AUTOCONT

Safetica Technologies

Produktová dokumentace
Safetica Discovery
Safetica Protection
Microsoft Bitlocker
Verze 9.9.x

Jan Strnad, AUTOCONT

OBSAH

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.

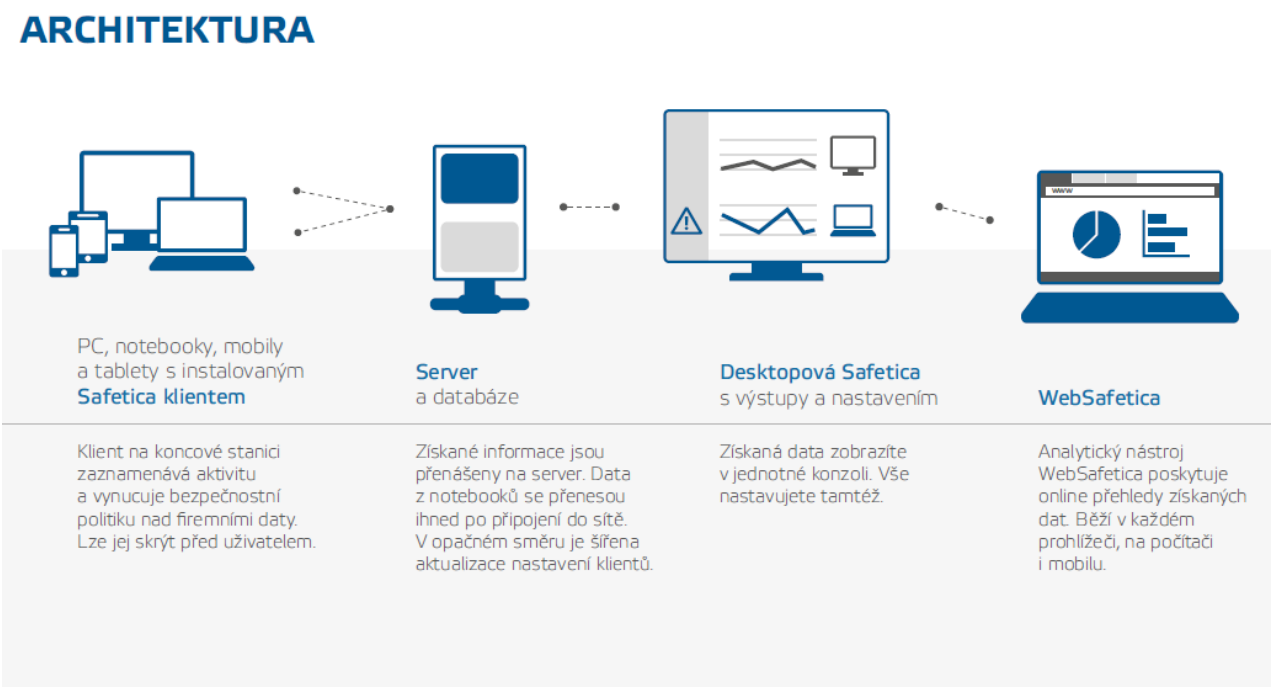
1.7. KONTROLA PŘIPOJOVANÝCH ZAŘÍZENÍ

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.

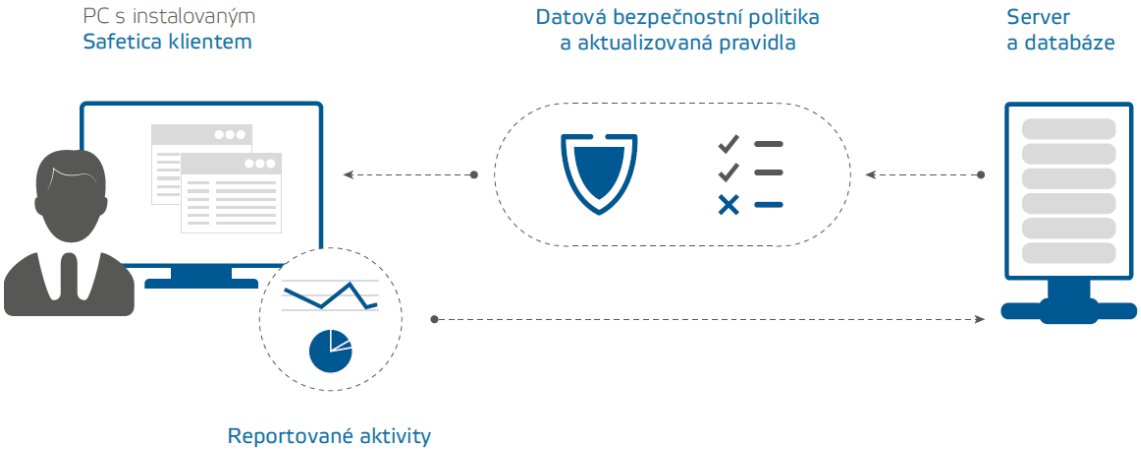


Komunikace klienta se serverem:

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 přeposílá. 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 umožnuje 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 počítacích, 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 součást Safetica pro správu Safetica klienta na koncových počítacích. Umožnuje 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 Agenta

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 vSphare 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, čí 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

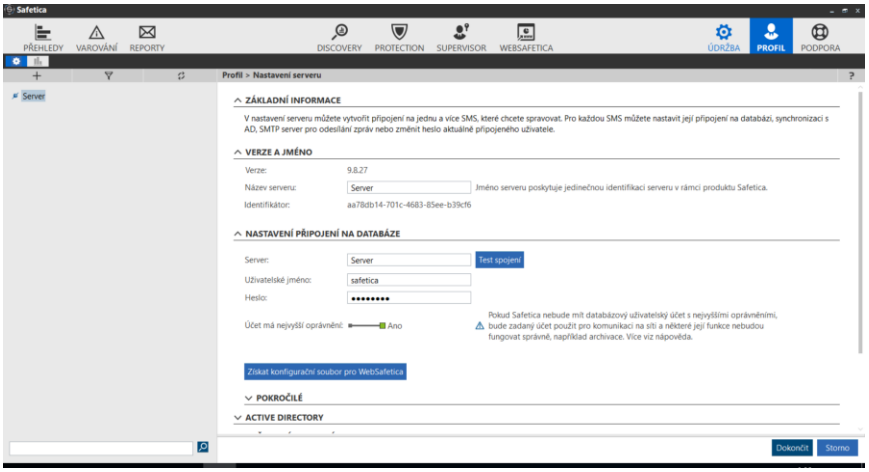
Instalace management konzole Safetica probíhá z instalačního balíku, který je dostupný na portále společnosti Safetica. Instalace obsahuje výše zmíněné komponenty, které je možné instalovat jako jeden celek v případě použití MS SQL Express, který je součástí instalačního balíčku.

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

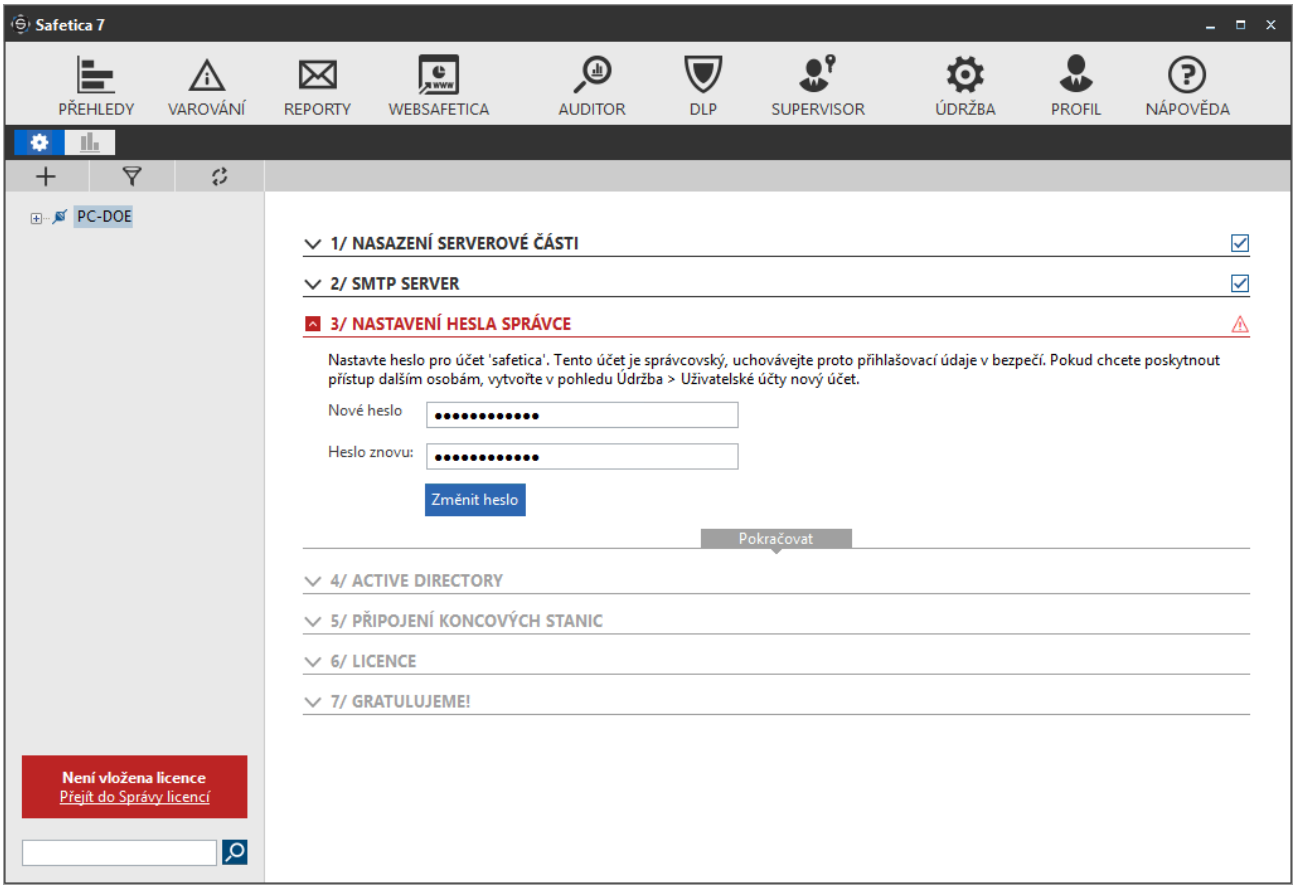
Safetica Web Console – instaluje komponenty do Microsoft IIS pro reporting a základní konfiguraci systému přes webový prohlížeč. Pro úspěšnou instalaci je nutné z management konzole získat konfigurační soubor pro připojení, na který se následně instalace Web konzole odkazuje. Konfigurační soubor je možné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

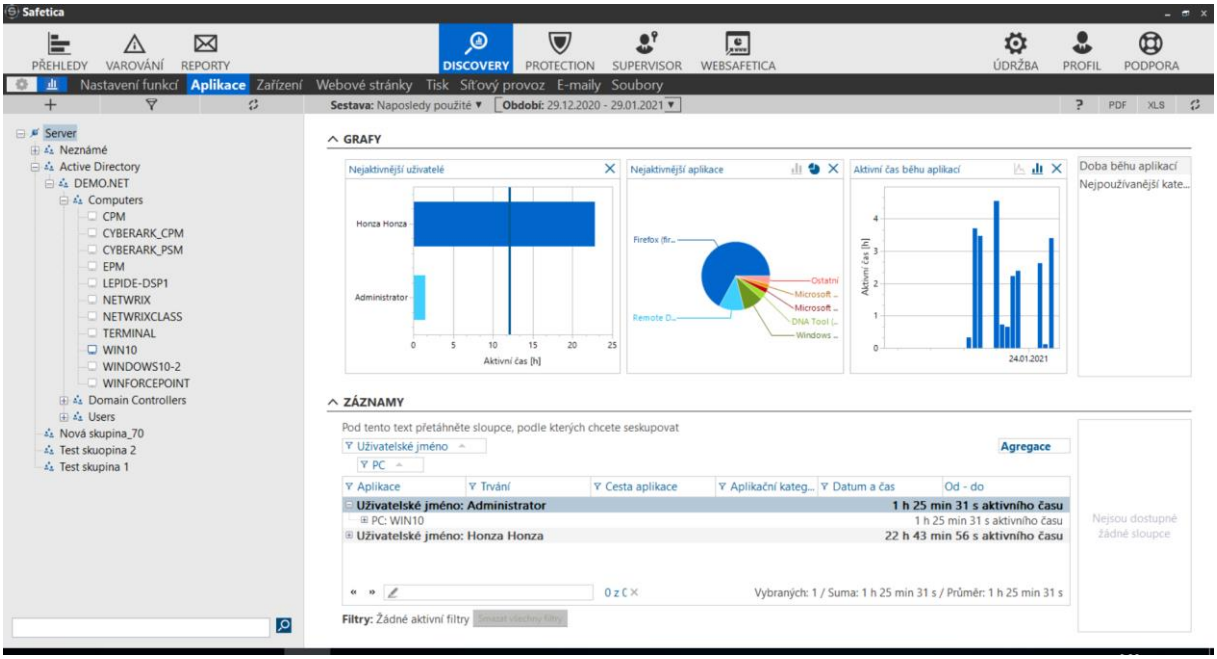
6. NASTAVENÍ DISCOVERY

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.

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

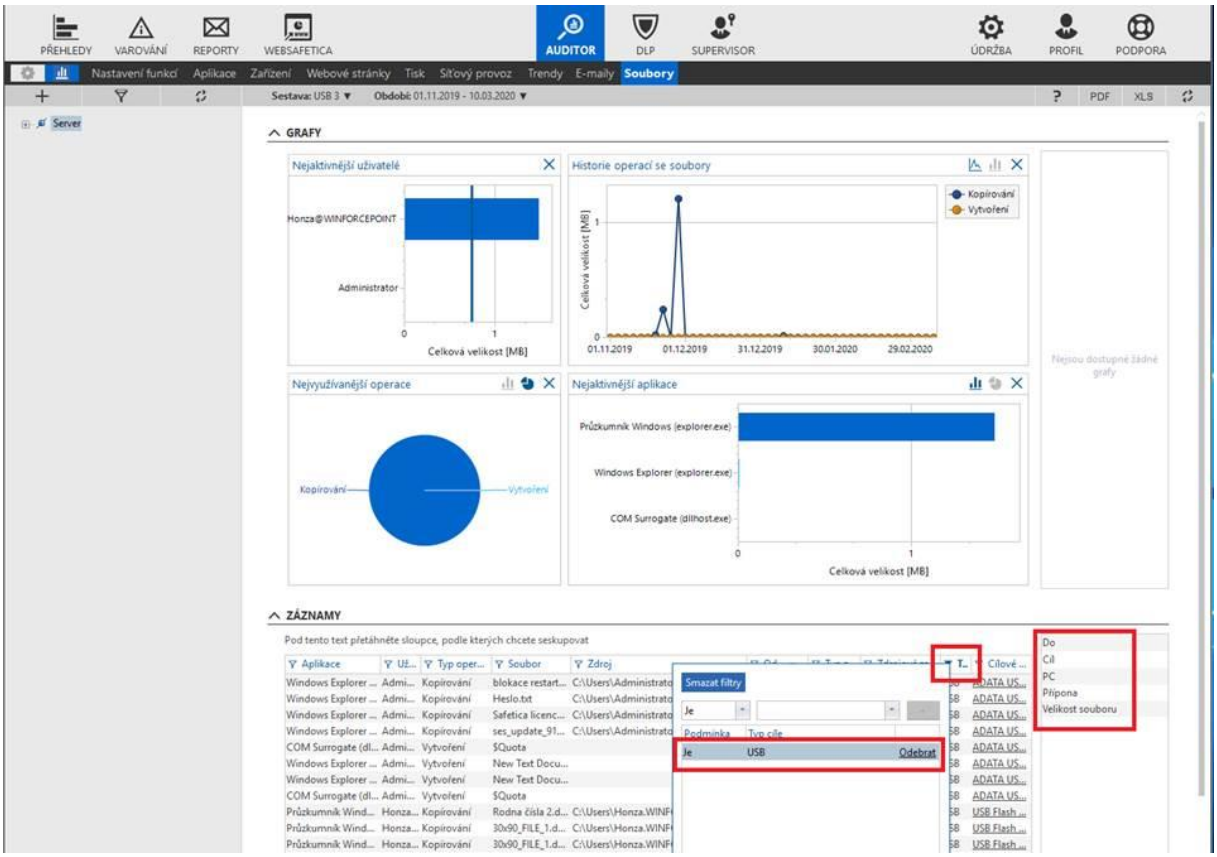
Poskytuje detailní přehled, odkud je jaké nastavení děděno a kde došlo k přerušení dědění.

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

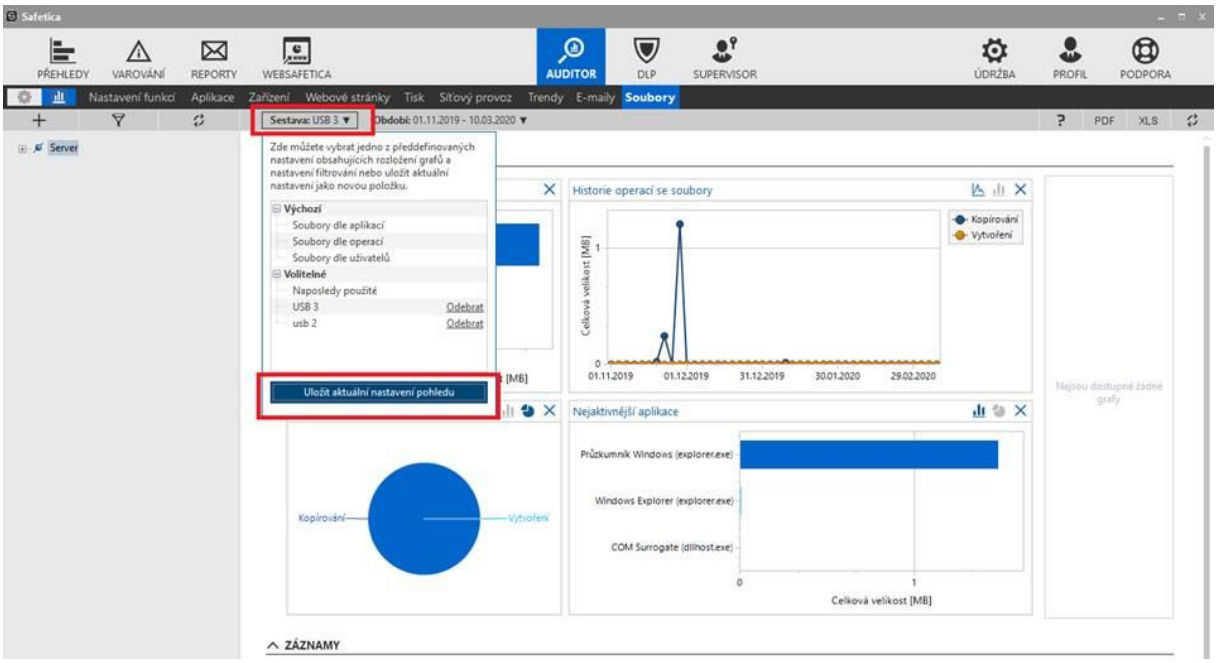
6.1. NASTAVENÍ A ULOŽENÍ FILTRŮ

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.

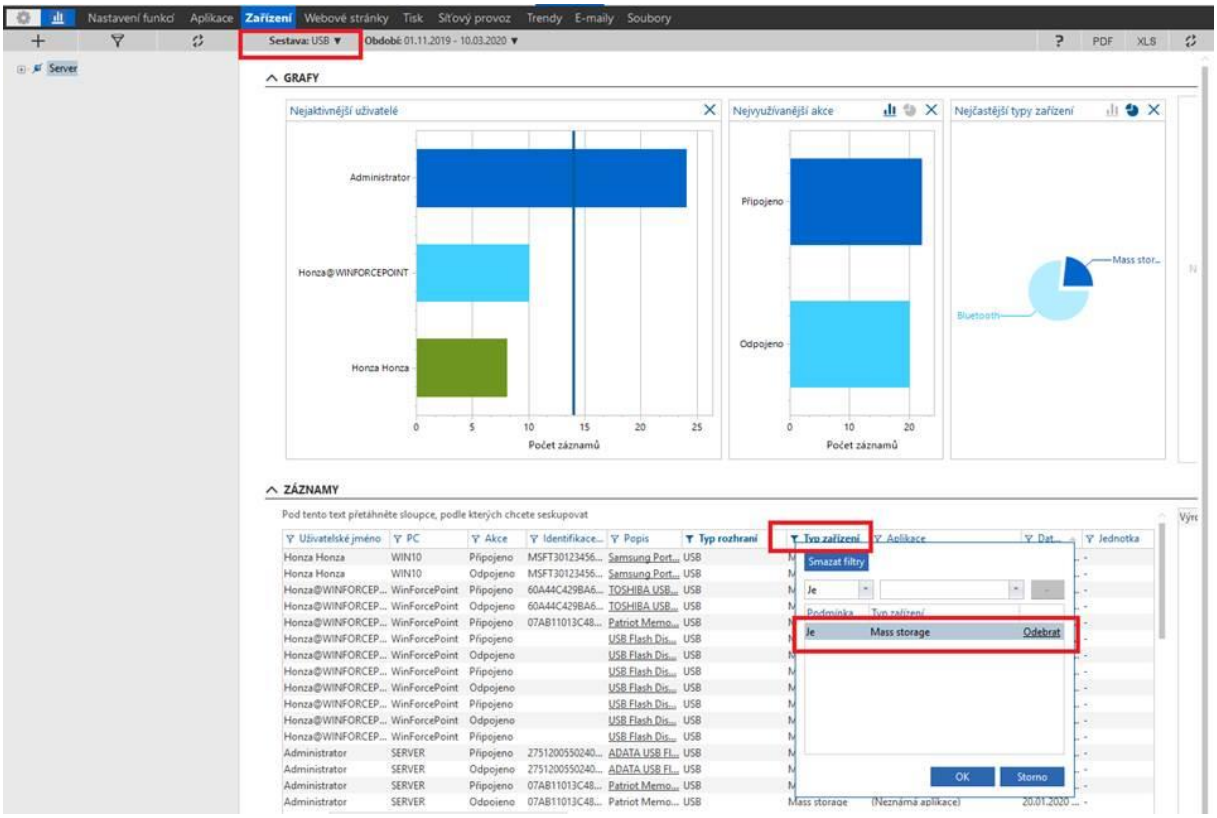
1. Je nutné v rámci správy vytvořit sestavu, ze které se bude generovat vlastní report – například práce se soubory na USB
   Zvolit si grafy, které se budou zobrazovat v reportu PDF a filtr na záznamy, které budou zobrazeny v XLS reportu



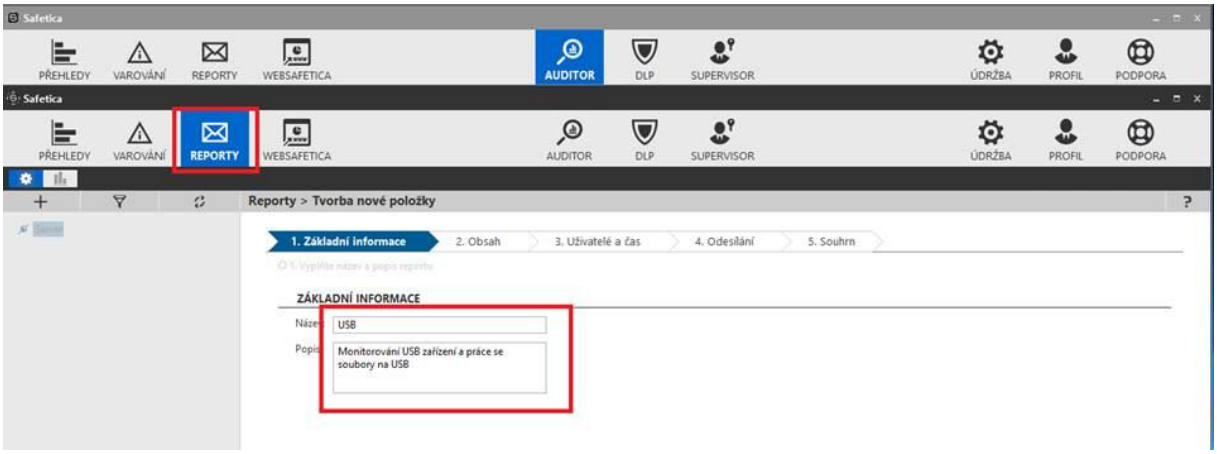
Následně sestavu uložit:



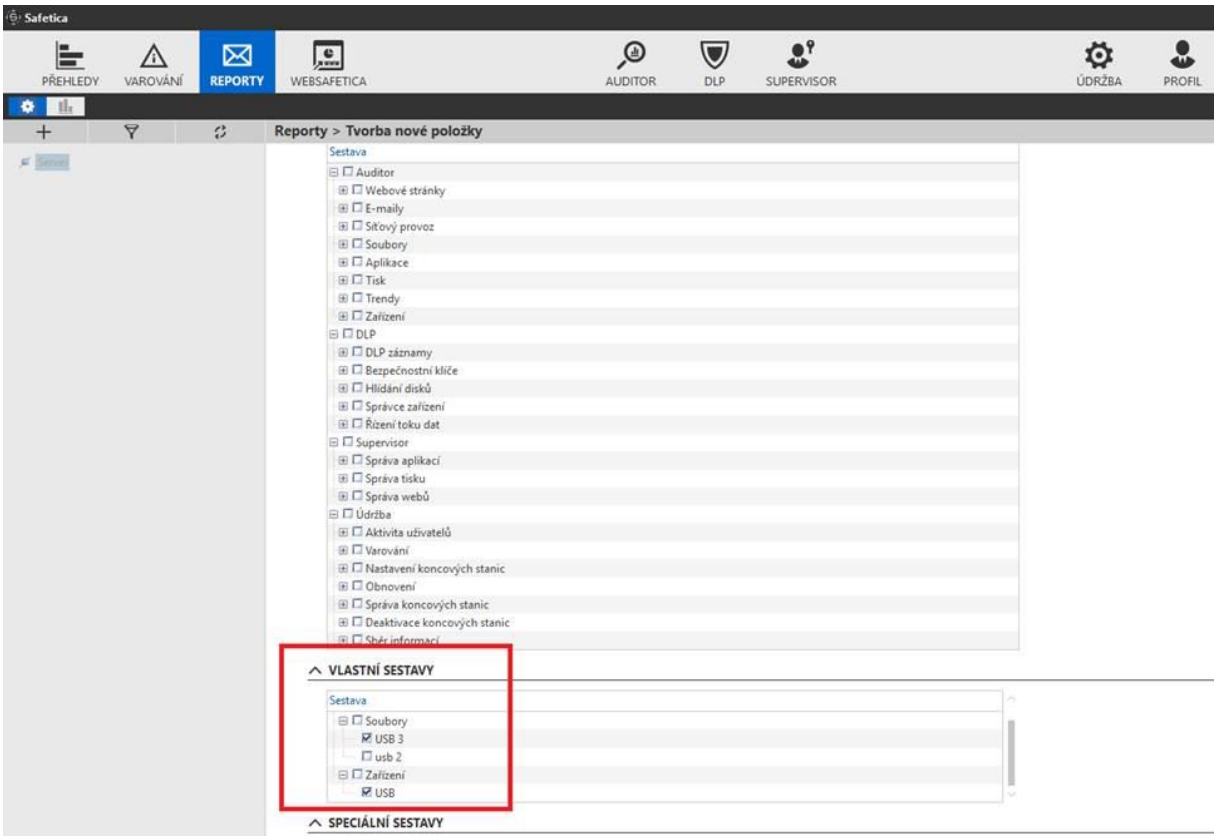
To samé je potřeba udělat pro reporty na zařízení:



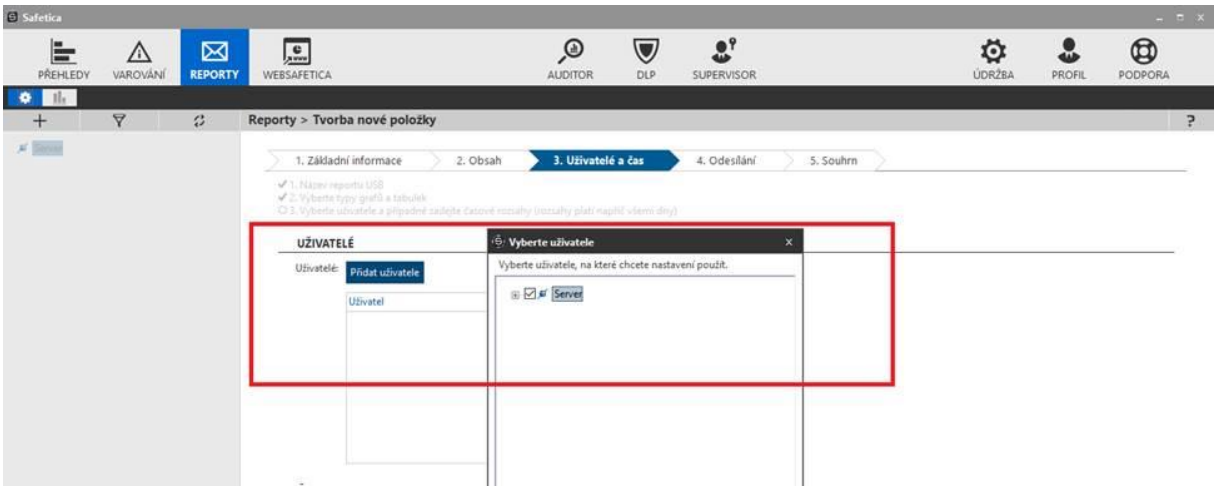
Nastavení reportů:



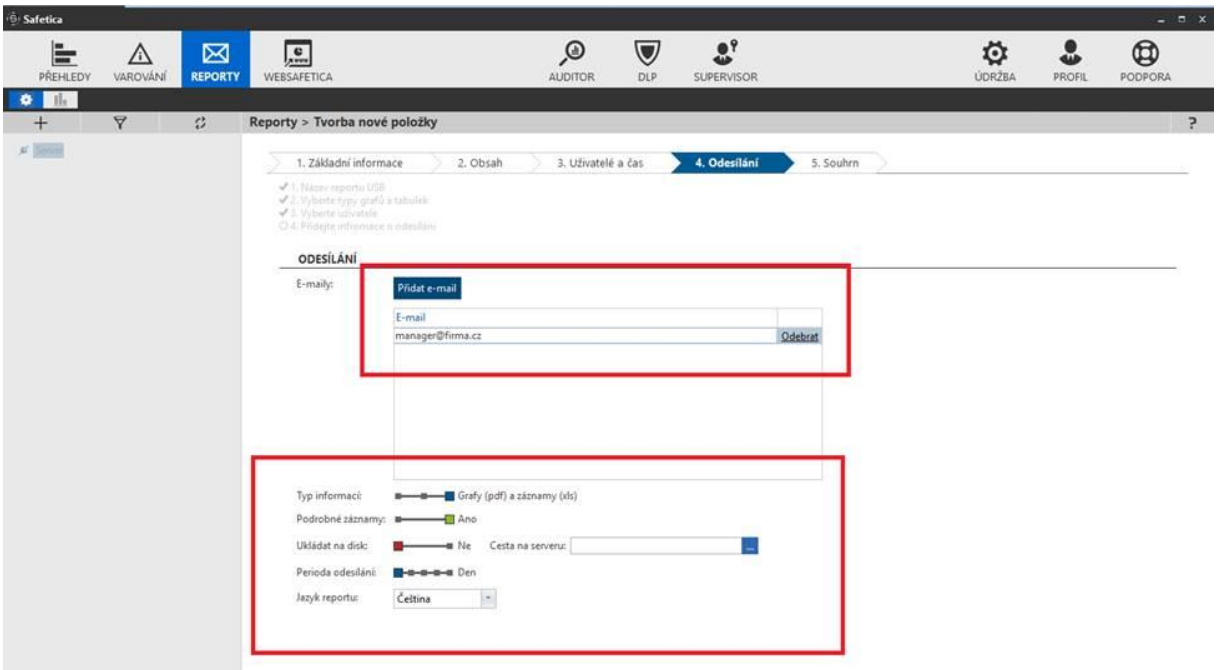
Vybrat vytvořené vlastní sestavy:



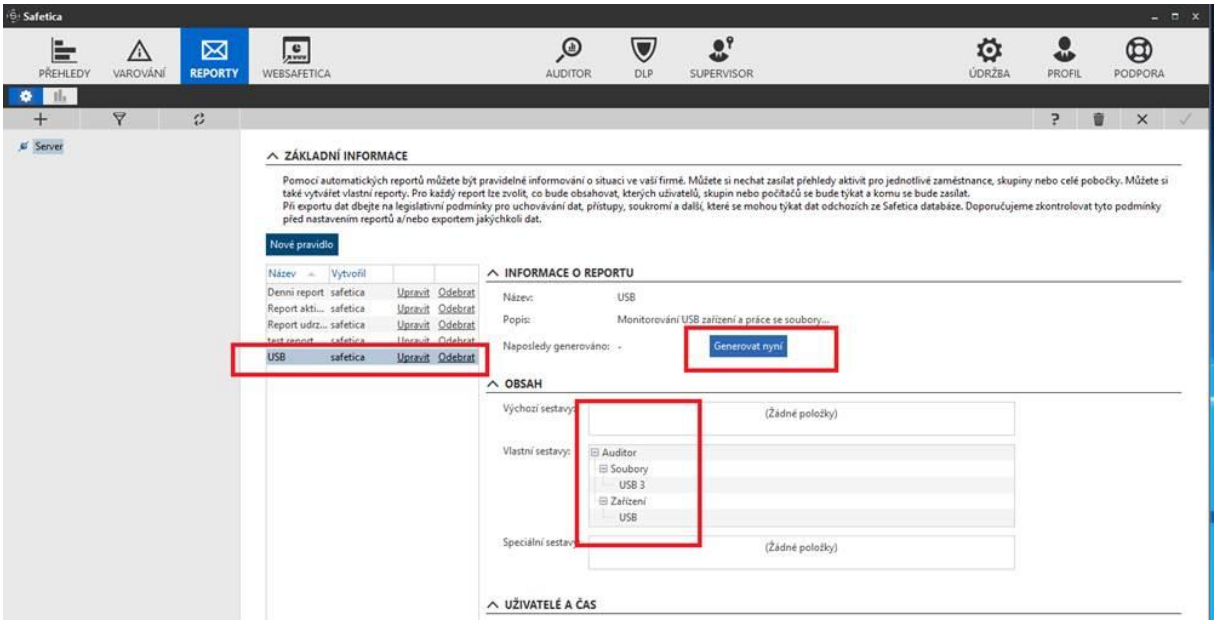
Vybrat uživatele/zařízení, pro které se bude generovat report:



Vybrat typ reportu a adresu příjemce:



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



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

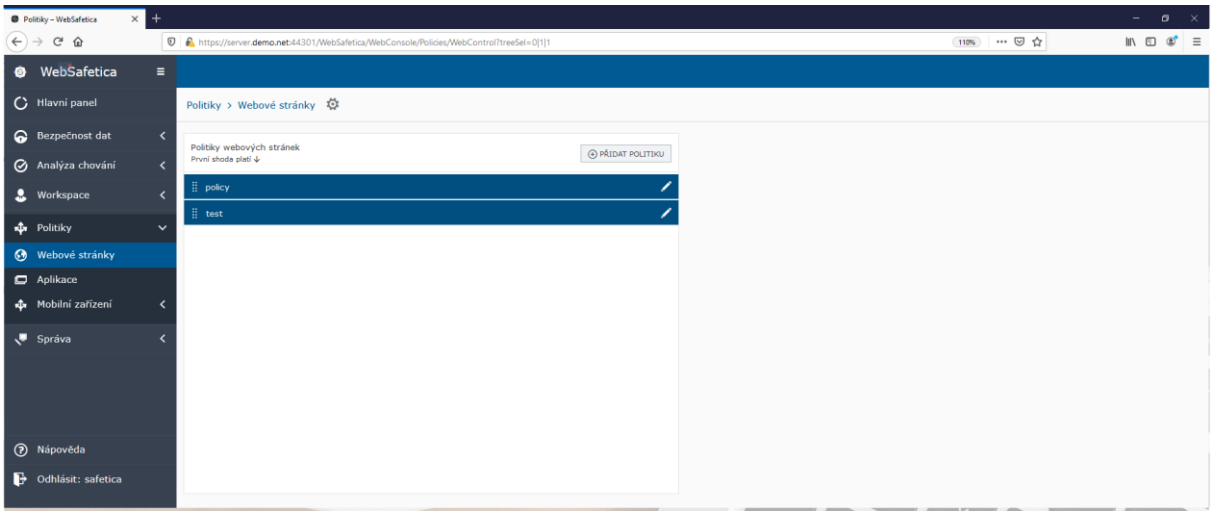
Supervizor je od verze Safetica 9.6 součástí Websafetica, není dostupný ve standardní konzoli Safetica.

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 blokované.

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

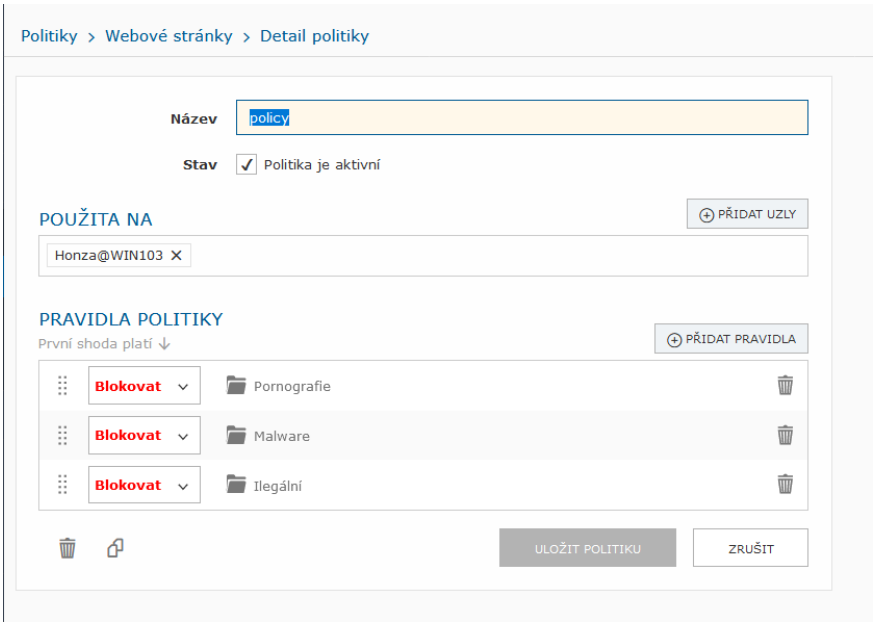
Ukázka konzole pro nastavení URL filtru:



Doporučené nastavení blokace webových stránek

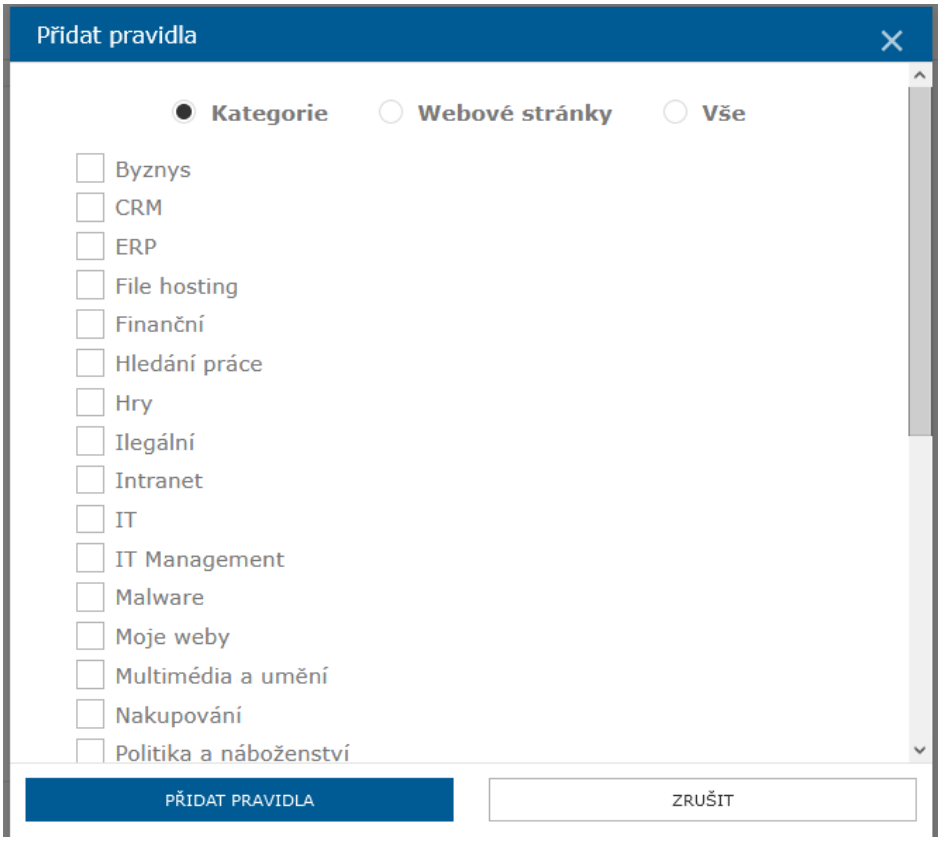
- Games – blokování herních webových stránek
- Illeagal – blokování nelegálních webových stránek
- Malware – blokování webových stánek s malware
- Pornography – blokování webových stránek s pornografickým materiálem
- Proxy web – blokování využívání proxy serverů

Ukázka nastavení politiky blokace webových stránek:

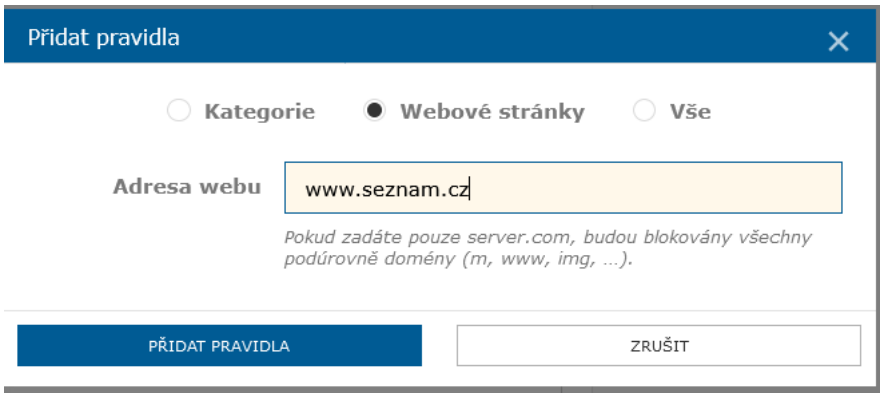


Pomocí tlačítka Přidat pravidla je možné přidat další kategorie nebo URL adresy, která budou pomocí politiky blokována. V rámci definice pravidla je možné přidávat jak konkrétní URL adresy, tak přednastavené kategorie od výrobce.

Definice kategorií webových stránek



Příklad manuálního přidání URL adresy:



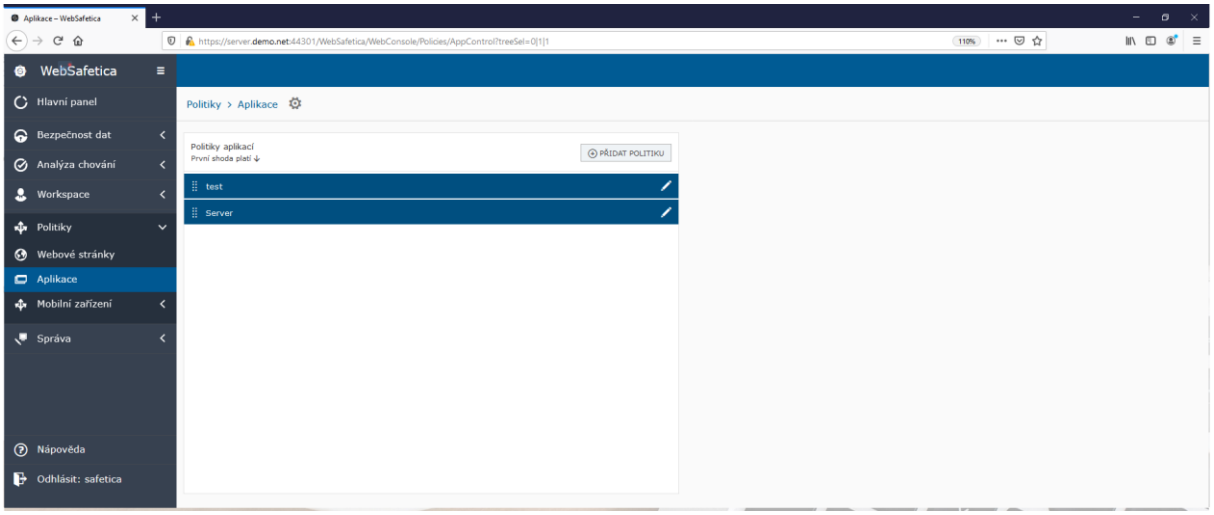
Nastavení Správy Webů je možné kdykoliv rozšířit o další kategorie, nebo definovat své vlastní kategorie s webových serverů, které budou povoleny nebo zakázány.

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 spouštěné 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.

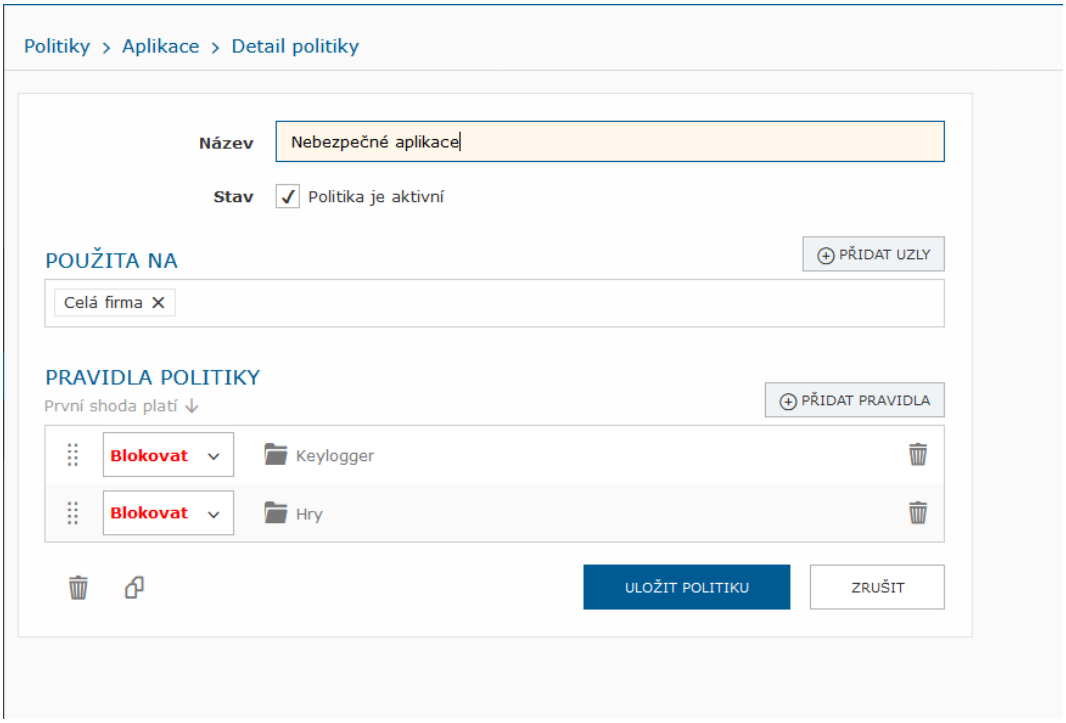


V rámci nasazení je možné využít přednastavené politiky pro blokaci závadný aplikací, nebo vytvořit vlastní politiku.

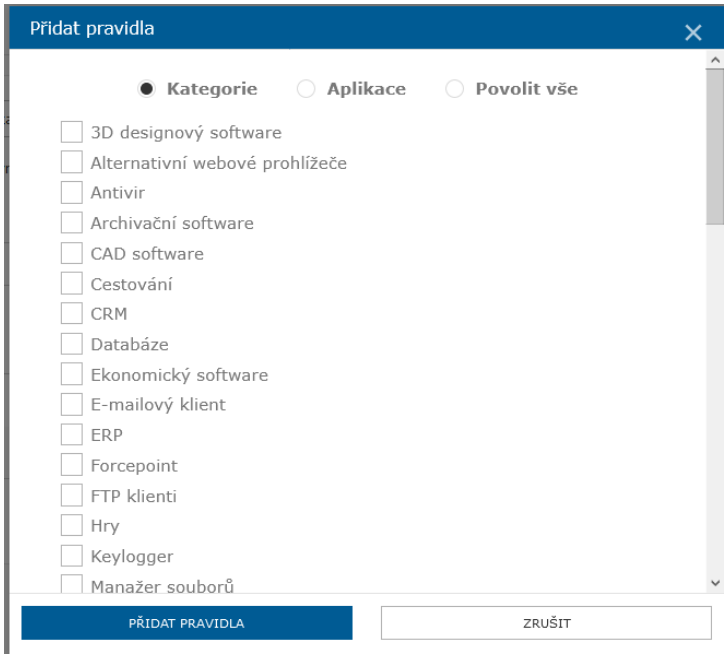
Doporučeno je blokovat tyto aplikační kategorie:

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

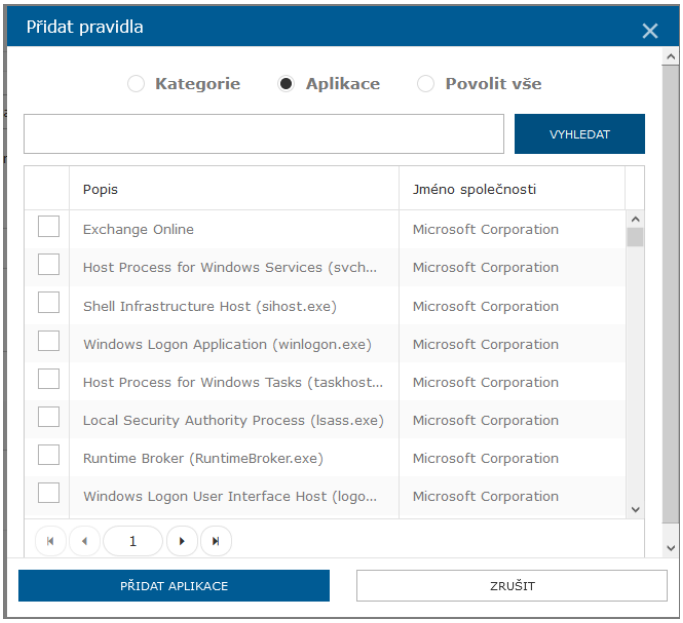
Nastavení politky pro blokaci aplikací



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

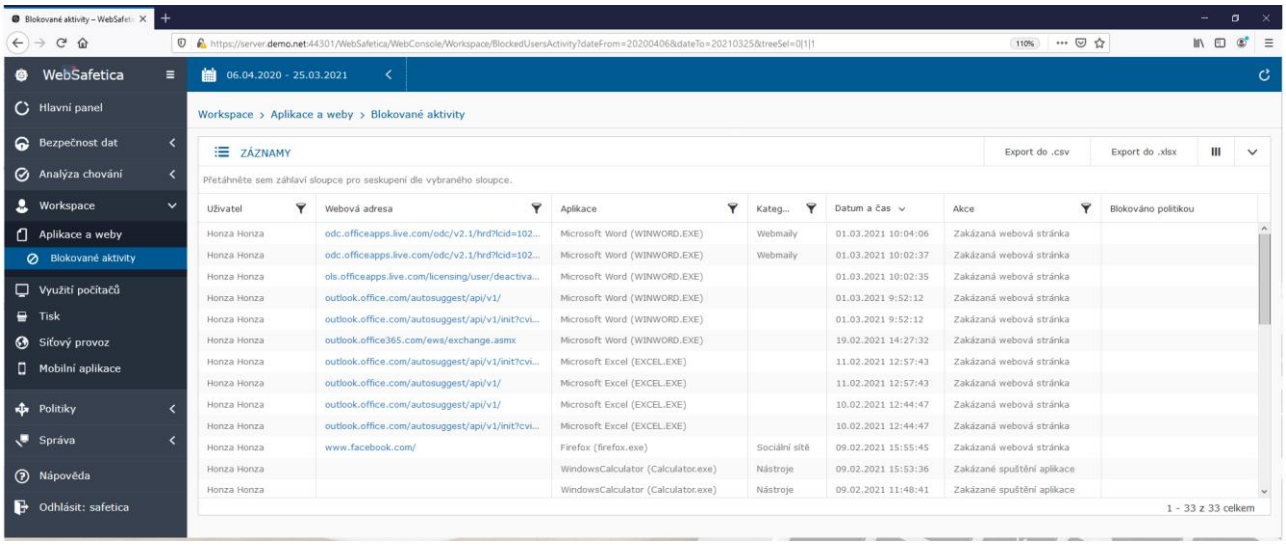


Nebo je možné zvolit aplikace ze seznamu načtených aplikací pomocí Discovery modulu



7.3. REPORTOVÁNÍ BLOKOVANÝCH WEBŮ A APLIKACÍ

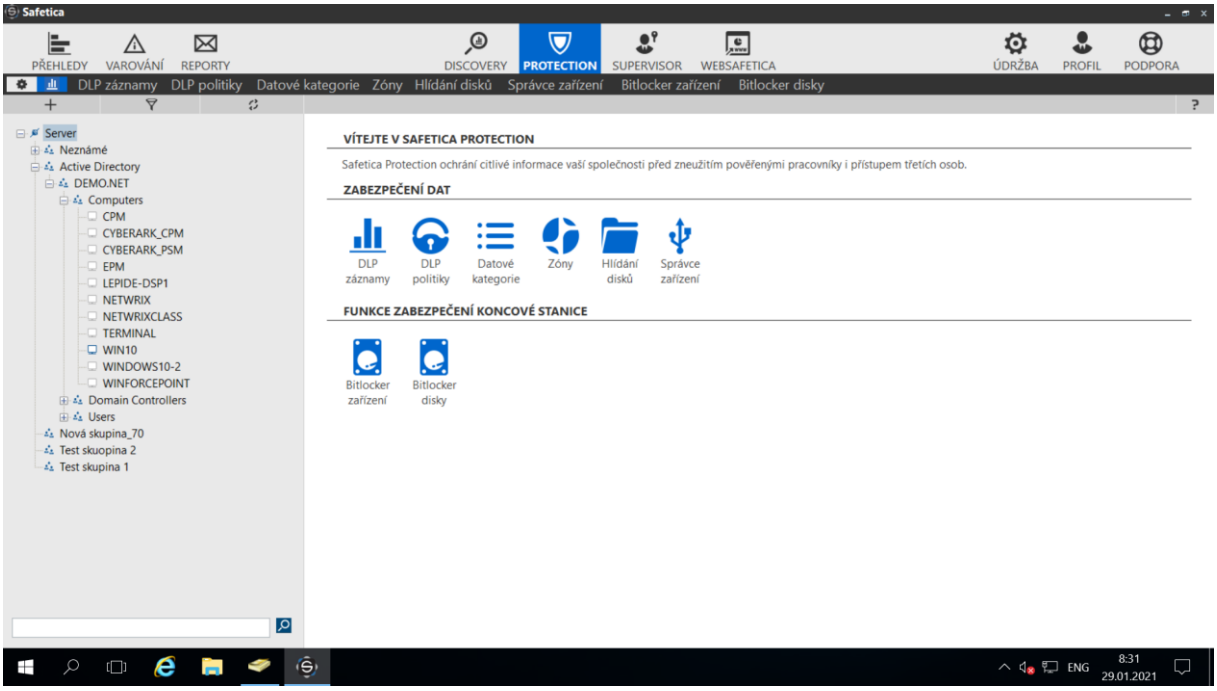
Události o blokovaném přístupu na webové stánky, nebo blokované aplikace jsou následně zobrazovány ve Websafetica konzoli Workspace / Aplikace a Weby / Blokované aktivity



8. NASTAVENÍ PROTECTION (DLP)

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

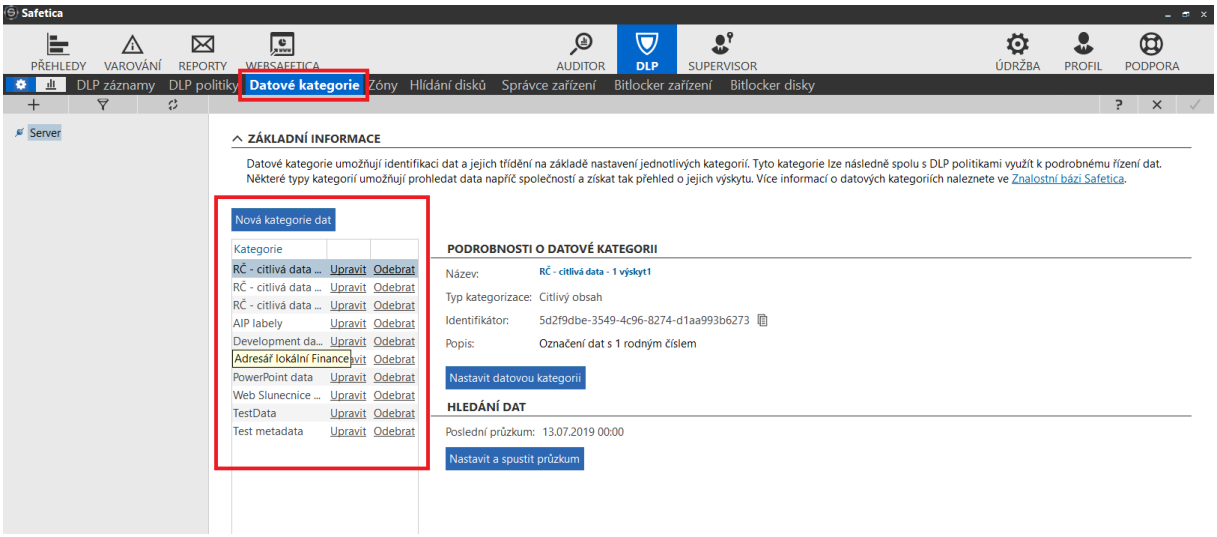
DLP je nejobsáhlejší část Safetica řešení. Umožňuje nastavení klasifikace dat a následná pravidla pro monitoring a blokaci citlivých údajů nebo klasifikovaných souborů.



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.

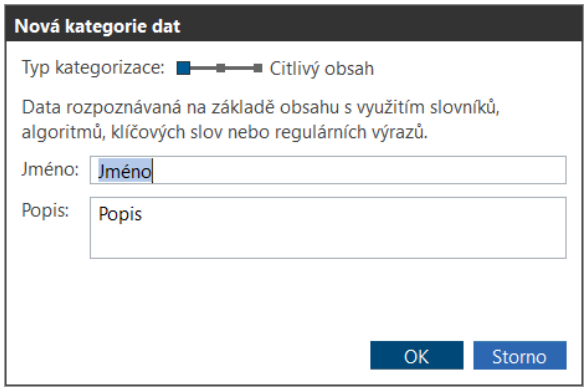


Klasifikaci dat v DLP Safetica je možné provádět několika způsoby.

- **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.



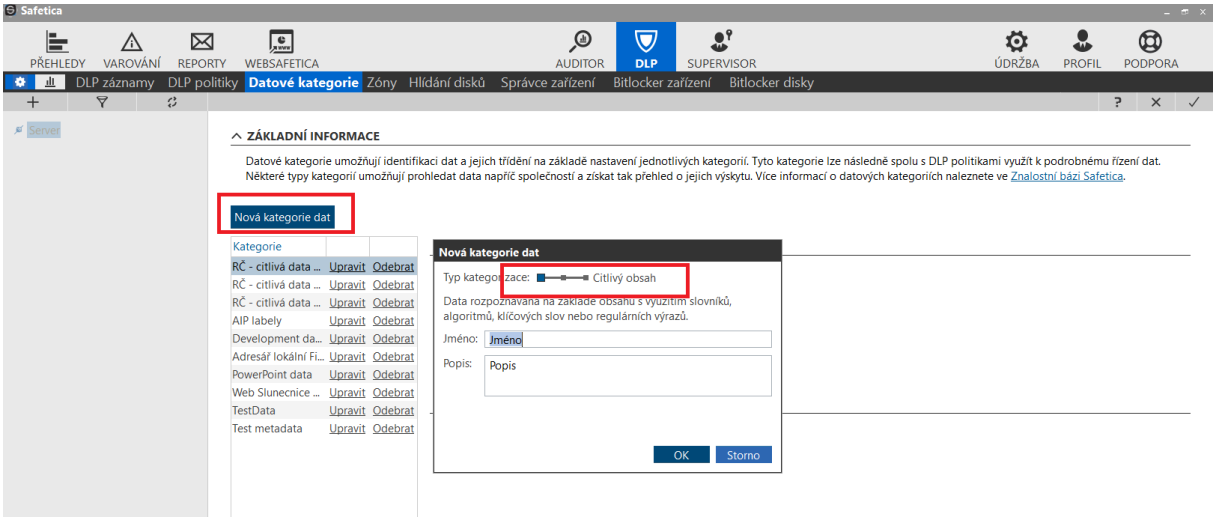
Je možné definovat pro každou definici samostatné pravidlo, nebo je možné kombinovat klasifikátory například data vytvořená aplikací a uložena na definované úložiště.

8.1.1. OBSAHOVÁ KLASIFIKACE DAT

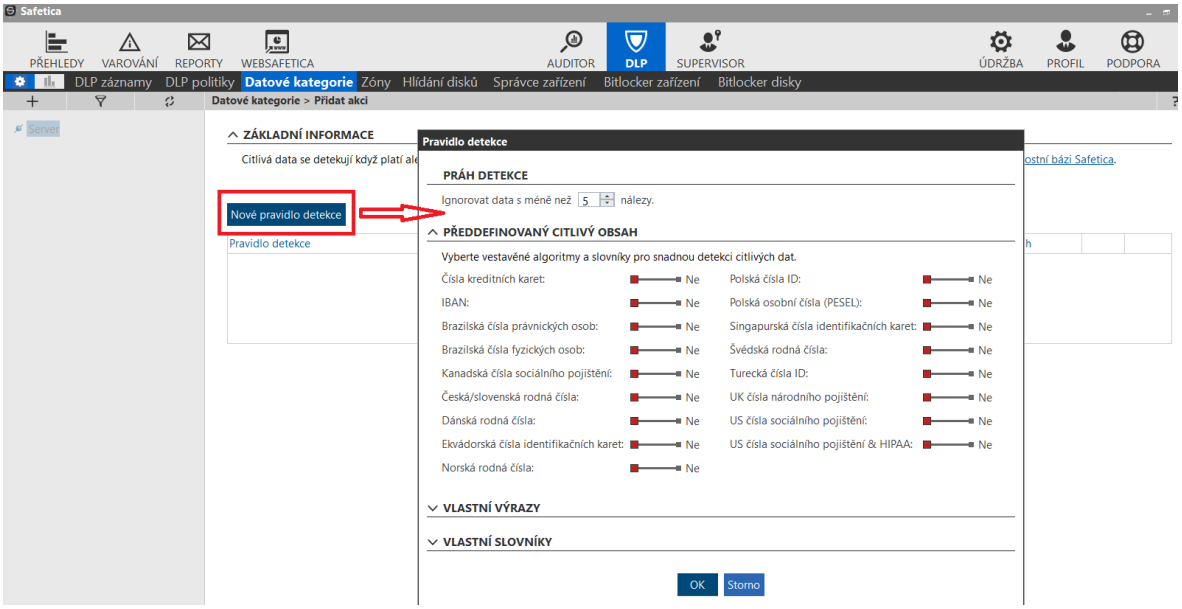
Umožňuje definovat slova nebo RegEx výrazy, které jsou citlivé.

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

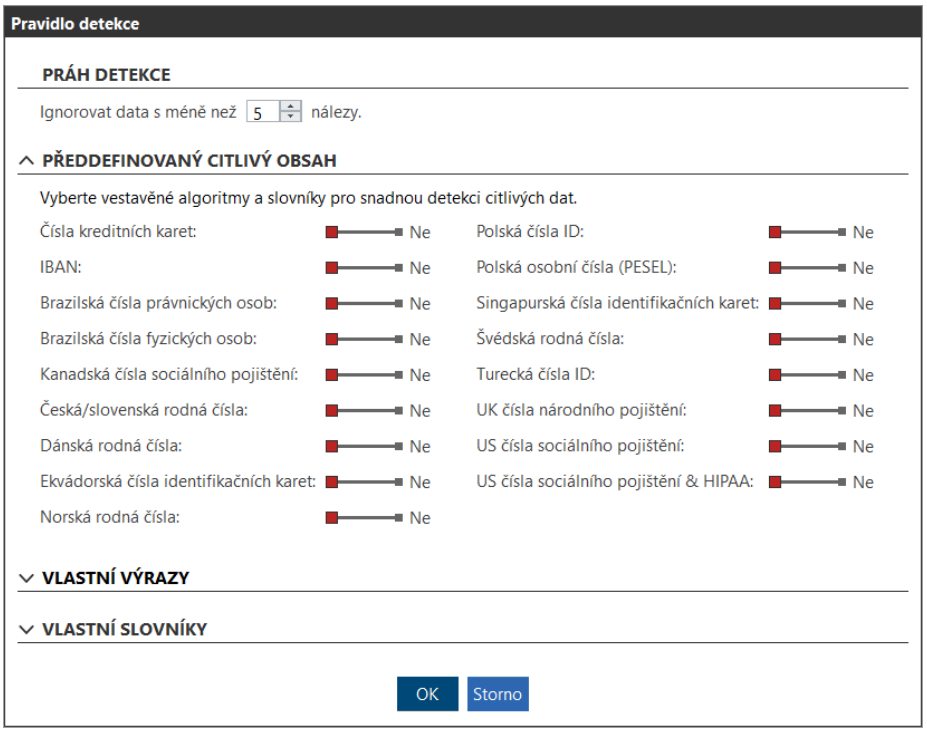
Příklad vytvoření nového klasifikačního pravidla pro citlivá data:



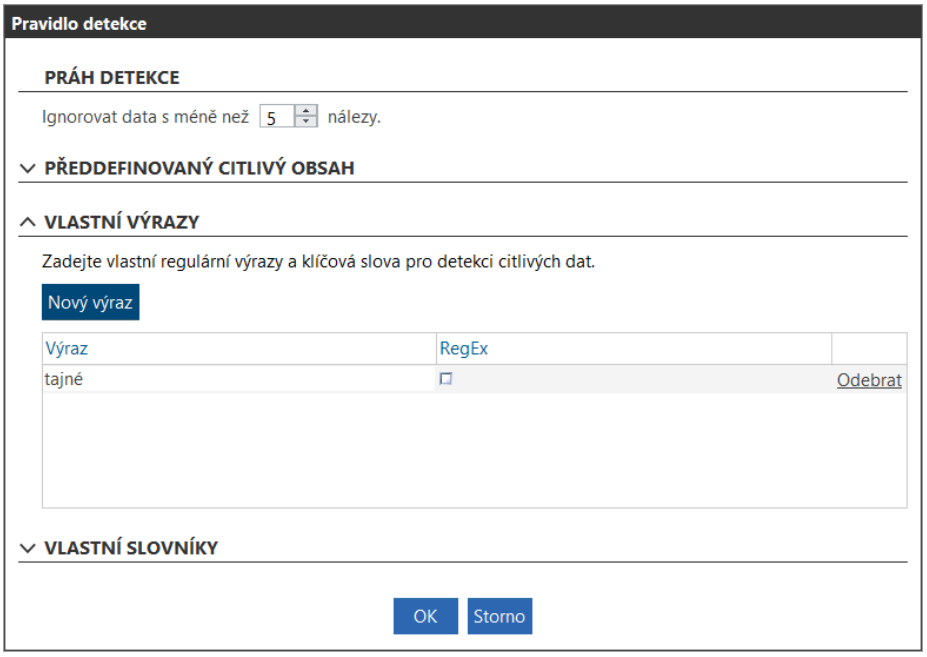
Definice pravidla pro citlivá data. Pomocí tlačítka „Nová kategorie dat“ je možné přidat nové pravidlo. Pravidla detekce je možné skládat, mezi pravidly platí operand „OR“.



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 5 nálezy.
PŘEDDEFINOVANÝ CITLIVÝ OBSAH
VLASTNÍ VÝRAZY
Zadejte vlastní regulární výrazy a klíčová slova pro detekci citlivých dat.
Nový výraz
Výraz
RegEx
tajné
Odebrat
VLASTNÍ SLOVNÍKY
OK
Storno

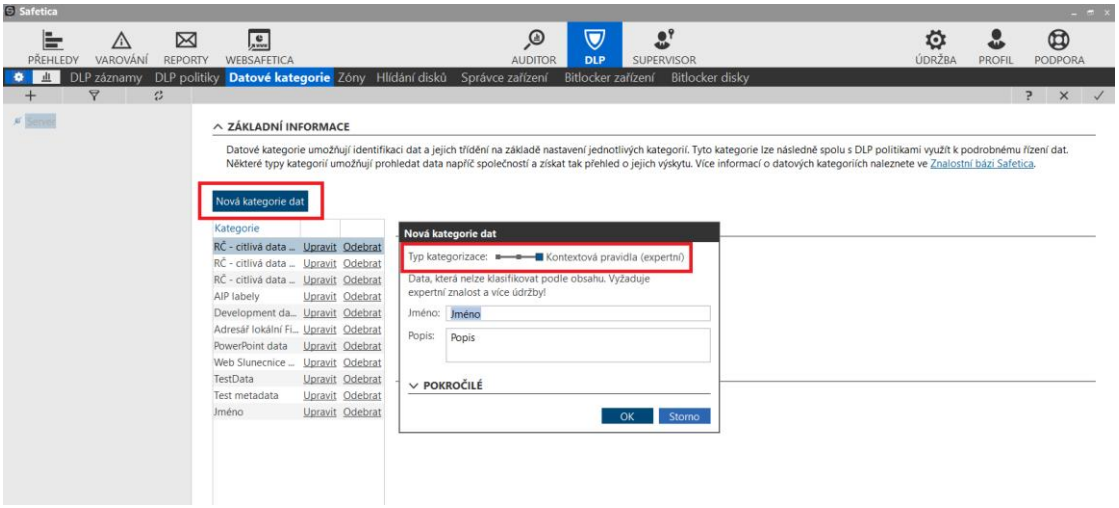
8.1.2. KONTEXTOVÁ KLASIFIKACE DAT

Kontextová klasifikace označuje soubory tagem na úložištích. Tag je uložen v extended atributech NTFS partition.

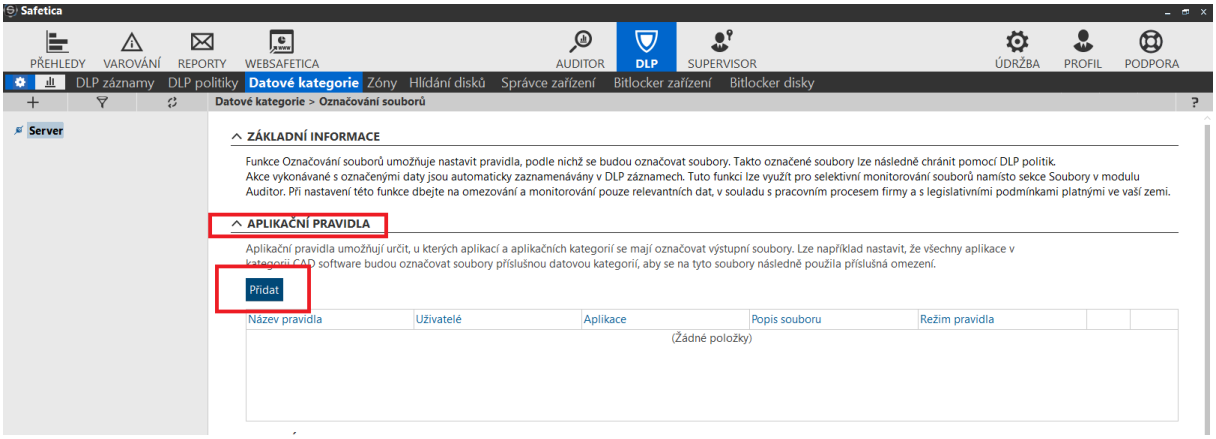
Kontextová klasifikace umožňují klasifikovat data na základě pravidel:

- 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 úložištích – lokální nebo sdílené adresáře/disky

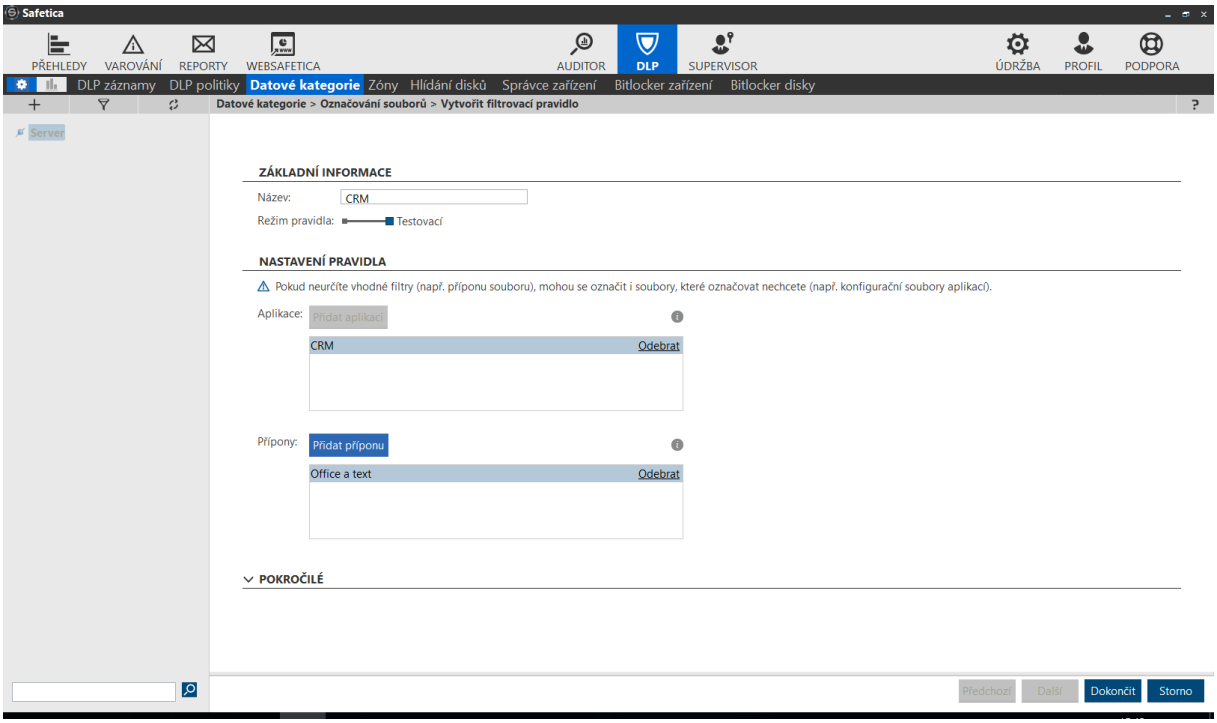
Příklad vytvoření kontextové klasifikace:



8.1.2.1 Nastavení aplikačního pravidla:



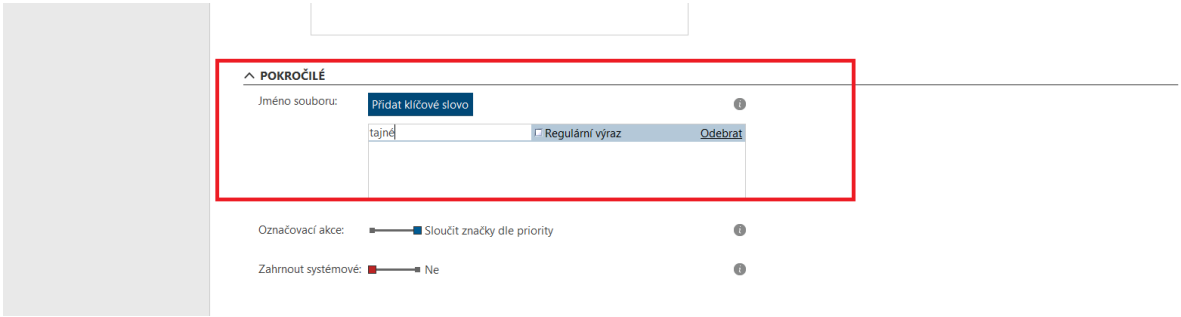
Definice aplikačního pravidla – výběr aplikace a souborů ,které budou klasifikovány tagem. Příklad – aplikace skupiny CRM a soubory s příponami Office a text:



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

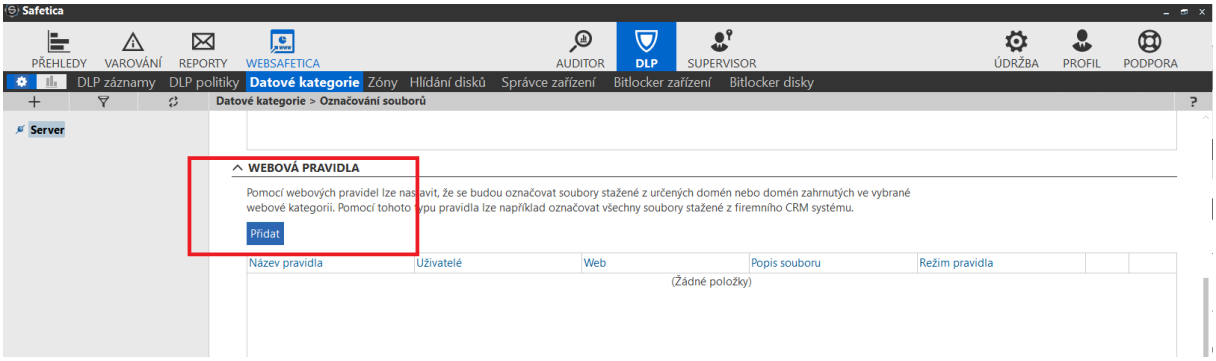
Klasifikaci dat je možné rozšířit a pokročilé nastavení, kde je možné definovat obsah, který bude při klasifikaci vyhledáván v souborech.



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 „tajné“.

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

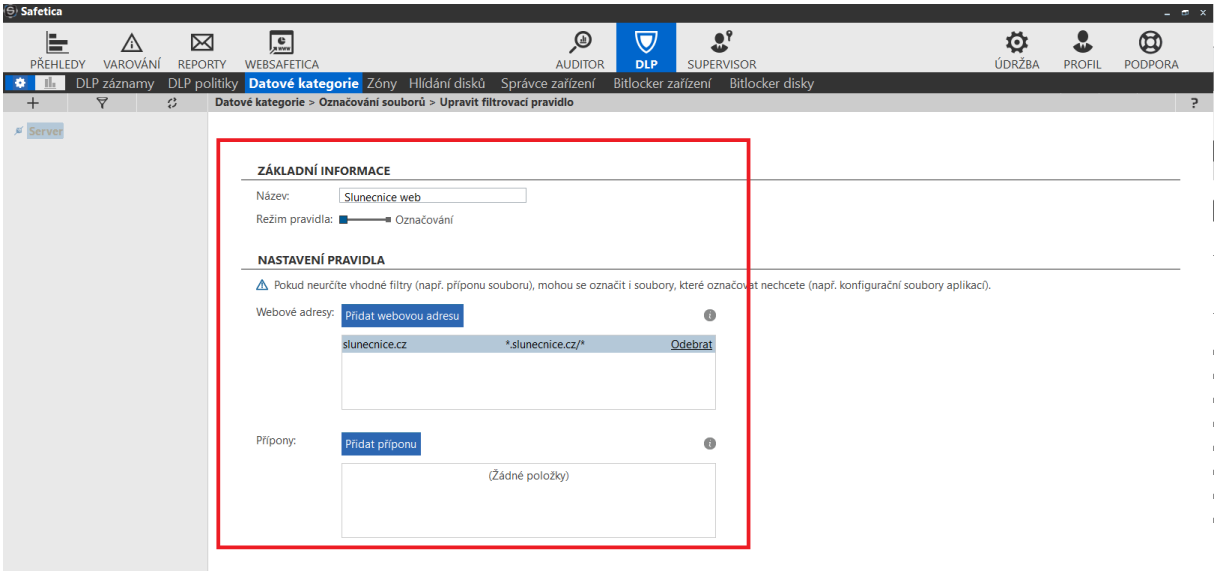
8.1.2.2 Nastavení webového pravidla



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.

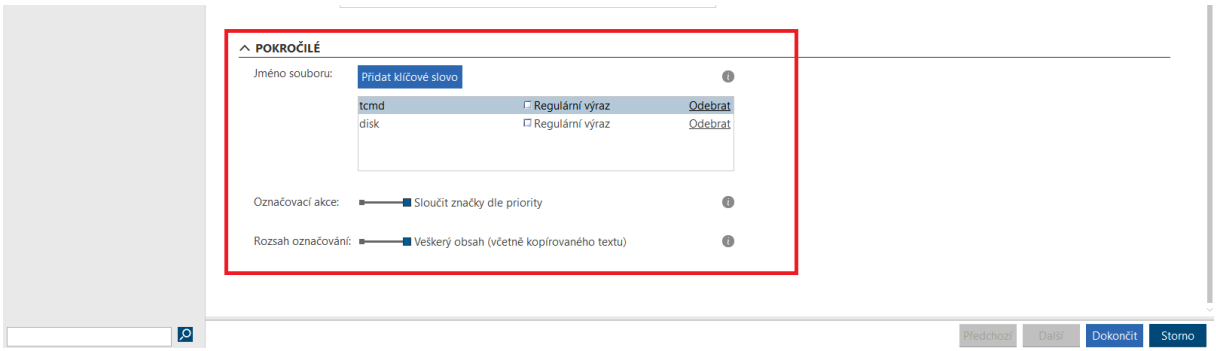
Soubory stažené z definované URL adresy s definovanou příponou budou označeny kontextovou značkou.



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

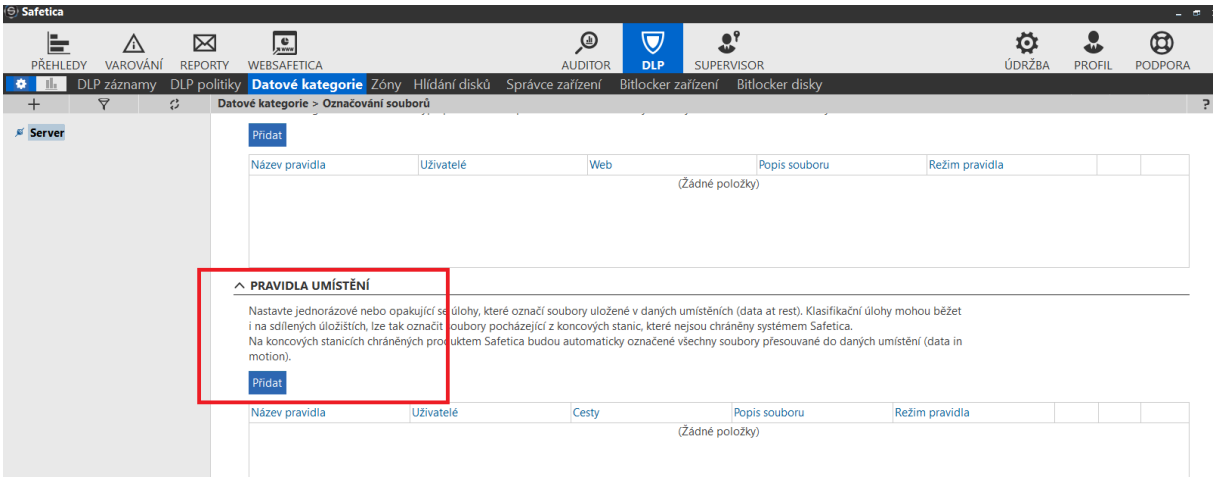
Klasifikaci dat je možné rozšířit a pokročilé nastavení, kde je možné definovat obsah, který bude při klasifikaci vyhledáván v souborech.



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.

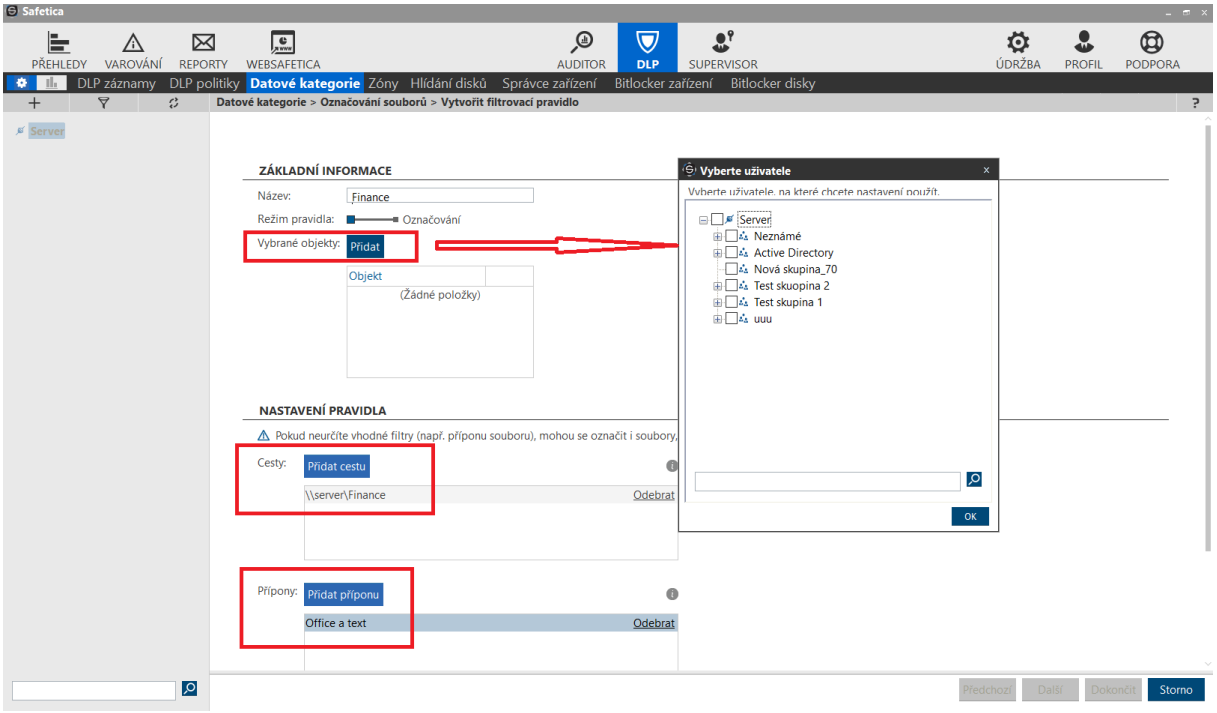
8.1.2.3 Nastavení pravidla umístění



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

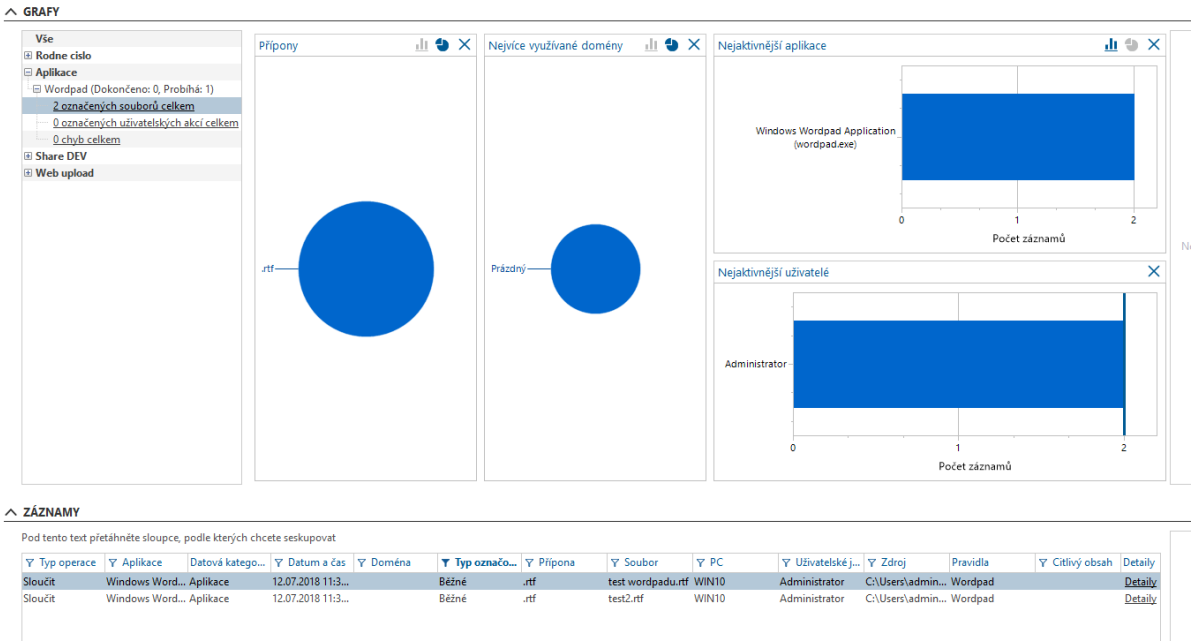
8.1.3. VIZUALIZACE ZOBRAZUJE VÝSLEDEK KLASIFIKACE DAT:

Vizualizace zobrazuje stav označování dokumentů.

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

- Aplikační pravidla
- Webová pravidla
- Pravidla umístění

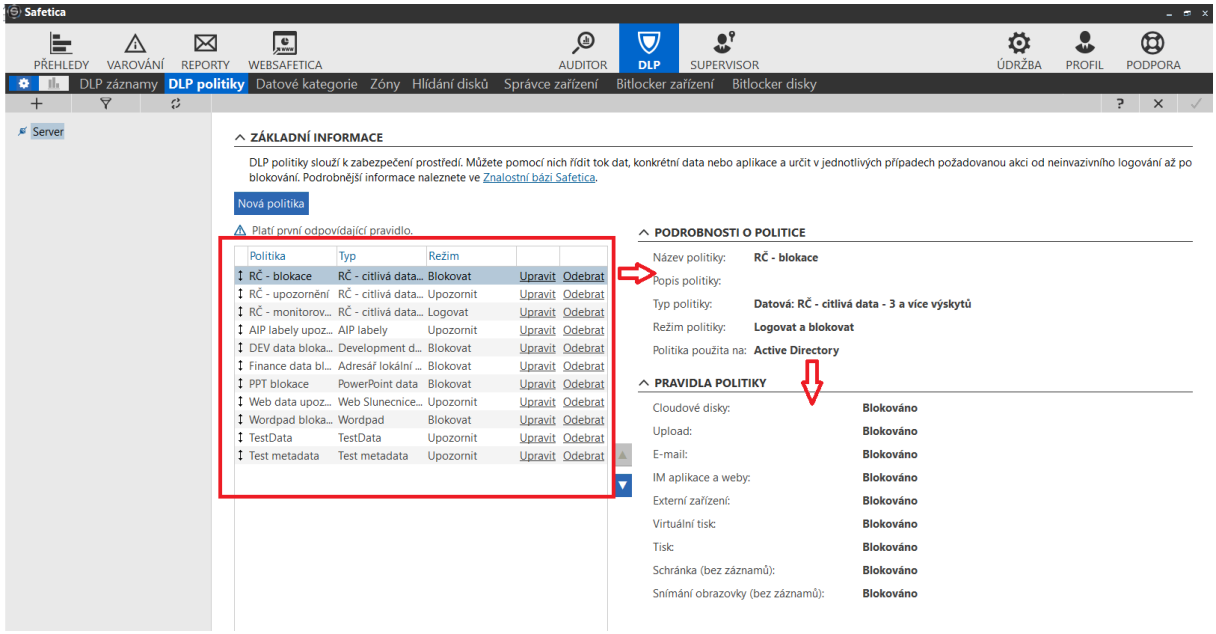
Citlivá data v seznamu nejsou – neoznačují se tagem, ale v případě detekce citlivého obsahu ve zpracovávaných datech si značku udržuje DLP enfine v operační paměti a není uložena se souborem.



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.



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.

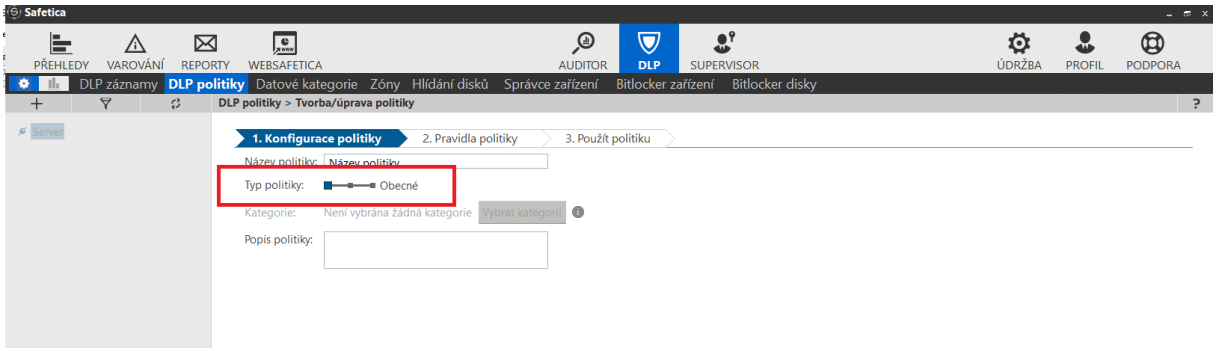
Obecné politiky jsou vhodné pro nastavení všeobecných podmínek toho, co je a co není povoleno, a je nejlepší je zařadit na konec seznamu DLP politik.

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

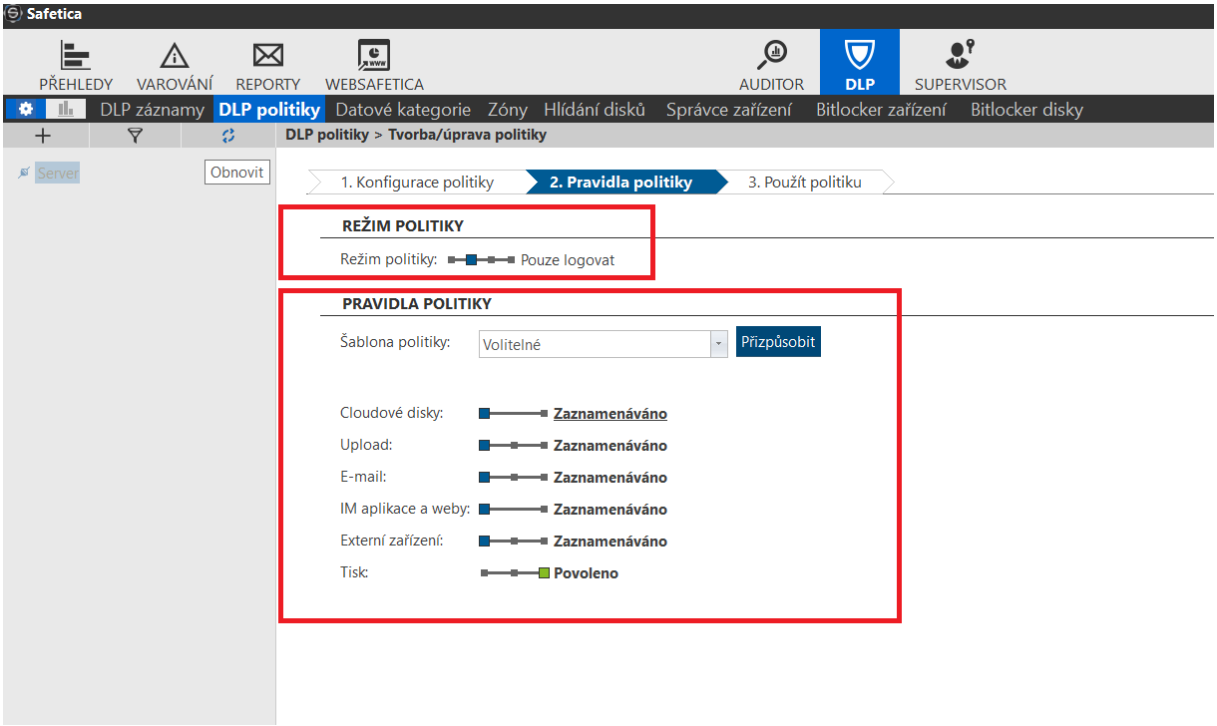
- Vypnuto – politika je vypnutá
- Pouze logovat – logují se události
- Logovat a upozornit – Safetica klient zobrazí okno, kde uživatel povolí nebo zakáže akci
- Logovat a blokovat – akce bude zakázána a logována

Pravidla politiky

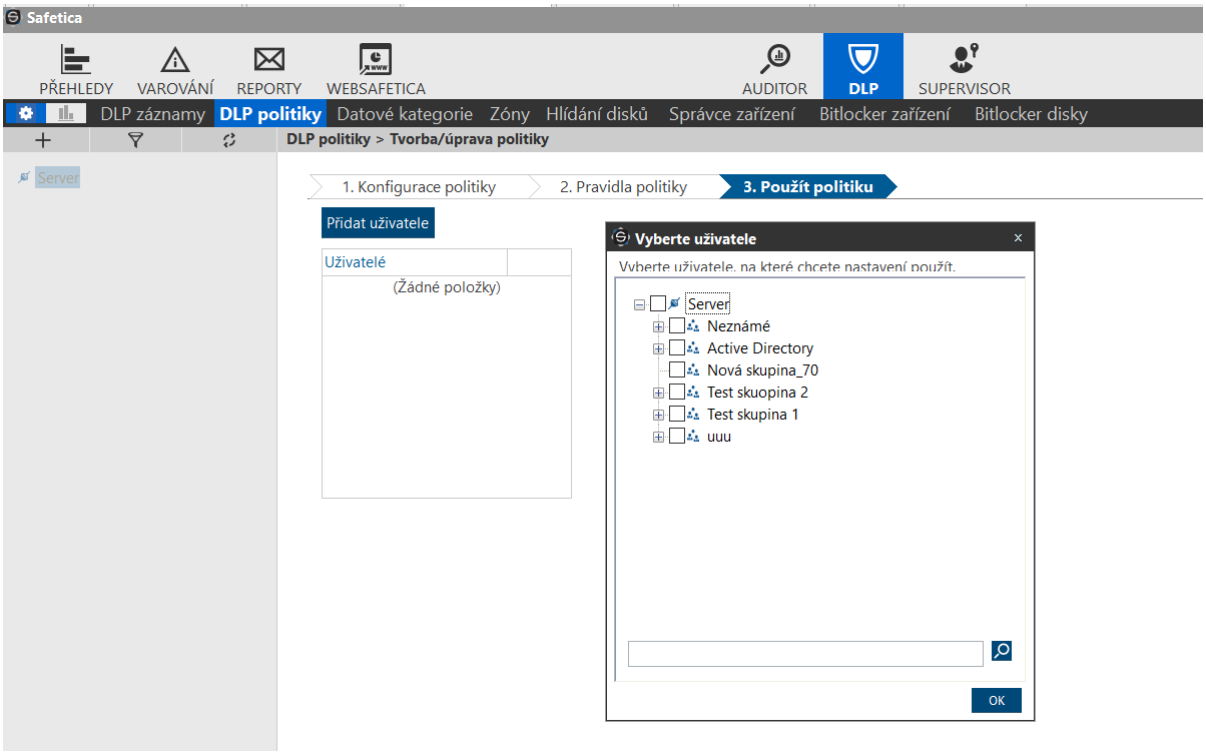
Definuje se chování DLP pravidla pro jednotlivé komunikační kanály – email, web, externí zařízení….

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 klasifikované kontextovou klasifikací Safetica, např. soubory uložené ve sdíleném síťovém umístění, stažené soubory z intranetu, exporty CRM atd.

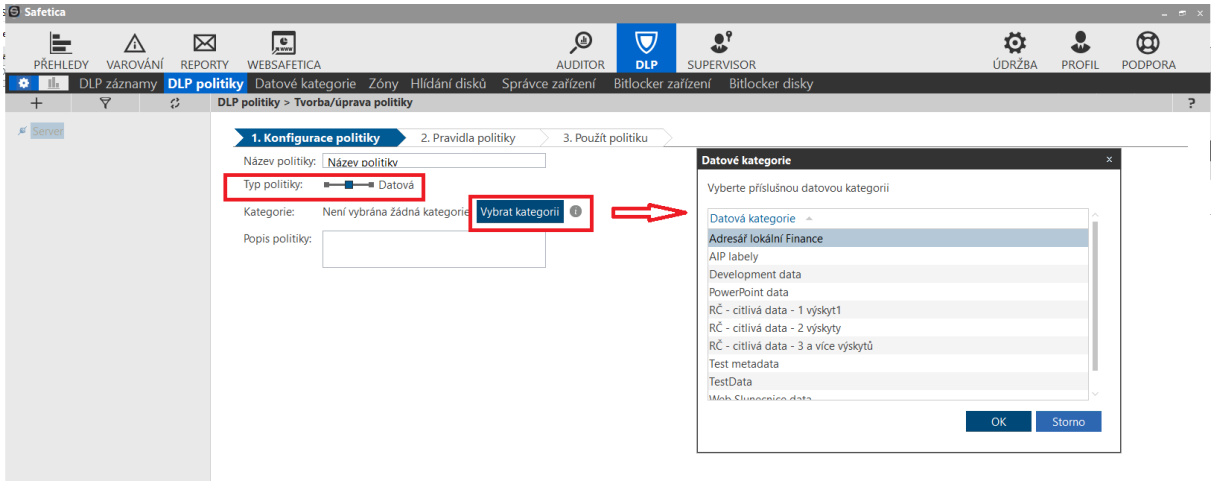
Datovou DLP politiku umisťujte do horní části seznamu politik, tak aby se uplatnila prioritně před obecnou politikou.

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

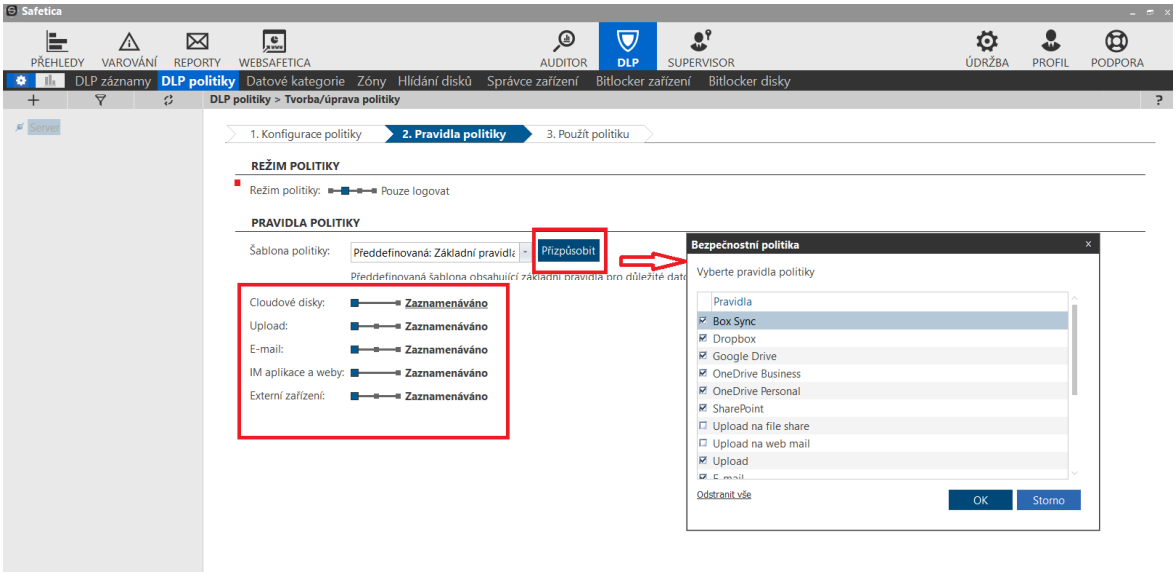
- Vypnuto – politika je vypnutá
- Pouze logovat – logují se události
- Logovat a upozornit – Safetica klient zobrazí okno, kde uživatel povolí nebo zakáže akci
- Logovat a blokovat – akce bude zakázána a logována

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.

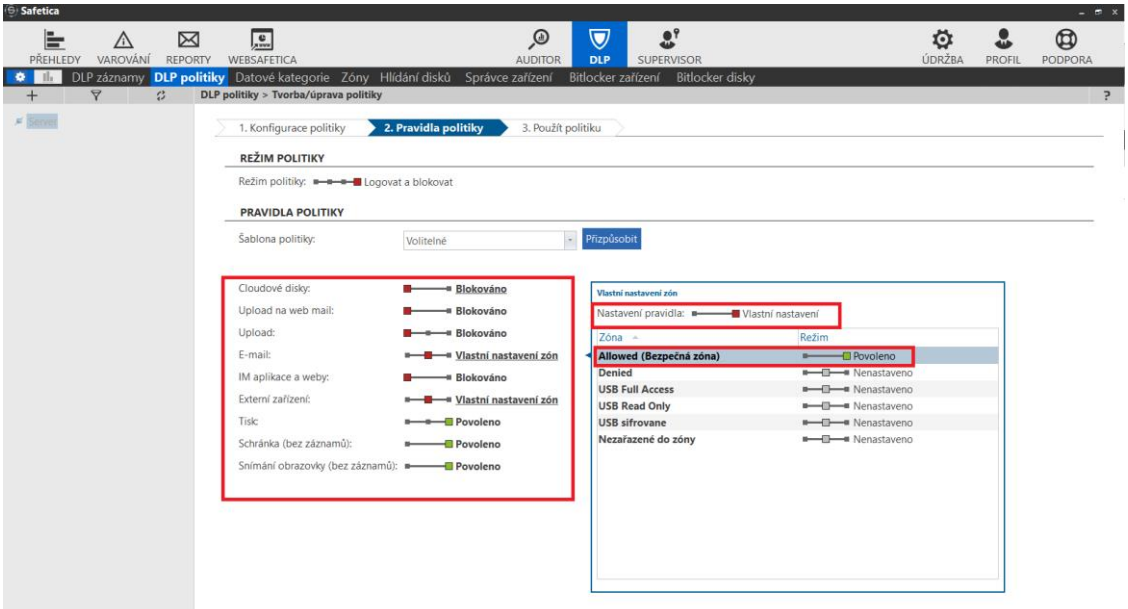
Při definici pravidla jsou výrobcem nabídnuty standardní komunikační kanály. Pomocí tlačítka „Přizpůsobit“ je možné zvolit další komunikační kanály, které budou v tomto DLP pravidle sledovány.



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

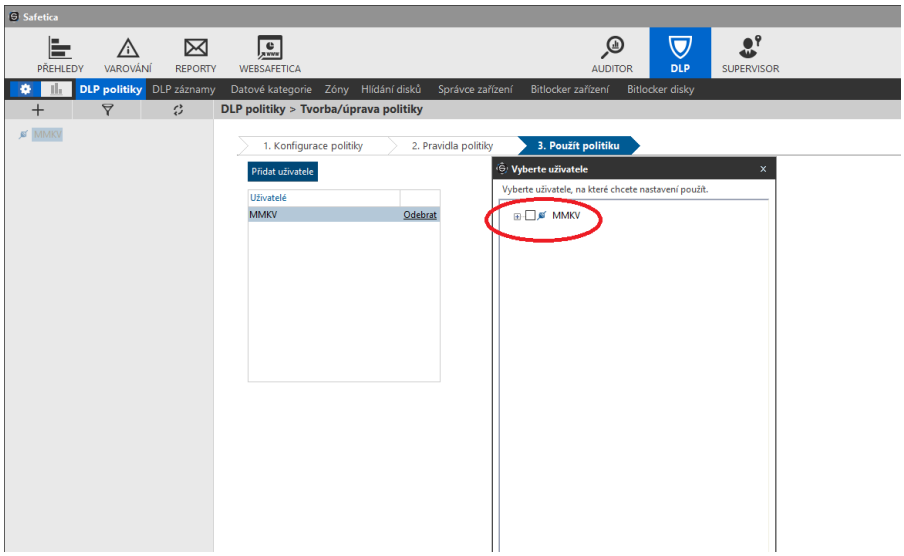
Odchod dat přes ostatní definované komunikační kanály je blokován



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 zóny, 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.

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



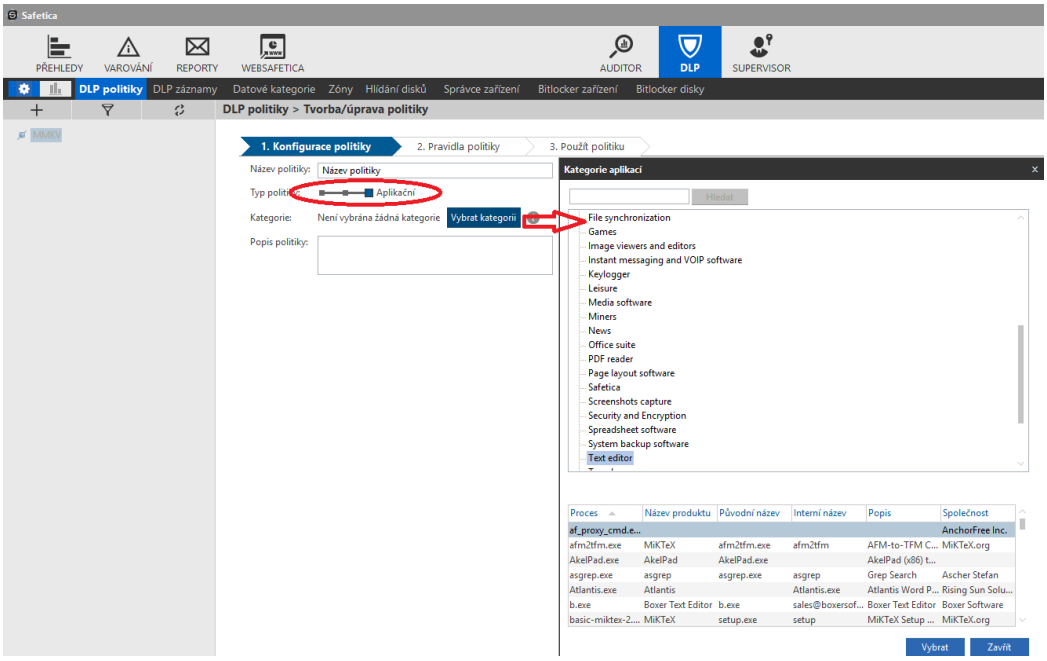
8.2.3. APLIKAČNÍ PRAVIDLA

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

Aplikační DLP politiku umisťujte do horní části seznamu politik spolu s datovými politikami, kde je seřaďte 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

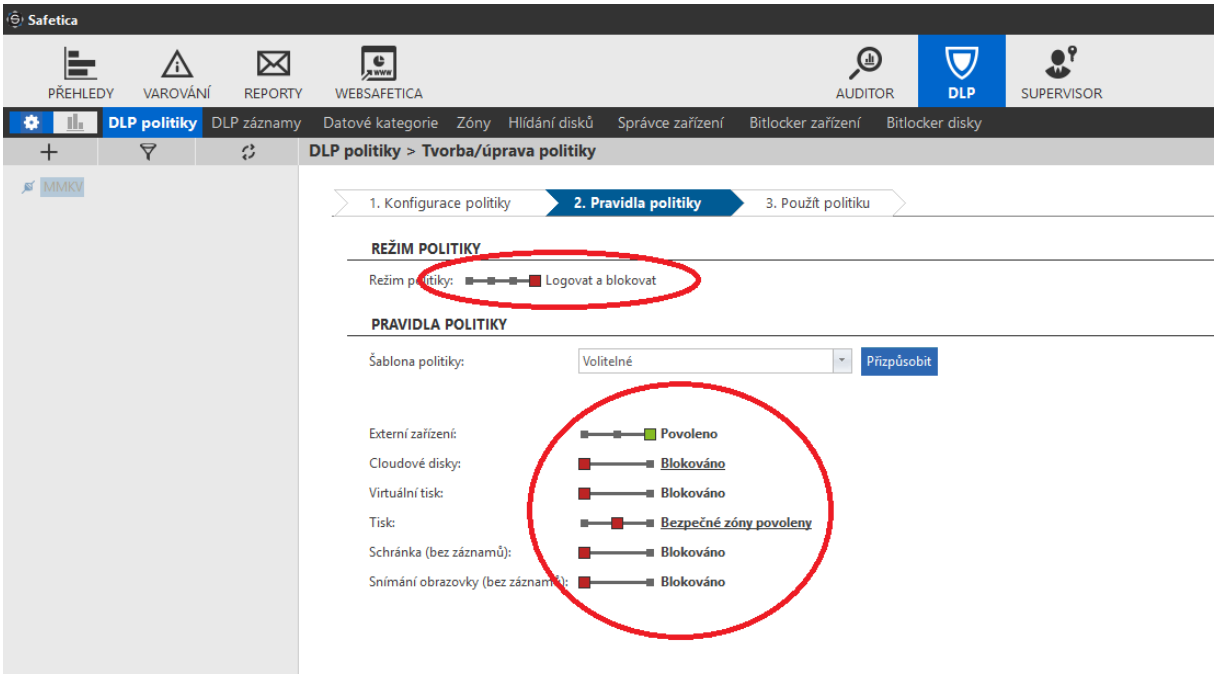
- Vypnuto – politika je vypnutá
- Pouze logovat – logují se události
- Logovat a upozornit – Safetica klient zobrazí okno, kde uživatel povolí nebo zakáže akci
- Logovat a blokovat – akce bude zakázána a logována

Pravidla politiky

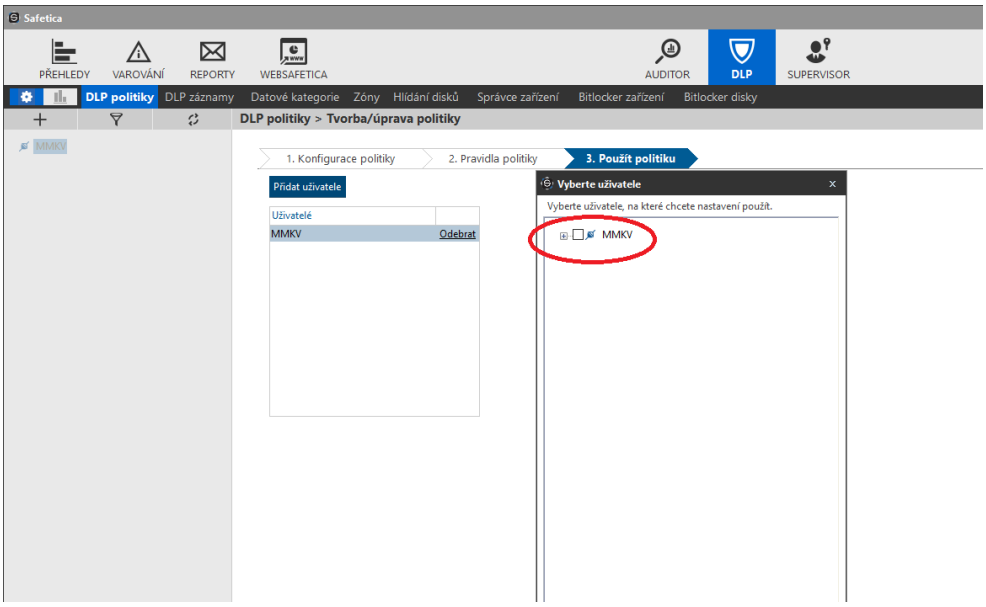
Definuje, jak budou moci nastavené aplikace komunikovat přes jednotlivé komunikační kanály – email, web, externí zařízení….

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

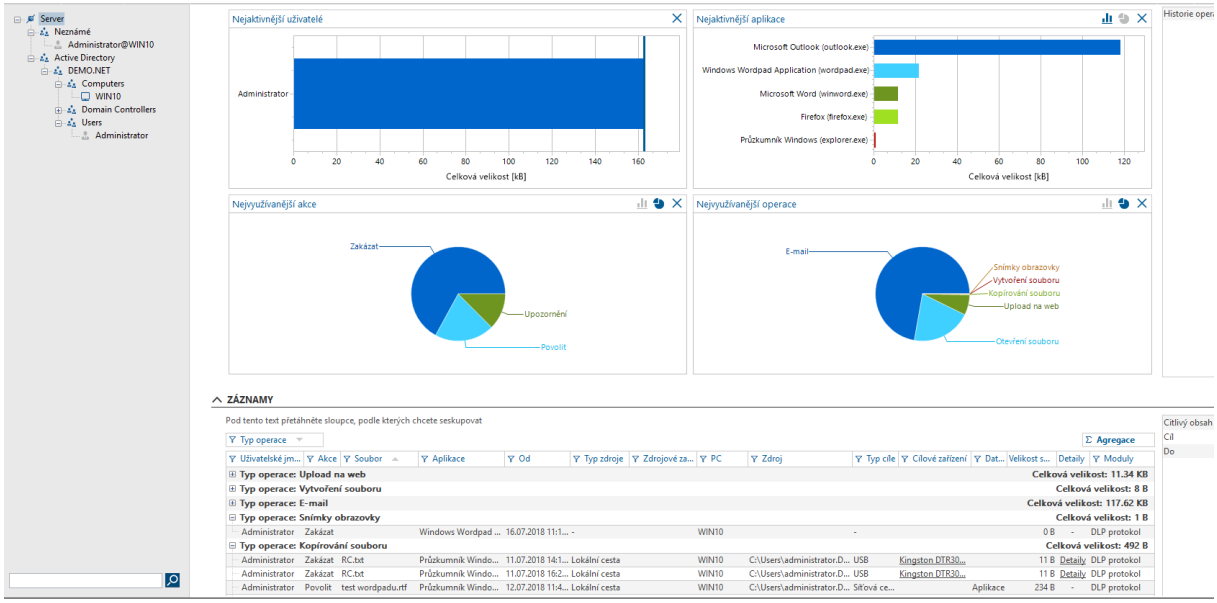


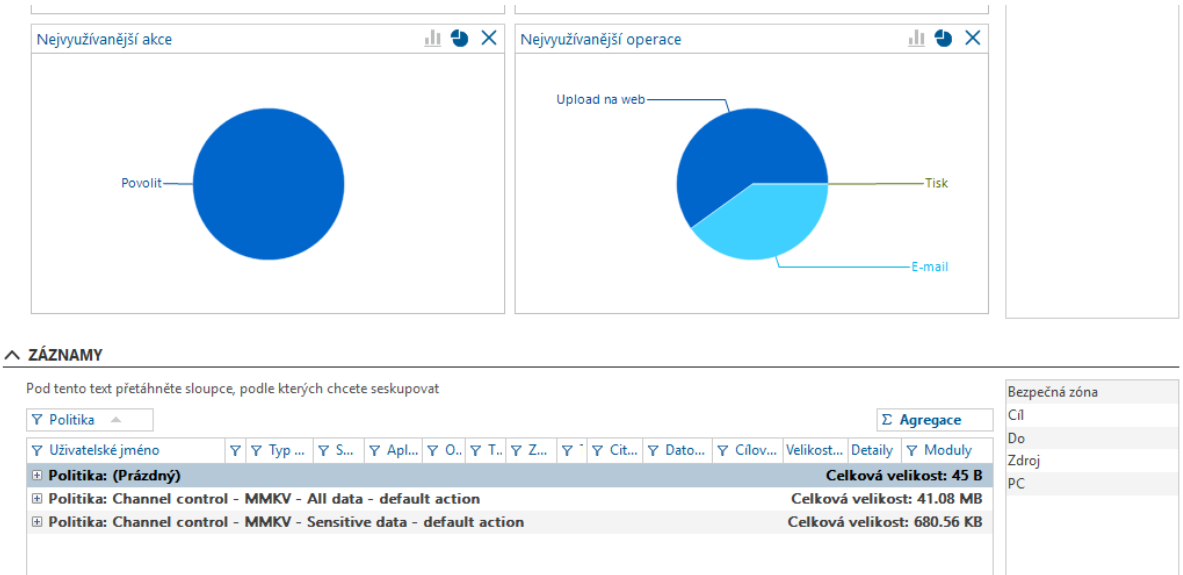
Použít politiku – definice, kde se bude politika uplatňovat – celá organizace, konkrétní uživatel, skupina nebo počítač:



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.

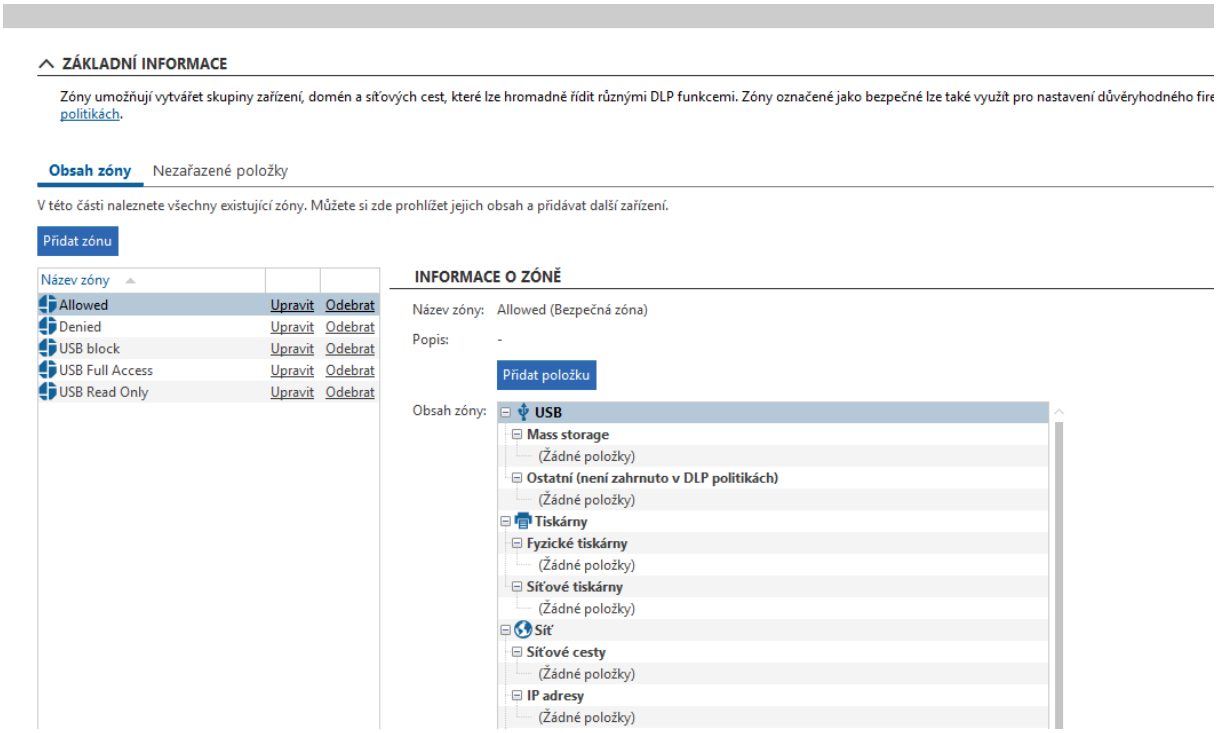




8.4. ZÓNY

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:

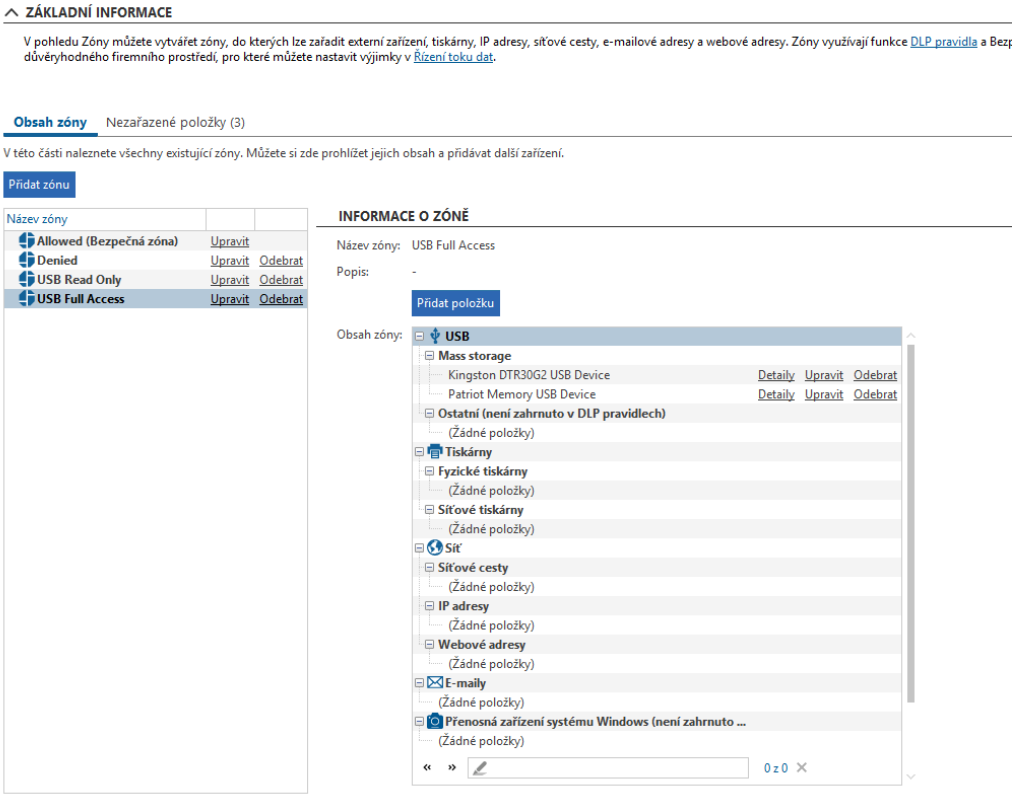
- Definice IP adres – lokání síť
- Definice emailových adres – lokální doména
- Definice webových adres – lokální webové servery
- Definice zařízení – USB flash disky, Bluetooth zařízení..



Příklad definice dalších zón, které je možné následně využit v nastaveni

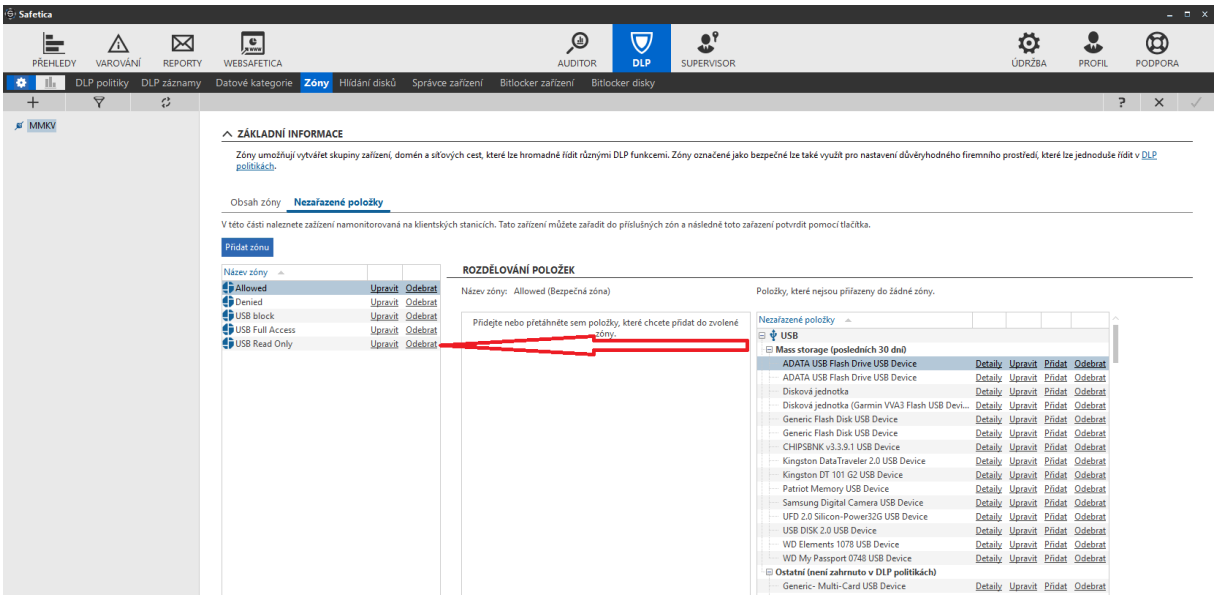
- USB Read Only
- USB Full Access
- USB Block

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



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



8.5. HLÍDÁNÍ DISKŮ

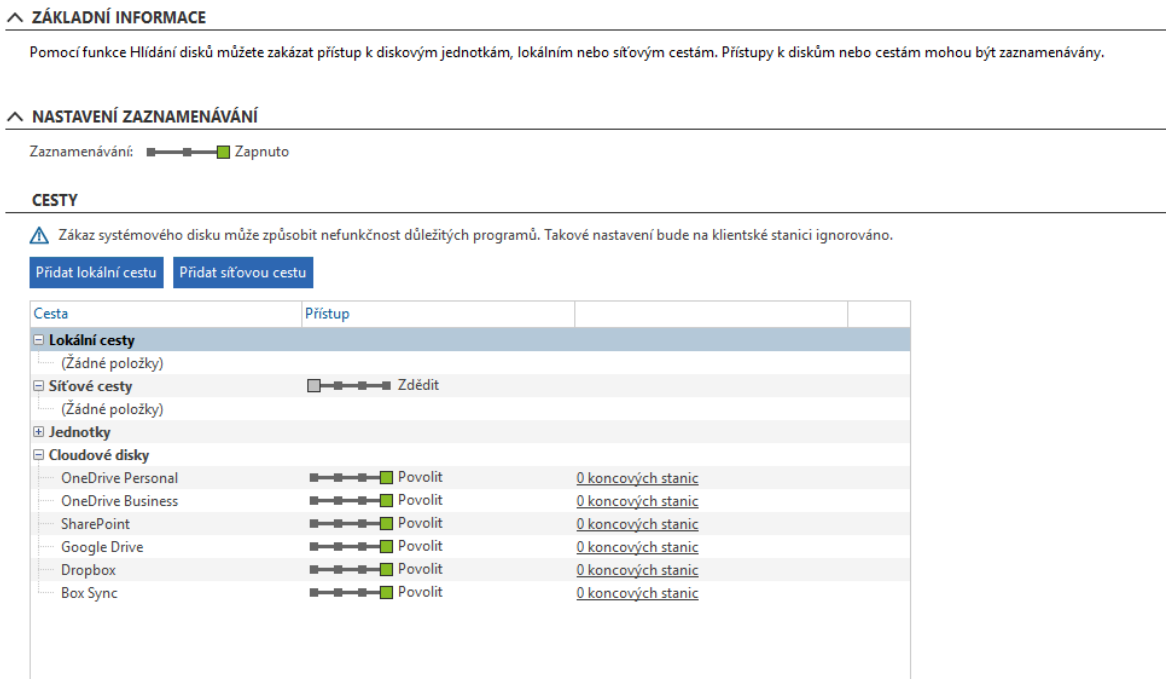
Pomocí hlídání disků je možné jednoduchými pravidly nastavit uživatelům oprávnění k přístupu k souborovému systému. Například zvolit disky, na které budou mít přístup, nebo ze kterých mohou jenom číst popřípadě zvolit přímo jednotlivé cesty respektive složky

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



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.

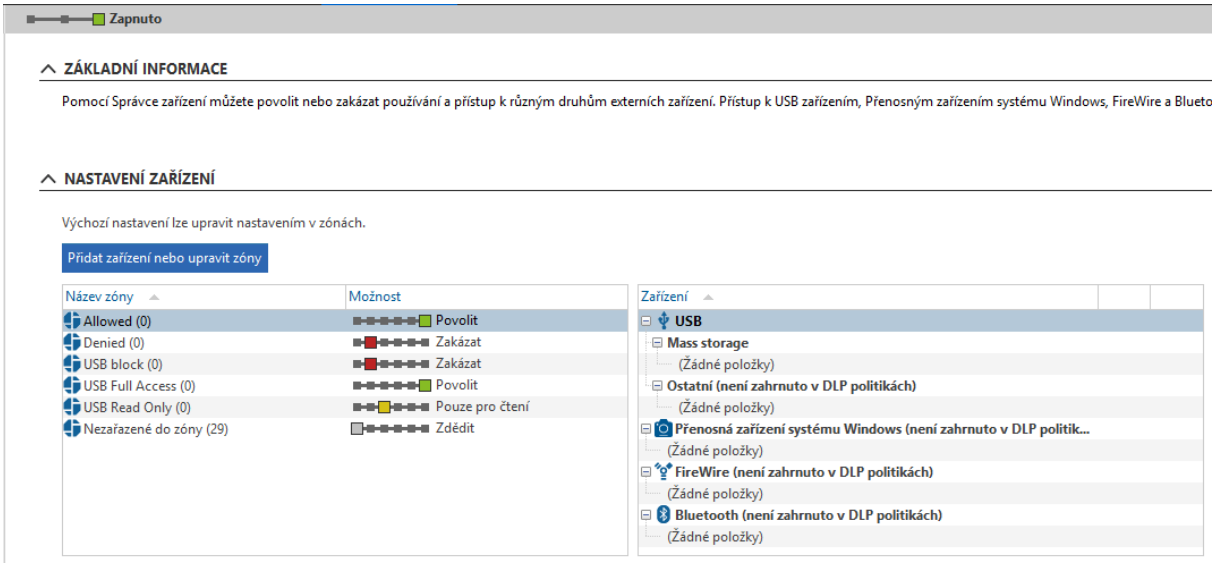
Je možné definovat globální pravidla pro jednotlivé typy portů, nebo nastavit detailní konfiguraci pro konkrétní zařízení, které bylo historicky připojeno k počítači s DLP agentem a je načteno nezařazených zařízeních – Nastavení Zóny.

Systém 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 Fulll access zóna povolena
- USB Block zóna blokována



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

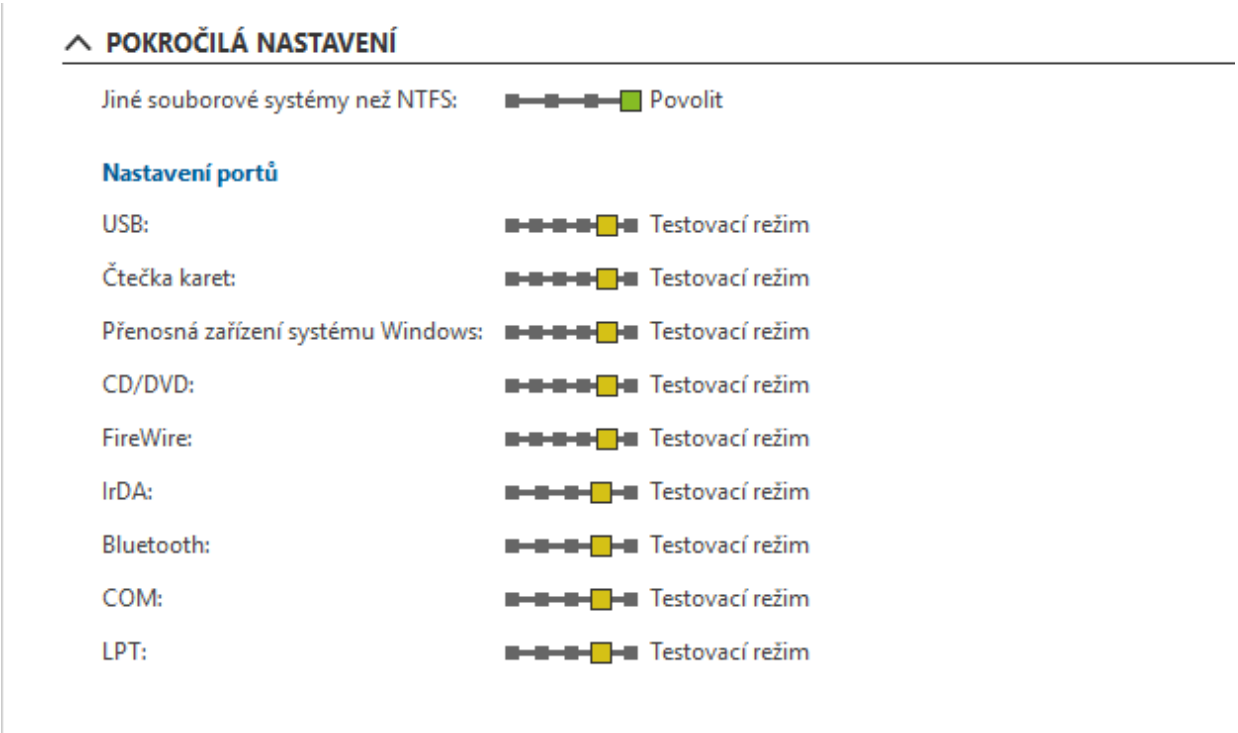
V této části je možné globálně upřesnit možnost přístupu k jednotlivým typům zařízení nebo jiným

souborovým systémů 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



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

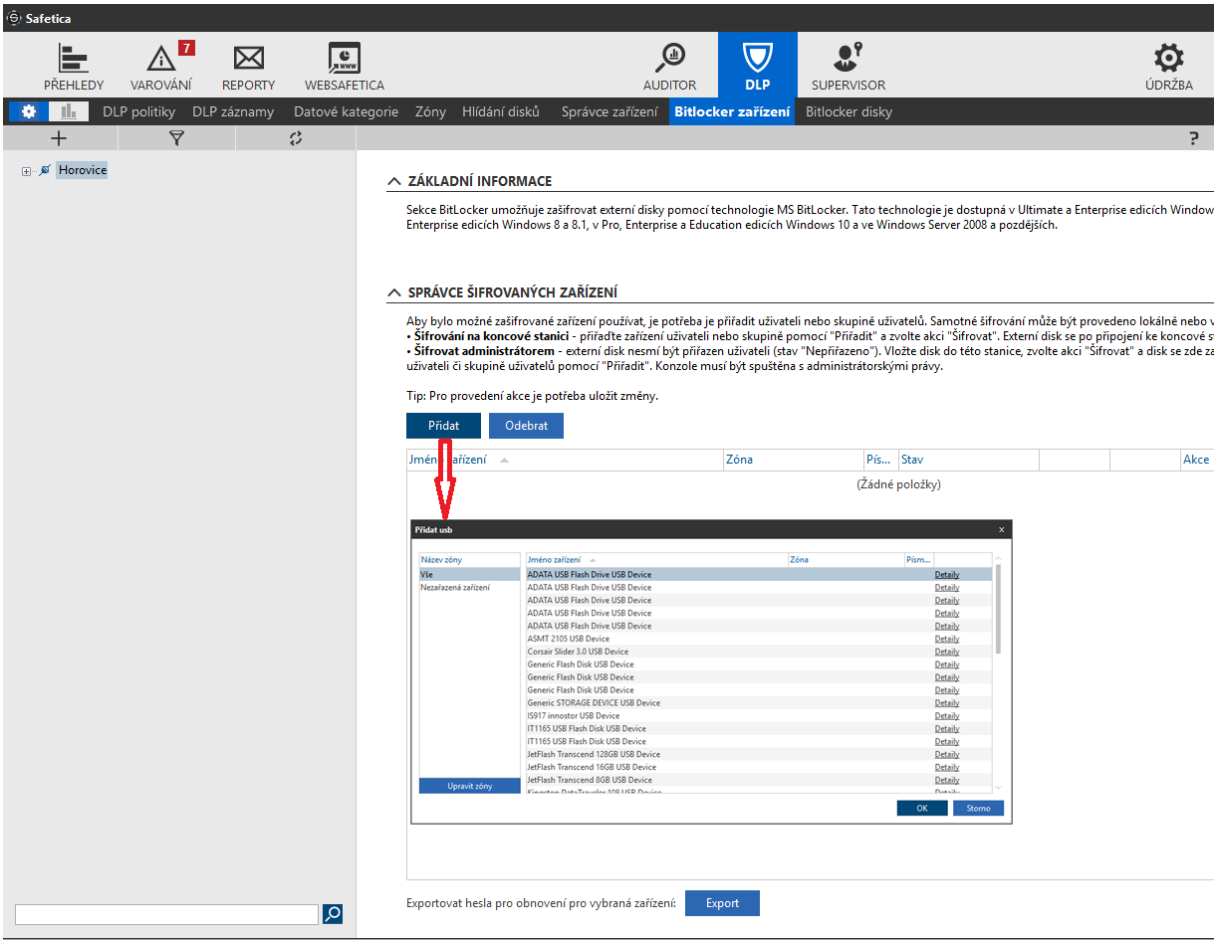
Tato funkce umožňuje šifrovat externí disky pomocí nástroje BitLocker od společnosti Microsoft. Přístup k zašifrovaným zařízením lze přiřazovat jednotlivým uživatelům, počítačům nebo skupinám.

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.

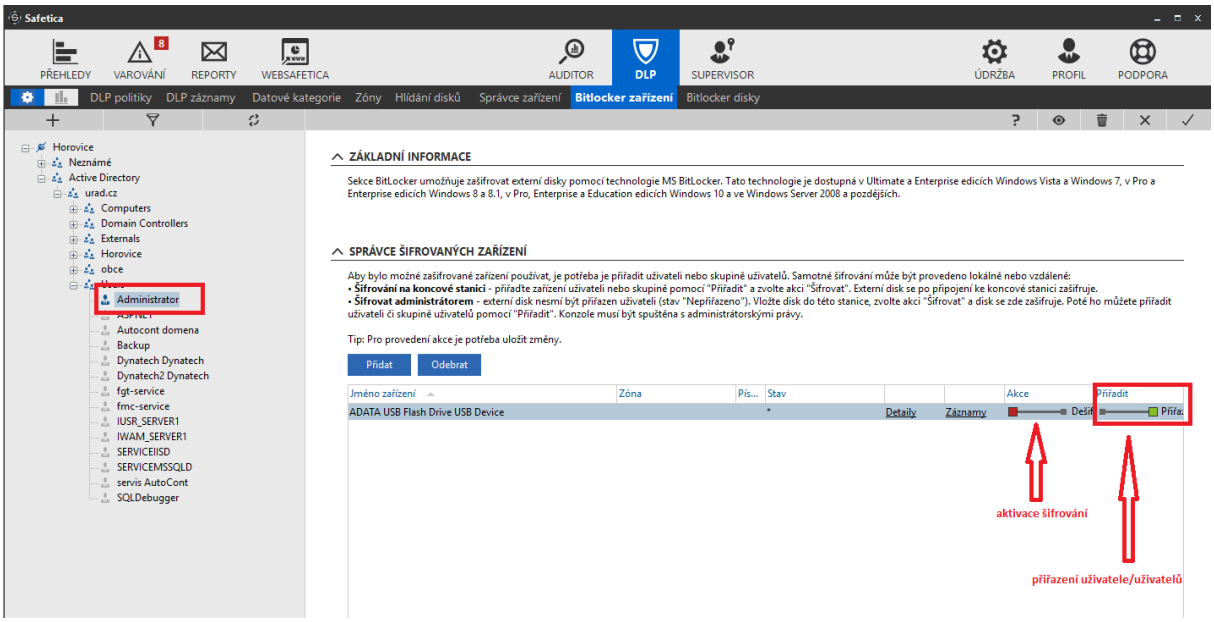
Tlačítkem „Přidat“ je možné vybrat zařízení, které má být pomocí technologie Bitlocker šifrováno.

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

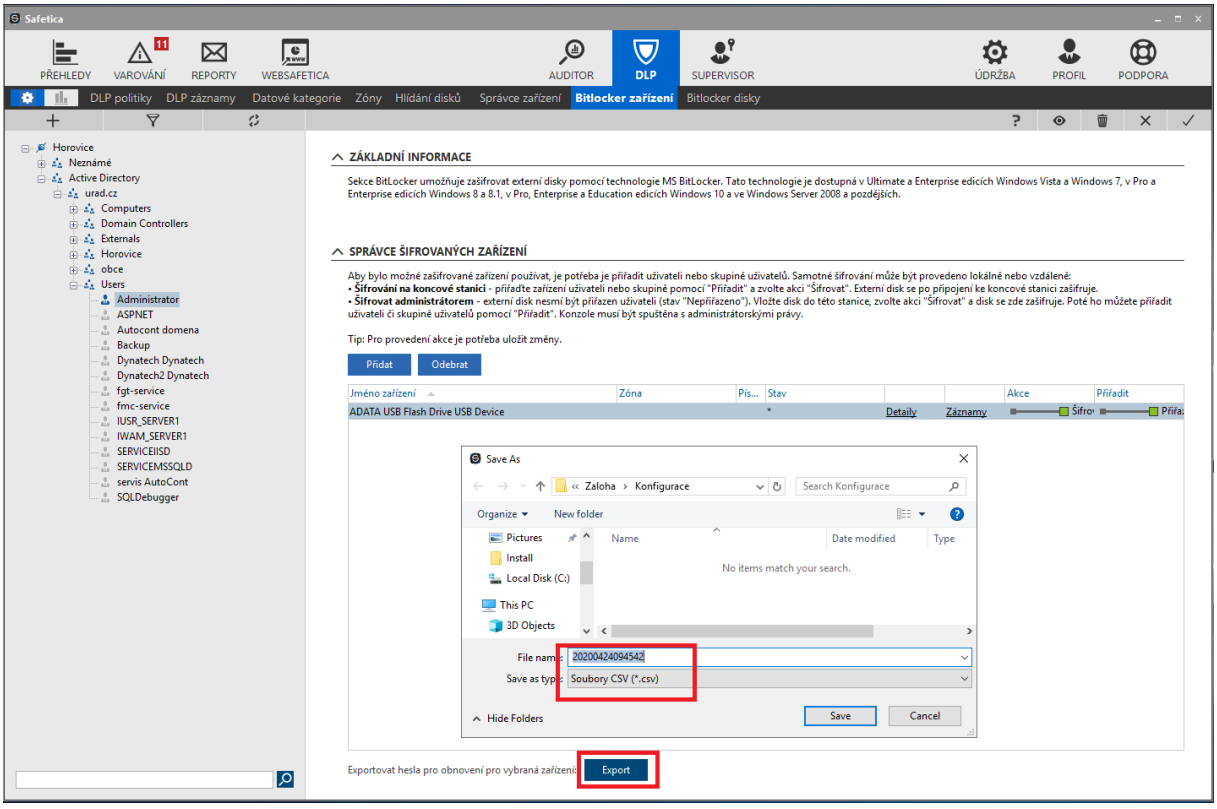


Po vybrání USB zařízení se nastavuje šifrování USB disku a přiřazení USB disku uživatelům, nebo počítačům, kterým bude tento USB disk transparentně přístupný po vložení do počítače.

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.

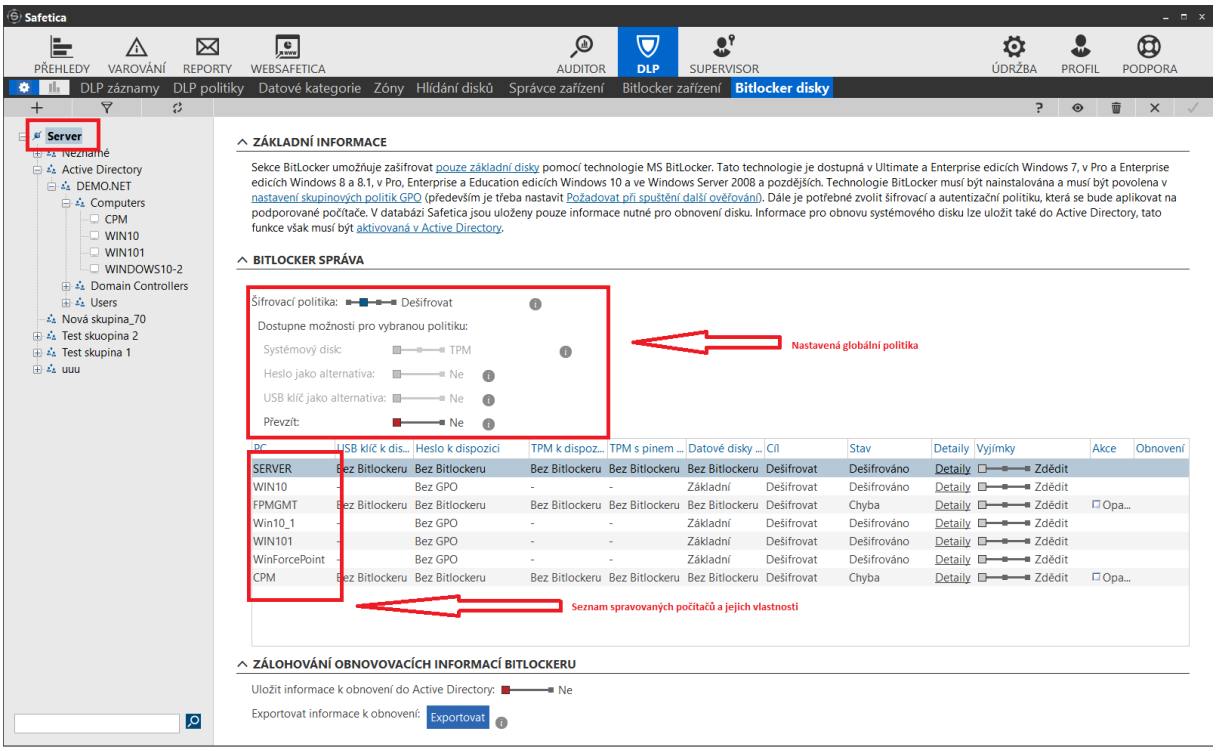
Safetica klient zajišťuje aktivaci šifrování Bilockerem na koncových počítačích uživatelů, volbu disků, které budou šifrovány, synchronizaci klíčů s Microsoft Active Directory a export klíčů do souboru – záloha.

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 šifrovaný, jaká je podpora TPM čipu, v jakém stavu daný počítač je.

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



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“

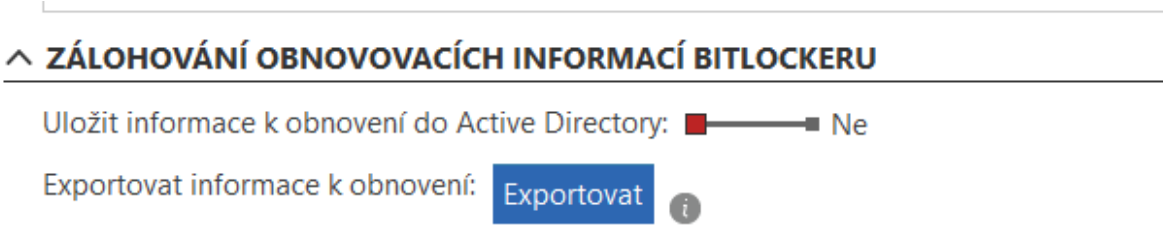
Je možné vybrat z následujících možností:

- **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.

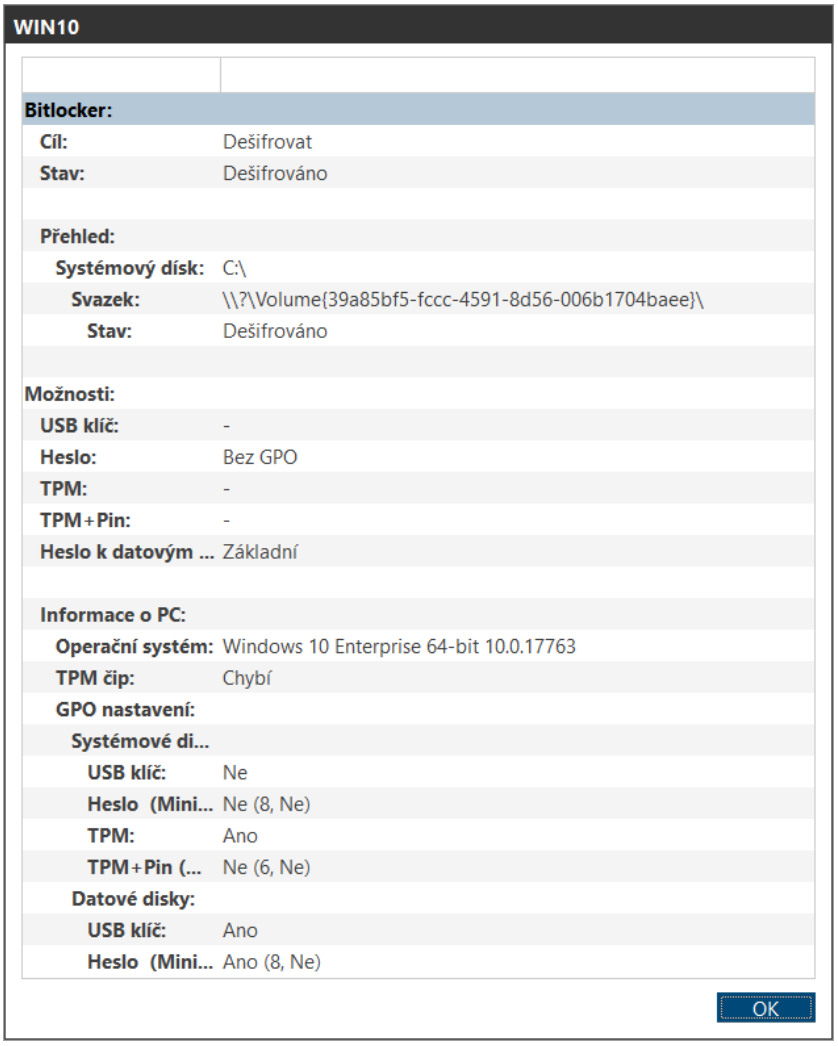
Na základě zvolené politiky je možné upravit některou z následujících možností:

- **Systémový disk** – nastavení způsobu odemykání systémového disku:
    - **Heslo** – při startu počítače bude uživatel požádán o zadání přístupového heslo, které si nastaví při aplikovaní 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 aplikovaní 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.

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



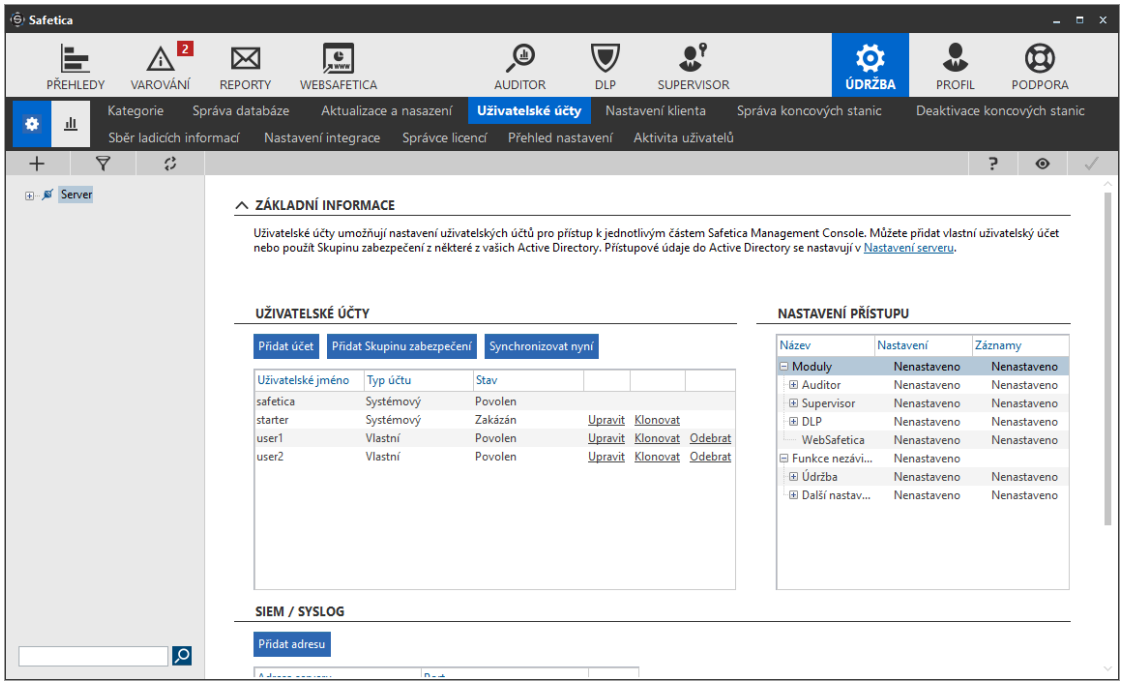
Stav šifrování je možné sledovat kliknutím na „Detaily“ pro zvolený počítač


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 di...
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

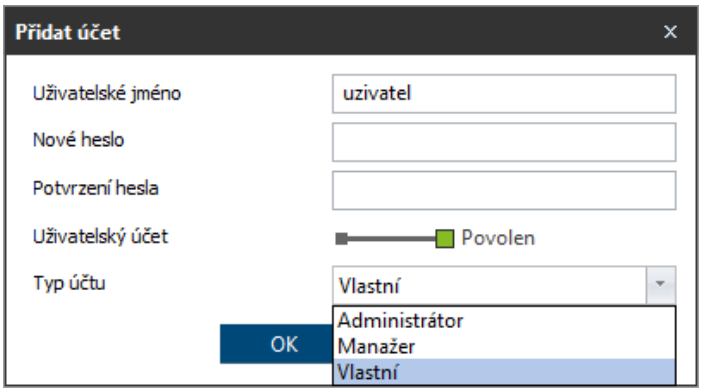
V rámci nastavení je možné definovat správce Safetica management konzole a jejich práva pro Správu

Definice se uživatele se nastavuje v záložce Údržba / Uživatelské účty



9.1. DEFINICE UŽIVATELE SAFETICA

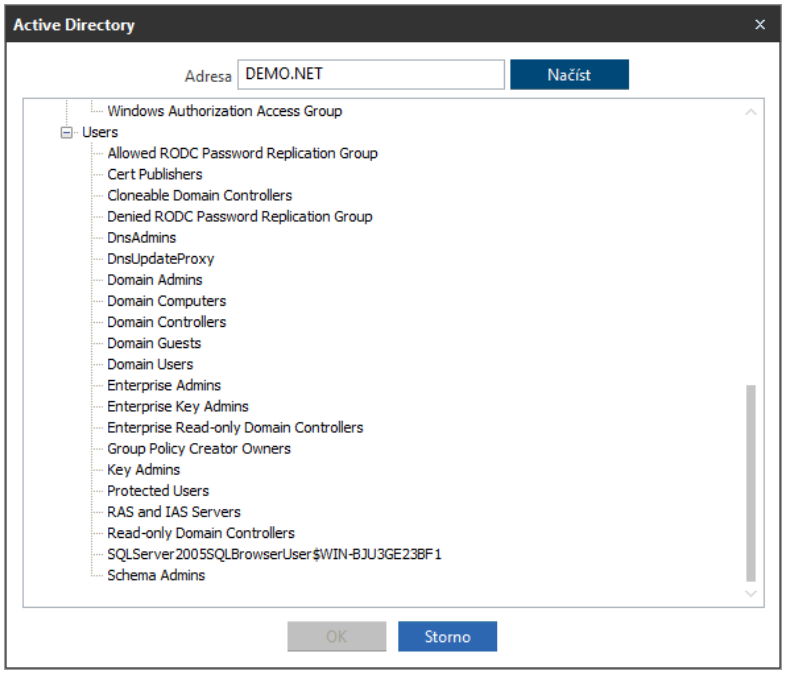
Pomocí tlačítka „Přidat uživatele“ se definuje uživatel systému Safetica



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.

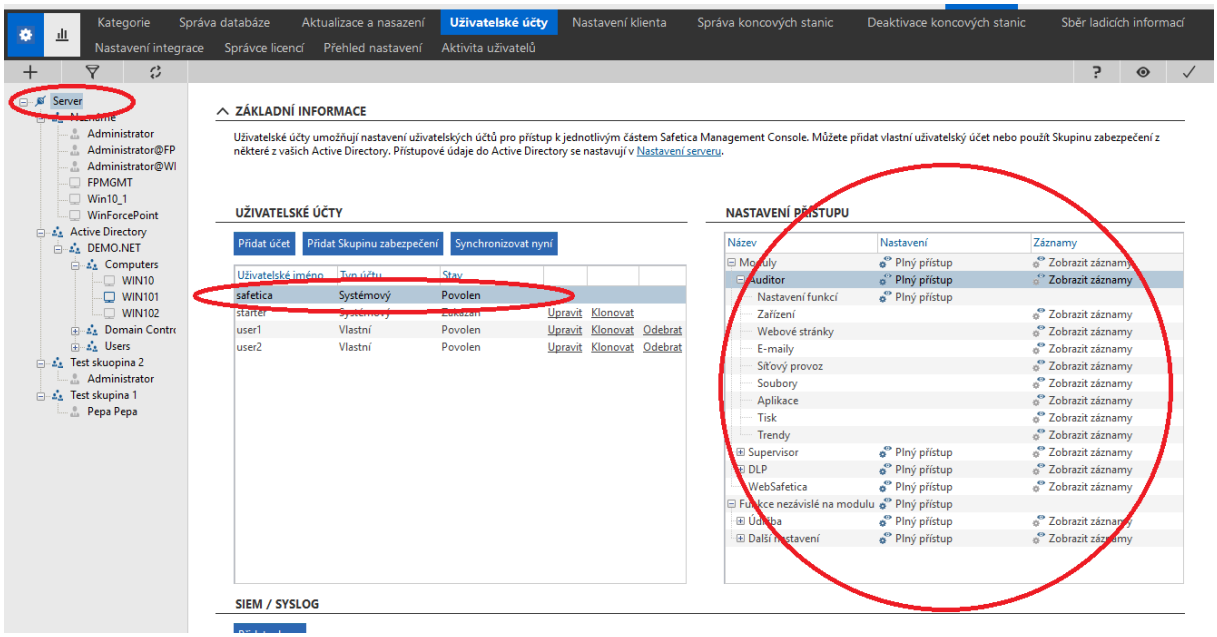
Pokud se přidá skupina z AD, všichni členové skupiny budou mít stejná práva přístupu ke správě systému Safetica.



9.2. NASTAVENÍ PRÁV UŽIVATELE

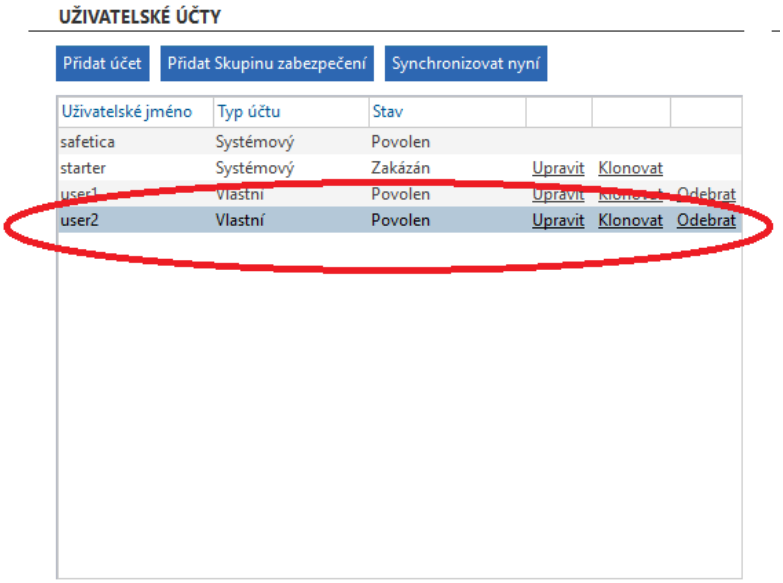
Pro nastavení práv na uživatele je nutné označit uživatele nebo skupinu, na kterých se budou práva nastavovat.

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



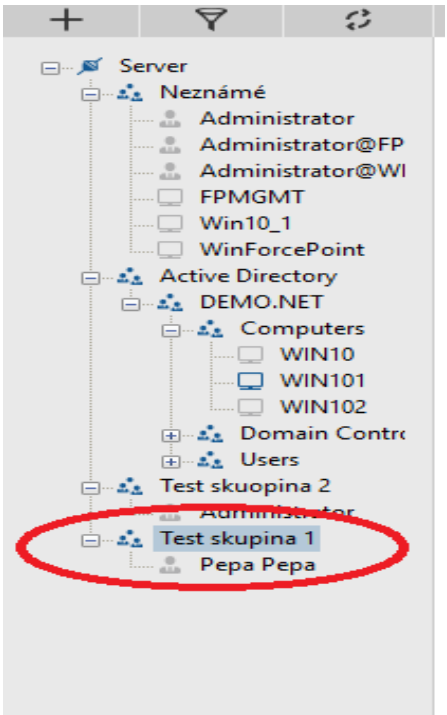
9.2.1. VÝBĚR UŽIVATELE,

Výběr skupiny, kde se budou nastavovat oprávnění



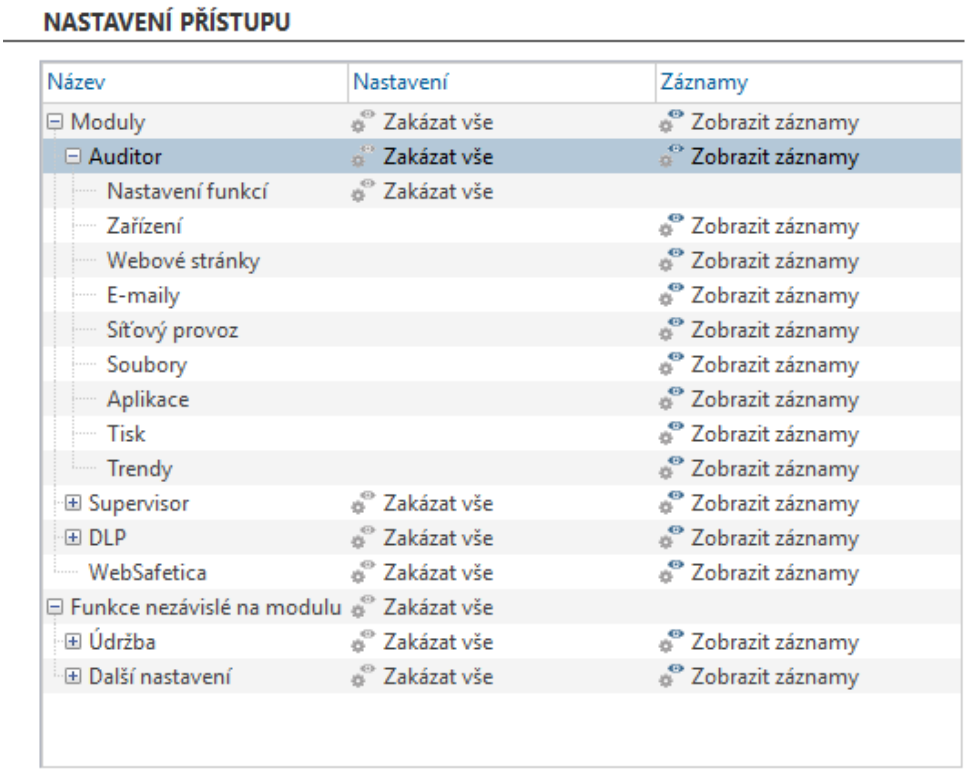
9.2.2. VÝBĚR SKUPINY

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.



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

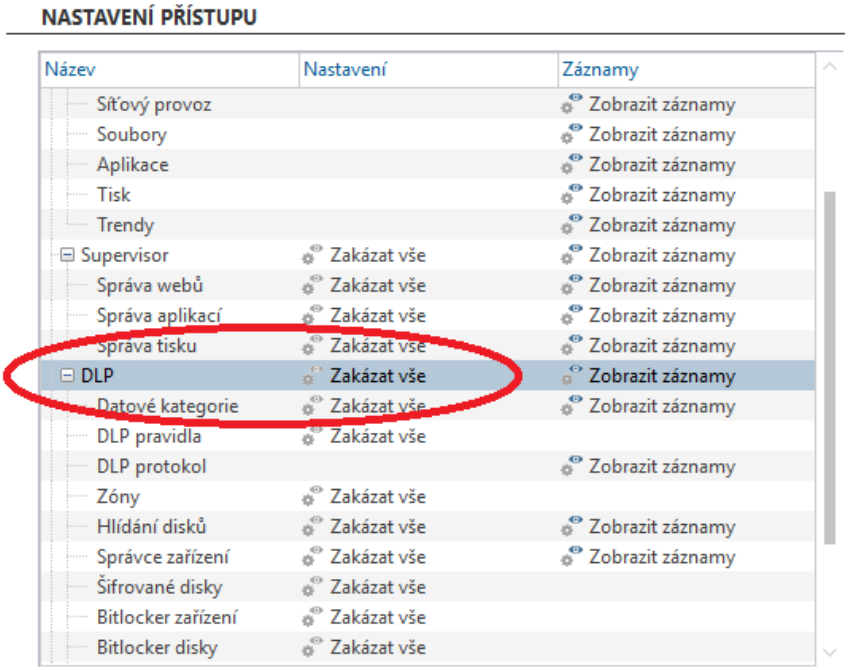
V rámci tohoto nastavení je možné definovat práva pro jednotlivé části modulů


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

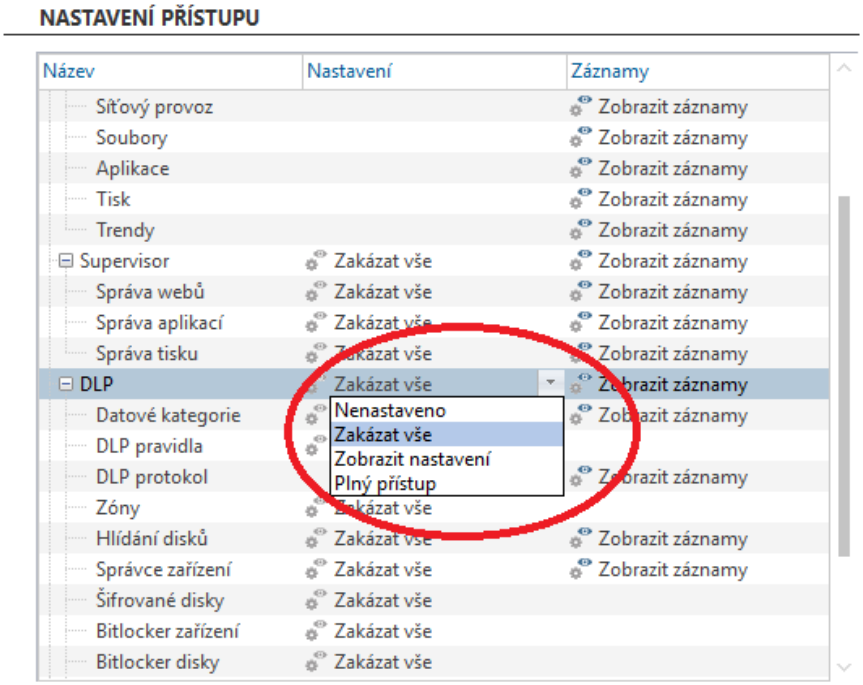
9.2.3.2 Položka „Nastavení“

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

Je možné vybrat jednotlivé položku modulů nebo celý modul



A následně definovat práva uživatele pro „Nastavení“



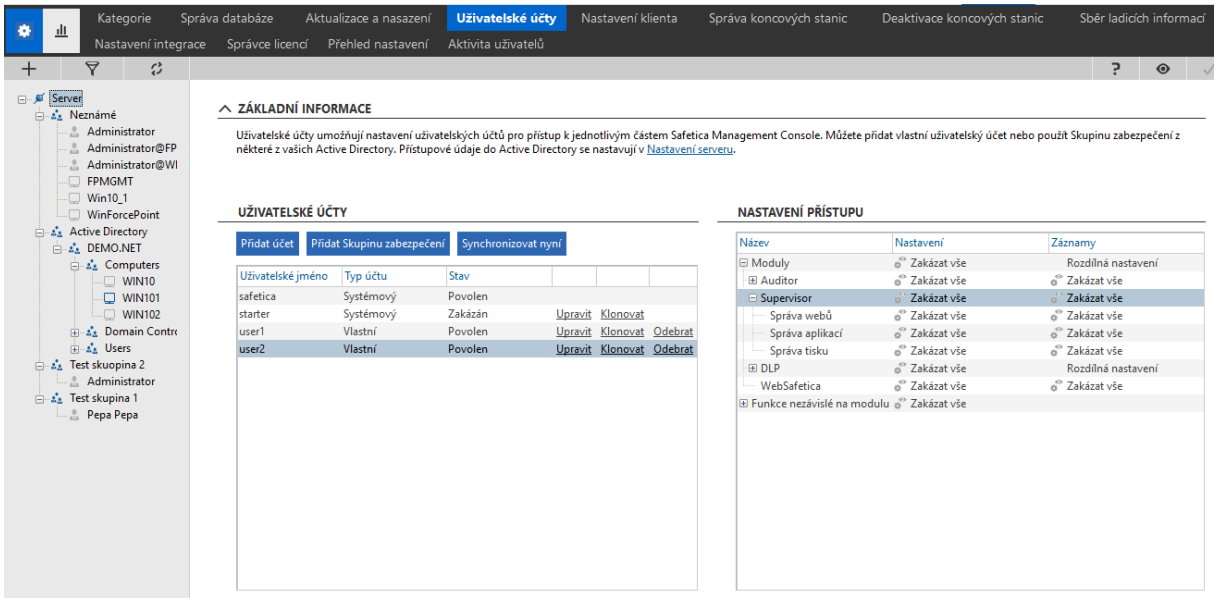
9.2.3.3 Položka „Záznamy“

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

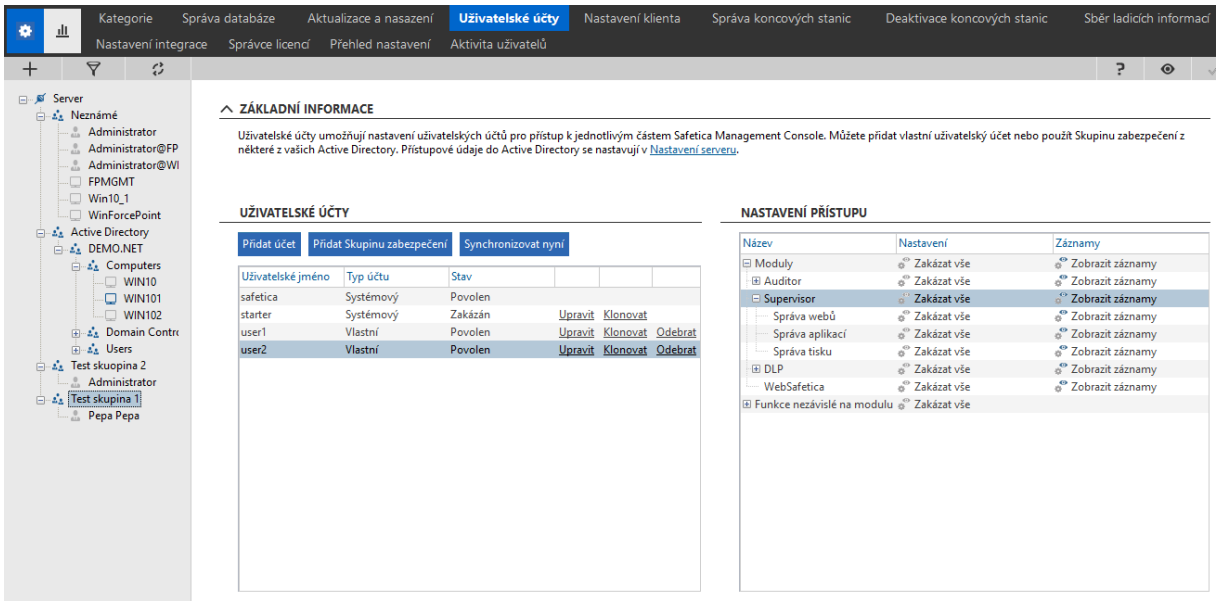
9.3. PŘÍKLAD NASTAVENÍ PRO UŽIVATELE USER 2

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

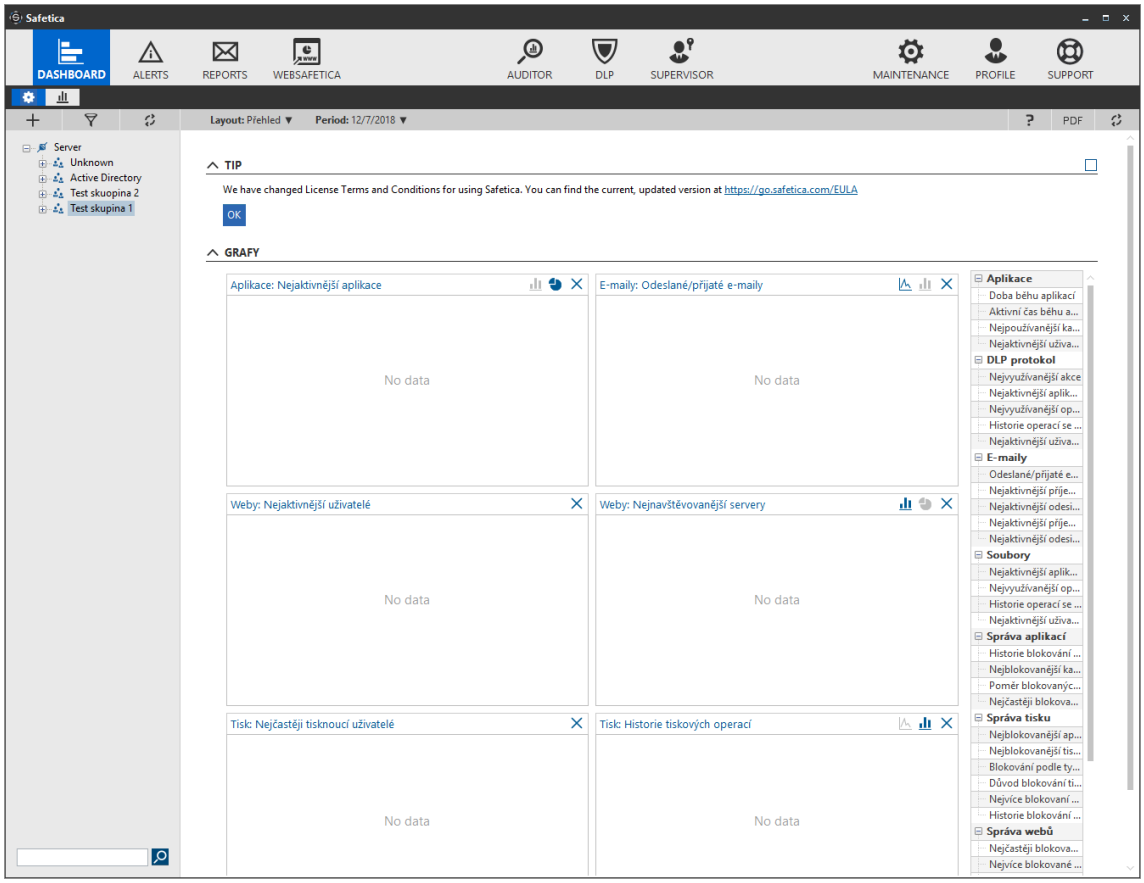
Přístup na celou společnost je zakázán



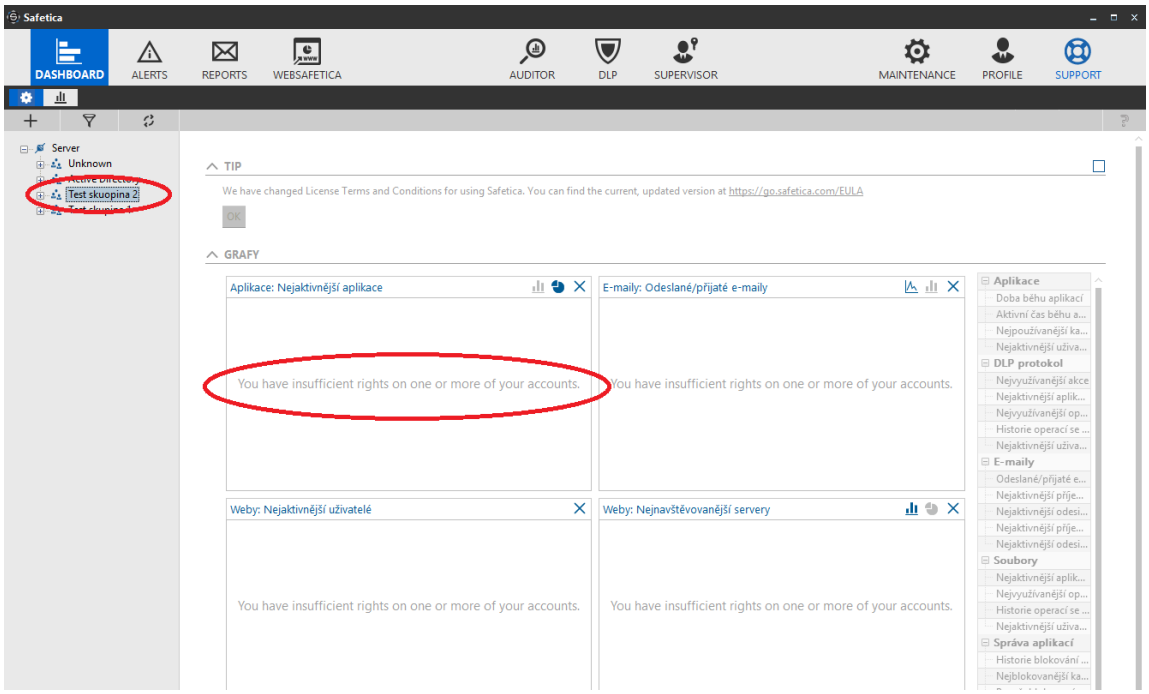
Přístup na skupinu „Test skupina 1“ je povolen pouze na zobrazení logů



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



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

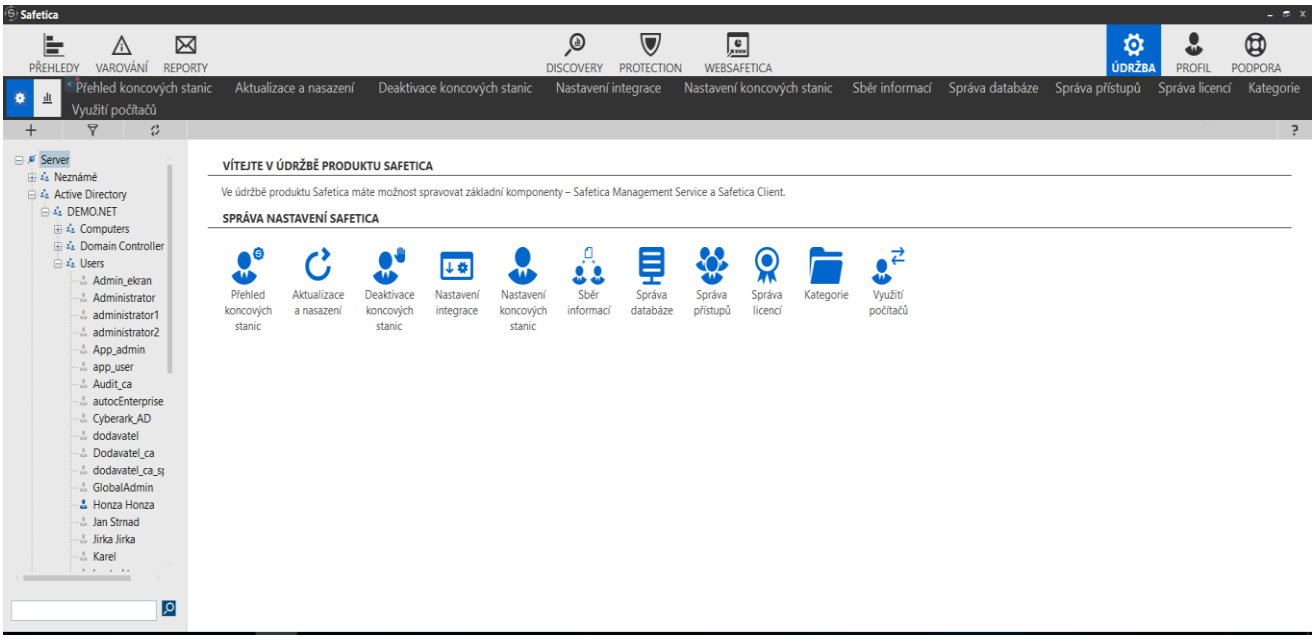


10. ÚDRŽBA

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.

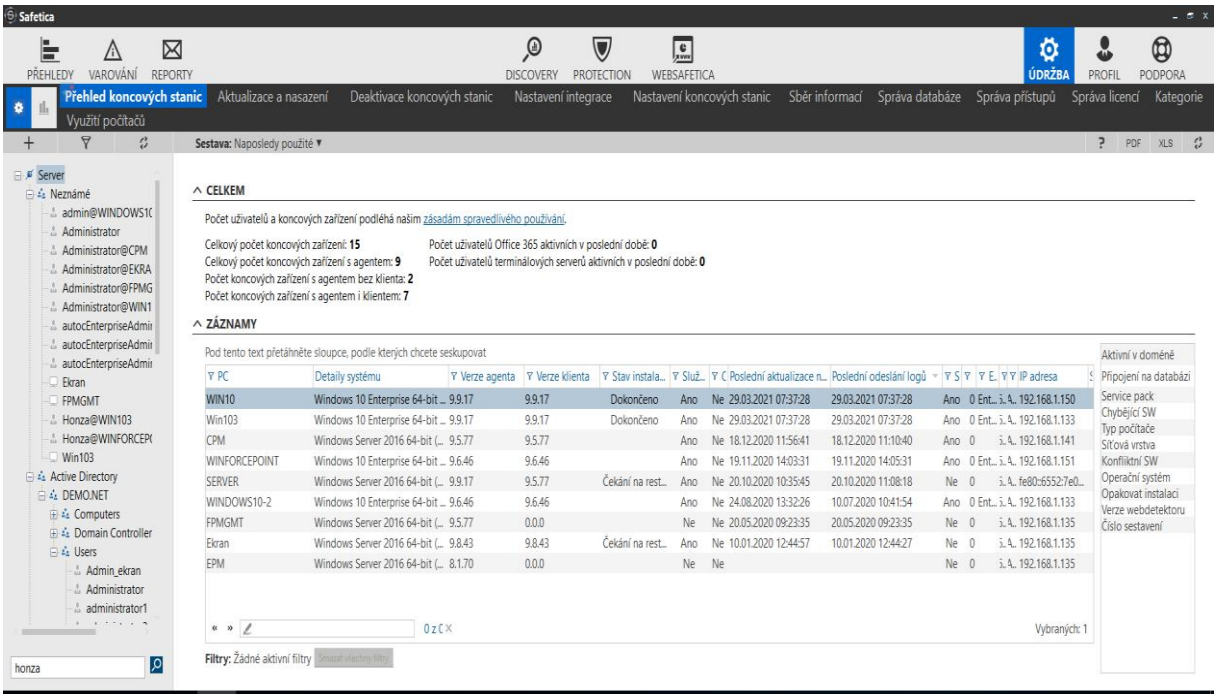
Údržba obsahuje tyto kategorie

- 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.



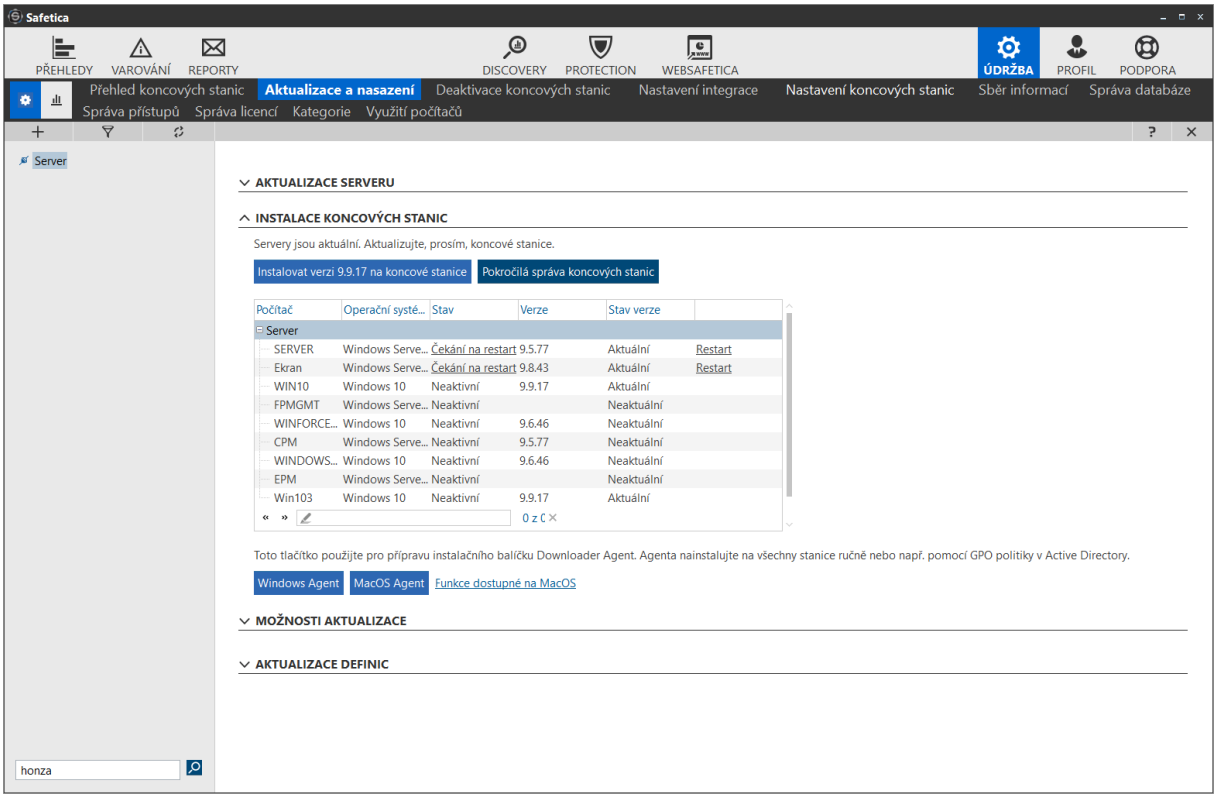
10.2. AKTUALIZACE A NASAZENÍ

Nastavení aktualizace systému a nasazení

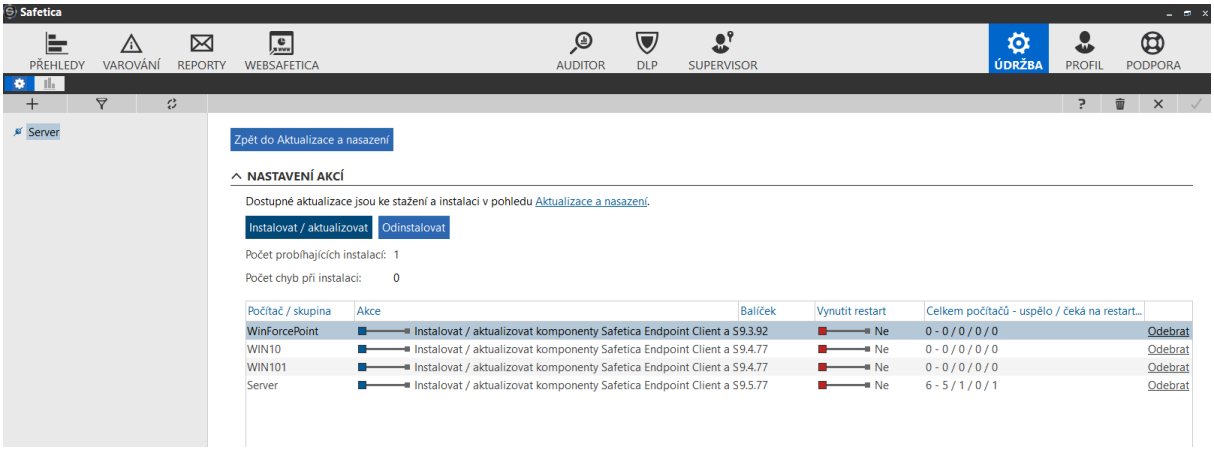
Umožňuje stáhnout a nainstalovat aktualizaci management konzole nebo koncových zařízení.

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.



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

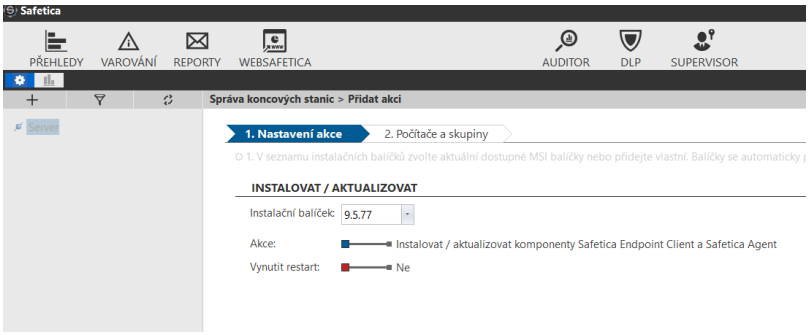


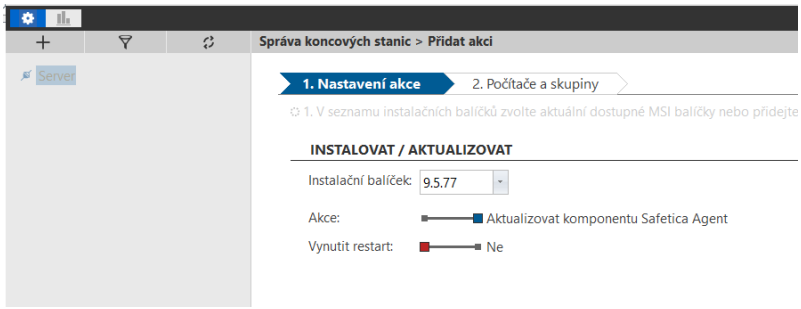
Správa koncových stanic umožňuje instalovat / upgradovat koncová zařízení, nebo odinstalovat Safetice SW z koncových stanic

Systém umožňuje vytvořit úlohy:

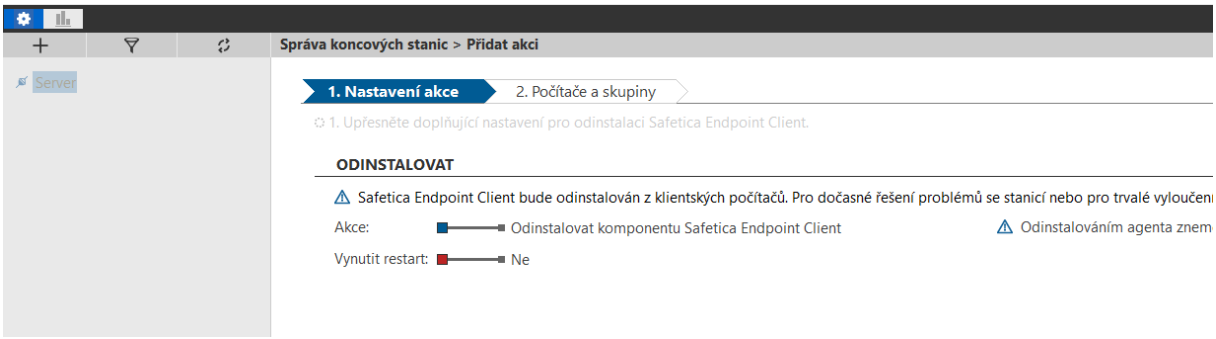
- Instalovat nebo aktualizovat Safetica agenta a klienta
- Odinstalovat Safetica klienta a agenta

Instalace nebo aktualizece komponent Safetica – agent, klient





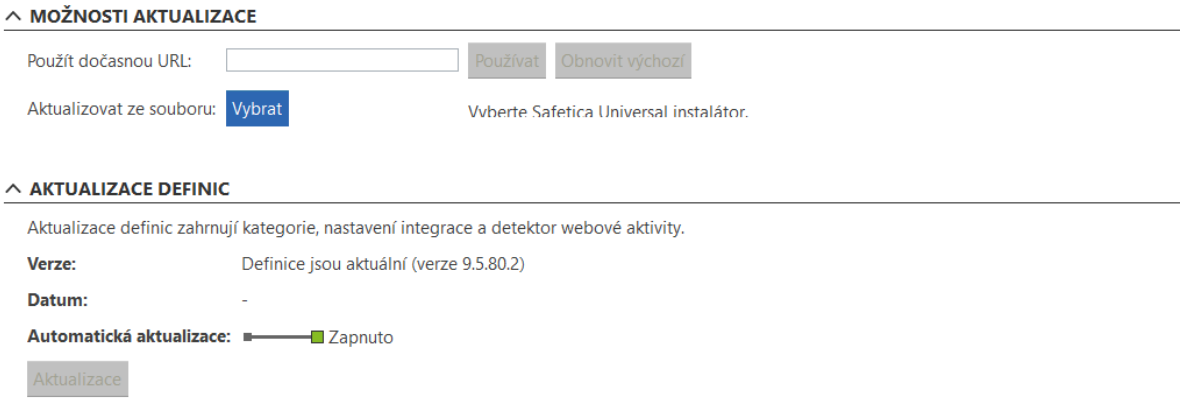
Odinstalace komponent Safetica – klient a agent



Součástí je i tlačítko „Windows agent“ a „MacOS agent“ – stáhne Safetica Agenta, 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“

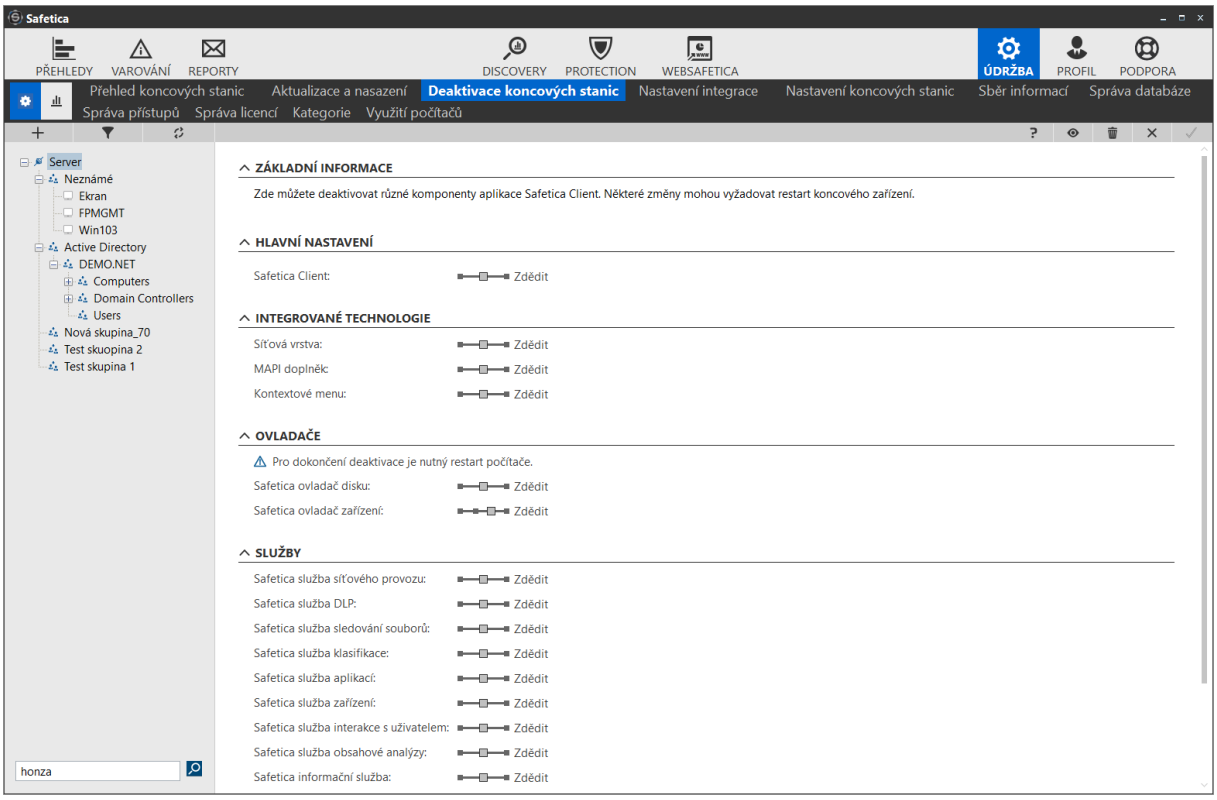


10.3. DEAKTIVACE KONCOVÝCH STANIC

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.

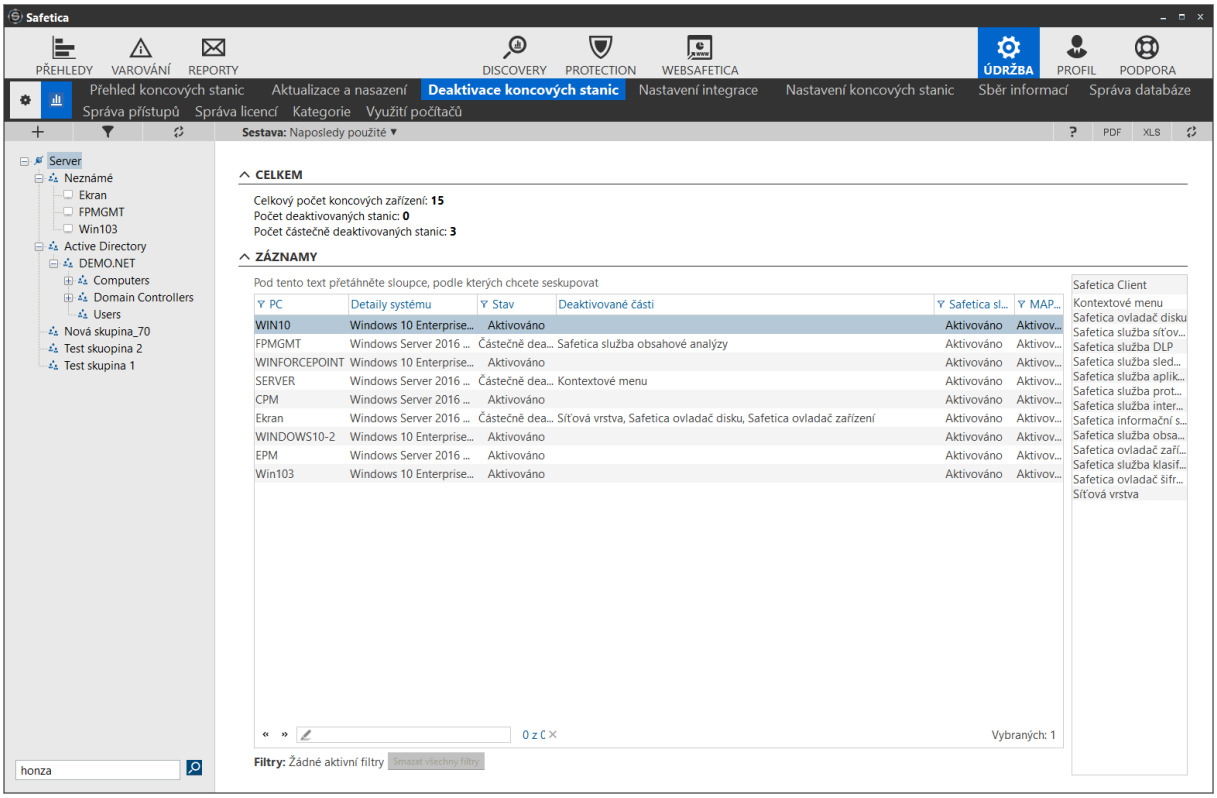
Tímto způsobem je velice jednoduché zjistit, zda klient Safetica nebo jeho komponenta způsobuje vzniklý problém.



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

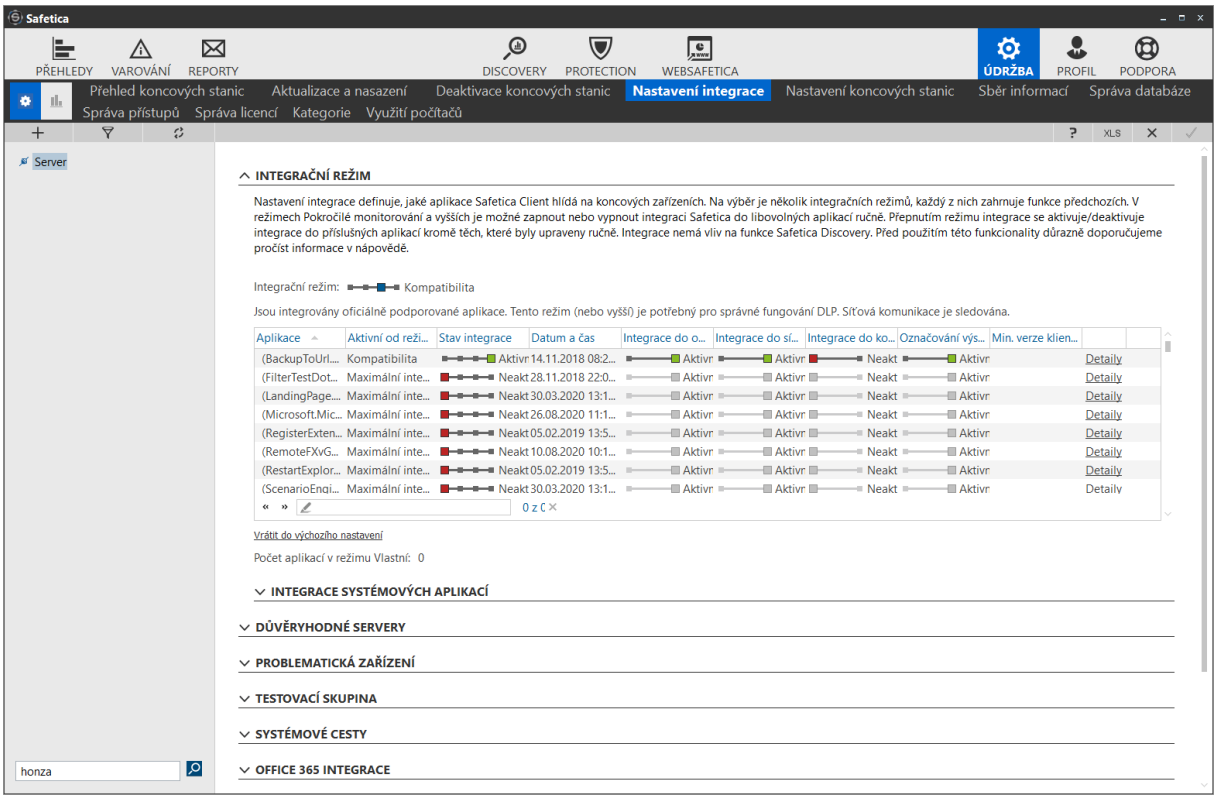
Deaktivace některých modulů vyžaduje restart stanice z důvodu aktivace/deaktivace ovladačů na OS.

Vizualizace zobrazuje stav aktivních a deaktivovaných stanic



10.4. NASTAVENÍ INTEGRACE

Nastavení integrace definuje chování Safetica klienta na koncových stanicích.



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

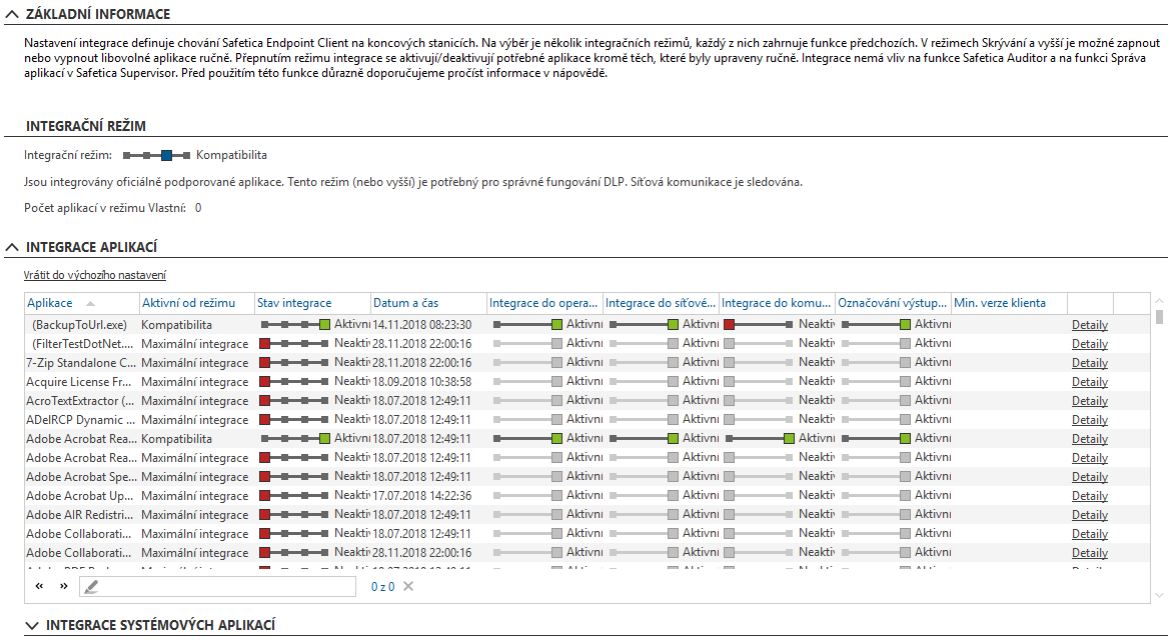
Seznam všech spuštěných aplikací na koncových systémech a jejich integrace se Safetica klientem.

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.



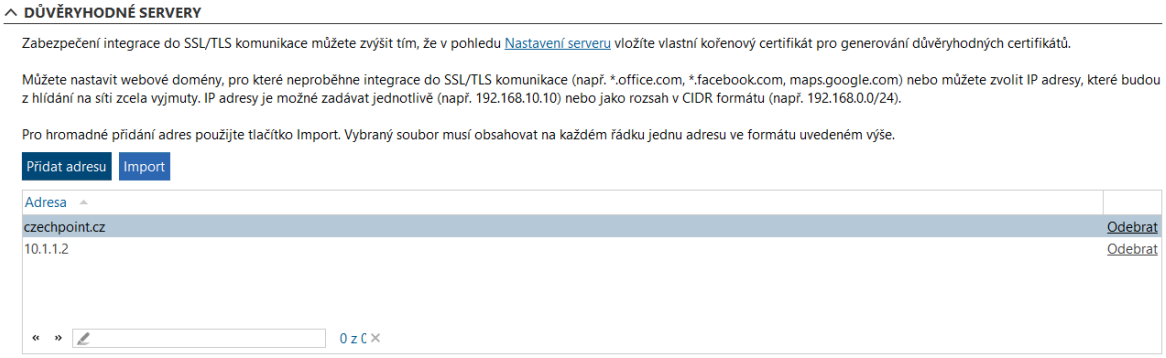
Integraci aplikací je často nutné použít pro aplikace, která nejsou defaultně od výrobce nastaveny. **Vždy je nutné nově integrovanou aplikaci otestovat.**

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.



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.

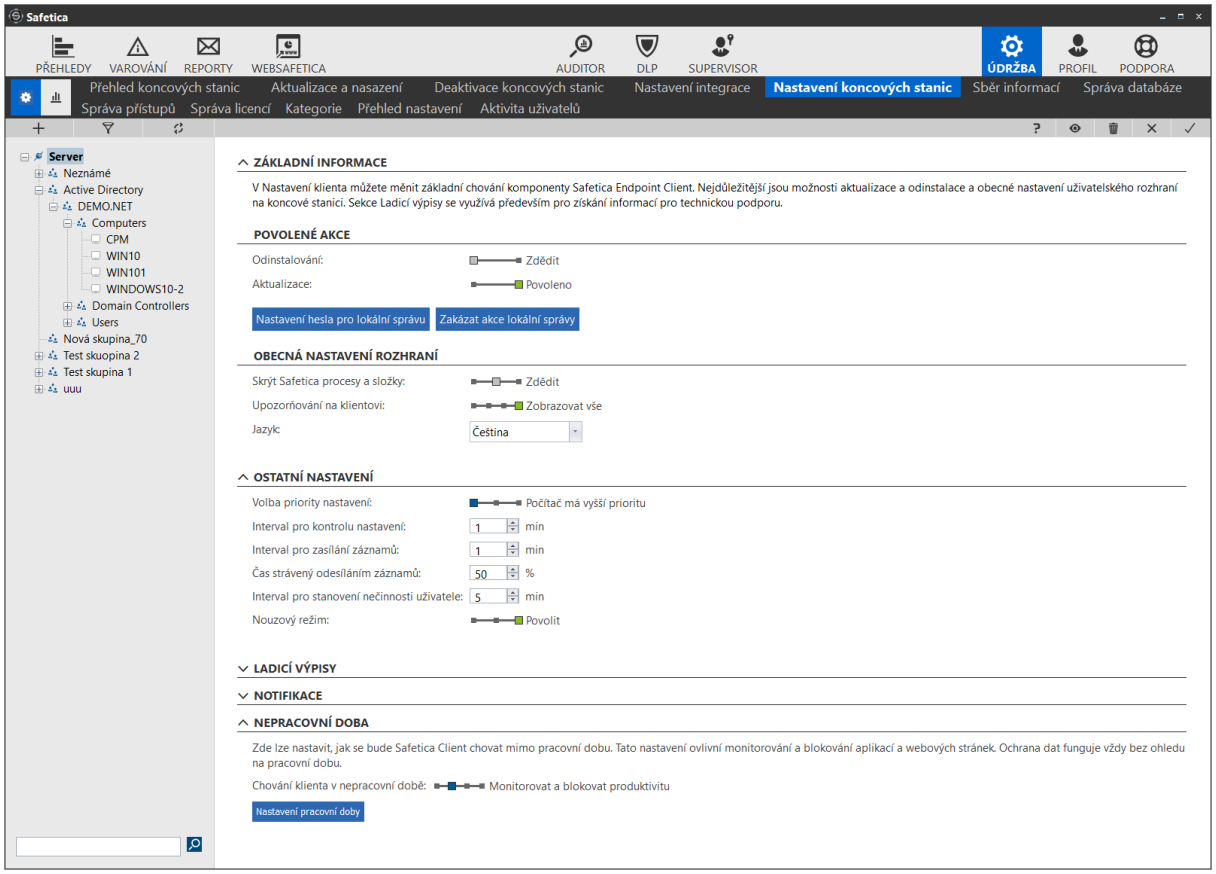
Příkladem mohou být čtečky karet.

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

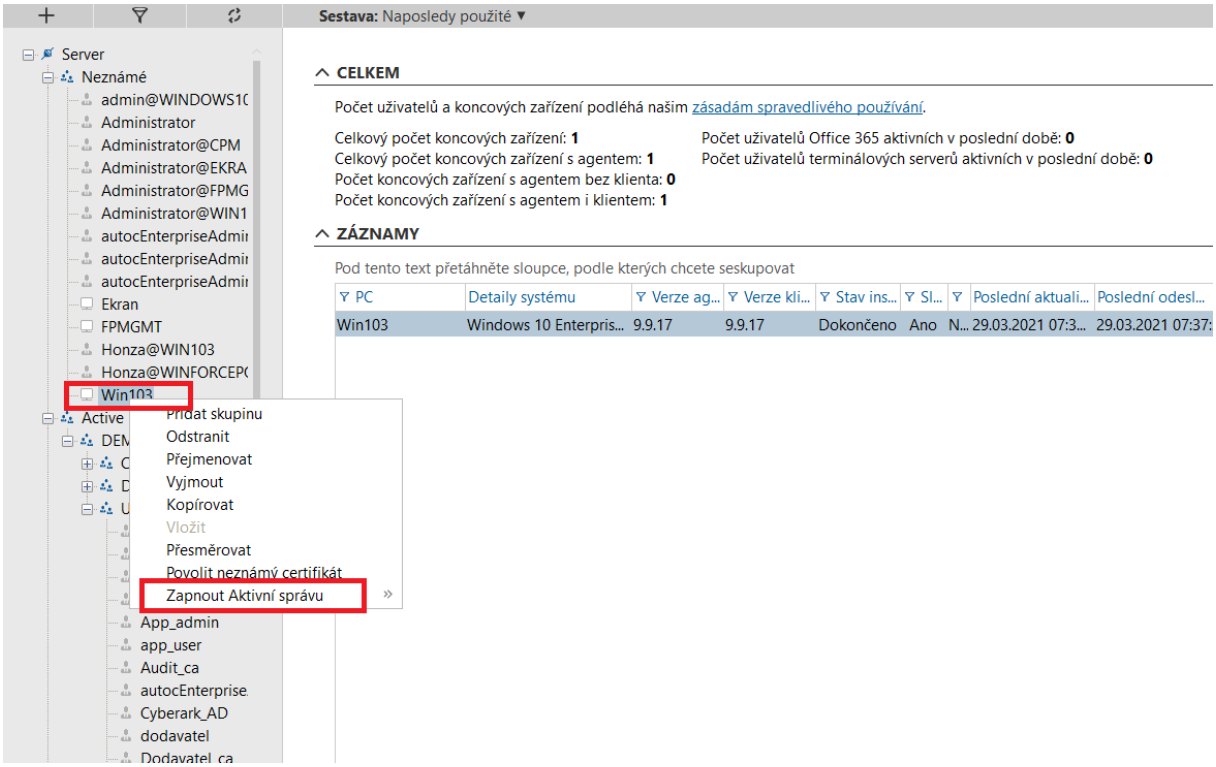


10.6. SBĚR INFORMACÍ

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“

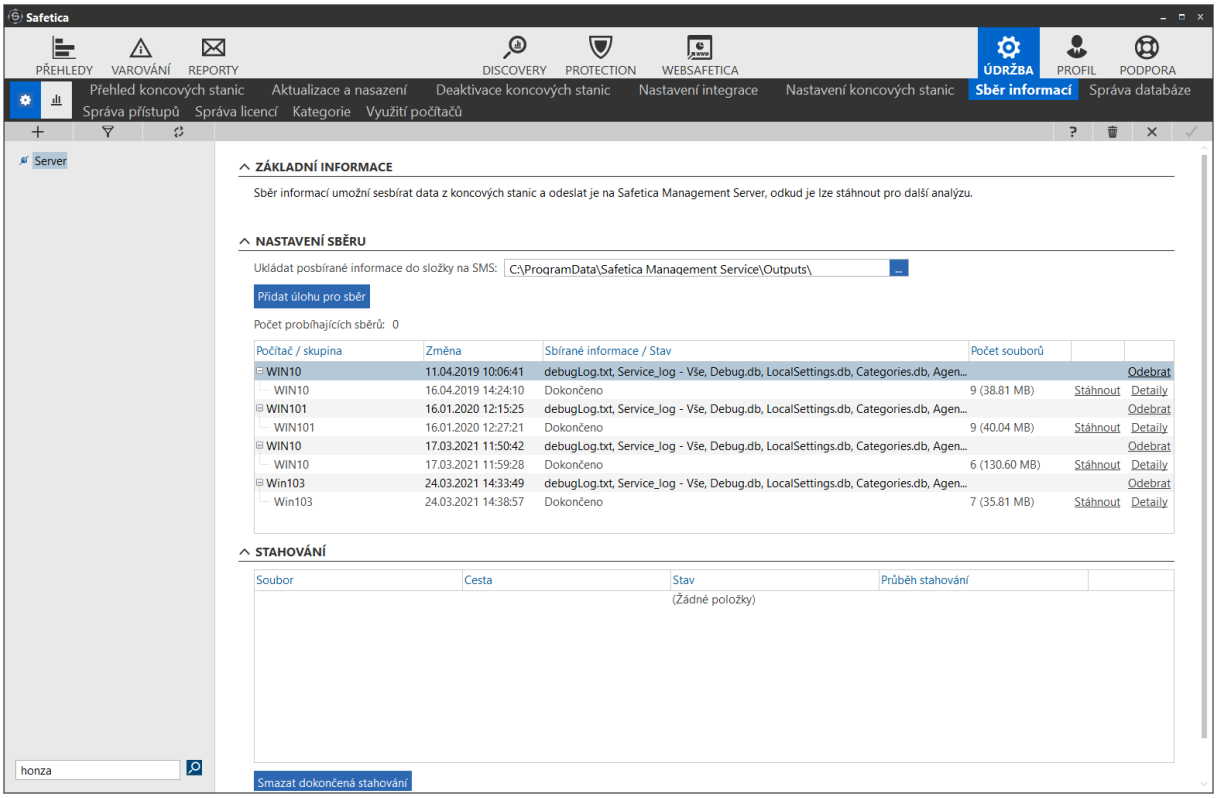


Zapnutím aktivní správy dojde na pracovní stanici k zapnutí detailního logování.

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

Aktivní logování je možné opět v kontextovém menu následně vypnout.

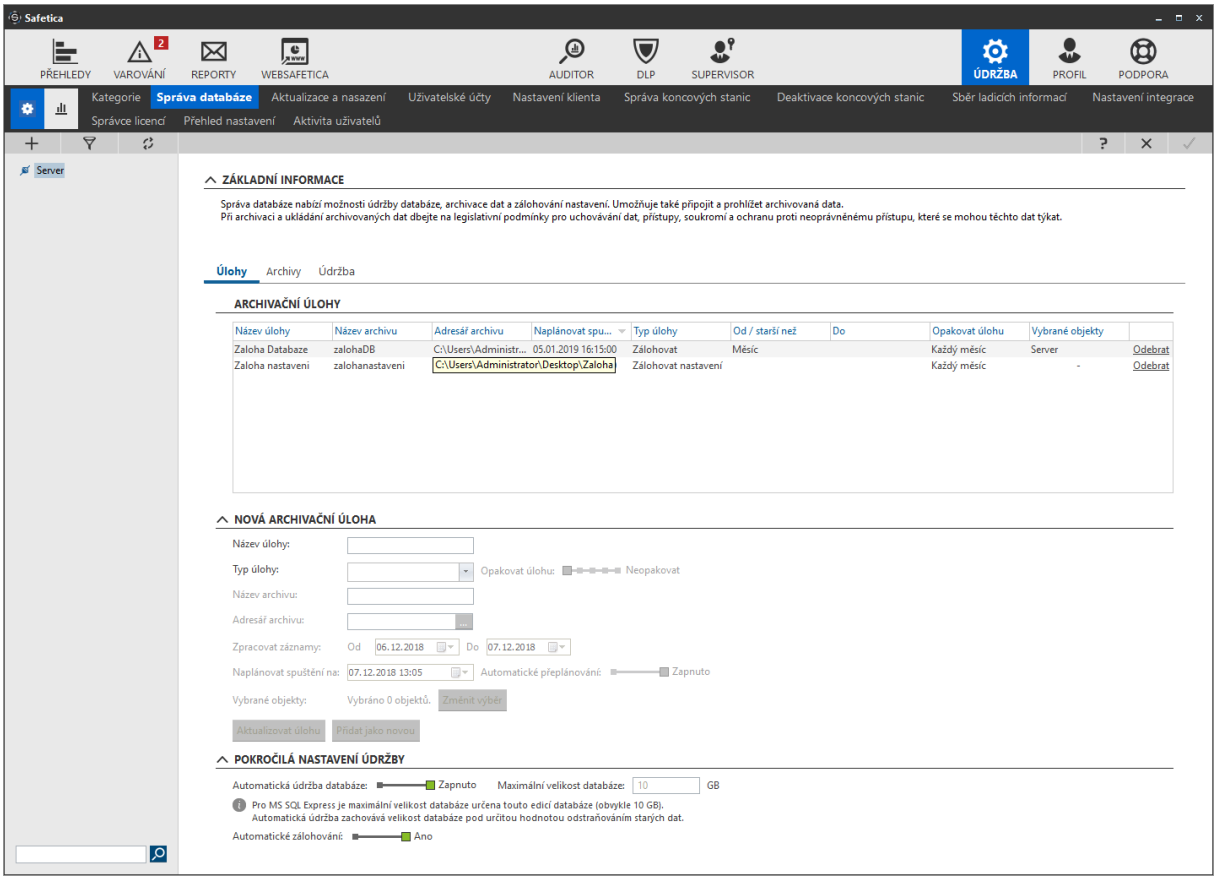
Veškeré logové informace jsou následně na pracovní stanici shromážděny a zaslány na management konzoli, odkud je možné tyto informace stáhnout a odeslat výrobci na hloubkovou analýzu.



10.7. SPRÁVA DATABÁZE

Správa databáze umožňuje definovat úlohy pro

- Zálohu databáze
- Odstranění dat z databáze
- Zálohu konfigurace



Dále je možné definovat archivaci databáze a její údržbu

10.8. SPRÁVA PŘÍSTUPŮ

Umožňuje definovat uživatele Safetica management konzole.

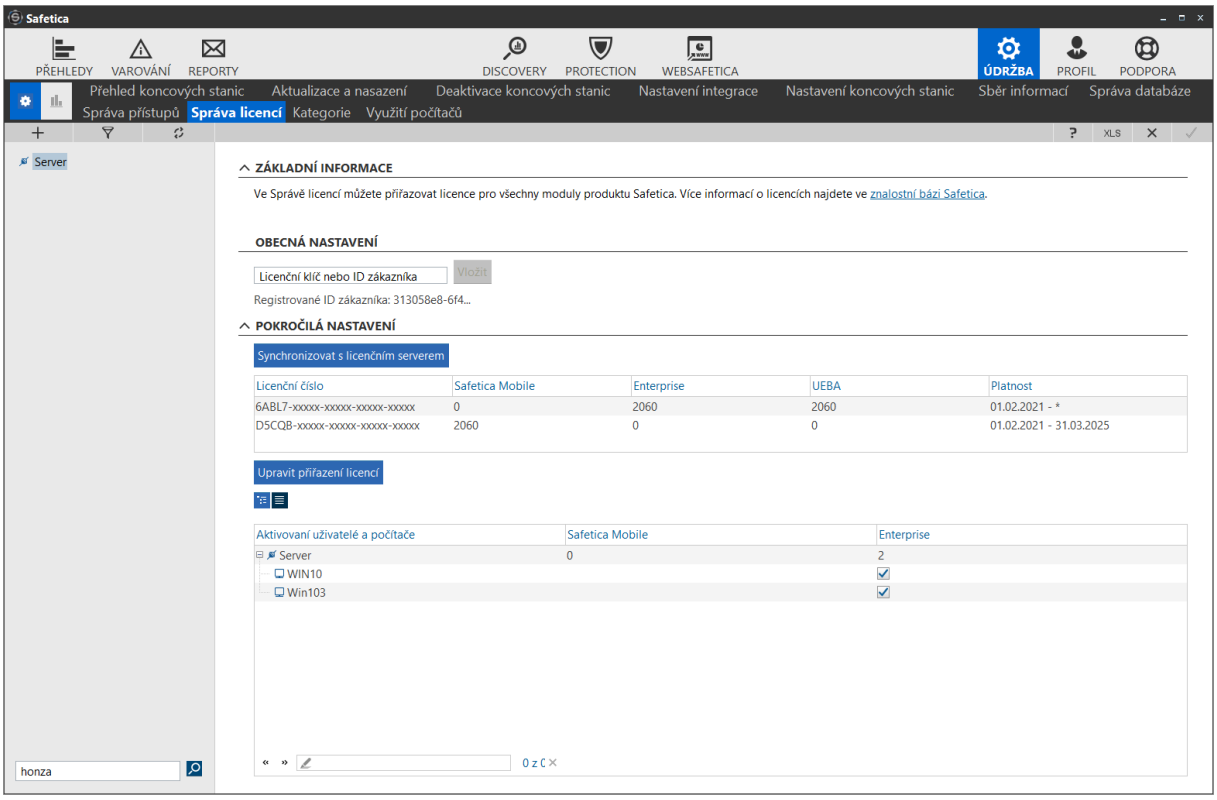
Detailní nastavení je v kapitole 8

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.



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

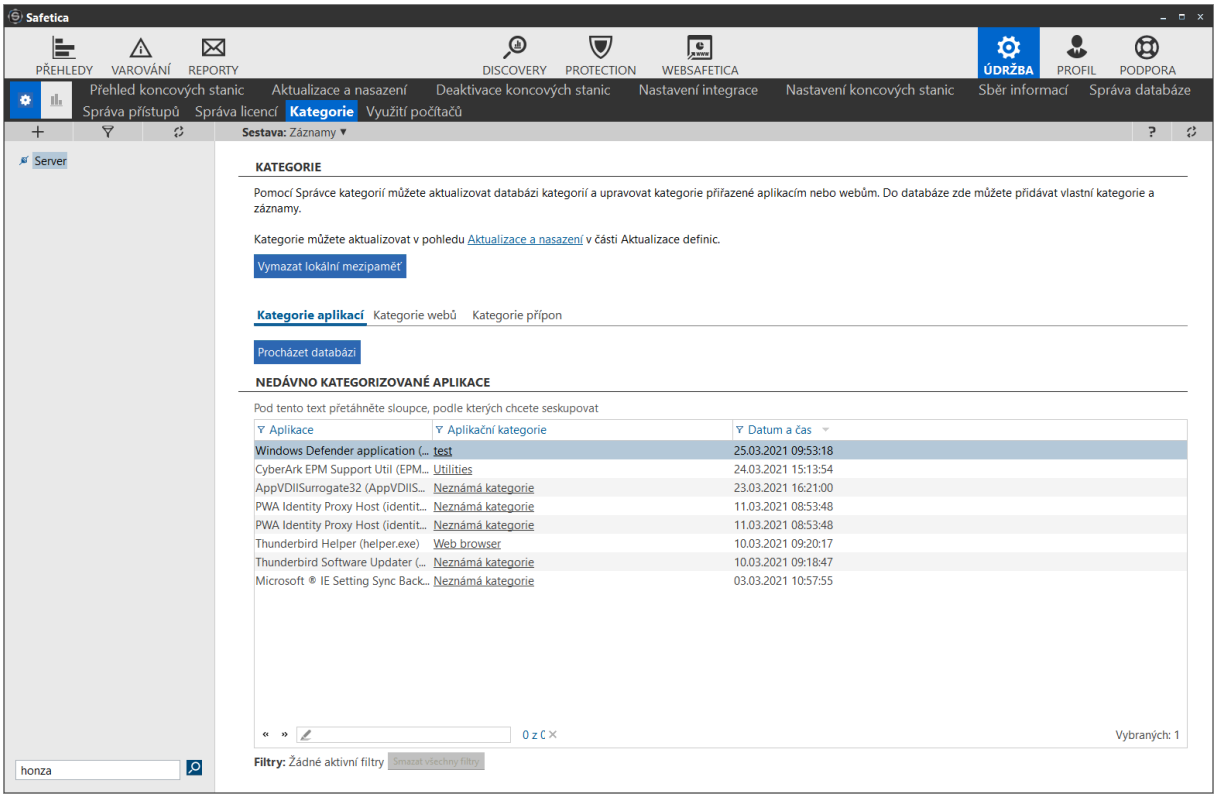
Zobrazuje seznam aplikací a jejich kategorizaci.

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“

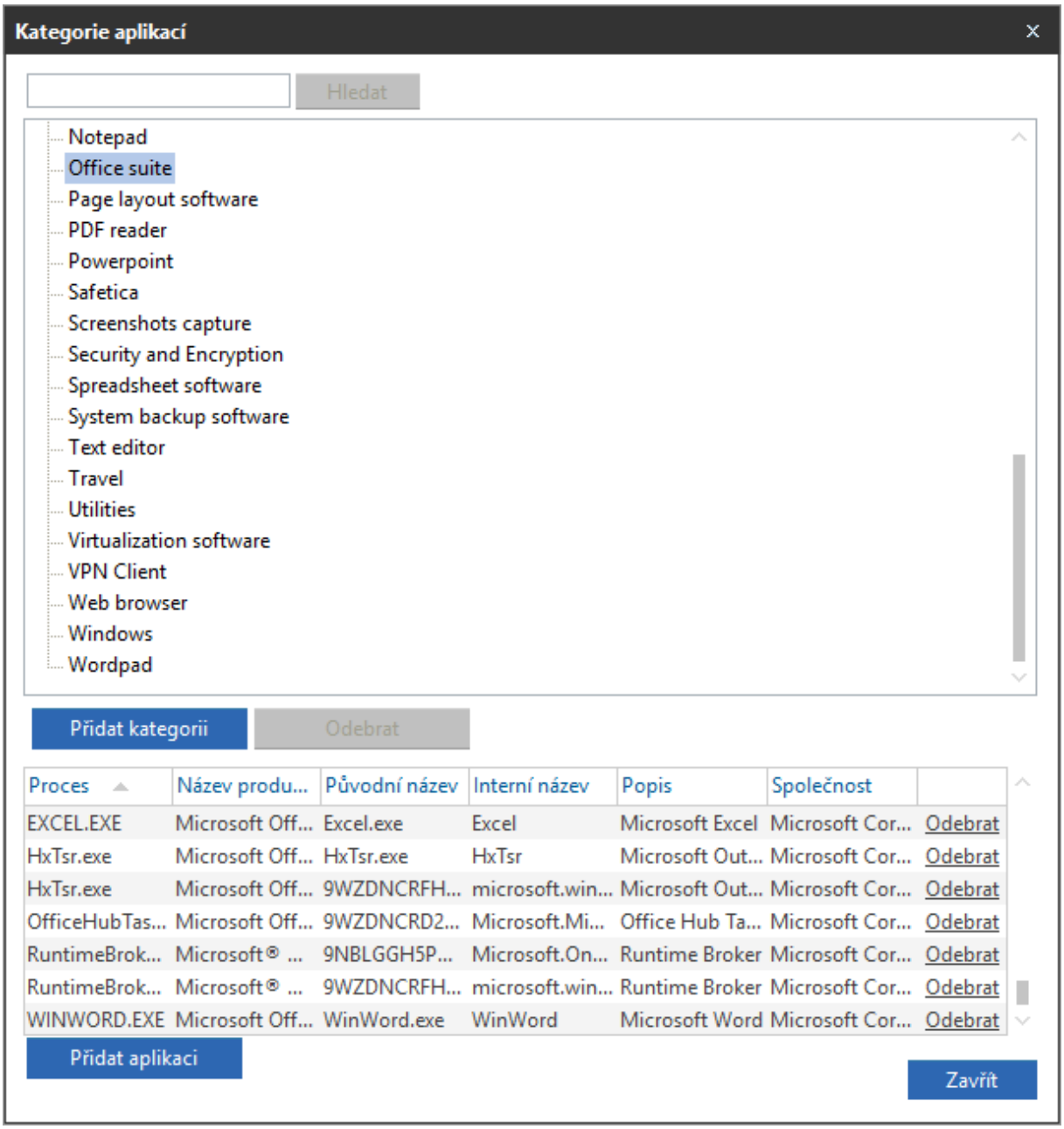
Každou neznámou aplikaci je možné manuálně kategorizovat do již stávajících kategorií, nebo do vlastní kategorie.

Základní nastavení kategorií aplikací



Databáze kategorií aplikací.

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



10.10.2. KATEGORIE WEBŮ

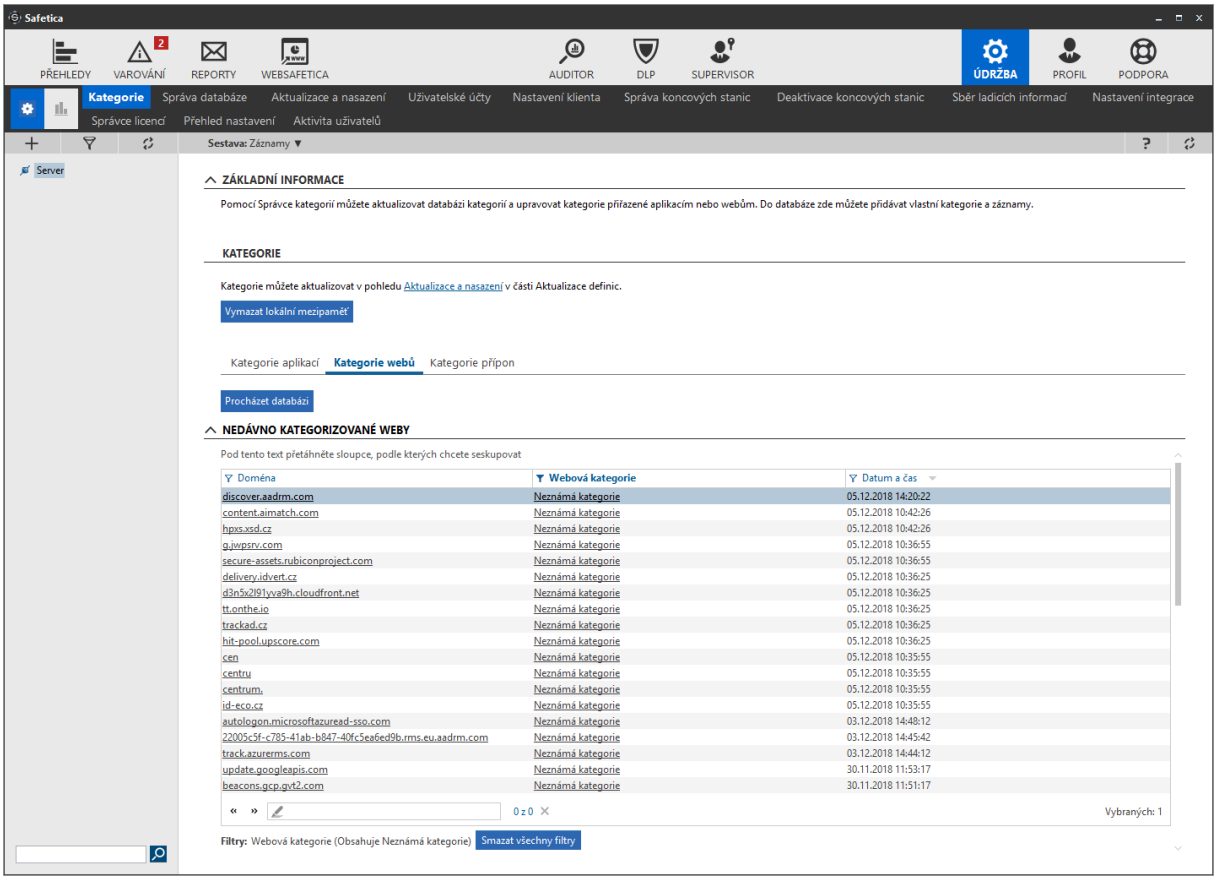
Zobrazuje seznam webů a jejich kategorizaci.

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“

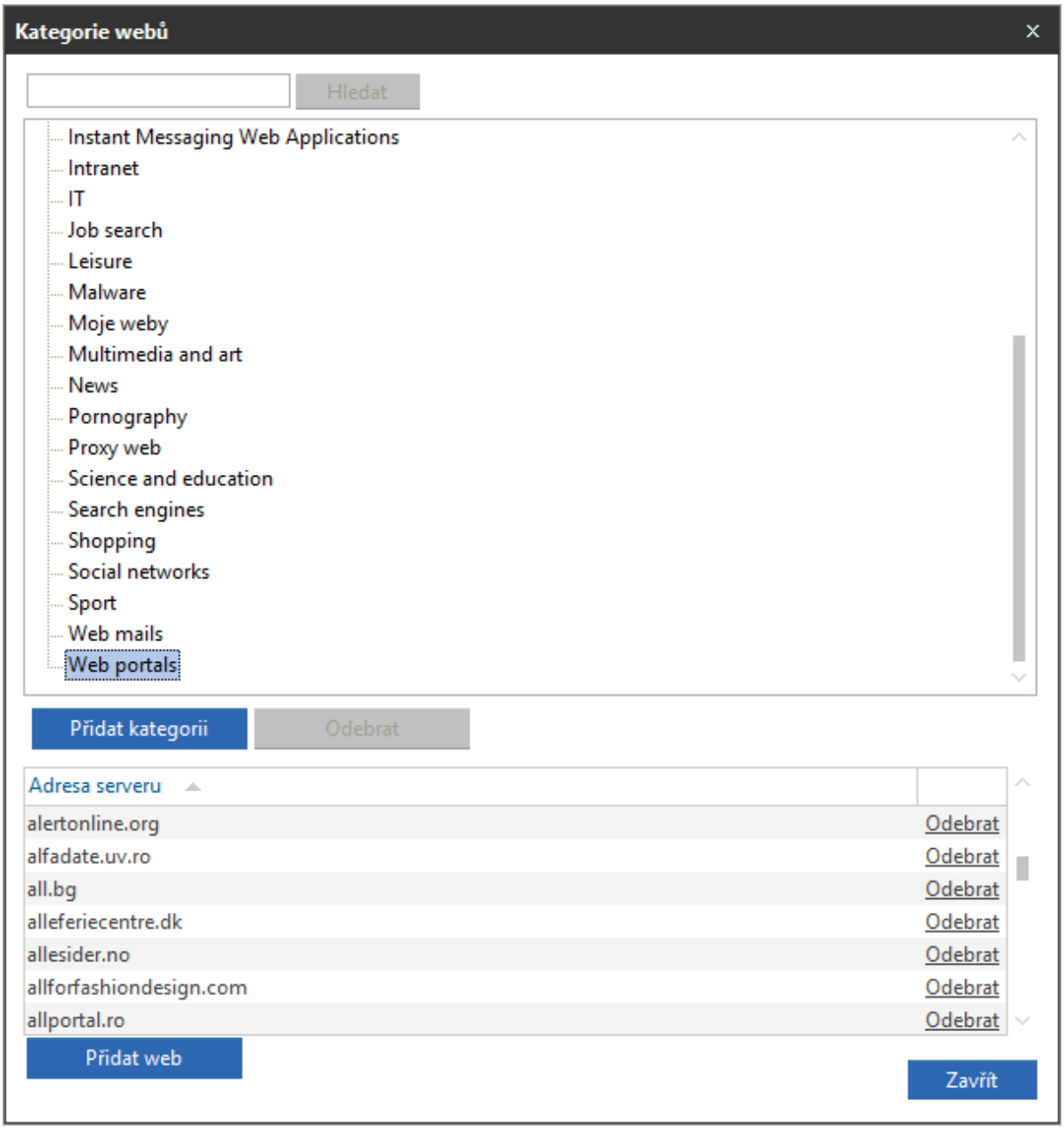
Každý neznámý web je možné manuálně kategorizovat do již stávajících kategorií, nebo do vlastní kategorie.

Základní nastavení kategorií webů



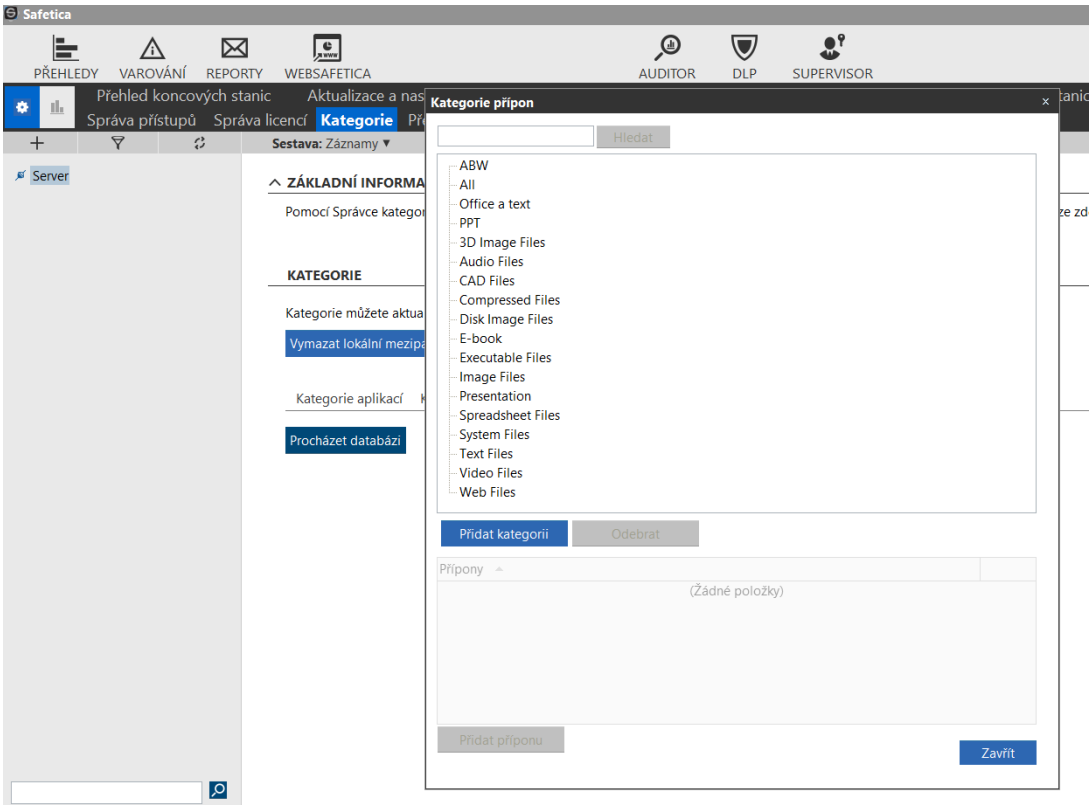
Databáze kategorií webů

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

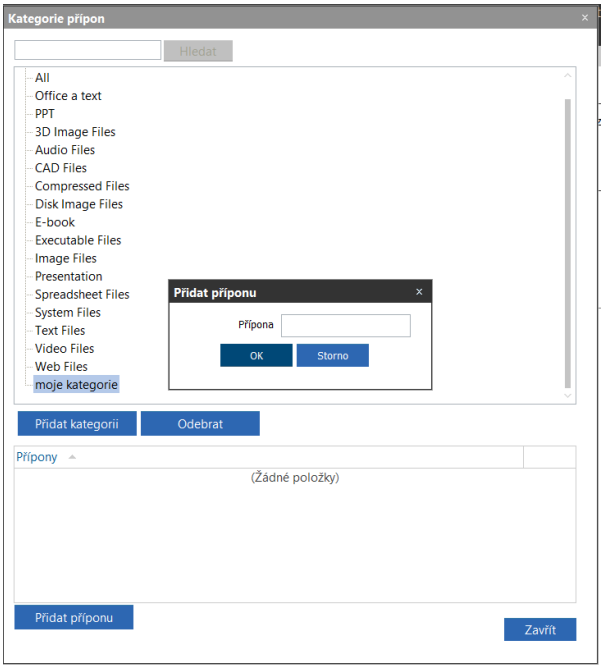


10.10.3. KATEGORIE PŘÍPON

Zobrazuje seznam přednastavených kategorií přípon.



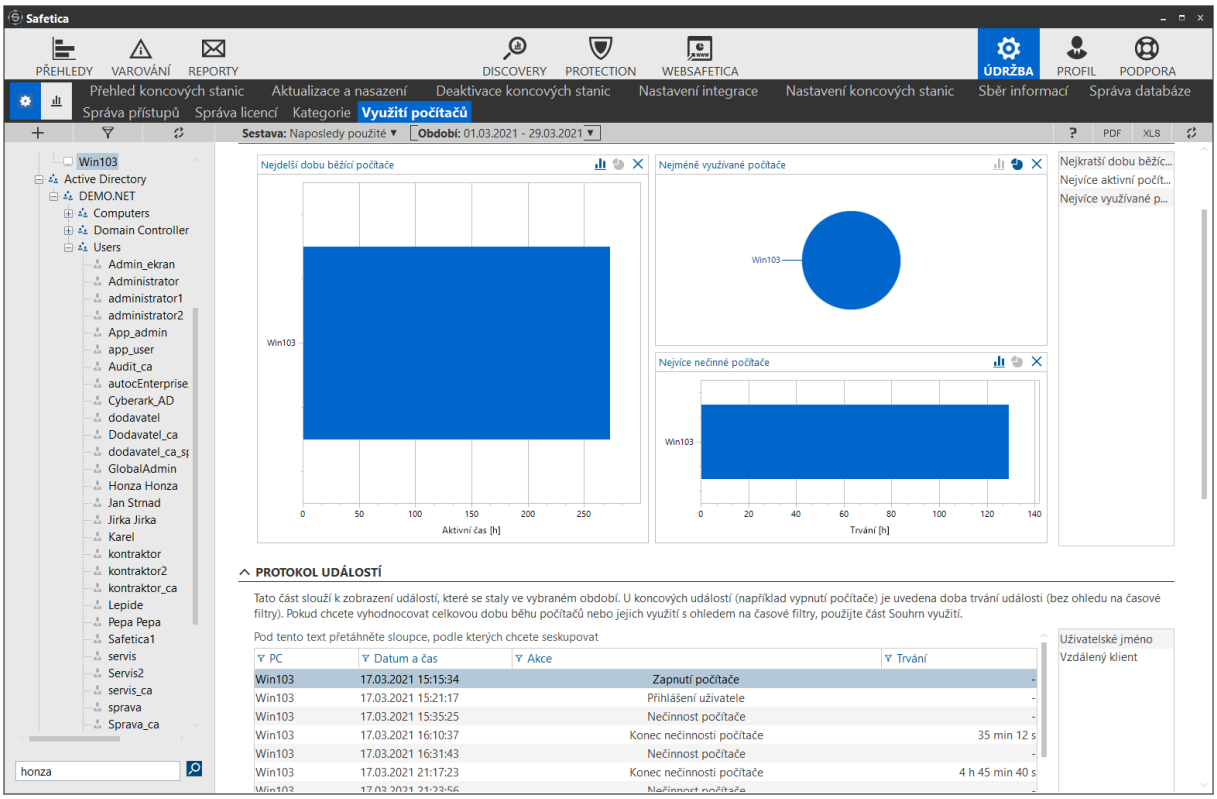
Systém umožňuje vytvářet vlastní kategorie přípon, do kterých se následně definují vlastní přípony souborů



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

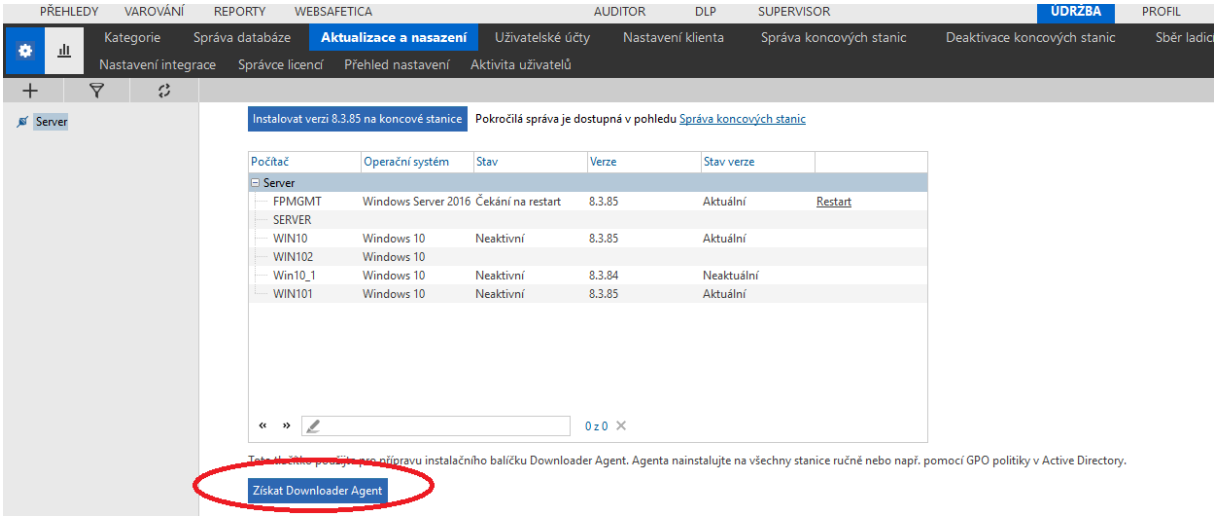
- Agent - Umožnuje jeho vzdálenou instalaci, aktualizaci a další správu. Jedná se o základní SW na klientské stanici, který je možné instalovat jak vzdáleně, například přes GPO, tak pomocí logon scriptu nebo spuštěním instalátoru na klientské stanici. Instalátor je MSI balíček.

- Klient - Klient zajišťuje na koncových stanicích veškeré bezpečnostní a monitorovací funkce. Instaluje se se vzdáleně ze Safetica management konzole pomocí Safetica Agenta, 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



Instalaci je možné provést přes Group policy. Detailní postup instalace je popsán Instalačním manuálu, 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 zvýší oprávnění. Zde bych doporučil provést nastavení z bodu č.10.

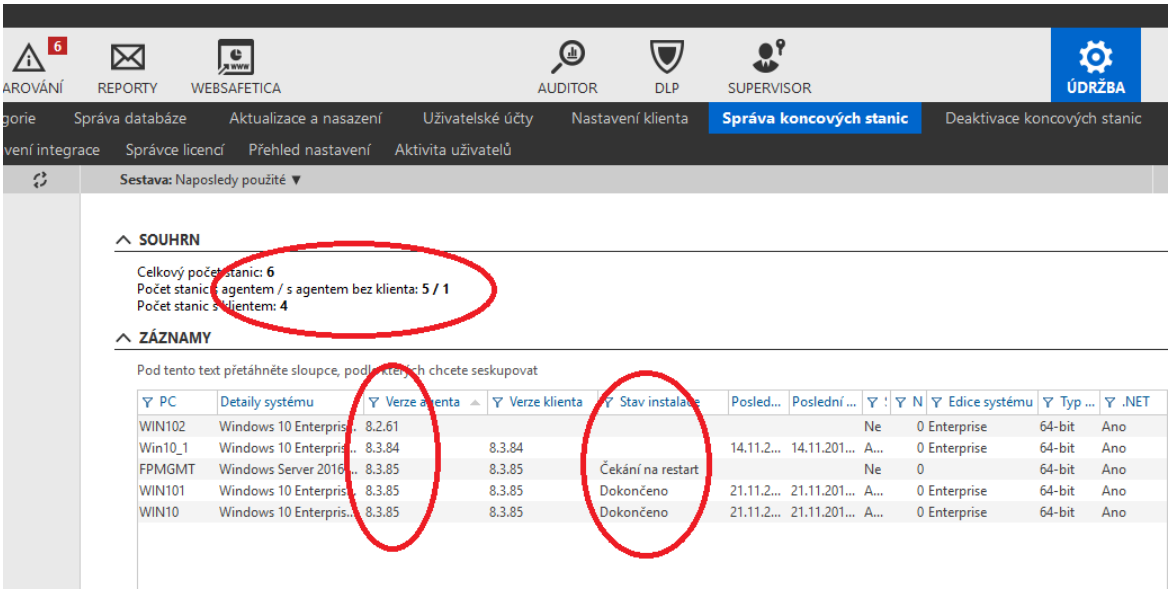
11.2. KONTROLA INSTALACE AGENTA

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.

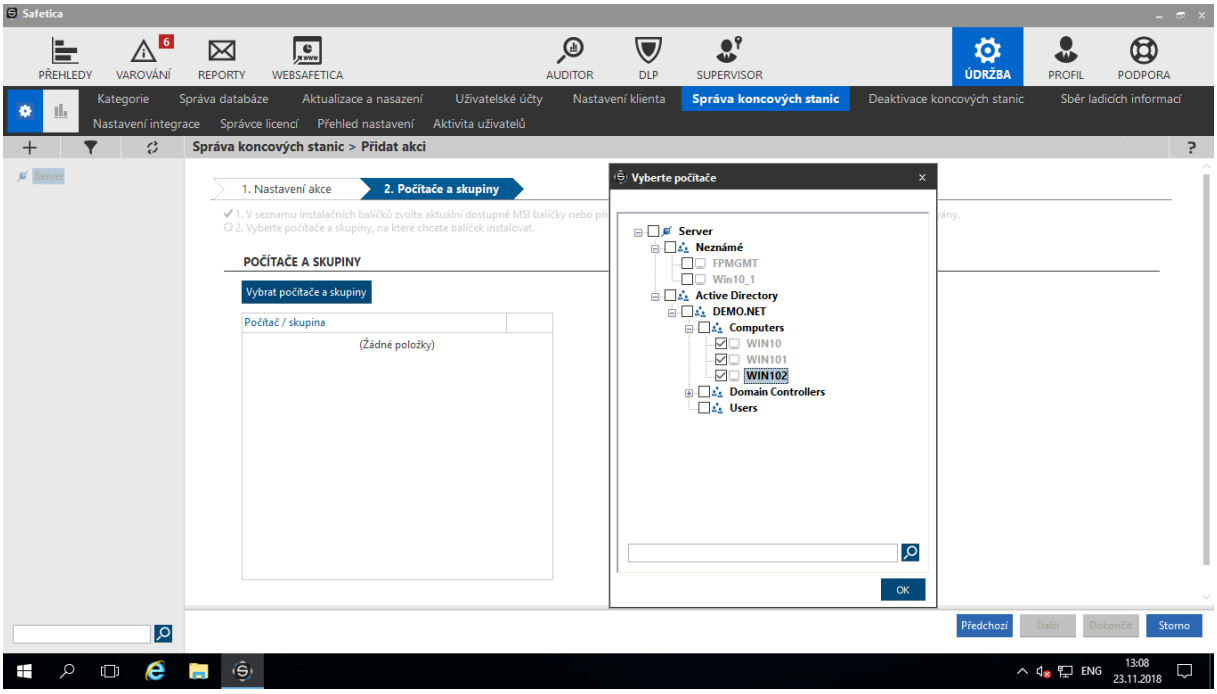


11.3. INSTALACE KLIENTA

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.

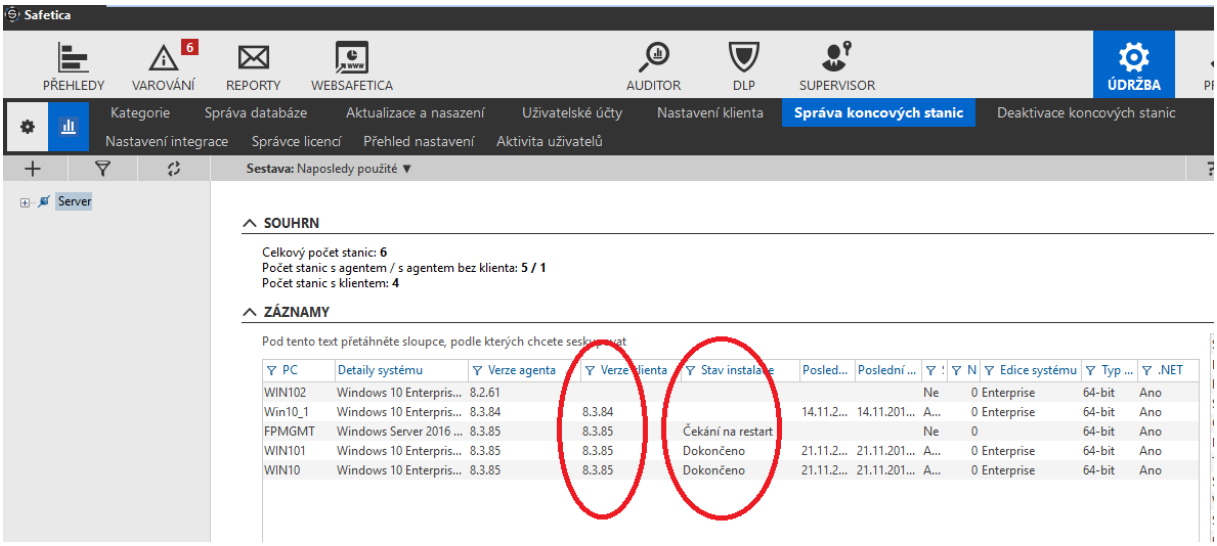
Instalace se provede z management konzole Safetica serveru v Údržba, Správa koncových stanic spuštěním průvodce instalací Instalovat / Aktualizovat. Budou zvoleny klientské stanice definované v předchozím kroku, viz příklad:



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.

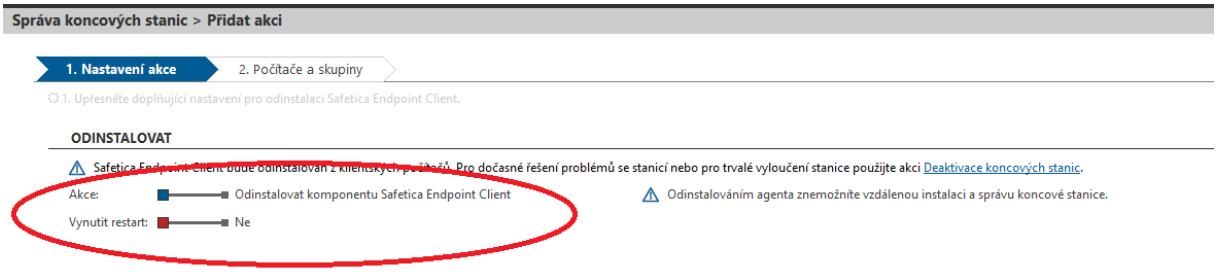


11.5. ODINSTALACE KLIENTA

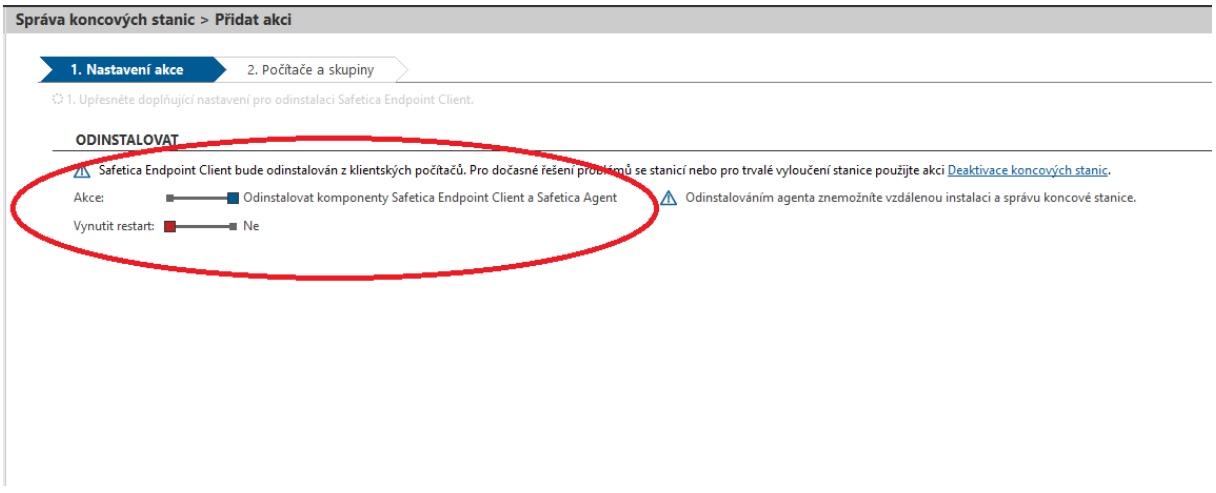
V případě nutnosti odinstalace klient je možné využít úlohu, která zajistí odebrání Safetica klienta popřípadě Safetica klienta i agenta z konkrétního počítače, nebo hromadně z více definovaných zařízení.

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

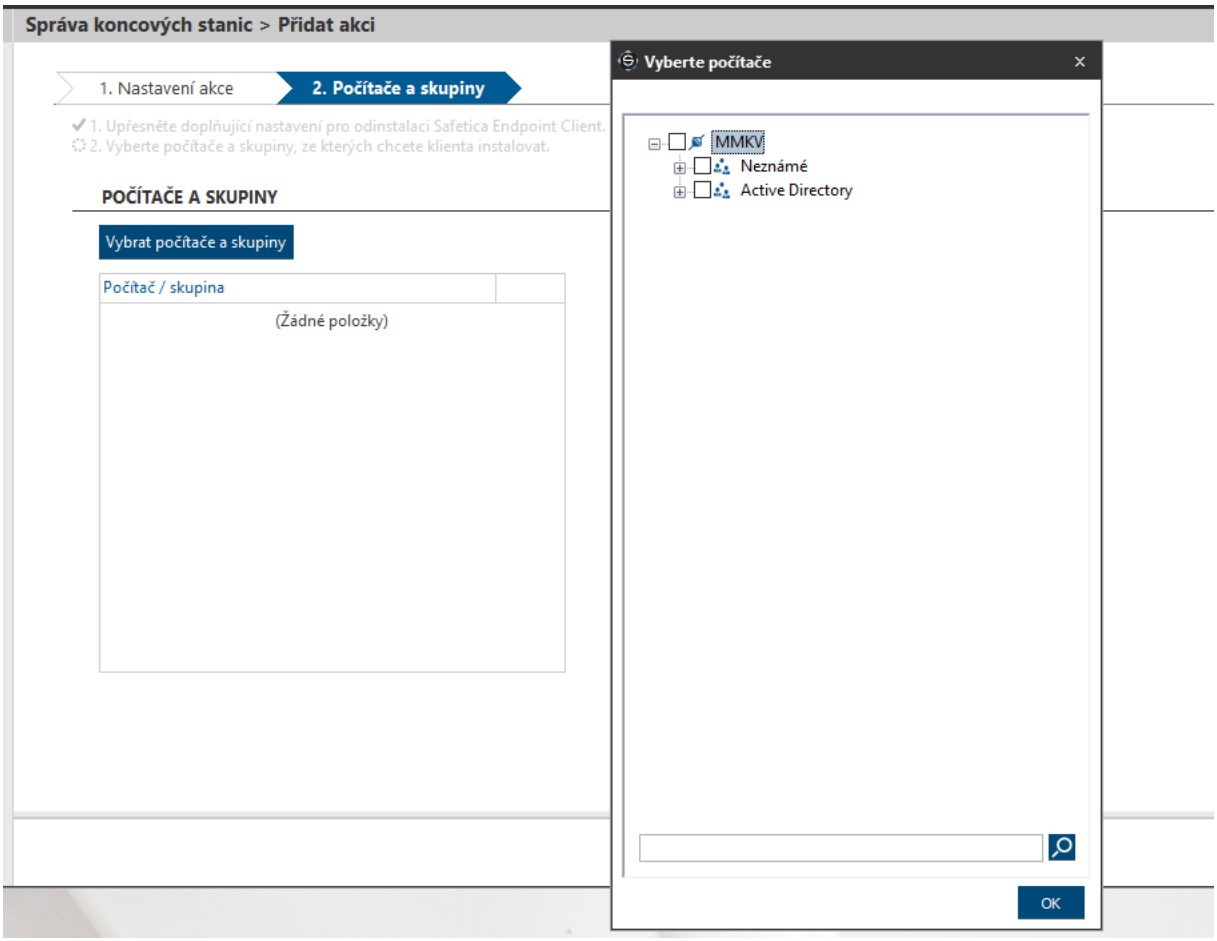
Volba možností odinstalace – odinstalace klienta



Volba možností odinstalace – kompletní odinstalace klienta i agenta



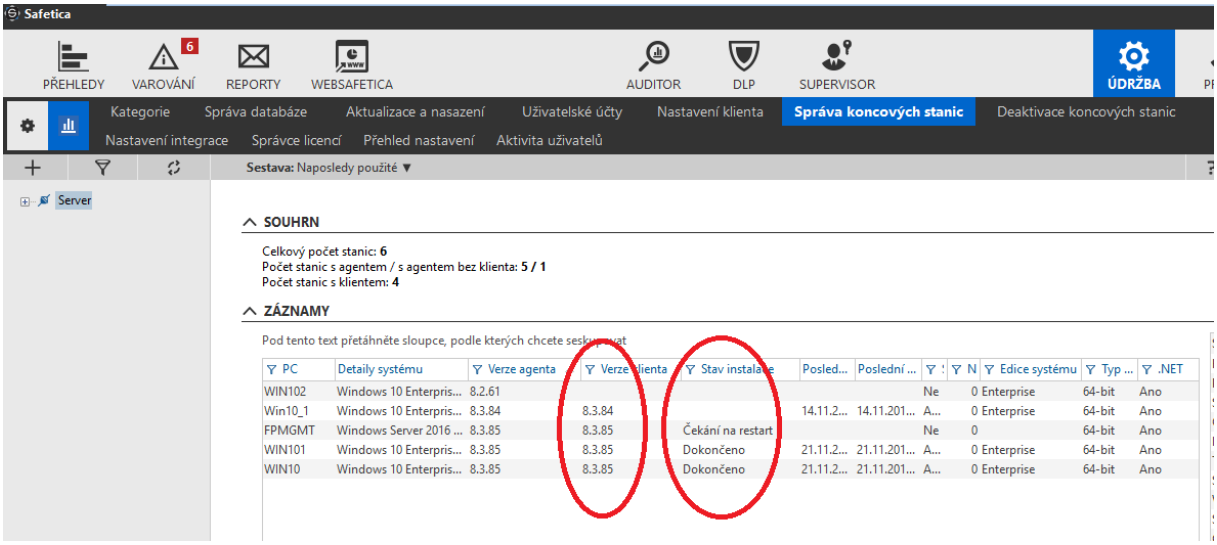
Výběr zařízení, kde dojde k odinstalaci Safetica komponent:



11.6. KONTROLA ODINSTALACE KLIENTA

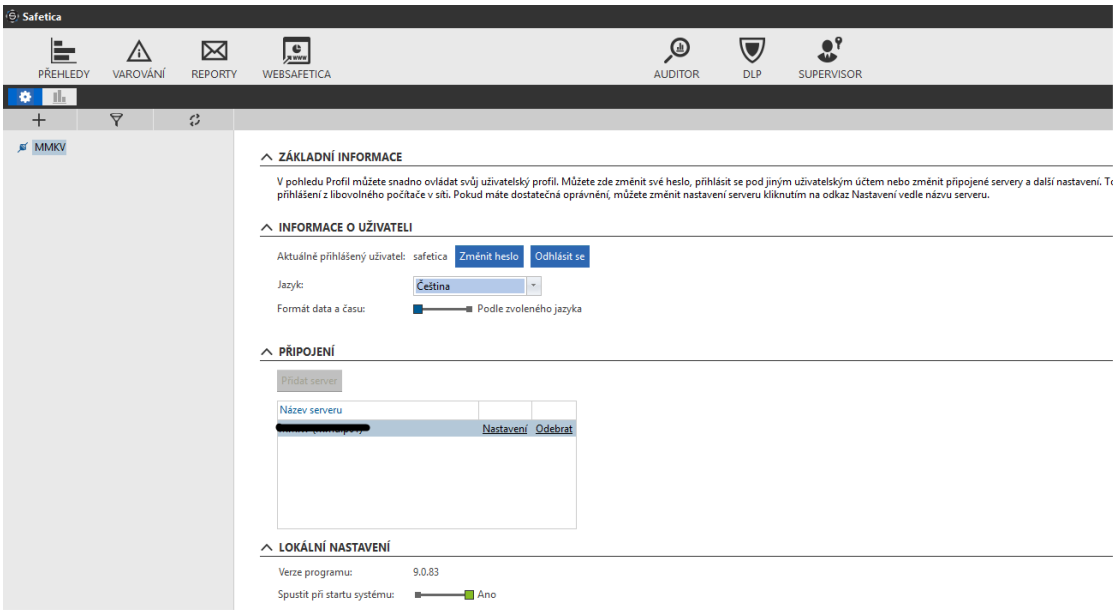
Po odinstalaci je potřeba provést kontrolu, zda se Safetica klient úspěšně odinstaloval, popřípadě na kterých klientských počítačích odinstalace selhala.

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.

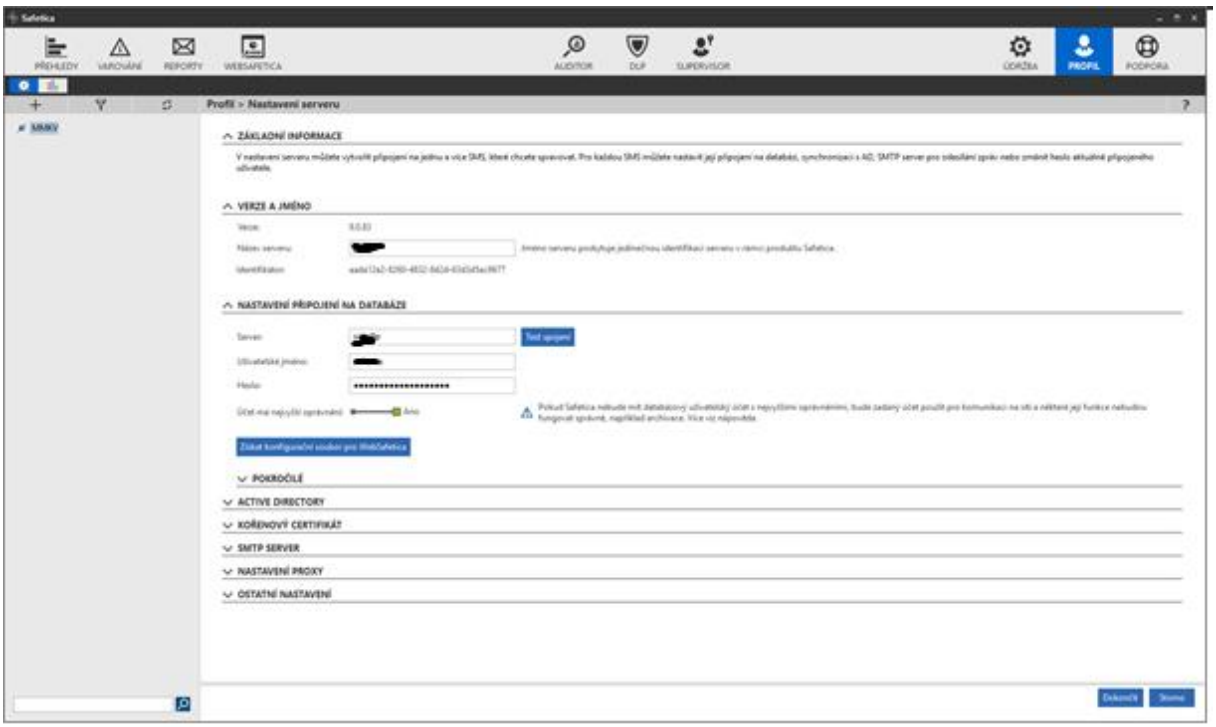

Safetica
PŘEHLEDY
VAROVÁNÍ
6
REPORTY
WEBSAFETICA
AUDITOR
DLP
SUPERVISOR
ÚDRŽBA
Kategorie
Správa databáze
Aktualizace a nasazení
Uživatelské účty
Nastavení klienta
Správa koncových stanic
Deaktivace koncových stanic
Nastavení integrace
Správce licencí
Přehled nastavení
Aktivita uživatelů
Sestava: Naposledy použité
Server
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 ...
Edice systému
Typ ...
.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

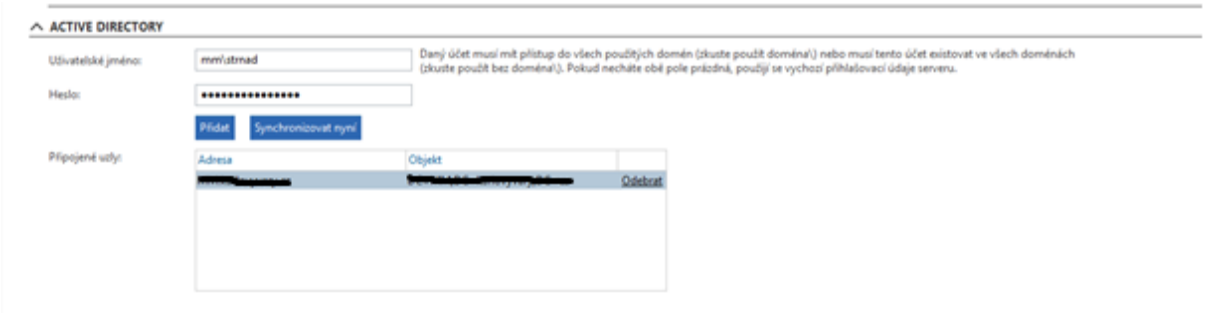
Profil umožňuje základní nastavení pro správu Safetica management konzole a databáze.



- 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.

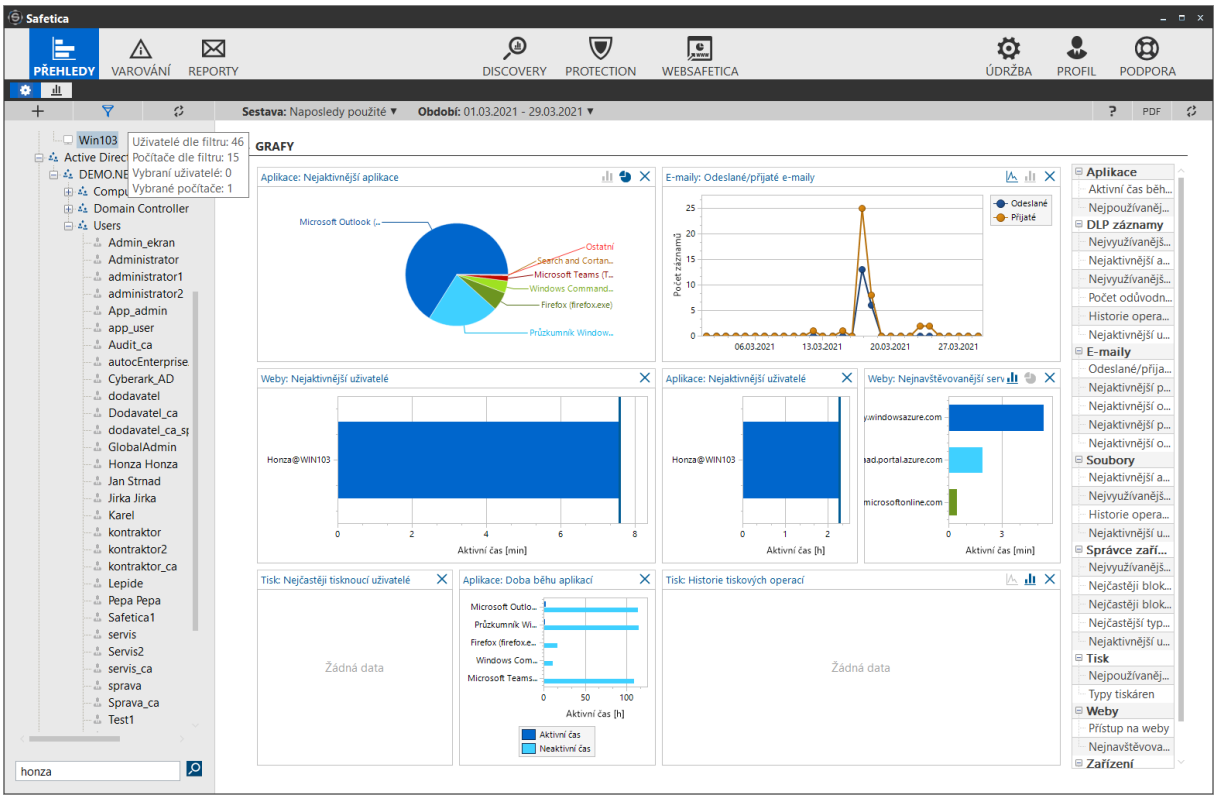
Jde o dashboardy, které zobrazují aktuální stav práce uživatelů a detekce událostí.

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

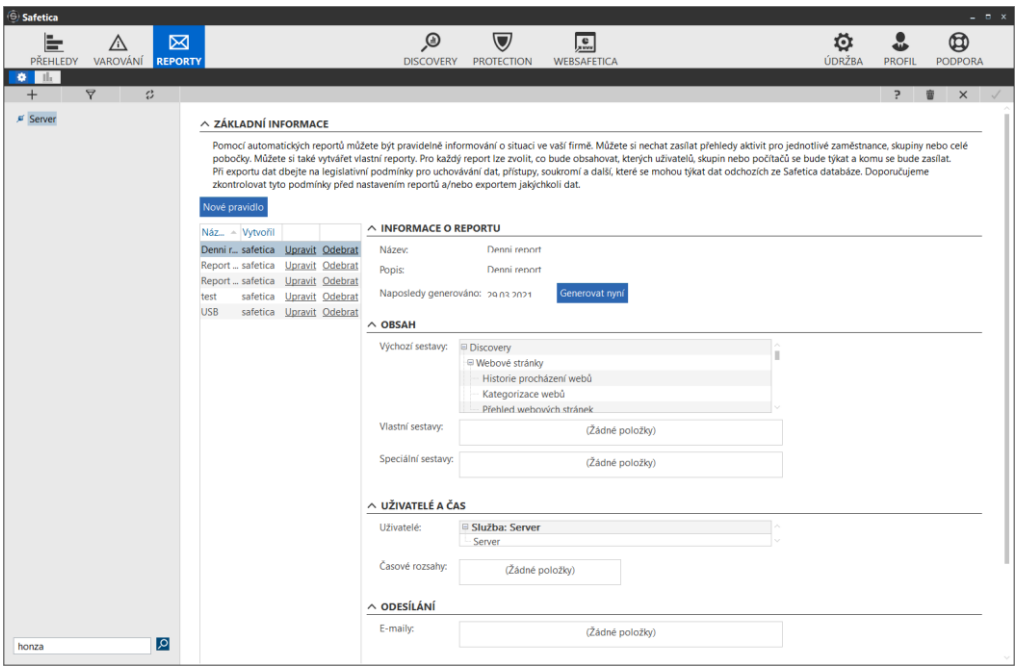
V horní liště je možné vybrat časové období k zobrazení, levý sloupec umožňuje vybrat počítač, uživatele nebo skupiny, popřípadě zobrazit stav za celou společnost.

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



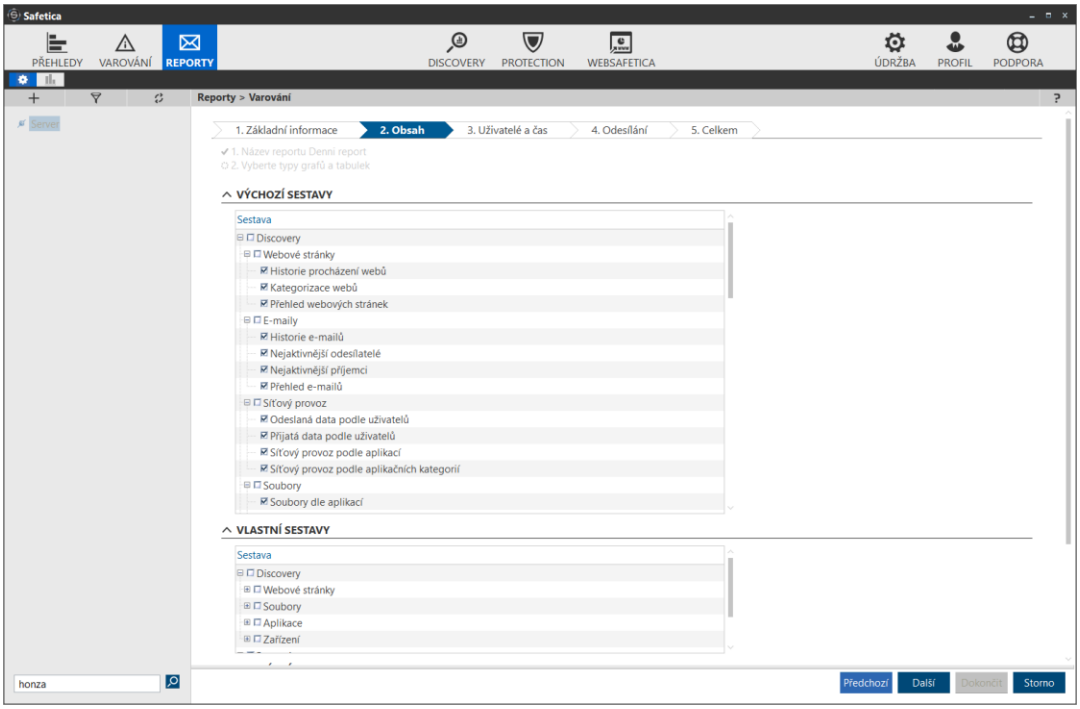
14. REPORTY

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

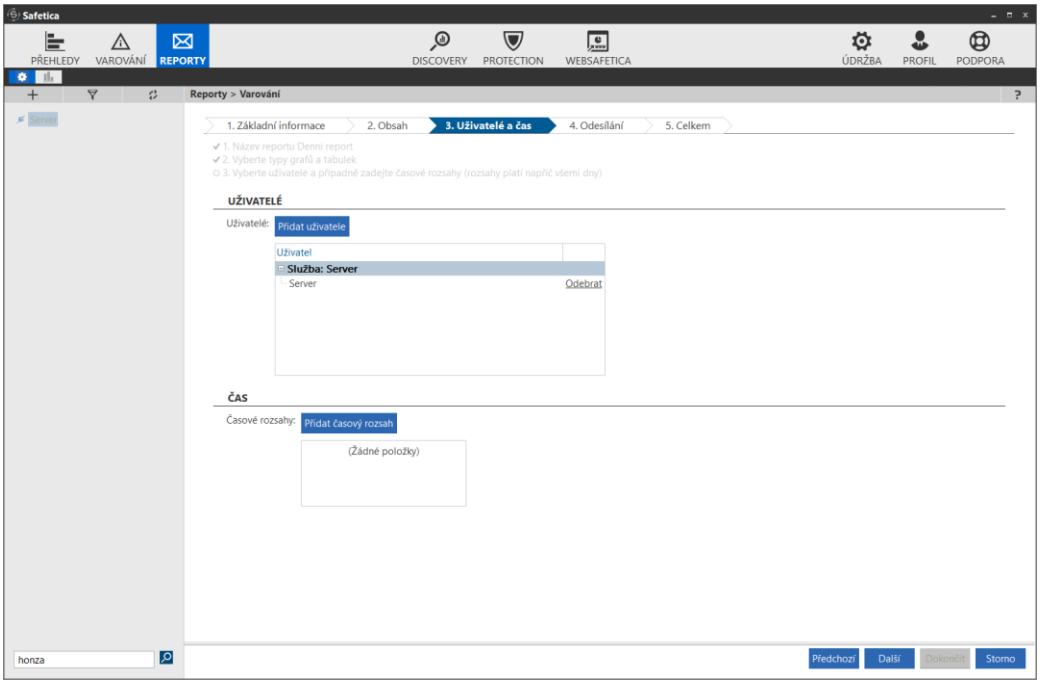


Je možné vytvořit různé reporty s obsahem, který se podle definice odešle na definovaného managera v nastaeném čase.

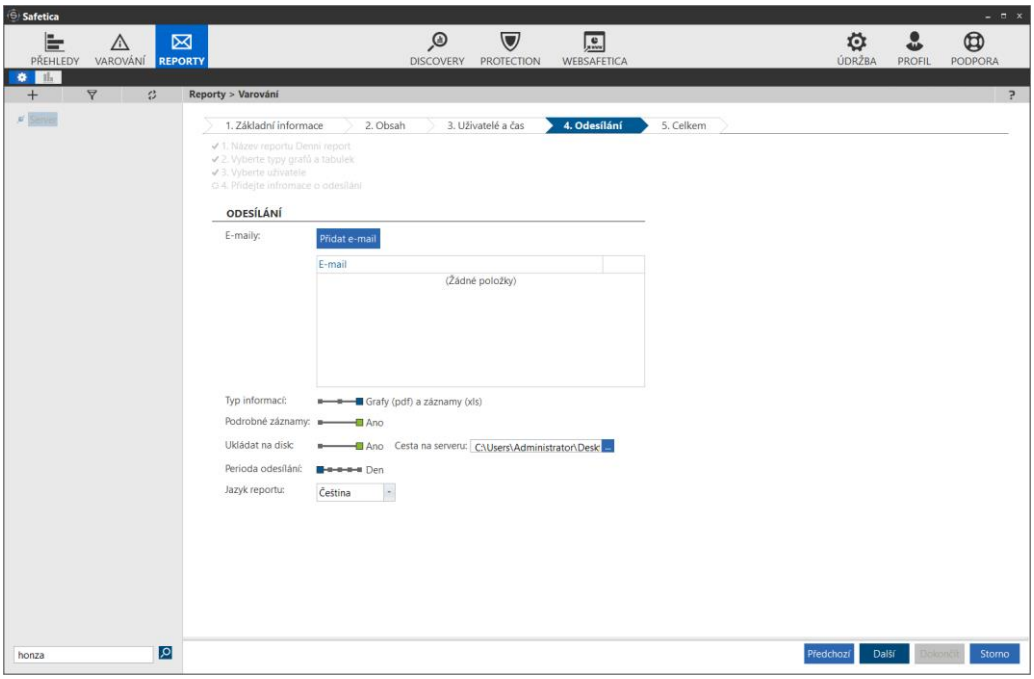
V rámci nastavení je možné zvolit kategorii událostí:



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.

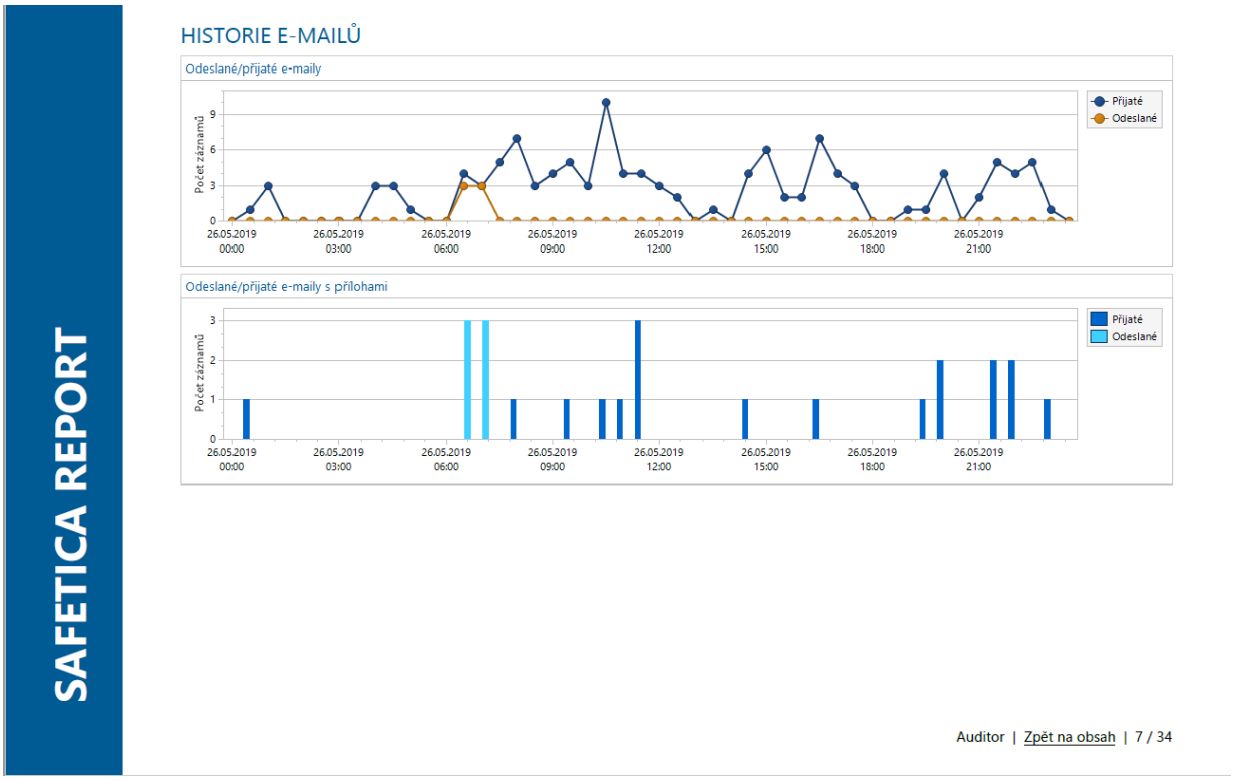


Report je možné zasílat emailem na definované uživatele.

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

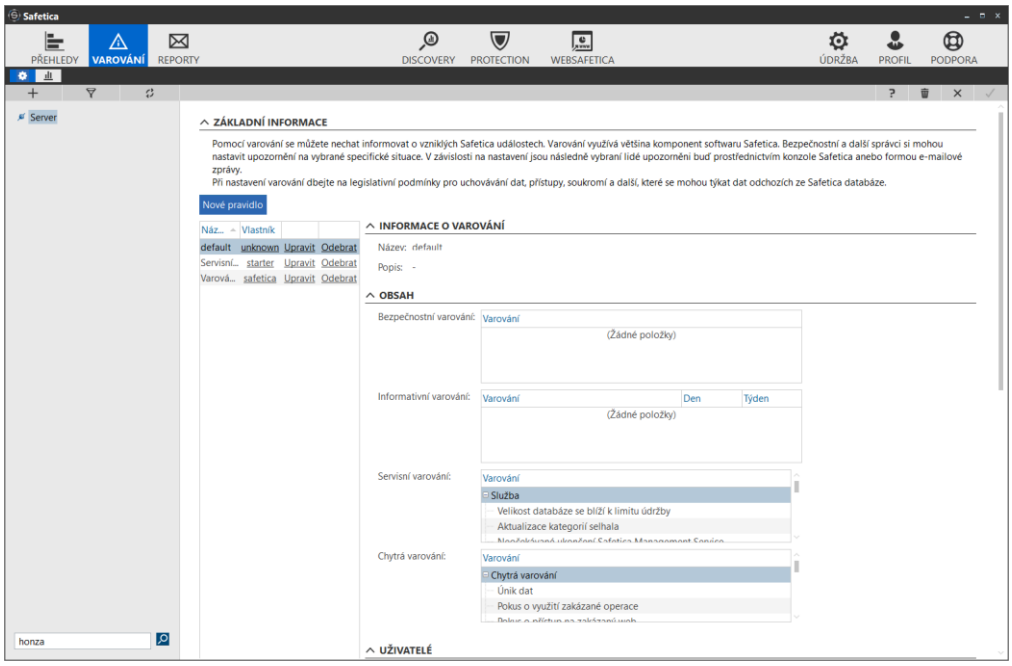
Je možné report uložit na disk podle specifikované cesty a nastavit periodu odesílání.

Příklad Safetica reportu:

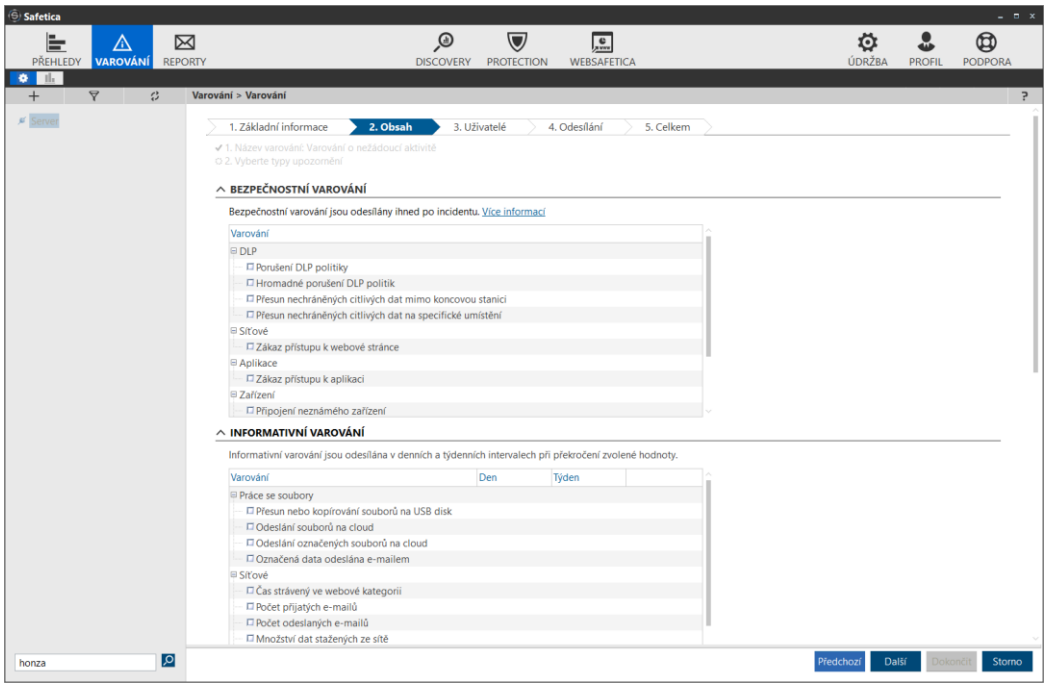


15. VAROVÁNÍ – NOTIFIKACE

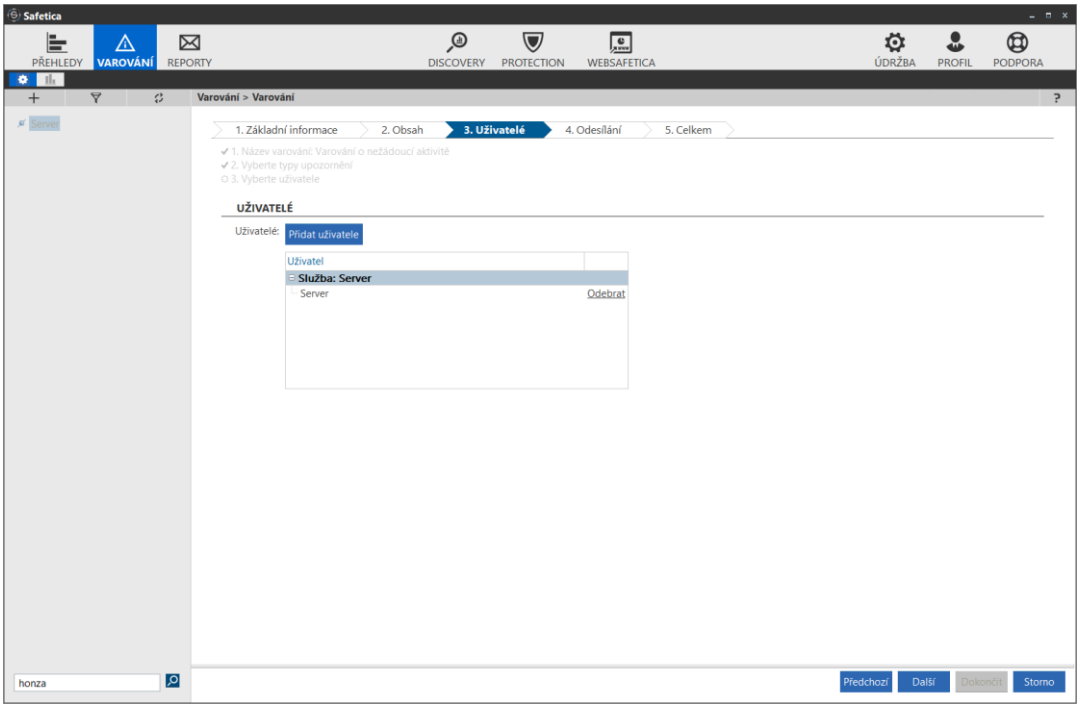
Systém umožňuje nastavit notifikace událostí Safetica systému na email nebo do SIEM systému.



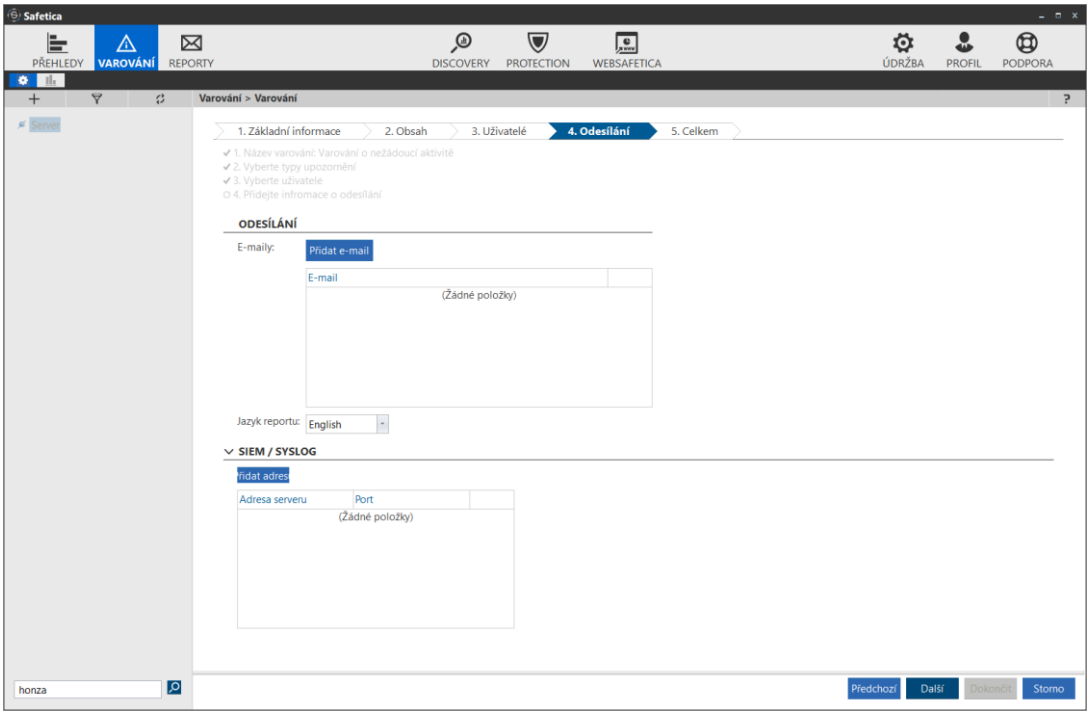
Je možné vybrat typ události, která bude odesílána:



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

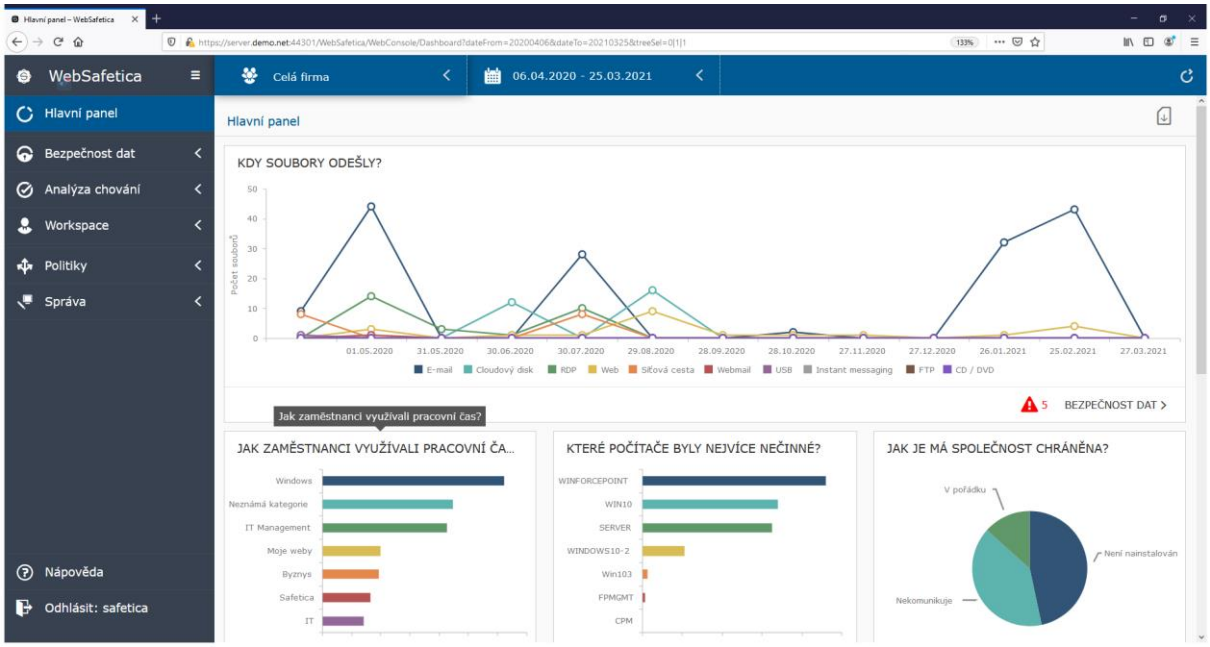
Websafetica je webové rozhraní pro nastavení a reporting Safetica Auditor.

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

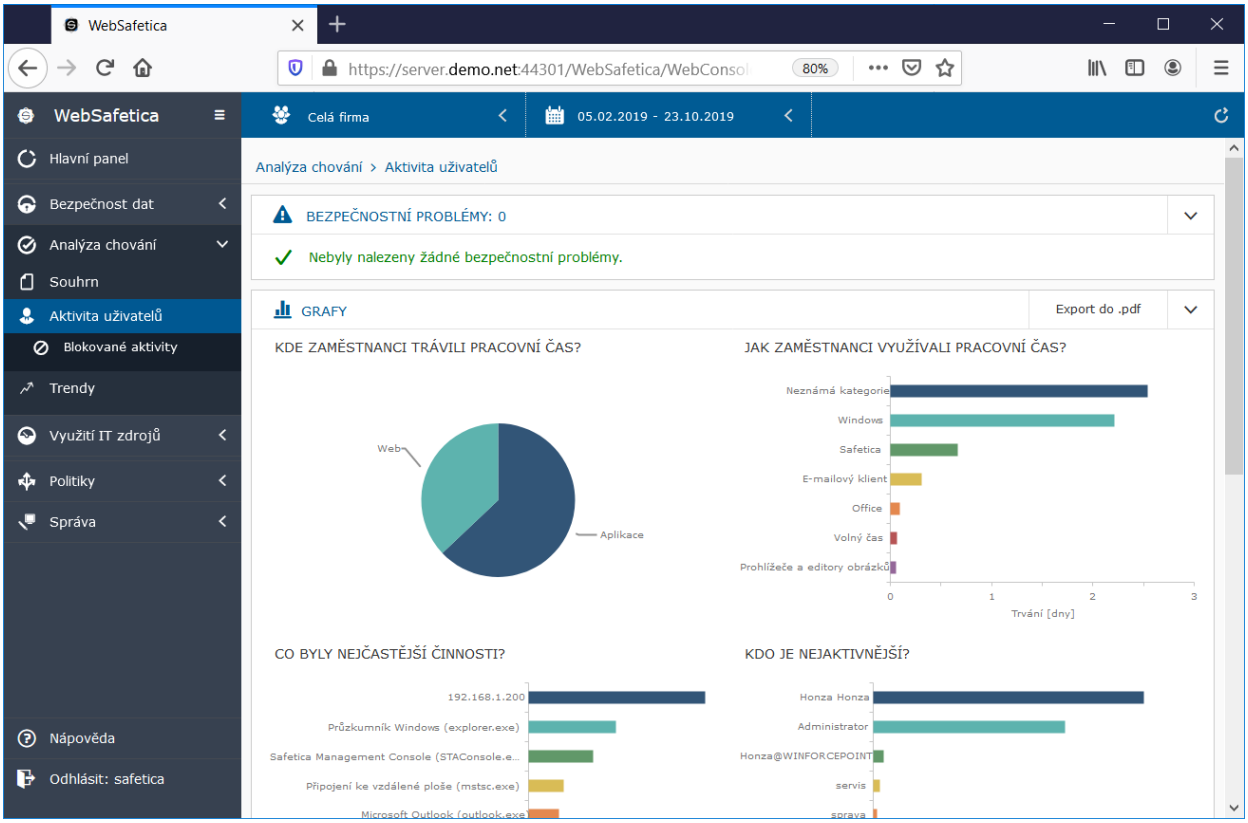
Websafetica je vhodná pro auditory, security manažery, kteří si mohou zobrazit chování uživatelů ve svém webovém prohlížeči.

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

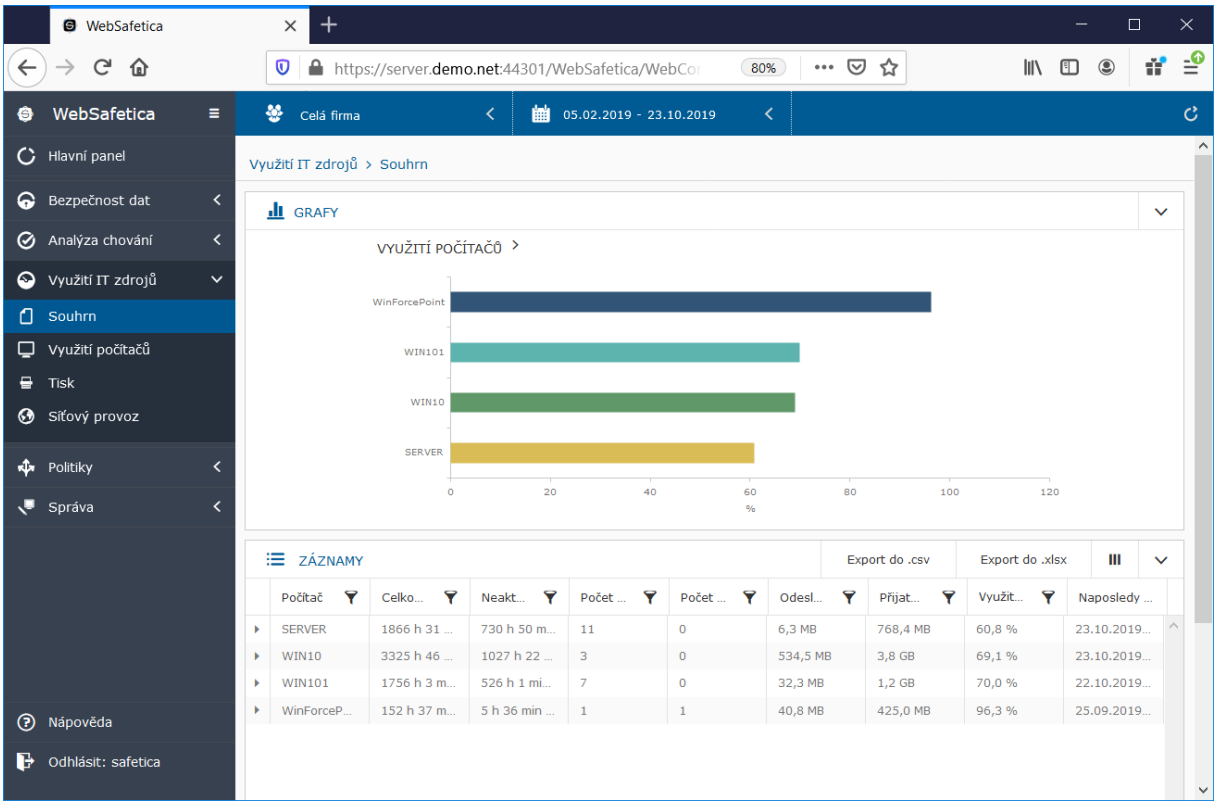
Základní pohled na dashboard Safetica



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



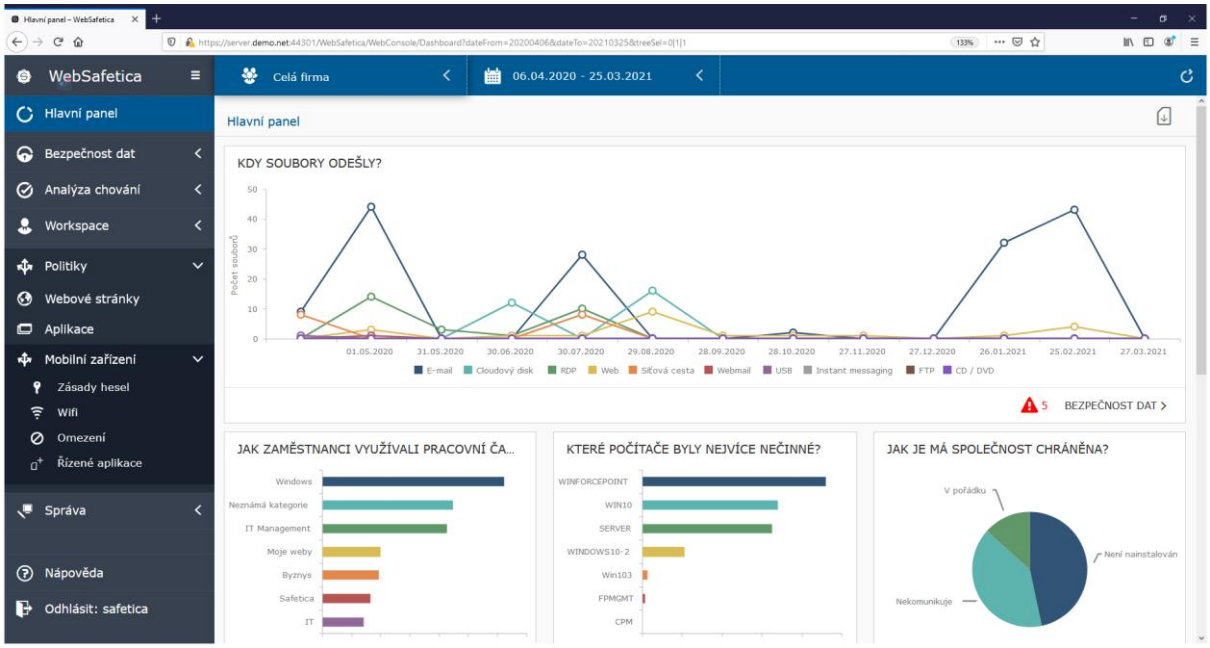
Pohled na využití IT zdrojů. Systém nabízí možnosti detailního filtrování na konkrétní uživatele, počítač nebo datum.



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:

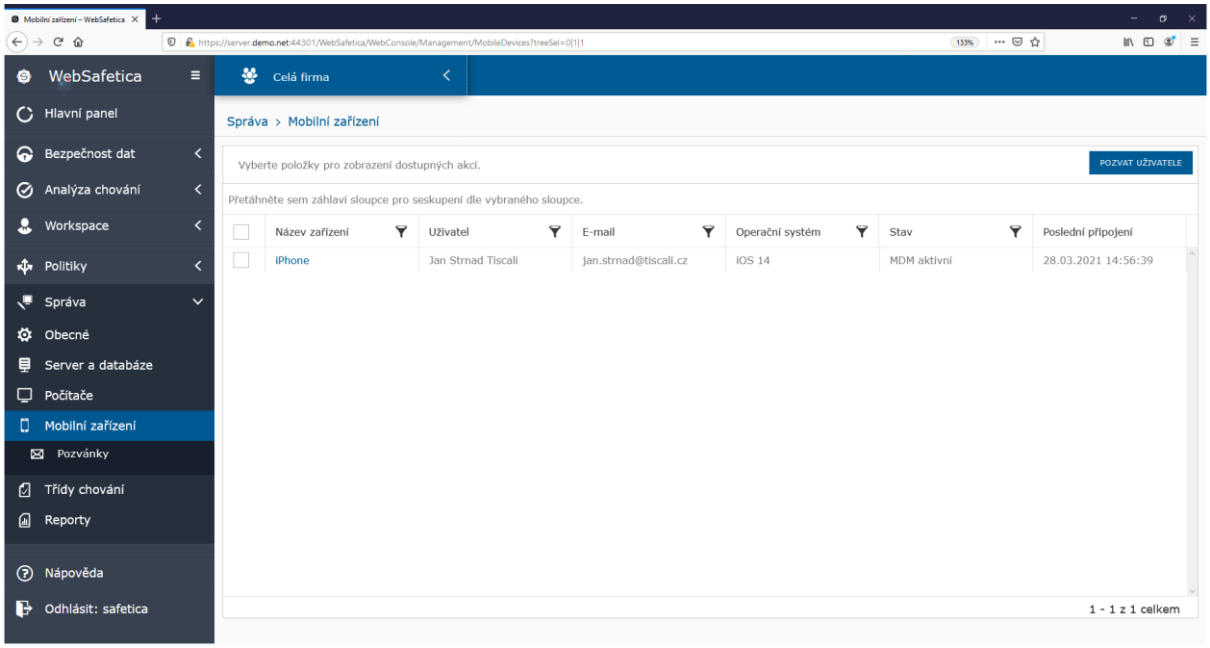
- Zásady hesel – vynucení a komplexnost hesla na mobilním zařízení
- Wifi – přednastavit uživateli mobilního zařízení wifi sítě, které může používat
- Omezení – politiky pro restrikce na mobilním zařízení
- Řízení aplikací – povolení nebo vynucení instalace aplikace na mobilním zařízení

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

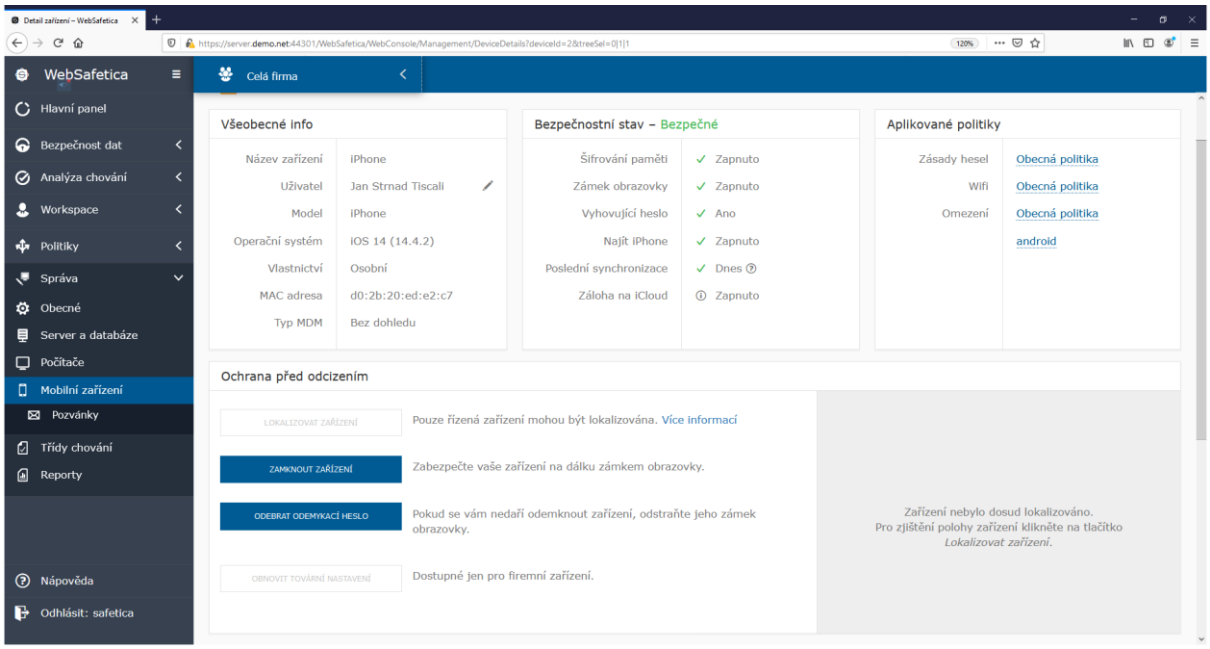
17.1. SEZNAM SPRAVOVANÝCH MOBILNÍCH ZAŘÍZENÍ

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

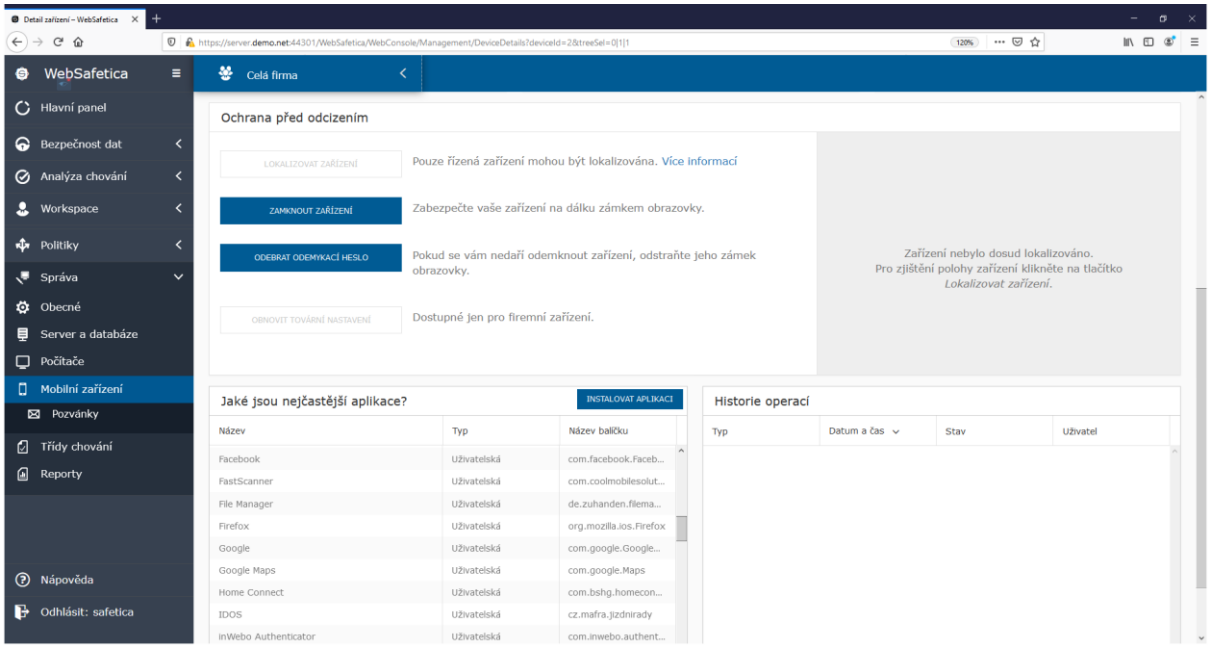
Seznam zobrazuje základní informace o mobilním zařízení:



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

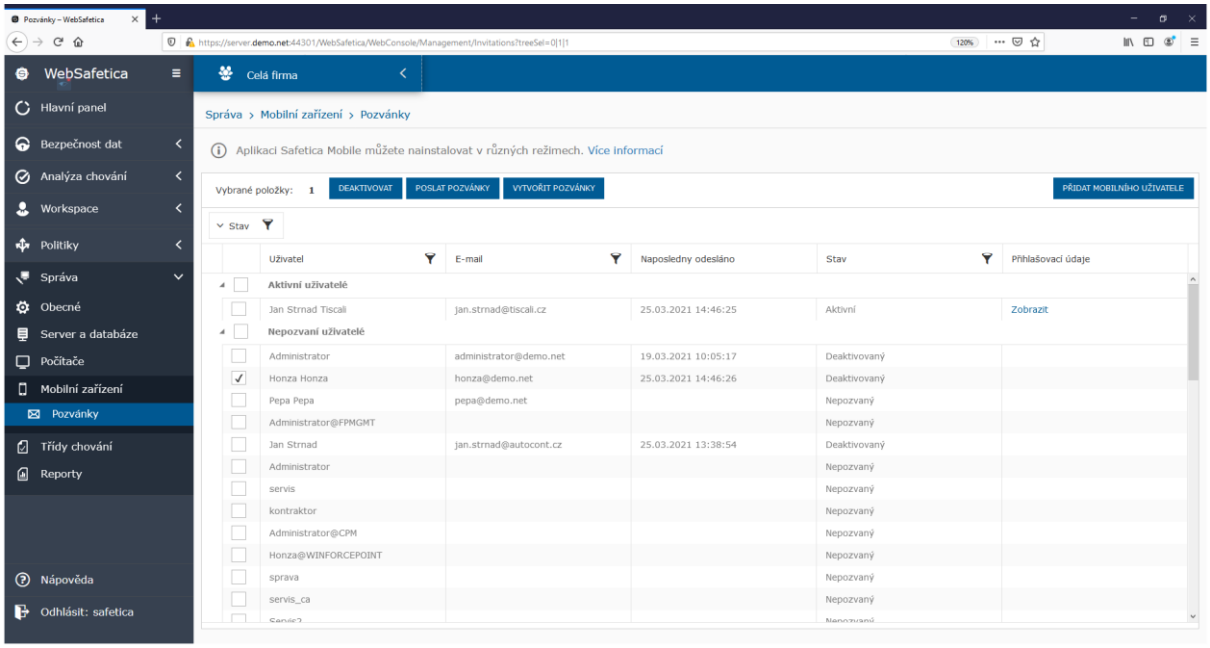


Detaily rovněž zobrazují seznam instalovaných aplikací na mobilním zařízení:

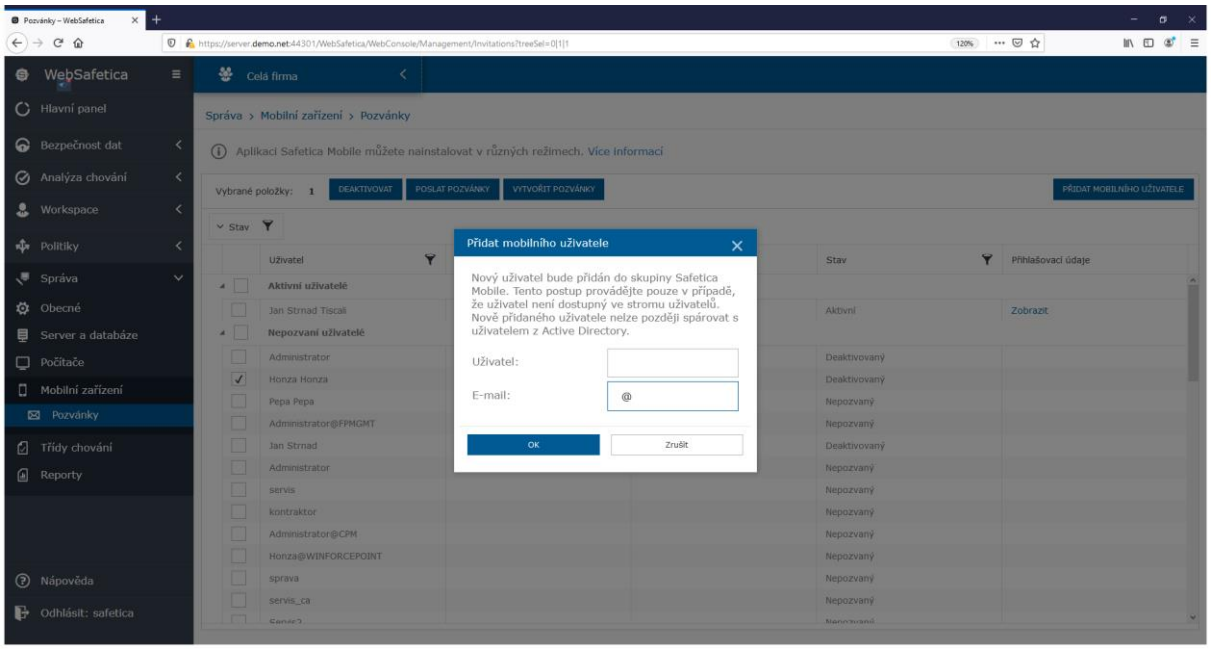


Samostatnou volbou jsou pozvánky, kde je možné nastavit pozvánku pro uživatele ke správě jeho mobilního zařízení.

Pozvánku je možné vytvořit na základě seznamu spravovaných uživatelů:



Nebo je možné pozvat uživatele na základě jeho emailové adresy:



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

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

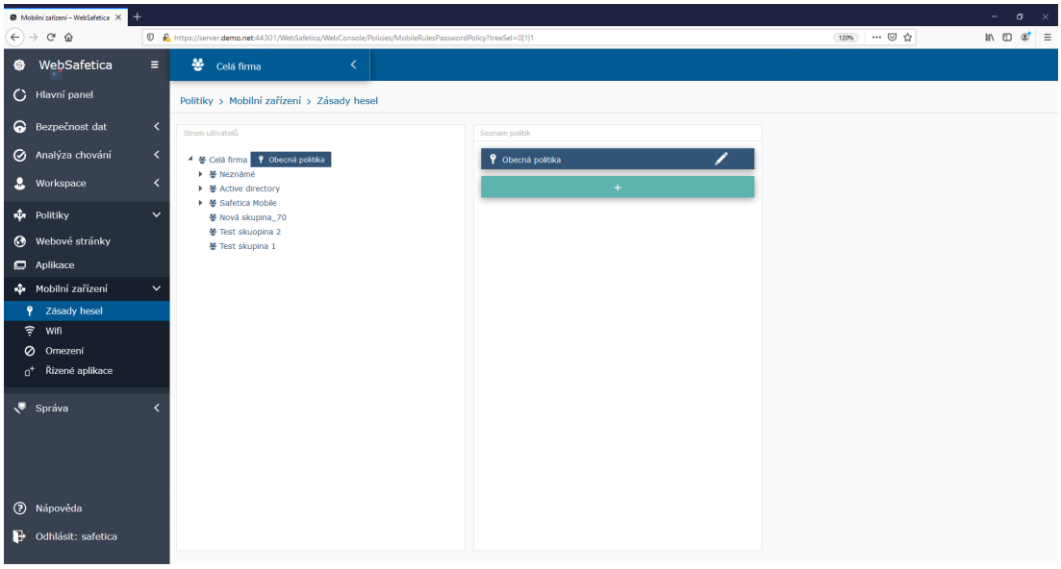
Politiku umožňují nastavení mobilního zařízení v několika úrovních

17.2.1. ZÁSADY HESEL

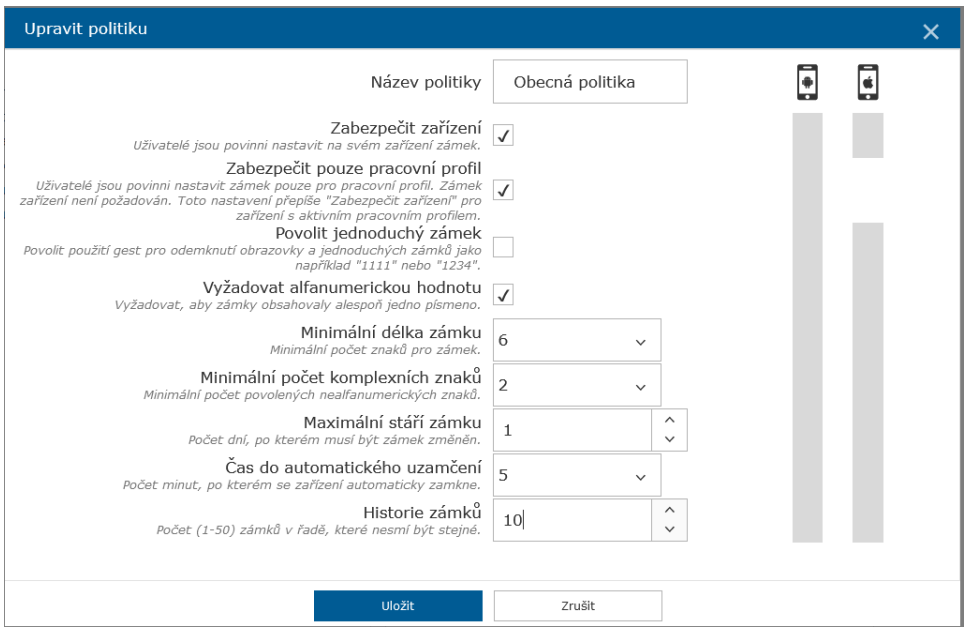
Politika pro vynucení hesla a jeho komplexnosti na mobilním zařízení.

Politiky se liší podle spravované platformy – Android a iOS.

Nastavení politiky a vytvoření nových politik



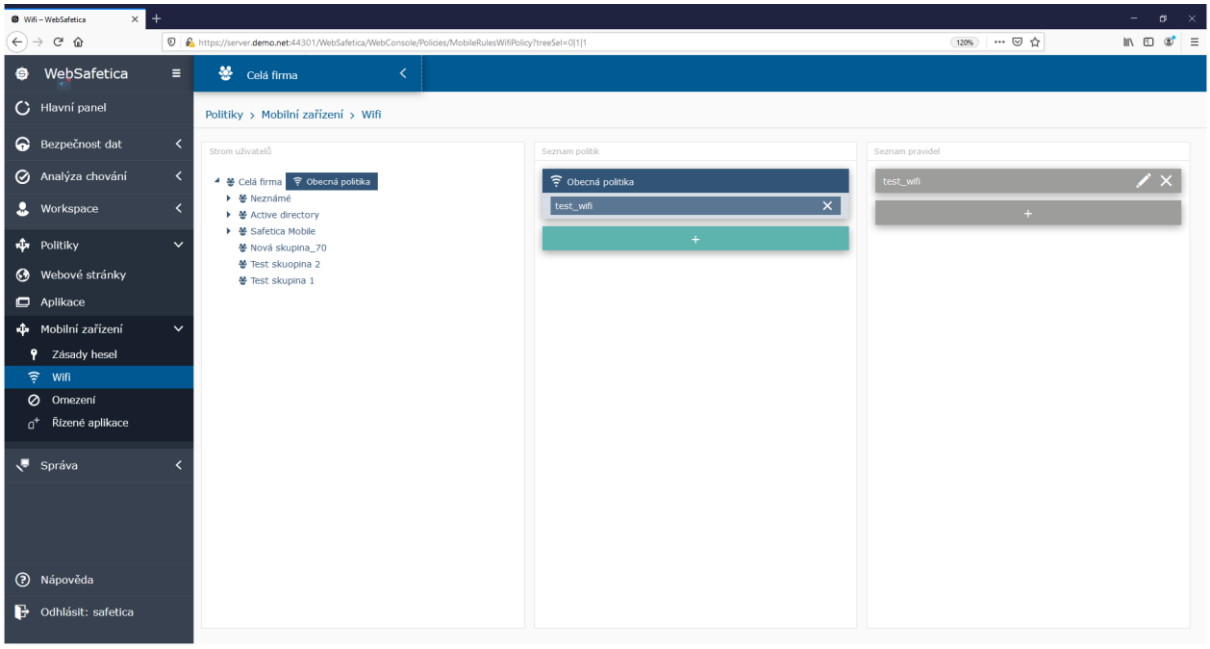
Konfigurace politiky a restrikcí:



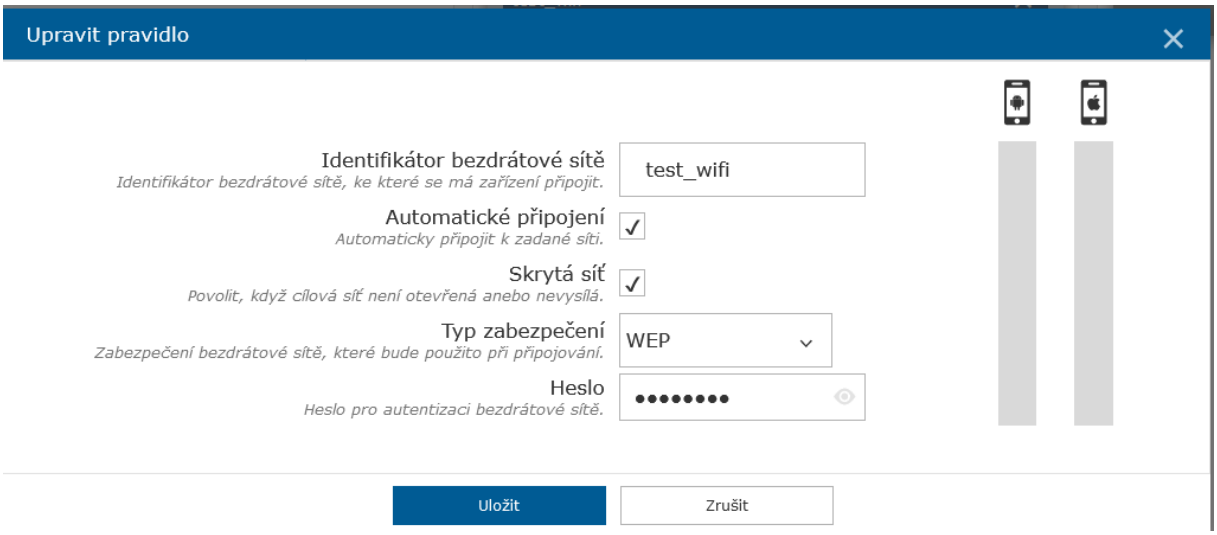
17.2.2. WIFI

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

Nastavení politik pro wifi sítě:



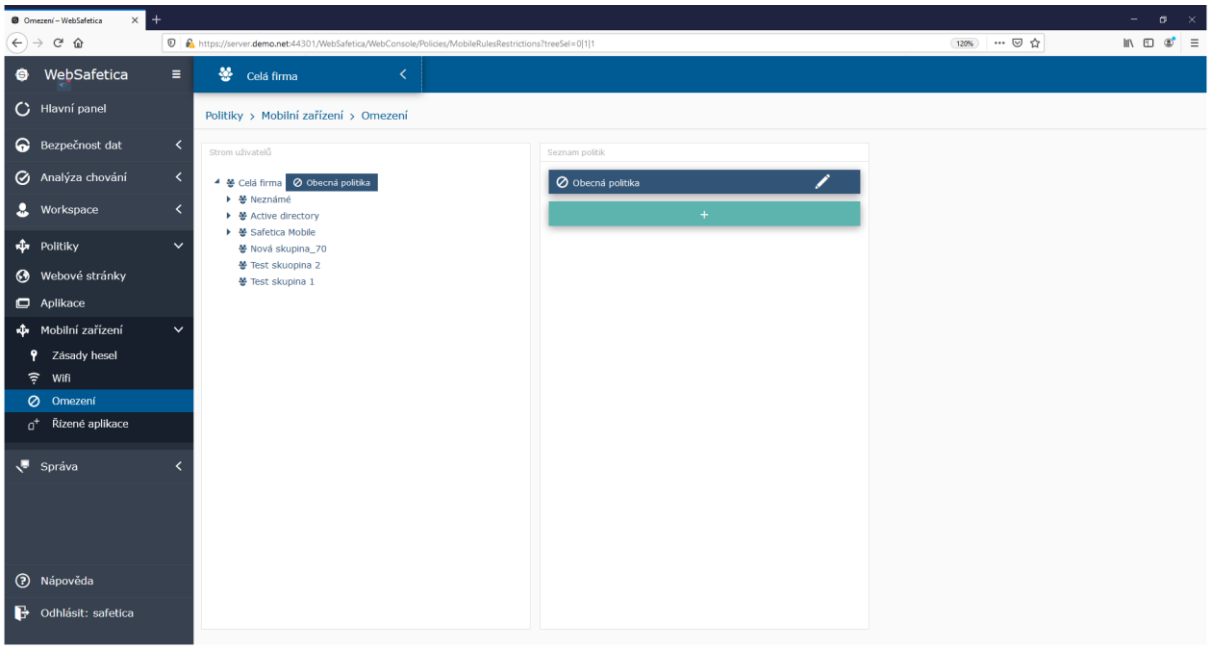
Konfigurace Wifi sítě:



17.2.3. OMEZENÍ

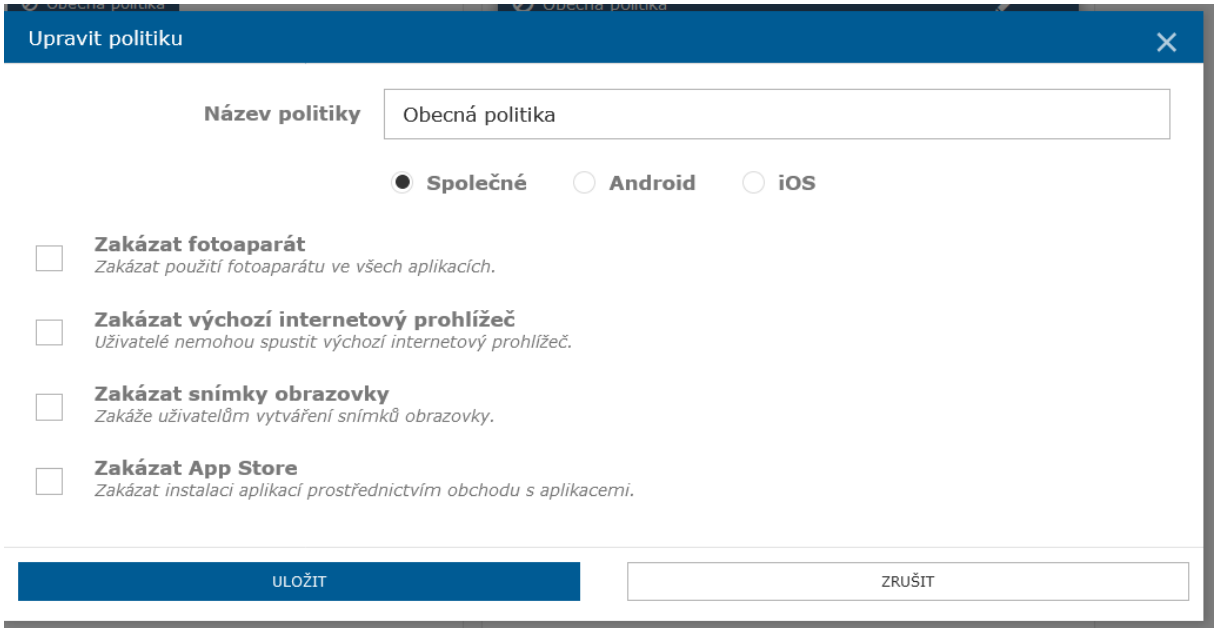
Politika restrikcí, které je možné uplatnit na mobilních zařízení včetně řízení firemního profilu

Nastavení jednotlivých politik:

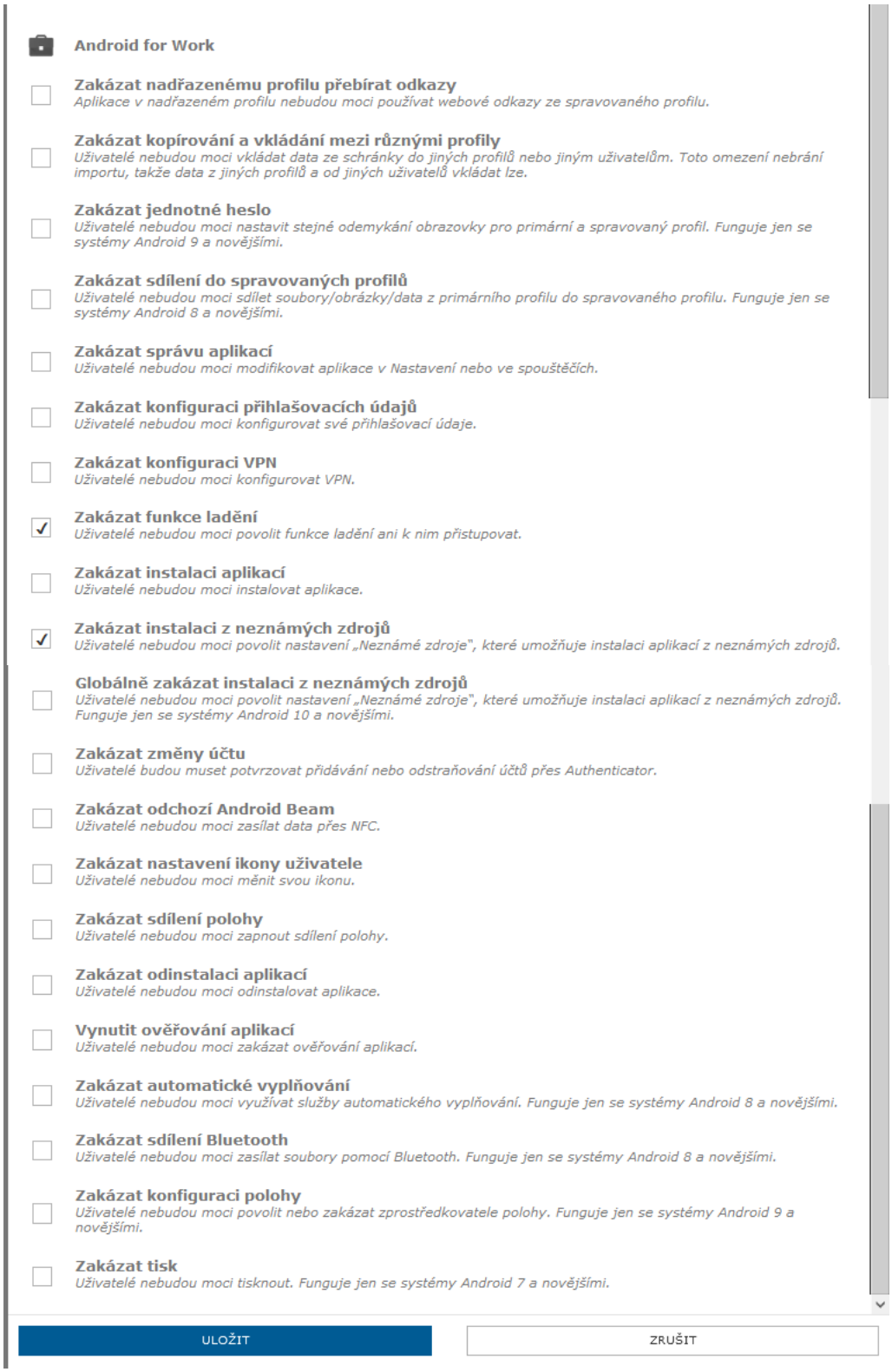


Konfigurace nastavení politiky

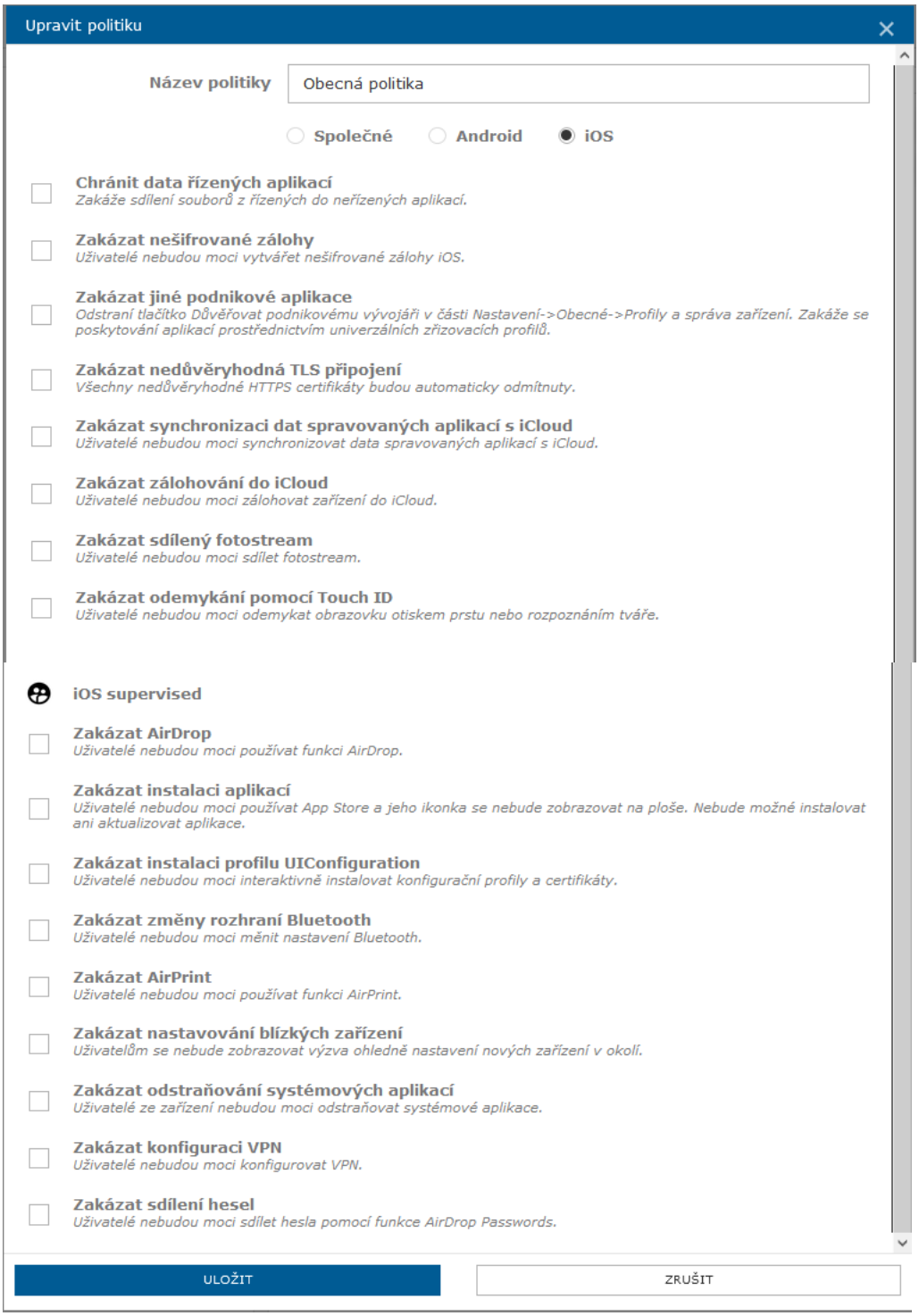
- Společná politika pro obě platformy – Android a iOS



- Politika pro Android

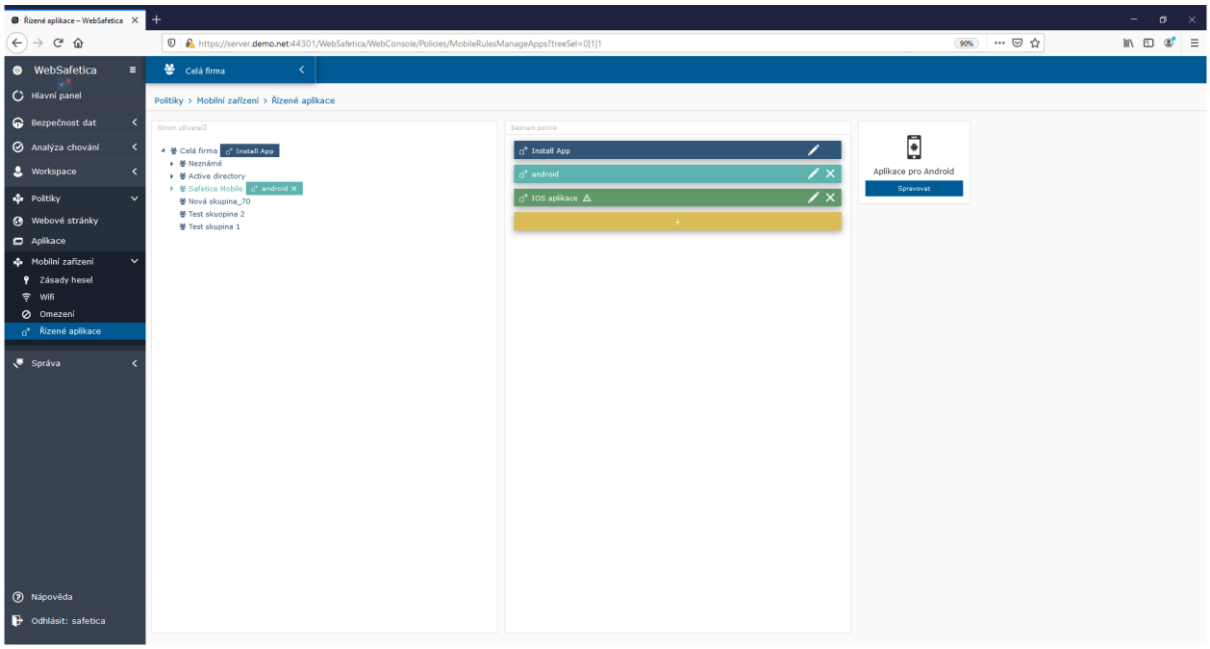


- Politika pro iOS



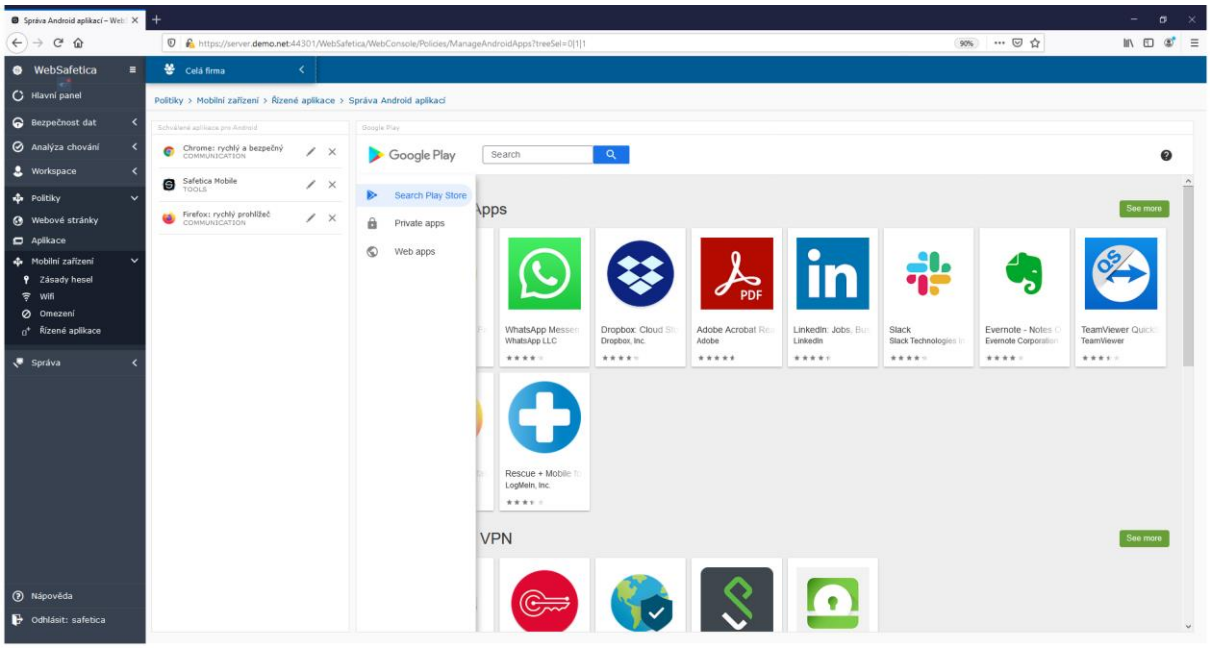
17.2.4. ŘÍZENÉ APLIKACE

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

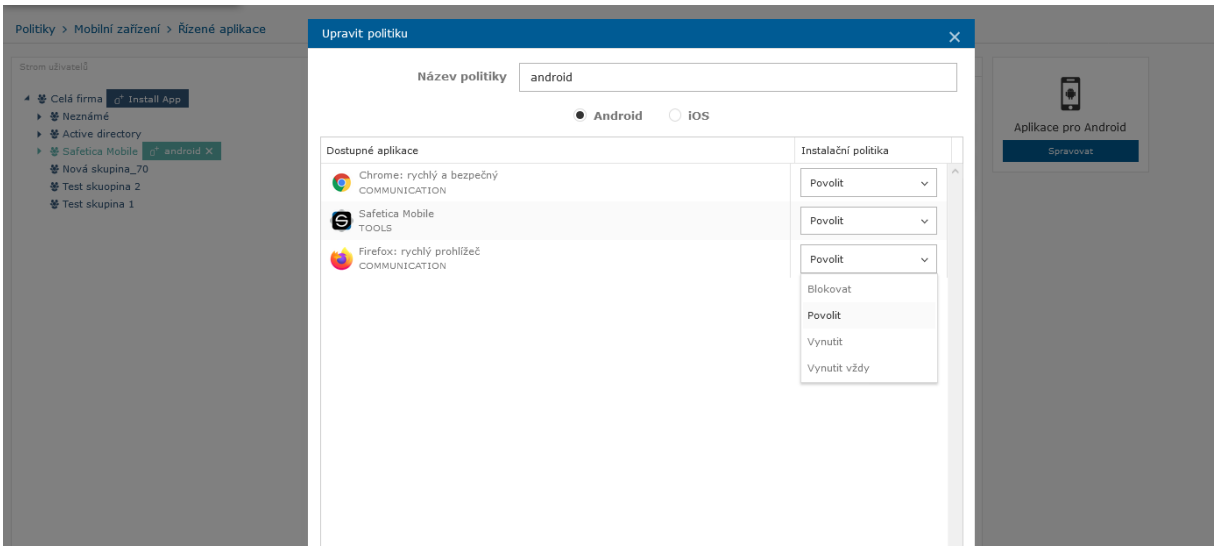


Správa aplikací pro Android s firemním profilem

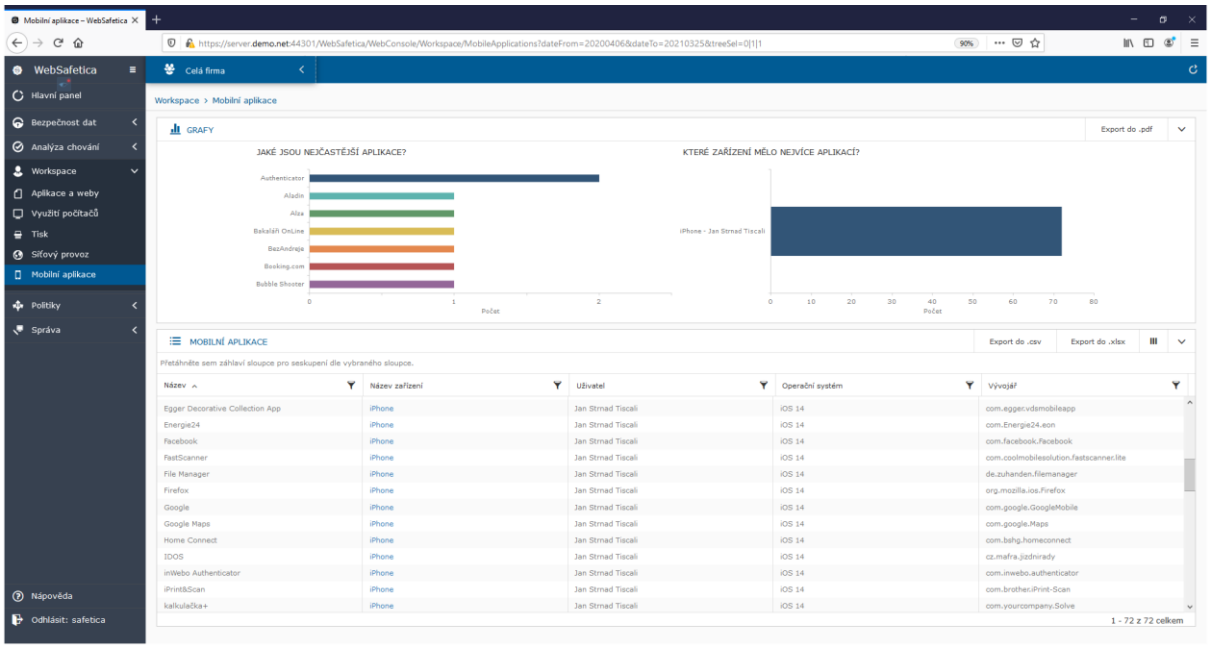
Systém umožňuje správci vybrat aplikace z Google Play, které bude moci uživatel ve svém firemním profilu používat.



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.



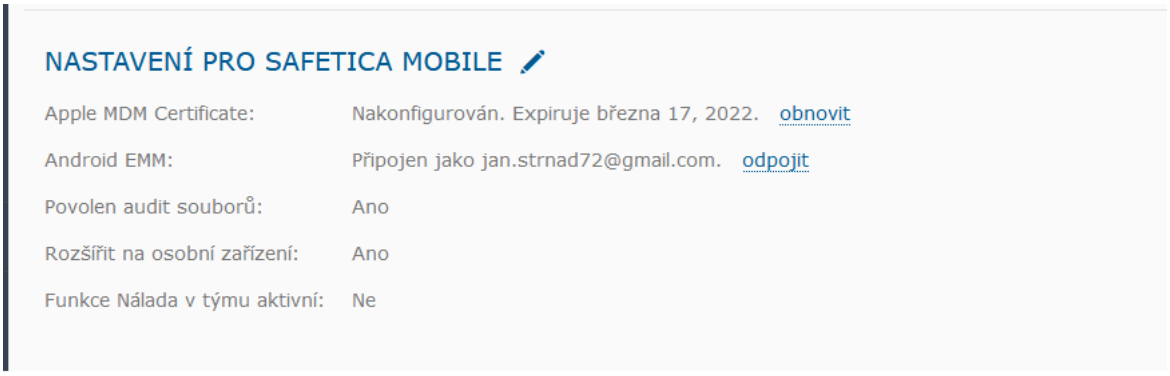
Seznam instalovaných aplikací je možné sledovat ve Workspace / Mobilní aplikace



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



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