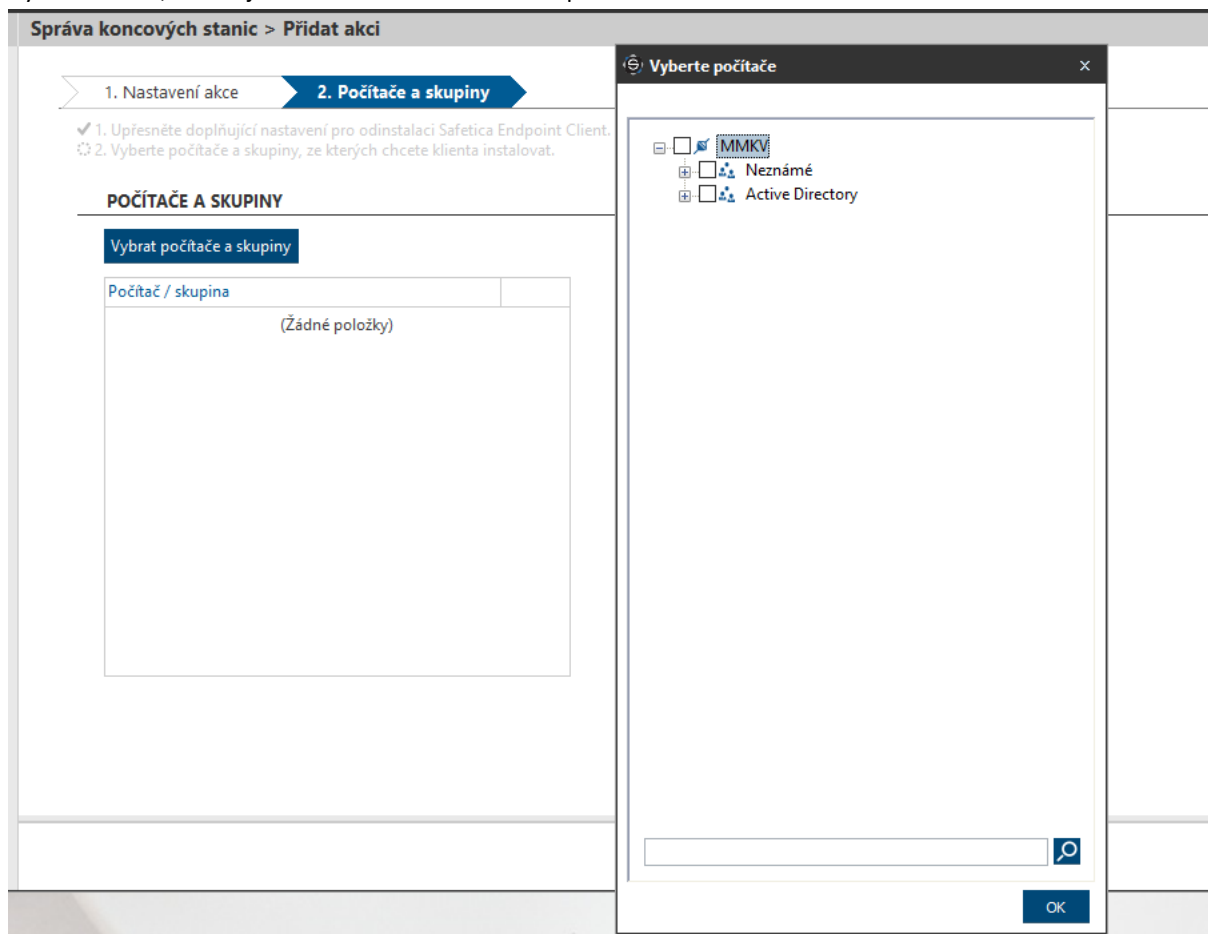
ODINSTALOVAT

⚠ Safetica Endpoint Client bude odinstalován z klientských počítačů. Pro dočasné řešení problémů se stanicí nebo pro trvalé vyloučení stanice použijte akci [Deaktivace koncových stanic](#).

Akce: Odinstalovat komponenty Safetica Endpoint Client a Safetica Agent Odinstalováním agenta znemožníte vzdálenou instalaci a správu koncové stanice.

Vynutit restart: Ne

Výběr zařízení, kde dojde k odinstalaci Safetica komponent:



11.6. KONTROLA ODINSTALACE KLIENTA

Po odinstalaci je potřeba provést kontrolu, zda se Safetica klient úspěšně odinstaloval, popřípadě na kterých klientských počítačích odinstalace selhala.

Aktivní klienty je možné kontrolovat na management konzoli v Údržba, Správa koncových zařízení ve sloupcích instalovaná verze klienta, stav instalace a datum a čas poslední komunikace s management serverem.

SOUHRN

Celkový počet stanic: 6
Počet stanic s agentem / s agentem bez klienta: 5 / 1
Počet stanic s klientem: 4

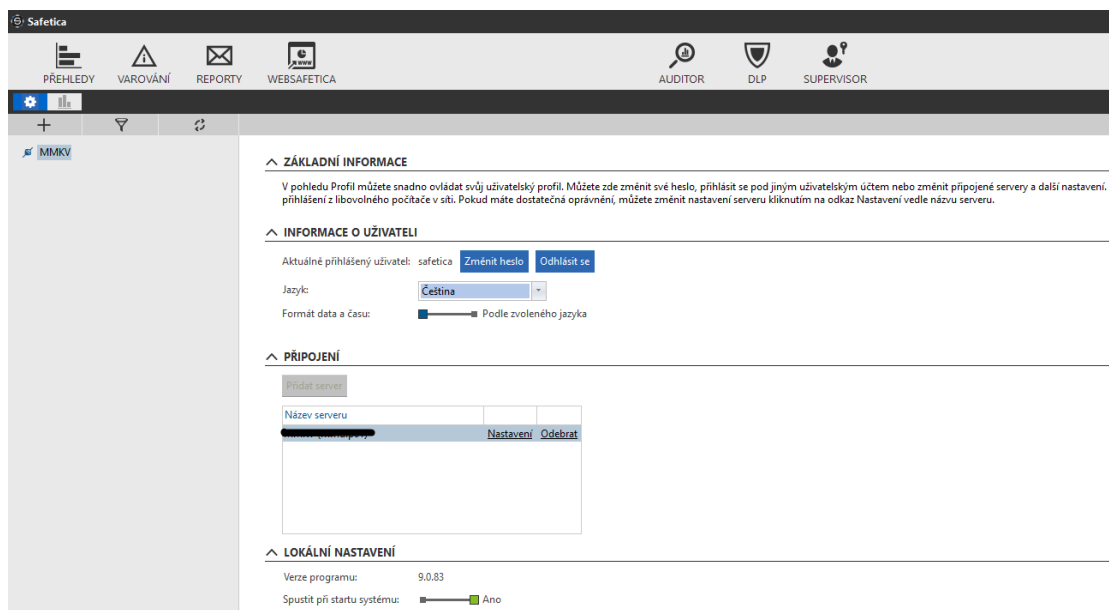
ZÁZNAMY

Pod tento text přetáhněte sloupce, podle kterých chcete seskupovat

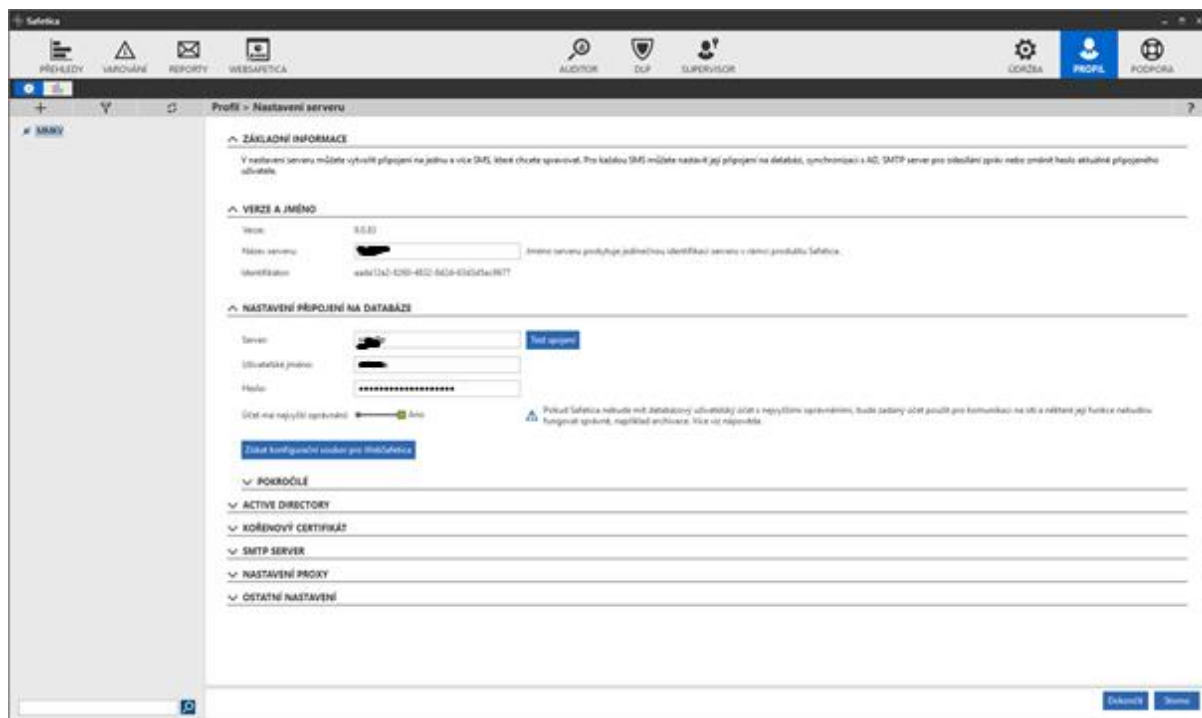
PC	Detaily systému	Verze agenta	Verze klienta	Stav instalace	Posled...	Poslední ...	Y	Y	N	Y	Edice systému	Y	Typ ...	Y	.NET
WIN102	Windows 10 Enterpris...	8.2.61					Ne	0	Enterprise		64-bit	Ano			
Win10_1	Windows 10 Enterpris...	8.3.84	8.3.84		14.11.2...	14.11.201...	A...	0	Enterprise		64-bit	Ano			
FPMGMT	Windows Server 2016 ...	8.3.85	8.3.85	Čekání na restart			Ne	0			64-bit	Ano			
WIN101	Windows 10 Enterpris...	8.3.85	8.3.85	Dokončeno	21.11.2...	21.11.201...	A...	0	Enterprise		64-bit	Ano			
WIN10	Windows 10 Enterpris...	8.3.85	8.3.85	Dokončeno	21.11.2...	21.11.201...	A...	0	Enterprise		64-bit	Ano			

12. PROFIL

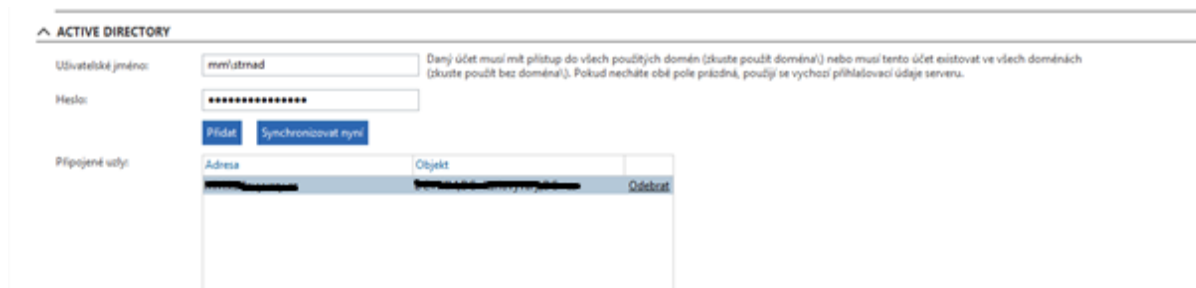
Profil umožňuje základní nastavení pro správu Safetica management konzole a databáze.



- Informace o uživateli - možnost změnit heslo a nastavit jazyk konzole
- Připojení – definice připojení dalším systémům
 - Databázový server
 - Active Directory server
 - SMTP server
 - Certifikáty
 - Proxy server



Nastavení Active Directory:



Synchronizace Safetica management konzole s AD probíhá každé 4 hodiny, popřípadě je možné provést okamžitou synchronizaci pomocí tlačítka „Synchronizovat nyní“.

13. PŘEHLEDY

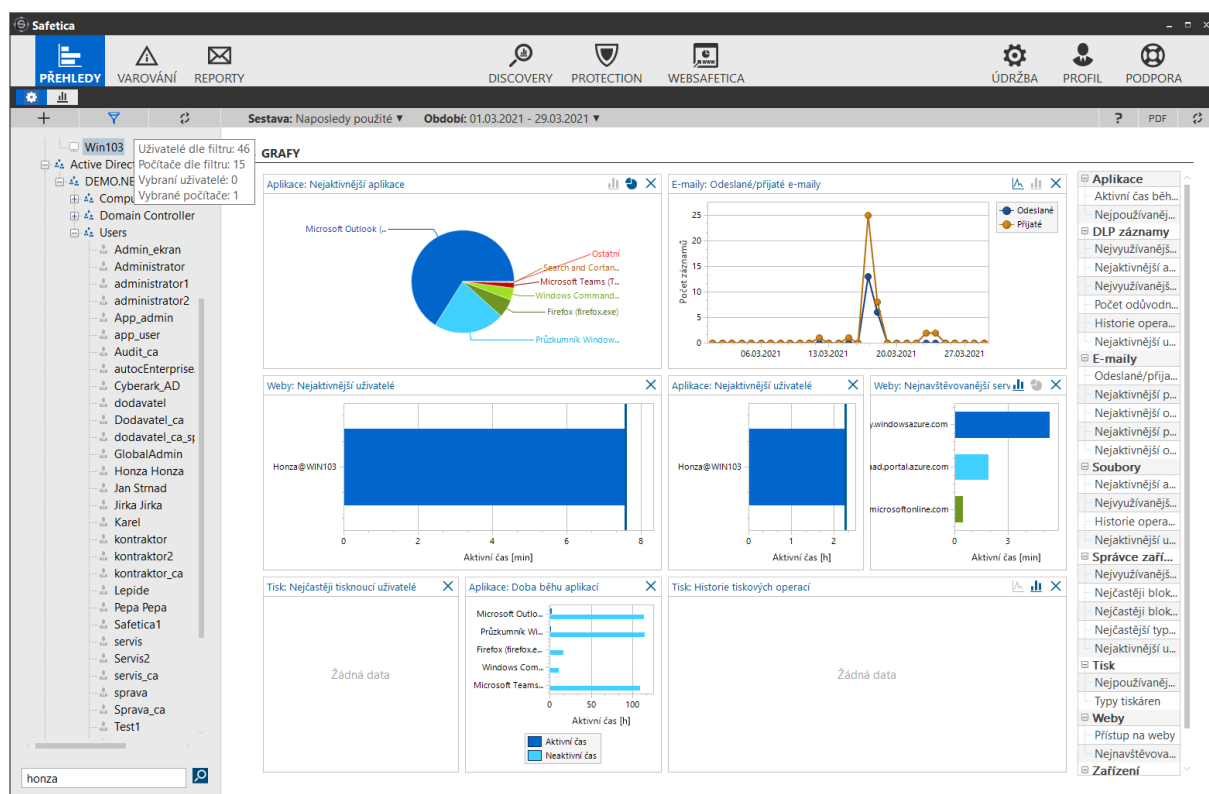
Po přihlášení k Safetica management konzoli se zobrazuje přehled fungování celého systému. Jde o dashboardy, které zobrazují aktuální stav práce uživatelů a detekce událostí.

Zobrazení je možné upravovat, každý správce Safetica DLP systému může mít své vlastní zobrazení.

Systém nabízí velké množství přednastavených dashboardů, které je možné vybrat v pravém sloupci

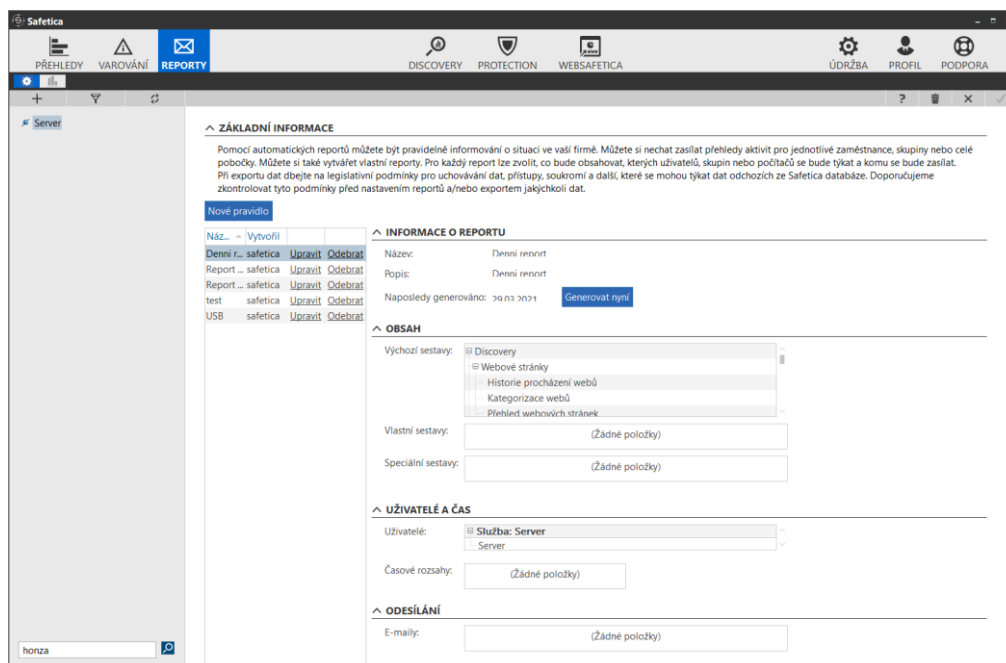
V horní liště je možné vybrat časové období k zobrazení, levý sloupec umožňuje vybrat počítač, uživatele nebo skupiny, popřípadě zobrazit stav za celou společnost.

Kliknutím na dashboard nebo jeho výseč je možné přejít do vizualizace konkrétních událostí. Systém přepne do zobrazení zvolené kategorie, nebo logu – Discovery nebo Protection



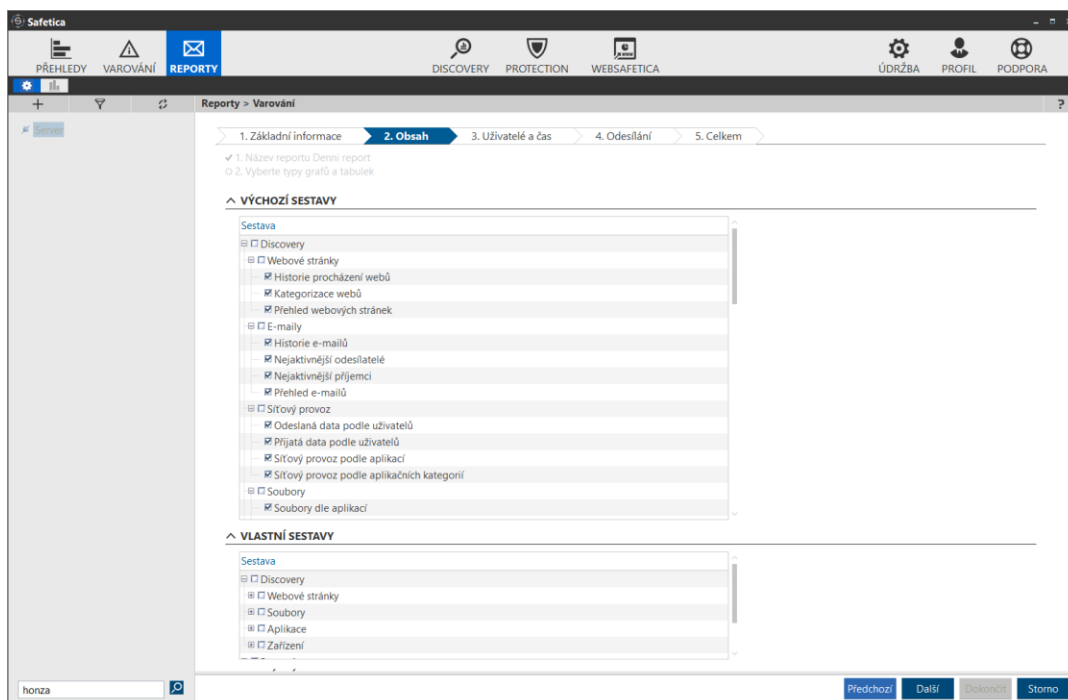
14. REPORTY

Položka „Reporty“ umožňuje nastavit automatizaci zasílání reportů o stavu Safetica systému.

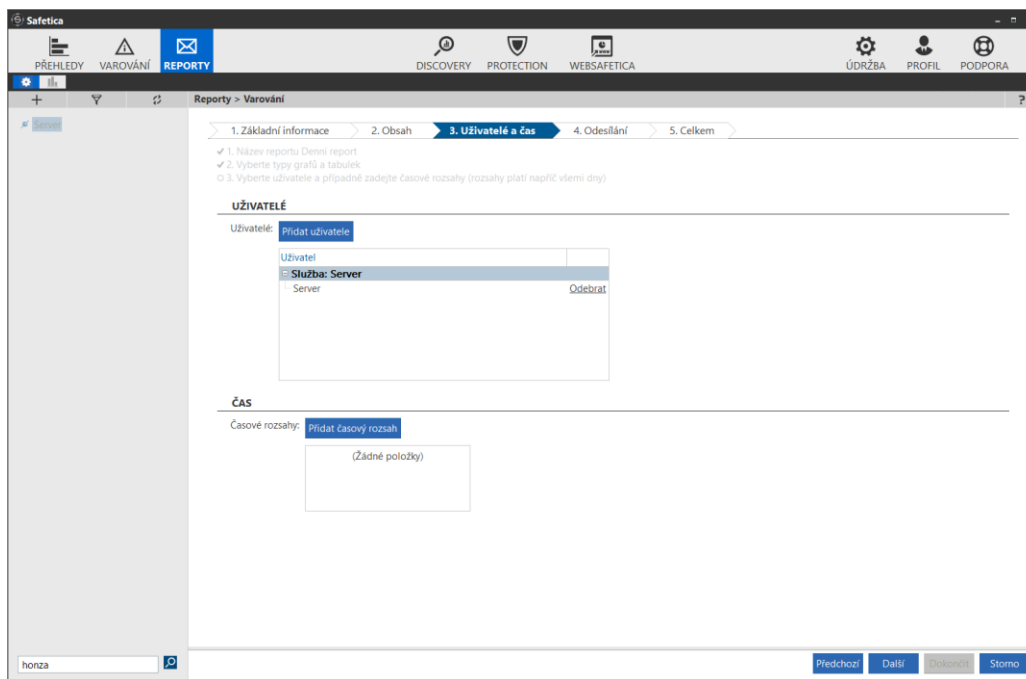


Je možné vytvořit různé reporty s obsahem, který se podle definice odešle na definovaného manažera v nastaveném čase.

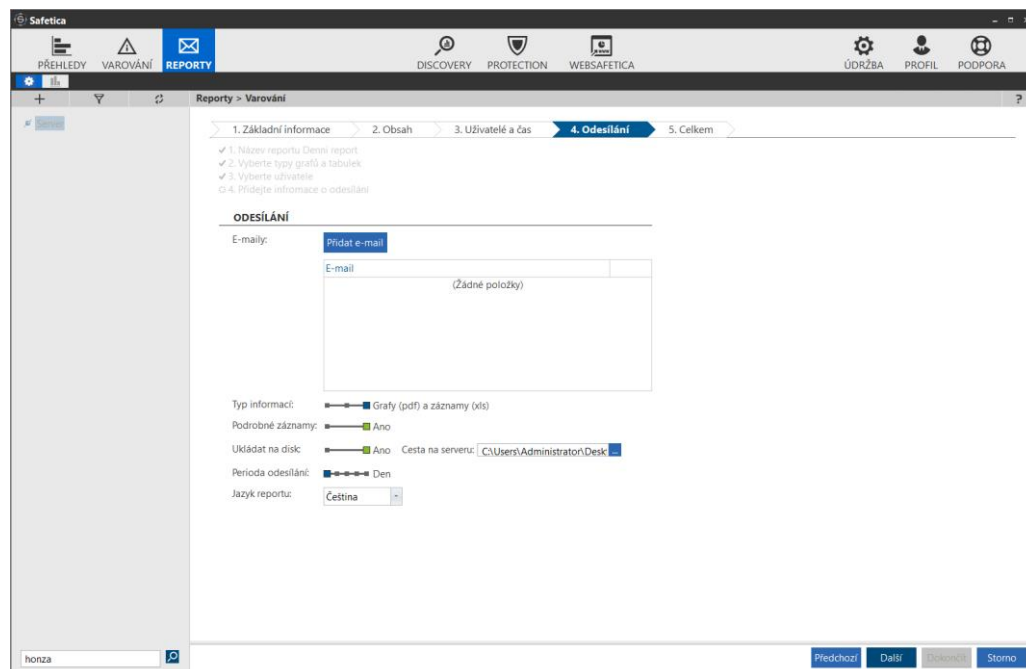
V rámci nastavení je možné zvolit kategorii událostí:



V dalším kroku je možné definovat uživatele, skupiny, zařízení nebo celou společnost a časové období, za které se report bude generovat.



V poslední kroku se definuje, kam se bude report posílat nebo ukládat a v jakém formátu.



Report je možné zasílat emailem na definované uživatele.

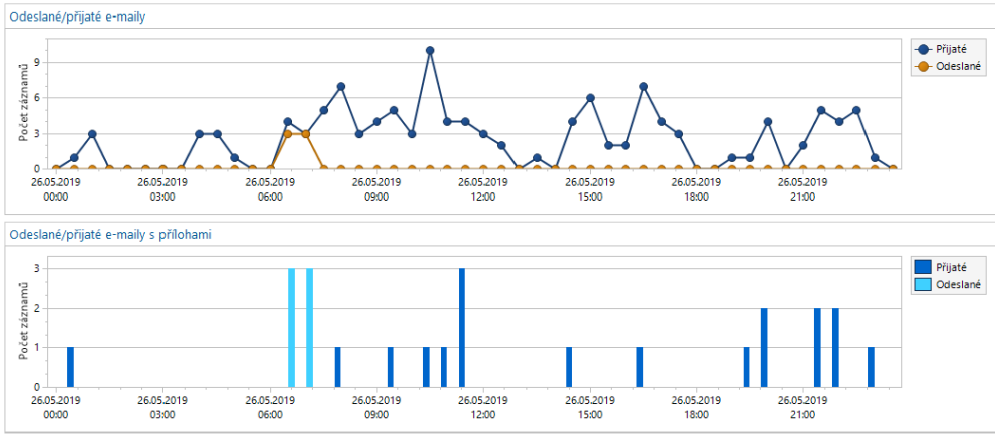
Report může být nastaven do formátů XLS nebo PDF, popřípadě kombinace obou formátů.

Je možné report uložit na disk podle specifikované cesty a nastavit periodu odesílání.

Příklad Safetica reportu:

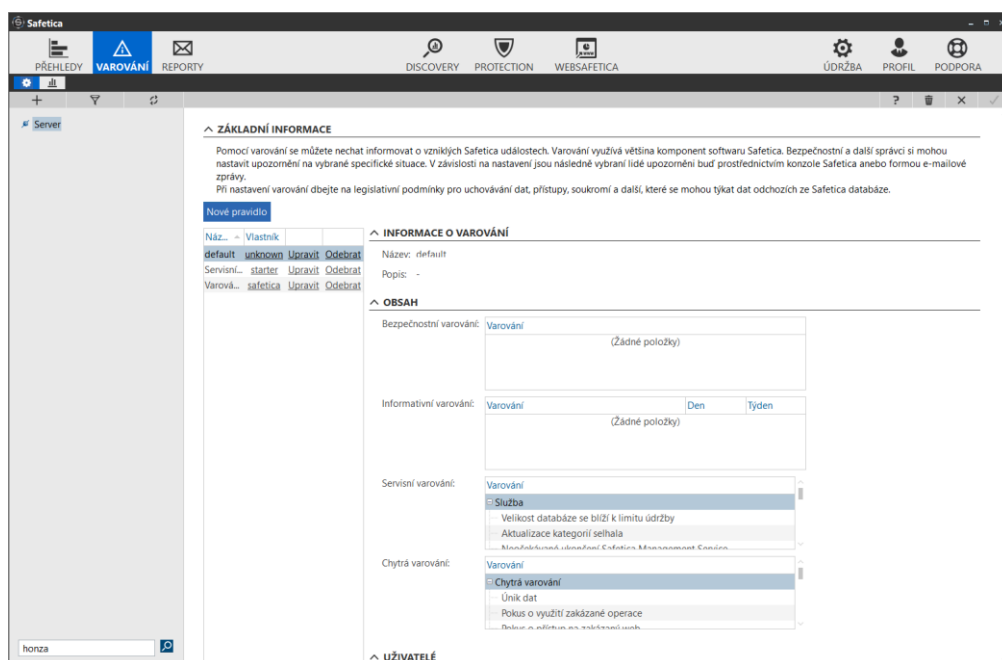
SAFETICA REPORT

HISTORIE E-MAILŮ

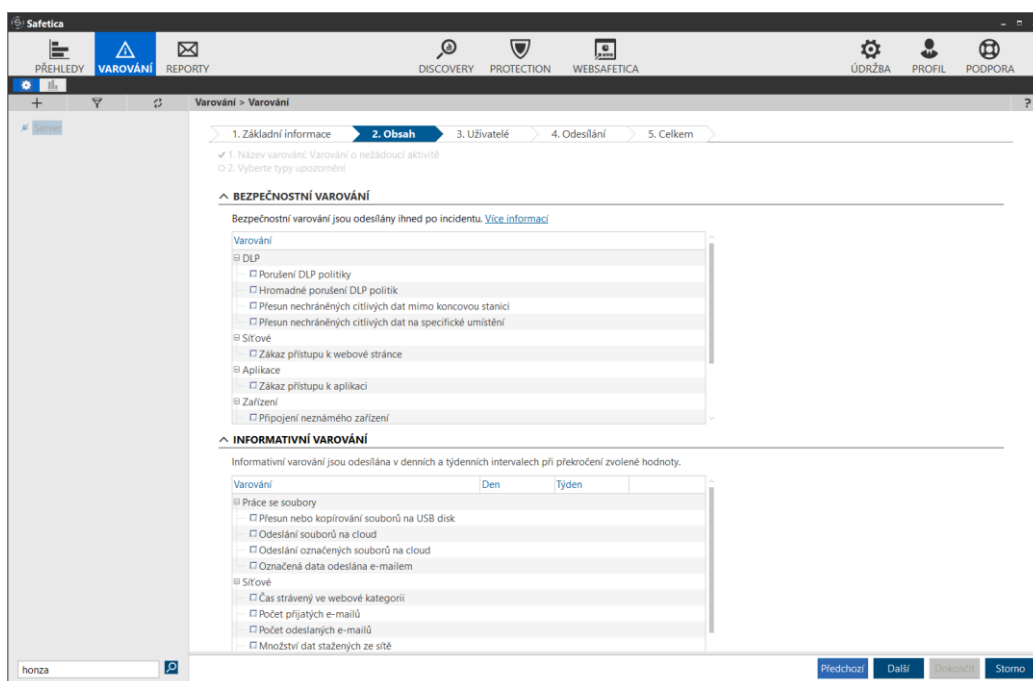


15. VAROVÁNÍ – NOTIFIKACE

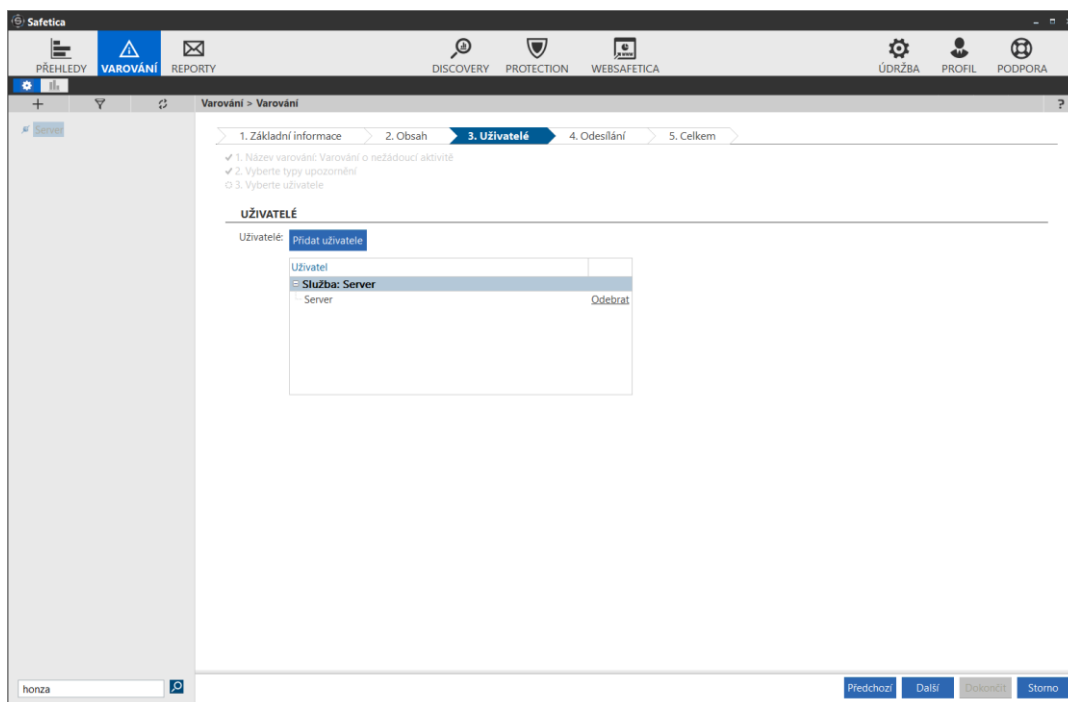
Systém umožňuje nastavit notifikace událostí Safetica systému na email nebo do SIEM systému.



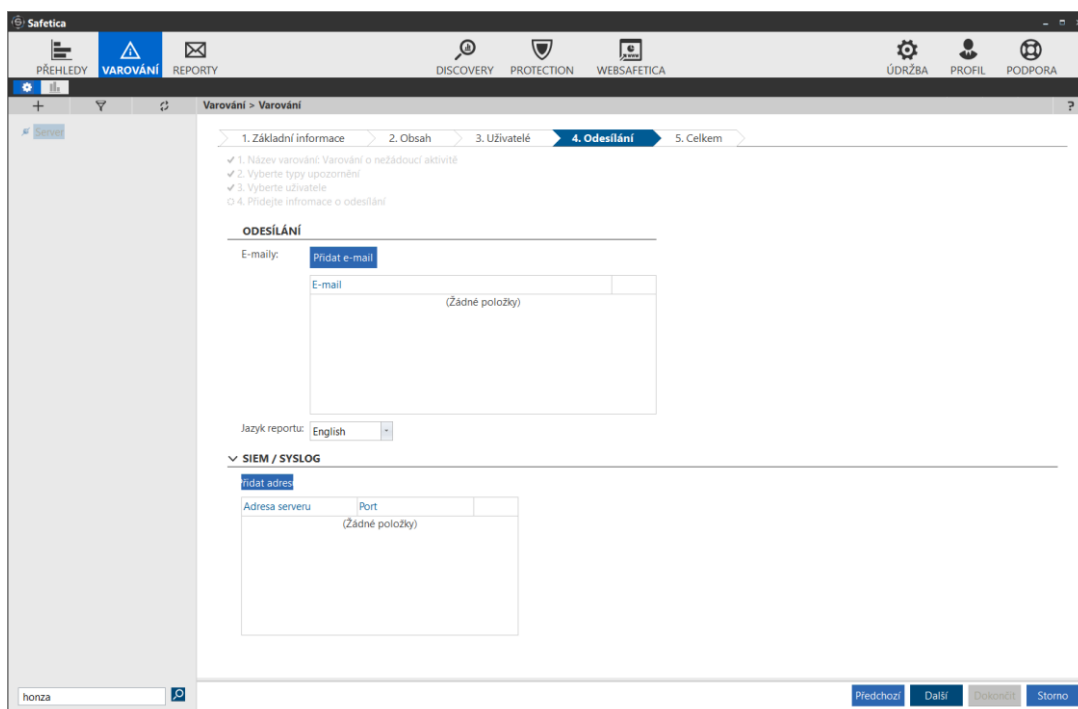
Je možné vybrat typ události, která bude odesílána:



Uživatele, skupinu nebo celou společnost, za které se budou události odesílat



V poslední kroku se volí komunikační kanál – email nebo SIEM systém:



Je možné definovat více úloh pro jednotlivé kategorie událostí a specifikovat komunikační kanály, kam se budou jednotlivé události odesílat.

16. WEBSAFETICA

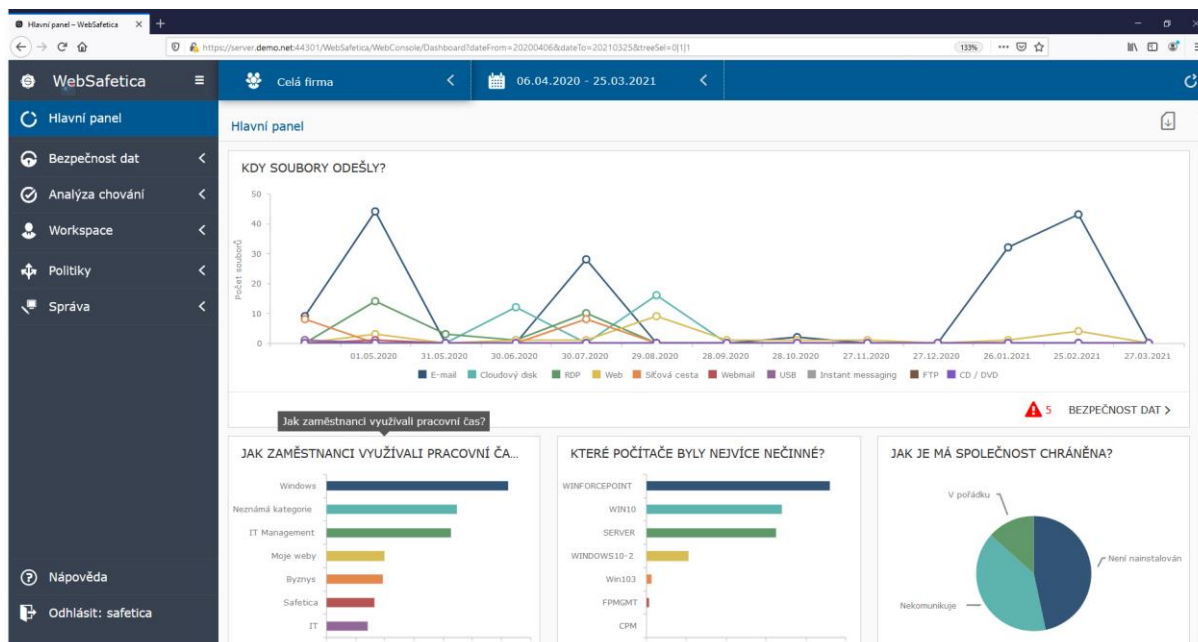
Websafetica je webové rozhraní pro nastavení a reporting Safetica Auditor.

Jde o druhou možnost, jak spravovat/monitorovat Safetica DLP ze standardního webového prohlížeče odkudkoliv ze sítě bez nutnosti instalovat konzoli Safetica (tzv. tlustého klienta)

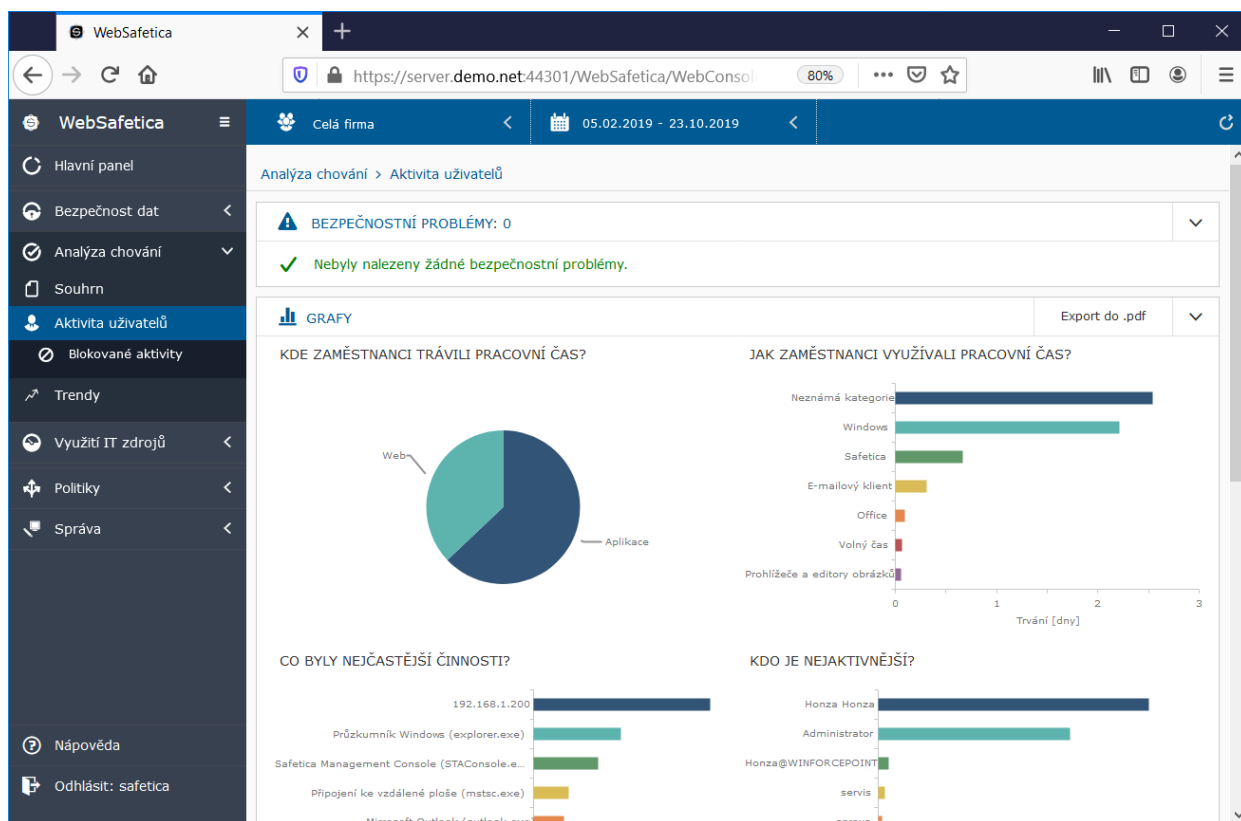
Websafetica je vhodná pro auditory, security manažery, kteří si mohou zobrazit chování uživatelů ve svém webovém prohlížeči.

Z Websafetica je možné pouze sledovat detekované události a provádět základní nastavení management konzole. Z Websafetica není možné provádět nastavení DLP Safetica.

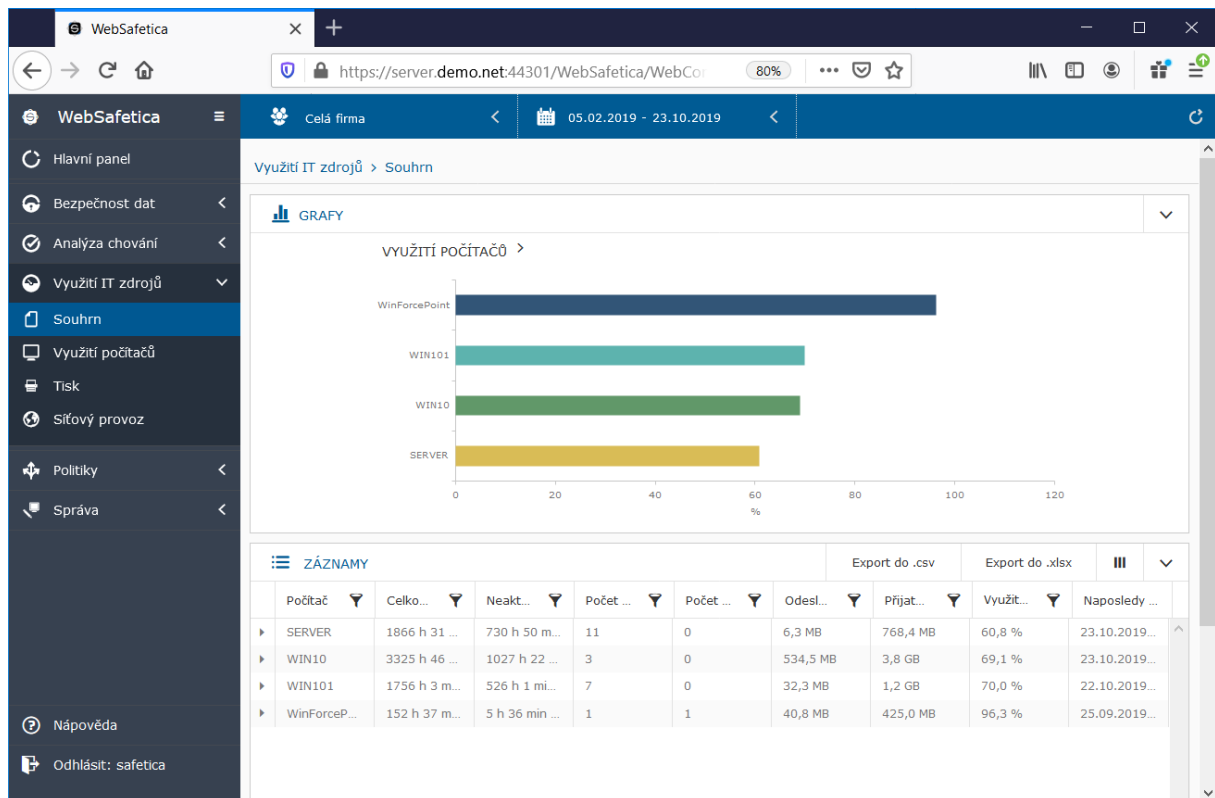
Základní pohled na dashboard Safetica



Pohled na aktivitu uživatelů. Systém nabízí možnosti detailního filtrování na konkrétní uživatele, počítač, datum, nebo typ činnosti (aplikace, weby)



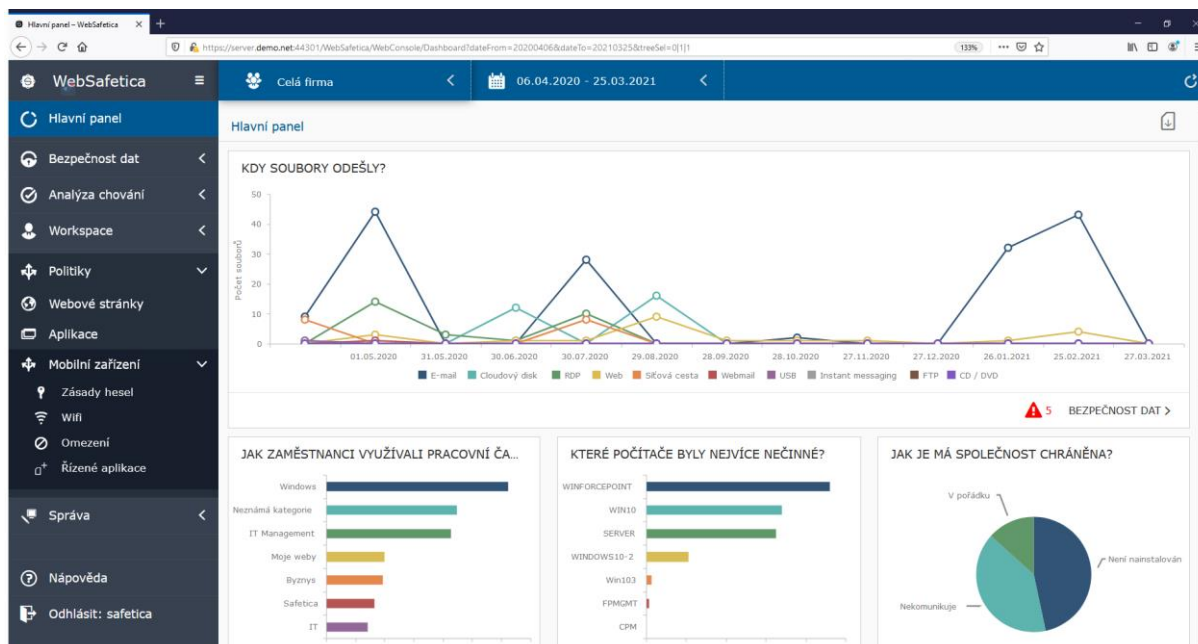
Pohled na využití IT zdrojů. System nabízí možnosti detailního filtrování na konkrétní uživatele, počítač nebo datum.



17. SPRÁVA MOBILNÍCH ZAŘÍZENÍ

Websafetica umožňuje správu mobilních zařízení technologií MDM.

Je možné nastavit politiky s restrikcemi pro mobilní zařízení ve správě



MDM Safetica umožňuje nastavit politiku pro:

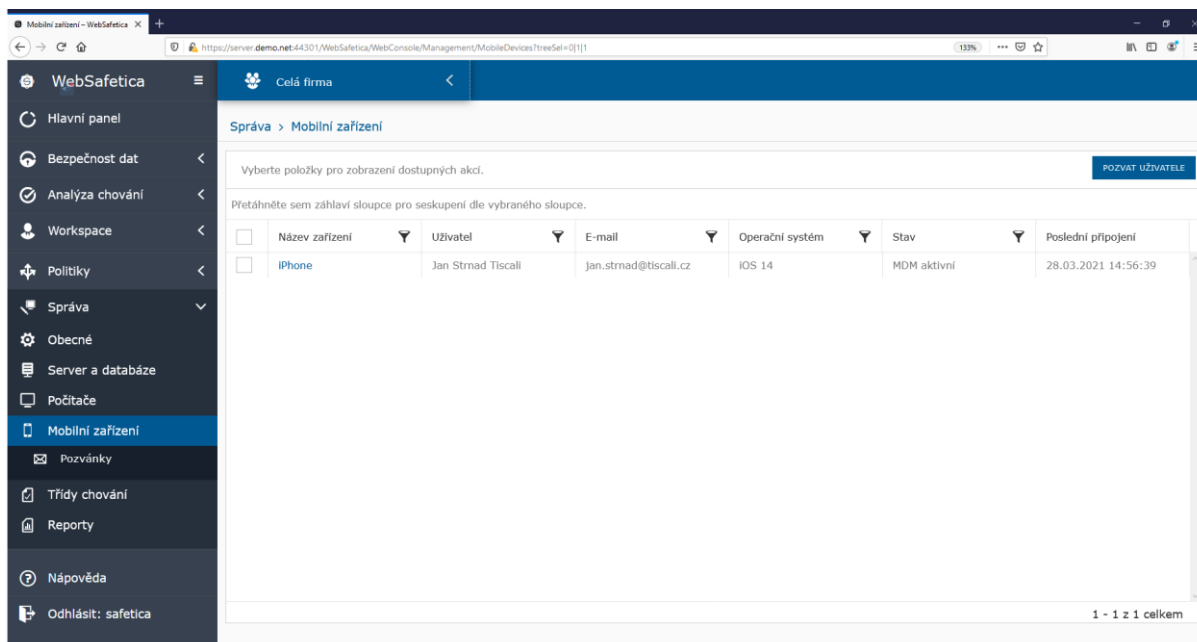
- Zásady hesel – vynucení a komplexnost hesla na mobilním zařízení
- Wifi – přednastavit uživateli mobilního zařízení wifi sítě, které může používat
- Omezení – politiky pro restrikce na mobilním zařízení
- Řízení aplikací – povolení nebo vynucení instalace aplikace na mobilním zařízení

Dále Safetica Mobile zobrazuje seznam spravovaných mobilních zařízení včetně generování pozvánek pro jejich správu.

17.1. SEZNAM SPRAVOVANÝCH MOBILNÍCH ZAŘÍZENÍ

Správa / Mobilní zařízení zobrazuje seznam všech zařízení, které má Safetica Mobile ve své aktivní správě.

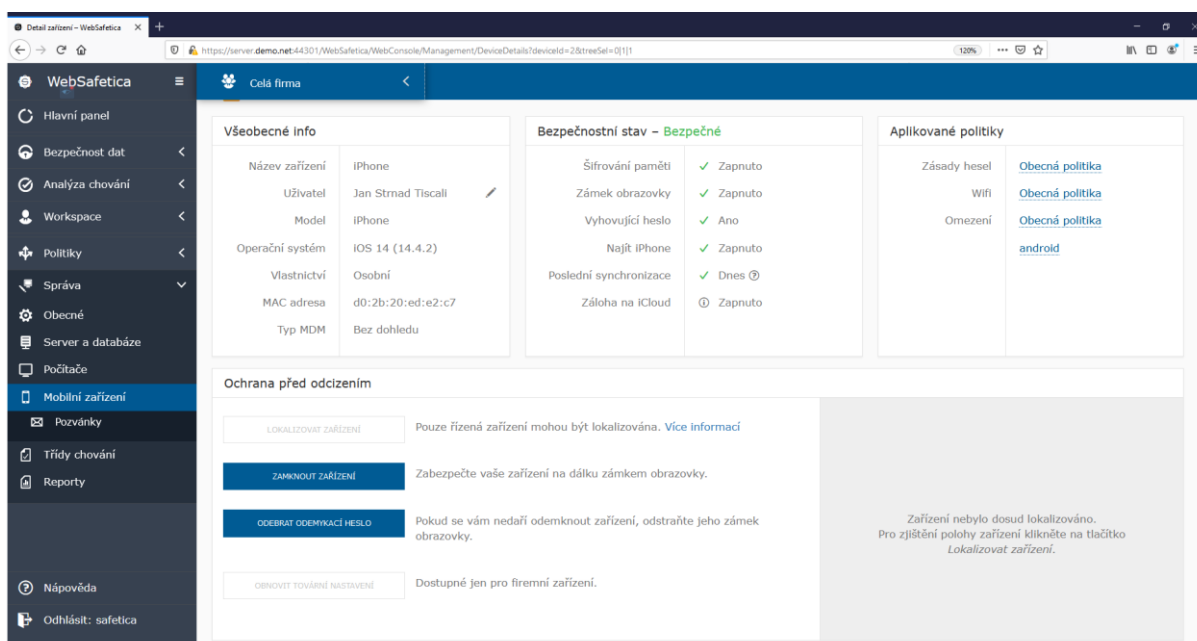
Seznam zobrazuje základní informace o mobilním zařízení:



The screenshot shows the 'Správa > Mobilní zařízení' page in the Safetica Mobile Management console. The page displays a table of managed devices. The table has columns for 'Název zařízení', 'Uživatel', 'E-mail', 'Operační systém', 'Stav', and 'Poslední připojení'. One device is listed: an iPhone owned by Jan Strnad Tiscali, with email jan.strnad@tiscali.cz, running iOS 14, and in an 'MDM aktivní' state, last connected on 28.03.2021 at 14:56:39. A 'POZVAT UŽIVATELE' button is visible in the top right corner of the table area.

<input type="checkbox"/>	Název zařízení	Uživatel	E-mail	Operační systém	Stav	Poslední připojení
<input type="checkbox"/>	iPhone	Jan Strnad Tiscali	jan.strnad@tiscali.cz	IOS 14	MDM aktivní	28.03.2021 14:56:39

Kliknutím na konkrétní mobilní zařízení se zobrazí jeho detail, včetně možnosti vyhledat jeho polohu, obnovit tovární nastavení nebo mobilní zařízení zamknout (možnosti správy jsou závislé na způsobu provisioningu k MDM systému – firemní nebo soukromé zařízení).



The screenshot shows the 'Detail zařízení' page for an iPhone. The page is divided into several sections:

- Všeobecné info:**
 - Název zařízení: iPhone
 - Uživatel: Jan Strnad Tiscali
 - Model: iPhone
 - Operační systém: iOS 14 (14.4.2)
 - Vlastnictví: Osobní
 - MAC adresa: d0:2b:20:ed:e2:c7
 - Typ MDM: Bez dohledu
- Bezpečnostní stav - Bezpečně:**
 - Síťování paměti: Zapnuto
 - Zámek obrazovky: Zapnuto
 - Vyhovující heslo: Ano
 - Najít iPhone: Zapnuto
 - Poslední synchronizace: Dnes
 - Záloha na iCloud: Zapnuto
- Aplikované politiky:**
 - Zásady hesel: [Obecná politika](#)
 - WiFi: [Obecná politika](#)
 - Omezení: [Obecná politika](#)
 - [android](#)
- Ochrana před odcizením:**
 - LOKALIZOVAT ZAŘÍZENÍ:** Pouze řízená zařízení mohou být lokalizována. [Více informací](#)
 - ZAMKNOUT ZAŘÍZENÍ:** Zabezpečte vaše zařízení na dálku zámkem obrazovky.
 - ODEBRAT ODEMKNACÍ HESLO:** Pokud se vám nedaří odemknout zařízení, odstraňte jeho zámek obrazovky.
 - OBNOVIT TOVÁRNĚ NASTAVENÍ:** Dostupné jen pro firemní zařízení.

A message at the bottom right states: 'Zařízení nebylo dosud lokalizováno. Pro zjištění polohy zařízení klikněte na tlačítko [Lokalizovat zařízení](#).'

Detaily rovněž zobrazují seznam instalovaných aplikací na mobilním zařízení:

Ochrana před odcizením

- LOKALIZOVAT ZAŘÍZENÍ** Pouze řízená zařízení mohou být lokalizována. [Více informací](#)
- ZAMKNOUT ZAŘÍZENÍ** Zabezpečte vaše zařízení na dálku zámkem obrazovky.
- ODEBRAT ODEMYKACÍ HESLO** Pokud se vám nedaří odemknout zařízení, odstraňte jeho zámek obrazovky.
- OBNOVIT TUVÁRNĚ NASTAVĚNÍ** Dostupné jen pro firemní zařízení.

Zařízení nebylo dosud lokalizováno. Pro zjištění polohy zařízení klikněte na tlačítko **Lokalizovat zařízení**.

Jaké jsou nejčastější aplikace? [INSTALOVAT APLIKACI](#)

Název	Typ	Název balíčku
Facebook	Uživatelská	com.facebook.Faceb...
FastScanner	Uživatelská	com.coolmobilesolut...
File Manager	Uživatelská	de.zuhanden.filema...
Firefox	Uživatelská	org.mozilla.ios.Firefox
Google	Uživatelská	com.google.Google...
Google Maps	Uživatelská	com.google.Maps
Home Connect	Uživatelská	com.bshg.homecon...
IDOS	Uživatelská	cz.mafra.jzdinrady
inWebO Authenticator	Uživatelská	com.inwebO.authent...

Historie operací

Typ	Datum a čas	Stav	Uživatel
-----	-------------	------	----------

Samostatnou volbou jsou pozvánky, kde je možné nastavit pozvánku pro uživatele ke správě jeho mobilního zařízení.

Pozvánku je možné vytvořit na základě seznamu spravovaných uživatelů:

Správa > Mobilní zařízení > Pozvánky

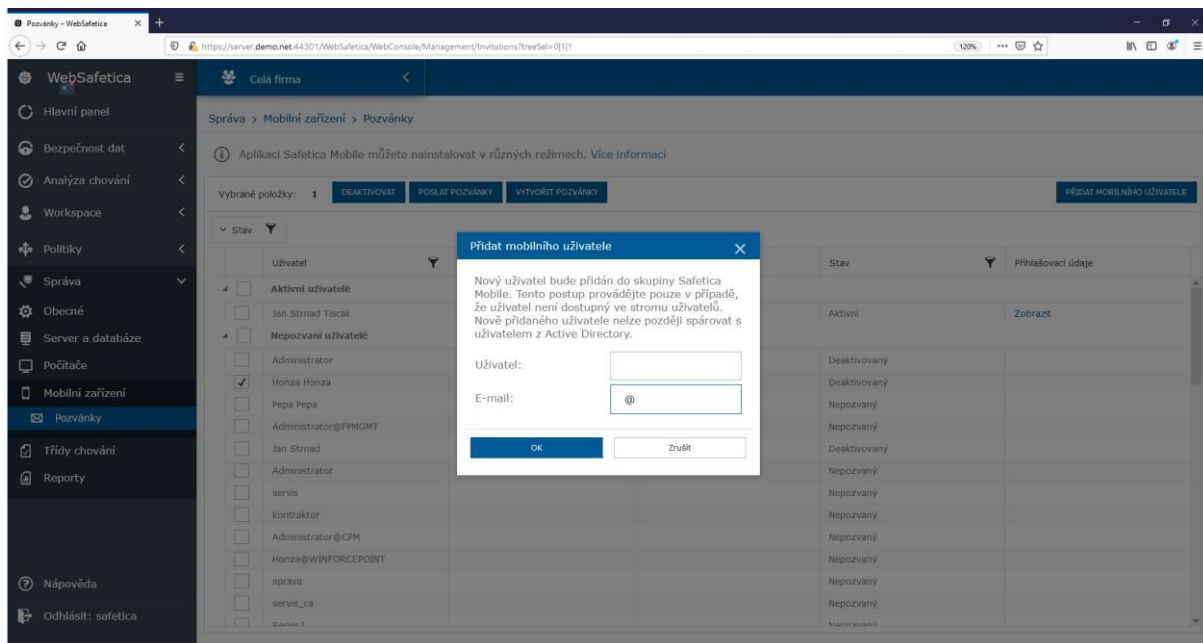
Aplikaci Safetica Mobile můžete nainstalovat v různých režimech. [Více informací](#)

Vybrané položky: 1 [DEAKTIVOVAT](#) [POSLAT POZVÁNKY](#) [VYTVOŘIT POZVÁNKY](#) [PŘIDAT MOBILNÍHO UŽIVATELE](#)

Stav

	Uživatel	E-mail	Naposledy odesláno	Stav	Přihlašovací údaje
Aktivní uživatelé					
<input type="checkbox"/>	Jan Strnad Tiscali	jan.strnad@tiscali.cz	25.03.2021 14:46:25	Aktivní	Zobrazit
Nepozvaní uživatelé					
<input type="checkbox"/>	Administrator	administrator@demo.net	19.03.2021 10:05:17	Deaktivovaný	
<input checked="" type="checkbox"/>	Honza Honza	honza@demo.net	25.03.2021 14:46:26	Deaktivovaný	
<input type="checkbox"/>	Pepa Pepa	pepa@demo.net		Nepozvaný	
<input type="checkbox"/>	Administrator@FPMGMT			Nepozvaný	
<input type="checkbox"/>	Jan Strnad	jan.strnad@autocont.cz	25.03.2021 13:38:54	Deaktivovaný	
<input type="checkbox"/>	Administrator			Nepozvaný	
<input type="checkbox"/>	servis			Nepozvaný	
<input type="checkbox"/>	kontraktor			Nepozvaný	
<input type="checkbox"/>	Administrator@CPM			Nepozvaný	
<input type="checkbox"/>	Honza@WINFORCEPOINT			Nepozvaný	
<input type="checkbox"/>	sprava			Nepozvaný	
<input type="checkbox"/>	servis_ca			Nepozvaný	
<input type="checkbox"/>	canica			Nepozvaný	

Nebo je možné pozvat uživatele na základě jeho emailové adresy:



Uživatelé následně dorazí pozvánka (nutné otevřít na mobilním zařízení, které má být ve správě MDM), kde odklikne „Přijmout pozvánku“

Předmět: Registrace do správy mobilních zařízení

Odesílatel: Safetica Mobile <mdm@safetica.com> ☆

25. března 2021 14:03 25. 3. 4 dny

[vytisknout](#) – [uložit email](#) – [zobrazit hlavičku](#)



Uživatel následně postupuje podle instrukcí na mobilním zařízení.

Dojde ke stažení aplikace Safetica Mobile, připojení k management konzoli, stažení profilu a nastavení mobilního zařízení.

Po úspěšné instalaci se mobilní zařízení zobrazí v seznamu na Websafetica management konzoli.

Detailní informace je možné nalézt na stránkách výrobce Safetica:

<https://www.safetica.com/products/safetica-mobile>

<https://support.safetica.com/en/knowledge-base/managing-mobile-devices>

Enrollment mobilních zařízení:

<https://support.safetica.com/en/knowledge-base/safetica-mobile-enrollment>

Volba módu při enrollmentu:

<https://support.safetica.com/en/knowledge-base/safetica-mobile-enrollment-modes>

17.2. POLITIKY SAFETICA MOBILE

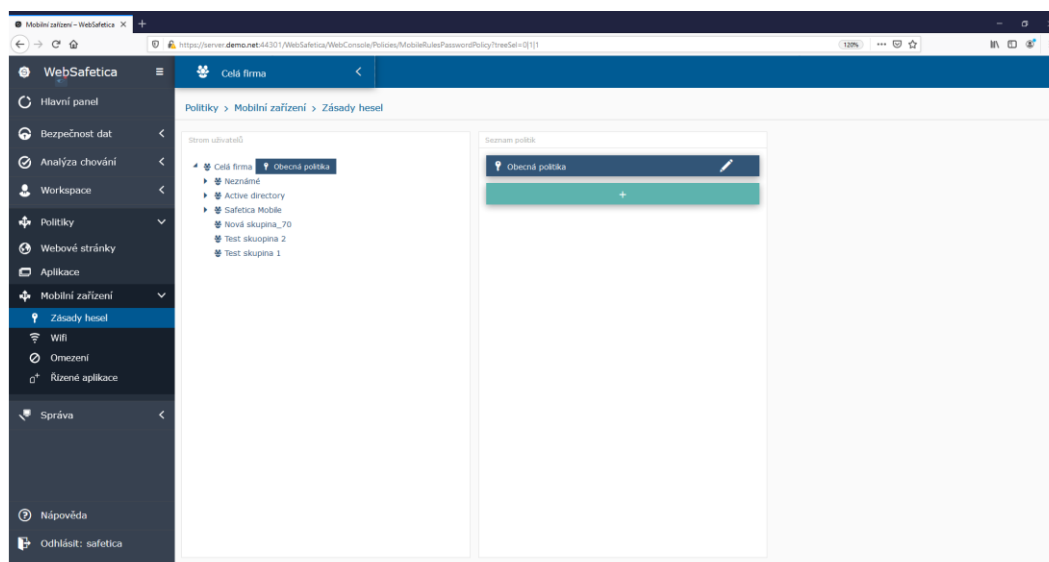
Politiku umožňují nastavení mobilního zařízení v několika úrovních

17.2.1. ZÁSADY HESEL

Politika pro vynucení hesla a jeho komplexnosti na mobilním zařízení.

Politiky se liší podle spravované platformy – Android a iOS.

Nastavení politiky a vytvoření nových politik



Konfigurace politiky a restrikcí:

Upravit politiku
✕

Název politiky

Zabezpečit zařízení
Uživatelé jsou povinni nastavit na svém zařízení zámek.

Zabezpečit pouze pracovní profil
Uživatelé jsou povinni nastavit zámek pouze pro pracovní profil. Zámek zařízení není požadován. Toto nastavení přepíše "Zabezpečit zařízení" pro zařízení s aktivním pracovním profilem.

Povolit jednoduchý zámek
Povolit použití gest pro odemknutí obrazovky a jednoduchých zámků jako například "1111" nebo "1234".

Vyžadovat alfanumerickou hodnotu
Vyžadovat, aby zámky obsahovaly alespoň jedno písmeno.



Minimální délka zámku
Minimální počet znaků pro zámek.

Minimální počet komplexních znaků
Minimální počet povolených nealfanumerických znaků.

Maximální stáří zámku
Počet dní, po kterém musí být zámek změněn.

Čas do automatického uzamčení
Počet minut, po kterém se zařízení automaticky zamkne.

Historie zámků
Počet (1-50) zámků v řadě, které nesmí být stejné.

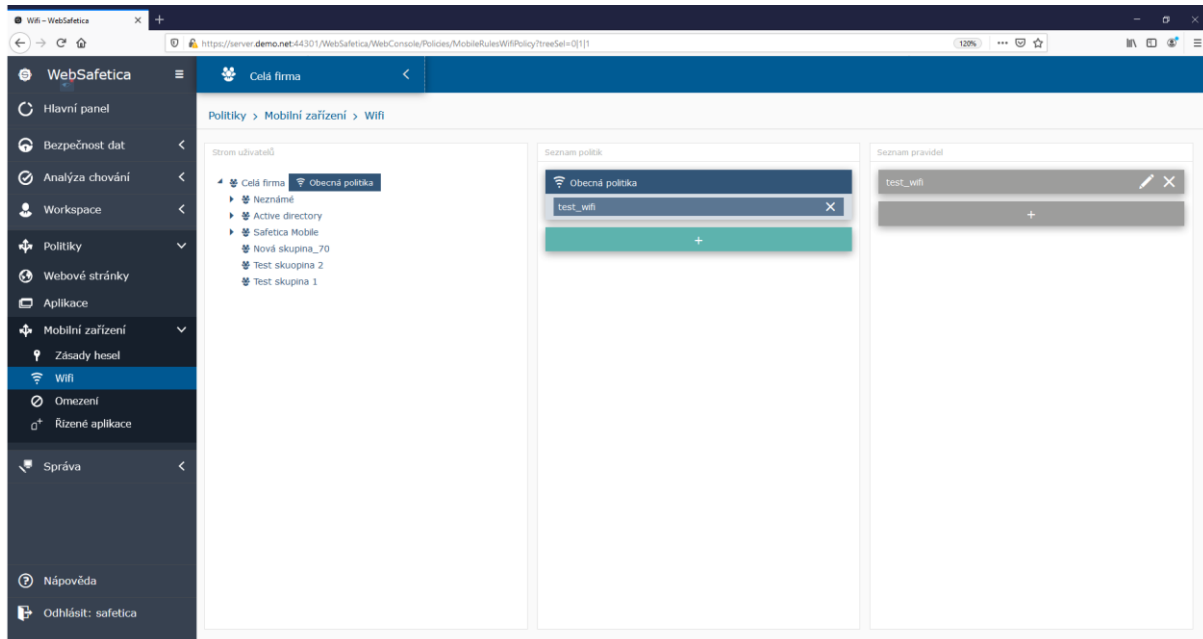



Uložit
Zrušit

17.2.2. WIFI

Politika umožňuje přednastavit wifi sítě, které bude moci uživatel mobilního zařízení používat

Nastavení politik pro wifi sítě:



Konfigurace Wifi sítě:

Upravit pravidlo
✕

Identifikátor bezdrátové sítě
Identifikátor bezdrátové sítě, ke které se má zařízení připojit.

test_wifi

Automatické připojení
Automaticky připojit k zadané síti.



Skrytá síť
Povolit, když cílová síť není otevřená anebo nevysílá.

Typ zabezpečení
Zabezpečení bezdrátové sítě, které bude použito při připojování.

WEP

Heslo
Heslo pro autentizaci bezdrátové sítě.

••••••••

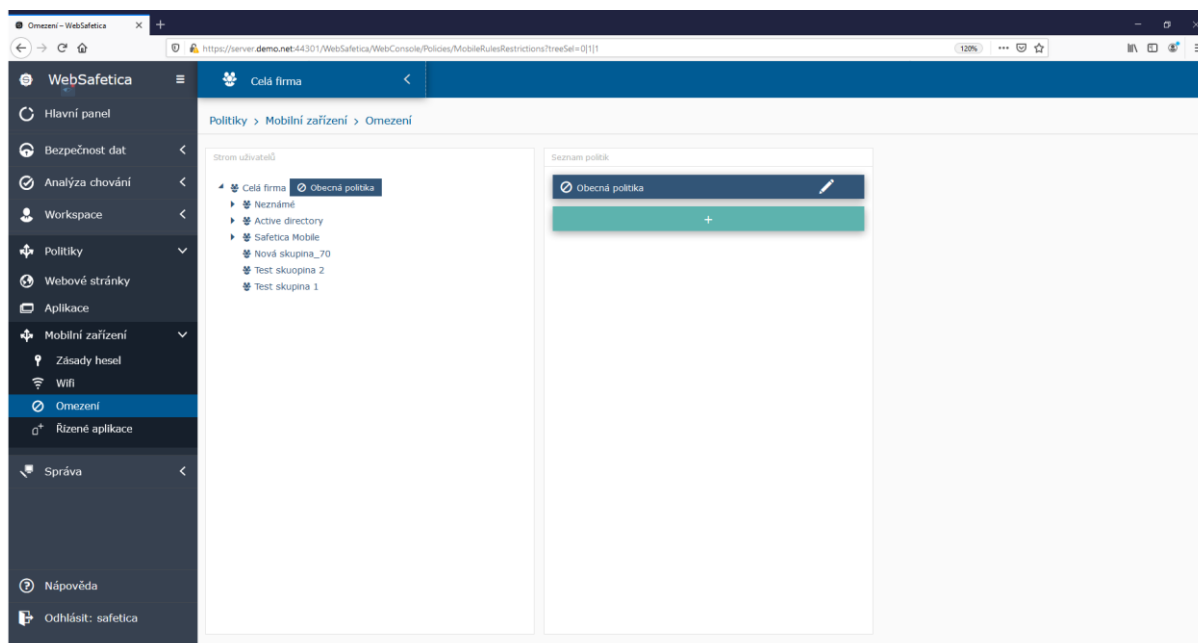
Uložit

Zrušit

17.2.3. OMEZENÍ

Politika restrikcí, které je možné uplatnit na mobilních zařízeních včetně řízení firemního profilu

Nastavení jednotlivých politik:



Konfigurace nastavení politiky

- Společná politika pro obě platformy – Android a iOS

Upravit politiku

Název politiky:

Společné Android iOS


Zakázat fotoaparát
Zakázat použití fotoaparátu ve všech aplikacích.

Zakázat výchozí internetový prohlížeč
Uživatelé nemohou spustit výchozí internetový prohlížeč.

Zakázat snímky obrazovky
Zakáže uživatelům vytváření snímků obrazovky.

Zakázat App Store
Zakázat instalaci aplikací prostřednictvím obchodu s aplikacemi.

- Politika pro Android

 **Android for Work**

Zakázat nadřazenému profilu přebírat odkazy
Aplikace v nadřazeném profilu nebudou moci používat webové odkazy ze spravovaného profilu.

Zakázat kopírování a vkládání mezi různými profily
Uživatelé nebudou moci vkládat data ze schránky do jiných profilů nebo jiným uživatelům. Toto omezení nebrání importu, takže data z jiných profilů a od jiných uživatelů vkládat lze.

Zakázat jednotné heslo
Uživatelé nebudou moci nastavit stejné odemykání obrazovky pro primární a spravovaný profil. Funguje jen se systémy Android 9 a novějšími.

Zakázat sdílení do spravovaných profilů
Uživatelé nebudou moci sdílet soubory/obrázky/data z primárního profilu do spravovaného profilu. Funguje jen se systémy Android 8 a novějšími.

Zakázat správu aplikací
Uživatelé nebudou moci modifikovat aplikace v Nastavení nebo ve spouštěčích.

Zakázat konfiguraci přihlašovacích údajů
Uživatelé nebudou moci konfigurovat své přihlašovací údaje.

Zakázat konfiguraci VPN
Uživatelé nebudou moci konfigurovat VPN.

Zakázat funkce ladění
Uživatelé nebudou moci povolit funkce ladění ani k nim přistupovat.

Zakázat instalaci aplikací
Uživatelé nebudou moci instalovat aplikace.

Zakázat instalaci z neznámých zdrojů
Uživatelé nebudou moci povolit nastavení „Neznámé zdroje“, které umožňuje instalaci aplikací z neznámých zdrojů.

Globálně zakázat instalaci z neznámých zdrojů
Uživatelé nebudou moci povolit nastavení „Neznámé zdroje“, které umožňuje instalaci aplikací z neznámých zdrojů. Funguje jen se systémy Android 10 a novějšími.

Zakázat změny účtu
Uživatelé budou muset potvrzovat přidávání nebo odstraňování účtů přes Authenticator.

Zakázat odchozí Android Beam
Uživatelé nebudou moci zasílat data přes NFC.

Zakázat nastavení ikony uživatele
Uživatelé nebudou moci měnit svou ikonu.

Zakázat sdílení polohy
Uživatelé nebudou moci zapnout sdílení polohy.

Zakázat odinstalaci aplikací
Uživatelé nebudou moci odinstalovat aplikace.

Vynutit ověřování aplikací
Uživatelé nebudou moci zakázat ověřování aplikací.

Zakázat automatické vyplňování
Uživatelé nebudou moci využívat služby automatického vyplňování. Funguje jen se systémy Android 8 a novějšími.

Zakázat sdílení Bluetooth
Uživatelé nebudou moci zasílat soubory pomocí Bluetooth. Funguje jen se systémy Android 8 a novějšími.

Zakázat konfiguraci polohy
Uživatelé nebudou moci povolit nebo zakázat zprostředkovatele polohy. Funguje jen se systémy Android 9 a novějšími.

Zakázat tisk
Uživatelé nebudou moci tisknout. Funguje jen se systémy Android 7 a novějšími.

ULOŽIT **ZRUŠIT**

- Politika pro iOS

Upravit politiku

Název politiky

Společné Android iOS

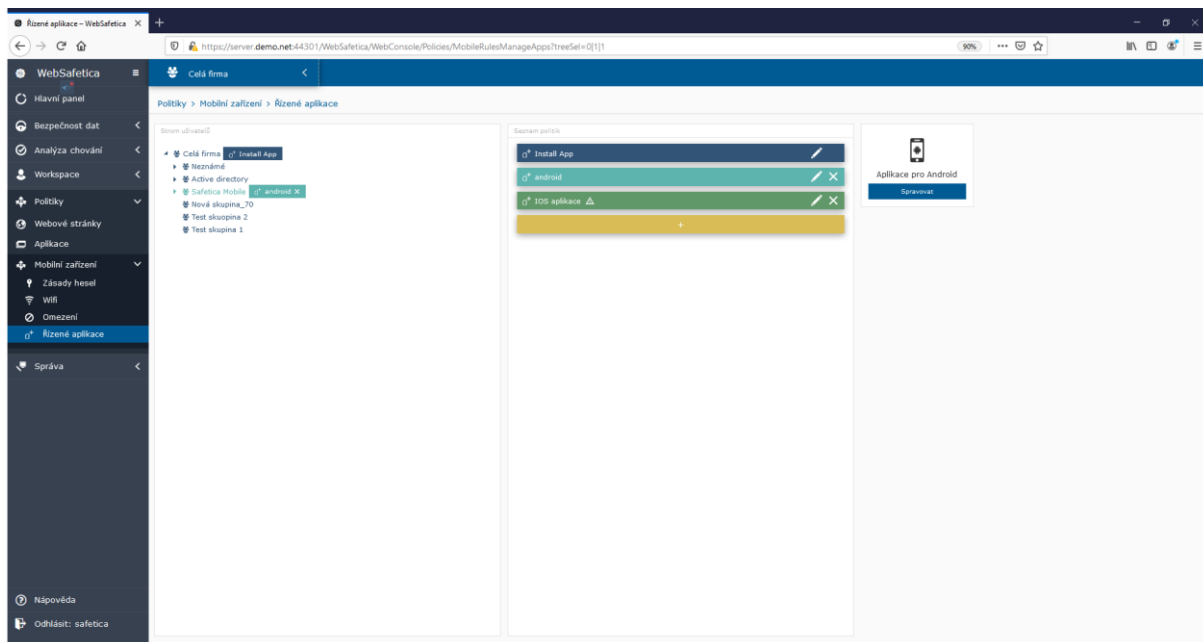
- Chránit data řízených aplikací**
Zakáže sdílení souborů z řízených do neřízených aplikací.
- Zakázat nešifrované zálohy**
Uživatelé nebudou moci vytvářet nešifrované zálohy iOS.
- Zakázat jiné podnikové aplikace**
Odstraní tlačítko Důvěřovat podnikovému vývojáři v části Nastavení->Obecné->Profily a správa zařízení. Zakáže se poskytování aplikací prostřednictvím univerzálních zřizovacích profilů.
- Zakázat nedůvěryhodná TLS připojení**
Všechny nedůvěryhodné HTTPS certifikáty budou automaticky odmítnuty.
- Zakázat synchronizaci dat spravovaných aplikací s iCloud**
Uživatelé nebudou moci synchronizovat data spravovaných aplikací s iCloud.
- Zakázat zálohování do iCloud**
Uživatelé nebudou moci zálohovat zařízení do iCloud.
- Zakázat sdílený fotostream**
Uživatelé nebudou moci sdílet fotostream.
- Zakázat odemykání pomocí Touch ID**
Uživatelé nebudou moci odemknout obrazovku otiskem prstu nebo rozpoznáním tváře.

iOS supervised

- Zakázat AirDrop**
Uživatelé nebudou moci používat funkci AirDrop.
- Zakázat instalaci aplikací**
Uživatelé nebudou moci používat App Store a jeho ikona se nebude zobrazovat na ploše. Nebude možné instalovat ani aktualizovat aplikace.
- Zakázat instalaci profilu UIConfiguration**
Uživatelé nebudou moci interaktivně instalovat konfigurační profily a certifikáty.
- Zakázat změny rozhraní Bluetooth**
Uživatelé nebudou moci měnit nastavení Bluetooth.
- Zakázat AirPrint**
Uživatelé nebudou moci používat funkci AirPrint.
- Zakázat nastavování blízkých zařízení**
Uživatelům se nebude zobrazovat výzva ohledně nastavení nových zařízení v okolí.
- Zakázat odstraňování systémových aplikací**
Uživatelé ze zařízení nebudou moci odstraňovat systémové aplikace.
- Zakázat konfiguraci VPN**
Uživatelé nebudou moci konfigurovat VPN.
- Zakázat sdílení hesel**
Uživatelé nebudou moci sdílet hesla pomocí funkce AirDrop Passwords.

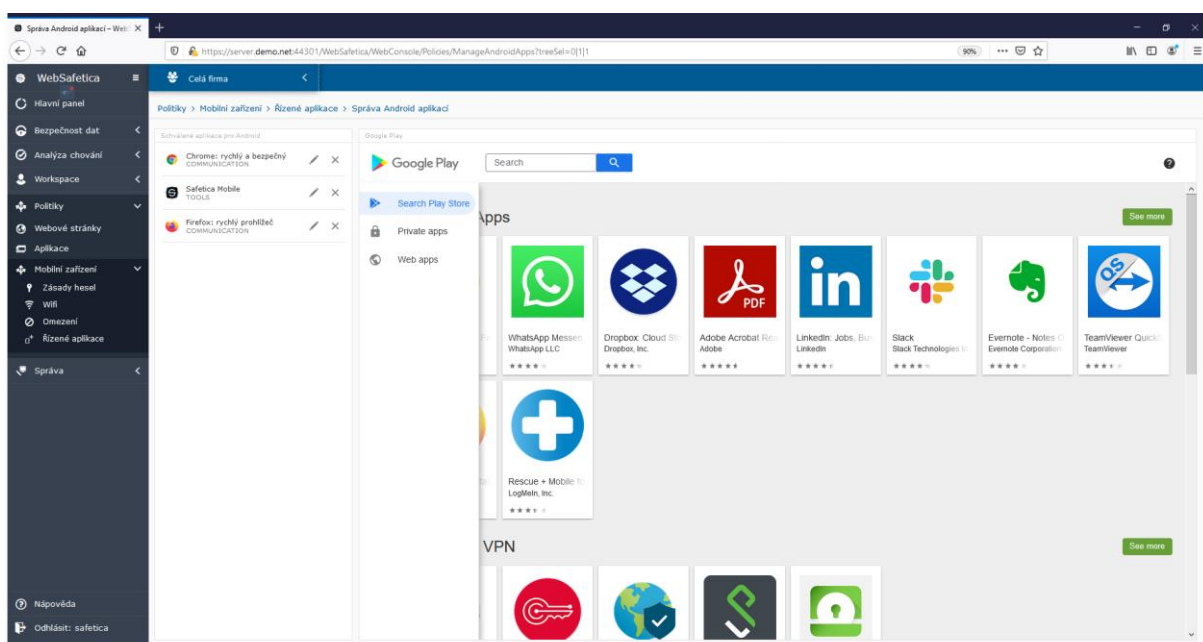
17.2.4. ŘÍZENÉ APLIKACE

Politika pro nastavení aplikací, které bude moci uživatel instalovat, nebo mu bude automatizovaně nainstalována.

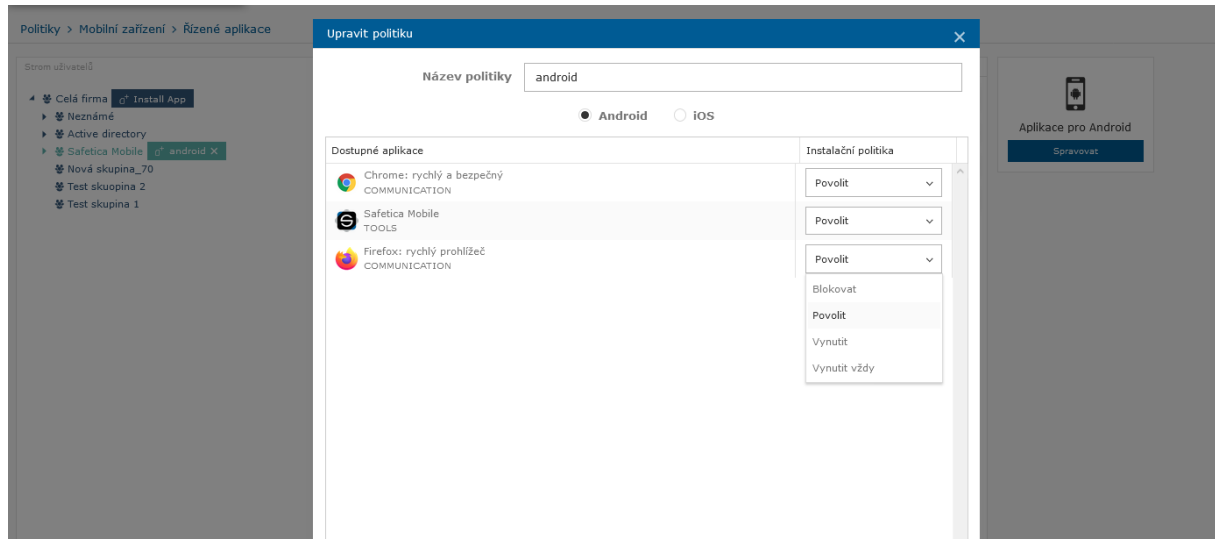


Správa aplikací pro Android s firemním profilem

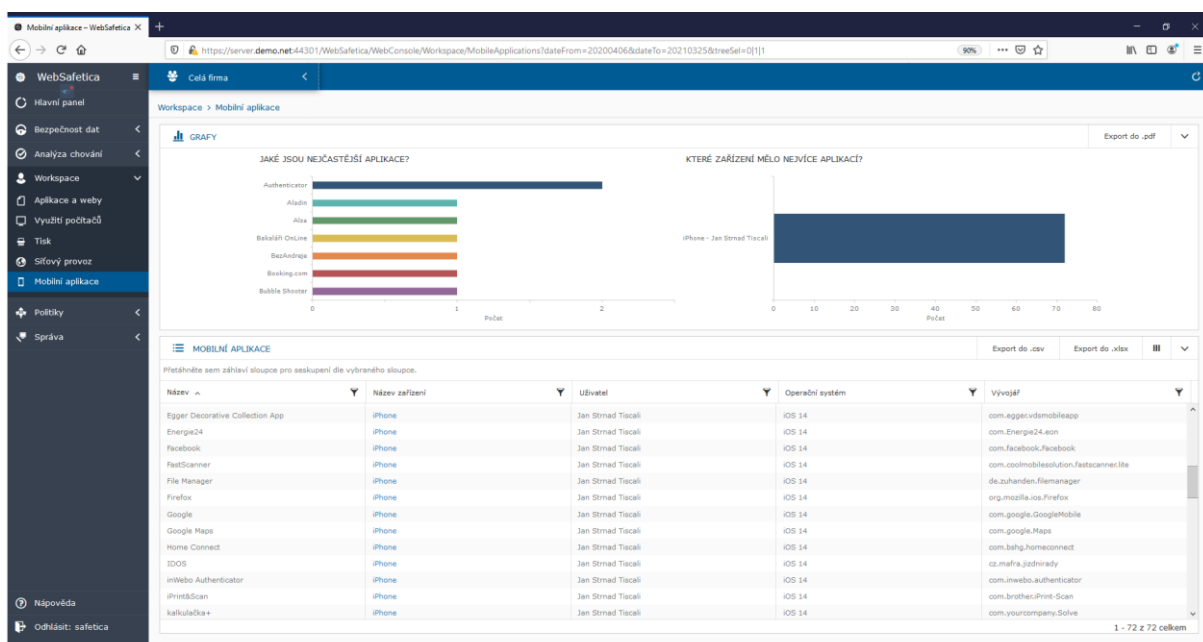
Systém umožňuje správci vybrat aplikace z Google Play, které bude moci uživatel ve svém firemním profilu používat.



Následně je možné v politice aplikací nastavit, zde bude tato aplikace uživateli dostupná a bude ji smět nainstalovat, nebo instalace aplikace bude vynucena a na mobilním zařízení se nainstaluje automaticky. Je možné i aplikace touto politikou blokovat.



Seznam instalovaných aplikací je možné sledovat ve Workspace / Mobilní aplikace



17.2.5. INTEGRACE SAFETICA MOBILE S ANDROID A IOS PROSTŘEDÍM

Safetica mobile využívá ke komunikaci a integraci aplikací nativní cloudové službu obou platforem – Google a Apple.

Před spuštěním vlastní správy mobilních zařízení je nutné zaregistrovat obě platformy do Safetica Mobile

NASTAVENÍ PRO SAFETICA MOBILE

Apple MDM Certificate:	Nakonfigurován. Expiruje března 17, 2022. obnovit
Android EMM:	Připojen jako jan.strnad72@gmail.com. odpojit
Povoleno audit souborů:	Ano
Rozšířit na osobní zařízení:	Ano
Funkce Nálada v týmu aktivní:	Ne

Apple MDM Certificate – konfigurace MDM certifikátu vůči platformě Apple

Detailní postup je zde:

<https://support.safetica.com/en/knowledge-base/safetica-mobile-configuration-apple-mdm-certificates>

Android EMM – napojení na platformu Android a Google Play – registrace organizace do Google portálu