ESET PROTECT

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

ESET PROTECT byl vyvinut společností ESET, spol. s r.o.

Pro více informací navštivte https://www.eset.cz.

Technická podpora: https://servis.eset.cz

REV. 2024-04-17

Představení ESET PROTECT

Vítejte v ESET PROTECT. ESET PROTECT je aplikace navržená pro správu až 50 000 bezpečnostních řešení ESET na stanicích, serverech i mobilních zařízeních z jednoho centrálního místa. Prostřednictvím ESET PROTECT Web Console můžete vzdáleně instalovat bezpečnostní řešení ESET na zařízení, monitorovat stav systému, spravovat jejich konfiguraci a rychle reagovat na nové problémy a hrozby na vzdálených zařízeních.

Více informací o technologiích ESET a typech útoků/detekcí naleznete ve slovníku pojmů.

Pro seznámení se s ESET PROTECT přejděte do kapitoly Začínáme s ESET PROTECT.

Následující bezpečnostní řešení ESET pro firmy byla přejmenována:

Původní název:	Nový název:	Přejmenováno ve verzi:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	

ESET PROTECT se skládá z následujících komponent:

ESET PROTECT jako služba

ESET PROTECT Web Console

- Webová konzole reprezentuje data uložená v databázi ESET PROTECT. Data vizualizuje na nástěnkách a prostřednictvím přehledů. Dále prostřednictvím ní vynutíte jednotnou konfiguraci produktů, přikážete spuštění úloh přímo v operačním systému nebo v jiných ESET produktech.

Live Installer

- Malý balíček obsahující ESET Management Agenta a bezpečnostní produkt pro snadné a pohodlné nasazení.

- ESET Management Agent je malá aplikace bez grafického rozhraní, která spouští příkazy na klientech připojených k ESET PROTECT. Spouští úlohy, sbírá protokoly z ESET aplikací, interpretuje a vynucuje nastavení (politiky), provádí další činnosti jako instalaci aplikací a monitoruje obecný stav počítače.

- Snadno získatelný, malý, předkonfigurovaný balíček obsahující agenta a bezpečnostní produkt v podobě streamovaného instalačního balíčku, který automaticky připojí stanici k vaší cloudové instanci, aktivuje produkt platnou licencí – to vše za minimální interakce uživatele. Instalační balíček automaticky identifikuje platformu a stáhne odpovídající verzi bezpečnostního produktu.

- Agent je malá aplikace, která zajišťuje veškerou komunikaci mezi stanicí (přesněji bezpečnostním řešením nainstalovaným na stanici) a ESET PROTECT.

Bezpečnostní produkty ESET

- Bezpečnostní produkt chrání klientské stanice a servery před hrozbami.

- ESET PROTECT podporuje následující bezpečnostní řešení ESET.

ESET Business Account

- Centrální místo pro firemní zákazníky a poskytovatel identity pro ESET PROTECT.
- Zajišťuje single-sign on do dalších produktů, poskytuje přehled o stavu vašich licencí, aktivovaných stanicích a správu uživatelů.
- ESET Business Account je vyžadován pro aktivování vaší ESET PROTECT instance.
- Více informací naleznete v online příručce k ESET Business Account.

ESET MSP Administrator 2

- Systém pro správu licencí pro ESET MSP partnery.
- Více informací naleznete v online příručce k ESET MSP Administrator 2.

ESET Remote Deployment Tool

- Nástroj, prostřednictvím kterého můžete ve vaší síti hromadně nasadit Live Installer.
- Pro usnadnění nasazení dokáže proskenovat vaší sít, synchronizovat se s AD, a podporuje také import seznamu cílů.

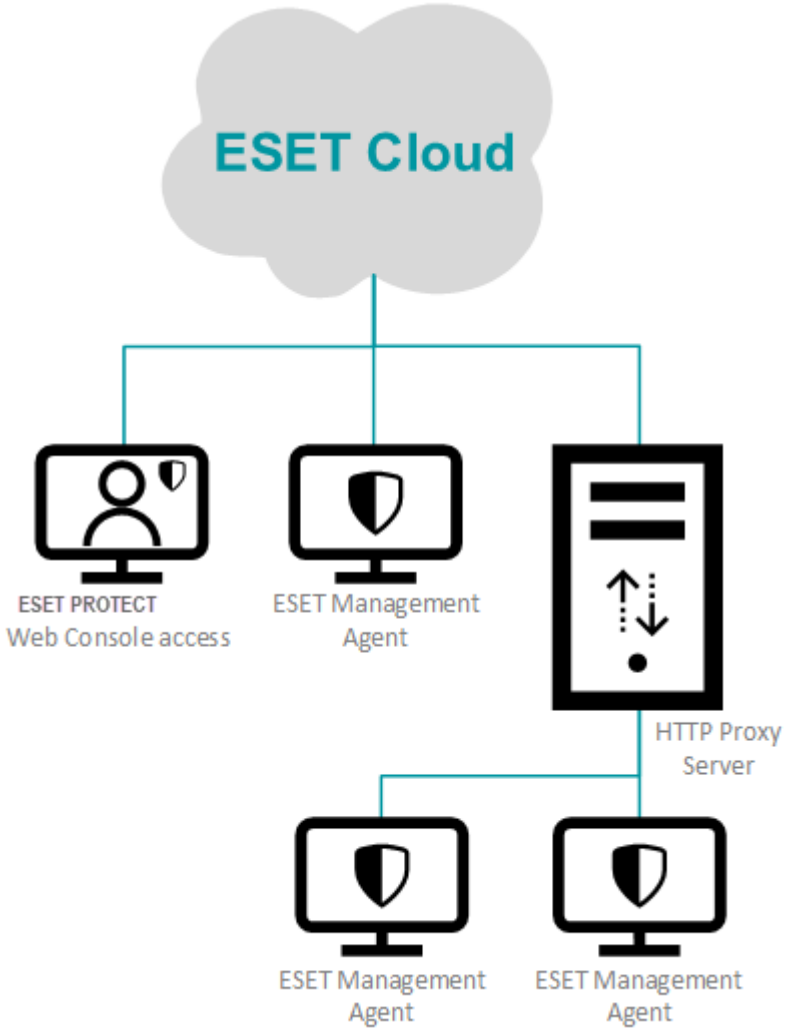
ESET Bridge (HTTP Proxy) – ESET Bridge můžete v rámci infrastruktury ESET PROTECT využít jako proxy službu.

- Do cache dokáže ukládat: aktualizace modulů ESET, instalační a aktualizační balíčky doručované z ESET PROTECT (například MSI instalátor pro ESET Endpoint Security), aktualizace bezpečnostního produktu ESET (aktualizace komponent a produktu), výsledky ESET LiveGuard.
- Pro přesměrování komunikace ESET Management Agentů na ESET PROTECT Server.

Pro synchronizaci počítačů v Active Directory s ESET PROTECT Web Console můžete použít ESET Active Directory Scanner.

Prostřednictvím ESET Cloud Mobile Management (Cloud MDM) můžete vzdáleně spravovat mobilní Android a iOS zařízení, a zajistit tak jejich bezpečnost.

Na diagramu je znázorněna architektura ESET PROTECT:



O této nápovědě

Tato příručka vás seznámí s ESET PROTECT a poskytne instrukce, jak ho používat.

Aby se předešlo nejasnostem a z důvodu zachování konzistence je terminologie používaná v této příručce založena na názvech parametrů ESET PROTECT. Používáme rovněž jednotnou sadu symbolů na zvýraznění částí kapitol, které jsou zvlášť důležité, případně by neměli uniknout vaší pozornosti.

Poznámka poskytuje cenné informace k dané funkci nebo odkaz na související kapitoly.

Tato akce vyžaduje vaši pozornost a neměli byste ji ignorovat. Obvykle obsahuje nekritické, ale však důležité informace.

Kritická informace, které byste měli věnovat pozornost. Upozornění jsou umístěna tak, aby vás včas varovala a zároveň vám pomohla vyvarovat se chybám, které by mohly mít negativní následky. Prosím, důkladně si přečtěte text ohraničený tímto označením, protože se týká velmi citlivých systémových nastavení nebo upozorňuje na možná rizika.

Příklad popisující uživatelský scénář, který doplní danou kapitolu. Příklady používáme pro vysvětlení složitějších témat.

Konvence	Význam
Tučné písmo	Názvy položek uživatelského rozhraní jako dialogová okna a tlačítka.

Konvence	Význam
Kurzíva	Zástupné znaky pro informace, které máte zadat. Například název souboru nebo cesta k souboru znamená, že máte zadat skutečnou cestu nebo název souboru.
`Courier New`	Příklady kódů nebo příkazů.
Hypertextový odkaz	Poskytuje rychlý přístup do odkazovaných kapitol nebo externích zdrojů. Hypertextové odkazy jsou zvýrazněny modře, mohou být podtržené.
%ProgramFiles%	Systémová složka operačního systému Windows, do které se standardně instalují programy a další součásti systému.

- Online příručka je primárním zdrojem nápovědy. V případě funkčního připojení k internetu se automaticky zobrazí nejnovější verze online příručky.
- Související informace tak naleznete jednoduchým procházením této struktury stránek. Pro nalezení požadovaných informací můžete využít vyhledávací pole v horní části.
- V Databázi znalostí naleznete odpovědi na nejčastější dotazy stejně jako doporučené řešení mnoha situací. Články pravidelně aktualizujeme a připravujeme návody na řešení aktuálních situací.
- ESET forum představuje jednoduchý způsob, jak ESET uživatelé mohou požádat o radu a pomoci ostatním. Můžete sem umístit váš problém nebo dotaz týkající se produktu ESET.
- Váš názor/zpětnou vazbu na konkrétní kapitolu příručky odešlete následujícím způsobem: V dolní části stránky klikněte na odkaz **Byla pro vás tato informace užitečná?**

Legenda ikon

V této kapitole uvádíme seznam všech ikon a piktogramů, se kterými se můžete setkat v ESET PROTECT Web Console. Některé ikonky představují akci, jiné typ objektu nebo jeho aktuální stav. Většina ikon může nabývat tří barev/stavů, díky čemuž snadno rozeznáte jejich funkci.

Výchozí ikona – akce je dostupná

Modrá ikona – takto barevně se ikona zvýraznění, když na ní najedete myší (možnost je aktivní)

Šedá ikona – akce není dostupná

Ikona	Popis
	Detaily spravovaného zařízení.
	Přidat zařízení – kliknutím přidáte nové zařízení. **Nová úloha** – kliknutím vytvoříte novou úlohu. **Nové oznámení** – kliknutím vytvoříte nové oznámení. **Nová statická/dynamická skupina** – kliknutím vytvoříte novou skupinu.
	Změnit – kliknutím upravíte konkrétní objekt.
	Duplikovat – ze stávající politiky můžete vytvořit novou politiku, pro niž je vyžadován nový název.
	Přesunout – kliknutím přesunete počítač, skupinu, atp. **Přístup skupiny** – Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.
	Odstranit – kliknutím odstraníte vybraný objekt.
	Přejmenovat více položek – pokud vyberte více položek, pomocí této možnosti je můžete hromadně přejmenovat – jednotlivě nebo využitím funkce najít a nahradit s podporou regulárních výrazů.
	Kontrola počítače – kliknutím spustíte na vybraném cíli volitelnou kontrolu počítače.
	Aktualizovat moduly – kliknutím spustíte na vybraném cíli aktualizaci modulů bezpečnostního produktu ESET. **Aktualizovat** > **Aktualizovat produkty ESET** – kliknutím inicializujete na vybraném cíli aktualizaci produktů ESET na novou verzi. **Aktualizovat** > **Aktualizovat operační systém** – kliknutím spustíte na vybraném cíli klientskou úlohu pro aktualizaci operačního systému.
	Audit log – kliknutím si zobrazíte Audit log pro vybranou položku.
	Mobil – obsahuje úlohy související s mobilními zařízení.
	Přeregistrovat – Přeregistrovat mobilní zařízení.
	Odemknout – kliknutím odemknete zařízení.
	Uzamknout – kliknutím uzamknete zařízení.
	Najít – kliknutím si vyžádáte informaci o pozici zařízení.
	Siréna / Zvuk ztraceného zařízení – spustí hlasitou sirénu, i přesto, pokud má zařízení ztlumenou hlasitost.
	Obnovení do továrního nastavení – kliknutím vytvoříte úlohu pro kompletní smazání obsahu zařízení.
	Napájení – v této části máte k dispozici možnosti pro **Vypnutí** nebo **Restartování** zařízení. V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje. **Obnovit** – kliknutím obnovíte soubor z karantény do původního umístění.
	Vypnout – pro vypnutí zařízení klikněte na **Napájení** > **Vypnout**. V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje. Deaktivovat produkty
	Odhlásit – pro odhlášení všech uživatelů z daného počítače klikněte na **Napájení** > **Odhlásit**.

Ikona	Popis
	Spustit úlohu – kliknutím můžete na daném zařízení spustit již existující úlohu a definovat podmínku spuštění. Úloha bude zařazena do fronty dle vámi definovaného nastavení. Spuštění úlohy bude naplánováno na nejbližší možnou dobu.
	Poslední úlohy – po najetí na tuto položku se zobrazí několik úloh, které jste naposledy použili. Kliknutím na úlohu ji okamžitě spustíte nad konkrétním cílem.
	Přiřadit uživatele... – kliknutím přiřadíte uživatele konkrétnímu zařízení. Seznam dostupných uživatelů můžete spravovat v sekci Uživatelé zařízení.
	Správa politik – politiky můžete přiřadit přímo z kontextového menu vybraného objektu. Kliknutím si zobrazíte dialogové okno pro přiřazení politiky vybraným klientům/skupinám.
	Probudit – kliknutím se ESET PROTECT Server pokusí navázat komunikaci s ESET Management Agentem prostřednictvím EPNS a vynutit okamžitou replikaci dat. To je užitečné, pokud nechcete čekat na pravidelný interval, kdy se ESET Management Agent připojuje k ESET PROTECT Server. To je užitečné v případě, kdy nechcete čekat na standardní interval replikace a chcete ihned spustit klientskou úlohu nebo aplikovat politiku.
	Izolovat od sítě
	Ukončit izolaci od sítě **Připojit ke vzdálené ploše** – vytvořte a stáhněte si *.rdp* soubor, který vám umožní připojit se k cílovému zařízení prostřednictvím RDP (Remote Desktop Protocol).
	Potlačit – kliknutím můžete potlačit počítač (Agent **nebude** do ESET PROTECT reportovat data). Po kliknutí se u počítače ve sloupci Potlačeno zobrazí ikona . Pro opětovné reportování dat z Agenta do ESET PROTECT klikněte na možnost **Zrušit potlačení**.
	Zrušit – pomocí této možnosti deaktivuje nebo odstraníte nastavení/výběr.
	Přiřadit – kliknutím přiřadíte politiku klientovi nebo skupině.
	Importovat – vyberte přehledy / politiky, které chcete importovat.
	Exportovat – vyberte přehledy / politiky, které chcete exportovat.
	Štítky – Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
	Statická skupina
	Dynamická skupina
	Příznak politiky: **Ignorovat**
	Příznak politiky: **Použít**
	Příznak politiky: **Vynutit**
	Podmínky spuštění – kliknutím si zobrazíte seznam podmínek spuštění vybrané klientské úlohy.
	Počítač
	Mobilní zařízení
	serveru
	Souborový server
	Poštovní server
	Gateway server
	Kolaborační server
	ESET Management Agent
	Mobile Device Connector
	ESET Rogue Detection Sensor
	ESET Bridge
	Typ detekce **Antivirus**. Po kliknutí si zobrazíte všechny zachycené Detekce. Klikněte na počítač a vyberte **Řešení** > **Zapnout bezpečnostní produkt** pro zapnutí bezpečnostního produktu ESET v počítači.
	Pro aktivování a zapnutí ESET LiveGuard Advanced na všech počítačích v dané statické skupině klikněte na ozubené kolečko vedle názvu skupiny a v kontextovém menu vyberte možnost **Řešení** > **Zapnout ESET LiveGuard**.
	ESET Inspect Connector V hlavním menu na záložce **Počítače** > kliknutím do políček vyberte jeden nebo více počítačů > klikněte na tlačítko **Počítač** > vyberte možnost **Řešení** > **Zapnout ESET Inspect**, čímž nasadíte ESET Inspect Connector na spravované stanice s Windows/Linux/macOS. Tlačítko ESET Inspect je dostupné pouze v případě, že vlastníte licenci na ESET Inspect a ESET Inspect máte připojen k ESET PROTECT. Uživatel Web Console potřebuje alespoň sadu oprávnění s hodnotou **pouze pro čtení** u možnosti **Přístup k ESET Inspect**.
	Pro zapnutí ESET Full Disk Encryption na konkrétním počítači na něj klikněte a v kontextovém menu vyberte možnost **Řešení** > **Zapnout šifrování**.
	Na zařízení je aktivní ESET Full Disk Encryption.
	Zranitelnosti
	Správa záplat

Nové funkce v ESET PROTECT

MDR nástěnka a týdenní přehled

Našim zákazníkům, kteří využívají službu ESET MDR, s potěšením představujeme novou MDR nástěnku. Na této nástěnce se v reálném čase shromažďují a zobrazují všechna důležitá data související s nepřetržitým sledováním hrozeb. Kromě toho budete dostávat pravidelné týdenní zprávy s nejnovějšími daty přímo do své e-mailové schránky. Tyto zprávy jsou rovněž přístupné v sekci Přehledy a automaticky se archivují. Zjistit více

Registrace mobilních zařízení postřednictvím Microsoft Entra ID

Přidali jsme možnost registrovat mobilní zařízení do ESET PROTECT prostřednictvím Microsoft Entra ID. Díky této zjednodušené metodě registrace již není nutné generovat jedinečné kódy pro každé zařízení. Nyní můžete snadno zaregistrovat všechna mobilní zařízení pomocí jediného odkazu nebo QR kódu, který rozešlete e-mailem nebo jiným preferovaným kanálem. Zjistit více

Další vylepšení a opravy chyb

V seznamu změn najdete informace o dalších vylepšeních.

Poznámky k vydání

Poznámky k vydání jsou k dispozici pouze v angličtině.

ESET PROTECT 5.2

Release date: April, 2024

- ADDED: MDR dashboard that displays real-time data for customers with the ESET MDR service
- ADDED: Weekly MDR report email sent automatically to customers with the ESET MDR service
- ADDED: Archive of MDR reports for customers with the ESET MDR service
- ADDED: Ability to enroll all mobile devices with one enrollment link or QR code via Microsoft Entra ID enrollment
- IMPROVED: Post-installation restart is not required for Linux products (ESET Endpoint Antivirus for Linux and ESET Server Security for Linux)
- IMPROVED: Using Google Play version of ESET Endpoint Security for Android instead of a web version when enrolling a mobile device in Device Owner mode
- FIXED: Error message displayed when opening the details or editing a server task with a trigger other than "Generate report"
- FIXED: Incorrect headline displayed in the webhook notifications sent to Microsoft Teams
- FIXED: Displaying "Product not installed" alert for "Common features" policies in some instances
- FIXED: No information about the mobile network is displayed when the device has multiple SIMs/eSIMs
- Other minor improvements and bug fixes

ESET PROTECT 5.1

Release date: February, 2024

- ADDED: Vulnerability & Patch Management for Windows servers (requires ESET Server Security for Microsoft Windows Server version 11.0 and later)
- ADDED: Enhanced ESET LiveGuard behavioral reports with detailed behavior of the sample (available for customers with ESET Inspect)
- IMPROVED: Migration of static group hierarchies from on-premises to cloud in large and MSP environments
- IMPROVED: Ability to send "ESET Inspect incidents" notification for all incident authors

- IMPROVED: Clarified wording related to Vulnerability & Patch Management
- FIXED: Incorrect installation date reported for Linux product
- FIXED: Table scrolling does not work after opening Details
- FIXED: Incorrect display of license time remaining before expiration next to the license end date in Computer Details
- Other minor improvements and bug fixes

ESET PROTECT 5.0

Release date: December, 2023

- ADDED: Name change for ESET PROTECT Cloud to ESET PROTECT
- ADDED: Enable automatic operating system updates (part of Vulnerability & Patch Management)
- ADDED: New preset policy with automatic operating system updates (part of Vulnerability & Patch Management)
- ADDED: Ability to download ESET LiveGuard behavioral reports
- ADDED: Option to send a notification to non-activated devices enrolled via Workspace ONE or Microsoft Intune (MDM)
- IMPROVED: Patch management restarts added to the Automatic problem resolving setting
- IMPROVED: Users with access to server settings can delegate access rights to other users for viewing and modifying the server settings
- IMPROVED: Devices API contains information about the BIOS serial number
- IMPROVED: New version of AV Remover in the Management Agent
- FIXED: Incorrect Dynamic Groups evaluation behavior on Agent startup
- FIXED: Devices API does not report installed security products
- REMOVED: Support for macOS Sierra (10.12), High Sierra (10.13) and Mojave (10.14)
- REMOVED: Support for Windows 7, 8 and 8.1
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.7

Release date: October, 2023

- ADDED: New REST API for ESET PROTECT Cloud
- IMPROVED: New information for MSP administrators about the MSP managing company in the All-in-one

installer

- FIXED: Agents lost connection after migration, followed by an upgrade
- FIXED: Agent service fails to stop in time, or system restart takes longer than expected in specific cases
- FIXED: Agent for macOS is not correctly reporting the system build number in specific cases
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.6

Release date: August, 2023

- ADDED: Setting time slots in Dynamic groups
- ADDED: Enrolling Android mobile devices from Workspace ONE
- IMPROVED: Added new setting in the ESET LiveGuard Basic built-in policy regarding the automatic document submissions (set to OFF by default)
- IMPROVED: Visual enhancements in the patches list in Patch Management
- IMPROVED: Added language settings for the mobile device enrollment email
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.5

Release date: July, 2023

- ADDED: ESET Vulnerability & Patch Management - a new protection layer monitoring vulnerabilities with the ability to patch all endpoints managed through our platform (requires ESET Endpoint Antivirus/Security for Windows version 10.1 and later)
- ADDED: New setting in "Set up your protection" wizard regarding ESET LiveGuard for new and existing customers
- ADDED: New Client task - Check for product update (requires ESET Endpoint Antivirus/Security for Windows version 10.1 and above)
- ADDED: The ability to test send email and webhook notifications
- ADDED: Webhook authentication to verify the credibility of the webhook notification
- IMPROVED: New version of the Log Collector in the Management Agent
- FIXED: Negative filter applied to the list of computers still visible after clearing the filters
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.4

Release date: June, 2023

- ADDED: New dashboard for customers using ESET Cloud Office Security
- ADDED: Data filter per customer for MSP administrators in the Dashboard section
- ADDED: New section for MSP administrators, "Managed Customers", offering an overview of all managed customers
- ADDED: Ability for MSP administrators to filter report templates per customer when creating scheduled reports
- ADDED: New delivery method for notifications - webhooks
- ADDED: New branding visuals within the console
- IMPROVED: Easier search within the console with no need to first choose a category
- IMPROVED: Ability to filter policies by name
- IMPROVED: Information about the creation and download of installers added to the Audit Log
- IMPROVED: MSP customers ready for a set up distinguished by an icon
- IMPROVED: Asynchronous sending of enrollment emails during the mobile device enrollment
- IMPROVED: Wi-fi settings available via QR code during Device owner enrollment (MDM)
- IMPROVED: New version of the AV Remover and Log Collector in the Management Agent
- CHANGED: The "Auto-updates" policy will become a part of the "Common features" policy when the new Configuration module is released (planned for July)
- FIXED: Creating a dynamic group template based on a value "LiveGuard is not working due to a license problem" not functioning properly
- FIXED: Dynamic group template based on a value "macOS is preventing the ESET security product from accessing some folders" not working properly
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.3

Release date: April, 2023

- ADDED: An MDR Report Template for offices and partners delivering ESET Services
- ADDED: A column for mobile device IMEIs in the device list and the possibility to filter the devices by IMEI
- ADDED: The ability to combine Computer name, Database version and Last connection in one report

- IMPROVED: Extended certificate validity for mobile devices - devices do not need to connect to an MDM server frequently to stay protected
- FIXED: Issues with displaying the Product Tour in the Safari browser
- FIXED: Various localization bugs
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.2

Release date: February, 2023

- ADDED: Detections are grouped by common attributes
- ADDED: Migration of mobile devices to cloud MDM
- ADDED: Syslog includes the operating system of a computer, and the full hierarchy and description of a static group
- ADDED: Product Navigator has a link to ESET Cloud Office Security (available later in April 2023)
- IMPROVED: Active Directory Synchronization (time of last sync, ability to deactivate and regenerate token)
- FIXED: Incorrect filter behavior when multiple license statuses are selected
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 4.1

Release date: January, 2023

- ADDED: Enrollment support for Android mobile devices via Microsoft Intune Management Console
- ADDED: Column "Investigated by ESET" in incident overview in the ESET Inspect dashboard
- ADDED: Ability to add column FQDN and Serial Number in the Computers section
- IMPROVED: Size values in Submitted Files
- FIXED: Inability to resolve/unresolve detections when the parent group is selected in the tree
- FIXED: Incorrect encryption process (EFDE) status in the ESET Solutions section
- FIXED: Wrong ESET LiveGuard license was shown while editing the existing software install task
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 4.0

Release date: November, 2022

- ADDED: Basic incident overview in the ESET Inspect dashboard

- ADDED: CEF format for Syslog
- ADDED: Reporting of absolute and relative free space for hard drives in HW inventory
- ADDED: Log out action in the Computer context menu (under Power)
- ADDED: Log out Client Task
- ADDED: Ability to filter Computers by FQDN
- ADDED: Ability to filter Computers by Serial Number
- ADDED: Last boot time in computer details
- ADDED: Ability to deploy LiveGuard on all devices in a static group via context menu action
- ADDED: Ability to reset default filters
- ADDED: Static Group name in Syslog events
- ADDED: Ability to see the progress of removing client tasks
- ADDED: Ability to filter unassigned policies in the Policies section
- ADDED: Ability to sort policies in the "Last Modified By" column
- ADDED: Support for time-elapsed (duration) filters in Dynamic Groups
- ADDED: Comma separator for thousands place in table numbers
- IMPROVED: Table numbers are now aligned right
- IMPROVED: Selecting a product from the repository in the Software Install task
- IMPROVED: "Deploy ESET LiveGuard" through the computer's or group's context menu now leverages a better mechanism that is used in the dedicated ESET Solutions section
- IMPROVED: Filtering by Detection Type
- IMPROVED: New version of Log Collector (version 4.6.0.0) in Management Agent
- IMPROVED: Solutions deployment supports computers in site/company location based on hierarchy
- IMPROVED: Example section in the "Select time interval" filter
- CHANGED: Limit from 100 to 1000 when opening selected objects
- CHANGED: Disabled optional use OPAL in built-in encryption policy "Encrypt all disks - Recommended"
- FIXED: The license list occasionally disappears when scrolling through a long License Management list
- FIXED: The date/time filter does not work correctly on the localized web console
- FIXED: All policies are hidden except auto-update when logging in to the console for the first time

- FIXED: Info message about default value for time-based criteria in Notifications is shown when it is not mandatory
- FIXED: Network adapter(s) screen informs that the latest version of an agent is required, even though the latest version is installed
- FIXED: Default presets for Computers/Detections sections are overwritten in a special scenario
- FIXED: Inaccurate problem count in License Management badge in specific scenarios
- FIXED: Missing limit for quarantine management actions, which causes an error message in some cases
- FIXED: HW inventory reports the TPM manufacturer version instead of the specification version
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.5

Release date: September, 2022

- ADDED: Initial configuration (Set up protection)
- ADDED: Dark theme
- ADDED: Ability to switch between Absolute and Relative time in tables
- ADDED: Ability to add column Hash in Detections section
- ADDED: Ability to search by Hash in the Detections section
- ADDED: Ability to search by Object in the Detections section
- ADDED: Ability to distinguish, whether BitLocker is activated on a particular machine
- ADDED: Filtering options in Computer details - Installed Applications screen
- ADDED: Computer preview - the ability to reset displayed sections into default
- ADDED: Ability to modify Computer name and Description directly from the Computer preview panel
- ADDED: Ability to mute/unmute Computer directly from the Computer preview panel
- ADDED: Section name as a prefix in the browser tab title
- IMPROVED: VDI support (mostly improvements around instant clones)
- IMPROVED: Network Adapters (part of Computer details - Details - Hardware) are more readable in the case of IPv4/IPv6
- IMPROVED: Multiplatform support when deploying or enabling features via Solutions in the Computer context menu
- IMPROVED: Displaying of Inspect button is now dependent on the permission set "Access to ESET Inspect"

- IMPROVED: Filter Advisor remembers item sorting
- IMPROVED: Information in the Detection type column was split into two separate columns Detection Category and Type
- IMPROVED: Creation of New Report Template for newly created Report category
- FIXED: Save filter set is not working correctly in all sections
- FIXED: Specific scenario causes license sync breakage (if static group below company has the same name as a site that is going to be created in EBA)
- FIXED: When you load a saved filter set, it is not applied unless you edit it (various sections)
- FIXED: Filter "≤ # OF ALERTS" is not working correctly (Computers section)
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.4

Release date: June, 2022

- ADDED: Advanced Filters in the Computers section
- ADDED: Native ARM64 support for ESET Management Agent for macOS
- ADDED: "Waiting" state in the Component version status section on Status Overview for better communication of auto-updates (available from ESET Endpoint Antivirus/Security for Windows version 9.1)
- ADDED: Site structure from ESET Business Account synchronizes in the static group tree
- ADDED: New rebooting option-administrator can set up reboots in a way that the end-users can postpone them (available from ESET Endpoint Antivirus/Security for Windows version 9.1)
- ADDED: Information on how many more devices can enable ESET LiveGuard on the ESET LiveGuard Dashboard
- ADDED: Dark Theme preview feature
- ADDED: Limited-input device-simple enrollment flow for Android-based devices that do not have access to emails or a camera for scanning QR codes
- ADDED: Support for deployment of the latest version in the software installation task (the latest version at the moment of task execution, it is not necessary to select a specific version anymore)
- ADDED: Creation date column in the Installers section
- ADDED: Reset functionality for columns in tables
- ADDED: Warning to Audit log access right
- ADDED: "Installation Date" column in Computer details - Installed Applications screen
- ADDED: Ability to select multiple monitored static groups in a single notification

- ADDED: Reporting human-readable Windows operating system version is displayed in the OS Service Pack column in the Computers section
- ADDED: OS build version collected from macOS is displayed in the OS Service Pack column in the Computers section
- ADDED: Agents tile in the Status Overview section for better identification of unmanaged computers
- ADDED: Instance ID is available in the console's About section (previously only available in ESET Business Account)
- ADDED: Console users can deploy ESET Full Disk Encryption (EFDE) on recommended (portable) devices in the ESET Solutions screen
- IMPROVED: EFDE does not deploy to devices using BitLocker for drive encryption
- IMPROVED: Reboot and shut down experience on macOS (user is notified about restart and can cancel it in 60 seconds)
- IMPROVED: Tasks planned ASAP are executed in the order in which they were created in the console
- IMPROVED: Admin password is not required when enrolling a new mobile device. However, ESET strongly recommends you use an admin password for the full functionality of certain features
- IMPROVED: Every ASAP trigger created by the user in the console must have an expiration set (less than six months)
- IMPROVED: HIPS detections now contain user and hash
- IMPROVED: New version of AVRemover and Log Collector in the Management Agent
- FIXED: Several functionality problems with the dynamic group template selector
- FIXED: Scheduled client tasks without "Invoke ASAP If Event Missed" pre-selected could be executed with the wrong timing if the computer woke up from sleep or hibernation
- FIXED: Tags assigned to a "Client Task" are automatically assigned to applicable computers
- FIXED: Unavailable EDR element in the Component version status section on the Status Overview screen
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.3

Release date: April, 2022

- ADDED: Manage up to 50,000 devices (according to purchased license)
- ADDED: Support for ESET Inspect Cloud (EDR solution)
- ADDED: Easy trial, deployment and purchase of ESET Full Disk Encryption (EFDE)
- ADDED: Preview feature - Advanced Filters in the Computers section

- ADDED: New buttons under the table in the Computers section and Detection section
- ADDED: Right-click tables to open the context menu
- ADDED: Enrollment link expiration and device certificate renewal information to the enrollment email
- ADDED: Built-in policies for V7 product for macOS and HTTP proxy
- ADDED: Ability to turn on the "Remote Host" column in the Computers section
- ADDED: Console users can configure (in Settings) the behavior of newly enrolled devices deduplication in the console
- ADDED: Console users receive an email notification that contains a link that redirects the user into the Computer details section in the console
- IMPROVED: Console users receive a notification about multiple detections occurring on managed computers aggregated in one email message
- IMPROVED: Remove button was moved behind the gear icon in the ESET Solutions section
- IMPROVED: Console users can click the chart in the ESET Solutions section and will be redirected to the Computers section
- IMPROVED: The latest versions of each product are prioritized in the product selection section of the software installation task
- IMPROVED: UI elements in tables
- CHANGED: ESET Dynamic Threat Defense to ESET LiveGuard in management consoles
- CHANGED: Remove tags icon in the Tags panel
- FIXED: Trigger for scheduled Reports cannot be edited
- FIXED: Exclusions table shows the "Occurred" column, but it is labeled as "Created on"
- FIXED: "Export table as" now exports all data, not just data on the page
- FIXED: Trigger via CRON shows different time after opening details of a specific trigger
- REMOVED: "Auto-loading" option in the Clients and Detections screen paging menu
- Various other minor bug fixes, security and performance improvements

ESET PROTECT Cloud 3.2

Release date: February, 2022

- ADDED: Easier enrollment for mobile devices
- ADDED: Easier deployment mechanism also extended for MSPs
- ADDED: New product tour

- ADDED: ESET Product Navigator to the header
- ADDED: New context menu action "Deploy ESET security product" (in Computers section)
- ADDED: AD user sync tool for ESET PROTECT Cloud
- ADDED: AD user sync-based features enabled for iOS devices
- IMPROVED: Context menu in Computers section
- IMPROVED: Installer creation Wizard
- IMPROVED: Email enrollment progress bar to indicate whether the task has been finished
- IMPROVED: Computer with IP column was divided into two columns in Submitted Files
- IMPROVED: Retention policy dialog is more user-friendly and upper limits are communicated in the Online Help guide
- FIXED: Last scan time in computer details
- FIXED: When "Module update failed" occurs, the computer is not moved to the related Dynamic Group, if the Dynamic Group was created
- FIXED: Policies under "Manage policies" over a group do not display for users with an administrator permission set
- FIXED: "Restart required" and "Inbound Communication" columns in the Detections list display incorrect values

ESET PROTECT Cloud 3.1.5

Release date: January, 2022

- ADDED: Easier deployment - the new simplified dialog for installer download, and reworked wizard for creation of the customized installer
- ADDED: Dynamic groups for mobile devices
- ADDED: Easy trial, deploy and purchase of ESET Dynamic Threat Defense (EDTD) also for MSP customers
- ADDED: Hide and Show action for EDTD Dashboard
- ADDED: Possibility to add Group Name column in the Detections section (not displayed by default)
- CHANGED: Default message contents (Computer first connected, Computer identity recovered, Computer cloning question created)
- IMPROVED: EDTD status (enabled/disabled) is reported properly to the console (requires ESET Endpoint Antivirus/Security for Windows version 9.0 and above) and leveraged in various sections (for example, action Enable is not offered for endpoint where the feature is already enabled)
- IMPROVED: Computer description can be multiline

- IMPROVED: User can define more than one naming pattern for VDI master image
- IMPROVED: Hover effect (Inverted color) on the cell with Computer name (in Computers section) and on the cell with Detection type (in Detections section)
- IMPROVED: Computer name and IP is now in separate columns in the Detection section
- FIXED: Multiple sorting does not work as expected when the top priority is assigned to the Alerts column
- FIXED: The overall status of the license might not be shown correctly in specific cases
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 3.0

Release date: October, 2021

- ADDED: Support for Automatic Product Updates (available from ESET Endpoint Antivirus/Security for Windows version 9.0)
- ADDED: Management for brute-force attack protection (available from ESET Endpoint Antivirus/Security for Windows version 9.0)
- ADDED: Easy trial, deploy and purchase of ESET Dynamic Threat Defense (EDTD)
- ADDED: Web control for Android devices
- ADDED: System updates management for Android
- ADDED: New column Logged users in Computers table
- ADDED: Windows OS build number is reported as a separate symbol (possibility to use it in Dynamic groups)
- ADDED: List of submitted files (EDTD) in Computer details, Detection and Quarantine section
- ADDED: New product categories in Component version status section on Status Overview
- ADDED: Full path to a computer in received notifications
- ADDED: Possibility disable the triggering of notifications for muted computers
- ADDED: Possibility to manage session protection (e.g., disable blocking requests from different IP addresses)
- CHANGED: Reducing and re-organizing columns in the Computers section
- IMPROVED: ESET Dynamic Threat Defense perception (added information of what was originally detected by EDTD)
- IMPROVED: Operating system update - allowing the user to postpone the required reboot
- IMPROVED: Operating system update task accessible not only from context menu over a group but also over a single device
- IMPROVED: Now is possible to visually distinguish locked policies in policies and computer details screens

(padlock icon)

- IMPROVED: When users create new permission sets, some checkboxes can grey out based on their permission (users can not give higher permission that they have)
- IMPROVED: Automatically selected newly created permission set when creating a new user
- IMPROVED: Basic support of installer file caching in script-based Agent Live Installers
- IMPROVED: Date and Time displayed in format according to language
- IMPROVED: Faster displaying of the planned flag on client tasks also after assigning to the significant amount of targets
- IMPROVED: The enrollment URL link is visible below the QR code, and the user can copy it in the enrollment wizard
- IMPROVED: New version of Log Collector in Management Agent
- FIXED: Idle session timeout was not matching settings in ESET Business Account
- FIXED: Triggers - infinite loading in some cases when the user changes trigger type
- FIXED: Unwanted machines moved during computers import
- FIXED: Missing notification about scheduled restart (macOS - osascript)
- FIXED: License is randomly changed when the software install task is edited
- FIXED: Notifications - Message preview is not displaying properly
- FIXED: macOS Big Sur, specific protections statuses are missing in dynamic groups and report templates
- FIXED: Users without access to an EDTD license cannot see the data on the EDTD Dashboard
- FIXED: Multiple sorting does not sort correctly
- FIXED: Performance issue when deleting a large number of exclusions
- FIXED: EDTD Deployment on Dynamic Group ends with error
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 2.4

Release date: August, 2021

- ADDED: Ability to manage up to 25,000 devices (according to purchased license)
- ADDED: New ESET Dynamic Threat Defense dashboard
- ADDED: Preview feature - Easy trial, deploy and purchase of ESET Dynamic Threat Defense
- ADDED: Ability to create a new trigger in client task details

- ADDED: Indicator of last connection status of managed computer (connected in last replication interval)
- ADDED: Computer preview - by clicking on computer name will be displayed side panel with the most important computer details
- ADDED: Detections preview - by clicking on detection type will be displayed side panel with the most important detection details
- CHANGED: Existing ESET Dynamic Threat Defense dashboard name change
- CHANGED: Triggers for server tasks and client tasks with frequencies lower than 15 minutes will not be allowed
- CHANGED: More granular communication of managed applications versions
- CHANGED: Automatic application of retention policy after the grace period
- CHANGED: After de-enrollment, ABM devices no longer offer the re-enroll task option
- IMPROVED: A user or a computer can only be assigned to 200 users or computers in one operation to retain adequate service responsiveness
- FIXED: Actions in the context menu for devices were disabled incorrectly (Enable ESET Dynamic Threat Defense, Network Isolation)
- FIXED: Licenses without an expiration date (for example, subscription licenses) were counted as expired in the Status Overview
- FIXED: Automatic update of company name in the console when changed in ESET Business Account or ESET MSP Administrator
- FIXED: Discrepancy in "Total number of devices" on the Dashboard compared to the total count of devices shown in the Computers tab
- FIXED: FaceID screen is now correctly skipped during ABM enrollment when selected in the wizard as one of the items to be skipped
- FIXED: "Title" in the properties of the exported PDF report

ESET PROTECT Cloud 2.3

Release date: June, 2021

- ADDED: Management of Apple devices running iOS and iPadOS, including Apple Business Manager
- ADDED: Native ARM64 support for ESET Management Agent for Windows
- ADDED: Support for VMWare Instant Clones
- ADDED: New audit information on the policy screen (Modification time, Last modified by, and Creation time)
- ADDED: Upgrade outdated operating systems in a computer group
- ADDED: Ability to copy a license Public ID to the clipboard via the context menu in license management

- ADDED: Ability to filter licenses on the license management screen based on the Public ID
- ADDED: Automatic resolution of HIPS logs
- ADDED: Computer description as a new attribute in Device Identifiers under computer details
- ADDED: Support for migration and backup of ESET Full Disk Encryption (EFDE) recovery data
- ADDED: New client task "Generate new FDE Recovery password" (available from EFDE client version 1.3 (EFDE - purchased separately))
- ADDED: Ability to retry encryption from the console if encryption fails (available from EFDE client version 1.3 (EFDE - purchased separately))
- IMPROVED: Preview feature – Computer preview (added new sections and the possibility to click on some elements and navigate to relevant details)
- IMPROVED: The Syslog export now also supports the information log level
- IMPROVED: The ESET Full Disk Encryption status now provides more details
- IMPROVED: Extended Hardware inventory details for the device with encryption-related fields
- IMPROVED: Disabled computers are not synced or deleted by the Active Directory scanner
- IMPROVED: Various UI and UX improvements
- CHANGED: Retention policy enforcement notification
- CHANGED: The CRON trigger can be planned for LOCAL or UTC time only
- CHANGED: The Wipe task has been dropped because it does not work properly in newer versions of Android. The Factory Reset task remains the only task for both Apple and Android devices
- CHANGED: Adjustments related to managed products name changes
- FIXED: Mobile device management allows manual selection of a suitable platform in case of unrecognized mobile devices
- FIXED: The License Owner name is not updated in License Management after changing it in ESET Business Account
- FIXED: A Client task cannot be scheduled for managed computer local time (only for browser time)
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 2.2

Release date: April, 2021

- NEW: New concept–Option to preview certain features
- NEW: Preview feature–Support for iOS / iPadOS (without ABM enrollment)

- NEW: Preview feature–Computer preview
- ADDED: Upgrade outdated products in a computer group
- ADDED: Default filter in the Detection screen (unresolved detections first)
- ADDED: Ability to use a second license to activate ESET Dynamic Threat Defense in a software installation task when an eligible endpoint product is selected
- ADDED: User management for users with global "write" access
- ADDED: Expiration time for client task triggers (Triggers tab)
- ADDED: New report–Computer Hardware Overview
- ADDED: Enabled non-root administration (other than the instance creator) to manage the security of other managed accounts (depends on the upcoming EBA release planned for April 2020)
- IMPROVED: Pause a task for ESET Full Disk Encryption (capability to select an exact date and time)
- IMPROVED: The encryption status tile is now more interactive
- IMPROVED: Extended information in detection details
- IMPROVED: A recommendation message is displayed when the Administrator tries to run a client task on more than 1,000 clients (using a group is recommended)
- IMPROVED: Assigning a policy to more than 200 individual devices is permitted (using a group is recommended)
- IMPROVED: Various performance improvements
- FIXED: Licenses with over 10,000 seats were displayed as infinite
- FIXED: In some cases, the "Planned" flag In a client task remained active after a task was executed
- FIXED: The license usage number did not display the correct number when a license was overused
- FIXED: Subunits were not used by percentage usage enumeration for mail security products
- FIXED: The operating system name (Big Sur) for macOS 11.1 and 11.2 was missing
- FIXED: Various other bug fixes and improvements

ESET PROTECT Cloud 2.1

Release date: February, 2021

- ADDED: Ability to look up specific computer based on the last logged user parameter
- ADDED: Support for policy-based migration from on-premises console to cloud console
- FIXED: Issue with opening/reading PDF reports sent by email (base64-encoded)

- FIXED: Non-root user with write permission rights for ESET PROTECT Cloud in ESET Business Account cannot import or create dynamic group templates
- FIXED: Device filters on Dashboards display different values than in tables
- FIXED: In some cases, Detail in the "Audit Log" overlapping other lines
- FIXED: Product deactivation fails with timeout (in certain cases) if started by "Delete not connected computers" server task
- FIXED: User cannot delete objects in some cases even with correct access rights
- FIXED: Name of the file is garbled when Japanese characters are used
- FIXED: Various other bug fixes and minor improvements

ESET PROTECT Cloud 2.0.148.0

Release date: December, 2020

- CHANGED: ESET Cloud Administrator renamed to ESET PROTECT Cloud
- ADDED: Ability to manage and protect Android mobile devices
- ADDED: Ability to manage FileVault (macOS) native encryption when an eligible license is present
- ADDED: Increased device management limit (up to 10,000 - dependent on purchased license size)
- ADDED: One-click deployment of ESET Dynamic Threat Defense if an eligible license is present
- ADDED: Ability to manage dynamic groups
- ADDED: Ability to manage notifications
- ADDED: Ability to define specific permission sets for selected users
- ADDED: Active Directory synchronization (Computers only)
- ADDED: Syslog log exporting
- ADDED: New “Audit log” section provides detailed information about specific actions
- ADDED: Ability to mass deploy the management agent to macOS devices
- ADDED: Second-level menu for advanced options
- ADDED: Secure Browser management
- ADDED: Support for sites (ESET Business Account) licenses including new "License user" column
- ADDED: Renew a license in the “License Management” screen
- ADDED: Ability to drill-down from expiring license issues in “Dashboards” and “Reports” to obtain more information in the “License Management” screen

- ADDED: New “Manage license” context menu
- ADDED: EULA update notifications that support auto-upgrade (uPCU) of endpoint products in managed environments
- ADDED: New ESET Full Disk Encryption (EFDE) management actions directly from “Computer details”
- ADDED: New EFDE Dynamic groups and Reports
- ADDED: Detection details (LiveGrid, Observed in organization, Virus Total)
- ADDED: One-click access to client task triggers
- ADDED: Unsupported browser warning
- ADDED: New "Seats allocated to sites" present in dedicated license report
- ADDED: Multi-line command scripts for Run Command task
- ADDED: Option to create a Computer user group in the “Add computer user” wizard
- CHANGED: Management Agent - supported operating systems
- CHANGED: Retention policy defaults
- CHANGED: License unit/sub-units visualization changed to "used/total" for online licenses and "X offline" for offline licenses
- CHANGED: Access to behavior reports (when EDTD is purchased and enabled) are available (in the UI) only if an eligible license is present
- IMPROVED: Ability to define a retention policy for certain logs
- IMPROVED: Exclusions mechanism extended to firewall threats
- IMPROVED: Computer details now directly accessible by clicking the computer name
- IMPROVED: One-click Network isolation
- IMPROVED: Columns ordering
- IMPROVED: Pop-up with search option
- IMPROVED: Hierarchical Dynamic groups tree
- IMPROVED: Multi-select in pop-up (modal) windows
- IMPROVED: Ability to create one exclusion from multiple detentions with standard exclusion criteria(s)
- IMPROVED: Breadcrumbs for better navigation in Wizards
- IMPROVED: Various other performance and security improvements
- FIXED: “Delete task action” removes all client tasks, not just selected items in a task list for a specific group

- FIXED: Status filter not visible for server tasks (only in client tasks)
- FIXED: Failed to send a wake-up call from the client task details executions
- FIXED: Incorrect target group type displays when editing a client trigger
- FIXED: “Status update” type notifications fail to save if they contain the “$” character
- FIXED: Import of policies with large file sizes
- FIXED: Infinite units or subunits in tooltips for licenses in the License Management screen display incorrectly
- FIXED: License-related notifications (for example, expiration/overuse) trigger when a license is suspended
- FIXED: Policy does not block the selected Scan profile
- FIXED: Filters previously set are not saved
- FIXED: Various other bug fixes

ESET Cloud Administrator 1.2.118.0

- Added: Support for ESET Dynamic Thread Defense (Sold separately. Available for purchase in upcoming weeks)
- Added: Submitted files screen
- ADDED: Ability to pause ESET Full Disk Encryption available from EFDE client version 1.2 (EFDE - purchased separately)
- ADDED: Automatic resolution of firewall logs and filtered websites
- ADDED: Ukrainian language
- ADDED: New filtering options
- ADDED: Many other performance, usability, and security improvements
- IMPROVED: Discontinued the default limit for the number of displayed static groups
- IMPROVED: Performance improvements in the “groups” tree on the “Computers” and “Detections” screens
- IMPROVED: Selected screens redesign: Users, scheduled reports and edit updates in the navigation bar
- IMPROVED: Unified table design for task selection, computers selection, and other features
- IMPROVED: Second-level menu added under "Change assignments" in the policy screen
- FIXED: Delay of product version status shown in the main web console
- FIXED: System applications are not reported on macOS 10.15
- FIXED: Language detection on macOS Catalina

- FIXED: Table sorting behavior: Clicking column headers adds columns to multi-sorting until it has been clicked 3 times
- FIXED: Last scan time in “computer details” screen won’t impact the computer security status tile
- FIXED: User cannot resolve detections when the “Resolved” column is not shown in the “detections” table
- FIXED: The side panel does not remember the expanded/collapsed state after log-out and log-in
- FIXED: Some threats cannot be marked as resolved
- FIXED: After moving computers from a specific group, the view is changed to the group "ALL."

ESET Cloud Administrator - ESET Management Agent release- June

- ADDED: New version of ESET Management Agent
- ADDED: Updating ESET Management Agent to the latest version can be deployed centrally alongside the cloud service update
- ADDED: Agent compatibility with H1/2021 Windows version 10

ESET Cloud Administrator 1.2.82.0

- IMPROVED: Email domain validation when sending live installer link was discontinued
- IMPROVED: Checkbox "automatically reboot when needed" not checked by default when activating EFDE from encryption tile
- IMPROVED: Dozens of usability, security, performance and stability improvements
- FIXED: Clicking column headers adds columns to multi-sorting until it has been clicked 3 times
- FIXED: Last Scan Time should note trigger red security status
- FIXED: Not possible to resolve detections when "Resolution" column is not shown
- FIXED: The side panel doesn't remember expanded/collapsed state after log-out and log-in
- FIXED: Agents stop connecting to cloud service under some circumstances
- FIXED: Recipients not visible in notifications emails
- FIXED: Computer with outdated OS are not visible in appropriate dynamic group
- FIXED: Ability to create hash exclusion without a hash present
- FIXED: ESET Full Disk Encryption not included within the selective export task configuration

ESET Cloud Administrator 1.2

- NEW: ESET Full Disk Encryption

- NEW: Tagging - mark all relevant objects (e.g., computers) using user-defined tags
- NEW: Support for the newest generation of Linux products, starting with ESET File Security for Linux v7
- NEW: Centralized Exclusions and wizard
- ADDED: Option to automatically delete computers that are not connecting
- ADDED: Option to rename computers based on defined criteria
- ADDED: Computer isolation task
- ADDED: Unified table design with new navigation elements
- ADDED: Ability to export tables across all the main screens to different formats
- ADDED: New "empty screen states" for simpler object creation
- ADDED: Detections view is now aggregated by time and other criteria to simplify operations and to resolve them
- ADDED: Execute one click actions from the "task executions" screen
- ADDED: Create a combined installer including ESET Full Disk Encryption
- ADDED: Option to deactivate individual products
- ADDED: New dynamic groups related to newly introduced products
- ADDED: Search by group name in computer screens and search bar
- ADDED: Option to save dashboard layout as preset for other users
- ADDED: Generate defined reports filtered to a selected group
- ADDED: Indonesian language support
- ADDED: New ESET Management Agent version (Windows) supports the latest security products
- IMPROVED: Many UI Improvements & other usability changes
- IMPROVED: Context menu now applies for all selected rows
- IMPROVED: Filtering panel has many new options such as autocomplete
- IMPROVED: New column selector element for primary tables
- IMPROVED: Layout of detections (previously "threats") screen with new detection details
- IMPROVED: Reports screen layout includes a one click report generation option
- IMPROVED: Task section was updated and triggers are now displayed in a separate view of "task details"
- IMPROVED: Layout of policies screen, with simpler orientation and navigation

- IMPROVED: Layout of notifications screen with notification details
- IMPROVED: Quick links menu
- IMPROVED: AV remover (part of management agent) supports auto update
- IMPROVED: Download speeds from the repositories were significantly improved
- IMPROVED: Management agent file size significantly reduced
- CHANGED: "Threats" section was renamed to "Detections"
- CHANGED: Management agent compatibility update related to macOS 10.7 and 10.8 support (see the documentation for more details)
- CHANGED: ESET Cloud Administrator ends support for Endpoint and Server Security versions 6.4 and earlier
- FIXED: Various other bug fixes and internal performance improvements

ESET Cloud Administrator 1.1.360.0

- Added: Full support for endpoint version 7.1 products
- Fixed: Various bugs

ESET Cloud Administrator 1.1.359.0

- Improved: Internal performance improvements

ESET Cloud Administrator 1.1.358.0

- Improved: Overall performance improvements
- Changed: Updated copyright information
- Fixed: ESET Cloud Administrator (ECA) server does not receive all "Web protection" threats
- Fixed: "Web protection" threat details view in the webconsole displays an unexpected error
- Fixed: An uncaught exception occurs when working with ECA
- Fixed: Indonesian language support is missing in product installation filters
- Fixed: Server Device Status chart is missing

ESET Cloud Administrator 1.1.356.0

- FIXED: Issue with too many notifications send from one incident

ESET Cloud Administrator 1.1.350.0

- New version of ESET Management Agent fixing various installation/upgrade/repair issues
- Internal service performance improvements
- Fixed invalid installer CA certificate encoding in GPO installer script

ESET Cloud Administrator 1.1.349

- Various minor performance improvements

ESET Cloud Administrator 1.1.345

- Various minor bug fixes
- Wrong information is displayed under "Policy Product" column while creating the ECA Live installer

ESET Cloud Administrator 1.1.343.0

- One-click actions
- New one-click action - One click upgrade option – even from aggregated data
- New One-click actions to resolve "resolvable" actions – activate, reboot, update OS, or various protection issues
- Hardware inventory
- Redesigned client details section
- New "incident overview" dashboard, with new types of graphical elements, and one-click navigation to threats
- Improved Automatic resolving of handled threats
- Option to generate live installer without security product selected
- New status overview section
- Live installer now support offline cache to speed up the deployment
- Overall UI improvements (polished UI, new vector icons, updated menus)
- Updated "overview" dashboard with one click navigation & Configurable RSS feed
- Redesigned quick links & help links
- New layout for wizard elements
- Ability to switch ECA do different language in EBA (support for NEW languages)

- Automatic detection of "machine cloning"
- Ability to send e-mail directly from ECA when sending installer
- Automatic log-outs
- New more streamlined way when adding computers or using introductory wizard
- Redesigned "filter bar" with the option to remove / reset / save filter presets + "category filter" moved to "filters"
- New columns for number / highest severity of alerts, cloning questions, and hardware detection reliability status
- Enhanced filtering options by product name, version, number of alerts, policies, threats, & other options
- New "remove computer from management" wizard, showing clear steps how to correctly remove devices from ECA
- Redesigned task wizard
- New task types - Diagnostic (enable diagnostic / Log Collector)
- Section "logs" now includes tabs to display "Log Collector" and new section for "diagnostic logs"
- Alerts - Alert (problem) details are reported from the supported security products
- New dynamic groups for desktops and servers
- Questions to resolve conflicts
- Possible to locate threats detected by the same scan
- Added current detection engine version and a hash value
- Possibility to filter by cause, threat type, scan, scanner and define more granular criteria for the time filter in threats
- Possibility to collapse and expand all reports in one click
- Software installation task executes a "pre-execution check", and reports "task failed" with further details
- New report template categories Hardware Inventory, Cloning Detection
- Restyled report creation wizard
- Extended options for filtering for specific values
- Redesigned installer generation flow
- Ability to configure LiveGrid and PUA settings when creating live installer
- Ability to configure Live Installer proxy settings during the installer creation

- Support for GPO (Group policy)
- New filter to "hide not-assigned policies"
- Policy details showing "assigned to" (combines computers / groups) and "applied on" (actually applied targets)
- New predefined policies for optimal usage of ESET Live Grid, and few tweaks to existing recommended templates for maximum protection
- Possibility to allow "local lists"
- Possible to edit multiple notifications at once
- New announcement channel to inform users about planned outages and other important events
- Improved migration from ERA6 (ESMC) managed environment when executing live installers

Podporované prohlížeče, ESET produkty a jazyky

Webovou konzoli ESET PROTECT lze spustit v následujících webových prohlížečích:

Webový prohlížeč
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

Pro co nejlepší práci s webovou konzolí ESET PROTECT doporučujeme používat vždy nejnovější verzi webového prohlížeče.

Aktuální verze bezpečnostních řešení ESET, které je možné spravovat prostřednictvím ESET PROTECT

Pro úplnou správu nejnovějších verzí bezpečnostních řešení ESET a jejich funkcí vám doporučujeme používat nejnovější verze ESET Management Agenta.

Produkt	Verze produktu
ESET Endpoint Security pro Windows	7.3+
ESET Endpoint Antivirus pro Windows	7.3+
ESET Endpoint Security pro macOS	6.10+
ESET Endpoint Antivirus pro macOS	6.10+
ESET File Security pro Windows Server	7.3+
ESET Server Security pro Microsoft Windows Server	7.3+
ESET Mail Security pro Microsoft Exchange Server	7.3+
ESET Security pro Microsoft SharePoint Server	7.3+

Produkt	Verze produktu
ESET Mail Security pro IBM Domino Server	7.3+
ESET File Security pro Linux:	7.2+
ESET Server Security pro Linux	7.2, 8.1, 9.x, 10.x
ESET Endpoint Antivirus pro Linux:	7.1, 8.1, 9.x, 10.x
ESET Endpoint Security pro Android	3.3+
ESET Inspect Connector	1.8+
ESET Full Disk Encryption pro Windows	
ESET Full Disk Encryption pro macOS	
ESET LiveGuard Advanced	

Podporované jazyky

Jazyk	Kód
English (United States)	en-US
Arabic (Egypt)	ar-EG
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Croatia)	hr-HR
Czech (Czech Republic)	cs-CZ
French (France)	fr-FR
French (Canada)	fr-CA
German (Germany)	de-DE
Greek (Greece)	el-GR
Hungarian (Hungary)*	hu-HU
Indonesian (Indonesia)*	id-ID
Italian (Italy)	it-IT
Japanese (Japan)	ja-JP
Korean (Korea)	ko-KR
Polish (Poland)	pl-PL
Portuguese (Brazil)	pt-BR
Russian (Russia)	ru-RU
Spanish (Chile)	es-CL
Spanish (Spain)	es-ES
Slovak (Slovakia)	sk-SK
Turkish (Turkey)	tr-TR
Ukrainian (Ukraine)	uk-UA

* V tomto jazyce je dostupný pouze produkt, nikoli online příručka.

Podporované operační systémy

V tabulce níže jsou uvedeny verze operační systémů, které jsou podporovány jednotlivými komponentami infrastruktury ESET PROTECT:

Verzování a podpora ESET Management Agenta

ESET Management Agent se řídí číslem verze ESET PROTECT On-Prem a politikou konce životního cyklu:

- Podporované verze ESET Management Agenta jsou 9.x–11.x.
- Pro každou verzi ESET Management Agenta je šest měsíců Úplné podpory a dva roky Částečné podpory. Poté dojde k ukončení životního cyklu dané verze.

Nejnovější podporovaná verze ESET Management Agenta je 11.x. Pro úplnou správu nejnovějších verzí bezpečnostních řešení ESET a jejich funkcí vám doporučujeme používat nejnovější verze ESET Management Agenta.

Windows

Operační systém	Agent	RD Sensor
Windows Server 2012 x64	9.x—10.x, 11.x	✔
Windows Server 2012 CORE x64	9.x—10.x, 11.x	✔
Windows Server 2012 R2 x64	9.x—10.x, 11.x	✔
Windows Server 2012 R2 CORE x64	9.x—10.x, 11.x	✔
Windows Storage Server 2012 R2 x64	9.x—10.x, 11.x	✔
Windows Server 2016 x64	9.x—10.x, 11.x	✔
Windows Storage Server 2016 x64	9.x—10.x, 11.x	✔
Windows Server 2019 x64	9.x—10.x, 11.x	✔
Windows Server 2022 x64	9.x—10.x, 11.x	✔
Windows Server 2022 CORE x64	11.x	

Operační systém	Agent	RD Sensor
Windows 10 x86	9.x—10.x, 11.x	✔
Windows 10 x64 (všechna oficiální sestavení)	9.x—10.x, 11.x	✔
Windows 10 ARM	9.x—10.x, 11.x	
Windows 11 x64	9.x (21H2) 10.x, 11.x (21H2,22H2) 10.1, 11.x (23H2)	✔
Windows 11 ARM	10.x, 11.x	

ESET Management Agent ve verzi 10.x je poslední verzí, která podporuje Windows 7/8.x a Windows Server 2008 R2/Microsoft SBS 2011.

Linux

Operační systém	Agent	RD Sensor
Ubuntu 18.04.1 LTS x64 Desktop	9.x—10.x, 11.x	✔
Ubuntu 18.04.1 LTS x64 Server	9.x—10.x, 11.x	✔
Ubuntu 20.04 LTS x64	9.x—10.x, 11.x	✔
Ubuntu 22.04 LTS x64	10.x, 11.x	✔
Linux Mint 20	10.x, 11.x	✔
Linux Mint 21	10.1, 11.x	✔
RHEL Server 7 x64	9.x—10.x, 11.x	✔
RHEL Server 8 x64	9.x—10.x, 11.x	
RHEL Server 9 x64	9.x—10.x, 11.x	✔
CentOS 7 x64	9.x—10.x, 11.x	✔
SLED 15 x64	9.x—10.x, 11.x	✔
SLES 12 x64	9.x—10.x, 11.x	✔
SLES 15 x64	9.x—10.x, 11.x	✔
Debian 9 x64	9.x—10.x, 11.x	✔
Debian 10 x64	9.x—10.x, 11.x	✔
Debian 11 x64	9.x—10.x, 11.x	✔
Debian 12 x64	10.1, 11.x	✔
Oracle Linux 8	9.x—10.x, 11.x	✔
Amazon Linux 2	9.x—10.x, 11.x	✔
Alma Linux 9	10.1, 11.x	✔
Rocky Linux 8	10.1, 11.x	
Rocky Linux 9	10.1, 11.x	

ESET Management Agent byl otestován a spuštěn na nejnovějších uvedených vedlejších verzích distribucí Linuxu.

Mac

Operační systém	Agent
macOS Catalina (10.15)	9.x—10.x, 11.x
macOS Big Sur (11.0)	9.x—10.x, 11.x
macOS Monterey (12.0)	9.x—10.x, 11.x
macOS Ventura (13.0)	9.x—10.x, 11.x
macOS Sonoma (14.0)	10.1, 11.x

Mobilní zařízení

Operační systém	EESA	EESA na zařízeních s omezenými možnostmi vstupu	EESA Vlastník zařízení	MDM iOS	MDM iOS ABM
Android 6.x+	✔	✔			
Android 7.x+	✔	✔	✔		
Android 8.x+	✔	✔	✔		
Android 9.0	✔	✔	✔		
Android 10.0	✔	✔	✔		
Android 11	✔	✔	✔		
Android 12	✔	✔	✔		
Android 13	✔	✔	✔		
Android 14	✔	✔	✔		
iOS 9.x+				✔	✔*
iOS 10.x+				✔	✔*
iOS 11.x+				✔	✔*
iOS 12.0.x				✔	✔*
iOS 13.x+				✔	✔
iOS 14.x+				✔	✔
iOS 15				✔	✔
iOS 16				✔	✔
iOS 17				✔	✔
iPadOS 13				✔	✔
iPadOS 14				✔	✔
iPadOS 15				✔	✔
iPadOS 16				✔	✔
iPadOS 17				✔	✔

* Program iOS ABM je k dispozici jen ve vybraných zemích.

Požadavky pro síť

Pro správnou funkci ESET PROTECT se ujistěte, že máte správně nastavený firewall dle níže uvedených síťových požadavků.

Domény a porty

Doména	Protokol	Port	Služba/komponenta	Popis
eba.eset.com	TCP	443	ESET Business Account	
msp.eset.com	TCP	443	ESET MSP Administrator	
identity.eset.com	TCP	443	ESET Identity Server	

Doména	Protokol	Port	Služba/komponenta	Popis
protect.eset.com	TCP	443	ESET PROTECT	
eu02.protect.eset.com	TCP	443	ESET PROTECT Web Console	Umístění: Evropa
us02.protect.eset.com	TCP	443		Umístění: USA
jp02.protect.eset.com	TCP	443		Umístění: Japonsko
*.a.ecaserver.eset.com	TCP	443	Spojení mezi agenty a ESET PROTECT	
edf.eset.com	TCP	443	Live Installer	
redirector.eset.systems	TCP	443		
repository.eset.com	TCP	80		Repozitář pro nasazení
epns.eset.com	TCP	8883	Spojení s EPNS službou (wake-up call)	
eu.mdm.eset.com (EVROPA) us.mdm.eset.com (USA) jp.mdm.eset.com (Japonsko)	TCP	443	Cloudové MDM	Registrace
checkin.eu.eset.com (EVROPA) checkin.us.eset.com (USA) checkin.jp.eset.com (Japonsko)	TCP	443		Check-in
mdmcomm.eu.eset.com (EVROPA) mdmcomm.us.eset.com (USA) mdmcomm.jp.eset.com (Japonsko)	TCP	443		Komunikace
mdm.eset.com (GLOBÁLNÍ)	TCP	443		Registrace zařízení s omezenými možnosti vstupu
	TCP	139	ESET PROTECT Remote Deployment Tool (Cílový port z pohledu stanice, na které spouštíte Remote Deployment Tool)	Použití ADMIN$ sdílení
	TCP	445		Přímý přístup ke sdíleným prostředkům prostřednictvím TCP/IP v průběhu vzdálené instalace (alternativa k TCP 139)
	UDP	137		Překlad jmen v průběhu vzdálené instalace
	UDP	138		Procházení v průběhu vzdálené instalace

IP adresy

IP adresa	Služba	Popis
20.82.100.209	Spojení mezi ESET Management Agent a ESET PROTECT	Umístění: Evropa
20.245.38.118		Umístění: USA
20.194.197.189		Umístění: Japonsko
13.69.61.76	Připojení k webové konzoli ESET PROTECT	Umístění: Evropa
23.99.91.144		Umístění: USA
20.46.163.70		Umístění: Japonsko

Síťové požadavky pro **ESET Connect** naleznete v Online nápovědě k ESET Connect.

Dostupnost služby

Dostupnost

Našim cílem je zajistit 99,5% dostupnost služby. V jeho dosažení nám pomáhají dobře nastavené procesy a naše úsilí. Odstávka služby ESET PROTECT nemá vliv na koncová zařízení, která jsou v danou chvíli stále zabezpečena.

ESET Status Portal zobrazuje aktuální stav cloudových služeb ESET, plánované odstávky a minulé incidenty. Pokud máte problém s podporovanou službou ESET a nevidíte ji uvedenou ve stavovém portálu, kontaktujte technickou podporu společnosti ESET.

Monitorovací týmy interně ověřují potenciální problémy a potvrzené incidenty jsou zveřejňovány a aktualizovány ručně, aby byla zachována vysoká důvěryhodnost a přesnost. Proto se ve stavovém portálu zobrazují s mírným zpožděním. Incidenty s krátkou dobou trvání nemusí být zveřejněny, pokud jsou vyřešeny před ručním potvrzením.

Údržba

Služba ESET PROTECT podléhá standardním postupům údržby. Všechny intervaly údržby, které překročí 15 minut jsou předem oznámeny administrátorům konzole. Odstávky v průběhu údržby nemají vliv na cílovou dostupnost služby. Údržba je prováděna během víkendů a mimo pracovní dobu (v případě EU datacentra v nočních EU hodinách, v případě US datacentra v nočních US hodinách, v případě JPN datacentra v nočních JPN hodinách).

Rozdíly mezi on-premise a cloudovou konzolí pro vzdálenou správu

ESET PROTECT obsahuje všechny klíčové funkce a možnosti, které znáte z ESET PROTECT On-Prem, ale byly upraveny tak, aby vyhovovaly potřebám správy pomocí cloudu. Z ESET PROTECT On-Prem můžete migrovat na ESET PROTECT.

V následující tabulce jsou popsány základní rozdíly mezi ESET PROTECT a ESET PROTECTOn-Prem.

Obecné rozdíly	ESET PROTECT	ESET PROTECT On-Prem
Hosting	Běží v cloudovém prostředí spravovaném společností ESET.	Běží ve vašem fyzickém nebo virtualizovaném prostředí.
Omezení správy zařízení	50.000 klientů.	Limitace se odvíjí od HW prostředků serveru.
Podporované verze produktů	• Firemní bezpečnostní produkty ve verzi 6 a novější.	• Firemní bezpečnostní produkty ve verzi 4 a novější.
Komponenty	• ESET Management Agent • RD Sensor • Deployment tool • Cloud MDM	• ESET Management Agent • RD Sensor • Deployment tool • MDM
Active Directory	Synchronizace s Active Directory je možná prostřednictvím nástroje ESET Active Directory Scanner.	Synchronizace s Active Directory je podporována.
Správa mobilních zařízení (MDM)	• Správa mobilních zařízení je možná prostřednictvím CloudMDM • Možnost registrovat Android zařízení s omezenými možnostmi vstupu.	• Správa mobilních zařízení je možná prostřednictvím MDM ESET PROTECT On-Prem. ⚠ Komponenta ESET PROTECT Mobile Device Management/Connector (MDM/MDC) (pouze on-premise) dosáhla konce životního cyklu v lednu 2024. Více informací. Doporučujeme vám, abyste provedli migraci do Cloud MDM.
Certifikáty	Certifikáty jsou spravovány společností ESET.	Můžete si vytvořit nové, upravit stávající a certifikáty i certifikační autority importovat/exportovat.
Přístupová oprávnění	Správa přístupových oprávnění byla přesunuta do ESET Business Account. Nicméně použitím vlastních sad oprávnění můžete uživatelům povolit přístup ke konkrétním částem ESET PROTECT.	Pokročilý model multitenantních přístupových oprávnění lze spravovat z prostředí ESET PROTECTOn-Prem.

Obecné rozdíly	ESET PROTECT	ESET PROTECT On-Prem
Správa licence	Správa licence byla přesunuta do ESET Business Account.	Licenci je možné částečně spravovat v ESET PROTECTOn-Prem a částečně ESET Business Account.
Jak přidat počítače	Počítače můžete přidat synchronizací Active Directory, z přehledu komponenty RD Sensor nebo prostřednictvím skriptu GPO/SCCM.	Počítače můžete přidat synchronizací s Active Directory, z přehledu komponenty RD Sensor nebo prostřednictvím GPO/SCCM skriptu, ručně zadáním názvu počítače a spuštěním úlohy na nasazení agenta, nebo nainstalováním agenta lokálně.
Další ochranné vrstvy	• Správa zranitelností a záplat • ESET LiveGuard • ESET Full Disk Encryption • ESET Inspect ESET PROTECT nepodporuje ESET Inspect On-Prem, podporuje však ESET Inspect. Při migraci z ESET PROTECT On-Prem do ESET PROTECT nebudete moci spravovat ESET Inspect On-Prem z ESET PROTECT, můžete však spravovat ESET Inspect z ESET PROTECT.	• ESET LiveGuard • ESET Full Disk Encryption • ESET Inspect On-Prem

Začínáme s ESET PROTECT

ESET PROTECT je hotové řešení určené pro správu bezpečnostních produktů ESET v malých a středně velkých sítích. Představuje nový přístup k bezpečnosti, který doplňuje širokou škálu on-premise ESET řešení jenž přichází s novou, flexibilní, cloudovou službou provozovanou a spravovanou společností ESET.

Je určen k okamžitému použití a ve srovnání s on-premise řešením nevyžaduje instalaci a konfiguraci. ESET PROTECT je navržen tak, aby bylo snadné jej nasadit a začít používat. Tato nová cloudová služba přichází s moderní webovou konzolí pro správu (ESET PROTECT Web Console), ke které můžete přistupovat odkudkoli a z jakéhokoli zařízení připojeného k internetu.

V následujících kapitolách vám představíme ESET PROTECT Web Console a ukážeme si, jak ji používat. Prostřednictvím konzole si můžete vytvořit instalační balíček, pomocí něhož najednou nainstalujete ESET Management Agenta i bezpečnostní produkt ESET. Po nasazení ESET Management Agenta budete schopni následně stanicím přiřazovat politiky, filtrovat je prostřednictvím dynamických skupin a data z nich získaných si generovat například do přehledů nebo zasílat jako oznámení.

Začínáme s ESET PROTECT

Používám ESET Business Account

1. Vytvoření nové instance ESET PROTECT.

2. Vytvoření ESET PROTECT uživatelů v ESET Business Account

3. Otevřete si ESET PROTECT Web Console. Prostudujte si také kapitoly Prohlídka ESET PROTECT a Seznámení s webovou konzolí ESET PROTECT.

4. Namapování uživatelů z ESET Business Account v ESET PROTECT Web Console.

5. Přidání klientských stanic do ESET PROTECT struktury.

6. Jak spravovat bezpečnostní řešení ESET pro ochranu koncových zařízení prostřednictvím ESET PROTECT?

Používám ESET MSP Administrator

1. Vytvoření nové instance ESET PROTECT.

2. Vytvoření ESET PROTECT uživatelů v ESET MSP Administrator.

3. Otevřete si ESET PROTECT Web Console. Prostudujte si také kapitoly Prohlídka ESET PROTECT a Seznámení s webovou konzolí ESET PROTECT.

4. Přidání uživatelů ESET MSP Administrator do ESET PROTECT Web Console v průběhu nastavení MSP zákazníka.

5. Přidání klientských stanic do ESET PROTECT struktury.

6. Jak spravovat bezpečnostní řešení ESET pro ochranu koncových zařízení prostřednictvím ESET PROTECT?

Vytvoření nové instance ESET PROTECT za použití ESET Business Account

Požadavky

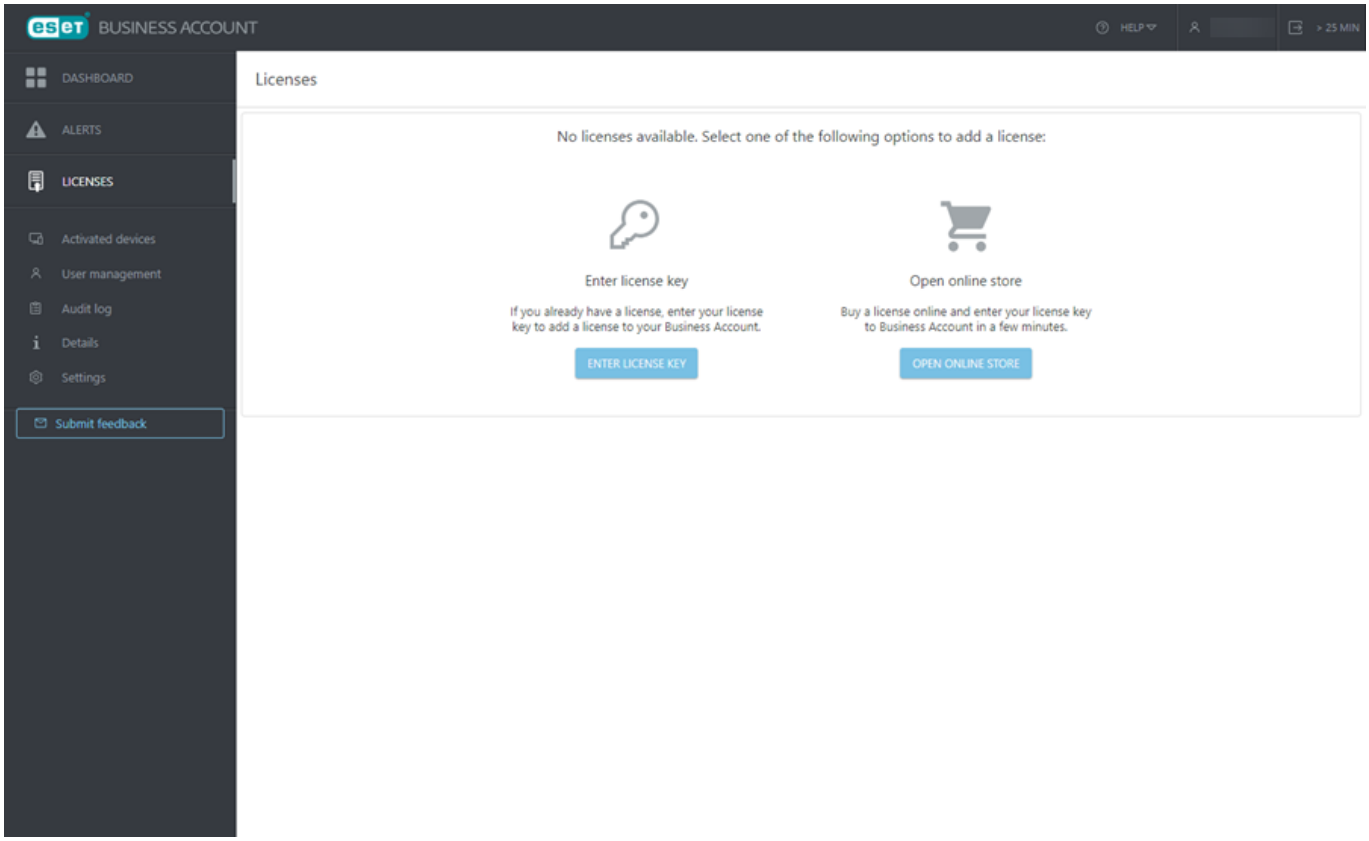
- Vytvořený účet superuživatele na portále ESET Business Account.
- Přidaná vhodná licence pro ESET PROTECT.

> Pokud máte na stejnou e-mailovou adresu založen EBA i EMA2 účet, ESET PROTECT je možné aktivovat pouze z jednoho účtu. Aktivovat nebo odstranit instanci budete schopni výhradně prostřednictvím účtu (EBA nebo EMA2), který si vyberete pro vytvoření ESET PROTECT instance.

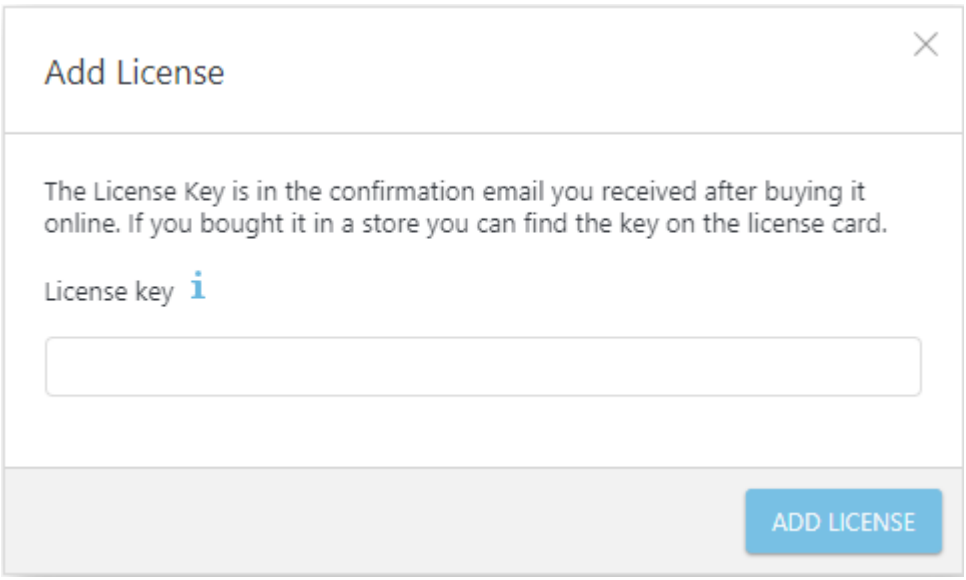
Vytvoření nové instance ESET PROTECT

1. Přihlaste na portál ESET Business Account. Pokud zatím účet nemáte, vytvořte si jej.

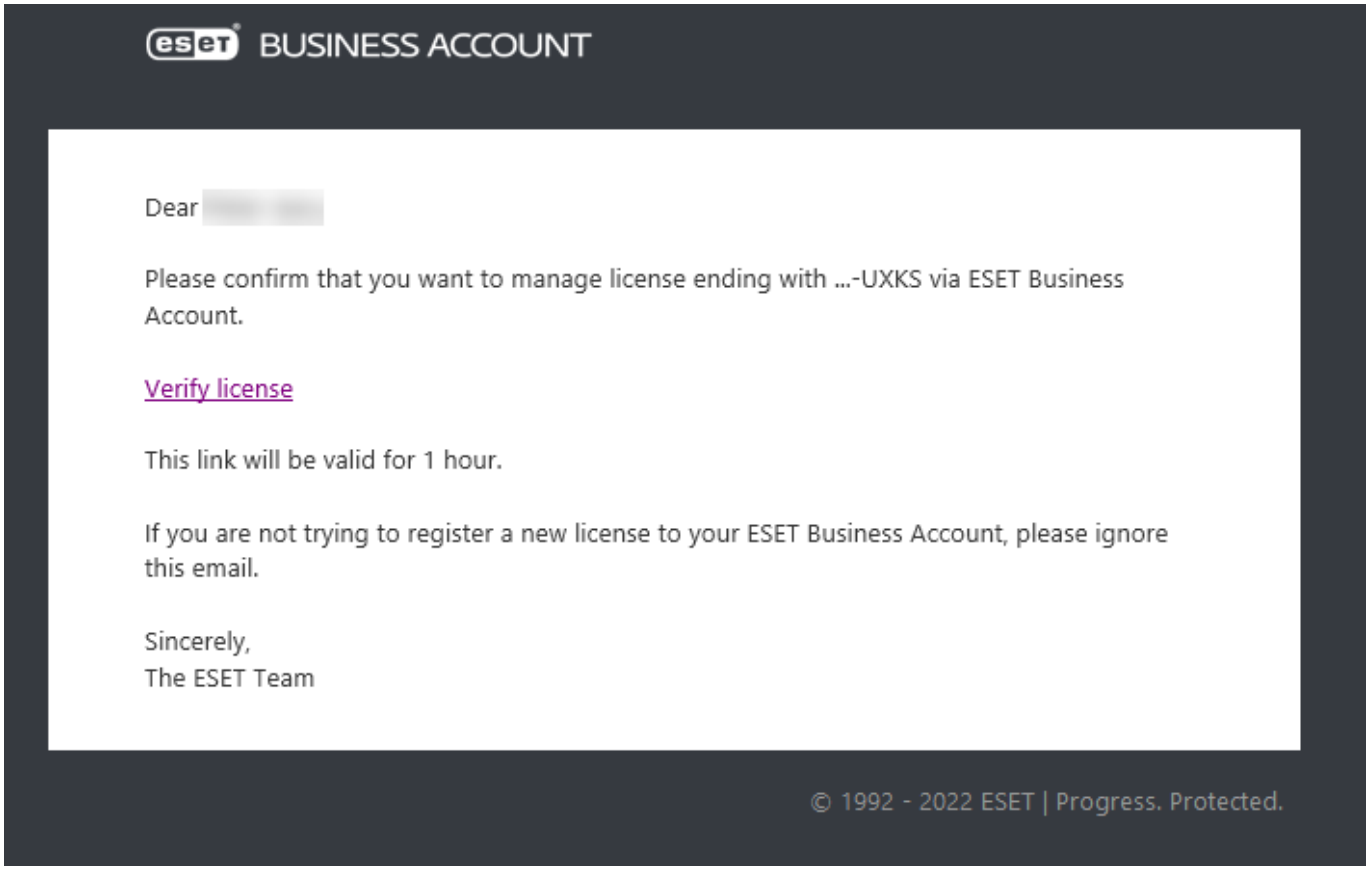
2. V hlavním menu přejděte na záložku **Licence** a klikněte na tlačítko **Zadat licenční klíč**.



3. V dialogovém okně **Přidat licenci** zadejte **licenční klíč** pro ESET PROTECT a klikněte na tlačítko **Přidat licenci**.



4. Následně obdržíte ověřovací e-mail. V případě, že vám nedorazí, postupujte podle kroků uvedených v Databázi znalostí. V e-mailu klikněte na odkaz **Ověřit licenci**.



5. Na **Nástěnce** se vám následně zpřístupní možnost pro **aktivaci ESET PROTECT**. Pokračujte kliknutím na **Aktivovat**.

⚠ Ověřte nastavení vašeho jazyka ve vašem účtu na portále ESET Business Account. Některé části produktu a předdefinované objekty ESET PROTECT se vytvoří v jazyce, který máte nastaven v ESET Business Account, a není možné jej později změnit.

6. Zobrazí se dialogové okno pro **aktivaci ESET PROTECT**. Přečtěte si a odsouhlaste podmínky použití.

7. Vyberte datové centrum nejbližší vámi spravované síti, ve kterém chcete vytvořit instanci, a klikněte na tlačítko **Pokračovat**.

⚠ Jakmile provedete potvrzení, nebude možné změnit datové centrum vaší instance.

8. Instance ESET PROTECT bude vytvořena. Vyčkejte několik minut, případně se můžete i odhlásit. Jakmile bude uvedena do provozu, zašleme vám upozornění e-mailem.

9. Klikněte na tlačítko **Pokračovat**. Může také na **Nástěnce** kliknout na tlačítko **Otevřít**. V nové záložce prohlížeče se otevře ESET PROTECT Web Console.

ESET PROTECT synchronizuje strukturu z ESET Business Account a ve Web Console je v sekci **Počítače** reprezentována jako strom statických skupin.

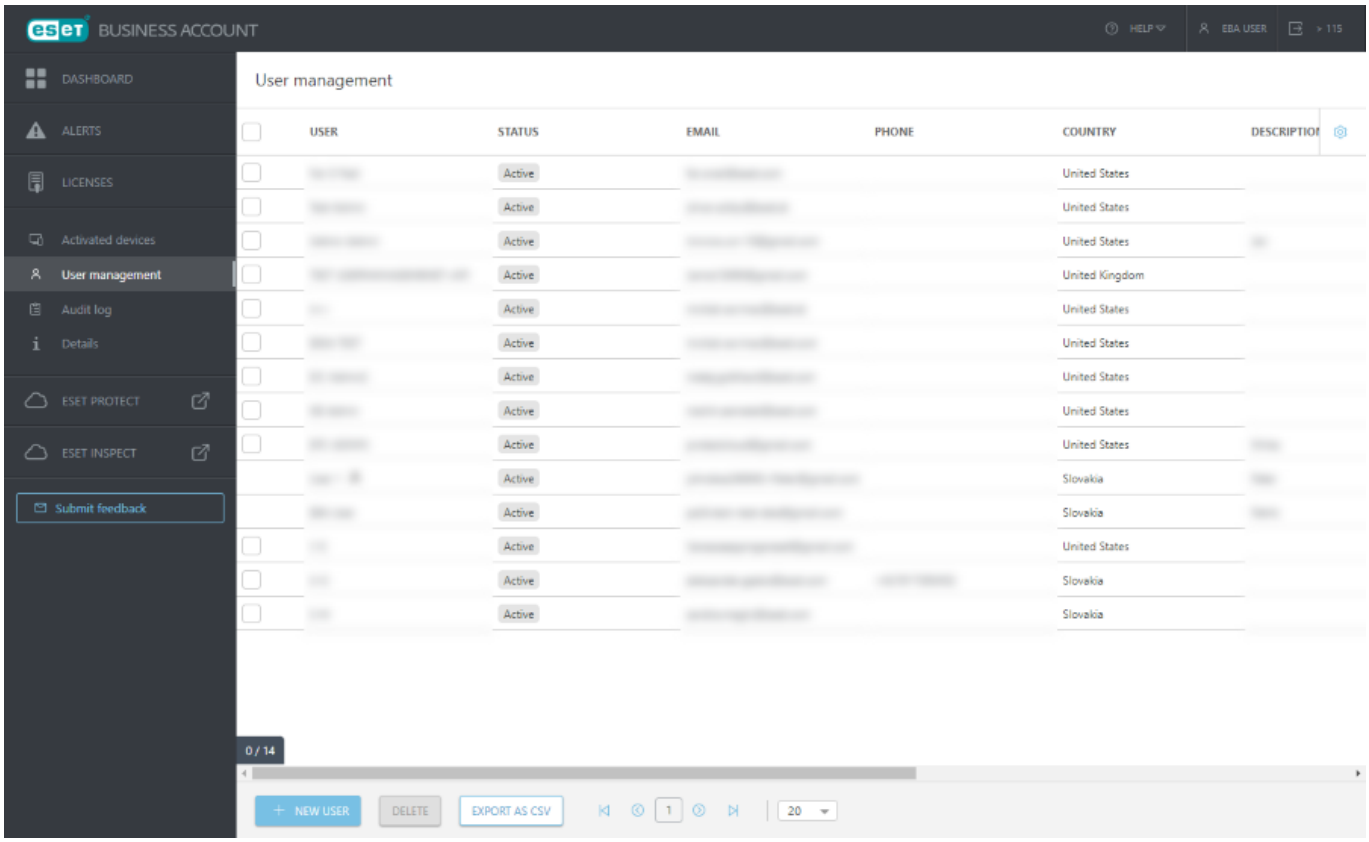
Vytvoření nového uživatele ESET PROTECT v ESET

Business Account

Pomocí níže uvedených kroků vytvoříte v ESET PROTECT nového uživatele pro ESET Business Account a namapujete jej na jeho uživatelský účet v ESET PROTECT:

1. Přihlaste se ke svému účtu na portále ESET Business Account.

2. V hlavním menu přejděte do sekce **Správa uživatelů** a klikněte na tlačítko **Nový uživatel**.



3. Vyplňte požadovaná pole (další informace naleznete v online nápovědě k ESET Business Account).

I.**Obecné** – v této části zadejte základní informace o uživateli

II.**Přístupová oprávnění**:

a)**Přístup ke společnosti** – vyberte úroveň přístupu ke společnosti: **Zápis**, **Čtení**, **Přístup pouze k vybraným lokalitám**.

> Pro zobrazení seznamu všech uživatelů z ESET Business Account v ESET PROTECT musí mít uživatel oprávnění pro **přístup ke společnosti** na úrovni **zápis**.

b)**Přístup ke správě uživatelů** – rozhodněte, zda bude tento uživatel schopen spravovat ostatní uživatele v ESET Business Account.

c)**Přístup k ESET PROTECT a ESET Inspect**:

- **Zápis** – uživatel má úplný přístup k ESET PROTECT.
- **Čtení** – uživatel si může v ESET PROTECT a ESET Inspect zobrazit pouze data.

- **Vlastní** – přístupové oprávnění si následně můžete definovat v ESET PROTECT v sekci Sady oprávnění.

- **Žádný přístup** – uživatel nemá přístup k ESET PROTECT ani ESET Inspect.

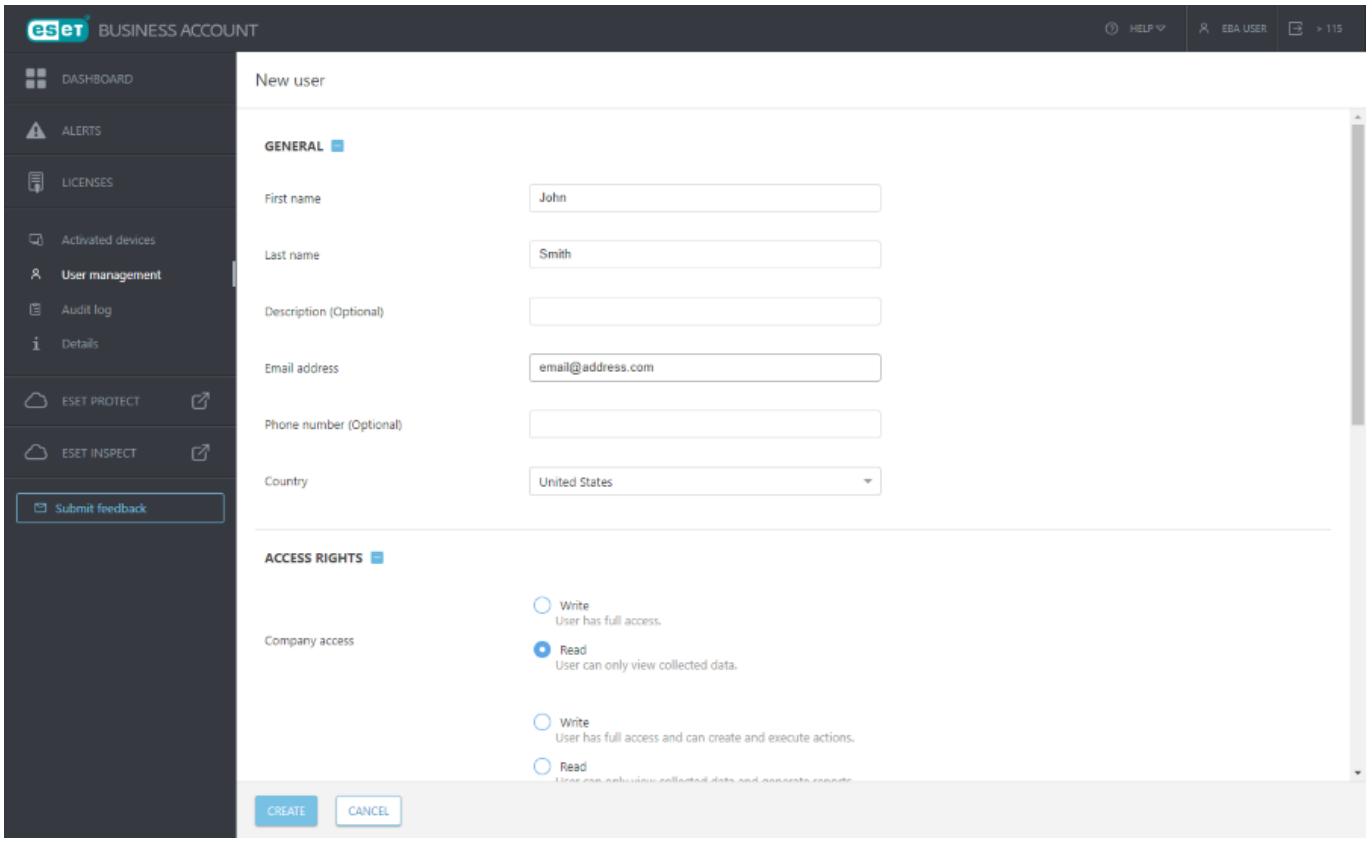
Pro přístup k ESET PROTECT musí mít uživatel oprávnění **Zápis** nebo **Čtení** alespoň k jedné společnosti s vhodnou (aktivní) licencí pro ESET PROTECT.

- Pro uživatele z lokality vyberte v části **Přístup k ESET PROTECT** možnost **Vlastní**.
- Pro vytvoření dalšího uživatele s administrátorským oprávněním postupujte podle kroků uvedených v článku Databáze znalostí Vytvoření druhého správce v ESET PROTECT (článek nemusí být dostupný v českém jazyce).

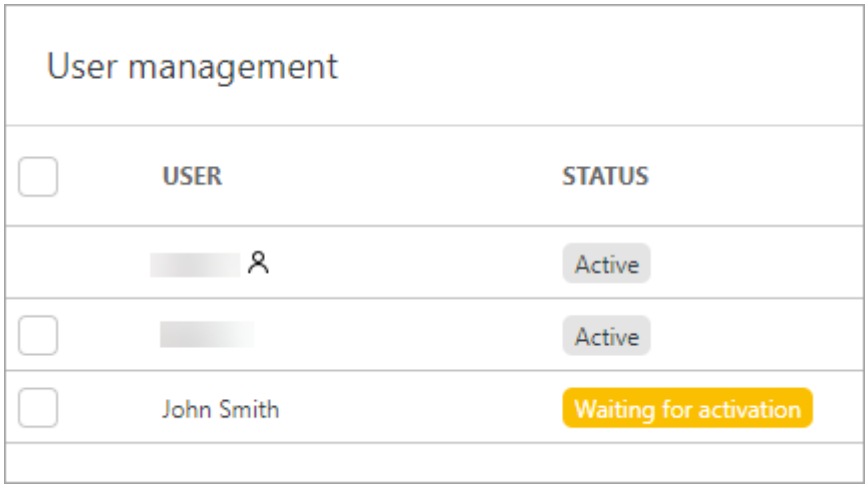
III.**Předvolby** – nastavte uživateli jazyk, ve kterém bude používat ESET Business Account a ESET PROTECT, a vyberte časové pásmo.

IV.**Zabezpečení** – v této části uživateli upravte bezpečnostní nastavení (doba platnosti hesla, doba neaktivity, dvoufaktorovou autentifikaci)

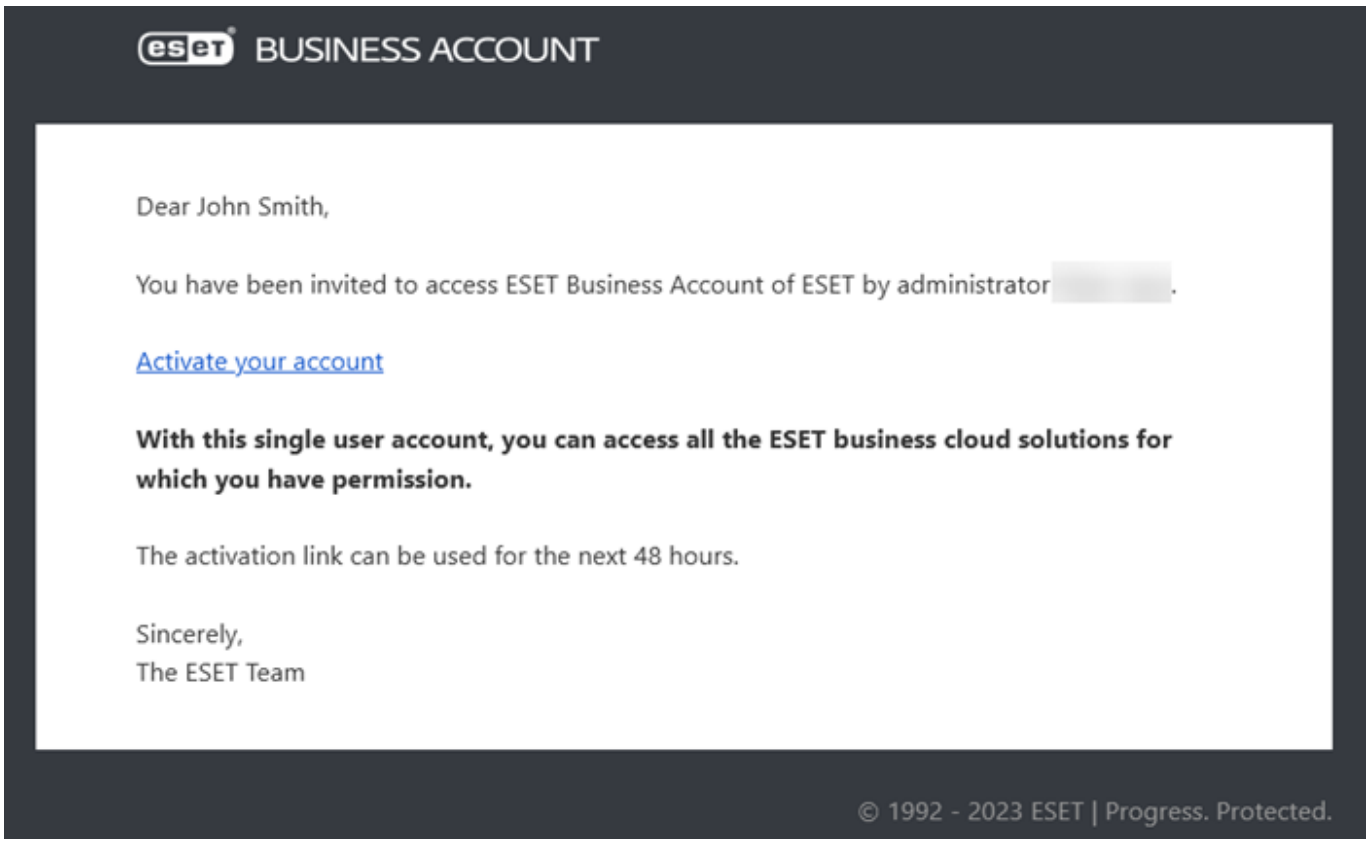
Pro dokončení akce klikněte na tlačítko **Vytvořit**.



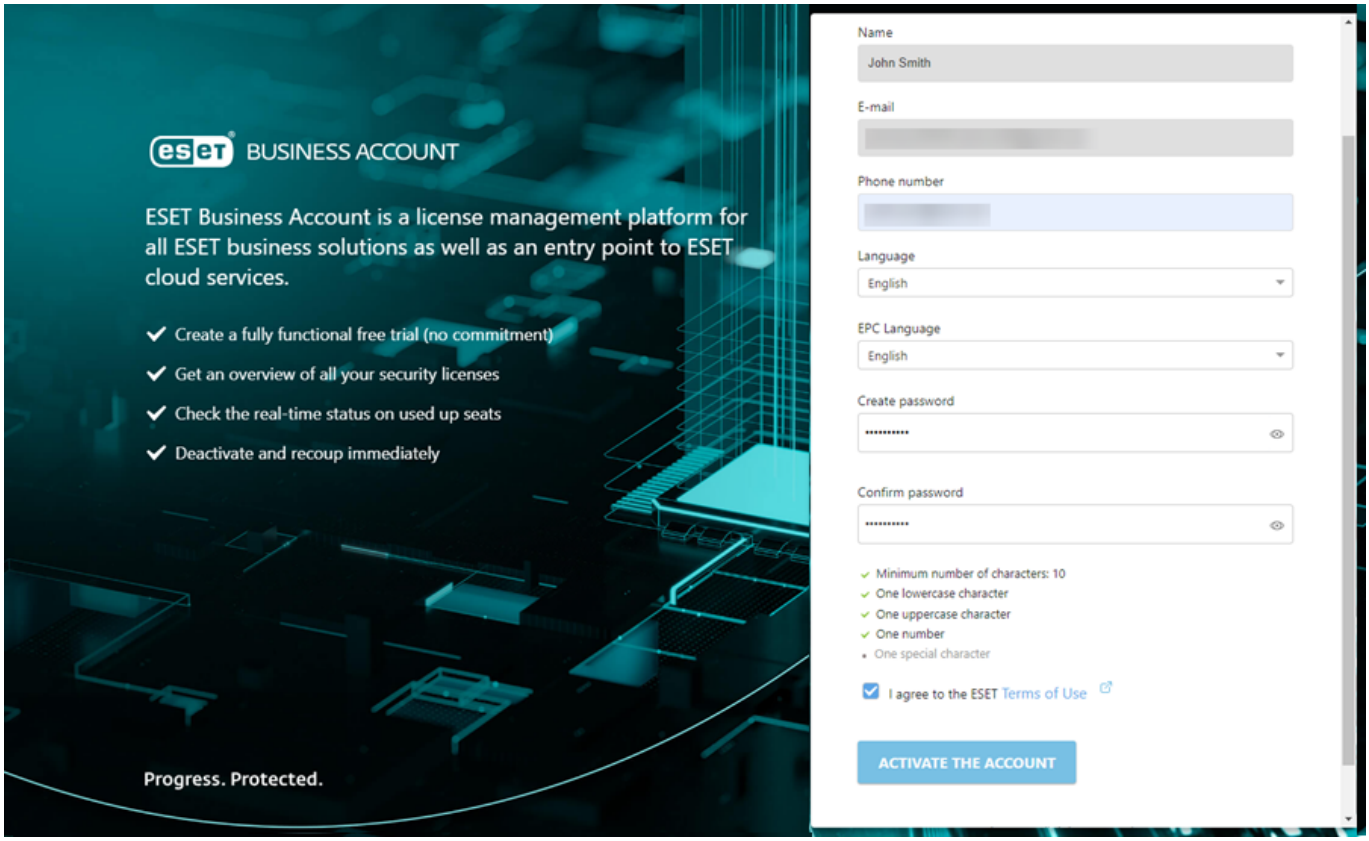
4. Nový uživatel se zobrazí v seznamu uživatelů v sekci Správa uživatelů s popiskem **Čekání na aktivaci.**



5. Uživatel obdrží aktivační e-mail (na e-mailovou adresu, kterou jste zadali při vytváření uživatele). Uživatel nyní musí kliknout na odkaz **Aktivujte svůj účet**.



6. Uživatel si nyní musí nakonfigurovat svůj učet, což spočívá v nastavení hesla (vyplnění pole **Vytvoření hesla** a **Potvrzení hesla**), dále zaškrtnutí pole **Přijímám ESET podmínky použití**. Následně klikne na tlačítko **Aktivovat účet**.



7. Namapování uživatele do ESET PROTECT Web Console

ESET PROTECT Web Console

ESET PROTECT Web Console představuje uživatelské rozhraní, prostřednictvím kterého můžete ovládat ESET PROTECT Server. Jedná se o centrální místo pro vzdálenou správu všech klientů a bezpečnostních produktů ESET. Webové rozhraní je dostupné z jakéhokoli zařízení, které má přístup k internetu, a má podporovaný internetový prohlížeč. Při prvním přihlášení do webové konzole se zobrazí Prohlídka ESET PROTECT.

Ve standardním rozložení webové konzole ESET PROTECT:

- Jméno aktuálně přihlášeného uživatele je zobrazeno v pravém horním rohu společně se zbývajícím intervalem do automatického odhlášení. **Odhlásit** se můžete kdykoli kliknutím na ikonu umístěnou vlevo od zobrazeného času zbývajícího do automatického odhlášení. Pokud nastavený čas z důvodu neaktivity vyprší, opět se přihlaste. Pro změnu uživatelského nastavení klikněte v pravém horním rohu webové konzole ESET PROTECT na jméno přihlášeného uživatele.

- Hlavní menu je neustále dostupné v levé části obrazovky, kromě případu, kdy je aktivní průvodce prvotním spuštěním. Menu si můžete v případě potřeby zmenšit kliknutím na ikonu **Sbalit menu**. Pro obnovení jeho velikosti klikněte na ikonu

- Pokud budete při práci s ESET PROTECT potřebovat nápovědu, klikněte v horní části okna na **Nápověda** > vyberte **Téma k aktuální obrazovce – Nápověda**. Zobrazí se okno nápovědy pro aktuální stránku. Kliknutím na **Nápověda** > O programu si zobrazíte verzi ESET PROTECT a další podrobnosti.

- V horní části ESET PROTECT Web Console je umístěno pole pro vyhledávání. Pro vyhledávání zadejte ve vyhledávání alespoň 3 a maximálně 30 znaků z těchto kategorií: **Název počítače**, **Popis počítače**, **IP adresa počítače**, **Název statické skupiny**, **Příčina detekce**, **Uživatelé počítače** a **Namapované účty**. V každé kategorii

najdete maximálně 3 výsledky. Kliknutím na výsledek zobrazíte podrobnosti a kliknutím na **Všechny výsledky** zobrazíte konkrétní část webové konzole s použitým filtrem kategorie.

- Pokud kliknete na **Rychlé odkazy**, zobrazíte si nabídku:

Rychlé odkazy
Nastavte svá zařízení
• Windows zařízení
• macOS zařízení
• Linux zařízení
• Mobilní zařízení
Správa zařízení
• Vytvořit klientskou úlohu
• Vytvořit novou politiku
• Přiřadit politiku
• Stáhnout politiku pro migraci
• Nastavit ochranu
Správa účtu
• Otevřít ESET Business Account
• Spravovat přístupová oprávnění
• Spravovat licence
Ostatní
• Náhled funkcí

- V levé horní části obrazovky vedle názvu ESET PROTECT najdete ikonu produktové navigace  , která vám pomůže přecházet mezi ESET PROTECT a ostatními produkty: ESET Inspect, ESET Business Account, ESET MSP Administrator, ESET Cloud Office Security (můžete zobrazit příslušné produkty na základě vaší licence a přístupových práv)

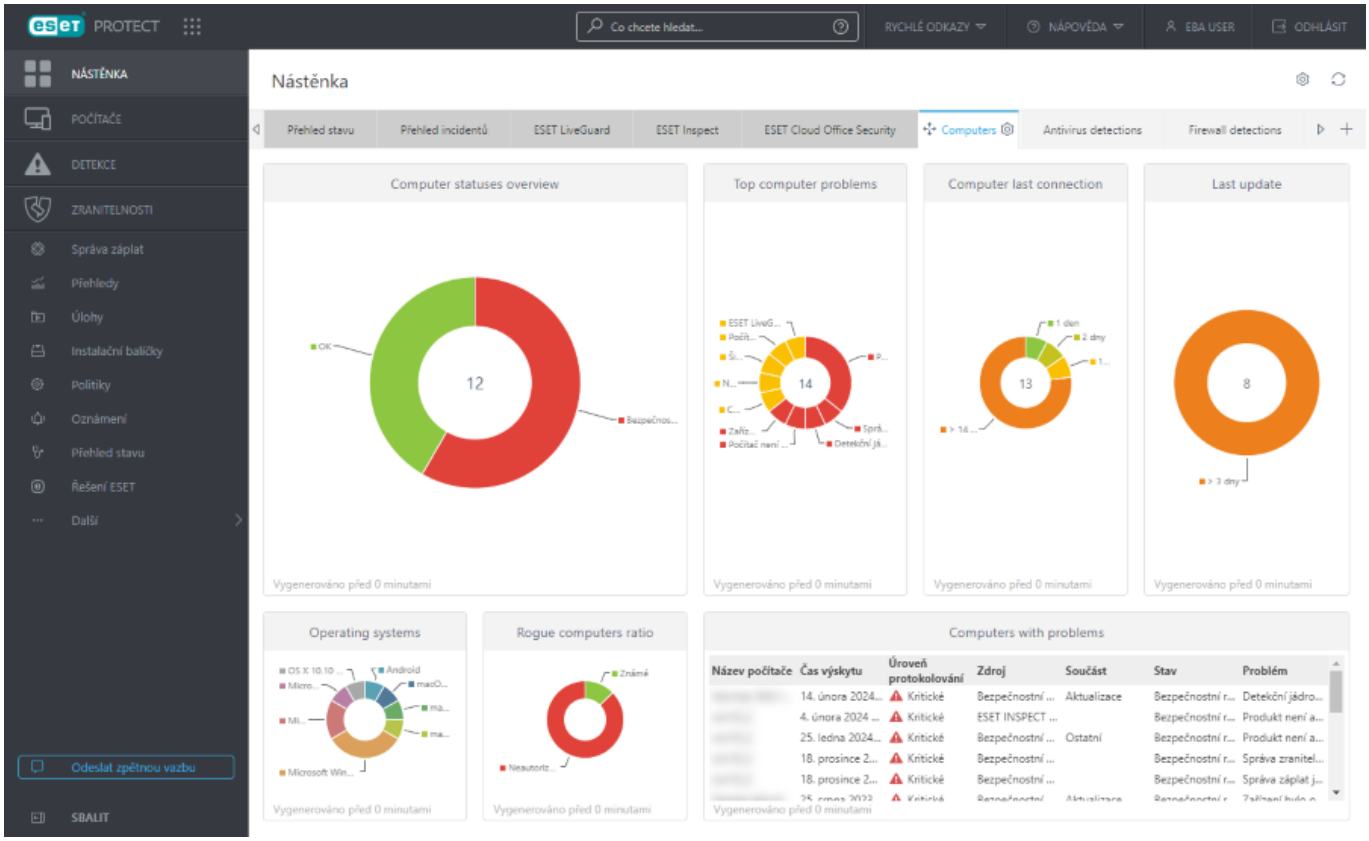
- Po kliknutí na ikonu **ozubeného kolečka** se zobrazí kontextové menu.

- Kliknutím na tlačítko **aktualizujete** zobrazená data.

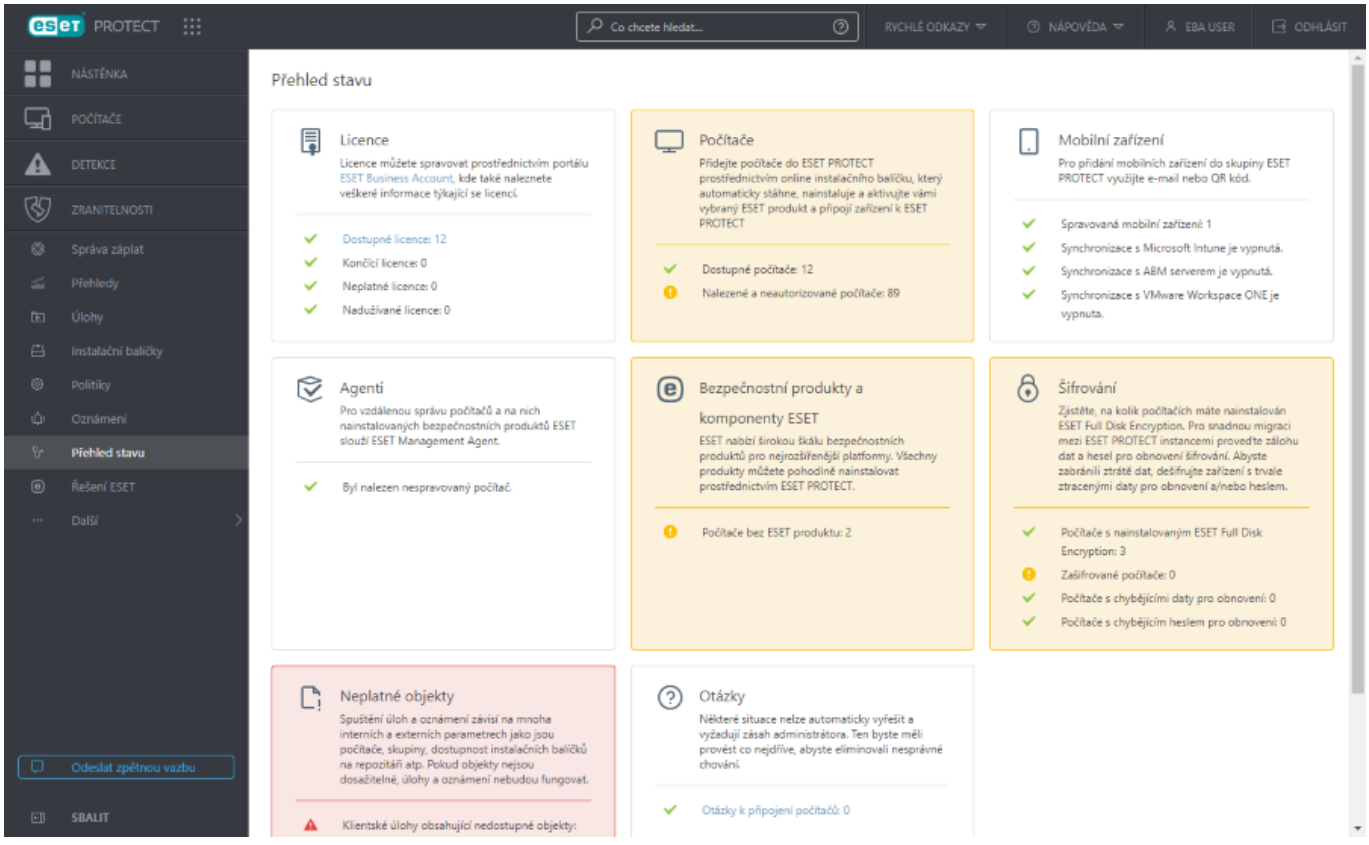
- Tlačítka v dolní části obrazovky jsou unikátní pro každou sekci a funkci. Detailně jsou popsána v jednotlivých kapitolách.

- ESET PROTECT Web Console informuje správce o aktualizaci Licenčních ujednání s koncovým uživatelem u spravovaných bezpečnostních řešení ESET nebo o neobvykle vysokém provozu u spravovaných zařízení.

- Kliknutím na logo ESET PROTECT přejděte na Nástěnku.

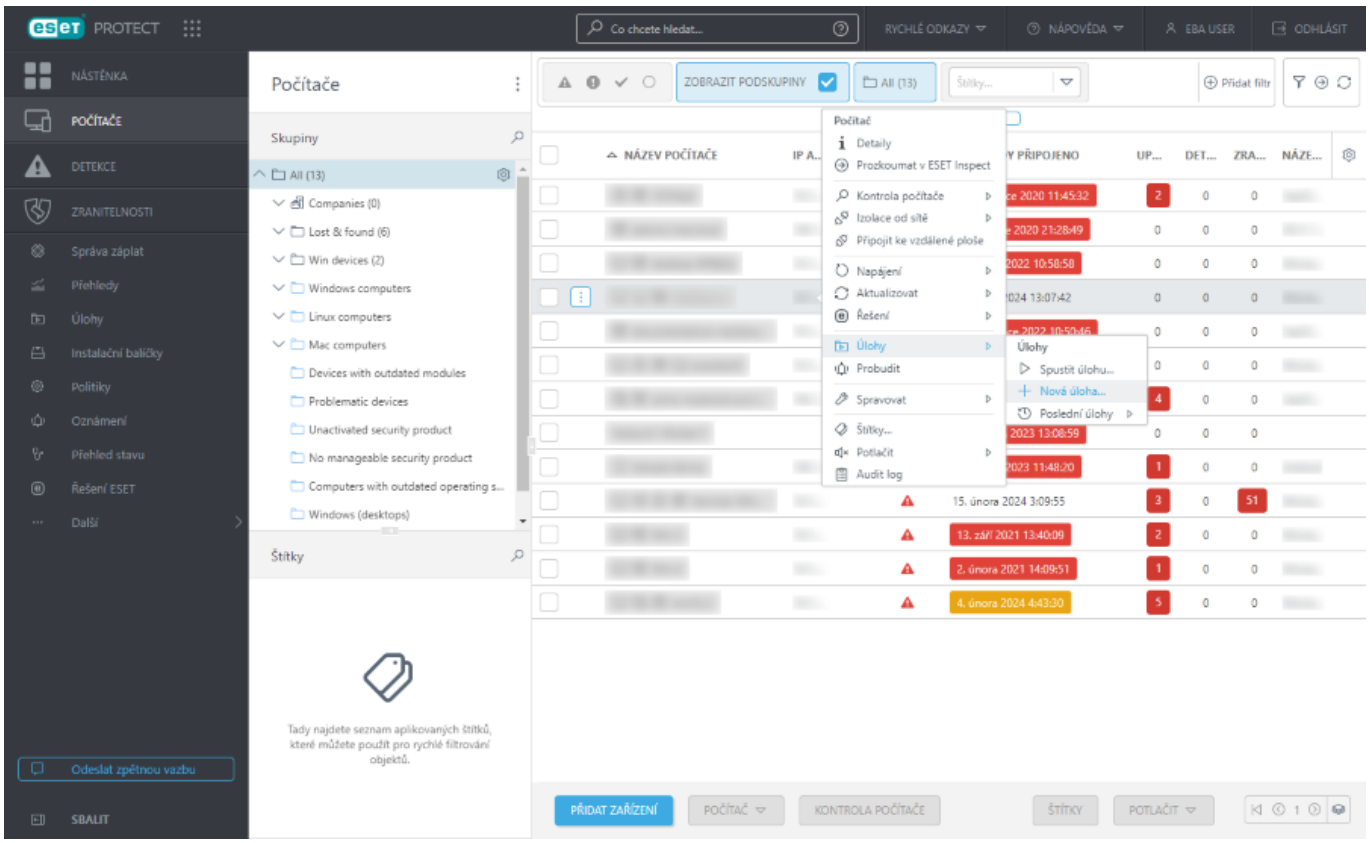


Přehledné informace o stavu ESET PROTECT a vaší infrastruktuře naleznete v hlavním menu na záložce **Stav serveru**. Zároveň tato obrazovka poslouží jako průvodce doporučenými akcemi.



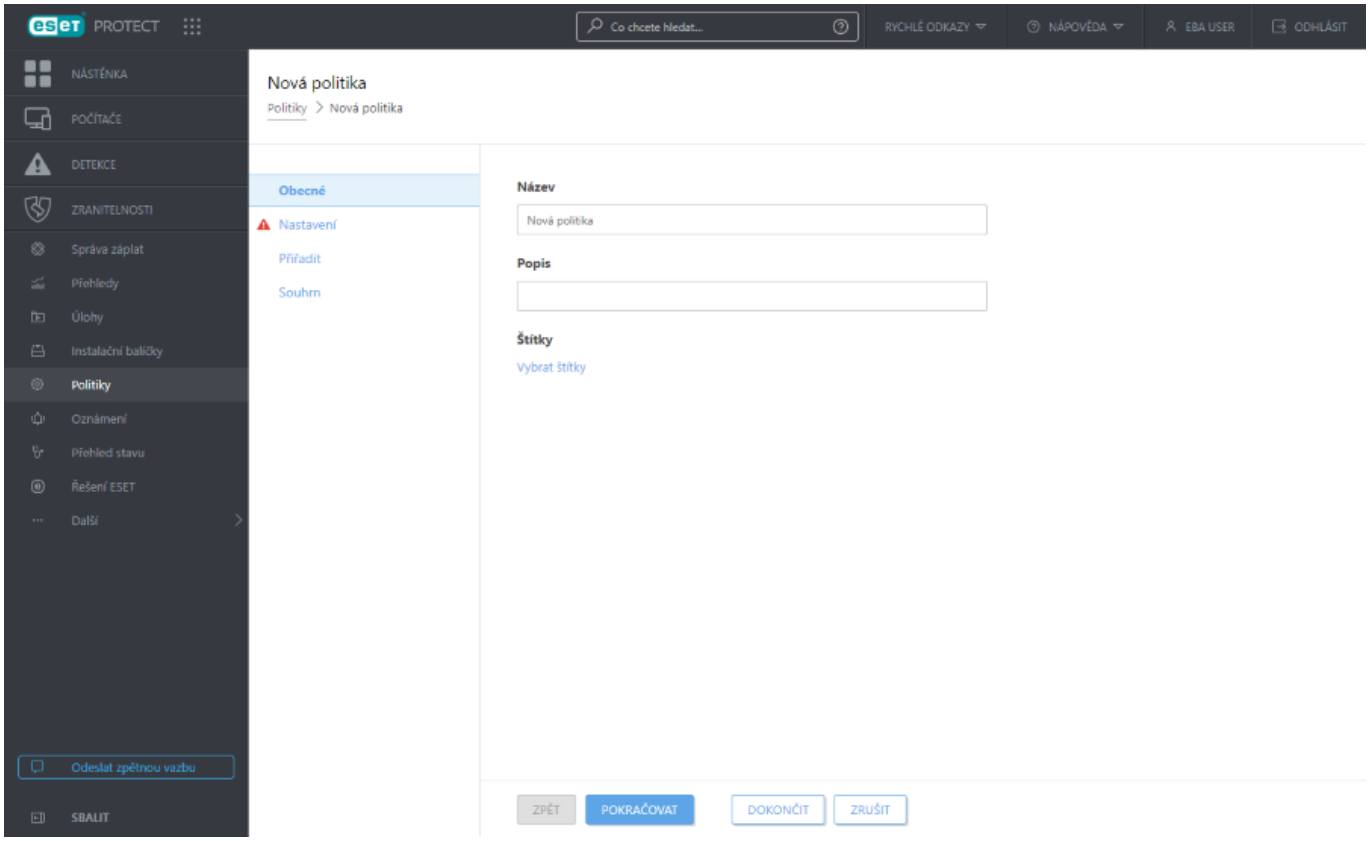
Obrazovky se stromovou strukturou mají specifické ovládací prvky. Stromová struktura je zobrazena v levé části obrazovky a související akce jsou zobrazeny ve spodní části. Po kliknutí na položku ve stromové struktuře se zobrazí podrobnější informace.

Prostřednictvím tabulek můžete spravovat jednotlivé klienty nebo celé skupiny (pokud vyberete více řádků tabulky). Po kliknutí na řádek se zobrazí kontextové menu k dané položce. Data zobrazená v tabulkách můžete filtrovat a třídit.



Objekty můžete v ESET PROTECT upravovat za pomoci průvodce. Všichni průvodci mají společné prvky:

- Jednotlivé kroky následují po sobě.
- Kdykoli se můžete vrátit na předchozí krok.
- Vyžadované nastavení je vždy označeno červeným vykřičníkem
- Na neplatné zadání budete upozorněni ve chvíli, kdy přejdete na další pole. Krok, který je chybný, označíme.
- Tlačítko **Dokončit** není dostupné, dokud nejsou všechny zadané údaje správné.



Přihlašovací obrazovka

Pro přihlášení do ESET PROTECT doporučujeme využívat účet ESET Business Account. Přímo z ESET Business Account můžete otevřít vaši ESET PROTECT instanci. Jedná se o doporučený způsob přihlášení, protože se zároveň přihlásíte do ESET Business Account i ESET PROTECT. Do ESET PROTECT se sice můžete přihlásit přímo, při použití funkcí vyžadujících aktivní přihlášení do ESET PROTECT se však můžete setkat s potížemi.

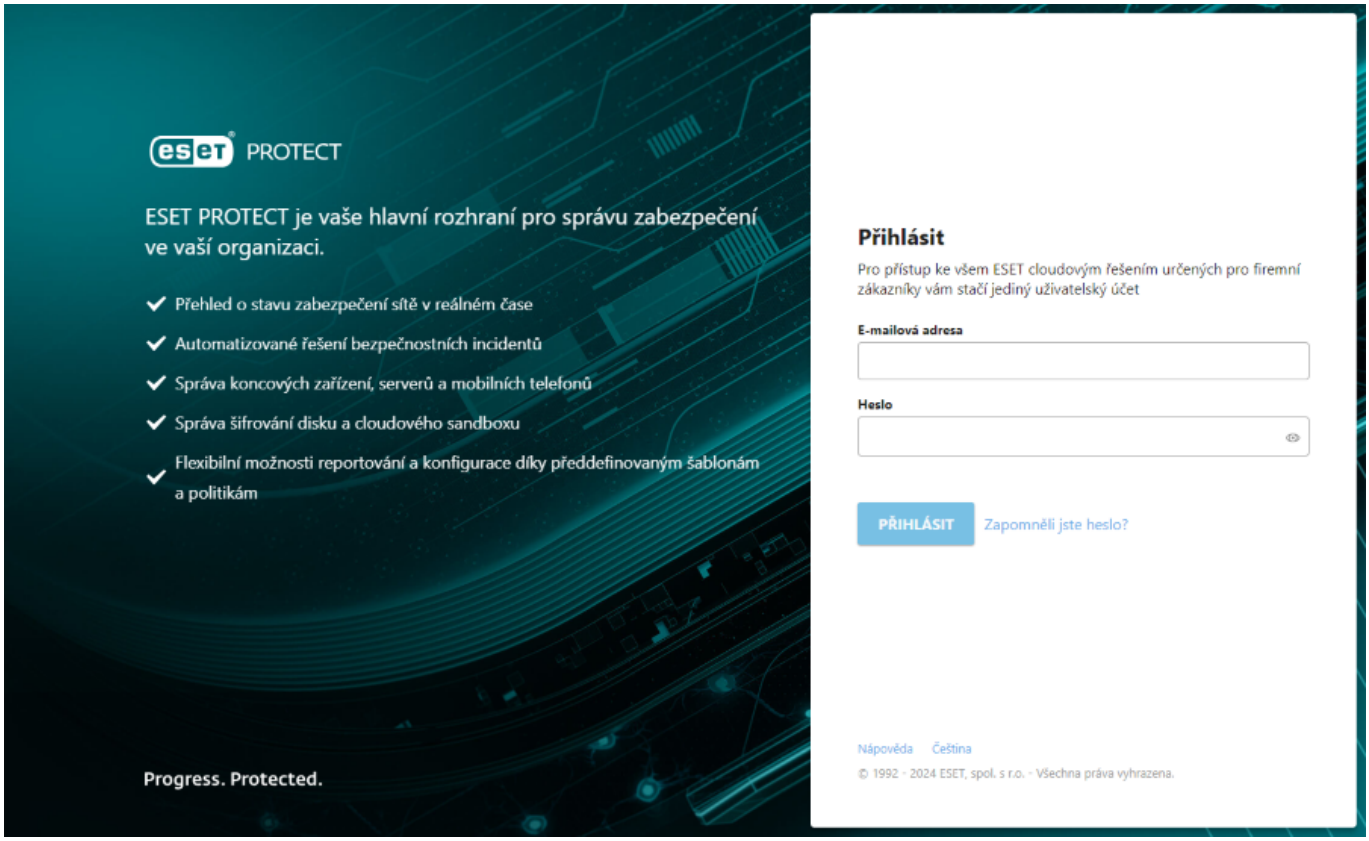
V obou případech pro přihlášení použijte přihlašovací údaje do ESET Business Account (uživatelské jméno a heslo).

> Pokud máte potíže s přihlášením nebo potřebujete zjistit význam jednotlivých hlášení, přejděte do kapitoly Web Console – řešení problémů.

Jazyk přihlašovací obrazovky a ESET PROTECT Web Console můžete změnit v nastavení svého uživatelského profilu ESET Business Account po kliknutí na své uživatelské jméno > **Předvolby** > **Jazyk**.

> Tato změna jazyka však nebude mít vliv na všechny prvky Web Console. Názvy některých objektů (výchozí nástěnky, politiky, úlohy, atp.) vytvořených v průběhu inicializace vaší instance ESET PROTECT se nezmění.

Pro obnovení zapomenutého hesla použijte funkci **Zapomněli jste heslo?**



Správa relace a bezpečnostní opatření

Zablokování IP adresy po neúspěšném přihlášení

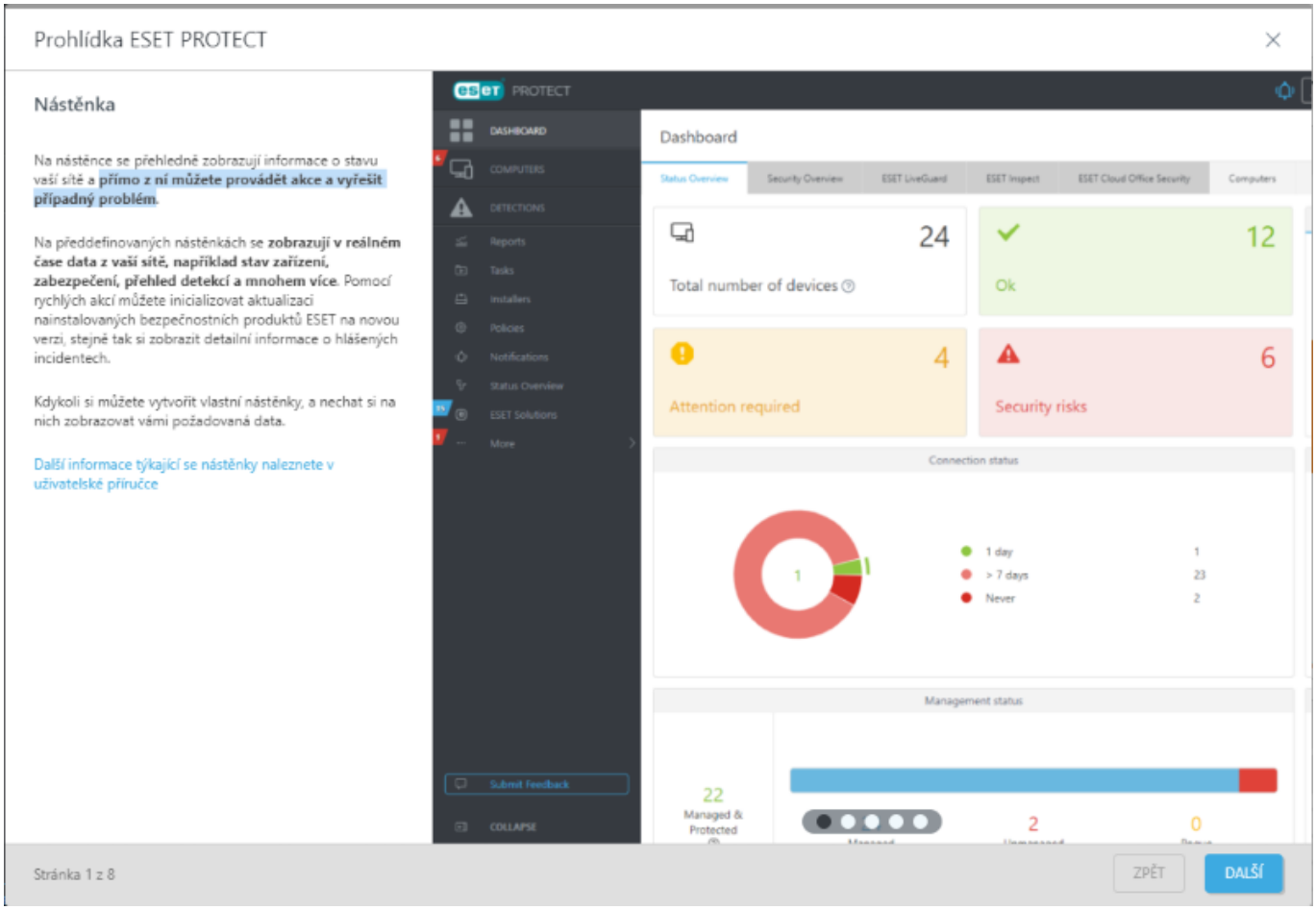
Po 10 neúspěšných pokusech o přihlášení bude IP adresa dočasně zablokována. Po uplynutí 15 minut se přihlaste platnými údaji. Toto neovlivní již existující relace.

Prohlídka ESET PROTECT

Při prvním přihlášení do Web Console se zobrazí **Prohlídka ESET PROTECT**.

Tento průvodce vás seznámí s nejdůležitějšími částmi ESET PROTECT Web Console, představí ESET Management Agenta a bezpečnostní řešení ESET. Přiblíží vám záložku Nástěnka, Počítače, Detekce, nastíní fungování úloh, politik, ukáže možnosti tvorby oznámení a představí vám funkci zajišťující automatickou aktualizace produktu.

V posledním kroku **Prohlídky ESET PROTECT** klikněte na tlačítko **Ochránit zařízení** a začněte nasazovat ESET Management agenty na počítače ve své síti. Instalační balíček agenta si můžete kdykoli vytvořit ručně (bez použití průvodce) v sekci **Instalační balíčky**, kde klikněte na tlačítko Vytvořit instalační balíček.



Prohlídku ESET PROTECT můžete kdykoli ukončit kliknutím na tlačítko **X**. Tím přejdete přímo do ESET PROTECT Web Console. Po příštím přihlášení do ESET PROTECT Web Console se **Prohlídka ESET PROTECT** již automaticky nezobrazí.

Prohlídku ESET PROTECT si můžete kdykoli zobrazit kliknutím na **Nápověda** > **Prohlídka ESET PROTECT**

Nastavit ochranu

Tento průvodce je dostupný pouze v případě, kdy k ESET PROTECT máte připojen založený účet na portále ESET Business Account.

Při prvním přihlášení do Web Console se zobrazí průvodce pro **konfiguraci ochrany** . Pomocí něj můžete snadno konfigurovat konkrétní nastavení zabezpečení globálně v celé síti – bez použití politik nebo využití dynamických skupin.

Kdykoli si jej můžete otevřít ručně:

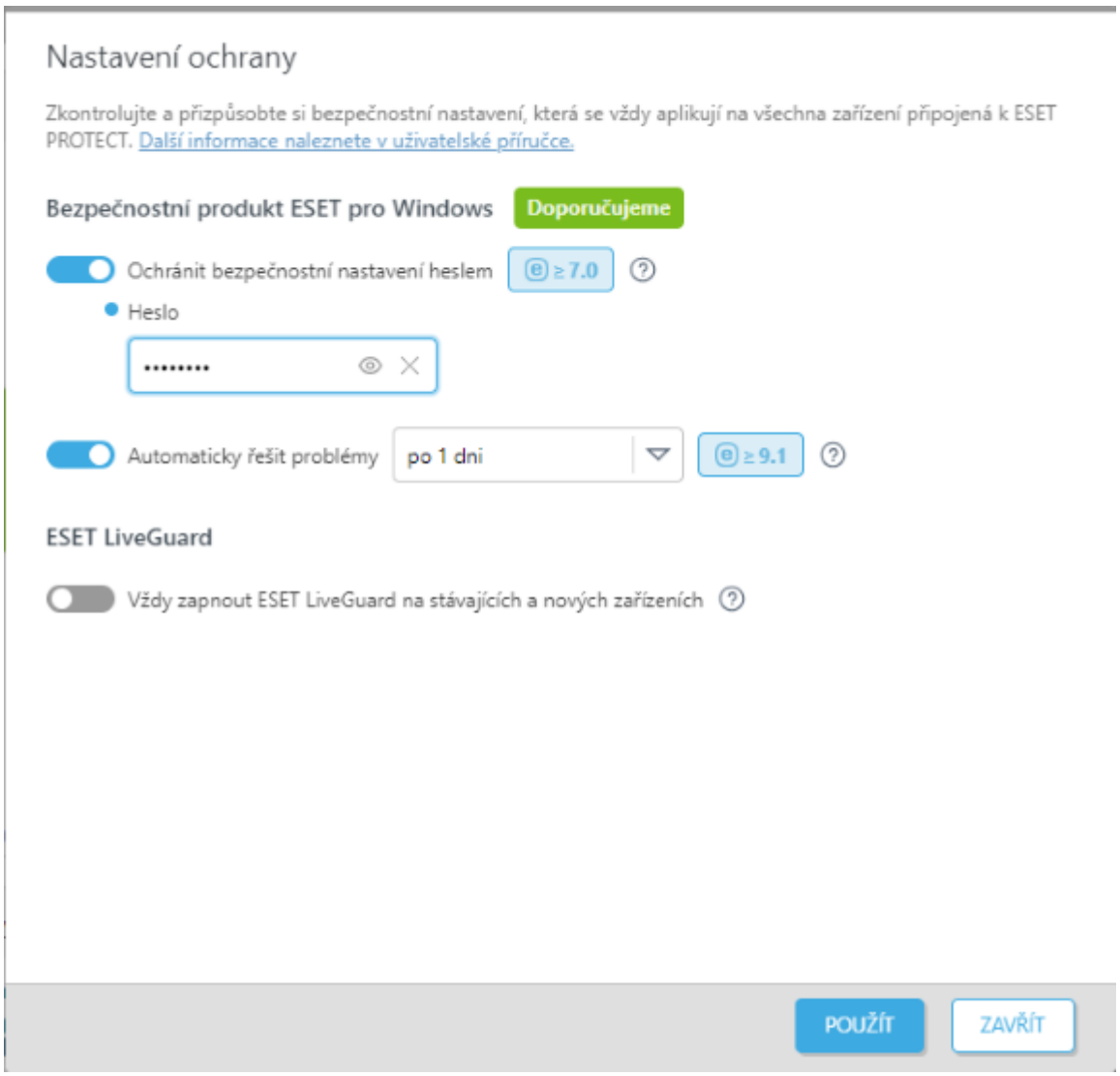
- Kliknutím na menu **Rychlé odkazy** a vyberte možnost **Nastavit ochranu**.
- V sekci **Počítače** klikněte u nejnadřazenější statické skupiny **Všechna zařízení** na ikonu ozubeného kolečka > v kontextovém menu vyberte možnost **Nastavit ochranu**.
- V sekci **Politiky** vyberte politiku s názvem **Ochrana nastavení – prostřednictvím ochrany nastavení** a klikněte na tlačítko **Nastavit ochranu**.

• V sekci **Stav serveru** klikněte na dlaždici **Komponenty a bezpečnostní produkty ESET** na tlačítko **Nastavit ochranu**.

Aby další uživatelé mohli využívat tohoto průvodce, musí mít přiřazena následující oprávnění:
• Oprávnění pro čtení ke statické skupině Všechna zařízení
• Oprávnění pro čtení politik
Aby další uživatelé mohli využívat tohoto průvodce, musí mít přiřazena následující oprávnění:
Část **Bezpečnostní produkt ESET pro Windows**:
• Oprávnění pro použití nad statickou skupinou Všechna zařízení
• Oprávnění pro zápis nad politikami
Pokud nebudete mít vyžadovaná přístupová oprávnění, uživatel nebude mít k dispozici část **Bezpečnostní produkt ESET pro Windows**.
Část **ESET LiveGuard**:
• Oprávnění pro použití nad statickou skupinou Všechna zařízení
• Oprávnění pro použití licencí
• Oprávnění pro vytvoření klientské úlohy na Aktivaci produktu
Pokud nebudete mít vyžadovaná přístupová oprávnění, uživatel nebude mít k dispozici část **ESET LiveGuard**.
Pokud nevlastníte licenci na službu ESET LiveGuard Advanced, uživatel nebude mít k dispozici část **ESET LiveGuard**.

Když vyprší platnost licence pro ESET LiveGuard Advanced, nastavení automatického nasazení se uloží, ale nezobrazí se. Po obnovení licence se vaše nastavení znovu zapne a zobrazí.

Průvodce vás vyzve ke zvýšení úrovně zabezpečení zařízení připojených k ESET PROTECT.



Bezpečnostní produkt ESET pro Windows

1. Pomocí možnosti **Ochránit bezpečnostní nastavení heslem** nastavíte na spravovaných zařízeních heslo, které bude bránit uživatelům (kteří jej neznají) měnit nastavení produktu.

Toto nastavení podporují následující produkty:
- Produkty z řady ESET Endpoint pro Windows od verze 7.0
- ESET Server Security for Microsoft Windows Server, ESET File Security for Microsoft Windows Server
- ESET Mail Security for Microsoft Exchange Server
- ESET Mail Security for IBM Domino
- ESET Security for Microsoft SharePoint Server

2. Do pole **Heslo** zadejte heslo skládající se minimálně z 8 znaků.

Heslo, které vytvoříte, se vždy automaticky aplikuje na všechna připojená zařízení. Heslo si zapamatujte. Pokud heslo zapomenete, můžete jej kdykoli přepsat nově definovaným v ESET PROTECT, nicméně předchozí heslo již nezískáte zpět.

3. Pomocí možnosti **Automatické řešení problémů** povolíte automatické restartování spravovaného zařízení, pokud je vyžadováno pro dokončení aktualizace bezpečnostního produktu ESET.

K restartování dojde automaticky, pokud administrátor nebo uživatel dané zařízení nerestartuje v definovaném

intervalu.

Toto nastavení podporují produkty z řady ESET Endpoint pro Windows od verze 9.1. Není dostupné v produktech určených pro ochranu serverů.

4. Vyberte interval, ve kterém chcete počítač automaticky restartovat:
   - Nelze odložit
   - Za 1 až 5 hodin
   - Za 1 až 30 dní

ESET LiveGuard

5. Pomocí možnosti **Vždy zapnout ESET LiveGuard na nových zařízeních** zajistíte, že se ESET LiveGuard Advanced automaticky zapne na nově připojených zařízeních, na kterých je nainstalovaný kompatibilní bezpečnostní produkt ESET.

Doporučujeme zvolit možnost **Optimální ochrana**, abyste přiřadili nové politiky s optimální ochranou. Výběr můžete změnit také v **ESET LiveGuard Advanced** v sekci Řešení ESET.

6. Pro aplikovaní bezpečnostního nastavení klikněte na tlačítko **Použít nyní**.

Nastavení můžete zkontrolovat v sekci **Politiky**, kdy si otevřete politiku s názvem **Ochrana nastavení – prostřednictvím ochrany nastavení**. Tyto politiky není možné měnit ani odstranit, můžete však měnit jejich přiřazení (standardně se aplikují na nejnadřazenější statickou skupinu **Všechna zařízení**).

Vypnutí nastavení

Jednotlivá nastavení můžete vypnout pomocí přepínače .

Po vypnutí možnosti **Ochránit bezpečnostní nastavení heslem** se pro ochranu nastavení na připojených zařízeních použije heslo definované v ostatních politikách. V případě, že heslo není definováno, nebude při změně nastavení těchto zařízeních nadále vyžadováno.

Uživatelské nastavení

V této části můžete konfigurovat osobní uživatelské nastavení. K nastavení **uživatelského účtu** se dostanete po kliknutí na jméno účtu v pravém horním rohu webové konzole ESET PROTECT (vedle tlačítka **Odhlásit**). Do webové konzole ESET PROTECT můžete být přihlášeni z různých webových prohlížečů, počítačů nebo mobilních zařízení současně. Naleznete zde rovněž informace o tom, z kolika zařízení jste přihlášeni.

Provedené nastavení se týká výhradně aktuálně přihlášeného uživatele.

Nastavení motivu

V této části si můžete vybrat motiv, ve kterém chcete ESET PROTECT používat:

- **Světlý (výchozí)**
- **Tmavý**
- **Barevný motiv systému** – barevný motiv webové konzole odpovídá barevnému motivu operačního systému.

Z rozbalovacího menu si vyberte motiv, který chcete použít:

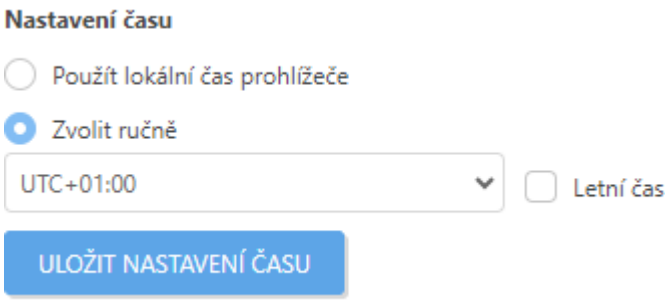
Vybraný motiv zůstane aktivní po odhlášení a opětovném přihlášení do Web Console.

Nastavení času

Každý uživatel webové konzole ESET PROTECT může mít nastaveno vlastní časové pásmo. Specifické nastavení časového pásma se použije pro každého uživatele bez ohledu na to, odkud přistupuje k webové konzole ESET PROTECT.

ESET PROTECT ukládá veškerá data v koordinovaném světovém čase, tedy v UTC (Coordinated Universal Time). UTC čas je automaticky převeden do časového pásma, ve kterém používáte webovou konzoli ESET PROTECT (v potaz se bere střídání času). Webová konzole ESET PROTECT údaje zobrazí v lokálním čase, ve kterém webová konzole ESET PROTECT běží (nikoli v UTC). Nastavení zobrazení času v webové konzoli ESET PROTECT můžete kdykoli přepsat ve svém uživatelském účtu.

Pokud nechcete zobrazovat čas v lokálním čase, odškrtněte možnost **Použít lokální čas prohlížeče** a **vyberte si časové pásmo ručně**. Dále se rozhodněte, zda se má zohledňovat posun způsobený letním časem.

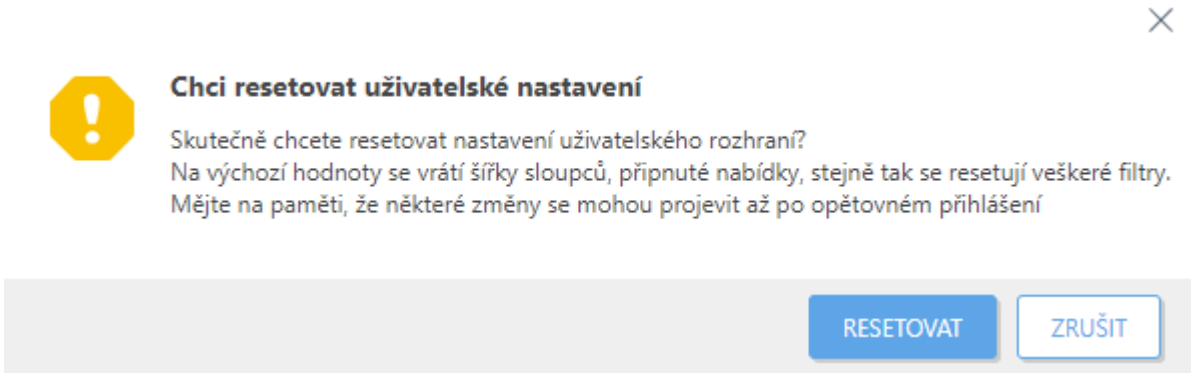


V některých částech webové konzole můžete narazit na možnost použití jiného časového pásma. Při vytváření podmínky spuštění se automaticky použije časové pásmo z ESET PROTECT Web Console. Volitelně můžete vybrat možnost **Použít lokální čas cíle**, čímž zajistíte, že se k provedení úlohy použije čas na cílovém zařízení, místo časového pásma, ve kterém je ESET PROTECT Web Console.

Změny týkající se času uložíte pomocí tlačítka **Uložit nastavení času**.

Uložený stav uživatele

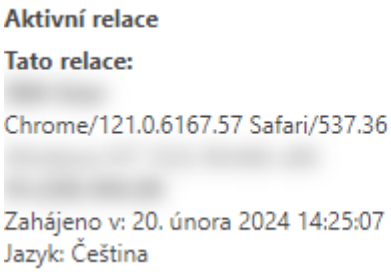
Pokud chcete obnovit uživatelské rozhraní na výchozí hodnoty (nastavení sloupců, zapamatované filtry, připnuté nabídky atp.), použijte možnost **Obnovit uložený stav uživatele**. To zahrnuje Prohlídku ESET PROTECT, velikost sloupců tabulky, zapamatované filtry, zvýrazněná menu aj.



Aktivní relace

V této části naleznete informace o aktivních relacích (kolikrát je uživatel přihlášen). K dispozici jsou tato data:

- Uživatelské jméno aktuálně přihlášeného uživatele.
- Podrobnosti o počítači, ze kterého je přistupováno k Web Console – webový prohlížeč a operační systém.
- IP adresa zařízení, ze kterého je uživatel k webové konzoli ESET PROTECT připojen.
- Datum a čas přihlášení.
- Jazyk zvolený pro webovou konzoli ESET PROTECT.



Aktuální relace je označena štítkem **Tato relace**.

Přizpůsobení filtrů a rozložení

Webová konzole ESET PROTECT umožňuje několika způsoby přizpůsobit rozložení zobrazených položek v hlavních sekcích (např. **Počítače, Úlohy** atd.):

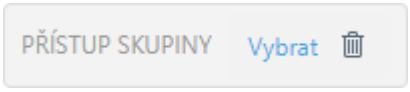
Správa filtrů

Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte

hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře.

Filtry si můžete uložit do svého uživatelského profilu pro budoucí použití. Kliknutím na ikonu **Předvolby** můžete spravovat uložené sady filtrů:

Sady filtrů	Seznam vámi uložených filtrů, které jedním kliknutím aplikujete. Aktuálně použitý filtr má u sebe příznak ✔. Vybráním možnosti **Zahrnout viditelné sloupce, řazení a stránkování** se uloží také tyto parametry.
Uložit sadu filtrů jako	Kliknutím si uložíte aktuální sadu filtrů jako novou předvolbu. Po uložení předvolby již nemůžete měnit konfiguraci filtrů.
Správa sad filtrů	Pomocí této možnosti můžete přejmenovat nebo odebrat existující sady filtrů. Změny se projeví po kliknutí na tlačítko **Uložit**.
Vymazat hodnoty filtru	Kliknutím vynulujete filtry na výchozí hodnoty. Uložená předvolba zůstane beze změny.
Odstranit filtry	Kliknutím odstraníte použité filtry. Uložená předvolba zůstane beze změny.
Odstranit nepoužité filtry	Kliknutím odstraníte filtry, ve kterých nemáte zadanou žádnou hodnotu.
Obnovit výchozí filtry	Pomocí této možností resetujete panel s filtry do výchozího nastavení.

Prostřednictvím filtru 

Přístup skupiny si můžete vybrat konkrétní statickou skupinu a zjistit, jaké objekty vidí uživatelé, kteří jsou členem dané skupiny.

Pro filtrování zobrazených objektů můžete využít štítky.

Rozložení postranního panelu

Pro zobrazení kontextového menu pro přizpůsobení postranního panelu klikněte na ikonu ⋮ na řádku s názvem sekce (dostupné možnosti se liší v závislosti na aktuálním rozložení).

- **Skrýt postranní panel**
- **Zobrazit postranní panel**
- **Skupiny**
- **Skupiny a štítky**
- **Štítky**

Pokud jsou skupiny viditelné, můžete vybrat použít jednu z níže uvedených možností:

- **Rozbalit vše**
- **Sbalit vše**

Správa hlavní tabulky

Pro změnu pořadí sloupců najeďte myší nad ikonu vedle názvu sloupce a pomocí technicky drag & drop jej přesuňte. Další možnosti naleznete v této kapitole v části **Úprava sloupců**.

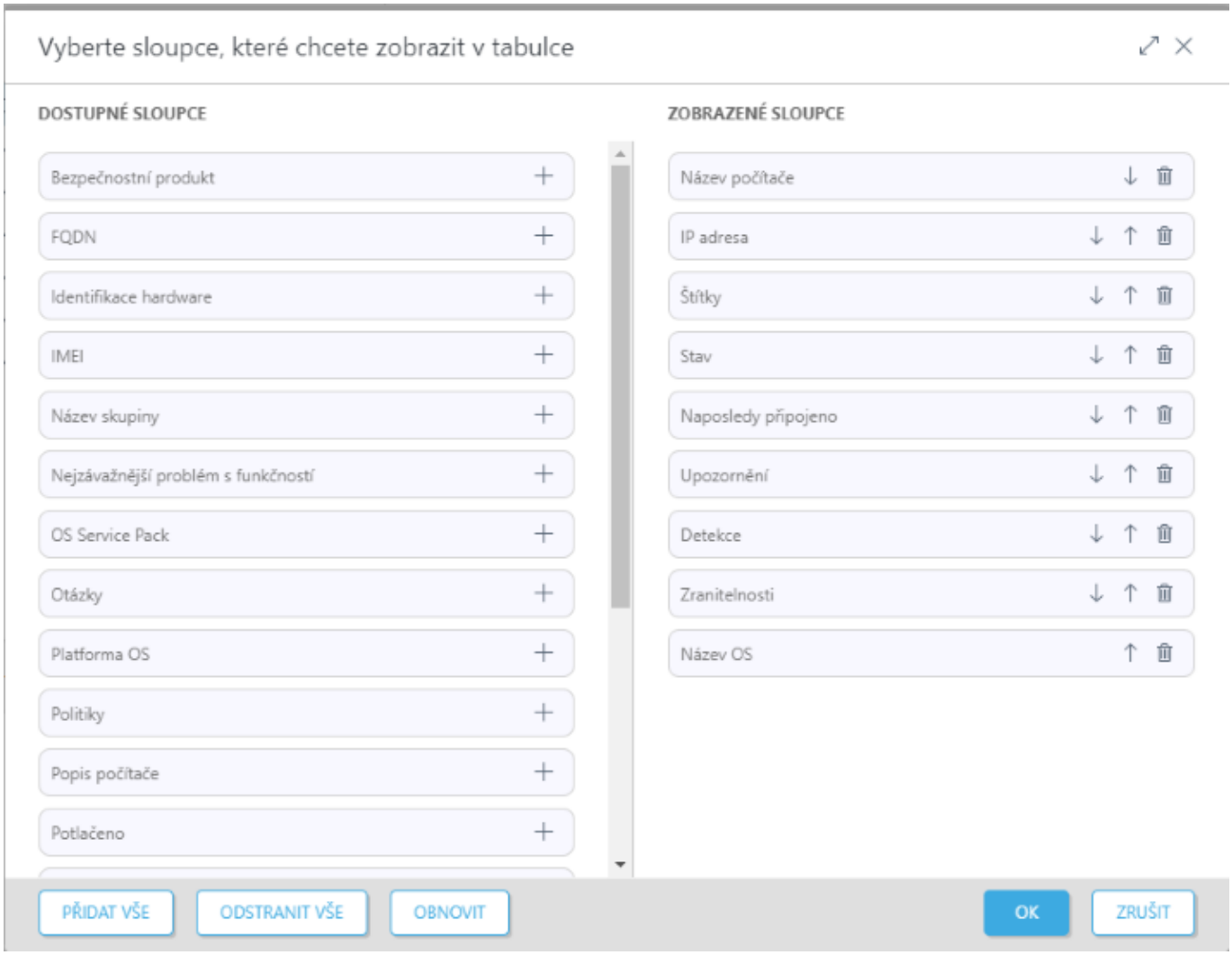
Pro seřazení dat podle jednoho sloupce klikněte do jeho záhlaví.

- Jedním nebo dvěma kliknutími seřadíte data v tabulce vzestupně (A–Z, 0–9) nebo sestupně (Z–A, 9–0).
- Po aplikování řazení se v záhlaví sloupce, dle kterého se data řadí, zobrazí malí šipka.
- Využít můžete rovněž pokročilé řazení.

Pro správu hlavní tabulky použijte ikonu ozubeného kolečka v jejím pravém horním rohu:

Akce

- **Upravit sloupce** –Pomocí této možnosti můžete přidat, odebrat a změnit pořadí zobrazených sloupců. Při správě sloupců můžete využít techniku drag and drop. Kliknutím na **Obnovit** obnovíte sloupce tabulky do výchozího stavu (výchozí dostupné sloupce ve výchozím pořadí).



- **Automaticky přizpůsobit** – pomocí této možnosti se šířka sloupců přizpůsobí velikosti okna.
- **Zobrazit relativní čas/Zobrazit absolutní čas** – vyberte si formát, ve kterém chcete zobrazovat časové

údaje v hlavní tabulce (například **Naposledy připojeno** v sekci **Počítače** nebo **Výskyt** v seznamu **Detekcí**). Pokud aktivní **zobrazení relativního času**, pro zobrazení absolutního stačí najet kurzorem myši nad relativní čas.

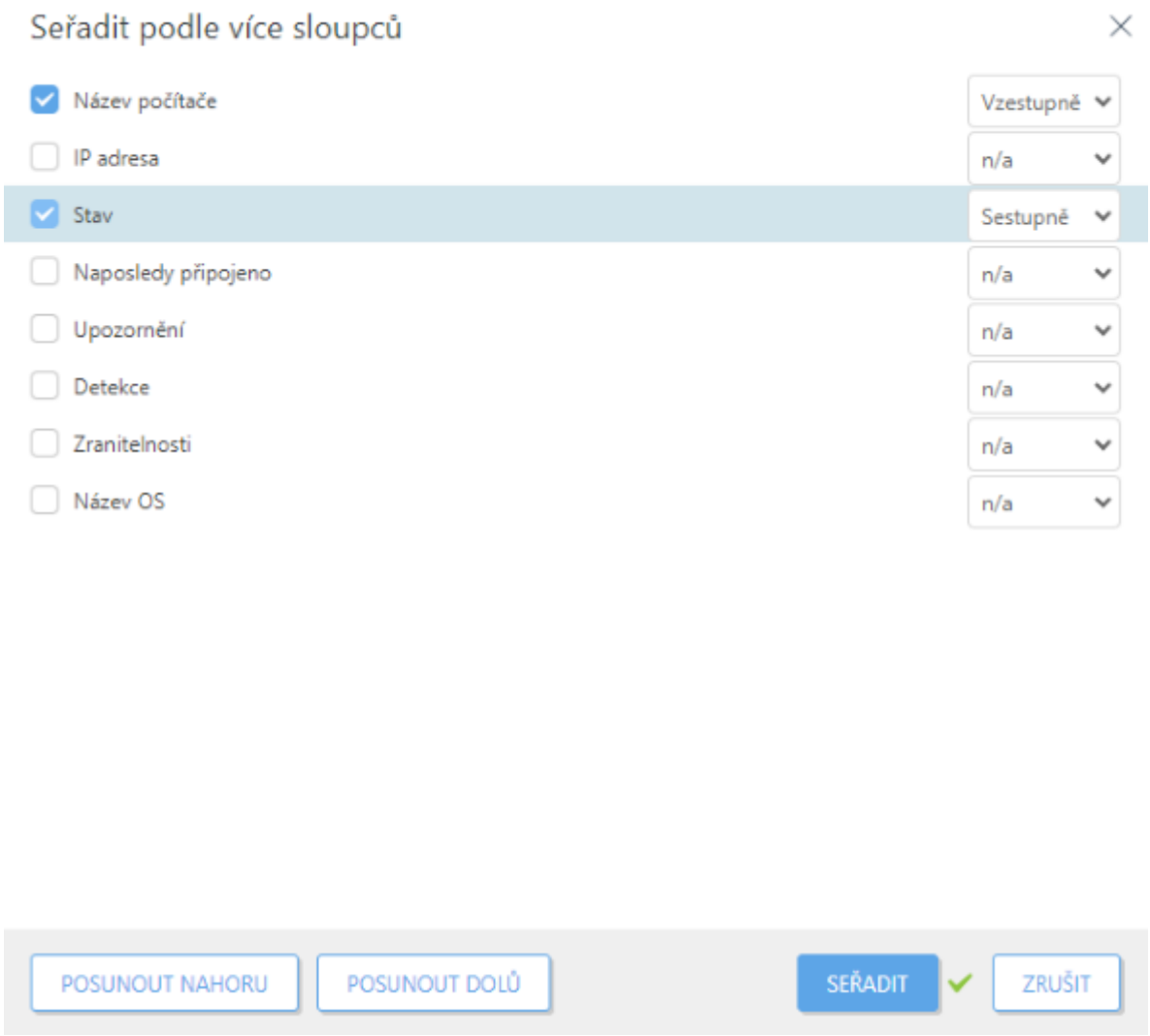
Řazení tabulky

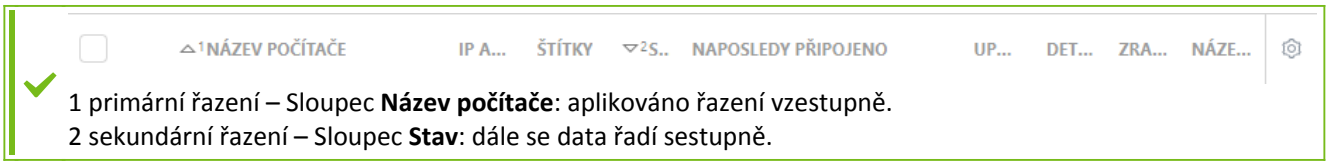
• **Zrušit řazení** – kliknutím resetujete řazení dat dle sloupců.

• **Pokročilé řazení** – data v tabulce můžete řadit podle více (až 4) sloupců. U každého sloupce můžete definovat:

oprioritu řazení – změnu pořadí sloupců provedete kliknutím na tlačítko **Přesunout nahoru** nebo **Přesunout dolů** (první sloupec: primární řazení; druhý sloupec?: sekundární řazení; atd.). Po aplikování pokročilého řazení se v záhlaví sloupců zobrazí čísla indexů, která reprezentují prioritu řazení.

ochování řazení – pomocí rozbalovacího menu se rozhodněte, zda chcete data řadit **Vzestupně** nebo **Sestupně**.





1 primární řazení – Sloupec **Název počítače**: aplikováno řazení vzestupně.
2 sekundární řazení – Sloupec **Stav**: dále se data řadí sestupně.

Přehledy

- **Exportovat tabulku jako** – pomocí této možnosti si můžete exportovat obsah tabulky do vámi požadovaného formátu. Vybrat si můžete formát *.pdf* nebo *.csv*. CSV je vhodný formát pouze pro tabulková data a jako oddělovač je použit středník ;. Pokud si stáhnete přehled ve formátu CSV a ve sloupci, ve kterém očekáváte text, jsou uvedena čísla, pro korektní zobrazení dat si stáhněte přehled ve formátu PDF.

- **Uložit šablonu přehledu** – kliknutím vytvoříte na základě zobrazených dat novou šablonu přehledu.

Štítky

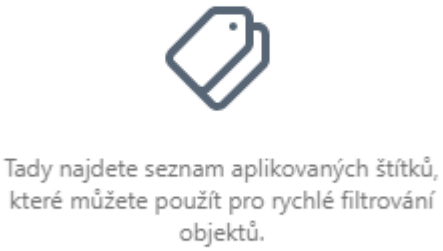
V ESET PROTECT si můžete označit související objekty (počítače, detekce, úlohy, instalační balíčky, politiky, oznámení, licence, …) uživatelskými štítky a používat je následně při filtrování a vyhledávání. Štítky jsou nativně dostupné na všech hlavních obrazovkách webové konzole ESET PROTECT.

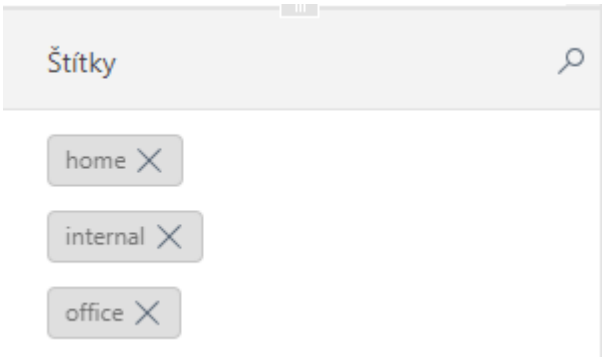
Štítek si představte jako uživatelem definované klíčové slovo (nálepku), které můžete přidat rozdílným objektům, abyste je později snáze nalezli. Příklad: Štítek "VIP" můžete přiřadit všem objektům, které souvisí se skupinou důležitých zaměstnanců.

Štítky si můžete vytvořit ručně, a stejně tak je přiřazovat. Výjimky tvoří MSP objekty, kterým jsou automaticky přiřazovány štítky s názvem zákazníka.

Panel štítky

Existující štítky můžete zobrazit v sekci **Štítky**, kterou najdete v levé dolní části nabídky webové konzole ESET PROTECT:





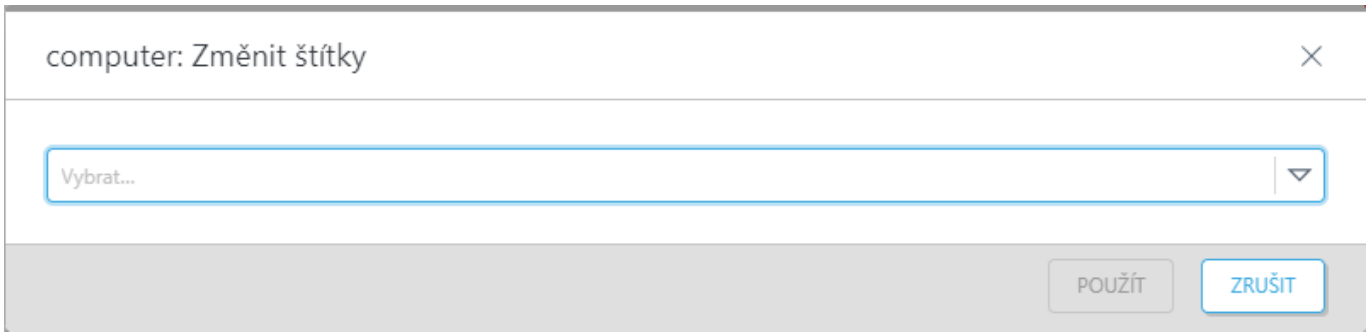
Oprávnění pro správu štítků

Aby mohl uživatel spravovat štítky daného objektu, musí mít oprávnění pro **použití** daného objektu. Mějte na paměti, že štítky mohou spravovat všichni uživatelé. Může se stát, že vámi vytvořený štítek smaže jiný uživatel.

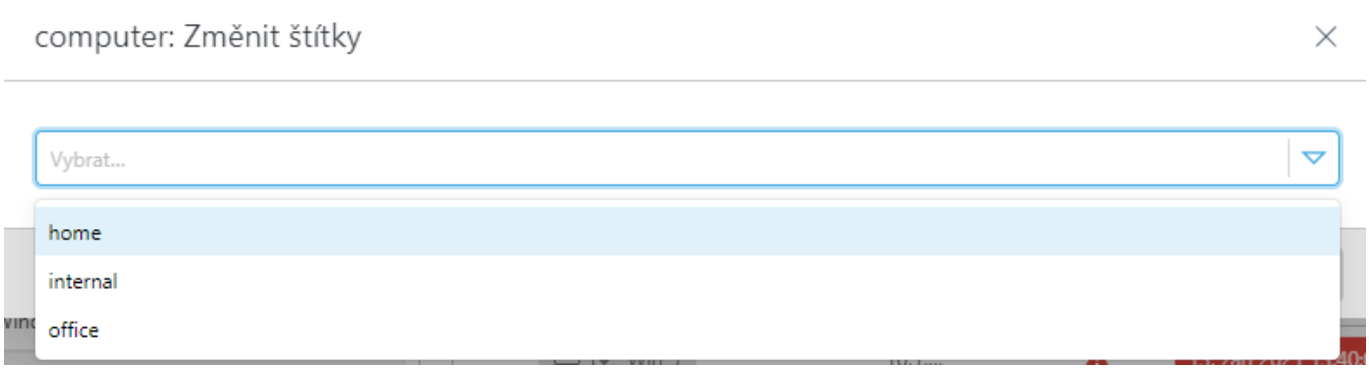
Přiřazení štítků

Každý štítek můžete přiřadit více objektům.

Pro přiřazení štítku objektu na něj klikněte a z kontextového menu vyberte možnost **Štítky**:

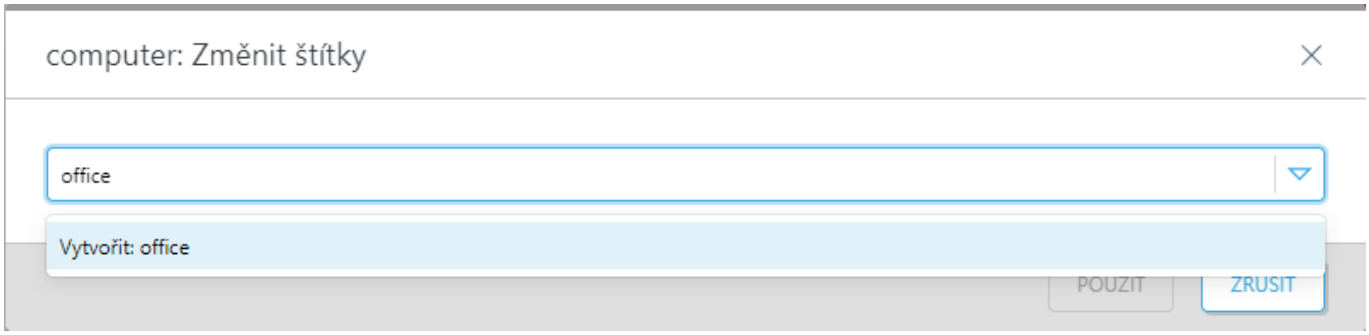


Pro přiřazení existujícího štítku klikněte do zobrazeného pole, vyberte požadovaný štítek ze seznamu a klikněte na tlačítko **Použít**.



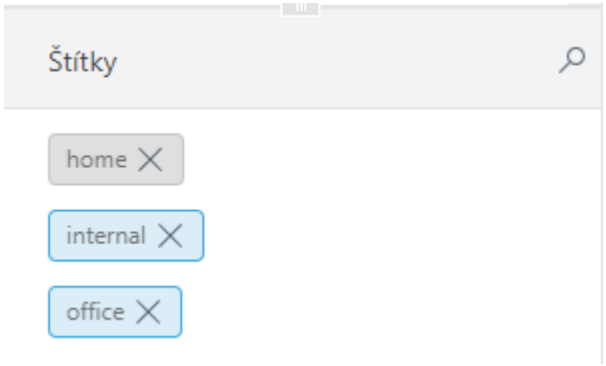
Vytvořit nového štítku

Pro vytvoření nového štítku zadejte do zobrazeného pole jeho název, klikněte na možnost **Vytvořit "vámi zadaný název štítku"** a akci potvrďte kliknutím na tlačítko **Použít**. Název existujícího štítku nelze upravit.



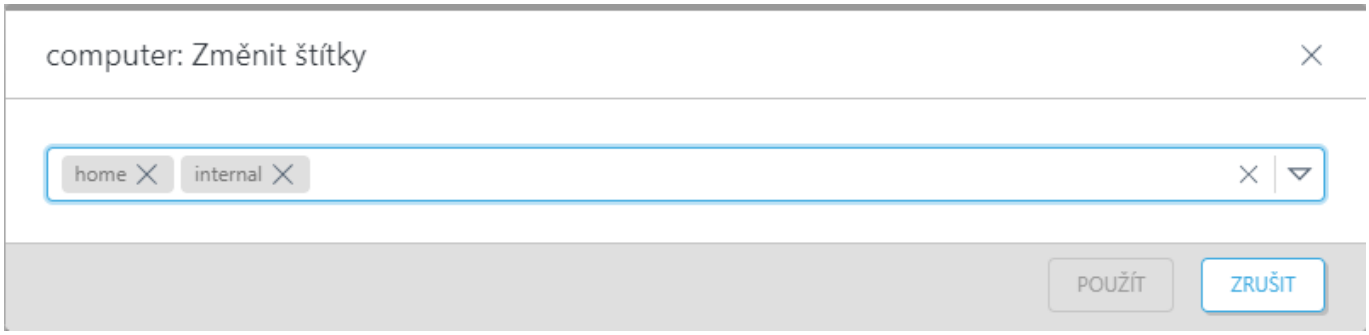
Filtrování objektů podle štítků

Pro aplikování štítku na aktuálně zobrazený seznam objektů na něj jednoduše klikněte. Vybraný štítek se podbarví modře.



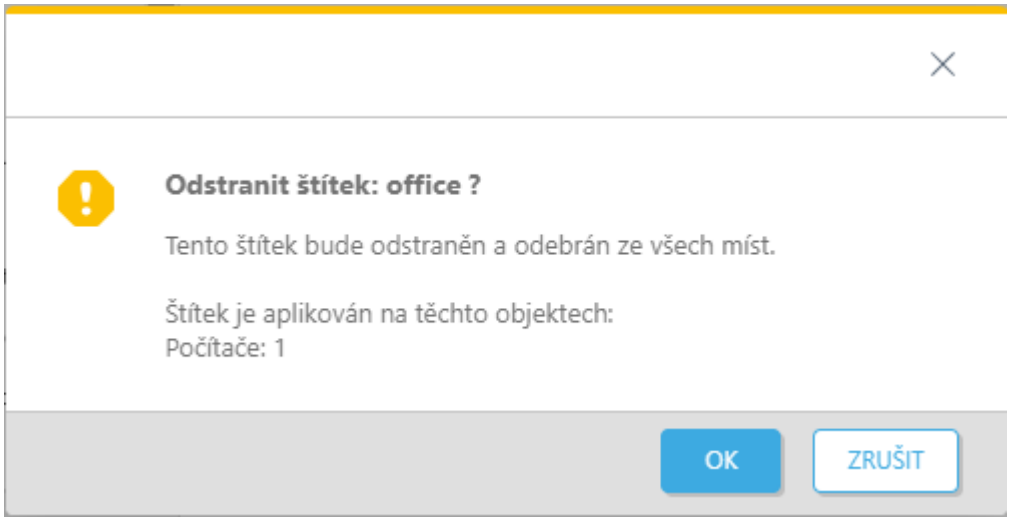
Odřazení štítku

Pro odebrání štítku od objektu na něj klikněte a z kontextového menu vyberte možnost **Štítky**: Štítek objektu odeberte pomocí ikonky X a potvrzením **Použít**.



Odstranění štítku

Pro smazání štítku na něj na panelu **Štítky** najeďte myší a klikněte na ikonu . Potvrďte kliknutím na **OK**, že chcete štítek odebrat ze všech objektů ve webové konzoli ESET PROTECT.



Importování CSV

Velké množství dat můžete do konzole importovat prostřednictvím *.csv* souboru. Tato možnost je dostupná ve vybraných částech ESET PROTECT. Sloupce se v jednotlivých částech konzole mění, v závislosti na importovaných datech.

1.Klikněte na tlačítko **Importovat CSV**.

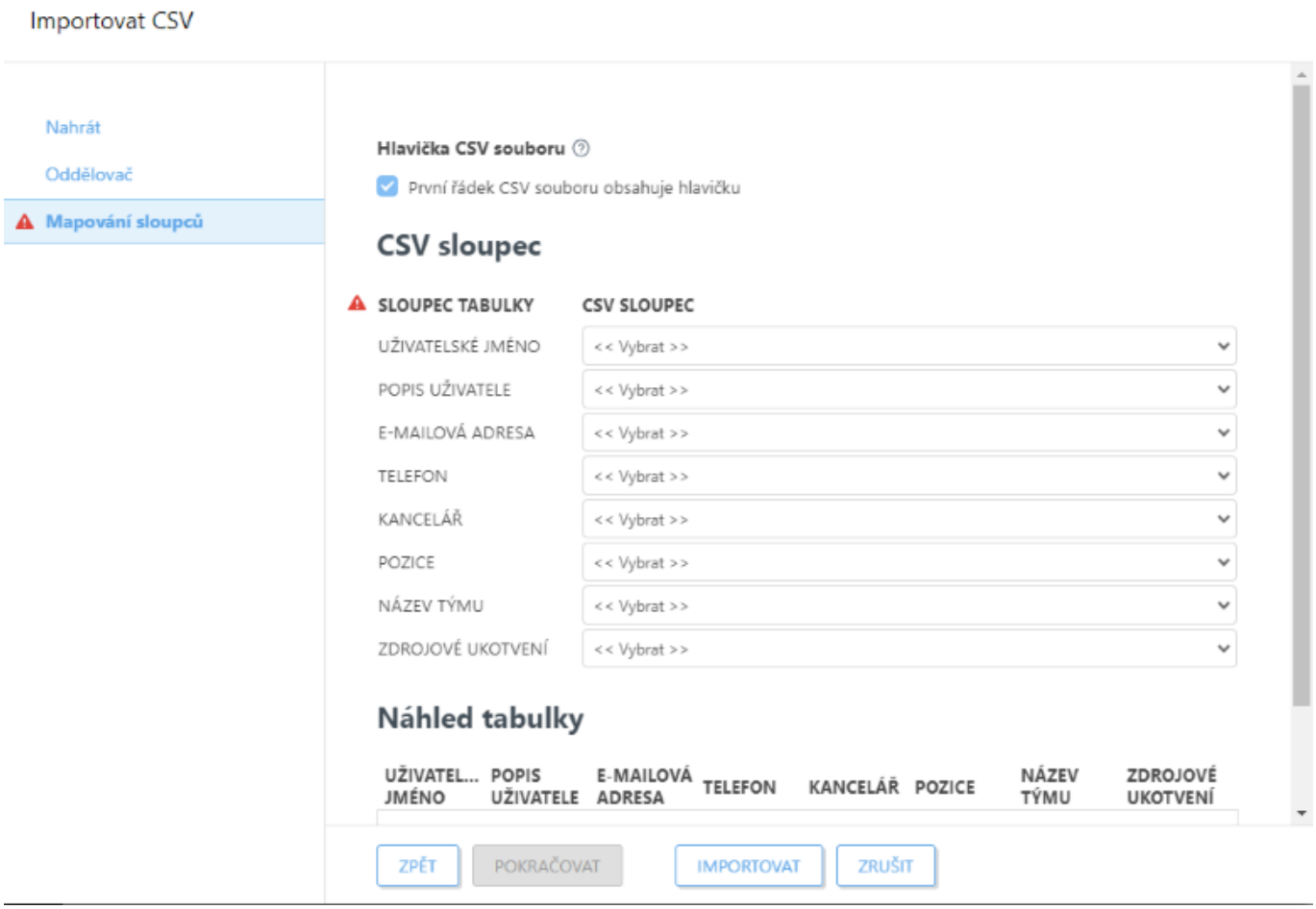
2.**Nahrát** – klikněte na **Vybrat soubor**, vyhledejte *.csv* soubor (s kódováním UTF-8), který chcete nahrát, a klikněte na **Nahrát**.

3.**Oddělovač** – v této části definujte znak, kterým jsou data oddělena. Z rozbalovacího menu můžete vybrat nejpoužívanější oddělovač (**středník**, **čárka**, **mezera**, **tabulátor**, **tečka**, **roura**), případně můžete zadat vlastní znak, který odpovídá vašemu *.csv* souboru. Pokud máte v *.csv* souboru použit jiný oddělovač, zaškrtněte možnost **Jiný…** a znak zadejte. Pro snadnější identifikaci oddělovače se v sekci **Náhled dat** zobrazuje část *.csv* dokumentu.

4.**Mapování sloupců** – po nahrání *.csv* souboru a jeho zpracování můžete ovlivnit mapování jednotlivých sloupců z *.csv* souboru se sloupci tabulky v ESET PROTECT. **Pomocí rozbalovacího menu namapujte CSV sloupec se sloupcem tabulky ESET PROTECT. Pokud importovaný *.csv* soubor obsahuje hlavičku, zaškrtněte možnost První řádek CSV souboru obsahuje hlavičku**. V opačném případě ponechte tuto možnost vypnutou.

5.V **Náhledu tabulky** se ujistěte, že je mapování sloupců nastaveno správně a import proběhne požadovaným způsobem.

6.Pokud jste sloupce namapovali správně a náhled tabulky vypadá korektně, pro zahájení importu dat klikněte na tlačítko **Importovat**.



Řešení problémů – Web Console

Vzhledem k tomu, že je ESET PROTECT hostován v cloudu, lze většinu chyb souvisejících s neúspěšným přihlášením vyřešit následujícími kroky:

- Vymažte cache prohlížeče a načtěte znovu přihlašovací stránku.
- V případě přetrvávajících potíží vyčkejte několik minut a zkuste se přihlásit znovu nebo v jiném z podporovaných prohlížečů.
- Pokud se vám problém nepodařilo vyřešit, kontaktujte ESET Technickou podporu.

V tabulce níže uvádíme přehled nejčastějších chybových hlášení a stavů souvisejících s přihlášením do Web Console společně s jejich vysvětlením a možnými kroky pro jejich vyřešení:

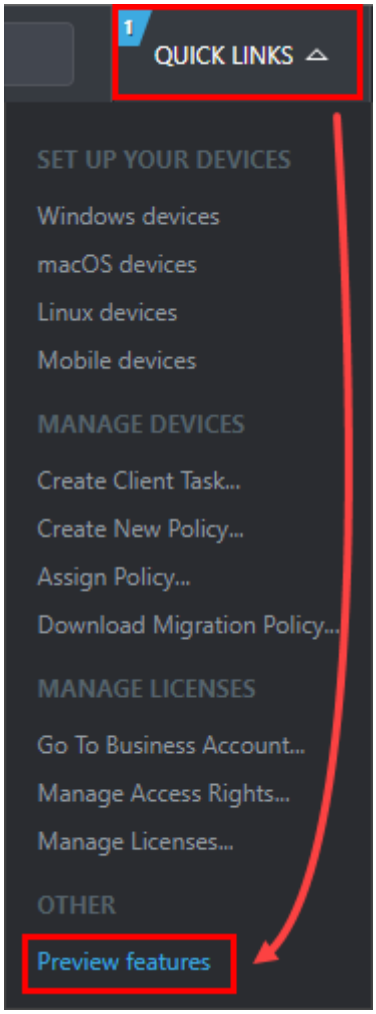
Chybová zpráva	Možný důvod
Neúspěšné přihlášení: Komunikace z vaší adresy byla dočasně zablokována.	Po 10 neúspěšných pokusech o přihlášení bude IP adresa dočasně zablokována. Po uplynutí 15 minut se přihlaste platnými údaji.
Neúspěšné přihlášení: Chyba při autentifikaci Neúspěšné přihlášení: Neúspěšné ověření na serveru	Server obdržel poškozený nebo neúplný autorizační token. Ujistěte se, že používáte správné přihlašovací údaje a že připojení k přihlašovací stránce je zabezpečené. V případě přetrvávajících potíží zkuste smazat cookies.

Chybová zpráva	Možný důvod
⚠ Neúspěšné přihlášení: Nepodařilo se připojit k serveru. Důvod: server není dostupný nebo neběží. ⚠ Neúspěšné přihlášení: Chyba při komunikaci ⚠ Neúspěšné přihlášení: Vypršel čas spojení	Zkontrolujte síťové připojení a nastavení firewallu a ujistěte se, že je webová konzole ESET PROTECT dostupná z vašeho zařízení.
⚠ Neúspěšné přihlášení: Uživatel nemá přiřazenou žádné přístupové oprávnění	Uživatelský účet, pod kterým se pokoušíte přihlásit nemáte přiřazené žádné přístupové oprávnění. Přihlaste se jako administrátor a danému uživateli přiřaďte odpovídající oprávnění. Pokud nemáte administrátorský přístup, kontaktujte v této žádosti svého správce.
JavaScript je vypnutý. Prosím, povolte jej ve svém prohlížeči.	JavaScript je vyžadován pro korektní fungování přihlašovací obrazovky. Povolte JavaScript nebo aktualizujte svůj webový prohlížeč.
Přihlašovací obrazovka se nezobrazuje nebo načítá ve smyčce.	Zkontrolujte síťové připojení a nastavení firewallu a ujistěte se, že je webová konzole ESET PROTECT dostupná z vašeho zařízení. ESET Status Portal zobrazuje aktuální stav cloudových služeb ESET, plánované odstávky a minulé incidenty. Pokud máte problém s podporovanou službou ESET a nevidíte ji uvedenou ve stavovém portálu, kontaktujte technickou podporu společnosti ESET. Monitorovací týmy interně ověřují potenciální problémy a potvrzené incidenty jsou zveřejňovány a aktualizovány ručně, aby byla zachována vysoká důvěryhodnost a přesnost. Proto se ve stavovém portálu zobrazují s mírným zpožděním. Incidenty s krátkou dobou trvání nemusí být zveřejněny, pokud jsou vyřešeny před ručním potvrzením.
"Nastala neočekávaná chyba" nebo "Nastala neošetřená chyba"	Tato chyba může nastat, pokud přistupujete k webové konzoli ESET PROTECT z prohlížeče, který není podporován webovou konzolí ESET PROTECT, viz podporované webové prohlížeče.
SEC_ERROR_INADEQUATE_KEY_USAGE (pouze Mozilla Firefox).	Mozilla Firefox má poškozené úložiště certifikátů.

Náhled funkcí

Prostřednictvím náhledu funkcí si můžete vyzkoušet nové funkce, které se objeví v dalších verzích ESET PROTECT.

Možnost pro aktivování **Náhledu funkcí** naleznete v horním menu **Rychlé odkazy**.



Po kliknutí se zobrazí přehled všech funkcí, které jsou v rámci programu náhled funkcí aktuálně dostupné, společně s jejich krátkým představením. Jednotlivé funkce můžete kdykoli **Aktivovat**, stejně tak **Deaktivovat**, a pomocí tlačítka **Odeslat zpětnou vazbu** nám dát vědět, jak se vám funkce líbila.

Po aktivování je náhled funkce trvale dostupný v konzoli pro vzdálenou správu.

V nejnovější verzi konzole pro vzdálenou správu je v rámci náhledu funkcí k dispozici:

> V aktuálním sestavení nejsou k vyzkoušení žádné nové funkce.

Synchronizace ESET PROTECT s Active Directory

Pro synchronizaci počítačů a uživatelů v Active Directory s ESET PROTECT Web Console můžete použít **ESET Active Directory Scanner**.

> Společnost ESET kontinuálně vyvíjí Active Directory Scanner a rozšiřuje jeho možnosti. Další podrobnosti naleznete v seznamu změn.

Požadavky

- ESET Active Directory Scanner spusťte pod Active Directory uživatelem na počítači připojeném do Active Directory.

- Podporované operační systémy (podpora HTTP/2): Windows 10, Windows Server 2016 a novější.
- Stažený a nainstalovaný .NET Core Runtime.
- Připravte si konfigurační soubor (*config.json*) pro synchronizaci uživatelů z Active Directory. Soubor *config.json* je součástí archivního souboru **Active Directory Scanner**.
- Uživatelské oprávnění pro **Přístupový token AD Scanner**: **Zápis**

Použití nástroje Active Directory Scanner

1. V ESET PROTECT Web Console si vytvořte GPO skript pro nasazení agenta.

2. Přihlaste se na počítač, který je členem Active Directory, svým Active Directory účtem. Ujistěte se, že splňuje veškeré výše uvedené požadavky.

3. Stáhněte si nejnovější verzi nástroje Active Directory Scanner.

4. Rozbalte stažený archiv.

5. Stáhněte si GPO skript pro nasazení agenta (vytvořený v kroku 1) a umístěte jej do složky *ActiveDirectoryScanner* (složka, ve které se nacházejí všechny soubory nástroje ESET Active Directory Scanner).

Synchronizace počítačů z Active Directory

1. V hlavním menu ESET PROTECT přejděte do sekce **Počítače** a vyberte statickou skupinu, do níž chcete synchronizovat strukturu Active Directory.
2. Na řádku se statickou skupinou klikněte na **ozubené kolečko** a v kontextovém menu vyberte **Active Directory Scanner**.
3. Pro získání přístupového tokenu klikněte na **Generovat**.

Každá statická skupina má svůj token. Token slouží jako jednoznačný identifikátor statické skupiny, do níž se synchronizuje obsah Active Directory. Pro zneplatnění aktuálně používaného tokenu (z bezpečnostních důvodů) vyberte možnost **Přegenerovat** a vytvořte si nový token. Pokud již probíhá synchronizace Active Directory s ESET PROTECT, po změně tokenu dojde k jejímu přerušení. Pro opětovné aktivování synchronizace použijte v nástroji ESET Active Directory Scanner nový token.
Chcete-li z bezpečnostních důvodů token smazat, klikněte na **Deaktivovat token**. Deaktivaci potvrďte kliknutím na **Deaktivovat**.

4. Spusťte Active Directory Scanner (`token_string` nahraďte zkopírovaným tokenem z předchozího kroku).

```
ActiveDirectoryScanner.exe --token token_string
```

Nejnovější verze nástroje Active Directory Scanner standardně nesynchronizuje deaktivované počítače z Active Directory. Pro synchronizaci deaktivovaných počítačů z Active Directory použijte parametr `--disabled-computers`:

```
ActiveDirectoryScanner.exe --token token_string --disabled-computers
```

5. Po vyzvání zadejte heslo k Active Directory účtu.
6. Jakmile Active Directory Scanner dokončí synchronizaci, struktura Active Directory (organizační jednotky včetně počítačů) se zobrazí ve webové konzoli ESET PROTECT v sekci **Počítače** jako nové statické skupiny.

Zahrnutí nebo vyloučení organizačních jednotek

Chcete-li zahrnout nebo vyloučit organizačních jednotku, určete cestu (např.: `"Users/Bratislava/TechDepartment"`). Ve výchozím nastavení `"ExcludeByID"` pracuje s `sid`.
Příklad syntaxe:

```
"Include": [
    "path"
            ],
            "Exclude": [
    "path"
            ],
            "ExcludeByID": [
    "sid1", "sid2"...
            ],
```

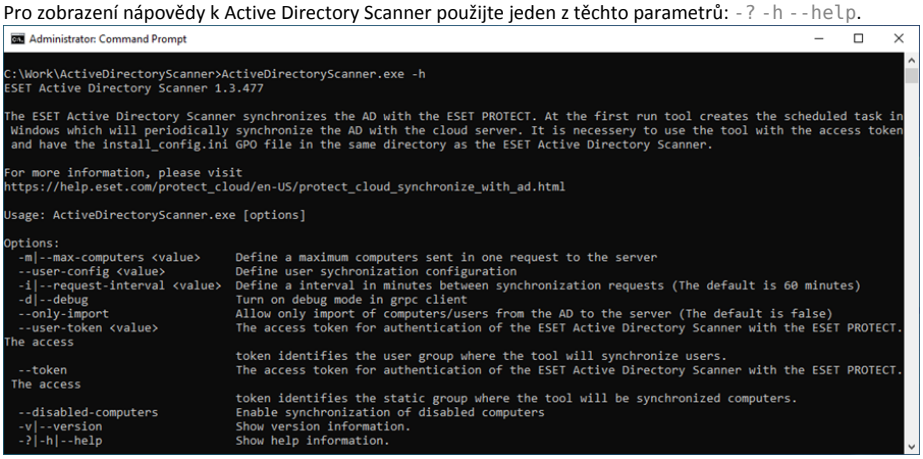
Příklad: `"Include" "path" "Users/Bratislava/TechDepartment"` má více podjednotek; jakoukoli podjednotku můžete vyloučit pomocí `"exclude" "path" "Users/Bratislava/TechDepartment/Test"`

Active Directory Scanner automaticky vytvoří v Plánovači Windows úlohu s názvem **Active Directory Synchronization** a naplánuje její spuštění na každou hodinu. V případě potřeby si můžete interval synchronizace s Active Directory kdykoli v Plánovači úloh upravit. Při provedení změn ve struktuře Active Directory se změny v ESET PROTECT Web Console projeví během příštího spuštění synchronizace.

Omezení synchronizace s Active Directory

- Active Directory Scanner synchronizuje pouze organizační jednotky Active Directory, ve kterých se nacházejí počítače s DNS názvy. Nesynchronizují se organizační jednotky, které neobsahují žádné počítače.
- Pokud se v Active Directory změní název organizační jednotky, při příští synchronizaci se v ESET PROTECT Web Console vytvoří nová statická skupina. Statická skupina odpovídající staré organizační jednotce bude v ESET PROTECT Web Console přejmenována a zůstane prázdná – počítače se přesunou do nové statické skupiny s novým názvem.
- Pokud v Active Directory odstraníte organizační jednotku, v ESET PROTECT Web Console dojde k odstranění všech počítačů nacházejících se v odpovídající statické skupině.
- Pokud z ESET PROTECT Web Console odstraníte synchronizovaný Active Directory počítač, při opětovné synchronizaci se již v konzoli znovu nezobrazí – ačkoli stále zůstává Active Directory.

Pro zobrazení nápovědy k Active Directory Scanner použijte jeden z těchto parametrů: `-? -h --help`.



V případě potíží vám mohou být vodítkem pro řešení problému protokoly umístěné ve složce *C:\ProgramData\ESET\ActiveDirectoryScanner\Logs*.

Pokud z Active Directory odstraníte počítač, odstraníte jej zároveň z webové konzole ESET PROTECT.

Synchronizace uživatelů z Active Directory

1. V hlavním menu ESET PROTECT přejděte do sekce **Další** > **Uživatelé zařízení** a vyberte skupinu uživatelů, do níž chcete synchronizovat strukturu Active Directory.
2. Na řádku vybrané skupiny uživatelů klikněte na **ozubené kolečko**, v kontextovém menu vyberte možnost **Active Directory Scanner** a zkopírujte si vygenerovaný přístupový token.
3. Pro získání přístupového tokenu klikněte na **Generovat**.

Každá statická skupina má svůj unikátní přístupový token. Token slouží jako jednoznačný identifikátor statické skupiny, do níž se synchronizuje obsah Active Directory.
Pro zneplatnění aktuálně používaného tokenu (z bezpečnostních důvodů) vyberte možnost **Přegenerovat** a vytvořte si nový token. Pokud již probíhá synchronizace Active Directory s ESET PROTECT, synchronizace se po změně tokenu přeruší. Pro opětovné aktivování synchronizace použijte v nástroji ESET Active Directory Scanner nový token.
Chcete-li z bezpečnostních důvodů token smazat, klikněte na **Deaktivovat token**. Deaktivaci potvrďte kliknutím na **Deaktivovat**.

3. Spusťte Active Directory Scanner (`token_string` nahraďte zkopírovaným tokenem z předchozího kroku).

```
ActiveDirectoryScanner.exe --user-token token_string --user-config config.json
```

Parametr `--user-token` použijte současně s parametrem `--token`. Nástroj bude následně synchronizovat počítače i uživatele.

Doporučení pro konfigurační soubor pro synchronizaci uživatelů (config.json)

Při konfiguraci souboru *config.json* postupujte podle doporučení pro formátování (umístěných ve stejné složce jako soubor *ActiveDirectoryScanner.exe*). Před úpravami si soubor zálohujte (v případě potřeby si kopii můžete znovu stáhnout).

- Odstraňte komentáře, slouží pouze jako návod.
- Pomocí polí `"Include"` a `"Exclude"` určete skupiny zahrnuté nebo vyloučené ze synchronizace.
- V souladu s pokyny v souboru *config.json* doporučujeme identifikovat skupiny pomocí `objectGUID` a nikoliv `Distinguished Name`.
- Hodnoty `objectGUID` zadejte v následujícím formátu:

```
"Include": [ "{objectGUID1}", "{objectGUID2}", ... ],
"Exclude": [ "{objectGUID3}", "{objectGUID4}", ... ],
```

- Vyměňte `{objectGUID}` za vlastní hodnoty `objectGUID` skupin, které chcete zahrnout nebo vyloučit. Každý `objectGUID` by měl mít formát hexadecimálního řetězce ve složených závorkách. Pokud máte například dvě skupiny s `objectGUID` hodnotami `"12345678-1234-5678-1234-1234567890AB"` a `"98765432-4321-8765-4321-0987654321AB"`, pak se `Include` by sekce vypadala takto:

```
"Include": [ "{12345678-1234-5678-1234-1234567890AB}", "{98765432-4321-8765-4321-0987654321AB}" ],
```

- Chcete-li vyloučit skupiny pomocí `objectGUID` `"55555555-5555-5555-5555-555555555555"` `Exclude` by sekce vypadala takto:

```
"Exclude": [ "{55555555-5555-5555-5555-555555555555}" ],
```

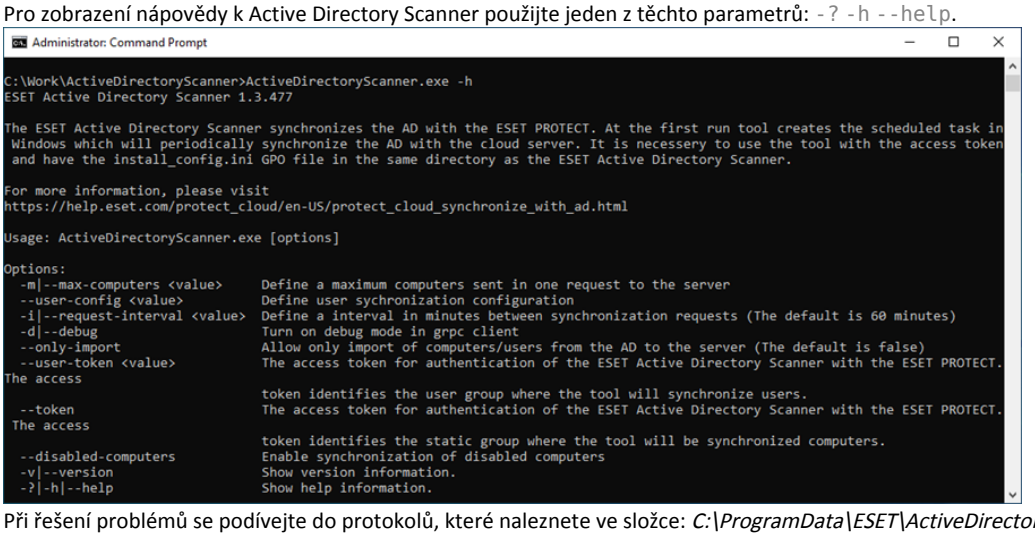
4. Po vyzvání zadejte heslo k Active Directory účtu.
5. Jakmile Active Directory Scanner dokončí synchronizaci, struktura Active Directory (organizační jednotky včetně počítačů/uživatel) se zobrazí v ESET PROTECT Web Console v sekci **Počítače/Uživatelé zařízení** jako nové statické skupiny nebo jako **Skupiny uživatelů** v sekci **Uživatelé zařízení**.

Active Directory Scanner automaticky vytvoří v Plánovači Windows úlohu s názvem **Active Directory Synchronization** a naplánuje její spuštění na každou hodinu. V případě potřeby si můžete interval synchronizace s Active Directory kdykoli v Plánovači úloh upravit. Při provedení změn ve struktuře Active Directory se změny v ESET PROTECT Web Console projeví během příštího spuštění synchronizace.

Omezení synchronizace s Active Directory

- Active Directory Scanner synchronizuje pouze AD organizační jednotky, ve kterých se nacházejí uživatelé. Nesynchronizují se organizační jednotky, které neobsahují žádné uživatele.
- Pokud v Active Directory odstraníte organizační jednotku, v ESET PROTECT Web Console dojde k odstranění všech uživatelů nacházejících se v odpovídající skupině uživatelů. Dojde k odstranění též prázdných skupin.
- Pokud z ESET PROTECT Web Console odstraníte synchronizovaného uživatele, při opětovné synchronizaci se již v konzoli znovu nezobrazí – ačkoli stále zůstává v Active Directory až do chvíle, než dojde ke změně synchronizovaných atributů v Active Directory.

Pro zobrazení nápovědy k Active Directory Scanner použijte jeden z těchto parametrů: `-? -h --help`.



Při řešení problémů se podívejte do protokolů, které naleznete ve složce: *C:\ProgramData\ESET\ActiveDirectoryScanner\Logs*.

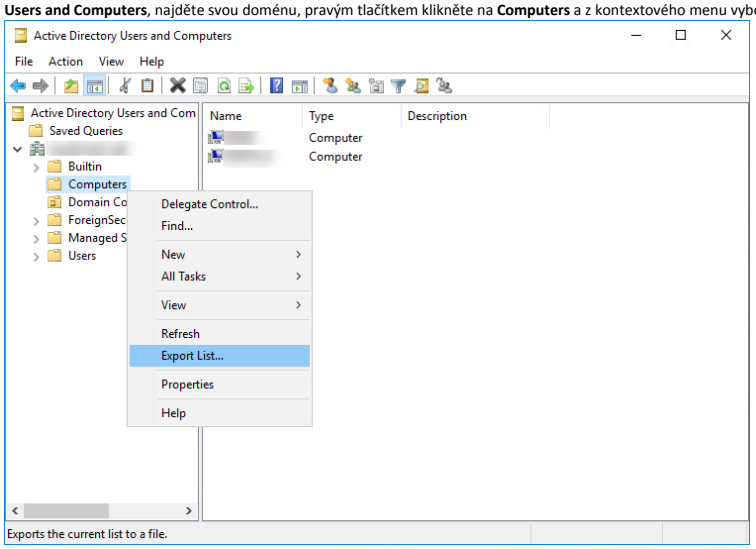
Alternativní řešení

Alternativně můžete využít jedno z níže uvedených řešení:
- Export seznam počítačů z Active Directory a jejich import do ESET PROTECT
- Nasazení ESET Management Agenta na počítače v Active Directory prostřednictvím GPO

Export seznam počítačů z Active Directory a jejich import do ESET PROTECT

Toto řešení zajistí jednorázovou synchronizaci s Active Directory. Následně se již nepromítnou žádné další změny, které v budoucnu v Active Directory provedete.

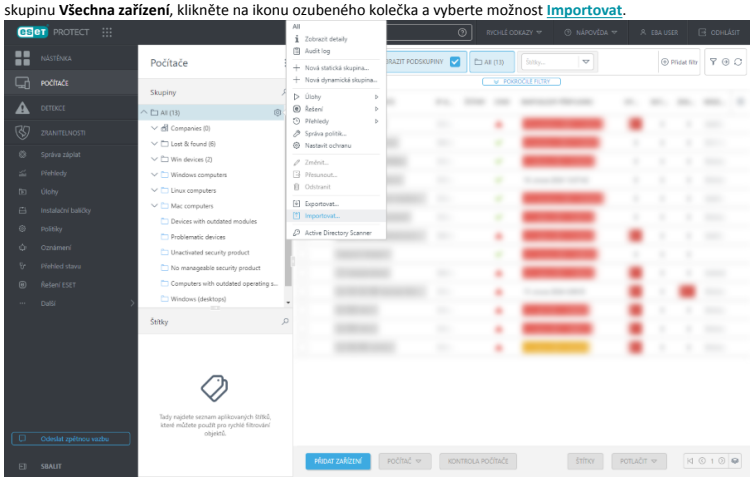
1. Exportujte seznam počítačů z Active Directory. Využít můžete mnoho nástrojů, záleží na tom, jak s pracujete Active Directory. Například si otevřete **Active Directory Users and Computers**, najděte svou doménu, pravým tlačítkem klikněte na **Computers** a z kontextového menu vyberte možnost **Export List**.



2. Seznam exportovaných počítačů z Active Directory si uložte jako *.txt* soubor.
3. Upravte seznam počítačů tak, aby odpovídal podporovanému formátu ESET PROTECT. Ujistěte se, že je na každém řádku pouze jeden počítač a záznamy jsou ve formátu:

```
\GROUP\SUBGROUP\Computer name
```

4. Uložte si aktualizovaný *.txt* soubor seznamem počítačů.
5. Naimportujte seznam počítačů z Active Directory do ESET PROTECT Web Console. V hlavním menu přejděte do sekce **Počítače**, vyberte nejnadřazenější statickou skupinu **Všechna zařízení**, klikněte na ikonu ozubeného kolečka a vyberte možnost **Importovat**.



Nasazení ESET Management Agenta na počítače v Active Directory prostřednictvím GPO

1. Vytvořte si GPO skript pro nasazení agenta.
2. Nasaďte ESET Management Agenta pomocí Group Policy Object (GPO) – začněte krokem č.3 v tomto článku v Databázi znalostí.
3. Po úspěšném nasazení ESET Management Agenta prostřednictvím GPO se počítač, který je členem Active Directory zobrazí v ESET Management Web Console na záložce **Počítače**.

Kdykoli v budoucnu přidáte do Active Directory nový **počítač**, nasadí se na něj agent a automaticky se zobrazí v ESET PROTECT Web Console.

Jak spravovat bezpečnostní řešení ESET pro ochranu koncových zařízení prostřednictvím ESET PROTECT

Předtím, než začnete konzoli používat ke správě bezpečnostních produktů ESET ve vaší síti, doporučujeme provést prvotní nastavení. V sekci Přehled stavu/Stav serveru máte přístup k nejdůležitějším nastavením, ale zároveň také informacím, zda je vše správně nastavené. Tato sekce je užitečná v případě, kdy jste přeskočili Prohlídku ESET PROTECT. Níže uvádíme základní informace ke správě bezpečnostních řešení prostřednictvím ESET PROTECT Web Console společně s přehledem akcí, které můžete vzdáleně provádět.

Instalace ESET Management Agenta a bezpečnostního produktu

Abyste mohli prostřednictvím ESET PROTECT spravovat koncové stanice, je nutné na ně nainstalovat ESET Management Agenta. Agenta na stanici můžete nainstalovat samostatně nebo společně s bezpečnostním produktem. Před instalací doporučujeme importovat licenci do ESET Business Account, aby ji bylo možné použít pro následné instalace. Bezpečnostní produkt můžete na stanici nainstalovat těmito způsoby:

- Ručním spuštěním instalačního balíčku obsahujícího agenta i bezpečnostní produkt ESET, případně vzdáleně prostřednictvím nástroje ESET Remote Deployment Tool.
- Klikněte na počítač a vyberte **Řešení** > **Zapnout bezpečnostní produkt** pro zapnutí bezpečnostního produktu ESET v počítači.
- Prostřednictvím klientské úlohy na instalaci aplikace nainstalujete bezpečnostní produkt na zařízení s již nasazeným ESET Management Agentem.

Správa bezpečnostního řešení pro ochranu koncových zařízení prostřednictvím ESET PROTECT

Veškerá bezpečnostní řešení pro ochranu koncových zařízení lze spravovat z ESET PROTECT Web Console. Veškeré nastavení bezpečnostního produktu provedete prostřednictvím politik, které můžete přiřazovat skupinám nebo konkrétním zařízením. Můžete například vytvořit politiku pro blokování přístupu k určitým webovým stránkám, změnit citlivost detekce skeneru nebo změnit další nastavení bezpečnostního řešení ESET. Pokud na zařízení aplikujete více politik, dojde k jejich sloučení, jak je uvedeno na tomto příkladu. Nastavení vynucená politikami z ESET PROTECT nemůže uživatel lokálně měnit. V případě potřeby můžete uživateli na dočasnou dobu povolit změnu nastavení. To se hodí při řešení problémů. Až uživatel odhalí příčinu nekorektního chování, můžete si stáhnout upravenou konfiguraci a převést ji do politiky.

Pro správu koncových stanic slouží úlohy. Klientské úlohy vytvořené v konzoli provádí na cílové stanici ESET Management Agent. Níže uvádíme přehled nejčastěji používaných úloh:

- Aktualizace modulů (včetně detekčního jádra)
- Volitelná kontrola počítače
- Spuštění příkazu
- Vyžádání konfigurace

Aktualizace bezpečnostních produktů ESET

1. Přejděte na **Nástěnku** > **Přehled stavu** > Stav verze komponent.
2. Kliknutím na žlutou/červenou část grafu reprezentující zastaralé aplikace můžete po vybrání možnosti **Aktualizovat nainstalované ESET produkty** inicializovat jejich aktualizaci.

Reportování stavu počítače a získávání informací z klientské stanice v ESET PROTECT

Každá stanice je do ESET PROTECT připojená prostřednictvím ESET Management Agenta. Agent reportuje na ESET

PROTECT server všechny požadované informace o klientské stanici. Všechny protokoly z koncových zařízení nebo jiných bezpečnostních řešení ESET se odesílají na ESET PROTECT Server.

Informace nejen o nainstalovaných ESET aplikacích, ale také operačním systému naleznete v detailech každého zařízení (na záložce **Počítače**. V hlavním menu na záložce Počítače najděte konkrétní zařízení, klikněte na něj a vyberte možnost **Detaily**. V sekci **Konfigurace** si můžete zobrazit seznam všech politik, které na zařízení aplikujete a vyžádat si aktuální konfiguraci nainstalovaných ESET produktů. Pokud chcete ze systému získat veškeré informace, na záložce **SysInspector** můžete zažádat o vygenerování detailního protokolu a následně si jej prohlédnout přímo ve webovém prohlížeči (tato možnost je dostupná pouze pro stanice s OS Windows).

Seznam všech detekcí na zařízeních ve vaší síti naleznete v hlavním menu Web Console v sekci Detekce. Detekce pro konkrétní zařízení si můžete zobrazit přímo na záložce **Počítače**. Vyberte zařízení, v kontextovém menu klikněte na **Detaily** a přejděte na záložku **Detekce a karanténa**. Pokud na stanici běží také ESET Inspect Connector, naleznete zde také ESET Inspect oznámení.

Pro zobrazení dat ze stanic ve vaší síti využijte přehledy, které můžete vygenerovat jednorázově, zobrazit si je na nástěnce nebo naplánovat jejich pravidelné generování a doručení. Přehledy představují nejrychlejší cestu k získání požadovaných dat. Využít můžete předdefinované přehledy, případně si vytvořte vlastní. Využít můžete předdefinované přehledy, které vám poskytnou například agregované informace o stavu vaší infrastruktury, zobrazí hromadně data o nainstalovaných aplikacích, nebo detekcích.

> Uživatel může použít pouze přehledy, ke kterým má přístup. Standardně jsou všechny předdefinované šablony přehledů uloženy v nejnadřazenější statické skupině **Všechna zařízení**. V přehledech se uživateli zobrazí výhradně data (počítače a události) z objektů, ke kterým má přístup. Pokud konkrétní šablonu sdílí mezi sebou více uživatelů, každý z nich uvidí pouze data ze zařízení, ke kterým má přístup. Více informací naleznete v kapitole seznam oprávnění.

ESET Push Notification Service

ESET Push Notification Service (EPNS) slouží k přijímání zpráv ze serveru ESET PROTECT, pokud má server ESET PROTECT oznámení pro klienta. Spojení funguje tak, aby ESET PROTECT mohl okamžitě klientovi odeslat (push) notifikaci. Pokud dojde k přerušení spojení, klient se jej pokusí znovu navázat. Hlavním důvodem persistentního spojení je zajištění příjmu zpráv na straně klienta.

Uživatel Web Console může prostřednictvím EPNS odeslat žádost o probuzení mezi ESET PROTECT Serverem a ESET Management agenty.

Detaily spojení

Chcete-li nakonfigurovat místní síť tak, aby umožňovala komunikaci s EPNS, je třeba, aby se ESET Management Agenti mohli připojit k serveru EPNS. Pokud agenti nedokáží navázat spojení s EPNS, probudí se pouze na základě Wake-Up call. Ujistěte se, že firewall umožňuje připojení k serveru EPNS (viz tabulka níže).

Kryptografický bezpečnostní protokol	TLS – nejnovější verze protokolu TLS podporovaná operačním systémem spravovaného zařízení
Protokol	MQTT (machine-to-machine connectivity protocol)

Port	• primární: 8883 • záložní připojení: 443 a proxy port definovaný v politice ESET Management agenta Port 8883 je preferovaný, protože se jedná o MQTT port. 443 je pouze záložní port a je sdílen s jinými službami. Může tedy dojít k tomu, že firewall přeruší spojení na portu 443 z důvodu nečinnosti nebo při dosažení maximálního limitu otevřených připojení s HTTP Proxy serverem.
Adresa	*epns.eset.com*
Kompatibilita proxy	Pokud pro směrování komunikace používáte HTTP Proxy, Wake-Up call se odešle prostřednictvím ní. Autentifikace není podporována. Ujistěte se, že máte politikou pro agenta správně nakonfigurovanou HTTP Proxy na zařízeních, na která zasíláte žádosti o probuzení (wake-up calls). V případě nefunkční HTTP Proxy se Wake-up call zašle přímo.

Řešení problémů

- Ujistěte se, že firewall povoluje připojení k EPNS (viz detaily komunikace v tabulce výše nebo článek Databáze znalostí).

VDI, klonování a detekce hardware

ESET PROTECT podporuje VDI prostředí, klonování stanic a nepersistentní úložné systémy. Tato funkce vyžaduje označení některého stroje jako master, případně vyřešení rozhodnutí při detekci klonů nebo změně hardware.

- Dokud nevyřešíte rozhodnutí, klientská stanice nebude replikovat data na ESET PROTECT Server. Stanice si při svém připojení pouze ověří, zda již bylo rozhodnutí vyřešeno.

- Vypnutí detekce hardware je nevratný proces, proto byste jej měli používat s opatrností a pouze na fyzických zařízeních!

- Pro vyřešení většího množství rozhodnutí použijte na záložce Stav serveru dlaždici **Rozhodnutí**.

Jaké operační systémy a hypervizory jsou podporovány?

Před tím, než začnete ESET PROTECT používat ve svém VDI prostředí, seznamte se v naší Databázi znalostí s podporovanými a nepodporovanými funkcemi jednotlivých VDI prostředí.

- Podporovány jsou pouze operační systémy Windows.

- ESET Full Disk Encryption můžete používat ve virtuálním prostředí, ale ESET Full Disk Encryption nelze klonovat

- Mobilní zařízení spravovaná prostřednictvím Cloud MDM nejsou podporována

- Propojené klony ve Virtual Boxu není možné od sebe odlišit.

- Ve velmi vzácných případech může ESET PROTECT detekci automaticky vypnout. K tomu dochází, když ESET PROTECT není schopen spolehlivě analyzovat hardware

- Podívejte se na seznam podporovaných konfigurací:

  - Citrix PVS 7.15+ s fyzickými počítači

- Citrix PVS 7.15+ s virtuálními počítači v Citrix XenServer 7.15+
- Citrix PVS 7.15+ a Citrix XenDesktop s Citrix XenServer 7.15+
- Citrix Machine Creation Services
- (bez PVS) Citrix XenDesktop s Citrix XenServer 7.15+
- VMware Horizon 8.0+ s VMware ESXi
- Microsoft SCCM (pro znovuzavádění obrazů)

- ESET PROTECT podporuje VDI jmenné vzory na všech podporovaných hypervizorech

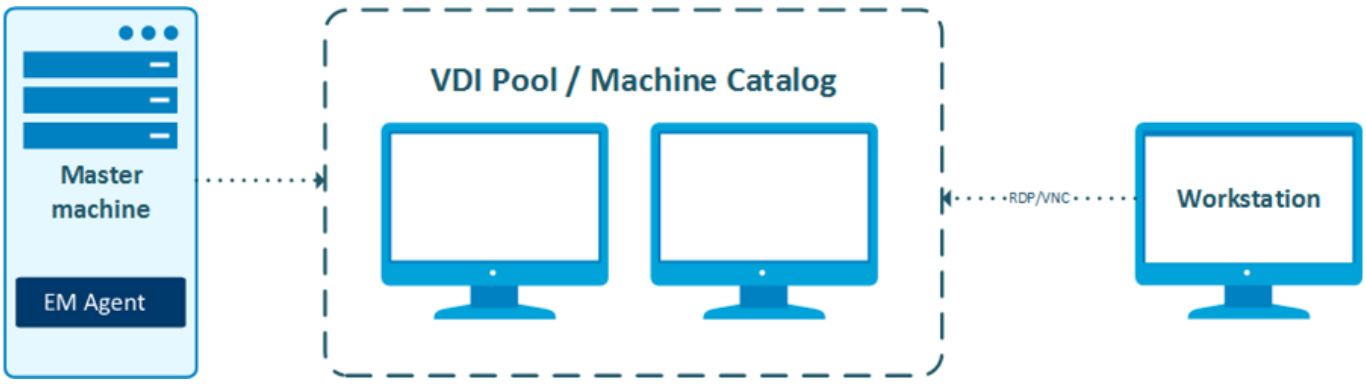
VDI prostředí

Ve VDI poolu můžete použít master stanici s již nainstalovaným ESET Management Agentem. Není vyžadován VDI konektor, veškerou komunikaci zajišťuje ESET Management Agent. ESET Management Agenta je však nutné na master stanici nasadit dříve, než ji umístíte do VDI poolu (katalogu stanic).

- Před vytvořením VDI poolu označte master zařízení v podrobnostech počítače > **Virtualizace** a poté vyberte možnost **Označit jako master pro klonování** > **Spojit s existujícím počítačem**
- Pokud je master zařízení odstraněno z ESET PROTECT, je obnovení jeho identity (klonování) zakázáno a nová zařízení z poolu pokaždé získají novou identitu (ve webové konzoli se vytvoří nový záznam o zařízení)
- Při prvním připojení zařízení z VDI poolu je povinný interval připojení 1 minuta. Po několika prvních replikacích je interval připojení zděděn od master zařízení
- Nikdy nevypínejte detekci hardware pro zařízení ve VDI poolu.
- Master zařízení můžete provozovat paralelně s klony a udržovat je tak aktuální

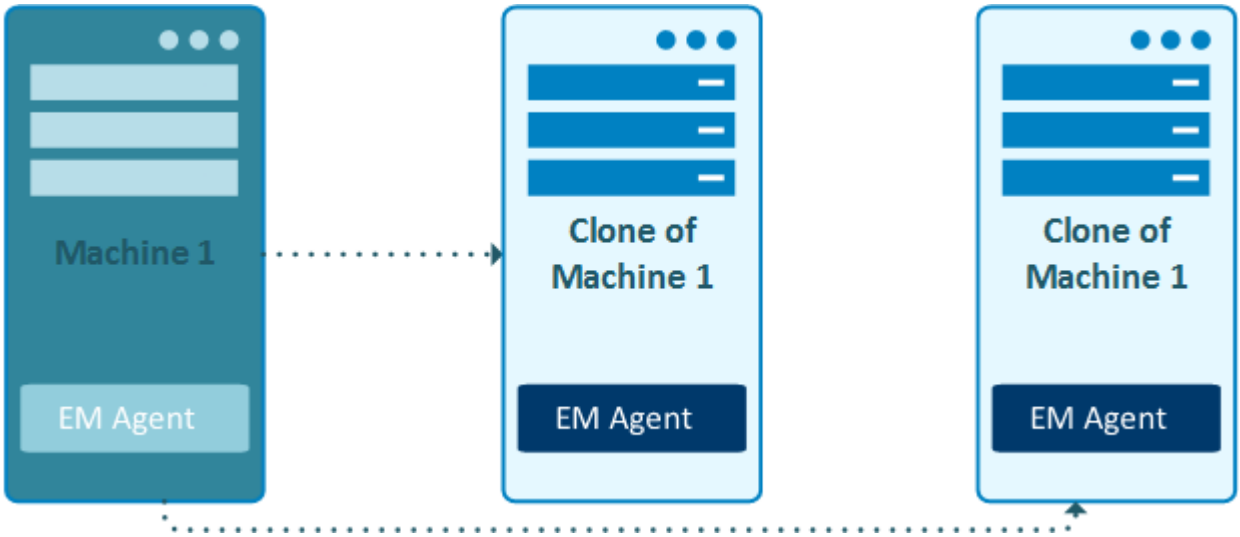
Výchozí skupina pro VDI zařízení

Nová zařízení klonovaná z masteru se zobrazí jako statická skupina v **Domovské skupině klonovaných počítačů** v okně Master pro klonování.



Klonování stanic na hypervizoru

Klonovat můžete běžné stanice. Počkejte, až se zobrazí otázka k rozhodnutí, a vyřešte ji volbou možnosti **Vytvořit počítač pouze jednou**.



Zavádění systémů na fyzické počítače z předpřipravených obrazů

Při instalaci nových počítačů ze zdrojového obrazu můžete mít v systému již nainstalovaného ESET Management agenta. V tomto případě máte dvě možnosti, jak situaci řešit:

Vytvořit nový počítač

Vytvořit nový počítač v ESET PROTECT po každém nasazení systému.

Při zjištění klonu může systém reagovat dvěma způsoby:

- Ručně – každý nový počítač řešte ručně v sekci Rozhodnutí a vyberte možnost **Vytvořit pokaždé nový počítač**.
- Automaticky – před klonováním označte master zařízení a vyberte možnost **Označit jako master pro klonování** > **Vytvořit nový počítač**.

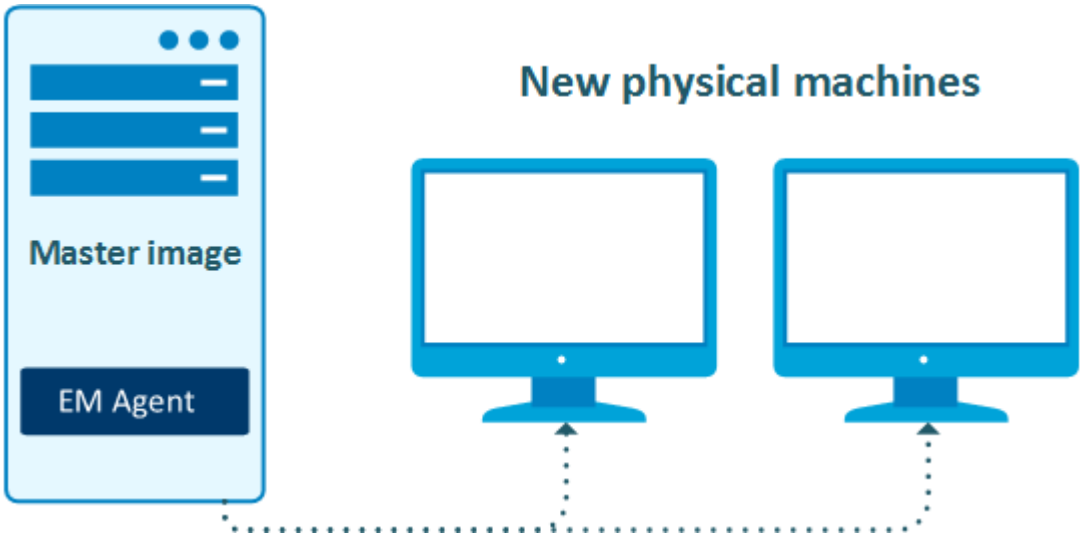
Spojit s existujícím počítačem

Pokud došlo k znovu zavedení systému na stanici, kterou již ESET PROTECT zná (byl na ní nainstalován ESET Management Agent), dojde ke spojení s již existujícím záznamem. Pokud nedojde ke shodě s již existujícím záznamem, vytvoří se po nasazení systému na nové zařízení nový počítač vESET PROTECT.

Při zjištění klonu může systém reagovat dvěma způsoby:

- Ručně – každý nový počítač řešte ručně v sekci Rozhodnutí a vyberte možnost **Spojit pokaždé s existujícím počítačem**.
- Automaticky – před klonováním označte master zařízení a vyberte možnost **Označit jako master pro klonování** > **Spojit s existujícím počítačem**.

Pokud máte image (šablonu) svého master zařízení, musíte jej aktualizovat. Po aktualizaci nebo přeinstalaci jakýchkoli komponent ESET na master zařízení vždy aktualizujte tento image.



Paralelní replikace

ESET PROTECT Server dokáže rozpoznat a vyřešit paralelní replikaci více zařízení na jednu identitu v ESET PROTECT. Na tuto událost budete upozornění v Detailech počítače na záložce **Upozornění** ('**Více připojení s identickým ID agenta**'). Máte dvě možností, jak tuto situaci vyřešit.

- Použijte akci jedním kliknutím dostupnou v upozornění na to, že počítače jsou rozděleny a detekce jejich hardwaru je trvale vypnuta
- Ve vzácných případech může dojít ke konfliktu i u zařízení s vypnutou detekcí hardwaru – pokud se tak stane, je jedinou možností úloha na obnovení klonovaného agenta
- Spusťte úlohu na obnovení klonovaného agenta, díky které nebudete muset vypínat detekci hardwaru

Řešení rozhodnutí o klonování

Při každém připojení stanice k ESET PROTECT se nový záznam vytvoří na základě dvou otisků hardware.

- UUID ESET Management agenta (univerzální jedinečný identifikátor) – změní se po přeinstalování ESET Management Agenta (viz Duplicitní záznamy (agenti).
- otisku hardware stanice – změní se, pokud dojde ke klonování stanice nebo jejímu znovu zavedení.

Otázka se zobrazí, když ESET PROTECT Server zjistí jednu z následujících věcí:

- klonované zařízení,
- změnu hardware na zařízení, na kterém je nainstalován ESET Management Agent.

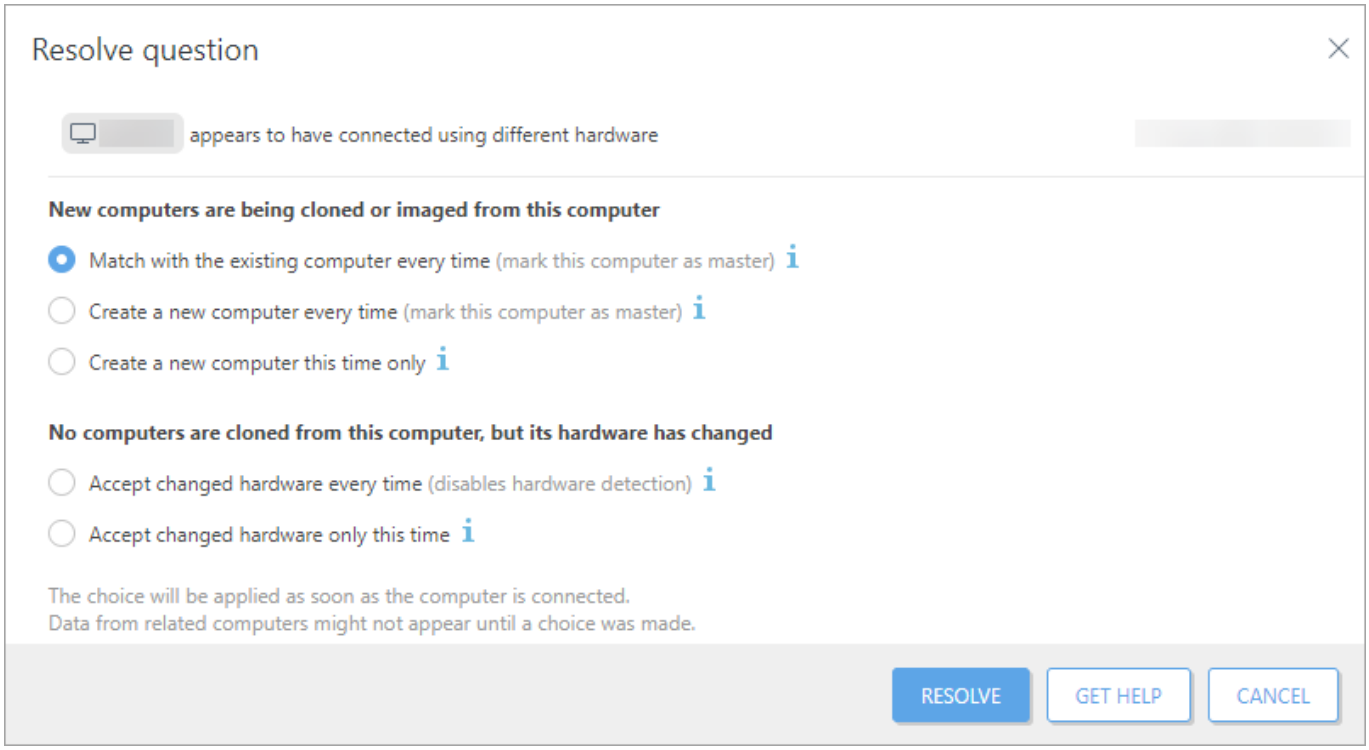
Zjištění otisku hardware není podporováno na:
- Linux, macOS, Android, iOS
- stanicích bez nainstalovaného ESET Management Agenta

Po kliknutí na rozhodnutí se zobrazí dialogové okno **Rozhodnutí**, ve kterém máte na výběr následující možnosti pro vyřešení dané situace:

Tento počítač bude používán pro klonování dalších strojů	Akce	Více detailů
Spojit pokaždé s existujícím počítačem	Tuto možnost vyberte v případě, že: • Používáte počítač jako master a všechny nově zavedené stroje chcete spojit s již existujícím záznamem v ESET PROTECT. • Používáte počítač jako master ve VDI prostředí a očekáváte, že po jejich znovu zavedení se změní jejich otisk hardware.	Více informací
Vytvořit pokaždé nový počítač	Tuto možnost vyberte, pokud jste počítač použili jako master a chcete, aby ESET PROTECT automaticky rozpoznával klony tohoto počítače a vytvářel pro ně novou identitu. Nepoužívejte ve VDI prostředích.	Více informací
Vytvořit nový počítač pouze jednou	Tuto možnost vyberte, pokud byl počítač naklonován pouze jednou. Tímto vytvoříte novou instanci pro klonovaný stroj.	Více informací

Nejedná se o klon, ale změnu hardware	Akce
Přijmout každou změnu hardware	Tímto trvale vypnete detekci hardware pro dané zařízení. Tuto možnost vyberte v případě, kdy došlo k reportování změn hardware, které se nestaly. **Mějte na paměti, že tato akce je nevratná!** Pokud detekci hardware vypnete , tuto informaci si zapamatuje agent i server. Opětovným nasazeným agenta neobnovíte vypnutou detekci HW. Stanice s vypnutou detekcí hardware nejsou vhodné pro VDI scénáře, které podporuje ESET PROTECT.
Přijmout tuto změnu hardware	Tuto možnost vyberte pro obnovení otisku hardware. Použijte ji v případě, pokud došlo ke změně hardware. Další změny hardware budou reportovány.

Kliknutím na tlačítko **Vyřešit** potvrdíte váš výběr. Klonování se vyřeší při příštím připojení klonovaného zařízení k ESET PROTECT.



Pokud otázku nevyřešíte do 30 dnů, bude automaticky vybrána možnost **Vytvořit nový počítač pouze jednou**.

Duplicitní záznamy (agenti)

Pokud je agent ESET Management na klientském počítači odinstalován (ale počítač není z Webové konzole odstraněn) a znovu nainstalován, jsou ve Webové konzoli dva stejné počítače. Rozeznáte je podle toho data připojení, u jednoho záznamu se aktualizuje čas, u druhého nikoli. Dialogové okno **Otázky** tuto situaci neřeší. Taková situace je důsledkem nesprávného postupu při odstraňování agenta. Jediným řešením je ručně odebrat počítač, který se nepřipojuje, z Webové konzole. Mějte na paměti, že historie a související data s původním záznamem budou ztracena.

Odstranění nepřipojujících se počítačů

Pokud ve VDI poolu počítačů nemáte správně nastavena rozhodnutí (viz výše), ve Web Console se pro každý restartovaný počítač vytvoří nová instance. Instance počítačů se vám začnou ve Web Console hromadit a dojde k překročení využití licence. Nedoporučujeme tento problém řešit nastavením úlohy na odstranění nepřipojujících se počítačů. Dojde tím k odstranění historie (protokolů) smazaných počítačů, nicméně nemusí dojít k uvolnění licencí.

Překročení počtu klientů povolených licencí

Po naklonování stanice s nainstalovaným ESET Management Agentem a aktivovaným bezpečnostním produktem může dojít k tomu, že si klon vyžádá další jednotku z licence. Tímto způsobem může brzy dojít k vyčerpání vaší licence. V prostředí VDI použijte k aktivaci produktů ESET offline licenční soubor a kontaktujte společnost ESET ohledně úpravy licence.

Oznámení na klonované počítače

Můžete si vybrat ze tří připravených oznámení pro akce související s klonováním. Pro nastavení oznámení zvolte v menu webové konzole **Oznámení**.

- **První připojení počítače** – upozorní, když je zařízení poprvé připojeno k vybrané statické skupině (ve výchozím nastavení je vybrána skupina **Všechna zařízení**)
- **Obnovení identity počítače** – upozorní, když bylo zařízení identifikováno na základě jeho hardwaru; zařízení bylo naklonováno z masteru nebo jiného známého zdroje
- **Detekováno potenciální klonování počítače** – upozorní na výraznou změnu hardwaru nebo na klonování, pokud zdrojový počítač nebyl předtím označen jako master

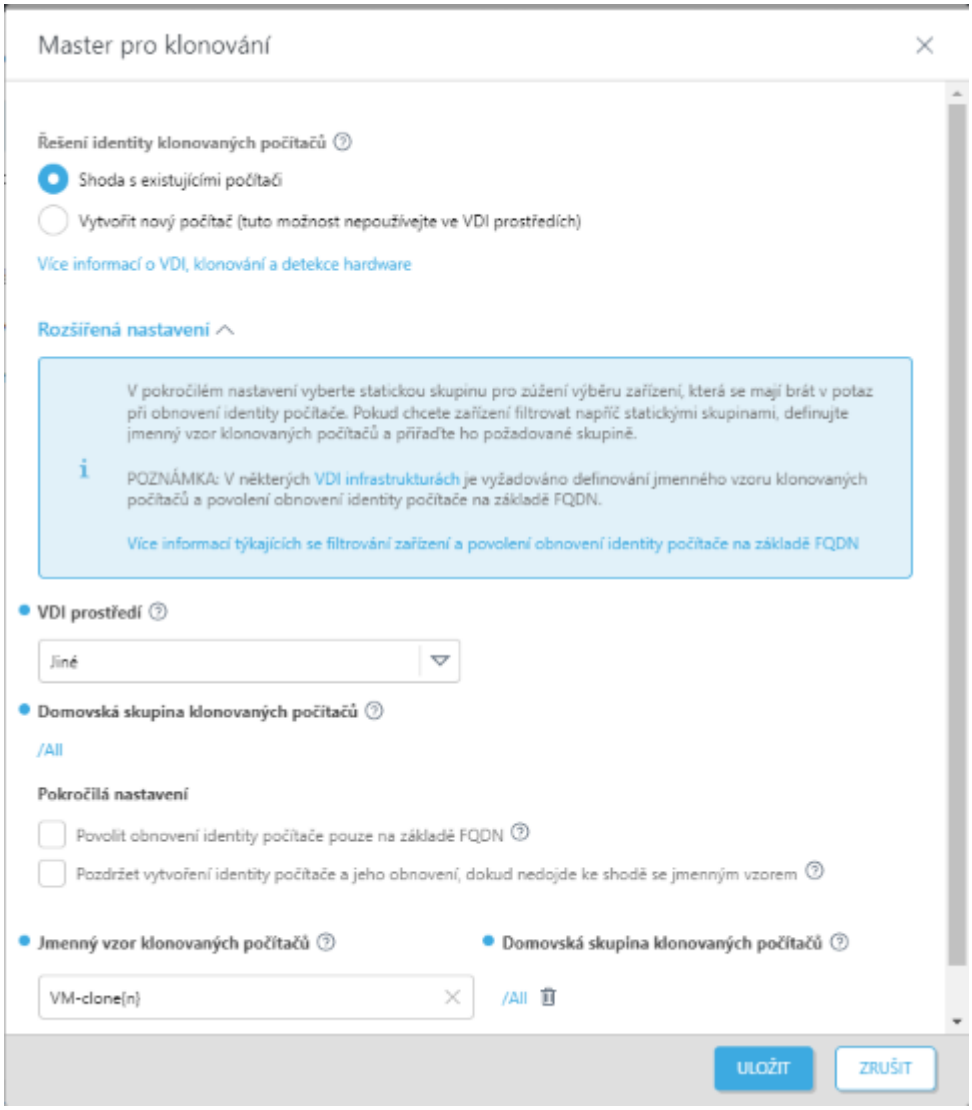
Identifikace hardware

ESET PROTECT získává detailní informace o každém připojeném zařízení a používá je k jejich rozpoznávání. Každé zařízení ESET PROTECT zařadí do jedné z následujících kategorií, a zjistit ji můžete na záložce **Počítače** ve sloupci **Identifikace hardware**.

- **Detekce hardware je zapnutá** – detekce je aktivní a korektně funguje.
- **Detekce hardware je vypnutá** – detekce byla zakázána uživatelem nebo automaticky za strany ESET PROTECT.
- **Žádné informace o hardware** – nejsou k dispozici žádné informace o hardware, nebo na zařízení běží nepodporovaný operační systém, případně je na něm nainstalovaná starší verze ESET Management agenta.
- **Detekce nevěrohodného hardware** – detekci uživatel označil jako nedůvěryhodnou, a proto bude vypnuta. Tento stav můžete zaznamenat pouze před dalším intervalem replikace, kdy jste vypnuli detekci.

Master pro klonování

Po kliknutí na tlačítko **Virtualizace** a vybrání možnosti **Označit jako master pro klonování** v detailech počítače se zobrazí následující oznámení:



Před vytvořením VDI poolu vyberte jednu z níže uvedených možností pro **Rozhodnutí o identitě klonového počítače**:

- **Spojit s existujícím počítačem** – pro více informací přejděte do kapitoly Vždy spojit s existujícím počítačem.
- **Vytvořit nový počítač** – pro více informací přejděte do kapitoly Vždy vytvořit nový počítač.

Pro nalezení počítačů označených jako Master pro klonování přejděte do sekce **Počítače** > klikněte na **Přidat filtr** > v seznamu vyberte **Master pro klonování** > filtr aktivujte pomocí **zaškrtávacího políčka**. Nastavení týkající se označení stanice jako **master pro klonování** můžete kdykoli změnit v detailech počítače:
- Možnosti konfigurace si zobrazíte po kliknutí na ikonu ozubeného kolečka na dlaždici **Virtualizace**.
- Pro zrušení tohoto nastavení klikněte na tlačítko **Virtualizace** > vyberte možnost **Odebrat označení jako Master pro klonování**.

Rozšířená nastavení

1. **VDI prostředí** – vybráním typu VDI prostředí dojde k předvyplnění požadovaného nastavení pro vaše prostředí.

- Virtuální počítače Citrix MCS/PVS Gen1

- Virtuální počítače Citrix PVS Gen2
- VMware Horizon linkované klony
- VMware Horizon instantní klony
- SCCM
- Ostatní

2. **Domovská skupina klonovaných počítačů** – Vyberte statickou skupinu pro zúžení výběru zařízení, která se mají brát v potaz při obnovení identity počítače. Vybraná statická skupina se zároveň použije jako cíl pro nově vytvářené virtuální počítače.

3. **Pokročilá nastavení**:

- **Povolit obnovení identity počítače pouze na základě FQDN** – tuto možnost prot obnovení identity počítače na základě FQDN zapněte v případě, kdy hardwarové atributy klonovaných počítačů generované vaší VDI infrastrukturou nelze v průběhu procesu obnovení považovat za spolehlivé.
- **Pozdržet vytvoření identity počítače a jeho obnovení, dokud nedojde ke shodě se jmenným vzorem** - tuto možnost vyberte v případě, kdy chcete zajistit, aby se při párování klonovaného počítače bral v potaz definovaný jmenný vzor. V takovém případě se proces vytvoření identity počítače a jeho obnovení nedokončí do chvíle, než bude nalezen odpovídající jmenný vzor.

Na základě vybraného VDI prostředí se provede výběr doporučených nastavení (některá mohou být povinná nebo nedostupná).

4. **Jmenný vzor klonovaných počítačů** – pro definování jmenného vzoru, podle kterého se budou filtrovat zařízení, klikněte na **Přidat nový**.

VDI jmenný vzor

ESET PROTECT rozeznává pouze klony odpovídající jmennému vzoru definovanému ve VDI prostředí:

- **VMware** – VDI jmenný vzor je povinný pro VMware instantní klony. VDI jmenný vzor musí obsahovat zástupný znak reprezentující unikátní číslo `{n}` generované VDI infrastrukturou ve formátu. Příklad: `VM-instant-clone-{n}`. Více informací o jmenných vzorech naleznete v dokumentaci společnosti VMware.
- **Citrix** – ve jmenném schématu katalogu strojů použijte znak křížku (`#`). Příklad: `VM-office-##`. Více informací o jmenném schématu naleznete v dokumentaci společnosti Citrix.

5. Klikněte na **Vybrat** a dále vyberte **domovskou skupinu klonovaných počítačů** – statickou skupinu, ve které se budou zařízení vyhledávat dle definovaného VDI jmenného vzoru.

6. Pro přidání více VDI jmenných vzorů a domovských skupin klikněte na **Přidat nový**.

7. Konfiguraci uložte kliknutím na tlačítko **Uložit**.

Pro nalezení počítačů označených jako Master pro klonování přejděte do sekce **Počítače** > klikněte na **Přidat filtr** > v seznamu vyberte **Master pro klonování** > filtr aktivujte pomocí **zaškrtávacího políčka**. Nastavení týkající se označení stanice jako **master pro klonování** můžete kdykoli změnit v detailech počítače:

- Možnosti konfigurace si zobrazíte po kliknutí na ikonu ozubeného kolečka na dlaždici **Virtualizace**.
- Pro zrušení tohoto nastavení klikněte na tlačítko **Virtualizace** > vyberte možnost **Odebrat označení jako Master pro klonování**.

ESET Bridge (HTTP Proxy)

ESET Bridge můžete v rámci infrastruktury ESET PROTECT využít jako proxy službu.

- Do cache dokáže ukládat: aktualizace modulů ESET, instalační a aktualizační balíčky doručované z ESET PROTECT (například MSI instalátor pro ESET Endpoint Security), aktualizace bezpečnostního produktu ESET (aktualizace komponent a produktu), výsledky ESET LiveGuard.

- Pro přesměrování komunikace ESET Management Agentů na ESET PROTECT Server.

Více informací týkající se instalace a konfigurace ESET Bridge naleznete v online příručce k ESET Bridge.

Uživatelé Apache HTTP Proxy

Začínáte s ESET PROTECT 4.0 (vydaným v listopadu 2022), ve kterém je Apache HTTP Proxy nahrazen ESET Bridge. Apache HTTP Proxy má částečnou podporu. Pokud používáte Apache HTTP Proxy, doporučujeme přejít na ESET Bridge.

Nasazení ESET Management Agenta

V této části příručky naleznete přehled všech možností, jak nasadit ESET Management Agent na klientské stanice ve své síti. Je to velice důležité, protože bezpečnostní řešení ESET na klientských zařízeních komunikuje s ESET PROTECT Serverem výhradně prostřednictvím Agenta.

Nasazení ESET Management Agenta

ESET Management Agenta můžete na klientskou stanici nasadit mnoha způsoby. Záleží na tom, zda chcete nasazení provádět lokálně nebo vzdáleně.

- Lokálně – nainstalujete ESET Management Agenta a bezpečnostní produkt ručně.

Tento způsob nasazení je vhodný pro malé sítě (do 50 počítačů), případně jej můžete využít při testování. Pro hromadné nasazení ESET Management Agenta doporučujeme používat doménovou politiku nebo SCCM.

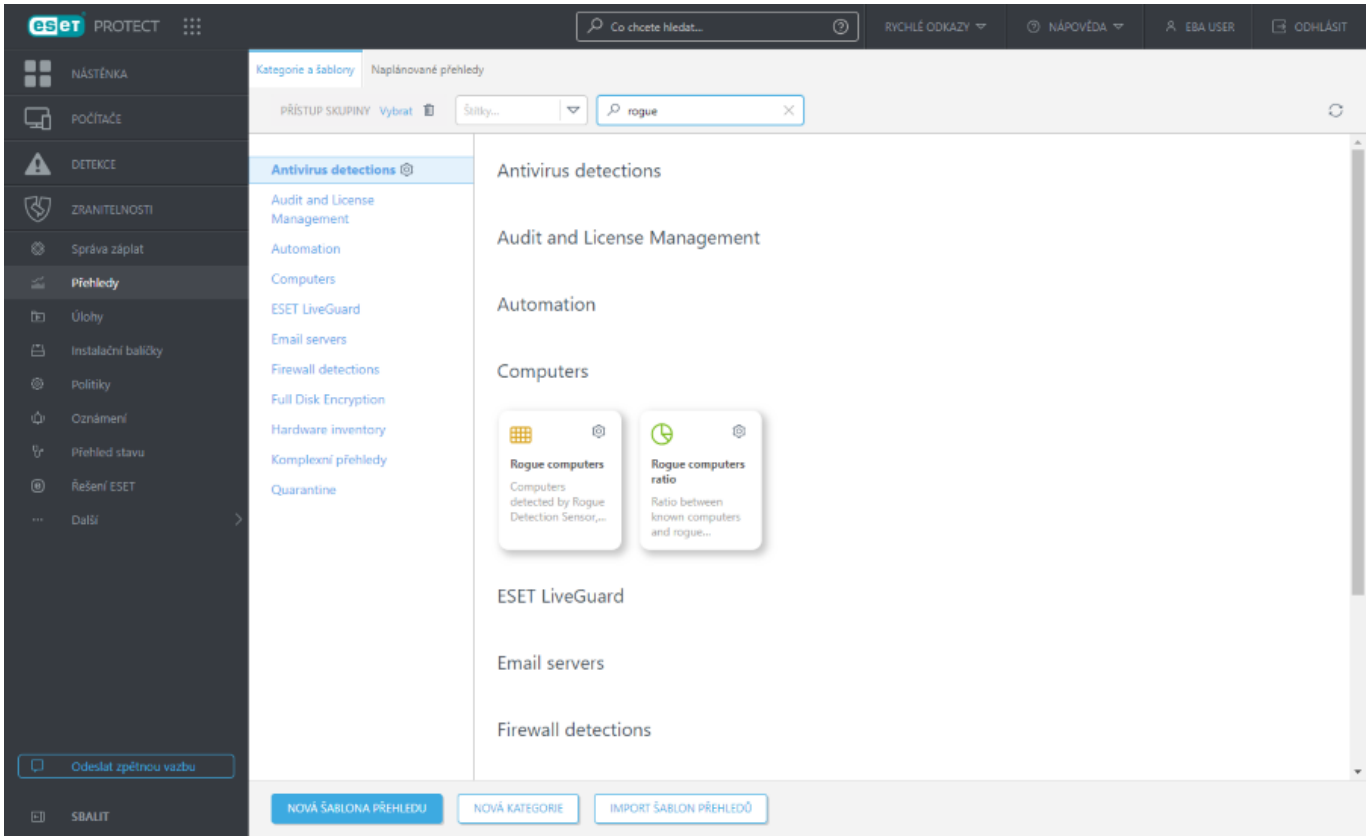
- Vzdáleně – tuto možnost doporučujeme pro hromadné nasazení na velké množství stanic.

Přidání počítačů prostřednictvím RD Sensor

RD Sensor vám pomůže najít nespravované počítače ve vaší síti. Monitoruje síť, ve které je nasazen, a pokud se do ní připojí zařízení, na kterém není nainstalován agent, předá tuto informaci do ESET PROTECT. RD Sensor není

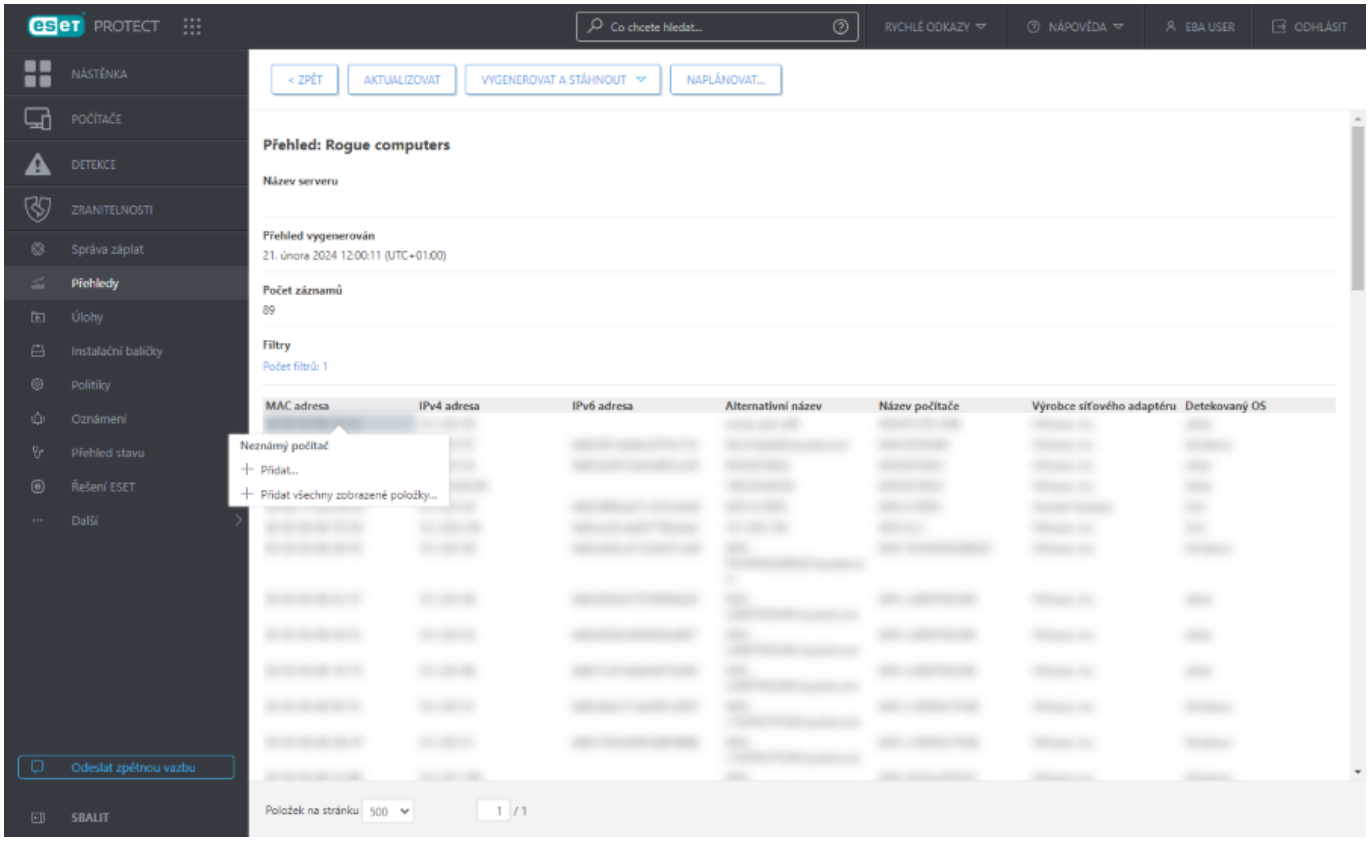
možné nasadit prostřednictvím Live Installer. Pro nasazení ESET RD Sensor do vaší sítě postupujte podle kroků uvedených v kapitole Instalace ESET RD Sensor.

Pokud již máte RD Sensor nainstalován, v hlavním menu Web Console přejděte do sekce **Přehledy** a klikněte na dlaždici reprezentující přehled **Nalezené počítače**.



V přehledu se zobrazují všechny počítače, které objevil RD Sensor. Množství zobrazovaných informací můžete ovlivnit politikou pro RD Sensor.

Pro přidání počítačů, které objevil RD Sensor do ESET PROTECT, si stáhněte přehled ve formátu *.csv*. Spusťte Deployment Tool, použijte možnost Importovat seznam počítačů a vyberte exportovaný seznam počítačů.



Výsledky analýzy sítě ESET RD Sensor zapisuje do protokolu `detectedMachines.log`. V souboru se nachází seznam všech počítačů, která tento nástroj objevil ve vaší síti. Obsah tohoto protokolu následně předává PRODUCT Serveru. Protokol naleznete ve složce:

- Windows
C:\ProgramData\ESET\Rogue Detection Sensor\Logs\detectedMachines.log

- Linux
/var/log/eset/RogueDetectionSensor/detectedMachines.log

Instalace ESET RD Sensor

ESET Rogue Detection Sensor můžete nainstalovat na Windows nebo Linux.

Požadavky

- Pouze pro Windows: WinPcap – použijte nejnovější verzi WinPcap (4.1.0 a novější)

- Síť musí být možné prohledávat (potřebujete mít otevřené porty, firewall nesmí blokovat příchozí komunikaci, atp.)

- Instance ESET PROTECT musí být dosažitelná

- Na lokálním počítači nainstalovaný ESET Management Agent pro správné fungování (reportování dat na Server)

V případě segmentovaných sítí je nutné Rogue Detection Sensor nainstalovat do každého segmentu, abyste získali komplexní seznam všech zařízení v celé síti.

instalace na Windows

Podle následujících kroků nainstalujte komponentu RD Sensor na Windows:

Ujistěte, že splňujete všechny výše uvedené požadavky pro instalaci.

1. Instalační balíčky ESET PROTECT pro individuální instalaci si stáhněte z webových stránek společnosti ESET ze sekce ESET PROTECT. (*rdsensor_x86.msi* nebo *rdsensor_x64.msi*).

2. Spusťte instalaci prostřednictvím instalačního balíčku.

3. Odsouhlaste licenční ujednání a pokračujte kliknutím na tlačítko **Další**.

4. Pokud souhlasíte se zasíláním informací o pádech a anonymních telemetrických dat do společnosti ESET (verze a typ operačního systému, verze produktu ESET a další informace související s produktem), zaškrtněte možnost **Zapojit se do programu vylepšování produktu**.

5. Vyberte umístění, kam chcete RD Sensor nainstalovat. Pokračujte kliknutím na tlačítko **Další** a instalaci zahajte kliknutím na tlačítko **Instalovat**.

6. ESET RD Sensor se po dokončení instalace automaticky spustí.

Protokol Rogue Detection Sensor naleznete ve složce: *C:\ProgramData\ESET\Rogue Detection Sensor\Logs*

Instalace na Linux

Podle následujících kroků nainstalujte komponentu RD Sensor na Linux pomocí příkazu v terminálu:

Ujistěte, že splňujete všechny výše uvedené požadavky pro instalaci.

1. Instalační balíčky ESET PROTECT pro individuální instalaci si stáhněte z webových stránek společnosti ESET ze sekce ESET PROTECT. (*rdsensor-linux-i386.sh* nebo *rdsensor-linux-x86_64.sh*).

2. Otevřete terminál a nastavte instalační balíček RD Sensor jako spustitelný: `chmod +x rdsensor-linux-x86_64.sh`

3. Spusťte instalaci prostřednictvím instalačního balíčku s oprávněním sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

4. Přečtěte si licenční ujednání s koncovým uživatelem. Pro pohyb na další stránku ujednání použijte klávesu **Mezerník**.
Následně se rozhodněte, zda s ujednáním souhlasíte. Pokud s ujednáním souhlasíte, stiskněte klávesu **Y**. V opačném případě stiskněte klávesu **N**.

5. Stisknutím klávesy **Y** odsouhlaste účast v programu vylepšování produktu. V opačném případě stiskněte klávesu **N**.

6. ESET RD Sensor se po dokončení instalace automaticky spustí.

7. Po dokončení instalace ověřte, zda služba běží pomocí příkazu:

```
sudo systemctl status rdsensor
```

Protokol Rogue Detection Sensor naleznete ve složce: */var/log/eset/RogueDetectionSensor/trace.log*

Konfigurace ESET Rogue Detection Sensor prostřednictvím politiky

Chování ESET RD Sensor můžete změnit prostřednictvím politiky. Nejčastěji uživatelé používají tuto možnost ke změně chování filtrování adres. Prostřednictvím politiky můžete například definovat adresy, které nechcete detekovat.

Pro vytvoření **politiky** přejděte v hlavním menu do sekce **Politiky** a upravte stávající nebo si vytvořte novou.

Filtry

IPv4 filtr

Zapnout filtrování IPv4 adres – aktivováním této možnosti (ne)bude komponenta detekovat pouze počítače z definovaných IPv4 rozsahů.

Filtry – rozhodněte se, zda chcete při detekci využívat seznam **povolených** nebo **blokovaných** adres.

Seznam **IPv4** adres – kliknutím na Změnit se zobrazí výše definovaný seznam adres.

Filtr prefixů **MAC** adres

Zapnout filtrování MAC **adres podle prefixu** – zapnutím filtrování budou detekovány pouze počítače, jejichž **MAC** adresy s prefixem (xx:xx:xx) se nachází v daném seznamu MAC adres, nebo pouze ty, které nejsou v seznamu blokovaných.

Režim filtrování – rozhodněte se, zda chcete při detekci využívat seznam **povolených** nebo **blokovaných** adres.

Seznam prefixů MAC adres – kliknutím na **Změnit** se zobrazí výše definovaný seznam **MAC** adres.

Detekce

Aktivní detekce – zapnutím této možnosti bude RD Sensor aktivně vyhledávat počítače v lokální síti. Tím můžete docílit většího počtu detekovaných zařízení, ale firewall na koncových stanicích může detekovat pokus o útok.

Detekce portů OS – RD Senzor využívá předkonfigurovaný seznam portů, na kterých vyhledává počítače v lokální síti. V případě potřeby si můžete seznam portů upravit.

Rozšířená nastavení

Zapojit se do programu vylepšování produktu – pomocí této možnosti se rozhodněte, zda chcete zasílat informace o pádech a anonymní telemetrická data do společnosti ESET (verze a typ operačního systému, verze produktu ESET a další informace související s produktem).

Přiřadit

Vyberte klienty, kterým chcete politiku přiřadit. Po kliknutí na tlačítko **Přiřadit** se zobrazí dialogové okno se všemi statickými i dynamickými skupinami. Vyberte klienty nebo skupiny, na které chcete politiku aplikovat, a klikněte na tlačítko **OK**.

Souhrn

Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**.

Lokální nasazení

Tento způsob je vhodný pro případ, kdy máte fyzicky přístup k dané stanici. Instalační balíček si můžete stáhnout například do sdílené složky, umístit si jej na výměnné médium nebo distribuovat e-mailem.

Instalační balíček je nutné spouštět pod uživatelem Administrator nebo uživatelem s oprávněním administrátora.

Tento způsob nasazení je vhodný pro malé sítě (do 50 počítačů), případně jej můžete využít při testování. Pro hromadné nasazení ESET Management Agenta doporučujeme používat doménovou politiku nebo SCCM.

Přejděte do sekce Instalační balíčky a vyberte požadovaný instalační balíček.

Lokálně můžete Agenta nasadit prostřednictvím:

- Instalačního balíčku agenta (a bezpečnostního produktu ESET) (Windows, macOS)
- Instalačního skriptu (Linux, macOS)

ESET Management Agent je předkonfigurovaný pro připojení k ESET PROTECT. Z tohoto důvodu jsou možnosti úprav v politice ESET Management agenta omezené.

Vytvoření Live Installer – Agent a bezpečnostní produkt ESET – Windows/macOS

Instalační balíček pro nasazení agenta a bezpečnostního produktu na Windows/macOS můžete vytvořit následujícími způsoby:

- V horní části klikněte na **Rychlé odkazy** > **Windows zařízení** nebo **macOS zařízení**
- V hlavním menu konzole přejděte do sekce **Instalační balíčky** a klikněte na **Vytvořit instalační balíček** a dále si vyberte platformu (**Windows** nebo **macOS**).
- Prohlídka ESET PROTECT

1. **Možnosti instalace a ochrany** – Vyberte tuto možnost, pokud chcete nastavit ochranu produktu již v průběhu instalace:

- Pouze pro Windows:

  oZapnout systém zpětné vazby ESET LiveGrid® (doporučujeme)

  oZapnout detekci potenciálně nechtěných aplikací – více informací naleznete v naší Databázi znalostí.

- Pokud souhlasíte se zasíláním informací o pádech a anonymních telemetrických dat do společnosti ESET (verze a typ operačního systému, verze produktu ESET a další informace související s produktem), zaškrtněte možnost **Zapojit se do programu vylepšování produktu**.

2. Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

3. Kliknutím na tlačítko **Stáhnout** zahajte stahování instalačního balíčku nebo si vyberte další možnosti pro distribuci instalačního balíčku.

Možnost **Přizpůsobit instalační balíček** můžete využít pro změnu parametrů balíčku:

4. **Distribuce** – **Stáhnout nebo odeslat instalační balíček, případně použít ESET Remote Deployment Tool** (Windows) nebo **Stáhnout nebo odeslat instalační balíček** (macOS).

Pokud jste vybrali jiný způsob instalace, postupujte dle odpovídajících pokynů:
- Nejprve nasadit agenta (instalační skript)
- Využít pro nasazení GPO nebo SCCM

5. **Obsah balíčku** – vyberte si jednu z níže uvedených možností:

- **Management Agent** – pokud v sekci **Komponenty** nevyberete žádnou jinou možnost, instalační balíček bude obsahovat pouze ESET Management Agenta. Tuto možnost vyberte v případě, kdy bezpečnostní produkt nainstalujete později nebo již je na stanici nainstalován.

- **Bezpečnostní produkt** – v balíčku bude bezpečnostní produkt a ESET Management Agent. Tuto možnost vyberte, pokud na stanici není instalován žádný bezpečnostní produkt ESET, a zároveň chcete na stanici nainstalovat také ESET Management agenta. Mějte na paměti, že v instalačním balíčku pro macOS není možné zrušit výběr bezpečnostního produktu ESET.

- Pouze pro Windows: **Full Disk Encryption** – zahrnuje instalátor ESET Full Disk Encryption. Tato možnost se zobrazí pouze s platnou licencí ESET Full Disk Encryption.

- Pouze pro Windows: **ESET Inspect Connector** – po vybrání této možnosti bude součástí instalační balíčku ESET Inspect Connector. Tato možnost se zobrazí pouze s platnou licencí ESET Inspect.

Chybějící zaškrtávací políčko produktu ESET

Pokud zaškrtávací políčko produktu ESET (**Full Disk Encryption** nebo **ESET Inspect Connector**) po výběru Nadřazené skupiny chybí nebo není automaticky zaškrtnuto, nemáte přidanou licenci produktu v ESET Business Accountnebo není přiřazená k lokalitě, případně společnosti ESET MSP Administrator, pro kterou jste vybrali Nadřazenou skupinu, i když máte přístupová práva k licenci. Přidání licence produktu ESET v lokalitě (v ESET Business Account) nebo společnosti (v ESET MSP Administrator). Poté se zpřístupní zaškrtávací políčko produktu ESET. Produkt ESET tak můžete zahrnout do instalačního programu.

6. Pokud souhlasíte se zasíláním informací o pádech a anonymních telemetrických dat do společnosti ESET

(verze a typ operačního systému, verze produktu ESET a další informace související s produktem), zaškrtněte možnost **Zapojit se do programu vylepšování produktu**.

7. **Nadřazená skupina** – vyberte nadřazenou skupinu, do které po nainstalování agenta dojde prostřednictvím webové konzole ESET PROTECT k umístění počítače.

- Vybrat můžete již existující nebo vytvořit novou statickou skupinu, do níž se zařízení umístí po nainstalování balíčku.

- Výběrem nadřazené skupiny přidáte do instalačního balíčky všechny politiky, které jsou na danou skupinu aplikované.

- Výběr nadřazené skupiny během vytváření instalačního programu nemá vliv na jeho umístění. Po vytvoření instalačního programu dojde k jeho umístění v uživatelském Přístupu skupiny. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

- Nadřazená skupina je povinná, pokud používáte ESET Business Account s Lokalitami nebo ESET MSP Administrator, a nepovinná, pokud používáte ESET Business Account bez Lokalit.

8. Přizpůsobit další nastavení

- Zadejte **název**, volitelně **popis**, šablony instalačního balíčku.
- Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
- **Počáteční konfigurace (volitelné)** – využijte tuto možnost pro uplatnění konfigurační politiky na ESET Management Agenta. V případě jejího využití klikněte na možnost **Vybrat**, a ze seznamu dostupných politik si vyberte vámi požadovanou. Pokud v seznamu nevidíte vyhovující politiku, vytvořte si novou politiku, a spusťte počáteční konfiguraci znovu.
- Pokud používáte HTTP Proxy (doporučujeme používat ESET Bridge), zaškrtněte políčko **Povolit nastavení HTTP Proxy** a nastavte Proxy (**Název serveru**, **Port**, **Uživatelské jméno** a **Heslo**) pro stažení instalačního programu přes Proxy. Nastavte také připojení ESET Management Agenta k Proxy, aby bylo možné přesměrovávat komunikaci mezi ESET Management Agentem a ESET PROTECT Serverem. Do pole **Název serveru** zadejte adresu stroje, na kterém běží HTTP Proxy. ESET Bridge standardně běží na portu 3128. V případě potřeby port změňte. Ujistěte se, že jste zadali port, který odpovídá konfiguraci HTTP Proxy (viz Politika pro ESET Bridge.

> Komunikační protokol používaný agentem pro spojení s ESET PROTECT Serverem nepodporuje autentifikaci. Pokud proxy řešení vyžaduje autentifikaci, komunikace mezi agenty a ESET PROTECT Serverem nebude funkční.

Možnost **Použít přímé spojení, pokud není dostupný proxy server** je předvybraná. Průvodce si toto nastavení vynutí jako záložní cestu pro instalaci – zaškrtnutí políčka nelze zrušit. Toto nastavení můžete zakázat pomocí Politiky ESET Management agenta:

- Při vytváření instalačního programu zahrňte politiku pro **Počáteční konfiguraci**.
- Po instalaci agenta ESET Management přiřaďte počítači politiku.

9. Klikněte na tlačítko **Dokončit** nebo **Nastavení produktu**.

10. Bezpečnostní produkt

a.Pro změnu předvybraného bezpečnostního produktu ESET a souvisejících informací klikněte na jeho název:
oVyberte si jiný kompatibilní bezpečnostní produkt ESET.
o Z rozbalovacího menu si vyberte **Jazyk**.
oDále zaškrtněte možnost **Rozšířené**. Standardně je vybrána nejnovější verze produktu. V případě potřeby si můžete vybrat starší verzi.
b. Pouze pro Windows: Vyberte tuto možnost, pokud chcete nastavit ochranu produktu již v průběhu instalace:
oZapnout systém zpětné vazby ESET LiveGrid® (doporučujeme)
oZapnout detekci potenciálně nechtěných aplikací – více informací naleznete v naší Databázi znalostí.
o**Umožnit v průběhu instalace změnu nastavení ochrany** – tuto možnost nedoporučujeme vybírat.

c.Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.
d.**Přizpůsobit další nastavení**:
o**Licence** – Po kliknutí si ze seznamu vyberte licenci, která se použije pro aktivaci produktu instalovaného na cílové zařízení. Touto licencí se aktivuje bezpečnostní produkt v průběhu instalace. V seznamu dostupných licencí nejsou zobrazené vypršelé (neplatné) a nadužívané licence (ve stavu **Chyby** nebo **Neaktuální**).
o**Konfigurace** – Volitelně můžete vybrat **Politiku**, která se na bezpečnostní produkt aplikuje již v průběhu instalace.
o Pouze pro Windows: **Spustit ESET AV Remover** – pokud integrujete tento nástroj do instalačního balíčku, při jeho spuštění dojde k vyhledávání a případnému odinstalování bezpečnostních řešení třetí stran.

Pouze pro Windows: Pokud jste v kroku 2 vybrali Full Disk Encryption nebo ESET Inspect Connector, můžete také změnit jejich nastavení.

Full Disk Encryption

a.Pro změnu předvybraného balíčku **ESET Full Disk Encryption** a souvisejících informací klikněte na jeho název:
o Z rozbalovacího menu si vyberte **Jazyk**.
oDále zaškrtněte možnost **Rozšířené**. Standardně je vybrána nejnovější verze produktu. V případě potřeby si můžete vybrat starší verzi.
b.Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.
c.**Konfigurace** – volitelně můžete vybrat politiku, která se na ESET Full Disk Encryption aplikuje již v průběhu instalace.
d.**Přizpůsobit další nastavení**:
o**Licence** – Po kliknutí si ze seznamu vyberte licenci, která se použije pro aktivaci produktu instalovaného na cílové zařízení. Touto licencí se aktivuje bezpečnostní produkt v průběhu instalace. V seznamu dostupných licencí nejsou zobrazené vypršelé (neplatné) a nadužívané licence (ve stavu **Chyby** nebo **Neaktuální**).

ESET Inspect Connector

Požadavky na ESET Inspect Connector:
- Pro aktivování ESET Inspect Connector musíte mít platnou na ESET Inspect.
- Na spravované stanici nainstalovaný kompatibilní bezpečnostní produkt ESET.

a.Pro změnu předvybraného balíčku **ESET Inspect** Connector a souvisejících informací klikněte na jeho název:
o Z rozbalovacího menu si vyberte **Jazyk**.
oDále zaškrtněte možnost **Rozšířené**. Standardně je vybrána nejnovější verze produktu. V případě potřeby si můžete vybrat starší verzi.

b.Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.
c.**Přizpůsobit další nastavení**:
o**Licence** – Po kliknutí si ze seznamu vyberte licenci, která se použije pro aktivaci produktu instalovaného na cílové zařízení. Touto licencí se aktivuje bezpečnostní produkt v průběhu instalace. V seznamu dostupných licencí nejsou zobrazené vypršelé (neplatné) a nadužívané licence (ve stavu **Chyby** nebo **Neaktuální**).
o**Konfigurace** – kliknutím na **Vybrat** vyberte existující politiku pro ESET Inspect Connector, případně si **vytvořte** novou. Politika se aplikuje v průběhu instalace ESET Inspect Connector.
11. Klikněte na tlačítko **Dokončit**.

12. Live Installer Balíček můžete distribuovat několika způsoby:

- Kliknutím na ikonu si zkopírujte do schránky odkaz ke stažení balíčku, který zašlete uživatelům. Ti si následně balíček Live Installer stáhnou a nainstalují.

- Kliknutím na možnost **Stáhnout** si balíček Live Installer stáhněte na své zařízení a následně osobně spusťte na cílové stanici nebo nahrajte do sdílené složky, do níž mají uživatelé přístup.

- Pouze pro Windows: Pro vzdálené nasazení balíčku Live Installer použijte ESET Remote Deployment Tool.

- Kliknutím na ikonu ESET PROTECT použije SMTP server pro doručení e-mailu, ve kterém uživatelů naleznou odkaz na stažení balíčku Live Installer.

  oPro přidání příjemce klikněte na **Přidat**, do pole **E-mailová adresa** zadejte adresu uživatele a potvrďte stisknutím klávesy **Enter** nebo klikněte na ikonu . Volitelně můžete kliknout na **Vytvořit uživatele**, následně zadejte **jméno** uživatele a klikněte na **Uložit**. Detaily uživatele můžete posléze změnit v sekci Uživatelé zařízení. Klikněte na **Zobrazit náhled e-mailu**, pomocí kontextového menu vyberte **Jazyk e-mailu** a klikněte na **Uložit**.

  oUživatele můžete přidat hromadně následujícími způsoby: klikněte na **Další** > **Přidat uživatele** (tím můžete vybrat e-mailové adresy uživatelů definovaných v sekci Uživatelé zařízení) nebo na **Další** > **Importovat CSV** / **Vložit ze schránky** (kdy můžete seznam adres importovat z CSV souboru, případně vlastní datové struktury).

Vytvořený Live Installer balíček se bude chovat a měnit automaticky dle kroků uvedených v této tabulce.
Live Installer vyžaduje připojení k internetu a není možné jej použít na offline počítači.
Live Installer pro macOS vyžaduje přímé připojení k internetu (na servery společnosti ESET). Není možné jej použít na macOS stanicích, které jsou k internetu připojeny prostřednictvím proxy serveru.

ESET PROTECT podporuje automatickou aktualizaci ESET Management agentů ve spravovaných počítačích.

13. Stažený instalační balíček spusťte na klientské stanici. Live Installer stáhne ESET Management Agenta a bezpečnostní produkt ESET kompatibilní s vaší platformou (x86, x64 nebo ARM64). Následně se na zařízení nainstaluje ESET Management Agent, bezpečnostní produkt ESET a dojde k jeho připojení do ESET PROTECT. Instalační balíček ESET Endpoint Antivirus/Security vytvořený v ESET PROTECT podporuje Windows 10 Enterprise for Virtual Desktop a Windows 10 pro více relací. Pro více informací týkajících se instalace přejděte do kapitoly průvodce instalaci (Windows nebo macOS).

Chování Live Installer

Po vytvoření se Live Installer uloží do vaší instance ESET PROTECT a bude se chovat dle informací uvedených v tabulce níže.

Akce	Chování odkazu pro stažení Live Installer	Chování staženého balíčku Live Installer
Smazání Live Installer z ESET PROTECT	Odkaz nebude k dispozici	Stažené kopie Live Installer přestanou fungovat
Live Installer se již nenachází v repozitáři	Odkaz nebude k dispozici V instalačním balíčku se zobrazí informace: **Vybraný balíček není v repozitáři dostupný**	Stažené kopie Live Installer přestanou fungovat
Dojde ke změně politiky, která je součástí Live Installer	Změna politiky neovlivní existující kopie Live Installer. Odkaz pro stažení bude stále směrovat na balíček s politikou z doby jeho vytvoření. Pokud chceme změny promítnout tak do instalačního balíčku, vytvořte si nové s vámi změněnou politikou.	Instalační balíček bude funkční, ale produkt ESET bude v konfiguraci, kterou jste definovali v době vytvoření balíčku.
Dojde k odstranění politiky, která je součástí Live Installer	Vedle instalačního balíčku se zobrazí informace: **Použitá politika není dostupná**, balíček nebude možné stáhnout. Si vytvořit kopii instalačního balíčku a přiřadit mu novou politiku.	Stažené kopie Live Installer přestanou fungovat
Dojde ke změně skupiny, která je použitá v Live Installer		Tato změna neovlivní existující instalační balíčky a počítač se po připojení k ESET PROTECT zařadí do aktualizované/přejmenované skupině.
Dojde k odstranění skupiny, která je použitá v Live Installer		Instalační balíček se zachová stejně, jako kdyby neměl k dispozici informaci o cílové skupině. Počítač se zařadí do výchozí skupiny **Ztráty a nálezy**.

Akce	Chování odkazu pro stažení Live Installer	Chování staženého balíčku Live Installer
Životnost Live Installer	Instalační balíčky Live Installer jsou platné 6 měsíců od svého vytvoření. Pro aktualizování odkazu pro stažení existujícího instalačního balíčku přejděte do sekce **Instalační balíčky**, vyberte požadovaný balíček a v kontextovém menu klikněte na možnost **Zobrazit odkaz ke stažení**. Platný instalační balíček si stáhněte prostřednictvím nového odkazu.	

Vytvoření instalačního skriptu agenta – Linux/macOS

Tento způsob instalace agenta je vhodný pro případ, kdy vám nevyhovují jiné metody instalace, případně je nemůžete použít. V tomto případě můžete uživatelům distribuovat instalační skript například prostřednictvím e-mailu nebo výměnných médií, a nechat instalaci na nich. Instalace prostřednictvím instalačního skriptu je bezobslužná, ale uživatel musí mít oprávnění administrátora.

Instalační skript agenta pro macOS/Linux můžete vytvořit následujícími způsoby:

- V horní části klikněte na **Rychlé odkazy** > **macOS zařízení** nebo **Linux zařízení**

- V hlavním menu konzole přejděte do sekce **Instalační balíčky** a klikněte na **Vytvořit instalační balíček** a dále si vyberte platformu (**macOS** nebo **Linux**).

- Prohlídka ESET PROTECT

Klikněte na možnost **Přizpůsobit instalační balíček** a dále vyberte možnost **Nejprve nasadit agenta (instalační skript)**.

1. Pokud souhlasíte se zasíláním informací o pádech a anonymních telemetrických dat do společnosti ESET (verze a typ operačního systému, verze produktu ESET a další informace související s produktem), zaškrtněte možnost **Zapojit se do programu vylepšování produktu**.

2. **Nadřazená skupina** – vyberte nadřazenou skupinu, do které po nainstalování agenta dojde prostřednictvím webové konzole ESET PROTECT k umístění počítače.

- Vybrat můžete již existující nebo vytvořit novou statickou skupinu, do níž se zařízení umístí po nainstalování balíčku.

- Výběrem nadřazené skupiny přidáte do instalačního balíčky všechny politiky, které jsou na danou skupinu aplikované.

- Výběr nadřazené skupiny během vytváření instalačního programu nemá vliv na jeho umístění. Po vytvoření instalačního programu dojde k jeho umístění v uživatelském Přístupu skupiny. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

- Nadřazená skupina je povinná, pokud používáte ESET Business Account s Lokalitami nebo ESET MSP Administrator, a nepovinná, pokud používáte ESET Business Account bez Lokalit.

3. Přizpůsobit další nastavení

- Zadejte **název**, volitelně **popis**, šablony instalačního balíčku.
- Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
- **Počáteční konfigurace (volitelné)** – využijte tuto možnost pro uplatnění konfigurační politiky na ESET Management Agenta. V případě jejího využití klikněte na možnost **Vybrat**, a ze seznamu dostupných politik si vyberte vámi požadovanou. Pokud v seznamu nevidíte vyhovující politiku, vytvořte si novou politiku, a spusťte počáteční konfiguraci znovu.
- Pokud používáte HTTP Proxy (doporučujeme používat ESET Bridge), zaškrtněte políčko **Povolit nastavení HTTP Proxy** a nastavte Proxy (**Název serveru**, **Port**, **Uživatelské jméno** a **Heslo**) pro stažení instalačního programu přes Proxy. Nastavte také připojení ESET Management Agenta k Proxy, aby bylo možné přesměrovávat komunikaci mezi ESET Management Agentem a ESET PROTECT Serverem. Do pole **Název serveru** zadejte adresu stroje, na kterém běží HTTP Proxy. ESET Bridge standardně běží na portu 3128. V případě potřeby port změňte. Ujistěte se, že jste zadali port, který odpovídá konfiguraci HTTP Proxy (viz Politika pro ESET Bridge.

> Komunikační protokol používaný agentem pro spojení s ESET PROTECT Serverem nepodporuje autentifikaci. Pokud proxy řešení vyžaduje autentifikaci, komunikace mezi agenty a ESET PROTECT Serverem nebude funkční.

Možnost **Použít přímé spojení, pokud není dostupný proxy server** je předvybraná. Průvodce si toto nastavení vynutí jako záložní cestu pro instalaci – zaškrtnutí políčka nelze zrušit. Toto nastavení můžete zakázat pomocí Politiky ESET Management agenta:

- Při vytváření instalačního programu zahrňte politiku pro **Počáteční konfiguraci**.
- Po instalaci agenta ESET Management přiřaďte počítači politiku.

4. Klikněte na tlačítko **Uložit a stáhnout**.

5. Stažený archiv rozbalte na klientovi, na kterém chcete instalovat ESET Management Agenta.

6. Spuštěním skriptu *PROTECTAgentInstaller.sh* (Linux nebo macOS) zahajte instalaci agenta. Postupujte podle kroků uvedených v následujících kapitolách:

- Nasazení agenta na Linux
- Nasazení agenta na macOS

> ESET PROTECT podporuje automatickou aktualizaci ESET Management agentů ve spravovaných počítačích.

Nasazení z vlastního síťového umístění

Pro nasazení agenta z vlastního repozitáře upravte instalační skript a nahraďte v něm odkaz ke stažení instalačního balíčku. Použít můžete název serveru nebo IP adresu.
Najděte a upravte následující řádky:
Linux:

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-i386.sh
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-x86_64.sh
```

macOS:

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_macosx_x86_64.dmg
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-macosx-x86_64_arm64.dmg
```

Nasazení agenta na Linux

Požadavky

- Přímá viditelnost na Server.
- Doporučujeme vždy **používat nejnovější verzi OpenSSL 1.1.1**. ESET Management Agent rovněž podporuje OpenSSL 3.x. Minimální podporována verze OpenSSL je openssl-1.0.1e-30. Nainstalováno můžete mít více verzí OpenSSL. Nicméně alespoň jedna z nich musí podporovaná.
    - Příkazem `openssl version` si zobrazíte aktuálně používanou (výchozí) verzi.
    - Zobrazit si můžete seznam všech verzí OpenSSL ve vašem systému. Po použití příkazu `sudo find / -iname *libcrypto.so*` se podívejte na konce názvů souborů.
    - Kompatibilitu na linuxu ověříte následujícím příkazem: `openssl s_client -connect google.com:443 -tls1_2`
- Aby ESET Management Agent dokázal korektně reportovat data o hardwaru z linuxových stanic/serverů, musí být na nich nainstalován nástroj `lshw`.

Linuxové distribuce	Terminálový příkaz
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- Na operačním systému CentOS doporučujeme dále nainstalovat balíček `policycoreutils-devel`. To provedete příkazem:

```
yum install policycoreutils-devel
```

Instalace

Ruční instalaci ESET Management Agenta na linuxu provedete prostřednictvím Terminálu.

> Komunikační protokol používaný agentem pro spojení s ESET PROTECT Serverem nepodporuje autentifikaci. Pokud proxy řešení vyžaduje autentifikaci, komunikace mezi agenty a ESET PROTECT Serverem nebude funkční.

Pro nasazení agenta na linuxovou stanici postupujte podle níže uvedených kroků.

1. Stáhněte si instalační skript agenta na klientskou stanici.
2. Z *.gz* archivu si rozbalte *.sh* soubor, příkazem `tar -xvzf PROTECTAgentInstaller.tar.gz`
3. Instalační balíček ESET Management Agenta musí být nastaven jako spustitelný. To provedete příkazem: `chmod +x PROTECTAgentInstaller.sh`
4. Spusťte *.sh* soubor přímo nebo pomocí Terminálu příkazem: `sudo ./PROTECTAgentInstaller.sh`.
5. Po zobrazení výzvy zadejte heslo ke svému uživatelského účtu a potvrzením klávesou **Enter** pokračujte v instalaci.
6. Po dokončení instalace ověřte, zda služba Agenta běží příkazem: `sudo systemctl status eraagent`

7. Po nainstalování agenta se počítač zobrazí v ESET PROTECT a můžete jej začít vzdáleně spravovat pomocí webové konzole.

Pokud se počítač s nainstalovaným agentem neobjeví ve vašem seznamu ESET PROTECT, proveďte řešení potíží.

ESET PROTECT podporuje automatickou aktualizaci ESET Management agentů ve spravovaných počítačích.

Nasazení agenta na macOS

1. Stáhněte si instalační skript agenta na klientskou stanici.

2. Dvojklikem na stažený archiv *PROTECTAgentInstaller.tar.gz* z něj rozbalte soubor *PROTECTAgentInstaller.sh* a uložte si jej na Plochu.

3. Klikněte na **Přejít** > **Utility** a dvojklikem na položku Terminál si otevřete nové okno Terminálu.

4. Povolení úplného přístupu k disku pro Terminál:

   a)Otevřete si **Předvolby systému** a přejděte do sekce **Zabezpečení a soukromí** > **Soukromí**.

   b)Abyste mohli provádět změny v nastavení, kliknutím v levém dolním rohu na ikonu zámku.

   c)Klikněte na **Úplný přístup k disku**.

   d)Klikněte na **+** > **Aplikace** > a přidejte **Terminál** do seznamu aplikací ve složce **Úplný přístup k disku**.

   e)Pro uzamčení nastavení klikněte v levém dolním rohu na ikonu zámku.

5. V novém okně terminálu spusťte následující příkazy:

```
cd Desktop
sudo bash PROTECTAgentInstaller.sh
```

6. Po zobrazení výzvy zadejte heslo ke svému uživatelského účtu a potvrzením klávesou **Enter** pokračujte v instalaci.

7. Povolení úplného přístupu k disku:

Lokálně:

   a)Otevřete si **Předvolby systému** a přejděte do sekce **Zabezpečení a soukromí** > **Soukromí**.

   b)Abyste mohli provádět změny v nastavení, kliknutím v levém dolním rohu na ikonu zámku.

   c)Klikněte na **Úplný přístup k disku**.

   d)Klikněte na tlačítko **+** > **Aplikace** > **ESET** > **Otevřít** a přidejte ESET Management Agenta do seznamu aplikací ve složce **Úplný přístup k disku**.

e)Pro uzamčení nastavení klikněte v levém dolním rohu na ikonu zámku.

Vzdáleně:

a)Stáhněte si .plist konfigurační soubor.

b)Vygenerujte si dvě UUID v libovolném generátoru UUID. Pomocí textového editoru nahraďte ve staženém konfiguračním profilu řetězce. Vložte vámi vygenerované UUID 1 a UUID 2 do staženého konfiguračního profilu.

c)Nasaďte .plist konfigurační profil prostřednictvím svého MDM serveru. Aby si počítače převzali konfiguraci, musí být registrovány k MDM serveru.

8. Po nainstalování agenta se počítač zobrazí v ESET PROTECT a můžete jej začít vzdáleně spravovat pomocí webové konzole.

ESET Management Agent od verze 9.1 nativně podporuje ARM64 zařízení s macOS; na tato zařízení se nainstaluje jeho ARM64 verze.
ESET PROTECT podporuje automatickou aktualizaci ESET Management agentů ve spravovaných počítačích.

Instalace agenta a řešení problémů

Po dokončení instalace ověřte, zda služba Agenta běží: Klikněte na **Přejít** > **Utility** a následně dvojklikem otevřete položku **Monitor aktivit**. Přejděte na záložku **Energie** nebo **CPU** a vyhledejte proces s názvem **ERAAgent**.

Protokoly ESET Management Agenta naleznete ve složce:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

Komunikační protokol používaný agentem pro spojení s ESET PROTECT Serverem nepodporuje autentifikaci. Pokud proxy řešení vyžaduje autentifikaci, komunikace mezi agenty a ESET PROTECT Serverem nebude funkční.

Vzdálené nasazení

Při nasazování ESET_MNG Agenta prostřednictvím serverové úlohy se ujistěte, že má PRODUCT Server i cílová stanice přístup k internetu.

Agenta můžete nasadit vzdáleně prostřednictvím:

- ESET Remote Deployment Tool – pomocí tohoto nástroje můžete nasadit all-in-one instalační balíček ESET Management Agenta i bezpečnostního řešení ESET vytvořený v ESET PROTECT Web Console.

- Doménové politiky (GPO) nebo Software Center Configuration Manager (SCCM) – Tuto možnost doporučujeme pro nasazení ESET Management Agenta na velké množství počítačů.

Pokud se vzdálené nasazení ESET Management Agent nezdařilo, případně agent nekomunikuje se serverem, pro odstranění problému přejděte do kapitoly Řešení problémů – Agent se nepřipojuje.

Nasazení Agenta prostřednictvím GPO nebo SCCM

Agenta můžete nasadit lokálně, vzdáleně, nebo využít doménovou politiku (GPO) či nástroje určené pro hromadné nasazení aplikací – například SCCM, Symantec Altiris či Puppet.

Při nasazování ESET_MNG Agenta prostřednictvím serverové úlohy se ujistěte, že má PRODUCT Server i cílová stanice přístup k internetu.

GPO/SCCM skript pro nasazení agenta na Windows můžete vytvořit po kliknutí na **Rychlé odkazy** > **Windows zařízení** nebo v sekci **Instalační balíčky** > **Vytvořit instalační balíček**.

1. Jako platformu vyberte Windows**Windows** > **Přizpůsobit instalační balíček** a **Využít pro nasazení GPO nebo SCCM**.

2. Pokud souhlasíte se zasíláním informací o pádech a anonymních telemetrických dat do společnosti ESET (verze a typ operačního systému, verze produktu ESET a další informace související s produktem), zaškrtněte možnost **Zapojit se do programu vylepšování produktu**.

3. **Nadřazená skupina** – vyberte nadřazenou skupinu, do které po nainstalování agenta dojde prostřednictvím webové konzole ESET PROTECT k umístění počítače.

   • Vybrat můžete již existující nebo vytvořit novou statickou skupinu, do níž se zařízení umístí po nainstalování balíčku.

   • Výběrem nadřazené skupiny přidáte do instalačního balíčky všechny politiky, které jsou na danou skupinu aplikované.

   • Výběr nadřazené skupiny během vytváření instalačního programu nemá vliv na jeho umístění. Po vytvoření instalačního programu dojde k jeho umístění v uživatelském Přístupu skupiny. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

   • Nadřazená skupina je povinná, pokud používáte ESET Business Account s Lokalitami nebo ESET MSP Administrator, a nepovinná, pokud používáte ESET Business Account bez Lokalit.

4. Přizpůsobit další nastavení

- Zadejte **název**, volitelně **popis**, šablony instalačního balíčku.
- Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
- **Počáteční konfigurace (volitelné)** – využijte tuto možnost pro uplatnění konfigurační politiky na ESET Management Agenta. V případě jejího využití klikněte na možnost **Vybrat**, a ze seznamu dostupných politik si vyberte vámi požadovanou. Pokud v seznamu nevidíte vyhovující politiku, vytvořte si novou politiku, a spusťte počáteční konfiguraci znovu.
- Pokud používáte HTTP Proxy (doporučujeme používat ESET Bridge), zaškrtněte políčko **Povolit nastavení HTTP Proxy** a nastavte Proxy (**Název serveru**, **Port**, **Uživatelské jméno** a **Heslo**) pro stažení instalačního programu přes Proxy. Nastavte také připojení ESET Management Agenta k Proxy, aby bylo možné přesměrovávat komunikaci mezi ESET Management Agentem a ESET PROTECT Serverem. Do pole **Název serveru** zadejte adresu stroje, na kterém běží HTTP Proxy. ESET Bridge standardně běží na portu 3128. V případě potřeby port změňte. Ujistěte se, že jste zadali port, který odpovídá konfiguraci HTTP Proxy (viz Politika pro ESET Bridge.

  Komunikační protokol používaný agentem pro spojení s ESET PROTECT Serverem nepodporuje autentifikaci. Pokud proxy řešení vyžaduje autentifikaci, komunikace mezi agenty a ESET PROTECT Serverem nebude funkční.

  Možnost **Použít přímé spojení, pokud není dostupný proxy server** je předvybraná. Průvodce si toto nastavení vynutí jako záložní cestu pro instalaci – zaškrtnutí políčka nelze zrušit. Toto nastavení můžete zakázat pomocí Politiky ESET Management agenta:
  - Při vytváření instalačního programu zahrňte politiku pro **Počáteční konfiguraci**.
  - Po instalaci agenta ESET Management přiřaďte počítači politiku.

5. Klikněte na tlačítko **Dokončit**.

6. Stáhněte si GPO/SCCM skript a instalační balíčky agenta (32-bit, 64-bit, ARM64). Alternativně si instalační *.msi* balíčky agenta můžete stáhnout z webových stránek společnosti ESET.

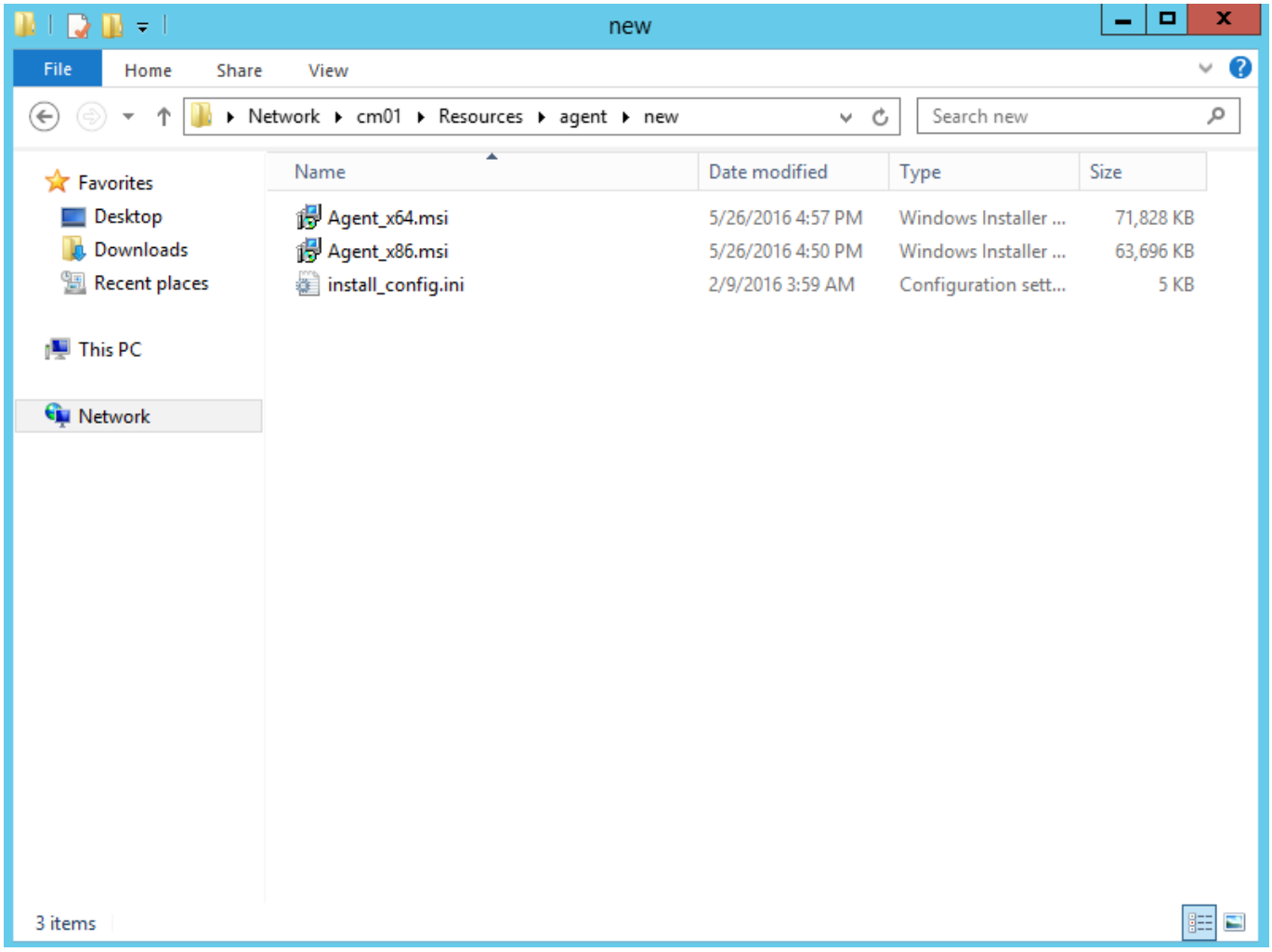
Kliknutím na jeden z níže uvedený odkazů si zobrazíte návod krok za krokem pro nasazení ESET Management Agenta:

- Nasadit ESET Management Agenta prostřednictvím GPO (Group Policy Object) – Články v databázi znalostí nemusí být dostupné ve vašem jazyce.
- Nasadit ESET Management Agent prostřednictvím SCCM (Software Center Configuration Manager)

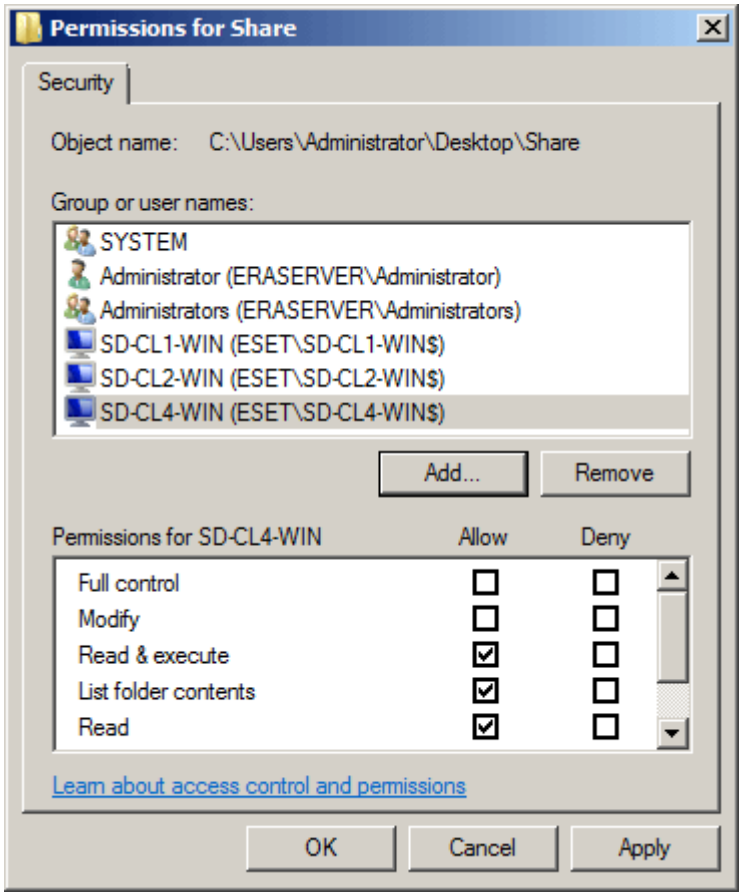
Nasazení prostřednictvím SCCM

Pro nasazení ESET Management Agenta prostřednictvím SCCM postupujte podle níže uvedených kroků:

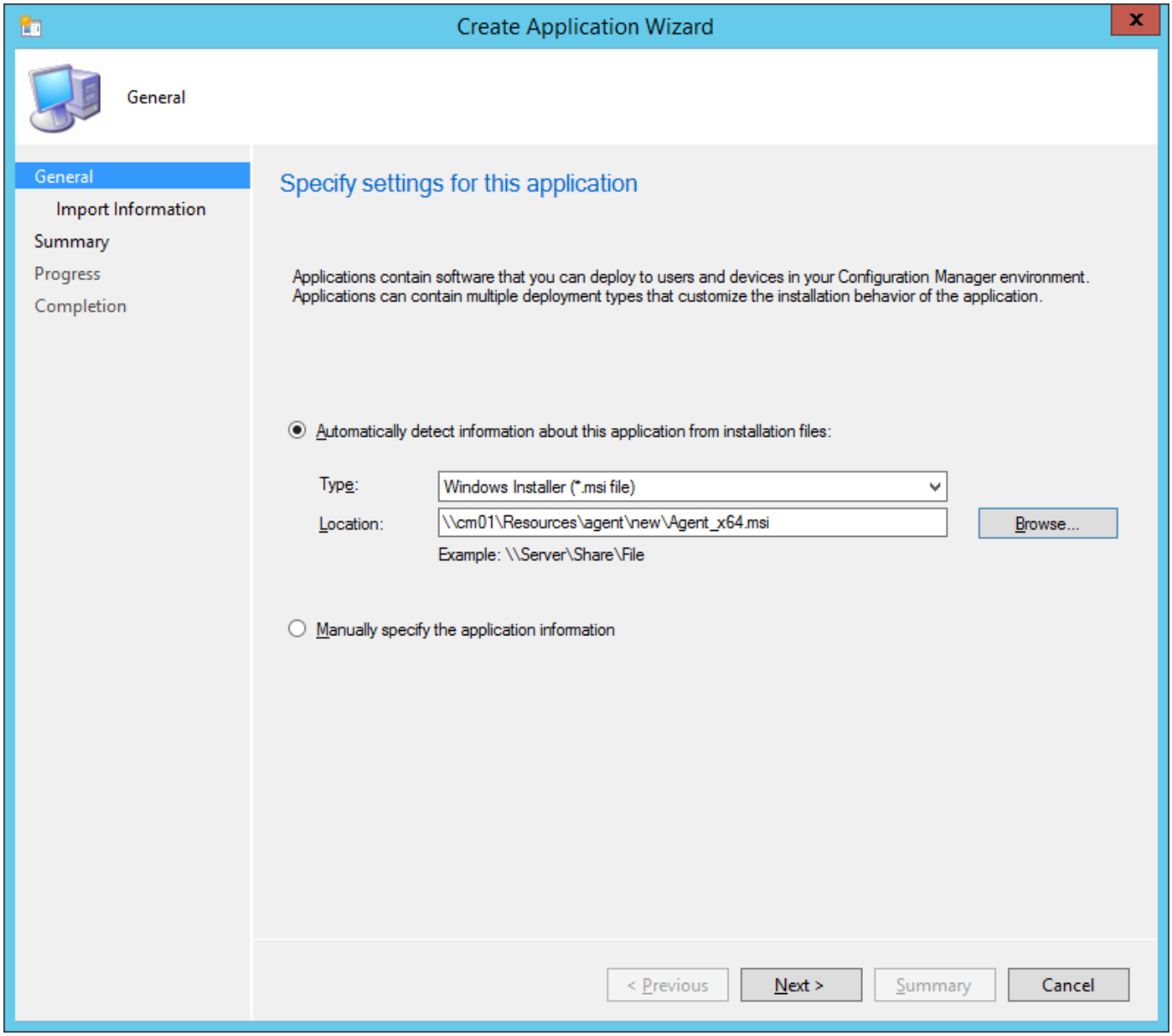
1. Umístěte instalační *.msi* balíček ESET Management Agenta a konfigurační soubor *install_config.ini*do sdílené složky.



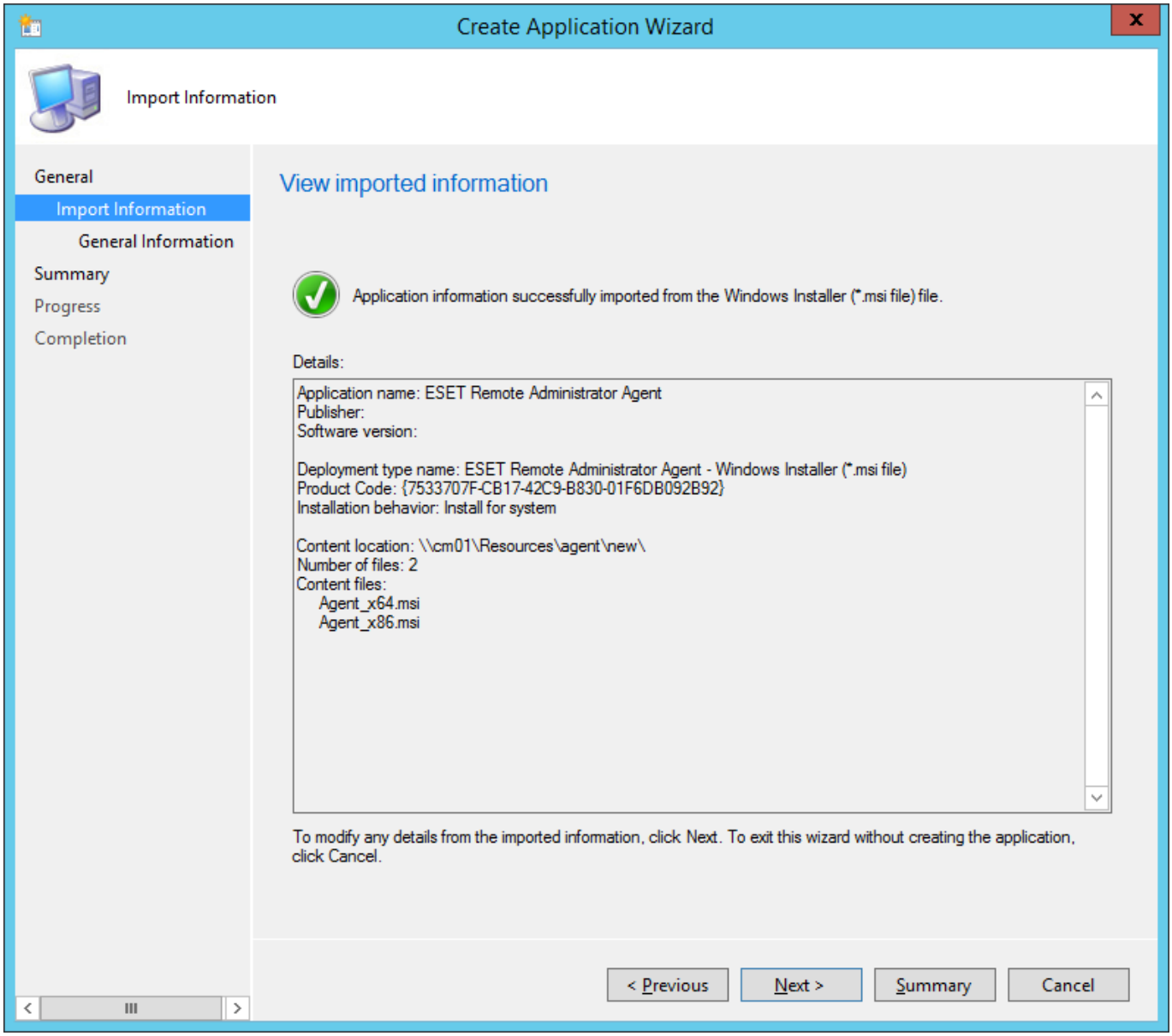
Klientská stanice (nikoli uživatel) musí mít oprávnění pro čtení i zápis do této sdílené složky.



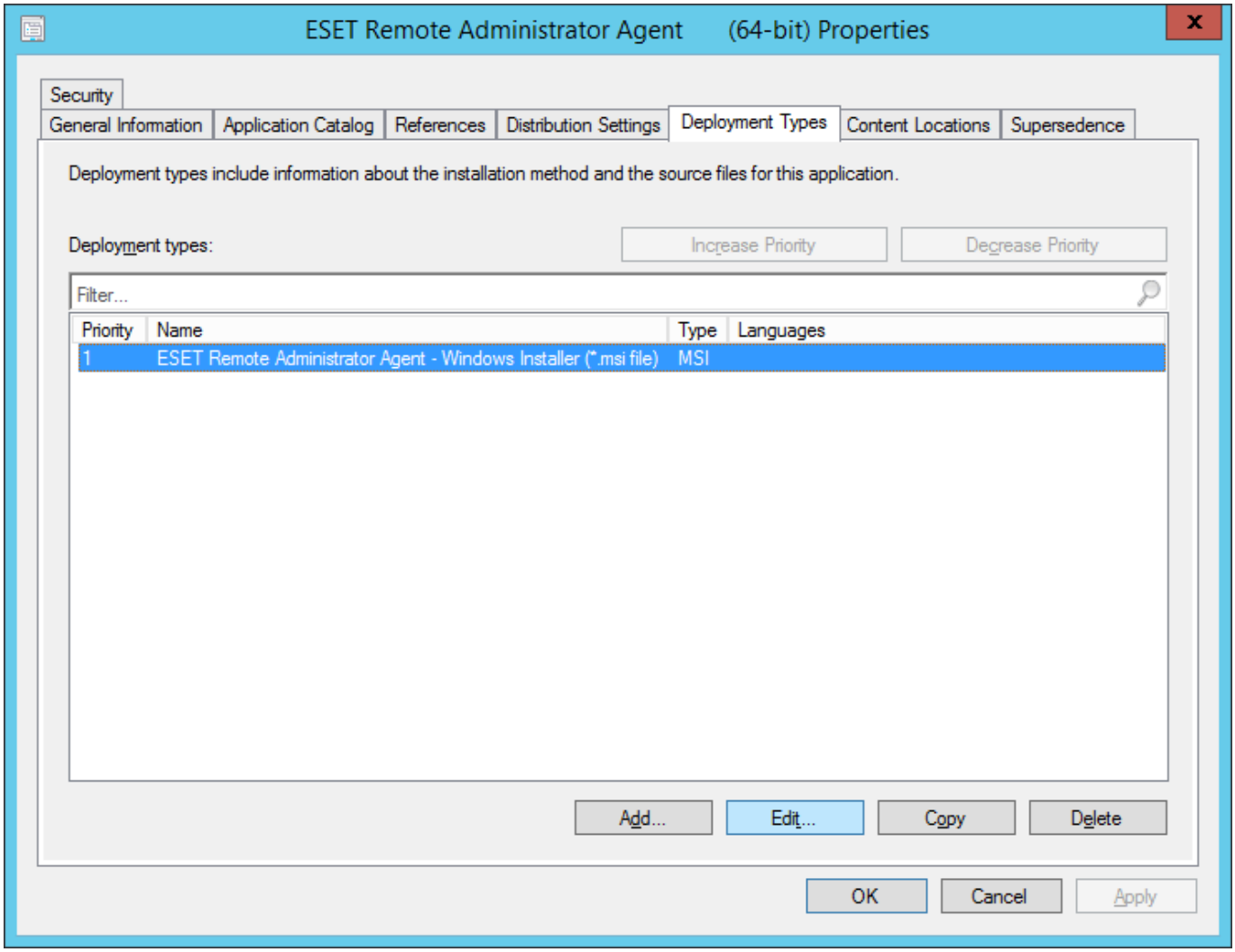
2. Otevřete SCCM konzoli a klikněte na **Software Library**. V části **Application Management** klikněte pravým tlačítkem na **Applications** a vyberte možnost **Create Application**. Vyberte možnost **Windows Installer (*.msi file)**.



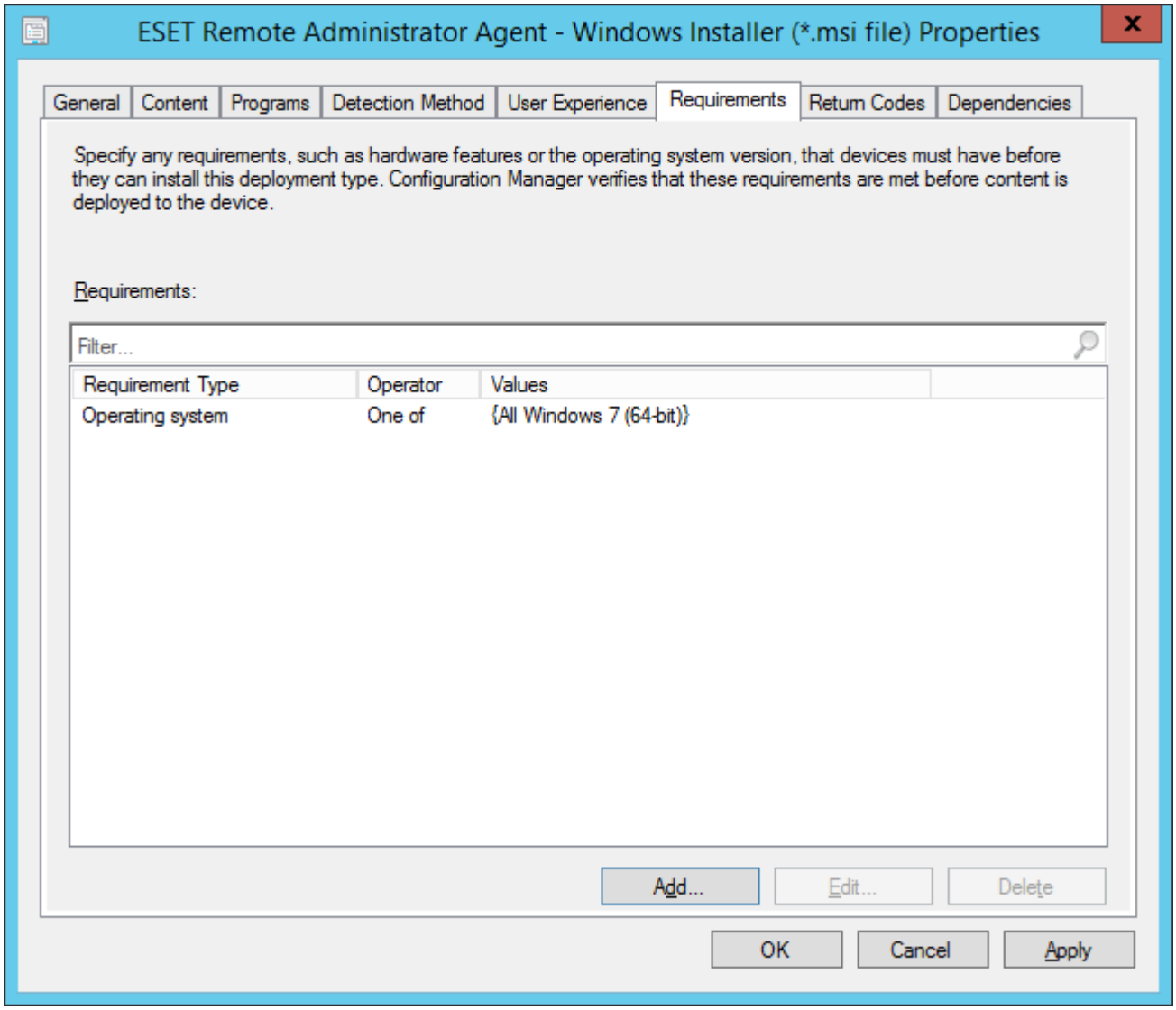
3. Zadejte všechny vyžadované informace o aplikaci a klikněte na tlačítko **Next**.

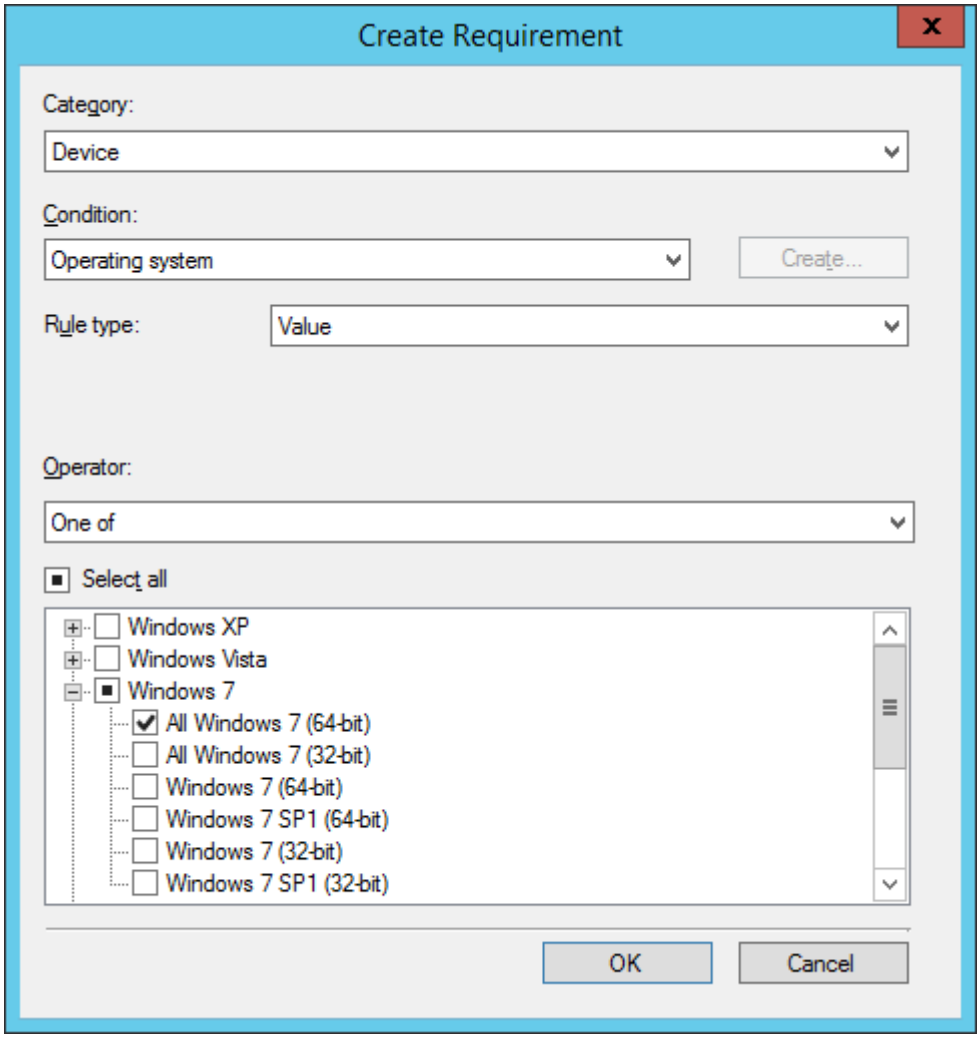


4. Pravým tlačítkem myši klikněte na aplikaci ESET Management Agent, přejděte na záložku **Deployment Types**, vyberte možnost **only deployment** a klikněte na tlačítko Edit.

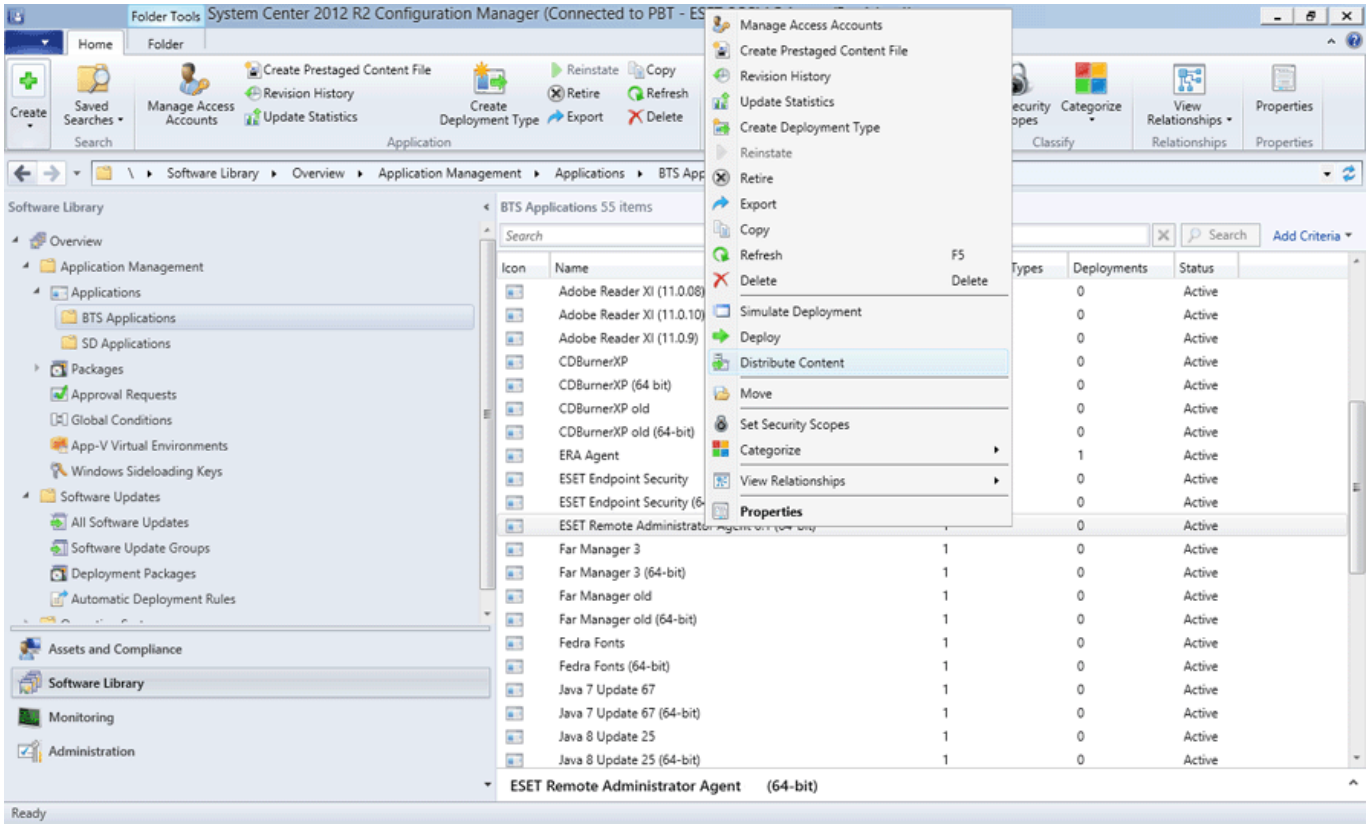


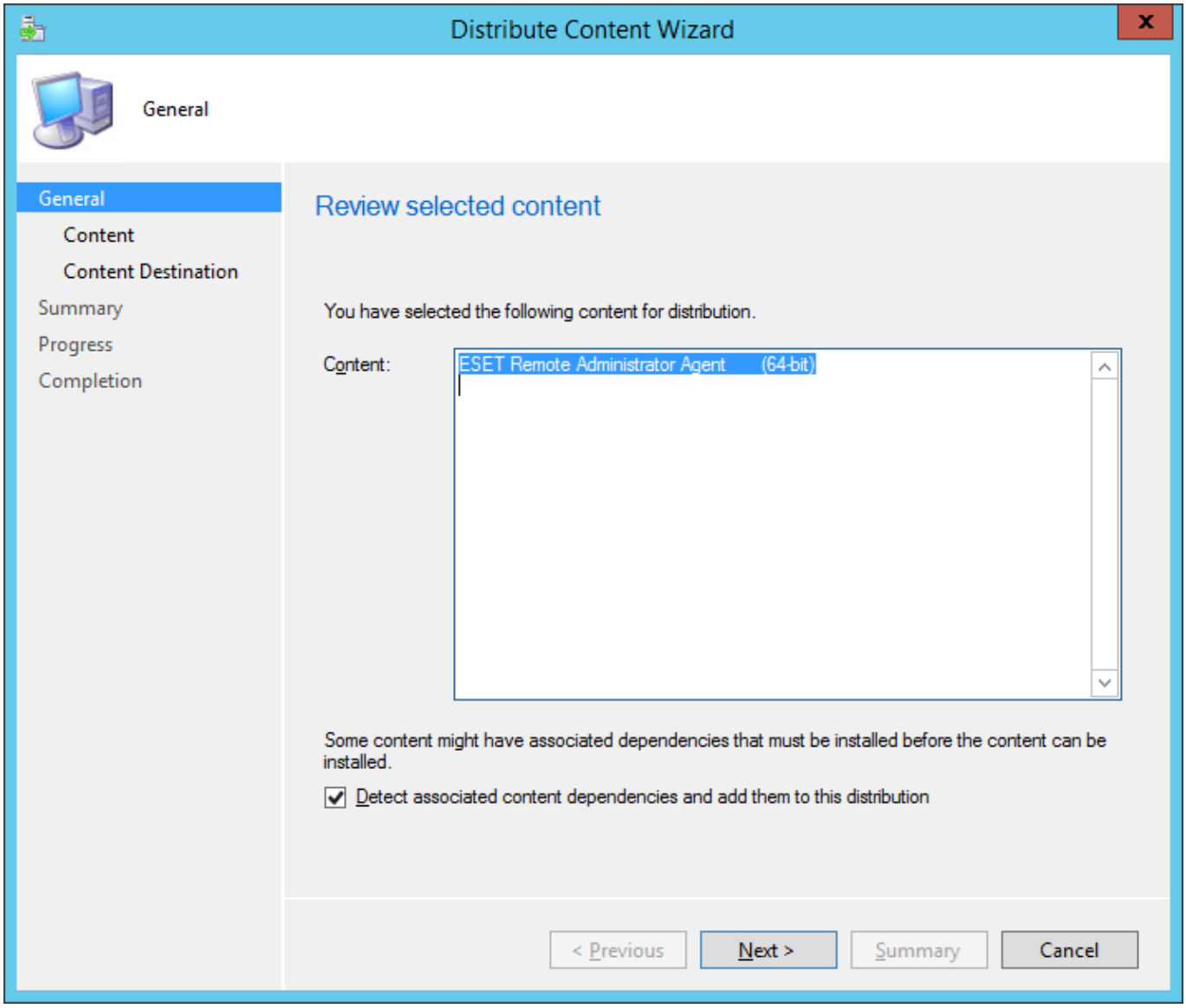
5. Přejděte na záložku **Requirements** a klikněte na tlačítko **Add**. Z rozbalovacího menu **Condition** vyberte možnost **Operating system**, jako **Operator** vyberte **One of** a definujte operační systémy, na které chcete balíček instalovat. Konfiguraci dokončete kliknutím na **OK**.

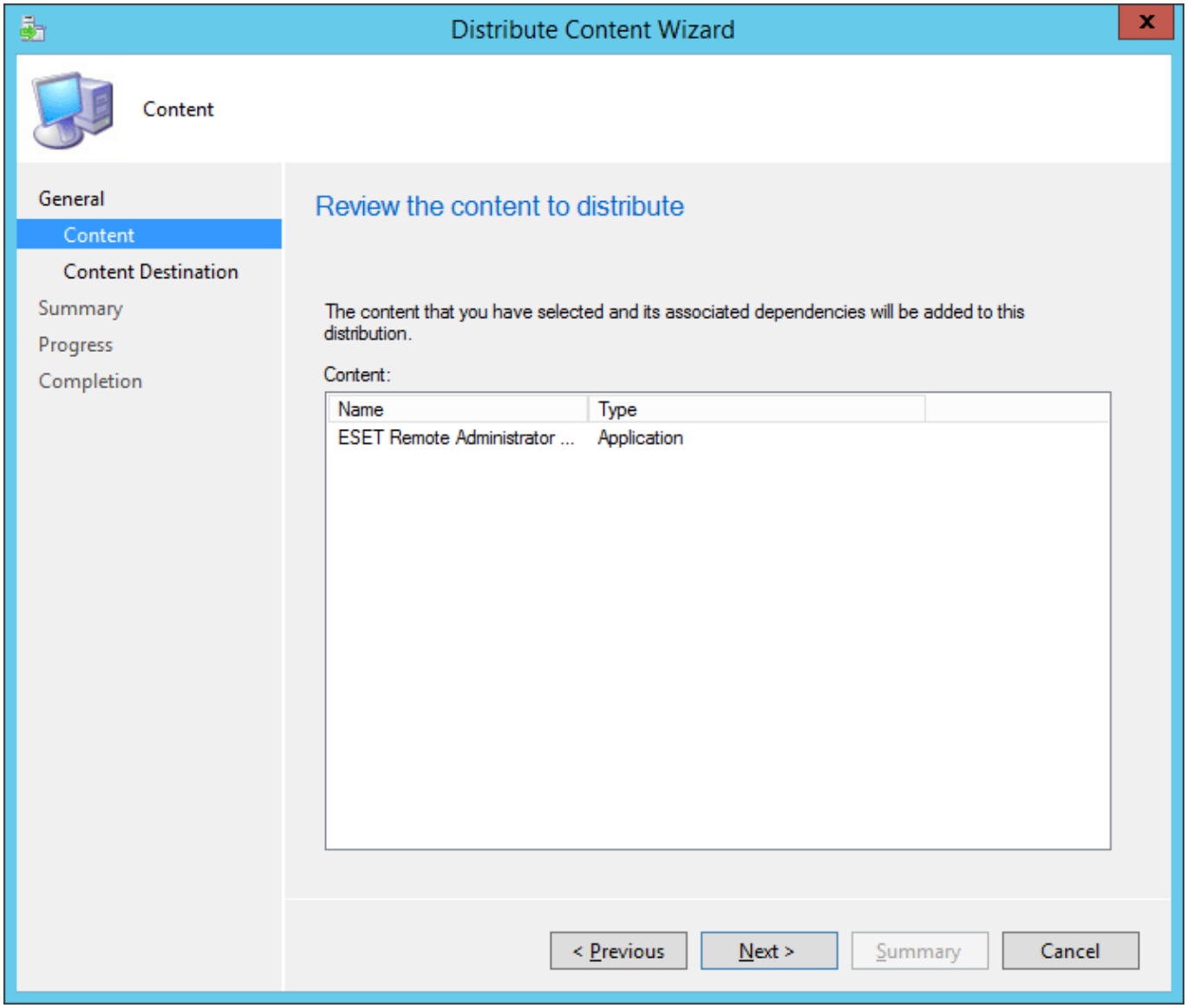

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply



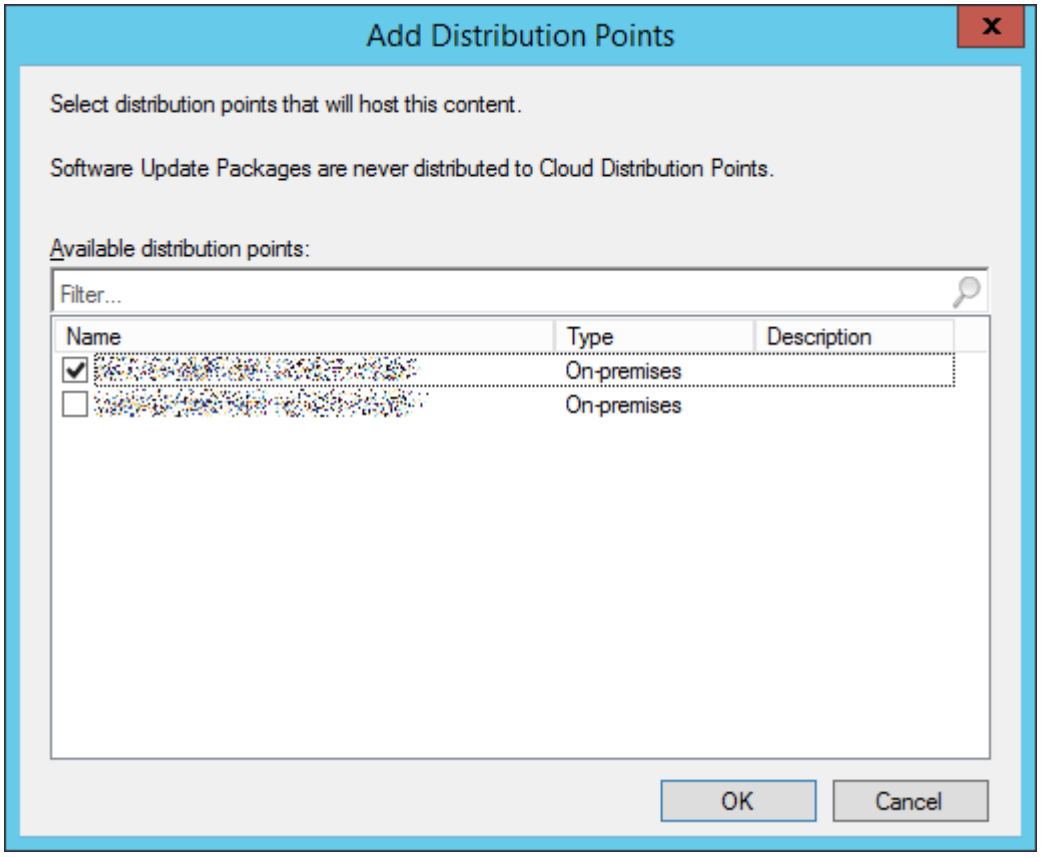
6. V System Center Software Library klikněte pravým tlačítkem na vámi nově vytvořenou aplikaci a z kontextového menu vyberte možnost **Distribute Content**. Dále postupujte podle kroků v průvodci nasazením aplikace.

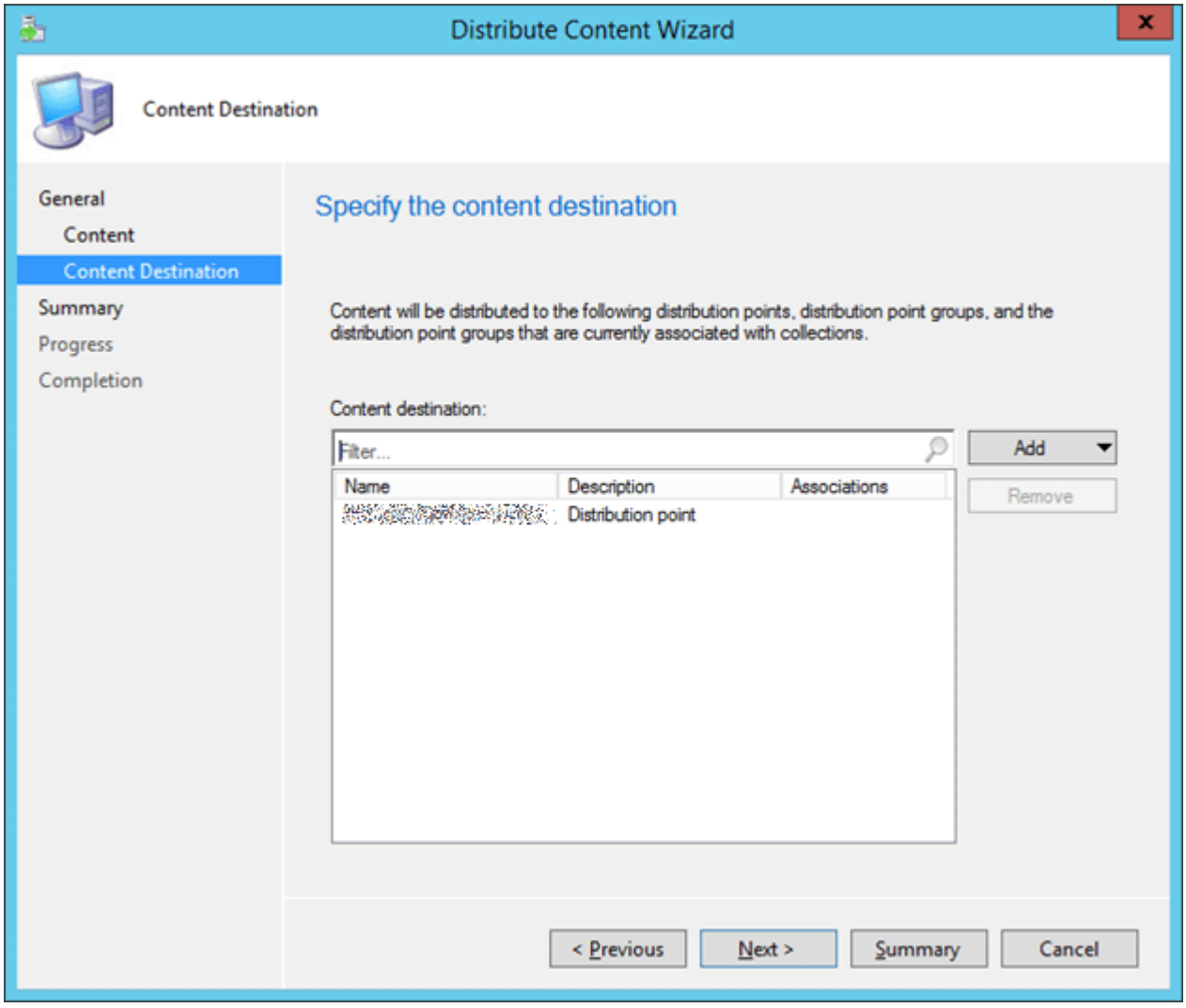

Folder Tools
System Center 2012 R2 Configuration Manager (Connected to PBT - ES
Home
Folder
Create
Saved Searches
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Search
Application
Categorize
View Relationships
Properties
Classify
Relationships
Properties
Software Library ▸ Overview ▸ Application Management ▸ Applications ▸ BTS App
Software Library
Overview
Application Management
Applications
BTS Applications
SD Applications
Packages
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Assets and Compliance
Software Library
Monitoring
Administration
BTS Applications 55 items
Search
Add Criteria
Icon
Name
Types
Deployments
Status
Adobe Reader XI (11.0.08)
Adobe Reader XI (11.0.10)
Adobe Reader XI (11.0.9)
CDBurnerXP
CDBurnerXP (64 bit)
CDBurnerXP old
CDBurnerXP old (64-bit)
ERA Agent
ESET Endpoint Security
ESET Endpoint Security (6
ESET Remote Administrator
Far Manager 3
Far Manager 3 (64-bit)
Far Manager old
Far Manager old (64-bit)
Fedra Fonts
Fedra Fonts (64-bit)
Java 7 Update 67
Java 7 Update 67 (64-bit)
Java 8 Update 25
Java 8 Update 25 (64-bit)
Active
ESET Remote Administrator Agent (64-bit)
Ready
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh F5
Delete Delete
Simulate Deployment
Deploy
Distribute Content
Move
Set Security Scopes
Categorize
View Relationships
Properties

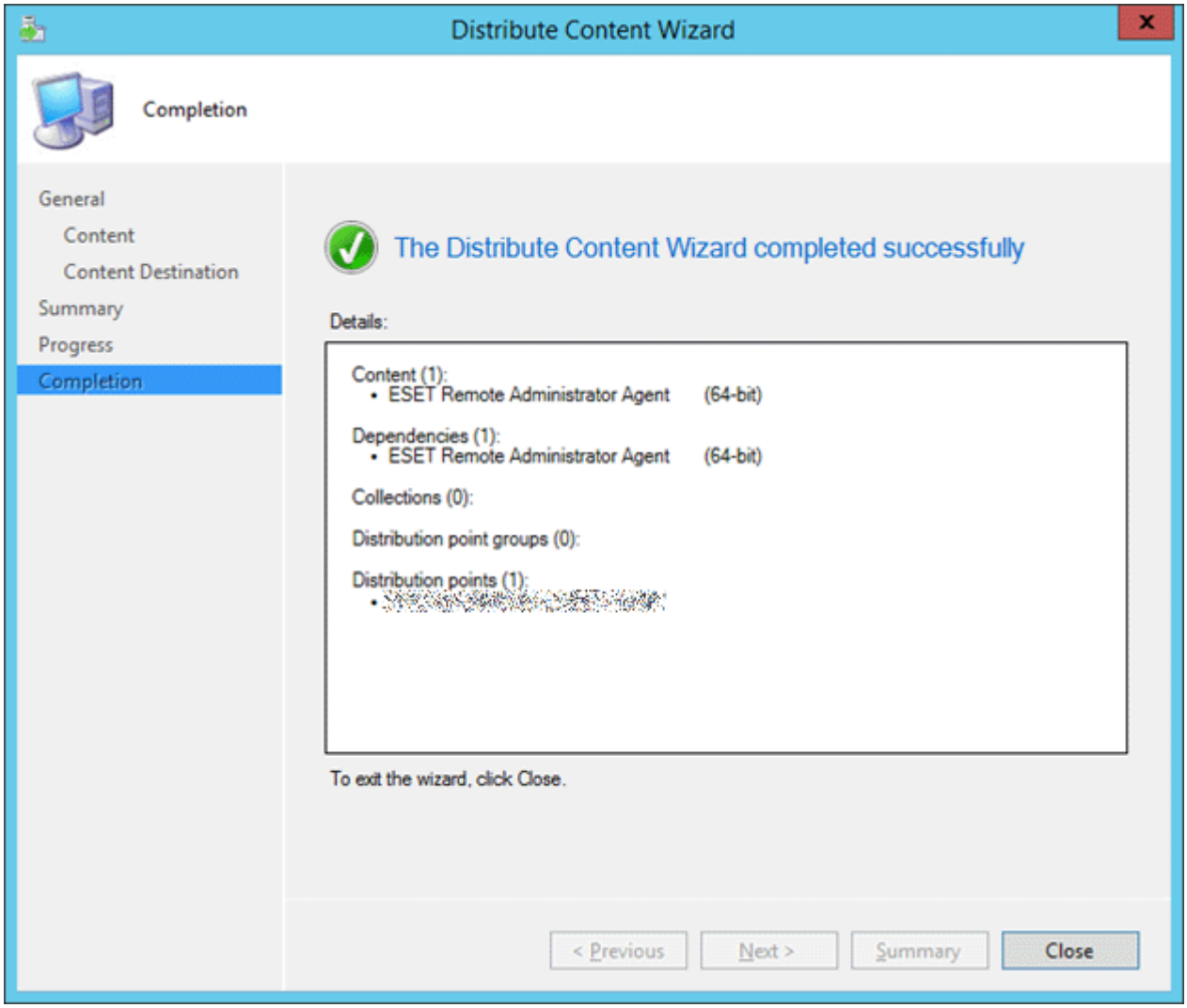

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

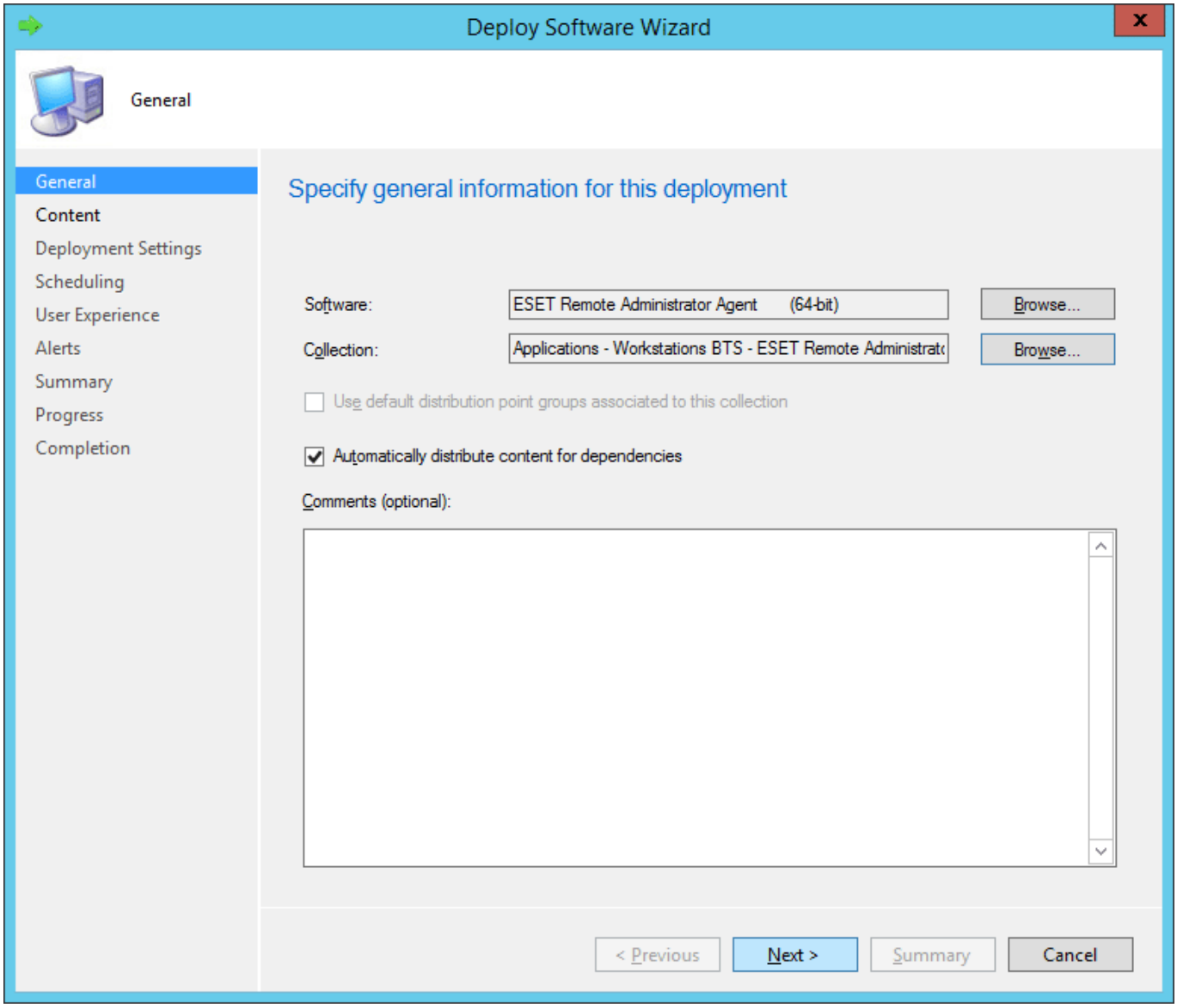


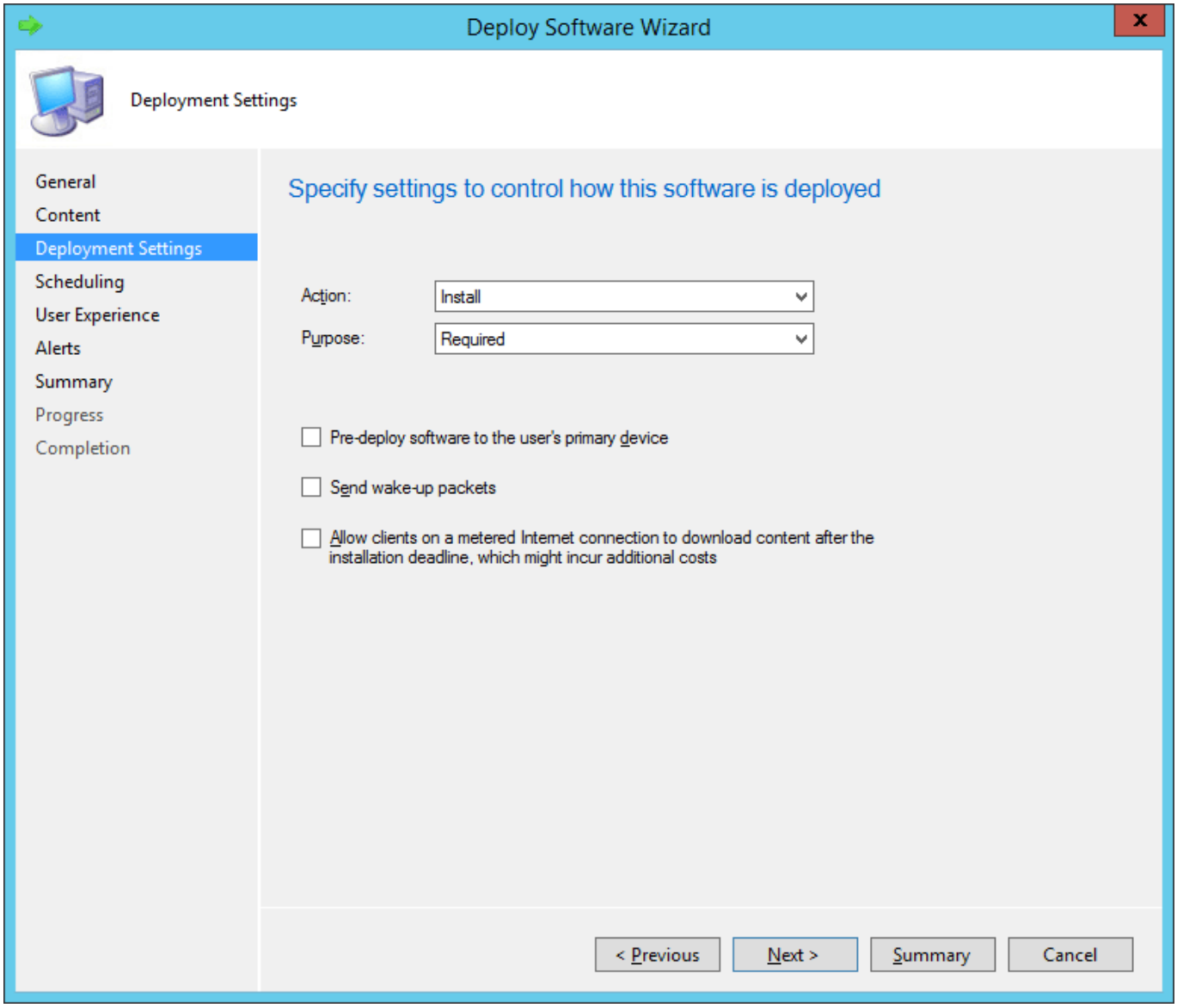
7. Klikněte pravým tlačítkem na název aplikace a vyberte možnost **Deploy**. Dále postupujte podle zobrazeného průvodce a vyberte cíle, na které chcete aplikaci nasadit.

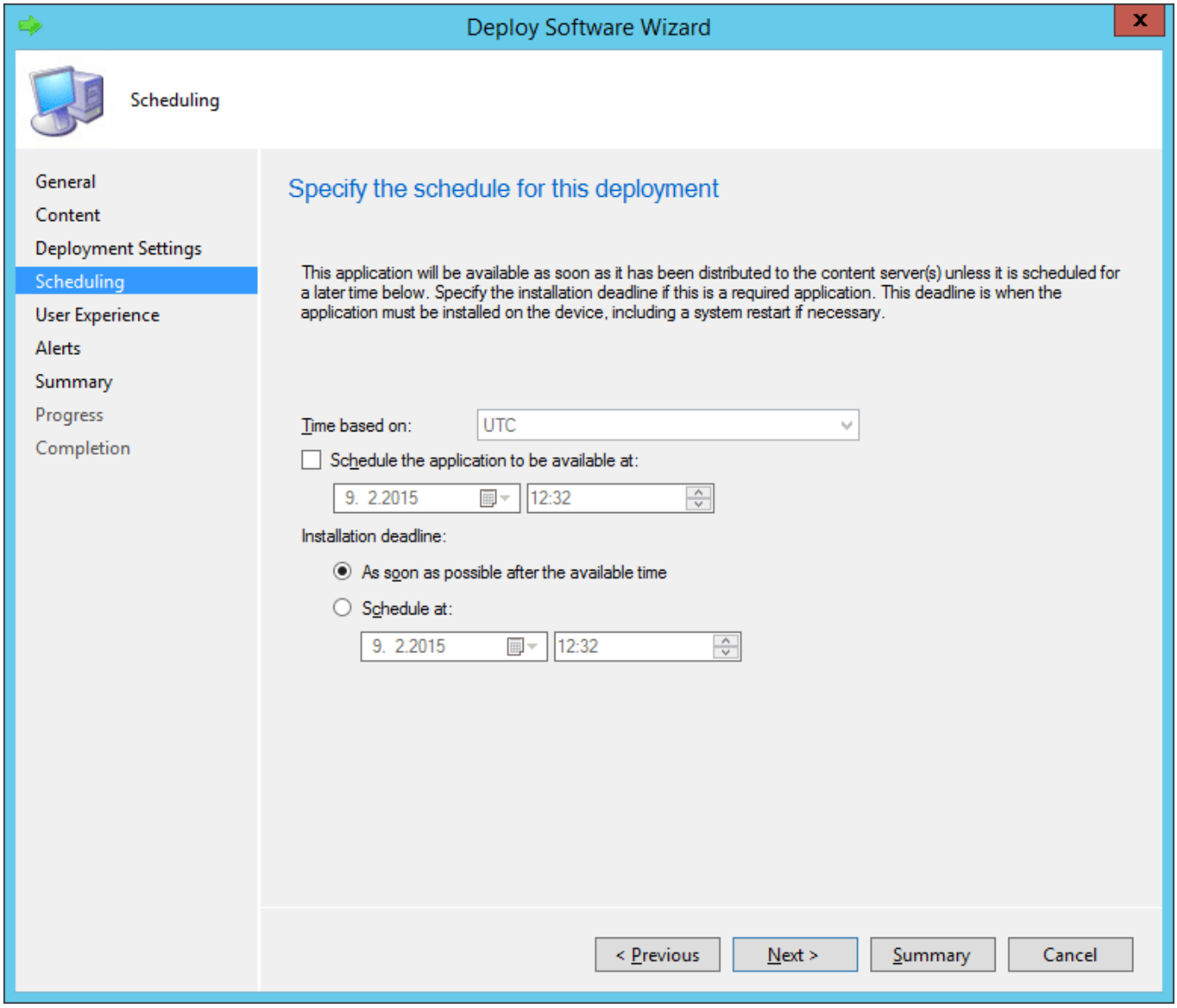

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

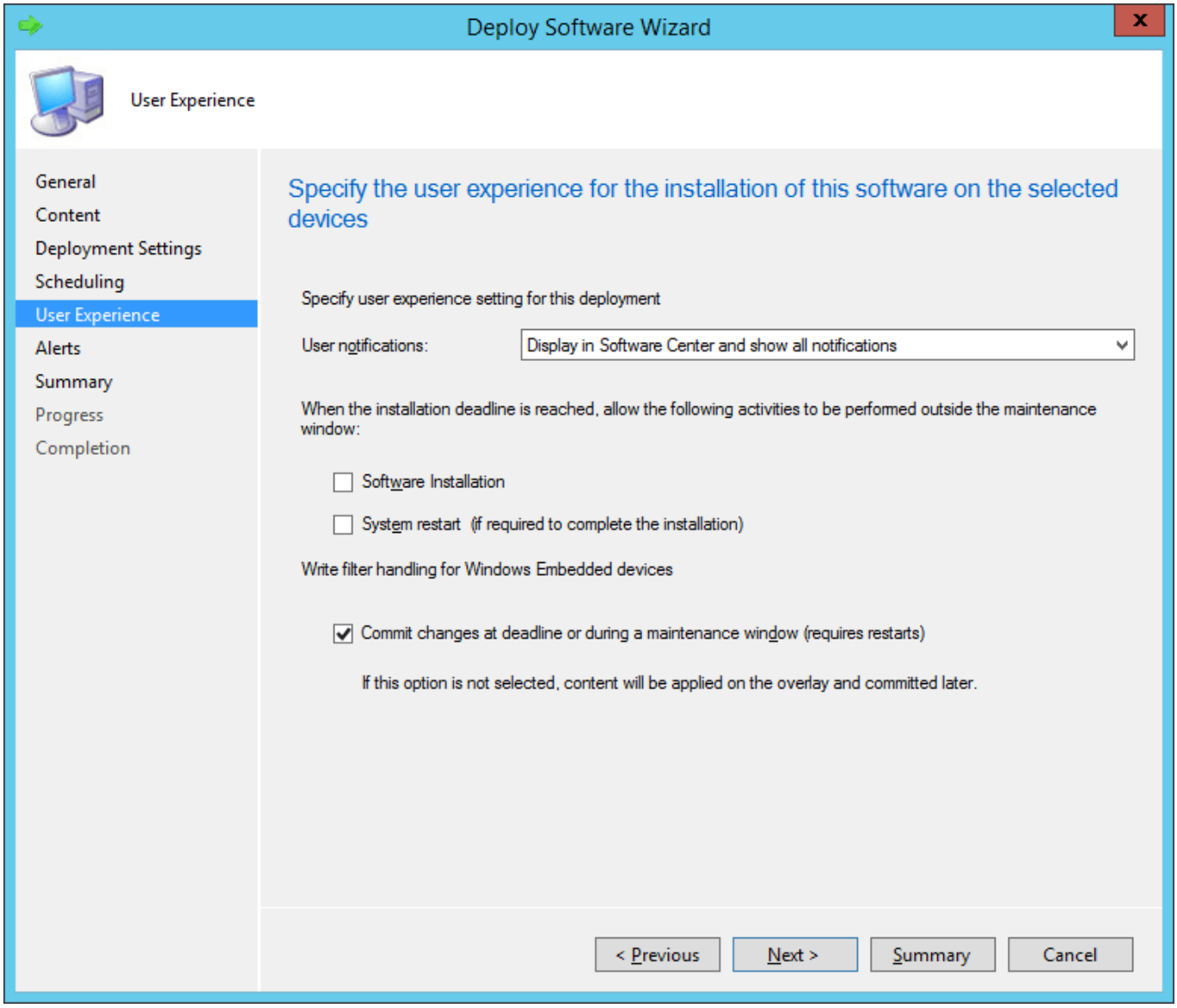

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Filter...
Add
Remove
Name
Description
Associations
Distribution point
< Previous
Next >
Summary
Cancel

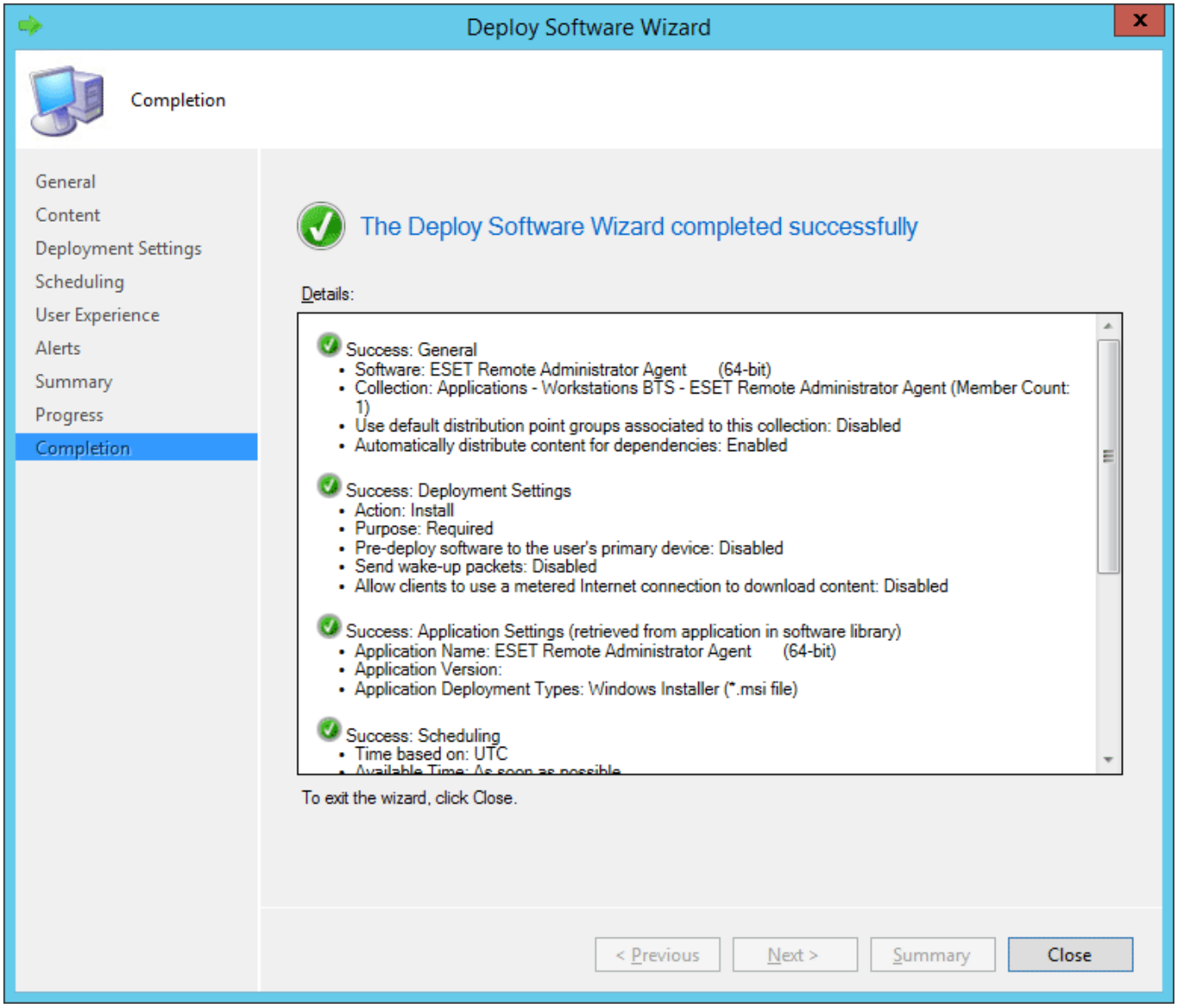

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel



ESET Remote Deployment Tool

ESET Remote Deployment Tool je nástroj určený pro vzdálené nasazení all-in-one instalačního balíčku vytvořeného v ESET PROTECT obsahujícího ESET Management Agenta a bezpečnostní produkt ESET.

Jedná se o samostatný nástroj, který je dostupný ke stažení na webových stránkách společnosti ESET. Primárně je určen pro malé a středně velké sítě, kdy jej spouštíte pod běžným administrátorským účtem.

ESET Remote Deployment tool je samostatný nástroj pro nasazení ESET Management Agenta a bezpečnostního produktu na stanice s podporovaným operačním systémem Microsoft Windows.

ESET Management Agent je předkonfigurovaný pro připojení k ESET PROTECT. Z tohoto důvodu jsou možnosti úprav v politice ESET Management agenta omezené.

Pro nasazení ESET Management a bezpečnostního produktu pomocí tohoto nástroje postupujte podle následujících kroků:

1. Stáhněte si ESET Remote Deployment Tool z webových stránek společnosti ESET.

2. Ujistěte se, že splňujete veškeré požadavky.

3. Spusťte ESET Remote Deployment Tool na klientské stanici.

4. Vyberte si jednu z níže uvedených možností:

   • Active Directory – prostřednictvím této možnosti si můžete seznam počítačů načíst z Active Directory. Můžete si rovněž exportovat seznam počítačů v Active Directory pro jejich importování do ESET PROTECT.

   • Scan Network – prostřednictvím této možnosti můžete najít počítače v konkrétním IP rozsahu.

   • Import list – prostřednictvím této možnosti můžete importovat seznam počítačů ze souboru.

   • Add computers manually – prostřednictvím této možnosti ručně zadejte názvy počítačů nebo jejich IP adresy.

Vzdálené nasazení může selhat z mnoha příčin. V případě neúspěchu přejděte do kapitoly Řešení problémů.

Požadavky pro použití ESET Remote Deployment Tool

Při nasazování ESET_MNG Agenta prostřednictvím serverové úlohy se ujistěte, že má PRODUCT Server i cílová stanice přístup k internetu.

Níže uvádíme požadavky pro použití ESET Remote Deployment Tool na platformě Windows:

- ESET PROTECT instance musí být vytvořená a funkční.
- Na cílové stanici musíte mít povoleny potřebné porty. Viz kapitola o portech pro ESET PROTECT Remote Deployment Tool.
- Vytvořený balíček Live Installer musíte mít stažený na pevném disku počítače, ze kterého chcete vzdálené nasazení prostřednictvím Deployment Tool provést.

Vzdálené nasazení může selhat z mnoha příčin. V případě neúspěchu přejděte do kapitoly Řešení problémů.

Výběr počítačů z Active Directory

Tato kapitola doplňuje předchozí a popisuje kroky pro nasazení ESET Management Agenta a bezpečnostního produktu ESET:

1. Přečtěte si a odsouhlaste **Licenční ujednání s koncovým uživatelem**. Pokračujte kliknutím na tlačítko **Next**.

2. Zadejte název nebo IP adresu **Active Directory serveru** a **port**, na kterém se k němu chcete připojit.

3. Dále zadejte přihlašovací údaje (**Username** a **Password**), pod kterými se chcete k Active Directory serveru přihlásit. Pokud vyberete možnost **Use current user credentials**, automaticky se doplní údaje aktuálně přihlášeného uživatele.

4. Možnost **Export computer list for ESET PROTECT** vyberte v případě, kdy chcete exportovat strukturu Active Directory a importovat ji do ESET PROTECT.

Pokud je počítač členem Active Directory, kliknutím na tlačítko **Next** budete automaticky přihlášení k výchozímu doménovému řadiči.

5. V dalším kroku vybere počítače, na které chcete instalační balíček nasadit, a pokračujte kliknutím na tlačítko **Next**. Pro zobrazení všech počítačů ve skupině zaškrtněte možnost **Include subgroups**.

6. V dalším kroku se zobrazí seznam všech zařízení dostupných pro nasazení. Ujistěte se, že jsou přidána všechna zařízení, a klikněte na **Další**.

Ujistěte se, že všechna zvolená zařízení mají stejnou platformu (64bitový nebo 32bitový operační systém).

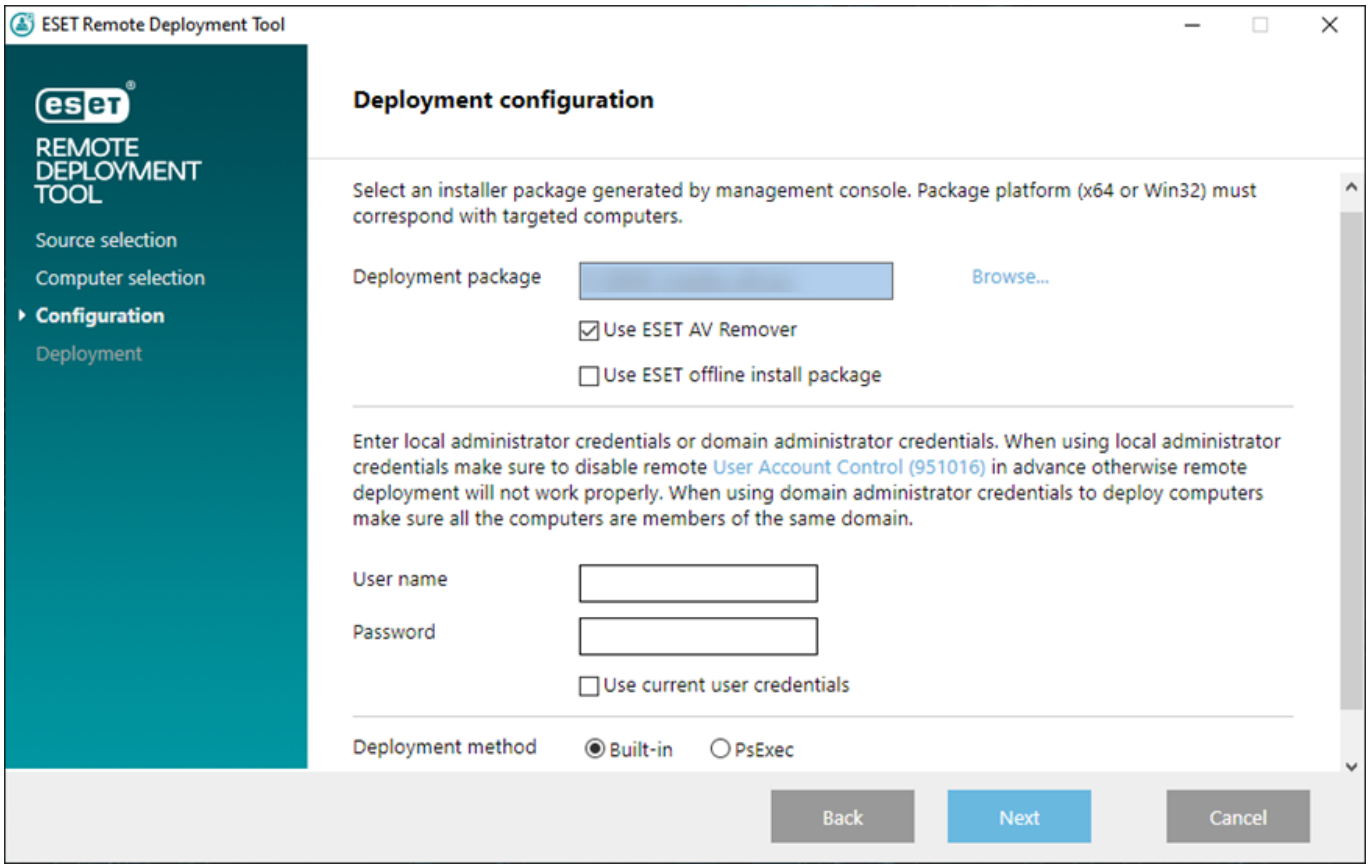
7. Klikněte na tlačítko **Procházet** a vyberte vytvořený instalační balíček v ESET PROTECT Web Console on-premise nebo cloud).

- Vybráním možnosti **Použít offline instalační balíček** (soubor *.dat*) nasadíte offline balíček vytvořený prostřednictvím Live Installer (pouze u ESET PROTECT).

- Pokud na cílové stanici není instalováno žádné další bezpečnostní řešení, odškrtněte možnost **Use ESET AV Remover**. ESET AV Remover dokáže odstranit podporovaná bezpečností řešení třetích stran.

8. Zadejte přihlašovací údaje k cílové stanici. V případě doménového prostředí zadejte **účet doménového administrátora**. Při použití **lokálního administrátorského účtu** vypněte na cílové stanici UAC. Při použití možnosti **Use current user credentials** se automaticky použijí přihlašovací údaje aktuálně přihlášeného uživatele.

9. Následně v sekci **Deployment method** vyberte způsob vzdáleného nasazení. Standardně je vybrána možnost **Built-in**, která vrací případné chybové hlášky Windows. Pro nasazení můžete využít také **PsExec** – nástroj třetí stany. Po vybrání možnosti nasazení klikněte na tlačítko **Next**.



Po vybrání možnost**PsExec** nasazení selže z důvodu, že nástroje není schopen odsouhlasit licenční ujednání (EULA) **PsExec**. Pro úspěšné nasazení si otevřete příkazový řádek a spusťte **PsExec** ručně.

10. Po úspěšném nasazení se zobrazí zpráva "Success". Nástroj ukončete kliknutím na tlačítko **Finish**. Pokud nasazení selže, pro získání bližších informací klikněte ve sloupci **Status** na **More info**. Následně si můžete exportovat seznam stanic, na něž se instalační balíček nepodařilo nasadit. Klikněte na tlačítko **Browse**, vyberte složku, do které chcete *.txt* soubor uložit, a klikněte na tlačítko **Export failed computer**.

Můžete zkontrolovat status log (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na klientském zařízená, abyste se ujistili, že ESET Management Agent funguje správně.

Vzdálené nasazení může selhat z mnoha příčin. V případě neúspěchu přejděte do kapitoly Řešení problémů.

Vyhledání počítačů v lokální síti

Tato kapitola doplňuje předchozí a popisuje kroky pro nasazení ESET Management Agenta a bezpečnostního produktu ESET:

1. Přečtěte si a odsouhlaste **Licenční ujednání s koncovým uživatelem**. Pokračujte kliknutím na tlačítko **Next**.

2. Do pole **IP Ranges** zadejte rozsah IP adres, ve kterém chcete počítače vyhledat. Příklad: *10.100.100.10-10.100.100.250*

3. Dále vyberte způsob detekce počítačů (**Scan methods**):

- **Ping scan** –- nástroj se pokusí najít živé počítače v síti pomocí příkazu `ping`.

Některé stanice v síti nemusí na příkaz `ping` reagovat z důvodu jeho blokování firewallem.

- **Port scan** – nástroj se pokusí stanici najít prostřednictvím techniky skenování portů.

4. Vyhledání počítačů zahajte kliknutím na tlačítko **Start Scan**.

5. V dalším kroku vybere počítače, na které chcete instalační balíček nasadit, a pokračujte kliknutím na tlačítko **Next**.

6. V dalším kroku se zobrazí seznam všech zařízení dostupných pro nasazení. Ujistěte se, že jsou přidána všechna zařízení, a klikněte na **Další**.

Ujistěte se, že všechna zvolená zařízení mají stejnou platformu (64bitový nebo 32bitový operační systém).

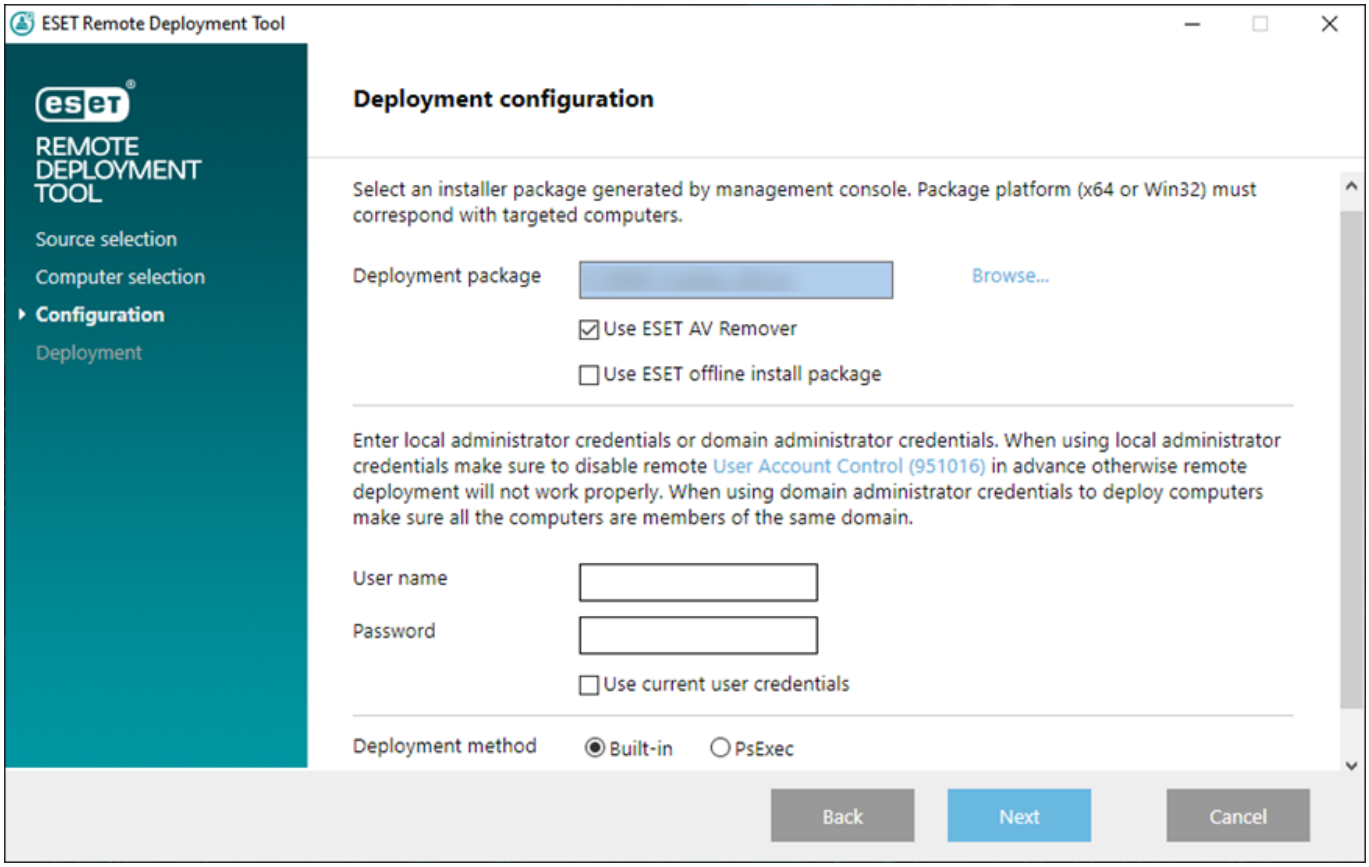
7. Klikněte na tlačítko **Procházet** a vyberte vytvořený instalační balíček v ESET PROTECT Web Console on-premise nebo cloud).

- Vybráním možnosti **Použít offline instalační balíček** (soubor *.dat*) nasadíte offline balíček vytvořený prostřednictvím Live Installer (pouze u ESET PROTECT).

- Pokud na cílové stanici není instalováno žádné další bezpečnostní řešení, odškrtněte možnost **Use ESET AV Remover**. ESET AV Remover dokáže odstranit podporovaná bezpečností řešení třetích stran.

8. Zadejte přihlašovací údaje k cílové stanici. V případě doménového prostředí zadejte **účet doménového administrátora**. Při použití **lokálního administrátorského účtu** vypněte na cílové stanici UAC. Při použití možnosti **Use current user credentials** se automaticky použijí přihlašovací údaje aktuálně přihlášeného uživatele.

9. Následně v sekci **Deployment method** vyberte způsob vzdáleného nasazení. Standardně je vybrána možnost **Built-in**, která vrací případné chybové hlášky Windows. Pro nasazení můžete využít také **PsExec** – nástroj třetí stany. Po vybrání možnosti nasazení klikněte na tlačítko **Next**.



Po vybrání možnost**PsExec** nasazení selže z důvodu, že nástroje není schopen odsouhlasit licenční ujednání (EULA) **PsExec**. Pro úspěšné nasazení si otevřete příkazový řádek a spusťte **PsExec** ručně.

10. Po úspěšném nasazení se zobrazí zpráva "Success". Nástroj ukončete kliknutím na tlačítko **Finish**. Pokud nasazení selže, pro získání bližších informací klikněte ve sloupci **Status** na **More info**. Následně si můžete exportovat seznam stanic, na něž se instalační balíček nepodařilo nasadit. Klikněte na tlačítko **Browse**, vyberte složku, do které chcete *.txt* soubor uložit, a klikněte na tlačítko **Export failed computer**.

Můžete zkontrolovat status log (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na klientském zařízená, abyste se ujistili, že ESET Management Agent funguje správně.

Vzdálené nasazení může selhat z mnoha příčin. V případě neúspěchu přejděte do kapitoly Řešení problémů.

Importování seznamu počítačů

Tato kapitola doplňuje předchozí a popisuje kroky pro nasazení ESET Management Agenta a bezpečnostního produktu ESET:

1. Přečtěte si a odsouhlaste **Licenční ujednání s koncovým uživatelem**. Pokračujte kliknutím na tlačítko **Next**.

2. Vyberte si jednu z možností:

   • **Text file**: prostřednictvím této možnosti můžete importovat textový soubor se seznamem počítačů (jejich názvy nebo IP adresami). Každý záznam oddělte novým řádkem.

   • **Export z konzole pro vzdálenou správu** Prostřednictvím této možnosti můžete importovat seznam počítačů exportovaný z ESET PROTECT Web Console.

3. Klikněte na tlačítko **Browse**, vyberte soubor který chcete nahrát, a pokračujte kliknutím na tlačítko **Next**.

4. V dalším kroku se zobrazí seznam všech zařízení dostupných pro nasazení. Ujistěte se, že jsou přidána všechna zařízení, a klikněte na **Další**.

Ujistěte se, že všechna zvolená zařízení mají stejnou platformu (64bitový nebo 32bitový operační systém).

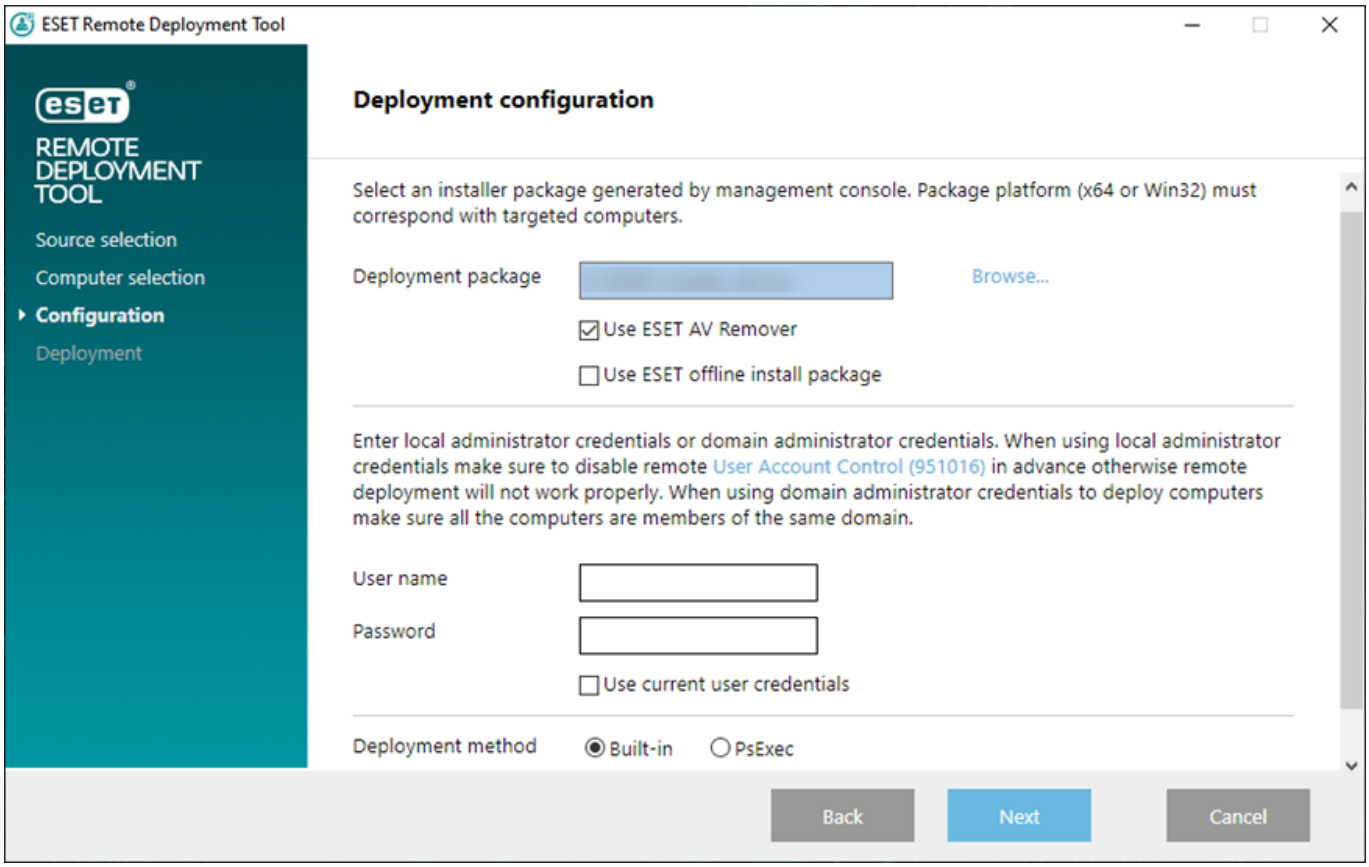
5. Klikněte na tlačítko **Procházet** a vyberte vytvořený instalační balíček v ESET PROTECT Web Console on-premise nebo cloud).

   • Vybráním možnosti **Použít offline instalační balíček** (soubor *.dat*) nasadíte offline balíček vytvořený prostřednictvím Live Installer (pouze u ESET PROTECT).

   • Pokud na cílové stanici není instalováno žádné další bezpečnostní řešení, odškrtněte možnost **Use ESET AV Remover**. ESET AV Remover dokáže odstranit podporovaná bezpečností řešení třetích stran.

6. Zadejte přihlašovací údaje k cílové stanici. V případě doménového prostředí zadejte **účet doménového administrátora**. Při použití **lokálního administrátorského účtu** vypněte na cílové stanici UAC. Při použití možnosti **Use current user credentials** se automaticky použijí přihlašovací údaje aktuálně přihlášeného uživatele.

7. Následně v sekci **Deployment method** vyberte způsob vzdáleného nasazení. Standardně je vybrána možnost **Built-in**, která vrací případné chybové hlášky Windows. Pro nasazení můžete využít také **PsExec** – nástroj třetí stany. Po vybrání možnosti nasazení klikněte na tlačítko **Next**.



Po vybrání možnost**PsExec** nasazení selže z důvodu, že nástroje není schopen odsouhlasit licenční ujednání (EULA) **PsExec**. Pro úspěšné nasazení si otevřete příkazový řádek a spusťte **PsExec** ručně.

8. Po úspěšném nasazení se zobrazí zpráva "Success". Nástroj ukončete kliknutím na tlačítko **Finish**. Pokud nasazení selže, pro získání bližších informací klikněte ve sloupci **Status** na **More info**. Následně si můžete exportovat seznam stanic, na něž se instalační balíček nepodařilo nasadit. Klikněte na tlačítko **Browse**, vyberte složku, do které chcete *.txt* soubor uložit, a klikněte na tlačítko **Export failed computer**.

Můžete zkontrolovat status log (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na klientském zařízená, abyste se ujistili, že ESET Management Agent funguje správně.

Vzdálené nasazení může selhat z mnoha příčin. V případě neúspěchu přejděte do kapitoly Řešení problémů.

Ruční přidání počítačů

Tato kapitola doplňuje předchozí a popisuje kroky pro nasazení ESET Management Agenta a bezpečnostního produktu ESET:

1. Přečtěte si a odsouhlaste **Licenční ujednání s koncovým uživatelem**. Pokračujte kliknutím na tlačítko **Next**.

2. Zadejte název nebo IP adresu stanice, na kterou chcete balíček nasadit, a pokračujte kliknutím na tlačítko **Next**. Každý záznam oddělte novým řádkem.

Ujistěte se, že všechna zvolená zařízení mají stejnou platformu (64bitový nebo 32bitový operační systém).

3. V dalším kroku se zobrazí seznam všech zařízení dostupných pro nasazení. Ujistěte se, že jsou přidána všechna zařízení, a klikněte na **Další**.

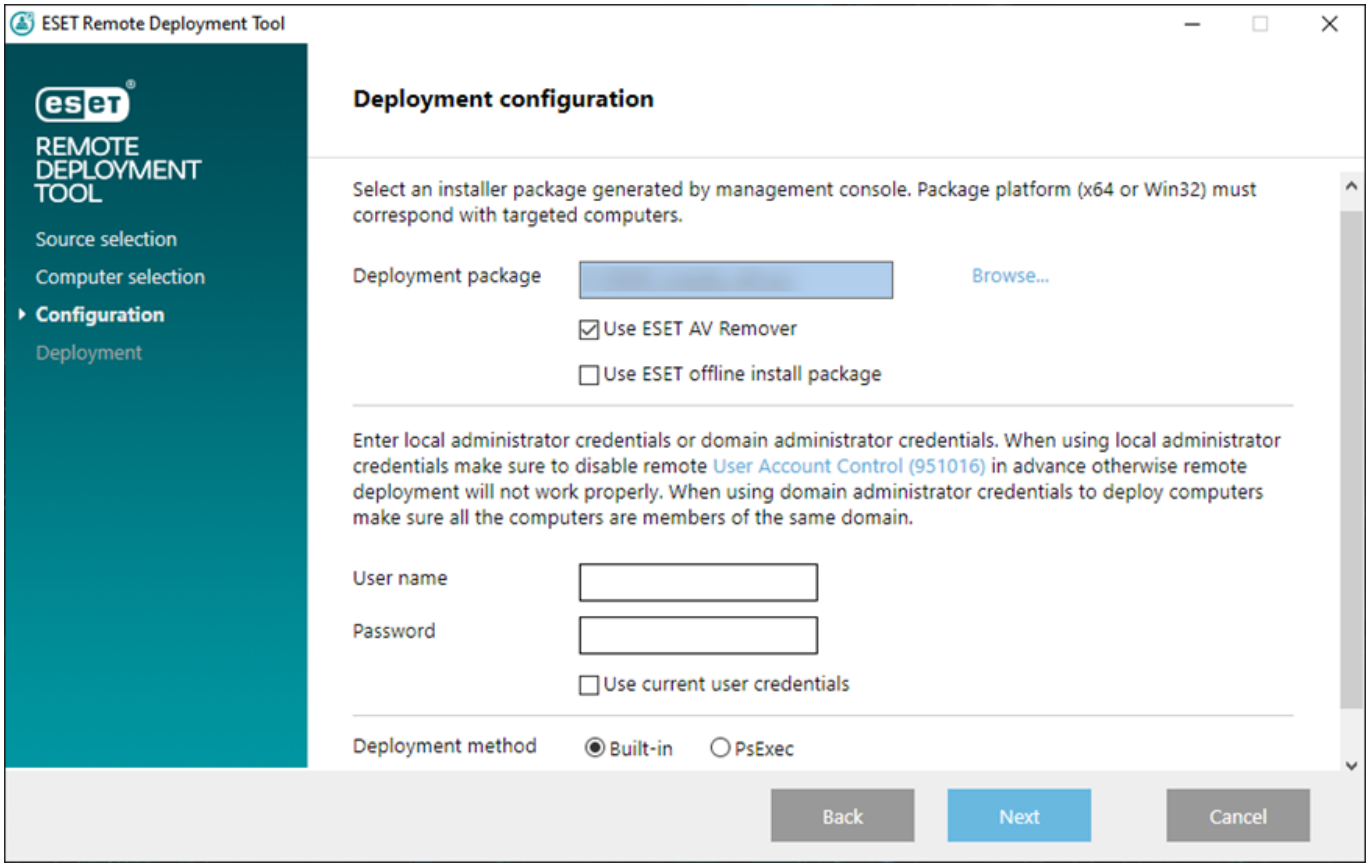
4. Klikněte na tlačítko **Procházet** a vyberte vytvořený instalační balíček v ESET PROTECT Web Console on-premise nebo cloud).

- Vybráním možnosti **Použít offline instalační balíček** (soubor *.dat*) nasadíte offline balíček vytvořený prostřednictvím Live Installer (pouze u ESET PROTECT).

- Pokud na cílové stanici není instalováno žádné další bezpečnostní řešení, odškrtněte možnost **Use ESET AV Remover**. ESET AV Remover dokáže odstranit podporovaná bezpečností řešení třetích stran.

5. Zadejte přihlašovací údaje k cílové stanici. V případě doménového prostředí zadejte **účet doménového administrátora**. Při použití **lokálního administrátorského účtu** vypněte na cílové stanici UAC. Při použití možnosti **Use current user credentials** se automaticky použijí přihlašovací údaje aktuálně přihlášeného uživatele.

6. Následně v sekci **Deployment method** vyberte způsob vzdáleného nasazení. Standardně je vybrána možnost **Built-in**, která vrací případné chybové hlášky Windows. Pro nasazení můžete využít také **PsExec** – nástroj třetí stany. Po vybrání možnosti nasazení klikněte na tlačítko **Next**.



Po vybrání možnost**PsExec** nasazení selže z důvodu, že nástroje není schopen odsouhlasit licenční ujednání (EULA) **PsExec**. Pro úspěšné nasazení si otevřete příkazový řádek a spusťte **PsExec** ručně.

7. Po úspěšném nasazení se zobrazí zpráva "Success". Nástroj ukončete kliknutím na tlačítko **Finish**. Pokud nasazení selže, pro získání bližších informací klikněte ve sloupci **Status** na **More info**. Následně si můžete exportovat seznam stanic, na něž se instalační balíček nepodařilo nasadit. Klikněte na tlačítko **Browse**, vyberte složku, do které chcete *.txt* soubor uložit, a klikněte na tlačítko **Export failed computer**.

Můžete zkontrolovat status log (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na klientském zařízená, abyste se ujistili, že ESET Management Agent funguje správně.

Vzdálené nasazení může selhat z mnoha příčin. V případě neúspěchu přejděte do kapitoly Řešení problémů.

ESET Remote Deployment Tool – řešení problémů

Jedná se o samostatný nástroj, který je dostupný ke stažení na webových stránkách společnosti ESET. Primárně je určen pro malé a středně velké sítě, kdy jej spouštíte pod běžným administrátorským účtem.

ESET Remote Deployment tool je samostatný nástroj pro nasazení ESET Management Agenta a bezpečnostního produktu na stanice s podporovaným operačním systémem Microsoft Windows.

Vzdálené nasazení se nemusí zdařit z mnoha příčin. V níže uvedené tabulce naleznete nejčastější z nich společně s informacemi vedoucími k jejich vyřešení.

Chybová zpráva	Možné důvody
The network path was not found (error code 0x35)	• Klient není v síti dosažitelný, firewall blokuje komunikaci • Příchozí komunikace na portech 135, 137, 138, 139 a 445 není povolena ve firewallu: Povolte sdílení souborů a tiskáren. • Nelze přeložit název klienta, není použit platný FQDN název počítače.
Access is denied (error code 0x5) **Nesprávné uživatelské jméno nebo heslo** (kód chyby 0x52e)	• Pokud je server i stanice připojena do domény, zadejte údaje doménového administrátora v plném tvaru, tedy ve formátu **doména\uživatel**. • Pokud nasazujete ze serveru, který je v jiné doméně, na cílové stanici deaktivujte vzdálené řízení uživatelských účtů. • Pokud nasazujete ze serveru, který je v jiné doméně, použijte lokální administrátorský účet. Název cílové stranice se před jméno uživatele doplní automaticky. • Účet administrátora nemá nastaveno heslo. • Nedostatečná přístupová oprávnění. • Administrativní sdílení ADMIN$ nejsou dostupná. • Administrativní sdílení IPC$ nejsou dostupná. • Je zapnuté zjednodušené sdílení
The installation package is not supported by this processor type (error code 1633)	Instalační balíček není určen pro tuto platformu. Ve webové konzoli ESET PROTECT si vytvořte a stáhněte nový balíček pro správnou platformu (64-bit nebo 32-bit).
The semaphore timeout period has expired	Klient nedokázal přistoupit k síťovému prostředku s balíčkem z důvodu vypnuté SMB 1.0 na tomto prostředku.

Na základě zjištěné příčiny odstraňte problém znemožňující instalaci:

Možný důvod	Řešení
Klient není v síti dosažitelný	Vyzkoušejte ze stanice (případně ESET PROTECT Serveru), z níž provádíte nasazení, ping na danou stanici. Pokud odpovídá; zkuste se vzdáleně připojit (například vzdálenou plochou).
Firewall blokuje komunikaci	Zkontrolujte nastavení Brány Windows Firewall na straně klienta, případně firewall třetí strany (pokud je nainstalován). Mějte na paměti, že v průběhu instalace se neotevřou ve firewallu porty 2222 a 2223. Ujistěte se, že jsou tyto porty otevřené na všech firewallech mezi klientem a serverem.
Nelze přeložit název klienta	Problém související s DNS můžete v některých případech identifikovat pomocí následujících kroků: • Do příkazového řádku na klientovi zadejte příkaz `nslookup` a doplňte jej o IP adresu nebo název serveru. Výsledek by se měl shodovat s informacemi zobrazenými po zadání příkazu ipconfig na serveru. Tedy po zadání příkazu nslookup a názvu serveru byste měli získat IP adresu serveru. Pro dokončení ověření správně nakonfigurované sítě proveďte ze serveru příkaz `nslookup` s dotazem na klienta, na kterého se nedaří vzdáleně nainstalovat ESET Management Agenta. Příkaz `nslookup` je nutné spustit na klientovi i serveru. • Ručně ověřte, zda v DNS záznamech nemáte duplicitní záznamy.
Účet administrátora nemá nastaveno heslo	Nastavte heslo pro účet administrátora (nepoužívejte prázdné heslo).
Nedostatečná přístupová oprávnění	Zkuste použít přihlašovací údaje doménového administrátora. Pokud je klientská stanice v pracovní skupině, použijte lokální účet administrátora. Aby bylo možné spustit úlohu nasazení agenta, je třeba aktivovat uživatelský účet správce. Vytvořte lokálního uživatele, který bude členem skupiny Administrators, nebo aktivujte vestavěný účet Administrator. Pro aktivaci účtu administrátora postupujte podle následujících kroků: 1.Otevřete příkazový řádek s oprávněním administrátora 2.Zadejte následující příkaz: `net user administrator /active:yes`
Administrativní sdílení ADMIN$ nejsou dostupná	Klientské zařízení musí mít povoleno sdílení zdroje ADMIN$. Pro ověření, zda je sdílení povoleno klikněte na **Start** > **Ovládací panely** > **Nástroje pro správu** > **Správa počítače** > **Sdílené složky** > **Sdílené složky**.
Administrativní sdílení IPC$ nejsou dostupná	Na serveru si otevřete příkazový řádek a zadáním níže uvedeného příkazu ověřte, zda máte přístup k IPC$ prostředkům: `net use \\clientname\IPC$`, kde `clientname` je název cílové stanice.
Je zapnuté zjednodušené sdílení	Pokud se vám zobrazila chybová zpráva "**Přístup odepřen**" a provozujete smíšené prostředí domény a pracovní skupiny, na stanicích, na které se vám nedaří nasadit agenta deaktivujte možnost **Používat zjednodušené sdílení** nebo **Používat průvodce sdílením**. Například ve Windows 11 proveďte následující: • Klikněte na tlačítko **Start**, do pole pro **vyhledávání** zadejte příkaz `Průzkumník souborů` a poté klikněte na položku **Možnosti Průzkumníka souborů**. V zobrazeném dialogovém okně přejděte na záložku **Zobrazení** a v sekci **Upřesnit nastavení** odškrtněte možnost **Používat průvodce sdílením**.

Ochrana agenta

ESET Management Agent je vybaven ochranným mechanismem. Díky tomu je:

- zajištěna ochranu záznamů ESET Management Agenta v registru (HIPS),
- znemožněna změna, nahrazení nebo odstranění souborů ESET Management Agenta (HIPS),
- zabráněno ukončení procesu ESET Management Agenta,
- znemožněno zastavení, pozastavení, ukončení nebo odinstalování služby ESET Management Agenta.

Další úroveň ochrany zajišťuje modul HIPS, který je součástí bezpečnostního produktu ESET.

Pro zajištění úplné ochrany ESET Management agenta musí být na koncové stanici nainstalován bezpečnostní produkt ESET (například ESET Endpoint Security) a musí mít být aktivní modul HIPS.

Ochrana heslem

Stejně jako bezpečnostní produkt ESET, také ESET Management Agenta provozovaného na Windows můžete ochránit heslem Tuto dodatečnou ochranu nastavíte prostřednictvím politiky pro ESET Management Agenta.

Pokud je Agent ESET Management chráněný heslem, pro odinstalaci, opravu nebo aktualizaci (se změnami) je nutné zadat heslo.

Nastavení ESET Management Agenta

Specifické nastavení ESET Management Agenta provedete prostřednictvím politiky ESET Management Agenta.

Pro ESET Management Agenta není vytvořená žádná předdefinovaná politika. Chcete-li vytvořit politiku ESET Management Agenta, klikněte na **Politiky** > **Nová politika** a v sekci **Nastavení** vyberte ´možnost**ESET Management Agent**, kde můžete upravit následující nastavení:

Nastavení

Nastavení chráněné heslem je ochranná funkce ESET Management Agenta (pouze pro systém Windows). Kliknutím na tlačítko **Nastavit** vedle položky **Nastavení chráněné heslem** povolíte ochranu nastavení ESET Management Agenta heslem.

- Nastavení chráněné heslem bylo vylepšeno ve verzi 10.1. Nastavte hesla zvlášť pro Agenta verze 10.0 a starší a 10.1 a novější.
- Uložte si heslo na bezpečné místo. Pokud je Agent ESET Management chráněný heslem, pro odinstalaci, opravu nebo aktualizaci (se změnami) je nutné zadat heslo.

Rozšířená nastavení

- **HTTP Proxy** – definujte proxy server, prostřednictvím kterého bude přistupovat klienti na internet. Zaškrtnutím nebo odškrtnutí políčka **Použít přímé spojení, pokud není dostupný proxy server** zapnete nebo vypnete tuto náhradní možnost.

- **Operační systém** – v této části naleznete nastavení související s reportováním dat z operačního systému. Například zapnutím možnosti **Oznámit jiné instalované aplikace než ESET** zajistíte, že agent bude reportovat také nainstalované aplikace třetích stran.

- **Program vylepšování produktu** – pomocí této možnosti aktivujete nebo zakážete zasílání informací o pádech a anonymních statistických dat do společnosti ESET.

- **Protokolování** – v této části nastavíte úroveň, od které se mají události zaznamenávat do protokolů. Pokud vyberte možnost **Trace**, do protokolu se zapíší veškeré informace. Vybráním možnosti **Fatal** se do protokolu zapíší nejvýše kritické informace. Soubory s protokoly ESET Management Agenta naleznete na klientské stanici.

Přiřadit

Vyberte klienty, kterým chcete politiku přiřadit. Po kliknutí na tlačítko **Přiřadit** se zobrazí dialogové okno se všemi statickými i dynamickými skupinami. Vyberte klienty nebo skupiny, na které chcete politiku aplikovat, a klikněte

na tlačítko **OK**.

Souhrn

Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**.

Můžete si vyžádat konfiguraci Agenta ve spravovaném zařízení a zobrazit použité nastavení politik Agenta: Klikněte na **Počítače** > klikněte na počítač > **Detaily** > **Konfigurace** > Vyžádat konfiguraci.

Vytvoření politiky pro ochranu odinstalace ESET Management Agenta

Níže uvádíme příklad, jak vytvořit novou politiku pro ESET Management Agenta, prostřednictvím které nastavíte heslo pro zabránění jeho neoprávněné odinstalace. Po aktivování této možnosti bude při pokusu o odinstalování nebo provedení opravné instalace ESET Management Agenta vyžadováno **heslo**. Další informace naleznete v kapitole ochrana agenta.

Obecné

Zadejte **název** nové politiky. Pole **Popis** je nepovinné.

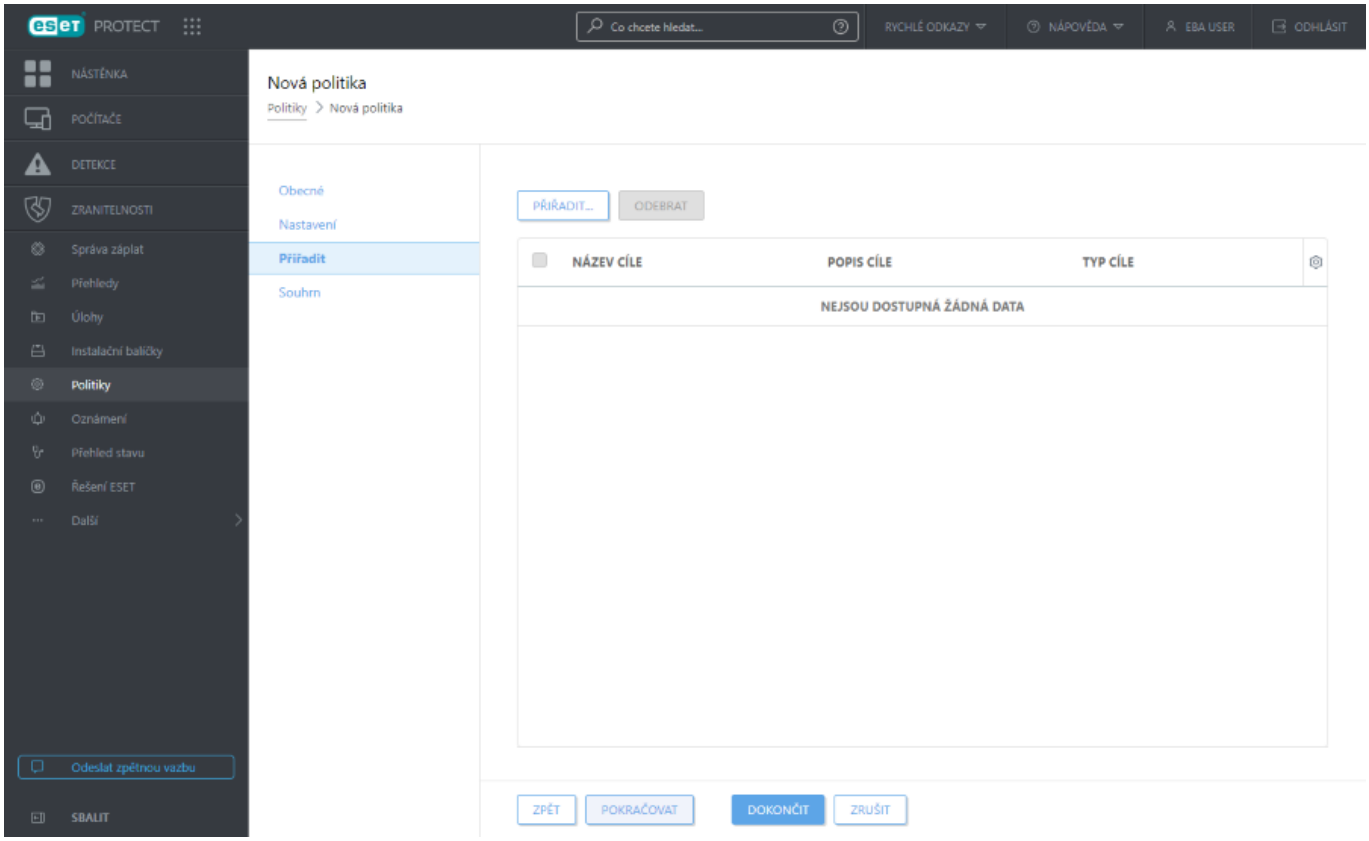
Nastavení

V rozbalovacím menu vyberte **ESET Management Agent** > rozbalte položku **Nastavení** > klikněte na **Nastavit** vedle položky **Nastavení chráněné heslem** a zadejte heslo. Toto heslo bude vyžadováno při pokusu o odinstalování nebo opravení produktu ESET Management.

Uložte si heslo na bezpečné místo. Pokud je Agent ESET Management chráněný heslem, pro odinstalaci, opravu nebo aktualizaci (se změnami) je nutné zadat heslo.

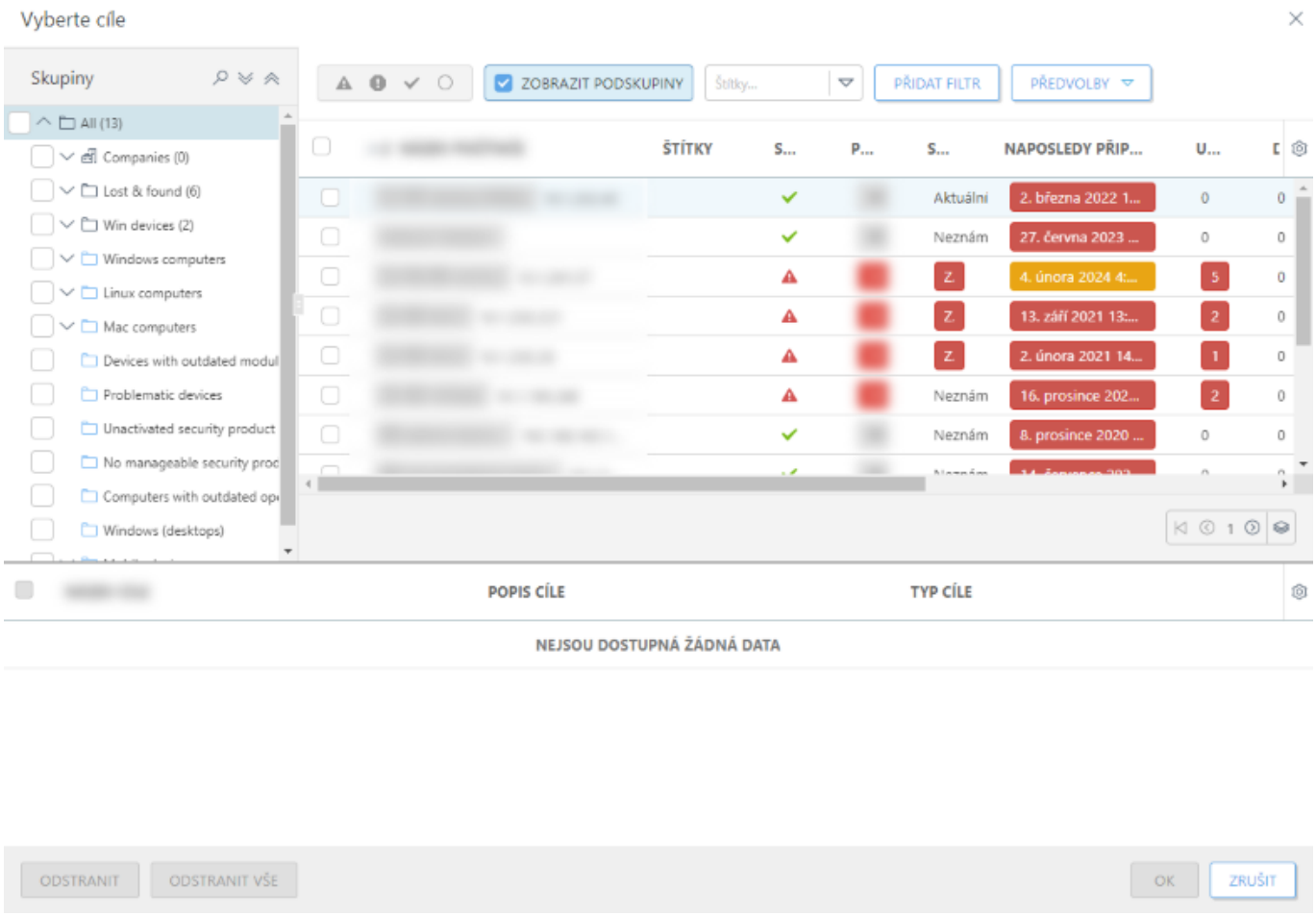
Přiřadit

V této části vyberte cíl (počítač nebo skupinu), kterému chcete danou politiku přiřadit.



Po kliknutí na tlačítko **Přiřadit** se zobrazí dialogové okno se všemi statickými i dynamickými skupinami. Vyberte požadovaný cíl (zařízení nebo skupina) a klikněte na tlačítko **OK**.

Pro zajištění, že se objekt aplikuje na všechna zařízení ve skupině, místo výběru jednotlivých stanic vyberte jako cíl celou skupinu. Zabráníte tím zároveň zpomalení Web Console.
Pokud vyberte velké množství počítačů, Web Console zobrazí varování.



Souhrn

Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**. Politika se na cíl aplikuje při jeho příštím připojení k ESET PROTECT.

Pro okamžité aplikování politiky můžete na cílový **počítač** odeslat **žádost o probuzení** (Wake-up Call).

Řešení problémů – Agent se nepřipojuje

Pokud se klient po nainstalování ESET Management Agenta stále nepřipojuje k ESET PROTECT serveru, je potřeba příčinu problému hledat lokálně na klientské stanici.

Ve výchozím nastavení se ESET Management Agent připojuje k ESET PROTECT Server standardně každých 10 minut.

Zkontroluje nejnovější protokol ESET Management Agenta. Naleznete jej ve složce:

Windows	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*
Linux	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
macOS	*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/* */Users/%user%/Library/Logs/EraAgentInstaller.log*

• **last-error.html** – protokol (tabulka) souhrnně zobrazující poslední zaznamenané chyby běhu ESET Management agenta.

• **software-install.log** – textový protokol poslední úlohy vzdálené instalace, kterou ESET Management Agent provedl.

• **trace.log** – podrobný protokol zahrnující veškeré činnosti i chyby ESET Management Agenta.

> Pro aktivaci diagnostického protokolování ESET Management Agenta vytvořte ve složce se souborem *trace.log* prázdný soubor *traceAll* (bez přípony) a restartujte počítač (aby došlo k restartování služby ESET Management Agenta).

• **status.html** – tabulka ukazující aktuální stav komunikace (synchronizace) ESET Management agenta s ESET PROTECT serverem. V protokolu je zároveň uvedena konfigurace HTTP Proxy, seznam aplikovaných politik (včetně aplikovaných výjimek) společně s informací, jakých dynamických skupin je zařízení členem.

Mezi nejčastější důvody, proč se ESET Management agent nedokáže spojit s ESET PROTECT, patří nesprávně fungující DNS server nebo blokování používaných portů na firewallu. Pro vyřešení se podívejte na seznam portů, které ESET PROTECT používá. Informace o upozornění **Zařízení používá připojení s podporou převzetí služeb při selhání** najdete v článku naší Databáze znalostí.

Hlavní menu ESET PROTECT

Všechny klienty můžete spravovat prostřednictvím webové konzole ESET PROTECT. Webová konzole ESET PROTECT je dostupná z jakéhokoli zařízení s podporovaným internetovým prohlížečem. **Hlavní menu** je neustále dostupné v levé části obrazovky, kromě případu, kdy je aktivní průvodce prvotním spuštěním. Menu si můžete v případě potřeby zmenšit kliknutím na ikonu **Sbalit menu**. Pro obnovení jeho velikosti klikněte na ikonu

Hlavní menu ESET PROTECT v levé části obrazovky obsahuje následující záložky:

Nástěnka
Spravované zákaznice/zákazníci
Počítače
Detekce
Zranitelnosti
Správa záplat
Přehledy
Úlohy
Instalační balíčky
Politiky
Oznámení
Stav serveru
ESET řešení
Další

Nástěnka

Nástěnka je výchozí stránka, která se zobrazí po přihlášení do ESET PROTECT Web Console. Standardně zobrazuje předdefinované přehledy o stavu vaší sítě. Prostřednictvím záložek v horní části se můžete přepínat mezi jednotlivými částmi nástěnky. Na každé nástěnce jsou umístěny jednotlivé přehledy.

Práce s nástěnkou

- **Přidat** – kliknutím na ikonu + v záhlaví nástěnky vytvoříte novou záložku. Zadejte název nástěnky a akci dokončete kliknutím na **Přidat nástěnku**. Tím se vám vytvoří prázdná nástěnka, na kterou si můžete přidat přehledy.

- **Přesunout** – klikněte vlevo vedle názvu nástěnky a pomocí techniky drag & drop ji přesuňte na požadované místo.

- Každou nástěnku si můžete přizpůsobit svým potřebám přidáním vlastních přehledů i úpravou již existujících. Můžete měnit také velikost zobrazených přehledů včetně jejich pozice.

- Vyberte nástěnku, klikněte na ikonu ozubeného kola nahoře (vedle) a vyberte možnost **Nastavit jako výchozí**, aby se tato nástěnka používala jako výchozí pro všechny nové uživatele webové konzole s přístupem k Nástěnce.

- MSP uživatelé mohou kliknutím **Vybrat** vedle **MSP zákazníka** filtrovat zobrazení nástěnky pro vybraného zákazníka.

Kliknutím na ozubené kolečko vpravo od názvu nástěnky se zobrazí kontextové menu, ve kterém jsou dostupné následující akce:

Aktualizovat	Kliknutím aktualizujete zobrazená data generovaného přehledu.
Odstranit	Kliknutím odstraníte nástěnku.
Přejmenovat	Kliknutím můžete změnit název nástěnky.
Duplikovat...	Kliknutím vytvoří kopii nástěnky ve své domovské složce.
Změnit rozložení	Pomocí této možnosti si můžete změnit rozložení nástěnky. Při změně může dojít k odstranění přehledů, které se do stávajícího rozložení nevejdou.

Tyto výchozí nástěnky nelze přizpůsobit: **Přehled stavu**, **Přehled bezpečnosti**, **ESET LiveGuard** a **ESET Inspect**.

Ve výchozím stavu je nástěnka ESET PROTECT rozdělena do následujících částí:

Přehled stavu

Nástěnka **Přehledu stavu** je výchozí, a zobrazí při prvním přihlášení do ESET PROTECT (pokud si nenastavíte jinou nástěnku jako výchozí). Naleznete zde souhrnné informace o stavu vámi spravované sítě.

Počet zařízení – zobrazuje počet spravovaných zařízení a filtrovaných podle naposledy reportovaného stavu. Kliknutím na konkrétní dlaždici se přepnete na záložku Počítače s aktivovaným filtrem.

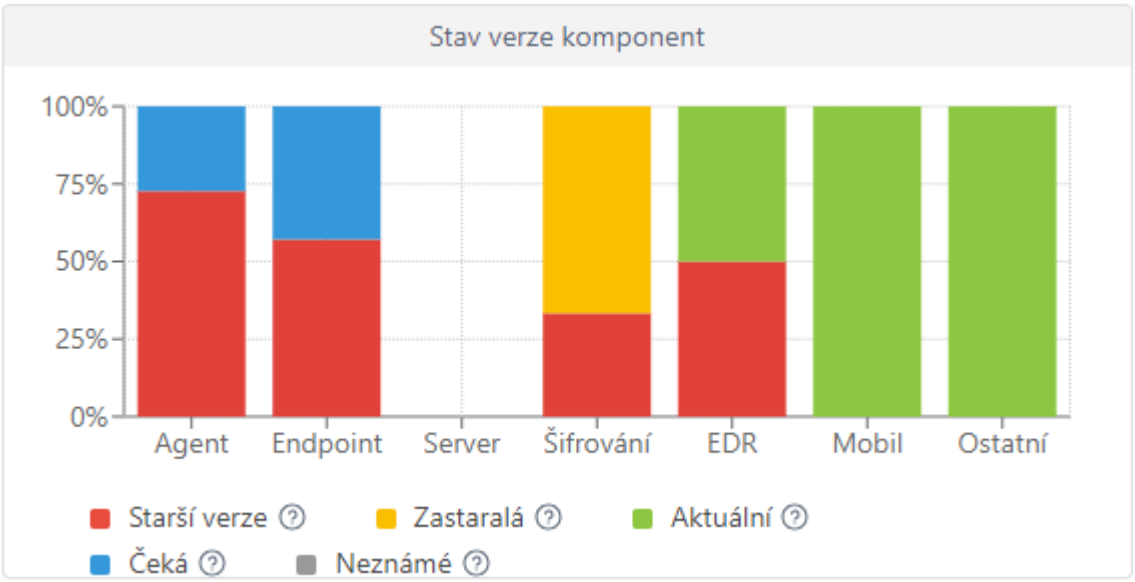
Stav zařízení – zobrazuje počty spravovaných zařízení agregované podle platformy. Pokud ve skupině není žádné

zařízení, zobrazí se informace popisující jejich připojení prostřednictvím instalačního balíčku.

Stav připojení – zobrazuje poměr naposledy připojených spravovaných zařízení.

Stav verze komponent

Tento graf zobrazuje poměr mezi aktuálními a zastaralými verzemi bezpečnostních produktů ESET a jejich komponent.



Kliknutím na žlutou/červenou část grafu reprezentující zastaralé aplikace můžete po vybrání možnosti **Aktualizovat nainstalované ESET produkty** inicializovat jejich aktualizaci. Doporučujeme se seznámit s životním cyklem firemních produktů.

- **Červená** – zastaralá verze komponenty/produktu ESET nebo verze, ve které byly objeveny závažné zranitelnosti (tato verze již není podporovaná a není dostupná v repozitáři).

- **Žlutá** (**zastaralá**) – nainstalovaná verze komponenty/produktu ESET je zastaralá, ale stále podporovaná. Podporovány a ve žlutém stavu jsou obvykle dvě verze dozadu od nejnovější verze, pokud však neobsahují nedávno objevené bezpečnostní zranitelnosti.

- **Zelená** (**OK**) – máte nainstalovanou nejnovější verzi komponenty/řešení ESET nebo poslední nainstalovaná verze komponenty/řešení ESET je kompatibilní s používanou verzí ESET PROTECT Web Console.

> Pokud se v ESET repozitáři nenachází novější kompatibilní verze komponenty/produktu ESET pro konkrétní verzi operačního systému nebo platformu (x86, x64, ARM64), je tato starší verze komponent/produktů ESET reportována se stavem **OK** (**zeleně**).

- **Modrá** (**čeká**) – automatické aktualizace jsou zapnuté a nejnovější verze se nainstaluje automaticky. Automatické aktualizace podporují:

  - ESET Management Agenti

- Bezpečnostní produkty ESET

> Pokud se komponenty ESET delší dobu neaktualizovaly, můžete je aktualizovat ručně kliknutím na modrý sloupec graf a vybráním možnosti **Aktualizovat nainstalované komponenty ESET**. Případně můžete použít klientskou úlohu Aktualizace Agenta pro aktualizaci Agentů a klientskou úlohu Instalace aplikace pro aktualizaci bezpečnostních řešení ESET.

- **Šedivá** (**neznámá**) – nebyla rozpoznána verze nainstalované komponenty/produktu ESET (to se může stát například v brzké době od instalace produktu ESET).

Stav spravované sítě – zobrazuje počet **spravovaných a chráněných** (stanice s agentem a bezpečnostním produktem), **spravovaných** (stanice s agentem), **nespravovaných** (stanice přidané do ESET PROTECT, ale zatím na nich nemáte nainstalovaného agenta) a **nalezených** (stanice, které ESET PROTECT nezná a detekoval je nástroj ESET Rogue Detection Sensor) zařízení ve vaší síti.

RSS kanál – zobrazuje RSS kanál z WeLiveSecurity a ESET Centra technické podpory (při vybrání češtiny z portálu servis.eset.cz). Kliknutím na ikonu ozubeného kolečka můžete **vypnout automatické přehrávání**, případně **deaktivovat** konkrétní **RSS kanál**.

Přehled incidentů

Na této nástěnce máte přehled o všech nevyřešených detekcích za posledních 7 dní seskupených podle způsobu detekce, závažnosti a také přehled zařízení a uživatelů s největším výskytem detekcí.

ESET LiveGuard

Pokud používáte ESET LiveGuard Advanced, naleznete zde užitečné přehledy týkající se této služby. Klikněte na ikonu ozubeného kola nahoře (vedle) a vyberte možnost **Skrýt/Zobrazitt ESET LiveGuard** pro skrytí nebo zobrazení dané nástěnky.

ESET Inspect

Pokud používáte ESET Inspect, naleznete zde mnoho statistických dat z ESET Inspect. Kliknutím na objekt si otevřete jeho detaily v ESET Inspect konzoli. Kliknutím na ikonu ozubeného kolečka v horní části (vedle) se můžete pomocí možnosti **Skrýt/Zobrazit ESET Inspect** rozhodnout, zda chcete mít k dispozici nástěnku, která se týká této služby.

Na této záložce naleznete následující informace týkající se ESET Inspect:

- **Nevyřešené detekce podle závažnosti** – celkový počet nevyřešených detekcí a přehled nevyřešených detekcí podle závažnosti – informační, varování nebo kritická.

- **Detekce podle závažnosti za posledních 7 dní** – kombinovaný spojnicový graf zobrazující počet detekcí podle závažnosti za posledních 7 dní

- **Top 10 počítačů s incidenty za posledních 7 dní** – název počítače, počet počítačů podle závažnosti detekce (červená – kritická, žlutá – varování, modrá – informační) a celkový počet detekcí

- **Počítače podle závažnosti detekce** – prstencový graf zobrazující počet počítačů podle závažnosti detekce – informační, varování a kritická.

• **Incidenty** – počet incidentů (vytvořených v ESET Inspect) podle stavu (**Otevřený**, **V řešení**, **Čeká**, **Vyřešeno**, **Uzavřeno** a **Neplatný**). Pro zobrazení více informací v ESET Inspect klikněte na číslo vedle stavu incidentu. Pokud pracovník ESET Technické podpory upraví incident v ESET Inspect, incident bude označený jako **Analyzováno společností ESET**.

ESET Cloud Office Security

Pokud používáte ESET Cloud Office Security, pomocí nástěnky si z něj zobrazíte přehled statistických dat. Kliknutím na objekt si otevřete jeho detaily v ESET Cloud Office Security konzoli. Klikněte na ikonu ozubeného kola nahoře (vedle ikony pro obnovení) a vyberte možnost **Skrýt/Zobrazit ESET Cloud Office Security** pro skrytí nebo zobrazení dané nástěnky.

ESET Cloud Office Security dlaždice obsahují následující informace:

• **Chránění uživatelé** – počet chráněných uživatelů

• **Využití licence** – počet použitých a nepoužitých licencí

• **Chráněné stránky SharePoint** – Počet chráněných webových stránek SharePoint

• **Chráněné skupiny Teams** – Počet chráněných skupin Teams

• **10 nejčastějších uživatelů s detekcemi za posledních 30 dní**- jméno a e-mail s počtem detekcí e-mailů a souborů u 10 nejčastějších uživatelů

• **Detekce za posledních 30 dní** – histogramový graf s počtem detekcí v konkrétních službách (**Teams**, **SharePoint**, **E-mail**, **Disk**) za posledních 30 dní; kliknutím na libovolnou službu v histogramovém grafu si otevřete Detekce v okně ESET Cloud Office Security

• **Objekty v karanténě** – počet objektů v karanténě nalezených v konkrétních službách za posledních 7 a 30 dní. Po kliknutí na libovolný řádek služby se zobrazí stránka Karantény v ESET Cloud Office Security

Počítače

Na této nástěnce naleznete přehled o spravovaných klientech jako je stav ochrany, informace o operačním systému, chybějících aktualizacích atp.

Detekce antivirem

Poskytuje informace získané od antivirového modulu na jednotlivých klientech – aktivní detekce, detekce zaznamenané za posledních 7/30 dní, atp.

Detekce firewallem

Přehled o všech zaznamenaných síťových událostech jsou seřazené dle jejich závažnosti., času hlášení atd.

ESET aplikace

Tato nástěnka zobrazuje informace o stavu nainstalovaných aplikací ESET.

Cloudová ochrana

Na této nástěnce máte k dispozici přehledy související s cloudovou ochranou vaší sítě zajišťovanou službou ESET LiveGrid® a v případě, že máte odpovídající licenci, též ESET LiveGuard Advanced.

ESET MDR

ESET MDR poskytuje přehled o incidentech a detekcích z ESET Inspect. Používání ESET MDR vyžaduje licenci ESET Inspect a úroveň **ESET PROTECT MDR**.

> **Dostupnost ESET MDR v jednotlivých zemích**
> ESET MDR je k dispozici v následujících zemích: USA, Kanada, Japonsko, Velká Británie, Nizozemsko, Francie, Itálie, země DACH (Německo, Rakousko, Švýcarsko), severské země (Švédsko, Norsko, Dánsko, Finsko, Island), Slovensko, Česká republika, Ukrajina.

Služba ESET MDR se vztahuje na všechna spravovaná zařízení se spuštěným programem ESET Inspect. Podle následujících kroků vyberte zařízení, u kterého chcete spravovat zabezpečení nezávisle na službě ESET MDR:

1. Otevřete ESET PROTECT a přejděte do sekce **Počítače**.
2. Klikněte na ikonu ozubeného kola vedle existující nadřazené statické skupiny a vyberte možnost **Nová statická skupina**.
3. Do pole **Název** zadejte `exempt` a klikněte na **Dokončit**.
4. Vyberte nadřazenou skupinu a vyberte zařízení, která chcete zahrnout do skupiny pro vyloučená zařízení.
5. Klikněte na tlačítko **Počítač** > **Spravovat** > **Přesunout do skupiny** a vyberte skupinu `exempt`.

Zařízení ve skupině `exempt` spravujete vy sami – incidenty můžete řešit ručně bez automaticky aplikovaných reakcí.

> K zobrazení **ESET MDR** na Nástěnce potřebujete následující sady oprávnění:
> • **Přehledy ESET MDR** – použít
> • **Přístup do ESET Inspect** – číst
> Data v dlaždicích se zobrazují na základě vlastních sad oprávnění v ESET Inspect a ESET PROTECT.

Po kliknutí na dlaždici si otevřete detaily ve webové konzoli ESET Inspect.

Dlaždice **ESET MDR** zobrazují následující informace:

- **Incidenty** – počet incidentů podle úrovně závažnosti za posledních sedm dní – **celkem**, **vysoká**, **střední** a **nízká**
- **Nejčastější nevyřešené incidenty** – seznam nejčastějších incidentů za posledních sedm dní – **název incidentu**, **autor**, **datum vytvoření**, **ovlivněná zařízení**, **stav** a **komu byl přidělen**
- **Stav incidentu** – prstencový graf s počtem incidentů podle jejich stavu za posledních sedm dní – **otevřený**, **probíhá**, **pozdržený**,**vyřešený**, **uzavřený** a **neplatný**
- **Nejčastěji ovlivněná zařízení** – seznam nejvíce ovlivněných zařízení podle úrovně závažnosti za posledních sedm dní – **název zařízení**, **incidenty** (úroveň závažnosti – **informativní**, **varování** nebo **kritická**), **název**

skupiny a **naposledy viděno**

• **Reakce** – prstencový graf s počtem reakcí na incident za posledních sedm dní – **zablokovat**, **vyléčit a zablokovat**, **izolovat** a **ukončit proces**

• **Tok incidentů** – **počet všech detekcí**, **počet detekcí souvisejících s incidenty** a **počet vytvořených incidentů** za posledních sedm dní

• **Incidenty v čase** – liniový graf s počtem incidentů zjištěných za posledních sedm dní podle úrovně závažnosti – **vysoká**, **střední** a **nízká**

Na každé dlaždici můžete kliknout na tlačítko ⋮ a:

• **Zobrazit vše** – kliknutím se dostanete do webové konzole ESET Inspect. Budete přesměrováni na konkrétní stránku s nastaveným filtrem (Čas vytvoření 7 dní)

• **Aktualizovat** – kliknutím obnovíte konkrétní dlaždici

Viz také Přehled ESET MDR.

Dostupné akce pro přehledy na nástěnce

Změnit velikost	Kliknutím zobrazíte přehled v režimu celé obrazovky.
Aktualizovat	Aktualizuje šablonu přehledu.
Stáhnout	Pro vygenerování a stažení přehledu klikněte na tlačítko **Vygenerovat a stáhnout**. Vybrat si můžete formát *.pdf* nebo *.csv*. CSV je vhodný formát pouze pro tabulková data a jako oddělovač je použit středník ;. Pokud si stáhnete přehled ve formátu CSV a ve sloupci, ve kterém očekáváte text, jsou uvedena čísla, pro korektní zobrazení dat si stáhněte přehled ve formátu PDF.
Změnit…	Umožňuje změnit šablonu přehledu za jinou ze seznamu šablon.
Změnit šablonu přehledu	Kliknutím upravíte šablonu přehledu. Následně se zobrazí průvodce, stejný jako při vytváření nové šablony přehledu.
Nastavit interval aktualizace	Umožňuje nastavit vlastní interval mezi aktualizacemi zobrazených dat.
Naplánovat	Naplánovat přehled – po kliknutí se zobrazí dialogové okno, ve kterém můžete definovat podmínku spuštění, kritérium a způsob doručení přehledu. Všechny naplánované přehledy naleznete na záložce **Naplánované přehledy.**
Odstranit	Odstraní šablonu přehledu z nástěnky.
Přejmenovat	Umožňuje přejmenovat šablonu přehledu.
Tato buňka	Umožňuje změnit rozložení nástěnky. Tato změna odstraní aktuální šablony z nástěnky.

Oprávnění pro nástěnku

Aby měl k šabloně uživatel přístup, musí mít přiděleno potřebné oprávnění. Na nástěnce lze použít pouze šablony přehledů ze skupiny, ke které má uživatel přístupové oprávnění. Pokud uživatel nemá žádná oprávnění pro čtení **přehledů a nástěnku**, nezobrazí se mu na nástěnce žádná data. Ve výchozím nastavení vidí administrátor všechna data.

• **Číst** – uživatel může zobrazit šablony přehledů a jejich kategorie, generovat přehledy na základě šablon a číst jejich nástěnku
• **Použít** – uživatel může upravovat svou nástěnku s dostupnými šablonami přehledů
• **Psát** – uživatel může vyvářet, upravovat nebo odstraňovat šablony a jejich kategorie
Všechny výchozí šablony se nacházejí ve skupině pro **všechna zařízení**.

Kontextové menu

Použitím kontextového menu na nástěnce se dostanete k bližším informacím. Umožňuje interaktivně vybrat konkrétní položky z přehledu a zobrazit o nich podrobné údaje. To znamená, že po kliknutí do přehledu si můžete zobrazit detailní informace (agregovaná data), případně provést související akci. Kontextové menu je dostupné na více úrovních.

V závislosti na kontextu jsou dostupné následující možnosti:

• Zobrazit **Detailní informace** – název počítače a jeho popis, název statické skupiny, do které zařízení patří atp. Zobrazí originální (neagregovaná) data pro vybraný řádek.

• Zobrazit **pouze** *„hodnotu“* – zobrazí pouze data s vybranou úrovní závažnosti: informativní, kritické, bezpeční rizika, bezpečnostní oznámení, atp.

• **Rozbalit sloupec** *"hodnota"* – zobrazí se agregované informace (obvykle jde o počet nebo součet). Například pokud je ve sloupci zobrazena pouze číslice a kliknete na možnost Rozbalit sloupec Počítač, zobrazí se detailní informace o počítačích.

• Zobrazit **Na záložce Počítače (všechny)** – přesměruje vás na záložku **Počítače** a zobrazí prvních 100 výsledků.

Akce jedním kliknutím

Po kliknutí do tabulky nebo grafu s přehledy zobrazujícími informace o nalezených problémech se v kontextovém menu zobrazí dodatečné položky:

• '*Úloha vedoucí k vyřešení upozornění*' – kliknutím na tuto možnost naplánujete na klientovi spuštění navržené úlohy (s podmínkou spuštění ihned).

Pokud situaci není možné vyřešit prostřednictvím úlohy a její řešení spočívá v úpravě konfigurace, zobrazí se následující možnosti:

o**Správa politik**

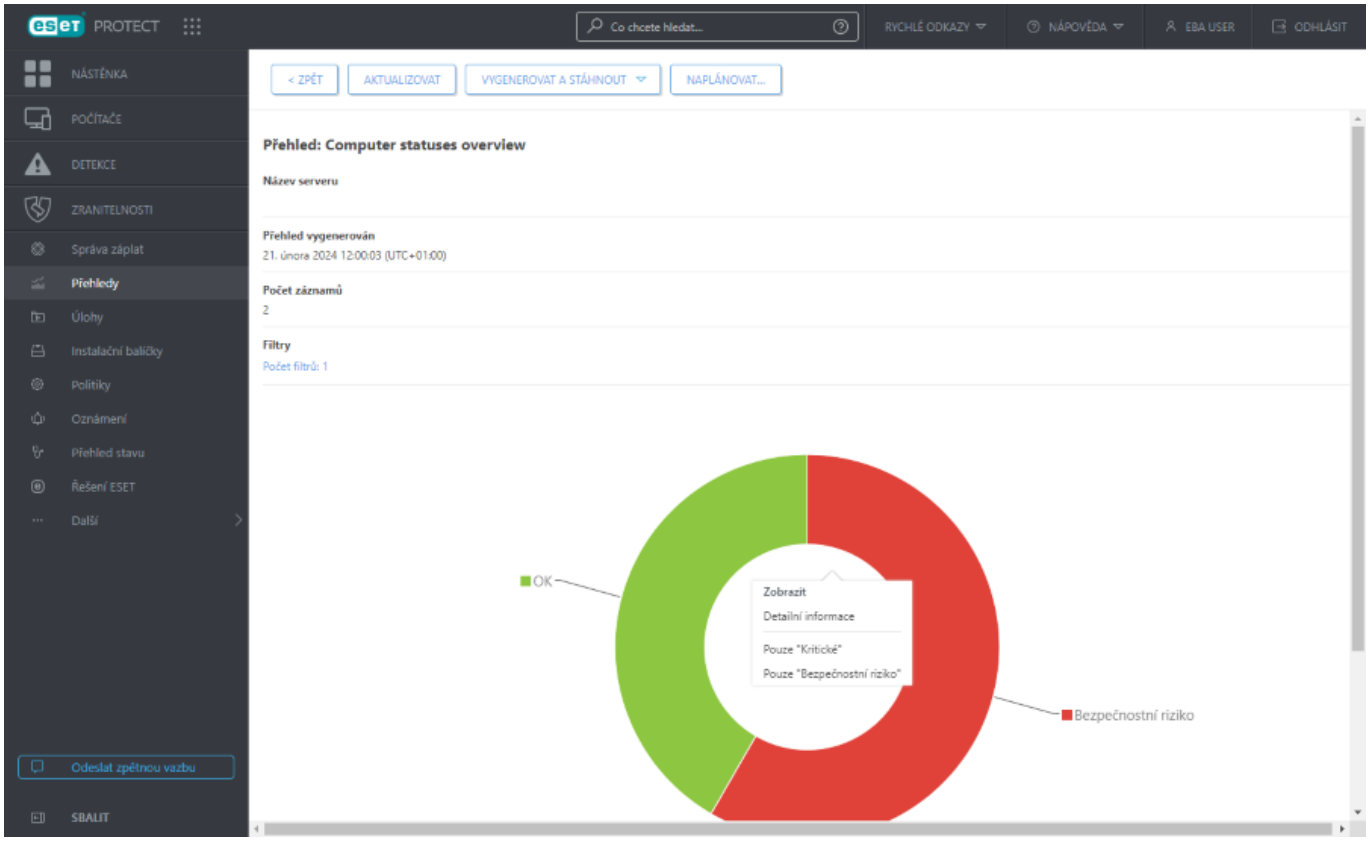
o**Nová politika**

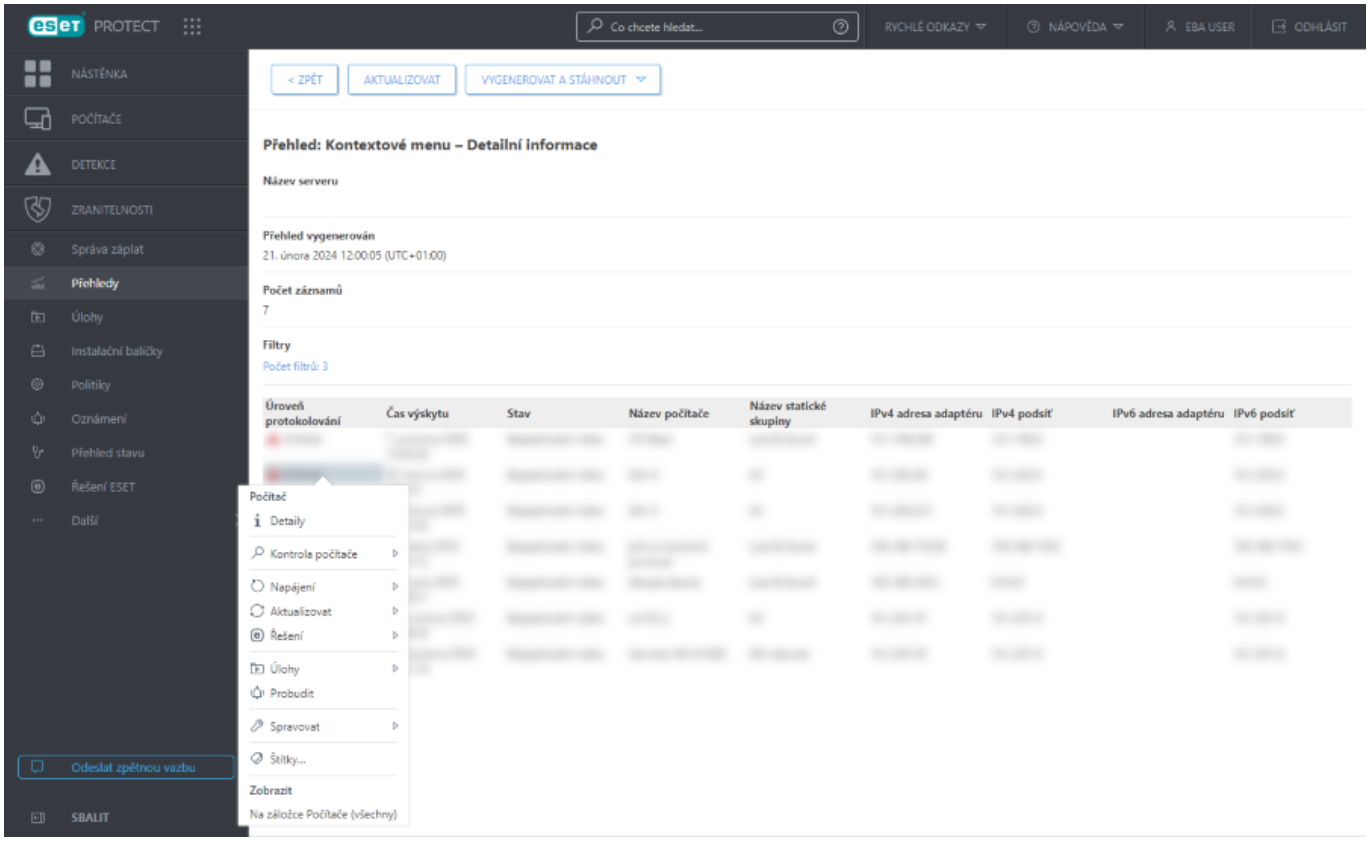
• **Najít na webu** – po vybrání této možnosti se text daného upozornění vyhledá prostřednictvím vyhledávače Google. Tuto možnost můžete využít v případě, kdy není dostupná žádná související akce (klientská úloha nebo úprava politiky), a zkusit řešení vyhledat na internetu.

Po vybrání libovolné možnosti se zobrazí prvních 1 000 záznamů.

Kliknutím na tlačítko **Vygenerovat a stáhnout** si můžete přehled stáhnout do svého PC. Vybrat si můžete formát *.pdf* nebo *.csv*. CSV je vhodný formát pouze pro tabulková data a jako oddělovač je použit středník `;`. Pokud si

stáhnete přehled ve formátu CSV a ve sloupci, ve kterém očekáváte text, jsou uvedena čísla, pro korektní zobrazení dat si stáhněte přehled ve formátu PDF.





Spravovaní zákazníci

Sekce **Spravovaní zákazníci** v hlavním okně ESET PROTECT je k dispozici pouze MSP uživatelům (Managed Service Provider).

V sekci **Spravovaní zákazníci** může MSP uživatel vidět seznam spravovaných zákazníků:

- Kliknutím na jméno zákazníka zobrazíte podrobnosti o něm – jde o podrobnosti o statických skupinách, protože statické skupiny v ESET PROTECT představují zákazníky
- Kliknutím na číslo v tabulce získáte podrobnosti o zařízeních, detekcích (nevyřešených) a licencích zákazníka

Hlavní tabulku můžete přizpůsobit (upravit zobrazené sloupce, přidat nebo odebrat sloupce).

Filtrování spravovaných zákazníků

Spravované zákazníky můžete filtrovat podle jejich jména:

- V sekci **Spravovaní zákazníci**Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře. Můžete také použít Předvolby filtru
- V ostatních sekcích webové konzole na Nástěnce při plánování nebo generování přehledu

Počítače

Všechna zařízení přidaná do ESET PROTECT naleznete v této sekci rozdělené do skupin. Každé zařízení členem právě jedné statické skupiny. Po kliknutí na konkrétní skupinu se v pravé části zobrazí seznam všech klientů, kteří se nacházejí v dané skupině.

Nespravovaná zařízení (stanice bez ESET Management Agenta) se nacházejí ve skupině **Ztráty a nálezy**. Stav, který je zobrazený u klienta v ESET PROTECT se může lišit od toho, co se zobrazuje uživatelům klientských stanic v hlavním okně bezpečnostních řešení. Proto, i když se určitý stav uživateli klientského zařízení nezobrazí, přesto může být ve webové konzoli ESET PROTECT hlášen. Pro přesunutí stanice do jiné skupiny můžete využít například techniku drag & drop.

Po kliknutí na tlačítko **Přidat zařízení** se zobrazí následující možnosti:

- **Počítače** – vybráním přidáte počítače do dané statické skupiny.
- **Mobilní zařízení** – vybráním přidáte mobilní zařízení do dané statické skupiny.

Kliknutím na zařízení se zobrazí kontextové menu s dostupnými akcemi, které nad zařízením můžete provést. Najednou můžete vybrat více zařízení a poté v dolní části obrazovky kliknout na tlačítko **Počítač**. Seznam dostupných akcí v menu **Počítač** se může v závislosti na zařízení (počítač/telefon) lišit. Více informací o jednotlivých ikonách a stavech naleznete v této kapitole. Kliknutím na číslo ve sloupci **Upozornění** budete přesměrování do odpovídající sekce v detailech počítače.

Ve sloupci **Naposledy připojeno** je uvedeno datum a čas posledního připojení spravovaného zařízení k serveru. Symbol zelené tečky značí, že se počítač naposledy k serveru připojil před méně než 10 minutami. V závislosti na hodnotě ve sloupci **Naposledy připojeno** se informace zvýrazní, abyste mohli snáze rozpoznat nepřipojující se zařízení

- Žlutá (chyba) – zařízení se k serveru nepřipojilo 2 až 14 dnů.
- Červená (varování) – zařízení se k serveru připojilo více než 14 dnů.

> Zaregistrovaná mobilní zařízení se musí k ESET PROTECT připojit jednou za 120 dní, aby se předešlo problémům s připojením. Tyto informace jsou uvedeny v registračním e-mailu nebo v QR kódu. Náhradní zařízení předem neregistrujte. Doporučujeme zaregistrovat pouze ta náhradní zařízení, která se budou používat v průběhu následujících 120 dní.

Po kliknutí na ikonu **Inspect** si v ESET Inspect Web Console zobrazíte sekci Počítače. Tlačítko ESET Inspect je dostupné pouze v případě, že vlastníte licenci na ESET Inspect a ESET Inspect máte připojen k ESET PROTECT. Uživatel Web Console potřebuje alespoň sadu oprávnění s hodnotou **pouze pro čtení** u možnosti **Přístup k ESET Inspect**.

Filtrování

Zařízení můžete filtrovat mnoha způsoby:

- Standardní filtr: Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře.

- Zařízení můžete filtrovat podle stavu: červená – **Chyby**, žlutá – **Varování**, zelená – **OK** a šedá – **Nespravovaná** zařízení. Ikona představuje aktuální stav bezpečnostního produktu ESET na daném klientovi. Kombinací jednotlivých filtrů můžete zobrazit pouze klienty, kteří vyhovují aktivním filtrům. Například pro zobrazení pouze počítačů s upozorněním ponechte aktivním oranžovou ikonu a zbývající deaktivujte. Pro zobrazení pouze klientů s upozorněním a chybami nechte aktivní červenou a oranžovou ikonu.

- Po kliknutí na **Přidat filtr** > **Kategorie produktu** můžete filtrovat konkrétní typy zařízení nebo počítače podle nainstalovaných produktů.

  - **Chráněno produktem ESET** – chráněné jsou Pracovní plocha, Mobil, Server, Poštovní server, Gateway Server, Kolaborační server, Souborový server.

  - **ESET PROTECT** – jednotlivé komponenty ESET PROTECT – ESET Management Agent, Rogue Detection Sensor.

  - **Ostatní** – ESET LiveGuard, ESET Inspect Connector, ESET Full Disk Encryption, ESET Bridge, ESET Správa zranitelností a záplat.

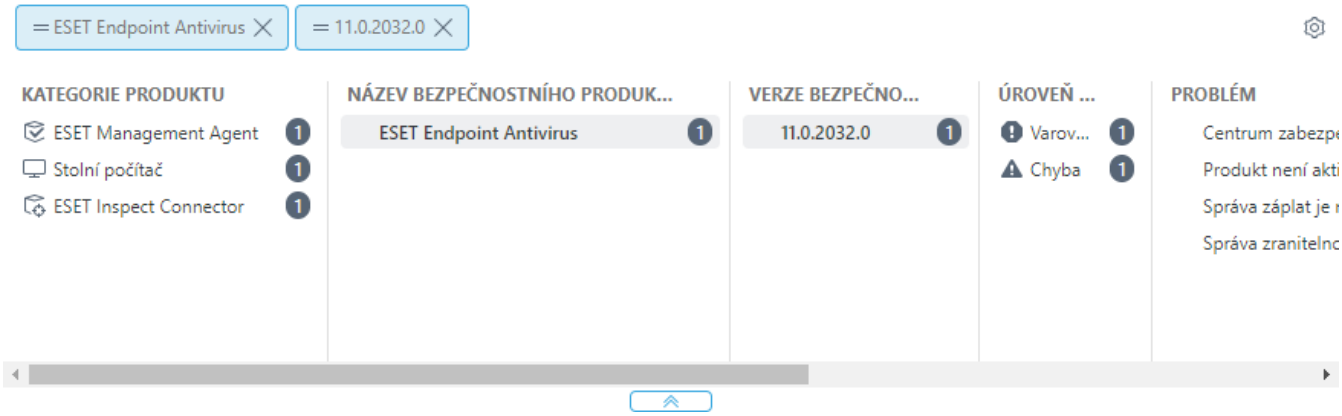
- Zaškrtnutím možnosti **Zobrazit podskupiny** zobrazíte také zařízení, která se nacházejí v podskupinách právě vybrané skupiny.

- V horní části obrazovky se seznamem **počítačů** se nachází rozbalovací panel **Pokročilé filtry**.

Na tomto panelu se v reálném čase zobrazuje náhled hodnot jednotlivých filtrů společně s přesným počtem výsledků.

Při filtrování většího množství počítačů díky pokročilým filtrům zjistíte, které hodnoty filtru vrátí zvládnutelný počet výsledků, a dokážete tak mnohem rychleji najít požadovaná zařízení.

Filtr aplikujete kliknutím na konkrétní položku ve sloupci. Aplikované filtry rozeznáte podle toho, že se u nich nachází modrá bublina. Kliknutím na aplikovaný filtr přepněte režim filtrování z **rovná se** na **nerovná se** (a opačně).



Pro seřazení hodnot v daném sloupci klikněte na ikonu ozubeného kolečka v tabulce, případně klikněte na ikonu ozubeného kola v horní části na panelu Pokročilých filtrů. Pomocí této možnosti můžete přidat, odebrat a ↓ ↑ změnit pořadí zobrazených sloupců. Při správě sloupců můžete využít techniku drag and drop. Kliknutím na **Obnovit** obnovíte sloupce tabulky do výchozího stavu (výchozí dostupné sloupce ve výchozím pořadí).

> Pokročilé filtrování je dostupné pouze nad statickými skupinami. V dynamických skupinách není možné používat pokročilé filtry.

- Pro pokročilé filtrování počítačů využijte dynamické skupiny nebo přehledy.
- Pro nalezení počítačů označených jako Master pro klonování klikněte na tlačítko **Přidat filtr**, v seznamu vyberte **Master pro klonování** a filtr aktivujte pomocí **zaškrtávacího políčka**.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.

- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

> Pokud v seznamu nemůžete najít určitý počítač a víte, že je v infrastruktuře ESET PROTECT, ujistěte se, že jsou vypnuty všechny filtry.

Detaily počítače

Pro zobrazení detailních informací o konkrétním zařízení si jej najděte ve statické nebo dynamické skupině, klikněte na daný řádek a v kontextovém menu vyberte možnost **Detaily**. Kliknutím na název zařízení vyvoláte postranní panel s Náhledem počítače.

Po kliknutí na ikonu **Inspect** si zobrazíte sekci Počítače v ESET Inspect Web Console. Tlačítko ESET Inspect je dostupné pouze v případě, že vlastníte licenci na ESET Inspect a ESET Inspect máte připojen k ESET PROTECT. Uživatel Web Console potřebuje alespoň sadu oprávnění s hodnotou **pouze pro čtení** u možnosti **Přístup k ESET Inspect**.

Zobrazená data jsou v dialogovém okně rozdělena do následujících kategorií:

Přehled

Počítač

- Název zařízení nebo popis si můžete kdykoli změnit kliknutím na ikonu . Pokud již v síti zařízení s daným názvem máte, vyberte v průběhu úpravy jména možnost **Povolit duplicitní názvy**.
- Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
- **FQDN** – plně kvalifikovaný název zařízení.
- **Nadřazená skupina** – statická skupina, do které zařízení patří.
- **IP adresa** – IP adresa zařízení.
- **Počet aplikovaných politik** – číslo reprezentující, kolik je na zařízení aplikováno politik.
- **Člen dynamických skupin** – seznam dynamických skupin, jejichž podmínkám při poslední replikaci vyhovovalo (nemusí být však aktuálně jejich členem).

Hardware

V této části naleznete základní informace o hardware daného zařízení včetně jeho identifikátorů a nainstalovaném operačním systému. Po kliknutí na tuto dlaždici budete přesměrování na záložku **Detaily** > **Hardware**. Další informace naleznete v kapitole Inventář hardware.

Upozornění

- **Upozornění** – odkaz na seznam problémů.
- **Počet nevyřešených detekcí** – číslo reprezentující počet nevyřešených detekcí na zařízení. Po kliknutí budete přesměrováni na záložku se seznamem nevyřešených detekcí.

• **Naposledy připojeno** –Ve sloupci **Naposledy připojeno** je uvedeno datum a čas posledního připojení spravovaného zařízení k serveru. Symbol zelené tečky značí, že se počítač naposledy k serveru připojil před méně než 10 minutami. V závislosti na hodnotě ve sloupci **Naposledy připojeno** se informace zvýrazní, abyste mohli snáze rozpoznat nepřipojující se zařízení

  oŽlutá (chyba) – zařízení se k serveru nepřipojilo 2 až 14 dnů.

  oČervená (varování) – zařízení se k serveru připojilo více než 14 dnů.

• **Čas posledního spuštění** – datum a čas posledního spuštění operačního systému na daném zařízení. Pro zobrazení **informace o posledním spuštění operačního systému** musí být na stanici nainstalován ESET Management Agenta ve verzi 10.0 a novější. Na zařízeních se starších verzí se zobrazí hodnota **n/a**.

• **Poslední kontrola** – datum a čas provedené poslední kontroly.

• **Detekční jádro** – verze detekčního jádra v nainstalovaném bezpečnostním produktu ESET.

• **Moduly** – stav detekčních modulů.

Produkty a licence

V této části naleznete informace o nainstalovaných produktech ESET na zařízení a použitých licencích. Po kliknutí na tuto dlaždici budete přesměrování na záložku **Detaily** > **Produkty a licence**.

Šifrování

Tato dlaždice se zobrazí pouze v detailech zařízení, které podporuje ESET Full Disk Encryption.

• Po zobrazení průvodce pro Zapnutí šifrování klikněte na tlačítko **Zašifrovat počítač**.

• Při aktivním šifrování po kliknutí na tlačítko **Spravovat** můžete definovat možnosti šifrování.

• V případě, kdy se uživatel není schopen přihlásit svým heslem nebo k zašifrovaným datům není z technických důvodů umožněn přístup, administrátor má na této dlaždici možnost pro inicializaci procesu obnovení šifrování.

ESET LiveGuard Advanced

Na této dlaždici naleznete základní informace o službě. Dlaždice může nabývat dvou stavů:

• Bílá – výchozí stav. Po aktivování a zapnutí ESET LiveGuard Advanced zůstává dlaždice stále bílá.

• Žlutá – pokud je problém se službou ESET LiveGuard Advanced, dlaždice se zbaví do žluta a zobrazí se na ní informace o problému.

K aktivaci ESET LiveGuard Advanced potřebujete licenci pro ESET LiveGuard Advanced.

Dostupné akce:

• **Zapnout** – kliknutím vytvoříte úlohu pro aktivaci produktu a aplikujete politiku, která na stanici zapne ESET LiveGuard Advanced. Pro aktivování a zapnutí na všech počítačích v dané statické skupině klikněte na ozubené kolečko vedle názvu skupiny a v kontextovém menu vyberte možnost **Řešení** > **Zapnout**

ESET LiveGuard. V konfiguračním okně vyberte úroveň ochrany a klikněte na **Zapnout**:

- **Optimální ochrana (doporučená)** – ohrožené soubory, včetně dokumentů, které podporují makra, budou odeslány na zabezpečený ESET server k automatické kontrole a analýze. Přístup k souborům je omezen, dokud nejsou vyhodnoceny jako bezpečné.
- **Základní ochrana** – ESET LiveGuard Advanced prohledá omezenou sadu souborů.

- Odeslané soubory – seznam všech souborů odeslaných na ESET servery.

Po zapnutí ESET LiveGuard Advanced:

- se na nástěnce ESET LiveGuard bude zobrazovat podrobné hlášení ESET LiveGuard Advanced ze spravované sítě.
- každé zařízení s ESET LiveGuard Advanced bude mít zapnutý Reputační systém ESET LiveGrid® a Systém zpětné vazby ESET LiveGrid®. Konfiguraci produktu ověřte v politikách.

Uživatelé

- **Přihlášení uživatelé** (pouze v případě počítačů) – seznam aktuálně přihlášených zařízení (ve tvaru doména\uživatel).
- **Přiřazení uživatelé**
  - Kliknutím na **Přiřadit uživatele** přiřadíte tomuto zařízení uživatele.

    V rámci jedné operace je možné počítači přiřadit nejvýše 200 uživatelů.
  - Kliknutím na ikonu koše zrušíte asociaci s uživatelem.
  - Kliknutím na jméno uživatele si zobrazíte jeho detaily.

Umístění

Tato dlaždice je k dispozici pouze pro mobilní zařízení. Polohu iOS zařízení registrovaných v Apple Business Manager (ABM) je možné zjistit pouze v případě, kdy je aktivní režim ztraceného zařízení.

Virtualizace

Tato dlaždice se zobrazí ve chvíli, kdy počítač označíte jako master pro klonování, a zobrazují se na ní informace týkající se VDI. Pro změnu VDI nastavení klikněte na ikonu ozubeného kolečka.

V dolní části okna jsou k dispozici následující tlačítka:

- V kontextovém menu tlačítka **Izolace od sítě** máte dostupné možnosti pro spuštění klientské úlohy související s izolací od sítě:
  - Izolovat od sítě
  - Ukončit izolaci od sítě

- Tlačítko **Virtualizace** využijete v případě, kdy klonujete počítače nebo při změně hardware. Pomocí něj určíte, co se má stát, pokud dojde ke klonování počítače, případně vypnete detekci hardware.

  - Označit jako master pro klonování

  - **Vypnout detekci hardware** – vybráním této možnosti trvale vypnete detekci změn. Mějte na paměti, že tato akce je nevratná!

  - **Odebrat označení jako master pro klonování** – vybráním této možnosti odeberete zařízení příznak master. Po aplikování tohoto nastavení se každý další klon této stanice zobrazí v sekci Rozhodnutí.

Zjištění otisku hardware není podporováno na:
- Linux, macOS, Android, iOS
- stanicích bez nainstalovaného ESET Management Agenta

Konfigurace

Konfigurace – v této části naleznete informace o aktuální konfiguraci nainstalovaných ESET produktů (ESET Management Agent, ESET Endpoint, …). Dostupné akce:

- Kliknutím na tlačítko **Vyžádat konfiguraci** vytvoříte úlohu pro ESET Management Agenta, který sesbírá konfiguraci ze všech spravovaných produktů nainstalovaných na zařízení. Úlohu provede ESET Management Agent při nejbližším připojení k ESET PROTECT Serveru. Konfiguraci produktů vrátí serveru v dalším intervalu replikace. Poté uvidíte v tomto dialogovém okně seznam konfigurací ze všech spravovaných produktů.

- Konfiguraci si můžete prostřednictvím kontextového menu otevřít a prohlédnout si ji v režimu pro čtení.

- Získanou konfiguraci můžete převést do politiky a použít jako základ pro novou politiku. Kliknutím na tlačítko **Převést do politiky** se aktuální konfigurace převede do průvodce tvorbou politiky, kde ji můžete upravit a následně uložit jako novou politiky.

- Pro potřeby diagnostiky a technické podpory si můžete konfiguraci produktu stáhnout do svého počítače. Vyberte konfiguraci a v rozbalovacím menu klikněte na možnost **Stáhnout pro diagnostiku**.

Aplikované politiky – seznam politik, které se na dané zařízení aplikují. Aplikovaná politika pro ESET produkt nebo funkci produktu, která na zařízení není nainstalována, bude v seznamu uvedena jako šedivá.

V seznamu jsou politiky přiřazené konkrétnímu zařízení, stejně tak politiky aplikované na skupiny (statické i dynamické), ve kterých se zařízení nachází.
Ikona zámku se zobrazí u politik, které není možné modifikovat. To platí pro některé předdefinované politiky (například politika s názvem Auto-updates nebo ESET LiveGuard politiky) a politiky, které uživatel nemůže měnit, protože nad nimi nemá oprávnění pro **zápis**.

Seznam můžete upravit kliknutím na tlačítko **Správa politik**. Politiky se na klienta aplikují dle pořadí (uvedeno ve sloupci **Pořadí politiky**). Pro změnu priority politiky ji vyberte pomocí zaškrtávacího pole a následně klikněte na tlačítko **Použít dříve** nebo **Použít později**.

Aplikované výjimky – seznam výjimek, které se na dané zařízení aplikují.

Protokoly (pouze pro počítače)

- **SysInspector** – kliknutím na možnost **Vyžádat protokol (pouze pro Windows)** vytvoříte novou klientskou úlohu Vyžádat SysInspector protokol. Po dokončení sběru dat a zaslání ESET SysInspector protokolu z klienta na server ho uvidíte v této sekci. Kliknutím na požadovaný záznam si ho můžete stáhnout nebo rovnou prohlédnout.

- **Log Collector** – kliknutím na možnost **Spustit ESET Log Collector** vytvoříte novou klientskou úlohu pro diagnostiku. Po dokončení sběru dat a zaslání protokolu z klienta na server ho uvidíte v této sekci. Kliknutím na požadovaný záznam si ho stáhnete do počítače.
- **Diagnostické protokoly** – kliknutím na **Diagnostika** > **Zapnout** aktivujete diagnostický režim v nainstalovaném bezpečnostním produktu. V diagnostickém režimu se všechny protokoly z produktu odešlou do ESET PROTECT Server. Protokoly budete mít k dispozici po dobu 24 hodin. Rozděleny jsou do následujících kategorií: **protokol antispamové ochrany**, **protokol firewallu**, **protokol modulu HIPS**, **protokol správy zařízení**, **protokol filtrování obsahu webu**. Pro vypnutí diagnostického režimu klikněte na tlačítko **Diagnostika** a vyberte možnost **Vypnout**.

Maximální velikost protokolu, který je možné ze zařízení přenést, je 15 MB.Protokoly jsou dostupné ve Web Console v **Detailech počítače** na záložce **Protokoly**. Pokud bude výsledný protokol větší než 15 MB, úloha skončí chybou. V takovém případě:
- Data ze stanice sesbírejte ručně.
- Upravte úroveň protokolování na klientovi a zkuste to znovu:
  - Pro získání pouze protokolů ESET Management Agenta z Windows stanic použijte parametr `/Targets:EraAgLogs`.
  - Pro vynechání protokolů z nainstalovaného bezpečnostního produktu ESET na linuxu/macOS použijte parametr `--no-productlogs`.

Provedené úlohy

Seznam úloh, které byly na zařízení spuštěny/jsou naplánovány ke spuštění. Úlohy můžete smazat, znovu spustit, duplikovat případně si zobrazit detaily provedení. Pomocí filtru můžete snadno a rychle najít konkrétní úlohu.

Instalované aplikace

Seznam aplikací nainstalovaných na zařízení. Standardně se reportují pouze aplikace ESET. Pro získání seznamu všech aplikací upravte politiku agenta.

Pokud spravujete zařízení se systémem Android a použili jste politiku povolující výjimky pro aplikace **(Správa aplikací** > **Zapnout správu aplikací** > **Povolit blokování** > **Výjimky**):

- On-premises MDM (ESET PROTECTOn-Prem) – aplikace v seznamu jsou zvýrazněny a jejich zabezpečení je ve stavu **Povoleno výjimkou**.

- Cloud MDM (ESET PROTECT) – aplikace v seznamu nejsou zvýrazněny a stav zabezpečení nemají.

U podporovaných aplikací můžete kliknout na tlačítko **Odinstalovat**, čímž vytvoříte úlohu pro odinstalaci aplikace.

- V případě potřeby můžete specifikovat **parametry odinstalace**. Jedná se o volitelné parametry instalačního balíčku, pokud je podporuje. Mějte na paměti, že odinstalační parametry jsou unikátní pro každou aplikaci. Naleznete je případně v dokumentaci k dané aplikaci.

- Pokud chcete vynutit restart operační systému, pokud jej instalace vyžaduje, vyberte možnost **Automaticky restartovat, když je potřeba**. Necháte-li tuto možnost neaktivní, rozhodnutí o restartu je na uživateli počítače. V tomto případě restartujte počítač ručně. V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje.

Po odinstalování ESET Management Agenta ze stanice nebude již dané zařízení spravované prostřednictvím ESET PROTECT:
- Po odinstalování ESET Management Agenta mohou některá nastavení bezpečnostního produktu ESET zůstat zachována.
- Pokud je Agent ESET Management chráněný heslem, pro odinstalaci, opravu nebo aktualizaci (se změnami) je nutné zadat heslo. Před odebráním zařízení ze správy doporučujeme prostřednictvím speciální politiky obnovit nastavení produktu na standardní hodnoty (především deaktivovat ochranu heslem).
- Dojde k přerušení všech běžících úloh vykonávaných agentem. Stav provedení této úlohy (**Běží**, **Dokončeno** nebo **Selhala**) se nemusí ve webové konzoli ESET PROTECT zobrazovat přesně v závislosti na replikaci.
- Po odinstalování agenta můžete bezpečnostní produkt spravovat lokálně prostřednictvím grafického rozhraní nebo eShell.

Pro aktualizaci nainstalovaných produktů ESET můžete kliknout na tlačítko **Aktualizovat ESET produkty**.

- ESET PROTECT podporuje automatickou aktualizaci ESET Management agentů ve spravovaných počítačích.
- iOS zařízení reportují do ESET PROTECT seznam nainstalovaných aplikací jednou denně. Není možné manuálně vynutit aktualizaci tohoto seznamu.

Upozornění

V této části naleznete seznam problémů a chybových stavů. U každého záznamu jsou k dispozici následující detaily: problém, stav, produkt, výskyt, závažnost, … Do této sekce se rychle dostanete, pokud v sekci **Počítače** kliknete na ikonu ve sloupci **Upozornění**. Zobrazená upozornění můžete vyřešit jedním kliknutím.

Rozhodnutí (pouze pro počítače)

V této sekci naleznete seznam rozhodnutí týkající se **klonování**. Pro více informací o řešení detekce klonovaných počítačů se podívejte do samostatné kapitoly.

Detekce a karanténa

- **Detekce** – seznam všech detekcí, které je možné filtrovat dle typu: **Kategorie detekce** – **Antivirus**, **Blokované soubory**, **Firewall**, **HIPS**, and **Webová ochrana**.

- **Karanténa** – seznam objektů uložených v karanténě na daném zařízení s detailními informacemi (název hrozby, typ hrozby, název objektu, velikost, první výskyt, …).

- Seznam všech odeslaných objektů k analýze na servery společnosti ESET naleznete ve Web Console v sekci **Odeslané soubory** společně s detaily o jejich chování.

Detaily

- **Obecné** – informace o spravovaném zařízení: Název OS, typ, verze, sériové číslo, FQDN, aj. Dále zde také naleznete informace o počtu aplikovaných politik, zda je zařízení potlačeno, času posledního připojení k serveru, atp.

- **Hardware** – informace o hardwaru, výrobci, modelu, CPU, RAM, úložišti (včetně jejich kapacity a volném místu), připojeném příslušenství, stejně tak síťových adaptérech a konfiguraci sítě (IP adresy, masky, podsítě). Další informace naleznete v kapitole Inventář hardware.

- **Produkty a licence** – informace o nainstalovaných ESET produktech na zařízeních, licencích a verzi detekčního jádra.

- **Šifrování** – pokud používáte ESET Full Disk Encryption, na této záložce naleznete informace o stavu šifrování.

Náhled počítače

Tento postranní panel se zobrazí, pokud v části **Počítače** kliknete v zobrazené tabulce na název zařízení. V náhledu detailů počítače naleznete nejdůležitější informace o vybraném zařízení.

Práce s náhledem počítačem:

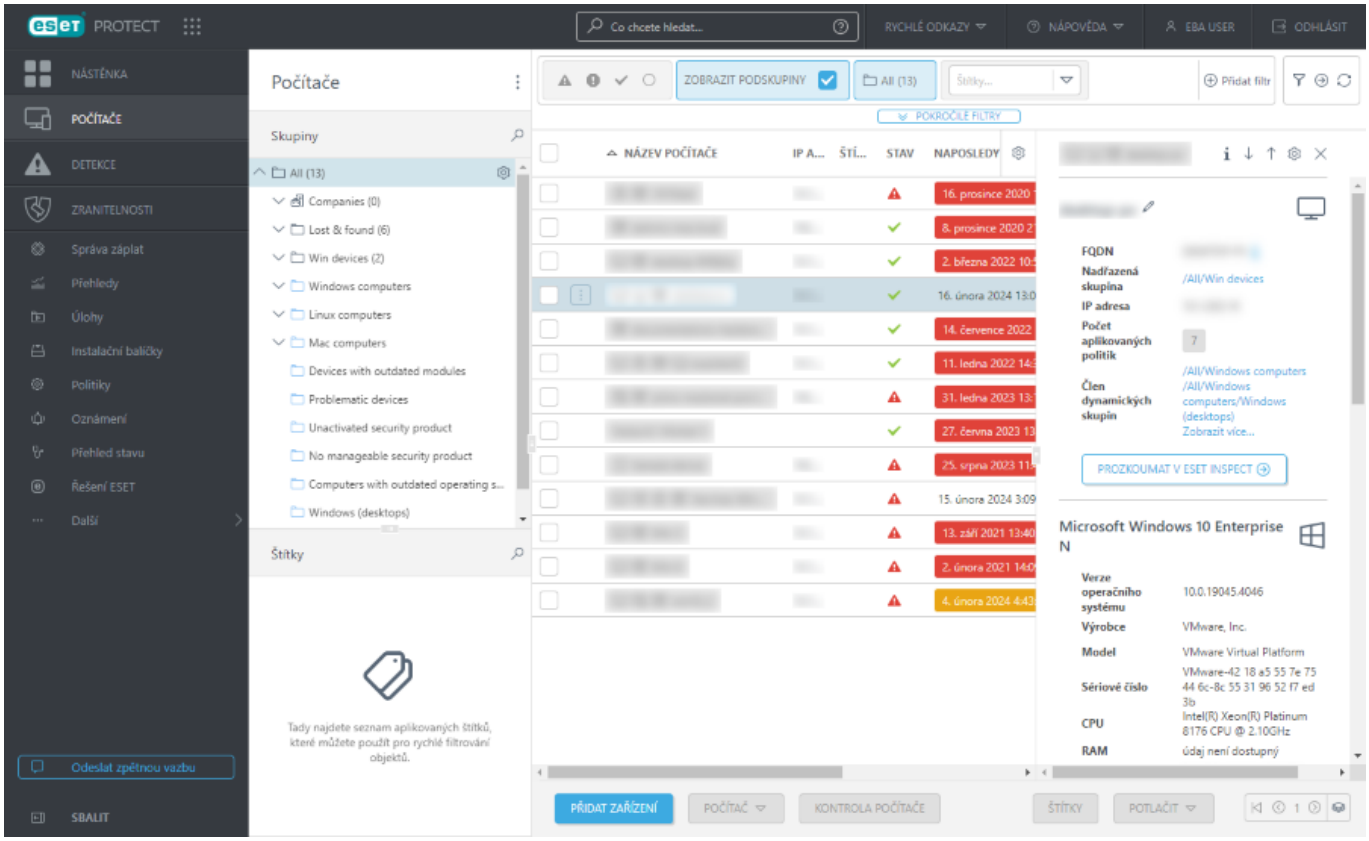
- **Zobrazit detaily** – po kliknutí se zobrazí standardní dialogové okno s Detaily počítače.

- **Další** – po kliknutí si zobrazíte detaily dalšího počítače v pořadí.

- **Předchozí** – po kliknutí si zobrazíte detaily předchozí počítače v pořadí.

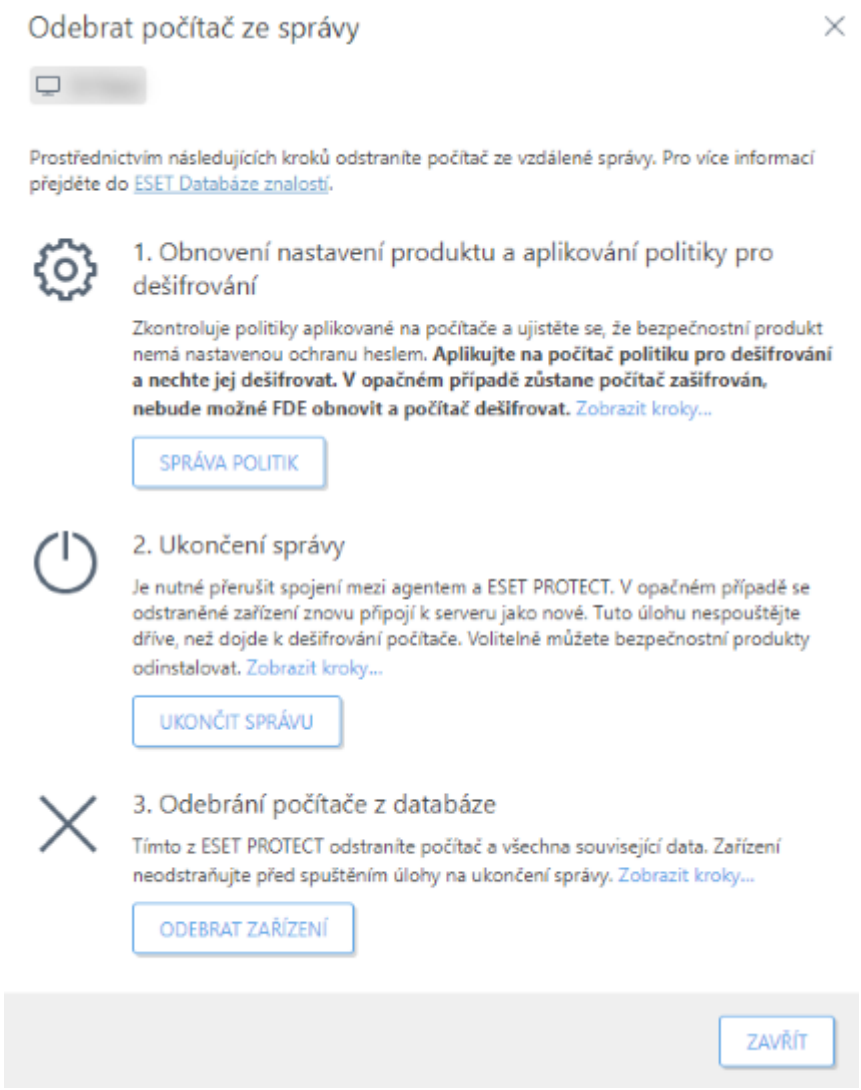
- **Správa obsahu detailů počítače** – po kliknutí se zobrazí dialogové okno, ve kterém můžete upravit jaké informace a v jakém pořadí chcete v náhledu počítače zobrazovat.

- **Zavřít** – kliknutím zavřete panel s náhledem počítače.



Odebrání počítače ze správy

Pro odebrání zařízení z konzole klikněte v hlavním okně na záložce **Počítače** na zařízení a v kontextovém menu vyberte možnost **Spravovat** > **Odstranit**. Následně se zobrazí dialogové okno s kroky, které je potřeba provést.



Před dalším krokem se ujistěte, že jste úspěšně dokončili předchozí krok. V opačném případě nedojde ke korektnímu a očekávanému odebrání zařízení.

1. **Obnovení nastavení produktu** – klikněte na tlačítko **Správa politik** a odeberte všechny politiky aplikované na zařízení. Doporučujeme prostudovat sekci **Pravidla odebrání politik** v kapitole **Politiky**. Pokud je nastaveno heslo pro přístup k nastavení aplikace, klikněte na **Zakázat heslo** a přiřaďte vybranému zařízení politiku **Zrušit ochranu heslem**. Alternativně můžete vytvořit novou politiku, v níž vynucení hesla zrušíte (pouze vyberte možnost Nastavit heslo, ale žádné nezadávejte). U zařízení zašifrovaných pomocí ESET Full Disk Encryption postupujte podle kroků pro dešifrování.

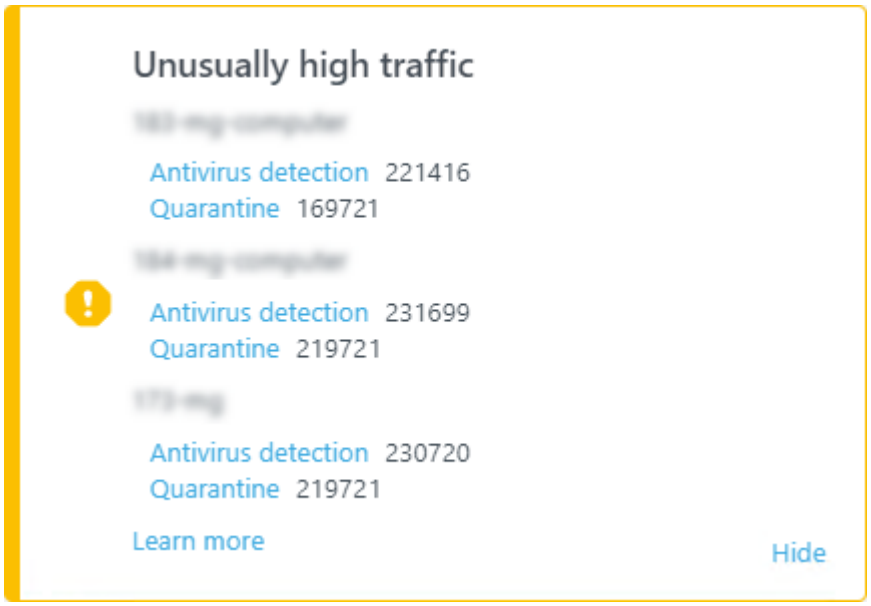
2. **Ukončení správy** – na stanici spusťte úlohu pro ukončení správy, nebo manuálně odinstalujte na stanici ESET Management Agenta, případně bezpečnostní produkt (v případě mobilních zařízení). Tím přerušíte komunikaci mezi stanicí a ESET PROTECT.

3. **Odebrání počítače z databáze** – ujistěte se, že se zařízení již nepřipojuje k ESET PROTECT. Poté ho můžete odstranit ze seznamu spravovaných zařízení.

Vybráním možnosti **Chci deaktivovat nainstalované ESET produkty** zajistíte odstranění licence ze všech ESET produktů nainstalovaných na daném zařízení. Více informací naleznete v kapitole deaktivace firemních produktů ESET.

Nezvykle intenzivní síťový provoz ze spravovaných počítačů

Administrátorům se po přihlášení do Web Console může v některých případech zobrazit upozornění poukazující na nezvykle intenzivní síťový provoz ze spravovaných počítačů.



Velké množství protokolů má negativní dopad na komunikaci mezi spravovanými počítači a ESET PROTECT:

- Nahrání dat ze spravovaných počítačů na ESET PROTECT potrvá delší dobu.
- Ve Web Console se nemusí zobrazovat aktuální stav dotčených spravovaných počítačů.

Administrátor Web Console musí vyřešit nezvykle intenzivní síťový provoz (může se jednat například o soubor v karanténě na koncové stanici nebo ESET PROTECT).

Okno s upozorněním se automaticky zavře, až dojde ke snížení počtu síťových spojení.

Skupiny

Skupiny slouží pro organizaci objektů do logických celků.

Jednotlivé počítače si můžete přidat do skupin a vytvořit si tak přehlednou strukturu počítačů. Díky tomu si můžete vytvořit přehlednou strukturu počítačů. Počítače můžete ručně přesouvat mezi statickými skupinami.

Do statických skupin počítače přidáte ručně, členem dynamické skupiny se stanou automaticky, pokud vyhovují definované podmínce. Ve chvíli, kdy se počítač stance členem skupiny, se na něj mohou začít aplikovat úlohy nebo politiky přiřazené dané skupině. Politiky a úlohy přiřazené skupině se automaticky aplikují na všechna zařízení v dané skupině. Existující dva typy skupin:

Statické skupiny

Statické skupiny jsou skupiny obsahující vámi definované počítače a další objekty. Přidat nebo odebrat členy můžete pouze ručně, nikoli pomocí dynamických kritérií. Každý počítač může být členem právě jedné statické

skupiny. Statickou skupinu můžete odstranit pouze v případě, že je prázdná – neobsahuje žádný objekt (počítač, politiku, úlohu, ...).

Dynamické skupiny

Dynamické skupiny jsou skupiny klientů (nepatří do nich jiné objekty jako úlohy nebo politiky), které byly sestaveny automaticky na základě specifických podmínek. Pokud klient přestane vyhovovat podmínce, bude ze skupiny automaticky odstraněn. Naopak počítače, které vyhovují podmínce, budou do skupiny automaticky přidány – odtud název dynamické.

Po kliknutí na ikonu ozubeného kolečka na řádku s názvem skupiny můžete nad skupinou provést akce a zobrazit si její detaily.

Počítače, které jsou členy této skupině se zobrazí v pravé části obrazovky.

Akce

V hlavním menu přejděte do sekce **Počítače** a vyberte skupinu, kterou chcete spravovat. Klikněte na ikonu ozubeného kolečka na řádku s názvem skupiny. V zobrazeném kontextovém menu jsou k dispozici následující možnosti:

Akce	Popis	Statické skupiny	Dynamické skupiny
Zobrazit detaily	Kliknutím si zobrazíte detailní informace o skupině.	✔	✔
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.	✔	✔
Nová statická skupina	Kliknutím se zobrazí průvodce vytvořením nové dynamické skupiny. Aktuálně vybraná skupina bude nadřazená nově vytvářené skupině, kdykoli to můžete změnit.	✔	x
Nová dynamická skupina	Kliknutím se zobrazí průvodce vytvořením nové dynamické skupiny. Aktuálně vybraná skupina bude nadřazená nově vytvářené skupině. Kdykoli to však můžete změnit.	✔	✔
Nové oznámení	Kliknutím vytvoříte nové oznámení nad touto skupinou.	x	✔
Úlohy	Pomocí této možnosti spustíte na všech klientech ve skupině konkrétní klientskou úlohu. **Kontrola** – kliknutím spustíte volitelnou kontrolu na zařízeních, která jsou členem dané skupiny. **Aktualizovat**: • **Aktualizovat moduly** – kliknutím spustíte aktualizaci modulů na zařízeních, která jsou členem dané skupiny. • **Aktualizovat ESET produkty** – po kliknutí se pro aktualizaci zastaralého bezpečnostního produktu ESET vytvoří klientská úlohu pro instalaci aplikace. • **Aktualizovat operační systém** – kliknutím spustíte na všech zařízeních v dané skupině klientskou úlohu pro aktualizaci operačního systému. **Mobil** – více informací naleznete v kapitole Anti-Theft akce. • **Přeregistrovat** – Přeregistrovat mobilní zařízení. • **Najít** – kliknutím vyžádáte informaci o poloze zařízení (GPS souřadnice). • **Uzamknout** – kliknutím uzamknete zařízení stejně jako při detekování podezřelé aktivity nebo označení zařízení jako ztracené. • **Odemknout** – kliknutím odemknete zařízení. • **Vymazat přístupový kód** – po kliknutí z iOS/iPadOS zařízení odstraníte přístupový kód. • **Siréna / Zvuk ztraceného zařízení** – spustí hlasitou sirénu, i přesto, pokud má zařízení ztlumenou hlasitost. • **Obnovení do továrního nastavení** – kliknutím vytvoříte úlohu pro kompletní smazání obsahu zařízení. **Spustit úlohu** – vyberte jednu nebo více klientských úloh, které chcete spustit na vybraných cílech. **Nová úloha** – kliknutím vytvoříte novou klientskou úlohu. Volitelně omezte spouštění úlohy. Úloha bude zařazena do fronty dle vámi definovaného nastavení. Spuštění úlohy bude naplánováno na nejbližší možnou dobu. Při použití této možnosti není možné definovat podmínku spuštění. K jejímu spuštění dojde okamžitě. **Poslední úlohy** – seznam naposledy použitých klientských úloh nad skupinami nebo zařízeními, které můžete okamžitě spustit.	✔	✔
Řešení	Pro spuštění ESET Inspect na všech počítačích v dané skupině klikněte na ozubené kolečko vedle názvu statické skupiny > vyberte možnost **Řešení** > **ZapnoutESET Inspect**. **Zapnout ESET LiveGuard** –Pro aktivování a zapnutí ESET LiveGuard Advanced na všech počítačích v dané statické skupině klikněte na ozubené kolečko vedle názvu skupiny a v kontextovém menu vyberte možnost **Řešení** > **Zapnout ESET LiveGuard**. **Zapnout Správu zranitelností a záplat** – kliknutím na vedle statické skupiny a výběrem **Řešení** > **Zapnout Správu zranitelností a záplat** zapnete na zařízení tuto správu.	✔	x
Přehledy	Vyberte si přehled, který chcete vygenerovat ze zařízení ve vybrané skupině.	✔	x
Správa politik	Kliknutím přiřadíte politiku vybrané skupině.	✔	✔
Změnit...	Kliknutím upravíte vybranou skupinu. Zobrazí se stejné možnosti jako při vytváření skupiny nové (statické nebo dynamické).	✔	✔
Přesunout	Pomocí této možnosti můžete přesunout vybranou skupinu do jiné skupiny.	✔	✔
Odstranit...	Kliknutím odstraníte vybranou skupinu.	✔	✔
Použít dříve **Použít později**	Pomocí těchto možností změníte pořadí dynamické skupiny. Změna pořadí může ovlivnit výsledné nastavení aplikované politikami na klientskou stanici.	x	✔
Importovat...	Pomocí této možnosti můžete, například z textového souboru, naimportovat seznam počítačů do vybrané skupiny. Pokud se počítač již ve skupině nachází, konflikt se vyřeší na základě vámi definované akce.	✔	x
Exportovat...	Kliknutím exportujete seznam členů skupiny, v případě zájmu též včetně podskupin, do *.txt* souboru. Tento seznam můžete použít pro import v budoucnu.	✔	x
Active Directory Scanner	Vygenerovaný přístupový token použijte pro ověření připojení nástroje ESET Active Directory Scanner k ESET PROTECT, aby mohl do vybrané statické skupiny synchronizovat obsah Active Directory.	✔	x

Detaily skupiny

Po vybrání možnosti **Zobrazit detaily** v kontextovém menu skupiny se zobrazí dialogové okno s následujícími informacemi:

Přehled

V této části můžete kliknutím na ikonu změnit **název** skupiny, případně **Přidat popis**. Dále zde máte k dispozici informace o tom, jaká je **nadřazená skupina** a jaké má daná skupina **potomky**. V případě, že jste vybrali dynamickou skupinu, je zde uveden operátor a podmínka, na základě které je přítomnost zařízení vyhodnocována.

Úlohy

V této části máte přehled o klientských úlohách přiřazených dané skupině.

Politiky

V této části máte přehled o politikách přiřazených dané skupině.

> Mějte na paměti, že v detailech skupiny uvidíte pouze politiky a úlohy přiřazené dané skupině. Nezobrazí se zde úlohy a politiky přiřazené jednotlivým zařízením v dané skupině.

Politiky se na klienta aplikují dle pořadí (uvedeno ve sloupci **Pořadí politiky**). Pro změnu priority politiky ji vyberte pomocí zaškrtávacího pole a následně klikněte na tlačítko **Použít dříve** nebo **Použít později**.

Upozornění

V této části máte přehled o upozorněních ze všech zařízeních, které jsou členy dané skupiny. Zobrazená upozornění můžete vyřešit jedním kliknutím.

Výjimky

V této části máte přehled o výjimkách aplikovaných na tuto skupinu.

Statické skupiny

Statické skupiny slouží pro:

- Třídění zařízení do skupin a podskupin,
- Třídění objektů (politik, úloh, ...),
- Definování domovské skupiny pro uživatele.

Domovská skupina je automaticky detekována na základě přiřazené sady oprávnění právě přihlášeného uživatele.

Příklad:
Právě přihlášený uživatel má oprávnění k **zápisu** u klientské úlohy **Instalace aplikace**. **Domovská skupina** uživatelského účtu je skupina s názvem "Oddělení_1". Pokud uživatel vytváří novou **klientskou úlohu pro instalaci aplikace**, skupina "Oddělení_1" se automaticky vybere jako **domovská skupina**.

Pokud vám předvybraná domovská skupina nevyhovuje, můžete ji ručně změnit.

Vytvořit si můžete libovolnou statickou skupinu, a ručně do ní přesunout požadovaná zařízení. Mějte na paměti, že každé zařízení (počítač nebo mobilní zařízení) se může nacházet pouze v jedné statické skupině. Možnosti pro správu skupin máte k dispozici pod tlačítkem Skupina, které naleznete v dolní části okna.

V PRODUCTNAME jsou předdefinovány dvě statické skupiny:

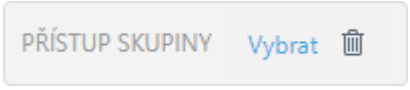
- **Všechna zařízení** – hlavní skupina pro všechna zařízení připojená k síti ESET PROTECT serveru. Všechny objekty vytvořené administrátorem se automaticky ukládají do této skupiny. Skupina je zobrazena vždy, a není možné změnit její název, jinak ji upravit nebo odstranit. Pokud přidělíte dalším uživatelům oprávnění pro přístup k této skupině, uvidí všechny objekty a skupiny.

- Skupina **Ztráty a nálezy** je potomkem skupiny **Všechna zařízení**. Každý nový počítač, který se připojí k ESET PROTECT serveru, se automaticky zobrazí v této skupině. Skupinu můžete přejmenovat, vytvořit si její kopii, ale nemůžete ji odstranit ani přesunout.

Pro přesunutí počítače do jiné Statické skupiny na něj klikněte, z kontextového menu vyberte možnost **Spravovat** > **Přesunout do skupiny** > v zobrazeném okně si vyberte požadovanou statickou skupinu > klikněte na tlačítko **OK**.

Statickou skupinu můžete odstranit v případě, kdy:
- Máte oprávnění pro zápis do této skupiny,
- Skupina je prázdná (nejsou v ní žádné počítače ani objekty).

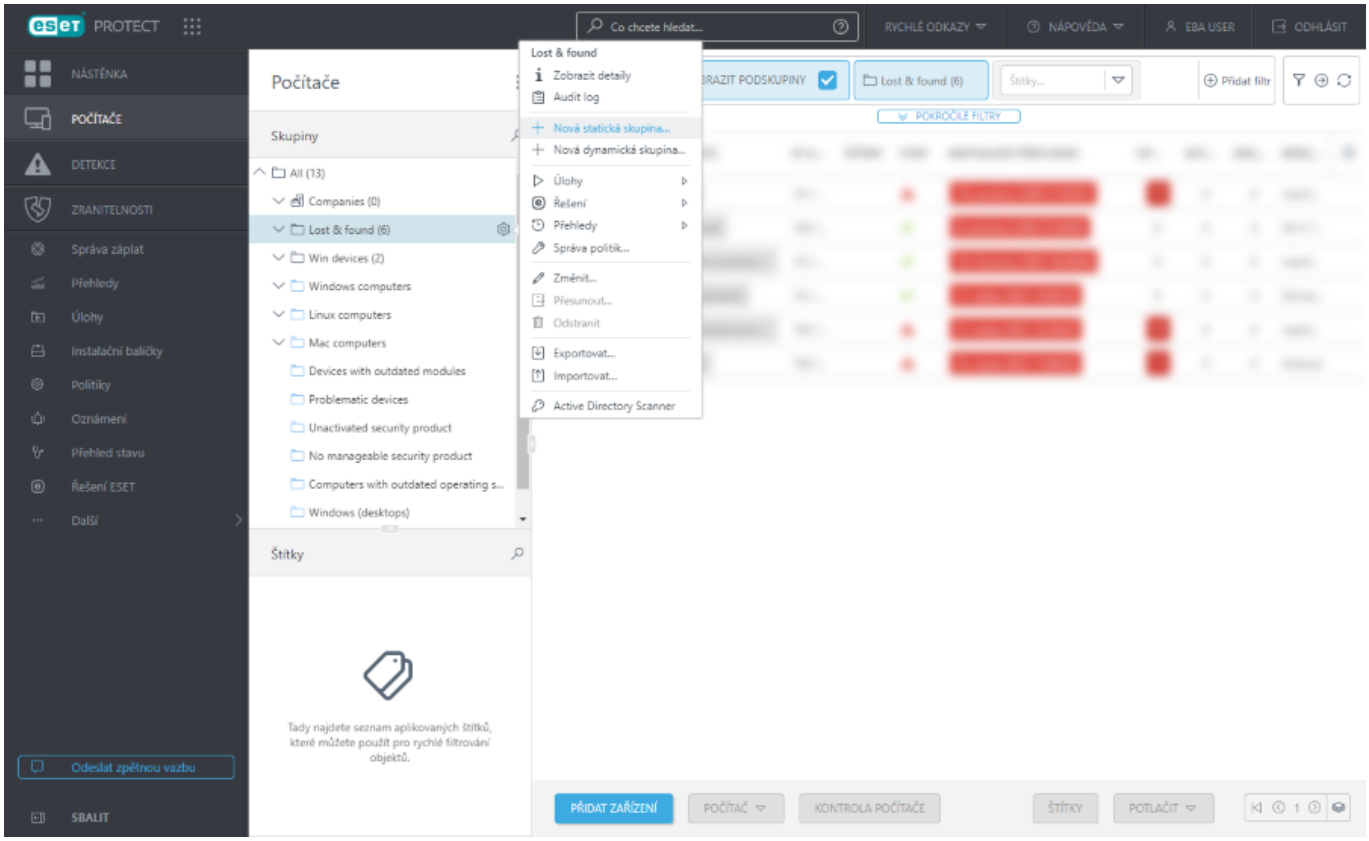
V případě, že skupina obsahuje objekty, pokus o její odstranění selže. Pro ověření, zda se v konkrétní skupině nacházejí objekty využijte filtr **Přístup skupiny** (například v části **Instalační balíčky**.



Klikněte na tlačítko **Vybrat** a vyfiltrujte si objekty, které patří do konkrétní statické skupiny. Následně je můžete odstranit, případě přesunout do jiné skupiny.

Vytvoření nové statické skupiny

Pro vytvoření nové staticky skupiny přejděte v hlavním menu na záložku **Počítače** a vyberte si skupinu do které chcete další skupinu vložit. Klikněte na ikonu ozubeného kolečka a vyberte možnost **Nová statická skupina....**



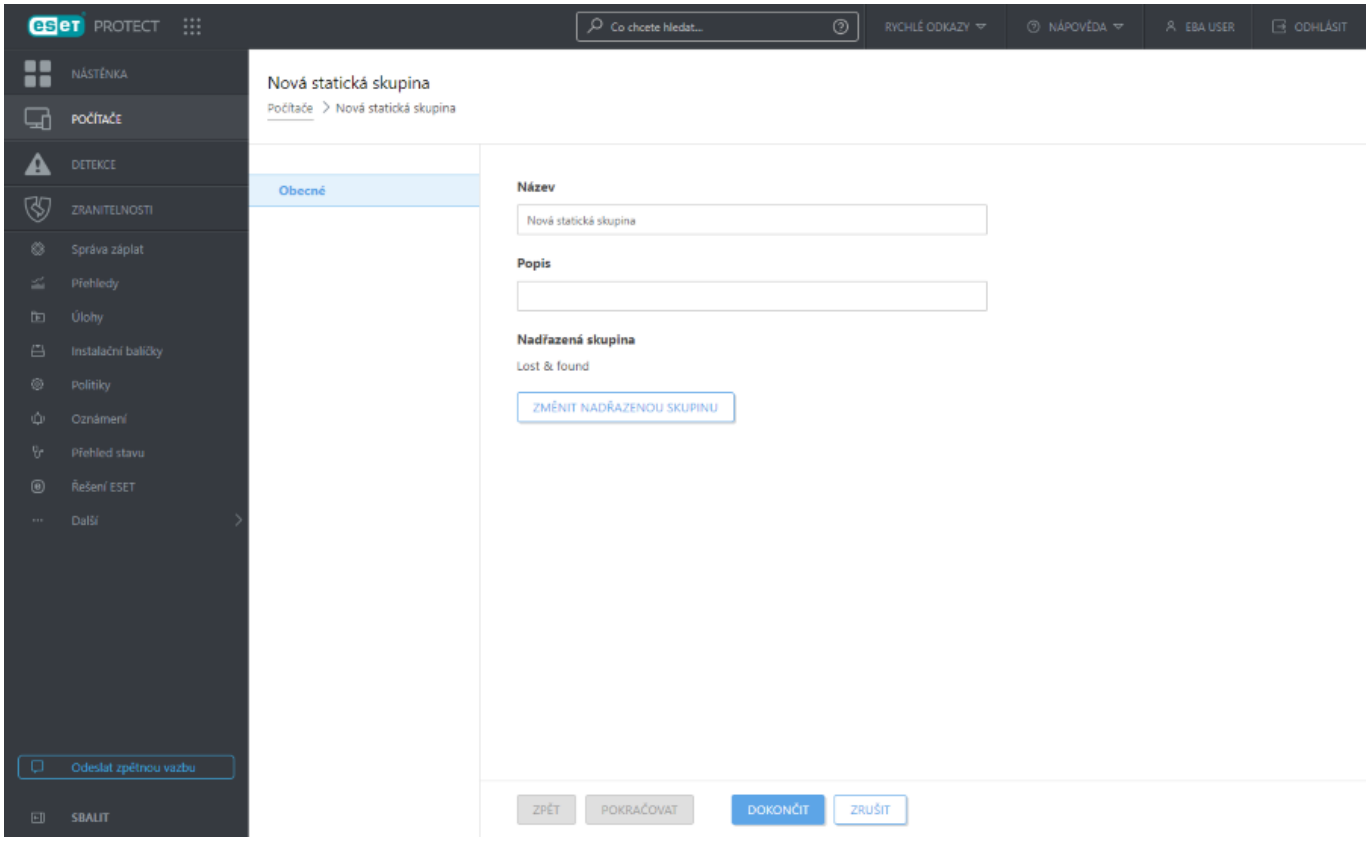
Obecné

Zadejte **název**, volitelně **popis**, nov vytvářené skupiny.

- V případě potřeby stále můžete změnit **nadřazenou skupinu**. Jako nadřazená skupina se automaticky použije skupina, kterou jste vybrali předtím, než jste otevřeli tohoto průvodce. Pro změnu nadřazené skupiny klikněte na tlačítko **Změnit nadřazenou skupinu** a vyberte požadovanou skupinu. Nadřazená skupina může být libovolná (statická i dynamická).

- Nadřazená skupina může být výhradně statická. Je to z důvodu, že potomkem dynamické skupiny nemůže být skupina statická.

Pro dokončení akce klikněte na tlačítko **Dokončit**.

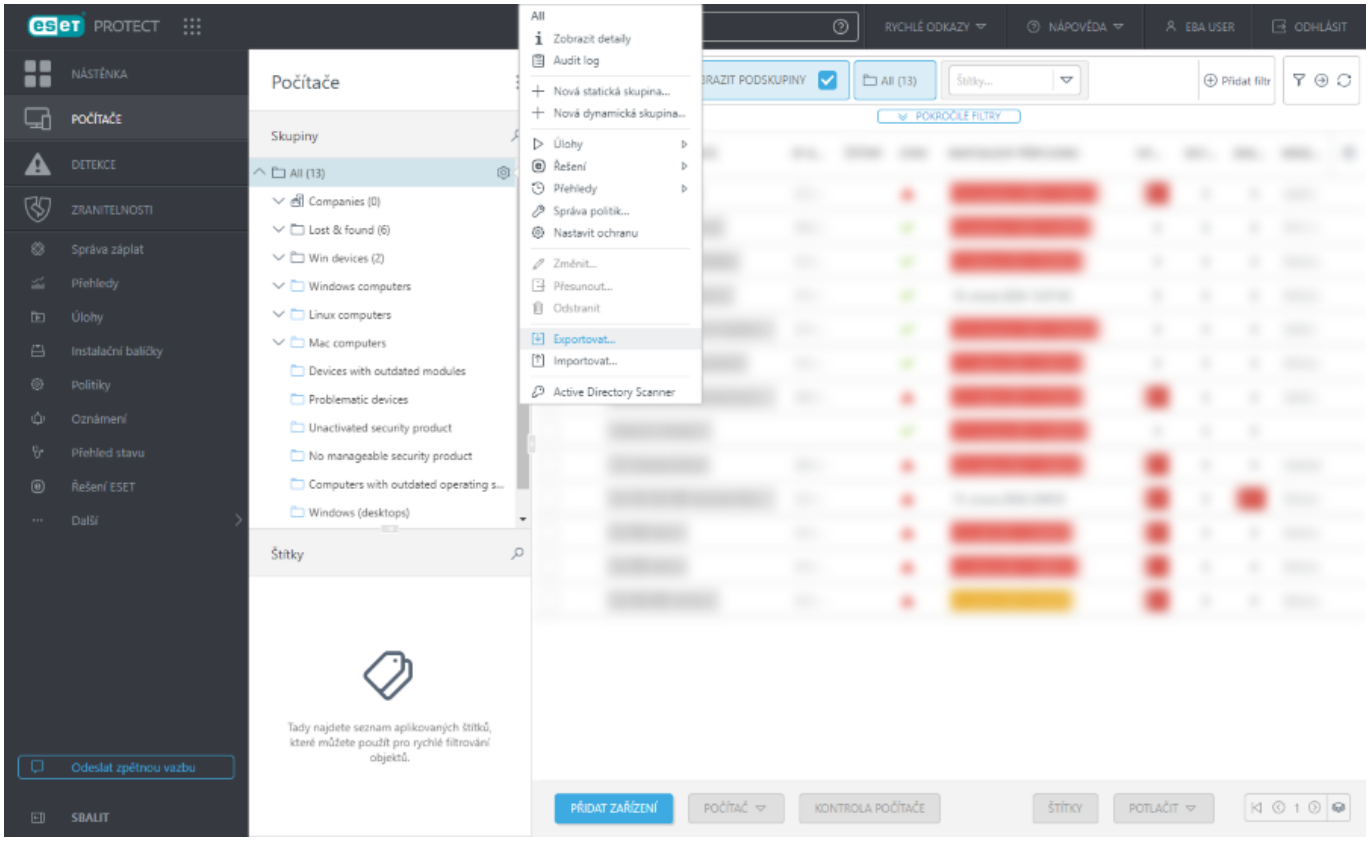


Exportování statických skupin

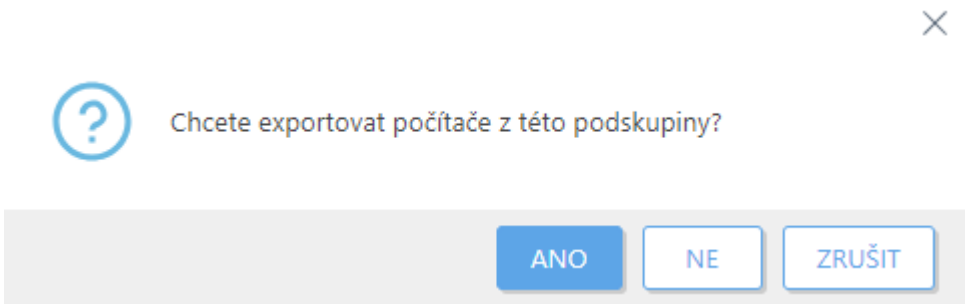
Seznam počítačů, které máte v ESET PROTECT struktuře, si můžete pohodlně exportovat. Exportovat můžete celou strukturu skupin včetně počítačů v nich obsažených a zálohovat tak pro budoucí použití, například při migraci serveru.

Exportovat můžete pouze statické skupiny, které obsahují alespoň jeden počítač. Prázdné skupiny nebudou exportovány.

1. V hlavním menu přejděte do sekce **Počítače** a vyberte skupinu, kterou chcete exportovat.
2. Klikněte na ikonu ozubeného kolečka a z kontextového menu vyberte možnost **Exportovat...**.



3. Pokud vybraná statická skupina obsahuje podskupiny, můžete se rovněž rozhodnout, zda chcete exportovat počítače z jejích potomků.

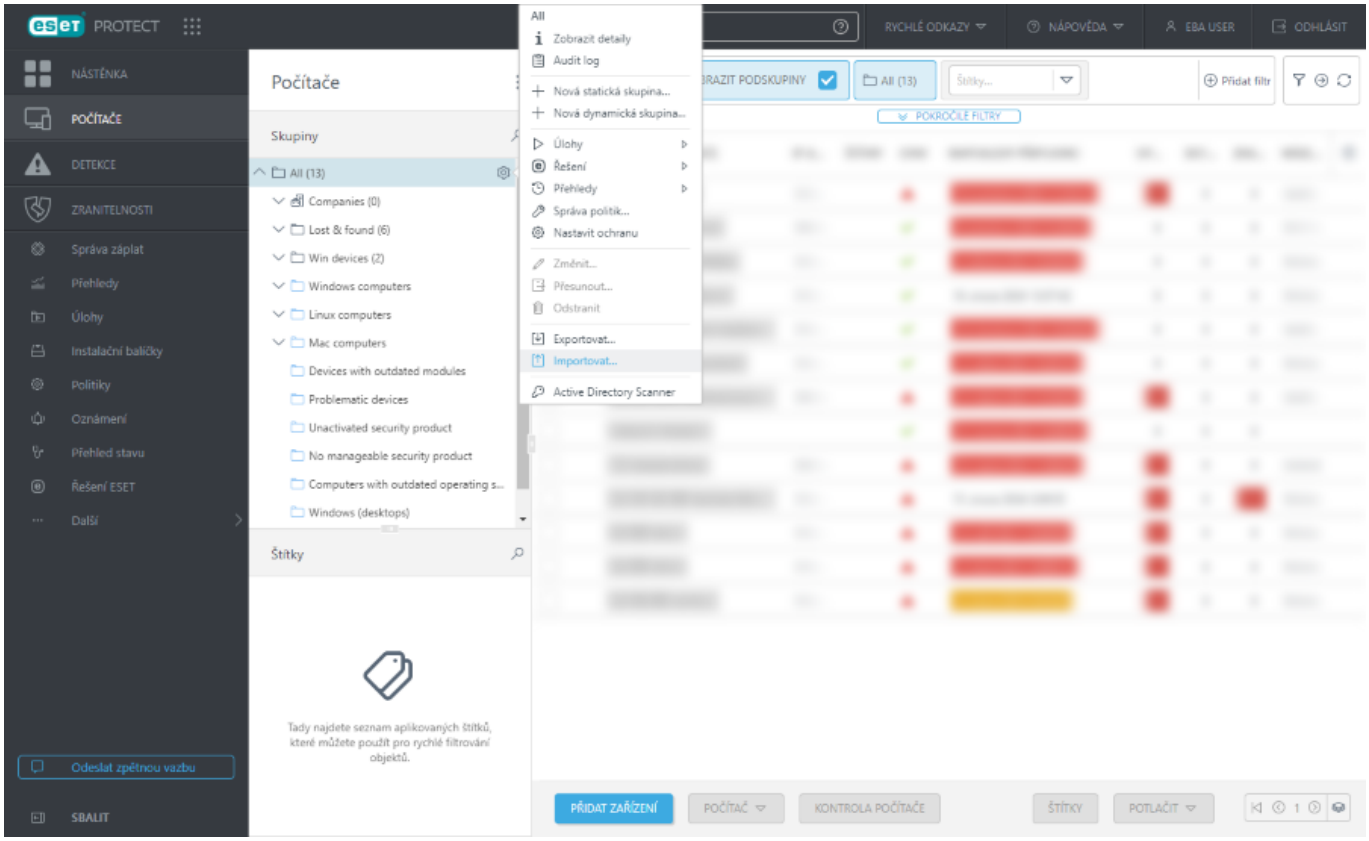


4. Soubor se uloží do *.txt* formátu.

> Dynamické skupiny není možné exportovat, protože obsahují pouze odkazy na počítače, které vyhovují kritériím definovaným v šabloně dynamické skupiny.

Importování statických skupin

Dříve exportované soubory statické skupiny můžete prostřednictvím ESET PROTECT Web Console kdykoli importovat do již existující struktury skupin zpět.



1. V hlavním menu přejděte do sekce **Počítače** a vyberte libovolnou statickou skupinu.

2. Klikněte na ikonu ozubeného kolečka a vyberte možnost **Importovat…**.

3. Klikněte na **Vyberte soubor** a najděte *.txt* soubor. Každý řádek v souboru musí obsahovat úplnou cestu k zařízení/IP adresu (se zpětným lomítkem jako oddělovačem). Příklad:

```
All\Lost & found\Computer_Name
All\Lost & found\10.20.30.40
```

4. Poté klikněte na tlačítko **Otevřít** . V textovém poli se zobrazí název vámi vybraného souboru.

5. Vyberte akci, která se použije při řešení konfliktů:

- **Nevytvářet ani nepřesouvat žádná zařízení, pokud byly ve struktuře nalezeny stejné záznamy** – pokud statická skupina již existuje a zařízení z *.txt* souboru již v této skupině jsou, budou tato zařízení přeskočena a nebudou importována. V případě výskytu kolize budete na tuto skutečnost upozorněni.

- **Přesunout existujících zařízení, pokud zatím v importovaných cestách neexistují. Pokud je to možné, ponechat ve stejné cestě pouze spravovaná zařízení** – pokud statická skupina již existuje a zařízení z *.txt* souboru již v této skupině jsou, je třeba před importem přesunout zařízení do jiných statických skupin. Po importu budou tato zařízení přesunuta zpět do původních skupin, odkud byly přesunuta.

- **Duplikovat existující zařízení, pokud zatím v importovaných cestách neexistují** – pokud statická skupina již existuje a zařízení z *.txt* souboru již v této skupině jsou, vytvoří se duplikáty těchto zařízení ve stejné statické skupině. V detailech originálního počítače budou zobrazeny všechny informace, u duplikátu se zobrazí pouze jeho název.

6. Pro dokončení akce klikněte na tlačítko **Importovat**.

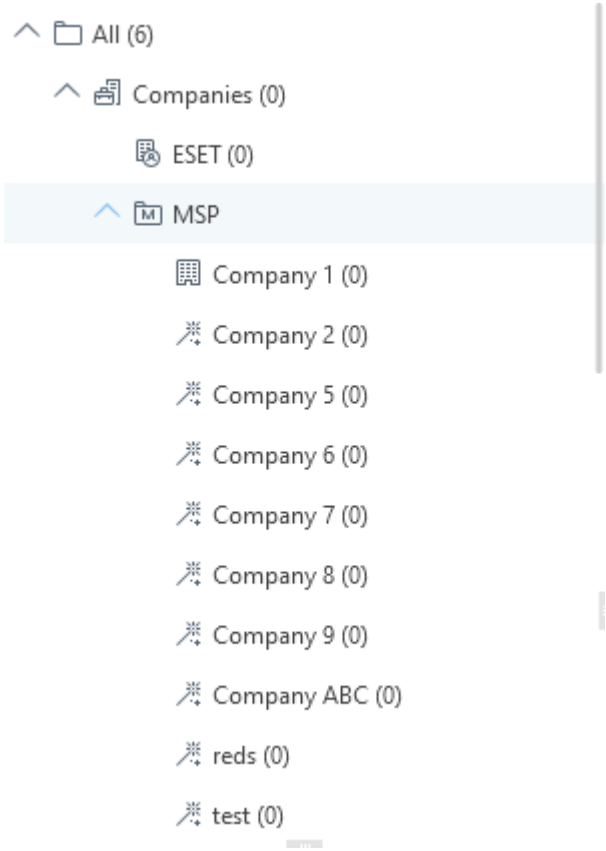
Strom statických skupin pro ESET Business Account / ESET MSP Administrator

Při nasazení ESET PROTECT prostřednictvím ESET Business Account dojde k přenesení struktury vaší společnosti z portálu ESET Business Account (včetně lokalit) do stromu statických skupin (nová funkce představená v ESET PROTECT3.4).

Při nasazení ESET PROTECT prostřednictvím ESET MSP Administrator dojde k přenesení struktury z portálu ESET MSP Administrator do stromu statických skupin. Přečtěte si další informace o ESET PROTECT pro poskytovatele spravovaných služeb.

Struktura stromu statických skupin pro ESET Business Account / ESET MSP Administrator

Strom statických skupin z ESET Business Account/ESET MSP Administrator naleznete na záložce **Počítače** zanořenou ve struktuře **Všechna zařízení** > **Společnosti**.



Ve statické skupině **Společnosti** naleznete:

- ESET Business Account společnost – v případě, že jste nasadili ESET PROTECT prostřednictvím ESET Business Account.
- ESET MSP Administrator strom – v případě, že jste nasadili ESET PROTECT prostřednictvím ESET MSP Administrator.

- Oba stromy – v případě, že jste ESET PROTECT nasadili prostřednictvím smíšeného účtu.

Pokud máte ESET MSP Administrator účet, další informace naleznete v kapitole Struktura entit v MSP.

Synchronizace lokalit z ESET Business Account

Pokud v rámci portálu ESET Business Account využíváte lokality, ESET PROTECT je automaticky synchronizuje se stromem statických skupin a přiřadí v rámci ESET Business Account společnosti licence z každé lokality příslušné statické skupině (označené ikonou).

- Ke správě lokalit doporučujeme využít automaticky vytvořený strom statických skupin (místo ručního vytváření statických skupin).
- Je třeba vytvořit administrátory lokalit s **vlastním** přístupem k ESET PROTECT a přiřadit jim oprávnění ručně. Každému administrátorovi lokality nastavte odpovídající statickou skupinu jeho lokality jako domovskou skupinu a přiřaďte mu sadu oprávnění odpovídající stejné domovské skupině.

Máte například vytvořené dvě lokality (**site1** a **site2**):
1.Vytvořte uživatele pro každou lokalitu (**site1_admin** a **site2_admin**).
2.Volitelné: Přiřaďte každému uživateli jeho odpovídající domovskou skupinu (lokalitu) – tedy skupinu **site1** uživateli **site1_admin** a **site2** uživateli **site2_admin**.
3.Vytvořte pro každého uživatele sadu oprávnění (**site1_permissions** pro uživatele **site1_admin** a **site2_permissions** pro uživatele **site2_admin**).
4.Propojte každou sadu oprávnění s odpovídající domovskou skupinu – tedy skupinu **site1** s oprávněním **site1_permissions** a skupinu **site2** s **site2_permissions**.
5.V každé sadě oprávnění definujte požadovaný úroveň přístupu k jednotlivým funkcím a částem Web Console (**čtení**, **použití**, **zápis**).
6.Přiřaďte každou sadu oprávnění jednotlivým uživatelům (sadu **site1_permissions** uživateli **site1_admin** a **site2_permissions** uživateli **site2_admin**).
7.Nyní uvidí administrátor každé lokality výhradně své lokality a jejich související objekty (například licence).

Při přejmenování lokality v ESET Business Account, která se synchronizuje v rámci stromu statických skupin, dojde ke změně jejího názvu také v ESET PROTECT.

Při odstranění lokality v ESET Business Account, která se synchronizuje v rámci stromu statických skupin, tuto změnu reflektujete do ESET PROTECT kliknutím na ikonu .

Sdílení objektů

Ve stromové struktuře ESET Business Account i ESET MSP Administrator se nachází další speciální statická skupina s názvem **Sdílené objekty**.

Tuto statickou skupinu můžete využít ke sdílení objektů Web Console (politik, šablon dynamických skupin, atd.) s ostatními uživateli, kteří mají omezené oprávnění (mají přístup ke statickým skupinám na stejné úrovni jako je skupina **Sdílené objekty** nebo níže ve stromové struktuře):

1. Objekty Web Console přesuňte pomocí funkce **Přístup skupiny** do statické skupiny Sdílené objekty. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

2. Uživateli přiřaďte oprávnění **Použít** ke skupině **Sdílené objekty**.

- Abyste zabránili modifikaci sdílených objektů, ujistěte se, že uživatelé s omezeným oprávněním nemají nad skupinou **Sdílené objekty** oprávnění pro **Zápis**. Oprávnění **Použít** je v tomto případě dostačující.
- Do statické skupiny **Sdílené objekty** nelze přesouvat počítače. Statická skupina **Sdílené objekty** se nezobrazuje mezi jednotlivými **Skupinami** na záložce **Počítače**.

Dynamické skupiny

Dynamické skupiny si můžete představit jako vlastní filtry na základě stavu počítače. Počítač může vyhovovat více filtrům, a proto může být členem více dynamických skupin. To je rozdíl oproti statickým skupinám, kdy počítač může být členem právě jedné statické skupiny.

Dynamické skupiny jsou skupiny vybraných klientů, které vyhovují definované podmínce. Aby se počítač stal členem dynamické skupiny, musí vyhovovat podmínkám definovaných v šabloně dynamické skupiny. Každá šablona může obsahovat několik pravidel. Tato pravidla můžete definovat v průběhu vytváření šablony. Pokud klient přestane vyhovovat podmínce, bude ze skupiny automaticky odstraněn. Naopak, pokud vyhoví podmínce, stane se členem dynamické skupiny.

Při každém připojení k ESET PROTECT agent ověří, zda nedošlo ke změně šablon dynamických skupin a jejich podmínek. Pokud zařízení vyhovuje podmínce definované v šabloně dynamické skupiny, automaticky se stane členem takové skupiny. Vyhodnocení probíhá na straně agenta (počítači), k získání výsledku není vyžadována žádná dodatečná komunikace se serverem. Agent rozhoduje o tom, do které dynamické skupiny klient patří, a na server odesílá pouze informace o výsledném rozhodnutí.

Pokud se zařízení (agent) k serveru nepřipojuje, například z důvodu, že je vypnuté, v dynamické skupině se nezobrazí. Ve skupině se zobrazí po připojení k serveru za předpokladu, že stále vyhovuje definované podmínce.

V ESET PROTECT je předdefinováno několik dynamických skupin pro filtrování počítačů a mobilních zařízení. V případě potřeby si můžete vytvořit vlastní dynamické skupiny. Provést to můžete dvěma způsoby:

- Nejprve vytvořte šablonu, a poté novou dynamickou skupinu.
- V průběhu vytváření nové dynamické skupiny definujte šablonu.

Dynamické skupiny můžete používat v dalších částech ESET PROTECT. Dynamickým skupinám můžete přiřazovat politiky (viz princip aplikování politik) nebo úlohy, které se mají aplikovat na všechny počítače, které jsou členem skupiny.

Dynamická skupina může být potomkem statické nebo jiné dynamické skupiny. Nicméně statická skupina nemůže být potomkem skupiny dynamické. Dynamické skupiny vždy filtrují pouze počítače z nadřazené (statické nebo dynamické) skupiny. Pokud je dynamická skupina potomkem jiné dynamické skupiny, filtruje pouze výsledky z nadřazené dynamické skupiny. Dynamické skupiny můžete v rámci stromové struktury přesouvat.

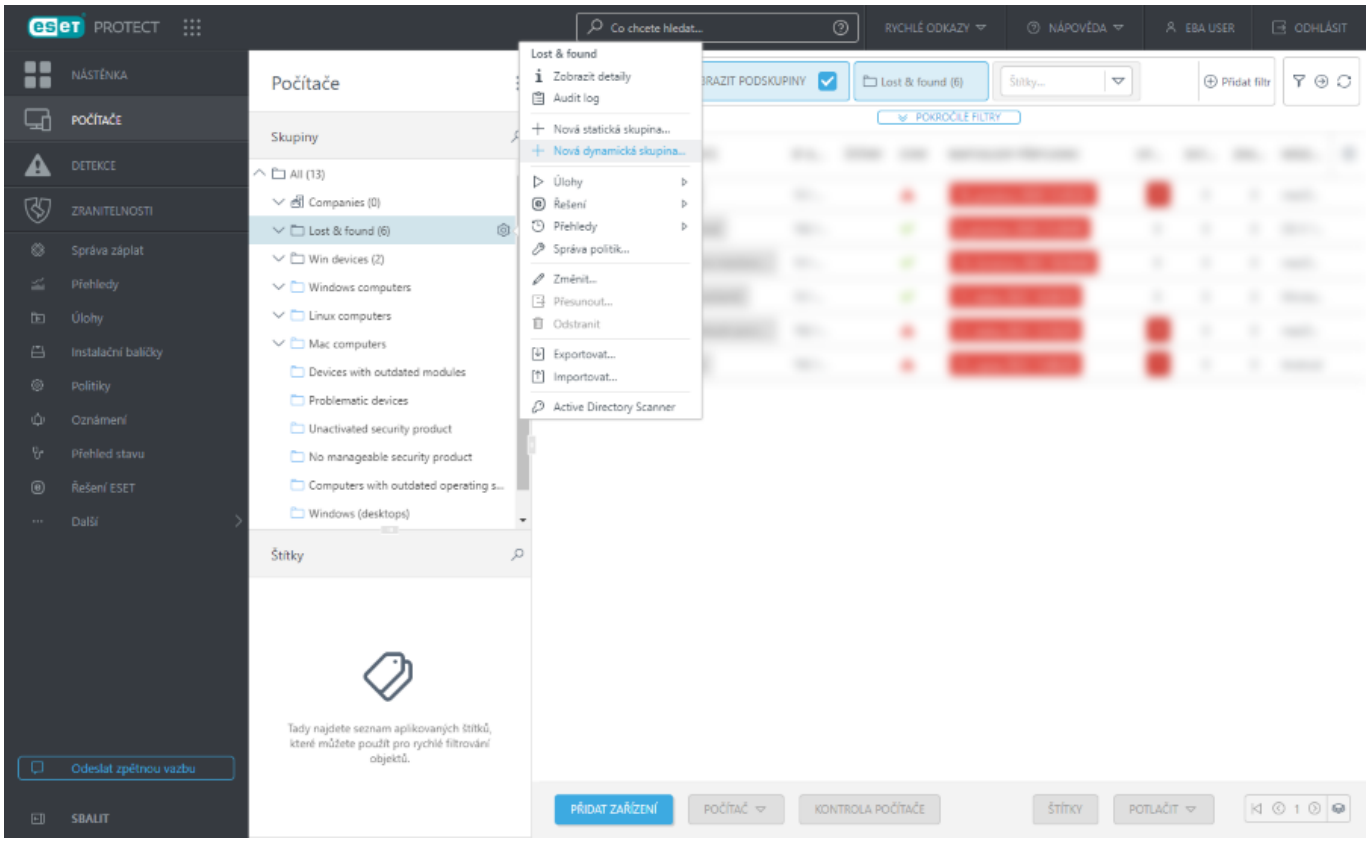
Možnosti pro správu dynamických skupin naleznete v kontextovém menu.

Vytvoření nové dynamické skupiny

Pro vytvoření nové dynamické skupiny postupujte podle níže uvedených kroků.

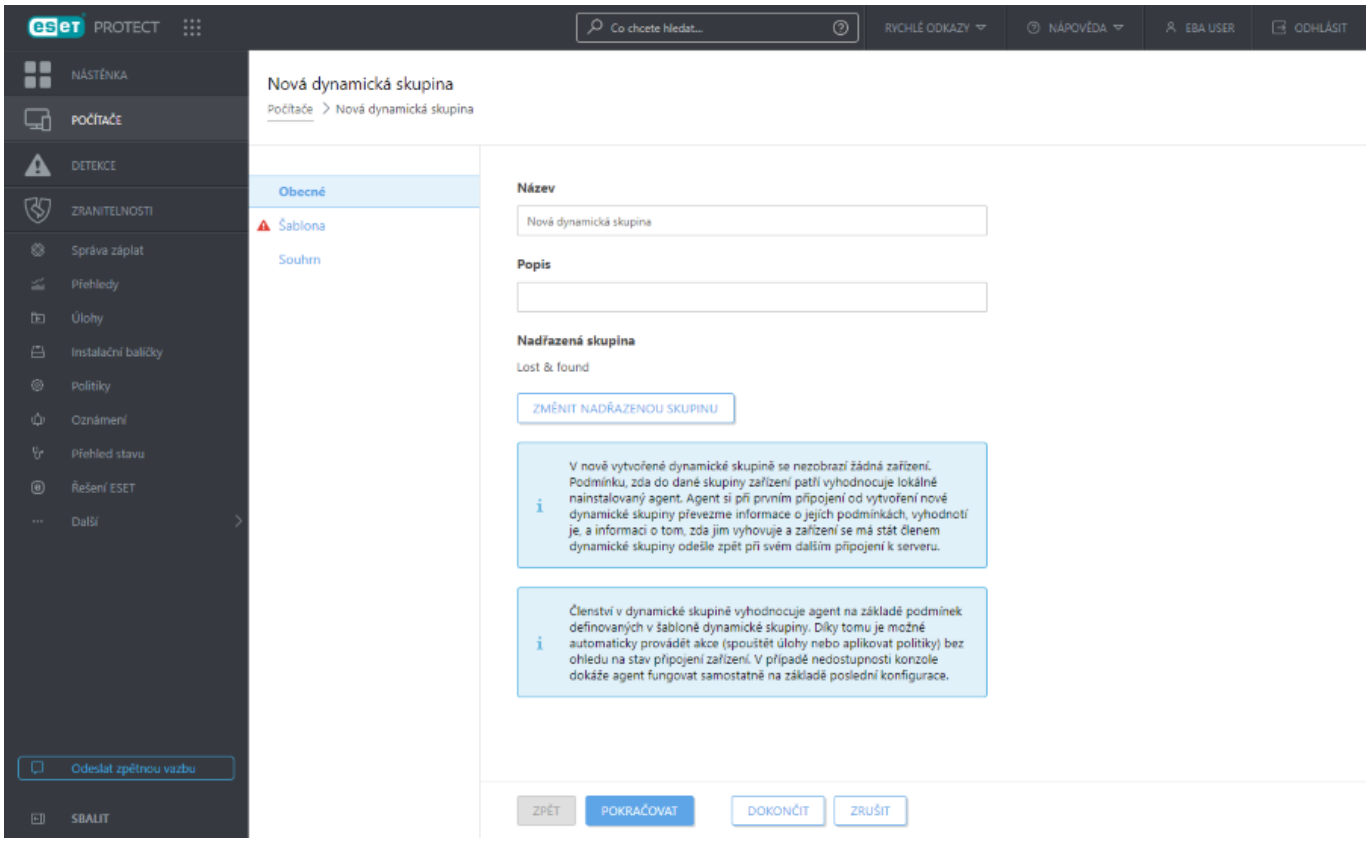
1. V hlavním menu na záložku **Počítače** a vyberte si skupinu, do které chcete další skupinu vložit. Klikněte na

ikonu ozubeného kolečka a vyberte možnost **Nová statická skupina…**. Následně se zobrazí průvodce vytvořením dynamické skupiny.



2. Zadejte název, volitelně popis, nové šablony dynamické skupiny.

3. Pro změnu nadřazené skupiny klikněte na tlačítko **Změnit nadřazenou skupinu** a vyberte požadovanou skupinu.



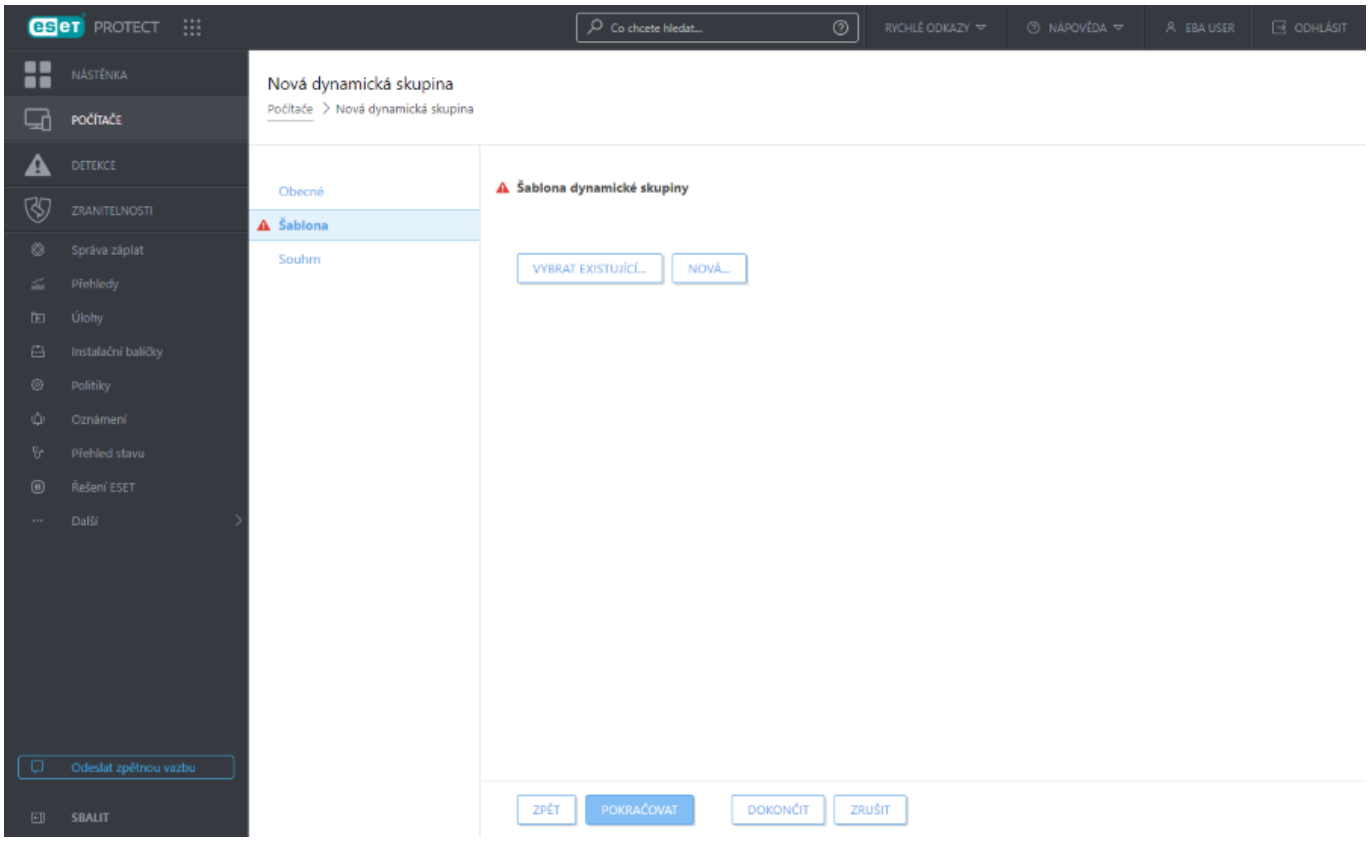
4. Přejděte do sekce **Šablona**. Každá dynamická skupina filtruje počítače na základě podmínky definované v šabloně dynamické skupiny. Z jedné šablony tak můžete vytvořit libovolné množství dynamických skupin. Z vytvořené šablony můžete vytvořit libovolné množství dynamických skupin.

> Šablona dynamické skupiny je statický objekt uložený v konkrétní statické skupině. Aby měl k šabloně uživatel přístup, musí mít přiděleno potřebné oprávnění. V opačném případě nebude schopen se šablonami pracovat a vytvářet na základě nich dynamické skupiny. Všechny předdefinované šablony dynamických skupin jsou umístěny ve statické skupině **Všechna zařízení** a má k nim přístup standardně pouze uživatel Administrator. Pokud chcete dalším uživatelům přidělit přístup k použití těchto šablon, přidělte jim další oprávnění. V opačném případě uživatelé tyto výchozí šablony neuvidí. Případně šablony přesuňte je do jiné statické skupiny, do níž mají uživatelé oprávnění přístup k těmto objektům.
> Pro duplikování šablon musí mít uživatel oprávnění pro **použití** objektu (šablona dynamické skupiny) ve zdrojové skupině a následně oprávnění pro **zápis** ve své domovské, v níž se kopie objektu vytvoří. Dále se podívejte na příklady duplikování objektů.

- Při vytváření nové dynamické skupiny můžete použít již existující šablonu. Klikněte na tlačítko **Vybrat existující** a ze seznamu si vyberte požadovanou šablonu.

- Pokud vám žádná šablona nevyhovuje, klikněte na tlačítko **Nová** a vytvořte novou šablonu.

Vzorové příklady šablon dynamických skupin naleznete v samostatné kapitole.



5. Pro její vytvoření klikněte na tlačítko **Dokončit**. Nová skupina se vytvoří jako potomek nadřazené skupiny.

Přesunutí statické nebo dynamické skupiny

Mějte na paměti, že existuje několik omezení a není proto možné přesouvat skupiny zcela libovolně. Dynamická skupina může být potomkem jakékoli statické nebo dynamické skupiny. Statická skupina nemůže být potomkem dynamické skupiny. Není možné manipulovat s předdefinovanými skupinami (**Všechna zařízení**, Ztráty a nálezy).

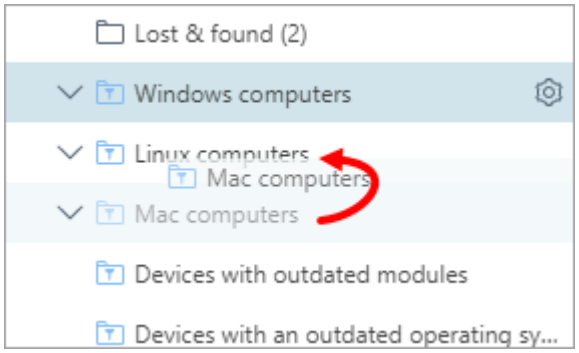
Ručně vytvořené statické skupiny můžete přesouvat podle potřeby.

Po kliknutí na ikonu ozubeného kolečka na řádku s názvem skupiny vyberte možnost **Přesunout…**. Zobrazí se dialogové okno se stromovou strukturou skupin. Následně vyberte skupinu (statickou nebo dynamickou), do které chcete stávající skupinu přesunout. Aktuálně vybraná skupina bude potomkem cílové skupiny. Případně můžete skupinu přesunout pouhým přetažením do jiné skupiny.

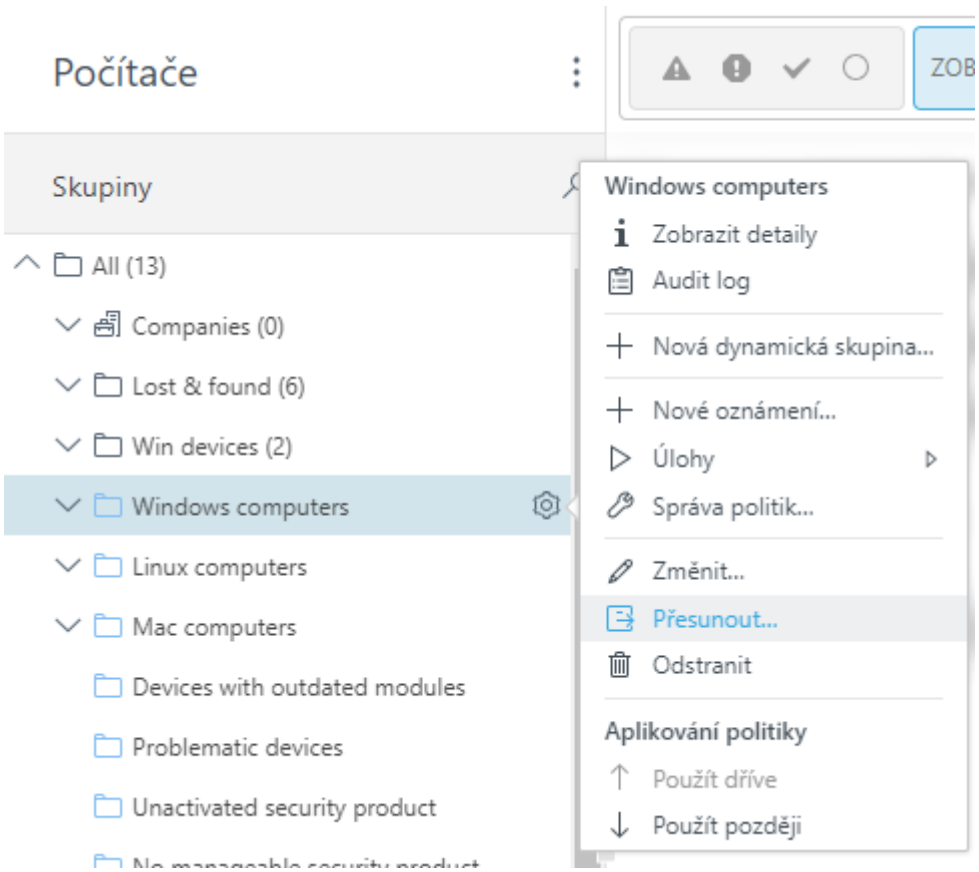
> Po přesunutí dynamické skupiny na nové místo dojde k vymazání jejich členů a stanice z nadřazené skupiny se začnou filtrovat dle podmínky definované v šabloně dynamické skupiny.

Skupiny můžete přesouvat třemi způsoby:

- **Drag and drop** – vyberte skupinu, kterou chcete přesunout a přetáhněte ji do jiné nadřazené skupiny.

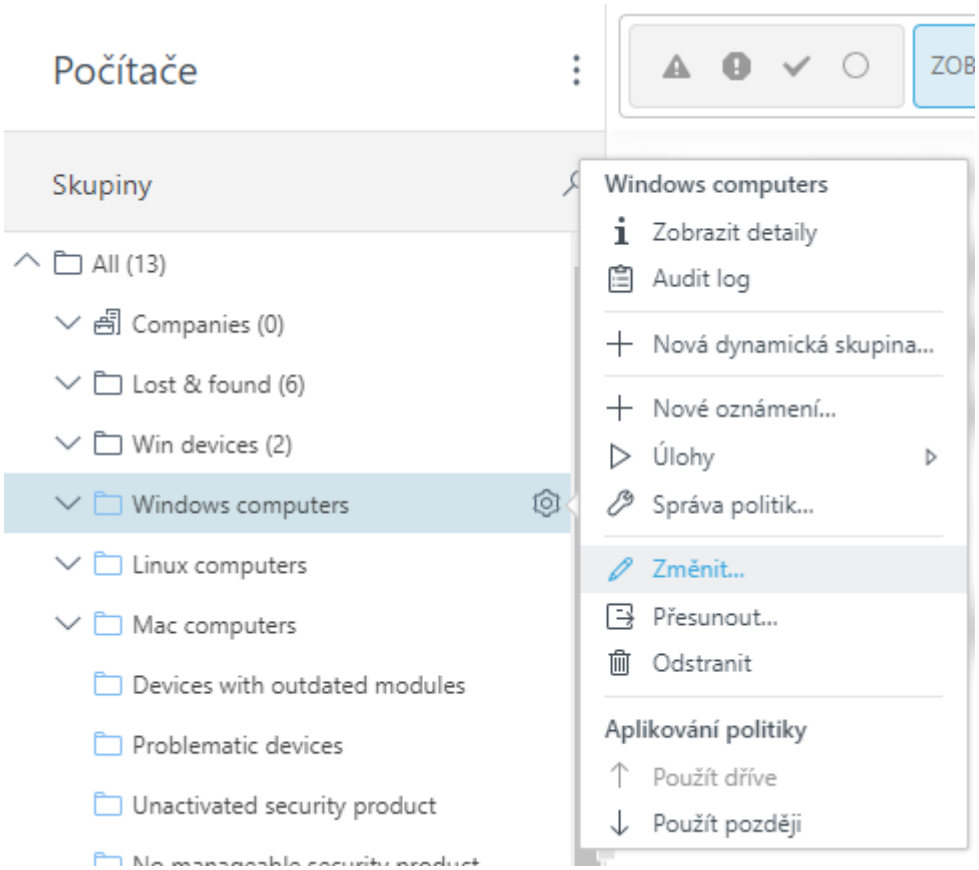


- Klikněte na ikonu ozubeného kolečka > **Přesunout…**. Ze seznamu vyberte požadovanou skupinu a klikněte na tlačítko **OK**.



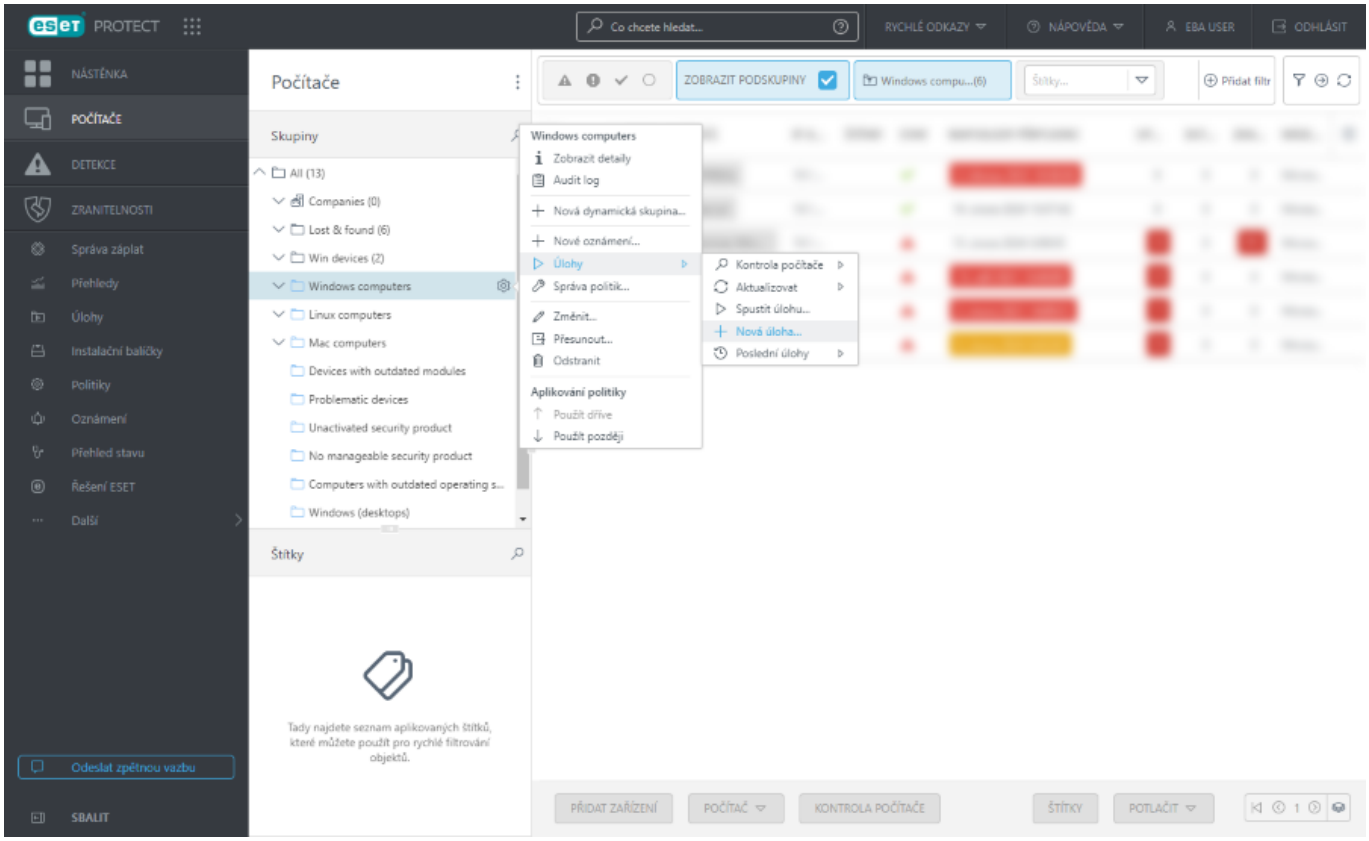
- Klikněte na ikonu ozubeného kolečka > **Změnit…** a následně klikněte na tlačítko **Změnit nadřazenou**

skupinu. Následně si ze seznamu vyberte požadovanou statickou skupinu a potvrďte kliknutím na tlačítko **OK**.



Přiřazení klientské úlohy počítači nebo skupině

Pro vytvoření nové úlohy a její přiřazení požadované skupině přejděte v hlavním menu do sekce **Počítače**. Vyberte **Statickou** nebo **Dynamickou** skupinu, klikněte na ikonu ozubeného kolečka a vyberte možnost **Úlohy** > **Nová úloha**. Následně se zobrazí průvodce vytvořením klientské úlohy.

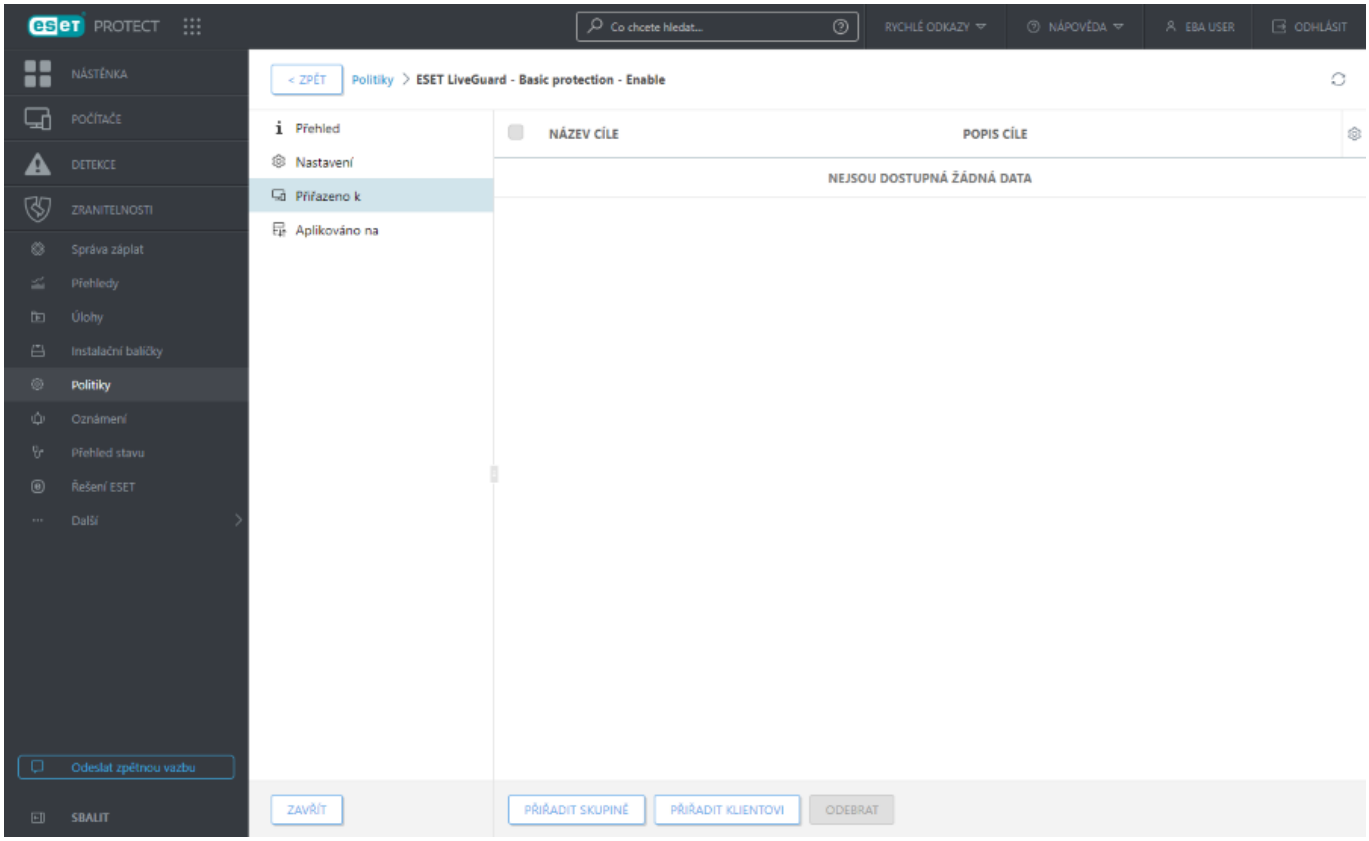


Přiřazení politiky skupině

Poté, co politiku vytvoříte, ji můžete jedním z následujících kroků přiřadit **Statické** nebo **Dynamické skupině**. Provést to můžete dvěma způsoby:

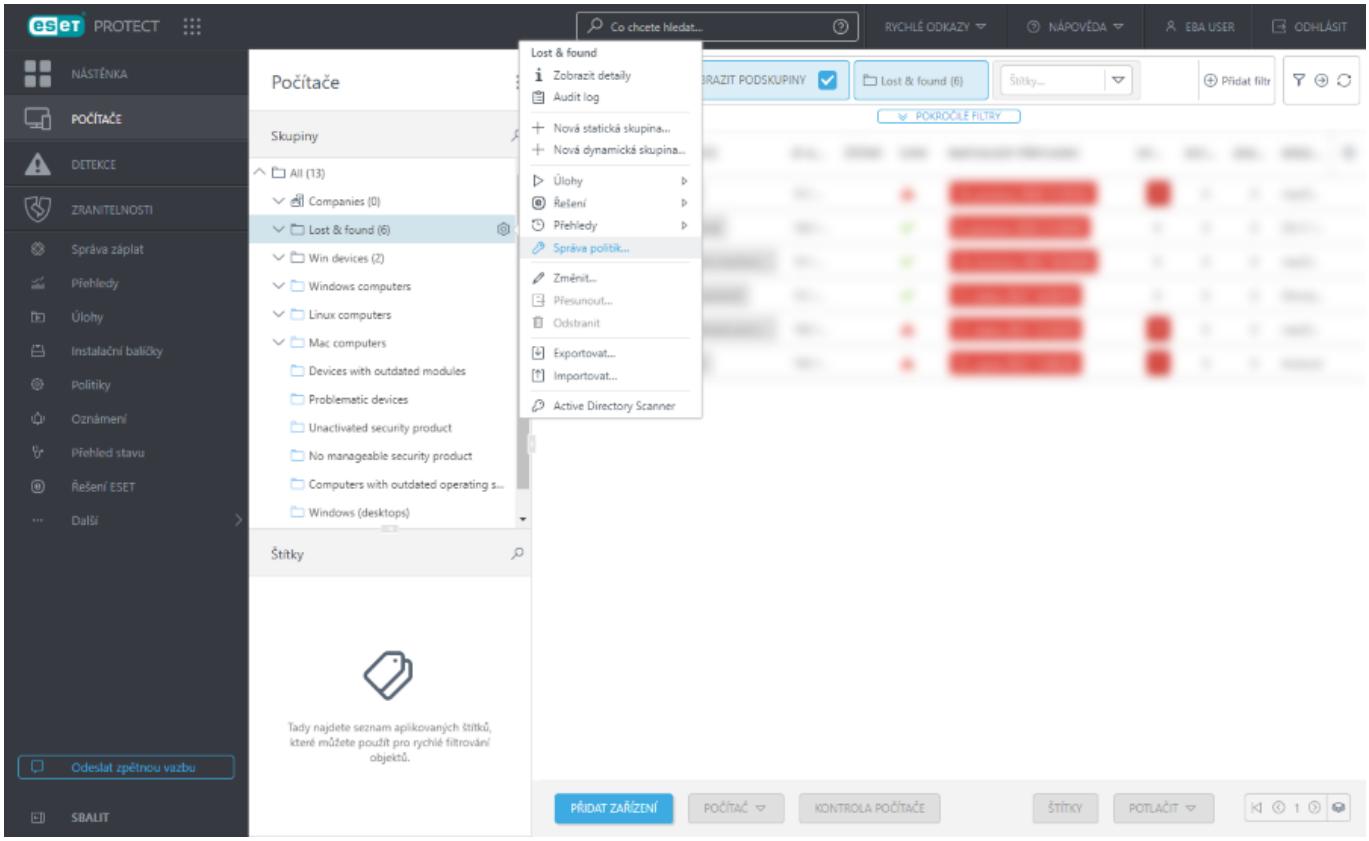
První možnost

V sekci **Politiky** vyberte politiku a klikněte na tlačítko **Akce** > **Zobrazit detaily**. Přejděte na záložku **Přiřazeno k** a klikněte na **Přiřadit skupině**. Následně si ze seznamu vyberte požadovanou statickou nebo dynamickou skupinu a potvrďte kliknutím na tlačítko **OK**.



Druhá možnost

1. V sekci **Počítače** klikněte na ikonu ozubeného kolečka u požadované skupiny a z kontextového menu vyberte možnost **Správa politik…**.



2. V dialogovém okně **Pořadí uplatňovaných politik** klikněte na tlačítko **Přiřadit politiku**.

3. Ze seznamu vyberte politiku, kterou chcete aplikovat na skupinu a pokračujte kliknutím na tlačítko **OK**.

4. Klikněte na tlačítko **Zavřít**.

Pro ověření, že je politika přiřazená skupině se v sekci skupiny přepněte na záložku **Politiky**.

Pro ověření, na jaké skupiny je politika aplikována vyberte možnost **Zobrazit detaily** > **Aplikováno na**.

> Pro více informací přejděte do kapitoly Politiky.

Detekce

V sekci **Detekce** naleznete přehled o všech detekcích na spravovaných počítačích.

V levé části obrazovky je zobrazena stejná stromová skupina jako na záložce Počítače. Seznam hrozeb tak můžete procházet po jednotlivých skupinách. Pro zobrazení všech detekcí vyberte nejnadřazenější skupinu **Všechna zařízení** a odstraňte všechny aplikované filtry.

> Více informací o technologiích ESET a typech útoků/detekcí naleznete ve slovníku pojmů.

Stav detekce

Na základě stavu označujeme detekce jako:

- **Aktivní detekce** – jedná se o detekce, které zatím nebyly vyléčeny. Pro vyléčení detekce a vynulování tohoto čítače spusťte **Hloubkovou kontrolu** s aktivním léčením, a bez výjimek, na složku, ve které došlo k detekci. Pro vynulování čítače musí kontrola doběhnout úspěšně a nesmí dojít k další detekci. Pokud detekci nezpracujete do 24 hodin od jejího výskytu, odebere se jí příznak **aktivní**, ale stále bude v seznamu označená jako nevyřešená.

- **Vyřešené detekce** – jedná se o detekce, které byly označeny uživatelem konzole jako vyřešené, ačkoli na zařízení nebyla provedena **Hloubková kontrola**. Pokud detekce ručně označíte jako vyřešené, stále se doby spuštění kontroly mohou zobrazovat ve filtrovaném seznamu výsledků.

Stav **Detekce zpracována** reprezentuje informaci, zda bezpečnostní produkt ESET provedl nad detekcí akci (na základě typu detekce a nastavené úrovni léčení):

- **Ano** – bezpečnostní produkt ESET provedl nad detekcí akci (odstranil ji, vyléčil nebo přesunul do karantény).

- **Ne** – bezpečnostní produkt ESET neprovedl s detekcí žádnou akci.

Filtr **Detekce zpracována** můžete využívat v přehledech, oznámeních i při tvorbě šablon dynamických skupin.

> Do karantény se nepřesunují všechny objekty detekované na klientské stanici. Možné případy:
> - Detekce, které nelze odstranit.
> - Chování objektu je podezřelé, ale není detekován jako malware, například PUA.

Agregování detekcí

Pro zjednodušení správy a jejich řešení jsou detekce agregovány podle času a dalších kritérií. Pokud dojde k opakované identické detekci, ve Web Console se v seznamu detekcí zobrazí pouze jednou (jako jeden řádek). Detekce starší než 24 hodin se agregují automaticky každou půlnoc. Agregované detekce rozpoznáte podle hodnoty X/Y (vyřešeno záznamů/celkový počet záznamů) ve sloupci **Vyřešeno**. Seznam agregovaných detekcí naleznete v detailech detekce na záložce **Výskyty**.

Detekce v archivech

Při výskytu detekce v archivu je do seznamu **detekcí** reportován daný archiv a každá detekce.

> Vyloučením archivu obsahujícím detekci nedojde k vyloučení samotné detekce. V tomto případě je nutné vyloučit jednotlivé detekce nacházející se v archivu. Maximální velikost souboru v archivu je 3 GB.

Vyloučené detekce již následně nebudou zaznamenávány – i když se budou nacházet v jiném archivu, nebo samostatně (nearchivované).

Filtrování detekcí

Standardně se zobrazují nevyřešené detekce za posledních 7 dní, a to ze všech kategorií. Detekce můžete filtrovat podle mnoha kritérií. Standardně se zobrazují filtry **Počítač je potlačen a Výskyt**.

> Některé filtry jsou standardně aktivní. Pokud se vám v hlavním menu u položky **Detekce** zobrazuje číslo, ale v této sekci žádné detekce nevidíte, ověřte, zda nemáte aktivní nějaké filtry.

Seskupování detekcí

Pro seskupení detekcí z rozbalovacího menu vyberte:

- **Neseskupeno** – výchozí zobrazení
- **Seskupeno podle počítače** – detekce seskupené dle názvu počítače
- **Seskupeno podle kategorie** – detekce seskupené dle kategorie detekce
- **Seskupeno podle typu** – detekce seskupené dle kategorie detekce a jejího typu
- **Seskupeno podle kontrolního součtu** – detekce seskupené dle kontrolního součtu
- **Seskupeno podle důvodu** – detekce seskupené dle důvodu
- **Seskupeno podle uživatele** – detekce seskupené dle uživatele

Chcete-li si zobrazit všechny detekce seskupené do určitého řádku, klikněte na libovolný řádek a poté na **Otevřít seznam detekcí**. Informace o skupině detekcí se následně zobrazí v horní části stránky. Použitím **šipky dolů** můžete přecházet mezi seskupenými detekcemi. Použitím **šipky zpět** se vrátíte zpět do detekčních skupin.

Pro získání konkrétních výsledků můžete použít další filtry jako je například:

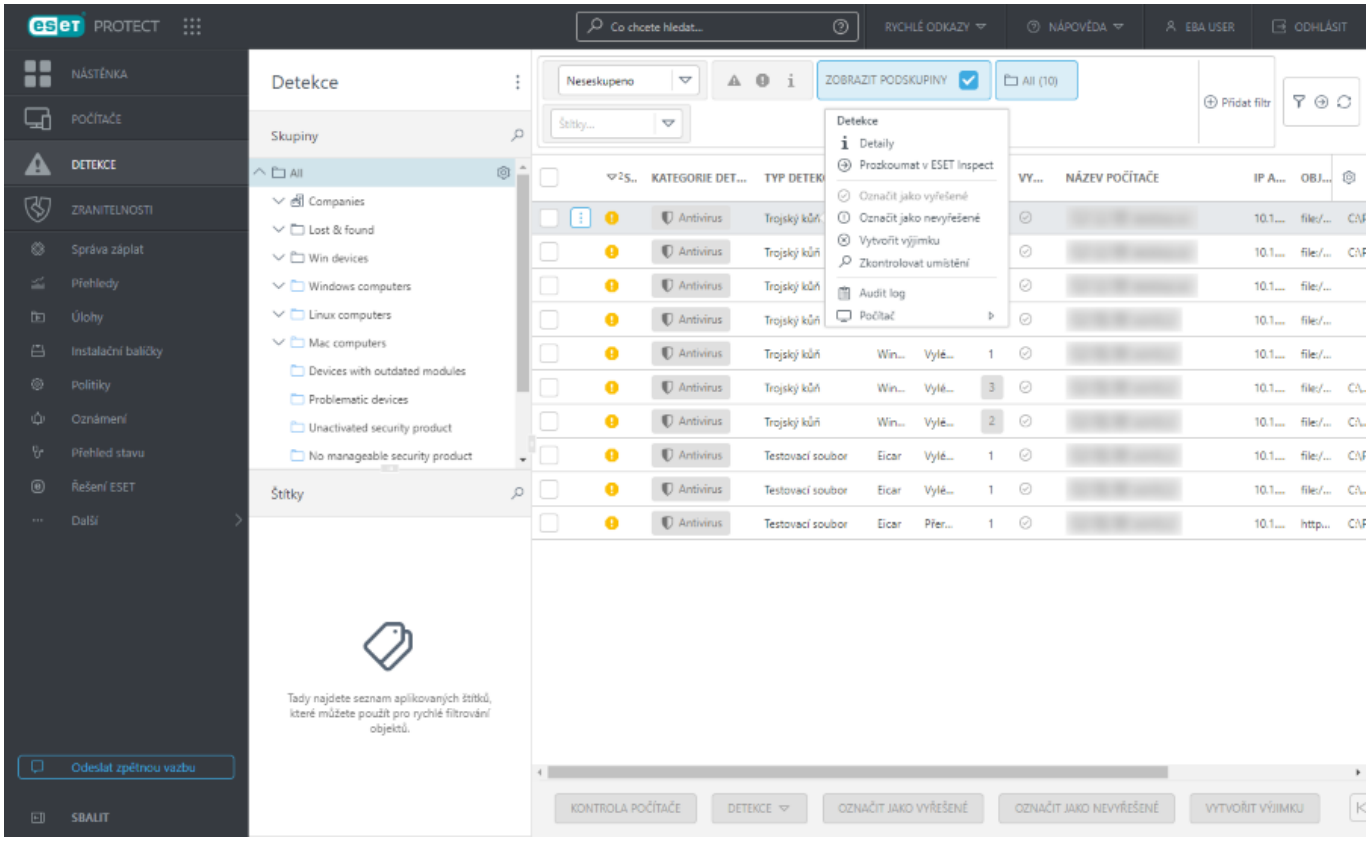
- **Kategorie detekce** – **Antivirus**, **Blokované soubory**, **Firewall**, **HIPS**, and **Webová ochrana**.
- **Typ detekce**
- **IP adresa** klienta, na kterém k detekci došlo
- **Skener** – vyberte typ skeneru, který detekci nahlásil. Příklad: po vybrání možnosti **Anti-ransomware skener** se zobrazí detekce, které reportovala Ochrana proti ransomware.
- **Akce** – vyberte akci provedenou nad detekcí. Bezpečnostní produkty ESET reportují do ESET PROTECT následující akce:
  - **vyléčeno** – detekce byla vyléčena.
  - **odstraněno / vyléčeno smazáním** – detekce byla odstraněna.
  - **byl součástí odstraněného objektu** – archiv obsahoval detekci, která byla odstraněna.
  - **blokováno / přerušeno spojení** – přístup k detekovanému objektu byl zablokován.
  - **ponecháno** – z mnoha důvodů nebyla provedena žádná akce. Příklad:
    - ➢ Uživatel v interaktivním upozornění ručně vybral možnost „neprovádět žádnou akci“.
    - ➢ V nastavení detekčního jádro v bezpečnostním produktu ESET je úroveň **ochrany** pro danou kategorii nižší než úroveň **hlášení**.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Správa detekcí



Po kliknutí na název detekce se zobrazí postranní panel se základními informacemi o detekci, tzv Náhled detekce.

Pro správu konkrétní detekce na ni klikněte a vyberte si dostupnou akci ze zobrazeného kontextového menu. Případně zaškrtněte více záznamů a následně použijte tlačítka v dolní části obrazovky Detekce:

- **Zkontrolovat** – pomocí této možnosti spustíte volitelnou kontrolu na klientovi, na kterém došlo k detekci.
- **Detaily** – kliknutím si zobrazíte Detaily detekce.
- V rozbalovacím menu v podsekci **Počítač** naleznete seznam dostupných akcí, které můžete provést nad počítačem, na kterém došlo k detekci. Jedná se o stejný seznam jako na záložce Počítače.
- **Audit log** – kliknutím si zobrazíte Audit log pro vybranou položku.
- **Označit jako vyřešené** nebo **Označit jako nevyřešené** – detekce můžete označit jako vyřešené nebo nevyřešené. Stejnou akci můžete provést také v Detailech počítače.
- **Zkontrolovat umístění** (dostupné pouze pro **Antivirové** detekce – soubory se známou cestou) – kliknutím vytvoříte úlohu na volitelnou kontrolu počítače s předdefinovaným cílem a cestou.
- **Vytvořit výjimku** (dostupné pouze pro **Antivirové** detekce a IDS pravidla **firewallu**) – kliknutím vytvoříte detekční výjimku.
- **Prozkoumat (Inspect)** – kliknutím si zobrazíte detaily objektu v ESET Inspect Web Console. Kliknutím na ikonu **Inspect** v pravém horním rohu otevřete ESET Inspect Web Console a přejdete do sekce Detekce. Tlačítko ESET Inspect je dostupné pouze v případě, že vlastníte licenci na ESET Inspect a ESET Inspect máte připojen k ESET PROTECT. Uživatel Web Console potřebuje alespoň sadu oprávnění s hodnotou **pouze pro čtení** u možnosti **Přístup k ESET Inspect**.
- Možnost **Odeslat soubor do ESET LiveGuard** je dostupná pouze pro **Blokované soubory**. Soubor k

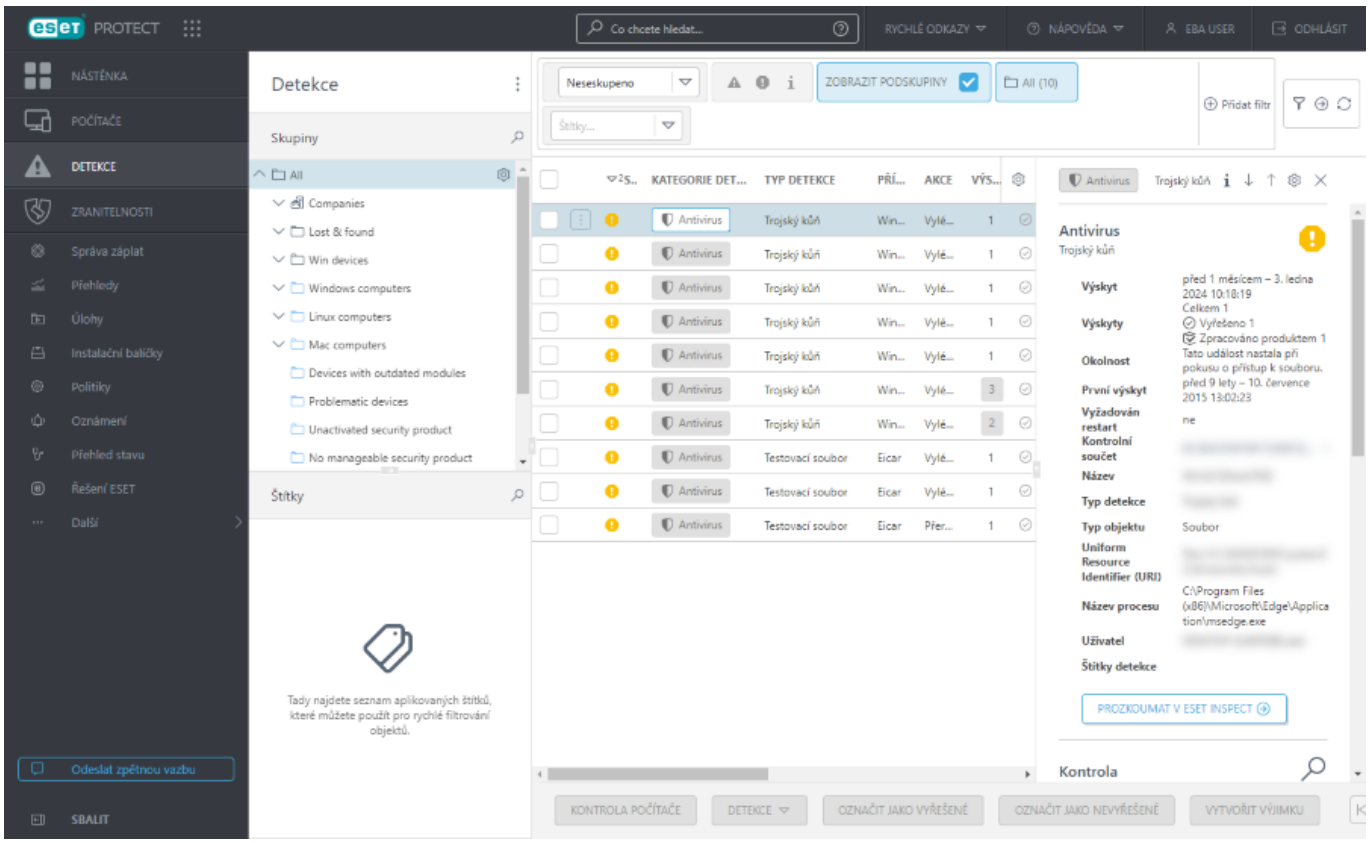
analýze lze odeslat do ESET LiveGuard Advanced přímo z webové konzole ESET PROTECT. Výsledek analýzy bude následně dostupný v sekci Odeslané soubory. Pro odeslání spustitelného souboru k analýze do ESET LiveGuard Advanced můžete rovněž využít nainstalovaný bezpečnostní produkt ESET, který je aktivován ESET LiveGuard Advanced licencí.

Náhled detekce

Tento postranní panel se zobrazí, pokud v části **Detekce** kliknete v zobrazené tabulce na název detekce. V náhledu detailů detekce naleznete nejdůležitější informace o vybrané detekci.

Práce s náhledem detekce:

- **Detaily** – po kliknutí se zobrazí standardní dialogové okno s Detaily detekce.
- **Další** – po kliknutí si zobrazíte detaily další detekce v pořadí.
- **Předchozí** – po kliknutí si zobrazíte detaily předchozí detekce v pořadí.
- **Správa obsahu detailů detekce** – po kliknutí se zobrazí dialogové okno, ve kterém můžete upravit jaké informace a v jakém pořadí chcete v náhledu detekce zobrazovat.
- **Zavřít** – kliknutím zavřete panel s náhledem detekce.



Detaily detekce

Detaily detekce jsou rozděleny do dvou sekcí:

- Na záložce **Přehled** se nacházejí obecné informace o detekci. Z této obrazovky můžete nad detekcí provést

různé akce (v závislosti na kategorii detekce se budou lišit). Případně můžete přejít přímo do detailů počítače a zobrazit si podrobnější informace o stanici, na níž k detekci došlo.

- Záložka **Výskyty** je dostupná pouze v případě, kdy došlo k agregaci detekce. Poté zde uvidíte seznam jednotlivých **výskytů** dané detekce. Všechny výskyty stejné detekce následně můžete hromadně označit jako (ne)vyřešené.

Vytvoření výjimky

Vybrané záznamy v sekci **Detekce** můžete vyloučit z kontroly a zabránit tak jejich detekci v budoucnu. Klikněte na detekci a ze zobrazeného kontextového menu vyberte možnost **Vytvořit výjimku**. Vyloučit je možné pouze **Antivirové** detekce a vytvořit výjimky na detekce **firewallu** – IDS pravidla. Vytvořené výjimky můžete aplikovat na počítače a/nebo skupiny. Pro jejich snadnější správu a lepší přehled o existujících výjimkách naleznete všechny vytvořené výjimky v sekci **Další** > **Výjimky**.

Výjimky používejte s rozmyslem. Jejich aplikováním může dojít k infikování počítače.

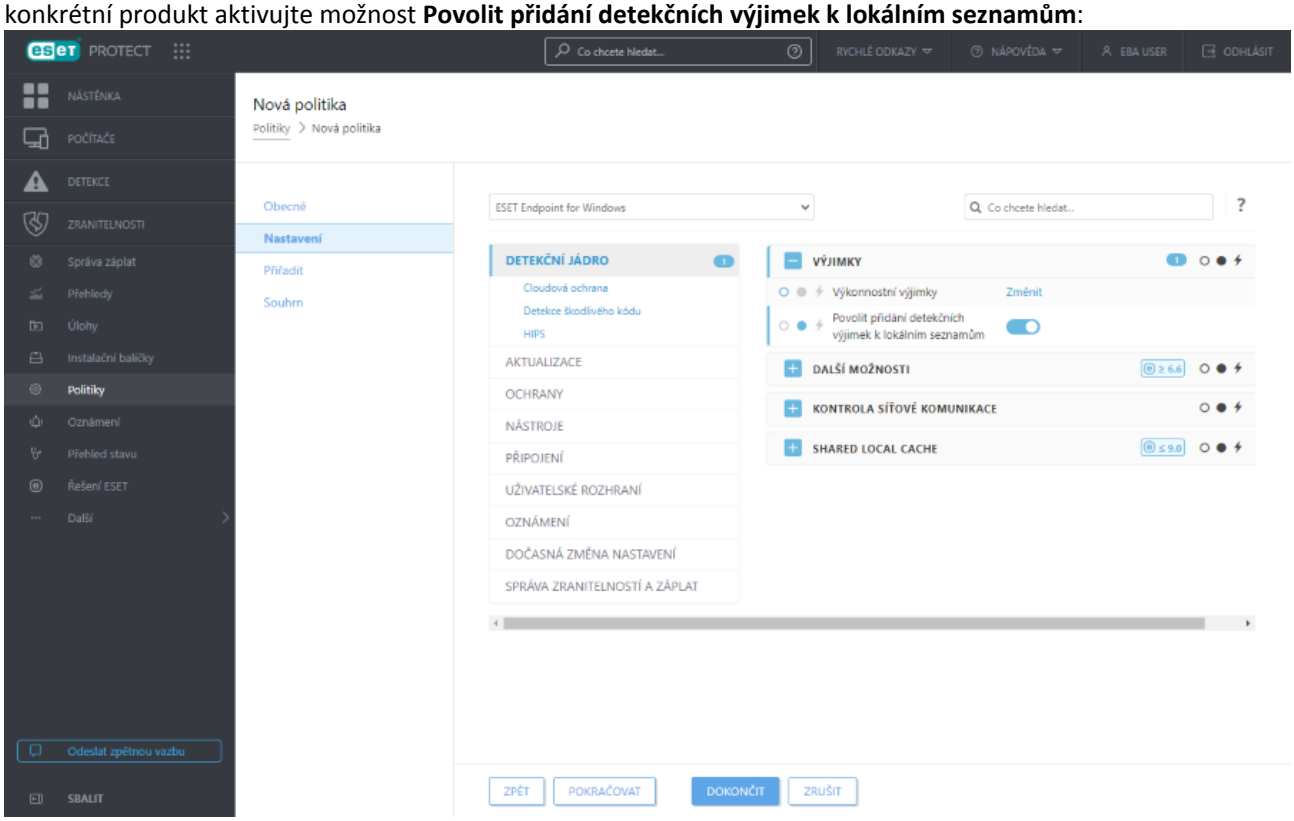
V ESET PROTECT jsou **antivirové** výjimky rozděleny do dvou kategorií:

- **Výkonnostní výjimky** – slouží k vyloučení souborů a složek na základě cesty. Definovat je můžete pomocí politiky. Prostudujte si formát a příklady výkonnostních výjimek.

- **Detekční výjimky** – prostřednictvím nich vyloučíte soubory na základě názvu detekce, cesty nebo podle hashe objektu. Prostudujte si příklady detekčních výjimek na základně názvu detekce.

Omezení detekčních výjimek

- V ESET PROTECT není možné definovat detekční výjimky prostřednictvím politiky pro konkrétní produkt.
- V případě, že máte v politikách definované detekční výjimky, můžete postupovat podle návodu na migraci výjimek.
- Standardně dojde na spravovaných počítačích po aplikování detekčních výjimek k nahrazení lokálního seznamu výjimek: Pokud chcete existující lokální seznam výjimek zachovat, před aplikováním výjimek nejprve v politice pro konkrétní produkt aktivujte možnost **Povolit přidání detekčních výjimek k lokálním seznamům**:



Nastavení

Detekce můžete vyloučit na základě vybraných **kritérií**.

Detekce antivirem

- **Cesta + Detekce** – pomocí této možnosti vyloučíte v konkrétním souboru nacházející se v dané cestě (například *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*) definovanou detekci.
- **Konkrétní soubory** – pomocí této možnosti vyloučíte soubor podle jeho hashe.
- **Detekce** – pomocí této možnosti vyloučíte v každém souboru konkrétní detekci.

Detekce v archivech

Při výskytu detekce v archivu je do seznamu **detekcí** reportován daný archiv a každá detekce.

Vyloučením archivu obsahujícím detekci nedojde k vyloučení samotné detekce. V tomto případě je nutné vyloučit jednotlivé detekce nacházející se v archivu. Maximální velikost souboru v archivu je 3 GB.

Vyloučené detekce již následně nebudou zaznamenávány – i když se budou nacházet v jiném archivu, nebo samostatně (nearchivované).

Detekce firewallu – IDS pravidla

- **Detekce a kontext** (doporučeno) – pomocí této možnosti vytvoříte výjimku na detekci firewallem na základě kombinace následujících kritérií: podle detekce, aplikace a IP adresy.
- **IP adresa** – pomocí této možnosti vytvoříte výjimku na detekci firewallem na základě vzdálené IP adresy. Tuto možnost použijte v případě, kdy síťová komunikace s konkrétním počítačem generuje falešné detekce.
- **Detekce** – pomocí této možnosti vytvoříte výjimku na konkrétní detekci a stejně tak budou příchozí falešné detekce ignorovány z libovolného množství počítačů.
- **Aplikace** – pomocí této možnosti vytvoříte v síťových detekcích výjimku na konkrétní aplikaci. Povolena bude síťová komunikace aplikace, která inicializovala IDS falešná poplachy.

Na základě typu detekce je vždy předvybrána doporučená možnost.

Pro automatické vyřešení souvisejících upozornění vyberte možnost **Vyřešit vyhovující upozornění**.

Volitelně můžete k vytvářené výjimce přidat **Komentář**.

Cíl

Mějte na paměti, že výjimky (**Antivirové** detekce a IDS pravidla **firewallu**) se aplikují pouze na kompatibilní bezpečnostní produkty ESET. Výjimky se neaplikují na nepodporované bezpečnostní produkty ESET. V takovém případě budou ignorovány.

Vytvořené výjimky se automaticky aplikují na domovskou skupinu uživatele, který výjimku vytváří.

Pro změnu přiřazení klikněte na tlačítko **Přidat cíle** a vyberte si počítače nebo skupiny, na které chcete výjimku aplikovat. Případně stávající cíl odeberte pomocí tlačítka **Odstranit cíle**.

Náhled

V této části se můžete podívat na detaily vytvářené výjimky. Ujistěte se, že všechny parametry jsou správné a odpovídají vašim požadavkům.

Mějte na paměti, že po vytvoření výjimky již není možné ji modifikovat. Změnit můžete pouze její přiřazení, případně ji odstranit.

Pro vytvoření výjimky klikněte na tlačítko **Dokončit**.

Seznam všech vytvořených výjimek je dostupný v sekci **Další** > **Výjimky**. Pro ověření, zda se na daný počítač nebo skupinu výjimka aplikuje, přejděte v hlavním menu do sekce Počítače. Najděte požadovaný počítač a vyberte možnost **Detaily počítače**. Následně přejděte na záložku Konfigurace > **Aplikované výjimky**. Případně si otevřete Detaily skupiny a přejděte na záložku **Výjimky**.

Bezpečnostní produkty ESET podporující výjimky

Výjimky se neaplikují na nepodporované bezpečnostní produkty ESET. V takovém případě budou ignorovány.

Detekční výjimky

Antivirové výjimky podporují všechny spravovatelné bezpečnostní produkty ESET. Výjimku tvoří:

- ESET Endpoint Security pro Android
- ESET LiveGuard Advanced
- ESET Inspect

IDS výjimky

Následující bezpečnostní produkty ESET podporují IDS výjimky modulu **firewall**:

- ESET Endpoint Antivirus pro Windows ve verzi 8.0 a novější
- ESET Endpoint Security pro Windows ve verzi 8.0 a novější

Ochrana proti ransomware

Firemní bezpečnostní produkty ve verzi 7 a novější jsou vybaveny samostatnou součástí proti **ransomware** Tato nová bezpečnostní funkce je součástí modulu HIPS a chrání počítač před ransomware. Při výskytu ransomware na stanici naleznete tuto informaci v ESET PROTECT Web Console na záložce **Detekce**. Pro zobrazení pouze ransomware detekcí klikněte na tlačítko **Přidat filtr**, vyberte možnost **Typ skeneru** a **Anti-Ransomware skener**. Pro více informací o této funkci přejděte do slovníku pojmů.

Ochranu proti ransomware můžete vzdáleně konfigurovat z ESET PROTECT Web Console prostřednictvím **politik** pro dané bezpečností řešení.

- **Zapnout ochranu proti ransomware** – bezpečnostní produkty ESET pro firemní uživatele dokáží automaticky blokovat podezřelé aplikace, které se chování jako ransomware.
- **Zapnout režim auditu** – po spuštění režimu budou detekce, které identifikuje ochrana proti ransomware, reportovány do ESET PROTECT Web Console. Bezpečnostní řešení ESET je na zařízeních nebudou blokovat. Jako administrátor se následně můžete rozhodnout, zda detekci zablokujete nebo pro ni **vytvoříte výjimku**. Nastavení politiky je dostupné výhradně prostřednictvím ESET PROTECT Web Console.

Standardně ochrana proti ransomware blokuje všechna aplikace, které se chovají potenciálně jako ransomware – včetně těch legitimních. **Režim auditování** doporučujeme na krátkou dobu zapnout na nově spravovaných počítačích, abyste mohli vytvořit výjimky pro legitimní aplikace, které by mohly být detekovány jako ransomware na základě svého chování (false positives). Nedoporučujeme však režim auditování používat trvale, protože ransomware po dobu běhu tohoto režimu není automaticky blokován.

ESET Inspect

ESET Inspect je komplexní EDR (Endpoint Detection and Response) systém, který nabízí následující funkce: detekce incidentů, správu incidentu a reakce na ně, sběr dat, indikaci na kompromitaci systémů, detekci anomálií, detekci chování a poručení firemní politiky. Pro více informací o produktu, jeho instalaci a možnostech se podívejte do ESET InspectESET Inspect příručky.

Následující bezpečnostní řešení ESET pro firmy byla přejmenována:

Původní název:	Nový název:	Přejmenováno ve verzi:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	

Konfigurace ESET Inspect

ESET Inspect můžete aktivovat prostřednictvím účtu ESET Business Account. Pro aktivaci ESET Inspect Connector musíte vlastnit licenci na ESET Inspect.

Tlačítko ESET Inspect je dostupné pouze v případě, že vlastníte licenci na ESET Inspect a ESET Inspect máte připojen k ESET PROTECT. Uživatel Web Console potřebuje alespoň sadu oprávnění s hodnotou **pouze pro čtení** u možnosti **Přístup k ESET Inspect**.

Nasazení ESET Inspect Connector na spravovaná zařízení

V hlavním menu na záložce **Počítače** > kliknutím do políček vyberte jeden nebo více počítačů > klikněte na tlačítko **Počítač** > vyberte možnost **Řešení** > **Zapnout ESET Inspect**, čímž nasadíte ESET Inspect Connector na spravované stanice s Windows/Linux/macOS.

Reportování ESET Inspect detekcí v ESET PROTECT

ESET PROTECT neukládá detekce odeslané z ESET Inspect, proto je neuvidíte v sekci Detekce. Statistiky ESET Inspect detekcí naleznete v **ESET PROTECT** na **Nástěnce** > **ESET Inspect**.

Další kategorií detekcí reportovaných ESET Inspect serverem jsou **Blokované soubory**. Jedná se o pokusy o spuštění souborů, které jsou prostřednictvím ESET Inspect blokovány (na základě kontrolního součtu).

Kliknutím na detekci a vybráním možnosti **Prozkoumat (Inspect)** si otevřete detaily detekce v ESET Inspect Web Console.

Zranitelnosti

V sekci **Zranitelnosti** je uveden přehled zjištěných zranitelností ve spravovaných zařízeních. Kontrola počítače zjišťuje, zda není nainstalovaný software ohrožen bezpečnostními riziky. Automatizovaná kontrola s okamžitým hlášením do konzole umožňuje stanovit priority zranitelností podle závažnosti, řídit bezpečnostní rizika a efektivně rozdělovat zdroje. Široká škála možností filtrování umožňuje identifikovat kritické bezpečnostní problémy a zaměřit se na ně.

Požadavky

Správu zranitelností a záplat můžete zobrazit a zapnout pouze pokud máte některou z následujících produktových řad:

- ESET PROTECT Elite
- ESET PROTECT Complete
- ESET PROTECT MDR

ESET Správu zranitelností a záplat můžete zapnout pouze na počítačích s operačním systémem Windows a aplikacemi:

- ESET Management Agent verze 10.1 a vyšší
- ESET Endpoint Security pro Windows verze 10.1 a vyšší
- ESET Endpoint Antivirus pro Windows verze 10.1 a vyšší
- ESET Server Security pro Microsoft Windows Server verze 11.0 a vyšší

ESET Vulnerability & Patch Management není podporována na procesorech ARM.

Zapnutí Správy zranitelností a záplat

1. Klikněte na **Počítače**.
2. Vyberte počítač nebo skupinu, u které chcete povolit Správu zranitelností a záplat.
3. Vyberte **Řešení** a klikněte na **Zapnout Správu zranitelností a záplat**.
4. V okně **Zapnout správu zranitelností a záplat**:

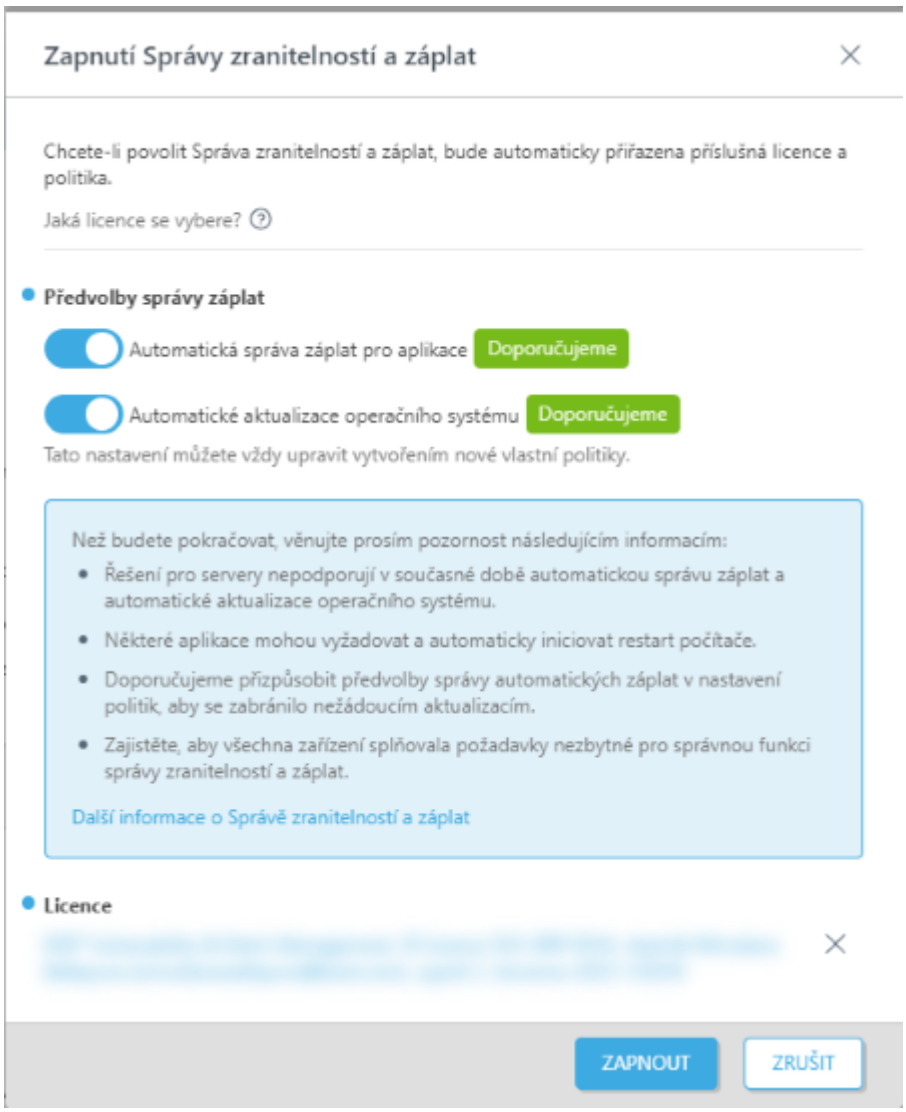
   a.Zkontrolujte, zda je zapnutý přepínač **Automatická správa záplat pro aplikace**, který automaticky aplikuje chybějící záplaty na vybraná zařízení.

   b.Zkontrolujte, zda je zapnutý přepínač **Automatické aktualizace operačního systému**, který automaticky aplikuje aktualizace operačního systému na vybraná zařízení.

Automatické aktualizace operačního systému jsou dostupné pouze pro ESET Endpoint pro Windows 11.0 a novější.

   c.Licence je předem vybrána.

   d.Klikněte na tlačítko **Zapnout**.



Pokud je Správa zranitelností a záplat zapnutá:

- Vedle názvu počítače se zobrazí ikona Zranitelnosti.
- V detailech počítače můžete vidět dlaždici **Správa zranitelností a záplat** ve stavu **Aktivní**.

> Některé aplikace vyžadují restartování počítače a po aktualizaci mohou restartovat počítač automaticky.

> Některé aplikace (například TeamViewer) mohou mít licenci vázanou na konkrétní verzi. Proveďte revizi aplikací. Chcete-li se vyhnout nepotřebným aktualizacím, nastavte při vytváření politiky **Automatické záplatování** > **Záplatovat všechny aplikace kromě vyloučených**.

Zobrazení zranitelností

Zranitelnosti můžete zobrazit několika způsoby:

- Klikněte na **Zranitelnosti** v hlavní nabídce a v sekci **Zranitelnosti** se zobrazí seznam zranitelností.
- Klikněte na **Počítače** > klikněte na počítač a na **Detaily** > v dlaždici **Správa zranitelností a záplat** klikněte na **Zobrazit zranitelnosti** a otevřete sekci **Zranitelnosti**.
- Klikněte na **Počítače** > ve sloupci **Zranitelnosti** klikněte na počet zranitelností ve vybraném počítači a

otevřete sekci **Zranitelnosti**.

Seskupování zranitelností

Pro seskupení zranitelností z rozbalovacího menu vyberte:

- **Neseskupeno** – výchozí zobrazení

- **Seskupení podle názvu aplikace** – zranitelnosti jsou seskupeny podle názvu zranitelné aplikace s počty **Dotčených zařízení** a **Zranitelností**. Po seskupení klikněte na řádek aplikace a po kliknutí na **Zobrazit zranitelnosti** se objeví zranitelnosti vybrané aplikace.

- **Seskupeno podle CVE** – zranitelnosti jsou seskupeny podle čísla CVE (Common Vulnerabilities and Exposure). CVE je identifikační číslo zranitelnosti. Po seskupení klikněte na řádek CVE a po kliknutí na **Zobrazit zařízení** se objeví zařízení (počítače) s danou zranitelností.

Filtrování

Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře.

- **Název aplikace** – název aplikace se zranitelností

- **Verze aplikace** – verze aplikace

- **Výrobce aplikace** – výrobce aplikace se zranitelností

- **Rizikové skóre** – skóre rizika zranitelnosti od 0 do 100

- **CVE** – číslo CVE (Common Vulnerabilities and Exposure), identifikační číslo zranitelnosti

- **Název počítače** – název postiženého počítače; kliknutím na název počítače zobrazíte podrobnosti o počítači se zranitelností

- **Kategorie** – kategorie zranitelnosti:

  - Zranitelnost aplikace

  - Zranitelnost operačního systému

- **První výskyt** – datum a čas, kdy byla zranitelnost v zařízení poprvé zjištěna

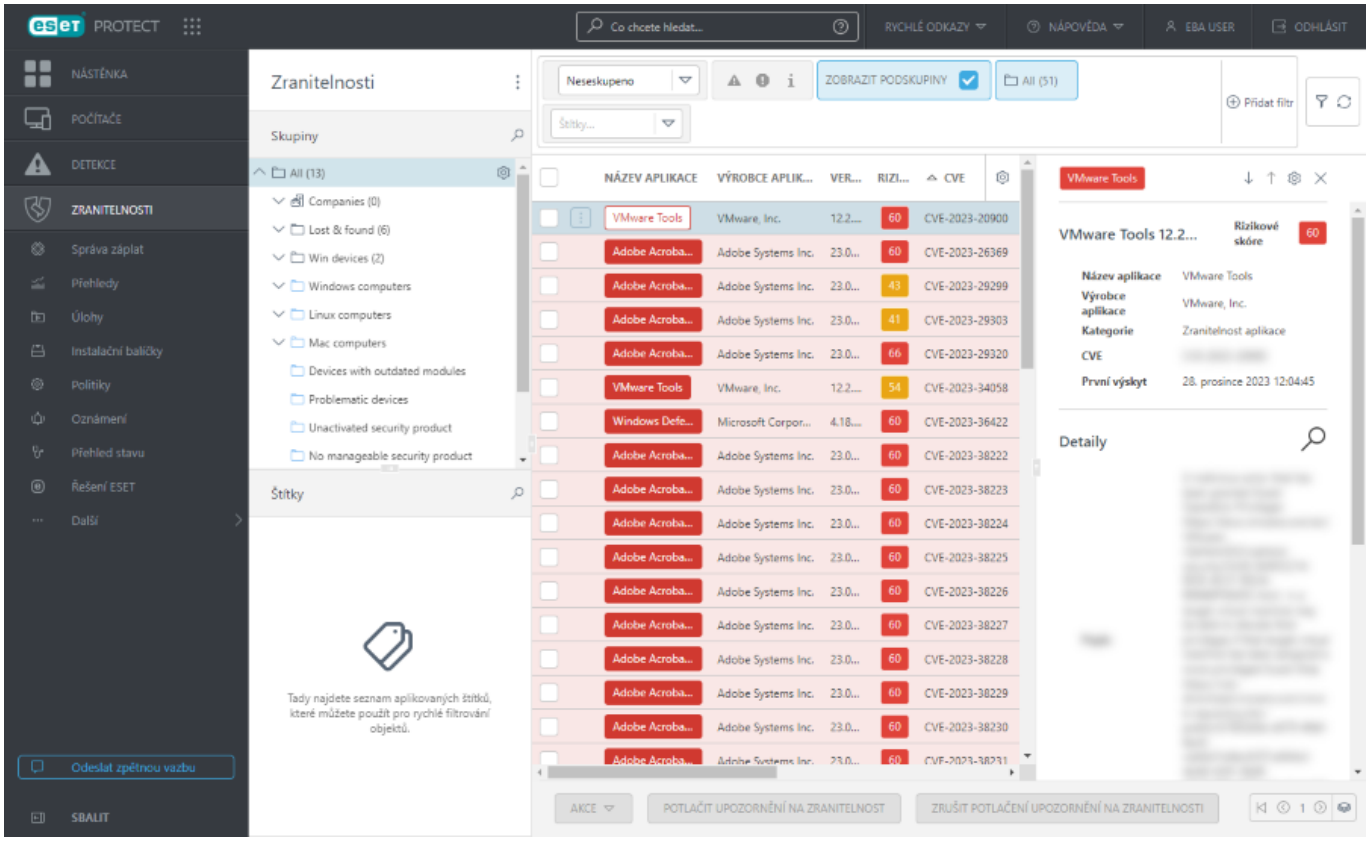
Rizikové skóre – hodnotí závažnost zranitelností zabezpečení počítačového systému. Rizikové skóre se vypočítává na základě následujících údajů:
- CVSSv2/CVSSv3
- Popularita CVE – ukazuje úroveň aktivity zranitelností
- Míra rizika kompromitace – ukazuje počet zařízení s potvrzenou zranitelností
- Životní cyklus CVE – udává dobu, která uplynula od prvního nahlášení zranitelnosti

Rizikové skóre je označováno následovně:
- šedá (0–29) – nízká závažnost
- žlutá (30–59) – střední závažnost
- červená (60–100) – kritická závažnost

Náhled zranitelnosti

Kliknutím na název aplikace se zobrazí podrobnosti o zranitelnosti na bočním panelu. S náhledem zranitelnosti můžete provádět následující manipulace:

- **Další** – zobrazí následující zranitelnost v bočním panelu
- **Předchozí** – zobrazí předchozí zranitelnost v bočním panelu
- **Správa obsahu detailů zranitelnosti** – umožňuje nastavit způsob zobrazení a pořadí sekcí bočního panelu s náhledem zranitelnosti
- **Zavřít** – zavře boční panel náhledu zranitelnosti



Další informace naleznete v seznamu aplikací chráněných funkcí Zranitelnosti.

Potlačení upozornění na zranitelnost

Upozorňování na zranitelnost na zařízeních můžete potlačit nebo toto potlačení zrušit:

- Klikněte na řádek počítače a klikněte na **Potlačit upozornění na zranitelnost** / **Zrušit potlačení upozornění na zranitelnost**
- Vyberte počítač a klikněte na tlačítko **Potlačit upozornění na zranitelnost** / **Zrušit potlačení upozornění na zranitelnost** ve spodní části stránky
- Vyberte počítač a klikněte na tlačítko **Akce** a poté vyberte možnost **Potlačit upozornění na zranitelnost** / **Zrušit potlačení upozornění na zranitelnost**

Kontrola zranitelností

Na vybraném zařízení můžete spustit okamžitou kontrolu zranitelností a chybějících záplat:

- Klikněte na řádek počítače a vyberte možnost **Počítač** > **Kontrola** > **Kontrola zranitelností**
- Vyberte počítač a klikněte na tlačítko **Akce** a vyberte možnost **Počítač** > **Kontrola** > **Kontrola zranitelností**
- Vyberte některou skupinu, klikněte na a vyberte **Úlohy** > **Kontrola** > **Kontrola zranitelností**

Úloha **Spustit kontrolu zranitelností** je naplánována tak, aby se provedla co nejdříve.

Tato úloha může požadovat vyšší výkon zařízení až po dobu 10 minut.

Můžete vytvořit šablonu přehledu s údaji o zranitelnosti a poté přidat tento přehled na Nástěnku.

Další informace naleznete v kapitole Nejčastější dotazy ke Správě zranitelností a záplat.

Aplikace chráněné funkcí Zranitelnosti

Seznam aplikací chráněných Zranitelnostmi je k dispozici pouze v angličtině.

Správa záplat

Správa záplat pomáhá zajistit, aby byly systémy a aplikace zabezpečeny proti známým zranitelnostem a zneužitím. V sekci Správa záplat jsou uvedeny všechny dostupné záplaty odstraňující zjištěné zranitelnosti a usnadňují řešení prostřednictvím automatických aktualizací softwaru. Díky možnostem záplatování můžete okamžitě zajistit, aby byla vaše koncová zařízení aktualizována nejnovějšími bezpečnostními záplatami.

Požadavky

Správu zranitelností a záplat můžete zobrazit a zapnout pouze pokud máte některou z následujících produktových řad:

- ESET PROTECT Elite
- ESET PROTECT Complete
- ESET PROTECT MDR

ESET Správu zranitelností a záplat můžete zapnout pouze na počítačích s operačním systémem Windows a aplikacemi:

- ESET Management Agent verze 10.1 a vyšší
- ESET Endpoint Security pro Windows verze 10.1 a vyšší
- ESET Endpoint Antivirus pro Windows verze 10.1 a vyšší
- ESET Server Security pro Microsoft Windows Server verze 11.0 a vyšší

ESET Vulnerability & Patch Management není podporována na procesorech ARM.

Uživatelé ESET Bridge

ESET Bridge ve výchozím nastavení blokuje síťovou komunikaci Správy záplat. ESET Bridge nemá vliv na hlášení o zranitelnostech.

Chcete-li povolit síťový komunikaci Správy záplat, vypněte pravidla ACL (Access Control List) v konfiguračním souboru ESET Bridge:

1.Otevřete konfigurační soubor pro ESET Bridge *restrict.conf.template* v textovém editoru:
- Windows: *C:\ProgramData\ESET\Bridge\Proxies\Nginx\Conf\restrict.conf.template*
- Linux: */var/opt/eset/bridge/nginx/conf/restrict.conf.template*

2.Změňte `set $valid_host 0;` na `set $valid_host 1;`.
3.Uložte soubor *restrict.conf.template*.
4.Restartujte službu ESET Bridge.

Vypnutí pravidel ACL umožňuje směrovat veškerou síťovou komunikaci přes ESET Bridge (ESET Bridge se stane otevřeným proxy serverem).

Správa záplat je automaticky povolena při aktivaci Správy zranitelností a záplat.

Zobrazení Správy záplat

Správu záplat můžete zobrazit různými způsoby:

- Kliknutím na položku **Správa záplat** v hlavní nabídce otevřete sekci **Správa záplat** a zobrazíte seznam záplat

- Klikněte na **Počítače** > vyberte možnost **Detaily** > v dlaždici **Správa zranitelností a záplat** a po kliknutí na **Zobrazit záplaty** otevřete sekci **Správa záplat**

Seskupování

Pro seskupení zranitelností z rozbalovacího menu vyberte:

- **Neseskupeno** – výchozí zobrazení

- **Seskupit podle názvu aplikace** – po seskupení klikněte na řádek s aplikací a po kliknutí na tlačítko **Zobrazit zařízení** zobrazíte zařízení (počítače), na která bude záplata aplikována

Filtrování

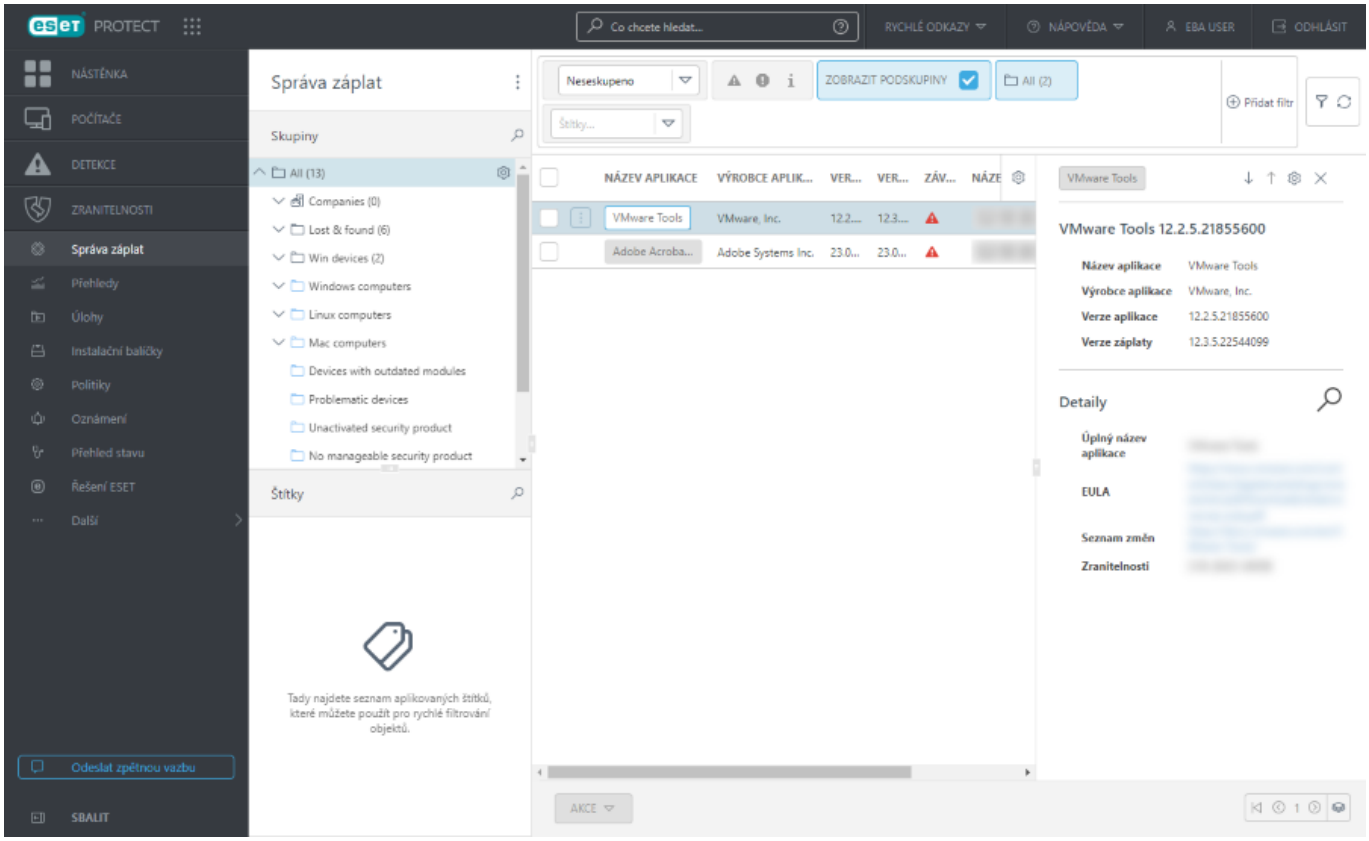
Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře.

- **Název aplikace** – název aplikace s danou zranitelností
- **Verze aplikace** – verze aplikace, která způsobuje zranitelnost
- **Verze záplaty** – verze záplaty
- **Závažnost** – stupeň závažnosti: informační, varovný nebo kritický
- **Název počítače** – název postiženého počítače
- **Výrobce aplikace** – jméno výrobce aplikace

Boční panel s detaily

Kliknutím na název aplikace se zobrazí podrobnosti o aplikaci na bočním panelu. Práce s náhledem aplikace:

- **Další** – zobrazí podrobnosti o další aplikaci na bočním panelu
- **Předchozí** – zobrazí podrobnosti o předchozí aplikaci na bočním panelu
- **Správa obsahu detailů záplaty** – umožňuje nastavit způsob zobrazení a pořadí sekcí bočního panelu
- **Zavřít** – zavře boční panel



Nasazení záplat

Záplatovat můžete pouze vybrané aplikace.

Doporučujeme zapnout automatickou správu záplat pomocí politiky.

Můžete povolit automatické aktualizace operačního systému a vybrat úrovně závažnosti pro použití aktualizací operačního systému prostřednictvím politik.
Automatické aktualizace operačního systému jsou dostupné pouze pro ESET Endpoint pro Windows 11.0 a novější.

Pokud je nastaveno automatické záplatování, dochází k záplatování automaticky během pravidelné údržby.

Některé aplikace vyžadují restartování počítače a po aktualizaci mohou restartovat počítač automaticky.

Některé aplikace (například TeamViewer) mohou mít licenci vázanou na konkrétní verzi. Proveďte revizi aplikací. Chcete-li se vyhnout nepotřebným aktualizacím, nastavte při vytváření politiky **Automatické záplatování** > **Záplatovat všechny aplikace kromě vyloučených**.

Záplaty můžete také nasadit prostřednictvím:

- Vyberte aplikace, které chcete záplatovat > klikněte na tlačítko **Akce** a na **Aktualizovat**.
- Chcete-li aplikaci opravit na všech dotčených zařízeních, použijte **Seskupení podle názvu aplikace**, vyberte řádek s názvem aplikace, klikněte na ⋮ a na **Aktualizovat**.

Po nasazení záplat pomocí tlačítka **Aktualizovat** se v části Úlohy automaticky vytvoří nová klientská úloha **Použití záplaty aplikace**. Na koncová zařízení budou záplaty instalovány na základě plánovače Správy zranitelností a záplat nastaveného v Politikách. U serverů se záplaty nainstalují po 60 sekundách odpočítávání bez možnosti odkladu.

Další informace naleznete v kapitole Nejčastější dotazy ke Správě zranitelností a záplat.

Aplikace chráněné Správou záplat

Seznam aplikací chráněných Správou záplat je k dispozici pouze v angličtině.

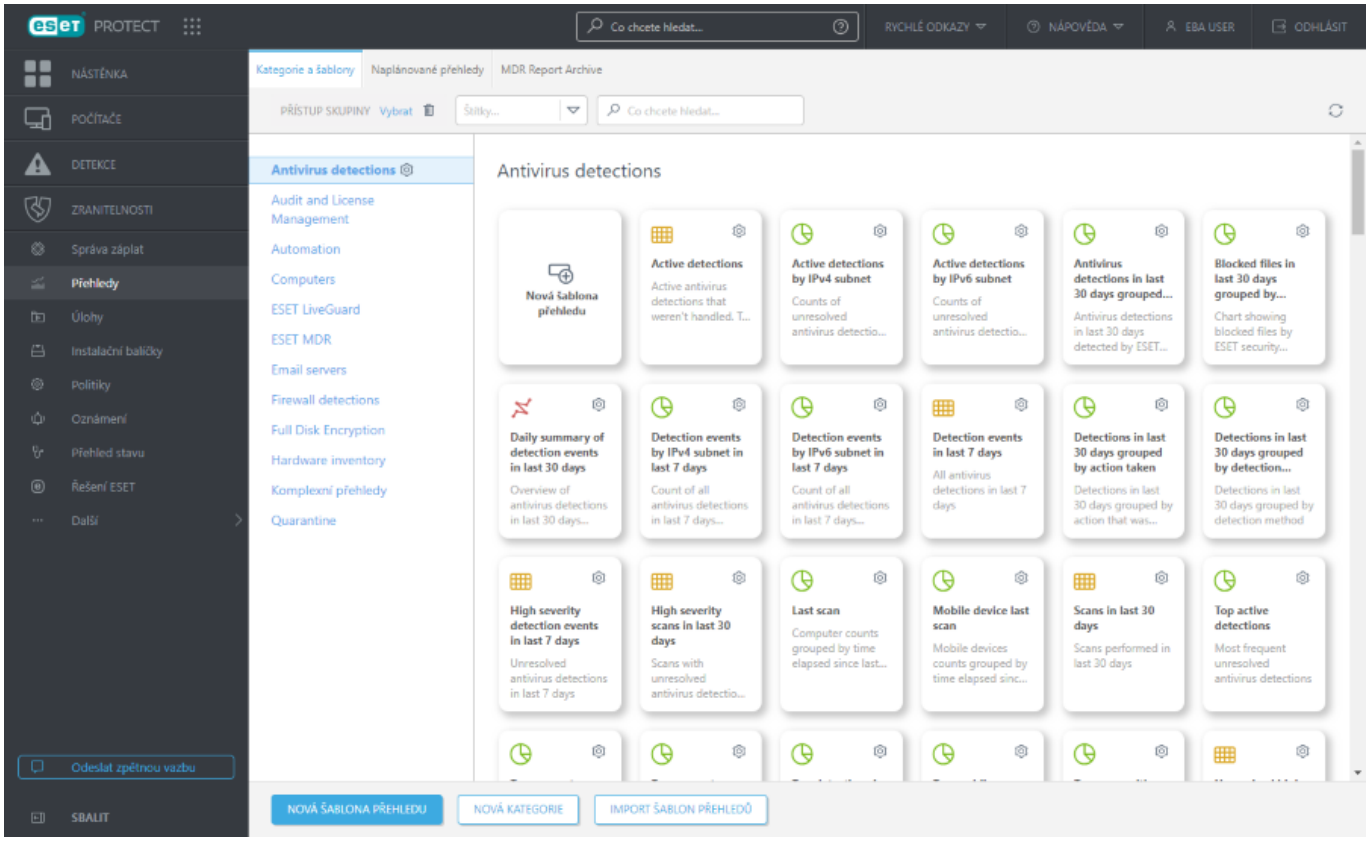
Přehledy

Přehledy představují nástroj pro získání dat z databáze v přehledné podobě. Tato sekce konzole je rozdělena do dvou částí:

- **Kategorie a šablony** – výchozí záložka v sekci **Přehledy**. Máte zde k dispozici seznam všech šablon rozdělených do tematických kategorií. Podle potřeby si můžete vytvářet nové šablony i kategorie a provádět s přehledy související akce.
- **Naplánované přehledy** – na této záložce si můžete prohlédnout, u jakých přehledů máte naplánováno

pravidelné zasílání na e-mail a v případě potřeby můžete rovnou naplánovat pravidelné generování dalších přehledů.

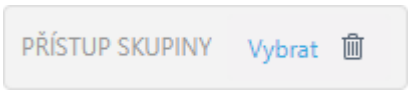
- **Archiv MDR přehledů** – na této záložce je najdete archiv ESET MDR přehledů.



Přehledy jsou generovány ze šablon, které jsou umístěny v jednotlivých kategoriích. Přehledy si můžete vygenerovat jednorázově nebo si jejich generování naplánovat. Pro okamžité vygenerování a zobrazení přehledu na něj najeďte myší a klikněte na tlačítko **Vygenerovat nyní**. Pokud si nevyberete žádnou předdefinovanou šablonu přehledu, kliknutím na tlačítko Nová šablona přehledu si vytvořte novou s vlastními parametry. Pokud si nevyberete žádnou předdefinovanou šablonu přehledu, kliknutím na tlačítko Nová šablona přehledu si vytvořte novou šablonu s vlastními parametry. Vytvořit si můžete také vlastní kategorii, do které si umístíte své přehledy, a hotové šablony (například z jiného serveru) můžete importovat.

V horní části této sekce se nachází vyhledávání. Vyhledávat můžete podle názvu kategorií a šablon přehledů, nikoli však v popisu.

Pro filtrování zobrazených objektů můžete využít štítky.

Prostřednictvím filtru 

Přístup skupiny si můžete vybrat konkrétní statickou skupinu a zjistit, jaké objekty vidí uživatelé, kteří jsou členem dané skupiny.

Používání šablon přehledů

Na dlaždici reprezentující šablonu přehledu klikněte na ikonu ozubeného kolečka : K dispozici jsou následující možnosti:

Vygenerovat	Kliknutím se přehled vygeneruje a zobrazí.

Stáhnout	Pro vygenerování a stažení přehledu klikněte na tlačítko **Vygenerovat a stáhnout**. Vybrat si můžete formát *.pdf* nebo *.csv*. CSV je vhodný formát pouze pro tabulková data a jako oddělovač je použit středník `;`. Pokud si stáhnete přehled ve formátu CSV a ve sloupci, ve kterém očekáváte text, jsou uvedena čísla, pro korektní zobrazení dat si stáhněte přehled ve formátu PDF.
Naplánovat	Naplánovat přehled – po kliknutí se zobrazí dialogové okno, ve kterém můžete definovat podmínku spuštění, kritérium a způsob doručení přehledu. Všechny naplánované přehledy naleznete na záložce **Naplánované přehledy.**
Změnit...	Kliknutím upravíte šablonu přehledu. Následně se zobrazí průvodce, stejný jako při vytváření nové šablony přehledu.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Duplikovat...	Kliknutím vytvoříte ve své domovské skupině kopii vybrané šablony přehledu.
Odstranit...	Kliknutím odstraníte vybranou šablonu přehledu.
Exportovat...	Kliknutím exportujete šablonu do .dat souboru.

Používání kategorií přehledů

Po kliknutí na ikonu ozubeného kolečka v pravé části záhlaví kategorie se zobrazí kontextové menu. K dispozici jsou následující možnosti:

Nová kategorie	Po kliknutí zadejte **název** nově vytvářené kategorie šablon přehledů.
Nová šablona přehledu	Kliknutím vytvoříte v dané kategorii novou šablonu přehledu.
Odstranit...	Kliknutím odstraníte kategorii společně se šablonami.
Změnit...	Kliknutím změníte název kategorie.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Exportovat...	Kliknutím exportujete kategorii společně se všemi šablonami do *.dat* souboru. Pomocí možnosti **Import šablon přehledů** je můžete kdykoli importovat. To je užitečné například při migraci na jiný ESET PROTECT server.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Funkce pro **Import** / **Export šablon přehledů** je určena pro importování a exportování šablon, nikoli vygenerovaných přehledů s aktuálními daty.

Oprávnění pro přístup k přehledům

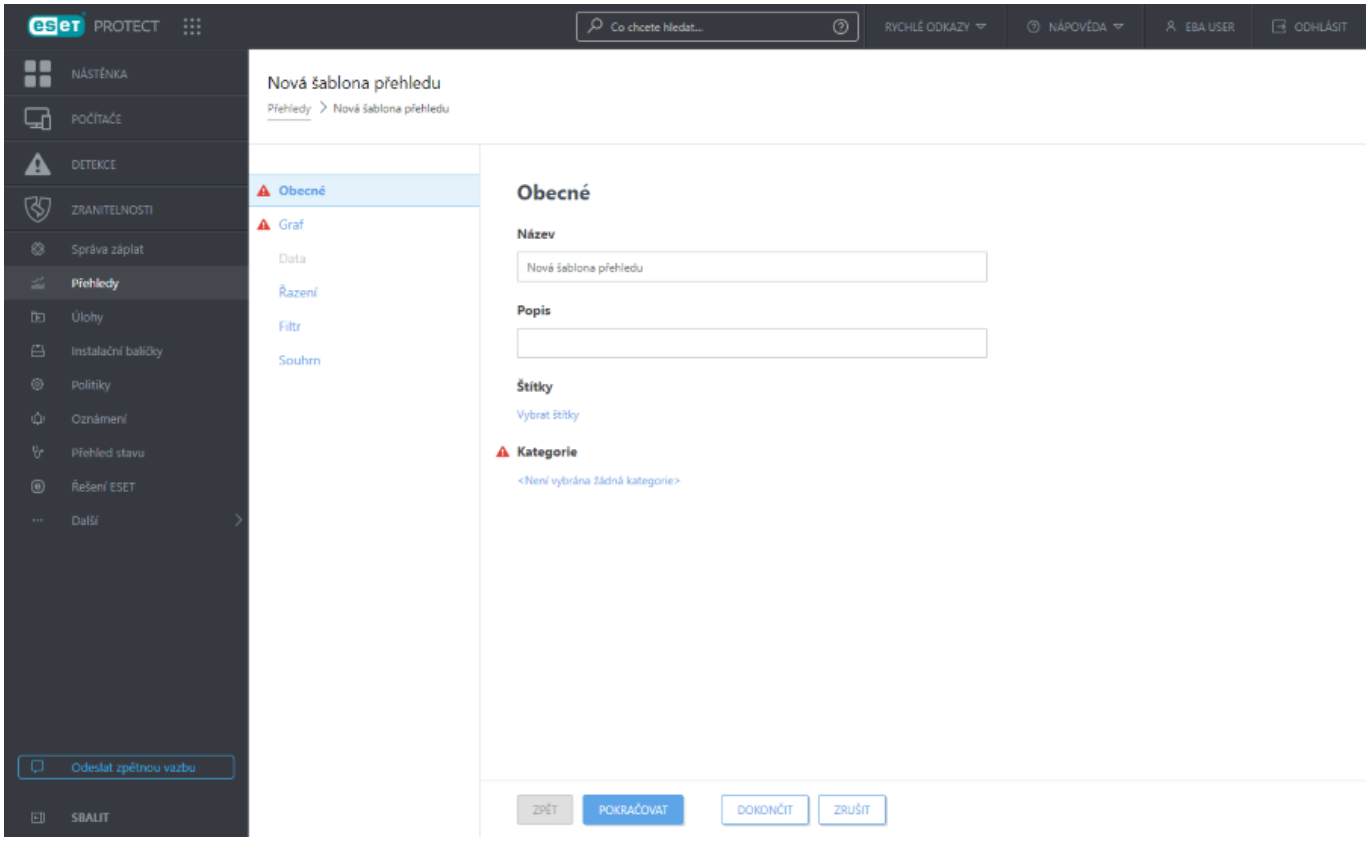
Šablony přehledů jsou statické objekty umístěné ve struktuře objektů ESET PROTECT databáze. Nová šablona přehledu se vytvoří v domovské skupině uživatele, které ji vytvářel. Abyste si mohli zobrazit přehledy, musíte mít přidělené oprávnění **Přehledy a nástěnka**. Zároveň je třeba, abyste měli přidělený také přístup k objektům (počítačům), ze kterých se mají data v přehledu zobrazit. Příklad: při vygenerování přehledu **Stav počítačů** budou v přehledu zohledněna data pouze ze zařízení, k nimž máte alespoň přístup pro **čtení**.

- **Číst** – uživatel může zobrazit šablony přehledů a jejich kategorie, generovat přehledy na základě šablon a číst jejich nástěnku
- **Použít** – uživatel může upravovat svou nástěnku s dostupnými šablonami přehledů
- **Psát** – uživatel může vyvářet, upravovat nebo odstraňovat šablony a jejich kategorie

Všechny výchozí šablony se nacházejí ve skupině pro **všechna zařízení**.

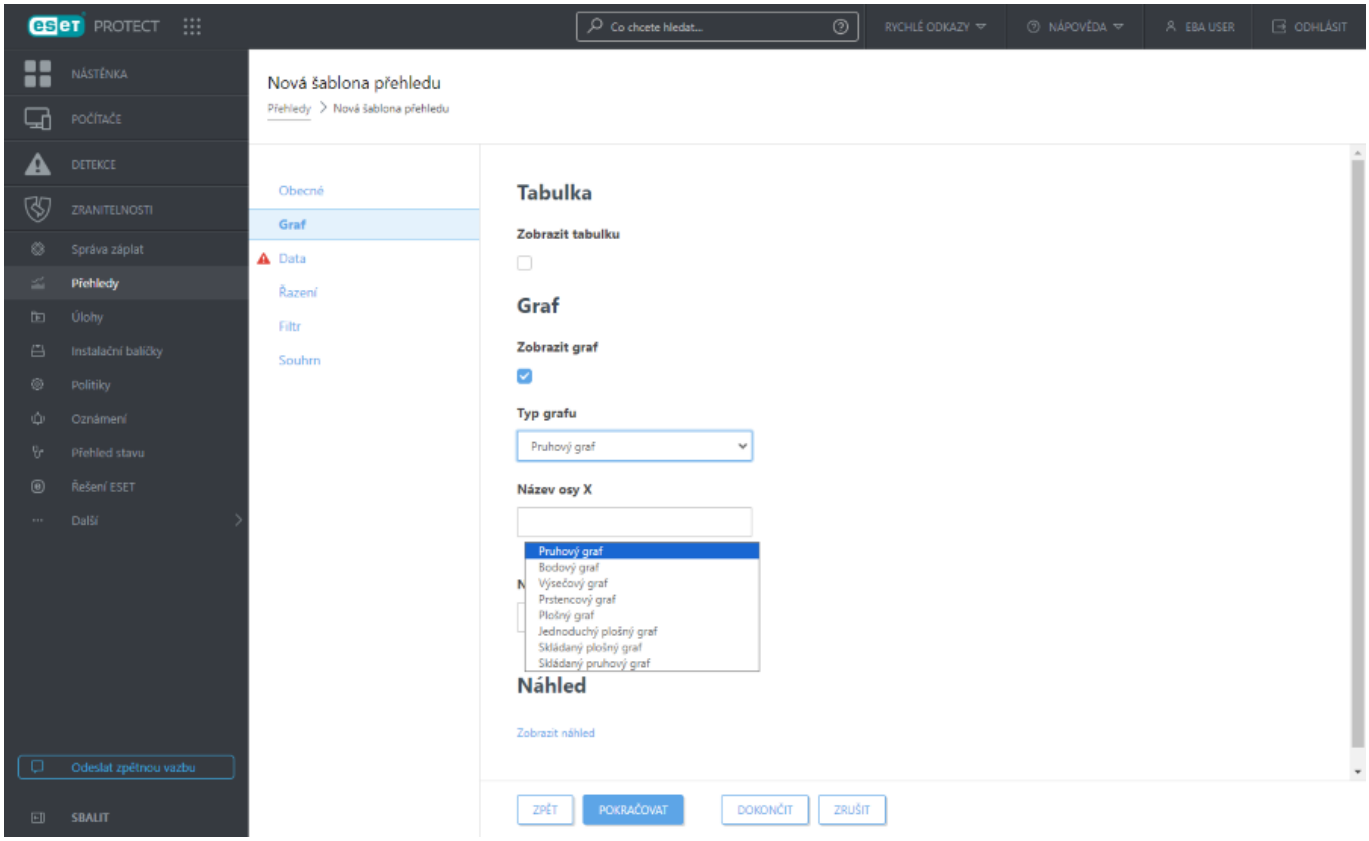
Vytvoření nové šablony přehledu

Pro vytvoření nové šablony přehledu přejděte v hlavním menu na záložku **Přehledy** a klikněte na tlačítko **Nová šablona přehledu**.



Obecné

Nejprve vyplňte obecné informace o šabloně. Zadejte **název**, volitelně **popis**, a vyberte **kategorii**, do které chcete šablonu umístit. Použít můžete jednu z předdefinovaných kategorií. Případně si vytvořte **novou kategorii** dle kroků popsaných v předchozí kapitole. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.



Graf

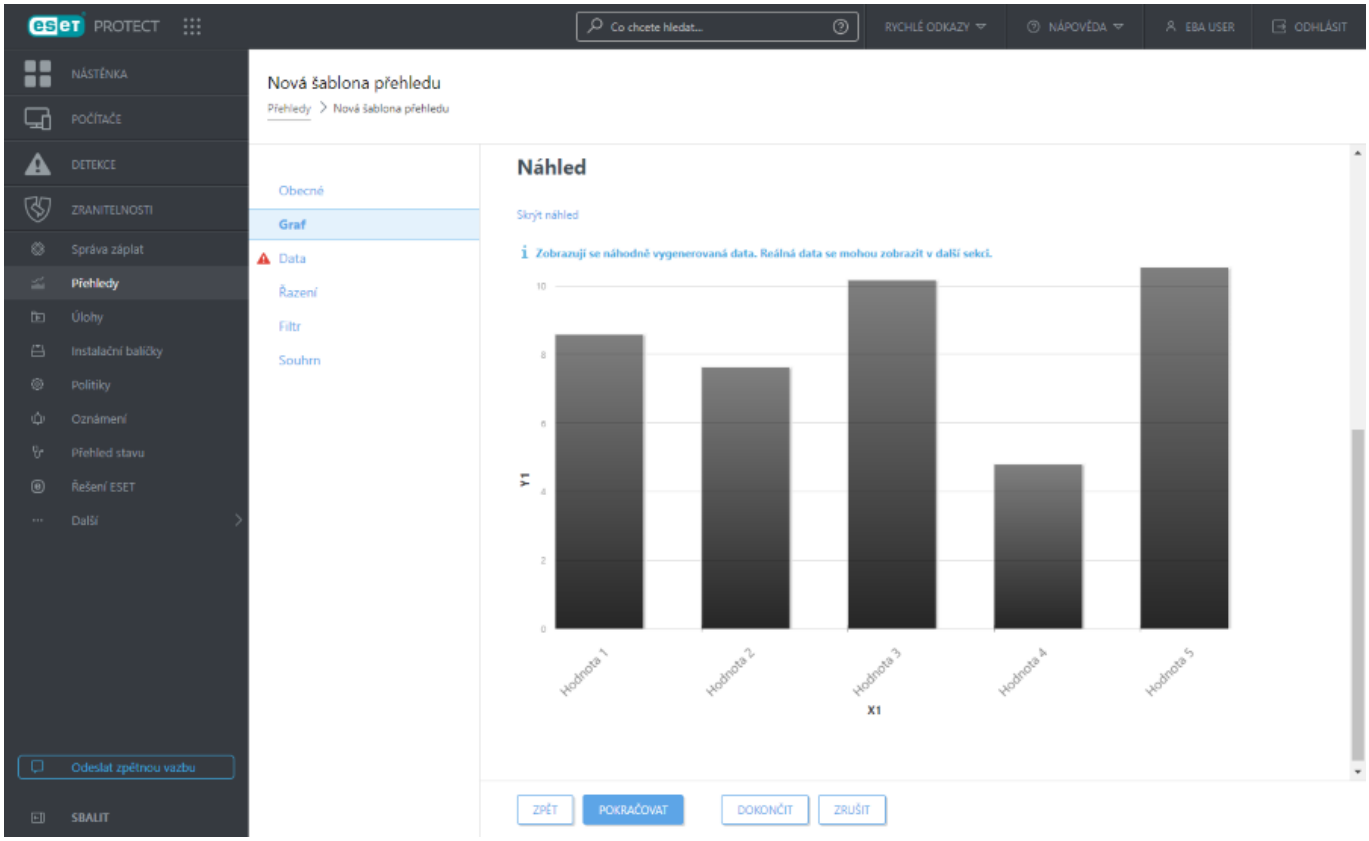
V sekci **Graf** si vyberte požadovaný typ **přehledu**. Rozhodněte se, zda má být výstupem **tabulka** nebo **graf**.

Náhled vybraného typu grafu si můžete zobrazit po kliknutí na **Zobrazit náhled**. Tím zjistíte, jak bude přehled reálně vypadat.

K dispozici jsou následující typy **grafu**:

- **Pruhový graf** – graf s obdélníkovými sloupci.
- **Bodový graf** – jednotlivé hodnoty jsou zobrazeny jako body.
- **Výsečový graf** – proporčně rozdělený kruhový graf.
- **Prstencový graf** – podobný jako výsečový graf, ale může obsahovat různé typy dat.
- **Plošný graf** – jednotlivé bodové hodnoty jsou propojeny spojnicí.
- **Jednoduchý plošný graf** – zobrazuje informace pomocí čar (nezobrazuje hodnoty jako body).
- **Skládaný plošný graf** – tento typ grafu použijte, pokud potřebujete analyzovat data v jiných jednotkách.
- **Skládaný pruhový graf** – do tohoto grafu můžete vybrat více druhů dat, které zobrazí v jednom sloupci.

Volitelně můžete zadat popisek pro osu **X** a **Y**, což vám usnadní orientaci v grafu.



Data

V této části vyberte **data**, která chcete zobrazit:

a.**Sloupce tabulky**: Informace do tabulky jsou přidávány automaticky na základě vybraného typu přehledu. Přizpůsobit můžete **název**, **popisek** a **formát** (viz níže).

b.**Osy grafu**: Vyberte data, která chcete zobrazit na ose **X** a **Y**. Kliknutím na **Přidat osu** otevřete okno s dalšími možnostmi. Výběr dostupných dat pro osu **Y** závisí na datech vybraných pro osu **X**, a opačně. Graf zobrazuje vztah mezi nimi, proto musí být data vzájemně kompatibilní. Vyberte požadovaná data a klikněte na **OK**.

Formát

Kliknutím na ikonu v sekci **Data** si zobrazíte pokročilé možnosti formátování. Vybrat si můžete **formát**, ve kterém se data zobrazí. Dále můžete přizpůsobit **sloupce tabulky** a **osy grafu**. Mějte na paměti, že všechny možnosti nemusí být dostupné pro každý typ dat.

Formát sloupce	Vyberte sloupec, který chcete formátovat. Pokud formátujete například sloupec **Název**, pro přidání stavových ikon vedle názvu vyberte sloupec **Závažnost**.
Minimální hodnota	Definujte spodní limit pro zobrazení dat.
Maximální hodnota	Definujte horní limit pro zobrazení dat.
Barva	Vyberte si barevné schéma sloupce. Barva se automaticky přizpůsobí dle hodnoty ve sloupci **formát sloupce**.
Ikona	Pomocí této možnosti přidáte do formátovaného sloupce stavové ikony dle hodnoty ve sloupci **Formát sloupce**.

Pomocí šipek ↓ ↑ změníte pořadí sloupců.

Řazení

Pokud vybraná **data** umožňují řazení, odemkne se vám tato možnost. Po kliknutí na **Přidat řazení** definujte vztah mezi vybranými daty. Vyberte počáteční informaci (hodnotu k řazení) a dále režim řazení – zda se data mají řadit **sestupně** nebo **vzestupně**. Tím ovlivníte výsledné zobrazení grafu. Pomocí tlačítek **Nahoru** a **Dolů** ovlivníte prioritu řazení. Kliknutím na ikonu koše 🗑 odstraníte parametr řazení.

Filtr

V této části můžete definovat režim filtrování. Klikněte na **Přidat filtr**, vyberte jaká data chcete filtrovat a zadejte výraz pro jejich filtrování. Tím omezíte množství zobrazených dat. Kliknutím na ikonu koše 🗑 odstraníte parametr řazení.

Souhrn

V této části se zobrazí **souhrnné informace** o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření **šablony přehledu** klikněte na tlačítko **Dokončit**.

Generování přehledu

Přehled můžete jednorázově vygenerovat jedním z níže uvedených způsobů:

- Klikněte na **Přehledy** a zvolte sekci **Kategorie a šablony**. Vyberte šablonu přehledu, kterou chcete vygenerovat. Pokud chcete provést změny v šabloně přehledu, najeďte myší na požadovanou šablonu, klikněte na ikonu ozubeného kolečka a klikněte a z kontextového menu vyberte možnost **Změnit**.
  - Pro vygenerování přehledu a jeho zobrazení v ESET PROTECT Web Console jednoduše klikněte na dlaždici, která reprezentuje jeho šablonu. Následně si ho v případě potřeby můžete uložit, kliknutím na tlačítko **Vygenerovat a stáhnout**, v požadovaném formátu do svého počítače. Vybrat si můžete formát *.pdf* nebo *.csv*. CSV je vhodný formát pouze pro tabulková data a jako oddělovač je použit středník `;`. Pokud si stáhnete přehled ve formátu CSV a ve sloupci, ve kterém očekáváte text, jsou uvedena čísla, pro korektní zobrazení dat si stáhněte přehled ve formátu PDF.
- V hlavním okně přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** > ＋ **Serverová úloha** a vytvořte úlohu na Generování přehledu.
  - Úloha se vytvoří a bude připravena k použití. Vyberte v seznamu vytvořenou úlohu a klikněte na možnost **Spustit nyní**. Úloha se okamžitě spustí a dojde k vygenerování přehledu na základě vámi definovaných parametrů.
  - Popis parametrů, které je možné konfigurovat, naleznete v kapitole Generování přehledu.

> ℹ Pokud máte přehled zobrazen v ESET PROTECT Web Console, po kliknutí na položku uvedenou v přehledu se zobrazí kontextové menu s dalšími možnostmi.

Šablona MDR přehledu

Šablona MDR přehledu je bezpečnostní report pro poskytovatele MDR (Managed Detection and Response).

K vygenerování MDR přehledu potřebujete licenci ESET Inspect. Uživatel potřebuje sadu oprávnění pro **Komplexní přehledy** (administrátor / pouze pro čtení / vlastní), aby mohl generovat šablonu MDR přehledu:

1. Klikněte na **Přehledy** a zvolte sekci **Kategorie a šablony**.
2. Klikněte na **Komplexní přehledy** a **Šablona MDR přehledu**.
3. Klikněte na **Vygenerovat a stáhnout**. Šablonu MDR přehledu můžete vygenerovat pouze jako soubor s příponou .odt.

Naplánování generování přehledu

Naplánovat pravidelné generování přehledu můžete několika způsoby:

- V hlavním okně přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** > **Serverová úloha** a vytvořte úlohu na Generování přehledu.
- V hlavním menu přejděte na záložku **Přehledy**, u šablony přehledu, který chcete generovat, klikněte na ikonu ozubeného kolečka a z kontextového menu vyberte možnost **Naplánovat**. Pokud vám žádný přehled z těch předdefinovaných nevyhovuje, vytvořte si novou šablonu.
- Na Nástěnce klikněte na ozubené kolečko u konkrétního přehledu a z kontextového menu vyberte možnost **Naplánovat**.
- V hlavním menu přejděte na záložku **Přehledy** > **Naplánované přehledy** a klikněte na tlačítko **Naplánovat přehled**.

Při plánování generování přehledu máte k dispozici několik možností:
- V jednom plánu můžete vybrat více šablon přehledů.
- MSP uživatelé mohou přehledy filtrovat podle zvoleného zákazníka.
- Nastavit doručení přehledu e-mailem.
- Volitelně můžete definovat podmínku spuštění a parametry pro zabránění její nadměrné aktivace.

Maximální povolená velikost e-mailu v ESET PROTECT infrastruktuře je 30 MB.

Pro vytvoření naplánované úlohy klikněte na tlačítko **Dokončit**. Úloha se vytvoří a následně se spustí v intervalu definovaném podmínkou spuštění (jednou nebo pravidelně) na základě nastaveného throttlingu (volitelně).

Naplánované přehledy

Informace o naplánovaném generování přehledů naleznete v sekci **Přehledy > Naplánované přehledy**. V této části a v kontextovém menu jednotlivých úloh jsou dostupné tyto akce:

Naplánovat	Kliknutím vytvoříte plán pro vygenerování existující šablony přehledu.
Zobrazit detaily	Kliknutím si zobrazíte detaily naplánované úlohy.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.

Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
Spustit nyní	Kliknutím spustíte naplánovanou úlohu.
Změnit…	Kliknutím upravíte parametry naplánované úlohy. Do plánu můžete přidat další šablony, odebrat je z něj, upravit nastavení plánovače, podmínky spuštění a možnosti doručení přehledů.
Duplikovat…	Kliknutím vytvoříte ve své domovské skupině kopii naplánované úlohy.
Odstranit…	Kliknutím odstraníte úlohu z plánovače. Touto akcí nedojde k ovlivnění šablony přehledu.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

ESET MDR

ESET MDR poskytuje přehled o incidentech a detekcích z ESET Inspect. Používání ESET MDR vyžaduje licenci ESET Inspect a úroveň **ESET PROTECT MDR**.

> **Dostupnost ESET MDR v jednotlivých zemích**
> ESET MDR je k dispozici v následujících zemích: USA, Kanada, Japonsko, Velká Británie, Nizozemsko, Francie, Itálie, země DACH (Německo, Rakousko, Švýcarsko), severské země (Švédsko, Norsko, Dánsko, Finsko, Island), Slovensko, Česká republika, Ukrajina.

Služba ESET MDR se vztahuje na všechna spravovaná zařízení se spuštěným programem ESET Inspect. Podle následujících kroků vyberte zařízení, u kterého chcete spravovat zabezpečení nezávisle na službě ESET MDR:

1. Otevřete ESET PROTECT a přejděte do sekce **Počítače**.
2. Klikněte na ikonu ozubeného kola vedle existující nadřazené statické skupiny a vyberte možnost **Nová statická skupina**.
3. Do pole **Název** zadejte `exempt` a klikněte na **Dokončit**.
4. Vyberte nadřazenou skupinu a vyberte zařízení, která chcete zahrnout do skupiny pro vyloučená zařízení.
5. Klikněte na tlačítko **Počítač** > **Spravovat** > **Přesunout do skupiny** a vyberte skupinu `exempt`.

Zařízení ve skupině `exempt` spravujete vy sami – incidenty můžete řešit ručně bez automaticky aplikovaných reakcí.

> Viz také Nástěnka ESET MDR.

ESET MDR přehled

ESET MDR přehled je týdenní souhrn bezpečnostních informací z různých zdrojů v síti.

K naplánování ESET MDR přehledu potřebujete následující sady oprávnění:
- **ESET MDR přehled** – zápis
- **Serverové úkoly a podmínky spuštění** – **Generování přehledu** – použití, zápis

Po aktivaci licence ESET PROTECT MDR se automaticky naplánuje jedna serverová úloha spojená s e-mailem administrátora.

Příjemci automaticky obdrží **týdenní ESET MDR přehled**.

1. Klikněte na **Přehledy** a vyberte záložku **Kategorie a šablony** > **ESET MDR**.
2. Klikněte na ikonu ozubeného kola u **Akcí** na **Týdenním přehledu ESET MDR** a klikněte na **Naplánovat**.
3. Případně můžete kliknout na **Vybrat štítky** a přiřadit k přehledu štítky. Klikněte na tlačítko **Pokračovat**.
4. V rozbalovacím menu **Jazykové prostředí** vyberte preferovaný jazyk přehledu a v rozbalovacím menu **Časové pásmo** vyberte časové pásmo. Nabídka **Typ podmínky spuštění** je vypnutá. Automaticky je vybrána možnost týdně (každé pondělí).
5. Do pole **Komu** zadejte e-mailovou adresu příjemce.
6. Můžete také vybrat možnost **Přizpůsobit zprávu** a zadat **předmět** a obsah **zprávy**.
7. Klikněte na tlačítko **Dokončit**.

Týdenní ESET MDR přehled můžete vytvořit také spuštěním serverové úlohy Generování přehledu:

1. Vyberte **Úlohy** > **Nová** > **Serverová úloha**.
2. Z rozbalovacího menu **Úloha** vyberte **Generování přehledu** a klikněte na **Pokračovat**.
3. Klikněte na **Přidat šablonu přehledu** a vyberte **Týdenní ESET MDR přehled**.
4. Do pole **Komu** zadejte e-mailovou adresu příjemce.
5. Můžete také vybrat možnost **Přizpůsobit zprávu** a zadat **předmět** a obsah **zprávy**.
6. Klikněte na tlačítko **Pokračovat**.
7. V rozbalovacím menu **Jazykové prostředí** vyberte preferovaný jazyk přehledu a v rozbalovacím menu **Časové pásmo** vyberte časové pásmo. Nabídka **Typ podmínky spuštění** je vypnutá. Automaticky je vybrána možnost týdně (každé pondělí).
8. Klikněte na tlačítko **Pokračovat**.
9. Zkontrolujte nastavení v části **Souhrn** a klikněte na **Dokončit**.

Týdenní ESET MDR přehled obdržíte jako .pdf soubor.
Pokud máte aktivní bezpečnostní řešení na úrovni ESET PROTECT MDR, bude se Týdenní ESET MDR přehled generovat každé pondělí.

Archiv MDR přehledů

Archiv MDR přehledů obsahuje všechny přehledy ESET MDR zaslané e-mailem. Obdržíte e-mail s odkazem na přehled a můžete se vrátit k jakémukoli ESET MDR přehledu vytvořenému v posledním roce.

Archiv ESET MDR přehledů najdete v sekci **Přehledy** > **Archiv MDR přehledů**.

Předpoklady
Archiv přehledů můžete zobrazit, pokud jste nastavili oprávnění pro **používání** v sadách pro **přehledy ESET MDR** a:
- aktivovali licenci ESET PROTECT MDR a ESET Inspect
- platnost vaší licence na ESET PROTECT MDR vypršela, ale v posledním roce jste naplánovali a dostali alespoň jeden přehled

Rozložení postranního panelu

Klikněte na ikonu ⋮ vedle názvu **archivu přehledů MDR** a pomocí kontextové nabídky upravte rozložení postranního panelu:

- **Skrýt postranní panel**
- **Štítky**

Filtrování archivu MDR přehledů

Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře.

Můžete použít:

- **Období od** – klikněte na toto pole a vyberte počáteční datum pro filtrování
- **Období do** – klikněte na toto pole a vyberte datum ukončení pro filtrování

Filtry si můžete uložit do svého uživatelského profilu pro budoucí použití. Kliknutím na ikonu **Předvolby** můžete spravovat uložené sady filtrů:

Sady filtrů	Seznam vámi uložených filtrů, které jedním kliknutím aplikujete. Aktuálně použitý filtr má u sebe příznak ✓. Vybráním možnosti **Zahrnout viditelné sloupce, řazení a stránkování** se uloží také tyto parametry.
Uložit sadu filtrů jako	Kliknutím si uložíte aktuální sadu filtrů jako novou předvolbu. Po uložení předvolby již nemůžete měnit konfiguraci filtrů.
Správa sad filtrů	Pomocí této možnosti můžete přejmenovat nebo odebrat existující sady filtrů. Změny se projeví po kliknutí na tlačítko **Uložit**.

Vymazat hodnoty filtru	Kliknutím vynulujete filtry na výchozí hodnoty. Uložená předvolba zůstane beze změny.
Odstranit filtry	Kliknutím odstraníte použité filtry. Uložená předvolba zůstane beze změny.
Odstranit nepoužité filtry	Kliknutím odstraníte filtry, ve kterých nemáte zadanou žádnou hodnotu.
Obnovit výchozí filtry	Pomocí této možností resetujete panel s filtry do výchozího nastavení.

Správa archivu MDR přehledů

Pro změnu pořadí sloupců najeďte myší na ikonu vedle názvu sloupce a sloupec přetáhněte. Viz **Upravit sloupce** níže.

Chcete-li seřadit data podle některého parametru **(Čas vytvoření**/**Období od**/**Období do**), klikněte na záhlaví sloupce a seřaďte řádky tabulky na základě údajů ve vybraném sloupci.

- Jedním nebo dvěma kliknutími seřadíte data v tabulce vzestupně (A–Z, 0–9) nebo sestupně (Z–A, 9–0)
- Po seřazení se v záhlaví sloupce, podle kterého se data řadí, zobrazí malá šipka

Pro správu archivu přehledů, klikněte na ikonu ozubeného kolečka :

Akce

- **Upravit sloupce** –Pomocí této možnosti můžete přidat, odebrat a změnit pořadí zobrazených sloupců. Při správě sloupců můžete využít techniku drag and drop. Kliknutím na **Obnovit** obnovíte sloupce tabulky do výchozího stavu (výchozí dostupné sloupce ve výchozím pořadí).
- **Automaticky přizpůsobit** – pomocí této možnosti se šířka sloupců přizpůsobí velikosti okna.
- **Zobrazit relativní čas**/**Zobrazit absolutní čas** – umožňuje změnit formát **času vytvoření**; najetím myší na **čas vytvoření** se zobrazí relativní/absolutní čas.

Řazení tabulky

- **Zrušit řazení** – kliknutím resetujete řazení podle některého sloupce

Sloupce archivu MDR přehledů

Archiv MDR přehledů obsahuje následující sloupce:

Typ přehledu – týdenní nebo měsíční

Upozornění uživatelé – e-mailová adresa uživatele, který obdržel ESET MDR přehled

Jazykové prostředí – jazyk ESET MDR přehledu

Čas vytvoření – datum vygenerování ESET MDR přehledu

Období od – počáteční datum údajů zaznamenaných v ESET MDR přehledu

Období do – datum ukončení údajů zaznamenaných v ESET MDR přehledu

Časové pásmo – časové pásmo ESET MDR přehledu

Akce archivu přehledů

Po kliknutí na přehled můžete vybrat jednu z akcí:

- **Stáhnout** – stáhne přehled v *.pdf* formátu
- **Odeslat e-mailem** – odešle přehled jako přílohu e-mailu. V rozbalovacího menu můžete vybrat **jazyk e-mailu** a po kliknutí na tlačítko **Přidat** můžete zadat **e-mailové adresy** příjemců. Můžete také kliknout na tlačítko **Více** a **Přidat uživatele** (vybrat adresu uživatele ze sekce Uživatelé zařízení), **Importovat CSV**(importovat vlastního seznamu adres z *.csv* souboru) nebo **Vložit ze schránky** (importovat vlastní seznam adres oddělených vlastním oddělovačem; tato funkce je podobná importu CSV). Po kliknutí na tlačítko **Odeslat** se zpráva odešle jako příloha na vybranou e-mailovou adresu.

> **Záznamy v archivu MDR přehledů**
> ESET MDR přehledy jsou v archivu MDR přehledů po dobu jednoho roku.

Zastaralé aplikace

Pro zobrazení neaktuálních komponent ESET PROTECT použijte přehled **Zastaralé aplikace** (dostupný v sekci **Přehledy** > **Počítače**).

To můžete provést několika způsoby:

- Vytvořte si novou nástěnku, případně upravte existující, a přidejte na ní přehled **Zastaralé aplikace**.
- V hlavním menu přejděte na záložku **Přehledy**, v kategorii **Počítače** najeďte na dlaždici přehledu **Zastaralé aplikace** a klikněte na tlačítko **Vygenerovat**.

Pokud máte v sítí zastaralou aplikaci:

- Pro aktualizaci ESET Management Agenta použijte klientskou úlohu Aktualizovat ESET Agenta.
- Pro aktualizaci bezpečnostních produktů ESET použijte klientskou úlohu Instalace aplikace.

SysInspector prohlížeč

Prostřednictvím SysInspector prohlížeče si můžete přímo ve WebConsole zobrazit SysInspector protokol z koncové stanice. Platí to pro případ, kdy jste si protokol vyžádali prostřednictvím klientské úlohy a úloha již doběhla. Protokoly si můžete v případě potřeby stáhnout do počítače a prohlédnout si je lokálně v aplikaci SysInspector.

> ESET SysInspector je možné spustit pouze na počítačích s Windows.

Jak si prohlédnout SysInspector protokol

Nástěnka

1.Vytvořte si novou nástěnku, případně upravte některou ze stávajících.

2.Jako šablonu přehledu vyberte **Historie SysInspector protokolů za posledních 30 dní** z kategorie **Automatizace**.

3.Vyberte požadovaný záznam a z kontextového menu vyberte možnost **Otevřít SysInspector prohlížeč**.

Přehled

1.Přejděte na záložku Přehledy rozbalte kategorii **Automatizace**.

2.Najděte přehled **Historie SysInspector protokolů za posledních 30 dní** a klikněte na tlačítko **Vygenerovat**.

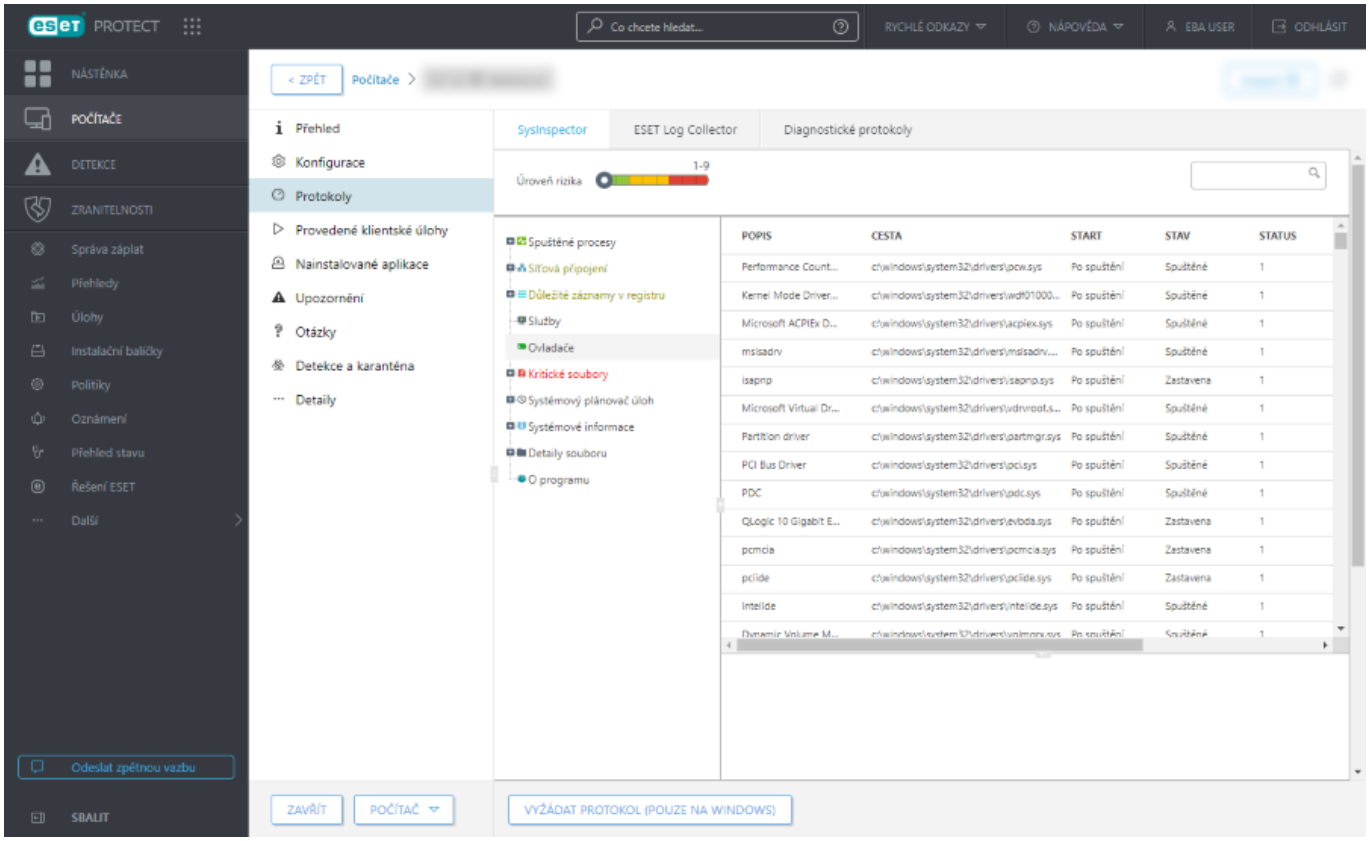
3.Vyberte požadovaný záznam a z kontextového menu vyberte možnost **Otevřít SysInspector prohlížeč**.

Detaily počítače

1.Přejděte na záložku Počítače.

2.Klikněte na konkrétní počítač (ve statické nebo dynamické skupině) a z kontextového menu vyberte možnost **Zobrazit detaily**.

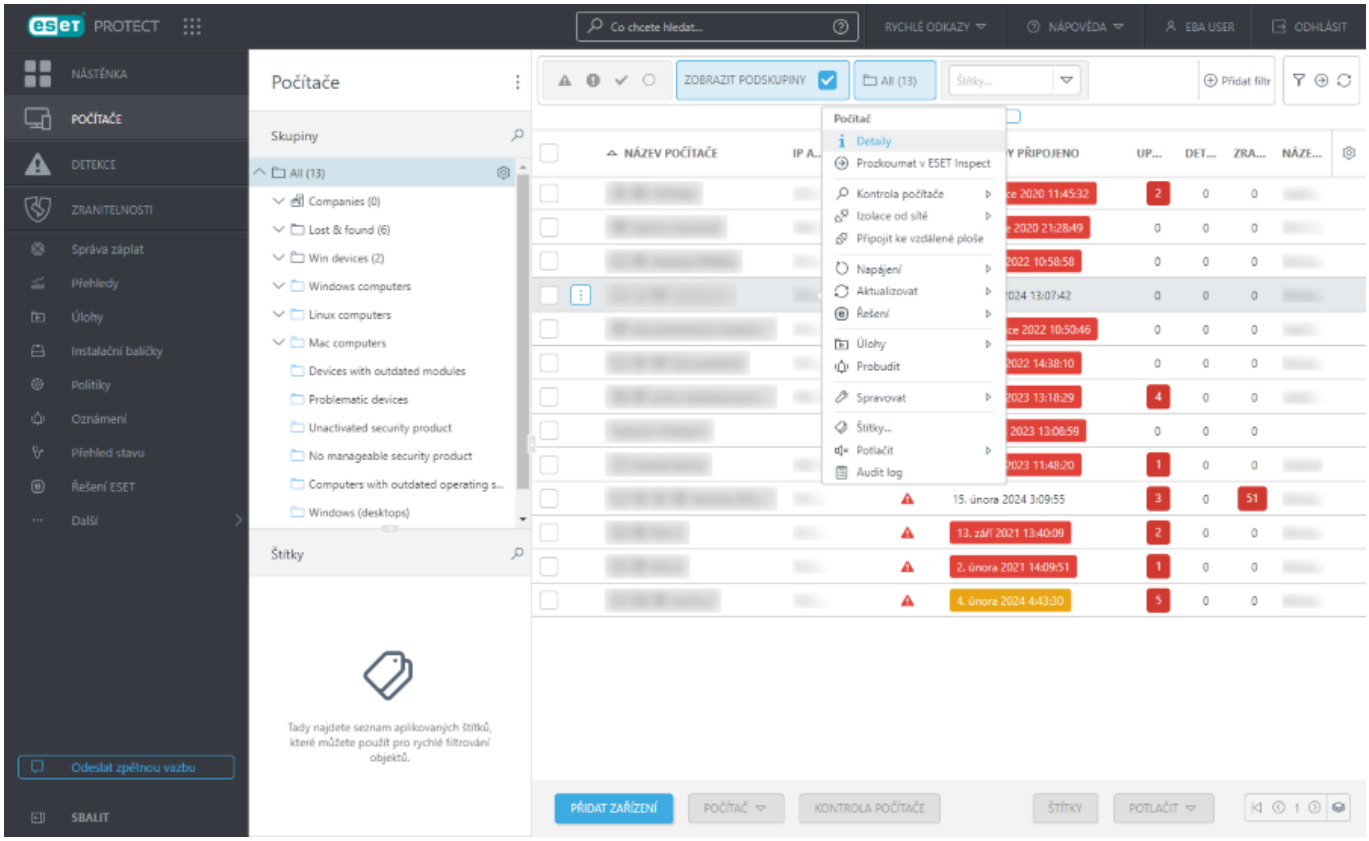
3.V zobrazeném dialogovém okně přejděte na záložku **Protokoly** > **SysInspector**, vyberte požadovaný záznam a z kontextového menu vyberte možnost **Otevřít SysInspector prohlížeč**.



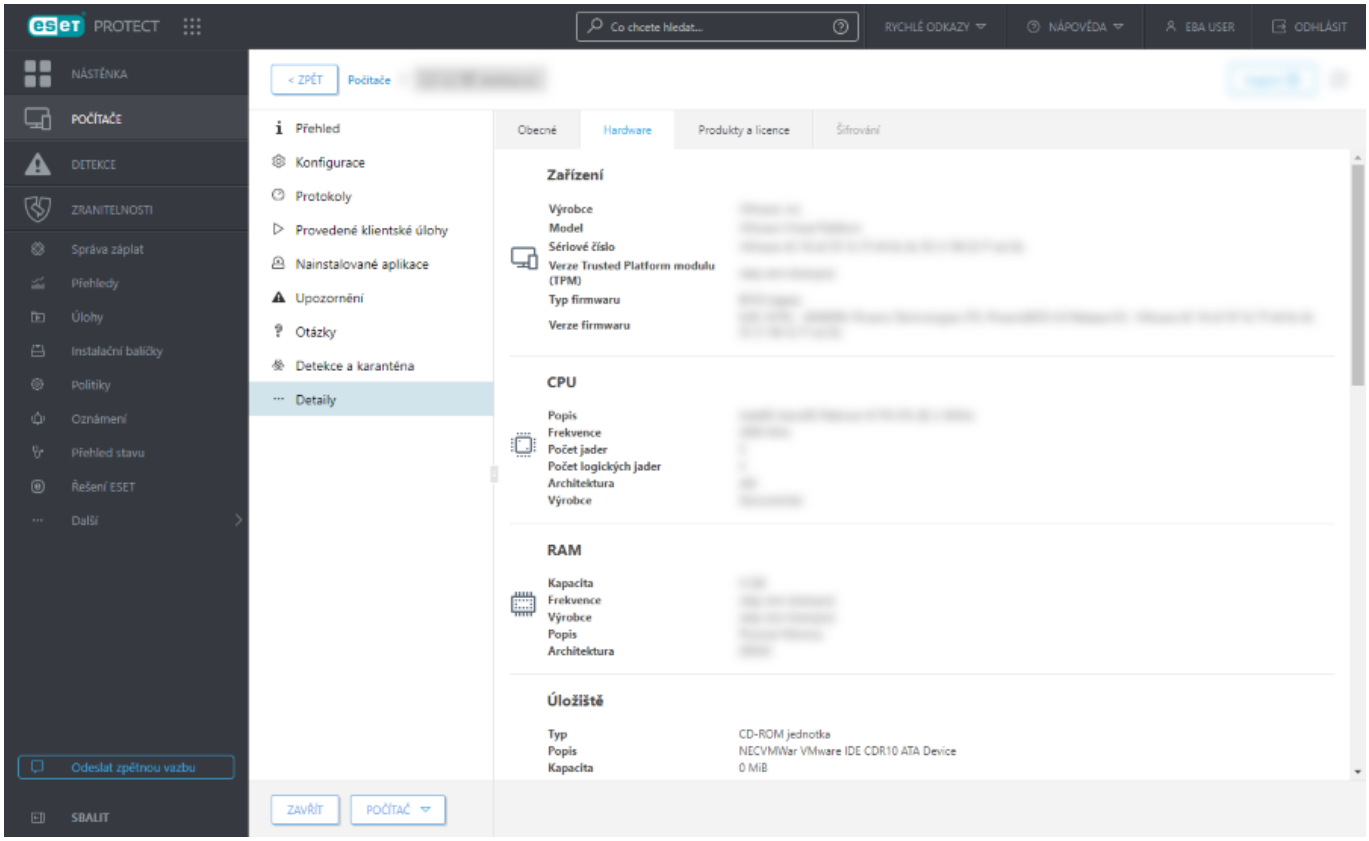
Hardwarový audit

ESET PROTECT dokáže získat informace o hardwaru (RAM, velikost úložiště, procesor…) ze zařízení připojených k serveru.

V hlavním menu klikněte na **Počítače**, vyberte zařízení a v kontextovém menu klikněte na možnost **Detaily**.



Přejděte do sekce **Detaily** a přepněte se na záložku **Hardware**.



Přehledy o hardwaru

Předdefinované přehledy týkající se inventáře hardware naleznete v sekci **Přehledy** > **Inventář hardware**. Kdykoli si můžete sestavit vlastní přehled s informacemi o hardwaru. Při vytváření nové šablony přehledu vyberte v sekci **Data** položky z kategorie **HW audit**. Po vybrání první položky do řádku tabulky nebo osy grafu se výběr dostupných dat zúží a zůstanou zobrazeny jen relevantní možnosti.

Dynamické skupiny na základě hardwaru

Hardwarové parametry můžete využít při tvorbě dynamických skupin. Při vytváření nové šablony dynamické skupiny vyberte jako pravidlo položku z kategorie **HW audit**. Následně můžete spravovaná zařízení můžete filtrovat na základě hardwarových parametrů.

Získaná data jsou rozdělena do následujících kategorií: Šasi, Zařízení, Monitor, Grafický adaptér, Vstupní zařízení, Úložiště, Síťové adaptéry, Tiskárny, Procesor, RAM a Zvukové adaptéry. Například si můžete vytvořit dynamickou skupinu, která bude filtrovat zařízení dle velikosti operační paměti.

Podpora hardwarového auditu

Informace o hardwaru jsou dostupné na všech podporovaných zařízeních se systémem Windows, Linux* a macOS.

* Aby ESET Management Agent dokázal korektně reportovat data o hardwaru z linuxových stanic/serverů, musí být na nich nainstalován balíček `lshw`.

Linuxové distribuce	Terminálový příkaz
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`

Linuxové distribuce	Terminálový příkaz
OpenSUSE	`sudo zypper install lshw`

Audit log jako přehled

V **Audit logu** jsou zaznamenány všechny akce a změny provedené uživateli v ESET PROTECT serveru.

Pro jeho vygenerování přejděte v hlavním menu na záložku **Přehledy** a v kategorii **Audit a správa licencí** vyberte **Audit log**.

Zobrazit si jej přímo a filtrovat v něm můžete ve Web Console v sekci **Další** > **Audit log**.

Pro zobrazení Audit logu musí mít uživatel Web Console v rámci sady oprávnění povolenou funkci **Audit log**.

Úlohy

Prostřednictvím **Úloh** můžete spravovat ESET PROTECT server, vzdáleně ovládat klientské stanice a bezpečnostní řešení ESET na nich nainstalované. Prostřednictvím úloh si můžete automatizovat běžné činnosti. Do začátku jsme pro vás připravili řadu nejpoužívanějších úloh, které stačí jen spustit. Kdykoli si úlohy můžete přizpůsobit svým potřebám nebo vytvořit nové. Prostřednictvím úloh provedete na stanici požadovanou akci. Abyste mohli klientské úlohy spouštět, musíte mít přístup nejen k nim, ale také cílovým objektům (počítačům nebo skupinám). Pro více informací přejděte do kapitoly seznam oprávnění.

Úlohy dělíme na: Klientské a Serverové.

- Klientské úlohy můžete přiřadit jednotlivým počítačů nebo celým skupinám počítačů (statickým nebo dynamickým). Klientské úlohy se provedou na základě definované podmínky spuštění. Každá klientská úloha může mít více podmínek spuštění. Požadavek na spuštění úlohy se na klienta přenese ve chvíli, kdy se ESET Management Agent připojí k ESET PROTECT serveru. Ze stejného důvodu může chvíli trvat, než se výsledek provedení úlohy replikuje zpět do ESET PROTECT Serveru.

- Serverové úlohy provádí ESET PROTECT Server přímo u sebe nebo jiných zařízeních. Serverové úlohy, kromě Nasazení ESET Agenta, není možné přiřadit jednotlivým klientům nebo skupinám. Každá serverová úloha má právě jednu podmínku spuštění. Pokud úlohu potřebujete spouštět při různých událostech, vytvořte si více stejných úloh s odlišnými podmínkami spuštění.

Vytvořit je můžete dvěma způsoby:

- Klikněte na tlačítko **Nová** a z menu vyberte položku **Klientská úloha** nebo **Serverová úloha**.

- V levé části okna si vyberte požadovaný typ úlohy, klikněte na tlačítko **Nová** a z menu vyberte položku Klientská úloha nebo Serverová úloha.

K dispozici máte následující typy úloh, které jsou pro přehlednost rozděleny do jednotlivých kategorií:

Všechny úlohy

Klientské úlohy

Bezpečnostní řešení ESET

Kontrola aktualizace produktu
Diagnostika
Ukončit izolaci počítače od sítě
Export konfigurace spravovaného produktu
Izolovat počítač od sítě
Aktualizace modulů
Obnovení modulů
Kontrola volitelných cílů
Aktivace produktu
Správa karantény
Spustit servisní skript SysInspector
Odeslat soubor do ESET LiveGuard
Kontrola serveru
Instalace aplikace
Vyžádat SysInspector protokol (pouze na Windows)
Nahrát soubor z karantény

ESET PROTECT

Diagnostika
Obnovit klonovaného ESET Agenta
Obnovit databázi ESET RD Sensor
Ukončit správu (odinstalovat ESET Management Agenta)
Aktualizovat Agenta

Operační systém

Odeslat zprávu
Odhlásit
Aktualizace operačního systému
Spustit příkaz
Vypnout počítač
Instalace aplikace
Odinstalace aplikace
Ukončit správu (odinstalovat ESET Management Agenta)

Mobilní zařízení

Anti-Theft akce
Odeslat zprávu
Export konfigurace spravovaného produktu
Aktualizace modulů
Kontrola volitelných cílů
Aktivace produktu
Instalace aplikace
Ukončit správu (odinstalovat ESET Management Agenta)

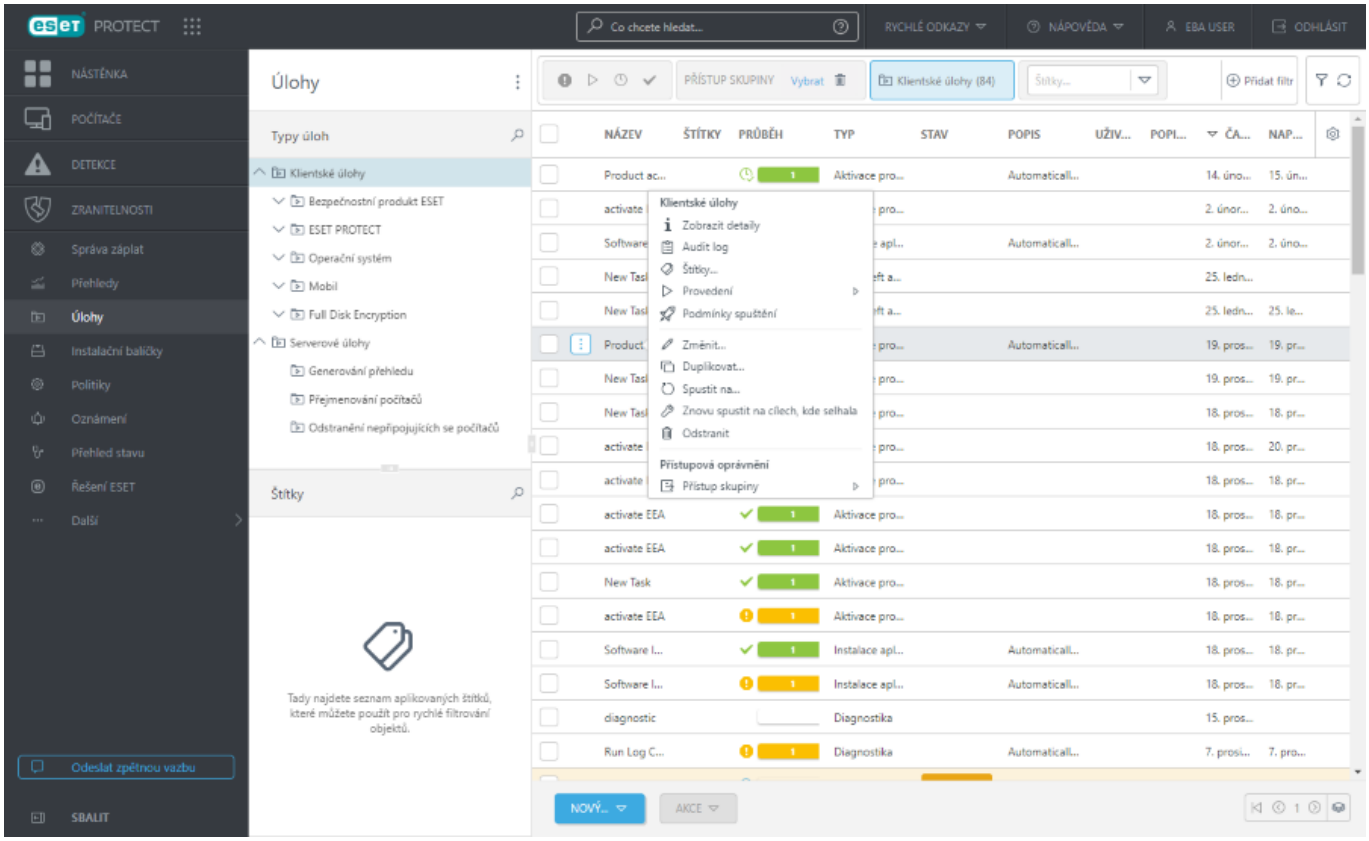
Serverové úlohy

Odstranění nepřipojujících se počítačů – prostřednictvím této úlohy smažete z Web Console zařízení, která se dlouho nepřipojila k ESET PROTECT.
Generování přehledu – tuto úlohu využijte pro pravidelné generování přehledů a jejich zasílání na e-mail nebo ukládání do souboru.
Přejmenování počítačů – prostřednictvím této úlohy můžete počítače hromadně přejmenovat do FQDN formátu.

Přehled stavu

U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Pokud chcete, aby se úloha spustila, musíte ji přiřadit podmínku spuštění.



V kontextovém menu úloh jsou dostupné následující možnosti:

Zobrazit detaily	Kliknutím si zobrazíte detaily úlohy: souhrn, provedení a podmínky spuštění (ty jsou dostupné pouze pro klientské úlohy).
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
Provedení	Dostupné pouze pro klientské úlohy: Po kliknutí si můžete snadno zobrazit konkrétní výsledky provedení a nad danými cíli provést požadovanou akci. Více informací naleznete v kapitole Detaily úlohy.
Podmínky spuštění	Dostupné pouze pro klientské úlohy: Kliknutím si zobrazíte seznam podmínek spuštění vybrané klientské úlohy.
Změnit...	Kliknutím upravíte parametry vybrané úlohy. To je užitečné ve chvíli, kdy chcete provést pouze drobnou úpravu. V opačném případě si vytvořte novou klientskou úlohu.
Duplikovat...	Po kliknutí vytvoříte kopii úlohy se stejnými parametry. Vyžadován je pouze nový název.
Spustit nyní	Dostupné pouze pro serverové úlohy: Kliknutím spustíte úlohu.
Spustit na...	Dostupné pouze pro klientské úlohy: Po kliknutí můžete vytvořit novou podmínku spuštění a definovat nový cíl (počítač nebo skupinu) pro spuštění úlohy.

Znovu spustit na cílech, kde selhala	Dostupné pouze pro klientské úlohy: Vytvoří novou podmínku spuštění a jako cíle vyberete ty, na kterých poslední spuštění úlohy nedoběhlo úspěšně. Není potřeba měnit žádné nastavení, pouze klikněte na tlačítko Dokončit.
Odstranit	Kliknutím odstraníte vybranou úlohu. • Pokud odstraníte úlohu, jejíž spuštění jste dosud nenaplánovali, úloha se odstraní a nikdy se nespustí. • Pokud odstraníte úlohu poté, co jste naplánovali její spuštění, úloha se provede, ale informace se ve Web Console nezobrazí.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Průběh úlohy

Tento barevný ukazatel reprezentuje stav provedení úlohy. Každá úloha má vlastní a zobrazuje se ve sloupci **Průběh**. Ukazatel mění svoji barvu v závislosti na stavu úlohy a zároveň je doplněn o počet stanic, na kterých je úloha v tomto stavu. Průběh úlohy může nabývat těchto stavů:

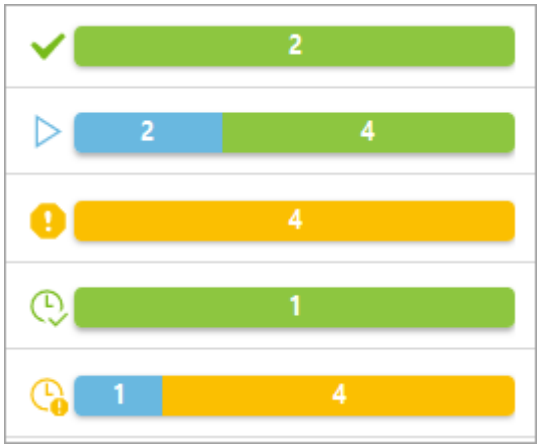
Běží (modrá)

Úspěšně dokončena (zelená)

Selhala (oranžová)

Nově vytvořená Úloha (bílá) – změna barvy indikátoru může chvíli trvat, ESET PROTECT server musí obdržet odpověď od ESET Management Agenta, aby zobrazil stav provedení. Ukazatel bude prázdný také v případě, pokud jste nedefinovali žádnou podmínku spuštění.

Kombinace výše uvedených:



Podrobné vysvětlení jednotlivých stavů a ikonek najdete v kapitole ikona stavu úlohy.

Ukazatel průběhu reprezentuje stav úlohy v době jejího posledního spuštění. Tuto informaci poskytuje ESET Management Agent. Ukazatel tedy reflektuje reálný stav klientské stanice – zobrazuje přesně to, co reportuje ESET Management.

Ikona

Ikona stavu úlohy se zobrazuje vedle ukazatele průběhu úlohy a poskytuje doplňující informace. Reprezentuje stav, zda není naplánováno spuštění úlohy společně s výsledkem provedení úlohy. Tato data poskytuje ESET PROTECT server. Ikona může mít tyto stavy:

Běží	Úloha je spuštěna alespoň na jednom cíli, není naplánováno spuštění na dalších cílech ani úloha na žádném cíli neselhala. Úloha zůstane v tomto stavu do chvíle, než doběhne na všech cílech.
Dokončeno	Úloha byla úspěšně dokončena na všech cílech a není naplánováno její spuštění na dalších cílech.
Chyba	Úloha je spuštěna na všech cílech, ale nejméně na jednom skončila s chybou. Není naplánováno její další spuštění.
Naplánováno	Spuštění úlohy je naplánováno, ale zatím nebyla spuštěna na žádném cíli.
Naplánováno/Běží	Spuštění úlohy je naplánováno, spustila se již na některých cílech a na žádném její provedení zatím neselhalo. Alespoň na jednom cíli již běž a na žádném zatím její provedení neselhalo.
Naplánováno/Dokončeno	Spuštění úlohy je naplánováno, na některých cílech již úspěšně doběhla a na žádném její provedení zatím neselhalo.
Naplánováno/Chyba	Spuštění klientské úlohy je naplánováno, na žádném cíli neběží a nejméně na jednom cíli její provedení selhalo. Tento stav se zobrazí i v případě, kdy již na některých cílech úloha doběhla úspěšně

Detaily úlohy

Po vybrání možnosti **Zobrazit detaily** nad konkrétní úlohou se zobrazí obrazovka, na které jsou informace dostupné na následujících záložkách:

Souhrn

Na této záložce naleznete souhrnné informace o nastavení úlohy.

Provedení

Na záložce **Provedení** se zobrazuje seznam počítačů s daným výsledkem provedení klientské úlohy. Záložka **Provedení** není k dispozici pro serverové úlohy.

Výsledky si v případě potřeby můžete filtrovat a omezit tak množství zobrazených dat.

Pro dodatečné filtrování výsledků provedení podle stavu klikněte na tlačítko **Přidat filtr**:

- **Naplánováno** - **ano** (spuštění klientské úlohy je naplánováno, ale zatím nebyla spuštěna na žádném cíli), **ne** (spuštění klientské úlohy bylo dokončeno).
- **Poslední stav** – **Žádný stav**, **Běží**, **Dokončeno**, **Neúspěšné**

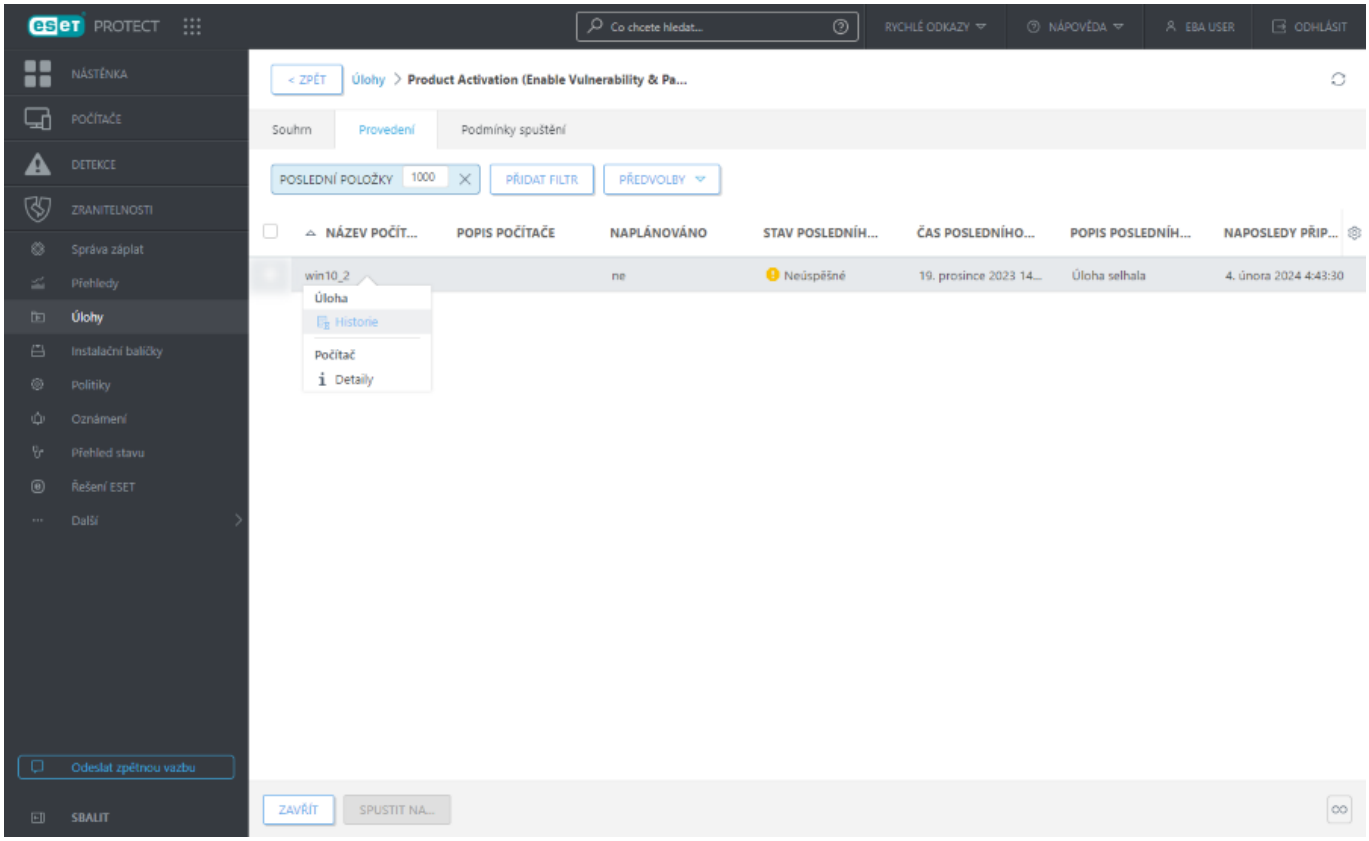
Filtr můžete kdykoli změnit nebo se jednoduše vrátit na předchozí obrazovku a zobrazit si počítače vyhovující jinému stavu.

Kliknutím na konkrétní záznam ve sloupci **Název počítače** nebo **Popis počítače** se zobrazí další možnosti:

- **Historie** – vybráním této možnosti si zobrazíte detailní informace o provedení klientské úlohy zahrnující **Výskyt**, **Produkt**, **Stav průběhu**, **Popis průběhu** a **Chybovou zprávu** (pokud je dostupná). Ve sloupci **Chybová zpráva** můžete zjistit konkrétní příčinu selhání klientské úlohy.

> - Pokud v **historii** provedení úlohy nevidíte žádný záznam, ujistěte se, že nemáte aktivní filtr pro časový **výskyt**, který by omezoval zobrazení položek na krátké časové období.
> - Při instalaci starších produktů ESET se jako chybová zpráva zobrazí informace: **Úloha byla doručena spravovanému produktu.**

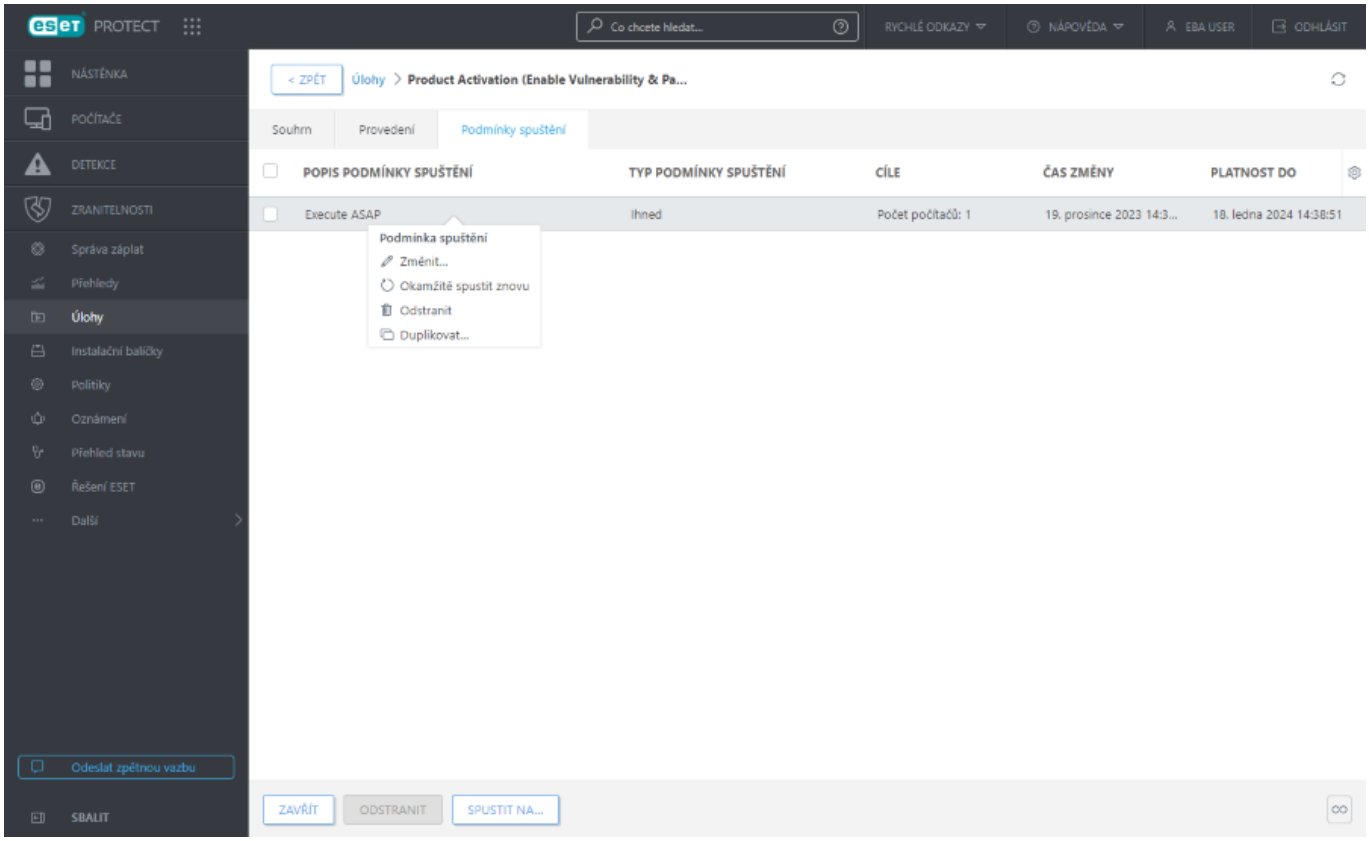
- **Detaily** – po kliknutí si zobrazíte Detaily vybraného zařízení.



Podmínky spuštění

Záložka **Podmínky spuštění** je dostupná pouze v případě klientských úloh a naleznete zde seznam všech podmínek spuštění pro danou úlohu. Pro jejich správu klikněte na podmínku spuštění a vyberte si jednu z možností:

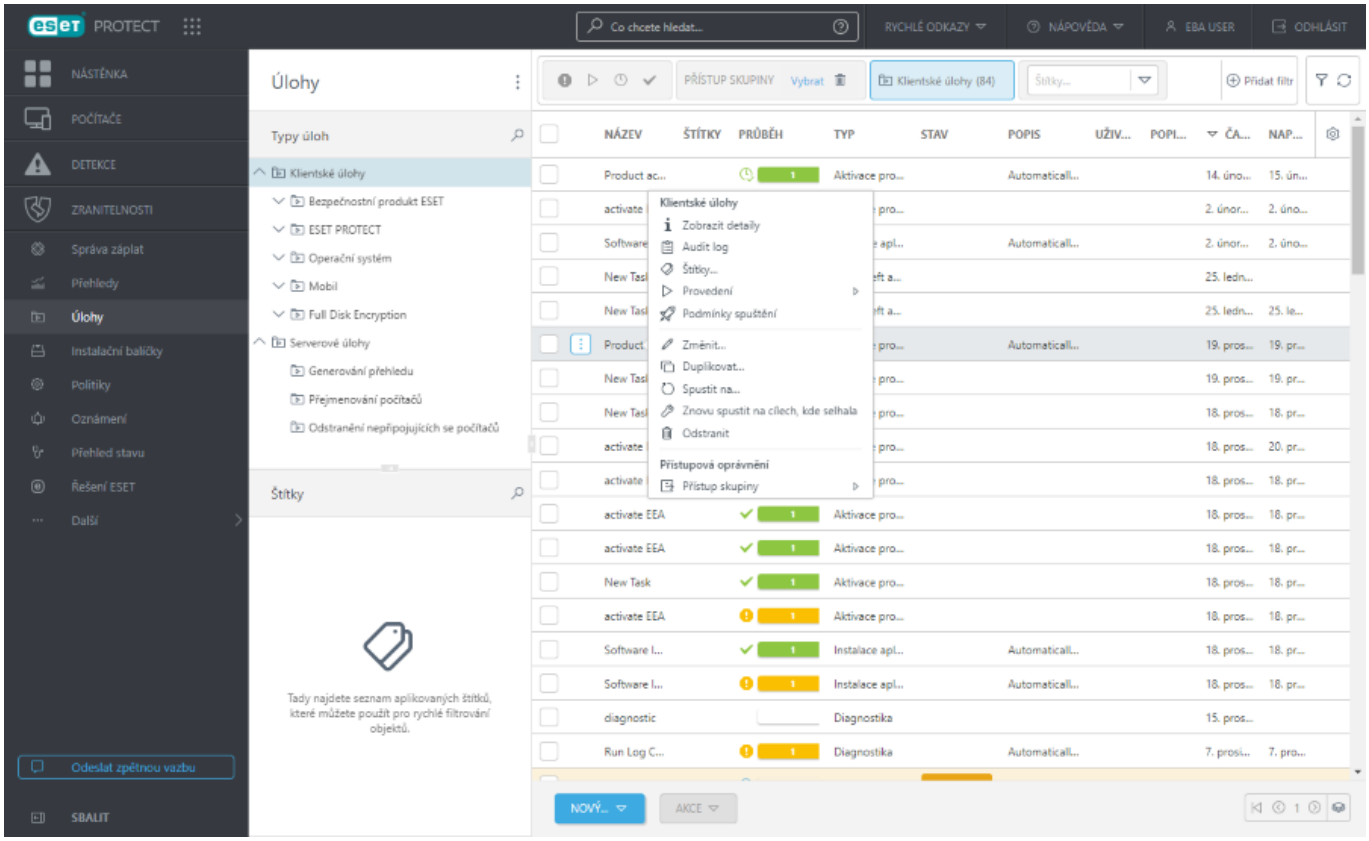
Změnit...	Kliknutím upravíte konkrétní podmínku spuštění.
Okamžitě spustit znovu	Po kliknutí znovu spustíte klientskou úlohu se stejnou podmínkou spuštění, tedy nad stejným cílem a se stejnými parametry.
Odstranit...	Kliknutím odstraníte vybranou podmínku spuštění. Pro odstranění více podmínek spuštění použijte zaškrtávací pole, a po provedení výběru klikněte na tlačítko **Odstranit**.
Duplikovat...	Po kliknutí vytvoříte kopii podmínky spuštění se stejnými parametry. Vyžadován je pouze nový název.



Klientské úlohy

Klientské úlohy můžete přiřadit jednotlivým počítačů nebo celým skupinám počítačů (statickým nebo dynamickým). Klientské úlohy se provedou na základě definované podmínky spuštění. Každá klientská úloha může mít více podmínek spuštění. Požadavek na spuštění úlohy se na klienta přenese ve chvíli, kdy se ESET Management Agent připojí k ESET PROTECT serveru. Ze stejného důvodu může chvíli trvat, než se výsledek provedení úlohy replikuje zpět do ESET PROTECT Serveru.

U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.



Prostudujte si informace o klientských úlohách (ukončení procesu) vytvořených v ESET Connect. Souhrn klientských úloh si můžete zobrazit, nemůžete jej však upravovat ani vytvářet.

Vytvoření nové klientské úlohy

1. Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

   • V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.

   • V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.

   • V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

2. V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

3. V sekci **Nastavení** definujte parametry úlohy.

4. V části **Souhrn** zkontrolujte, zda parametry úlohy odpovídají vašim potřebám, a úlohu vytvořte kliknutím na tlačítko **Dokončit**.

5. Pro vytvoření podmínky spuštění klikněte na tlačítko **Vytvořit podmínku spuštění**. Pokud chcete podmínku vytvořit později, klikněte na tlačítko **Zavřít**.

Podmínky spuštění klientské úlohy

Pro spuštění klientské úlohy na koncové stanici musíte vytvořit nejprve její podmínku. Pro vytvoření podmínky spuštění klikněte v sekci **Úlohy** na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**. Alternativně můžete přiřadit klientskou úlohy počítači nebo skupině.

Při vytváření podmínky spuštění nejprve vyberte **cíl** (počítač nebo skupinu), na kterém chcete úlohu spustit. Po definování cílů nastavte podmínku pro **spuštění** úlohy v konkrétním čase, nebo při výskytu události. Pokročilé možnosti pro plánování spuštění úlohy naleznete v sekci **rozšířená nastavení**.

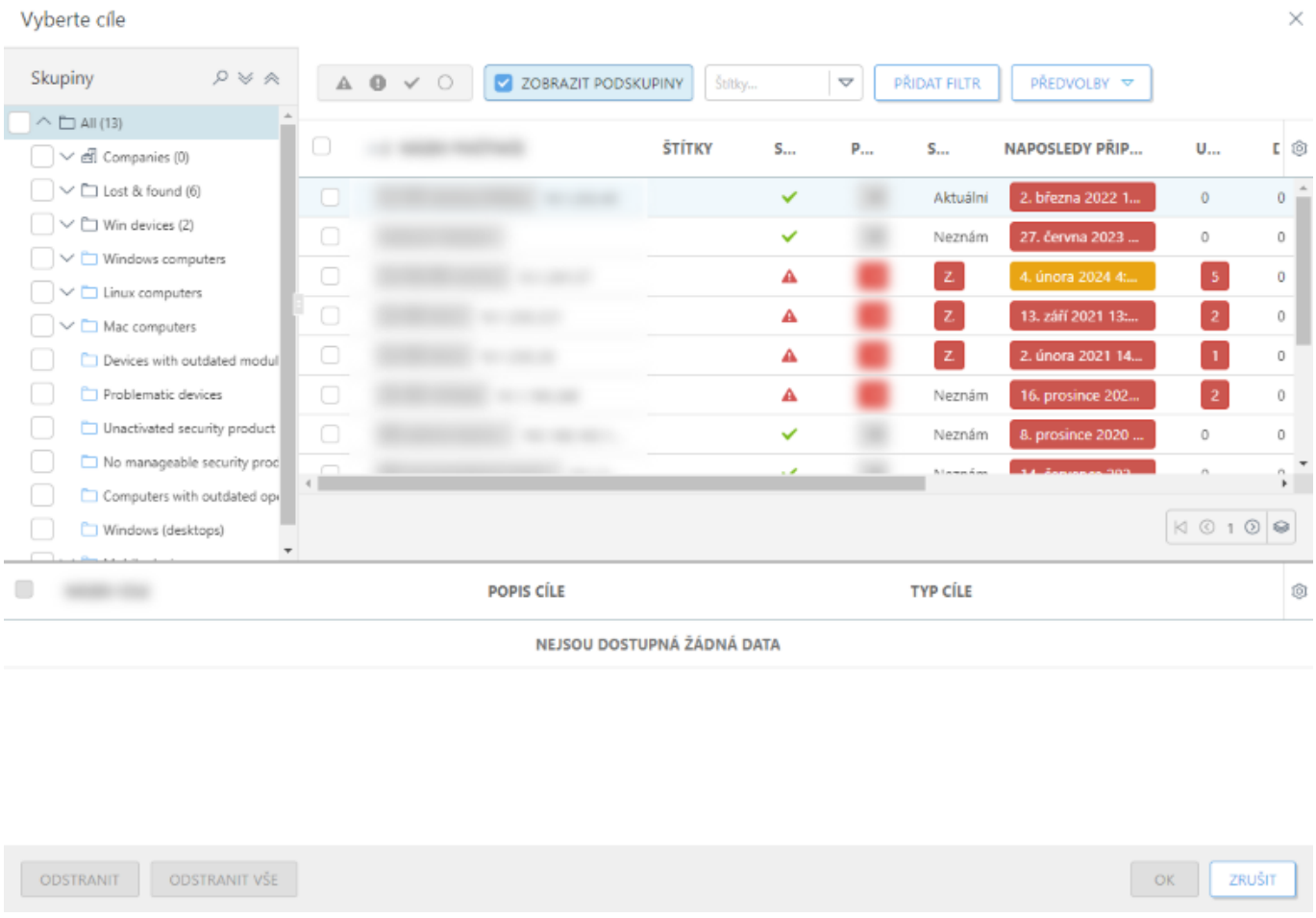
Obecné

Zadejte **název podmínky, volitelně popis**, a následně přejděte do sekce **Cíl**.

Cíl

V této části můžete jako **cíl** vybrat klienty (jednotlivé počítače nebo celé skupiny), na kterých chcete úlohu spustit. Kliknutím na **Přidat cíle** můžete vybrat statické nebo dynamické skupiny.

> Pro zajištění, že se objekt aplikuje na všechna zařízení ve skupině, místo výběru jednotlivých stanic vyberte jako cíl celou skupinu. Zabráníte tím zároveň zpomalení Web Console.
> Pokud vyberte velké množství počítačů, Web Console zobrazí varování.



Po vybrání klientů klikněte na tlačítko **OK** a přejděte do sekce **Podmínka spuštění**.

Podmínka spuštění

– definuje, kdy se má úloha provést.

- **Ihned** – spustí úlohu co nejdříve od chvíle, co klient kontaktuje ESET PROTECT a získá informace o konkrétní úloze. Pokud úloha nebude klientovi doručena do data stanoveného v sekci **Platnost do**, úloha bude odebrána z fronty – úloha nebude odstraněna, pouze se neprovede. Platnost podmínky může být nejvýše 6 měsíců.
- **Naplánované spuštění** – spustí úlohu ve stanovený čas.
- **Při výskytu události** – spustí úlohu na základě definovaných parametrů. Podmínka spuštění se aktivuje při výskytu konkrétní události v protokolu. Při definování události můžete vybrat **typ protokolu**, použít **logický operátor** a **kritéria filtrování**, které aktivují spuštění úlohy.
- **Při připojení do dynamické skupiny** – spustí úlohu při přesunutí klienta do definované dynamické skupiny. Tato možnost není dostupná při výběru jednotlivých klientů nebo statické skupiny.
- CRON výraz – interval pro spuštění podmínky spuštění můžete definovat také prostřednictvím CRON výrazu.

> Pro více informací o tvorbě podmínek přejděte do kapitoly typy podmínek spuštění.

Rozšířená nastavení

Prostřednictvím throttlingu můžete omezit počet provedení úlohy v případě, že použijete podmínku spuštění **Při výskytu události** nebo **Při připojení do dynamické skupiny** (viz výše), a zabránit tak nadměrnému spuštění úlohy. Pro více informací přejděte do kapitoly zabránění aktivace podmínky spuštění.

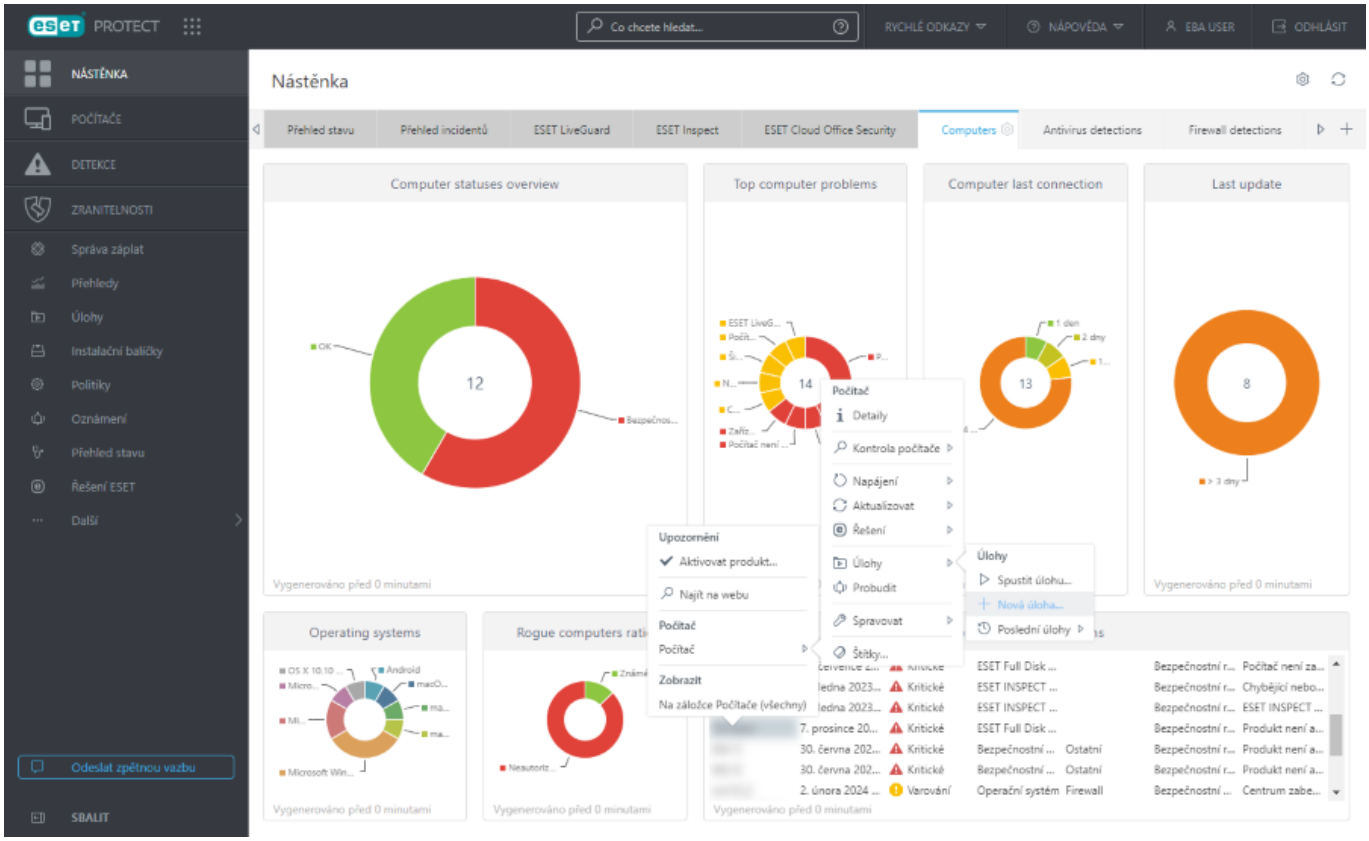
Po dokončení konfigurace této části klikněte na tlačítko **Dokončit**

Přiřazení klientské úlohy počítači nebo skupině

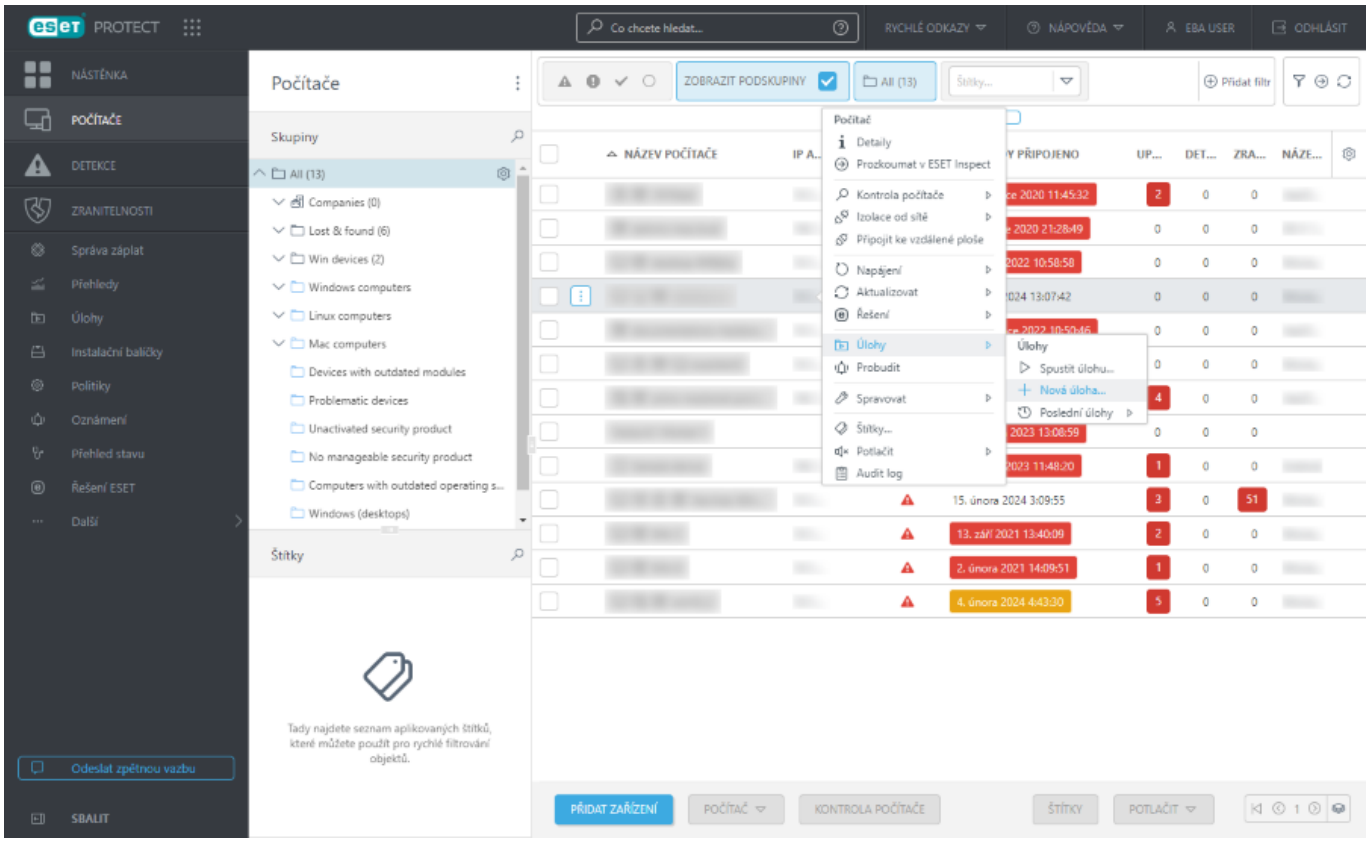
Pro přiřazení klientské úlohy skupině máme popsán v samostatné kapitole.

Novou úlohu můžete přiřadit počítačům dvěma způsoby:

1. V hlavním menu přejděte na záložku **Nástěnka** > **Počítače** > **Počítače s problémy**, klikněte na počítač a v kontextovém menu vyberte možnost **Počítač** > **Úlohy** > **Nová úloha…**.



2. V hlavním menu přejděte na záložku **Počítače**, vyberte cílový počítač a z kontextového menu vyberte možnost **Úlohy** > **Nová úloha…**.



Následně se zobrazí průvodce vytvořením klientské úlohy.

Anti-Theft akce

Technologie **Anti-Theft** chrání mobilní zařízení před neoprávněným přístupem.

Pokud mobilní zařízení (registrované a spravované prostřednictvím ESET PROTECT) uživatel ztratí nebo mu bude odcizeno, některé Anti-Theft se provedou automaticky, jiné můžete provést prostřednictvím této klientské úlohy.

Po výměně SIM kartu za jinou (nedůvěryhodnou), ESET Endpoint Security pro Android automaticky zařízení **uzamkne**, a na definované telefonní číslo(a) automaticky zašle SMS s upozorněním. Tato zpráva bude obsahovat:

- telefonní číslo aktuálně vložené SIM karty,
- její **IMSI** (International Mobile Subscriber Identity),
- a **IMEI** telefonu (International Mobile Equipment Identity).

Neoprávněný uživatel nebude vědět, že byla tato zpráva odeslána, protože se automaticky odstraní ze zařízení a vlákna odeslaných zpráv. Můžete si prostřednictvím klientské úlohy také vyžádat **GPS** souřadnice ztraceného mobilního zařízení nebo vzdáleně vymazat všechna data v něm uložená.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

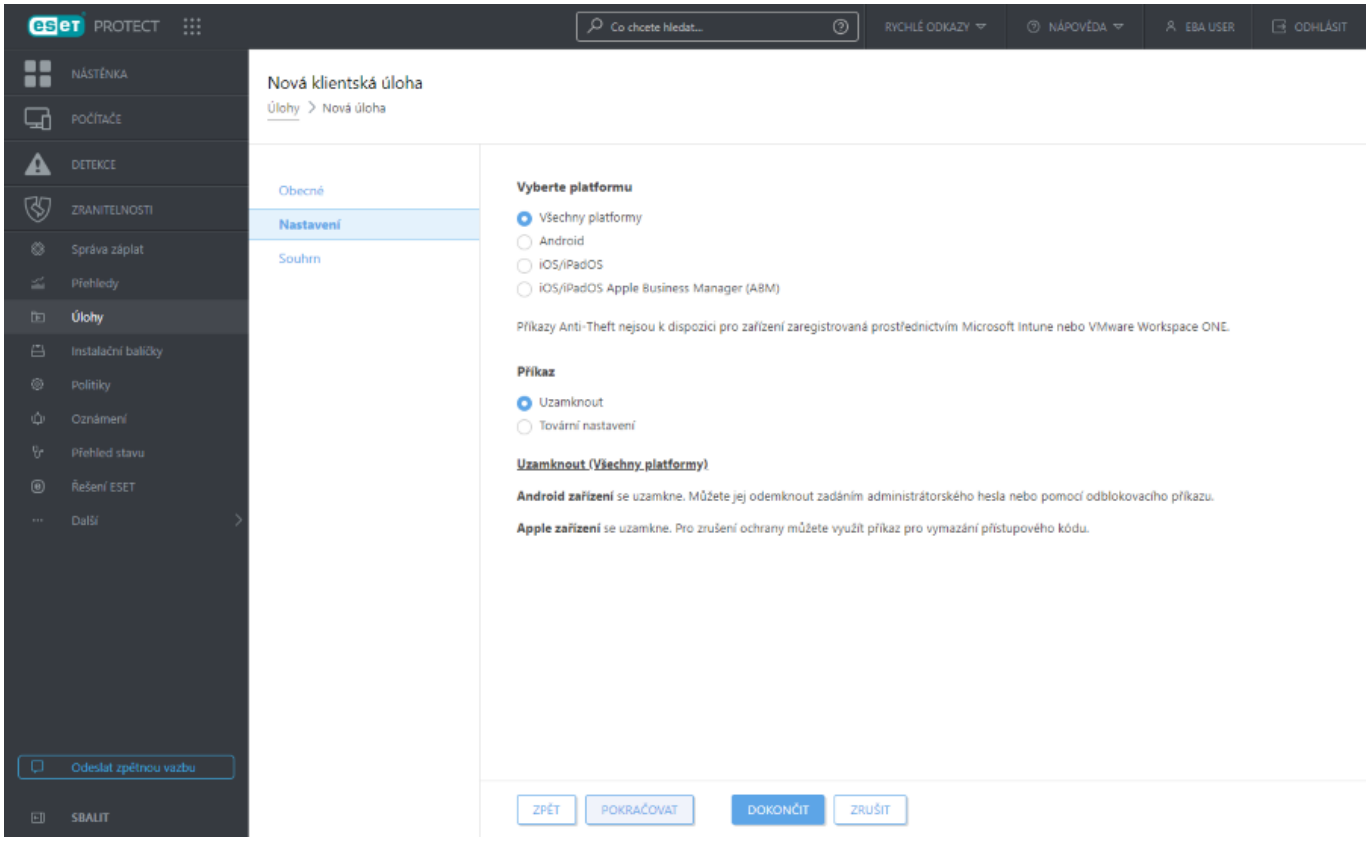
Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

Akce	Chování dle OS	Popis
Najít		Zařízení odešle na definované telefonní číslo SMS zprávu obsahující GPS souřadnice. Pokud bude získána přesnější pozice, po 10 minutách zašle zařízení další SMS. Získané informace se zobrazí v detailech zařízení. Úloha pro **zjištění polohy** bude funkční, pouze pokud je na zařízení povolena GPS.
		Nepodporováno.
Uzamknout		Zařízení se uzamkne. Odblokovat jej bude možné zadáním administrátorským heslem nebo **vzdáleným příkazem**.
		Zařízení se uzamkne. Kód pro přístup do zařízení bude možné smazat pomocí **vzdáleného příkazu**.
Odemknout		Zařízení se odemkne. Aktuálně vložená SIM karta bude přidána do seznamu důvěryhodných SIM karet (byla-li SIM karta vyměněna).
		Nepodporováno.
Siréna/zvuk režimu ztraceného zařízení		Na zařízení se po dobu 5 minut spustí siréna, i pokud je hlasitost ztlumena, nebo do odemčení zařízení.
		Nepodporováno.
Vymazat přístupový kód		Nepodporováno.
		Tímto odstraníte přístupový kód ze zařízení. Při zapnutí zařízení bude uživatel vyzván k nastavení nového přístupového kódu.
Obnovení do továrního nastavení		Všechna data na zařízení budou vymazána zničením hlaviček souborů a zařízení se obnoví do továrního nastavení. Tato akce může trvat několik minut.
		Zařízení bude obnoveno do továrního nastavení a veškerá nastavení i data budou odstraněna. Tato akce může trvat několik minut.

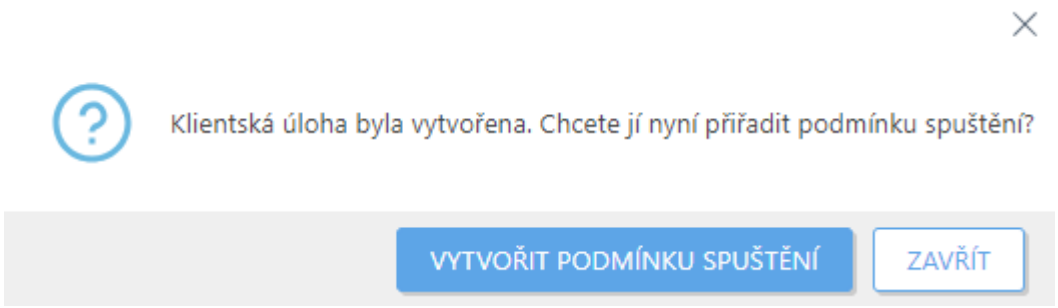
Akce	Chování dle OS	Popis
Najít a Zapnout režim ztraceného zařízení		Tato možnost je podporována pouze na iOS ABM zařízeních. Zařízení se přepne do "režimu ztraceného zařízení", uzamkne se a může být odemčeno pouze úlohou **Vypnout režim ztraceného zařízení** zaslanou z ESET PROTECT. Volitelně si můžete přizpůsobit údaje (telefonní číslo, obsah zpráv a patičku) zobrazené na obrazovce zamčeného zařízení. Stav ochrany zařízení se změní na **Ztracené**.
Vypnout režim ztraceného zařízení		Tato možnost je podporována pouze na iOS ABM zařízeních. Zařízení bude možné běžně používat a jeho stav se změní zpět.



Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Podmínky spuštění klientské úlohy na mobilních zařízeních

Pro klientské úlohy na mobilních zařízeních můžete použít pouze tyto podmínky spuštění:

- Ihned
- Při připojení do dynamické skupiny

Klientské úlohy s jinými než výše uvedenými podmínkami spuštění skončí chybovou zprávou **Nepodporovaný typ podmínky spuštění**.

Kontrola aktualizace produktu

Úloha **Kontrola aktualizace produktu** vynucuje vyhledání dostupných aktualizací pro bezpečnostní řešení ESET (automatické aktualizace) instalovaných na spravovaných zařízeních:

Podporované bezpečnostní produkty ESET:

- ESET Endpoint Antivirus/Security pro Windows verze 10.1 a novější
- ESET Server Security pro Microsoft Windows Server verze 11.0 a novější

- Pokud je k dispozici novější verze bezpečnostního řešení ESET, dojde k jejímu stažení.

- Aktualizace bezpečnostního řešení ESET vyžaduje restart zařízení, ale ne ihned (restart není vynucen). Správce ESET PROTECT může ovšem vynutit aktualizaci a restart počítače vzdáleně z webové konzole pomocí klientské úlohy Vypnout počítač u které zaškrtne políčko **Restartovat počítač(e)**.

- Dřívější verze bezpečnostního řešení ESET zůstává plně funkční až do restartu zařízení. Aktualizace proběhne až po jeho restartu.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.

- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.

- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

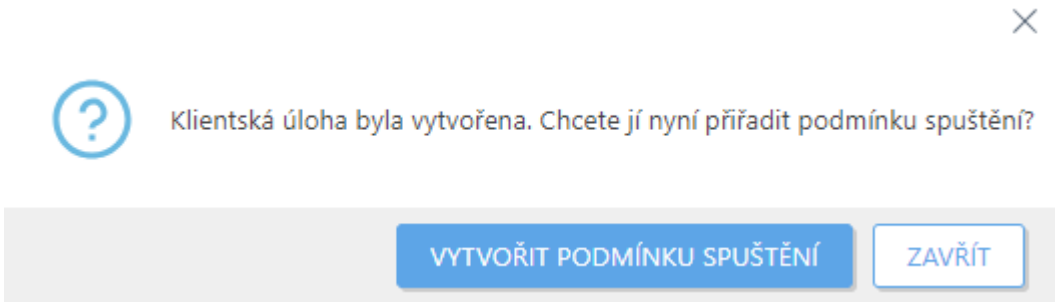
Nastavení

Pro tuto úlohu není dostupné žádné **nastavení**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Diagnostika

Pomocí této úlohy můžete na spravovaném zařízení a bezpečnostním produktu ESET inicializovat **diagnostickou akci**.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

Diagnostická akce

- **Spustit ESET Log Collector** – tento nástroj sesbírá specifická data (jako jsou protokoly a konfigurace produktu) z vybrané stanice, které mohou usnadnit řešení problému.

  - **Parametry ESET Log Collector** – parametry můžete definovat při spuštění nástroje na Windows, macOS i Linux. Pro sesbírání všech dostupných dat ponechte pole **Parametry ESET Log Collector** prázdné. Při definování parametrů vyberte vždy jako cíl pouze stanice odpovídající platformě, jejíž parametry jste použili.

> Maximální velikost protokolu, který je možné ze zařízení přenést, je 15 MB.Protokoly jsou dostupné ve Web Console v **Detailech počítače** na záložce **Protokoly**. Pokud bude výsledný protokol větší než 15 MB, úloha skončí chybou. V takovém případě:
> - Data ze stanice sesbírejte ručně.
> - Upravte úroveň protokolování na klientovi a zkuste to znovu:
>   - Pro získání pouze protokolů ESET Management Agenta z Windows stanic použijte parametr `/Targets:EraAgLogs`.
>   - Pro vynechání protokolů z nainstalovaného bezpečnostního produktu ESET na linuxu/macOS použijte parametr `--no-productlogs`.

- **Nastavit diagnostický režim** - Diagnostický režim zahrnuje protokol: **Protokol antispamové ochrany, protokol firewallu**, **protokol modulu HIPS, protokol správy zařízení**, **protokol filtrování obsahu webu**. Hlavní účelem diagnostického režimu je sběr dat potřebných pro řešení problémů.

  - **Zapnout** – pomocí této možnosti aktivujete diagnostického protokolování všech nainstalovaných ESET aplikací.

  - **Vypnout** – pomocí této možnosti deaktivujete diagnostické protokolování. V opačném případě se automaticky vypne po restartování počítače.

Pro úspěšné sesbírání diagnostických protokolů je nutné splnění těchto požadavků:

- Diagnostický režim je podporován pouze na Windows a macOS.
- Na klientské stanici musí být nainstalovaný a aktivovaný bezpečnostní produkt ESET.

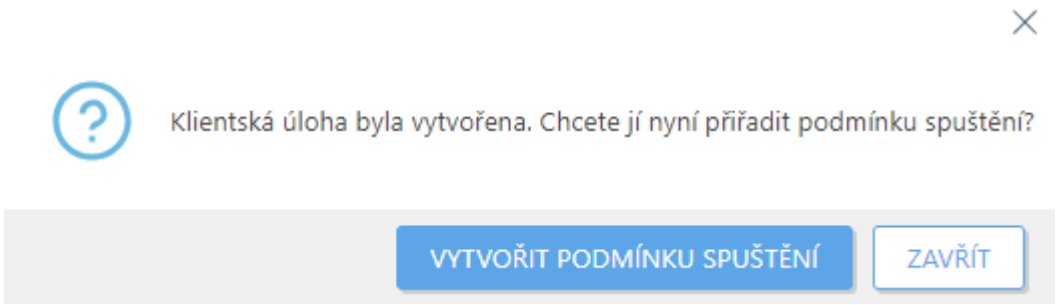
> ESET Management Agent zasílá ze stanice protokoly sesbírané nainstalovaným produktem ESET. Typy protokolů a jejich citlivost závisí na produktu a jeho konfiguraci. Úroveň sběru protokolů můžete pro každý produkt definovat pomocí politik.

Diagnostické protokoly starší 24 hodin budou automaticky odstraněny. Tím je zajištěno, že nedojde k nadměrnému zatížení databáze ESET PROTECT.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Vytvořené protokoly následně najdete v detailech počítače: na záložce **Protokoly** > **Diagnostické protokoly**.

Odeslat zprávu

Pomocí této funkce můžete **odeslat zprávu** na jakékoli zařízení (počítač, tablet, mobilní zařízení atp.). Zpráva se následně zobrazí uživateli na obrazovce. Způsob zobrazení závisí na operačním systému.

- Windows – zpráva se zobrazí na Ploše jako oznámení.

> Na Windows využíváme komponentu msg.exe, která je dostupná pouze v edicích Windows Professional a Enterprise. Pokud v síti používáte domácí edice operačního systému, žádná zpráva se nezobrazí.

- macOS a Linux - zpráva se zobrazí pouze v terminálu.

> Pro zobrazení zprávy musí mít uživatel terminál otevřený. Nedojde k jeho spuštění.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

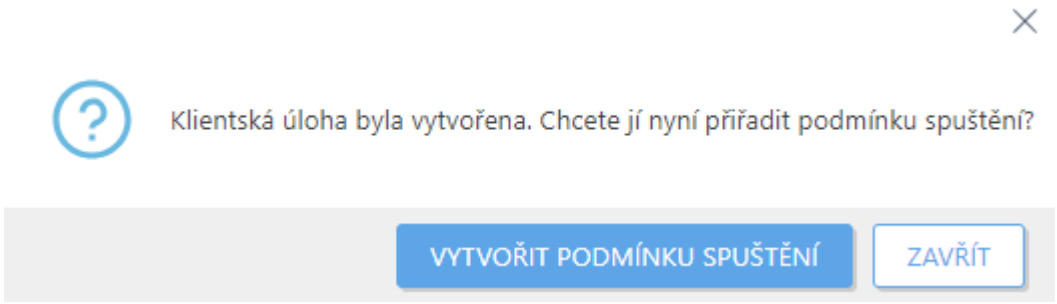
Nastavení

Zadejte **předmět** a **obsah zprávy**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Ukončit izolaci počítače od sítě

Prostřednictvím této úlohy **ukončíte** izolaci počítače a obnovíte jeho síťovou komunikaci. Tuto úlohu použijte pouze v případě, kdy jste vyřešili bezpečnostní incident.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

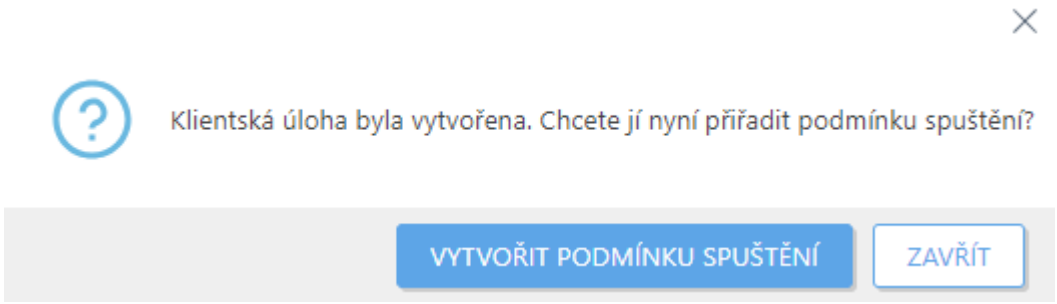
V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Pro tuto úlohu není dostupné žádné **nastavení**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Export konfigurace spravovaného produktu

Tuto úlohu můžete použít pro **získání konfigurace** bezpečnostního produktu ESET, který je nainstalovaný na klientské stanici, nebo jednotlivých komponent ESET PROTECT.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

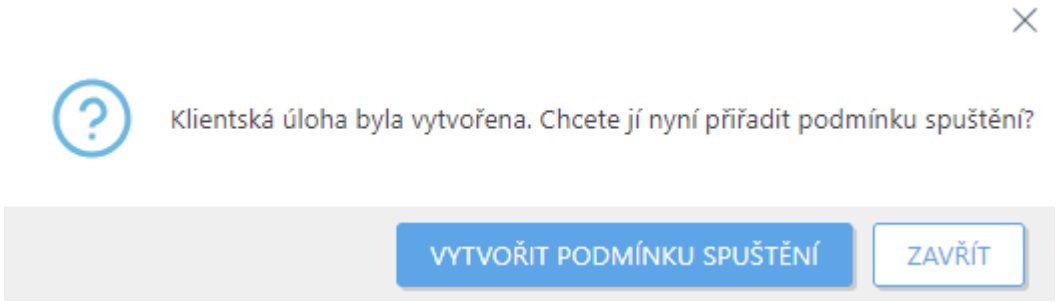
Export konfigurace spravovaného produktu.

- **Produkt** – vyberte bezpečnostní řešení ESET nebo komponentu ESET PROTECT, ze které chcete získat konfiguraci.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Po dokončení úlohy naleznete získaná data v detailech počítače na záložce **Konfigurace**.

Izolace počítače od sítě

Prostřednictvím této úlohy **izolujete od sítě** vybrané počítače od sítě, což znamená, že bude blokována veškerá komunikace kromě spojení potřebných pro správné fungování produktů ESET. Povoleno bude:

- získání IP adresy
- komunikace *ekrn.exe*, ESET Management Agenta a ESET Inspect Connector
- přihlášení do domény

Úloha Izolace od sítě je kompatibilní pouze s bezpečnostními řešeními ESET (Endpoint Antivirus/Security a řešeními pro ochranu serverů).
Izolováním počítače od sítě dojde ovlivnění normálního fungování počítače, proto byste měli tuto možnost používat pouze za mimořádných okolností. Izolaci můžete ukončit prostřednictvím odpovídající klientské úlohy.

Podporované operační systémy

Izolace od sítě je k dispozici pro zařízení se systémem Windows a macOS.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

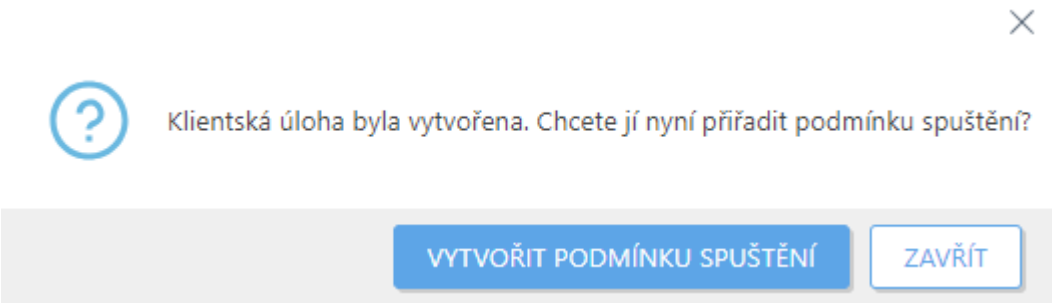
V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Pro tuto úlohu není dostupné žádné **nastavení**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Odhlásit

Prostřednictvím této úlohy **odhlásíte** všechny uživatele z cílového počítače. Tuto možnost naleznete též v kontextovém menu daného zařízení v sekci **Napájení** > **Odhlásit**.

Pro úspěšné provedení musí být na stanici nainstalován ESET Management Agent ve verzi 10.0 a novější. Na zařízeních se starší verzí agenta provedení klientské úlohy pro odhlášení **selže**.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

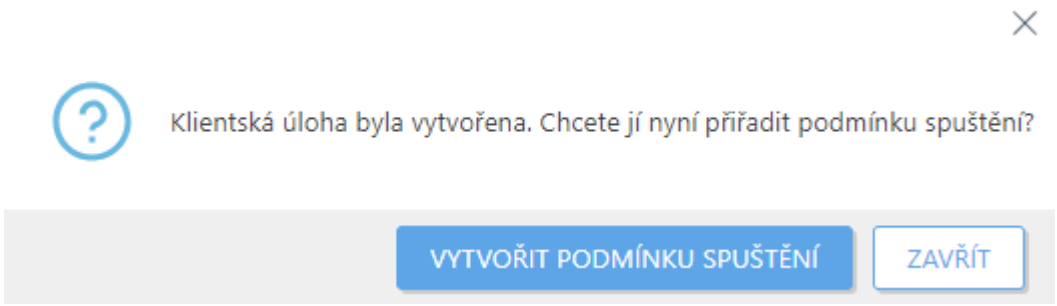
V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Pro tuto úlohu není dostupné žádné **nastavení**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Aktualizace modulů

Pomocí této úlohy **aktualizujete moduly** bezpečnostního produktu ESET na cílové stanici. Toto je obecná úloha platná pro všechny bezpečnostní produkty bez ohledu na platformu. Seznam všech aktualizovaných modulů naleznete v koncovém produktu v sekci **O programu**.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

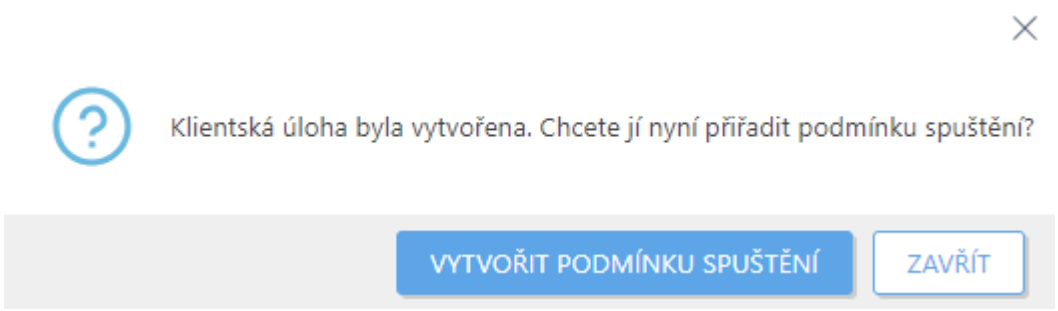
Nastavení

- **Vyprázdnit aktualizační cache** – tato možnost odstraní všechny dočasné aktualizační soubory z klienta, což může vyřešit většinu problémů s nefunkční aktualizací detekčních a programových modulů.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

> **Nastavení vlastního aktualizačního serveru**
> Pokud vám aktualizace modulů bezpečnostního produktu ESET selhávají z důvodu geoblokace, pomocí politiky definujte vlastní aktualizační server:
> 1. V konfigurační šabloně pro požadovaný bezpečnostním produkt ESET přejděte do sekce **Aktualizace** > **Profily** > **Aktualizace**.
> 2. V části **Aktualizace modulů** deaktivujte možnost **Automatický výběr serveru** do pole **Vlastní server** zadejte adresu aktualizačního serveru. Příklad: pro aktualizaci produktů ESET Endpoint Antivirus/Security 9 na platformě Windows z US serverů zadejte *http://us-update.eset.com/eset_upd/ep9/* (pro verzi 8 použijte URL *http://us-update.eset.com/eset_upd/ep8/*).
> 3. Do pole **Uživatelské jméno** a **Heslo** zadejte klasické licenční údaje (ve formátu EAV-XXXXXXXX) Tyto údaje naleznete na licenčním portále v sekci klasický licenční soubor.

Obnovení modulů

Pokud máte podezření, že aktualizace modulů bezpečnostního produktu ESET způsobuje nestabilní chování počítače (případně jste nechtěli testovací aktualizace aplikovat na všechny stanice), pomocí této úlohy můžete **vrátit předchozí verzi modulů** a na stanovený časový interval zakázat jejich další aktualizace. Po provedení této úlohy se na klientské stanici vrátí starší verze modulů.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

V této části stanovte interval, po jakou dobu chcete pozastavit aktualizace.

Akce

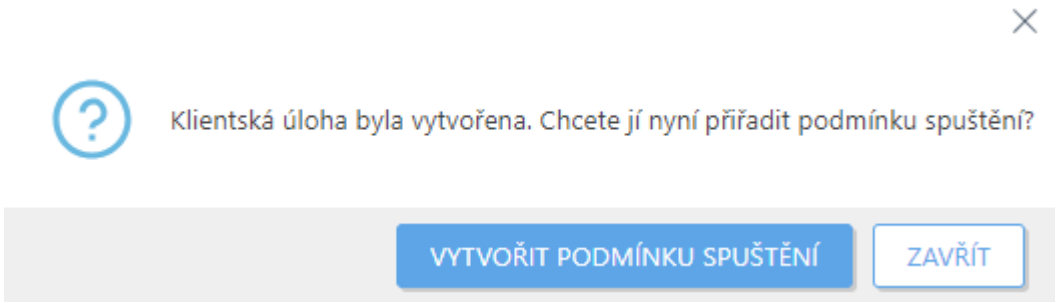
- **Povolit aktualizace** – opětovně povolí aktualizace.
- **Obnovit moduly a pozastavit aktualizaci** – vyberte interval (24/36/48 hodin nebo do odvolání), na jakou dobu chcete aktualizace **pozastavit**.

Při použití možnosti **do odvolání** buďte opatrní, představuje bezpečnostní riziko.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Volitelná kontrola

Úloha **Volitelná kontrola** umožňuje ručně spustit kontrolu na klientském zařízení (mimo pravidelné naplánované kontroly).

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

Vypnout po dokončení kontroly – vybraním této možnosti zajistíte vypnutí počítače po dokončení kontroly.

V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje.

Profil kontroly

Z rozbalovacího menu si vyberte profil, který chcete použít:

- **Hloubková kontrola** – předdefinovaný nejdůkladnější profil kontroly, který zkontroluje všechny soubory, což si na druhou stranu vyžádá velké množství systémových prostředků a kontrola potrvá déle.

- **Smart kontrola** – slouží pro rychlé spuštění kontroly počítače a automaticky léčí nebo odstraňuje infikované soubory a nevyžaduje interakci uživatele. Výhodou Smart kontroly je snadná obsluha, kdy není nutné cokoli dalšího konfigurovat. Smart kontrola zkontroluje všechny soubory na lokálních jednotkách a automaticky je vyléčí nebo odstraní. Úroveň léčení je nastavena na standardní úroveň.

- **Kontrola z kontextového menu** – použije se předdefinovaný profil na klientovi a vybrat můžete cíle kontroly.

- **Vlastní profil** – volitelná kontrola umožňuje zadat parametry kontroly, například cíle a metody. Výhodou tohoto profilu je, že si kontrolu můžete přizpůsobit vašim potřebám. Po dokončení nastavení si výsledný profil kontroly můžete na klientovi uložit pro použití v budoucnu. Před provedením kontroly s tímto profilem již musí být profil vytvořen. Následně při vytváření úlohy vyberte z rozbalovacího menu možnost **Vlastní profil** a níže zadejte název vytvořeného profilu, který chcete při kontrole použít.

Léčení

Standardně je vybrána možnost **Kontrolovat a léčit**. To znamená, že nalezené infiltrace budou automaticky vyléčeny. Případě přesunuty do karantény.

Cíle kontroly

Standardně je aktivní možnost **Kontrolovat všechny cíle**. V případě potřeby můžete tuto možnost deaktivovat a kontrolovat pouze vámi definované cíle. Po deaktivování zadejte do pole **Přidat cíl** absolutní cestu ke složce nebo souboru. Po zadání cíle klikněte na tlačítko **Přidat**. Vámi zadaný cíl se následně zobrazí v poli **Cíle kontroly**. Jako **cíl kontroly** můžete použít předdefinované proměnné uvedené v tabulce níže.

Cíl kontroly	Kontrolovaná umístění
`${DriveRemovable}`	Všechny výměnné jednotky a zařízení.
`${DriveRemovableBoot}`	Bootovací sektory všech výměnných jednotek.
`${DriveFixed}`	Pevné disky (HDD, SSD).
`${DriveFixedBoot}`	Bootovací sektory pevných disků.
`${DriveRemote}`	Namapované síťové jednotky.
`${DriveAll}`	Všechny dostupné jednotky.
`${DriveAllBoot}`	Bootovací sektory všech jednotek a UEFI. Pro více informací o UEFI skeneru přejděte do slovníku pojmů.
`${DriveSystem}`	Systémové jednotky.
`${Share}`	Sdílené jednotky (platné pouze pro serverové produkty).
`${Boot}`	Hlavní bootovací sektor.
`${Memory}`	Operační paměť.
`${Registry}`	Systémový registr (pouze pro ESET Endpoint 8 a novější).
`${Wmi}`	WMI databáze (pouze pro ESET Endpoint 8 a novější).

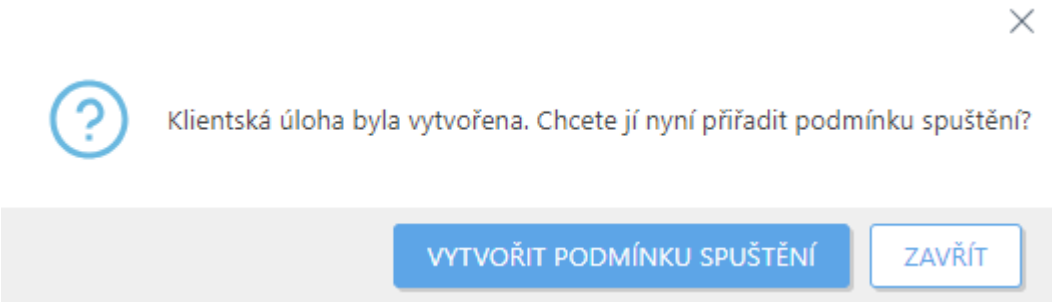
Níže si ukážeme, jak můžete definovat cíle **volitelné kontroly počítače**:
■Soubor: *C:\Users\Data.dat*
■Složka: *C:\MyFolder*
■Unixová cesta: */usr/data*
■Windows UNC cesta: *\\server1\scan_folder*
■Předdefinovaná proměnná: `${Memory}`

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.

- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Aktualizace operačního systému

Pomocí této úlohy můžete na cílovém počítači provést aktualizaci operačního systému. Tuto úlohu lze spustit na Windows, Linuxu i macOS.

- **macOS** – úloha k instalaci aktualizací používá příkaz (nainstalují se všechny aktualizace):

```
/usr/sbin/softwareupdate --install --all
```

- **Linux** – úloha nainstaluje všechny aktualizace (dojde k aktualizování všech balíčků). Ke kontrole dostupnosti využívá řadu balíčkovacích nástrojů, čímž je zajištěna podpora většiny distribucí. Používají se následující příkazy:

Debian/Ubuntu:

```
apt-get update --assume-no && apt-get dist-upgrade --assume-yes
```

CentOS/Red Hat:

```
yum update -y
```

SLES/SLED:

```
zypper --non-interactive update -t patch
```

- **Windows** – úloha nainstaluje aktualizace operačního systému. Využívá Windows API. Nenainstalují se aktualizace funkcí, které zajišťují aktualizaci systému Windows na novější verzi.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

- **Automaticky přijmout EULA** (pouze na Windows) – vyberte tuto možnost, pokud chcete automaticky přijmout licenční ujednání (EULA). Uživateli se nezobrazí žádný text. Pokud tuto možnost neaktivujete, úloha přeskočí aktualizace vyžadující odsouhlasení EULA.
- **Nainstalovat volitelné aktualizace** (pouze na Windows) – pokud vyberete tuto možnost, nainstalují se také volitelné aktualizace operačního systému.
- **Povolit restart** (Windows a macOS) – pomocí této možnosti vynutíte restart operačního systému po dokončení instalace aktualizací, které restart vyžadují.

V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje. Pokud spravovaný počítač nepodporuje možnosti pro úpravu chování restartování:

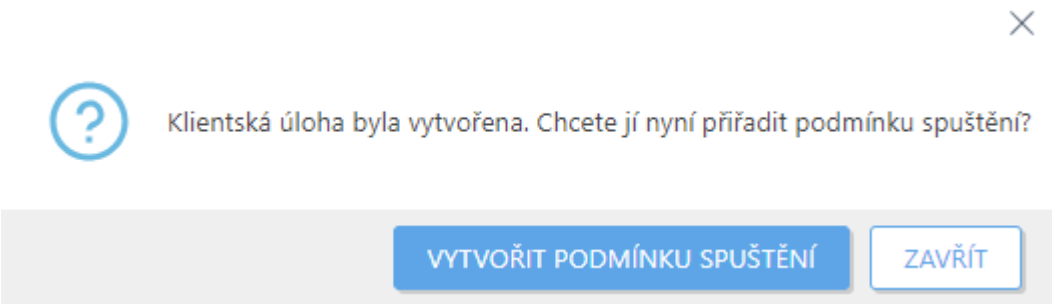
- Windows upozorní uživatele před vynuceným restartem 4 hodiny předem a opakovaně 10 minut před restartováním.
- macOS se automaticky restartuje po dokončení aktualizace.

- Aktualizace vyžadující restart se nainstalují též v případě, kdy jste nevybrali možnost **Povolit restart**.
- **Nastavení** definovaná v úloze se neaplikují v případě spuštění úlohy na nepodporovaném operačním systému.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Správa karantény

Pomocí této úlohy můžete spravovat **objekty uložené v karanténě** ESET PROTECT – infikované nebo podezřelé objekty, které nalezly bezpečnostní produkty ESET na klientských stanicích v průběhu kontroly.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

Možnosti správy karantény

Akce – vyberte akci, kterou chcete provést s objekty umístěnými v karanténě.

- **Obnovit objekt** –obnoví objekt do svého původního umístění, ale nadále bude kontrolován a může být kdykoli znovu přesunut do karantény.
- **Obnovit objekt a příště vyloučit** – obnoví objekt do svého původního umístění a vytvoří se na něj výjimka.
- **Vymazat objekt** – trvale odstraní objekt.

Typ filtru – umožní filtrovat objekty v karanténě na základě níže uvedených kritérií.

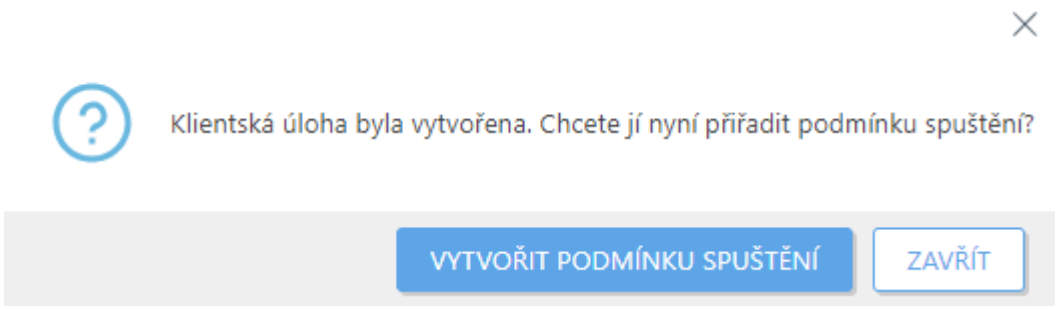
Nastavení filtru:

- **Kontrolních součet objektů** – zadejte kontrolní součty objektů umístěných v karanténě. Přidat je možné pouze existující objekty, například soubory z karantény.
- **Výskyt** > **Výskyt od**, **Výskyt do** – vyberte časové období, ve kterém byl objekt umístěn do karantény.
- **Velikost** > **Minimální/maximální velikost (v bajtech)** – definujte minimální a maximální velikost objektu v karanténě.
- **Název detekce** – vyberte detekci z karantény.
- **Název objektu** – vyberte objekt z karantény.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Aktivace produktu

Pomocí této úlohy vzdáleně **aktivujete produkt** ESET nainstalovaný na koncovém zařízení (počítači nebo mobilním zařízení).

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

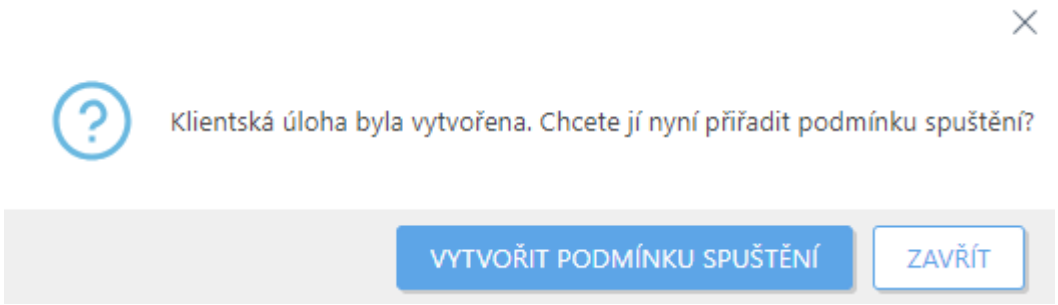
Nastavení

Možnosti aktivace produktu – Po kliknutí si ze seznamu vyberte licenci, která se použije pro aktivaci produktu instalovaného na cílové zařízení. Licence se použije k aktivaci produktu ESET, který je nainstalovaný na cílovém zařízení. V seznamu dostupných licencí nejsou zobrazené vypršelé (neplatné) a nadužívané licence (ve stavu **Chyby** nebo **Neaktuální**).

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Obnovit klonovaného ESET Agenta

Pokud ve své síti klonujete a znovu nasazujete systémy s již nainstalovaným ESET Management Agentem dle scénáře popsaného v Databázi znalostí, pak více agentů má stejné SID, což způsobí problémy. Pomocí této úlohy **resetujete agenty** na cílových zařízeních a zajistíte unikátní ID pro každou instalaci.

ESET Management Agent na Windows detekuje klonované stanice automaticky a není v takovém případě potřeba tuto úlohu používat. Tuto úlohu pro rozdělení klonů potřebujete pouze pro klonovaná zařízení s OS linux, macOS a Windows zařízení s vypnutou detekcí hardware.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Tuto úlohu spouštějte s rozmyslem. Jakmile dojde k odebrání stávajícího ESET Management Agenta, všechny běžící úlohy budou přerušeny. Jejich stav (**Běží**, **Dokončeno**, **Selhala**) se nemusí v závislosti na aktuálním stavu replikace zobrazit správně.

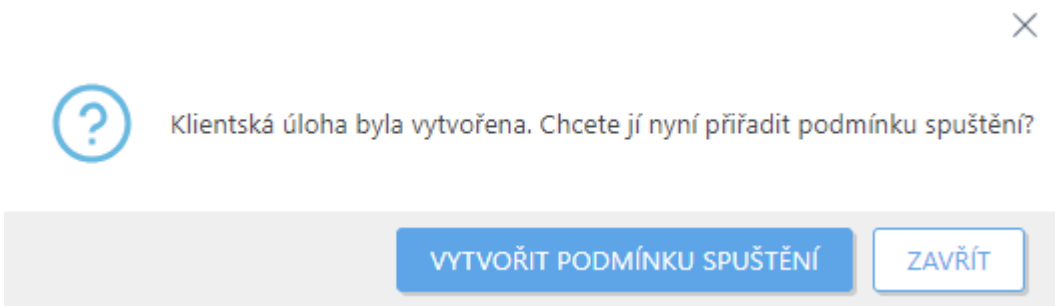
Pro tuto úlohu není dostupné žádné **nastavení**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská

úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Obnovit databázi ESET RD Sensor

Pomocí této úlohy vymažete cache nástroje **ESET Rogue Detection Sensor**. Po dokončení úlohy se do cache uloží nové výsledky vyhledávání. Nedojde však tím k odstranění detekovaných zařízení. To je užitečné v případě, kdy nalezená zařízení jsou v cache, ale jejich seznam nebyl předán serveru.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

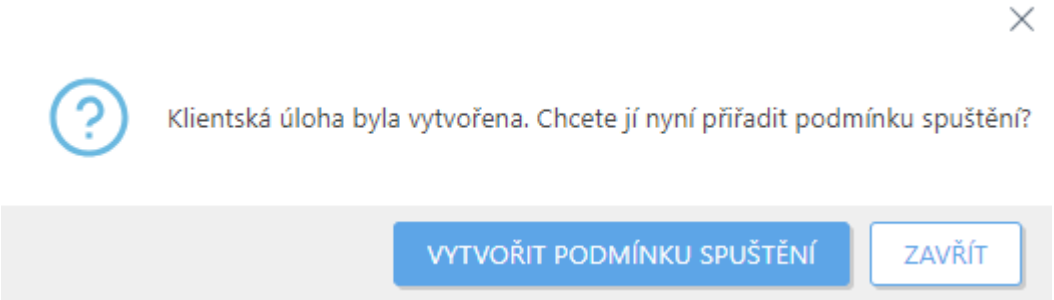
Pro tuto úlohu není dostupné žádné **nastavení**.

Při vytváření podmínky spuštění vyberte počítač, na kterém je RD Sensor nainstalován.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Spustit příkaz

Pomocí této úlohy **spustíte** na cílové stanici konkrétní příkaz. Do pole zadejte stejný obsah, který byste zadávali do příkazového řádku.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Mějte na paměti, že zadaný příkaz se spustí tiše na pozadí. Uživatel tedy neuvidí žádný výstup a může selhat provedení příkazů vyžadujících grafické rozhraní.

Prostřednictvím této úlohy můžete spouštět `ecmd` příkazy. Pro více informací přejděte do Databáze znalostí.

Operační systém	Uživatel, pod kterým se příkaz spustí	Výchozí pracovní složka	Dostupná síťová umístění	Aplikace, ve které se příkaz spustí
Windows	*Local System*	*C:\Windows\Temp*	pouze umístění v rámci domény a dostupná pro uživatele Local System	Příkazový řádek (`cmd.exe`)
Linux nebo macOS	*root*	*/tmp*	umístění připojená a dostupná pod uživatelem root	Terminál

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku

klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

- **Příkaz ke spuštění** – zadejte příkaz, který chcete provést.
- **Pracovní složka** – definujte složku, v níž chcete příkaz spustit.

Zadat můžete příkaz na více řádků. Maximální délka příkazu:
- Web Console dokáže zpracovat 32 768 znaků. Pokud kopírujete dlouhý příkaz, může dojít k jeho zkrácení.
- Linux a macOS dokáže zpracovat celý příkaz. Windows má však omezení na 8.191 znaků.

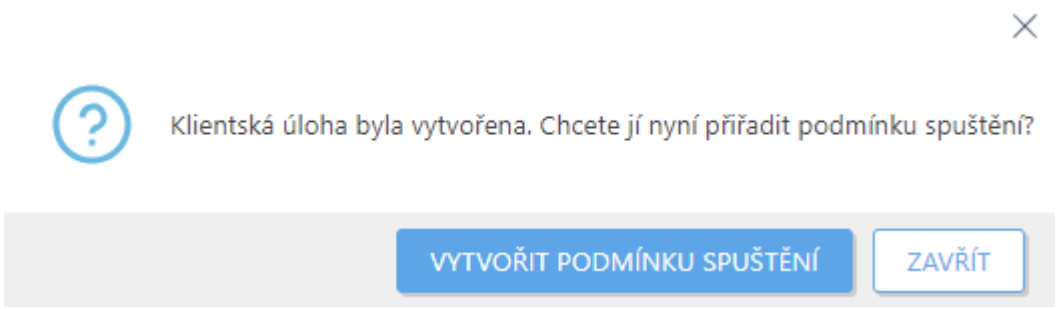
- Pro spuštění skriptu, který se nachází na klientské stanici ve složce *C:\Users\user\script.bat* postupujte podle následujících kroků:
1.Vytvořte novou klientskou úlohu **Spustit příkaz**.
2.V sekci **Nastavení**:
Zadejte `call script.bat` jako **příkaz pro spuštění**.
A jako **pracovní složku**: *C:\Users\user*
3.Klikněte na tlačítko **Dokončit** a vytvořte podmínku spuštění pro odeslání úlohy na klientskou stanici.
- Pro spuštění více řádkového příkazu pro vzdálené restartování Windows služby použijte níže uvedené příkazy (kde `service_name` nahraďte skutečným názvem služby, například `wuauserv` pro službu Windows Update):

```
net stop service_name
net start service_name
```

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Analyzování úlohy na spuštění příkazu

1. V hlavním menu přejděte do sekce **Úlohy**, klikněte na požadovanou úlohu a v kontextovém menu vyberte možnost **Detaily** > **Provedení**. Dále klikněte na v tabulce na řádek ve sloupci **Historie**.

2. Ve sloupci **Chybová zpráva** je uvedeno prvních 255 znaků z celého výstupu úlohy pro spuštění příkazu. Můžete si tedy vytvářet přehledy a zpracovávat tato data z více počítačů. Kompletní výstup si můžete získat stažením Log Collector protokolu z konkrétního počítače. To v provedete v **Detailech** na záložce **Protokoly** > Log Collector.

Spustit servisní skript SysInspector

Pomocí této úlohy můžete ze systému **odstranit** nechtěné objekty. Pro vytvoření servisního skriptu SysInspector je nejprve nutné z dané stanice získat ESET SysInspector protokol. Po získání protokolu můžete označit nežádoucí objekty, které chcete odstranit a upravený protokol spustit na cílové stanici. Poté dojde k odstranění označených objektů.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

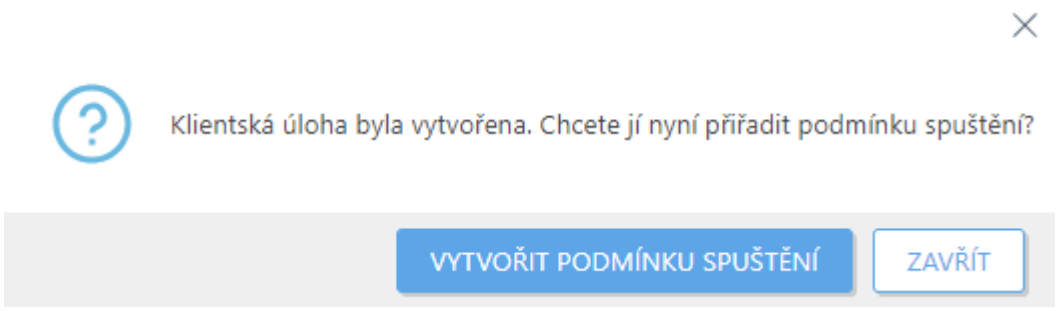
- **Servisní skript SysInspector** – pomocí tlačítka **Procházet** vyberte požadovaný servisní skript. Před spuštěním úlohy již musíte mít servisní skript vytvořen.
- **Akce** – servisní skript následně nahrajte kliknutím na tlačítko **Nahrát**. Pokud si skript potřebujete prohlédnout, například u již existující úlohy, můžete v ESET PROTECT Web Console kliknout na tlačítko **Stáhnout**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

• Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.

• Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Výsledek provedení úlohy naleznete v odpovídajícím přehledu (například provedené klientské úlohy).

Odeslat soubor do ESET LiveGuard

Pro spuštění této úlohy přejděte do sekce **Detekce**.

Možnost **Odeslat soubor do ESET LiveGuard** je dostupná pouze pro **Blokované soubory**. Soubor k analýze lze odeslat do ESET LiveGuard Advanced přímo z webové konzole ESET PROTECT. Výsledek analýzy bude následně dostupný v sekci Odeslané soubory. Pro odeslání spustitelného souboru k analýze do ESET LiveGuard Advanced můžete rovněž využít nainstalovaný bezpečnostní produkt ESET, který je aktivován ESET LiveGuard Advanced licencí.

Kontrola volitelných cílů

Prostřednictvím této úlohy zkontrolujete **vybrané cíle**, které na serveru vidí bezpečnostní produkt ESET. V závislosti na bezpečnostním produktu můžete spustit níže uvedené kontroly:

Produkt	Kontrola počítače	Popis
ESET Server Security (dříve známý jako ESET File Security pro Windows Server)	**Hyper-V kontrola**	Tato kontrola zkontroluje disky virtuálních strojů běžících na Microsoft Hyper-V Serveru bez nutnosti instalace ESET Management Agenta do těchto virtualizovaných strojů.
ESET Security pro Microsoft SharePoint Server	**Kontrola SharePoint databáze, Hyper-V kontrola**	Pomocí této možnosti získáte do ESET PROTECT **seznam cílů**, které reportuje ESET Security pro Microsoft SharePoint.
ESET Mail Security pro Microsoft Exchange Server	**Volitelná kontrola databáze poštovních schránek, Hyper-V kontrola**	Pomocí této možnosti získáte do ESET PROTECT seznam cílů. Při vytváření úlohy v ESET PROTECT se zobrazí seznam cílů z nichž si vyberte ty, které chcete v rámci **volitelné kontroly databáze poštovních schránek** zkontrolovat.

Produkt	Kontrola počítače	Popis
ESET Mail Security pro IBM Domino	**Volitelná kontrola databáze, Hyper-V kontrola**	Pomocí této možnosti získáte do ESET PROTECT **seznam cílů**, které reportuje ESET Mail Security pro IBM Domino.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

- Klikněte na**Vybrat** v části **Kontrolovaný server** a vyberte počítač s nainstalovaným produktem ESET Server Security. Následně budete mít k dispozici seznam cílů, které je možné zkontrolovat.
- Vyberte **podmínku spuštění**. Standardně je použita podmínka "provést co nejdříve".

Cíle kontroly

V této části máte dostupné cíle kontroly, které reportuje bezpečnostní produkt do ESET PROTECT z daného serveru. Chcete-li tento seznam použít, musí být zapnuto **Generovat seznam cílů** v politice pro serverový produkt v části **Nástroje** > **Cíle kontroly konzole ESET Management**:

- **Generovat seznam cílů** – pomocí této možnosti aktivujete generování seznamu cílů pro ESET PROTECT.
- **Interval aktualizace (v minutách)** – definujte interval, ve kterém se budou zjišťovat dostupné cíle. Mějte na paměti, že prvotní získání cílů potrvá polovinu tohoto intervalu.

Následně vyberte cíle, které chcete zkontrolovat. Více informací naleznete v kapitole ESET PROTECT: cíle kontroly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené úloze. Zkontrolujte, zda nastavení odpovídá vašim představám, pokračujte kliknutím na **Dokončit**.

U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Vypnout počítač

Prostřednictvím této úlohy můžete vzdáleně **restartovat** nebo **vypnout** počítač.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

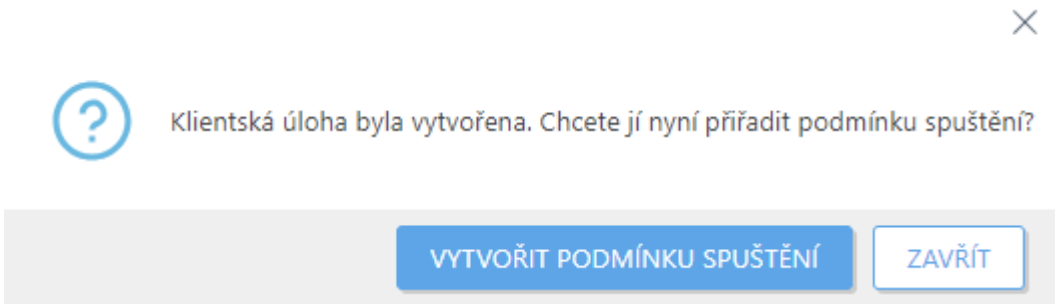
- **Restartovat počítač** – tuto možnost vyberte pouze v případě, pokud chcete cílový počítač restartovat. V opačném případě, pro vypnutí počítače, ponechte toto pole prázdné.

V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Instalace aplikace

Pomocí klientské úlohy na **instalaci aplikace** můžete na klientskou stanici:

- Nainstalovat bezpečnostní produkt ESET. Stejnou akci je možné provést prostřednictvím kontextového v sekci **Počítače**. Klikněte na počítač a vyberte **Řešení** > **Zapnout bezpečnostní produkt** pro zapnutí bezpečnostního produktu ESET v počítači.

- Aktualizace bezpečnostních produktů ESET. Spuštěním novějšího instalačního balíčku dojde k přeinstalování koncového produktu na novou verzi. Okamžitou aktualizaci produktu ESET můžete inicializovat přímo z **Nástěnky** prostřednictvím akce jedním kliknutím. Pro úspěšnou aktualizaci produktu přejděte do této kapitoly.

- Klikněte sem, pokud potřebujete Instalovat aplikaci třetí strany.

Obě komponenty (ESET PROTECT server i ESET Management Agent) vyžadují přístup k internetu, aby se dokázaly připojit k repozitáři a provést z něj instalaci. Pokud nemáte přístup k internetu, vzdálená instalace selže, a je nutné aplikace instalovat lokálně. Případně si vytvořte offline repozitář. Pro zabránění selhání klientské úlohy provede ESET Management Agent před spuštění úlohy pro instalaci/aktualizaci produktu ESET kontrolu, zda:
- má stanice přístup k repozitáři,
- je dostatek místa na disku pro instalaci produktu (neověřuje se na Linuxu).

Pokud zašlete klientskou úlohu pro instalaci aplikace na počítač, který je v doméně, a máte instalační balíček uložen na síťové složce, musí mít počítač (nikoli uživatel) *oprávnění pro čtení* z dané složky. Provést to můžete prostřednictvím těchto kroků:
1.Přidejte účet počítače do Active Directory (například *NewComputer$*).
2.Klikněte pravým tlačítkem myši na složku, ve které se nachází instalační balíček, a vyberte možnost **Vlastnosti**. V zobrazeném dialogovém okně přejděte na záložku **Sdílení** a klikněte na tlačítko **Sdílet**. Následně objektu *NewComputer$* přidělte **oprávnění pro čtení**. Mějte na paměti, že na konci názvu počítače je nutné ponechat znak "$".
Instalace ze sdílených umístění je možné pouze v případě, že je stanice členem domény.
Nepoužívejte úlohu pro instalaci aplikací k aktualizaci ESET Management Agentů. K tomuto účelu slouží úloha pro aktualizaci agenta.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.

- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a

vyberte možnost + **Klientská úloha**.

• V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

Instalační balíček – k dispozici jsou dvě možnosti:

• **Instalovat balíček z repozitáře**

o**Vyberte operační systém** – kliknutím vyberte operační systém na cílovém zařízení.

o**Vyberte balíček z repozitáře** – klikněte na **Vybrat balíček** a instalační balíček si vyberte z repozitáře (například ESET Endpoint Security). Z rozbalovacího menu si vyberte **Jazyk**. Standardně je vybrána nejnovější verze produktu. V případě potřeby si můžete vybrat starší verzi. Pro aktualizování produktu vyberte z repozitáře jeho nejnovější verzi. Volitelně klikněte na **Přizpůsobit další nastavení** a vyberte si ručně požadovanou verzi produktu ESET. Kliknutím na **Zobrazit seznam změn** přehledný seznam změn vybrané verze produktu. Dále klikněte na tlačítko **OK**.

o**Nainstalovat nejnovější verzi** – po zaškrtnutí této možnosti se vždy nainstaluje nejnovější verze vybraného produktu ESET, pokud je pro něj již přijata odpovídající EULA.

• **Instalovat balíček z URL** – zadejte konkrétní URL k instalačnímu balíčku (nepoužívejte URL, které vyžadují autentifikaci):

o*http://server_address/ees_nt64_ENU.msi* – pokud instalujete z veřejného serveru nebo máte v síti vlastní HTTP server.

o*file://\\pc22\install\ees_nt64_ENU.msi* – pokud instalujete ze síťového úložiště.

o*file://C:\installs\ees_nt64_ENU.msi* – pokud je instalační balíček na klientské stanici, na které úlohu chcete spustit.

Licence ESET –Po kliknutí si ze seznamu vyberte licenci, která se použije pro aktivaci produktu instalovaného na cílové zařízení. Touto licencí se aktivuje bezpečnostní produkt v průběhu instalace. V seznamu dostupných licencí nejsou zobrazené vypršelé (neplatné) a nadužívané licence (ve stavu **Chyby** nebo **Neaktuální**).

• Licenci vyberte pouze v případě, kdy produkt zatím není aktivován nebo jej chcete přeaktivovat jinou licencí.

• Při aktualizaci není nutné vybírat licenci.

Aktivovat ESET LiveGuard – tato možnost je dostupná v případě, kdy vyberete ESET LiveGuard Advanced licenci a kompatibilní bezpečnostní produkt ESET. Vybráním této možnosti zajistíte aktivování ESET LiveGuard Advanced po dokončení úlohy na instalaci aplikace. Po dokončení budete schopni ESET LiveGuard Advanced konfigurovat prostřednictvím politiky.

Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

Pokud jste vybrali bezpečnostní produkt ESET pro Windows – Vyberte tuto možnost, pokud chcete nastavit ochranu produktu již v průběhu instalace:

- **Zapnout systém zpětné vazby ESET LiveGrid® (doporučujeme)**
- **Zapnout detekci potenciálně nechtěných aplikací** – více informací naleznete v naší Databázi znalostí.

Parametry instalace (volitelné):

- Parametry příkazového řádku můžete využít pouze v případě, kdy je grafické rozhraní MSI instalátoru spuštěno v některém z omezených režimů (**reduced**, **basic** nebo **none**).
- Pro více informací, jaké přepínače podporuje konkrétní verze **msiexec**, se podívejte do dokumentace Windows Installer.
- Parametry pro instalaci prostřednictvím příkazového řádku naleznete v odpovídajících uživatelských příručkách: produkty z řady ESET Endpoint, resp. produkty pro ochranu serverů.

Pokud chcete vynutit restart operační systému, pokud jej instalace vyžaduje, vyberte možnost **Automaticky restartovat, když je potřeba**. Necháte-li tuto možnost neaktivní, rozhodnutí o restartu je na uživateli počítače. V tomto případě restartujte počítač ručně. V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje.

Instalace aplikací třetích stran

Pomocí této úlohy můžete **instalovat** také aplikace třetích stran.

Operační systém	Podporované typy instalačních balíčků	Podpora parametrů
Windows	*.msi*	Instalační *.msi* balíček se vždy pouští jako tichá instalace. Není možné definovat msiexec parametry. Použít můžete pouze parametry samotného instalačního balíčku, které jsou pro každou aplikaci odlišné (pokud existují).
Linux	*.deb, .rpm, .sh*	Parametry můžete použít pouze u *.sh* souborů (*.deb* a *.rpm* balíčky nepodporují parametry).
macOS	*.pkg, .dmg* (obsahující *.pkg* soubor	Instalační parametry nejsou podporovány.
Android	*.apk*	Instalační parametry nejsou podporovány.
iOS	*.ipa*	Instalační parametry nejsou podporovány.

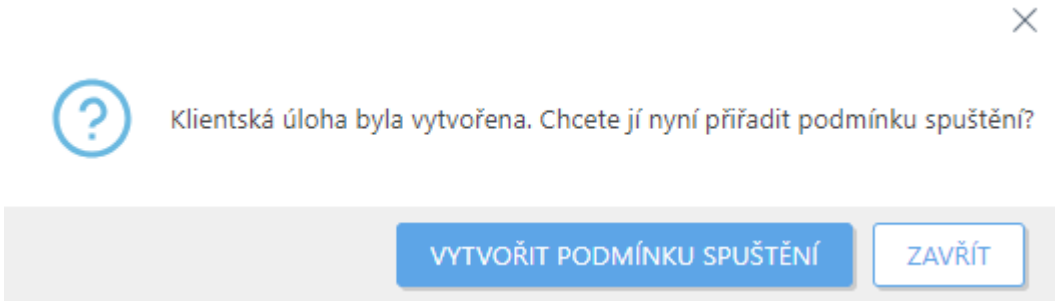
Chcete pomocí skriptu *install_script.sh* nainstalovat aplikaci na Linux, který má dva parametry: `-a` představuje první parametr, `-b` představuje druh parametr.
Instalace v terminálu (pod uživatelem root ze složky, kde je *umístěn* skript *install_script.sh*):
`./install_script.sh -a parameter_1 -b parameter_2`
Instalace prostřednictvím úlohy:
- Do pole **Instalovat balíček z URL** zadejte cestu k souboru, například: *file:///home/user/Desktop/install_script.sh*
- Jako **parametry instalace** zadejte: `-a parameter_1 -b parameter_2`.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky

spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Seznam chybových zpráv při instalaci

- Instalační balíček nebyl nalezen.
- Je vyžadována novější verze služby Windows Installer.
- Nainstalovaná je jiná verze produktu nebo konfliktní aplikace.
- Již probíhá jiná instalace. Před pokračováním dokončete tuto instalaci.
- Instalace nebo odinstalace byla úspěšně dokončena, ale je vyžadován restart.
- Úloha selhala z důvodu výskytu chyby. Otevřete si trace log Agenta, případně protokol software-install.log a najděte návratový kód instalátoru.

Safetica software

Co je Safetica?

Safetica je řešení třetí strany, které je součástí ESET Technology Alliance. Safetica poskytuje IT řešení pro zabránění ztráty dat (DLP) a doplňuje tak portfolio bezpečnostních řešení ESET. Primárním účelem Safetica software je:

- Zabránění ztráty dat – monitorování všech pevných disků, USB jednotek, síťového přenosu, e-mailů a tiskáren stejně jako aplikací přistupujících k souborům
- Reportování a blokování aktivity – pro souborové operace webové stránky, e-maily, instant messaging, používání aplikací a vyhledávání

Jak Safetica pracuje?

Safetica vyžaduje nasazení agenta (Safetica Endpoint Client) na každou stanici z níž chcete získat data a zajišťuje komunikaci mezi serverem (Safetica Management Service). Tento server shromažďuje informace o aktivitách na pracovních stanicích a distribuuje na ně politiky pro ochranu dat.

Integrace Safetica v ESET PROTECT

ESET Management Agent detekuje a reportuje Safetica aplikace jako ESET aplikace (v **Detailech zařízení** v sekci Instalované aplikace). Webová konzole ESET PROTECT aktualizuje Safetica Agenta, pokud je k dispozici nová verze.

Nasazení Safetica Agenta

Safetica Agenta můžete nasadit přímo z webové konzoleESET PROTECT prostřednictvím klientské úlohy pro instalaci aplikace, kdy si balíček vyberete z ESET repozitáře a v parametrech instalace zadáte `STSERVER=Server_name` (kde `Server_name` je název nebo IP serveru, na kterém máte nainstalovánu **Safetica Management službu**).

Safetica Agenta můžete nainstalovat také prostřednictvím klientské úlohy Spustit příkaz.

Použití úlohy na spuštění příkazu

```
msiexec /i safetica_agent.msi STSERVER=Server_name
```

Přidáním parametru `/silent` na konec příkazu zajistíte spuštění instalace v tzv. "tichém" režimu. Příklad:
`msiexec /i safetica_agent.msi STSERVER=Server_name /silent`
Pro nainstalování Safetica Agenta výše uvedeným způsobem se již musí .msi balíček na cílové stanici nacházet. Pro spuštění instalace z *.msi* balíčku nacházejícího se na sdíleném úložišti je nutné v příkazu definovat cestu:
`msiexec /i Z:\sharedLocation\safetica_agent.msi STSERVER=Server_name`

Aktualizace Safetica Agenta

Pro aktualizování Safetica Agenta na spravovaném počítači přejděte do jeho **Detailů** > Nainstalované aplikace, v seznamu klikněte na **Safetica Agent** a následně na tlačítko **Aktualizovat ESET aplikace**.

Odinstalace Safetica Agenta

Pro odinstalování Safetica Agenta ze spravovaného počítače přejděte do jeho **Detailů** > Nainstalované aplikace, v seznamu klikněte na **Safetica Agent** a následně na tlačítko **Odinstalovat**.

Odinstalace aplikace

Pomocí této úlohy můžete z cílové stanice **odinstalovat** produkty ESET, případně další aplikace, které nepotřebujete.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

Možnosti odinstalace aplikace

Z rozbalovací nabídky vyberte možnost **Odinstalovat**:

Aplikaci ze seznamu

- **Název balíčku** – vyberte komponentu ESET PROTECT, bezpečnostní řešení ESET nebo aplikaci třetí strany. Standardně se reportují pouze aplikace ESET. Pro získání seznamu všech aplikací upravte politiku agenta. V seznamu se zobrazí všechny nainstalované balíčky na dané stanici, které je možné vzdáleně odinstalovat.

Po odinstalování ESET Management Agenta ze stanice nebude již dané zařízení spravované prostřednictvím ESET PROTECT:
- Po odinstalování ESET Management Agenta mohou některá nastavení bezpečnostního produktu ESET zůstat zachována.
- Pokud je Agent ESET Management chráněný heslem, pro odinstalaci, opravu nebo aktualizaci (se změnami) je nutné zadat heslo. Před odebráním zařízení ze správy doporučujeme prostřednictvím speciální politiky obnovit nastavení produktu na standardní hodnoty (především deaktivovat ochranu heslem).
- Dojde k přerušení všech běžících úloh vykonávaných agentem. Stav provedení této úlohy (**Běží**, **Dokončeno** nebo **Selhala**) se nemusí ve webové konzoli ESET PROTECT zobrazovat přesně v závislosti na replikaci.
- Po odinstalování agenta můžete bezpečnostní produkt spravovat lokálně prostřednictvím grafického rozhraní nebo eShell.

- **Verze balíčku** – vybrat můžete pouze **konkrétní verzi** dané aplikace, případně odinstalovat všechny verze balíčku.

- **Parametry odinstalace** – v případě potřeby definujte parametry odinstalace.

- Pokud chcete vynutit restart operační systému, pokud jej instalace vyžaduje, vyberte možnost **Automaticky restartovat, když je potřeba**. Necháte-li tuto možnost neaktivní, rozhodnutí o restartu je na uživateli počítače. V tomto případě restartujte počítač ručně. V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje.

Antivirový program třetí strany pomocí nástroje ESET AV Remover

Standardně se reportují pouze aplikace ESET. Pro získání seznamu všech aplikací upravte politiku agenta.

Seznam podporovaných antivirových programů naleznete v Databázi znalostí. Nejedná se o klasickou odinstalaci prostřednictvím systémového panelu **Programy a funkce**. Pro odstranění je použit nástroj třetí strany, který dokáže aplikaci odstranit kompletně včetně záznamů v registru.

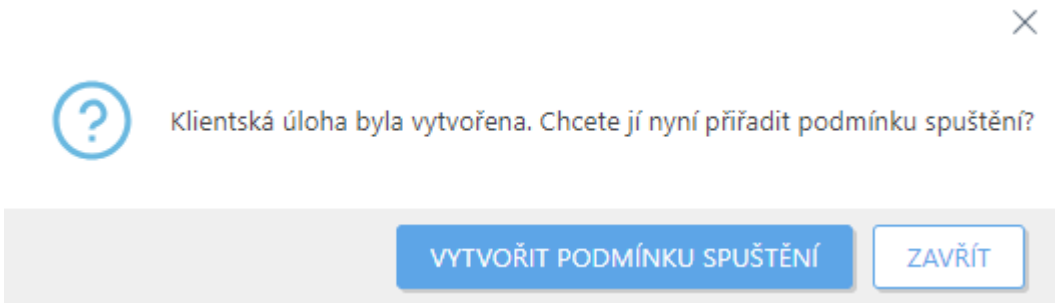
Postup pro odinstalaci antivirových řešení třetích stran naleznete v Databázi znalostí v článku Remove third-party antivirus software from client computers using ESET PROTECT.

Pokud máte nastavení produktu ESET chráněno heslem, podrobnější informace naleznete v Databázi znalostí.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

> Máte-li nastavení produktu ESET chráněno heslem, je potřeba jej zadat při vytváření odinstalační úlohy. V opačném případě odinstalace selže. Příklad výsledku: **Product: ESET Endpoint Security -- Error 5004. Pro pokračování v odinstalaci je potřebné zadat správné heslo.** Jako parametr tedy zadejte PASSWORD=vašeheslo. Případně na stanici aplikujte Databázi politiku, která nejprve zruší ochranu heslem. Poté budete schopni produkt odinstalovat vzdáleně prostřednictvím úlohy.

Ukončit správu (odinstalovat ESET Management Agenta)

Prostřednictvím této úlohy odinstalujete ESET Management Agenta z cílového zařízení. Pokud je jako cíl vybrán počítač, dojde k odebrání ESET Management Agenta. V případě mobilního zařízení dojde k jeho odregistrování z MDM.

Po odinstalování ESET Management Agenta ze stanice nebude již dané zařízení spravované prostřednictvím ESET PROTECT:
• Po odinstalování ESET Management Agenta mohou některá nastavení bezpečnostního produktu ESET zůstat zachována.
• Pokud je Agent ESET Management chráněný heslem, pro odinstalaci, opravu nebo aktualizaci (se změnami) je nutné zadat heslo. Před odebráním zařízení ze správy doporučujeme prostřednictvím speciální politiky obnovit nastavení produktu na standardní hodnoty (především deaktivovat ochranu heslem).
• Dojde k přerušení všech běžících úloh vykonávaných agentem. Stav provedení této úlohy (**Běží**, **Dokončeno** nebo **Selhala**) se nemusí ve webové konzoli ESET PROTECT zobrazovat přesně v závislosti na replikaci.
• Po odinstalování agenta můžete bezpečnostní produkt spravovat lokálně prostřednictvím grafického rozhraní nebo eShell.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

• V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.

• V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.

• V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

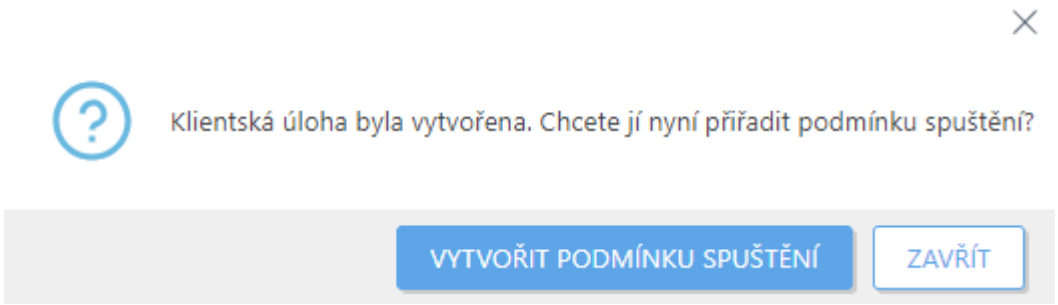
Pro tuto úlohu není dostupné žádné **nastavení**.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

• Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.

• Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Vyžádat SysInspector protokol (pouze pro Windows)

Pomocí této možnosti získáte **SysInspector protokol** z bezpečnostního produktu na cílové stanici, který tuto funkci podporuje.

ESET SysInspector je možné spustit pouze na počítačích s Windows.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost + **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > + **Nová úloha**. Tuto úlohu můžete spustit v sekci **Počítače**, kde klikněte na požadovaný počítač a vyberte možnost **Detaily**. Dále přejděte na záložku **Protokoly** a klikněte na tlačítko **Vyžádat protokol (pouze na Windows)**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

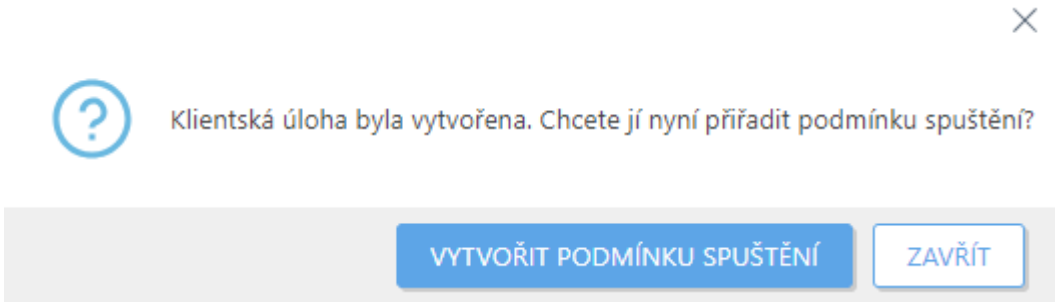
Nastavení

- **Uložit protokol na klienta** – vyberte tuto možnost, pokud chcete SysInspector protokol uložený na klientovi odeslat také na ESET PROTECT server. Pokud bude máte na klientovi nainstalován například ESET Endpoint Antivirus, protokol se standardně uloží do složky *C:\Program Data\ESET\ESET Security\SysInspector*.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Po dokončení sběru dat a zaslání ESET SysInspector protokolu z klienta na server ho uvidíte v této sekci. Kliknutím na požadovaný záznam si ho můžete stáhnout nebo rovnou prohlédnout.

Aktualizovat Agenta

Pomocí této úlohy **aktualizujete ESET Management Agenta** na nejnovější verzi.

ESET PROTECT podporuje automatickou aktualizaci ESET Management agentů ve spravovaných počítačích.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
- V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Pro zabránění selhání klientské úlohy provede ESET Management Agent před spuštění úlohy pro instalaci/aktualizaci produktu ESET kontrolu, zda:

- má stanice přístup k repozitáři,
- je dostatek místa na disku pro instalaci produktu (neověřuje se na Linuxu).

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku

klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

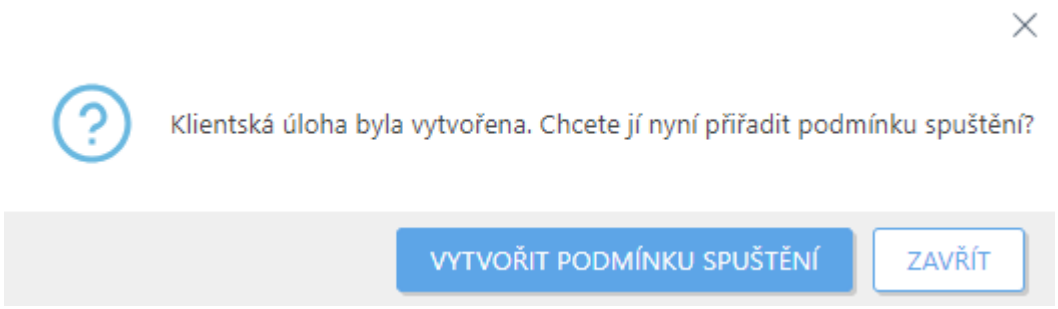
Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

Pokud chcete vynutit restart operační systému, pokud jej instalace vyžaduje, vyberte možnost **Automaticky restartovat, když je potřeba**. Necháte-li tuto možnost neaktivní, rozhodnutí o restartu je na uživateli počítače. V tomto případě restartujte počítač ručně. V případě potřeby můžete upravit chování restartování/vypnutí spravovaného počítače. Na počítači musí být nainstalován ESET Management Agent ve verzi 9.1 a novější společně s bezpečnostním produktem ESET, který toto nastavení podporuje.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

- Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.
- Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Získat soubor z karantény

Pomocí této úlohy můžete vzdáleně **získat obsah karantény** z cílové stanice. Prostřednictví této úlohy nahráváte soubor umístěný v karanténě do sdílené složky ve své síti. Proto byste měli být při použití této úlohy opatrní a používat ji s rozmyslem.

Novou klientskou úlohu můžete vytvořit jedním z následujících způsobů:

- V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.

• V hlavním menu přejděte na záložku **Úlohy**, vyberte si požadovaný typ úlohy a klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.

• V hlavním menu na záložce **Počítače** klikněte na požadované zařízení a v kontextovém menu vyberte možnost **Úlohy** > **Nová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Nastavení

• **Objekt v karanténě** – vyberte objekt v karanténě, který chcete získat.

• **Heslo k objektu** – zadejte heslo, kterým bude výsledný archiv z bezpečnostních důvodů opatřen. Mějte na paměti, že heslo se zobrazí v čitelné podobě v odpovídajícím přehledu.

• **Nahrát do** – zadejte umístění, do kterého chcete objekt z karantény nahrát. Použijte následující syntaxi: *smb://server/share*

• **Uživatelské jméno/heslo pro nahrání** – pokud je pro přístup a zápis do zadaného umístění (síťového úložiště atp.) vyžadováno oprávnění, zadejte platné přihlašovací údaje. Pokud se jedná o doménového uživatele, použijte formát `DOMAIN\username`.

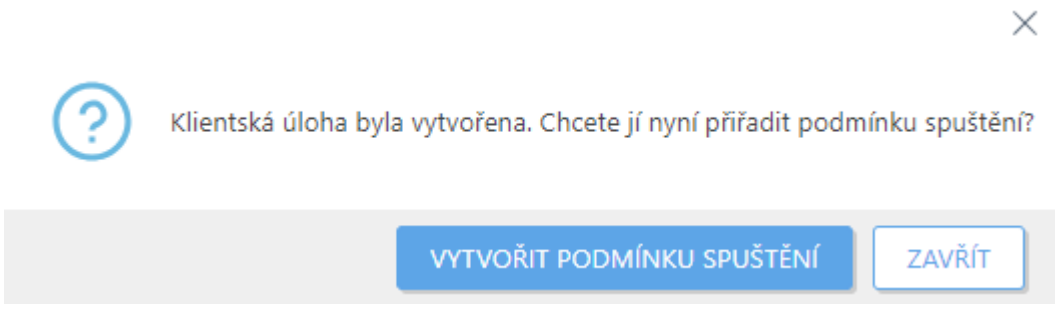
Při tvorbě podmínky spuštění se ujistěte, že jste vybrali cíl, kde je soubor umístěn v karanténě.

Souhrn

Zkontrolujte, zda parametry klientské úlohy vyhovují vašim potřebám a klikněte na tlačítko **Dokončit**. Klientská úloha se vytvoří a zobrazí se malé dialogové okno:

• Po kliknutí na tlačítko Vytvořit podmínku spuštění (doporučujeme) můžete rovnou definovat cíl (počítač nebo skupinu), nad kterým chcete klientskou úlohu spustit.

• Pokud okno **zavřete**, můžete podmínku spuštění vytvořit později. Pro pozdější vytvoření podmínky spuštění klikněte na instanci dané úlohy a z kontextového menu vyberte možnost **Spustit na**.



U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Objekt z karantény se následně nahraje do vámi **definovaného umístění**:

- Soubor je uložen do *.zip* archivu opatřeného heslem. Heslo k *.zip* je jeho název (kontrolní součet objektu v karanténě).
- Soubor je v archivu bez přípony. Pro jeho obnovení soubor přejmenujte a přidejte do názvu původní příponu.

Serverové úlohy

Serverové úlohy provádí ESET PROTECT Server přímo u sebe nebo jiných zařízeních. Serverové úlohy, kromě Nasazení ESET Agenta, není možné přiřadit jednotlivým klientům nebo skupinám. Každá serverová úloha má právě jednu podmínku spuštění. Pokud úlohu potřebujete spouštět při různých událostech, vytvořte si více stejných úloh s odlišnými podmínkami spuštění.

Serverové úlohy

- Odstranění nepřipojujících se počítačů
- Generování přehledu
- Přejmenování počítačů

Serverové úlohy a oprávnění

Serverové úlohy a podmínky spuštění jsou prováděny pod konkrétním uživatelem. Jedná o uživatele, který naposledy úlohu, resp. podmínku, upravil. To znamená, že pro provedení akce musí uživatel potřebná oprávnění. Pro spuštění úlohy se použije uživatel z podmínky spuštění. Pokud máte nastavení **Spustit úlohu okamžitě po dokončení**, uživatel, který ji spustí, bude ten, který aktuálně přihlášený v ESET PROTECT Web Console. Uživatel má oprávnění (**číst**, **použít**, **zápis**) ke konkrétnímu **typu úlohy**, pokud toto oprávnění obsahuje sada oprávnění definovaná v sekci **Další** > **Sady oprávnění**, která je platná pro statickou skupinu v níž se nachází požadovaná serverová úloha. Více informací naleznete v kapitole seznam oprávnění.

Filip, jehož domovskou skupinou je *Filipova skupina*, chce odstranit *Serverovou úlohu 1*: **Generování přehledu**. Protože úlohu vytvořil *Petr*, je umístěna v jeho domovské skupině (*Petrova skupina*). Aby mohl *Filip* úlohu odstranit:
- *Filip* musí mít přiřazenou sadu oprávnění s hodnotou **Zápis** u položky **Serverové úlohy a podmínky spuštění** > **Generování přehledu**.
- Jako **statická skupina** musí být v dané sadě oprávnění nastavena *Petrova skupina*.

Oprávnění pro práci se serverovými úlohami

- Pro vytvoření nové serverové úlohy musí mít určitě oprávnění Zápis u konkrétního typu úlohy a dále k objektům používaným v úloze (počítačům a skupinám, přehledům, ...).
- Pro úpravu existující serverové úlohy musí mít uživatel oprávnění **Zápis** u konkrétního typu úlohy a dále k objektům používaným v úloze (počítačům a skupinám, licencím, ...).

- Pro odstranění serverové úlohy musí mít uživatel oprávnění **Zápis** u konkrétního typu úlohy.
- Pro spuštění serverové úlohy musí mít uživatel oprávnění **Použít** u konkrétního typu úlohy.

Pro vytvoření nové serverové úlohy

1. Pro vytvoření nové serverové úlohy přejděte v hlavním menu Web Console na záložku **Úlohy** a klikněte na tlačítko **Nová...** > **Serverová úloha**. Případně si nejprve vyberte požadovaný typ úlohy a poté klikněte na tlačítko **Nová** > **Serverová úloha**.

2. V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Dále si můžete vybrat jednu z níže uvedených možnosti pro vytvoření podmínky spuštění:

- **Spustit úlohu okamžitě po dokončení** – tuto možnost vyberte, pokud chcete úlohu spustit okamžitě poté, co kliknete na tlačítko Dokončit.
- Pokud si chcete definovat vlastní podmínku spuštění, vyberte možnost **Nastavit podmínku spuštění** a následně se zpřístupní sekce Podmínka spuštění a Rozšířená nastavení.

Pokud chcete jen vytvořit úlohu a spouštět ji ručně, případně vytvoříte podmínku spuštění později, nevybírejte žádnou možnost.

3. V sekci **Nastavení** definujte parametry úlohy.

4. Pokud jste aktivovali možnosti **Nastavit podmínku spuštění**, definujte parametry pro spuštění úlohy.

5. V části **Souhrn** zkontrolujte, zda parametry úlohy odpovídají vašim potřebám, a úlohu vytvořte kliknutím na tlačítko **Dokončit**.

> Pokud máte uživatele, kteří pravidelně používají některé ze serverových úloh, nechte je vytvořit si (v jejich domovské skupině) nové úlohy, ke kterým budou mít přístup pouze oni. Při každém spuštění úlohy se použije oprávnění executing user. Při používání sdílených/společných úloh by nemuselo být vždy zcela jasné, kdo úlohu vlastně spustil.

Odstranění nepřipojujících se počítačů

Tuto úlohu můžete použít pro odebrání počítačů podle zadaných kritérií. Pokud se například ESET Management Agent v klientském zařízení nepřipojil po dobu 30 dnů, může být z webové konzole ESET PROTECT odebrán.

Přejděte na záložku Počítače. Ve sloupci **Naposledy připojeno** je uvedeno datum a čas posledního připojení spravovaného zařízení k serveru. Symbol zelené tečky značí, že se počítač naposledy k serveru připojil před méně než 10 minutami. V závislosti na hodnotě ve sloupci **Naposledy připojeno** se informace zvýrazní, abyste mohli snáze rozpoznat nepřipojující se zařízení

- Žlutá (chyba) – zařízení se k serveru nepřipojilo 2 až 14 dnů.

oČervená (varování) – zařízení se k serveru připojilo více než 14 dnů.

Pro vytvoření nové serverové úlohy přejděte v hlavním menu Web Console na záložku **Úlohy** a klikněte na tlačítko **Nová…** > **Serverová úloha**. Případně si nejprve vyberte požadovaný typ úlohy a poté klikněte na tlačítko **Nová** > **Serverová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Dále si můžete vybrat jednu z níže uvedených možnosti pro vytvoření podmínky spuštění:

- **Spustit úlohu okamžitě po dokončení** – tuto možnost vyberte, pokud chcete úlohu spustit okamžitě poté, co kliknete na tlačítko Dokončit.

- Pokud si chcete definovat vlastní podmínku spuštění, vyberte možnost **Nastavit podmínku spuštění** a následně se zpřístupní sekce Podmínka spuštění a Rozšířená nastavení.

Pokud chcete jen vytvořit úlohu a spouštět ji ručně, případně vytvoříte podmínku spuštění později, nevybírejte žádnou možnost.

Nastavení

Název skupiny – vyberte již existující statickou skupinu, ze které chcete odstranit nepřipojující se počítače, případně si vytvořte novou.

Počet dní, po které se počítač nepřipojil – zadejte počet dní.

Deaktivovat licenci – tuto možnost vyberte, pokud chcete na cílovém počítači deaktivovat produkt ESET a odstranit vazbu z licenčního portálu.

Odebrat nespravované počítače – tuto možnost vyberte, pokud chcete odstranit také nespravované počítače (zařízení, na kterých není nainstalován agent).

Podmínka spuštění

V části **podmínka spuštění** můžete definovat parametry pro spuštění úlohy. Každá **serverová úloha** má právě jednu podmínku spuštění. To znamená, že pro každou **serverovou úlohu** je nutné vytvořit novou podmínku spuštění. Tato sekce se zpřístupní, pokud v části **Obecné** aktivujete možnost **Nastavit podmínku spuštění**. Úlohu můžete vytvořit bez podmínky spuštění. Přidat ji můžete později nebo úlohu kdykoli spustit ručně.

Rozšířená nastavení

V této části můžete vytvořit pokročilá pravidla pro aktivaci podmínky spuštění a tzv. throttlingem zabránit nadměrnému spouštění úlohy. Definování throttlingu je volitelné.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené úloze. Zkontrolujte, zda nastavení odpovídá vašim představám, pokračujte kliknutím na **Dokončit**.

U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Generování přehledu

Pomocí této úlohy si naplánujete jednorázové nebo pravidelné **generování** některé z předdefinovaných nebo vámi vytvořených šablon přehledu.

Pro vytvoření nové serverové úlohy přejděte v hlavním menu Web Console na záložku **Úlohy** a klikněte na tlačítko **Nová…** > **Serverová úloha**. Případně si nejprve vyberte požadovaný typ úlohy a poté klikněte na tlačítko **Nová** > **Serverová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Dále si můžete vybrat jednu z níže uvedených možnosti pro vytvoření podmínky spuštění:

- **Spustit úlohu okamžitě po dokončení** – tuto možnost vyberte, pokud chcete úlohu spustit okamžitě poté, co kliknete na tlačítko Dokončit.
- Pokud si chcete definovat vlastní podmínku spuštění, vyberte možnost **Nastavit podmínku spuštění** a následně se zpřístupní sekce Podmínka spuštění a Rozšířená nastavení.

Pokud chcete jen vytvořit úlohu a spouštět ji ručně, případně vytvoříte podmínku spuštění později, nevybírejte žádnou možnost.

Nastavení

Šablona přehledu – klikněte na možnost Přidat šablonu přehledu a ze seznamu vyberte alespoň jednu šablonu přehledu. Při vytváření úlohy bude mít uživatel k dispozici pouze šablony přehledů, které se nacházejí v jeho domovské skupině, resp. šablony, k nimž má přístup. V jedné úloze si můžete vybrat více šablon přehledů.

MSP uživatelé mohou přehledy filtrovat podle zvoleného zákazníka.

- **Komu** – zadejte e-mailové adresy příjemců, kterým chcete odeslat přehled. Více adres oddělte čárkou (,). Případně můžete přidat další příjemce do pole Kopie nebo Skrytá kopie.
- ESET PROTECT předvyplní předmět a tělo e-mailu na základě vybrané šablony přehledu. Pro přizpůsobení **Předmětu** a **Zprávy** aktivujte zaškrtávací pole v sekci **Přizpůsobit zprávu**.
  - **Předmět** – zadejte předmět zprávy. Doporučujeme zadat výrazný předmět, takový, abyste si mohli e-

maily pohodlně třídit ve svém poštovním klientovi. Toto pole není povinné, ale nenechávejte jej prázdné.

- **Zpráva** – zadejte tělo zprávy, ve které bude přehled.

- **Odeslat e-mail, pokud je přehled prázdný** – pomocí této možnosti zajistíte odesílání e-mailu také v případě, že v přehledu nebudou žádná data.

Po kliknutí na odkaz **Zobrazit možnosti tisku** se zobrazí následující možnosti:

- **Výstupní formát** – vyberte formát, do kterého chcete přehled vygenerovat. Vybrat si můžete formát *.pdf* nebo *.csv*. CSV je vhodný formát pouze pro tabulková data a jako oddělovač je použit středník `;`. Pokud si stáhnete přehled ve formátu CSV a ve sloupci, ve kterém očekáváte text, jsou uvedena čísla, pro korektní zobrazení dat si stáhněte přehled ve formátu PDF.

> Při použití CSV formátu bude datum a čas uložen v UTC formátu. Pokud budete přehled generovat do PDF, použije se lokální čas serveru.

- **Výstupní jazyk** – vyberte jazyk zprávy. Standardně se použije jazyk, ve kterém používáte ESET PROTECT Web Console.

- **Velikost stránky/Rozlišení (DPI)/Orientace stránky/Možnosti barvy/Jednotky/Okraje** – vyberte možnosti, které vyhovují vašim potřebám tisku. Tato nastavení jsou relevantní v případě, kdy chcete přehled vytisknout do formátu PDF (nikoli CSV).

Podmínka spuštění

V části **podmínka spuštění** můžete definovat parametry pro spuštění úlohy. Každá **serverová úloha** má právě jednu podmínku spuštění. To znamená, že pro každou **serverovou úlohu** je nutné vytvořit novou podmínku spuštění. Tato sekce se zpřístupní, pokud v části **Obecné** aktivujete možnost **Nastavit podmínku spuštění**. Úlohu můžete vytvořit bez podmínky spuštění. Přidat ji můžete později nebo úlohu kdykoli spustit ručně.

Rozšířená nastavení

V této části můžete vytvořit pokročilá pravidla pro aktivaci podmínky spuštění a tzv. throttlingem zabránit nadměrnému spouštění úlohy. Definování throttlingu je volitelné.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené úloze. Zkontrolujte, zda nastavení odpovídá vašim představám, pokračujte kliknutím na **Dokončit**.

U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Přejmenování počítačů

Tuto úlohu využít pro automatické **přejmenování počítačů** zobrazených v ESET PROTECT Web Console, například do FQDN formátu. Po nainstalování ESET PROTECT je již tato serverová úloha připravena. Pokud se název zařízení od prvního připojení změnil, tato úloha zajistí jeho přejmenování na správný název.

Tato úloha automaticky přejmenovává každou hodinu počítače umístěné ve statické skupině **Ztráty a nálezy**.

Pro vytvoření nové serverové úlohy přejděte v hlavním menu Web Console na záložku **Úlohy** a klikněte na tlačítko **Nová…** > **Serverová úloha**. Případně si nejprve vyberte požadovaný typ úlohy a poté klikněte na tlačítko **Nová** > **Serverová úloha**.

Obecné

V této části zadejte **obecné informace** o vytvářené úloze, jako je **název a volitelně popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.
V rozbalovacím menu **Úloha** si vyberte typ úlohy, kterou chcete vytvořit a konfigurovat. Pokud jste typ úlohy definovali před kliknutím na tlačítko **Nová**, její typ již bude předvybrán. Na základě **typu úlohy** se mění možnosti její konfigurace a chování (viz seznam klientských úloh).

Dále si můžete vybrat jednu z níže uvedených možnosti pro vytvoření podmínky spuštění:

- **Spustit úlohu okamžitě po dokončení** – tuto možnost vyberte, pokud chcete úlohu spustit okamžitě poté, co kliknete na tlačítko Dokončit.
- Pokud si chcete definovat vlastní podmínku spuštění, vyberte možnost **Nastavit podmínku spuštění** a následně se zpřístupní sekce Podmínka spuštění a Rozšířená nastavení.

Pokud chcete jen vytvořit úlohu a spouštět ji ručně, případně vytvoříte podmínku spuštění později, nevybírejte žádnou možnost.

Nastavení

Název skupiny – vyberte statickou nebo dynamickou skupinu, ve které chcete počítače přejmenovat.

Přejmenovat na základě:

- **Název počítače** – jednoznačný identifikátor počítače v lokální síti
- **FQDN (Fully Qualified Domain Name) počítače** – začíná názvem počítače a dále následují názvy všech nadřízených domén

Podmínka spuštění

V části **podmínka spuštění** můžete definovat parametry pro spuštění úlohy. Každá **serverová úloha** má právě jednu podmínku spuštění. To znamená, že pro každou **serverovou úlohu** je nutné vytvořit novou podmínku spuštění. Tato sekce se zpřístupní, pokud v části **Obecné** aktivujete možnost **Nastavit podmínku spuštění**. Úlohu můžete vytvořit bez podmínky spuštění. Přidat ji můžete později nebo úlohu kdykoli spustit ručně.

Rozšířená nastavení

V této části můžete vytvořit pokročilá pravidla pro aktivaci podmínky spuštění a tzv. throttlingem zabránit nadměrnému spouštění úlohy. Definování throttlingu je volitelné.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené úloze. Zkontrolujte, zda nastavení odpovídá vašim představám, pokračujte kliknutím na **Dokončit**.

U každé úlohy je v sekci **Úlohy** její průběh, ikona stavu a zobrazit si můžete její detaily.

Typy podmínek spuštění

Podmínky spuštění fungují jako senzory, které definovaným způsobem reagují na určité události. Slouží pro provedení nějaké činnosti, nejčastěji se používají pro spuštění úloh. Aktivovány mohou být plánovačem nebo systémovou událostí.

Podmínky spuštění klientské úlohy nelze používat opakovaně. Každá podmínka spuštění je pevně svázána s konkrétní úlohou. Pro každou úlohu je nutné vytvořit novou podmínku spuštění.

Pokud přiřadíte nově vytvořené úloze podmínku spuštění, úloha se spustí až ve chvíli, kdy dojde ke splnění podmínek (vyjma podmínky Ihned). V případě potřeby můžete zabránit nadměrnému generování přehledů.

Podmínky spuštění klientské úlohy na mobilních zařízeních

Pro klientské úlohy na mobilních zařízeních můžete použít pouze tyto podmínky spuštění:

- Ihned
- Při připojení do dynamické skupiny

Klientské úlohy s jinými než výše uvedenými podmínkami spuštění skončí chybovou zprávou **Nepodporovaný typ podmínky spuštění**.

Typ podmínky spuštění

- **Jakmile je to možné** – dostupné pouze pro klientské úlohy. Vybráním této možnosti dojde k naplánování spuštění úlohy na co nejbližší možnou dobu, poté co kliknete na tlačítko **Dokončit**. Platnost úlohy je omezena datem stanovým v poli **Platnost do**. Po uplynutí této doby se úloha již nespustí. Platnost podmínky může být nejvýše 6 měsíců.

Naplánované

Podmínky spuštění můžete použít také pro naplánování spuštění úlohy ve stanovený datum a čas. Úlohu můžete spustit pouze **jednou**, opakovaně na základě časového kritéria nebo CRON výrazu.

- **Naplánovat jednou** – na základě této podmínky se úloha spustí jednou ve stanový datum a čas. Ke zpoždění spuštění může dojít při použití náhodného intervalu.

- **Denně** – na základě této podmínky se úloha spustí každý den. Můžete ji nechat spouštět pravidelně každý den ve stanovený čas nebo definovat konečné datum, po jehož uplynutí se úloha již nespustí. Například můžete úlohu nechat spouštět 10 po sobě jdoucích týdnů.

- **Týdně** – na základě této podmínky se úloha spustí ve vybrané dny v týdnu. Například můžete naplánovat spuštění na každé pondělí a pátek v období od 1.6. do 31.8.

- **Měsíčně** – na základě této podmínky se úloha spustí ve vybrané dny v měsíci. V případě potřeby můžete aktivovat **opakování** a nechat úlohu spouštět například každé druhé pondělí.

- **Ročně** – na základě této podmínky se úloha spustí každý rok (není-li stanoveno jinak) ve **stanovený** datum a čas.

Možnost **Náhodný interval prodlevy** je dostupná v případě plánovaných podmínek spuštění. Představuje maximální prodlevu pro spuštění úlohy. Definováním náhodného intervalu můžete zabránit přetížení serveru.

Pavel přiřadil **úloze** podmínku spuštění s **týdenním opakováním** a **začátkem** v *pondělí 10.2.2017 v 8:00:00*. **Náhodný interval** je nastaven na *1 hodinu* a **konec je stanoven** na *6.4.2017 v 00:00:00*. To znamená, že úloha se spustí každé pondělí mezi 8 až 9 hodinou, dokud neuplyne stanové datum.

- Pro okamžité spuštění úlohy, pokud její provedení neproběhlo ve stanovený čas, vyberte možnost **Provést jakmile je to možné, pokud úloha nebyla provedena**.
- Při vytváření podmínky spuštění se automaticky použije časové pásmo z ESET PROTECT Web Console. Volitelně můžete vybrat možnost **Použít lokální čas cíle**, čímž zajistíte, že se k provedení úlohy použije čas na cílovém zařízení, místo časového pásma, ve kterém je ESET PROTECT Web Console.

Dynamická skupina

Níže uvedené podmínky dynamických skupiny jsou dostupné pouze pro spuštění klientských úloh:

- **Změna obsahu dynamické skupiny** – tato podmínka se uplatí, při změně počtu zařízení v definované dynamické skupině. Například zařízení se stane členem dynamické skupiny nebo ji opustí.

- **Změna obsahu dynamické skupiny z důvodu překročení mezní hodnoty** – uplatní se, pokud počet zařízení překročí nebo spadne pod definovanou hodnotu. Například ve skupině Počítače s neaktualizovaným operačním systémem bude více než 100 počítačů.

- **Změna obsahu dynamické skupiny ve sledovaném období** – uplatní se, pokud se velikost dynamické skupiny změnila ve sledovaném období. Například počet zařízení ve skupině vzrostl za poslední hodinu o 10 %.

- **Změna obsahu dynamické skupiny oproti porovnávané skupině** – uplatní se, pokud se ve sledované skupině změní počet zařízení ve srovnání s jinou skupinou (statickou nebo dynamickou). Například bude infikováno více než 10 % všech zařízení, tedy porovnává se počet zařízení ve skupině **Infikovaná zařízení** se statickou skupinou **Všechna zařízení**.

Ostatní

- **Při připojení do dynamické skupiny** – dostupné pouze pro klientské úlohy. – tato podmínka se uplatí po každé, když se zařízení stane členem dynamické skupiny.

Možnost **při připojení do dynamické skupiny** je dostupná v případě, kdy jste jako cíl vybrali dynamickou skupinu. Tato podmínka zajistí, že se úloha spustí na každé nově přidané zařízení do skupiny. Na zařízeních, která již jsou členem dynamické skupiny, musíte úlohu spustit ručně.

- **Při výskytu události** – spustí úlohu, pokud se v protokolech vyskytne definovaná událost. Příklad: při nalezení hrozby v **protokolu kontroly počítače**. Tento typ podmínky nabízí možnosti pro zabránění nadměrného spuštění (throttling).

- **CRON výraz** – podmínka se uplatní ve stanovený datum a čas.

CRON výraz

CRON výraz můžete použít při sestavování podmínky spuštění. Nejčastěji se používají pro opakované spouštění. Jedná se o řetězec sestávající se z 6 nebo 7 částí, které reprezentují jednotlivé hodnoty časového plánu. Tato pole jsou oddělena mezerou a mohou obsahovat libovolnou z povolených hodnot včetně jejich kombinací.

CRON výraz může být jednoduchý jako `* * * * ? *`, ale také komplexní jako `0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020`

Seznam hodnot, které můžete při sestavování CRON výrazu použít:

Pole	Vyžadováno	Hodnota	Povolené speciální znaky
Sekundy	Ano	0-59	`, - * / R`
Minuty	Ano	0-59	`, - * / R`
Hodiny	Ano	0-23	`, - * / R`
Den v měsíci	Ano	1-31	`, - * / ? L W`
Měsíc	Ano	1-12 nebo JAN-DEC	`, - */`
Den v týdnu	Ano	0-6 nebo SUN-SAT	`, - / ? L #`
Rok	Ano	1970-2099	`, - * /`

Syntaxe cron výrazu je následující:

```
┌──────────── Sekundy (0–59)
│ ┌────────── Minuty (0–59)
│ │ ┌──────── Hodiny (0–23)
│ │ │ ┌────── Den v měsíci (1–31)
│ │ │ │ ┌──── Měsíc (1–12 nebo JAN-DEC)
│ │ │ │ │ ┌── Den v týdnu (0–6 nebo SUNSAT)(například 0 je stejné jako SUN)
│ │ │ │ │ │ ┌ Rok
* * * * * ? *
```

- 0 0 0 znamená půlnoc (0 sekund, 0 minut, 0 hodin).
- ? (otazník) použijte pro hodnotu, kterou nemůžete definovat, protože jste ji již definovali v jiném poli (například den v měsíci nebo den v týdnu).
- * (hvězdička) představuje každý výskyt – tedy každou sekundu, minutu, hodinu, den v měsíci, den v týdnu, rok.
- SUN znamená neděle.

> U názvů dnů v týdnů a měsíců se nerozlišuje velikost písmen. Příklad: MON se akceptujte stejně jako mon, i jan bude vyhodnocen stejně jako JAN.

Speciální znaky:

Čárka (,)

Čárku použijte pro oddělení jednotlivých položek v seznamu. Příklad: použití "MON,WED,FRI" v šestém poli (den v týdnu) znamená pondělí, čtvrtek a pátek.

Spojovník (-)

Definuje rozsah. Například 2012-2020 znamená každý rok mezi 2012 a 2020, včetně.

Zástupný znak (*)

Použijte jako zástupný znak pro všechny přípustné hodnoty. Příklad: * v druhém poli znamená provedení každou minutu. Mějte na paměti, že zástupný znak nelze uplatnit v poli den v týdnu.

Otazník (?)

Při definování konkrétního dne musíte specifikovat, zda jde o den v měsíci nebo týdnu. Nelze kombinovat obě možnosti. Pokud definujete den v měsíci, v poli pro den v týdnu musíte použít ?, a opačně. Příklad: pokud chcete zajistit spuštění konkrétní den v měsíci, řekneme 10., ale nezáleží vám na tom, jaký je to den v týdnu, zadejte do čtvrtého pole (den v měsíci) hodnotu 10 a do šestého pole (den v týdnu) zadejte ? (otazník).

Hash (#)

Se používá pro definování "n-tého" dne v měsíci. Příklad: 4#3 v poli den v týdnu znamená třetí středu v čtvrtek (4.den = čtvrtek a #3 = 3. čtvrtek v měsíci). Pokud zadáte #5 a měsíc nemá tolik dní, podmínka se v daný měsíc neuplatní.

Lomítko (/)

Použijte pro inkrementování rozsahu (-). Příklad: 3-59/15 v druhém poli (minuty) představuje třetí minutu v hodině a následně každých dalších 15 minut.

Poslední (L)

Při použití v pátém poli (dnu v týdnu) můžete vytvořit specifickou konstrukci jako je například poslední pátek (5L) v daném měsíci. Zadáním L do pole den v měsíce definujete poslední den v měsíci. V případě ledna by se jednalo o 31. den, v únoru 28. den (pro nepřestupný rok).

Pracovní den v týdnu (W)

Znak **W** je možné použít v poli den v měsíci. Tento znak se používá pro zjištění nejbližšího pracovního dne (pondělí – pátek) k danému dni. Pokud do pole den v měsíci zadáte 15W, znamená to nejbližší pracovní den k 15. dni v měsíci. V případě, že 15. připadne na sobotu, podmínka se spustí v pátek 14. V případě, že 15. připadne na neděli, podmínka se spustí v pondělí 16. Nicméně, pokud zadáte 1W jako den v měsíci, a 1. bude sobota, podmínka se aktivuje až 3. v pondělí.

Znaky **L** a **W** můžete kombinovat v poli pro den v měsíci. Použitím hodnoty **LW** vyfiltrujete poslední pracovní den v měsíci..

Náhodně (R)

R představuje speciální znak ESET PROTECT CRON výrazu, pomocí kterého zajistíte provedení v náhodný čas. Například R 0 0 * * ? * znamená, že se podmínka spustí každý den v 00:00, ale v náhodnou sekundu (0-59).

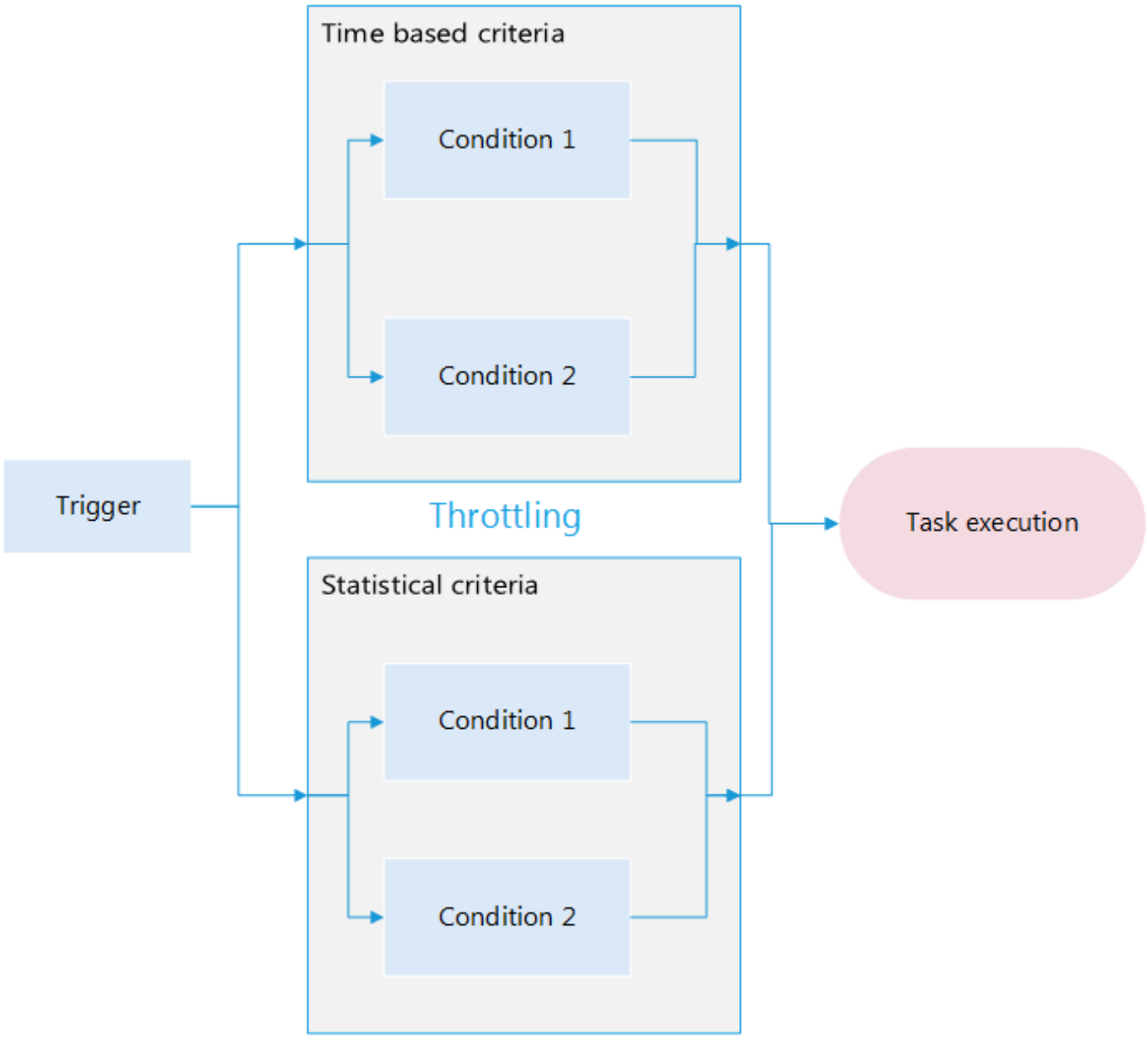
Při definování intervalu připojení ESET Management Agenta doporučujeme používat náhodný interval pro zabránění připojení všech agentů k ESET PROTECT Server.

Níže uvádíme reálné příklady CRON výrazů:

CRON výraz	Význam
`0 0 12 * * ? *`	Spustí se každý den ve 12pm (v poledne).
`R 0 0 * * ? *`	Spustí každý den v 00:00, ale v náhodnou sekundu (0-59).
`R R R 15W * ? *`	Spustí se každý měsíc v 15. den v náhodný čas (sekundu, minutu, hodinu). V případě, že 15. připadne na sobotu, podmínka se spustí v pátek 14. V případě, že 15. připadne na neděli, podmínka se spustí v pondělí 16.
`0 15 10 * * ? 2016`	Spustí se každý den v 10:15am po celý rok 2016.
`0 * 14 * * ? *`	Spustí se každou minutu mezi 2pm a 2:59pm, každý den.
`0 0/5 14 * * ? *`	Spustí se každých 5 minut mezi 2pm a 2:55pm, každý den.
`0 0/5 14,18 * * ? *`	Spustí se každých 5 minut mezi 2pm a 2:55pm, a každých 5 minut mezi 6pm a 6:55pm, každý den.
`0 0-5 14 * * ? *`	Spustí se každou minutu mezi 2pm a 2:05pm, každý den.
`0 10,44 14 ? 3 WED *`	Spustí se v 2:10pm a 2:44pm, každou středu v březnu.
`0 15 10 ? * MON-FRI *`	Spustí se v 10:15am v pondělí, úterý, středu, čtvrtek a pátek.
`0 15 10 15 * ? *`	Spustí se v 10:15am každý 15. den v měsíci.
`0 15 10 ? * 5L *`	Spustí se v 10:15am poslední pátek v měsíci.
`0 15 10 ? * 5L 2016-2020`	Spustí se v 10:15am poslední pátek v měsíci v roce 2016, 2017, 2018, 2019 a 2020.
`0 15 10 ? * 5#3 *`	Spustí se v 10:15am třetí pátek v měsíci.
`0 0 * * * ? *`	Spustí se opakovaně každou hodinu.

Rozšířená nastavení - Zabránění aktivace podmínky spuštění

Throttling se používá v případech, kdy potřebujete omezit spouštění úlohy. Obvykle v případě úloh, jejichž podmínka spuštění je vázána na se opakující událost. Každá podmínka spuštění je vyhodnocována podle níže uvedeného schématu. Ke spuštění úlohy dojde pouze při splnění všech definovaných podmínek. Pokud nejsou definovány žádná kritéria pro zabránění aktivace podmínky spuštění, úloha se vždy spustí. Časově definované podmínky mají přednost před statistickými podmínkami



K dispozici jsou následující podmínky:

- **Časové kritérium**
- **Statistické kritérium**
- **Kritérium protokolu událostí**

Aby došlo k aktivaci podmínky a spuštění úlohy:

- Musí být splněny všechny podmínky.
- Všechny podmínky musí být definovány. Pokud je jedna prázdná, bude přeskočena.
- Všechny časové podmínky musí být splněny – jsou vyhodnocovány logickým operátorem **AND**.
- Při použití logického operátoru **AND** musí být splněny všechny statistické podmínky. Při použití operátoru **OR** musí být splněna alespoň jedna statistická podmínka.
- Statistické i časové podmínky musí být splněny – jsou vyhodnocovány logickým operátorem **AND**.

Pokud jsou všechny podmínky splněny, stavové informace všech observerů se vynulují. To platí pro časové i statistické podmínky. Informace se také resetují při restartování agenta nebo ESET PROTECT Serveru. K resetování dojde také při každé změně podmínky spuštění. Doporučujeme vždy používat jednu statistickou podmínky a více časových. Více statistických podmínek může vést k neočekávaným spuštěním úlohy.

Předvolba

K dispozici jsou tři předdefinované předvolby. Po vybrání předvolby se přepíše výchozími hodnotami vámi zadané nastavení pro zabránění nadměrné aktivace podmínky spuštění. Načtené hodnoty si můžete dle potřeby modifikovat, ale není možné vytvářet vlastní předvolby.

Časové kritérium

Časové období (T2) – definujte časový úsek, za který chcete podmínku aktivovat pouze jednou. Například zadáte-li 10 sekund a během této doby se událost vyskytne vícekrát, k aktivaci podmínky dojde pouze jednou.

> Pro zabránění spuštění úlohy častěji, než jednou za 15 minut, je nutné nastavit časové kritérium (restrikce znázorněna ikonou zámku 🔒):
> • Serverové úlohy (včetně generování přehledu) – všechny typy podmínek spuštění.
> • Klientské úlohy – **naplánované** typy podmínek spuštění a definované pomocí **CRON výrazu**.

Naplánovat (T1) – definujte časové úseky pro aktivaci podmínky. Po kliknutí na **Přidat období** se zobrazí dialogové okno , ve kterém můžete definovat rozsah času, opakování a další parametry dle vybraných parametrů Zadejte vámi požadovaný **rozsah času**. Z menu **Opakování** vyberte jednu z možností a dále nastavte zobrazené možnosti. Sledované období můžete definovat také CRON výrazem. Parametry uložíte kliknutím na tlačítko **OK**. Přidat můžete více rozsahů– řazeny jsou chronologicky.

Pro aktivaci podmínky musí být splněna všechna definovaná kritéria.

Statistické kritérium

Podmínka – statistické podmínky můžete kombinovat:

- **Odeslat oznámení při splnění všech statistických kritérií** - při vyhodnocování je použit logický operátor **OR**.
- **Odeslat oznámení při splnění alespoň jednoho statistického kritéria** – při vyhodnocování je použit logický operátor **OR**.

Počet výskytů (S1) – povoleno bude pouze každé X-té provedení. Například zadáte-li hodnotu 10, započítán bude pouze každý desátý tik.

Počet výskytů ve sledovaném období

Počet výskytů (S2) – započítány budou pouze tiky ve stanoveném období. Tímto definujete minimální opakování události pro spuštění úlohy. Například zadáte-li hodnotu 10, povolíte spuštění úlohy, pokud se událost ve sledovaném období vyskytla 10krát. Čítač se vynuluje při každém aktivování podmínky.

Časové období – zadejte období, ve kterém chcete výskyty sledovat.

Třetí statistické kritérium (kritérium protokolu událostí) je dostupné pouze pro některé typy podmínek spuštění. Přejděte do sekce **Podmínka spuštění** > **Typ podmínky spuštění** > **Šablona protokolu událostí**.

Kritéria protokolu

Toto kritérium vyhovuje ESET PROTECT jako třetí statistické kritérium (S3). Operátor (AND / OR) definovaný v sekci **Použití statistického kritéria** se aplikuje na všechny tři statistické podmínky. Toto kritérium doporučujeme použít při definování serverové úlohy na **Generování přehledu**. Při sestavování kritéria musíte vyplnit všechna níže uvedená pole. Při aktivaci podmínky dojde k resetování čítače.

Podmínka – definujte události nebo sadu událostí, které aktivují podmínku. Dostupné možnosti:

- **Vyskytne se po sobě v řadě** – definujte počet událostí, které se musí pro aktivaci podmínky vyskytnout po sobě v řadě. Události musí být unikátní.
- **Vyskytne se od posledního výskytu** – definujte počet událostí, které se mají vyskytnout, aby došlo k aktivaci podmínky.

Počet výskytů – zadejte číslo, reprezentující počet charakteristických událostí s daným symbolem, které se mají vyskytnout pro aktivaci podmínky.

Symbol – v závislosti na vybraném typu definujte **symbol**, který se bude v protokolu vyhledávat, který je použit v **podmínce spuštění**. Pro zobrazení nabídky klikněte na **Vybrat**. Symbol můžete odstranit kliknutím na **Odebrat**.

> Pokud použijete kritérium protokolu při definování podmínky spuštění serverové úlohy, do vyhodnocování jsou zahrnuty data za všech zařízení. To může vést k velkému množství unikátních symbolů v řadě. Použití možnosti **Vyskytne se po sobě v řadě** volte výhradně v případě, kdy to má smysl. Chybějící hodnota (N/A) nebude považována za "unikátní", proto v takovém případě dojde k resetování čítače.

Další parametry

Jak je popsáno výše, ne každý výskyt události aktivuje podmínku spuštění. Možné akce pro události, které neaktivovaly podmínku:

- Pokud došlo k přeskočení více než jedné události, seskupí se **N** událostí do jedné (uložená data potlačených tiků) [**N** <= 100].
- Pokud se **N** == 0, zpracuje se pouze poslední událost (**N** znamená historii výskytů, kdy je vždy zpracována poslední událost).
- Sloučí se všechny události, které neaktivovaly podmínku spuštění (poslední tik se sloučí s **N** historickými tiky).

V případě, že se podmínky spuštění aktivují příliš často, zkuste postupovat podle následujících kroků:

- Pokud chcete podmínku aktivovat pouze v případě, že se vyskytne více stejných událostí, nikoli jedna, použijte statistické kritérium S1.
- Pokud chcete podmínku aktivovat pouze při výskytu clusteru událostí, použijte statistické kritérium S2.
- Pokud chcete ignorovat události s nechtěnými hodnotami, použijte statistické kritérium S3.

• Pokud chcete ignorovat události, které se vyskytují v čase, který pro vás není relevantní (například pracovní hodiny), použijte časové kritérium T1.

• Pro nastavení minimálního časového intervalu mezi dvěma podmínkami spuštění použijte časové kritérium T2.

> Jednotlivé podmínky můžete libovolně kombinovat a vytvořit tak komplexní scénáře pro aktivaci podmínky spuštění úlohy. Více informací a příklady použití naleznete v této kapitole.

Příklady

Na těchto příkladech si ukážeme, jak jsou podmínky pro zabránění aktivace (T1, T2, S1, S2, S3) spojovány a vyhodnocovány.

> "Tik" představuje impuls pro podmínku spuštění. "T" představuje časové kritérium, "S" představuje statistické kritérium. "S3" představuje kritérium protokolu událostí.

S1: Kritérium pro počet výskytů (povolit každý třetí tik)

Čas	00	01	02	03	04	05	06	Změna podmínky spuštění	07	08	09	10	11	12	13	14	15
Tiky	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: Kritérium pro počet výskytů ve stanovený časový interval (povolit, pokud se vyskytnou 3 tiky během 4 sekund)

Čas	00	01	02	03	04	05	06	Změna podmínky spuštění	07	08	09	10	11	12	13
Tiky	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Kritérium pro unikání hodnoty (povolit, pokud se vyskytnou v řadě 3 unikátní hodnoty)

Čas	00	01	02	03	04	05	06	Změna podmínky spuštění	07	08	09	10	11	12	13
Hodnota	A	B	B	C	D	G	H		J	K	n/a	L	M	N	N
S3					1									1	

S3: Kritérium pro unikání hodnoty (povolit, pokud se od posledního tiku vyskytnou 3 unikátní hodnoty)

Čas	00	01	02	03	04	05	06	07	Změna podmínky spuštění	08	09	10	11	12	13	14
Hodnota	A	B	B	C	D	G	H	I		J	K	n/a	L	M	N	N
S3				1			1						1			

T1: Povolit tiky ve stanový časový interval (každý den v 8:10 po dobu 60 sekund)

Čas	8:09:50	8:09:59	8:10:00	8:10:01	Změna podmínky spuštění	8:10:59	8:11:00	8:11:01
Tiky	x	x	x	x		x	x	x
T1			1	1		1		

Toto kritérium nemá žádný stav. Změny podmínky nemá žádný vliv na výsledek.

T2: Povolit jeden tik ve stanový časový interval (nejvýše jednou za 5 sekund)

Čas	00	01	02	03	04	05	06	Změna podmínky spuštění	07	08	09	10	11	12	13
Tiky	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Kombinace S1+S2

- S1: každý pátý tik
- S2: 3 tiky během 4 sekund

Čas	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Tiky	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Výsledek			1				1								1		

Výsledek je vyhodnocen jako: S1 (logický OR) S2

Kombinace S1+T1

- S1: S1: každý třetí tik
- T1: T1: každý den v 8:08 po dobu 60 sekund

Čas	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Tiky	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
Výsledek						1			1	

Výsledek je vyhodnocen jako: S1 (logický AND) T1

Kombinace S2+T1

- S2: 3 tiky během 10 sekund
- T1: T1: každý den v 8:08 po dobu 60 sekund

Čas	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Tiky	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	

Čas	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Výsledek							1			

Výsledek je vyhodnocen jako: S2 (logický AND) T1.

Mějte na paměti, že stav S2 se vynuluje pouze v případě, kdy globální výsledek je 1.

Kombinace S2+T2

- S2: 3 tiky během 10 sekund
- T2: T2: nejvýše jeden výskyt za 20 sekund

Čas	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Tiky	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Výsledek			1													1		

Výsledek je vyhodnocen jako: S2 (logický AND) T2.

Mějte na paměti, že stav S2 se vynuluje pouze v případě, kdy globální výsledek je 1.

Instalační balíčky

V této sekci si můžete vytvořit instalační balíčky a skripty pro instalaci ESET Management Agenta. Instalační balíčky uložené v ESET PROTECT Web Console si můžete kdykoli stáhnout.

V hlavním menu konzole přejděte do sekce **Instalační balíčky**, klikněte na tlačítko **Vytvořit instalační balíček** a dále si vyberte cílový operační systém.

Vyberte nastavení instalačního programu, přijměte Licenční ujednání s koncovým uživatelem (EULA) a vyberte jednu z možností distribuce instalačního programu (nastavení instalačního programu a možnosti distribuce se mohou lišit v závislosti na operačním systému):

- Kliknutím na tlačítko **Stáhnout** zahajte stahování instalačního balíčku.
- Kliknutím na ikonu **Kopírovat** zkopírujete odkaz na stažení instalačního balíčku do schránky.
- Kliknutím na ikonu **E-mail** odešlete e-mailem odkaz na stažení instalačního balíčku.

Pomocí možnosti **Přizpůsobit instalační balíček** můžete upravit další parametry instalačního balíčku ještě před jeho stažením:

Windows

- Stáhnout instalační balíček nebo použít ESET Remote Deployment Tool – v průběhu jeho vytváření instalačního balíčku můžete vybrat politiku pro ESET Management Agenta a bezpečnostní produkt, licenci pro aktivaci bezpečnostního produktu a nadřazenou skupinu, do které se stanice zařadí. Instalační balíček můžete následně spustit lokálně nebo použít pro vzdálené nasazení (pomocí ESET Remote Deployment Tool).

- Využít pro nasazení GPO nebo SCCM –Tuto možnost doporučujeme pro nasazení ESET Management Agenta na velké množství počítačů.

macOS

- Stáhnout nebo odeslat instalační balíček – v průběhu jeho vytváření instalačního balíčku můžete vybrat politiku pro ESET Management Agenta a bezpečnostní produkt, licenci pro aktivaci bezpečnostního produktu a nadřazenou skupinu, do které se stanice zařadí.

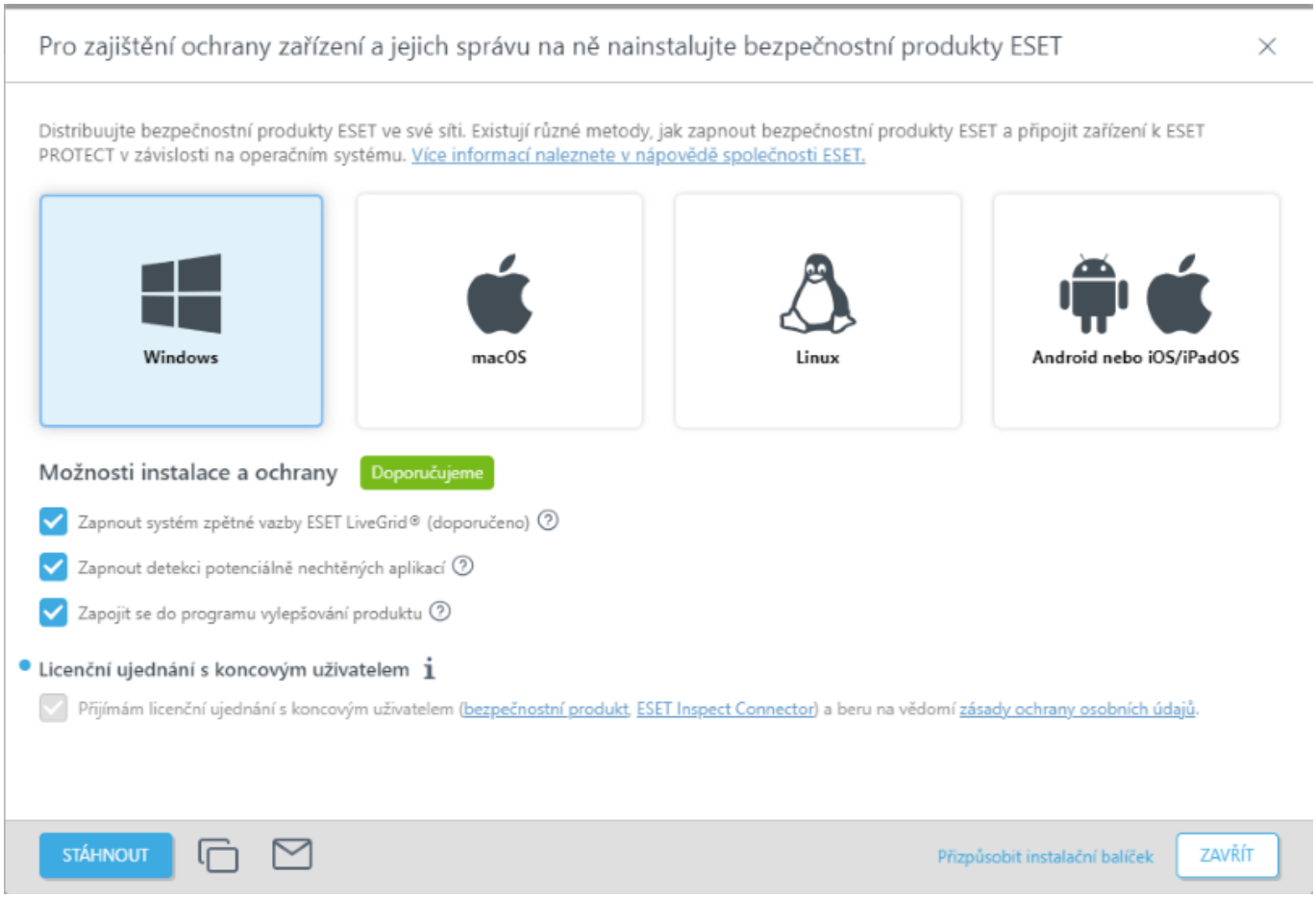
- Nejprve nasadit agenta (instalační skript)Tento způsob instalace agenta je vhodný pro případ, kdy vám nevyhovují jiné metody instalace, případně je nemůžete použít. V tomto případě můžete uživatelům distribuovat instalační skript například prostřednictvím e-mailu nebo výměnných médií, a nechat instalaci na nich. Instalace prostřednictvím instalačního skriptu je bezobslužná, ale uživatel musí mít oprávnění administrátora.

Linux

- Nejprve nasadit agenta (instalační skript)Tento způsob instalace agenta je vhodný pro případ, kdy vám nevyhovují jiné metody instalace, případně je nemůžete použít. V tomto případě můžete uživatelům distribuovat instalační skript například prostřednictvím e-mailu nebo výměnných médií, a nechat instalaci na nich. Instalace prostřednictvím instalačního skriptu je bezobslužná, ale uživatel musí mít oprávnění administrátora.

Android nebo iOS/iPadOS

Tato možnost slouží pro registraci mobilních zařízení v cloudové webové konzoli.



Oprávnění pro přístup k instalačním balíčkům

Aby uživatel mohl vytvářet instalační balíčky a modifikovat stávající, musí mít oprávnění **zápis** pro **Skupiny a počítače** a **Uložené instalační balíčky**.

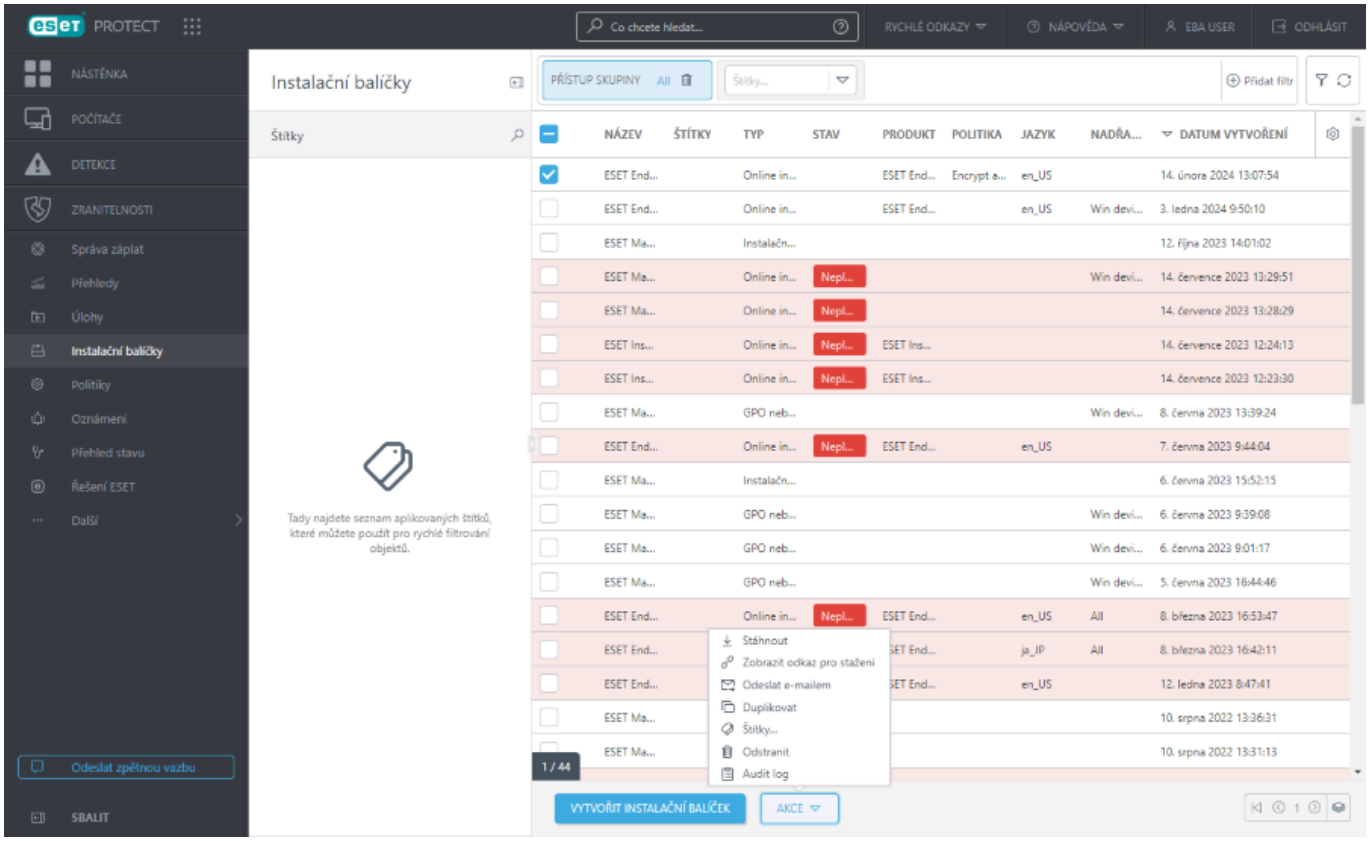
Pro stažení již vytvořených instalačních balíčků potřebuje uživatel oprávnění **Použít** pro **Skupiny a počítače** a **Uložené instalační balíčky**.

- Aby mohl uživatel při tvorbě instalačních balíčků nebo skriptů vybrat **politiku** (v sekci **Rozšířené** > **Počáteční konfigurace** > **Způsob konfigurace**, musí mít oprávnění pro přístup (**Použít**) k **politikám**.
- Aby mohl uživatel při tvorbě instalačního balíčku vybrat licenci, musí mít uživatel oprávnění pro přístup (**Použít**) k **licencím**.
- Výběr Nadřazené skupiny během vytváření instalačního programu nemá vliv na jeho umístění. Po vytvoření instalačního programu dojde k jeho umístění v uživatelském Přístupu skupiny. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Domovská skupina je automaticky detekována na základě přiřazené sady oprávnění právě přihlášeného uživatele.

Příklad:
Právě přihlášený uživatel má oprávnění k **zápisu** u klientské úlohy **Instalace aplikace**. **Domovská skupina** uživatelského účtu je skupina s názvem "Oddělení_1". Pokud uživatel vytváří novou **klientskou úlohu pro instalaci aplikace**, skupina "Oddělení_1" se automaticky vybere jako **domovská skupina**.

Pokud vám předvybraná domovská skupina nevyhovuje, můžete ji ručně změnit.



Jak stáhnout instalační balíček?

1. V hlavním menu přejděte na záložku **Instalační balíčky**.
2. Vyberte balíček, který chcete stáhnout.
3. V kontextovém menu **Akce** klikněte na **Stáhnout**.
4. Instalační balíček najdete ve složce, do které ukládá webový prohlížeč stažené soubory.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Politiky

Prostřednictvím politik vynutíte požadovanou konfiguraci produktů ESET nainstalovaných na koncovém zařízení. Díky tomu nebudete muset konfigurovat jednotlivé stanice ručně. Aplikovat je můžete přímo na konkrétní počítače nebo celé skupiny počítačů (statické i dynamické). Každému počítači nebo skupině můžete přiřadit libovolné množství politik.

Politiky a oprávnění

Pro vytváření a přiřazování politik počítačům a skupinám musí mít uživatel potřebné oprávnění. Níže uvádíme přehled oprávnění, která potřebujete pro konkrétní akce:

- Pro zobrazení seznamu politik včetně jejich konfigurace přiřaďte uživateli oprávnění pro **čtení**.
- Pro přiřazení politiky konkrétnímu objektu musí mít oprávnění **Použít**.
- Pro vytváření a úpravu politik potřebujete oprávnění pro **zápis**.

Více informací naleznete v kapitole seznam oprávnění.

Ikona zámku se zobrazí u politik, které není možné modifikovat. To platí pro některé předdefinované politiky (například politika s názvem Auto-updates nebo ESET LiveGuard politiky) a politiky, které uživatel nemůže měnit, protože nad nimi nemá oprávnění pro **zápis**.

- Uživatel *Jiří* provádí audit politik a potřebuje si zobrazit jejich seznam včetně konfigurace: musí mít nastaveno oprávnění pro **čtení politik**.
- Uživatel *Pavel* potřebuje aplikovat politiky na konkrétní zařízení: musí mít nastaveno oprávnění **Použít** u **politik** a také položky **Skupiny a počítače**.
- Oprávnění pro vytváření politik má standardně pouze předdefinovaný uživatel *Administrator*. Pokud chcete toto oprávnění přidělit dalšímu uživateli, nastavte mu **Zápis** u položky **Politiky**.

Aplikování politik

Politiky se aplikují v pořadí podle statických skupin. Výjimku tvoří dynamické skupiny, kdy se politiky aplikují v opačném pořadí (směrem od potomka k rodiči). Díky tomuto principu můžete vytvářet globální politiky pro statické skupiny a politiky se specifickým nastavením přiřazovat podskupinám. Pomocí příznaků jste schopni konkrétní nastavení produktu vynutit v globální politice a zajistit, že nastavení již nepřepíše žádná ESET PROTECT politika umístěná ve stromu níže. Princip aplikování politik na klienty je popsán v této kapitole.

Odebrání politik

Pokud se rozhodnete politiku odstranit, výsledná konfigurace závisí na verzi použitého bezpečnostního řešení ESET na koncové stanici:

- Pokud odeberete politiku nebo vyberete příznak **Ignorovat** se konfigurace automaticky vrátí na předchozí lokální hodnoty. Pokud stanice přestane být členem dynamické skupiny, na kterou byla aplikována politika, klient již nebude nastavení z dané politiky používat. Toto chování se týká:

Bezpečnostní řešení ESET pro Windows	– verze řešení 7 a novější
Bezpečnostní produkty ESET pro macOS	– verze řešení 7 a novější
Bezpečnostní produkty ESET pro Linux	– verze řešení 8.1 a novější

- Starší bezpečnostní řešení ESET (než je uvedeno výše): Nastavení klienta se nevrátí na původní hodnoty, a zůstane v poslední známé konfiguraci. Nastavení zůstane stejné jako v době, kdy se politika naposledy aplikovala. To samé platí v případě dynamických skupin. Pokud se počítač stane jejím členem a je na ni aplikována politika. Nastavení zůstane beze změny i poté, kdy počítač přestane být členem dynamické skupiny. Z tohoto důvodu doporučujeme vytvořit politiku s výchozím nastavením a přiřadit ji nejnadřazenější

skupině **Všechna zařízení**. Tím zajistíte, že při opuštění dynamické skupiny obdrží počítač výchozí/požadované nastavení.

Slučování politik

Výsledné nastavení, které se aplikuje na klienta, vznikne sloučením všech aplikovaných politik

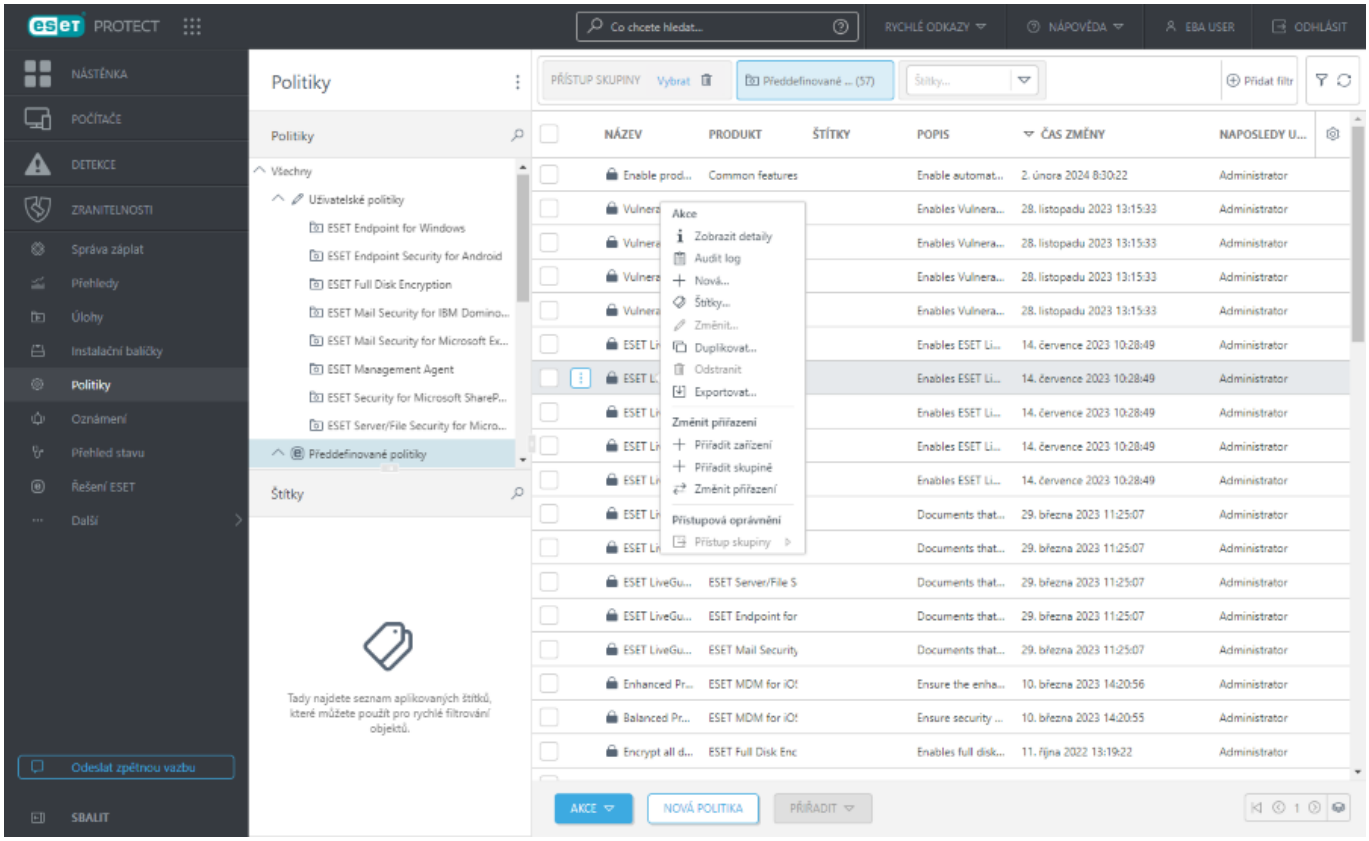
> Doporučujeme vytvářet politiky od obecných (například s nastavením aktualizace serveru) a přiřazovat je globálním skupinám. až po politiky se specifickým nastavením (například blokování výměnných médií) a přiřazovat je podskupinám nebo přímo konkrétním klientům. Důvodem je, že při slučování politik je nastavení dříve aplikované politiky přepsáno nastavením z později aplikované politiky (pokud není v politice řečeno jinak pomocí příznaku).

Průvodce vytvořením nové politiky

Politiky jsou řazeny podle kategorií reprezentovány jednotlivými ESET produkty. Pro přehlednost jsou politiky dále rozděleny na **předdefinované** a **vámi vytvořené (uživatelské)**.

Politiky slouží pro vzdálenou konfiguraci bezpečnostních produktů ESET stejně, jako kdybyste požadované změny prováděli přímo na klientovi v Rozšířeném nastavení. Na rozdíl od politik v Active Directory, politiky v ESET PROTECT neumožňují provádění skriptů ani příkazů.

Pro rychlejší nalezení požadované položky v politice můžete použít vyhledávání. Pokud do vyhledávání zadáte například výraz "HIPS", zobrazí se pouze relevantní sekce. Pokud kliknete v pravé části konfigurační šablony na ikonu , zobrazí se relevantní nápověda daného bezpečnostního produktu.



Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Vytvoření nové politiky

1.Klikněte na tlačítko **Akce** > **Nová**.

2.V této části zadejte obecné informace o vytvářené politice, jako je **název**, a volitelně **popis**. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.

3.Dále z rozbalovacího menu **Produkt** vyberte ESET produkt, pro který chcete vytvořit politiku.

4.Pomocí příznaků určete, jak má politika dané nastavené zpracovat.

5.Vyberte klienty, kterým chcete politiku přiřadit. Po kliknutí na tlačítko **Přiřadit** se zobrazí dialogové okno se všemi statickými i dynamickými skupinami. Vyberte klienty nebo skupiny, na které chcete politiku aplikovat, a klikněte na tlačítko **OK**.

6.Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**.

Příznaky

Každému nastavení v politice můžete přiřadit příznak a ovlivnit výsledné nastavení při jejich slučování. Prostřednictvím příznaku určíte, jak má politika dané nastavení zpracovat.

U každého nastavení můžete použít jeden z následujících příznaků:

Ignorovat – nastavení nebude tuto politikou propsáno na klienta. Může jej uživatel měnit, případně bude přepsáno jinou politikou.

Použít – nastavení s tímto příznakem bude odesláno klientovi. Může být přepsáno politikou, která se aplikuje později. Při aplikování politiky na klienta se nastavení změní na to, které je v politice definované, bez ohledu na to, jak bylo nastavené lokálně. Může jej uživatel měnit, případně bude přepsáno jinou politikou.

Vynutit – nastavení s tímto příznakem má nejvyšší prioritu a nemůže být přepsáno jinou politikou uplatňovanou později (i v případě, že má stejný příznak). To zajistí, že se nastavení nezmění ani po sloučení všech politik.

Pro snadnější orientaci v konfiguraci se u každé sekce zobrazuje číslo. Toto číslo reprezentuje počet nastavení, která jste v dané sekci vynutili, a chcete je na klientské stanici aplikovat. Zároveň se další číslo zobrazuje vedle názvu jednotlivých kategorií (ve stromové struktuře vlevo). Toto číslo reprezentuje počet nastavení ve všech podsekcích. Tímto způsobem snadno zjistíte, kolik nastavení/pravidel aplikujete.

Pro pohodlnější konfiguraci produktu můžete:

- **Aplikovat** všechna nastavení v dané sekci pomocí ikonky ,
- Odstranit všechny příznaky v dané sekci pomocí ikonky **Ignorovat**.

Doporučujeme prostudovat informace týkající se odebrání politik a vliv této akce na konfiguraci produktu.

Jak uživatelům přidělit přístup ke všem politikám:

Administrator chce *Filipovi* přidělit oprávnění pro vytváření i úpravu politik v jeho skupině a zároveň chce, aby Filip viděl politiky, které *Administrator* vytvořil. Politiky, které vytvořil *Administrator*, budou mít příznak **Vynutit**. Uživatel *Filip* uvidí všechny politiky, ale není schopen upravovat politiky, které vytvořil *Administrator*. Je to z důvodu, že má nad statickou skupinou *Všechna zařízení* pouze **oprávnění pro čtení politik**. Dále *Filipovi* přidělíme oprávnění pro vytváření politik v jeho domovské skupině *San Diego*. *Administrator* musí provést tyto kroky:

Vytvoření prostředí

1.Vytvoří novou statickou skupinu s názvem *San Diego*.

2.Vytvoří novou sadu oprávnění s názvem *Politiky – Všechna zařízení – Filip*, ve které jako statickou skupinu nastaví *Všechna zařízení* a u položky **Politiky** nastaví oprávnění **Číst**.

3.Vytvoří novou sadu oprávnění s názvem *Filipovi politiky,* ve které jako statickou skupinu nastaví *San Diego*. Dále u položky **Politiky** a **Skupiny a počítače** nastaví oprávnění **Zápis**. Toto oprávnění umožní *Filipovi* vytvářet a upravovat politiky v jeho domovské skupině (San Diego).

4.Vytvoří nového uživatele s názvem *Filip* a v sekci **Sady oprávnění** vybere *Politiky – všechna zařízení – Filip* a *Politiky Filip*.

Vytvoření politik

5.Vytvoří novou politiku s názvem *Všichni – Zapnout firewall*. V sekci **Nastavení** vybere z rozbalovacího menu **ESET Endpoint for Windows**. V konfigurační šabloně přejde do větve **Síťová ochrana** > **Firewall** > **Obecné** a u všech nastavení kliknutím na aplikuje příznak **Vynutit**. V sekci **Přiřadit** vybere skupinu *Všechna zařízení*.

6.Vytvoří novou politiku s názvem *Filip – Zapnout firewall*. V sekci **Nastavení** vybere z rozbalovacího menu **ESET Endpoint for Windows**. V konfigurační šabloně přejde do větve **Síťová ochrana** > **Firewall** > **Obecné** a u všech nastavení aplikuje příznak **Použít**. V sekci **Přiřadit** vybere skupinu *San Diego*.

Výsledek

Politiky, které vytvořil *Administrator* se aplikují jako první, protože jsou přiřazeny nejnadřazenější skupině *Všechna zařízení*. Nastavení s příznakem **Vynutit** má nejvyšší prioritu a nemůže být přepsáno politikou aplikovanou později. Následně se aplikují politiky vytvořené *Filipem*.

Přejděte do sekce **Další** > **Skupiny**. Vyberte skupinu **San Diego**, klikněte na konkrétní počítač a z kontextového menu vyberte možnost **Zobrazit detaily**. Následně přejděte na záložku **Konfigurace** > **Aplikované politiky** a uvidíte výsledné pořadí aplikovaných politik.

POŘAD...	PRODUKT	NÁZEV POLITIKY	POPIS POLITIKY
1 (aplikuje se jak...	Common features	Enable produ...	Enable automatic...
2	ESET Endpoint fo...	Protection se...	This policy enabl...

První politiku vytvořil *Administrator*, druhou *Filip*.

Domovská skupina je automaticky detekována na základě přiřazené sady oprávnění právě přihlášeného uživatele.

Příklad:
Právě přihlášený uživatel má oprávnění k **zápisu** u klientské úlohy **Instalace aplikace**. **Domovská skupina** uživatelského účtu je skupina s názvem "Oddělení_1". Pokud uživatel vytváří novou **klientskou úlohu pro instalaci aplikace**, skupina "Oddělení_1" se automaticky vybere jako **domovská skupina**.

Pokud vám předvybraná domovská skupina nevyhovuje, můžete ji ručně změnit.

Správa politik

Politiky jsou řazeny podle kategorií reprezentovány jednotlivými ESET produkty. Pro přehlednost jsou **politiky dále rozděleny na předdefinované** a vámi vytvořené (uživatelské).

Seznam dostupných akcí nad politikami:

Zobrazit detaily	Kliknutím si zobrazíte detailní informace o vybrané politice.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Nová...	Po kliknutí se zobrazí průvodce pro vytvoření nové politiky.
Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
Změnit...	Kliknutím upravíte již existující politiku.
Duplikovat...	Po kliknutí vytvoříte kopii již existující politiky. Vyžadováno je pouze zadání nového názvu.
Změnit přiřazení	Prostřednictvím této možnosti přiřadíte politiku klientovi nebo skupině klientů.
Odstranit...	Kliknutím odstraníte vybranou politiku. Doporučujeme prostudovat informace týkající se odebrání politik a vliv této akce na konfiguraci produktu.
Importovat...	Klikněte na tlačítko **Politiky** > **Importovat** a **vyberte soubor**, který chcete importovat. Prostřednictvím této možnosti můžete naimportovat zálohované politiky z externího *.dat* souboru, který jste dříve exportovali z ESET PROTECT Web Console. Není možné importovat *.xml* soubor, který obsahuje nastavení exportované z koncového bezpečnostního produktu ESET. Importované politiky se zobrazí v sekci **Uživatelské politiky**.
Exportovat...	Pomocí zaškrtávacího pole vyberte politiky, které chcete exportovat, klikněte na tlačítko **Akce** a vyberte možnost **Exportovat...**. Následně se politiky exportují do *.dat* souboru. Pro exportování všech politik v dané kategorii klikněte na zaškrtávací pole v záhlaví tabulky.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Jak se politiky aplikují na klienta

Skupiny a počítače mohou mít přiřazeno libovolné množství politik. Počítač se může nacházet hluboko ve stromové struktuře, kdy na každou ze skupin se aplikují samostatné politiky.

Nejdůležitějším kritériem pro aplikování politiky (výsledného nastavení) je jejich pořadí. To je odvozeno od pořadí skupiny a pořadí, ve kterém jsou politiky na skupinu aplikovány.

Pro zobrazení všech politik, které se na dané zařízení aplikují, přejděte v detailech počítače na záložku Aplikované politiky.

Výsledná politika, která se na klienta aplikuje, se sestaví po provedení následujících kroků:

1. Zjištění pořadí skupin, ve kterých se klient nachází,
2. Načtení politik ze všech skupin, ve kterých se klient nachází,
3. Sloučení politik do výsledné politiky.

Pořadí skupin

Politiky mohou být přiřazeny skupinám **a aplikovány v požadovaném pořadí. Při zjišťování pořadí politik, ve kterém se budou aplikovat na koncové zařízení, se používají níže uvedená pravidla.**

Pravidlo 1: Statické skupiny jsou vyhodnocovány od svého kořene, tedy nejnadřazenější statické skupiny **Všechna zařízení**.

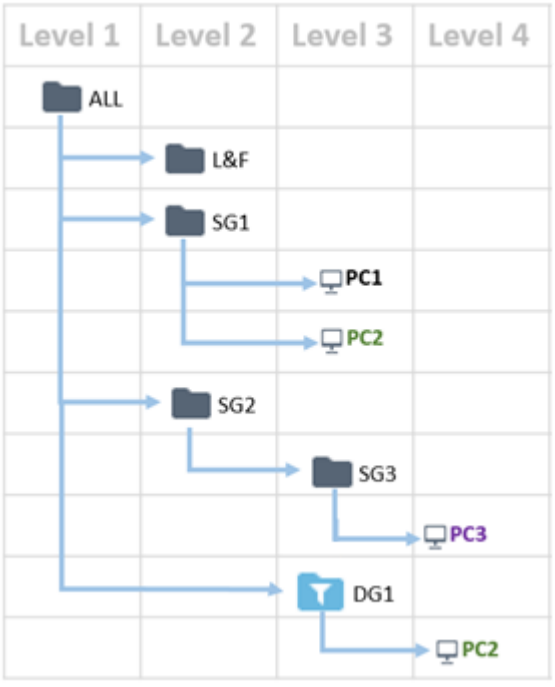
Pravidlo 2: V každém uzlu jsou nejprve prohledány statické skupiny, dle jejich pořadí – podle algoritmu prohlídka do šířky.

Pravidlo 3: Po projití všech statických skupin v daném uzlu se prochází dynamické skupiny.

Pravidlo 4: Prochází se všichni potomci dynamické skupiny, podle jejich pořadí.

Pravidlo 5: Prohlídka stromu končí u klientského zařízení.

Politika se aplikuje na počítač. To znamená, že prohlídka stromu končí u počítače, na který se má aplikovat.



Na základě výše uvedených pravidel se na počítače aplikují politiky v tomto pořadí:

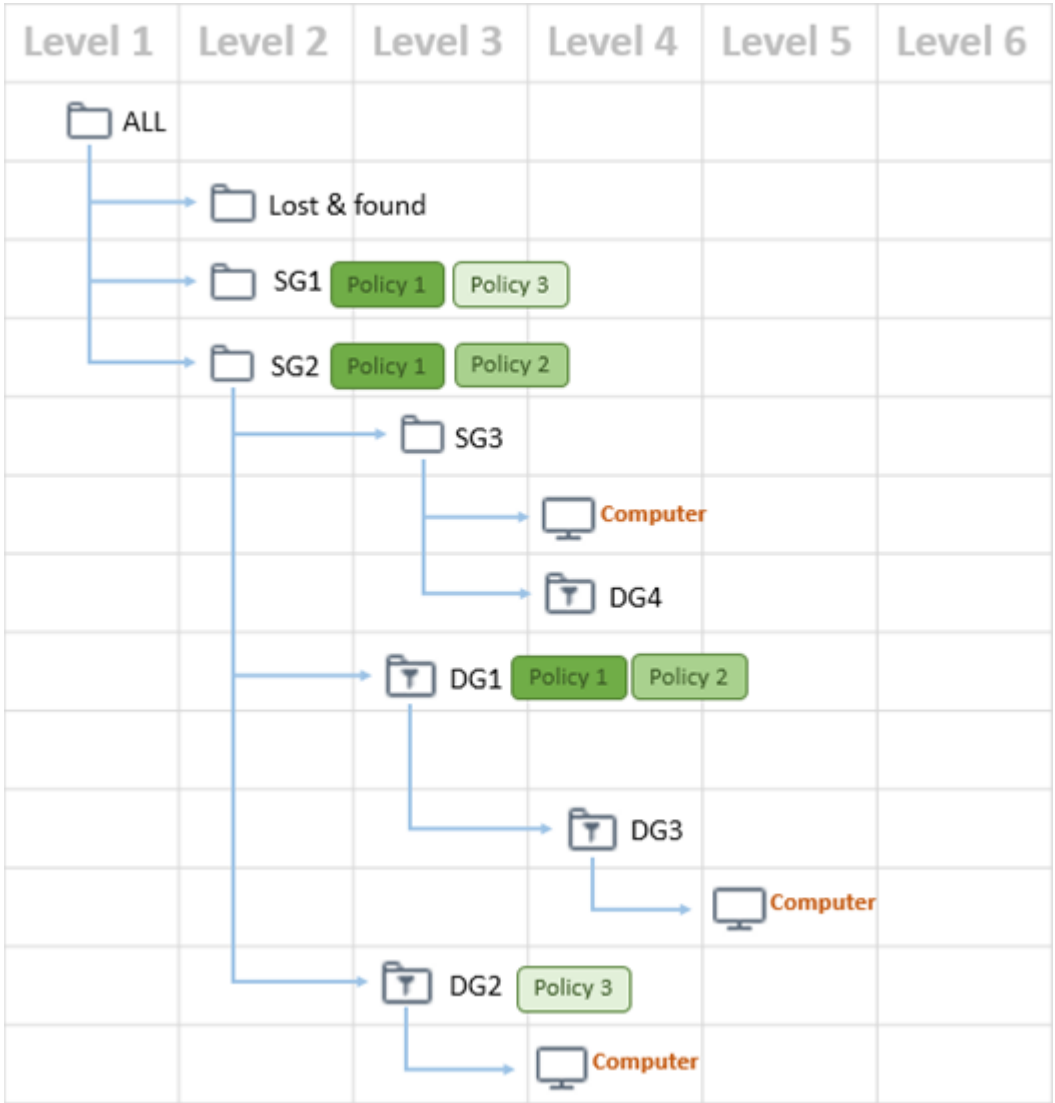
PC1:	PC2:	PC3:
1.ALL 2.SG1 3.PC1	1.ALL 2.SG1 3.DG1 4.PC2	1.ALL 2.SG2 3.SG3 4.PC3

Získání seznamu politik

Po získání seznamu skupin dojde k načtení politik, které mají dané skupiny přiřazeny. Politiky se načítají ve stejném pořadí, v jakém jsou aplikovány na skupiny. Prioritu (pořadí) politiky můžete měnit. Každá politika je platná pro konkrétní produkt (ESET Management Agent, ESET Endpoint Security…).

Pokud skupina nemá přiřazenou žádnou skupinu, bude ze seznamu odstraněna.

Statickým i dynamickým skupinám máme v našem případě přiřazeny tři politiky (viz obrázek):



Pořadí, ve kterém se politiky aplikují na počítač

V níže uvedeném seznamu jsou uvedeny skupiny a k nim přiřazené politiky.

1. Všechna zařízení – odstraníme ze seznamu, protože neobsahuje žádnou politiku
2. Statická skupina 2 – získáme Politiku 1 a 2
3. Statická skupina 3 – odstraníme ze seznamu, protože neobsahuje žádnou politiku
4. Dynamická skupina 1 – získáme Politiku 1 a 2
5. Dynamická skupina 3 – odstraníme ze seznamu, protože neobsahuje žádnou politiku
6. Dynamická skupina 2 – získáme Politiku 3
7. Dynamická skupina 4 – odstraníme ze seznamu, protože neobsahuje žádnou politiku
8. Počítač – odstraníme ze seznamu, protože neobsahuje žádnou politiku

Finální seznam politik, které se budou na klienta aplikovat:

1. Politika 1
2. Politika 2
3. Politika 1
4. Politika 2
5. Politika 3

Slučování politik

Pokud je na produkt ESET již aplikována jiná politika, při aplikování další dojde ke sloučení stejných nastavení. Politiky se slučují postupně. Při slučování pravidel platí pravidlo, že nastavení z naposledy načtené politiky přepisuje nastavení z dříve načtené politiky. Pro změnu tohoto chování, resp. vynucení konkrétního nastavení, můžete použít příznaky. U seznamů může být dále nastaveno, co se má při sloučení stát – zda dojde k nahrazení, přidání záznamů na začátek nebo konec).

Mějte na paměti, že výslednou nastavení ovlivňuje hierarchie skupin a pořadí politik. Sloučení dvou politik může vrátit odlišný výsledek, pokud změníte jejich pořadí.

V případě seznamů (výjimek, pravidel firewallu, ...) se můžete rozhodnout co se stane, pokud bude stejná položka definována ve více politikách. Tímto můžete stejné nastavení definovat ve více politikách.

- **Nahradit** – výchozí pravidlo, které se použije při slučování politik. Znamená, že každá později aplikovaná politika přepíše seznam položek definovaný v dříve aplikované politice.
- **Připojit** – pokud se aplikuje stejné nastavení ve více politikách, toto pravidlo umožňuje tato nastavení přidat nakonec. Definované záznamy z této politiky se přidají na konec seznamu, který vznikne sloučením politik.

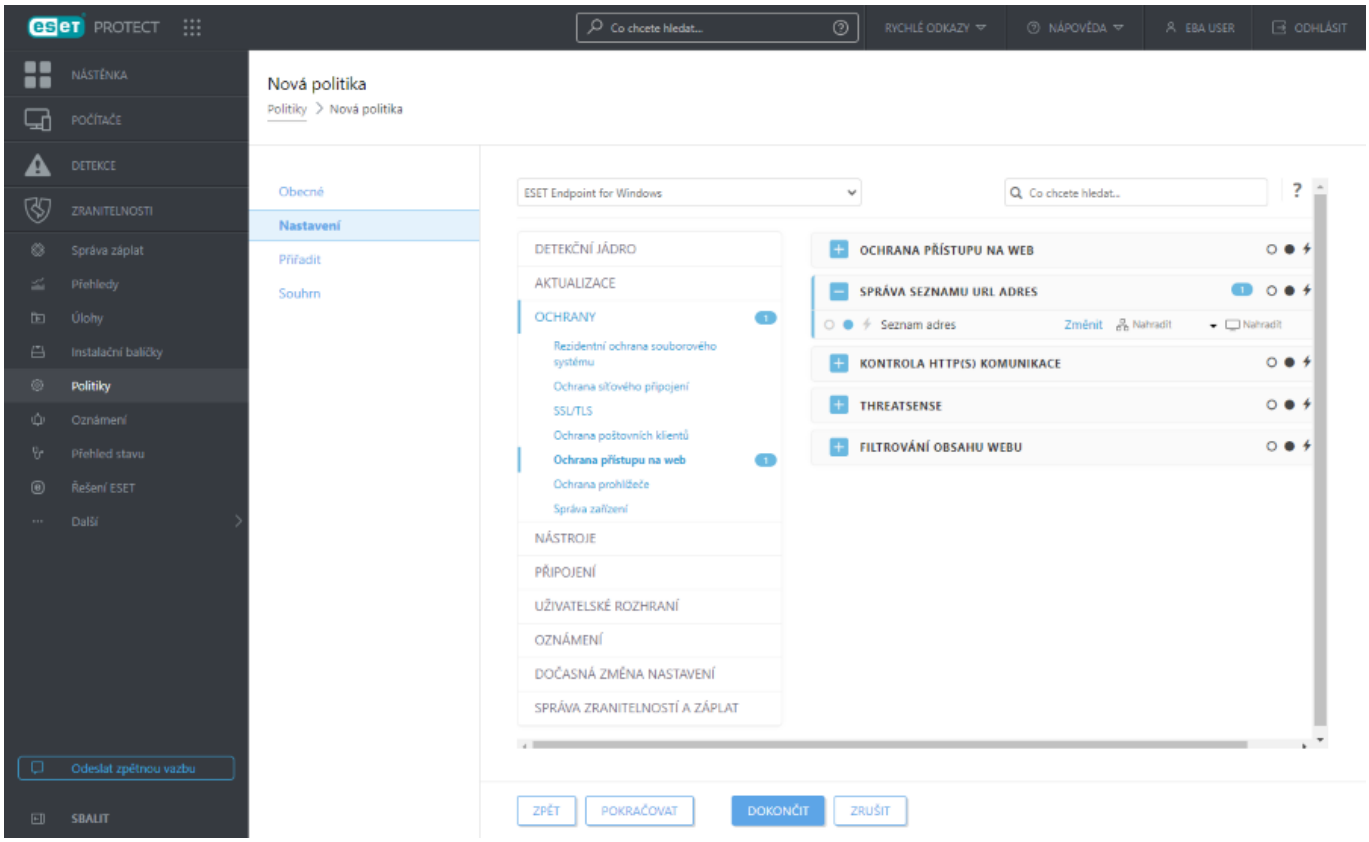
• **Přidat na začátek** – pokud se aplikuje stejné nastavení ve více politikách, toto pravidlo umožňuje tato nastavení přidat na začátek. Definované záznamy z této politiky se přidají na začátek seznamu (budou tedy nadřazeny ostatním položkám/pravidlům), který vznikne sloučením politik.

Sloučení lokálních seznamů se seznamy definovanými v politikách

Poslední verze bezpečnostních produktů ESET (seznam podporovaných verzí naleznete v tabulce níže) přináší podporu slučování seznamů definovaných na lokální stanici se seznamy definovanými prostřednictvím politik. Standardně se seznamy (například webových stránek) definované na lokální stanici přepíší seznamy definovanými v politice. V případě potřeby můžete definovat, jak se oba seznamy sloučí. Definovat můžete následující možnosti slučování:

• tato ikonka představuje možnosti pro slučování politik

• tato ikonka představuje možnosti pro slučování lokálního nastavení s politikami
Možnosti sloučení jsou stejné: **Nahradit**, **Přidat na začátek**, **Přidat na konec**.



Doporučujeme prostudovat informace týkající se odebrání politik a vliv této akce na konfiguraci produktu.

Příklad slučování politik

V tomto příkladu si ukážeme a vysvětlíme:

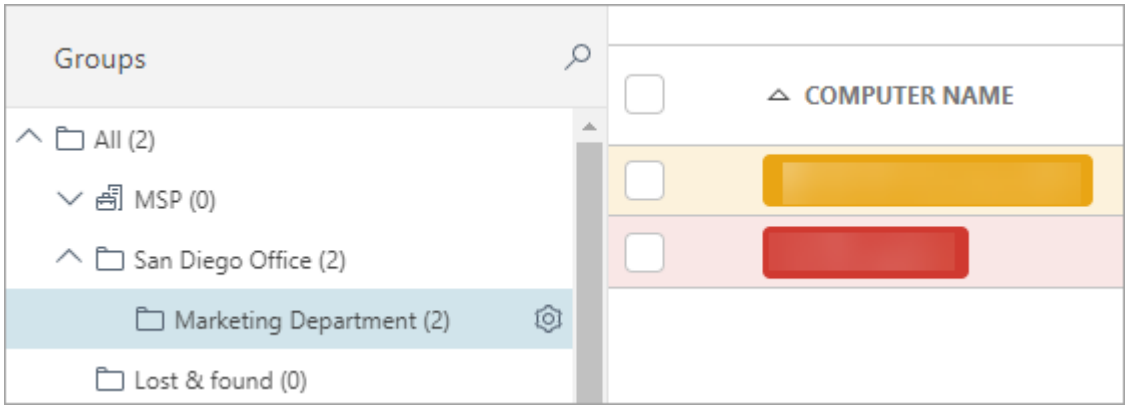
• Jak aplikovat politiku na ESET Endpoint,

• Jak fungují příznaky a slučují se seznamy.

Uživatel *Administrator* chce docílit následujícího stavu:

- Zakázat pobočce *San Diego* přístup na webové stránky *www.forbidden.uk, www.deny-access.com, www.forbidden-websites.ukwww.forbidden-website.com*.

- Povolit *Marketingovému oddělení* přístup na stránky *www.forbidden.uk, www.deny-access.com*.



Administrator musí provést tyto kroky:

1. *Administrator* již má vytvořenou statickou skupinu *San Diego office* a *Marketing department*, která je jejím potomkem.

2. V hlavním menu v sekci **Politiky** vytvoří novou politiku:

   i)Pojmenuje ji *San Diego office*.

   ii)V sekci **Nastavení** vybere **ESET Endpoint for Windows.**

   iii)Přejděte na **Ochrany** > **Ochrana přístupu na web** > **Správa seznamu URL adres**

   iv)Kliknutím na možnost **Změnit** se u dané položky zvýrazní příznak (**Použít**).

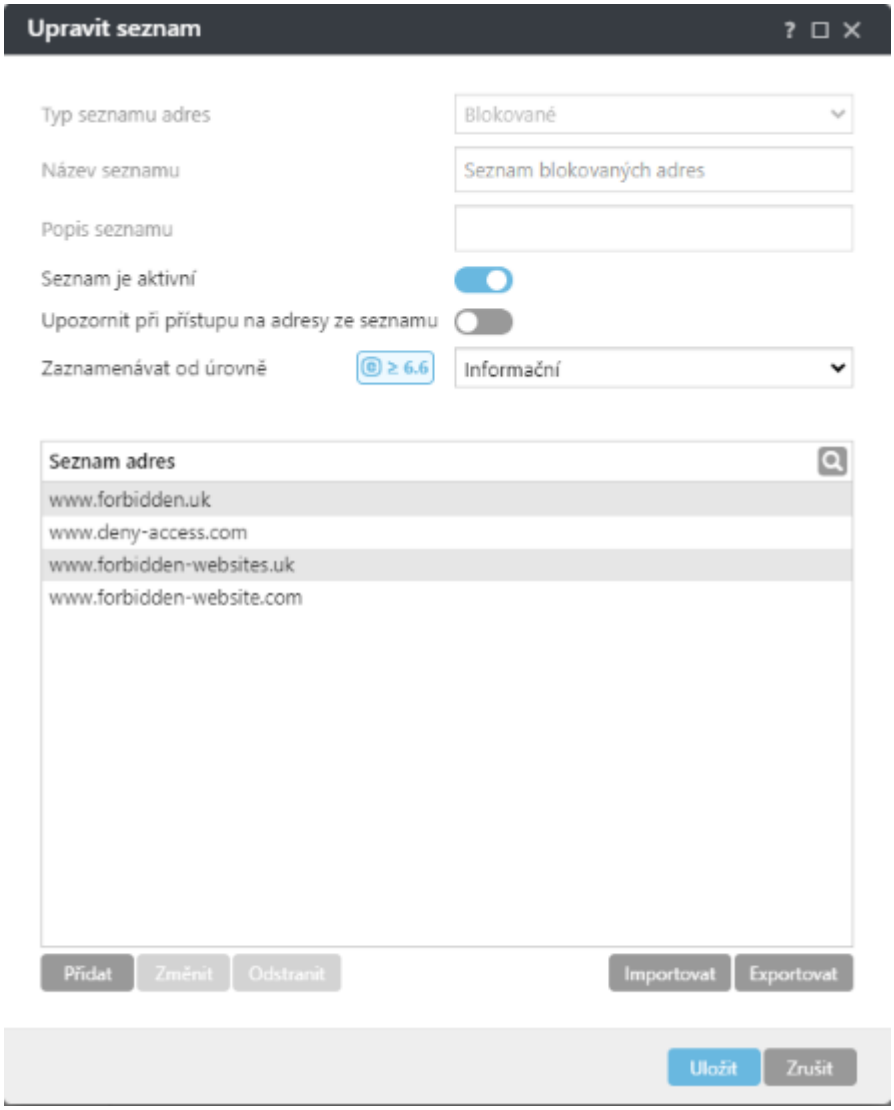
   v)V zobrazeném okně vybere **Seznam blokovaných adres** a klikne na tlačítko **Změnit**.

   vi)Do seznamu přidá požadované adresy: *www.forbidden.uk, www.deny-access.com, www.forbidden-websites.uk, www.forbidden-website.com*. Uloží seznam blokovaných webových stránek.

   vii) V sekci **Přiřadit** vybere statické skupiny *San Diego Office* a její podskupinu *Marketing Department.*

   viii) Vytvoření politiky potvrdí kliknutím na tlačítko **Dokončit**.

Prostřednictvím této politiky zakázal administrátor přístup na definované stránky ze zařízení, která se nachází ve statické skupině *San Diego office* a *Marketing department*.

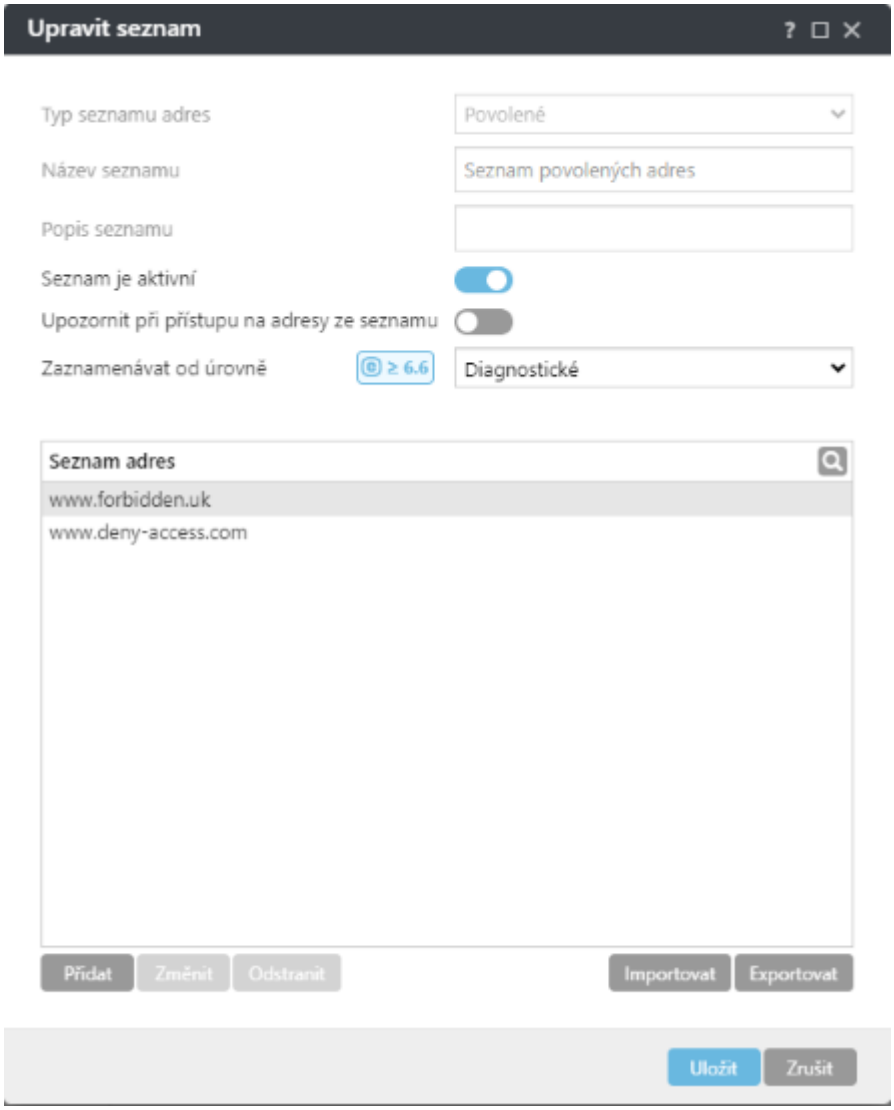


3. Pro povolení přístupu marketingovému oddělení na vybrané adresy musí administrátor vytvořit další **politiku**.

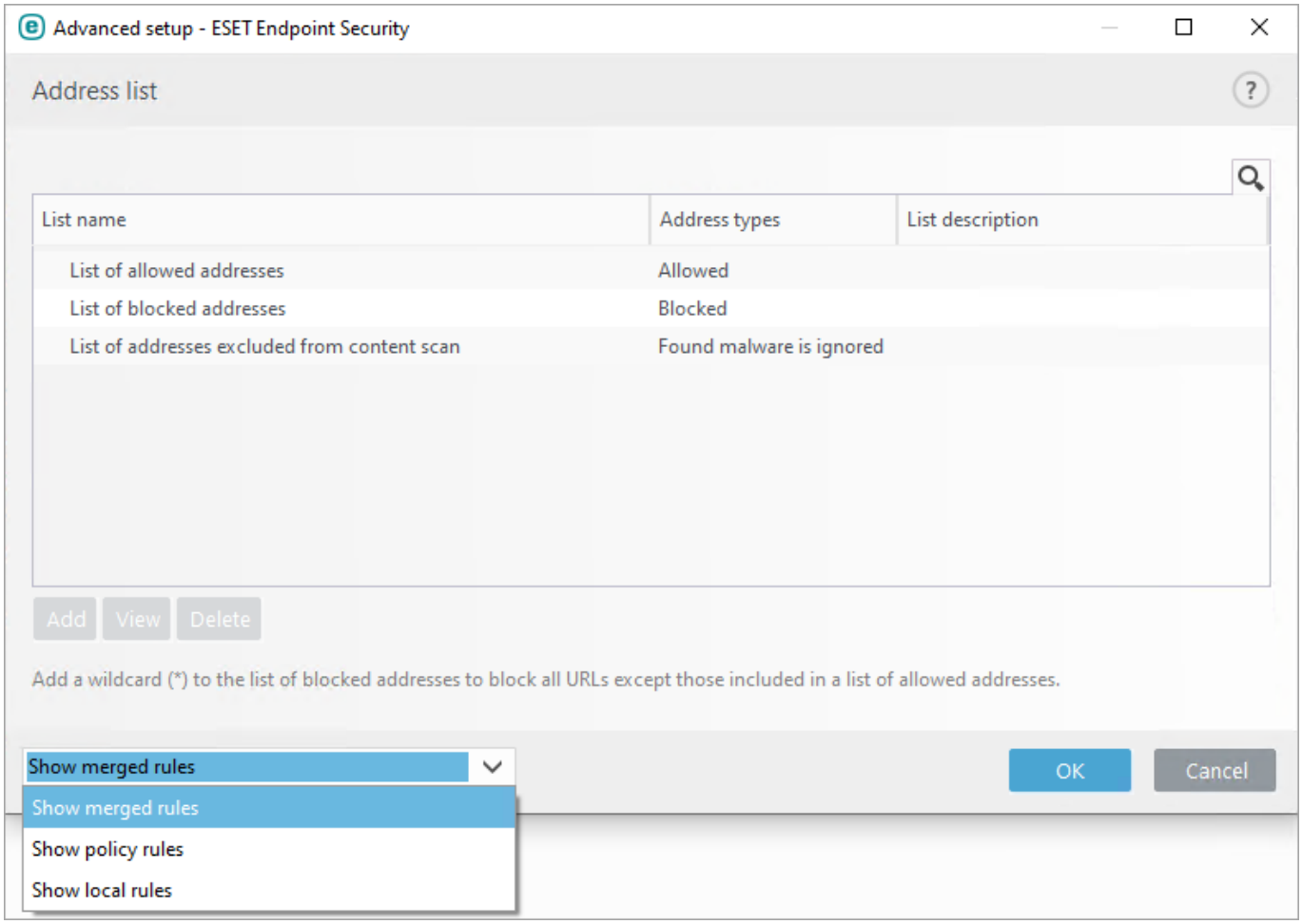
i)Pojmenujte ji *Marketing department*.
ii)V sekci **Nastavení** vybere **ESET Endpoint for Windows.**
iii)Přejděte na **Ochrany** > **Ochrana přístupu na web** > **Správa seznamu URL adres**
iv)Klikne na ikonu (**Použít**), **vybere možnost** přidat na začátek a klikne na tlačítko **Změnit**. Tím zajistí, že se při sloučení politik položky nepřepíší, ale přidají se na začátek existujícího seznamu.
v)V zobrazeném okně vybere **Seznam blokovaných adres** a klikne na tlačítko **Změnit**.
vi)Do seznamu přidá požadované adresy: *www.forbidden.uk*, *www.deny-access.com*. Uloží seznam povolených webových stránek.
vii) V sekci **Přiřadit** vybere statickou skupinu *Marketing Department.*

viii) Vytvoření politiky potvrdí kliknutím na tlačítko **Dokončit**.

Prostřednictvím této politiky povolil administrátor přístup na definované stránky ze zařízení, která se nachází ve statické skupině *Marketing department*.



4. Výsledná konfigurace bude obsahovat seznam adres definovaný v politice *San Diego office* a seznam z politiky *Marketing department*. Otevřete **ESET Endpoint Security** a přejděte do **Nastavení** > **Rozšířená nastavení** > **Ochrany** > **Ochrana přístupu na web** > **Správa seznamu URL adres**. Následně se zobrazí konfigurace správy URL adres.



Výsledná konfigurace bude obsahovat:

- Seznam adres z politiky *San Diego Office*.
- Seznam adres z politiky *Marketing Department*.

Vzdálená konfigurace produktu prostřednictvím ESET PROTECT

Politiky slouží pro vzdálenou konfiguraci bezpečnostních produktů ESET stejně, jako kdybyste požadované změny prováděli přímo na klientovi v Rozšířeném nastavení. Na rozdíl od politik v Active Directory, politiky v ESET PROTECT neumožňují provádění skriptů ani příkazů.

Od verze 6 můžete v bezpečnostních produktech odlišně nastavit reportování stavů a ovlivnit, které se zobrazí uživateli, a které se budou zasílat do konzole. Toto nastavení naleznete v konfiguraci produktu v sekci **Uživatelské rozhraní** > **Prvky uživatelského rozhraní** > **Stavy**:

- **Zobrazit uživateli** – stav produktu se uživateli zobrazí v hlavním okně programu,
- **Odeslat do konzole** – stav produktu bude reportován do ESET PROTECT.

Připravili jsme pro vás několik vzorových příkladů, jak prostřednictvím politik konfigurovat produkty ESET:

- Konfigurace ESET Management Agenta

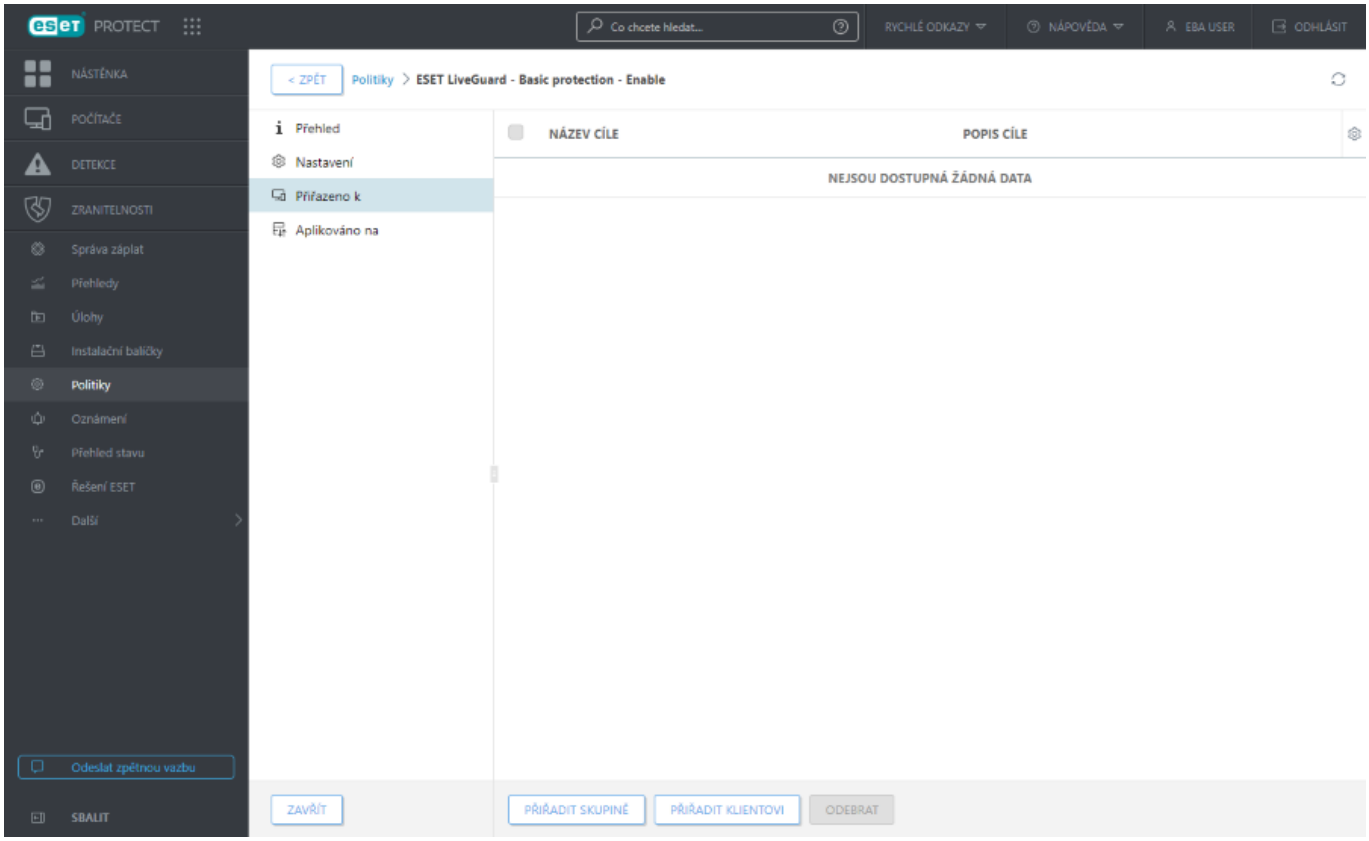
- Konfigurace ESET Rogue Detection Sensor prostřednictvím politiky

Přiřazení politiky skupině

Poté, co politiku vytvoříte, ji můžete jedním z následujících kroků přiřadit **Statické** nebo **Dynamické skupině**. Provést to můžete dvěma způsoby:

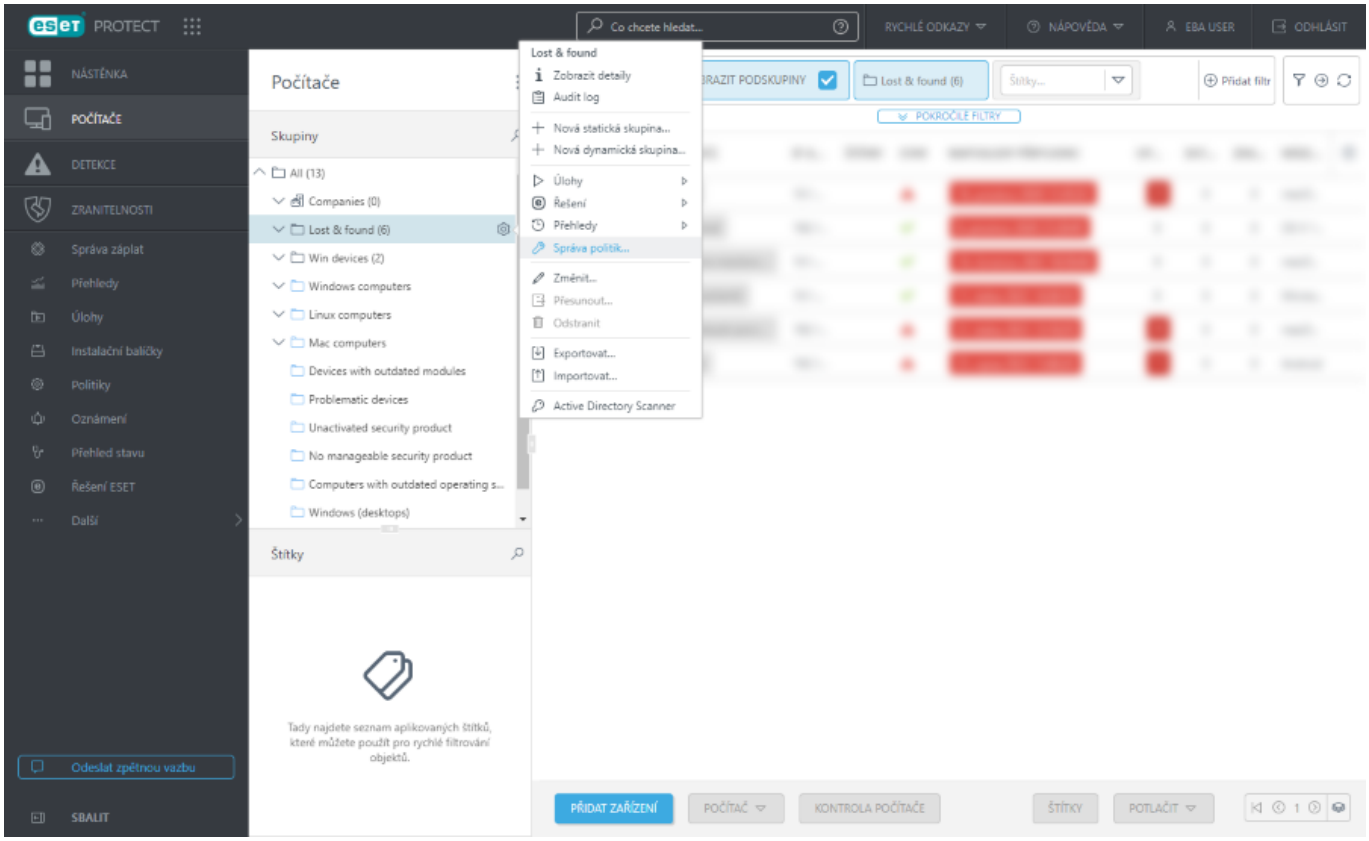
První možnost

V sekci **Politiky** vyberte politiku a klikněte na tlačítko **Akce** > **Zobrazit detaily**. Přejděte na záložku **Přiřazeno k** a klikněte na **Přiřadit skupině**. Následně si ze seznamu vyberte požadovanou statickou nebo dynamickou skupinu a potvrďte kliknutím na tlačítko **OK**.



Druhá možnost

1. V sekci **Počítače** klikněte na ikonu ozubeného kolečka u požadované skupiny a z kontextového menu vyberte možnost **Správa politik…**.



2. V dialogovém okně **Pořadí uplatňovaných politik** klikněte na tlačítko **Přiřadit politiku**.

3. Ze seznamu vyberte politiku, kterou chcete aplikovat na skupinu a pokračujte kliknutím na tlačítko **OK**.

4. Klikněte na tlačítko **Zavřít**.

Pro ověření, že je politika přiřazená skupině se v sekci skupiny přepněte na záložku **Politiky**.

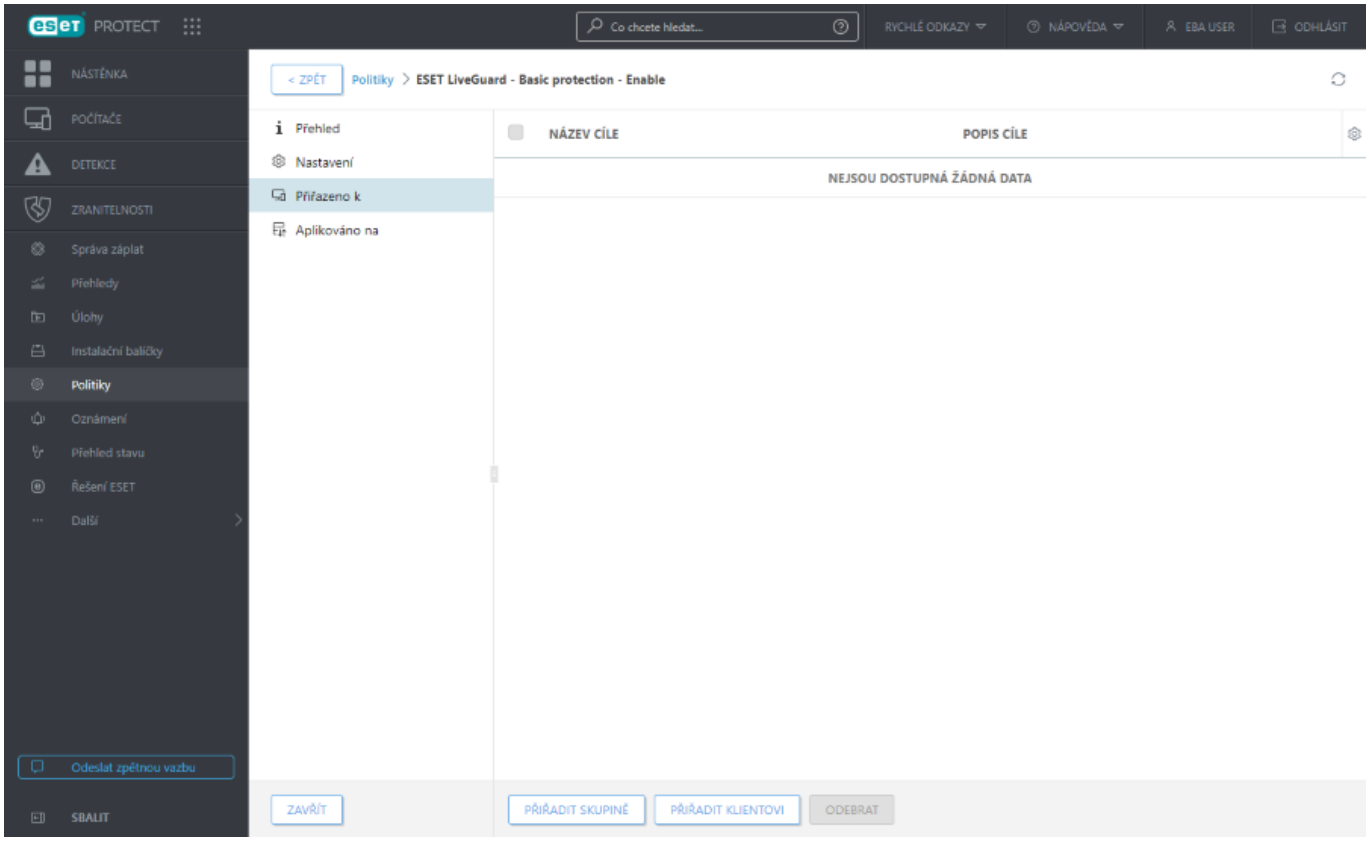
Pro ověření, na jaké skupiny je politika aplikována vyberte možnost **Zobrazit detaily** > **Aplikováno na**.

Pro více informací přejděte do kapitoly Politiky.

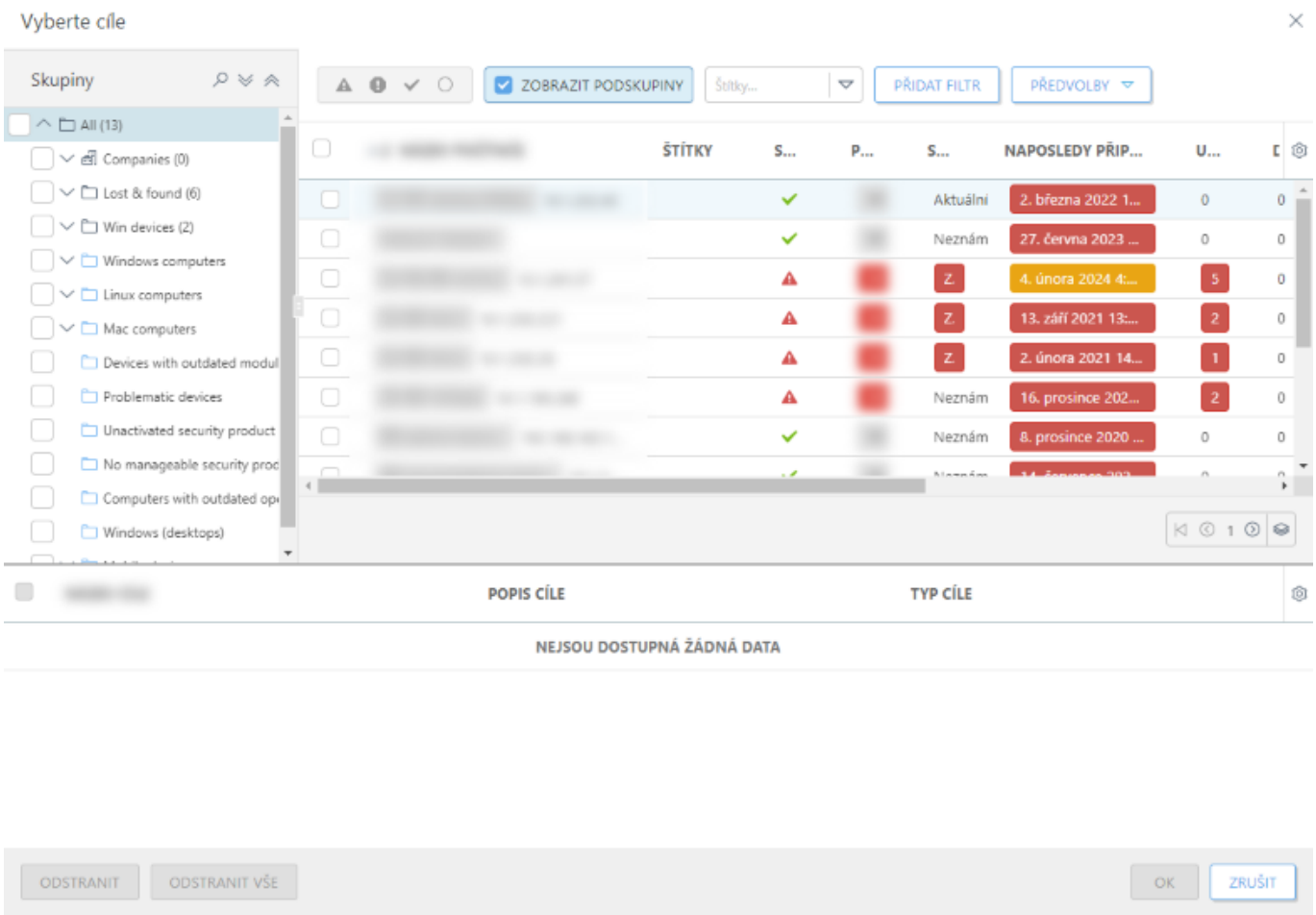
Přiřazení politiky klientovi

Pro přiřazení politiky klientské stanici přejděte v hlavním menu do sekce **Politiky**, vyberte politiku a klikněte na tlačítko **Akce** > **Zobrazit detaily**. Přejděte do sekce **Přiřazeno k** a klikněte na **Přiřadit klientovi**.

Pro zajištění, že se objekt aplikuje na všechna zařízení ve skupině, místo výběru jednotlivých stanic vyberte jako cíl celou skupinu. Zabráníte tím zároveň zpomalení Web Console.
Pokud vyberte velké množství počítačů, Web Console zobrazí varování.



Vyberte cílové zařízení a klikněte na tlačítko **OK**. Politika se přiřadí všem vámi vybraným zařízením (aplikuje se však až když se zařízení připojí k serveru).



Seznam všech klientů, kterým je politika přiřazena (nemusí znamenat, že je již aplikována), naleznete na záložce **Přiřazeno k**.

Jak použít režim dočasné změny nastavení?

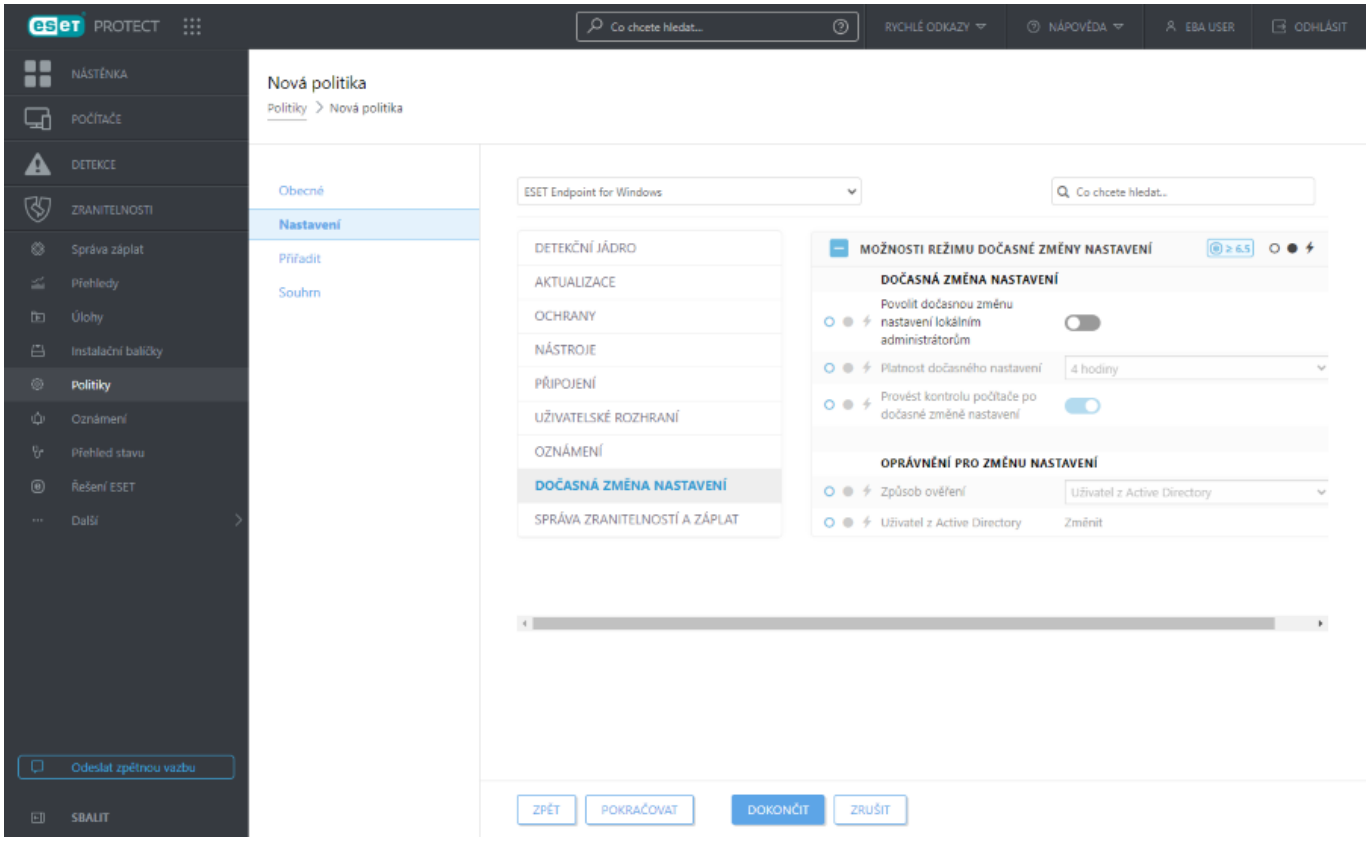
Uživatelé, kteří používají bezpečnostní řešení ESET pro ochranu koncových zařízení pro Windows, mohou využít režim dočasné změny nastavení. Režim dočasné změny nastavení můžete zapnout pouze vzdáleně z webové konzole ESET PROTECT. Tento režim jim umožní měnit nastavení, které je jinak vynucenou politiku, a není možné jej lokálně měnit. Dočasně měnit nastavení mohou vámi definovaní uživatelé z Active Directory, případně všichni uživatelé za předpokladu, že znají heslo. Režim dočasné změny nastavení může být aktivní nejvýše 4 hodiny.

Omezení režimu dočasného nastavení

- Režim dočasné změny nastavení nelze vzdáleně z ESET PROTECT Web Console ukončit. Vypne se automaticky po uplynutí stanového intervalu, případně jej uživatel může deaktivovat ručně.
- Uživatel, který použije režim dočasné změny nastavení, musí mít rovněž oprávnění administrátora Windows. V opačném případě nebude schopen uložit změny v nastavení produktu ESET.
- Ověřování Active Directory skupiny je ve spravovaném prostředí podporováno v následujících bezpečnostních řešeních:
  - ESET Endpoint Security
  - ESET Server Security pro Microsoft Windows Server (dříve ESET File Security pro Microsoft Windows Server)
  - ESET Mail Security pro IBM Domino
  - ESET Mail Security pro Microsoft Exchange Server

Pro povolení **režimu dočasné změny nastavení** na konkrétní stanici:

1. V hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.
2. V sekci **Obecné** zadejte **název** politiky, volitelně **popis**.
3. V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows**.
4. V konfigurační šabloně přejděte na záložku **Dočasná změna nastavení**. Pomocí přepínače tuto možnost aktivujte a nastavte její parametry.
5. V sekci **Přiřadit** vyberte konkrétní stanici nebo skupinu zařízení, na které chcete politiku uplatnit.
6. Souhrnné informace naleznete v sekci **Přehled** a politiku uložte kliknutím na tlačítko **Dokončit**.



Uživatel *Filip* měl problém s přístupem na konkrétní webovou stránku. Administrátor se rozhodl, že umožní *Filipovi* dočasně měnit nastavení, aby mohl svépomocí identifikovat příčinu. Filip provedl změny v konfiguraci programu a nyní mu přístup na web funguje. Administrátor si následně jeho konfiguraci vzdáleně stáhl do ESET PROTECT a převedl do politiky.

Administrátor k tomu využil tento postup:

1.V hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.

2.Zadejte **název** nové politiky, volitelně **popis**. V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows**.

3.V konfigurační šabloně přejděte na záložku **Dočasná změna nastavení**. Pomocí přepínače tuto možnost aktivujte, nastavte limit na 1 hodinu a vyberte *konkrétního uživatele* z Active Directory.

4.Přiřaďte politiku požadované stanici (v našem případě *počítači Filipa*) a politiku uložte kliknutím na tlačítko **Dokončit**.

5.Uživatel *Filip* má nyní v rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu možnost pro dočasnou změnu nastavení a může měnit konfiguraci programu.

6.V ESET PROTECT Web Console na záložce **Počítače** najděte konkrétní stanici (v našem případě *Filipa*) a klikněte na možnost **Zobrazit detaily**.

7.Přejděte na záložku **Konfigurace** a klikněte na tlačítko **Vyžádat konfiguraci**. Tím naplánujete získání konfigurace s podmínkou spuštění Ihned.

8.Vyčkejte, než agent zašle serveru konfiguraci produktu. Vyberte požadovaný produkt, jehož nastavení chcete získat, a klikněte na tlačítko **Otevřít konfiguraci**.

9.Klikněte na tlačítko **Převést do politiky**.

10. Zadejte **název** nové politiky, volitelně **popis**.

11. V sekci **Nastavení** zkontrolujte konfiguraci a případně ji ještě upravte.

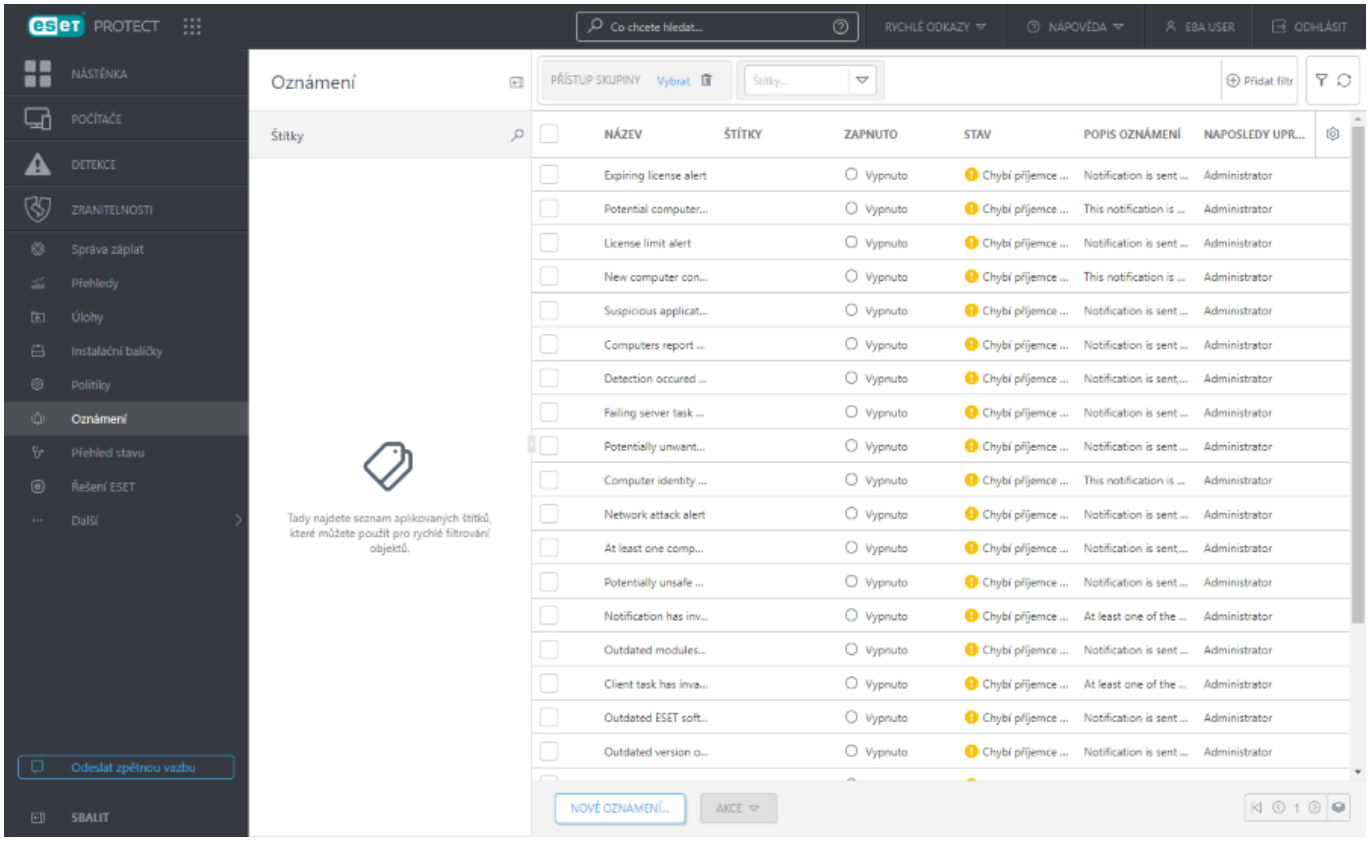
12. **Přiřaďte** politiku požadované stanici (v našem případě *Filipovi*).

13. Pro uložení nastavení klikněte na tlačítko **Dokončit**.

14. Nezapomeňte stanici, kterou používá Filip, odebrat politiku, která mu umožnila dočasně měnit nastavení produktu.

Oznámení

Oznámení představují účinný a pohodlný nástroj pro zjištění stavu vaší sítě. Při výskytu nové události v síti (definované v konfiguraci oznámení) si můžete nechat zaslat upozornění prostřednictvím e-mailu, abyste na ni mohli vhodně reagovat. SMTP server vyžadovaný pro zasílání oznámení je nakonfigurován automaticky. Z vaší strany není vyžadován žádný další zásah. K dispozici máte několik předdefinovaných automatických oznámení zaměřených na hlášení detekcí, informování o zastaralých verzí produktů ve vaší síti atp. Podrobné informace o oznámení a jeho podmínce spuštění naleznete v popisu oznámení.



Pro vytvoření nového oznámení klikněte v dolní části na tlačítko **Nové oznámení**.

Možnosti pro správu oznámení se zobrazí po vybrání konkrétního oznámení a následném kliknutí na tlačítko **Akce**.

Pro vytvoření filtru klikněte na tlačítko **Přidat filtr**. Následně si ze seznamu vyberte požadovaný filtr. Zadejte hledaný výraz, případně si požadovaný filtr vyberte ze seznamu, a stiskněte klávesu **Enter**. Aktivní filtr je zvýrazněn modře.

Oznámení, uživatelé a oprávnění

Použití oznámení vázáno na oprávnění uživatele. Oznámení se vždy spustí pod uživatelem, který naposledy oznámení upravoval. Uživatel uvidí pouze oznámení, ke kterým má přístup. V rámci oznámení obdržíte data výhradně z objektů, ke kterým máte přístup (alespoň pro **čtení**).

Pro správnou funkčnost oznámení je nezbytné, aby uživatel měl potřebná oprávnění ke všem odkazovaným objektům (zařízením, skupinám, šablonám, ...). Obecně k tomu stačí oprávnění **Číst** a **Použít**. Pokud uživatel nemá potřebná oprávnění, nebo o ně kdykoli přijde, oznámení nebude fungovat. Neúspěšná oznámení jsou zvýrazněna a na definovanou e-mailovou adresu se odešle upozornění.

Vytvoření oznámení – uživatel musí mít oprávnění pro vytváření (**Zápis**) oznámení ve své domovské skupině. Všechna nově vytvořená oznámení se uloží do jeho domovské skupiny.

Úprava oznámení – uživatel musí mít oprávnění pro vytváření (**Zápis**) oznámení v konkrétní statické skupině.

Úprava oznámení – uživatel musí mít oprávnění pro vytváření (**Zápis**) oznámení v konkrétní statické skupině.

Filip, jehož **domovskou skupinou** je *Filipova skupina*, chce odstranit (případně upravit) *Oznámení 1*: Protože oznámení vytvořil *Petr*, je umístěno v jeho domovské skupině (*Petrova skupina*). Aby mohl *Filip* upravit *Oznámení 1*:
- *Filip* musí mít přiřazenou sadu oprávnění s hodnotou **Zápis** u položky Oznámení**.**
- Jako **statická skupina** musí být v dané sadě oprávnění nastavena *Petrova skupina*.

Domovská skupina je automaticky detekována na základě přiřazené sady oprávnění právě přihlášeného uživatele.

Příklad:
Právě přihlášený uživatel má oprávnění k **zápisu** u klientské úlohy **Instalace aplikace**. **Domovská skupina** uživatelského účtu je skupina s názvem "Oddělení_1". Pokud uživatel vytváří novou **klientskou úlohu pro instalaci aplikace**, skupina "Oddělení_1" se automaticky vybere jako **domovská skupina**.

Pokud vám předvybraná domovská skupina nevyhovuje, můžete ji ručně změnit.

Klonování a VDI

Pro detekci klonovaných stanic máme předpřipravena tři oznámení, které si můžete v případě potřeby upravit nebo je využít při tvorbě vlastních.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Správa oznámení

Přístup k oznámením získáte po kliknutí v hlavním menu na ikonu **Oznámení**. V zobrazené sekci konzole máte k dispozici tyto možnosti:

- Kliknutím na tlačítko **Nové oznámení** vytvoříte nové oznámení.
- V kontextovém menu oznámení máte k dispozici následující možnosti:

Zobrazit detaily	Kliknutím si zobrazíte detailní informace zahrnující konfiguraci a způsob distribuce. Pro zobrazení náhledu oznámení klikněte na možnost **Zobrazit náhled zprávy**.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.

Zapnout / Vypnout	Kliknutím změníte stav oznámení. Vypnutá oznámení nejsou vyhodnocována a zasílána. Všechna oznámení jsou standardně **Vypnutá**.
Změnit...	Kliknutím můžete upravit parametry a způsob doručení oznámení.
Duplikovat...	Kliknutím vytvoříte ve své domovské skupině kopii oznámení.
Odstranit	Kliknutím odstraníte oznámení.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Nové oznámení

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářeného oznámení. Z důvodu jeho snadnější identifikace v budoucnu.

Pokud chcete vypnout zapnuté oznámení, klikněte na přepínač , a stav se změní na **Vypnuto** .

Konfigurace

Událost – oznámení můžete vytvořit na základě výskytu třech typů událostí. Pro každý typ události jsou v sekci **konfigurace** dostupné jiné možnosti. Dostupné jsou tyto typy událostí:

- Události na spravovaných počítačích nebo skupinách
- Změny stavu serveru
- Změna dynamické skupiny

Rozšířená nastavení

Pomocí těchto možností můžete ovlivnit citlivost aktivace oznámení a zabránit jejich nadměrnému zasílání. Pro více informací se podívejte do kapitoly throttling.

Distribuce

V této části definujte způsob doručení oznámení.

Události na spravovaných počítačích nebo skupinách

Tento typ události nesouvisí s dynamickými skupinami, ale je založen na událostech z bezpečnostních produktů nainstalovaných na spravovaných stanicích. Pro vytvoření oznámení si vyberte kategorii a filtr konkrétní události.

Kategorie – vyberte jednu z následujících kategorií:

- **Detekce firewallu**
- **Detekce antivirem**

- **Kontrola počítače**
- **HIPS**
- **ESET Inspect upozornění**
- **Zablokovaný soubor**
- **První připojení počítače**
- **Obnovení identity počítače**
- **Vytvoření rozhodnutí o klonování počítače**
- **Nalezen nový MSP zákazník**
- **Incidenty ESET Inspect**

V závislosti na vybrané kategorii se v sekci **Nastavení** > **Filtrovat podle** zobrazí dostupné události, podle kterých můžete filtrovat. Hodnoty jsou porovnávány přímo s událostmi, které reportují klienti. Neposkytujeme seznam možných hodnot, které mohou být reportovány.

Sledovaná statická skupina – výběrem statických skupin můžete zúžit seznam zařízení, ze kterých chcete dostávat oznámení. Pokud nevyberte žádnou statickou skupinu, obdržíte oznámení ze všech zařízení, k nimž máte přístup.

Přeskočit potlačená zařízení – po vybrání této možnosti nebudete dostávat oznámení ze zařízení, která jsou označena jako potlačená (v oznámeních nebudou uvedena potlačená zařízení).

Nastavení

V části **Nastavení** vyberte **spojku** a zadejte hodnoty filtru (v sekci **Filtrovat podle**). Použít můžete vždy jen jeden operátor, který se použije při vyhodnocování hodnot. Pro vytvoření filtru klikněte na **Přidat filtr**.

Výchozí obsah zprávy má informativní účel a nelze jej přizpůsobit. Zprávu doručenou prostřednictvím oznámení můžete přizpůsobit v sekci Distribuce.

Změny stavu serveru

Toto oznámení se odešle v případě, kdy dojde ke změně stavu objektu. Interval pro zaslání oznámení se odvíjí na vybrané **kategorii**. Využít můžete některé z předdefinovaných nastavení nebo použít vlastní parametry.

Načíst předvolbu nastavení – kliknutím na tlačítko Vybrat si můžete vybrat některou z předdefinovaných konfigurací. Pro vymazání konfigurace použijte tlačítko Vyčistit.

Kategorie – vyberte kategorii objektů. Na základě tohoto výběru se v sekci Nastavení zobrazí odpovídající možnosti konfigurace.

Sledovaná statická skupina – výběrem statických skupin můžete zúžit seznam zařízení, ze kterých chcete dostávat oznámení. Pokud nevyberte žádnou statickou skupinu, obdržíte oznámení ze všech zařízení, k nimž máte přístup.

Nastavení

Vyberte **spojku** a zadejte hodnoty filtru (v sekci **Filtrovat podle**). Při definování více hodnot se pro všechny hodnoty v jednom filtru použije stejná spojka. Kliknutím na **Přidat** přidáte novou hodnotu do filtru. Při použití více filtrů se v pro vyhodnocování použijte logický operátor *AND* (oznámení se zašle pouze v případě, kdy výsledek vyhodnocení všech hodnot bude *true* – kladný).

Některé filtry mohou způsobit nadměrnou aktivaci zasílání oznámení. Proto doporučujeme použít throttling pro agregaci oznámení.

Seznam dostupných filtrů

Kategorie	Hodnota	Komentář
Spravovaní klienti	Relativní časový interval (naposledy připojeno)	Vyberte interval, ve kterém chcete událost sledovat.
	Nepřipojené počítače (v %)	Hodnota mezi 0 a 100. Je možné použít pouze v kombinaci s filtrem **Relativní časový interval**.
Licence	Relativní časový interval (licence vyprší)	Vyberte období, ve kterém chcete sledovat konec platnosti licence.
	Využití licence (v %)	Hodnota mezi 0 a 100 vypočítávána na základě **jednotek** z licence použitých k aktivaci. V případě ESET Mail Security se hodnota ve sloupci Počet vypočítává na základě zakoupených poštovních schránek (hodnota ve sloupci **Rozsah**).
	Typ uživatele licence	Vyberte **Společnost**, **MSP Zákazníka** nebo **Lokalitu**.
Klientské úlohy	Úloha	Vyberte konkrétní úlohu. Pokud žádné nevyberete, vyhodnocovány budou všechny.
	Úloha je platná	Vyberte jednu z možností: **Ano** / **Ne**. Při vybrání možnosti **Ne** se oznámení zašle v případě, kdy alespoň jedna z definovaných úloh (filtr **Úloha**) bude neplatná.
Serverové úlohy	Počet (neúspěšné)	Počet selhání vybrané úlohy.
	Poslední stav	Poslední reportovaný stav vybrané úlohy.
	Úloha	Vyberte konkrétní úlohu. Pokud žádné nevyberete, vyhodnocovány budou všechny.
	Úloha je platná	Vyberte jednu z možností: **Ano** / **Ne**. Při vybrání možnosti **Ne** se oznámení zašle v případě, kdy alespoň jedna z definovaných úloh (filtr **Úloha**) bude neplatná.
	Relativní interval času (čas výskytu)	Vyberte interval, ve kterém chcete událost sledovat.
Instalované aplikace	Název aplikace	Úplný název aplikace. Pro sledování více aplikací použijte spojku **je jeden z** a přidejte další záznamy.
	Výrobce aplikace	Úplný název výrobce. Pro sledování více výrobců použijte spojku **je jeden z** a přidejte další záznamy.
	Stav verze aplikace	Při vybrání možnosti **Zastaralá** se oznámení zašle v případě, kdy alespoň jedna z aplikací není aktuální.
Oznámení	Oznámení	Vyberte konkrétní oznámení. Pokud žádné nevyberete, vyhodnocovány budou všechny.
	Oznámení je zapnuté	Vyberte jednu z možností: **Ano** / **Ne**. Při vybrání možnosti **Ne** se oznámení zašle v případě, kdy alespoň jedno z definovaných oznámení (filtr **Oznámení**) bude vypnuté.
	Oznámení je platné	Vyberte jednu z možností: **Ano** / **Ne**. Při vybrání možnosti **Ne** se oznámení zašle v případě, kdy alespoň jedno z definovaných oznámení (filtr **Oznámení**) bude neplatné.

Výchozí obsah zprávy má informativní účel a nelze jej přizpůsobit. Zprávu doručenou prostřednictvím oznámení můžete přizpůsobit v sekci Distribuce.

Změna dynamické skupiny

Toto oznámení se odešle při splnění definované podmínky nad sledovanou dynamickou skupinou. V rámci jednoho oznámení můžete definovat pouze jednu podmínku pro konkrétní dynamickou skupinu.

Dynamická skupina – vyberte dynamickou skupinu, která bude vyhodnocována.

Nastavení – Podmínky

Vyberte typ podmínky, která aktivuje oznámení.

- **Upozornit při každé změně obsahu dynamické skupiny** – oznámení se aktivuje, pokud se nové zařízení stane členem skupiny, případně některé ze zařízení přestane být jejím členem.

ESET PROTECT kontroluje obsah dynamických skupin každých 20 minut.
Příklad: pokud je první kontrola provedena v 10:00, další kontroly proběhnou v 10:20, 10:40 a 11:00. V případě, že se změní stav dynamické skupiny v 10:05 a opětovně v 10:13, při kontrole provedené v 10:20 ESET PROTECT nerozpozná změní a neupozorní vás na to.

- **Upozornit, pokud velikost skupiny překročí definovanou hodnotu** – vyberte operátor pro Velikost skupiny a

zadejte Mezní hranici:

- **Větší než** – oznámení se odešle, pokud velikost skupiny překročí mezní hranici.
- **Menší než** – oznámení se odešle, pokud velikost skupiny klesne pod mezní hranici.

- **Upozornit, pokud se velikost skupiny změní za určitou dobu** – definujte mezní hranici a časové období pro aktivaci oznámení. Mezní hranici můžete definovat na přesný počet klientů nebo procentuálně (počet členů dynamické skupiny). Časové období definujte v minutách, hodinách nebo dnech, po kterém dojde k vyhodnocení změny obsahu skupiny. Příklad: před sedmi dny byl na 10 klientech nainstalován neaktuální bezpečnostní produkt a mezní hranice byla nastavena na 20. Pokud se počet klientů ve skupině zvýší na 30, budete o tom informováni.

- **Upozornit na změnu obsahu dynamické skupiny oproti porovnávané skupině** – oznámení se odešle, pokud se ve sledované dynamické skupině změní počet zařízení ve srovnání s jinou skupinou (statickou nebo dynamickou). Rozdíl ve velikosti – definujte mezní hranici při jejímž dosažení se aktivuje oznámení.

Oznámení na dynamickou skupinu můžete vytvořit pouze . Pro zobrazení dynamických skupin musíte mít oprávnění pro **čtení** do nadřazené statické skupiny.

Distribuce

Při vytváření oznámení je nutné vybrat alespoň jeden způsob jejího doručení.

Můžete vybrat oba způsoby distribuce – **Odeslat e-mailem** a **Odeslat webhook**. Poté:
1. Vyplňte **Nastavení distribuce pošty**.
2. Vyplňte **Nastavení distribuce webhooku**.

Odeslat e-mailem

Po vybrání možnosti **Odeslat e-mailem** je nutné zadat alespoň jednoho příjemce zprávy.Standardně se zasílá e-mail v HTML formátu s logem ESET PROTECT umístěným v hlavičce.

Nastavení distribuce pošty

- **E-mailová adresa** – zadejte e-mailovou adresu příjemce oznámení.
- Klikněte na ikonu + přidáte dalšího příjemce.
- Uživatele můžete přidat hromadně následujícími způsoby: klikněte na **Další** > **Přidat uživatele** (tím můžete vybrat e-mailové adresy uživatelů definovaných v sekci Uživatelé zařízení) nebo na **Další** > **Importovat CSV** / **Vložit ze schránky** (kdy můžete seznam adres importovat z CSV souboru, případně vlastní datové struktury).
- **Další** > **Kopírovat a vložit** – po kliknutí můžete seznam adres zkopírovat ze schránky (tato funkce funguje podobně jako Import CSV). Tato funkce funguje podobně jako import dat z CSV.

Přidat do zprávy odkaz – po aktivování této možnosti se do těla e-mailu s oznámením vloží odkaz, prostřednictvím kterého si ve webové konzoli otevřete detailní informace.

Odeslat testovací e-mail – klikněte na **Odeslat** a odešlete testovací e-mail na výše uvedenou adresu.

Odeslat webhook

Pro odeslání oznámení prostřednictvím webhooků lze použít ESET PROTECT. Oznámení obdržíte jako zprávu od ESET PROTECT ve svém primárním komunikačním kanálu.

- **Adresa URL webhooku** – zadejte URL adresu webhooku komunikačního kanálu

> ✓ Níže naleznete příklad adresy URL webhooku Teams:
> *https://xxxxx.webhook.office.com*
> Po zadání URL webhooku pro Teams, **JSON payload** se nezobrazí.

  - **Přidat do webhooku odkaz** – po zaškrtnutí políčka zahrnete odkaz do Web Console s podrobnostmi o události z oznámení. Tato funkce platí pro webhooky Teams

  - Po zadání vlastní URL adresy webhooku (neplatí pro Teams nebo Slack) můžete nastavit Autentifikaci

- **JSON payload** – zadejte platný JSON. Můžete použít proměnné. Klikněte na tlačítko **Přidat proměnnou** a vyberte proměnnou: **Předmět**, **Obsah**, **Odkaz**

  - Pokud v **Náhledu zprávy** vyplníte **Předmět** a **Obsah**, hodnoty proměnných se automaticky použijí v **JSON payload**

  - Pro vytvoření upravené JSON pro komunikační kanál třetí strany, podívejte se do jejich oficiální nápovědy, například Discord

- **Autentifikace** – zobrazí se při zadání vlastní URL adresy webhooku. Chraňte svá data a zvyšte zabezpečení ověřování pomocí webhooku. Vyberte možnost:

  - **Bez autentifikace** – zvolte tuto možnost, pokud přijímač webhooku nevyžaduje žádné ověřování. Doporučujeme přidat ověřování pro ochranu dat a zvýšení zabezpečení.

  - **Ověřovací token** – zadejte do pole **Ověřovací token**.

  - **Základní autentifikace** – zadejte **Uživatelské jméno** a **Heslo**.

- **Odeslat testovací webhook** – kliknutím na tlačítko **Odeslat** odešlete testovací webhook na zadanou URL adresu webhooku.

Obecná pole v sekci Distribuce

- **Náhled zprávy** – náhled zprávy zobrazené v oznámení, který obsahuje nakonfigurovaná nastavení v textové podobě. Pomocí proměnných si můžete přizpůsobit předmět i obsah zprávy. Proměnné budou vždy nahrazeny aktuálními hodnotami z doby generování oznámení. Tato možnost není povinná, ale doporučuje se pro lepší filtrování.

  - **Předmět** – předmět zprávy oznámení; kliknutím na ikonu upravíte text; přesný předmět může zlepšit třídění a filtrování zpráv

- **Obsah** – kliknutím na ikonu můžete upravit obsah; po úpravě obsahu můžete kliknutím na ikonu obnovit výchozí obsah zprávy

> Pro **Události na spravovaných počítačích nebo skupinách** můžete přidat proměnné do **Předmětu** a **Obsahu**. Tím zahrnete do oznámení konkrétní informace. Pro zobrazení seznamu proměnných klikněte na tlačítko **Přidat proměnnou** nebo napište $.

- **Obecné**

  - **Jazyk** – jazyk výchozí zprávy; obsah zprávy se nepřekládá

  - **Časové pásmo** – definujte časové pásmo pro proměnnou **Čas výskytu** (`${timestamp}`), kterou jste použili ve vámi přizpůsobeném obsahu oznámení.

> Pokud k události došlo v 3:00 lokálního času, lokální čas je UTC+2 a časové pásmo jste nastavili na UTC+4, uvedený čas v oznámení bude 5:00.

Pro vytvoření oznámení klikněte na tlačítko **Dokončit**.

Stav serveru

ESET PROTECT Server provádí pravidelnou diagnostiku. Informace o stavu ESET PROTECT ve vaší infrastruktuře a statistická data naleznete v sekci **Stav serveru**. Tyto informace vám zároveň mohou pomoci s počátečním nastavením ESET PROTECT. Pro zobrazení těchto dat přejděte v hlavním menu ESET PROTECT do sekce **Stav serveru**.

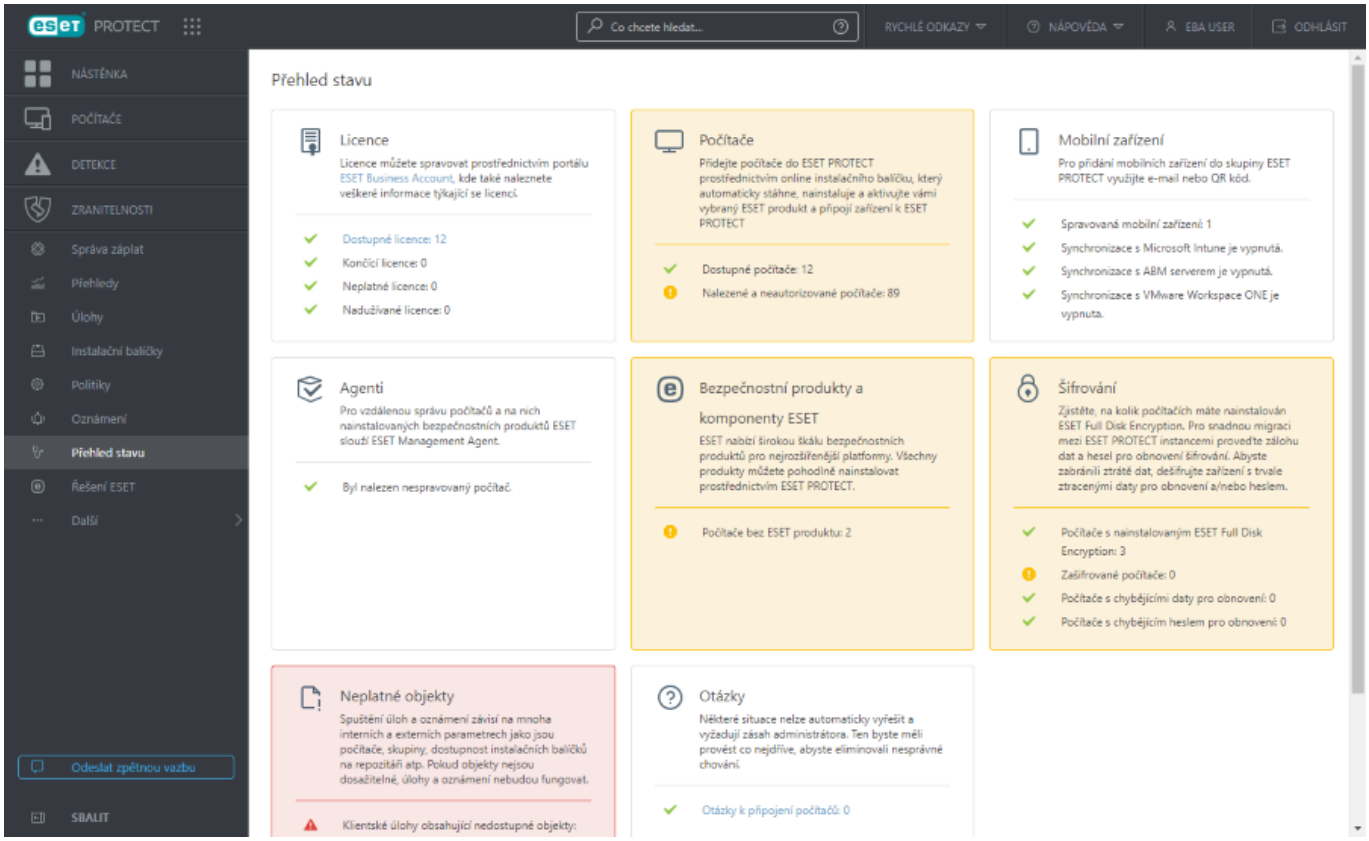
Po kliknutí na konkrétní dlaždici se zobrazí v pravé části okna detailnější informace. Barvy jednotlivých dlaždic se mohou lišit v závislosti na stavu jednotlivých položek (vždy se zobrazuje nejzávažnější stav):

Barva	Ikona	Význam ikony	Popis
Zelená		OK	U žádné položky v dané sekci není evidován problém.
Žlutá		Varování	Alespoň u jedné položky v sekci je varování.
Červená		Chyba	Alespoň u jedné položky v sekci je chyba.
Šedivá		Obsah není dostupný	Obsah není dostupný z důvodu nedostatečných přístupových oprávnění uživatele ESET PROTECT konzole. Administrator v takovém případě musí přidat uživateli oprávnění pro přístup k danému typu objektu, nebo se uživatel musí přihlásit pod jiným uživatelem.
Modrá		Informační	Rozhodnutí souvisí s připojenými počítači, viz sekci **Rozhodnutí** v dolní části této počítače.

Okno **Stav serveru** je rozděleno do následujících sekcí:

Licence	ESET PROTECT využívá ESET licenční systém. Pro správu licencí přejděte do svého účtu na portále ESET Business Account.
Počítače	• **Přidat počítač** – umožnuje přidat zařízení ve vaší síti do struktury ESET PROTECT.
Mobilní zařízení	**Přidat mobilní zařízení** – registrace mobilního zařízení. • **Nastavení registrace Microsoft Entra ID** – nastavení registrace Microsoft Entra ID. • **Synchronizace s Microsoft Intune** – nastavení synchronizace s Microsoft Intune. • **Synchronizace s ABM** – nastavení synchronizace s Apple Business Manager (ABM). • **Synchronizace s VMware Workspace ONE** – nastavení synchronizace s VMware Workspace ONE.

Agenti	• **Nasadit Agenta** – ESET Management Agenta můžete na cílová zařízení nasadit různými způsoby.
Bezpečnostní produkty a komponenty ESET	• **Nová politika** – umožňuje vytvořit politiku pro změnu konfigurace bezpečnostního produktu ESET nainstalovaného na klientských zařízeních. • **Instalovat aplikaci** – pokud už máte nasazeného ESET Management Agenta, můžetenainstalovat bezpečnostní produkt z ESET repozitáře nebo zadat umístění instalačního balíčku (URL nebo síťovou složku). • **Nastavit ochranu** – zkontrolujte a přizpůsobte si nastavení zabezpečení, která se aplikují na všechna zařízení připojená k ESET PROTECT.
Šifrování	Pokud máte spravovaná zařízení zašifrovaná prostřednictvím ESET Full Disk Encryption, následující možnosti použijte k tomu, abyste zabránili ztrátě dat pro obnovení šifrování. • **Exportovat** – umožňuje exportovat aktuálních data pro obnovení ESET Full Disk Encryption před migrací šifrovaných zařízení. • **Importovat** – umožňuje importovat data pro obnovení ESET Full Disk Encryption po migraci šifrovaných zařízení do nové instance ESET PROTECT.
Neplatné objekty	V této části můžete ověřit, zda klientské nebo serverové úlohy, podmínky spuštění nebo oznámení nejsou navázány na již neexistující nebo nedostupné objekty. Po kliknutí budete přesměrováni do konkrétní sekce s problémovými objekty.
Rozhodnutí	Při detekci klonového zařízení nebo změny hardware se v této sekci zobrazí rozhodnutí, které je nutné vyřešit. Pro více informací přejděte do kapitoly řešení klonovaných počítačů.
Stav MSP	MSP stavy jsou k dispozici v instancích s MSP účtem.



Řešení ESET

V této části naleznete zjednodušeného průvodce pro nasazení následujících produktů:

- **ESET LiveGuard Advanced**
- **ESET Full Disk Encryption**

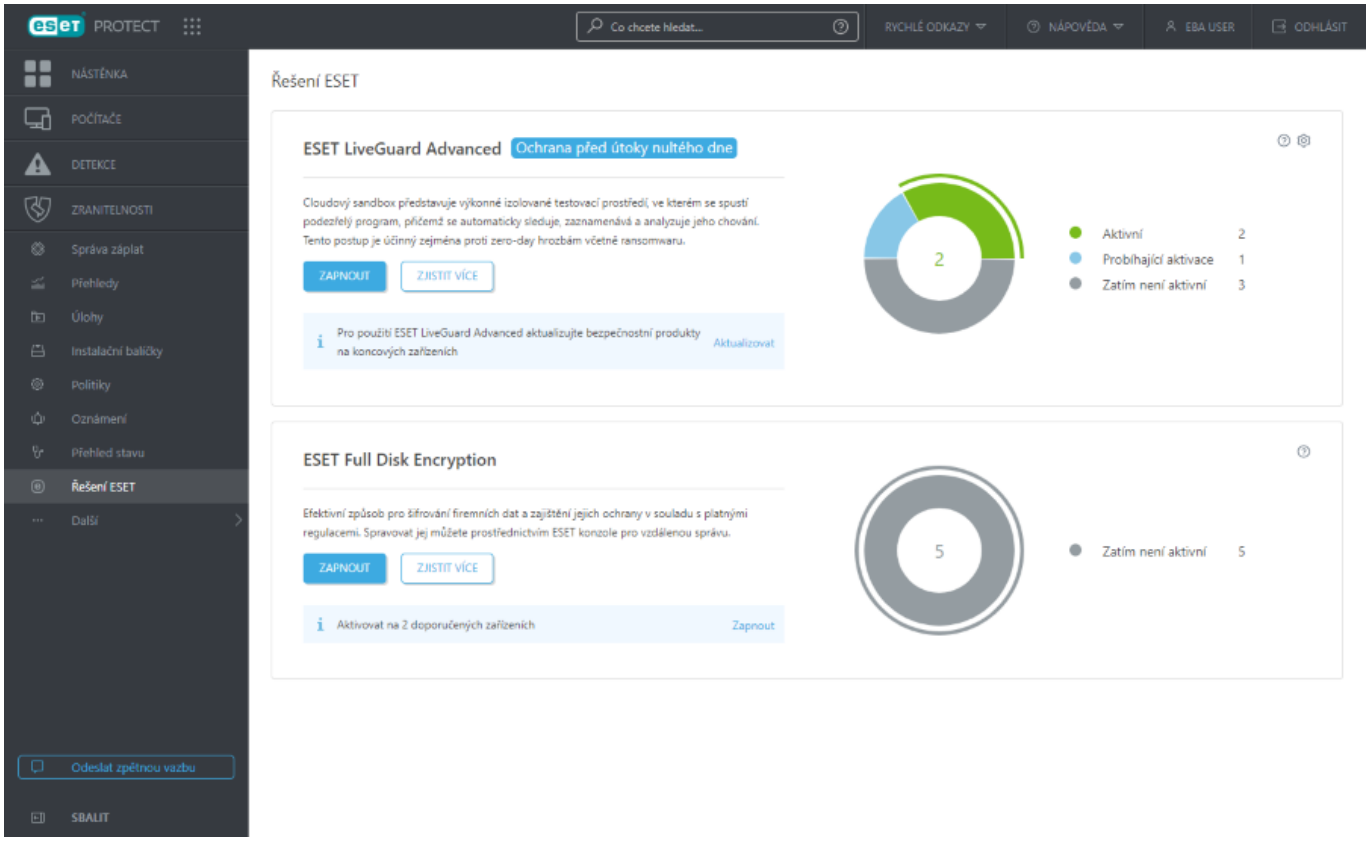
U každého produktu máte k dispozici následující možnosti:

- **Vyzkoušet** – uživatelé, kteří zatím nevlastní licenci na tento produktu, si mohou po kliknutí požádat o zkušební licenci.
- **Koupit** – kliknutím zakoupíte licenci pro vybraný produkt.
- **Zapnout** – zapne vybraný produkt na všech vhodných zařízeních. Pro více informací se podívejte do podsekce u každého produktu.
- Pro odebrání ESET LiveGuard Advanced nebo ESET Full Disk Encryption ze všech zařízení klikněte na ikonu **ozubeného kolečka** a vyberte možnost **Odebrat**.
- **Zjistit více** – zobrazí stránku se základními informacemi o vybraném produktu.

Nad každou kategorií reprezentovanou v grafu je k dispozici **kontextové menu**, prostřednictvím kterého si můžete zobrazit výsledky prvních 100 zařízení.

Omezení pro nasazení

- Pro aktivaci této funkce musí mít uživatelský účet přidělené **oprávnění pro zápis**.
- Každá MSP společnost můžete funkci vyzkoušet nejvýše jednou.



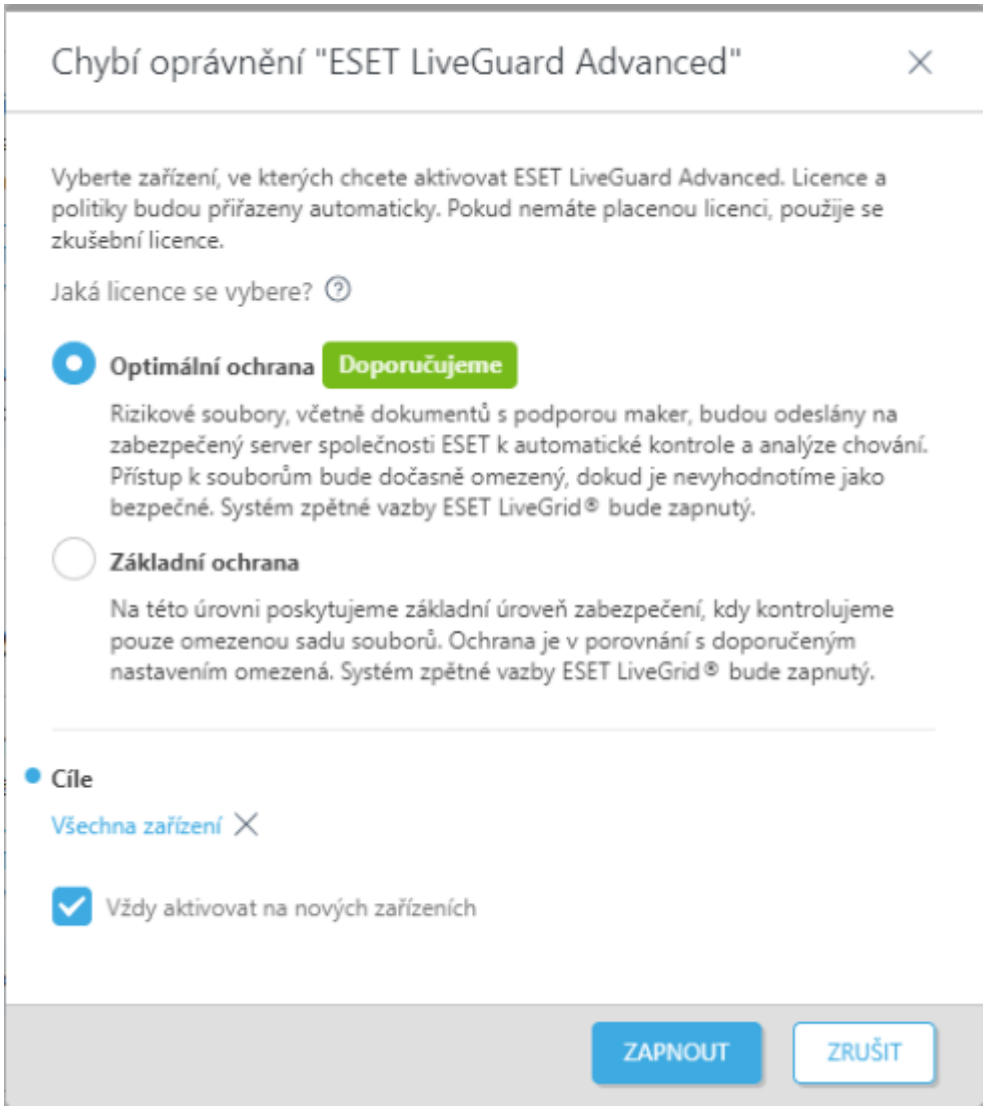
Zapnout ESET LiveGuard Advanced

Vyberte sekci **Řešení ESET**; v **ESET LiveGuard Advanced** klikněte na**Koupit** a budete přesměrováni na návod, jak přejít na vyšší bezpečnostní úroveň ESET PROTECT. Po dokončení rozšíření licence budete schopni aktivovat a zapnout ESET LiveGuard Advanced ve své síti.

Zkušební licence

Pokud již máte aktivní zkušební licenci a poté zakoupíte plnou licenci produktu, budete mít k dispozici možnost pro migraci zařízení na novou licenci.

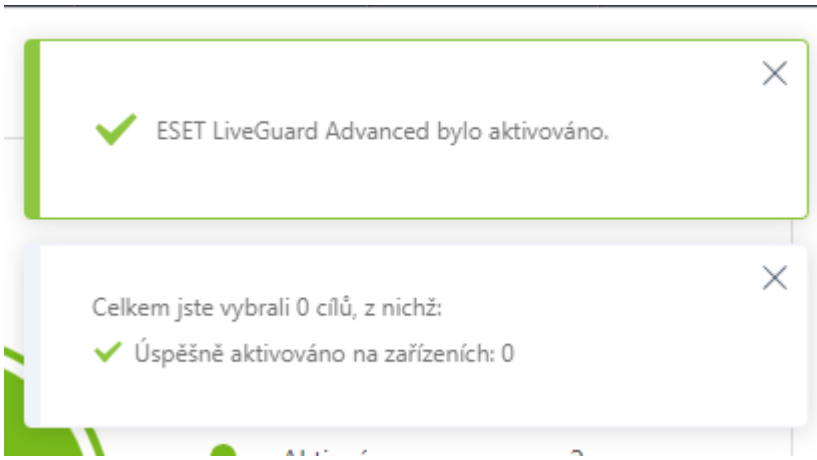
Po kliknutí na tlačítko **Nasadit** se zobrazí dialogové okno. Zde můžete vybrat **Optimální ochranu** (doporučeno) nebo **Základní ochranu**. V tomto okně vyberte **Cíle**, na které chcete službu nasadit. Ponechat můžete předvybranou výchozí možnost **Všechna zařízení**, případně si jako cíl vyberte konkrétní počítače nebo skupiny (statické/dynamické). Pokud ponecháte předvybranou výchozí skupinu **Všechna zařízení**, můžete zaškrtnout možnost **Vždy zapnout na nových zařízeních**. Tím zajistíte automatické nasazení služby ESET LiveGuard Advanced na všech nových zařízeních, která v budoucnu připojíte k ESET PROTECT. Svůj výběr potvrďte kliknutím na **Zapnout**.



Základní ochrana: V průběhu nasazení se aplikuje předdefinovaná politika **ESET LiveGuard – Zapnout**.
Optimální ochrana: V průběhu nasazení se aplikuje předdefinovaná politika **ESET LiveGuard – Optimální ochrana – Zapnout**.

Na vybraných cílech se spustí klientská úloha pro aktivaci produktu ESET LiveGuard Advanced.

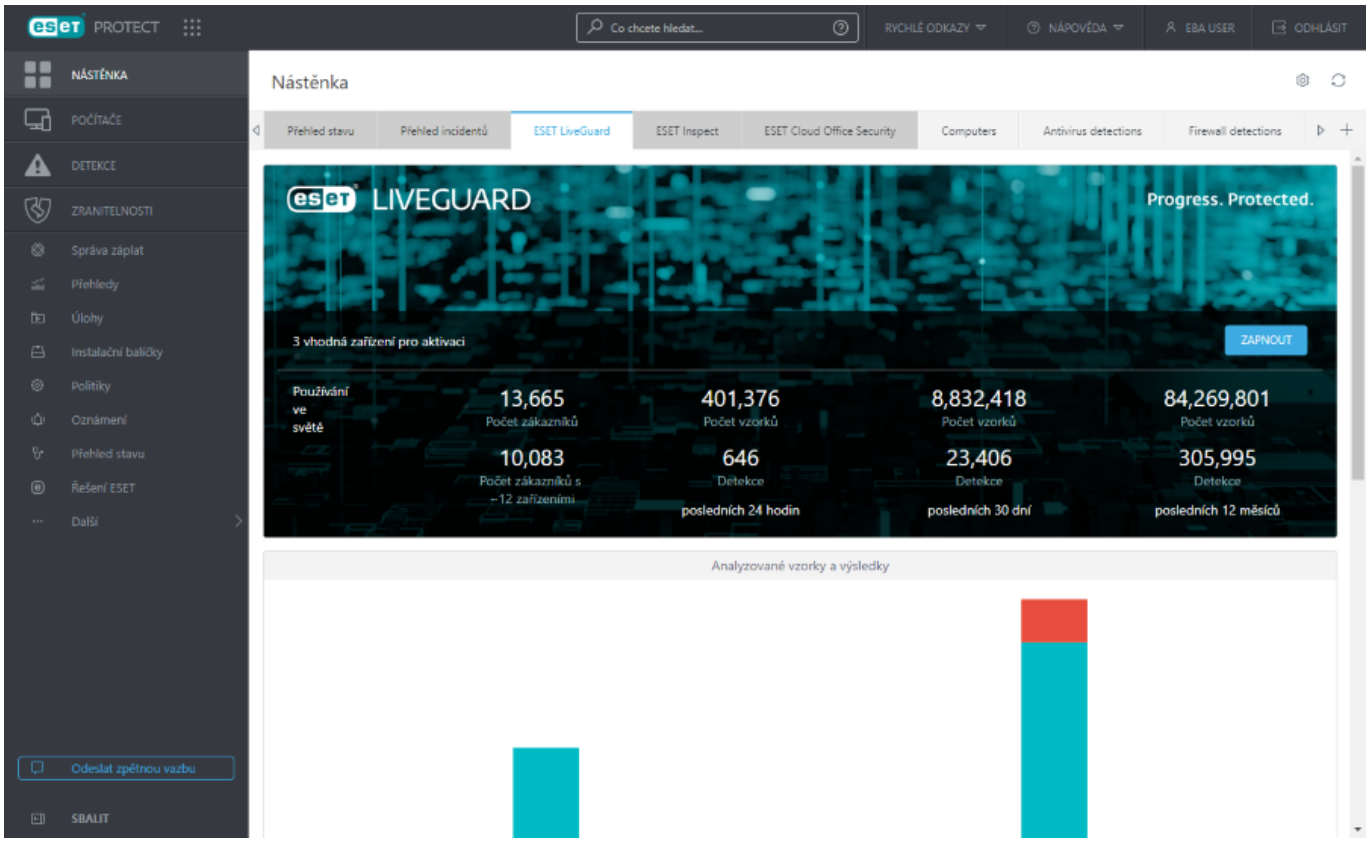
Po pravé straně obrazovky se zobrazí malé oznamovací okno obsahující informace týkající se nasazení.



Průběh nasazení můžete sledovat v sekci **Řešení ESET**.

Po zapnutí ESET LiveGuard Advanced:

- se na nástěnce ESET LiveGuard bude zobrazovat podrobné hlášení ESET LiveGuard Advanced ze spravované sítě.
- každé zařízení s ESET LiveGuard Advanced bude mít zapnutý Reputační systém ESET LiveGrid® a Systém zpětné vazby ESET LiveGrid®. Konfiguraci produktu ověřte v politikách.



Odstranění ESET LiveGuard Advanced

V detailech spravovaného zařízení klikněte v pravém horním rohu dlaždice ESET LiveGuard Advanced na ikonu ozubeného kolečka a vyberte možnost **Odebrat ESET LiveGuard Advanced**. Tím produkt deaktivujete a odstraníte související politiky ze všech vybraných zařízení.

Zakázat automatické nasazení

V detailech spravovaného zařízení klikněte v pravém horním rohu dlaždice ESET LiveGuard Advanced na ikonu ozubeného kolečka a vyberte možnost **Zakázat automatické nasazení**. Tím zakážete automatickou aktivaci a zapnutí této služby na nově přidaných zařízeních.

Zapnout ESET Full Disk Encryption

Vyberte sekci **Řešení ESET**; v **ESET Full Disk Encryption** klikněte na **Koupit** a budete přesměrováni na postup pro přechod na vyšší bezpečnostní úroveň ESET PROTECT. Po dokončení roušíření licence budete schopni nasadit a aktivovat ESET Full Disk Encryption ve své síti.

Zvolte **Zapnout** a zobrazí se nové okno, ve kterém:

1.jako **Cíle** můžete ponechat předvybranou výchozí možnost **Všechna zařízení**, případně si jako cíl vyberte konkrétní počítače nebo skupiny (statické/dynamické).

2.si vyberte **Jazyk**, ve kterém se ESET Full Disk Encryption nasadí na vybraná zařízení.

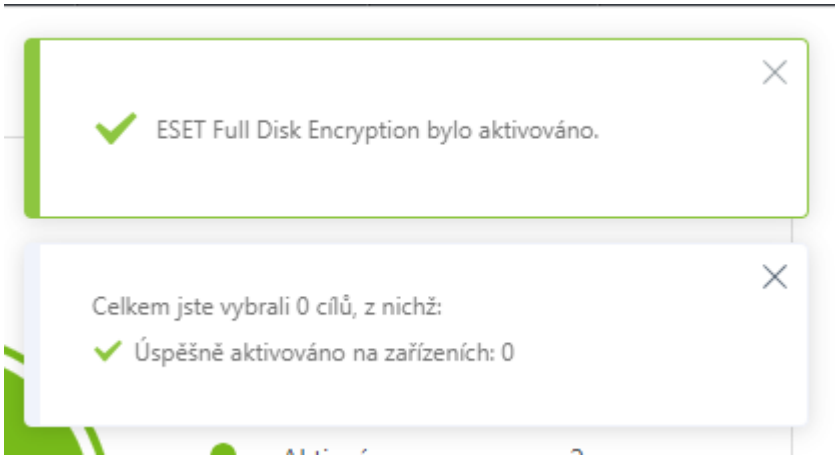
3.Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

4.Klikněte na **Zapnout**. ESET PROTECT provede úlohu pro aktivaci a úlohu instalace aplikace pro ESET Full Disk Encryption na všech vybraných spravovaných zařízeních.

V průběhu nasazení se aplikuje předdefinovaná politika **Zašifrovat všechny disky – použít TPM, pokud je dispozici – OPAL se nepoužije**.

Po pravé straně obrazovky se zobrazí malé oznamovací okno obsahující informace týkající se nasazení.

Pro úspěšné nasazení ESET Full Disk Encryption na spravované zařízení jsou vyžadovány další kroky ze strany uživatele. Postupujte podle kroků uvedených v uživatelské příručce k ESET Full Disk Encryption.



Průběh nasazení můžete sledovat v sekci **Řešení ESET**.

Odstranění ESET Full Disk Encryption

V detailech spravovaného zařízení klikněte v pravém horním rohu dlaždice **ESET Full Disk Encryption** na ikonu ozubeného kolečka a vyberte možnost **Odebrat ESET Full Disk Encryption**. Tím produkt deaktivujete, dešifrujete všechny zašifrované disky a odstraníte související politiky ze všech vybraných zařízení.

Při odebrání produktu se aplikuje předdefinovaná politika **Dešifrovat všechny disky**.

Další

V části **Další** naleznete pokročilé možnosti pro konfiguraci ESET PROTECT. Najdete zde nástroje, které můžete jako administrátor potřebovat při správě klientů a bezpečnostních produktů ESET, stejně tak zde naleznete rozšířená nastavení ESET PROTECT. Pomocí nástrojů dostupných v této části a jejich vhodným nastavením si výrazně usnadníte správu celé infrastruktury.

V sekci ··· **Další** máte přístup k následujícím funkcím:

Detekce o Odeslané soubory o Výjimky o Karanténa
Počítače o Uživatelé zařízení o Šablony dynamických skupin
Licence o Správa licence
Přístupová oprávnění o Uživatelé o Sady oprávnění
Audit aktivity o Audit log
Administrace o Nastavení

Odeslané soubory

ESET LiveGuard Advanced je služba, která poskytuje pokročilou ochranu proti zcela novým hrozbám. Jakýkoli uživatel ve vaší síti může prostřednictvím bezpečnostního produktu ESET odeslat k analýze libovolný vzorek k analýze do cloudu. Jako administrátor ESET PROTECT máte následně k dispozici přehled o chování daného vzorku. Postupy pro odeslání vzorku k analýze máme uvedeny v uživatelské příručce ESET LiveGuard Advanced.

Seznam všech odeslaných objektů k analýze na servery společnosti ESET naleznete ve Web Console v sekci **Odeslané soubory** společně s detaily o jejich chování. V tomto přehledu jsou uvedeny všechny soubory odeslané z klientů do ESET LiveGrid® (v případě, že je na stanici ESET LiveGrid® aktivován) společně se soubory odeslanými do ESET LiveGuard Advanced ručně z ESET PROTECT Web Console.

Seznam odeslaných souborů

V seznamu souborů naleznete informace související s odesláním jako je datum a čas, uživatel, počítač atp. Po kliknutí na záznam se zobrazí kontextové menu, ve kterém máte k dispozici níže uvedené možnosti.

Zobrazit detaily	Po kliknutí se zobrazí detailní informace o **posledním odeslání vzorku**.
Zobrazit chování	Po kliknutí se zobrazí přehled s detailním chováním vzorku. Tato možnost je dostupná pouze soubory zaslané k analýze do ESET LiveGuard Advanced.
Exportovat přehled	Po kliknutí se zobrazí detailní přehled o chování vzorku. Tato možnost je dostupná pouze soubory zaslané k analýze do ESET LiveGuard Advanced.
Vytvořit výjimku	Po vybrání jednoho nebo více souborů a kliknutí na možnost **Vytvořit výjimku** vyloučíte daný objekt z detekce.

Detaily souboru

V tomto dialogovém okně naleznete detailní informace týkající se odeslaného vzorku. V případě vícenásobných odeslání stejného souboru se vždy zobrazí data z posledního odeslání.

Stav	Reprezentuje výsledek analýzy. **Neznámý** – soubor zatím nebyl analyzován. **Čistý** – žádné z detekčních technik neoznačilo soubor jako škodlivý. **Podezřelý** a **Velmi podezřelý** – soubor je podezřelý, ale nemusí se jednat přímo o škodlivý kód. **Škodlivý** – daný soubor je škodlivý.
Průběh	Představuje průběh analýzy. Příznak **Opětovné analyzování** znamená, že je již k dispozici výsledek, ale může se po dokončení analýzy změnit.
Naposledy zpracováno	Jeden soubor může být odeslán k analýze vícekrát a z více počítačů. Jedná se o čas poslední analýzy.
Odesláno	Čas odeslání.
Chování	Kliknutím na tlačítko Zobrazit chování si zobrazíte analýzu z ESET LiveGuard Advanced nebo kliknutím na tlačítko **Exportovat přehled** si přehled stáhnete. Tato možnost je dostupná pouze v případě, kdy je na počítači nainstalován podporovaný bezpečnostní produkt je aktivován prostřednictvím platné licence na ESET LiveGuard Advanced.
Počítač	Název počítače, ze kterého byl soubor odeslán.
Uživatel	Uživatel počítače, který soubor odeslal.
Důvod	Důvod odeslání souboru.
Odesláno do	Část ESET cloudu, do které byl soubor zaslán. Ne každý systém vám vrátí výsledek analýzy.
Kontrolní součet	SHA1 hash odeslaného souboru.
Velikost	Velikost odeslaného souboru.
Kategorie	Kategorie souboru. Kategorie nemusí odpovídat příponě souboru.

Více informací o přehledech chování souboru naleznete v uživatelské příručce k ESET LiveGuard Advanced.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Výjimky

V této sekci naleznete seznam všech vytvořených výjimek platných pro **antivirové** detekce a IDS pravidla **firewallu**. Máte tak lepší přehled o existujících výjimkách a na jednom místě nástroje pro jejich správu.

Po vybrání jedné nebo více výjimek klikněte na tlačítko **Detekce** a zobrazí se možnosti pro jejich správu:

- **Změnit přiřazení** – pomocí této možnosti změníte cíle, na které se výjimka aplikuje.
- **Zobrazit ovlivněné počítače** – kliknutím si zobrazíte seznam počítačů, na kterých je výjimka aplikována.
- **Audit log** – kliknutím si zobrazíte Audit log pro vybranou výjimku.

- **Odstranit** – kliknutím odstraníte vybranou výjimku.

- **Přístup skupiny** > **Přesunout** Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Pokud se vyloučená detekce nebo akce firewallu opětovně vyskytne na spravovaných počítačích, čítač ve sloupci **Počet uplatnění** se po aplikování výjimky adekvátně navýší.

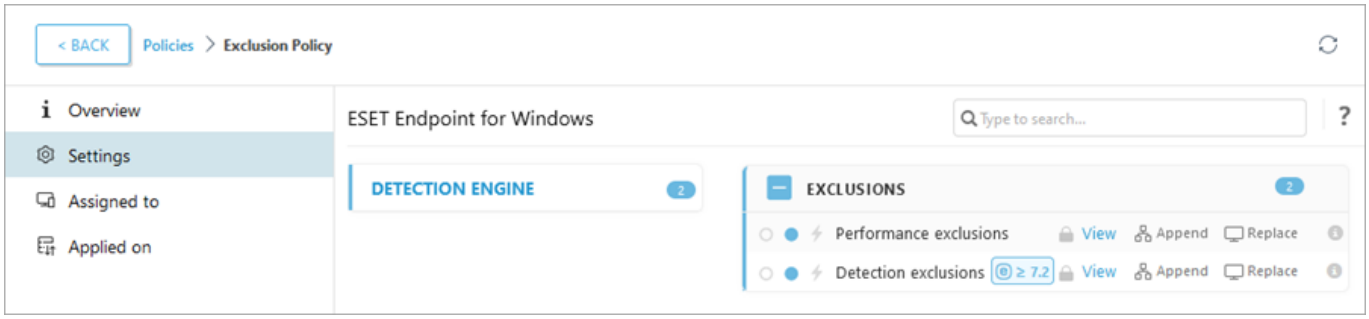
Migrace výjimek z politiky

V ESET PROTECT není možné definovat antivirové detekční výjimky prostřednictvím politiky pro konkrétní produkt. Pokud jste dříve v politikách definovali výjimky, pro jejich migraci do sekce **Výjimky** představené v ESET PROTECT postupujte podle níže uvedených kroků:

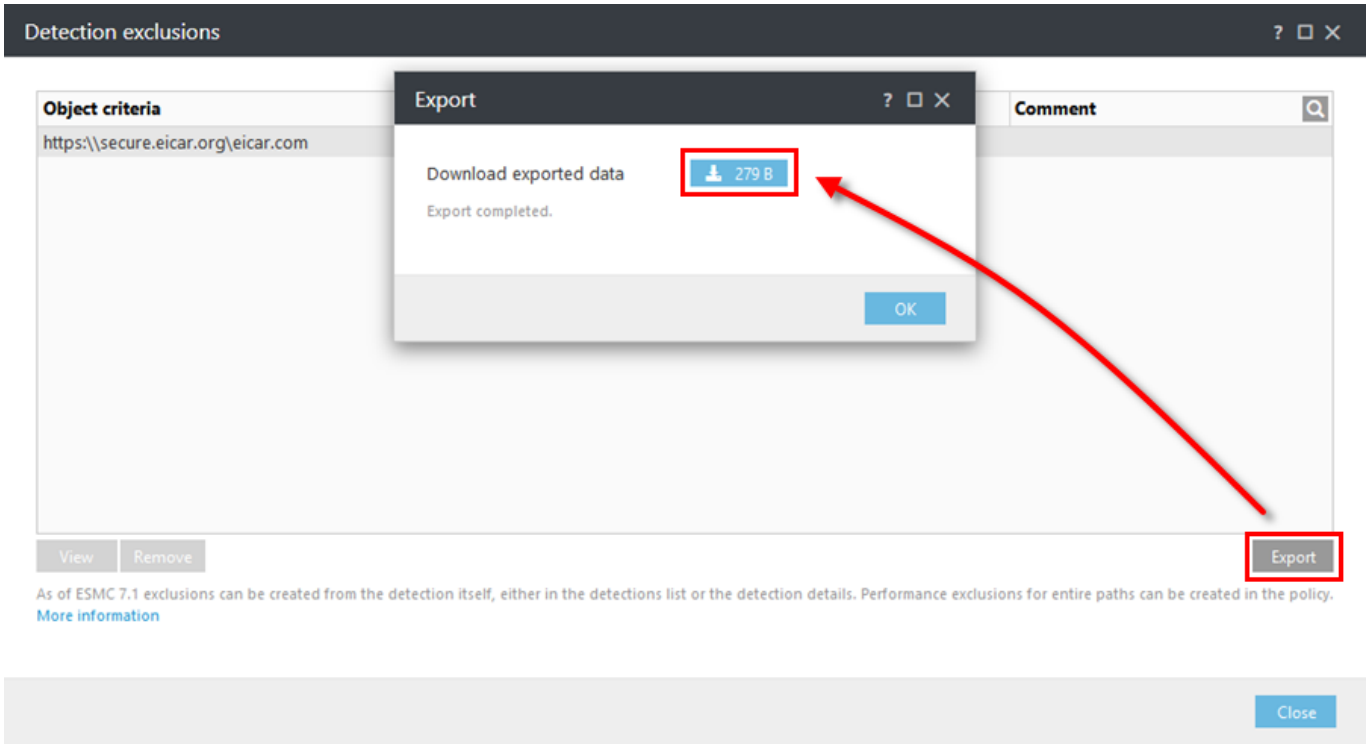
1. V hlavním menu Web Console přejděte na záložku **Politiky**. Klikněte n politiku, která obsahuje výjimky, a z kontextového menu vyberte možnost **Zobrazit detaily**.

2. Přejděte na záložku **Nastavení** a v **konfigurační šabloně** následně do sekce **Detekční jádro**.

3. Na řádku **Detekční výjimky** klikněte na možnost **Zobrazit**.

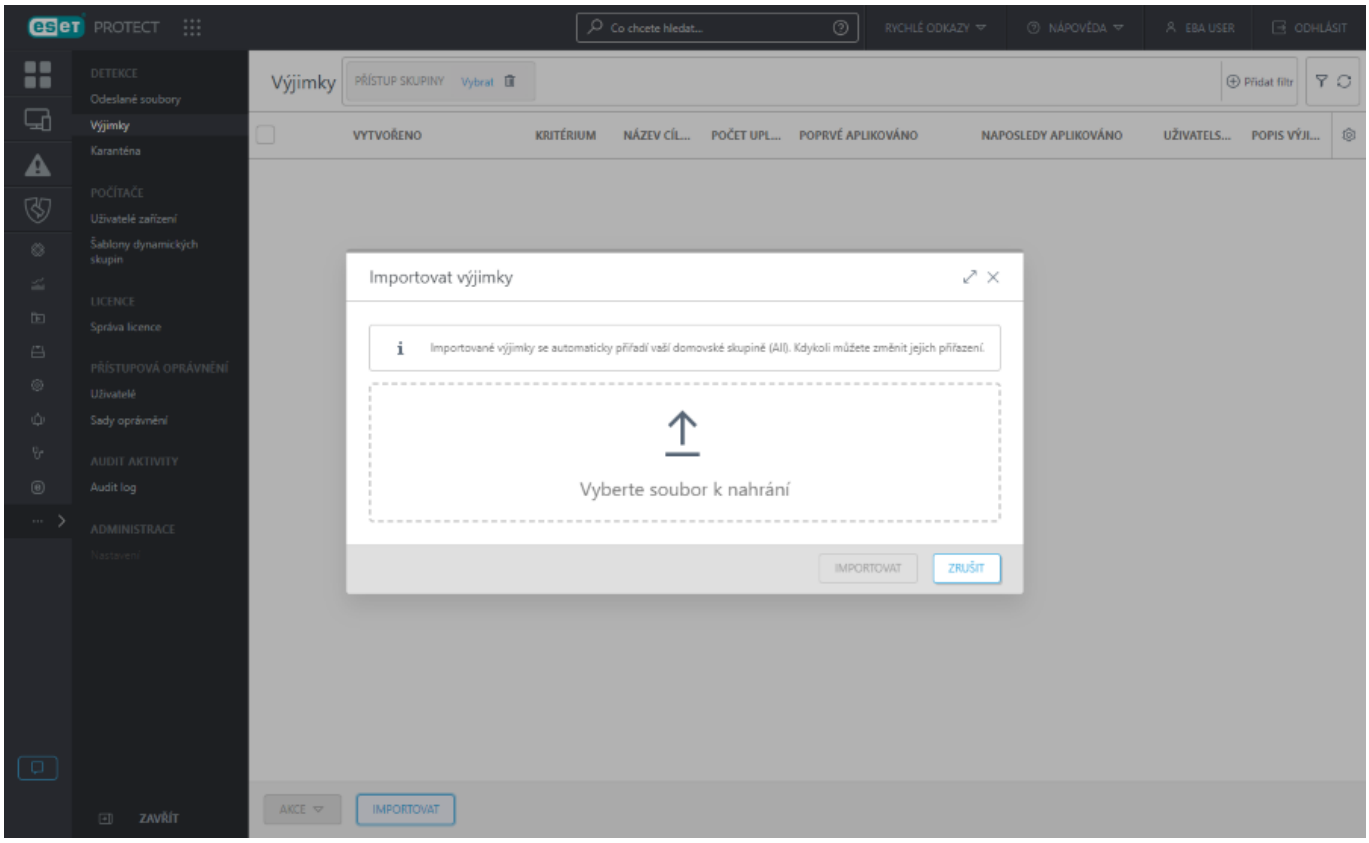


4. Klikněte na tlačítko **Exportovat**, následně na ikonu na řádku **Stáhnout exportovaná data** a soubor *export.txt* si uložte. Dále klikněte na tlačítko **OK**.



5. V hlavním menu ESET PROTECT Web Console přejděte do sekce **Další** > **Výjimky**.

6. Klikněte na tlačítko **Importovat** pro importování detekčních výjimek ze souboru. Klikněte do pole **Vyberte soubor k nahrání** a najděte stažený soubor *export.txt*, případně jej jednoduše přetáhněte.



7. Importování detekčních výjimek potvrďte kliknutím na tlačítko **Importovat**. Importované detekční výjimky se následně zobrazí v seznamu.

Omezení při přiřazování detekčních výjimek

- V průběhu migrace nedojde k zachování přiřazení. Importované detekční výjimky se automaticky přiřadí vaší domovské skupině. Pokud ji chcete přiřadit jinému cíli (počítači/skupině), klikněte na výjimku a vyberte možnost **Změnit přiřazení**.
- Mějte na paměti, že výjimky (**Antivirové** detekce a IDS pravidla **firewallu**) se aplikují pouze na kompatibilní bezpečnostní produkty ESET. Výjimky se neaplikují na nepodporované bezpečnostní produkty ESET. V takovém případě budou ignorovány.

Přizpůsobení filtrů a rozložení

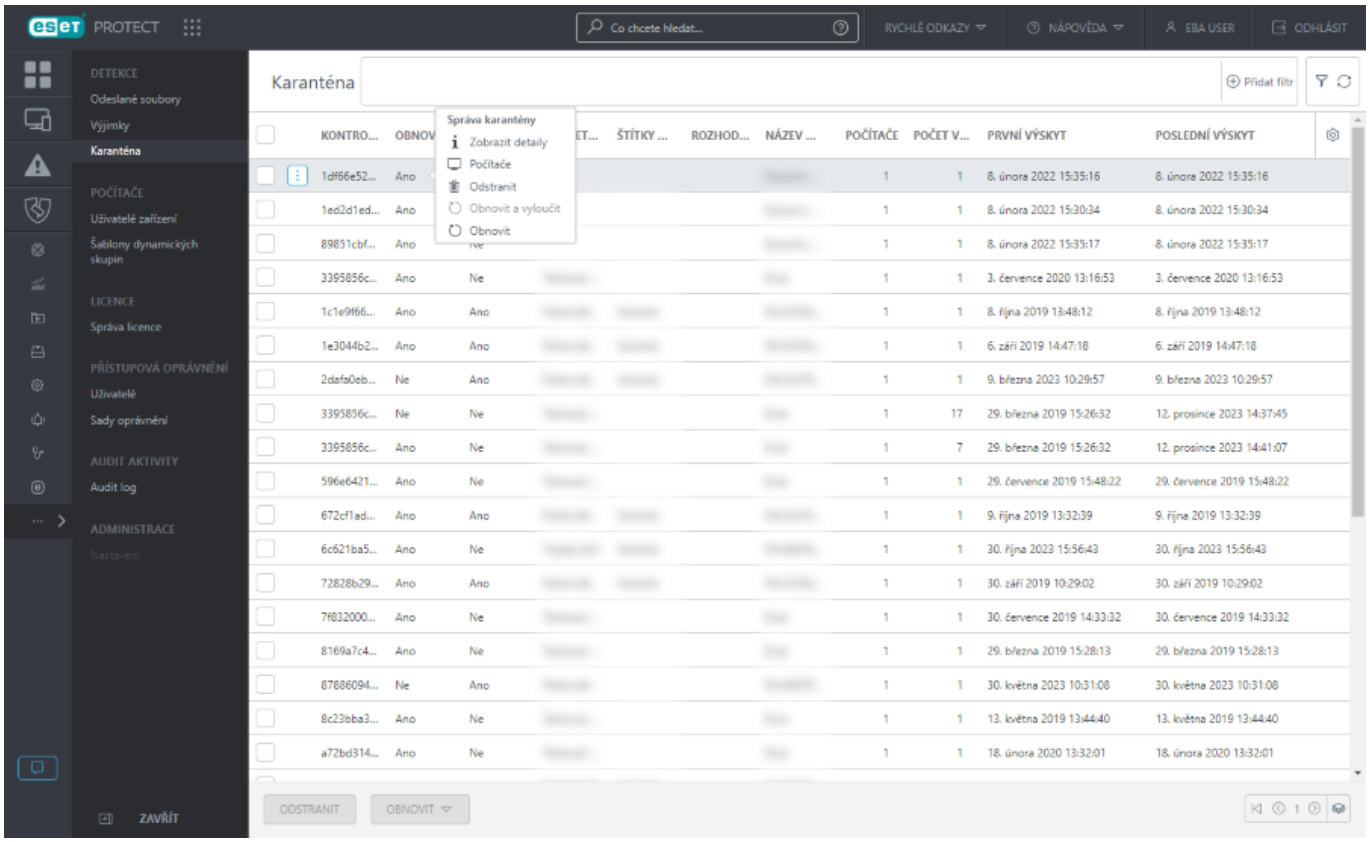
Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Karanténa

V této sekci naleznete seznam souborů, které na spravovaných stanicích přesunul do karantény bezpečnostní produkt ESET. Jedná se o soubory, které nebylo možné vyléčit, jejich odstranění by nebylo bezpečné nebo vhodné – mohlo se jednat například o falešnou detekci.

Do karantény se nepřesunují všechny objekty detekované na klientské stanici. Možné případy:
- Detekce, které nelze odstranit.
- Chování objektu je podezřelé, ale není detekován jako malware, například PUA.



Soubory z karantény můžete **Odstranit** nebo **Obnovit** do původního umístění. Vybráním možnosti **Obnovit a**

vyloučit zabránit tomu, aby jej bezpečnostní produkt znovu umístil do karantény.

Objekty v karanténě můžete filtrovat dle mnoha kritérií.

Obsah **karantény** si můžete zobrazit dvěma způsoby:

1. V hlavním menu přejděte do sekce **Další** > **Karanténa**.

2. V hlavním okně přejděte na záložku **Počítače**, vyberte konkrétní zařízení a v kontextovém menu klikněte na možnost **Zobrazit detaily**. V zobrazeném okně přejděte na záložku **Detekce a karanténa** > Karanténa.

Po kliknutí na objekt umístěný v karanténě se zobrazí **kontextové menu karantény**, ve kterém jsou k dispozici níže uvedené možnosti:

Zobrazit detaily – po kliknutí se zobrazí detaily o detekci (zdrojové zařízení, název hrozby, typ hrozby, cesta, atp.)

Počítače – kliknutím budete přesměrováni na záložku **Počítače** s aktivním filtrem zařízení, na kterém se soubor v karanténě nachází.

Odstranit – pomocí této možnosti odstraníte soubor z karantény a cílového zařízení.

Obnovit – pomocí této možnosti obnovíte soubor do jeho původního umístění.

Obnovit a vyloučit – pomocí této možnosti obnovíte soubor do jeho původního umístění a vyloučíte z detekce.

Nahrát – kliknutím vytvoříte klientskou úlohu pro získání souboru z karantény. Tato akce je dostupná po vybrání možnosti **Zobrazit detaily**.

Prostřednictví klientské úlohy pro získání souboru **nahráváte** soubor umístěný v karanténě do sdílené složky ve své síti. Proto byste měli být při použití této funkce **opatrní** a používat ji s rozmyslem.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Uživatelé zařízení

V této části můžete spravovat uživatele a skupiny uživatelů. Tuto možnost lze využít ke spárování uživatelů se zařízením, a zajistit tak synchronizaci informací o uživateli. Doporučujeme nejprve synchronizovat uživatele s Active Directory. Po vytvoření počítače jej můžete přiřadit konkrétnímu uživateli. Díky tomu snadno najdete počítač, který je uživatele, a zobrazit si o něm související informace.

Uživatele a skupiny uživatelů můžete spravovat také pro potřeby správy mobilních zařízení se systémem iOS pomocí politik přiřazených iOS zařízením. Můžete upravovat uživatele nebo přidávat Vlastní atributy.

Nezaměňujte **Uživatele zařízení** s uživateli, kteří mají přístup do **ESET PROTECT Web Console**. V této části můžete spárovat uživatele se zařízením, a zajistit tak synchronizaci informací o uživateli. Pro správu uživatelů ESET PROTECT Web Console a sad oprávnění přejděte do ESET Business Account.

- Zvýraznění uživatelé nemají přiřazeno žádné zařízení. Pro přiřazení zařízení klikněte na uživatele, v kontextovém menu vyberte možnost Změnit... a Přejděte do sekce **Přiřazená zařízení**. Pro přiřazení zařízení uživateli klikněte na možnost **Přiřadit zařízení**.

- Přiřadit nebo odebrat zařízení **uživateli** můžete přímo z detailů počítače. V hlavním menu na záložce **Počítače** najděte konkrétní zařízení, klikněte na něj a v kontextovém menu vyberte možnost **Zobrazit detaily**. Uživatel může mít přiřazeno více zařízení. Následně v detailech zařízení v sekci Přehled klikněte na možnost **Přidat uživatele** na dlaždici Uživatelé. Tím daného uživatele přiřadíte přímo zařízení. Pokud již je zařízení přiřazen uživatel, po kliknutí na jeho jméno si zobrazíte detailní informace.

- Uživatele a skupiny můžete pohodlně přesouvat také prostřednictvím techniky Drag & Drop. Vyberte uživatele nebo skupinu, podržte pravé tlačítko myši a přesuňte ji.

Akce dostupné v kontextovém menu uživatele:

V kontextovém menu uživatele můžete provádět další akce. Více informací o jednotlivých ikonách naleznete v kapitole legenda ikon.

Zobrazit detaily – kliknutím zobrazíte detailní informace jako je **e-mailová adresa**, **lokalita** nebo **přiřazená zařízení**. Uživatel může mít přiřazeno více než jedno zařízení. Přímo v tomto dialogovém okně můžete uživatele **přejmenovat**, přidat uživateli **popis** nebo změnit **nadřazenou skupinu**, do které patří. Při vytváření MDM politik pro iOS zařízení můžete použít **vlastní atributy**.

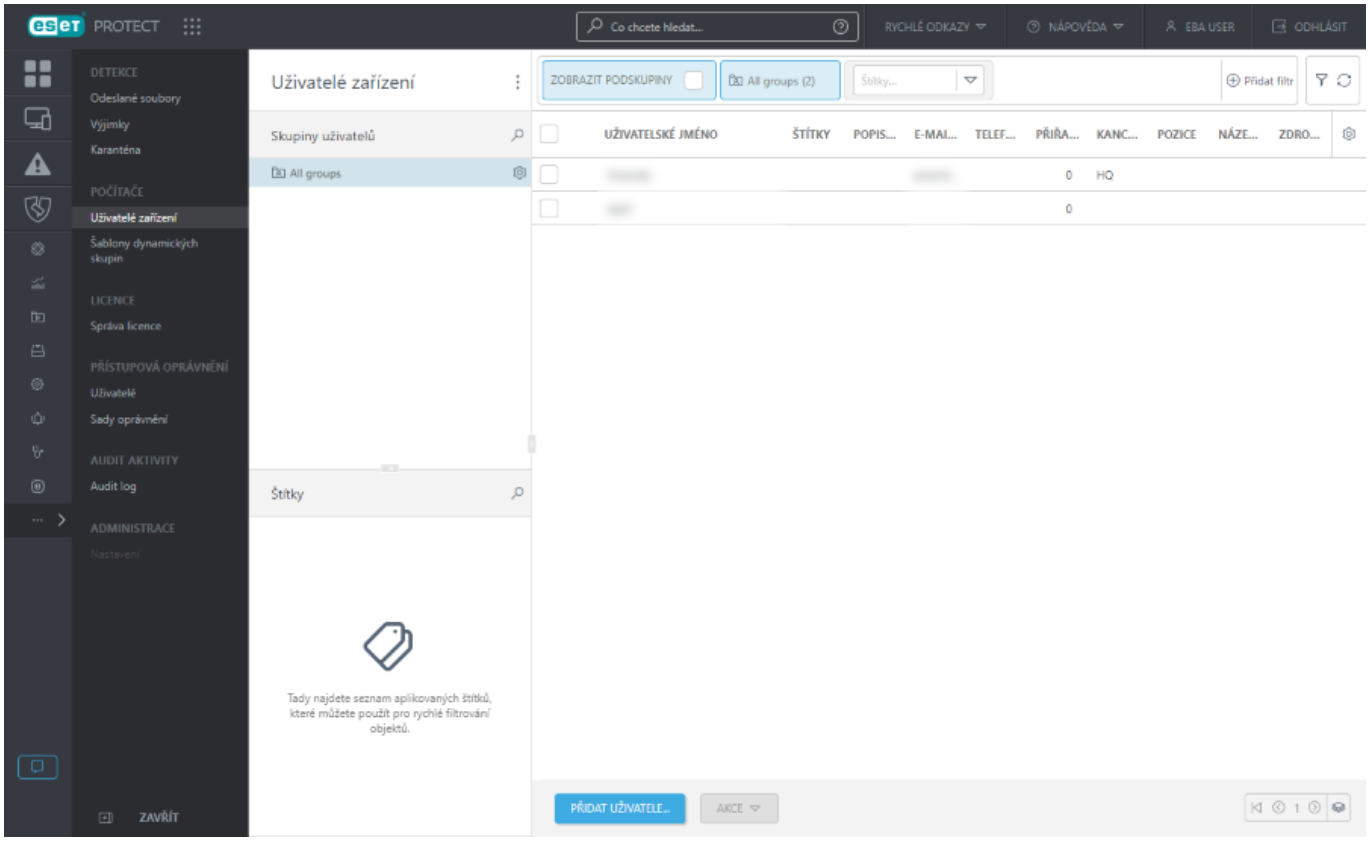
Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Přidání nových uživatelů

1. Pro přidání uživatele klikněte v hlavním menu na **Uživatelé zařízení** > **Přidat uživatele**. Tuto možnost využijte pro ruční přidání uživatelů, kteří nebyli načteni automaticky prostřednictvím serverové úlohy Synchronizace uživatelů.



2. Nejprve zadejte **jméno uživatele**. Pro přidání dalších uživatelů klikněte na +**Přidat**. Velké množství uživatelů můžete přidat hromadně importováním z CSV, kdy nahrajete na server *.csv* soubor obsahující seznam uživatelů. **Kopírovat a vložit** – po kliknutí můžete seznam adres zkopírovat ze schránky (tato funkce funguje podobně jako Import CSV). Volitelně můžete přidat **popis**, pro snadnější identifikaci uživatele.

3. **Nadřazenou skupinu** můžete vybrat již existující nebo vytvořit novou.

4. Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.

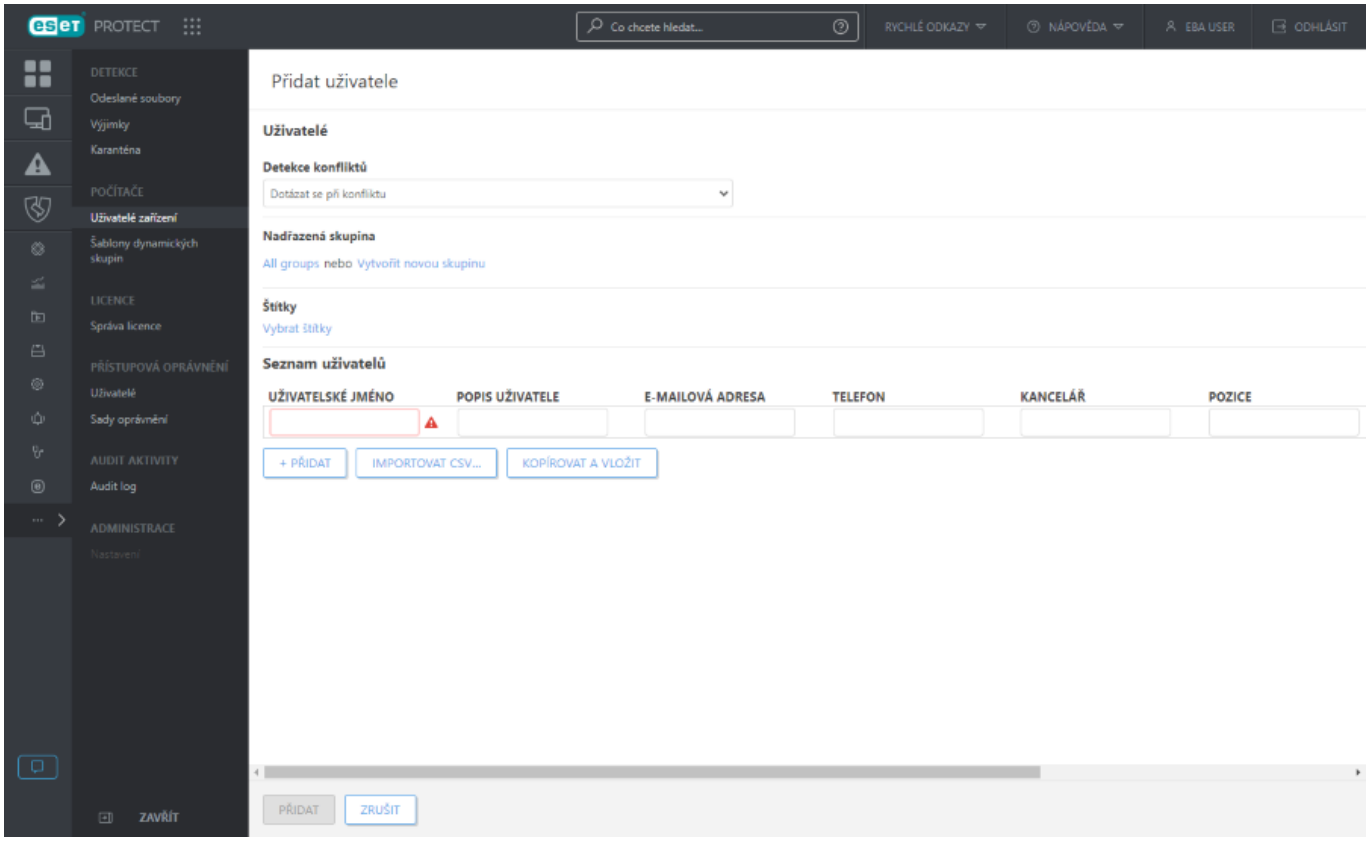
5. Z rozbalovacího menu **Detekce konfliktů** vyberte akci, která se má provést, pokud již uživatel v ESET PROTECT existuje:

- **Dotázat se při konfliktu** – když je zjištěn konflikt, program vás požádá o výběr akce (viz možnosti níže).

- **Přeskočit konfliktní uživatele** – uživatelé se stejným jménem nebudou přidáni. Tuto možnost použijte také v případě, kdy v ESET PROTECT využíváte vlastní atributy, a nechcete, aby došlo k jejich přepsání při synchronizaci s Active Directory.

- **Přepsat konfliktní uživatele** – stávající uživatelé v ESET PROTECT budou přepsáni uživateli z Active Directory. Pokud má uživatel stejné SID, existující uživatel v ESET PROTECT bude odstraněn ze skupiny, ve které byl zařazen.

6. Akci dokončete kliknutím na tlačítko **Přidat**. Uživatel se vytvoří v nadřazené skupině uživatelů.



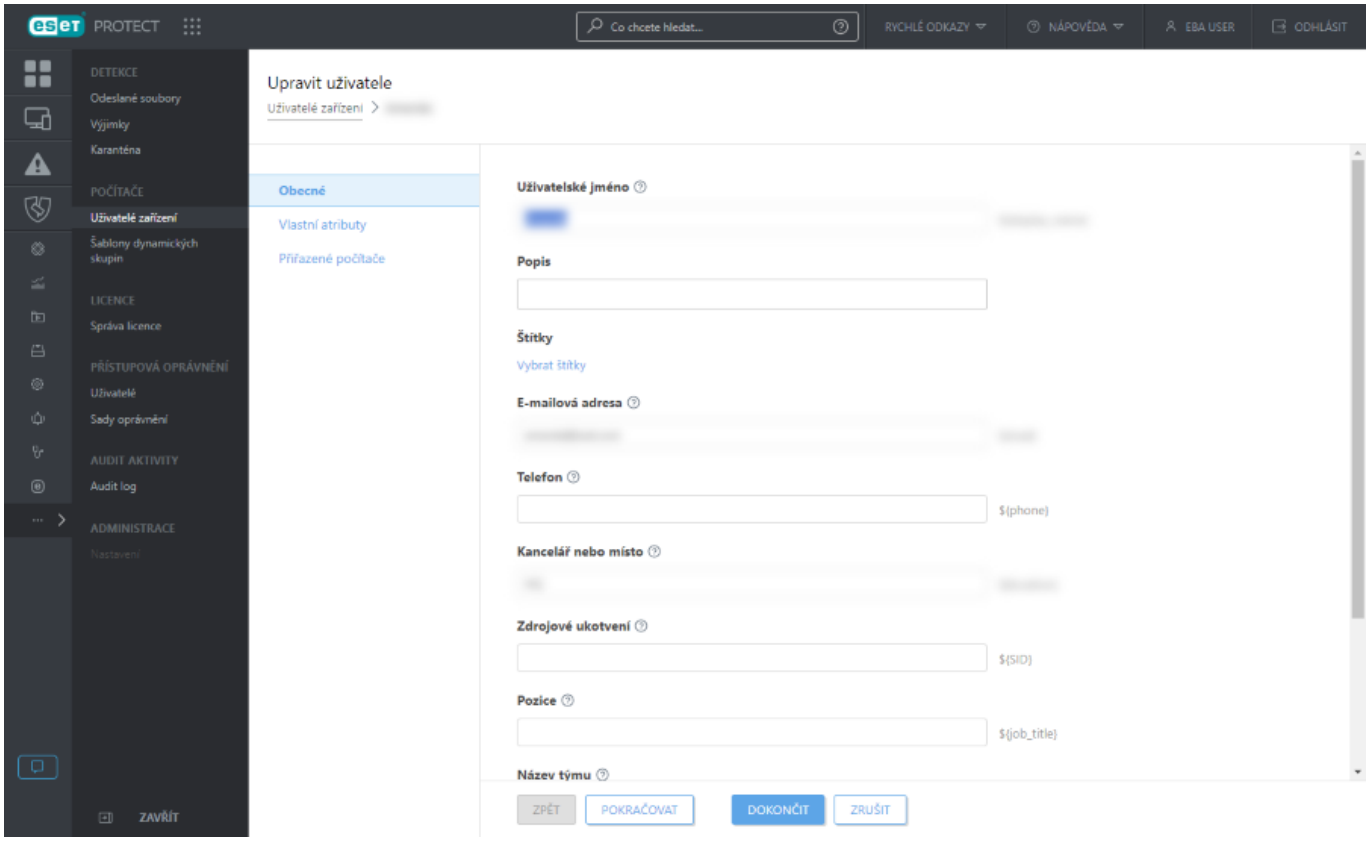
Úprava uživatelů

V detailech uživatele můžete upravit **obecné informace**, stejně tak seznam **přiřazených zařízení**.

Obecné

Detaily uživatele zahrnují:

- **Jméno uživatele** a **popis** – výhradně pro informativní účely.
- **Štítky** –Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
- **E-mailová adresa** – adresa příjemce oznámení.
- **Telefon** a **Kancelář nebo místo** – pouze pro informativní účely.
- **Zdrojové ukotvení** – můžete být spojeno s některými funkcemi ESET PROTECT, které vyžadují informace z AD (například režim dočasné změny nastavení v politikách pro koncová zařízení).



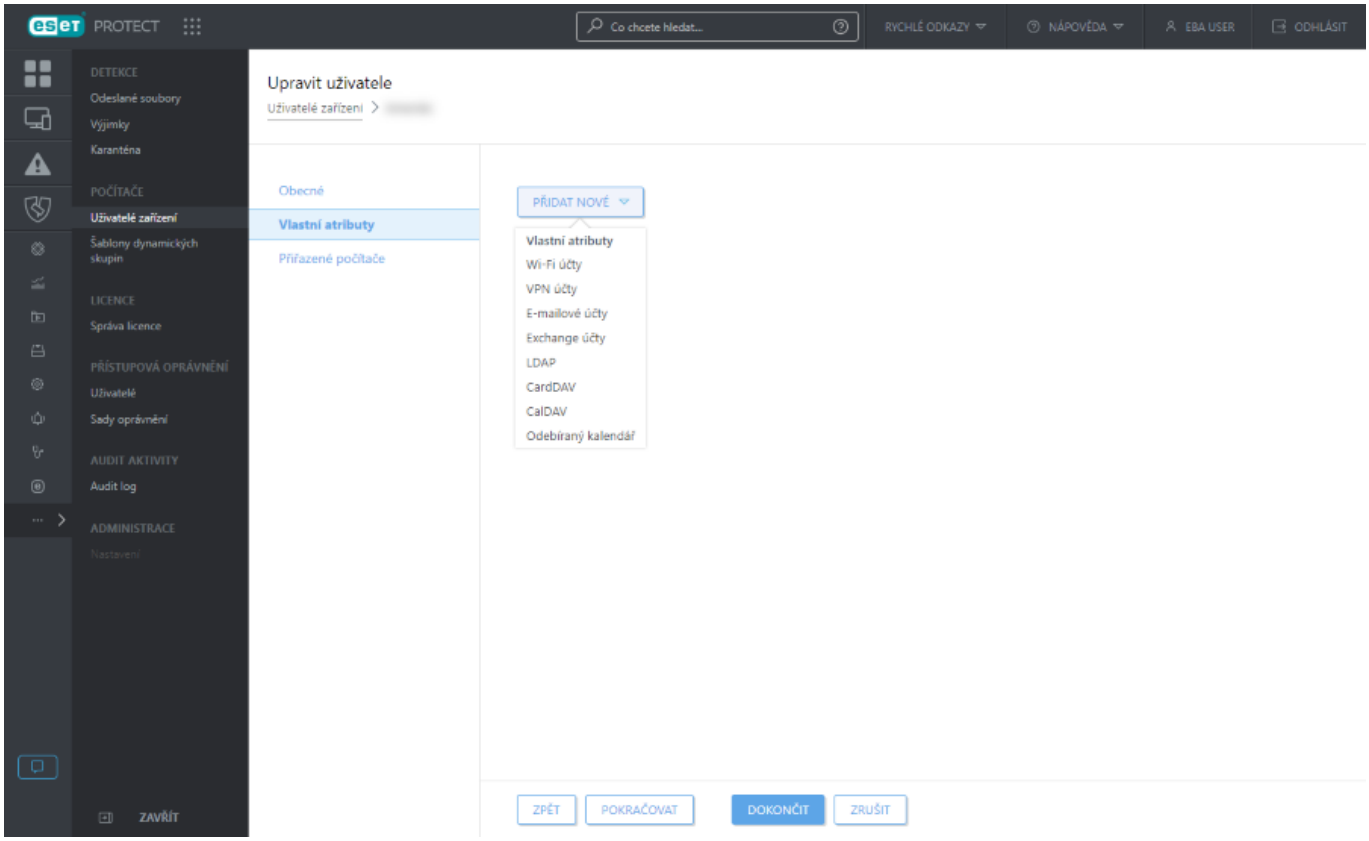
Vlastní atributy

V této části kliknutím na Přidat nový můžete uživatelskému účtu přiřadit další atribut. Po kliknutí na tlačítko **Přidat nové** si vyberte kategorii:

- **Wi-Fi účty** – profily lze použít k přenesení firemních nastavení Wi-Fi přímo do spravovaných zařízení.
- **VPN účty** – můžete nastavit VPN spolu s přihlašovacími údaji, certifikáty a dalšími potřebnými informacemi, aby byla VPN snadno dostupná pro uživatele.
- **E-mailové účty** – používá se pro všechny e-mailové účty, které používají IMAP nebo POP3. Pokud využíváte Exchange server, využijte níže uvedené nastavení Exchange ActiveSync.
- **Exchange účty** – pokud vaše společnost používá Microsoft Exchange, můžete zde vytvořit veškerá nastavení, abyste co nejvíce krátili dobu nastavování přístupu uživatelů k poště, kalendáři a kontaktům.
- **LDAP (alias atributu)** – tato funkce je užitečná zejména v případě, že vaše společnost využívá LDAP pro kontakty. Prostřednictvím této možnosti spárujete LDAP kontakty s iOS kontakty.
- **CalDAV** – obsahuje nastavení pro jakýkoli kalendář, který používá specifikace CalDAV.
- **CardDAV** – pro kontakty synchronizované prostřednictvím specifikace CardDAV lze informace pro synchronizaci nastavit zde.
- **Odebíraný kalendář** – pokud jsou nastaveny nějaké kalendáře CalDAV, můžete zde nastavit přístup ke kalendářům ostatních pouze pro čtení.

Některá z polí se stanou atributem, který pak lze jako proměnnou použít při vytváření politik pro mobilní zařízení se systémem iOS. Např.: Přihlášení `${exchange_login/exchange}` nebo E-mailová adresa

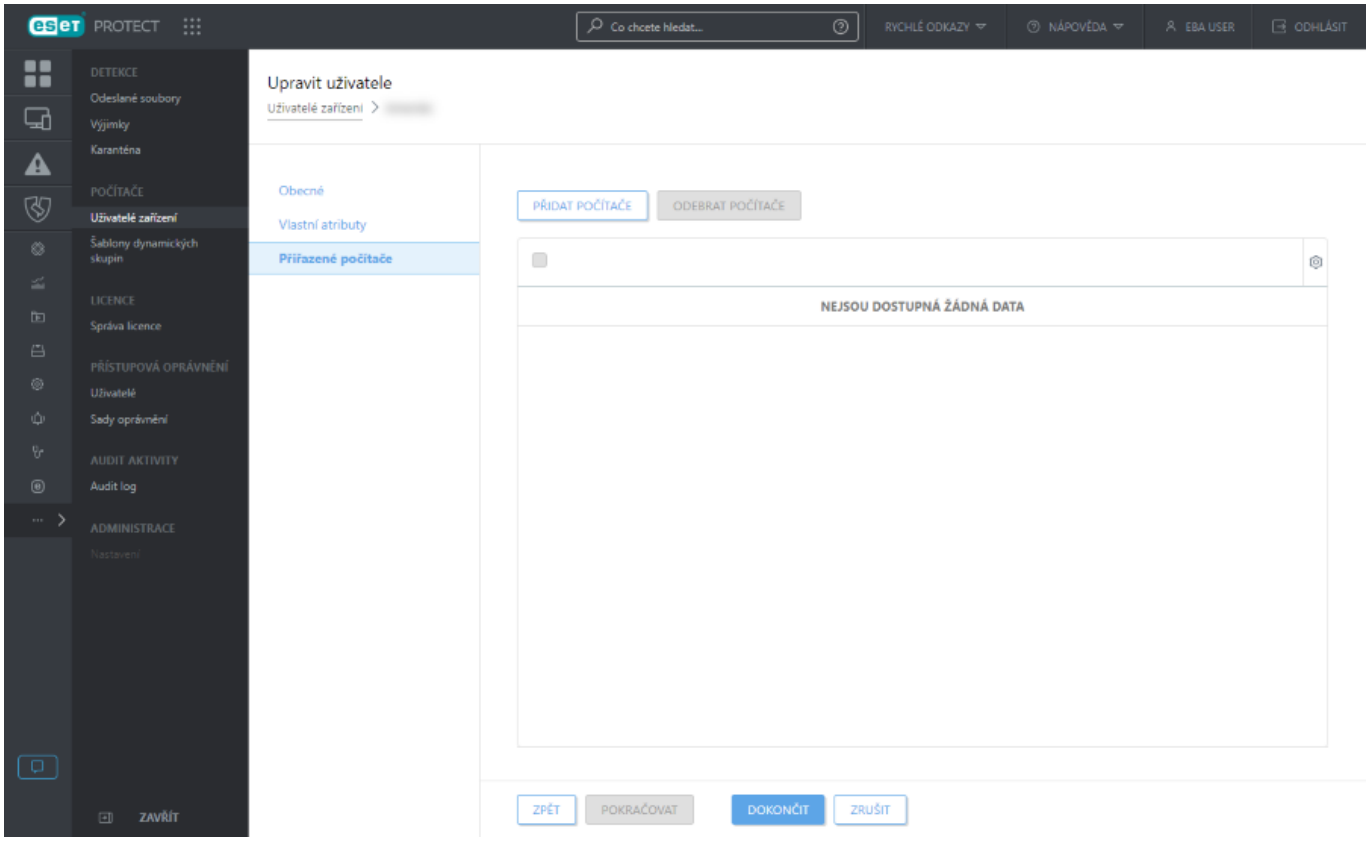
${exchange_email/exchange}.



Přiřazená zařízení

V této části můžete vybrat konkrétní zařízení, které uživateli patří. Po kliknutí na **Přidat počítače** se zobrazí seznam všech statických a dynamických skupin a jejich členů. Vyberte požadované zařízení a klikněte na tlačítko **OK**.

V rámci jedné operace je možné uživateli přiřadit nejvýše 200 počítačů.

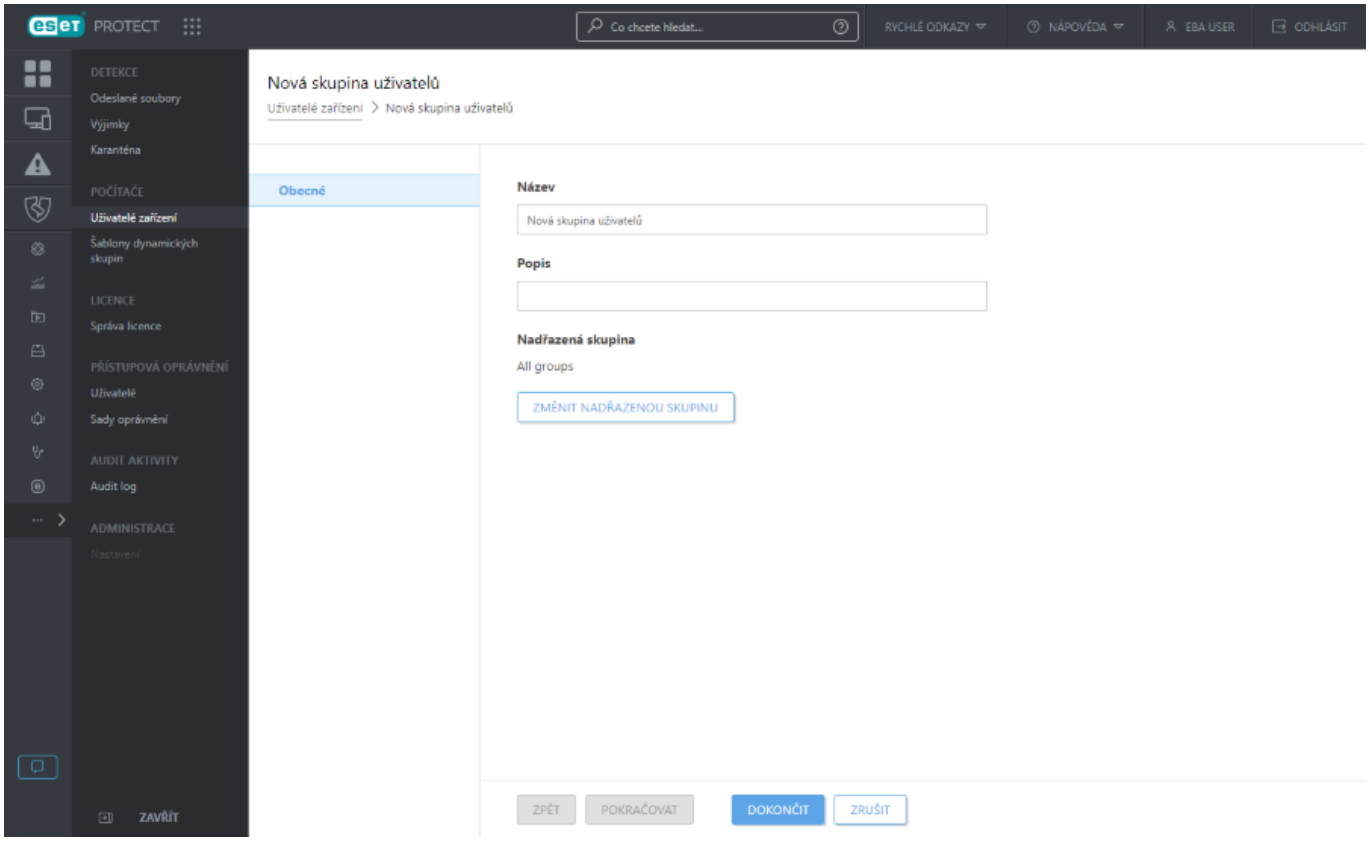


Vytvoření nové skupiny uživatelů

Pro vytvoření nové skupiny uživatelů přejděte v hlavním menu do sekce **Uživatelé zařízení**. Vyberte nadřazenou skupinu, klikněte na ozubené kolečko a vyberte možnost **Nová skupina uživatelů…**.

Obecné

Zadejte **název, volitelně popis**, nové vytvářené skupiny uživatelů. V případě potřeby si můžete změnit nadřazenou skupinu. Jako nadřazená skupina se použije skupina, kterou jste vybrali předtím, než jste otevřeli tohoto průvodce. Pro změnu nadřazené skupiny klikněte na tlačítko **Změnit nadřazenou skupinu** a vyberte požadovanou skupinu. Nadřazená skupina může být libovolná (statická i dynamická). Pro dokončení akce klikněte na tlačítko **Dokončit**.



Šablony dynamických skupin

Počítač se stane automaticky členem dynamické skupiny ve chvíli, kdy jeho stav bude vyhovovat podmínce definované v šabloně dynamické skupiny. Agent rozhoduje o tom, do které dynamické skupiny klient patří, a na server odesílá pouze informace o výsledném rozhodnutí. Více informací naleznete v níže uvedených kapitolách:

Šablona dynamické skupiny je statický objekt uložený v konkrétní statické skupině. Aby měl k šabloně uživatel přístup, musí mít přiděleno potřebné oprávnění. V opačném případě nebude schopen se šablonami pracovat a vytvářet na základě nich dynamické skupiny. Všechny předdefinované šablony dynamických skupin jsou umístěny ve statické skupině **Všechna zařízení** a má k nim přístup standardně pouze uživatel Administrator. Pokud chcete dalším uživatelům přidělit přístup k použití těchto šablon, přidělte jim další oprávnění. V opačném případě uživatelé tyto výchozí šablony neuvidí. Případně šablony přesuňte je do jiné statické skupiny, do níž mají uživatelé oprávnění přístup k těmto objektům.
Pro duplikování šablon musí mít uživatel oprávnění pro **použití** objektu (šablona dynamické skupiny) ve zdrojové skupině a následně oprávnění pro **zápis** ve své domovské, v níž se kopie objektu vytvoří. Dále se podívejte na příklady duplikování objektů.

- Vytvoření šablony dynamické skupiny
- Pravidla pro vytváření šablony dynamické skupiny
- Vzorové příklady šablon dynamických skupin

Správa šablon dynamických skupin

Šablony můžete spravovat v sekci **Další** > **Šablony dynamických skupin**. V kontextovém menu jsou dostupné tyto možnosti:

Nová šablona	Kliknutím vytvoříte ve své domovské skupině novou šablonu přehledu.
Zobrazit detaily	Kliknutím si zobrazíte detaily o vybrané šabloně.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
Změnit...	Kliknutím upravíte vybranou šablonu. Pokud kliknete na možnost **Uložit jako**, budete vyzváni k zadání názvu nově vytvářené šablony a vytvoříte ve své domovské skupině kopii existující šablony. Následně budete vyzváni k zadání názvu nově vytvářené šablony.
Duplikovat	Kliknutím vytvoříte novou šablonu dynamické skupiny na základě existující. Při jejím vytváření bude vyžadováno zadání názvu nově vytvářené šablony. Kopie se vytvoří ve vaší domovské skupině.
Odstranit...	Kliknutím odstraníte šablonu přehledu.
Importovat...	Kliknutím importujete šablony dynamických skupin ze souboru. V průběhu importování je ověřována struktura souboru, zda není poškozen.
Exportovat...	Kliknutím exportujete šablony dynamických skupin do souboru. To je užitečné v průběhu migrace nebo za účelem zálohování. Výsledný soubor nedoporučujeme modifikovat. Může dojít k poškození dat.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.
- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Nová šablona dynamické skupiny

V hlavním menu přejděte do sekce **Další** > **Šablony dynamických skupin** a klikněte v dolní části okna na tlačítko **Nová šablona**.

Obecné

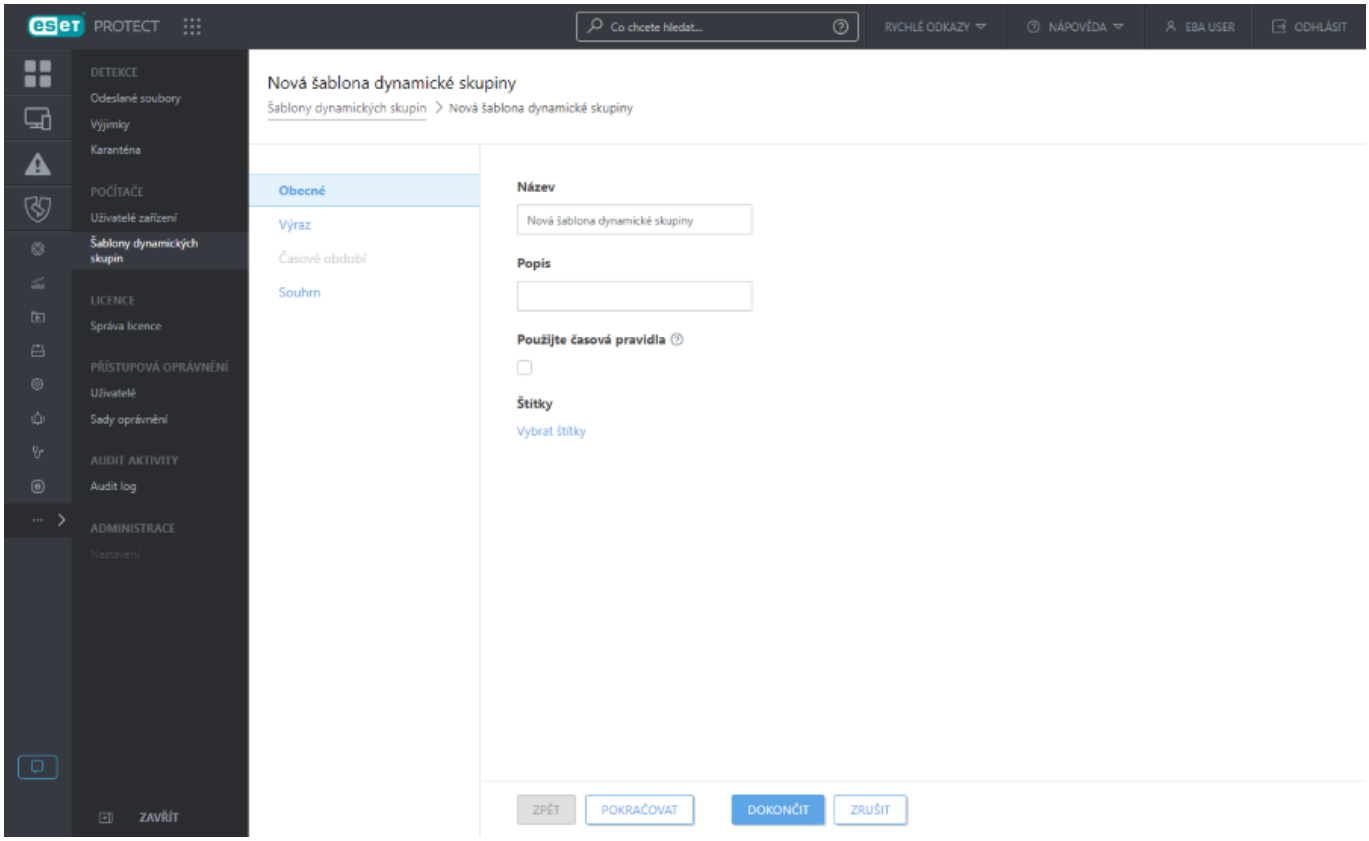
Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.

Výraz

Při vytváření se můžete inspirovat příklady, na kterých lépe pochopíte princip dynamických skupin.



Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

Pravidla pro šablony dynamických skupin

Při vytváření šablon dynamických skupin můžete použít velké množství logických i porovnávacích operátorů.

V dalších kapitolách naleznete podrobnější informace, které pomohou pochopit princip fungování dynamických skupin, a také užitečné tipy pro jejich vytváření.

- Operace
- Podmínky a logické spojky
- Vyhodnocování parametrů šablony
- Možnosti automatizace v ESET PROTECT

- Šablony dynamických skupin
- Vzorové příklady šablon dynamických skupin

Operace

Při definování více pravidel (podmínek) je nutné vybrat operátor, který se použije při jejich sloučení (vyhodnocení) V závislosti na výsledku se počítač stane členem dynamické skupiny používající tuto šablonu, nebo nikoli.

- Vybraný **operátor** funguje nejen v kombinaci více pravidel, ale také při jediném pravidle.
- Operátory není možné kombinovat. Při vytváření šablony dynamické skupiny můžete použít vždy jeden operátor a ten se aplikuje na všechny operandy.

AND – všechny definované podmínky musí být splněny.	Ověří, zda jsou všechny podmínky pravdivé (pozitivní) – počítač musí vyhovět všem požadovaným parametrům.
OR – alespoň jedna z definovaných podmínek musí být splněna.	Ověří, zda je alespoň jedna podmínka pravdivé (pozitivní) – počítač musí vyhovět alespoň jednomu požadovanému parametru.
NAND – alespoň jedna z podmínek nesmí být splněna.	Ověří, zda je alespoň jedna podmínka nepravdivá (negativní) – počítač nesmí vyhovět alespoň jednomu požadovanému parametru.
NOR – žádná z podmínek nesmí být splněna.	Ověří, zda jsou všechny podmínky nepravdivé (negativní) – počítač nesmí vyhovět žádnému požadovanému parametru.

Podmínky a logické spojky

Šablona dynamické skupiny se skládá z pravidel, která jsou mezi sebou spojena logickými operátory/spojkami.

Po kliknutí na **+ Přidat pravidlo** se zobrazí dialogové okno s mnoha položkami rozdělenými do kategorií. Příklad:

Instalované aplikace > **Název aplikace**

Síťové adaptéry > **MAC adresa**

Edice OS > **Název OS**

Seznam dostupných pravidel naleznete v Databázi znalostí.

Pro vytvoření pravidla vyberte podmínku, logický operátor a zadejte hodnotu. Zadaná hodnota bude vyhodnocena v závislosti na použitém operátoru.

Jako hodnoty můžete použít řetězce, čísla, výčtové typy, IP adresy, masky produktu a identifikátory (například počítače, písmen disků atp.). Jednotlivé typy hodnot se pojí pouze s některými logickými operátory. ESET PROTECT Web Console vždy zobrazí pouze ty relevantní.

- **"= (rovná se)"** – cílový řetězec musí přesně odpovídat zadané hodnotě. Při porovnávání se nerozlišuje velikost písmen.
- **"> (větší než)"** – hodnota je větší než definovaná. Tento operátor můžete použít také při definování rozsahu IP adres.

• **"≥ (větší nebo rovno)"** – hodnota je větší nebo rovna hodnotě definované. Tento operátor můžete použít také při definování rozsahu IP adres.

• **"< (menší než)"** – hodnota je menší než definovaná. Tento operátor můžete použít také při definování rozsahu IP adres.

• **"≤ (menší nebo rovno)"** – hodnota je menší nebo rovna hodnotě definované. Tento operátor můžete použít také při definování rozsahu IP adres.

• **"obsahuje"** – vyhledá zadané znaky v cílovém řetězci. V případě řetězce se vyhledává podřetězec. Při vyhledávání se nerozlišuje velikost písmen.

• **"má předponu"** – vyhledá na začátku cílového řetězce definované znaky. Při porovnávání se nerozlišuje velikost písmen. Například v řetězci "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319" předpona představuje "Micros", "Micr" nebo "Microsof" atp.

• **"má příponu"** – vyhledá na konci cílového řetězce definované znaky. Při porovnávání se nerozlišuje velikost písmen. Například v řetězci "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319" přípona představuje "319" nebo "0.30319" atp.

• **"má masku"** – hodnota musí vyhovovat definované masce v šabloně. Při definování masky můžete použít jakékoli znaky a doplnit je o speciální symboly: '*' – představuje libovolný počet znaků (0 a více) a '?' nahrazuje právě jeden znak. Příklad: "6.2.*" nebo "6.2.2033.?".

• **"regex"** – hodnota musí vyhovovat definovanému regulárnímu výrazu. Regex je nutné zadat v **Perl** syntaxi.

Regulární výraz, *regex* resp. *regexp* je sekvence znaků definující vyhledávací masku. Například *gray|grey* a *gr(a|e)y* jsou ekvivalentní zápisy, které vyhovují slovům "*gray*", "*grey*".

• **"je jeden z"** – hodnota se musí shodovat z libovolnou hodnotou v seznamu šablony. Pro přidání další hodnoty klikněte na **+ Přidat**. Každý řádek představuje jeden záznam v seznamu. Při porovnávání se nerozlišuje velikost písmen.

• **"je jeden z (maska řetězce)"** – hodnota musí odpovídat masce libovolné hodnoty v seznamu. Při porovnávání se nerozlišuje velikost písmen. Příklady: *endpoint-pc*, *Endpoint-PC*.

• **"má hodnotu"**

Pro vytvoření šablony dynamické skupiny, která bude sledovat čas uplynulý od definované události, zaškrtněte možnost **Změřit uplynulý čas**. Tím aktivujete časová pravidla. Na stanici musí být nainstalován ESET Management Agent ve verzi 10.0 a novější.

Negativní spojky:

Mějte na paměti, že negativní spojky netestují neexistenci. Negativní operátory používejte opatrně, protože v případě protokolů, které obsahují více řádků, například Nainstalované aplikace, jsou vyhodnocovány všechny řádky. Pro pochopení principu jejich použití se podívejte na vzorové příklady šablon dynamických skupin a Vyhodnocování parametrů šablony.

• **"≠ (nerovná se)"** – cílový řetězec nesmí odpovídat zadané hodnotě. Při porovnávání se nerozlišuje velikost písmen.

• **"neobsahuje"** – cílový řetězec nesmí obsahovat definované znaky. Při vyhledávání se nerozlišuje velikost písmen.

• **"nemá předponu"** – zjistí, zda se na začátku cílového řetězce nenachází definované znaky. Při porovnávání se nerozlišuje velikost písmen.

• **"nemá příponu"** – zjistí, zda se na konci cílového řetězce nenachází definované znaky. Při porovnávání se nerozlišuje velikost písmen.

• **"nemá masku"** – cílový řetězec nesmí vyhovovat definované šabloně.

• **"není regex"** – cílový řetězec nesmí vyhovovat definovanému regulárnímu výrazu (regex). Regex je nutné zadat v **Perl** syntaxi. Tato možnost je dostupná pro zjednodušení, abyste nemuseli používat negativní regulární výrazy.

• **"není v"** – cílový řetězec v celém seznamu nesmí vyhovovat zadané hodnotě. Při porovnávání se nerozlišuje velikost písmen.

• **"není v (maska řetězce)"** – cílový řetězec nesmí vyhovovat definované masce.

• **"nemá hodnotu"**

Vyhodnocování parametrů šablony

Parametry šablony vyhodnocuje ESET Management Agent, nikoli ESET PROTECT server – na ESET PROTECT server je odeslán pouze výsledek. V průběhu vyhodnocování ESET_MNG Agent zjišťuje, zda daný počítač vyhovuje podmínkám definovaným v šabloně dynamické skupiny. Níže si na několika příkladech vysvětlíme proces vyhodnocování.

Při tvorbě podmínek je nutné rozlišovat testování existence (něco s určitou hodnotou neexistuje) a testování rozdílu (něco existuje, ale má jinou hodnotu). Níže uvádíme základní pravidla pro pochopení rozdílu:
• Pro ověření existence: Operace bez negace (**AND**, **OR**) a operátor bez negace (=, >, <, **obsahuje**,...).
• Pro ověření existence odlišné hodnoty: Operace **AND** a operátory obsahující alespoň jednu negaci (=, >, <, **obsahuje**, **neobsahuje**,...).
• Pro ověření neexistence hodnoty: Operace s negací **NAND** nebo **NOR** a operátory bez negace (=, >, <, **obsahuje**, …).
Pro ověření přítomnosti seznamu položek (například seznamu konkrétních aplikací nainstalovaných na počítači) vytvořte pro každou položku v seznamu samostatnou dynamickou skupinu, a každou z nich vytvářejte jako potomka předchozí. Počítač se všemi položkami se stane členem poslední podskupiny.

Stav počítače je souhrn mnoha informací reprezentovaný tabulkou. U některých dat ESET_MNG Agent získá pouze jeden záznam (operační systém, velikost RAM atp.), v jiných případech (IP adresy, instalované aplikace atp.) může získat více záznamů.

Vizualizace získaných dat z klienta:

IP adresa síťového adaptéru	MAC adresa síťového adaptéru	Název OS	Verze OS	Velikost RAM (v MB)	Instalované aplikace

IP adresa síťového adaptéru	MAC adresa síťového adaptéru	Název OS	Verze OS	Velikost RAM (v MB)	Instalované aplikace
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Výsledný stav je složen ze skupin informací (sloupců tabulky). Každá skupina dat obsahuje souvislé informace uspořádané do řádků. Počet řádků se může v každé skupině lišit.

Podmínky jsou vyhodnocovány podle skupin a řádků – pokud je definováno více podmínek pro skupinu, vyhodnocovány jsou jen hodnoty v daném řádku.

Příklad 1:

Máme definovanou podmínku:

```
IP adresa síťového adaptéru = 10.1.1.11 AND MAC adresa síťového adaptéru = 4A-64-3F-10-FC-75
```

V tomto případě pravidlu nevyhovuje žádný počítač, protože neexistuje žádný řádek, ve kterém by byly obě hodnoty pravdivé.

IP adresa síťového adaptéru	MAC adresa síťového adaptéru	Název OS	Verze OS	Velikost RAM (v MB)	Instalované aplikace
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Příklad 2:

Máme definovanou podmínku:

```
IP adresa síťového adaptéru = 192.168.1.2 AND MAC adresa síťového adaptéru = 4A-64-3F-10-FC-75
```

V tomto případě obě buňky na řádku vyhovují podmínce, a proto je pravidlo vyhodnoceno jako pravdivé (TRUE). Počítač bude zařazen do dynamické skupiny, která používá tuto šablonu.

IP adresa síťového adaptéru	MAC adresa síťového adaptéru	Název OS	Verze OS	Velikost RAM (v MB)	Instalované aplikace
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security

IP adresa síťového adaptéru	MAC adresa síťového adaptéru	Název OS	Verze OS	Velikost RAM (v MB)	Instalované aplikace
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Příklad 3:

Máme definovanou podmínku:

```
IP adresa síťového adaptéru = 10.1.1.11 OR MAC adresa síťového adaptéru = 4A-64-3F-10-FC-75
```

V tomto případě podmínce vyhovují dva počítače, protože stačí, aby byla splněna jen jedna z jejich částí. Počítač bude zařazen do dynamické skupiny, která používá tuto šablonu.

IP adresa síťového adaptéru	MAC adresa síťového adaptéru	Název OS	Verze OS	Velikost RAM (v MB)	Instalované aplikace
192.168.1.2	4A-64-3F-10-FC-75	Windows 11 Enterprise	10.0.22621	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Vzorové příklady šablon dynamických skupin

Předdefinované šablony naleznete v sekci **Další** > **Šablony dynamických skupin**.

Připravili jsme několik vzorových šablon dynamických skupin, které vám přiblíží jejich fungování a můžete je využít ve své síti:

Dynamická skupina – počítač chráněný bezpečnostním produktem ESET
Dynamická skupina – počítač s aplikací v konkrétní verzi
Dynamická skupina – počítač, na kterém není nainstalován žádná aplikace nebo v požadované verzi
Dynamická skupina – aplikace je nainstalovaná, ale v jiné verzi
Dynamická skupina – počítač je v definované síti
Dynamická skupina – nainstalovaný, ale neaktivovaný serverový produkt
Jak automaticky nainstalovat bezpečnostní produkt ESET na nově připojenou stanici s OS Windows
Vynucení politiky na základě polohy klienta

Příklady dynamických skupin a jejich použití naleznete také v **Databázi znalostí** v článcích:

Příklady užitečných šablon dynamických skupin v ESET PROTECT – příklady, jak využít Inventář hardware k vytvoření pravidel pro dynamické skupiny, jejichž součástí jsou zařízení, která vybraná hardwarová kritéria splňují.
Konfigurace ESET PROTECT pro automatické nasazení bezpečnostní produktů pro koncová zařízení na nechráněné stanice
Konfigurace bezpečnostních produktů pro koncová zařízení pro použití odlišných aktualizačních profilů v závislosti na připojené síti
Vytvoření nového certifikátu pro pracovní stanice připojeném v ESET PROTECT automaticky do dynamické skupiny

Články v databázi znalostí nemusí být dostupné ve vašem jazyce.

Kombinací vhodných operátorů a podmínek jste schopni dosáhnout vysoké míry automatizace. Záleží pouze na vašich požadavcích, protože možnosti tvorby dynamických skupin jsou téměř neomezené.

Dynamická skupina – počítač chráněný bezpečnostním produktem ESET

Tuto dynamickou skupinu můžete použít pro automatizaci úloh, které chcete provést okamžitě po nainstalování produktu na stanici, například: aktivace, kontrola počítače, atp.

V hlavním menu Web Console přejděte do sekce **Další** > **Šablony dynamických skupiny** a vytvořte novou šablonu kliknutím na tlačítko **Nová šablona…**.

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Výraz

1.Z rozbalovacího menu operace vyberte logický operátor: **AND** (Všechny podmínky musí být splněny)

2.Klikněte na **+ Přidat pravidlo** a vyberte tyto podmínky: **Počítač** > **Maska spravovaných produktů** > **je jeden z** > **Chráněno produktem ESET: Počítač**. Případně vyberte vámi požadovanou masku produktu.

Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

Dynamická skupina – počítač s aplikací v konkrétní verzi

Tuto dynamickou skupinu můžete použít pro vyfiltrování počítačů, na kterých se nachází aplikace v konkrétní verzi. To může být užitečné například v případě, kdy potřebujete zjistit, na kterých stanicích máte starší verze aplikace. Použít můžete také operátor **"obsahuje"** nebo **"má předponu"**.

V hlavním menu Web Console přejděte do sekce **Další** > **Šablony dynamických skupiny** a vytvořte novou šablonu kliknutím na tlačítko **Nová šablona…**.

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Výraz

1.Z rozbalovacího menu operace vyberte logický operátor: **AND** (Všechny podmínky musí být splněny)

2.Klikněte na **+ Přidat pravidlo** a vyberte tyto podmínky:

- **Instalované aplikace** > **Název aplikace** > **= (rovná se)** > *ESET Endpoint Security*
- **Instalované aplikace** > **Verze aplikace** > **= (rovná se)** > *6.2.2033.0*

Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

šablona dynamické skupiny

Dynamická skupina – počítač, na kterém není nainstalován žádná aplikace nebo v požadované verzi Tuto dynamickou skupinu můžete použít pro zjištění, na kterých stanicích nemáte aktuální verzi produktu nebo aplikaci nemáte na počítači vůbec nainstalovanou.

Následně můžete dané skupině přiřadit klientskou úlohu pro instalaci aplikace. Použít můžete také operátor **"obsahuje"** nebo **"má předponu"**.

V hlavním menu přejděte do sekce **Další** > **Šablony dynamických skupin** a klikněte v dolní části okna na tlačítko **Nová šablona**.

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Výraz

1.Z rozbalovacího menu operace vyberte logický operátor: **NAND** (Alespoň jedna podmínka nesmí být splněna)

2.Klikněte na **+ Přidat pravidlo** a vyberte tyto podmínky:

- **Instalované aplikace** > **Název aplikace** > **= (rovná se)** > *ESET Endpoint Security*
- **Instalované aplikace** > **Verze aplikace** > **= (rovná se)** > *6.2.2033.0*

Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

Dynamická skupina – aplikace je nainstalovaná, ale v

jiné verzi

Tuto dynamickou skupinu můžete použít pro vyfiltrování počítačů, na kterých se sice nachází aplikace, ale je v jiné verzi, než definované. To může být užitečné například v případě, kdy potřebujete zjistit, na kterých stanicích nemáte vámi požadovanou verzi produktu. Lze použít různé operátory, ale je třeba zajistit, aby testování verzí probíhalo s negovaným operátorem.

V hlavním menu přejděte do sekce **Další** > **Šablony dynamických skupin** a klikněte v dolní části okna na tlačítko **Nová šablona**.

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Výraz

1. Z rozbalovacího menu operace vyberte logický operátor: **AND** (Všechny podmínky musí být splněny)

2. Klikněte na **+ Přidat pravidlo** a vyberte tyto podmínky:

   - **Instalované aplikace** > **Název aplikace** > **= (rovná se)** > *ESET Endpoint Security*
   - **Nainstalované aplikace** > **Verze aplikace** > **≠ (nerovná se)** > *6.2.2033.0*

Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

Dynamická skupina – počítač je v definované síti

Tuto dynamickou skupinu můžete použít pro vyfiltrování všech počítačů, které se nacházejí v konkrétním segmentu sítě. Následně na takové klientské stanice můžete uplatňovat specifické nastavení, například pro aktualizaci modulů. Rozsahy můžete definovat podle mnoha způsoby.

V hlavním menu přejděte do sekce **Další** > **Šablony dynamických skupin** a klikněte v dolní části okna na tlačítko

Nová šablona.

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Výraz

1.Z rozbalovacího menu operace vyberte logický operátor: **AND** (Všechny podmínky musí být splněny)

2.Klikněte na **+ Přidat pravidlo** a vyberte tyto podmínky:

- **IP adresy** > **IP adresa adaptéru** > **≥ (větší nebo rovno)** > *10.1.100.1*
- **IP adresy** > **IP adresa adaptéru** > **≤ (menší nebo rovno)** > *10.1.100.254*
- **IP adresy** > **Maska adaptéru** > **= (rovná se)** > *255.255.255.0*

Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

Dynamická skupina – nainstalovaný, ale neaktivovaný serverový produkt

Tuto dynamickou skupinu můžete použít pro vyfiltrování všech serverů, na kterých máte nainstalován bezpečnostní produkt, ale zatím není aktivován. Následně na ně můžete spustit klientskou úlohu pro aktivaci odpovídající licencí. V tomto příkladu použijeme ESET Mail Security pro Microsoft Exchange Server, nicméně vybrat můžete více produktů.

V hlavním menu přejděte do sekce **Další** > **Šablony dynamických skupin** a klikněte v dolní části okna na tlačítko **Nová šablona**.

Obecné

Zadejte **název**, volitelně **popis**, nově vytvářené šablony dynamické skupiny.

Výběrem možnosti **Použijte časová pravidla** aplikujete **Časová pravidla** a nastavíte konkrétní čas, během kterého je spuštěné přiřazování zařízení do dynamických skupin.

Výraz

1. Z rozbalovacího menu operace vyberte logický operátor: **AND** (Všechny podmínky musí být splněny)
2. Klikněte na **+ Přidat pravidlo** a vyberte tyto podmínky:
   - **Počítač** > **Maska spravovaných produktů** > **je jeden z** > **Chráněno produktem ESET: Poštovní server**
   - **Problémy s funkčností/ochranou** > **Zdroj** > **= (rovná se)** > **Bezpečnostní produkt**
   - **Problémy s funkčností/ochranou** > **Problém** > **= (rovná se)** > **Produkt není aktivován**

Časová pravidla

Nastavení časového intervalu pro novou šablonu dynamické skupiny. Klikněte na tlačítko **Přidat**. Klikněte na pole s časem a z rozbalovací nabídky vyberte **Počáteční čas** a **Konec**. Vyberte frekvenci (Každý den / Pracovní den / Víkend) nebo den v týdnu a čas. Zvolený čas musí být delší než 1 minuta a kratší než 24 hodin. Po nastavení **Počátečního času** a **Konce** se ve sloupci **Doba** zobrazí doba trvání nastaveného času. Přidat můžete další časové intervaly.

Souhrn

V této části se zobrazí souhrnné informace o vytvářené šabloně. Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření šablony dokončete kliknutím na tlačítko **Dokončit**. Vytvořenou šablonu můžete následně použít při vytváření nové dynamické skupiny.

Jak automatizovat ESET PROTECT?

Pomocí dynamických skupin můžete automatizovat instalaci produktu, aktualizace operačního systému, kontrolu počítače, aktivaci nově nainstalovaných produktů a další úlohy. Níže uvádíme několik vzorových příkladů.

Jak automaticky nainstalovat bezpečnostní produkt ESET na nově připojenou stanici s OS Windows

> ⚠ V tomto příkladu se předpokládá, že na stanici není instalováno bezpečnostní řešení třetí strany ani produkt ESET určený pro domácnosti (například ESET Smart Security). Instalaci produktu ESET na stanici s aktivním řešením třetí strany nedoporučujeme. V takovém případě nejprve produkt odinstalujte, ručně nebo prostřednictvím nástroje ESET AV Remover.

1. Vytvořte dynamickou skupinu s názvem *Nechráněné počítače*.
a.Vytvořte ji jako potomka předdefinované skupiny **Windows počítače** > **Windows (stanice)**.
b.Dále klikněte na tlačítko **Nová šablona**.
c.Přidejte pravidlo: **Počítač** > **Maska spravovaných produktů**.
d.Jako spojku vyberte **nerovná se**.
e.Vyberte masku **Chráněno produktem ESET: Počítač**
f.Skupinu vytvořte kliknutím na tlačítko **Dokončit**.
2. V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
a.Zadejte název úlohy, volitelně popis, a z rozbalovacího menu **Úloha** vyberte možnost **Instalace aplikace**.
b.V sekci **Nastavení** vyberte instalační balíček a případně definujte další parametry instalace.
c.Úlohu vytvořte kliknutím na tlačítko **Dokončit** a následně klikněte na tlačítko **Vytvořit podmínku spuštění**.
d.V sekci **Cíl** klikněte na tlačítko **Přidat skupiny** a vyberte vytvořenou skupinu *Nechráněné počítače*.
e.V sekci **Podmínka spuštění** vyberte možnost **Při připojení do dynamické skupiny**.
f.Podmínku spuštění uložte kliknutím na tlačítko **Dokončit**.
Úloha na instalaci aplikace se spustí automaticky na každém zařízení, které se od této chvíle stane členem dynamické skupiny. Pokud již ve skupině byla zařízení předtím, než jste úlohu vytvořili, musíte ji na těchto stanicích spustit ručně.

Vynucení politiky na základě polohy klienta

1. Vytvořte dynamickou skupinu s názvem *Subnet 120*.
a.V průvodci vyberte jako nadřazenou skupinu **Všechna zařízení**.
b.Dále klikněte na tlačítko **Nová šablona**.
c.Přidejte pravidlo: **IP adresy** > **Podsíť**.
d.Jako operátor vyberte **rovná se (=)**.
e.Zadejte podsíť, kterou chcete filtrovat, například 10.1.120.0 (poslední číslo musí být 0, aby filtr obsáhl všechny IP adresy ze subnetu 10.1.120.).
f.Skupinu vytvořte kliknutím na tlačítko **Dokončit**.
2. Přejděte na záložku **Politiky**.
a.Klikněte na tlačítko **Nová politika.**
b.V sekci **Nastavení** vyberte z rozbalovacího menu položku **ESET Management Agent**.
c.V konfigurační šabloně změňte **Interval připojení** na 5 minut.
d.V sekci **Přiřadit** klikněte na tlačítko **Přiřadit...** a pomocí zaškrtávacího pole vyberte vytvořenou dynamickou skupinu *Subnet 120*. Pro potvrzení klikněte na tlačítko **OK**.
e.Vytvoření politiky potvrdí kliknutím na tlačítko **Dokončit**.
Politika se automaticky aplikuje na klienty, kteří se stanou členem této dynamické skupiny.

Pro ověření, co se stane s aplikovanými politikami ve chvíli, kdy počítač přestane být členem dynamické skupiny (již nebude vyhovovat definované podmínce), přejděte do kapitoly pravidla pro odebrání politik.

Dále se podívejte na příklady šablon dynamických skupin.

Správa licence

Seznam licencí a možnosti pro jejich přidání naleznete v ESET PROTECT Web Console v sekci **Další** > **Správa licence**. V této části se zobrazí licence synchronizované z ESET Business Account, které jste použili pro nasazení ESET PROTECT.

Pro použití licencí z jiného ESET Business Account je nutné licence přesunout do ESET Business Account, který jste použili pro nasazení ESET PROTECT.

Prostřednictvím ESET PROTECT můžete vzdáleně aktivovat vaše bezpečnostní řešení ESET.

Viz také Časté dotazy k licencím (firemní uživatelé).

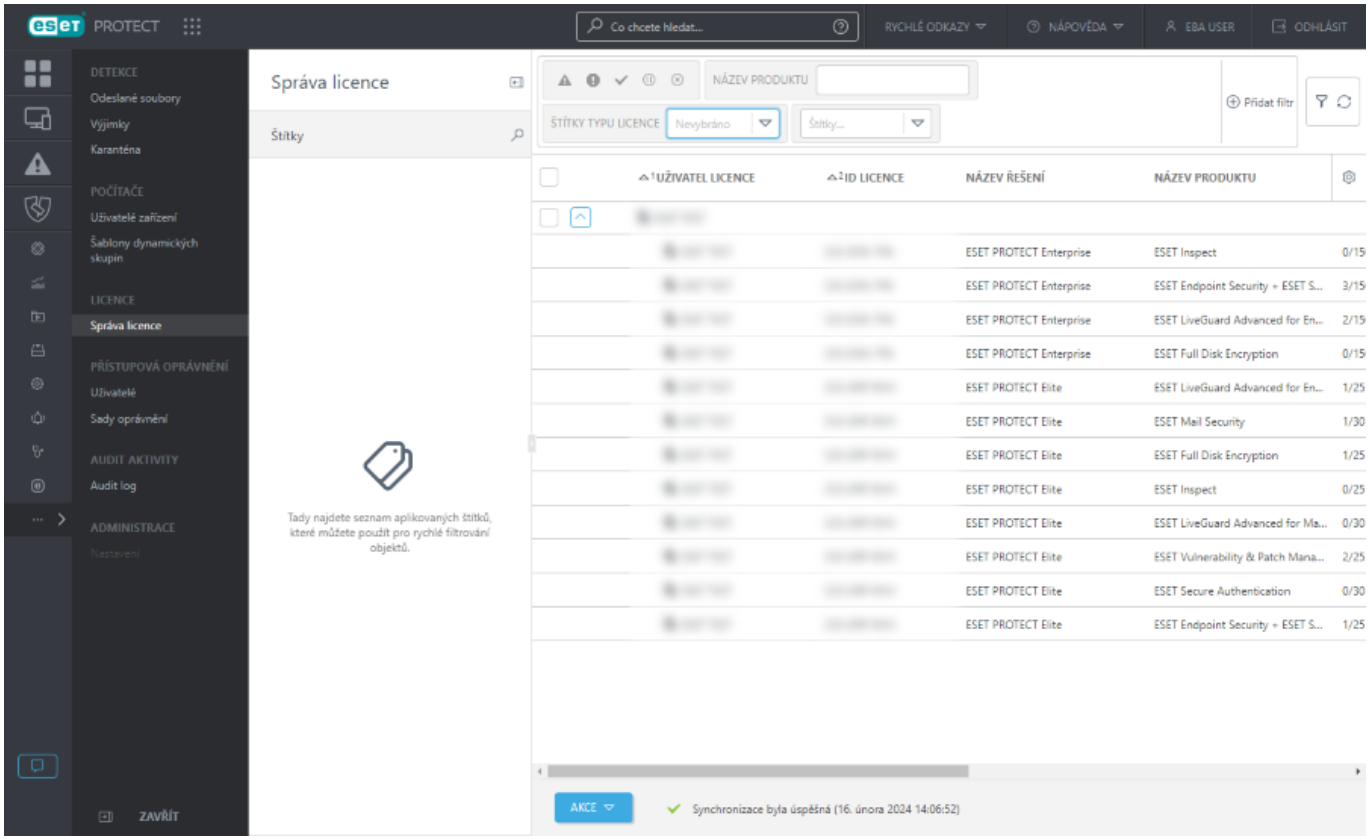
Oprávnění pro přístup k licencím

Pro přístup k licencím musí mít uživatel potřebná oprávnění. Oprávnění se vždy vztahuje pouze na licence umístěné v konkrétní statické skupině, do které má uživatel přístup. Přehled všech oprávnění naleznete v této kapitole.

Pouze administrátor, jehož domovskou skupinou jsou **Všechna zařízení** a má oprávnění pro **Zápis** licencí, může licence přidávat nebo odebírat. Každá licence je reprezentovaná **veřejným ID** a je u ní uveden počet jednotek. Administrátor může dalším uživatelům delegovat oprávnění pro přístup k licenci, aby ji mohli používat pro aktivaci, případně ji následně přesunout do jiné statické skupiny. Licence není možné rozdělit.

Licence z ESET MSP Administrator 2 se rozdělí do fondů dle jednotlivých společností. Licence není možné z tohoto fondu přesunout.

Správa licencí ve Web Console



Licence přidané pod konkrétním ESET Business Account uživatelem nebo stejnou společností jsou seskupeny do fondu licencí. Pro zobrazení detailních informací o licenci klikněte na , čímž rozbalíte daný fond licencí.

V ESET Business Account a ESET PROTECT můžete licence rozpoznat podle:

- **ID licence**
- **Typ licence**: **Firemní** (placená licence), **Zkušební** (zkušební licence), **MSP** (Managed Services Provider

licence) a **NFR** (neprodejná licence).

Mezi další informace patří:

- **jméno vlastníka** licence a **kontaktní informace**.
- **uživatel licence** a typ: **Společnost**, **Lokalita**, **MSP zákazník**.
- **název řešení,** pod které produkty ESET patří. Přečtěte si více o řadách ochrany ESET.
- **název produktu**, na který licence platí,
- celkový **stav** licence (zda licence vypršela, došlo k překročení počtu klientů povolených licencí a jiná upozornění),
- počet **klientů** aktivovaných prostřednictvím této licence, V případě ESET Mail Security se hodnota ve sloupci Počet vypočítává na základě zakoupených poštovních schránek (hodnota ve sloupci **Rozsah**).
- **rozsah** představuje počet schránek, uživatelů, připojení (v případě serverových produktů), na které jste si zakoupili licenci,
- **platnost** představuje datum vypršení platnosti licence. v případě licencí ve formě předplatného nemusí být uvedeno datum platnosti,

Licence můžete filtrovat podle **stavu**:

OK – zelená	Licence je platná a je úspěšně registrovaná.
Chyba – červená	Licence není registrovaná, její platnost vypršela nebo je nadužívána.
Varování – oranžová	Licence je téměř vyčerpána nebo se blíží konec její platnosti.
Deaktivováno nebo pozastaveno	Licence je deaktivována nebo její platnost byla dočasně pozastavena.
Neaktuální	Platnost vaší licence vypršela.

Vypršelé a nadužívané licence (ve stavu **Chyba** nebo **Neaktuální**) nejsou viditelné v seznamu dostupných licencí v průvodci All-in-one instalačním balíčkem, klientské úloze Aktivace produktu a klientské úloze Instalace softwaru.

Kliknutím na tlačítko **Akce** se zobrazí možnosti pro správu fondu licencí:

Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
Přístup skupiny > **Přesunout**	Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.
Synchronizovat licence	Kliknutím vynutíte synchronizaci licenčních informací do ESET PROTECT. Licence se s licenčními servery ESET automaticky synchronizují jednou denně. Pokud jste licence přidali prostřednictvím ESET Business Account nebo ESET MSP Administrator, synchronizace s těmito portály probíhá rovněž jednou denně.
Otevřít EBA	Kliknutím se otevře portál ESET Business Account. Tato akce je k dispozici pouze v případě, kdy jste ji přidali prostřednictvím ESET Business Account.

Otevřít EMA	Kliknutím se otevře portál ESET MSP Administrator. Tato akce je k dispozici pouze v případě, kdy jste ji přidali prostřednictvím ESET MSP Administrator.

Po rozbalení fondu licencí a kliknutí na konkrétní licenci můžete provést následující akce. Dostupnost jednotlivých akcí se odvíjí od typu vybrané licence:

Použít licenci pro aktivaci	Kliknutím vytvoříte úlohu pro aktivaci produktu vybranou licencí.
Štítky	Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
Správa licence	Licence můžete spravovat, pokud je máte synchronizovány s portálem ESET Business Account nebo ESET MSP Administrator. Pokud dochází k nadužívání licence, navyšte si její kapacitu nebo deaktivujte některá zařízení.
Prodloužit licenci	Obnovte licenci, jejíž platnost vypršela, skončila, byla pozastavena nebo deaktivována, na ESET Business Account nebo ESET MSP Administrator.
Koupit licenci	Aktualizujte zkušební licenci na ESET Business Account nebo ESET MSP Administrator.
Audit log	kliknutím si zobrazíte Audit log pro vybranou položku.
Zkopírovat veřejné ID licence	Kliknutím si do schránky zkopírujete ID licence.

Předplatné licencí

ESET PROTECT podporuje správu licencí ve formě předplatného. Platnost předplatného si můžete zkontrolovat v sekci **Správa licence** ve sloupci **Platnost**, případně v sekci **Počítače** v Detailech konkrétního zařízení.

Podpora ESET Business Account lokalit

Nyní můžete ze svého ESET Business Account importovat kompletní strukturu společnosti a rozdělovat části licence jednotlivým lokalitám.

Aktivace ESET firemních produktů

Licenci pro ESET PROTECT nemůžete použít pro aktivaci bezpečnostních produktů ESET nainstalovaných na spravovaných stanicích. Pro aktivaci jednotlivých bezpečnostních produktů ESET použijte licenci určenou pro daný produkt.

Licence k produktům ESET můžete v ESET PROTECT distribuovat dvěma způsoby:

- pomocí úlohy instalace aplikace
- pomocí úlohy aktivace produktu

Deaktivace ESET firemních produktů

Firemní produkty ESET můžete deaktivovat (odebrat licenci k produktu) prostřednictvím ESET PROTECT Web Console několika způsoby:

- v hlavním menu na záložce **Počítače** vyberte požadované počítače a v kontextovém menu klikněte na

možnost **Deaktivovat produkty** – po kliknutí deaktivujete všechny ESET produkty nainstalované na vybraných zařízeních (odstraníte vazbu z licenčních serverů společnosti ESET). Produkt se deaktivujte i v případě, že nebyl aktivován prostřednictvím ESET PROTECT. Daná licence přitom nemusí být spravovaná prostřednictvím ESET PROTECT.

Pokud vyberte pouze jeden počítač, na kterém je nainstalováno více ESET produktů (například ESET Endpoint a ESET Inspect Connector), můžete se rozhodnout, který z nich chcete deaktivovat.

- Odebrání počítače ze správy

- Vytvořte klientskou úlohu na Odstranění nepřipojujících se počítačů, ve které vyberte možnost **Deaktivovat licenci**.

Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Správa postranního panelu a hlavní tabulky zobrazující data.

- Přidáním filtrů a jejich uložením jako předvolby. Pro filtrování zobrazených objektů můžete využít štítky.

Jak Administrator může přidělit přístup k licenci dalším uživatelům

Existuje výchozí účet Administrator a dále jsou definovány další tři uživatelské účty:
• *Filip* jehož domovská skupina je *Praha*
• *Pavel* jehož domovská skupina je *Sydney*
• *Petr* jehož domovská skupina je *Tokio*
Administrator naimportoval tři licence. To znamená, že se umístily do statické skupiny Všechna zařízení a další uživatelé k licencím nemají přístup.
Administrator klikne na ikonu **ozubeného kolečka** u fondu licencí, ke kterému chce uživatelům přidělit přístup. Následně v kontextovém menu vybere možnost **Přístup skupiny** > **Přesunout** a následně vybere statickou skupinu, do které mají uživatelé přístup. V případě *Filipa* vybere skupinu *Praha*. Aby *Filip* licenci viděl a mohl ji používat, musí mít přiděleno oprávnění **Použít** u položky **Licence** ve své statické skupině *Praha*.
Pokud se následně *Filip* přihlásí, v sekci Další > Správa licence uvidí licenci. Administrátor zopakuje výše uvedený proces pro uživatele *Pavla* a *Petra*, aby měli přístup ke svým licencím.

Vhodné licence pro cloud

Licence vhodné pro cloud můžete použít v produktu ESET PROTECT. Přečtěte si více o řadách ochrany ESET.

V cloudovém ESET PROTECT nelze používat ochranu pomocí řešení řady ESET PROTECT on-prem.

V tabulce níže je uvedeno, které licence lze použít k vytvoření instance ESET PROTECT, a které produktové řady se používají pouze k aktivaci konkrétních funkcí produktu.

Název produktové řady	Licence vhodné pro vytvoření ESET PROTECT instance prostřednictvím ESET Business Account	Licence vhodné pro vytvoření ESET PROTECT instance prostřednictvím ESET MSP Administrator
ESET PROTECT Essential	✔	
ESET PROTECT Entry (dříve: ESET Endpoint Protection Advanced Cloud)	✔	✔

Název produktové řady	Licence vhodné pro vytvoření ESET PROTECT instance prostřednictvím ESET Business Account	Licence vhodné pro vytvoření ESET PROTECT instance prostřednictvím ESET MSP Administrator
ESET Secure Business Cloud	✔	
ESET PROTECT Advanced (dříve: ESET Remote Workforce Offer)	✔	✔
ESET PROTECT Complete	✔	✔
ESET PROTECT Enterprise	✔	✔
ESET PROTECT Mail Plus	✔	✔
ESET PROTECT Elite	✔	✔
ESET PROTECT MDR	✔	
ESET Security for Microsoft SharePoint Server (Per Server)	✔	
ESET LiveGuard Advanced		
ESET LiveGuard Advanced for Endpoint Security + ESET Server Security (ESET File Security)		
ESET LiveGuard Advanced for Mail Security		
ESET Full Disk Encryption pro ECA		

Více informací o technologiích ESET a typech útoků/detekcí naleznete ve slovníku pojmů.

Přístupová oprávnění

Pomocí přístupových oprávnění můžete spravovat uživatele webové konzole ESET PROTECT a uživatelská oprávnění.

Bezpečnostní model

Tato nastavení týkající se přístupových oprávnění se aplikují pouze na uživatele, kteří mají na portále ESET Business Account (EBA) nastavené **vlastní oprávnění**. **Vlastní oprávnění** můžete ve webové konzoli ESET PROTECT přiřadit pouze uživatelům, kteří mají na portále ESET Business Account roli **superuživatel**.

Níže uvádíme vysvětlení klíčových výrazů používaných v bezpečnostním modelu:

Výraz	Vysvětlení
Domovská skupina	Domovská skupina je skupina, do které se ukládají objekty (zařízení, úlohy, šablony, politiky, ...) vytvořené uživatelem. Každý uživatel má definován pouze jednu domovskou skupinu.
Objekt	Objekty jsou umístěné ve **statických skupinách**. Přístup k objektům závisí na tom, zda má uživatel přístup do dané skupiny. Snadno tak můžete přístup přidělit dalšímu uživateli (například v době dovolené). Jedinou výjimku představují serverové úlohy a oznámení, které využívají koncept "executing user" (úlohy a oznámení jsou spouštěny pod uživatelským účtem).
Přístup skupiny	Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.
Administrator	Uživatel, jehož domovskou skupinou jsou **Všechna zařízení** a má přiřazena administrátorská oprávnění, je plnohodnotný administrátor.
Přístupové oprávnění	Oprávnění pro přístup k objektu nebo spouštění úloh. Kompletní seznam přístupových oprávnění a funkcí naleznete v této kapitole.
Sada oprávnění	Sada oprávnění reprezentuje oprávnění, která jsou přiřazená uživateli přistupujícímu k částem ESET PROTECT Web Console. Definují, jaké funkce ESET PROTECT Web Console uživatel uvidí, a ke kterým nebude mít přístup. Uživateli můžete přiřadit libovolné množství sad oprávnění. Oprávnění se aplikují vždy na objekty umístěné v definovaných statických skupinách. **Skupiny**, na které se oprávnění aplikuje, definujete v sadě oprávnění v sekci **Statické skupiny**.
Funkce	Funkce je typ objektu nebo akce. Přístup můžete definovat na těchto úrovních: **Čtení**, **Zápis**, **Použít**. Kombinaci těchto funkcí aplikovaných na skupinu se říká sada oprávnění.

Vzorové příklady

Napříč administrátorskou příručkou uvádíme příklady pro práci s přístupovými oprávněními. Níže uvádíme jejich seznam:

- Jak duplikovat politiky
- Rozdíl mezi Použít a Zápis
- Jak nastavit oprávnění administrátorům ve firmě s více pobočkami
- Jak sdílet objekty prostřednictvím jejich duplikování
- Jak odebrat oznámení
- Jak vytvořit politiky

- Umožnit administrátorovi přístup pro zobrazení všech politik
- Jak sdílet licenci mezi všemi administrátory

Uživatelé

Správu uživatelů v ESET PROTECT Web Console naleznete v sekci **Další**.

- Detaily uživatele a akce nad uživateli
- Namapovaní uživatelé
- Přiřazení sady oprávnění konkrétnímu uživateli

Firma s více pobočkami

Společnost má dvě pobočky a správu každé zajišťuje jiný administrátor. Každý z nich tedy potřebuje oprávnění k odlišným skupinám.
Představte si dva administrátory, *Filipa* v *Praze* a *Jiřího* v *Brně*. Oba potřebují mít v konzoli přístup ke stanicím, které spravují a chtějí používat **nástěnku, politiky, přehledy** a **šablony dynamických skupin**.
Administrator musí podniknout tyto kroky:
1.Vytvořit nové statické skupiny: *Praha* a *Brno.*
2.Vytvořit nové sady oprávnění:
a)**Sadu** s názvem *Sada oprávnění pro pobočku v Praze*, přístupem ke statické skupině *Praha* a úplným oprávněním.
b)**Sadu** s názvem *Sada oprávnění pro pobočku v Brně*, přístupem ke statické skupině *Brně* a úplným oprávněním.
c)**Sadu** s názvem *Všechna zařízení / Nástěnka*, přístupem ke statické skupině *Všechna zařízení* a níže uvedenými oprávnění:
- **Čtení** u položky **Klientské úlohy**
- **Použít** u položky **Šablony dynamických skupin**
- U položky **Přehledy a nástěnka** přidělíte oprávnění **Použít**;
- **Použít** u položky **Politiky**
- U položky **Odeslat e-mail** přidělíte oprávnění **Použít**
- U položky **Licence** přidělíte oprávnění **Použít**.
- **Zápis** u položky **Oznámení**

3.Vytvořit uživatele *Filip*, nastavit mu domovskou skupinu *Praha* a přiřadit *Sadu oprávnění pro pobočku v Praze* a *Všechna zařízení / Nástěnka*.
4.Vytvořit uživatele *Jiří*, nastavit mu domovskou skupinu *Brno* a přiřadit *Sadu oprávnění pro pobočku v Brně* a *Všechna zařízení / Nástěnka*.
Po provedení výše uvedených kroků mohou oba uživatelé (*Filip* a *Jiří*) používat stejné úlohy, politiky, přehledy a šablony dynamických skupin, ale vždy je mohou aplikovat pouze na své stanice, resp. v přehledech uvidí jen data ze stanic, ke kterých mají přístup.

Sdílení objektů

Pokud jako administrátor chcete přidělit přístup k vámi vytvořeným nebo předdefinovaným objektům (šablonám dynamických skupin, přehledům, politikám, ...), můžete to udělat dvěma způsoby:

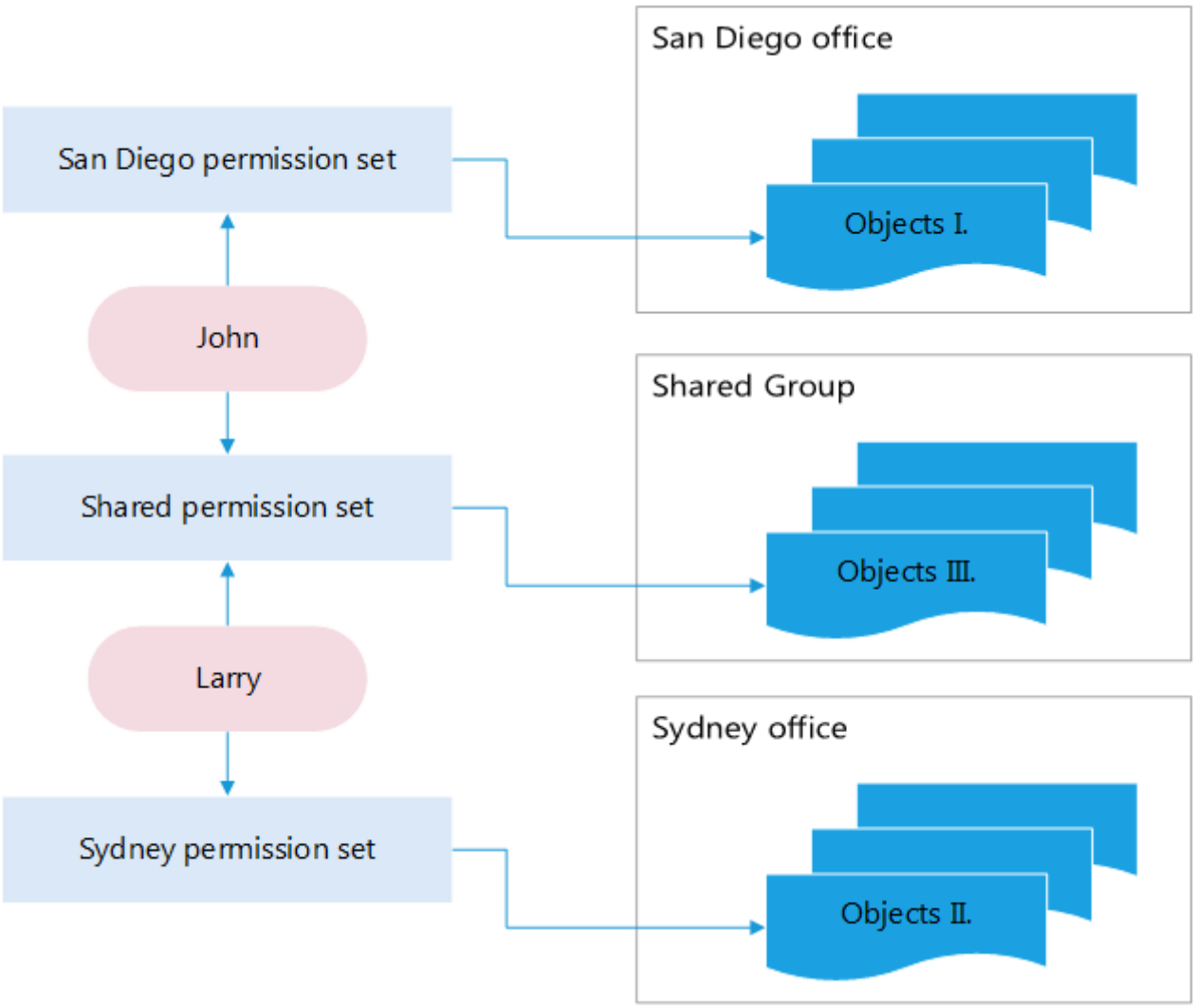
- Přesunout objekty do sdílené skupiny, do které mají přístup všichni uživatelé.
- Vytvořit kopii objektů a přesunout je do statické skupiny, do které má konkrétní uživatel přístup (viz

příklad níže).

Pro duplikování objektů musí mít uživatel oprávnění pro **čtení** originálních objektů a **zápis** daného typu objektu ve své **domovské skupině**.
Administrator, jehož domovskou skupinou jsou *Všechna zařízení*, chce *Filipovi* přidělit přístup k *Šabloně A.* Protože šablonu vytvořil *Administrator*, šablona je umístěna v jeho domovské skupině (*Všechna zařízení*).
Administrator musí provést tyto kroky:
1.V hlavním menu Web Console přejde do sekce **Další** > **Šablony dynamických skupin**.
2.Vybrat *Šablonu A* a z kontextového menu vybrat možnost **Duplikovat**. V případě potřeby změní název a šablon uloží kliknutím na tlačítko **Dokončit**.
3.Kopie objektu se opět vytvoří ve statické skupině *Všechna zařízení* (domovské skupině uživatele *Administrator*).
4.Následně Administrator vybere kopii šablony (v sekci **Další** > *Šablony dynamických skupin*), v kontextovém menu klikne na **Přístup skupiny** > **Přesunout** a vybere **Filipovu** statickou skupinu. Dále klikněte na tlačítko **OK**.

Jak sdílet objekty s více uživateli prostřednictvím sdílené skupiny

Pro lepší pochopení nového bezpečnostního modelu jsme připravili názorné schéma. V níže uvedeném příkladu máme dva uživatelské účty. Každý z nich má vlastní domovskou skupinu, ve které si může vytvářet objekty. *Filip* má přiřazenou *Sadu oprávnění pro pobočku v Praze*, což mu umožňuje pracovat s *objekty* ve své domovské skupině. Obdobně je na tom *Jiří*. V případě, že si uživatelé chtějí vyměňovat mezi sebou objekty (politiky, přehledy, ...), použijí k tomu statickou skupinu *Sdílená skupina*. Oba uživatelské účty mají přiřazenou *Sdílenou sadu oprávnění* a v seznamu *skupin* vidí statickou skupinu **Sdílené objekty**.



Přizpůsobení filtrů a rozložení

Web Console si můžete přizpůsobit svým potřebám:

- Přidáním filtrů a jejich uložením jako předvolby.
- Pro filtrování zobrazených objektů můžete využít štítky.

Detaily uživatele a akce nad uživateli

Pro správu uživatele na něj klikněte a v zobrazeném kontextovém menu si vyberte jednu z níže dostupných akcí:

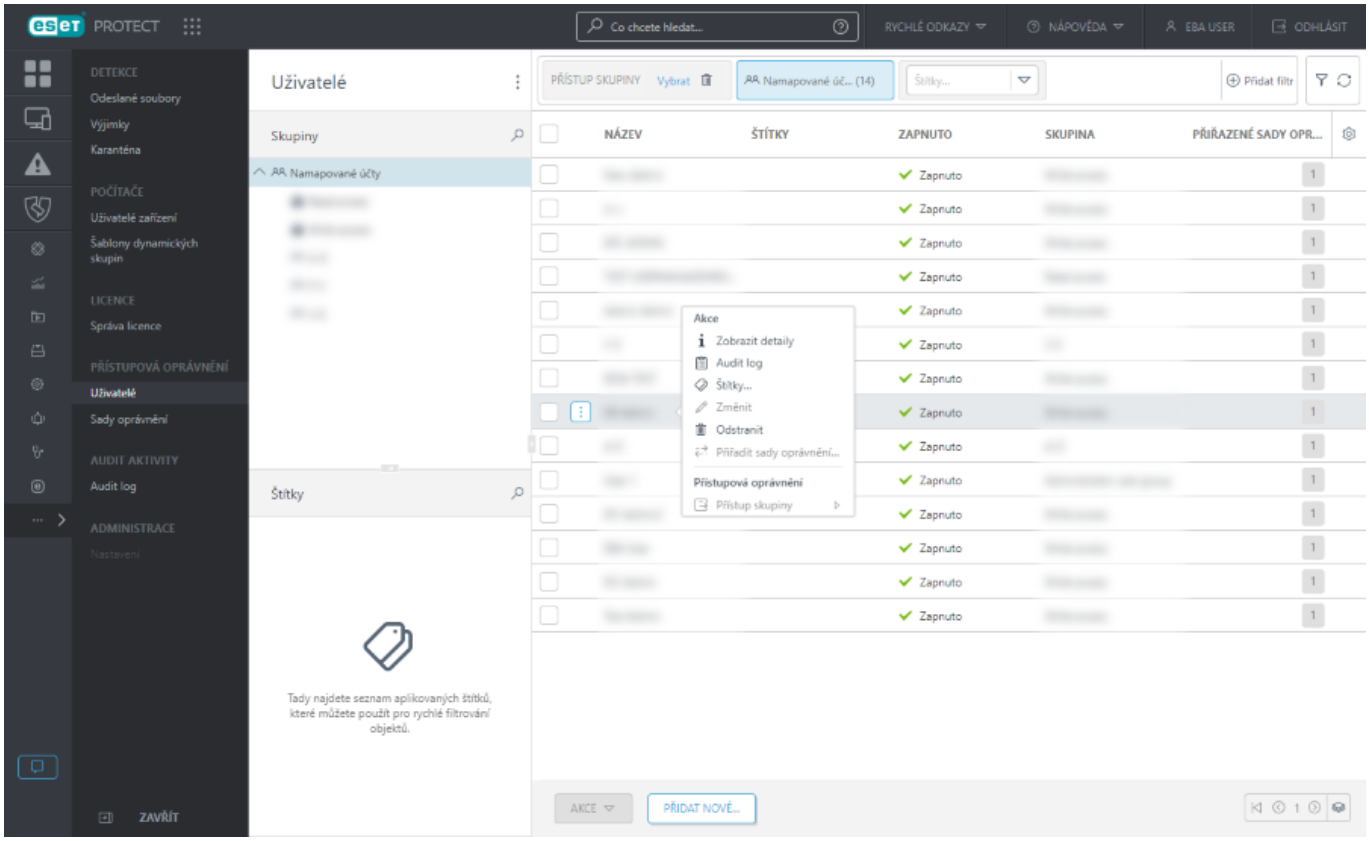
Akce

- **Zobrazit detaily** – kliknutím si zobrazíte detaily uživatele.
- **Audit log** – kliknutím si zobrazíte Audit Log pro všechny uživatele.
- **Audit log pro vybraného uživatele** – kliknutím si zobrazíte Audit log pro vybraného uživatele.
- **Štítky** – Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.

- **Přiřadit sady oprávnění** – kliknutím uživateli přiřadíte sadu oprávnění.

Přístupová oprávnění

- **Přístup skupiny** > **Přesunout** Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.



Detaily uživatele

Detaily uživatele jsou rozděleny do dvou sekcí:

- **Přehled** – v této části jsou dostupné obecné informace o uživateli. Uživatele můžete spravovat pomocí tlačítka **Akce** ve spodní části obrazovky.

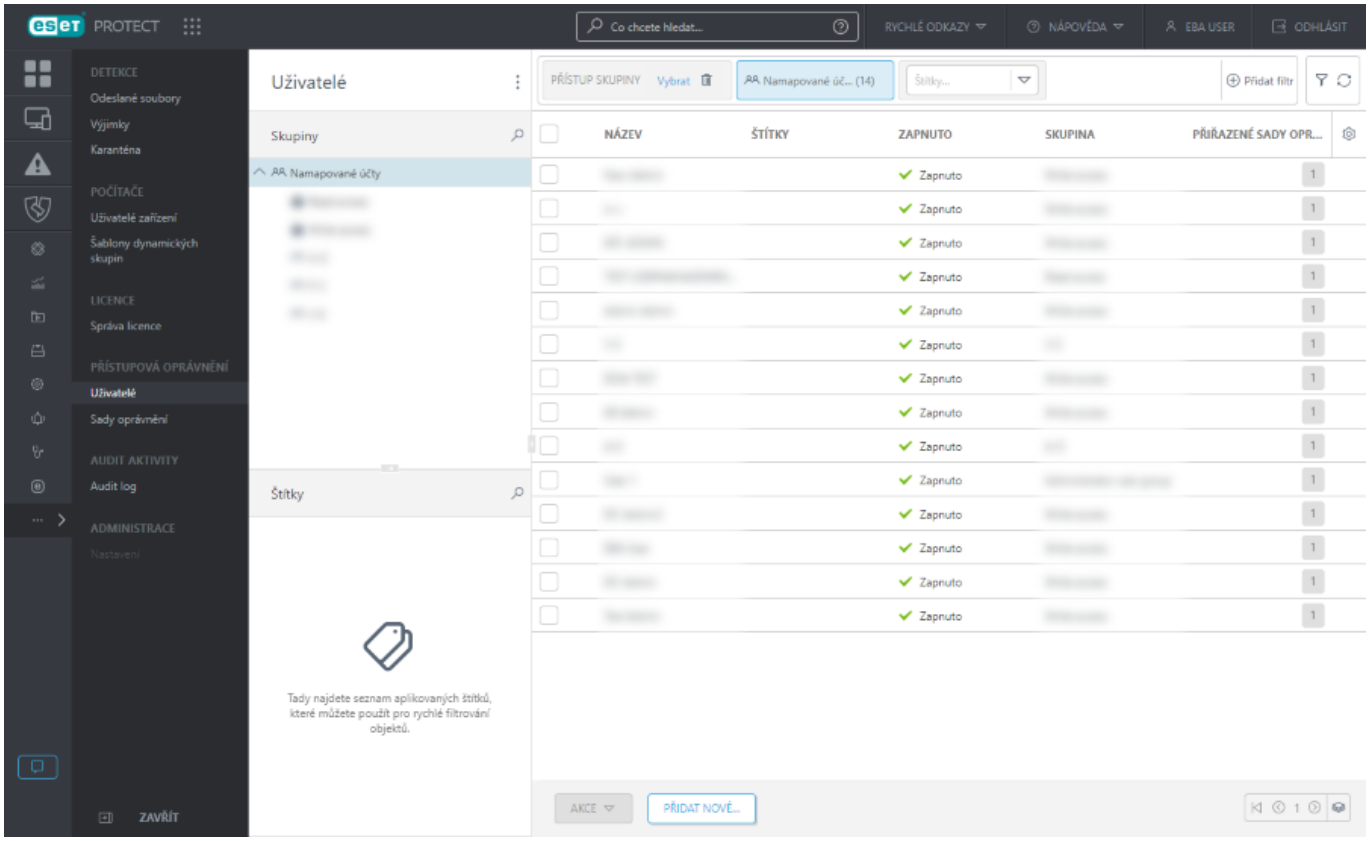
- **Sady oprávnění** – v této části naleznete seznam sad oprávnění, které má uživatel přiřazeny. Pro jejich správu klikněte na danou sadu oprávnění.

Namapovaní ESET Business Account uživatelé

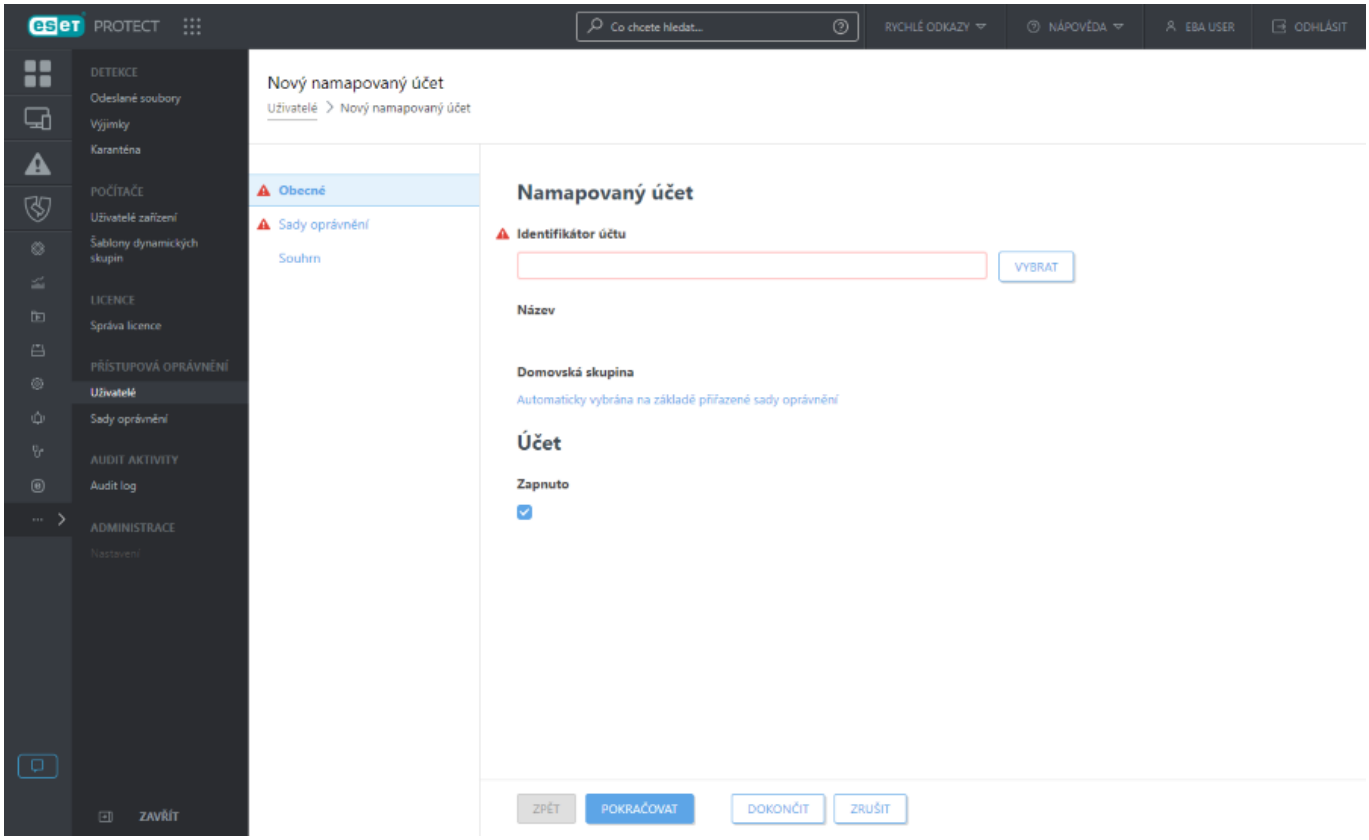
Pro namapování uživatele v ESET PROTECT vytvořeného na portále ESET Business Account postupujte podle níže uvedených kroků:

1. Přihlaste se k ESET Business Account a použijte účet, prostřednictvím kterého jste vytvořili nového uživatele v ESET Business Account, nepoužívejte zatím nově vytvořený účet.

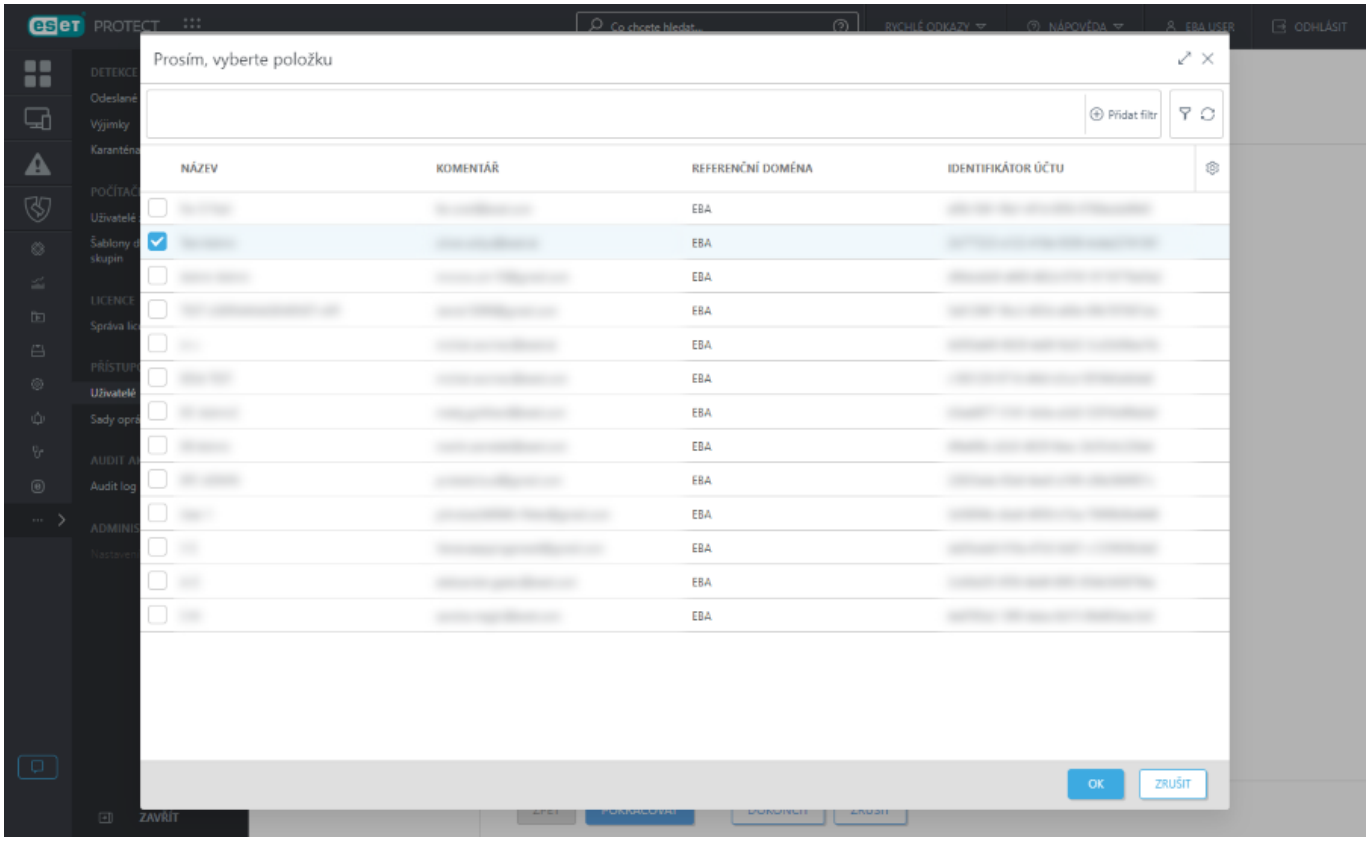
2. Otevřete si ESET PROTECT Web Console. V hlavním menu přejděte do sekce **Další** > **Uživatelé**, vyberte možnost **Namapované účty** a klikněte na tlačítko **Přidat nový**.



3. V části **Identifikátor účtu** klikněte na možnost **Vybrat**.



4. Vyberte vámi vytvořeného uživatele na portále ESET Business Account a klikněte na tlačítko **OK**.

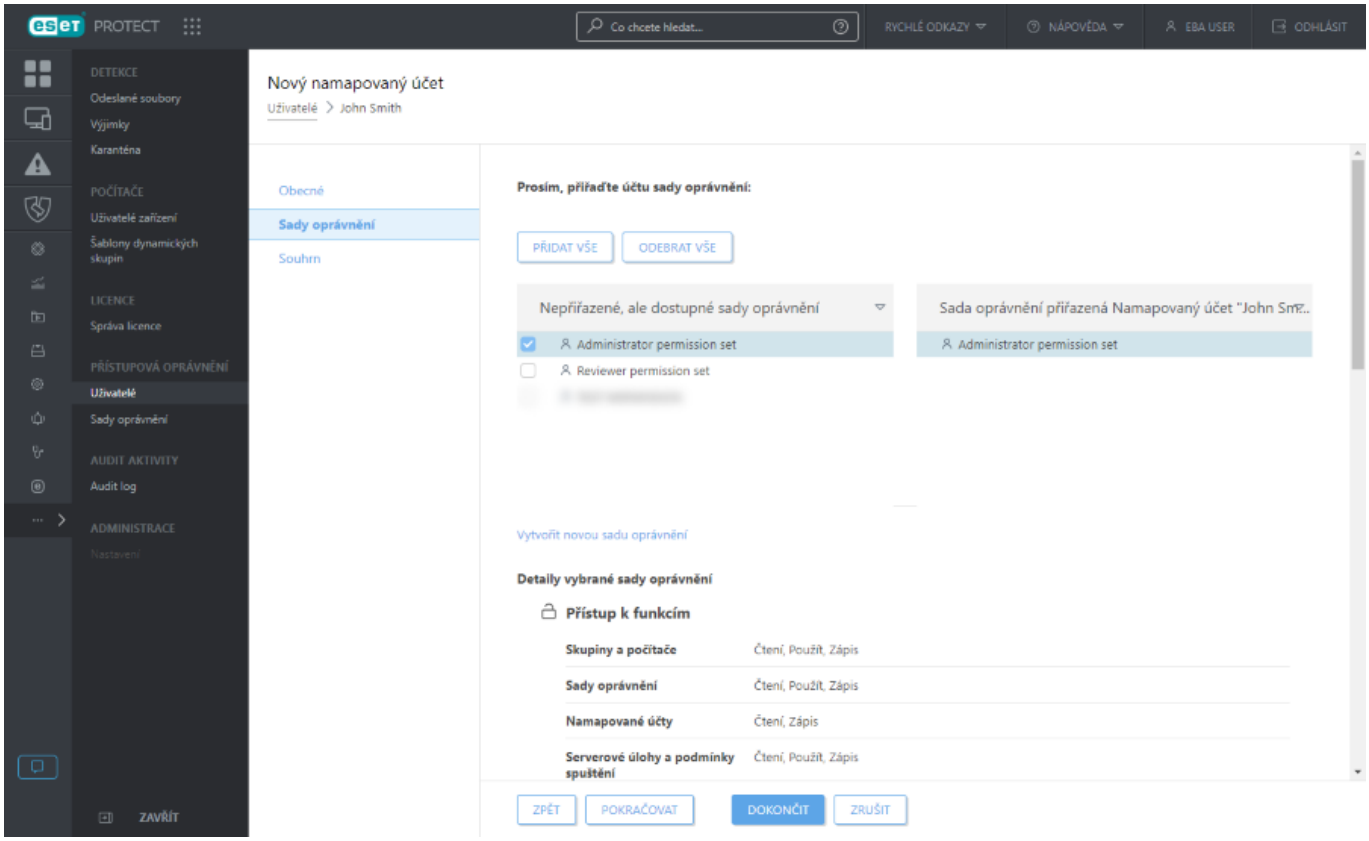


5. **Domovská skupina** je automaticky detekována na základě přiřazené sady oprávnění právě přihlášeného uživatele.

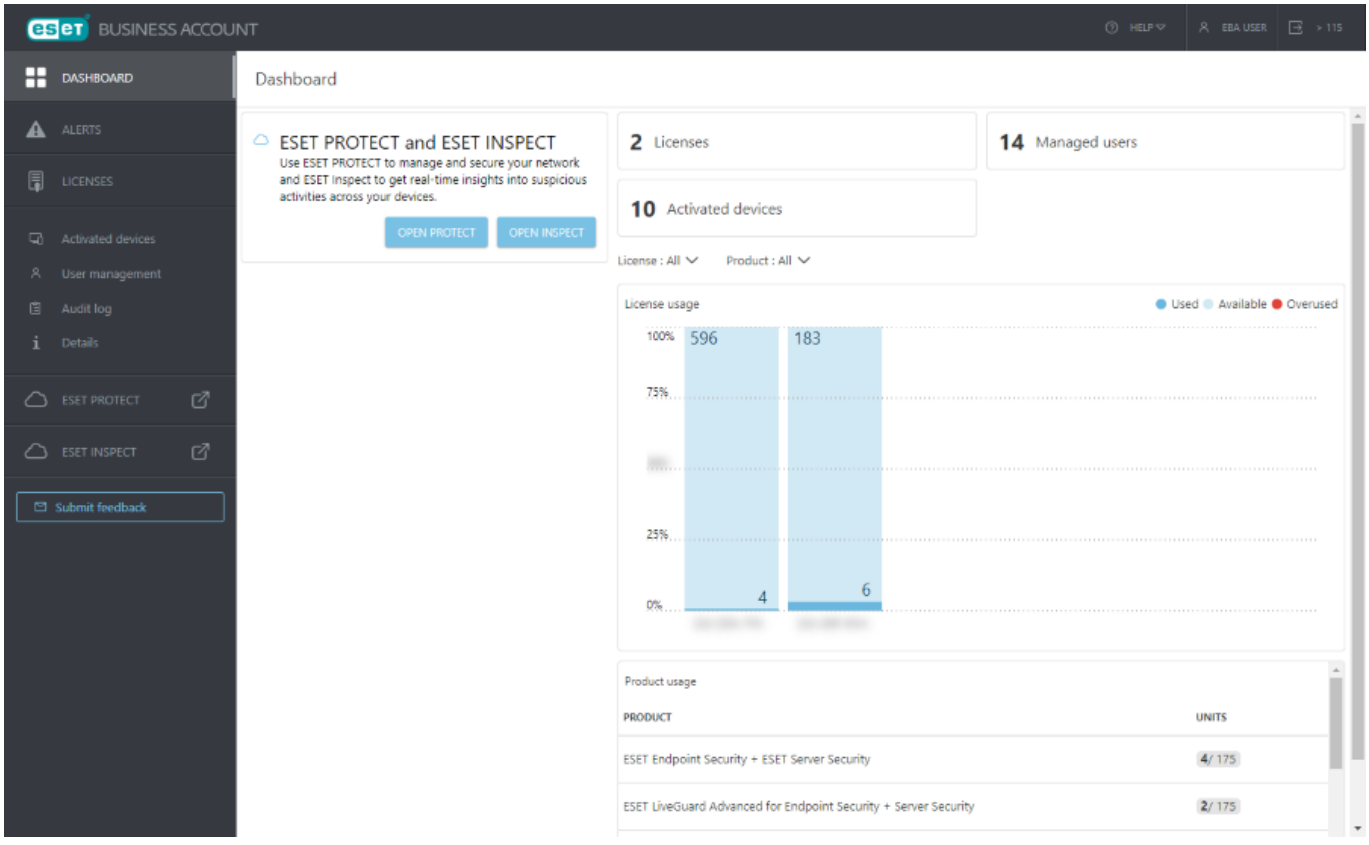
> **Příklad:**
> Právě přihlášený uživatel má oprávnění k **zápisu** u klientské úlohy **Instalace aplikace**. **Domovská skupina** uživatelského účtu je skupina s názvem "Oddělení_1". Pokud uživatel vytváří novou **klientskou úlohu pro instalaci aplikace**, skupina "Oddělení_1" se automaticky vybere jako **domovská skupina**.

Pokud vám předvybraná domovská skupina nevyhovuje, můžete ji ručně změnit.

6. V sekci **Sady oprávnění** se zobrazí úroveň přístupového oprávnění, které jste uživateli přiřadili v průběhu vytváření uživatele na portále ESET Business Account. Pokud jste vybrali možnost **Vlastní**, je nutné uživateli v ESET PROTECT přiřadit existující sadu oprávnění (případně si nejprve vytvořte novou sadu oprávnění). Klikněte na tlačítko **Dokončit**.



7. Uživatelům, kterým jste udělili přístup k ESET PROTECT, uvidí po přihlášení ke svému účtu ESET Business Account možnost pro otevření ESET PROTECT.

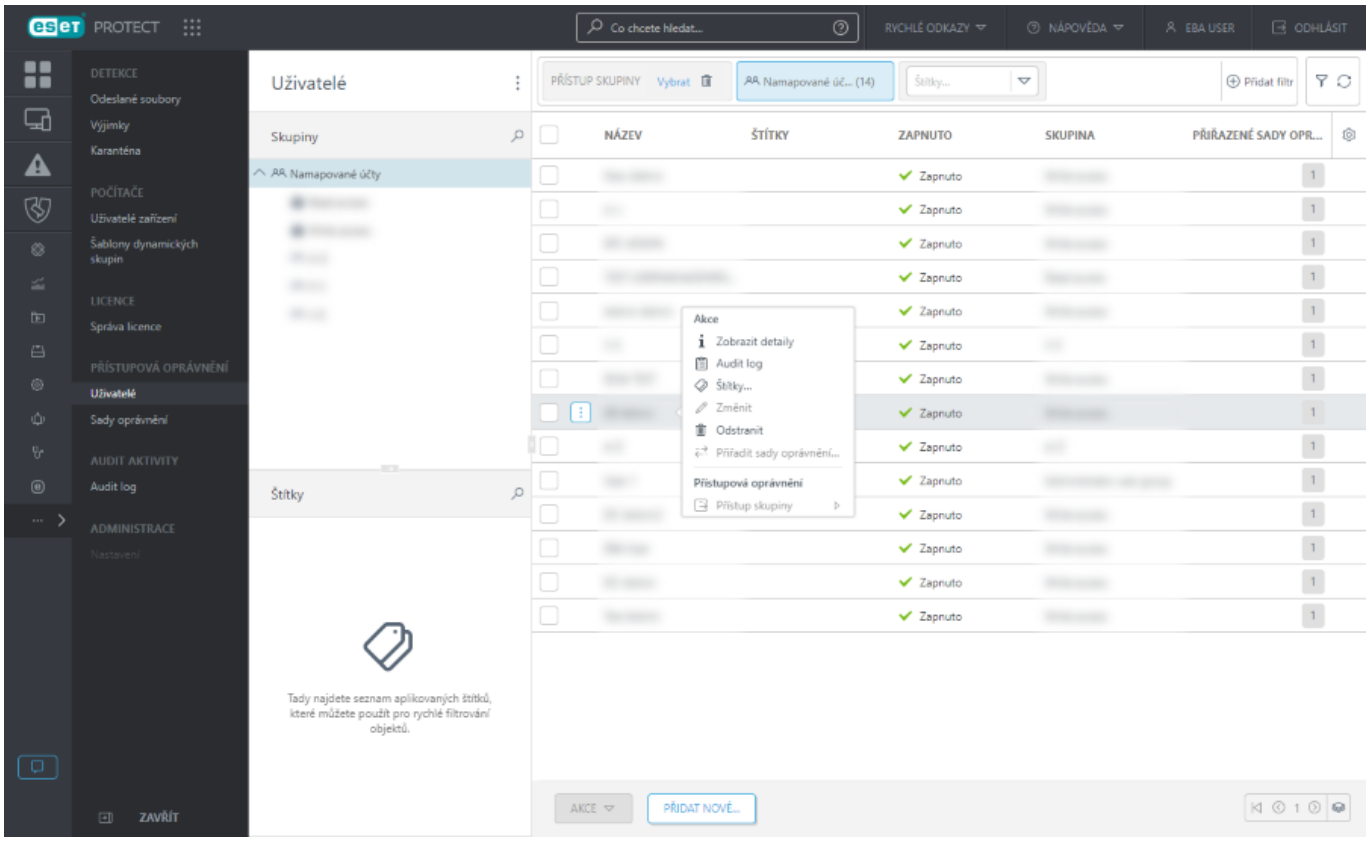


Přiřazení sady oprávnění konkrétnímu uživateli

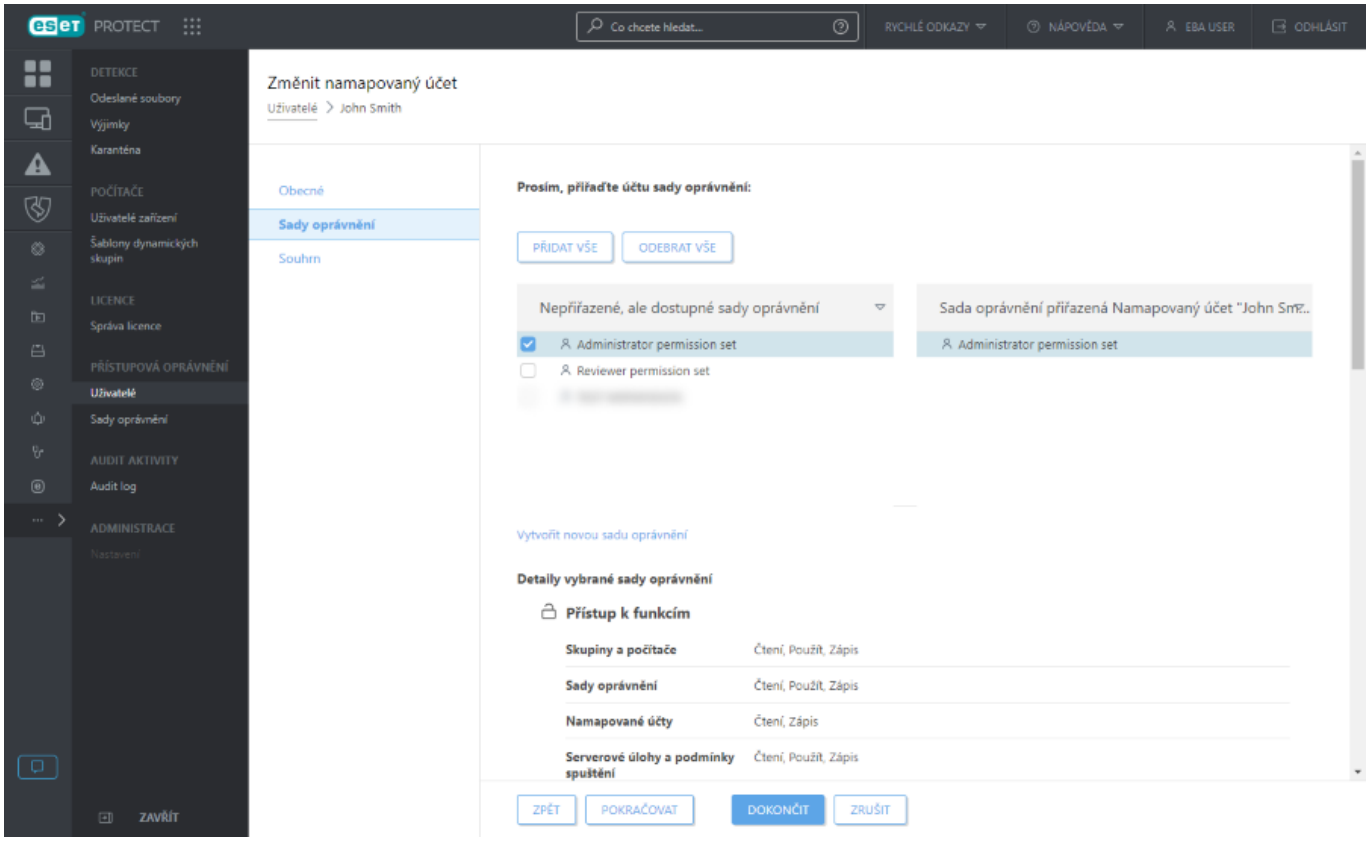
1. Sadu oprávnění můžete uživateli přiřadit dvěma způsoby:

   a)V hlavním menu přejděte do sekce **Další** > **Uživatelé**. Klikněte na uživatele a v kontextovém menu vyberte možnost **Přiřadit sady oprávnění**.

   b)V části **Uživatelé** vyberte uživatele, a klikněte na **Změnit**.



2. V části Sady oprávnění vyberte z tabulky **Nepřiřazené, ale dostupné sady oprávnění** takové, které uživateli chcete přiřadit. Pro více informací přejděte do kapitoly Správa oprávnění.



Sady oprávnění

Sada oprávnění jsou oprávnění přiřazená uživateli, který přistupuje k ESET PROTECT Web Console. Jinými slovy definují, jakou část Web Console si mohou uživatelé zobrazit, a akce, které mohou provádět. Rozsah platnosti sady oprávnění definuje statická skupina. Přístupová oprávnění (definovaná v sekci **Funkce**) se aplikují na objekty, které se nacházejí ve vybraných **Statických skupinách** a má k nim mít uživatel přístup. Přidělením přístupu ke statické skupině uživatel automaticky získá přístup také k jejím podskupinám. Díky tomuto principu jste schopni vytvořit strukturu statických skupin podle jednotlivých lokalit a lokálním administrátorům přidělit oprávnění pouze pro přístup k jejich počítačům/objektům. Více informací naleznete v samostatném příkladu.

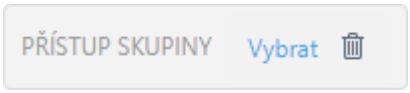
Uživateli můžete přidělit takové oprávnění, že si jej nebude schopen zobrazit a ani neuvidí další vytvořené uživatele. Všechny objekty, které jakýkoli uživatel vytváří, se ukládají do jeho domovské skupiny. Objekt, reprezentující nového uživatele, se vytvoří v domovské skupině uživatele, který jej vytvořil. Protože uživatele zpravidla vytváří Administrator, uloží se do skupiny *Všechna zařízení*.

Sady oprávnění se sčítají. Pokud uživateli přiřadíte více sad oprávnění, výsledná zásada vznikne jejich sečtením.

Sloučení sad oprávnění

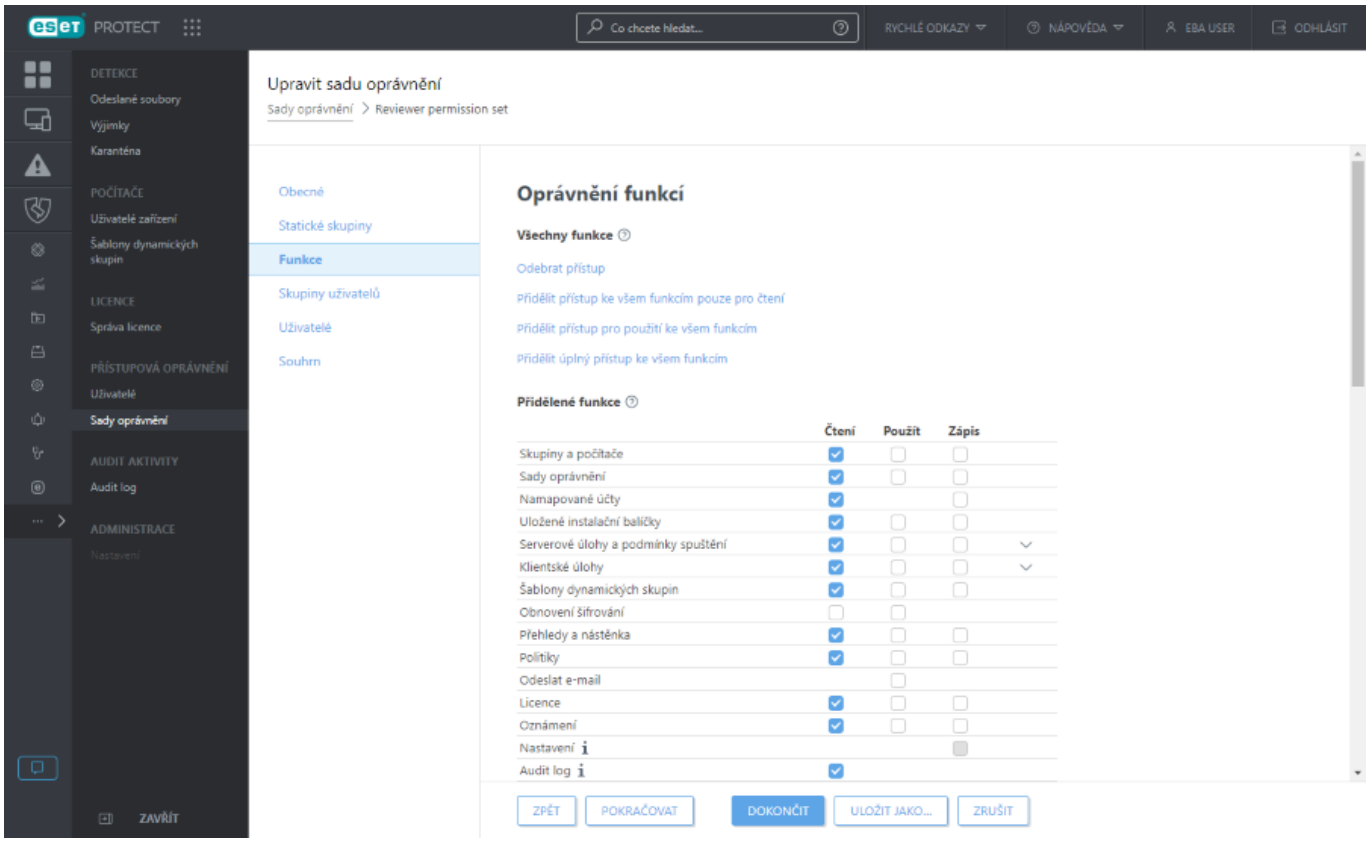
Výsledná zásada definující oprávnění pro přístup k objektu vznikne sloučením všech sad oprávnění přiřazených uživateli. Mějte příklad, kdy uživatel má přiřazeny dvě sady oprávnění. Jednu s úplným oprávněním do jeho domovské skupiny a druhou, v níž má pouze oprávnění pro čtení a použití u položky Skupiny a počítače. To znamená, že bude schopen nad počítači z druhé skupiny spouštět úlohy vytvořené ve své domovské skupině.

Obecně, uživatel může spouštět objekty z jedné statické skupiny nad jinou statickou skupinou, za předpokladu, že má oprávnění ke konkrétnímu typu objektu v dané skupině.

Prostřednictvím filtru 

Přístup skupiny si můžete vybrat konkrétní statickou skupinu a zjistit, jaké objekty vidí uživatelé, kteří jsou členem dané skupiny.

Pro filtrování zobrazených objektů můžete využít štítky.



Níže uvádíme několik důležitých tipů:
- Zamyslete se nad tím, zda všichni uživatelé potřebují přístup ke **klientské úloze** pro **spuštění příkazu**. Jedná se o velmi účinnou úlohu, ale v nesprávných rukách může být zneužita.
- Uživatelé, kteří nejsou administrátoři, by neměli mít přístup k **sadám oprávnění**, **namapovaným uživatelským účtům**.
- Pokud potřebujete vytvořit komplexnější model oprávnění, vytvořte si více sad oprávnění a dle povahy je přidělujte.

Oprávněním pro přístup k audit logu získá uživatel možnost zobrazit si všechny zaznamenané akce (všech uživatelů a ze všech domén auditu) – i takových, k nimž nemá daný uživatel oprávnění pro přístup.

Při práci s oprávněními můžete uživatelům přidělit rozdílnou úroveň přístupu. K dispozici máte tyto možnosti: **Čtení**, **Použít** a **Zápis**.

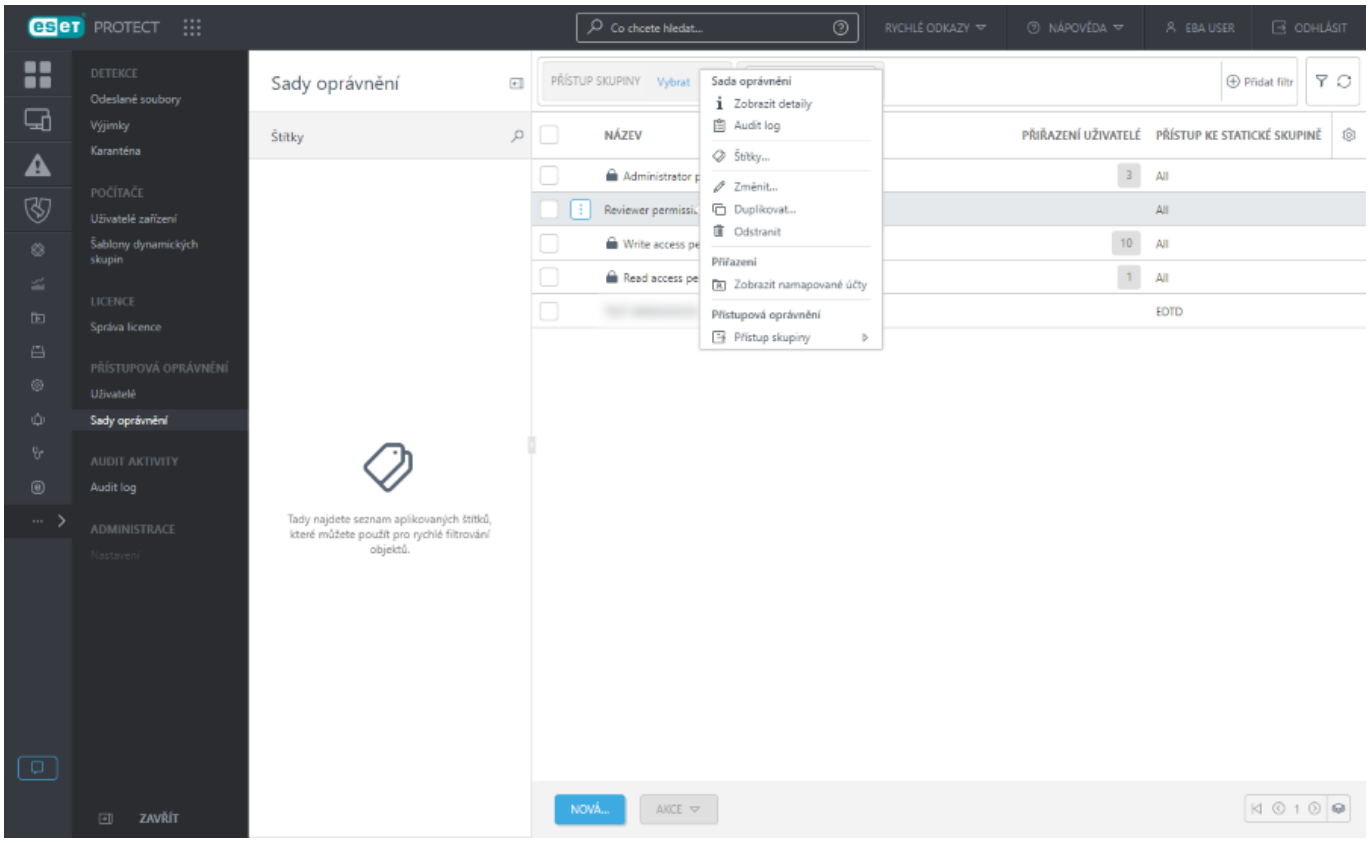
Aplikace

Pro duplikování objektů musí mít uživatel oprávnění pro **čtení** originálních objektů a **zápis** daného typu objektu ve své **domovské skupině**.
Filip, jehož domovskou skupinou je *Filipova skupina*, si chcete zkopírovat (zduplikovat) *Politiku 1*. Protože politiku vytvořil *Petr*, je umístěna v jeho domovské skupině s názvem *Petrova skupina*.
1.Pro dosažení je nutné: Vytvořit novou statickou skupinu, například *Sdílené politiky*.
2.Přiřadit oběma uživatelům (*Filipovi* a *Petrovi*) oprávnění pro **čtení politik** ve skupině *Sdílené politiky*.
3.*Petr* musí přesunout *Politiku 1* do skupiny *Sdílené politiky*.
4.Uživatel *Filip* musí mít oprávnění pro **vytvoření politik** ve své domovské skupině.
5.*Filip* nyní v seznamu politik uvidí *Politiku 1* a může si ji **zduplikovat**. Následně se mu zobrazí v jeho domovské skupině.

Rozdíl mezi Použít a Zápis

Pokud nechcete, aby mohl *Filip* modifikovat politiky umístěné ve skupině *Sdílené politiky*, *vytvořte* pro něj sadu oprávnění, ve které v sekci:
• Funkce **Politiky**: vyberte pouze možnost **Čtení** a **Použít**
• **Statické skupiny**: vyberte Sdílené politiky
Poté, co tuto sadu oprávnění přiřadíte *Filipovi*, bude schopen si sdílené politiky zobrazit a aplikovat. *Nedokáže* je však modifikovat ani mazat. Pokud budete chtít, aby Filip mohl vytvářet, upravovat a mazat politiky ve skupině *Sdílené politiky*, přiřaďte mu oprávnění pro **zápis**.

Správa oprávnění



Pro správu sady oprávnění na ní klikněte a v zobrazeném kontextovém menu si vyberte jednu z níže dostupných akcí:

Sada oprávnění

- **Zobrazit detaily** – kliknutím si zobrazíte detaily sadu oprávnění.
- **Audit log** – kliknutím si zobrazíte Audit log pro vybranou položku.
- **Štítky** – Pomocí této možnosti můžete přiřadit, odebrat, vytvořit nebo odstranit štítky.
- **Změnit** – kliknutím upravíte sadu oprávnění.
- **Duplikovat** – kliknutím vytvoříte kopii existující sady oprávnění, a můžete ji použít jako základ při vytváření nové sady oprávnění. Kopie se vytvoří v domovské skupině uživatele, který ji vytvářel.
- **Odstranit** – kliknutím odstraníte vybranou sadu oprávnění.

Přiřazení

- **Zobrazit namapované účty** – kliknutím zobrazíte seznam namapovaných účtů, které mají danou sadu oprávnění přiřazenou.

Přístupová oprávnění

- **Přístup skupiny** > **Přesunout** – Přesuňte objekt do jiné statické skupiny, kde je k dispozici uživatelům s dostatečnými právy k cílové skupině. To je užitečné, pokud chcete šablonu poskytnout jinému uživateli. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv.

> ⚠ Všechny předdefinované sady oprávnění mají přiřazen přístup k nejnadřazenější statické skupině **Všechny zařízení**. Při přiřazování těchto oprávnění uživatelům buďte opatrní. Uživatel tak získá přístup ke všem objektům v ESET PROTECT.

Vytvoření nebo úprava sady oprávnění

Pro vytvoření nové sady oprávnění klikněte na tlačítko **Nová**. Chcete-li upravit existující sadu oprávnění, klikněte na požadovanou a v kontextovém menu vyberte možnost **Změnit**.

Obecné

Zadejte **název** nové sady (vyžadované nastavení). Volitelně zadejte **popis** a vyberte **štítky**.

Pro přiřazení štítku klikněte na možnost **Vybrat štítky**.

Statické skupiny

Kliknutím na **Vybrat** můžete přidat jednu nebo více statických skupin, pro které bude sada platná (případně si **vytvořte novou skupinu**. Na objekty umístěné ve vybraných statických skupinách se aplikují oprávnění definovaná v sekci **Funkce**.

Funkce

Vyberte jednotlivé součásti Web Console, ke kterým chcete uživateli přidělit přístup. Uživatel s daným oprávněním bude mít přístup k souvisejícím úlohám. Oprávnění můžete definovat až na konkrétní typy klientských a serverových úloh. K dispozici jsou čtyři předdefinované sady funkcí. Použijte jednu z nich nebo oprávnění definujte ručně.

Přidělením oprávnění **Zápis** automaticky přidělení oprávnění **Použít** a **Čtení**. Přidělením oprávnění **Použít** automaticky přidělení oprávnění **Čtení**.

Skupiny uživatelů

Vyberte jednu nebo více skupin uživatelů, jejichž parametry se mohou použít v politice (například: režim dočasné změny nastavení).

Uživatelé

V této části vyberte uživatele, kterým chcete sadu přiřadit. Seznam dostupných uživatelů naleznete v levé části. Vyberte konkrétní uživatele nebo pro výběr všech klikněte na tlačítko **Přidat vše**. Vpravo je uveden seznam uživatelů, kterým sadu přiřadíte. Tato akce není nezbytně nutná, vytvořenou sadu můžete uživateli přiřadit později.

Souhrn

Zkontrolujte, zda nastavení odpovídá vašim představám a vytvoření sady oprávnění dokončete kliknutím na tlačítko **Dokončit**. Sada oprávnění se vytvoří v domovské skupině uživatele, které ji vytvářel.

Pro vytvoření kopie upravované sady oprávnění klikněte na tlačítko **Uložit jako**. Následně budete vyzváni k zadání názvu nové sady oprávnění.

Seznam oprávnění

Typy oprávnění

Při vytváření nebo úpravě sady oprávnění v sekci **Další** > **Přístupová oprávnění** > **Nová / Změnit** máte v sekci **Funkce** k dispozici kompletní seznam oprávnění, které můžete použít. Oprávnění v ESET PROTECT Web Console jsou rozdělena do několika kategorií, například **Skupiny a počítače**, **Politiky**, **Klientské úlohy**, **Přehledy**, **Oznámení** a další. Navíc ještě můžete určit způsob oprávnění ke konkrétnímu objektu. K dispozici máte možnost **Čtení**, **Použít** a **Zápis**. Níže uvádíme charakteristiku uvedených možností:

- Oprávnění pro **čtení** je vhodné pro audit. Jinými slovy, uživatel si může zobrazit data, ale nemůže je modifikovat.
- Oprávnění pro **použití** umožňuje uživateli použití objektů (spuštění úlohy, přiřazení politiky, ...), ale neumožňuje jejich modifikaci nebo odstranění.
- Oprávnění pro **zápis** umožňuje uživatelům plnohodnotnou manipulaci s objekty – jejich duplikování, úpravu, vytváření i mazání.

Některé typy oprávnění (uvedené níže) nedefinují přístup k objektům, ale uživateli umožňují použití konkrétní funkce. Jedná se o globální nastavení, nezáleží na statické skupině definované v dané sadě oprávnění. Použití funkce je následně limitováno dalšími oprávněními, která definují přístup k objektům. Například oprávnění pro **Export přehledu do souboru** umožní použití této funkce, ale data zobrazená v přehledu již budou ovlivněna dalšími oprávněními, ve kterých je definován přístup ke konkrétním statické skupině.

Do Databáze znalostí jsme připravili vzorové příklady oprávnění, které uživatel potřebuje k provádění konkrétních úloh.

Funkce, ke kterým nemá aktuální uživatel v rámci svého oprávnění přístup, budou nedostupné (šedivé).

Uživateli můžete přiřadit oprávnění pro použití těchto globálních funkcí:

- **Nasazení ESET Agenta**
- **Přehledy a nástěnka** (Vyžadováno pro fungování nástěnky. Zobrazená data již závisí na oprávnění, které uživateli definují přístup ke konkrétní skupině počítačů)
- **Odeslat e-mail**
- **Exportovat přehled do souboru**
- **Přístupový token AD Scanner**
- **Komplexní přehledy**
- **ESET MDR přehledy**

Seznam dostupných kategorií oprávnění:

Skupiny a počítače

Čtení – oprávnění pro zobrazení počítačů a skupin.

Použít – oprávnění pro použití počítače/skupiny jako cíle klientské úlohy nebo politiky.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání počítačů. Zahrnuje rovněž přejmenování počítačů a skupin.

Sady oprávnění

Čtení – oprávnění pro zobrazení seznamu sad oprávnění a jejich konfiguraci.

Použít – oprávnění pro přidělení/odebrání sady oprávnění uživatelům nebo doménovým skupinám.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání sad oprávnění.

Aby mohl uživatel přiřazovat nebo odebírat sady oprávnění, musí mít nastaveno oprávnění pro **Zápis** u položky **Namapované účty**.

Namapované účty

Čtení – oprávnění pro zobrazení seznamu namapovaných účtů.

Zápis – oprávnění pro přidělení/odebrání sady oprávnění.

Uložené instalační balíčky

Čtení – oprávnění pro zobrazení seznamu uložených instalačních balíčků.

Použít – oprávnění pro stažení vytvořených uložených instalačních balíčků.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání instalačních balíčků.

Serverové úlohy a podmínky spuštění

Čtení – oprávnění pro zobrazení seznamu klientských úloh a jejich konfigurace (vyjma citlivých polí jako jsou hesla).

Použít – oprávnění pro spuštění serverových úloh jako aktuálně přihlášený uživatel.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání serverových úloh.

Kategorie můžete rozbalit kliknutím na ikonu ⌄ a vybrat jeden nebo více typů serverových úloh .

Klientské úlohy

Čtení – oprávnění pro zobrazení seznamu klientských úloh a jejich konfigurace (vyjma citlivých polí jako jsou hesla).

Použít – oprávnění pro spuštění/přerušení běhu klientských úloh. Mějte na paměti, že pro přiřazení/zrušení přiřazení úlohy (počítači nebo skupině) musí mít uživatel přístup (oprávnění Použít) ke konkrétním objektům.

Zápis – oprávnění pro vytvoření, úpravu nebo odstranění klientských úloh. Mějte na paměti, že pro přiřazení/zrušení přiřazení úlohy (počítači nebo skupině) musí mít uživatel přístup (oprávnění **Použít**) ke konkrétním objektům.

Kliknutím na ikonu ⌄ rozbalíte seznam všech kategorií úloh a vybrat můžete pouze konkrétní typy úloh.

Šablony dynamických skupin

Čtení – oprávnění pro zobrazení seznamu šablon dynamických skupin a jejich konfigurace.

Použít – oprávnění pro vytvoření nové dynamické skupiny s použitím existujících šablon.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání šablon dynamických skupin.

Obnovení šifrování

Čtení

Použít – oprávnění pro inicializaci procesu na obnovení šifrování.

Přehledy a nástěnka

Čtení – oprávnění pro zobrazení seznamu šablon přehledů a jejich kategorií. Na základě šablon si uživatel může přehledy vygenerovat. Má přístup ke své nástěnce založené na výchozí nástěnce.

Použít – oprávnění pro změnu přehledů zobrazených na nástěnce. Uživatel si může vybrat některý z existujících přehledů.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání šablon přehledů a jejich kategorií. Uživatel si může plně konfigurovat nástěnku.

Politiky

Čtení – oprávnění pro zobrazení seznamu politik a jejich konfigurace.

Použít – oprávnění pro přiřazení/odebrání politiky počítači nebo skupinu. Mějte na paměti, že pro přiřazení/zrušení přiřazení politiky musí mít uživatel přístup (oprávnění **Použít**) ke konkrétním objektům.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání politik.

Odeslat e-mail

Použít – oprávnění pro odesílání e-mailů. (Potřeba pro odesílání oznámení a generovaných přehledů e-mailem.)

Licence

Čtení – oprávnění pro zobrazení seznamu licencí včetně jejich využití.

Použít – oprávnění pro použití licence pro aktivaci (v rámci klientské úlohy Aktivace produktu nebo Instalace aplikace).

Zápis – oprávnění pro přidání nebo odebrání licencí. (Domovskou skupinou uživatele musí být statická skupina

Všechna zařízení. Standardně má tento přístup pouze výchozí uživatel Administrator.)

Oznámení

Čtení – oprávnění pro zobrazení seznamu oznámení a jejich konfigurace.

Použít – oprávnění pro přiřazení štítků.

Zápis – oprávnění pro vytvoření, úpravu nebo odebrání oznámení.

Nastavení

Zápis – oprávnění měnit nastavení ESET PROTECT.

Audit log

Čtení – oprávnění pro zobrazení Audit logu a vygenerování stejnojmenného přehledu.

Přístupový token AD Scanner

Čtení

Zápis – vyžadováno pro synchronizaci s AD.

Komplexní přehledy

Použití – oprávnění generovat šablony MDR přehledů.

ESET MDR přehledy

Použití – oprávnění vyžadované pro archiv MDR přehledů.

Zápis – oprávnění generovat ESET MDR přehledy.

Přidělené funkce ESET Inspect

Seznam jednotlivých funkcí ESET Inspect, ke kterým bude mít uživatel přístup. Pro více informací se podívejte do Online nápovědy ESET Inspect. Uživatel Web Console potřebuje alespoň sadu oprávnění s hodnotou **pouze pro čtení** u možnosti **Přístup k ESET Inspect**.

Audit log

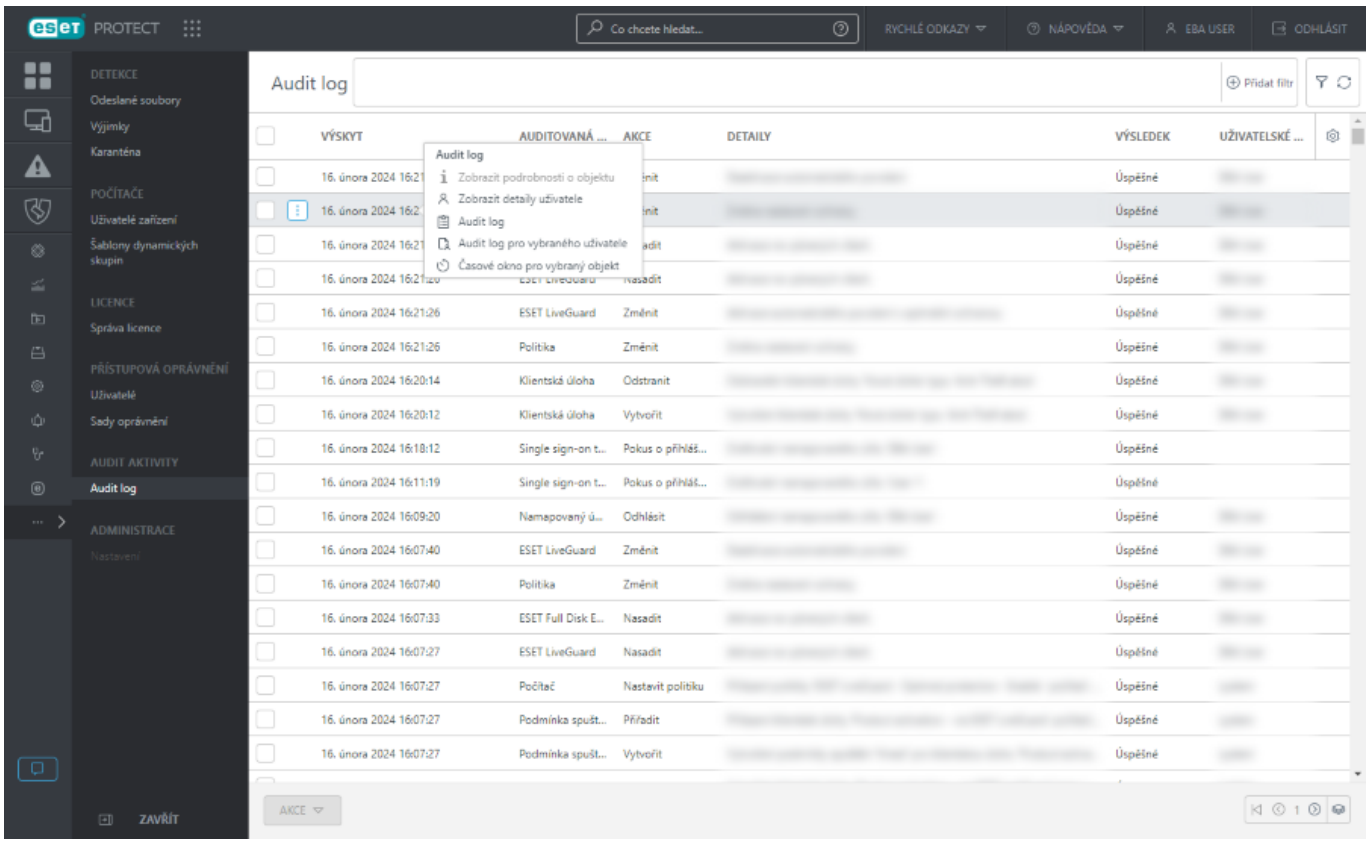
Do audit logu se zaznamenává každá akce provedená uživatelem v ESET PROTECT Web Console. Záznamy v audit logu se vytvoří při každém vzniku nebo modifikaci objektu (počítač, politika, detekce, atp.) v ESET PROTECT Web Console.

V ESET PROTECT naleznete Audit log v samostatné sekci. Naleznete v ní stejné informace jako ve vygenerovaném přehledu Audit log, nicméně nabízí pohodlnější možnosti pro filtrování zobrazených dat. Audit log pro většinu objektů Web Console si můžete zobrazit přímo z jejich kontextového menu po vybrání možnosti **Audit log**.

Díky audit logu můžete jako administrátor sledovat aktivity prováděné v ESET PROTECT Web Console, což oceníte především v případě, kdy ji používá více uživatelů.

Pro zobrazení Audit logu musí mít uživatel Web Console v rámci sady oprávnění povolenou funkci **Audit log**.

Oprávněním pro přístup k audit logu získá uživatel možnost zobrazit si všechny zaznamenané akce (všech uživatelů a ze všech domén auditu) – i takových, k nimž nemá daný uživatel oprávnění pro přístup.



Po kliknutí na záznam v audit logu máte k dispozici následující akce:

Zobrazit podrobnosti o objektu	Kliknutím si zobrazí detailní informace o auditovaném objektu.
Zobrazit detaily uživatele	Kliknutím si zobrazíte detailní informace o uživateli, který akci nad objektem provedl.
Audit log	Kliknutím si zobrazíte Audit log pro vybraný objekt.
Audit log pro vybraného uživatele	Kliknutím si zobrazíte Audit log pro vybraného uživatele.
Časové okno pro vybraný objekt	Kliknutím si zobrazíte Audit log pro vybraný objekt s aktivovaným filtrem pro časový výskyt.

Pro dodatečné filtrování výsledků klikněte na tlačítko **Přidat filtr**:

- **<= Výskyt** – zadejte datum a čas, před nímž byla akce provedena.
- **>= Výskyt** – zadejte datum a čas, po němž byla akce provedena.
- **Akce** – vyberte provedenou akci.
- **Doména auditu** – vyberte modifikovaný objekt Web Console.
- **Auditovaný uživatel** – vyberte uživatele Web Console, který akci provedl.
- **Výsledek** – vyberte výsledek akce.

Nastavení

V této sekci si můžete jako administrátor upravit parametry pro zasílání informací na svůj Syslog server a definovat dobu, po níž bude cloudová konzole uchovávat protokoly.

Sekce **Nastavení** je dostupná pouze uživateli s dostatečnými oprávněními (například s účtem superuživatele (ESET Business Account) nebo root uživatele (ESET MSP Administrator)).

Obecné

Syslog

ESET PROTECT může oznámení a informace o událostech zasílat na váš Syslog server. Dále je možné na syslog server přeposílat také exportované protokoly z klientských produktů ESET.

Uchovávání dat

V této části si můžete nastavit dobu pro úklid jednotlivých typů protokolů uložených v cloudové konzoli. Pro jednotlivé kategorie můžete nastavit interval ve dnech/týdnech/měsících nebo letech. Interval údržby můžete definovat samostatně pro následující typy protokolů:

Typ protokolu	Příklad typu protokolu
Protokoly detekce	• Antivirus • Blokované soubory • Firewall • HIPS • Webová ochrana (filtrované webové stránky)
Protokoly správy	• Úlohy • Podmínky spuštění • Exportovaná konfigurace • Registrace
Audit log	• Audit log a Audit log vygenerovaný do přehledu.
Protokoly monitorování	• Správa zařízení • Filtrování obsahu webu • Přihlášení uživatelé

Diagnostické protokoly se každý den odstraňují. Jako uživatel si nemůžete změnit interval jejich odstranění.

Limity úložiště:

Typ protokolu	Minimum	Standardní	Maximum
Protokoly detekce	1 den	90 dní	365 dní
Protokoly správy	1 den	30 dní	30 dní
Audit log	1 den	180 dní	730 dní
Protokoly monitorování	1 den	30 dní	30 dní

Podrobnější informace, co se stane s daty po vypršení platnosti poslední vhodné licence, naleznete v samostatné kapitole.

Ochrana relací Web Console

Blokovat žádosti z odlišných IP adres

- **Povolit**: tuto možnost použijte pro omezení rozsahu IP adresy, ze kterých mohou uživatele přistupovat k vaší Web Console.
- **Vypnout**:
  - **Trvale zakázat** – vybráním této možnosti nebude filtrován přístup k vaší Web Console podle IP adres.
  - **Vypnout na** – vyberte časové období, po které nebude platit restrikce na přístup pouze z povolených IP adres.

Statické skupiny

Automaticky párovat nalezené počítače – pokud je tato možnost **zapnutá**, nalezené počítače se budou automaticky párovat se zařízeními umístěnými ve statických skupinách na základě názvu stanice, který reportuje ESET Management Agent.

- Pokud se párování nezdaří, počítač bude umístěn do výchozí skupiny Ztráty a nálezy.
- Pokud nelze názvu stanice důvěřovat, doporučujeme automatické párování počítačů vypnout.

Správa mobilních zařízení (MDM)

Registrace Microsoft Entra ID

Viz Registrace Microsoft Entra ID (Android nebo iOS).

Synchronizace s Apple Business Manager (ABM)

Viz Synchronizace s Apple Business Manager (ABM) (iOS).

Synchronizace s Microsoft Intune

Viz Synchronizace s Microsoft Intune (Android).

VMware Workspace ONE Synchronizace

Viz Synchronizace s VMware Workspace ONE (Android).

Migrace mobilních zařízení z ESET PROTECT (on-premise)

Další informace si přečtěte v kapitole MDM Migration Tool.

Export protokolů do syslogu

ESET PROTECT dokáže exportovat specifické protokoly/události a zasílat je na váš Syslog server. Na Syslog server se exportují události z následujících kategorií: Detekce, Firewall, HIPS, Audit a ESET Inspect. Jedná se o události, které vygenerovaly produkty ESET (například ESET Endpoint Security) na klientských stanicích. Tyto informace následně může ze syslog serveru přebírat jakýkoli SIEM (Security Information and Event Management) nástroj. Data do Syslogu zasílá ESET PROTECT.

1. Pro aktivaci zasílání dat na Syslog server přejděte v hlavním menu Web Console do sekce **Další** > **Nastavení** > **Syslog**. Pomocí přepínače aktivujte možnost **Používat Syslog server**.

Uživatelé syslog serveru mají přístup ke všem exportovaných protokolům.

2. Vyberte si formát, do kterého chcete události exportovat. K dispozici máte tyto formáty:

   - JSON (JavaScript Object Notation)
   - LEEF (Log Event Extended Format) – formát používaný aplikací IBM QRadar
   - CEF (Common Event Format)

Pokud chcete na Syslog server zasílat pouze některé události, vytvořit si oznámení s vámi požadovaným filtrem.

Syslog server

V případě potřeby si můžete aktivovat také Export protokolů do syslogu, kdy bude zasílat informace o detekcích, zablokované komunikaci personálním firewallem a blokovaných akcích modulem HIPS atp. získaných z koncových stanic s ESET Endpoint Security.

Pro aktivaci zasílání dat na Syslog server postupujte podle následujících kroků:

1.Klikněte na **Další** > **Nastavení**. Na záložce **Syslog server** aktivujte pomocí přepínače možnost **Používat Syslog server**.

2.Dále vyplňte vyžadovaná pole:

a.**Formát datové části**: – JSON, LEEF nebo CEF

b.**Formát obálky protokolu – BSD** (specifikace), **Syslog** (specifikace)

c.**Zaznamenávat od úrovně – Informační**, **Varování**, **Chyba** nebo **Kritické**

d.**Typ události protokolu**: vyberte typ, který chcete zasílat (**Antivirus**, **HIPS**, **Firewall**, **Webová ochrana**, **Audit Log**, **Blokované soubory**, **ESET Inspect upozornění**).

e.**Cílová IP adresa nebo FQDN syslog serveru kompatibilního s protokolem TLS** – IPv4 adresa nebo název cílového Syslog serveru

f.**Ověřovat kořenové certifikáty certifikační autority TLS spojení** – pomocí přepínače rozhodněte, zda chcete zapnout ověřování spojení mezi vaším Syslog serverem a ESET PROTECT. Po zapnutí ověřování se zobrazí nové pole, do kterého zkopírujte požadovaný řetězec certifikátu. Certifikát serveru musí splňovat následující požadavky:

- Celý řetězec certifikátu v PEM formátu musí být nahrán a uložen v konfiguraci pro export do Syslogu (to znamená kořenovou CA, neboť služba nedisponuje vestavěným úložištěm důvěryhodných certifikátů)

- V certifikátu vašeho Syslogu serveru je použit Subject Alternative Name (DNS=/IP=), kdy alespoň jeden ze záznamů odpovídá zadanému názvu serveru (FQDN/IP) v konfiguraci

> K úspěšnému ověření potřebujete certifikát od autority verze 3 (a novější) s rozšířením Basic Constraints.
> Ověřování připojení s protokolem TLS se vztahuje pouze na certifikáty. Zakázání ověřování nemá vliv na nastavení protokolu TLS v ESET PROTECT.

Po dokončení změn klikněte na tlačítko **Použít nastavení**. Změny v konfiguraci se uplatní do 10 minut.

> Do standardního protokolu se zapisují všechny události. Naopak na Syslog server se exportují některé nepravidelné události, jako jsou oznámení a události z klientských stanic.

Bezpečnostní omezení a limity syslogu

Z důvodu bezpečnostních požadavků na připojení k syslog serveru je níže uvedené nastavení stálé a není jej možné změnit:

- Transportní protokol: TLS

- TCP port: 6514

Ze stejných důvodů jsou na straně přijímacího syslog serveru povinná níže uvedená nastavení:

- IP adresa: Globálně routovatelná IPv4 adresa

- IDN názvy: Musí použít ASCII reprezentaci ("xn--")

- FQDN: Musí být přeložitelný na jednu pevnou IPv4 adresu.

> Použití FQDN:
> Pokud je váš Syslog server dostupný na více strojích / IP adresách (CDN), není možné zaručt, kdy a jak často dojde k opětovnému překladu FQDN. Je však zaručeno, že k prvnímu překladu FQN dojde do 10 minut od spuštění serveru, pokud je exportování do Syslogu povoleno a správně nakonfigurováno.

Dodatečné bezpečnostní nastavení

Administrátoři by měli ve firewallu na Syslog serveru povolit příjem exportovaných událostí pouze z níže uvedených IP rozsahů:

- Odchozí IP adresy z ESET PROTECT pro region Evropy: 51.136.106.164/30
- Odchozí IP adresy z ESET PROTECT pro region USA: 40.81.8.148/30
- Odchozí IP adresy z ESET PROTECT pro region Japonsko: 20.78.10.184/30

Události exportované do JSON formátu

JSON (JavaScript Object Notation) je jednoduchý formát pro výměnu dat. Je založený na dvou datových strukturách: kolekce párů název-hodnota a seřazeném seznamu hodnot.

Exportované události

V této části uvádíme formát všech exportovaných událostí společně s popisem jednotlivých atributů. Zprávy událostí jsou reprezentovány JSON objektem, kdy některé části jsou povinné, jiné volitelné. Každá exportovaná událost bude obsahovat tyto atributy:

event_type	řetězec		Typ exportované události: • Threat_Event (Detekce **antivirem**) • FirewallAggregated_Event (Detekce **firewallem**) • HipsAggregated_Event (Detekce **HIPS**) • Audit_Event (Audit log) • FilteredWebsites_Event (Filtrované webové stránky – **Webová ochrana**) • EnterpriseInspectorAlert_Event (ESET Inspect upozornění) • BlockedFiles_Event (Blokované soubory)
ipv4	řetězec	volitelné	IPv4 adresa počítače, který vygeneroval událost
ipv6	řetězec	volitelné	IPv6 adresa počítače, který vygeneroval událost
hostname	řetězec		Název počítače, který vygeneroval událost
source_uuid	řetězec		UUID počítače, který vygeneroval událost
occurred	řetězec		Čas v UTC formátu, kdy událost vznikla. Formát: %d-%b-%Y %H:%M:%S
severity	řetězec		Závažnost události. Možné hodnoty (seřazeno od málo kritických po nejzávažnější): `Informační`, `Oznámení`, `Varování`, `Chyba`, `Kritické`, `Mimořádné`.
group_name	řetězec		Statická skupina, ve které se nachází počítač, který vygeneroval událost. Pokud je cesta delší než 255 znaků, bude obsahovat group_name pouze název statické skupiny.
group_description	řetězec		Popis statické skupiny.
os_name	řetězec		Informace o operačním systému počítače.

Na Syslog Server se zasílají při všech úrovních závažnosti a všechny níže uvedené události: Pokud chcete na Syslog server zasílat pouze některé události, vytvořit si oznámení s vámi požadovaným filtrem. Reportované hodnoty závisí na nainstalovaném bezpečnostním produktu ESET (a jeho verzi) na spravovaném zařízení, ESET PROTECT pouze reportuje obdržená data. Z tohoto důvodu společnost ESET nemůže poskytnout úplný seznam všech hodnot. Doporučujeme sledovat síť a filtrovat protokoly na základě obdržených hodnot.

Vlastní klíče související s event_type:

Threat_Event

Na Syslog server se zasílají všechny Detekce **antivirem** ze spravovaných koncových stanic. Záznam o detekci vypadá následovně:

threat_type	řetězec	volitelné	Typ detekce
threat_name	řetězec	volitelné	Název detekce
threat_flags	řetězec	volitelné	Štítek související s detekcí
scanner_id	řetězec	volitelné	ID skeneru
scan_id	řetězec	volitelné	ID kontroly
engine_version	řetězec	volitelné	Verze skenovacího jádra
object_type	řetězec	volitelné	Typ objektu související s touto událostí
object_uri	řetězec	volitelné	URI objektu
action_taken	řetězec	volitelné	Provedená akce s objektem
action_error	řetězec	volitelné	Chybová zpráva v případě, že se "akci" nepodařilo úspěšně provést
threat_handled	bool	volitelné	Informace o tom, zda byla detekce vyřešena
need_restart	bool	volitelné	Informace, zda je vyžadován restart
username	řetězec	volitelné	Název uživatelského účtu spojeného s touto událostí
processname	řetězec	volitelné	Název procesu spojeného s touto událostí
circumstances	řetězec	volitelné	Krátký popis s informací, co způsobilo událost
hash	řetězec	volitelné	SHA1 kontrolní součet (detekce) data streamu.
firstseen	řetězec	volitelné	Datum a čas první detekce na zařízení. V závislosti na výstupním formátu (JSON nebo LEEF) generuje ESET PROTECT firstseenatribut (a další atributy související s časem) v odlišném tvaru: • JSON formát: "%d-%b-%Y %H:%M:%S" • LEEF formát: "%b %d %Y %H:%M:%S"

Příklad Threat_Event JSON protokolu:

```
Jun 21 11: 46: 40 030 - MG ERAServer[5648]: {
    "event_type": "Threat_Event",
    "ipv4": "192.168.30.30",
    "hostname": "030-mg",
    "group_name": "All/Lost & found",
```

```
        "os_name": "Microsoft Windows 11 Pro",
        "group_description": "Lost & found static group",
        "source_uuid": "1361a9f6-1d45-4561-b33a-b5d6c62c71e0",
        "occured": "21-Jun-2021 09:46:15",
        "severity": "Warning",
        "threat_type": "Virus",
        "threat_name": "XF/Gydhex.A",
        "scanner_id": "Real-time file system protection",
        "scan_id": "virlog.dat",
        "engine_version": "23497 (20210621)",
        "object_type": "file",
        "object_uri": "file:///C:/Users/Administrator/Downloads/xls/YICT080714.xls",
        "action_taken": "Deleted",
        "threat_handled": true,
        "need_restart": false,
        "username": "030-MG\\Administrator",
        "processname": "C:\\Program Files\\WinRAR\\WinRAR.exe",
        "circumstances": "Event occurred on a newly created file.",
        "firstseen": "21-Jun-2021 09:46:14",
        "hash": "5B97884A45C6C05F93B22C4059F3D9189E88E8B7"
    }
```


FirewallAggregated_Event

Protokoly událostí, které vygeneruje ESET Firewall (**Detekce firewallem**), sesbírá ESET Management agent za účelem snížení množství přenášených dat během replikace ESET Management agenta / ESET PROTECT serveru. Záznam o událostech firewallu vypadá následovně:

event	řetězec	volitelné	Název události
source_address	řetězec	volitelné	Adresa zdroje události
source_address_type	řetězec	volitelné	Typ adresy zdroje události
source_port	číslo	volitelné	Port zdroje události
target_address	řetězec	volitelné	Adresa cíle události
target_address_type	řetězec	volitelné	Typ adresy cíle události
target_port	číslo	volitelné	Port cíle události

event	řetězec	volitelné	Název události
protocol	řetězec	volitelné	Protokol
account	řetězec	volitelné	Název uživatelského účtu spojeného s touto událostí
process_name	řetězec	volitelné	Název procesu spojeného s touto událostí
rule_name	řetězec	volitelné	Název pravidla
rule_id	řetězec	volitelné	ID pravidla
inbound	bool	volitelné	Informace, zda se jednalo o příchozí spojení
threat_name	řetězec	volitelné	Název detekce
aggregate_count	číslo	volitelné	Počet, který udává, kolik stejných zpráv vygenerovalo bezpečnostní řešení na stanici mezi dvěma po sobě jdoucími replikacemi spravujícího ESET Management agenta a ESET PROTECT Serverem.
action	řetězec	volitelné	Akce
handled	řetězec	volitelné	Informace o tom, zda byla detekce vyřešena

Příklad FirewallAggregated_Event JSON protokolu:


```
Jun 21 3: 54: 07 030 - MG ERAServer[5648]: {
 "event_type": "FirewallAggregated_Event",
 "ipv4": "192.168.30.30",
 "hostname": "w16test",
     "group_name": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
 "occured": "21-Jun-2021 13:10:04",
 "severity": ""Warning",
 "event": "Security vulnerability exploitation attempt",
 "source_address": "127.0.0.1",
 "source_address_type": "IPv4",
 "source_port": 54568,
 "target_address": "127.0.0.1",
 "target_address_type": "IPv4",
 "target_port": 80,
 "protocol": "TCP",
 "account": "NT AUTHORITY\\NETWORK SERVICE",
```

```
 "process_name": "C:\\Program Files\\Apache Software Foundation\\apache-
tomcat-9.0.41\\bin\\tomcat9.exe",

 "inbound": true,

 "threat_name": "CVE-2017-5638.Struts2",

 "aggregate_count": 1

}
```


HIPSAggregated_Event

Před odesláním událostí na syslog server jsou zprávy z modulu HIPS ( Detekce **HIPS**) nejprve filtrovány podle nastavené **závažnosti**. Záznam o událostech modulu HIPS vypadá následovně:

application	řetězec	volitelné	Název aplikace
operation	řetězec	volitelné	Operace
target	řetězec	volitelné	Cíl
action	řetězec	volitelné	Akce
action_taken	řetězec	volitelné	Provedená akce s objektem
rule_name	řetězec	volitelné	Název pravidla
rule_id	řetězec	volitelné	ID pravidla
aggregate_count	číslo	volitelné	Počet, který udává, kolik stejných zpráv vygenerovalo bezpečnostní řešení na stanici mezi dvěma po sobě jdoucími replikacemi spravujícího ESET Management agenta a ESET PROTECT Serverem.
handled	řetězec	volitelné	Informace o tom, zda byla detekce vyřešena

Příklad HipsAggregated_Event JSON protokolu:


```
Jun 21 13: 54: 07 030 - MG ERAServer[5648]: {

    "event_type": "HipsAggregated_Event",

    "ipv4": "192.168.30.181",

    "hostname": "test-w10-uefi",

    "group_name": "All/Lost & found",

    "os_name": "Microsoft Windows 11 Pro",

    "group_description": "Lost & found static group",

    "source_uuid": "5dbe31ae-4ca7-4e8c-972f-15c197d12474",

    "occured": "21-Jun-2021 11:53:21",

    "severity": "Critical",

    "application": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\ja
va.exe",
```

```
    "operation": "Attempt to run a suspicious object",
    "target": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\trojan.
exe",
    "action": "blocked",
    "handled": true,
    "rule_id": "Suspicious attempt to launch an application",
    "aggregate_count": 2
}
```


Audit_Event

ESET PROTECT přeposílá na Syslog interní audit log. Záznam o událostech vypadá následovně:

domain	řetězec	volitelné	Doména
action	řetězec	volitelné	Akce
target	řetězec	volitelné	Cíl, nad kterým je akce prováděna
detail	řetězec	volitelné	Detailní popis akce
user	řetězec	volitelné	Uživatel, který akci provádí
result	řetězec	volitelné	Výsledek akce

Příklad Audit_Event protokolu:


```
Jun 21 11: 42: 00 030 - MG ERAServer[5648]: {
    "event_type": "Audit_Event",
    "ipv4": "192.168.30.30",
    "hostname": "030-MG",
    "group_name": "All/Lost & found",
    "os_name": "Microsoft Windows 11 Pro",
    "group_description": "Lost & found static group",
    "source_uuid": "72cdf05f-f9c8-49cc-863d-c6b3059a9e8e",
    "occured": "21-Jun-2021 09:42:00",
    "severity": "Information",
    "domain": "Native user",
    "action": "Login attempt",
    "target": "Administrator",
    "detail": "Authenticating native user 'Administrator'.",
```

```
    "user": "",
    "result": "Success"
}
```


FilteredWebsites_Event

ESET PROTECT přeposílá seznam filtrovaných webových stránek (Detekce **webové ochrany**) na Syslog. Záznam o událostech vypadá následovně:

processname	řetězec	volitelné	Název procesu spojeného s touto událostí
username	řetězec	volitelné	Název uživatelského účtu spojeného s touto událostí
hash	řetězec	volitelné	SHA1 hash filtrovaného objektu
event	řetězec	volitelné	Typ události
rule_id	řetězec	volitelné	ID pravidla
action_taken	řetězec	volitelné	Akce
scanner_id	řetězec	volitelné	ID skeneru
object_uri	řetězec	volitelné	URI objektu
target_address	řetězec	volitelné	Adresa cíle události
target_address_type	řetězec	volitelné	Typ adresy cíle události (25769803777 = IPv4; 25769803778 = IPv6)
handled	řetězec	volitelné	Informace o tom, zda byla detekce vyřešena

Příklad FilteredWebsites_Event JSON protokolu:


```
Jun 21 3: 56: 03 020 - MG ERAServer[5648]: {
 "event_type": "FilteredWebsites_Event",
 "ipv4": "192.168.30.30",
 "hostname": "win-test",
     "group_name": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
 "occured": "21-Jun-2021 03:56:20",
 "severity": "Warning",
 "event": "An attempt to connect to URL",
 "target_address": "192.255.255.255",
 "target_address_type": "IPv4",
 "scanner_id": "HTTP filter",
```

```
 "action_taken": "blocked",        "object_uri": "https://test.com",
 "hash": "ABCDAA625E6961037B8904E113FD0C232A7D0EDC",
 "username": "WIN-TEST\\Administrator",
 "processname": "C:\\Program Files\\Web browser\\brwser.exe",
 "rule_id": "Blocked by PUA blacklist"
}
```


EnterpriseInspectorAlert_Event

ESET PROTECT přeposílá ESET Inspect upozornění na Syslog. Záznam o událostech vypadá následovně:

processname	řetězec	volitelné	Název procesu, který způsobil tento alarm
username	řetězec	volitelné	Vlastník procesu
rulename	řetězec	volitelné	Název pravidla, které aktivovalo tento alarm
count	číslo	volitelné	Počet oznámení, vygenerovaných tímto typem, od posledního alarmu
hash	řetězec	volitelné	SHA1 hash alarmu
eiconsolelink	řetězec	volitelné	Odkaz na alarm do ESET Inspect konzole
eialarmid	řetězec	volitelné	ID části odkazu alarmu ($1 v ^http.*/alarm/([0-9]+)$)
computer_severity_score	číslo	volitelné	Úroveň závažnosti počítače
severity_score	číslo	volitelné	Skóre závažnosti pravidla

Příklad EnterpriseInspectorAlert_Event JSON protokolu:


```
Jun 16 16:19:00 Win2016Std ERAServer[2772]: {
 "event_type": "EnterpriseInspectorAlert_Event",
 "ipv4": "192.168.30.30",
 "hostname": "shdsolec.vddjc",
     "group_name": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "source_uuid": "csd77ad2-2453-42f4-80a4-d86dfa9d0543",
 "occured": "13-Jun-2021 07:45:00",
 "severity": "Warning",
 "processname": "ProcessName",
 "username": "UserName",
```

```
 "rulename": "RuleName2",
 "count": 158,
 "eiconsolelink": "http://eiserver.tmp/linkToConsole",
 "computer_severity_score": "1",
 "severity_score": "1"
}
```


BlockedFiles_Event

ESET PROTECT přeposílá blokované soubory pomocí ESET Inspect na Syslog. Záznam o událostech vypadá následovně:

processname	řetězec	volitelné	Název procesu spojeného s touto událostí
username	řetězec	volitelné	Název uživatelského účtu spojeného s touto událostí
hash	řetězec	volitelné	SHA1 hash blokovaného souboru
object_uri	řetězec	volitelné	URI objektu
action	řetězec	volitelné	Akce
firstseen	řetězec	volitelné	Datum a čas první detekce na zařízení (formát data a času).
cause	řetězec	volitelné	
description	řetězec	volitelné	Popis blokovaného souboru
handled	řetězec	volitelné	Informace o tom, zda byla detekce vyřešena

Události exportované do LEEF formátu

Pokud chcete na Syslog server zasílat pouze některé události, vytvořit si oznámení s vámi požadovaným filtrem.

LEEF formát je upravený formát událostí pro aplikaci IBM® Security QRadar®. Události mají standardní a vlastní atributy.

- ESET PROTECT používá některé ze standardních atributů popsaných v dokumentaci společnosti IBM.
- Vlastní atributy jsou shodné s JSON formátem. V atributu deviceGroupName je uvedena statická skupina, ve které se počítač nachází. Ten události generuje. Pokud je cesta delší než 255 znaků, bude obsahovat deviceGroupName pouze název statické skupiny. V atributu deviceOSName je uvedena informace o operačním systému počítače. deviceGroupDescription obsahuje popis statické skupiny.

Kategorie událostí:

- Detekce antivirem
- Firewall
- Filtrované webové stránky – Webová ochrana
- HIPS

- Audit
- Upozornění ESET Inspect
- Blokované soubory

Další informace o Log Event Extended Format (LEEF) si přečtěte na webových stránkách IBM.

Události exportované do CEF formátu

Pokud chcete na Syslog server zasílat pouze některé události, vytvořit si oznámení s vámi požadovaným filtrem.

CEF je textový formát protokolu vyvinutý společností ArcSight™. Zpráva ve formátu CEF se skládá z CEF hlavičky a CEF rozšíření. Rozšíření obsahuje seznam párů klíč-hodnota.

CEF hlavička

Hlavička	Příklad	Popis
Device Vendor	ESET	
Device Product	ProtectCloud	
Device Version	10.0.5.1	Verze ESET PROTECT
Device Event Class ID (Signature ID):	109	Unikátní identifikátor kategorie události na zařízení: • 100-199 Detekce hrozby • 200-299 Událost firewallu • 300-399 HIPS událost • 400–499 Záznam z audit logu • 500-599 ESET Inspect událost • 600-699 Blokované soubory • 700-799 Filtrované webové stránky
Event Name	Detected port scanning attack	Popis s informací, co způsobilo událost
Severity	5	Zaznamenávat od úrovně: • 2 – Informační • 3 – Oznámení • 5 – Varování! • 7 – Chyba • 8 – Kritická • 10 – Fatální

CEF rozšíření společné pro všechny kategorie

Název rozšíření	Příklad	Popis
cat	ESET Threat Event	Kategorie události: • ESET Threat Event • ESET Firewall Event • ESET HIPS Event • ESET RA Audit Event • ESET Inspect Event • ESET Blocked File Event • ESET Filtered Website Event
dvc	10.0.12.59	IPv4 adresa počítače, který vygeneroval událost
c6a1	2001:0db8:85a3:0000:0000:8a2e:0370:7334	IPv6 adresa počítače, který vygeneroval událost
c6a1Label	Device IPv6 Address	
dvchost	COMPUTER02	Název počítače, který vygeneroval událost
deviceExternalId	39e0feee-45e2-476a-b17f-169b592c3645	UUID počítače, který vygeneroval událost
rt	Jun 04 2017 14:10:0	Čas v UTC formátu, kdy událost vznikla. Formát je %b %d %Y %H:%M:%S
ESETProtectDeviceGroupName	All/Lost & found	Statická skupina, ve které se nachází počítač, který vygeneroval událost. Pokud je cesta delší než 255 znaků, bude obsahovat ESETProtectDeviceGroupName pouze název statické skupiny.
ESETProtectDeviceOsName	Microsoft Windows 11 Pro	Informace o operačním systému počítače.
ESETProtectDeviceGroupDescription	Lost & found static group	Popis statické skupiny.

CEF rozšíření podle kategorie

Detekce hrozby

Název rozšíření	Příklad	Popis
cs1	W97M/Kojer.A	Název nalezené hrozby
cs1Label	Threat Name	
cs2	25898 (20220909)	Verze detekčního jádra
cs2Label	Engine Version	
cs3	Virus	Typ detekce
cs3Label	Threat Type	
cs4	Real-time file system protection	ID skeneru

Název rozšíření	Příklad	Popis
cs4Label	Scanner ID	
cs5	virlog.dat	ID kontroly
cs5Label	Scan ID	
cs6	Failed to remove file	Chybová zpráva v případě, že se "akci" nepodařilo úspěšně provést
cs6Label	Action Error	
cs7	Event occurred on a newly created file	Krátký popis s informací, co způsobilo událost
cs7Label	Circumstances	
cs8	0000000000000000000000000000000000000000	SHA1 kontrolní součet (detekce) data streamu.
cs8Label	Hash	
act	Cleaned by deleting file	Provedená akce s objektem
filePath	file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC	URI objektu
fileType	File	Typ objektu související s událostí
cn1	1	Detekce byla zpracována (1) nebo nebyla zpracována (0)
cn1Label	Handled	
cn2	0	Vyžadován restart (1) nebo není vyžadován restart (0)
cn2Label	Restart Needed	

Název rozšíření	Příklad	Popis
suser	172-MG\\Administrator	Název uživatelského účtu spojeného s touto událostí
sprod	C:\\7-Zip\\7z.exe	Název procesu zdroje události
deviceCustomDate1	Jun 04 2019 14:10:00	
deviceCustomDate1Label	FirstSeen	Datum a čas první detekce na zařízení. Formát je %b %d %Y %H:%M:%S

Příklad protokolu o zachycených hrozbách ve formátu CEF:

CEF:O|ESET|Protect|10.0.0.0|183|File scanner cleaned a virus|5|deviceExternalId=e9d26759-fd21-47f1-9751-d2e7194c41a8 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Threat Event rt=Jun 04 2017 14:10:00 cs1=W97M/Kojer.A cs1Label=Threat Name cs2=25898 (20220909) cs2Label=Engine Version cs3=Virus cs3Label=Threat Type cs4=Real-time file system protection cs4Label=Scanner ID cs5=virlog.dat cs5Label=Scan ID act=Cleaned by deleting fileType=File filePath=file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC cn1=1 cn1Label=Handled suser=172-MG\\Administrator sprod=C:\\7-Zip\\7z.exe cs7=Event occurred on a newly created file. cs7Label=Circumstances eviceCustomDate1=Jun 04 2019 14:10:00 deviceCustomDate1Label=FirstSeen cs8=0000000000000000000000000000000000000000 cs8Label=Hash

Události firewallu

Název rozšíření	Příklad	Popis
msg	TCP Port Scanning attack	Název události
src	127.0.0.1	IPv4 adresa zdroje události
c6a2	2001:0db8:85a3:0000:0000:8a2e:0370:7334	IPv6 adresa zdroje události
c6a2Label	Source IPv6 Address	
spt	36324	Port zdroje události
dst	127.0.0.2	IPv4 adresa cíle události
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	IPv6 adresa cíle události
c6a3Label	Destination IPv6 Address	
dpt	24	Cílový port události
proto	http	Protokol
act	Blocked	Akce
cn1	1	Detekce byla zpracována (1) nebo nebyla zpracována (0)

Název rozšíření	Příklad	Popis
cn1Label	Handled	
suser	172-MG\\Administrator	Název uživatelského účtu spojeného s touto událostí
deviceProcessName	someApp.exe	Název procesu spojeného s touto událostí
deviceDirection	1	Informace, zda se jednalo o příchozí (0) nebo odchozí spojení (1)
cnt	3	Počet udávající, kolik stejných zpráv produkt na stanici vygeneroval mezi dvěma replikacemi ESET Management Agenta na ESET PROTECT.
cs1		ID pravidla
cs1Label	Rule ID	
cs2	custom_rule_12	Název pravidla
cs2Label	Rule Name	
cs3	Win32/Botnet.generic	Název hrozby
cs3Label	Threat Name	

Příklad protokolu o událostech firewallu ve formátu CEF:

```
CEF:O|ESET|Protect|10.0.0.0|109|Detected port scanning attack|5|deviceExternalId=39e0feee-45e2-476a-b07f-169b592c3645 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET Firewall Event rt=Jun 04 2017 14:10:00 msg=TCP Port Scanning attack src=127.0.0.1 spt=36324 dpt=21 dst=127.0.0.2 proto=http act=Blocked cnt=1 cn1=1 cn1Label=Handled suser=myAccount deviceProcessName=someApp.exe cs2=rule_118882389 cs2Label=Rule Name deviceDirection=0 cs3=Win32/Botnet.generic cs3Label=Threat Name
```

HIPS události

Název rozšíření	Příklad	Popis
cs1	Suspicious attempt to launch an application	ID pravidla
cs1Label	Rule ID	
cs2	custom_rule_12	Název pravidla
cs2Label	Rule Name	
cs3	C:\\someapp.exe	Název aplikace
cs3Label	Application	
cs4	Attempt to run a suspicious object	Operace
cs4Label	Operation	
cs5	C:\\somevirus.exe	Cíl
cs5Label	Target	
act	Blocked	Akce
cs2	custom_rule_12	Název pravidla
cn1	1	Detekce byla zpracována (1) nebo nebyla zpracována (0)
cn1Label	Handled	

Název rozšíření	Příklad	Popis
cnt	3	Počet udávající, kolik stejných zpráv produkt na stanici vygeneroval mezi dvěma replikacemi ESET Management Agenta na ESET PROTECT.

Příklad protokolu o událostech HIPS ve formátu CEF:

```
CEF:O|ESET|Protect|10.0.0.0|303|Attempt to run a suspicious object Blocked|5|dvchost=test_bcmcjkbpgp deviceExternalId=82e114a8-9070-4868-8ee2-1e87b7b85ee3 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group cat=ESET HIPS Event rt=Jun 04 2019 14:10:00 cs3=C:\\someapp.exe cs3Label=Application cs4=Attempt to run a suspicious object cs4Label=Operation cs5=C:\\somevirus.exe cs5Label=Target act=Blocked cn1=1 cn1Label=Handled cs1=Suspicious attempt to launch an application cs1Label=Rule ID cnt=1
```

Záznamy z audit logu

Název rozšíření	Příklad	Popis
act	Login attempt	Akce
suser	Administrator	Uživatel, který akci provádí
duser	Administrator	Cílový uživatel zabezpečení (například při pokusech o přihlášení)
msg	Authenticating native user 'Administrator'	Detailní popis akce
cs1	Native user	Doména
cs1Label	Audit Domain	
cs2	Success	Výsledek akce
cs2Label	Result	

Příklad protokolu auditu ve formátu CEF:

```
CEF:O|ESET|Protect|10.0.0.0|449|Native user login|2|dvc=10.15.172.133 dvchost=BRNH00006D deviceExternalId=db4a82c0-e1c6-49be-8bac-a436136ed1f4 cat=ESET RA Audit Event rt=Sep 21 2022 13:10:23 cs1=Native user cs1Label=Audit Domain act=Login attempt duser=Administrator msg=Authenticating native user 'Administrator'. cs2=Success cs2Label=Result
```

ESET Inspect události

Název rozšíření	Příklad	Popis
deviceProcessName	c:\\imagepath_bin.exe	Název procesu, který způsobil tento alarm
suser	HP\\home	Vlastník procesu
cs2	custom_rule_12	Název pravidla, které aktivovalo tento alarm
cs2Label	Rule Name	
cs3	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	SHA-1 kontrolní součet alarmu
cs3Label	Hash	
cs4	https://inspect.eset.com:443/console/alarm/126	Odkaz na alarm do ESET Inspect Web Console

Název rozšíření	Příklad	Popis
cs4Label	EI Console Link	
cs5	126	ID části odkazu alarmu ($1 v ^http.*/alarm/([0-9]+)$)
cs5Label	EI Alarm ID	
cn1	275	Úroveň závažnosti počítače
cn1Label	ComputerSeverityScore	
cn2	60	Skóre závažnosti pravidla
cn2Label	SeverityScore	
cnt	3	Počet oznámení, vygenerovaných tímto typem, od posledního alarmu

Příklad protokolu události v ESET Inspect ve formátu CEF:

```
CEF:O|ESET|Protect|10.0.0.0|500|ESET Inspect Alert|5|dvchost=test_lrghlbjyoa
deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found
ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static
group cat=ESET Inspect Alert rt=Sep 21 2022 07:31:55
deviceProcessName=c:\\mother_process_info_imagepath_dir\\mother_process_info_imagepath_bin.exe
suser=HP\\home cs2=9_1_0addd4e8baf8e87d4bc4ed77fadc cs2Label=Rule Name
cs3=78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9 cs3Label=Hash
cs4=https://dev-inspect.eset.com:443/console/alarm/126 cs4Label=EI Console Link cs5=126 cs5Label=EI Alarm
ID cn1=275 cn1Label=ComputerSeverityScore cn2=60 cn2Label=SeverityScore
```

Blokované soubory

Název rozšíření	Příklad	Popis
act	Execution blocked	Akce
cn1	1	Detekce byla zpracována (1) nebo nebyla zpracována (0)
cn1Label	Handled	
suser	HP\\home	Název uživatelského účtu spojeného s touto událostí
deviceProcessName	C:\\Windows\\explorer.exe	Název procesu spojeného s touto událostí
cs1	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	SHA-1 kontrolní součet blokovaného souboru
cs1Label	Hash	
filePath	C:\\totalcmd\\TOTALCMD.EXE	URI objektu
msg	ESET Inspect	Popis zablokovaného souboru
deviceCustomDate1	Jun 04 2019 14:10:00	
deviceCustomDate1Label	FirstSeen	Datum a čas první detekce na zařízení. Formát je %b %d %Y %H:%M:%S
cs2	Blocked by Administrator	Příčina
cs2Label	Cause	

Příklad protokolu o blokovaných souborech ve formátu CEF:

```
CEF:O|ESET|Protect|10.0.0.0|600|Blocked File Event|5|dvchost=test_lrghlbjyoa
deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found
ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static
group cat=ESET Blocked File Event rt=Sep 21 2022 07:31:55 act=Execution blocked cn1=1 cn1Label=Handled
suser=HP\\home deviceProcessName=C:\\Windows\\explorer.exe
cs1=78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9 cs1Label=Hash filePath=C:\\totalcmd\\TOTALCMD.EXE
deviceCustomDate1=Sep 21 2022 07:31:55 deviceCustomDate1Label=FirstSeen cs2=Blocked by Administrator
cs2Label=Cause msg=ESET Inspect
```

Filtrované webové stránky

Název rozšíření	Příklad	Popis
msg	An attempt to connect to URL	Typ události
act	Blocked	Akce
cn1	1	Detekce byla zpracována (1) nebo nebyla zpracována (0)
cn1Label	Handled	
suser	Peter	Název uživatelského účtu spojeného s touto událostí
deviceProcessName	Firefox	Název procesu spojeného s touto událostí
cs1	Blocked by PUA blacklist	ID pravidla
cs1Label	Rule ID	
requestUrl	https://kenmmal.com/	URL zablokovaného požadavku
dst	172.17.9.224	IPv4 adresa cíle události
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	IPv6 adresa cíle události
c6a3Label	Destination IPv6 Address	
cs2	HTTP filter	ID skeneru
cs2Label	Scanner ID	
cs3	8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5	SHA1 hash filtrovaného objektu
cs3Label	Hash	

Příklad protokolu o filtrovaných webových stránkách ve formátu CEF:

```
CEF:O|ESET|Protect|10.0.0.0|716|Filtered Website Event|5|dvchost=test_lrghlbjyoa
deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found
ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static
group cat=ESET Filtered Website Event rt=Sep 21 2022 07:31:55 msg=An attempt to connect to URL
dst=172.17.9.224 cs2=HTTP filter cs2Label=Scanner ID act=Blocked cn1=1 cn1Label=Handled
requestUrl=https://kenmmal.com cs3=8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5 cs3Label=Hash
suser=Peter deviceProcessName=Firefox cs1=Blocked by PUA blacklist cs1Label=Rule ID
```

ESET PROTECT pro poskytovatele spravovaných služeb

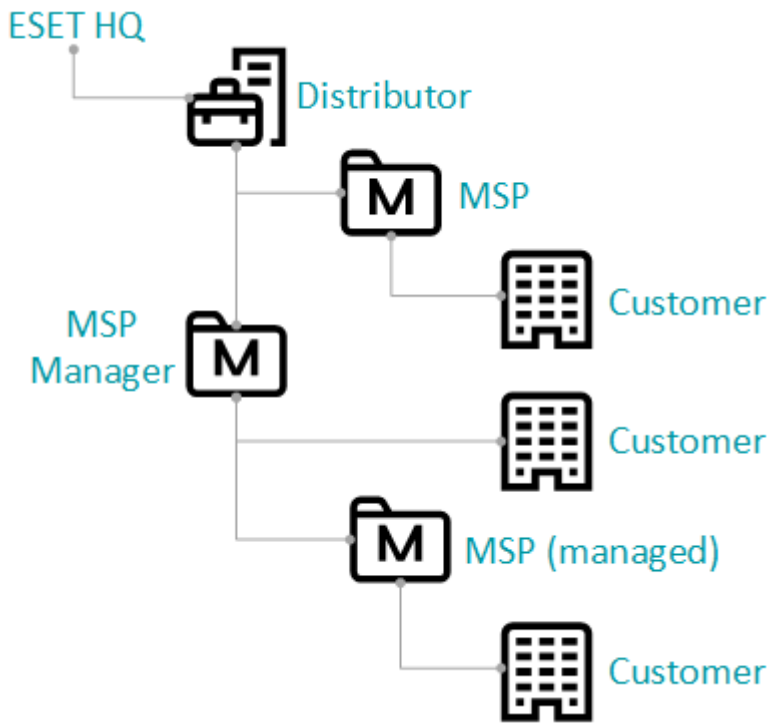
Kdo je MSP

MSP je zkratka pro "Managed Service Provider". MSP obvykle poskytují IT služby svým zákazníkům, například správu bezpečnostních produktů (ESET Endpoint Antivirus aj.).

- MSP mají jiné požadavky a potřeby při používání ESET PROTECT, než SMB nebo enterprise zákazníci. Více informací naleznete v kapitole doporučené scénáře nasazení pro MSP.
- Pro více informací o ESET MSP programu kontaktujte lokálního partnera ESET nebo navštivte webovou stránku ESET Managed Service Provider Program.

Struktura entit v MSP

ESET PROTECT synchronizuje strukturu z ESET MSP Administrator a ve Web Console je v sekci **Počítače** reprezentována jako strom statických skupin.



- **Distributor** – distributorem je ESET partner, MSP nebo MSP Manager.
- **MSP Manager** – spravuje více MSP společností. MSP Manager může mít přímo pod sebou koncové zákazníky.
- **MSP** – cílový čtenář této příručky. MSP poskytuje služby svým zákazníkům. MSP například vzdáleně spravuje počítače zákazníka, instaluje na ně a spravuje bezpečnostní produkty ESET.
- **Spravovaný MSP** – zastává podobnou roli jako MSP, nicméně je spravován MSP Managerem.
- **Zákazník** – koncový uživatel licence na ESET produkt. Zákazník by neměl konfigurovat produkty ESET. Zákazník může mít různé stavy označené ikonou:

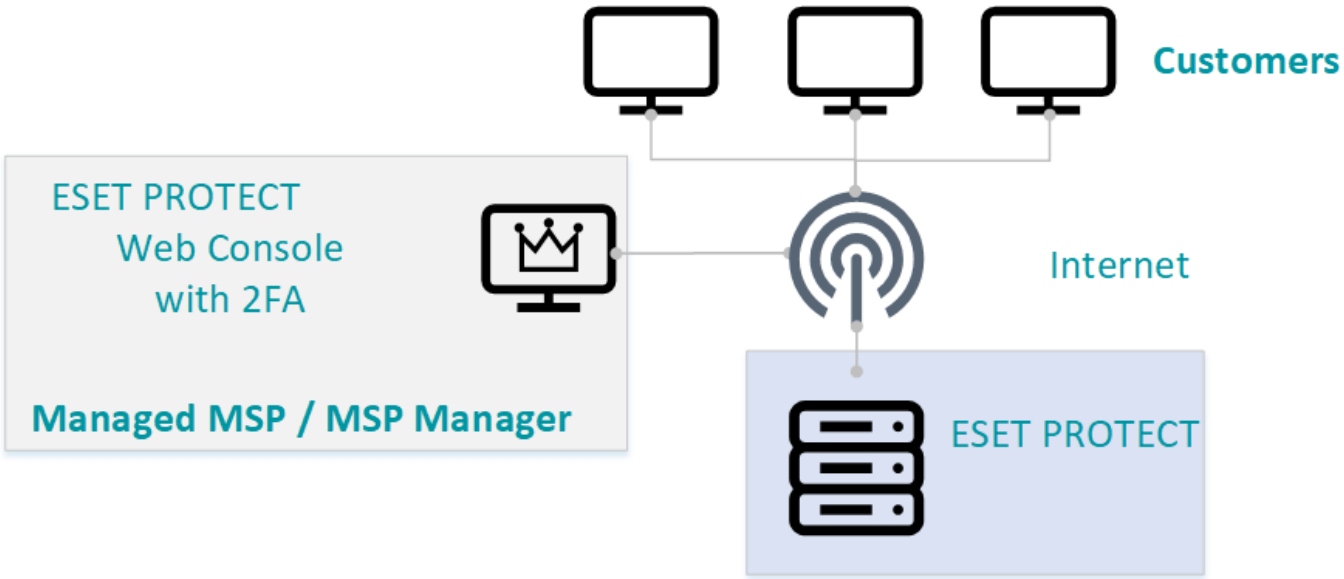
- – zákazník ještě nebyl nastaven.
- – zákazník byl nastaven, nebo jste nastavení zákazníka přeskočili.
- – zákazník byl odstraněn.

Po synchronizaci účtu MSP si mohou uživatelé MSP zobrazit seznam spravovaných zákaznických účtů v hlavní nabídce ESET PROTECT > Spravovaní zákazníci.

Specifika MSP prostředí

Infrastruktura konzole pro vzdálenou správu se v případě MSP obchodního modelu liší od SMB nebo enterprise prostředí. V MSP prostředí se typicky zákazníci nacházejí mimo síť MSP společnosti. ESET Management Agenti nainstalovaní na počítačích zákazníka musí mít přímou konektivitu na ESET PROTECT z veřejné části internetu. Ujistěte se, že jste otevřeli příslušné porty umožňující viditelnost ESET PROTECT.

Standardní konfigurace MSP:



ESET PROTECT nasazený prostřednictvím smíšeného účtu

Smíšený účet je ten, který má stejné přihlašovací údaje do portálu ESET Business Account a ESET MSP Administrator. V tomto případě můžete ESET PROTECT instanci vytvořit z libovolného účtu. Po vytvoření instance k ní můžete přistupovat z obou účtu (EMA 2 i EBA). Odstranit instanci ESET PROTECT však můžete pouze prostřednictvím účtu, který jste použili pro její vytvoření.

Funkce v ESET PROTECT pro uživatele MSP

ESET PROTECT nabízí funkce určené MSP uživatelům. MSP funkce jsou dostupné uživatelům, kteří nasadili instanci ESET PROTECT prostřednictvím:

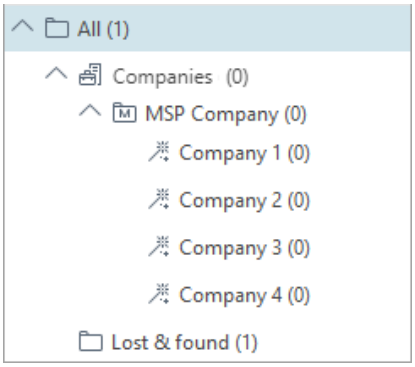
- ESET MSP Administrator (EMA 2) účtu
- ESET Business Account účtu, který má stejné přihlašovací údaje také do EMA 2

Průvodce konfigurací zákazníka

Průvodce konfigurací MSP zákazníka představuje klíčovou funkci ESET PROTECT pro MSP uživatele. Pomocí této funkce můžete přizpůsobit instalační balíček ESET Management Agenta pro vašeho zákazníka.

MSP strom

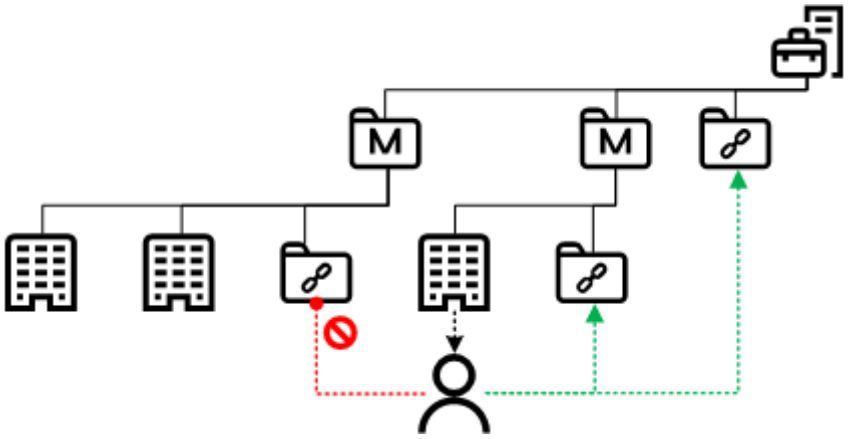
ESET PROTECT se synchronizuje s ESET MSP portálem (EMA 2) a vytvoří MSP strom. MSP strom představuje strukturu počítačů reprezentující strukturu společností ve vašem EMA 2 účtu. Pro odlišení používají položky v MSP stromu jiné ikony, než standardní zařízení a skupiny ESET PROTECT. MSP strom není možné prostřednictvím Web Console modifikovat.



Sdílené objekty

ESET PROTECT po synchronizaci MSP účtu vytvoří MSP strom. Pro každého MSP uživatele a MSP manažera je k dispozici jedna skupina s názvem **Sdílené objekty**. Přístup skupiny nastavuje Statickou skupinu objektu a přístup k objektu na základě uživatelských přístupových práv. Do statické skupiny **Sdílené objekty** nelze přesouvat počítače. Statická skupina **Sdílené objekty** se nezobrazuje mezi jednotlivými **Skupinami** na záložce **Počítače**. Prostřednictvím této **skupiny** si v rámci MSP můžete sdílet objekty jako jsou politiky a úlohy.

Každý MSP uživatel vytvořený průvodcem konfigurací zákazníka má oprávnění pro čtení a použití všech objektů ve skupině **Sdílené objekty**, která se nachází nad ním. Pro zjištění, k jakým skupinám má uživatel přístup, a jaké operace může provádět, se podívejte na sady oprávnění, které má uživatel přiřazeny. Uživatelé mají vždy přístup k nadřazené skupině Sdílené objekty, nikoli skupinám paralelních MSP manažerů.



Spravované zákaznice/zákazníci

Po synchronizaci účtu MSP si mohou uživatelé MSP zobrazit seznam spravovaných zákaznických účtů v hlavní nabídce ESET PROTECT > Spravovaní zákazníci.

Stav MSP

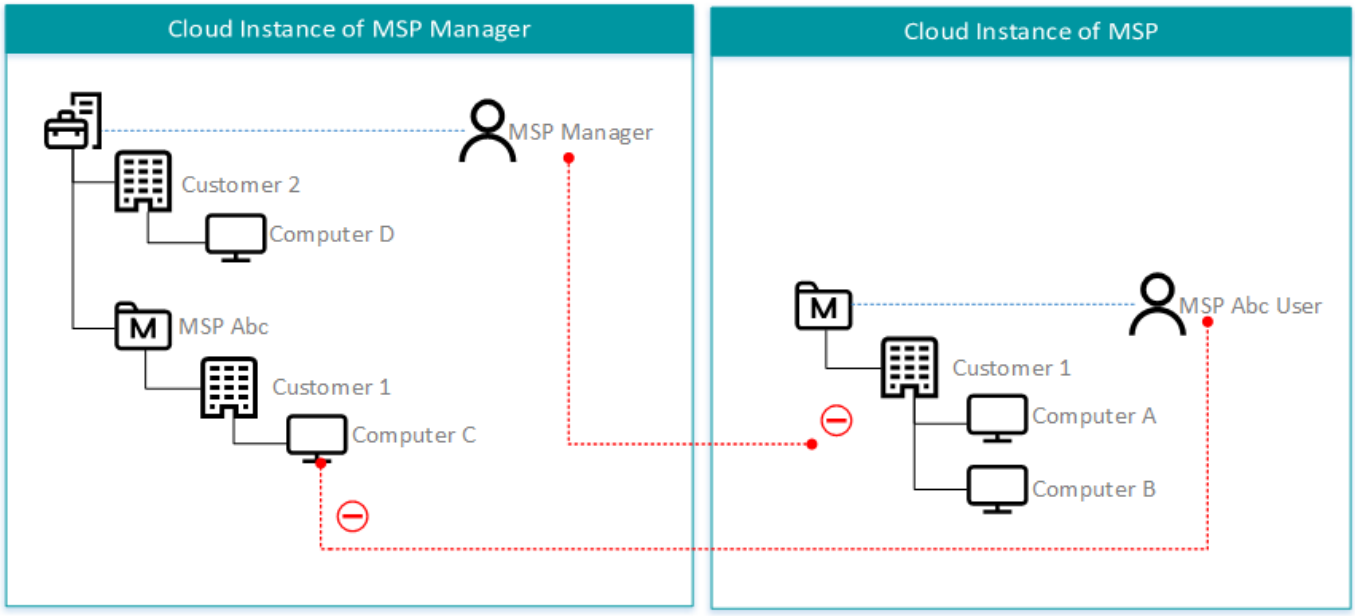
V sekci Přehled stavu se objeví nová MSP dlaždice. Na této dlaždici naleznete základní informace o svém MSP účtu.

Více instancí ESET PROTECT v MSP struktuře

Při pro nasazení cloudové instance použili MSP účet, jednotlivé MSP instance jsou od sebe odděleny. Instance MSP Managera nejsou mezi sebou propojeny. Sdílejí stejnou strukturu společnosti (MSP strom), ale nesdílejí mezi sebou počítače, stejně tak další objekty jako úlohy nebo politiky. Jedinou výjimkou jsou licence. Ty jsou sdíleny hierarchicky, stejně jako v ESET MSP Administrator. MSP Manager si může zobrazit své MSP licence ve Web Console a přiřadit je zařízením.

Níže uvádíme příklad:

MSP uživatel nemá přístup k počítačům v rámci instance MSP Managera, ačkoli se počítače nacházejí ve statické skupině MSP zákazníka. Je to z důvodu, že jednotlivé cloudové instance jsou od sebe odděleny.

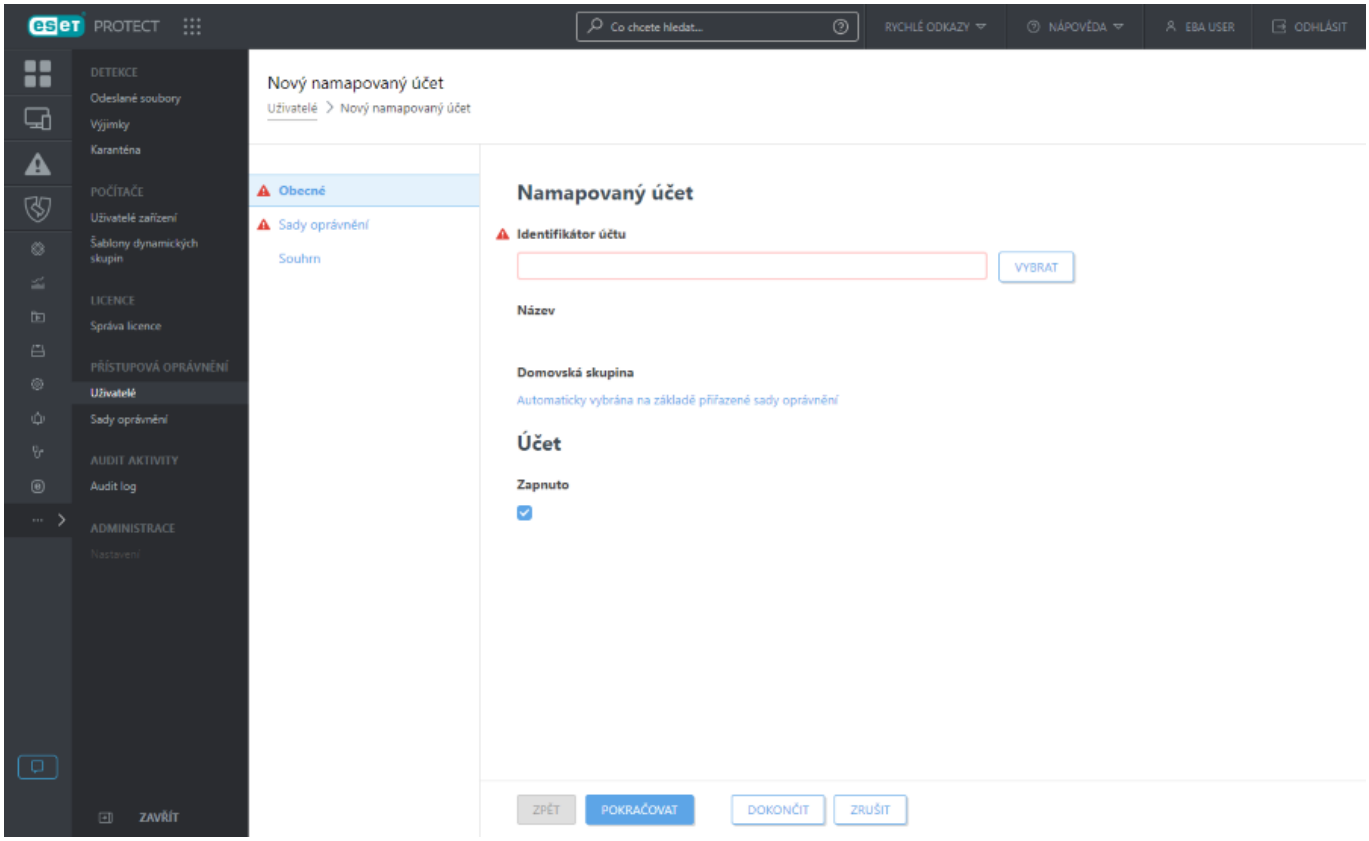


Vytvoření nového uživatele ESET PROTECT v ESET MSP Administrator

Abyste mohli vytvořit nového uživatele pro ESET PROTECT Web Console, musíte jej nejprve vytvořit v ESET MSP Administrator (EMA 2). Návod krok za krokem naleznete v online příručce k portálu EMA 2. Nového uživatele můžete vytvořit v průběhu nastavení MSP zákazníka nebo pomocí níže uvedených kroků.

- Zjistěte, jak fungují uživatelská oprávnění v EMA 2 a ESET PROTECT.
- Zjistěte, jak vytvořit ESET PROTECT instanci.

1. Otevřete si Web Console.
2. Přejděte na záložku **Uživatelé**.

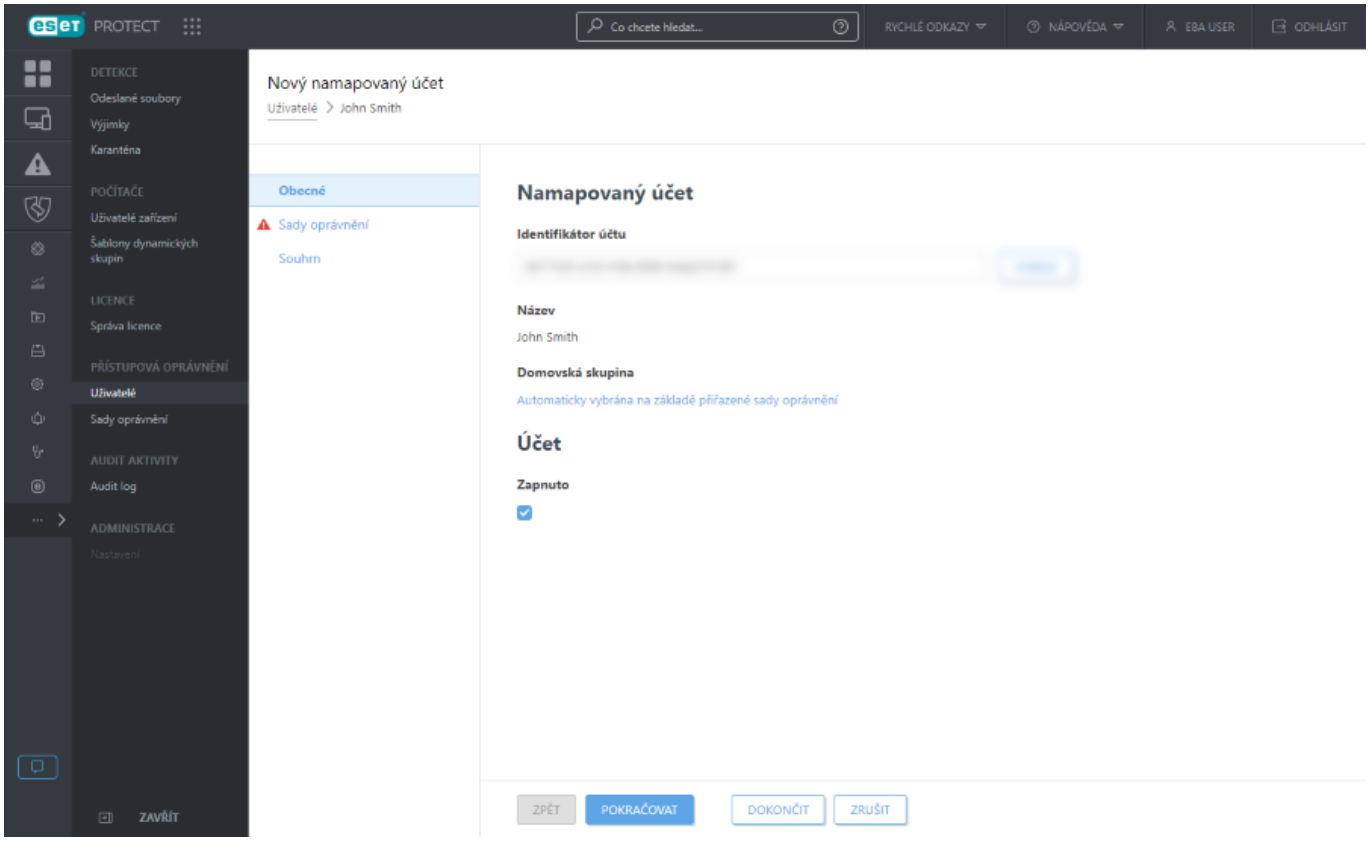


3. Vedle pole **Identifikátor účtu** klikněte na možnost **Vybrat** a následně vyberte uživatele, kterému chcete povolit přístup do ESET PROTECT.

4. Uživateli můžete přiřadit existující štítek, případně vytvořit nový.

5. Vedle pole **Domovská skupina** klikněte na tlačítko **Vybrat**. Domovská skupina je reprezentována statickou skupinou, do níž se ukládají objekty vytvořené uživatelem.

6. Klikněte na **Sady oprávnění**.



7. Vyberte sadu oprávnění, kterou chcete uživateli přiřadit. Sada oprávnění definuje úroveň přístupových oprávnění uživatele. Každá sada oprávnění umožňuje uživateli provádět akce nad konkrétní statickou skupinou. Přístup ke skupině je definován v každé sadě oprávnění. Uživateli můžete přiřadit libovolné množství sad oprávnění. Můžete si vybrat jedno z navržených oprávnění nebo si vytvořit nové.

> **Nastavení oprávnění pro domovskou skupinu**
> Přiřaďte vybranému uživateli sadu oprávnění k jeho domovské skupině. Bez přístupového oprávnění k domovské skupině neuvidí objekty v ní umístěné a nebude je schopen ani ve své domovské skupině vytvářet.

8. Pro uložení změn klikněte na tlačítko **Dokončit**.

Uživatel se nyní může do ESET PROTECT Web Console přihlásit svými přihlašovacími údaji k EMA 2.

Proces nasazení pro MSP

1.Dokončete průvodce konfigurací MSP zákazníka. Při vytváření instalačního balíčku vyberte možnost **Pouze agent**.

2.Na stanice zákazníka nasaďte ESET Management Agenta – lokálně nebo vzdáleně.

3.Nainstalujte bezpečnostní produkty ESET a nakonfigurujte je prostřednictvím politik.

Níže uvedené schéma popisuje proces registrace MSP zákazníka.

Lokální nasazení agenta

Lokální nasazení Instalátoru samostatného agenta

Instalátor samostatného agenta (*.exe* pro Windows nebo *.sh* pro Linux) obsahuje veškeré potřebné informace pro klientskou stanici. Díky tomu je možné ESET Management Agenta stáhnout a nainstalovat. Pokud instalujete na linuxovou stanici, ujistěte se, že splňuje veškeré požadavky.

Spustit jej můžete lokálně, případně z výměnného média (například USB disku).

Klientská stanice musí mít přístup k internetu, aby si mohla stáhnout instalační balíček Agenta a následně připojila k ESET PROTECT.

V případě potřeby si můžete skript upravit podle svých požadavků. Tuto možnost doporučujeme pouze zkušeným uživatelům.

Lokální nasazení prostřednictvím all-in-one instalačního balíčku

Instalační balíček pro ochranu stanice (tzv. all-in-one instalační balíček) obsahuje bezpečnostní produkt ESET dle vašeho výběru a předkonfigurovaný instalátor ESET Management Agenta.

Pro více informací se podívejte do příručky k instalačnímu balíčku.

Vzdálené nasazení agenta

Vzdálené nasazení Instalátoru samostatného agenta

Instalátor samostatného agenta (*.exe* pro Windows nebo *.sh* pro Linux) obsahuje veškeré potřebné informace pro klientskou stanici. Díky tomu je možné ESET Management Agenta stáhnout a nainstalovat. Pokud instalujete na linuxovou stanici, ujistěte se, že splňuje veškeré požadavky. V tomto případě můžete uživatelům distribuovat online například prostřednictvím e-mailu nebo výměnných médií, a nechat instalaci na nich. Pokud máte tu možnost, využijte k distribuci a spuštění instalačního balíčku nástroje třetí strany určené pro vzdálenou správu.

Klientská stanice musí mít přístup k internetu, aby si mohla stáhnout instalační balíček Agenta a následně připojila k ESET PROTECT.

Vzdálené nasazení prostřednictvím all-in-one instalačního balíčku

Instalátor určený pro ochranu stanice (tzv. all-in-one instalační balíček) můžete vzdáleně v síti nasadit

prostřednictvím ESET Remote Deployment Tool. Pro více informací se podívejte do uživatelské příručky k ESET Remote Deployment Tool.

MSP licence

Informace o licencích a společnostech

• Každé licenci je přiřazen štítek s názvem společnosti. Pokud společnost později přejmenujete, název štítku zůstane beze změny. Jeho název si však můžete ručně kdykoli změnit.

• Všechny importované licence jsou kompatibilní s ESET PROTECT bezpečnostním modelem. Díky tomu každý uživatel vytvořený prostřednictvím průvodce konfigurací MSP zákazníka bude mít přístup pouze ke svým licencím.

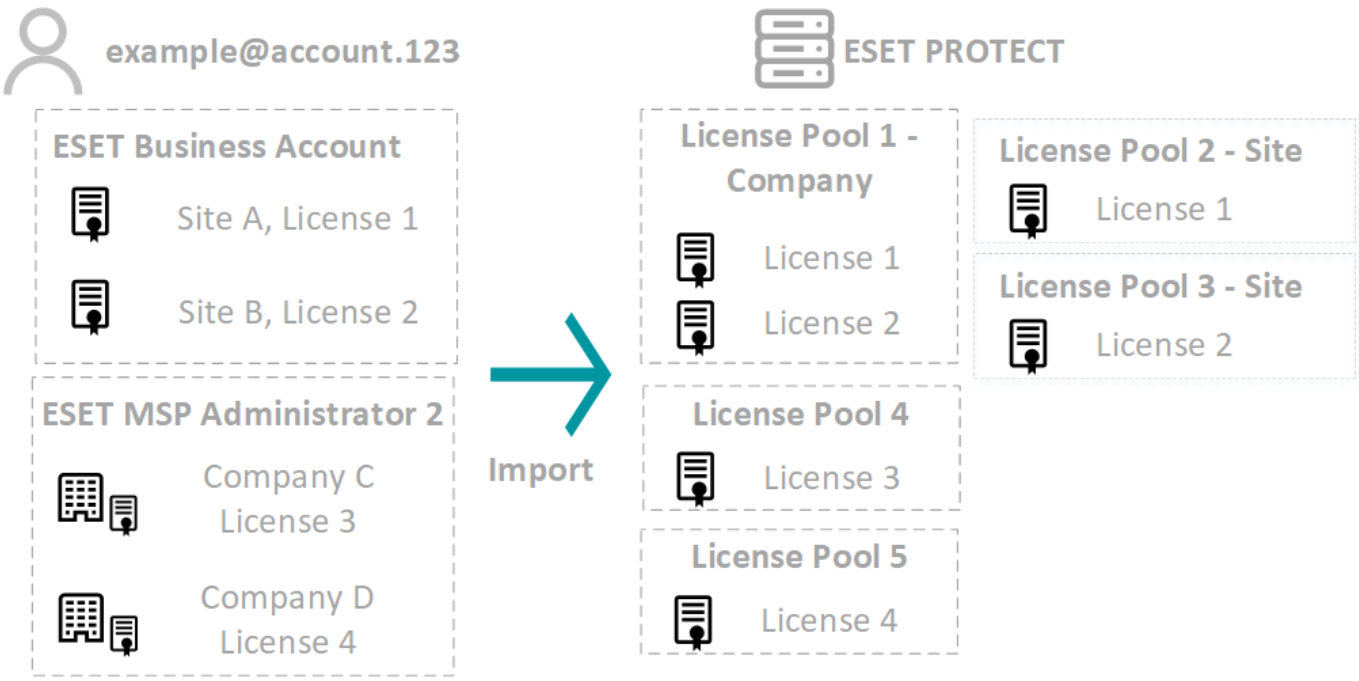
• Pokud ve své MSP struktuře máte společnost, která v době synchronizace neměla žádnou licenci, dojde k synchronizaci pouze MSP stromu z pohledu počítačů, nikoli licenční MSP strom.

• Pokud do ESET MSP Administrator 2 přidáte novou společnost, do MSP stromu v ESET PROTECT se přidá při další synchronizaci.

• Licence z ESET MSP Administrator 2 se rozdělí do fondů dle jednotlivých společností. Licence není možné z tohoto fondu přesunout.

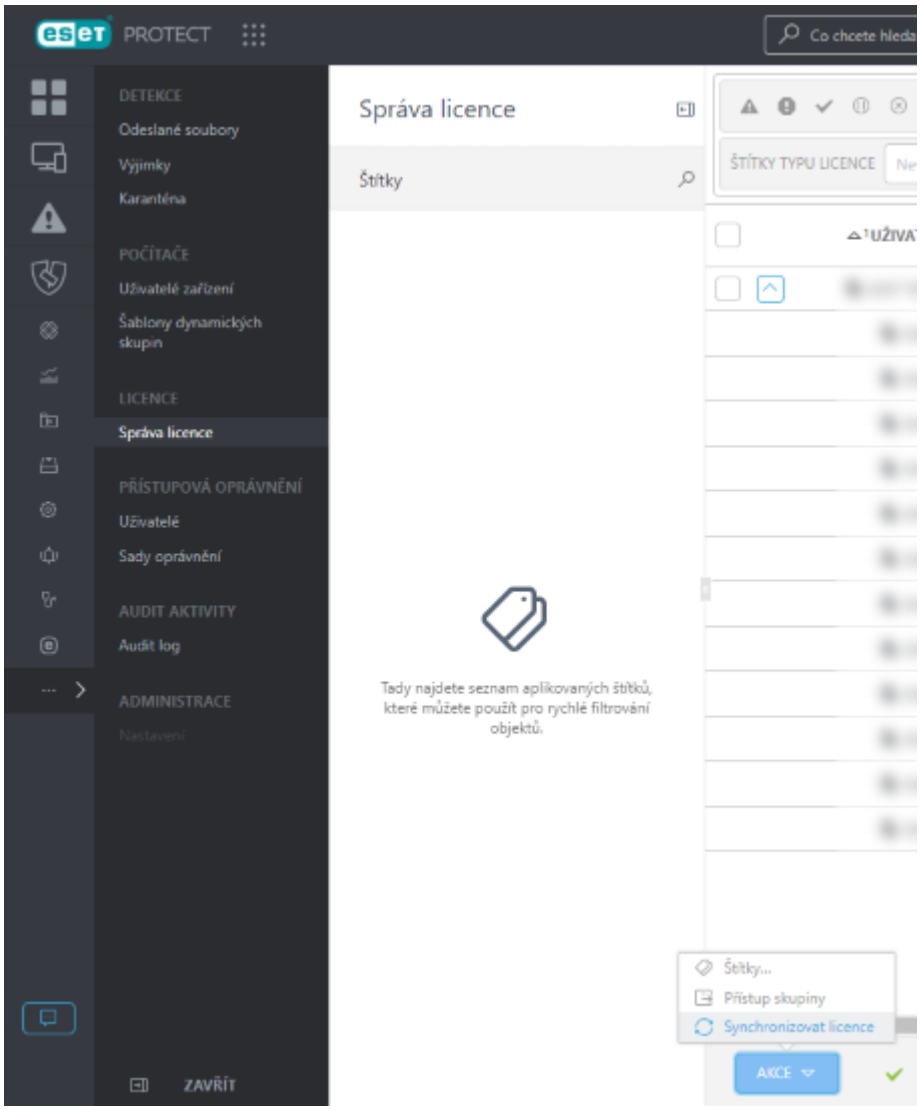
• V sekci Správa licence naleznete informace o názvu společnosti nebo lokality ve sloupci **Uživatel licence**. Uvedené jméno **uživatele licence** můžete využít při generování přehledů.

• Pokud máte licence na ESET Business Account a ESET MSP Administrator 2 portále pod stejným účtem, do ESET PROTECT se synchronizují všechny licence z obou účtů. Po importování se všechny ESET Business Account licence uloží do jednotlivých fondů licencí. Licence z ESET MSP Administrator 2 se rozdělí do fondů dle jednotlivých společností.



Ruční synchronizace

ESET PROTECT provádí synchronizaci s licenčními servery jednou denně. Pokud jste provedli změny ve svém MSP účtu a chcete změny replikovat do seznamu licencí a MSP stromu, přejděte do sekce **Správa licence**, klikněte na tlačítko **Akce** a vyberte možnost **Synchronizovat licence**.



Nastavení MSP zákazníka

Po vytvoření instance ESET PROTECT prostřednictvím MSP účtu dojde k synchronizaci MSP stromu a můžete zahájit konfiguraci společností. Průvodce konfigurací MSP zákazníka vytvoří:

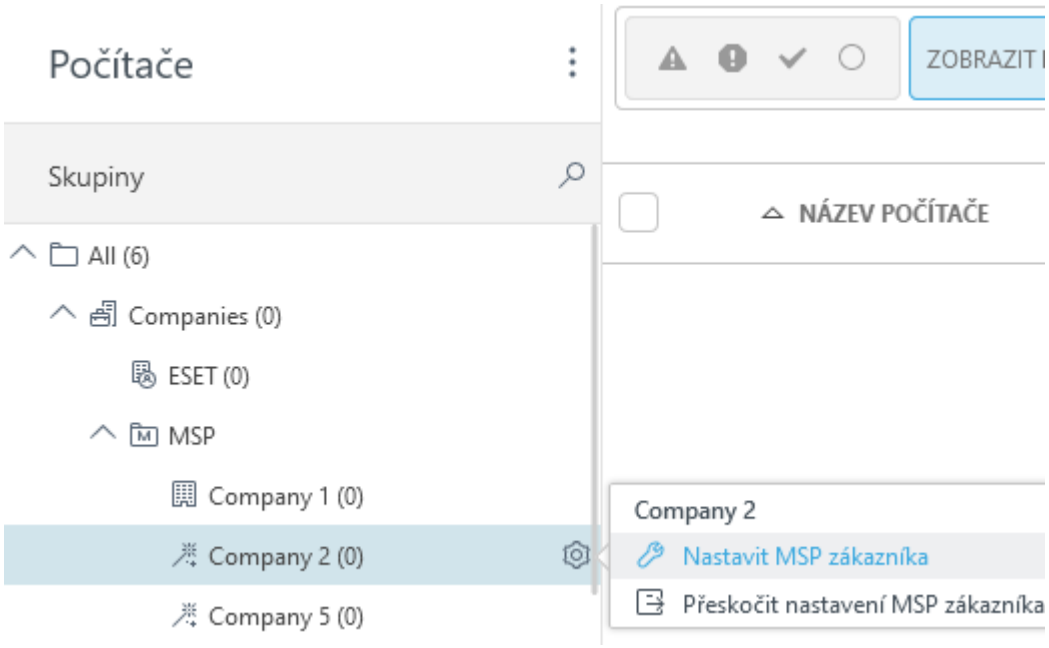
- Unikátní instalační balíček ESET Management Agenta nebo balíček obsahující agent i bezpečnostní produkt. Průvodce konfigurací MSP zákazníka nepodporuje vytvoření instalačních balíčků obsahujících ESET Full Disk Encryption nebo ESET Inspect Connector.

Konfiguraci MSP zákazníka můžete sice přeskočit, nicméně ji doporučujeme dokončit.

Konfigurovat můžete pouze společnosti, které mají alespoň 1 platnou licenci.

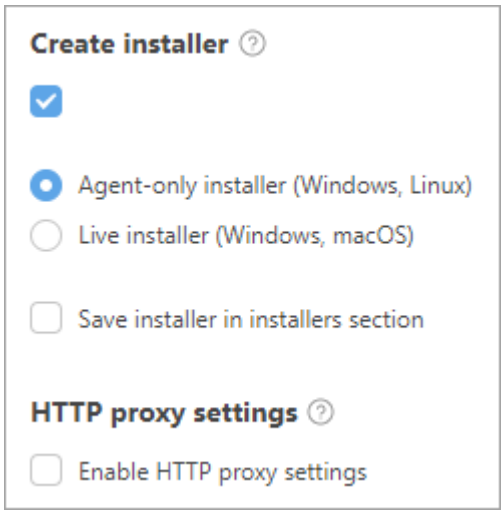
1. V hlavním menu Web Console na záložce **Počítače** klikněte na ozubené kolečko u společnosti, kterou chcete

konfigurovat, a vyberte možnost **Spustit konfiguraci MSP zákazníka**.



2. Pokud budete chtít tuto konfiguraci uložit jako výchozí, zaškrtněte možnost **Zapamatovat si nastavení**. Klikněte na tlačítko **Pokračovat**.

3. Pokud chcete v průběhu konfigurace vytvořit unikátní instalační balíček (doporučeno), zaškrtněte možnost **Vytvořit instalační balíček**.



4. Můžete si vybrat jeden z níže uvedených typů instalačních balíčků:

- **Instalátor samostatného agenta (Windows, Linux)**

- **All-in-one instalační balíček (Windows, macOS)** – instalační balíček bude obsahovat ESET Management Agenta a vámi vybraný firemní bezpečnostní produkt ESET.

All-in-one instalační balíček (Windows, macOS)

Produkt/Verze – po kliknutí vyberte bezpečnostní produkt ESET, který se nainstaluje společně s ESET Management Agentem. Standardně je vybrána nejnovější verze produktu. V případě potřeby si můžete vybrat starší verzi.
Z rozbalovacího menu si vyberte **Jazyk**.
Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

Pokud chcete balíček uložit do sekce Instalační balíčky pro jeho použití v budoucnu, vyberte možnost **Uložit mezi ostatní instalační balíčky**.

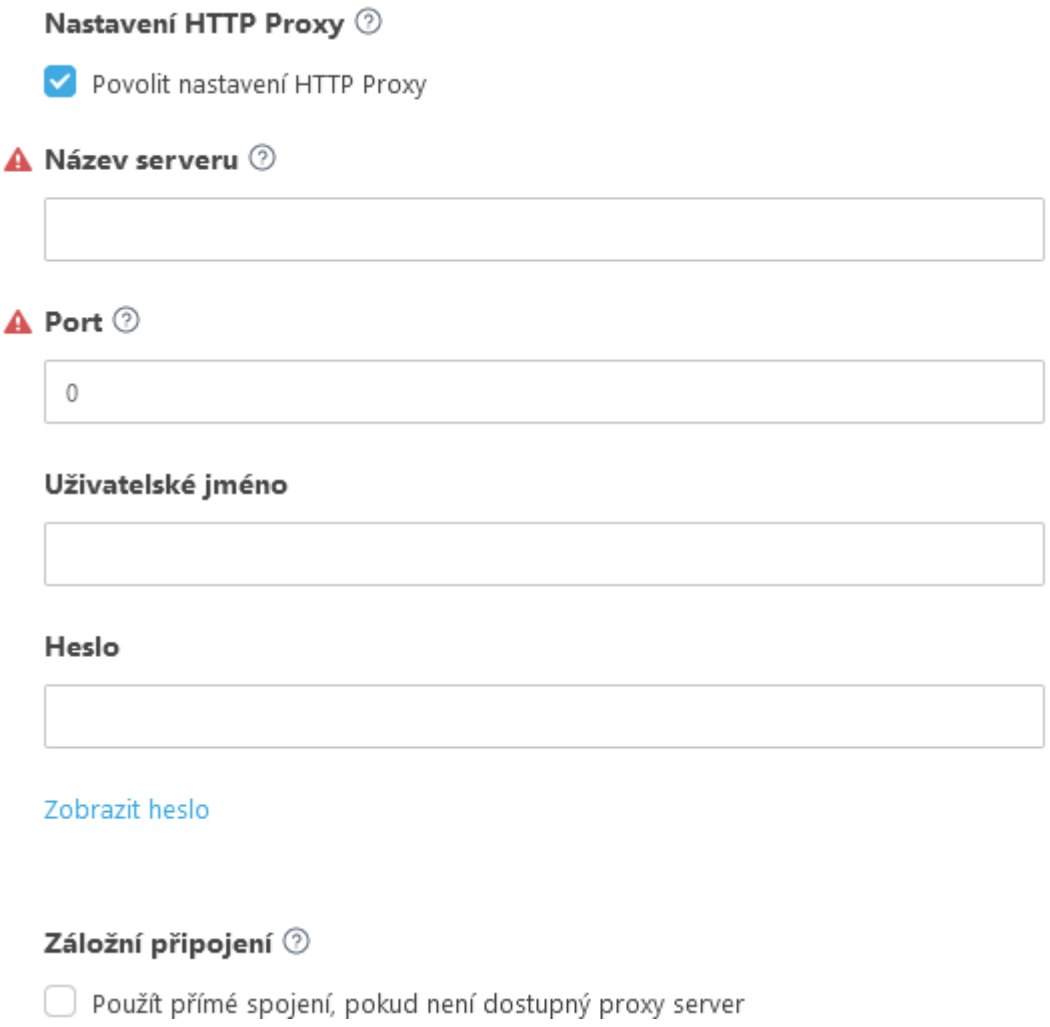
Povolit nastavení HTTP Proxy

Pokud používáte HTTP Proxy (doporučujeme používat ESET Bridge), zaškrtněte políčko **Povolit nastavení HTTP Proxy** a nastavte Proxy (**Název serveru**, **Port**, **Uživatelské jméno** a **Heslo**) pro stažení instalačního programu přes Proxy. Nastavte také připojení ESET Management Agenta k Proxy, aby bylo možné přesměrovávat komunikaci mezi ESET Management Agentem a ESET PROTECT Serverem. Do pole **Název serveru** zadejte adresu stroje, na kterém běží HTTP Proxy. ESET Bridge standardně běží na portu 3128. V případě potřeby port změňte. Ujistěte se, že jste zadali port, který odpovídá konfiguraci HTTP Proxy (viz Politika pro ESET Bridge.

> Komunikační protokol používaný agentem pro spojení s ESET PROTECT Serverem nepodporuje autentifikaci. Pokud proxy řešení vyžaduje autentifikaci, komunikace mezi agenty a ESET PROTECT Serverem nebude funkční.

Možnost **Použít přímé spojení, pokud není dostupný proxy server** je předvybraná. Průvodce si toto nastavení vynutí jako záložní cestu pro instalaci – zaškrtnutí políčka nelze zrušit. Toto nastavení můžete zakázat pomocí Politiky ESET Management agenta:

- Při vytváření instalačního programu zahrňte politiku pro **Počáteční konfiguraci**.
- Po instalaci agenta ESET Management přiřaďte počítači politiku.



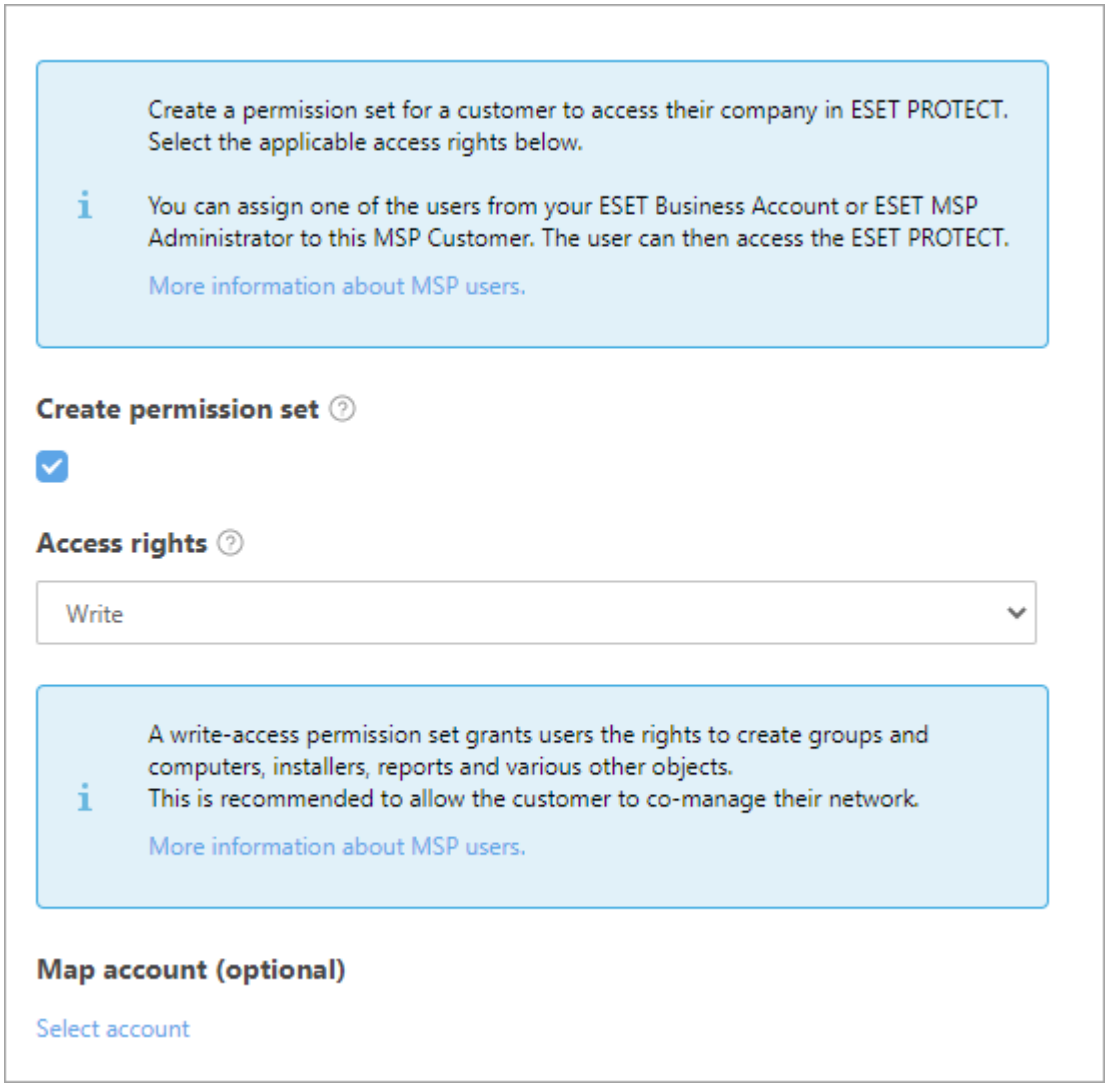
5. Kliknutím na tlačítko **Pokračovat** pro přechod do sekce **Uživatel**.

6.Můžete vybrat uživatele z EMA 2 a přidělit mu oprávnění pro správu ESET PROTECT.

a)Zaškrtněte pole u možnosti **Vytvořit sadu oprávnění**.

b)**Přístupová oprávnění** – tento uživatel bude schopen se přihlásit do Web Console a spravovat svá firemní zařízení. Jako úroveň přístupových oprávnění vyberte **Čtení** nebo **Zápis**.

c)**Namapovat účet (nepovinné)** – klikněte na možnost **Vyberte účet** a vyberte si jeden z dostupných.



Máte potíže při vytváření uživatelů? Ujistěte se, že máte potřebná oprávnění.

Pro vytvoření instalačních balíčků klikněte na tlačítko **Dokončit**. Balíčky si kdykoli můžete stáhnout ze sekce Instalační balíčky (za předpokladu, že jste vybrali možnost pro uložení instalačního balíčku). Live Installer Balíček můžete distribuovat několika způsoby:

- Kliknutím na ikonu si zkopírujte do schránky odkaz ke stažení balíčku, který zašlete uživatelům. Ti si následně balíček Live Installer stáhnou a nainstalují.

- Kliknutím na možnost **Stáhnout** si balíček Live Installer stáhněte na své zařízení a následně osobně spusťte na cílové stanici nebo nahrajte do sdílené složky, do níž mají uživatelé přístup.

- Pouze pro Windows: Pro vzdálené nasazení balíčku Live Installer použijte ESET Remote Deployment Tool.

- Kliknutím na ikonu ESET PROTECT použije SMTP server pro doručení e-mailu, ve kterém uživatelů naleznou odkaz na stažení balíčku Live Installer.

  - Pro přidání příjemce klikněte na **Přidat**, do pole **E-mailová adresa** zadejte adresu uživatele a potvrďte stisknutím klávesy **Enter** nebo klikněte na ikonu . Volitelně můžete kliknout na **Vytvořit uživatele**, následně zadejte **jméno** uživatele a klikněte na **Uložit**. Detaily uživatele můžete posléze změnit v sekci Uživatelé zařízení. Klikněte na **Zobrazit náhled e-mailu**, pomocí kontextového menu vyberte **Jazyk e-mailu** a klikněte na **Uložit**.

  - Uživatele můžete přidat hromadně následujícími způsoby: klikněte na **Další** > **Přidat uživatele** (tím můžete vybrat e-mailové adresy uživatelů definovaných v sekci Uživatelé zařízení) nebo na **Další** > **Importovat CSV** / **Vložit ze schránky** (kdy můžete seznam adres importovat z CSV souboru, případně vlastní datové struktury).

Vytvořený Live Installer balíček se bude chovat a měnit automaticky dle kroků uvedených v této tabulce.
Live Installer vyžaduje připojení k internetu a není možné jej použít na offline počítači.
Live Installer pro macOS vyžaduje přímé připojení k internetu (na servery společnosti ESET). Není možné jej použít na macOS stanicích, které jsou k internetu připojeny prostřednictvím proxy serveru.

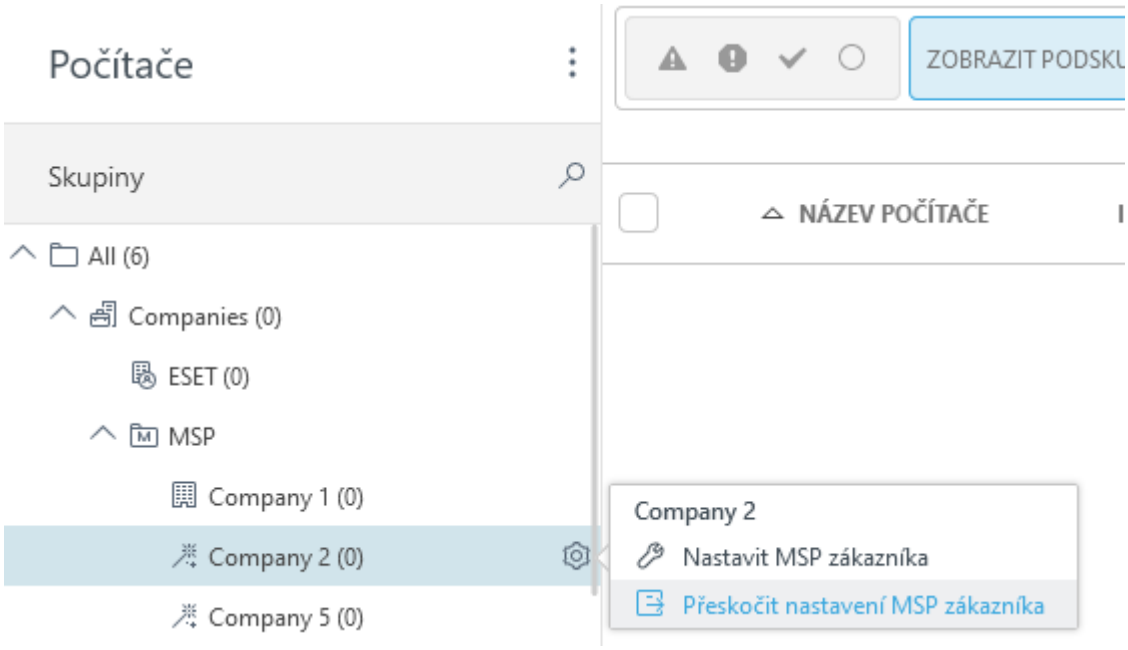
Dále si přečtěte informace pro lokální nebo vzdálené nasazení ESET Management Agenta.

Přeskočit nastavení MSP zákazníka

Konfiguraci můžete přeskočit kliknutím na **Přeskočit nastavení MSP zákazníka**. Případně můžete vytvořit instalační balíček později. Toto nastavení nedoporučujeme vynechávat.

Pokud nastavení přeskočíte, ikona společnosti se změní, stejně jako kdyby jsi nakonfigurovali.

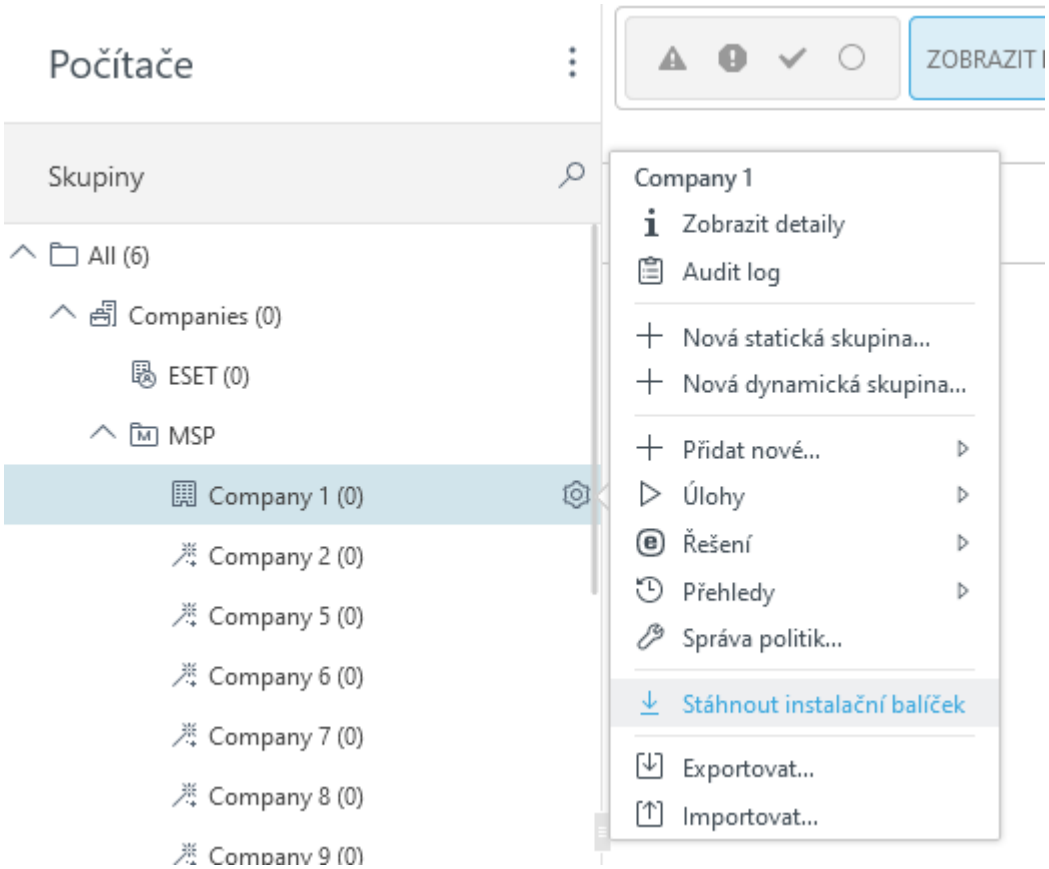
Pokud nastavení přeskočíte, na stejné ESET PROTECT instanci již nebudete schopni pro danou společnost znovu spustit průvodce nastavením.



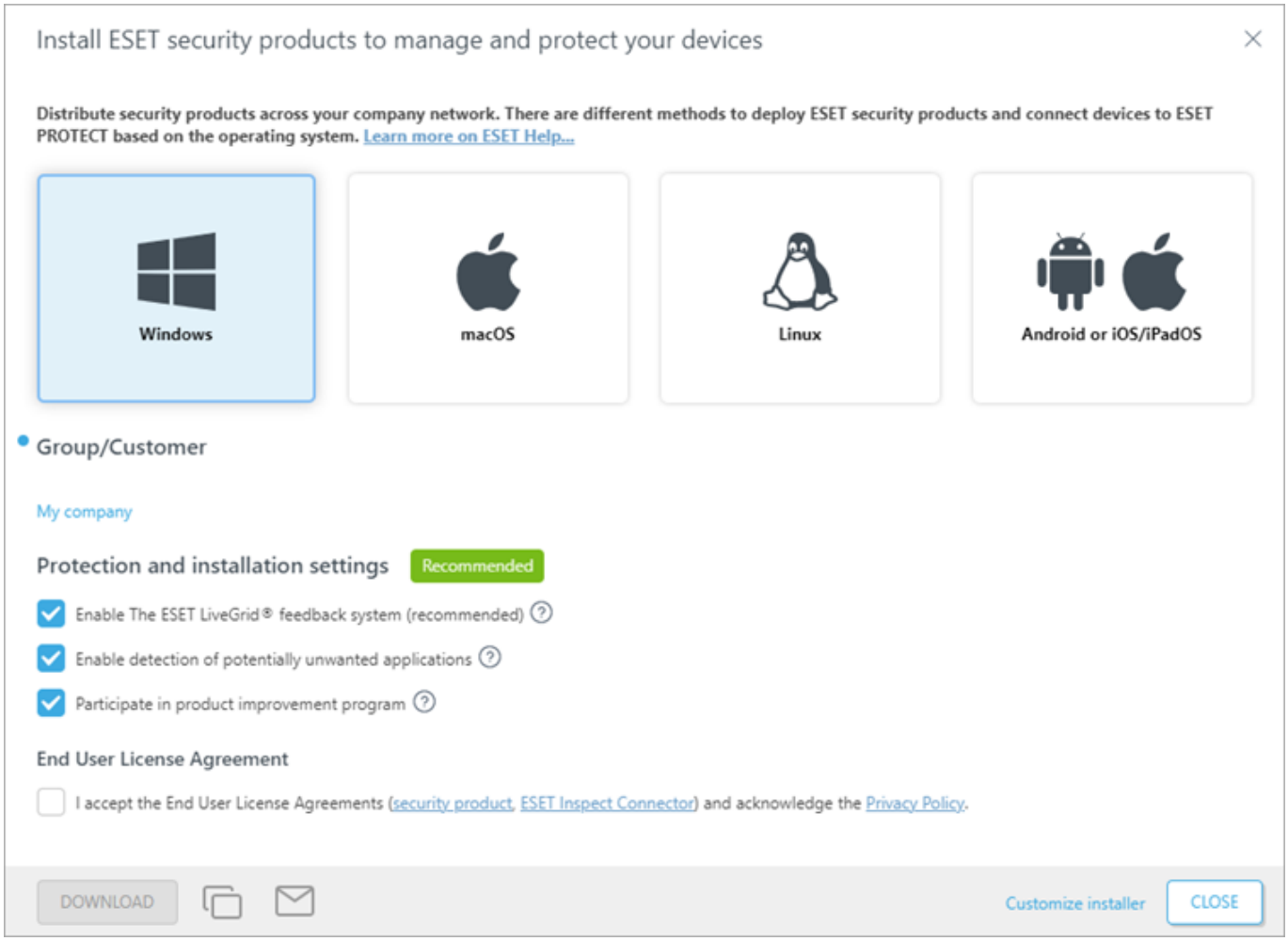
Vytvoření instalačního balíčku

1. Ve webové konzoli přejděte do sekce **Počítače**.

2. Klikněte na ikonu ozubeného kolečka u společnosti, pro kterou chcete vytvořit balíček, a vyberte možnost **Stáhnout instalační balíček**.



3. Vytvořte a přizpůsobte si instalační balíček, následně jej stáhněte.



MSP uživatelé

Během Nastavení MSP zákazníka můžete přidat existujícího uživatele z EMA2 nebo EBA do ESET PROTECT. Oprávnění vytvořeného uživatele si můžete zkontrolovat, případně kdykoli upravit v sekci **Další** > **Přístupová oprávnění** > **Uživatelé**.

Vyžadovaná oprávnění

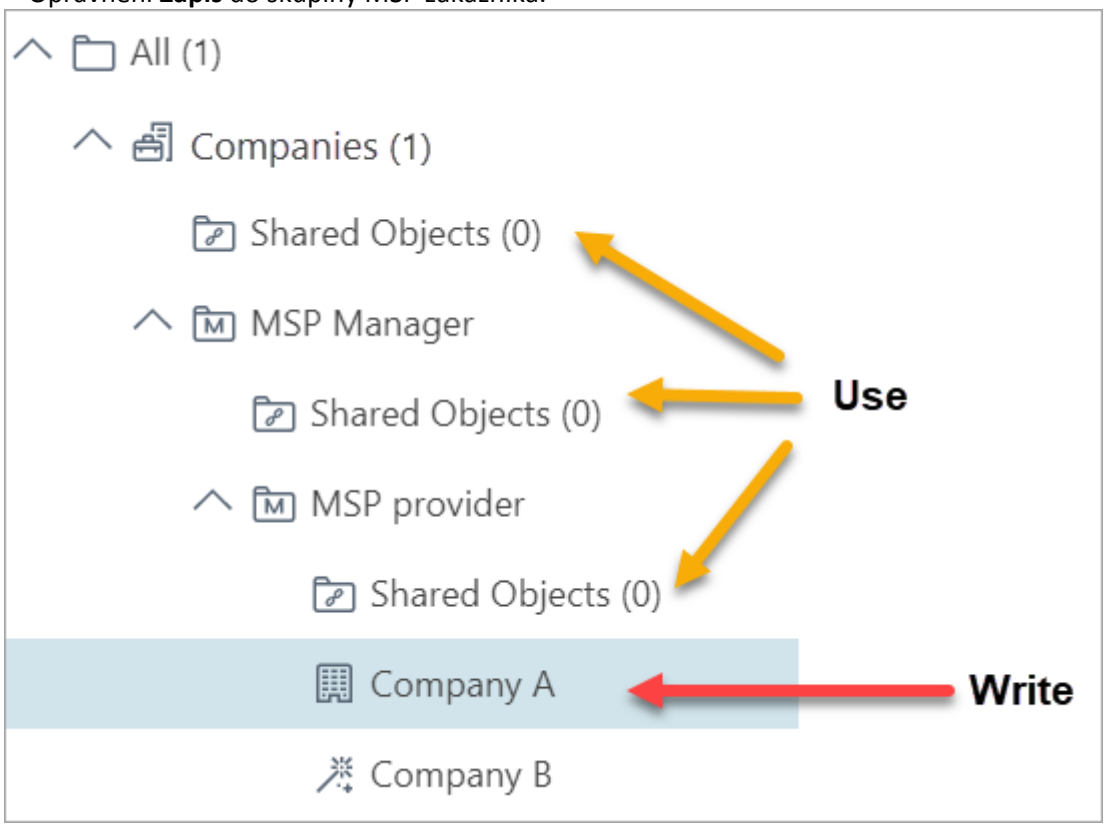
Pro vytvoření nového uživatele v průběhu nastavení MSP zákazníka potřebujete oprávnění ke společnosti, kterou konfigurujete, a ke skupině **Sdílené objekty**.

Detailní schéma oprávnění

Nastavení jedné společnosti

Přístupová oprávnění vyžadovaná pro vytvoření uživatele v průběhu konfigurace *Společnosti A*:

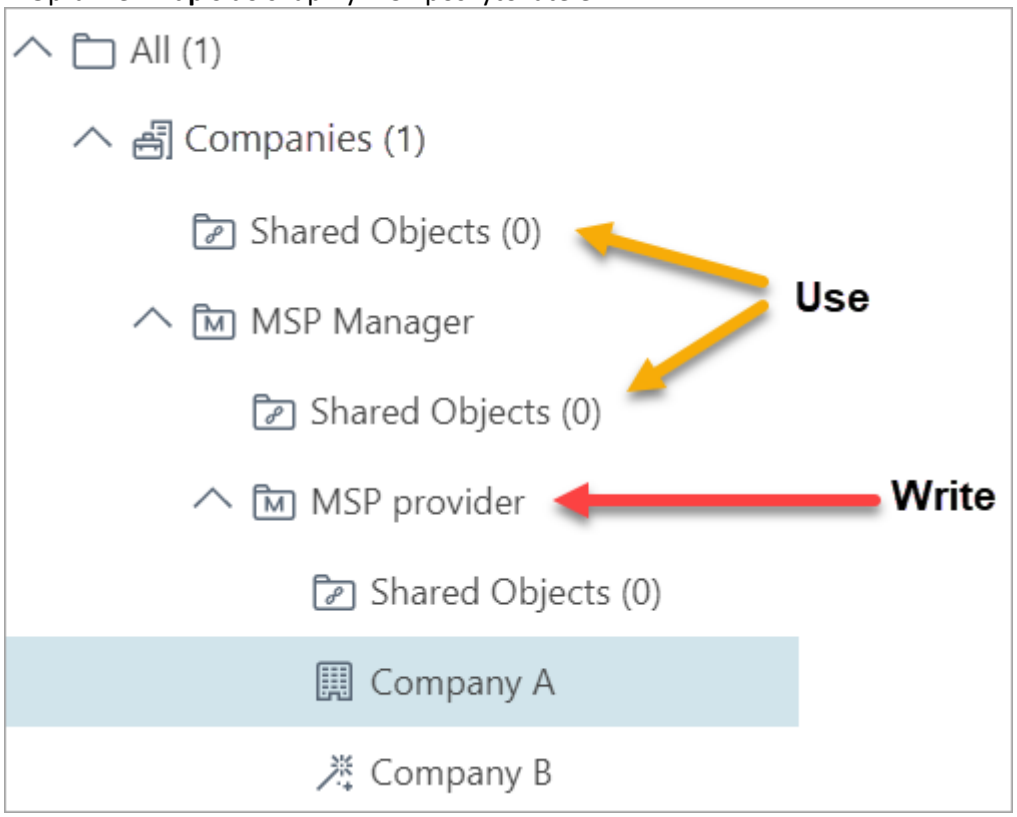
- Oprávnění **Použít** ke skupině **Sdílené objekty**.
- Oprávnění **Zápis** do skupiny MSP zákazníka.



Nastavení všech skupiny jedním MSP

Přístupová oprávnění vyžadovaná pro všechny uživatelů všem společnostem patřících *MSP poskytovateli*:

- Oprávnění **Použít** ke skupině **Sdílené objekty**.
- Oprávnění **Zápis** do skupiny MSP poskytovatele.



Mít přístupová oprávnění znamená, že uživatel právě provádějící akce má přiřazené sady oprávnění umožňujícími mu přístup k výše uvedeným skupinám. Pokud nebudete mít vyžadovaná přístupová oprávnění, průvodce nastavení MSP zákazníka skončí chybou.

Funkce MSP uživatele

- Může se přihlásit do ESET PROTECT Web Console, spravovat svá zařízení a objekty k nimž má přístup.

ESET PROTECT pro každého MSP uživatele eviduje následující nastavení:

- **Popis** – nativní uživatel vytvořený průvodcem konfigurací MSP zákazníka
- **Štítky** – každému uživateli je přiřazen štítek s názvem společnosti
- **Domovská skupina** – statická skupina dané společnosti
- **Automatické odhlášení** – 15 minut
- Účet je aktivní a není vyžadována změna hesla
- **Sady oprávnění** – každý MSP uživatel má přiřazeny 2 sady oprávnění. Jednu ke své domovské skupině a druhou pro přístup do skupiny **Sdílené objekty**.

Přiřazení štítků MSP objektům

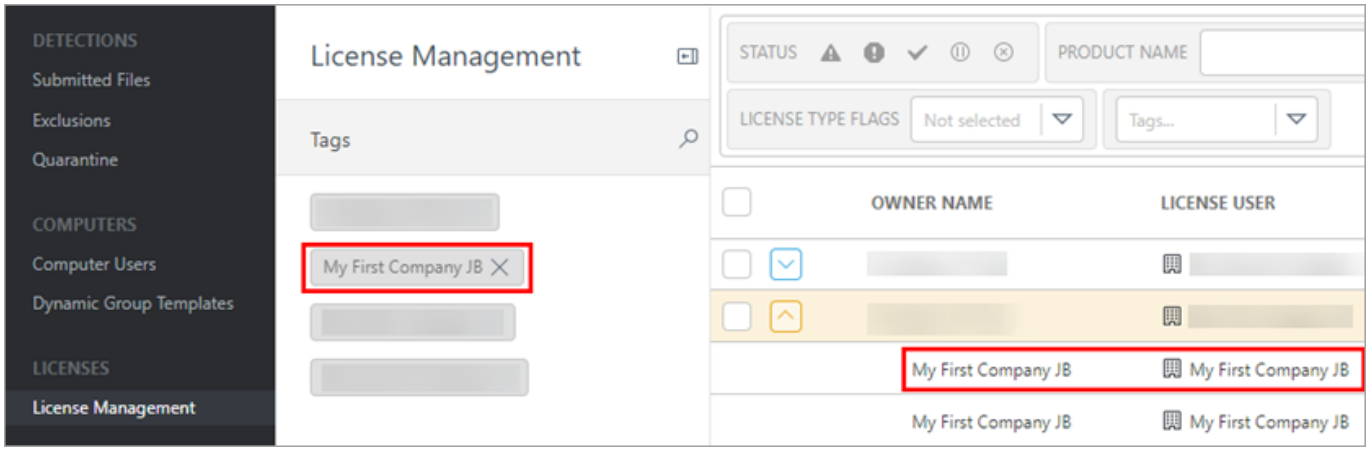
Pokud v ESET PROTECT použijete EMA 2 účet, aktivuje se automatické tagování MSP objektů. Níže uvedeným objektům se štítek přiřadí automaticky:

- Licencím importovaným prostřednictvím MSP účtu,
- Instalační balíčky
- Uživatelům a jejich sadám oprávnění vytvořeným prostřednictvím průvodce konfigurací MSP zákazníka.

Štítek si můžete představit jako nálepku, kterou využijete při filtrování objektů.

- Název automatického štítku odpovídá **Uživateli licence** (názvu společnosti v EMA 2. Neobsahuje pouze znaky , ", které ESET PROTECT ze štítku odstraní).
- Pokud po provedení synchronizace zákazníka na EMA 2 portále přejmenujete, štítek tuto změnu nebude reflektovat.
- Kdykoli si můžete vytvořit vlastní štítky a přiřadit je libovolným objektům.
- Štítky můžete kdykoli odebrat.

Kliknutím na ikonu si zobrazíte panel **Štítky**.



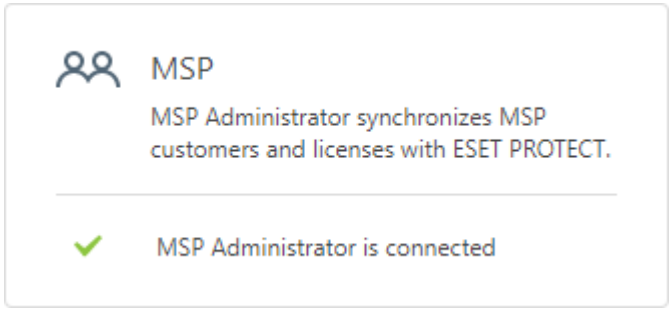
Stav MSP

Komplexní informace o stavu ESET PROTECT naleznete v sekci Stav serveru. Pokud si vytvoříte instanci ESET PROTECT pomocí účtu EMA 2 nebo smíšeného účtu (EMA 2 a EBA), je k dispozici MSP dlaždice s informacemi týkajícími se MSP.

Stavy MSP

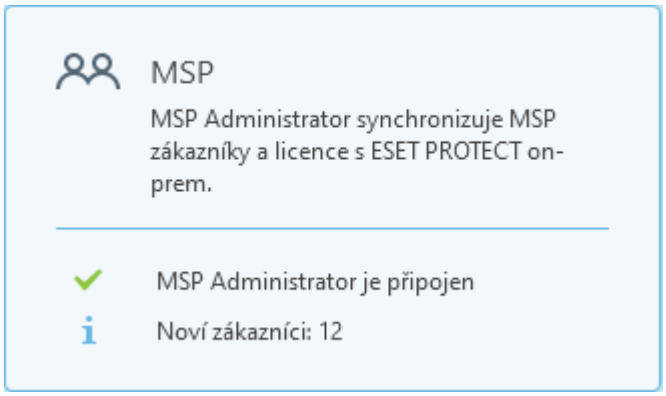
Účet je synchronizován

Váš účet je synchronizován a není vyžadována žádná akce.



Probíhá synchronizace

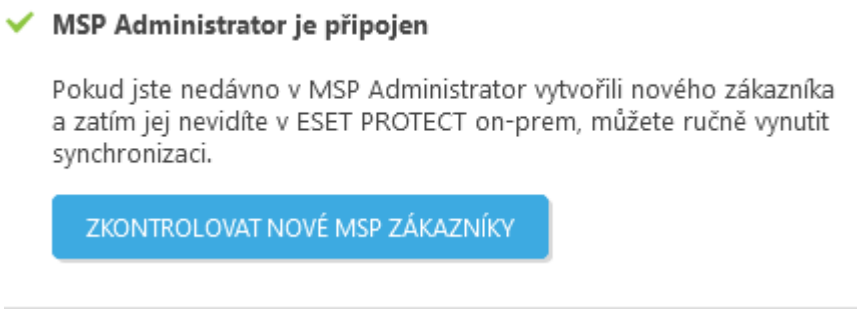
Na pozadí probíhá synchronizace s MSP účtem. V případě velkých účtů může tato akce trvat několik hodin. Po dokončení synchronizace se dlaždice podbarví bíle.



Dostupné akce

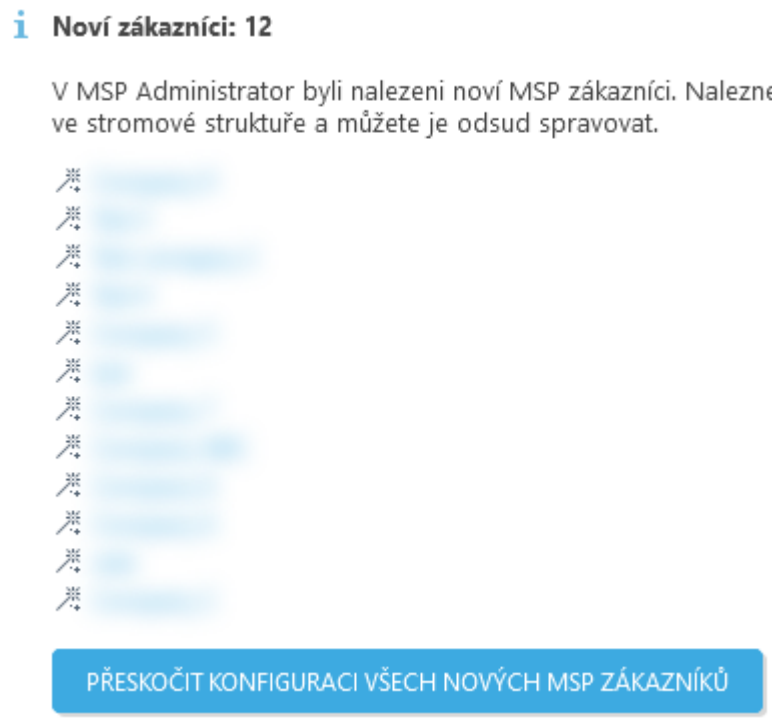
Pro více informací klikněte na MSP dlaždici.

- **Zkontrolovat nové MSP zákazníky** – kliknutím vynutíte synchronizaci licencí (aktualizaci MSP stromu).



- **Noví klienti** – pokud jste zatím nenastavili všechny společnosti, klikněte na jejich název a dále postupujte dle kroků v průvodci konfigurací zákazníka.

- **Přeskočit konfiguraci všech nových MSP zákazníků** – tuto možnost vyberte, pokud chcete přeskočit průvodce konfigurací pro všechny dosud nenastavené zákazníky.



Cloudová správa mobilních zařízení

ESET Cloud Mobile Device Management (Cloud MDM) je rozšíření do ESET PROTECT. Prostřednictvím ESET Mobile Device Management můžete vzdáleně spravovat mobilní Android a iOS zařízení, a zajistit tak jejich bezpečnost.

ESET Cloud MDM představuje agent-less řešení, kdy agenti neběží přímo na mobilních zařízeních (z důvodu prodloužení výdrže baterie a minimalizace dopadu na výkon zařízení). Agenti pro spravovaná mobilní zařízení jsou

virtualizováni v ESET cloudu.

Zabezpečení a správa používaných certifikátů jsou plně v režii společnosti ESET. Administrátorům tak odpadají starosti související s obnovením certifikátu, případně ověření, a nemusí se zabývat tím, zda vyhovují posledním bezpečnostním standardům.

Ujistěte se, že na svých mobilních zařízeních používáte podporovou verzi systému, a vaše síť splňuje požadavky.

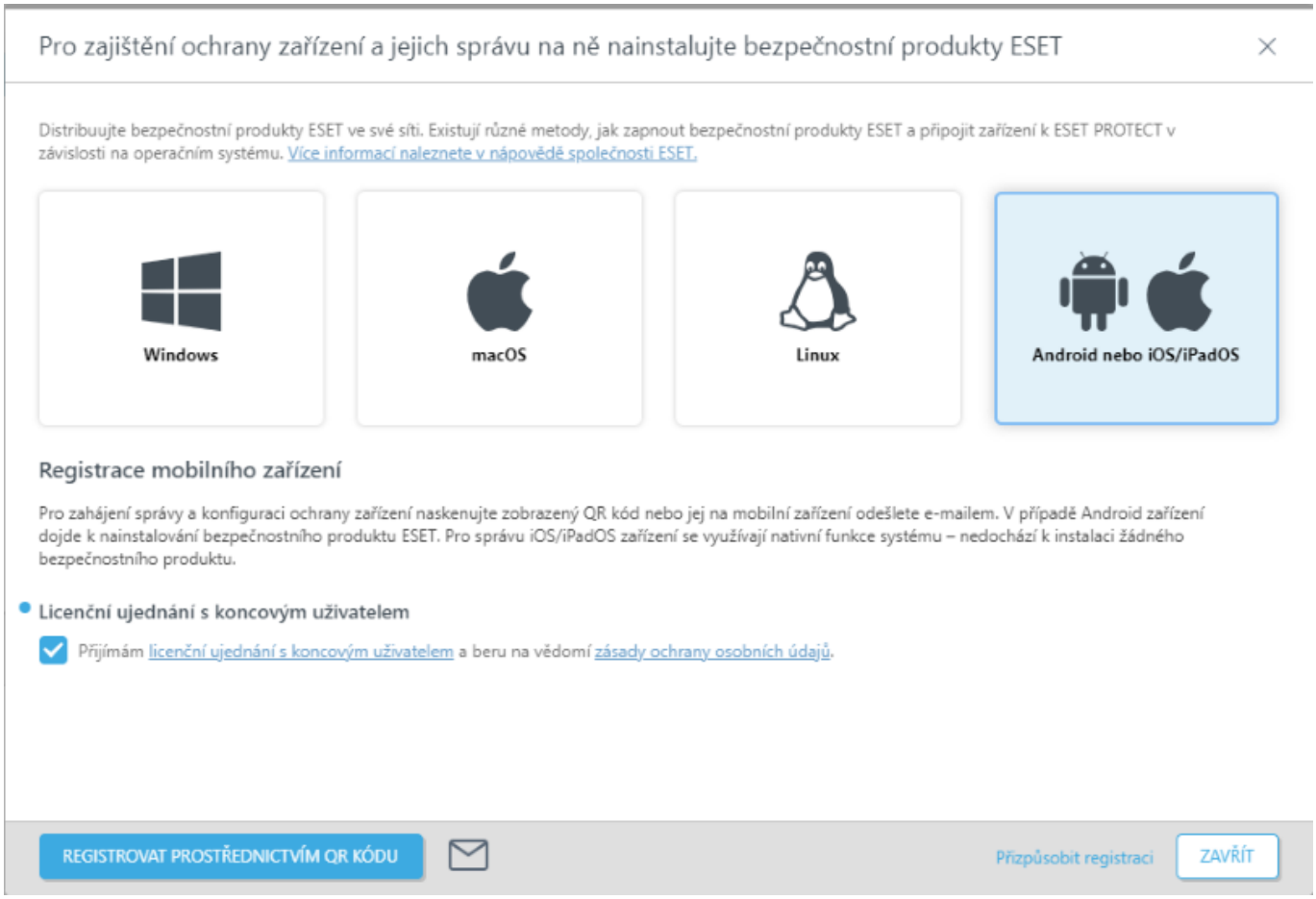
> Zaregistrovaná mobilní zařízení se musí k ESET PROTECT připojit jednou za 120 dní, aby se předešlo problémům s připojením. Tyto informace jsou uvedeny v registračním e-mailu nebo v QR kódu. Náhradní zařízení předem neregistrujte. Doporučujeme zaregistrovat pouze ta náhradní zařízení, která se budou používat v průběhu následujících 120 dní.

Proces správy mobilních zařízení:

- Registrace mobilních zařízení – v závislosti na tom, jaký typ mobilních zařízení plánujete spravovat a v jakém režimu, před zahájením správy mobilních zařízení proveďte několik kroků. Cloud MDM podporuje tyto typy registrace mobilních zařízení:
  - Registrace zařízení s OS Android
  - Registrace zařízení s OS Android v režimu Vlastník zařízení
  - Registrace Microsoft Entra ID (Android nebo iOS)
  - Synchronizace s Microsoft Intune (Android)
  - Synchronizace s VMware Workspace ONE (Android)
  - Registrace iOS zařízení
  - Synchronizace (iOS) s Apple Business Manager (ABM)
- Správa mobilních zařízení – po registraci mobilních zařízení se systémem Android je můžete začít spravovat.

Registrace – přidání mobilních zařízení

Pro správu mobilních zařízení proveďte jeho registraci v cloudové konzoli pro vzdálenou správu: v hlavním menu na záložce **Počítače** klikněte na tlačítko **Přidat zařízení** a vyberte možnost **Android nebo iOS/iPadOS**.



Licenční ujednání s koncovým uživatelem – zaškrtněte pole, čím přijmete ujednání (EULA) a Zásady ochrany osobních údajů.

a)Pro vygenerování QR kódu klikněte na **Registrovat prostřednictvím QR kódu**:

1.V zobrazeném dialogovém okně zadejte **název zařízení** nového mobilního zařízení, které chcete zaregistrovat, a klikněte na **Vygenerovat QR kód**.

2.Pro zaregistrování mobilního zařízení naskenujte QR kód.

3.Po úspěšném zaregistrování požadovaného mobilního zařízení klikněte na **Registrovat další**. Tím zajistíte vygenerování nového QR kódu pro registraci dalšího zařízení. Po dokončení registrace průvodce ukončete kliknutím na tlačítko **Zavřít**.

b)Kliknutím na ikonu si zobrazíte průvodce pro **Registraci mobilních zařízení prostřednictvím e-mailu**:

V této části zadejte informace o zařízeních, které chcete registrovat. K dispozici máte následující funkce:

- **Přidat** – kliknutím přidáte další řádek do tabulky, ve kterém zadejte název zařízení a s ním spojenou e-mailovou adresu. (v případě registrace prostřednictvím e-mailu se na ní zašle e-mail s registračním odkazem). Pokud kliknete na tlačítko **Párovat s existujícím uživatelem** a vyberete uživatele, automaticky se doplní/přepíše zadaná e-mailová adresa údajem definovaným v sekci **Další** > Uživatelé zařízení. Pro přidání dalšího klikněte na tlačítko **Přidat** a vyplňte požadované informace.

- **Další**:

  o**Přidat uživatele** – po kliknutí vyberte uživatele ze seznamu definovaného v sekci **Další** > Uživatelé

zařízení.

- **Importovat CSV** – pomocí této možnosti můžete pohodlně přidat velké množství zařízení. Stačí nahrát *.csv* obsahující seznam zařízení. Více informací naleznete v kapitole Importování CSV.

- **Vložit ze schránky** – po kliknutí můžete seznam adres oddělený vlastním oddělovačem zkopírovat ze schránky (tato funkce funguje podobně jako Import CSV).

> Abyste byli schopni rozpoznat jednotlivá zařízení, doporučujeme definovat **název zařízení** i v případě, kdy budete seznam **importovat hromadně z CSV** souboru. Pod tímto **názvem** uvidíte přidané mobilní zařízení v sekci **Počítače**. Pokud ponecháte pole **Název zařízení** prázdné, jako **název zařízení** se použije e-mailová adresa – tak zařízení následně uvidíte v sekci **Počítače** i **Skupiny**. Při registraci více zařízení se vyhněte použití stejné e-mailové adresy. V opačném případě budou mít zařízení stejný název, a nebudete je schopni od sebe odlišit.

Pro zobrazení náhledu e-mailu a úpravu **předmětu** a **obsahu** zprávy klikněte na tlačítko **Přizpůsobit e-mail**.

c)Kliknutím na **Přizpůsobit registraci** si zobrazíte pokročilé možnosti registrace (viz níže).

Obecné

Vyberte typ registrace:

- **Android nebo iOS/iPadOS** – standardní proces registrace Android nebo iOS/iPadOS zařízení.

- **Vlastník zařízení se systémem Android** - má plnou kontrolu nad spravovaným zařízením se systémem Android.

- **Android zařízení s omezenými možnosti vstupu** – jedná se alternativní proces registrace určený pro Android zařízení bez fotoaparátu (nelze naskenovat QR kódu) nebo poštovním službám (nelze otevřít registrační odkaz).

> Způsoby synchronizace:
> - Zařízení se systémem Android a iOS spravovaná v Microsoft Entra ID
> - Mám Android zařízení spravované prostřednictvím Microsoft Intune
> - Mám iOS zařízení spravované prostřednictvím ABM
> - Android zařízení spravovaná prostřednictvím VMware Workspace ONE

Distribuce

V sekci **Distribuce** se rozhodněte, jakým způsobem chcete doručit registrační odkaz. Způsob si vyberte v závislosti na množství a fyzické dostupnosti mobilních zařízení.

- **Odeslat e-mailem** – pomocí této možnosti odešlete hromadně registrační odkaz na libovolné množství zařízení. Jedná se o nejefektivnější řešení pro registraci velkého množství zařízení, případně pokud nemáte k mobilnímu zařízením fyzický přístup. Tato možnost vyžaduje interakci ze strany uživatele.

- **Naskenujte QR kód** – pomocí této možnosti zaregistrujete jedno konkrétní zařízení. U dalších zařízení proveďte stejné kroky. Tuto možnost doporučujeme pouze v případě, že pro registraci máte menší počet mobilních zařízení. Tento způsob je vhodný pro případ, kdy uživatele mobilních zařízení nechcete ničím zatěžovat a registraci provedete svépomocí (máte fyzický přístup k mobilnímu zařízení). Tuto možnost můžete využít také v případě, kdy máte nové mobilní zařízení, které po nakonfigurování předáte uživateli.

• **Vložit bezpečnostní kód** – registrace jednoho mobilního zařízení s Androidem, které nemá kameru ani e-mailového klienta.

Nadřazená skupina – vyberte skupinu pod kterou bude zařízení po registraci patřit.

Přizpůsobit další nastavení

Licence – vyberte vhodnou licenci, kterou chcete použít pro aktivaci bezpečnostního produktu na mobilním zařízení.

Štítky – pro snadnější identifikaci mobilního zařízení vyberte z již existujících nebo si vytvořte štítek nový.

Nastavení produktu

Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

U Vlastníka zařízení Android nakonfigurujte další nastavení:

• Zaškrtnutím políčka **Ponechat v mobilních zařízeních nainstalované systémové aplikace** zachováte předinstalované aplikace.

• Po zaškrtnutí políčka **Konfigurovat síť Wi-Fi** proveďte potřebnou konfiguraci. Zadejte **SSID** (název) a vyberte **Typ zabezpečení** – **Žádné**, **WPA** nebo **WEP**. Pokud jste vybrali WPA nebo WEP, zadejte **Heslo**.

QR kód nesdílejte ani neukládejte – obsahuje heslo k Wi-Fi.

Seznam

V této části zadejte informace o zařízeních, které chcete registrovat. K dispozici máte následující funkce:

• **Přidat** – kliknutím přidáte další řádek do tabulky, ve kterém zadejte název zařízení a s ním spojenou e-mailovou adresu. (v případě registrace prostřednictvím e-mailu se na ní zašle e-mail s registračním odkazem). Pokud kliknete na tlačítko **Párovat s existujícím uživatelem** a vyberete uživatele, automaticky se doplní/přepíše zadaná e-mailová adresa údajem definovaným v sekci **Další** > Uživatelé zařízení. Pro přidání dalšího klikněte na tlačítko **Přidat** a vyplňte požadované informace.

• **Další**:

o**Přidat uživatele** – po kliknutí vyberte uživatele ze seznamu definovaného v sekci **Další** > Uživatelé zařízení.

o**Importovat CSV** – pomocí této možnosti můžete pohodlně přidat velké množství zařízení. Stačí nahrát *.csv* obsahující seznam zařízení. Více informací naleznete v kapitole Importování CSV.

o**Vložit ze schránky** – po kliknutí můžete seznam adres oddělený vlastním oddělovačem zkopírovat ze schránky (tato funkce funguje podobně jako Import CSV).

Abyste byli schopni rozpoznat jednotlivá zařízení, doporučujeme definovat **název zařízení** i v případě, kdy budete seznam **importovat hromadně z CSV** souboru. Pod tímto **názvem** uvidíte přidané mobilní zařízení v sekci **Počítače**. Pokud ponecháte pole **Název zařízení** prázdné, jako **název zařízení** se použije e-mailová adresa – tak zařízení následně uvidíte v sekci **Počítače** i **Skupiny**. Při registraci více zařízení se vyhněte použití stejné e-mailové adresy. V opačném případě budou mít zařízení stejný název, a nebudete je schopni od sebe odlišit.

Pro zobrazení náhledu e-mailu a úpravu **předmětu** a **obsahu** zprávy klikněte na tlačítko **Přizpůsobit e-mail**.

Registrace

V této části můžete zkontrolovat parametry všech registrovaných zařízení.

Odkaz na registraci v e-mailu nebo QR kódu platí 14 dní.

- **Odeslat e-mail** – kliknutím si zobrazíte seznam zařízení a e-mailových adres. Kliknutím na tlačítko **Náhled e-mailu** si můžete zobrazit šablonu zprávy, která bude zaslána na každou e-mailovou adresu uvedenou v seznamu. Klikněte na tlačítko **Odeslat** zašlete zprávu na definované e-mailové adresy. Pokud v okně pro potvrzení kliknete na **Zobrazit více**, zobrazí se seznam e-mailových adres, na které registrační e-mail odesíláte. Kliknutím na tlačítko **Exportovat** vyexportujete seznam zařízení a e-mailů ve formátu CSV.

- **Naskenujte QR kód** – zobrazíte si seznam zařízení určených k registraci. V pravé části obrazovky se zobrazí unikátní QR kód pro jednotlivá zařízení.

- **Vložit bezpečnostní kód** – do tohoto pole zadejte vygenerovaný bezpečnostní kód na mobilním zařízení, které chcete zaregistrovat.

Zaregistrovaná mobilní zařízení se musí k ESET PROTECT připojit jednou za 120 dní, aby se předešlo problémům s připojením. Tyto informace jsou uvedeny v registračním e-mailu nebo v QR kódu. Náhradní zařízení předem neregistrujte. Doporučujeme zaregistrovat pouze ta náhradní zařízení, která se budou používat v průběhu následujících 120 dní.

Registraci mobilního zařízení dokončíte podle následujících kroků:

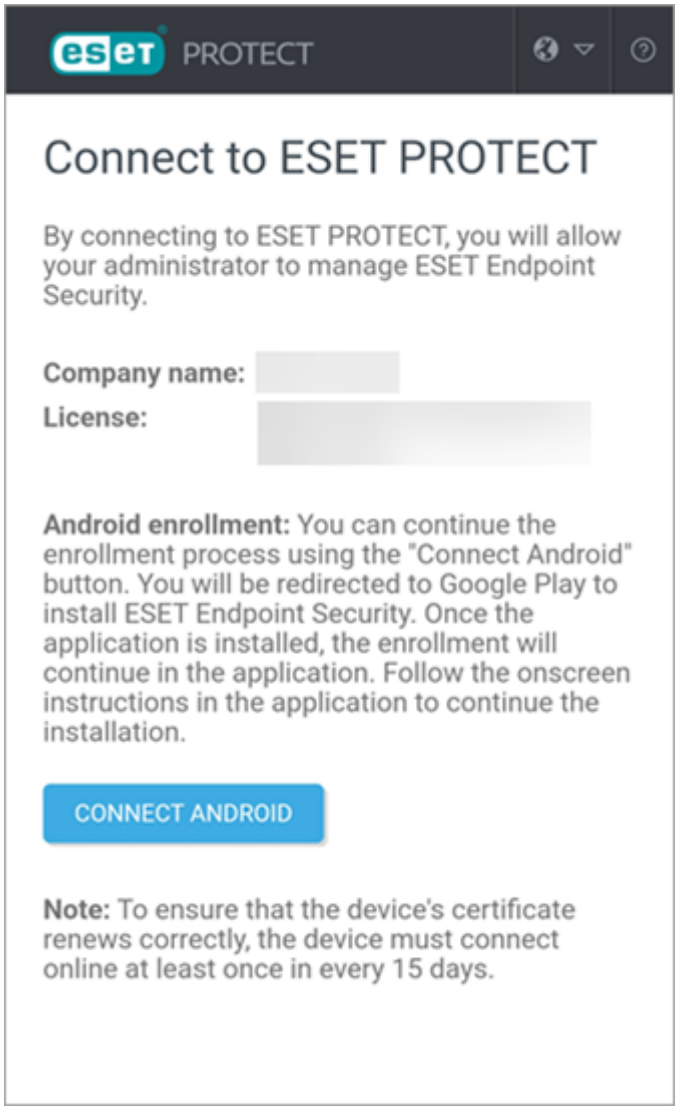
- Registrace zařízení s OS Android
- Registrace zařízení s OS Android – vlastník zařízení
- Registrace zařízení s iOS

Registrace zařízení s OS Android

Podle níže uvedených kroků zaregistrujte zařízení s OS Android v ESET PROTECT:

Zaregistrovaná mobilní zařízení se musí k ESET PROTECT připojit jednou za 120 dní, aby se předešlo problémům s připojením. Tyto informace jsou uvedeny v registračním e-mailu nebo v QR kódu. Náhradní zařízení předem neregistrujte. Doporučujeme zaregistrovat pouze ta náhradní zařízení, která se budou používat v průběhu následujících 120 dní.

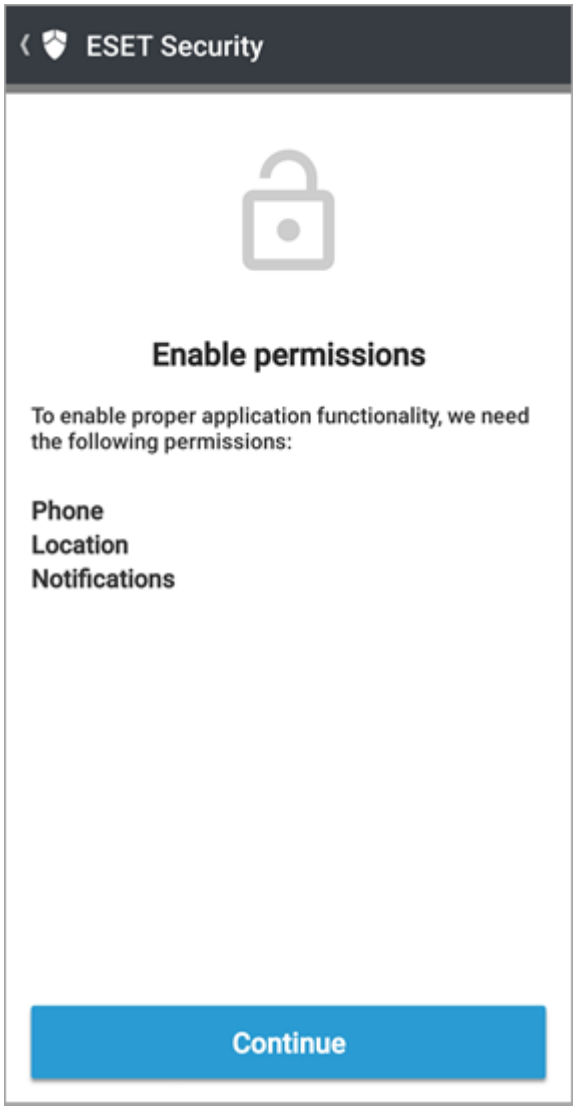
1. Otevřete odkaz pro registraci z e-mailu nebo kódu QR a ťukněte na **Připojit Android**.



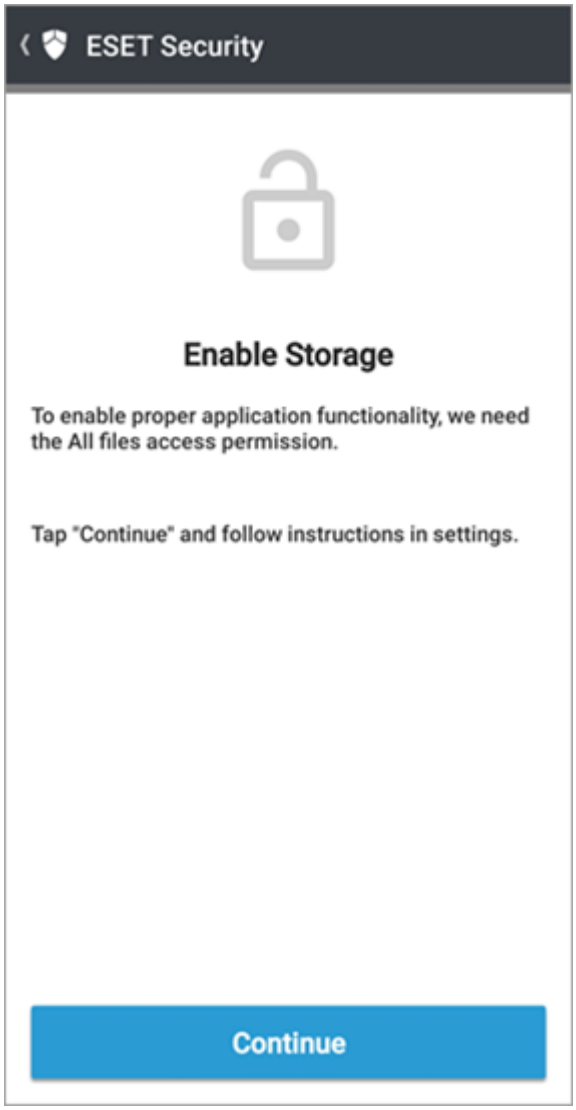
Pokud nemáte ESET Endpoint Security pro Android nainstalován na vašem mobilním zařízení, budete automaticky přesměrováni do obchodu Google Play, kde si můžete aplikaci stáhnout.

Pokud se zobrazí oznámení **No app found to open URL**, zkuste otevřít odkaz pro registraci ve výchozím webovém prohlížeči pro Android.

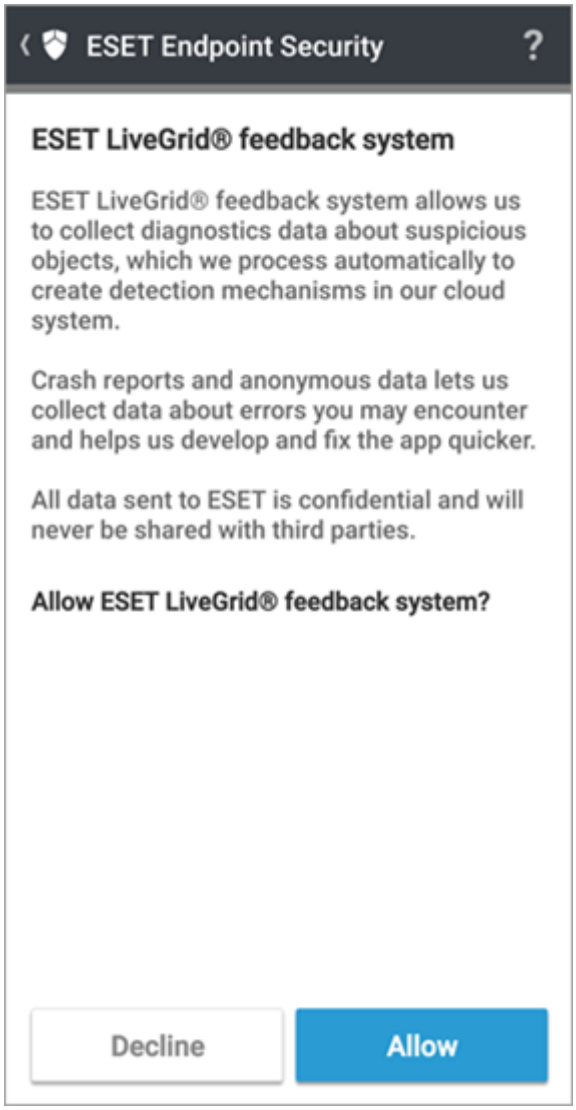
2. Ťuknutím na **Pokračovat** povolte požadovaná oprávnění pro **Telefon**, **Polohu** a **Oznámení**:



3. Ťuknutím na **Pokračovat** povolíte oprávnění pro přístup ke všem souborům.

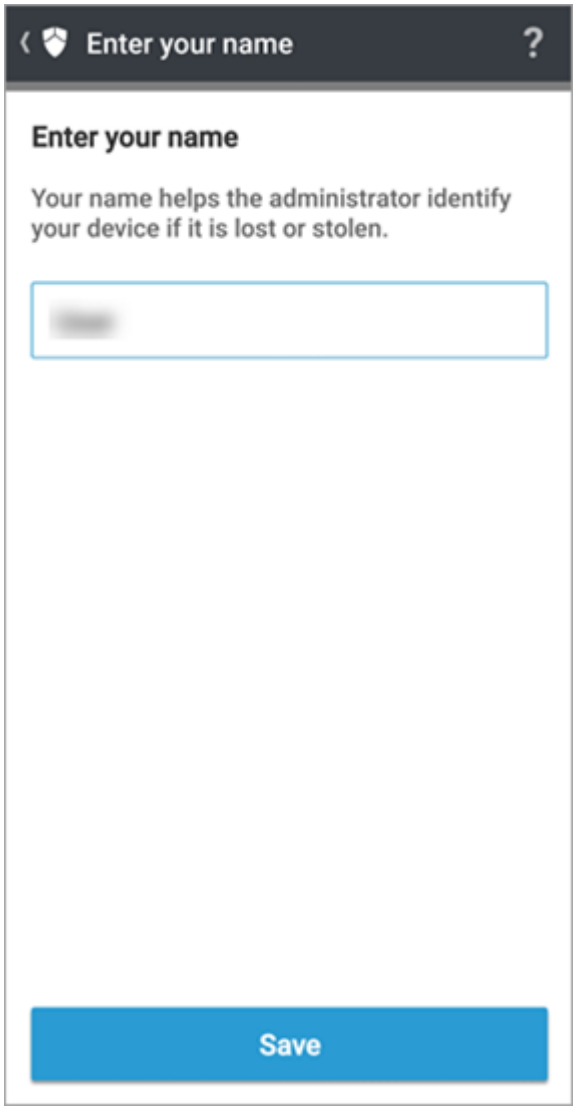


4. Ťuknutím na **Povolit** nebo **Zamítnout** zapnete nebo vypnete ESET LiveGrid®.

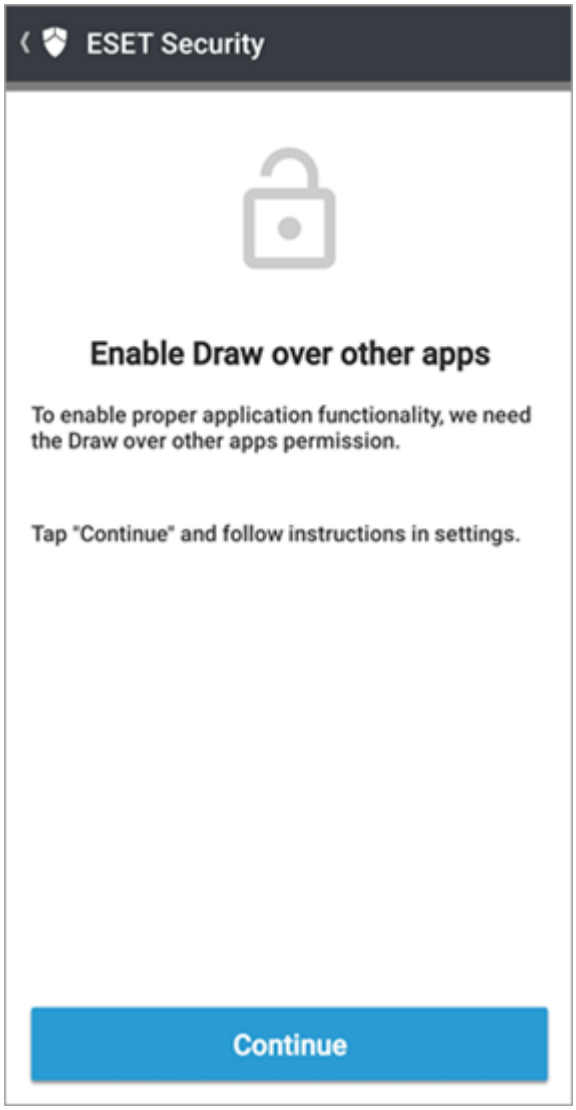


5. Zadejte své jméno a ťukněte na **Uložit**.

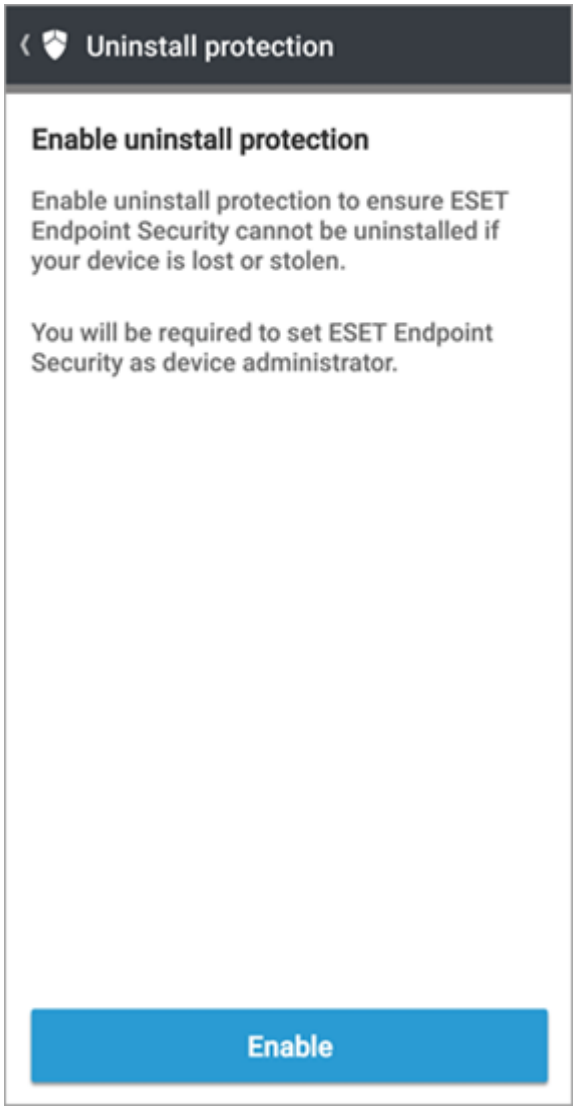
Jméno není viditelné na ESET PROTECT a používá se pro funkci Anti-Theft a pro diagnostické protokoly.



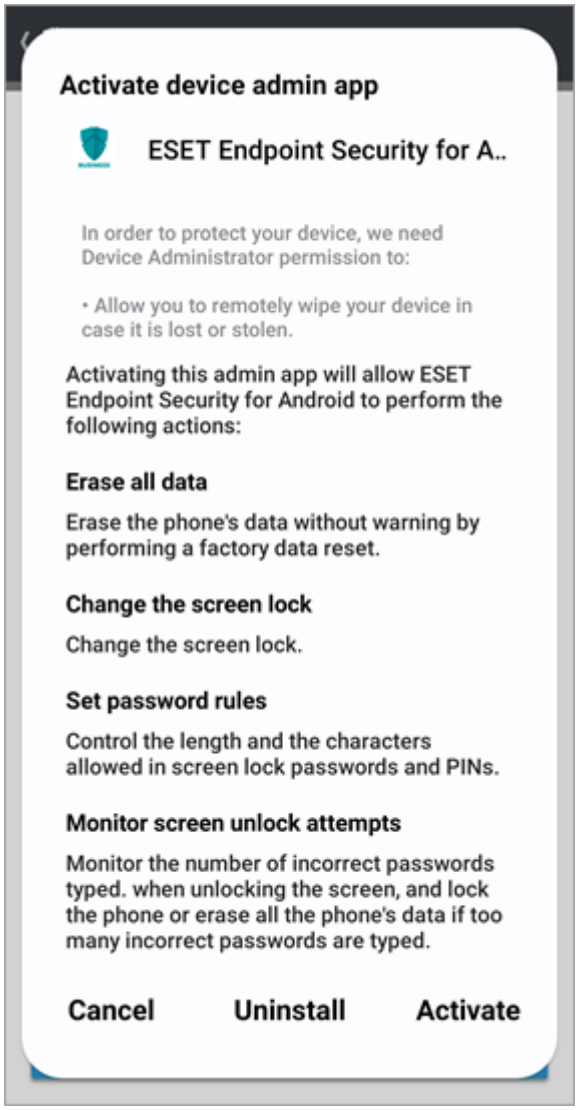
6. Ťuknutím na **Pokračovat** povolte vykreslení přes další aplikace.



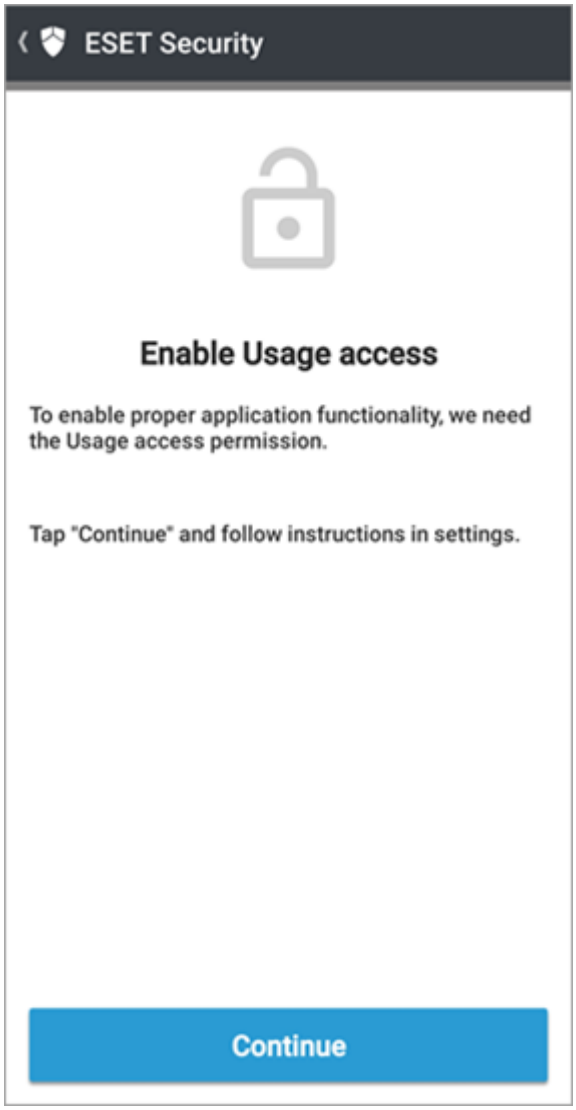
7. Ťuknutím na **Povolit** povolíte ochranu před odinstalováním, aby na ESET Endpoint Security pro Android nemohlo dojít k odinstalování v případě ztráty nebo krádeže zařízení.



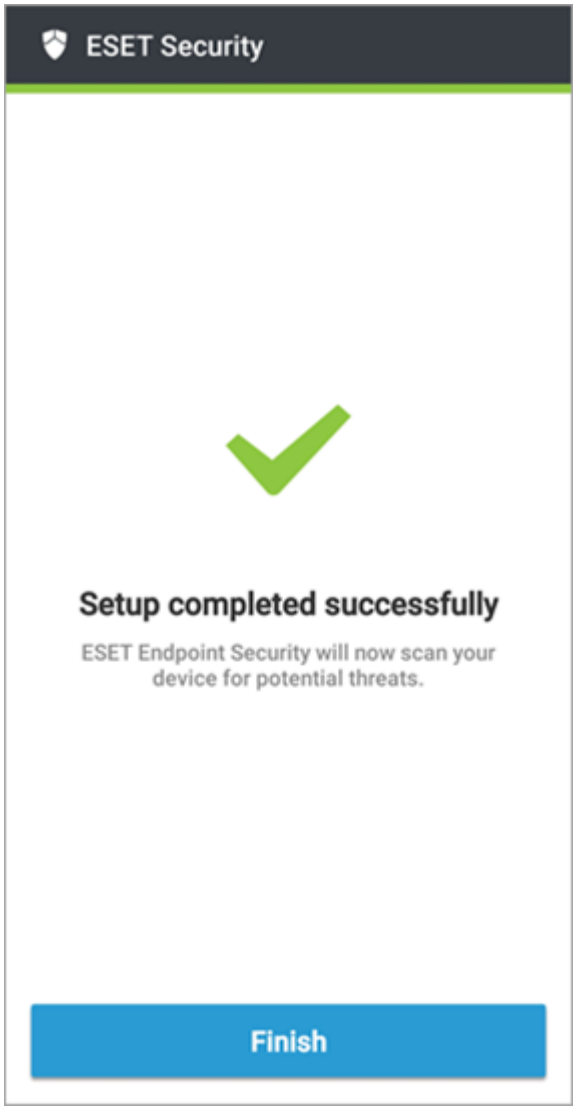
8. Ťuknutím na **Aktivovat** povolíte pro administrátora zařízení oprávnění k ESET Endpoint Security pro Android.



9. Ťuknutím na **Pokračovat** povolte oprávnění přístupu k datům o používání.



10. Ťukněte na **Dokončit**.



ESET Endpoint Security pro Android se otevře a ESET PROTECT nyní spravuje mobilní zařízení.

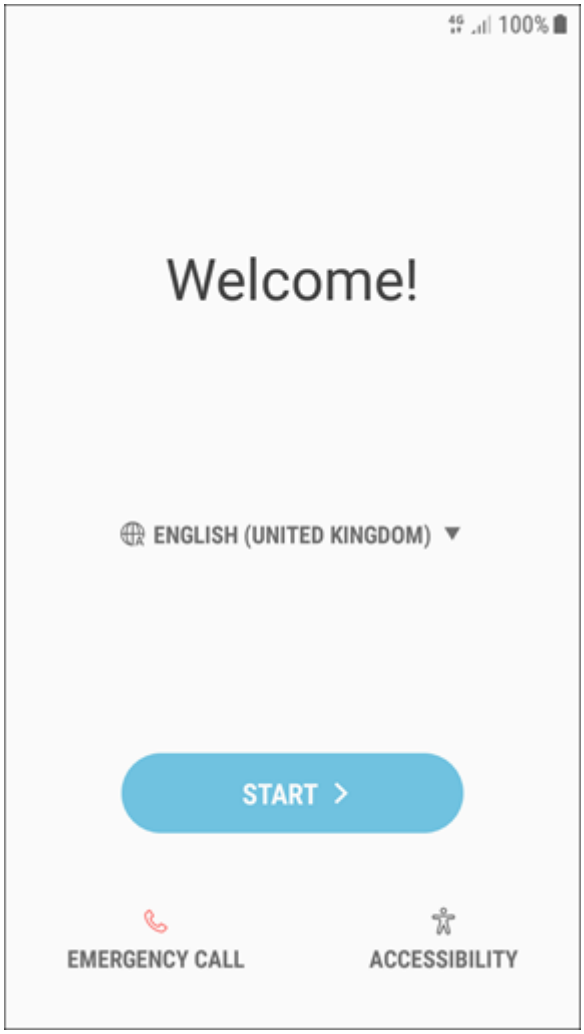
Registrace zařízení s OS Android – Vlastník zařízení

Registrace typu Vlastník zařízení je k dispozici pouze pro zařízení se systémem Android 7 a novějším. Zařízení se systémem Android musí být obnoveno do továrního nastavení nebo po vybalení z krabice, aby bylo možné provést následující kroky registrace.

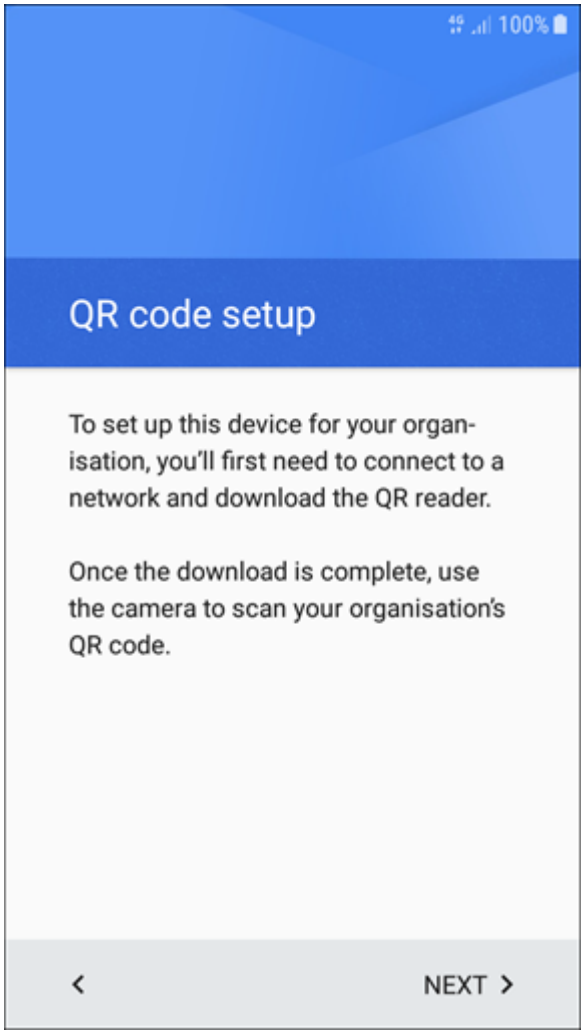
1. Zapněte mobilní zařízení.

2. Zadejte PIN k SIM kartě (je-li používán).

3. Na uvítací obrazovce vyberte preferovaný jazyk a poté šestkrát ťukněte na obrazovku kolem textu **Vítejte**, čímž spustíte nastavení QR kódu.

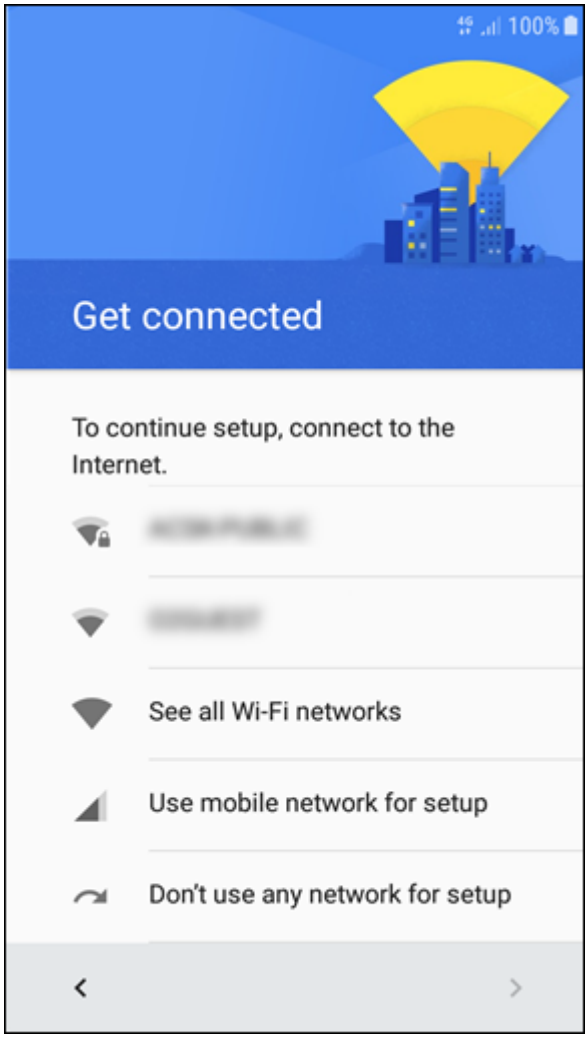


4. Zobrazí se obrazovka **Průvodce konfigurací QR kódem**. Pokračujte ťuknutím na tlačítko **Další**.



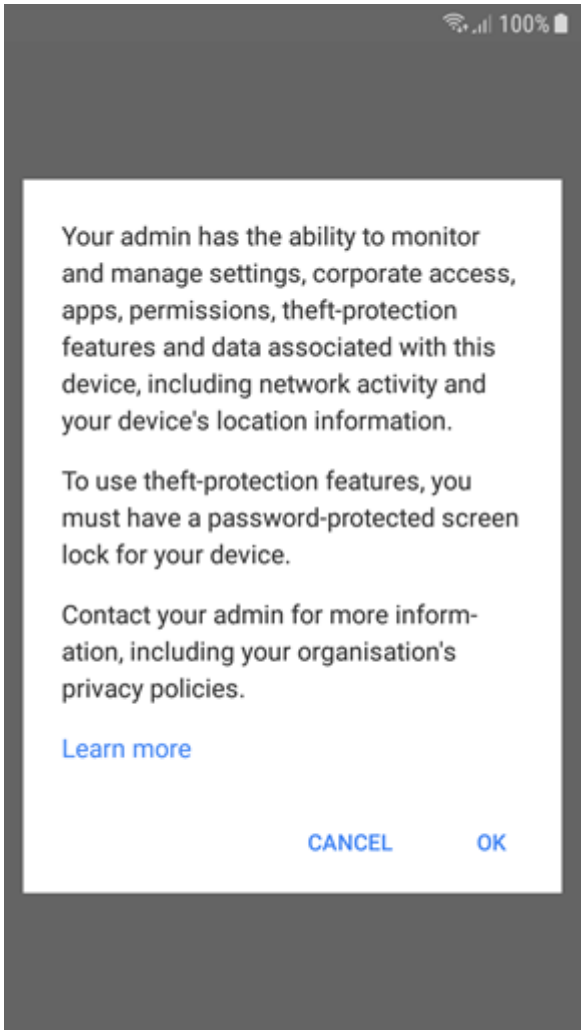
Některá zařízení mohou vyžadovat zašifrování úložiště (někdy je to nutné i pro připojení nabíječky). Budete-li k tomu vyzváni, vyberte způsob šifrování a postupujte podle kroků na obrazovce.

5. Zvolte připojení k internetu, abyste si mohli stáhnout čtečku QR kódů potřebnou pro další krok.

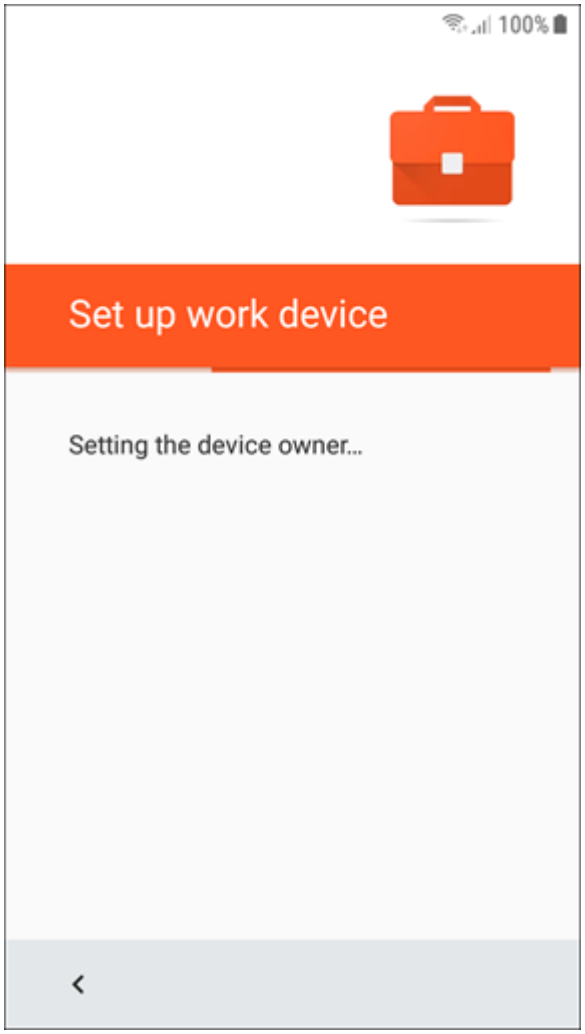


6. V tomto kroku se nainstaluje čtečka QR kódů. Po dokončení instalace naskenujte QR kód vygenerovaný ve webové konzoli ESET PROTECT.

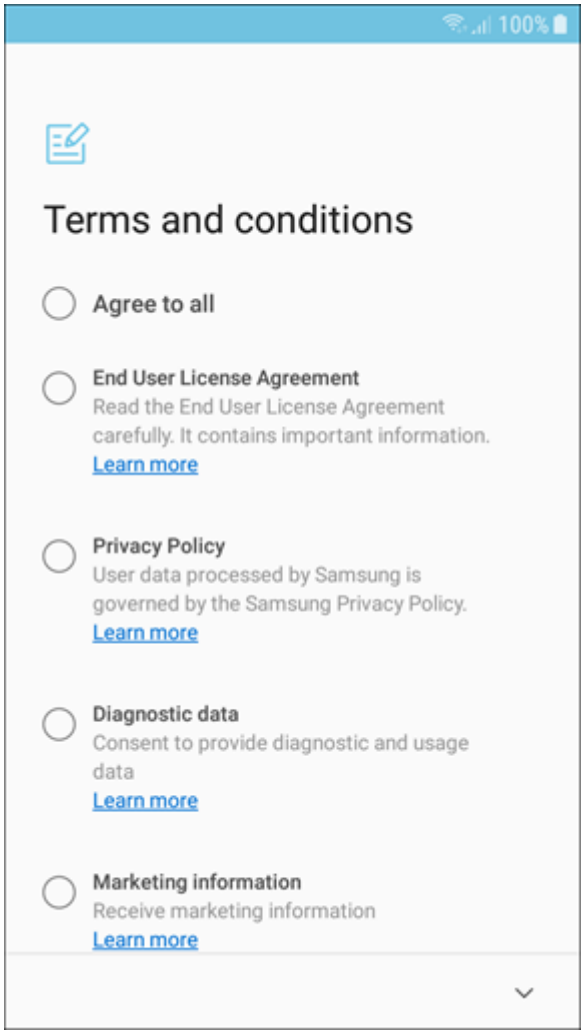
7. Následně budete vyzváni k potvrzení toho, že rozumíte tomu, co děláte (přidělujete administrátorovi oprávnění Vlastník zařízení). Pokračujte ťuknutím na tlačítko **OK**.



8. Nainstaluje se aplikaceESET Endpoint Security pro Android a budou nastavena požadovaná oprávnění.



9. Vybráním možnosti **Odsouhlasit vše** akceptujte EULA, zásady ochrany osobních údajů, zasílání diagnostických dat a příjem marketingových dat.



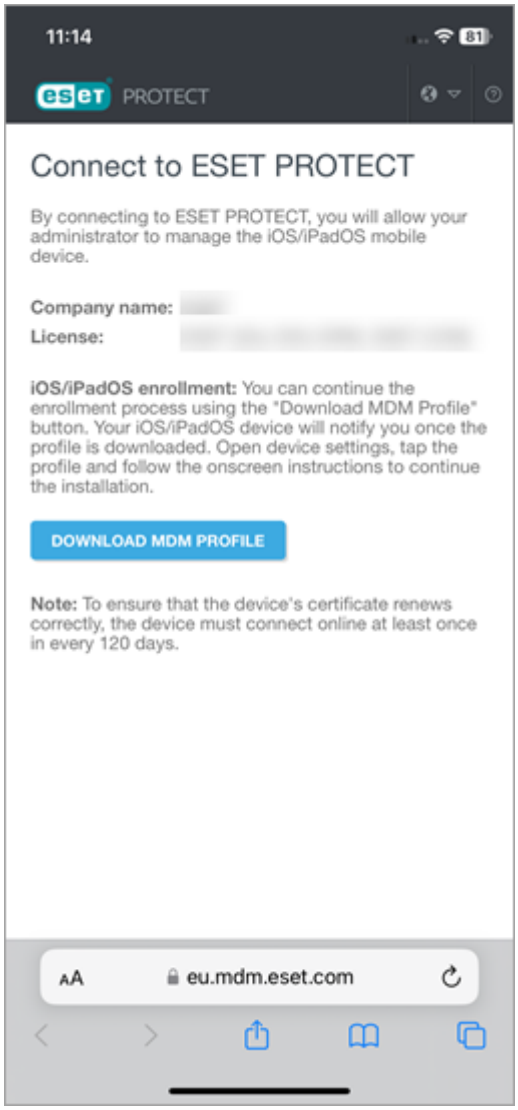
10. Zařízení je nyní registrováno v režimu Vlastník zařízení.

Registrace zařízení s iOS

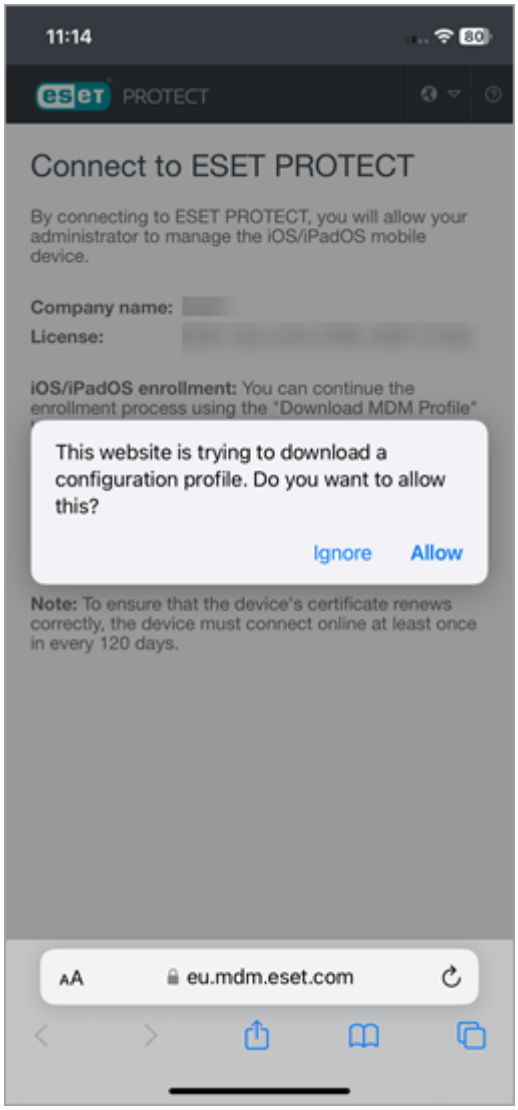
Podle níže uvedených kroků zaregistrujte iOS zařízení v ESET PROTECT:

Zaregistrovaná mobilní zařízení se musí k ESET PROTECT připojit jednou za 120 dní, aby se předešlo problémům s připojením. Tyto informace jsou uvedeny v registračním e-mailu nebo v QR kódu. Náhradní zařízení předem neregistrujte. Doporučujeme zaregistrovat pouze ta náhradní zařízení, která se budou používat v průběhu následujících 120 dní.

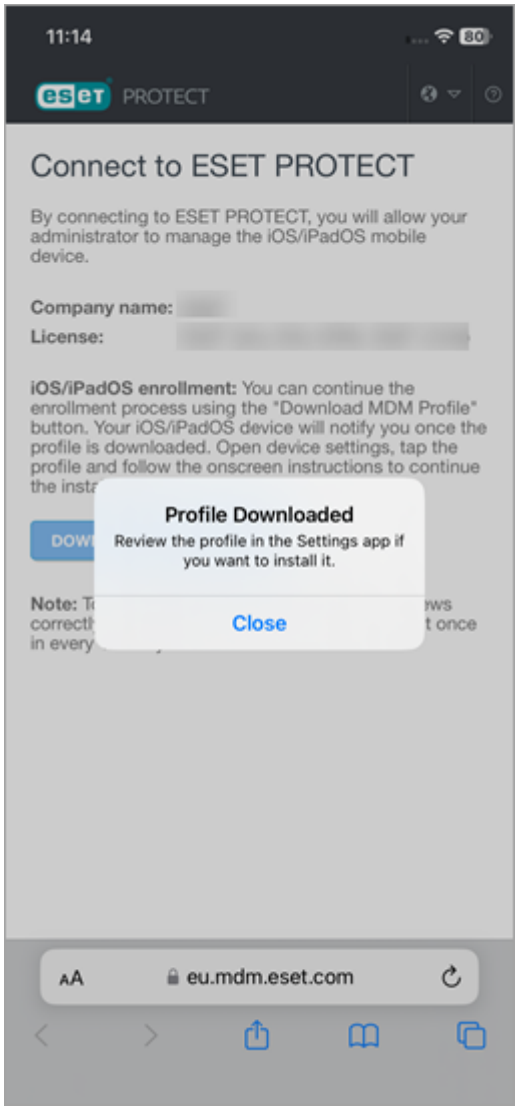
1. Otevřete odkaz pro registraci z e-mailu nebo QR kódu a ťukněte na **Stáhnout MDM profil**.



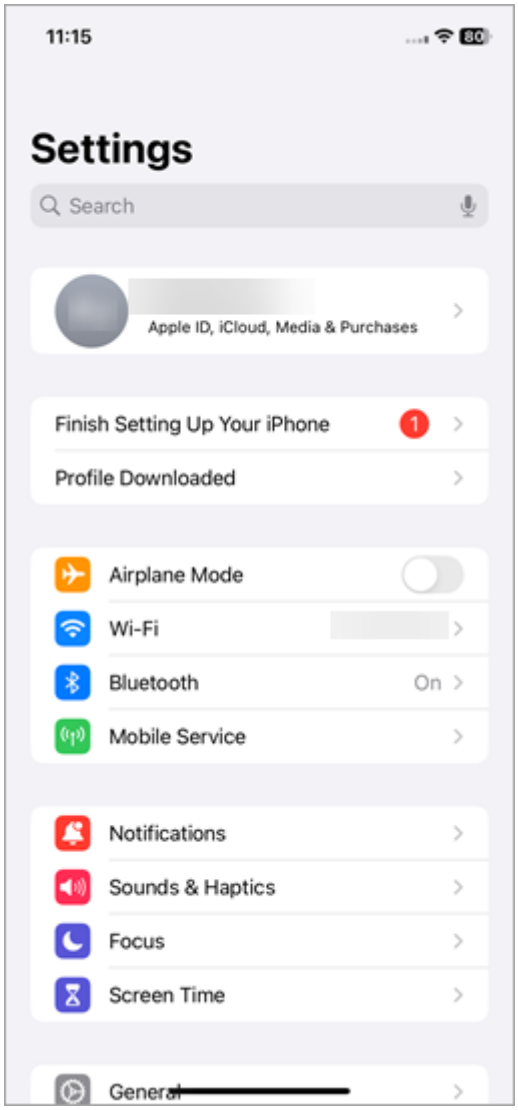
2. Ťukněte na **Povolit**.



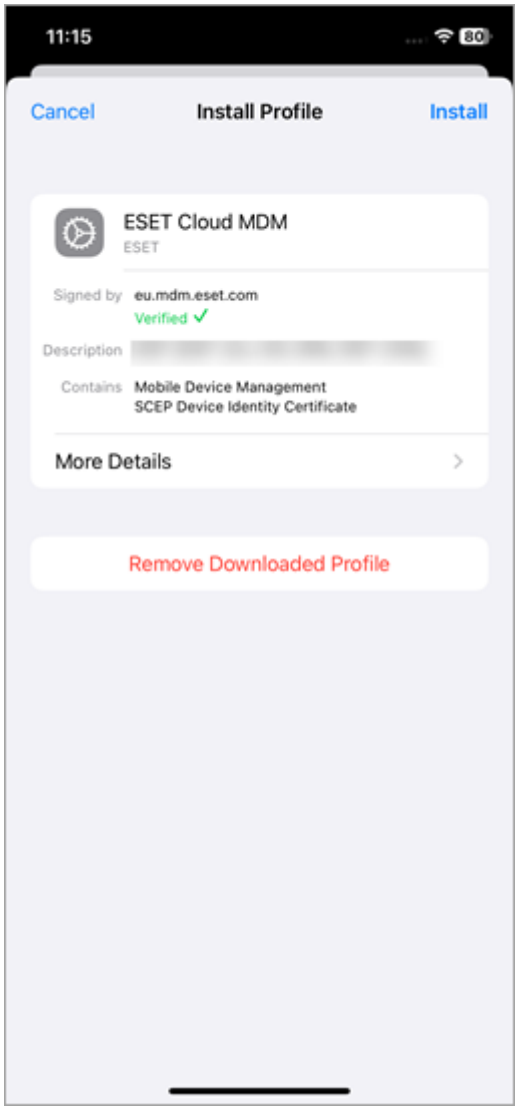
3. Ťukněte na **Zavřít**.



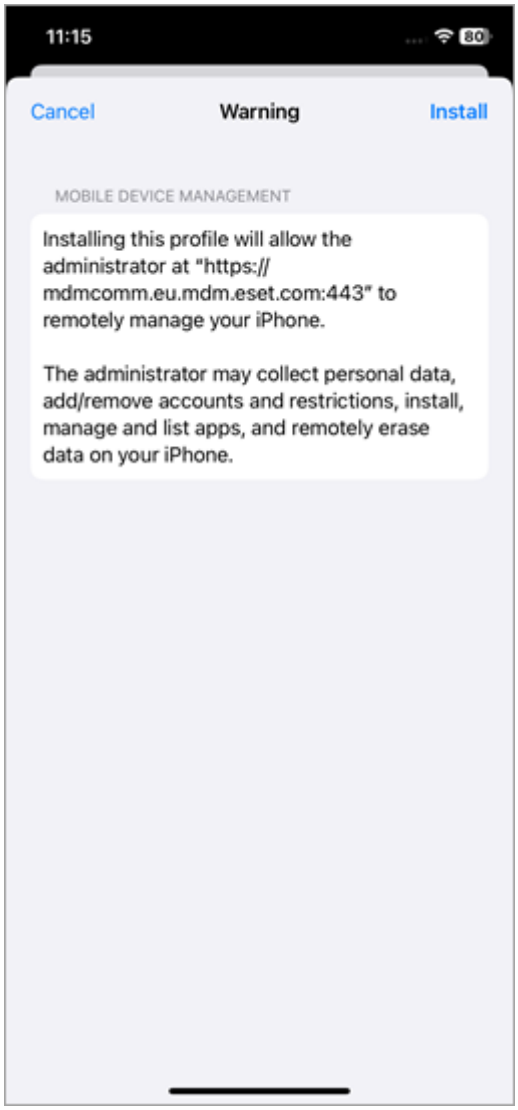
4. Otevřete **Nastavení** aplikace a ťukněte na **Stažený profil**.



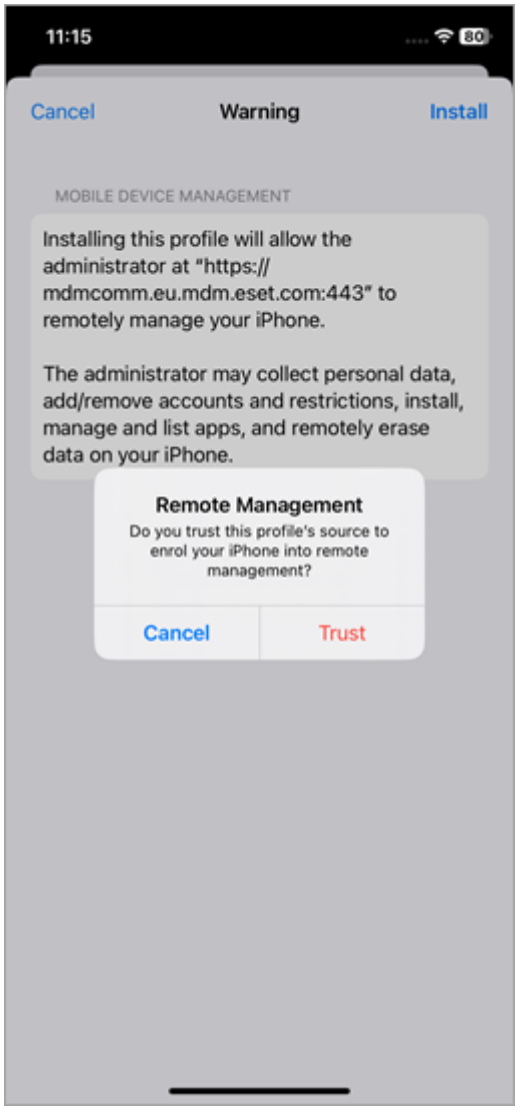
5. Ťuknutím na **Instalovat** nainstalujete ESET Cloud MDM profil.



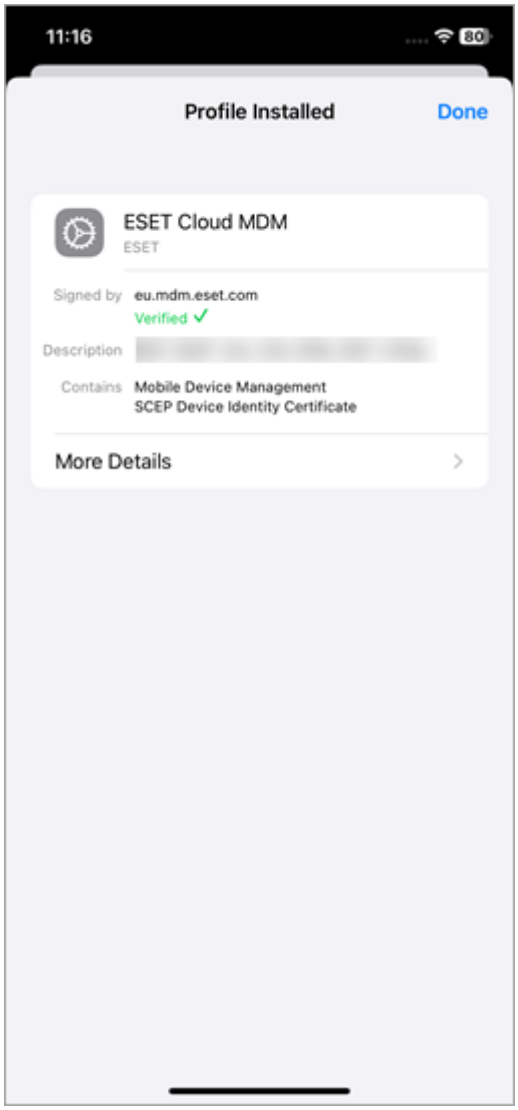
6. Ťukněte na **Instalovat**.



7. Ťuknutím na **Důvěřovat** nainstalujte nový profil.



8. Ťukněte na **Dokončit**.

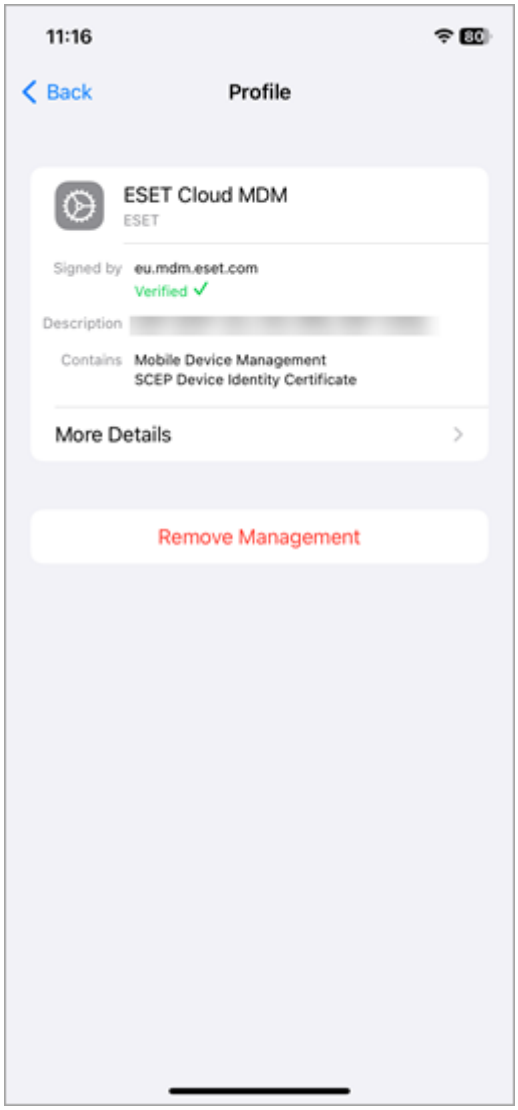


ESET PROTECT nyní spravuje mobilní zařízení. Registrační profil umožňuje konfigurovat zařízení a nastavit bezpečnostní politiky pro uživatele nebo skupiny. Podrobnosti o profilu najdete v **Nastavení** aplikace > **Obecné** > **VPN a Správa zařízení**.

Odstranění registrovaného profilu

Chcete-li odebrat registrovaný profil, otevřete **Nastavení** aplikace > **Obecné** > **VPN a Správa zařízení** > ťukněte na **Odebrání**.

Odebráním registračního profilu se odstraní všechna firemní nastavení (pošta, kalendář, kontakty atd.) a mobilní zařízení se systémem iOS se vyřadí ze správy. Zařízení se přestane připojovat k ESET PROTECT a jeho stav se změní na varovné upozornění a po 14 dnech na červené upozornění.



Registrace pomocí Microsoft Entra ID (Android nebo iOS)

Uživatel Microsoft Entra ID (dříve Azure Active Directory) může registrovat mobilní zařízení se systémem Android nebo iOS v ESET PROTECT.

Pro tento typ registrace mobilního zařízení potřebujete uživatelský účet Microsoft Entra ID. Všechna mobilní zařízení můžete zaregistrovat prostřednictvím jednoho odkazu.

1. Ve webové konzoli ESET PROTECT klikněte na **Další** > **Nastavení** > **Registrace pomocí Microsoft Entra ID**.
2. Pro získání autorizačního tokenu klikněte na **Získat token**.
3. Přihlaste se pomocí svého účtu Microsoft Entra ID a přijměte požadované povolení.
4. V části **Schválení uživatelé** vyberte uživatele Microsoft Entra ID, kteří mohou registrovat mobilní zařízení:
   - **Všichni uživatelé** – všichni uživatelé Microsoft Entra ID se mohou zaregistrovat
   - **Pouze uživatelé z určité skupiny** – vyberte skupinu uživatelů Microsoft Entra ID, kteří se mohou

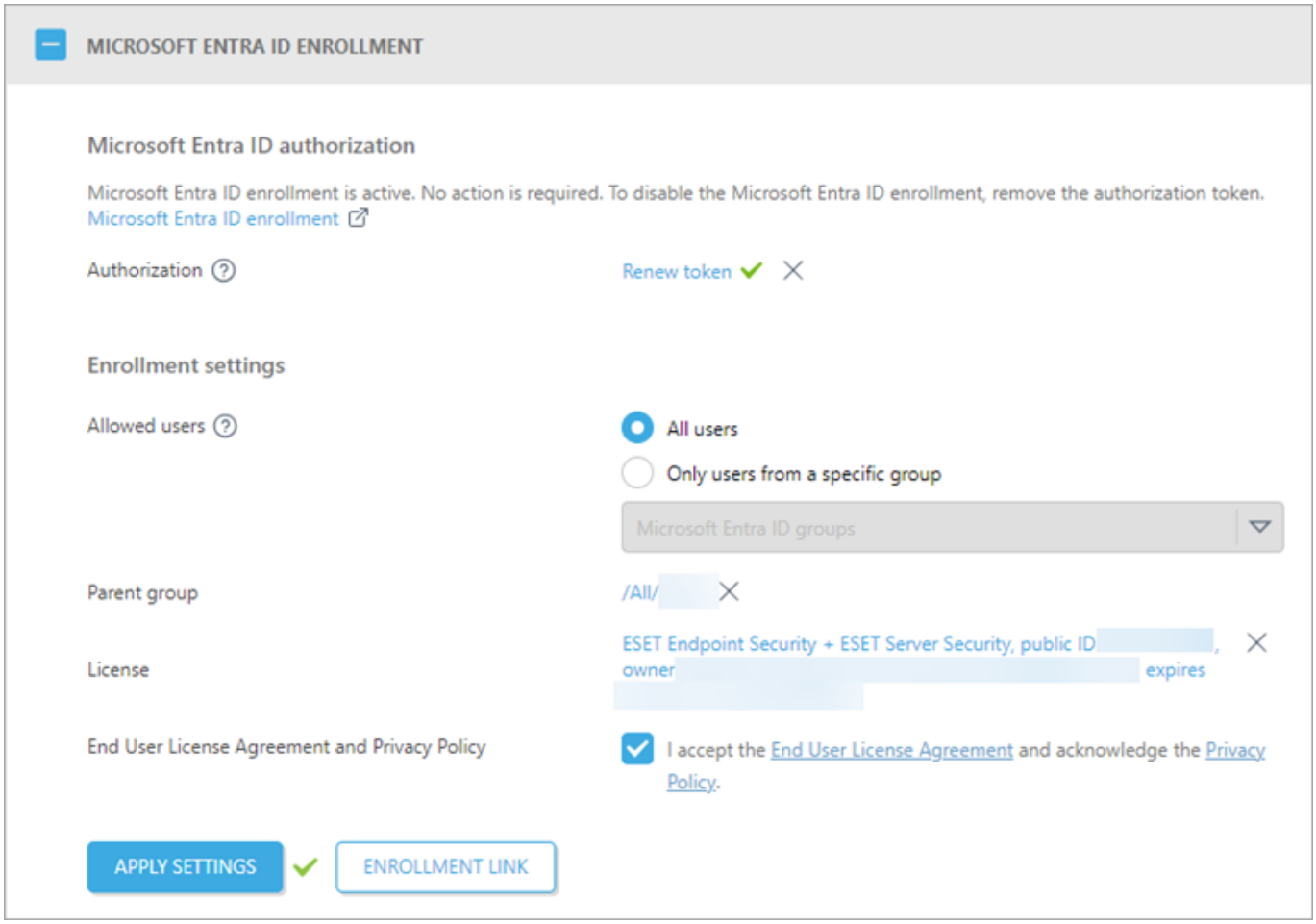
zaregistrovat

5. Vyberte **nadřazenou skupinu,** do které budou zaregistrovaná mobilní zařízení patřit.

6. Výběrem **licence** aktivujte zaregistrovaná mobilní zařízení.

7. Zaškrtněte možnost **Přijímám licenční ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

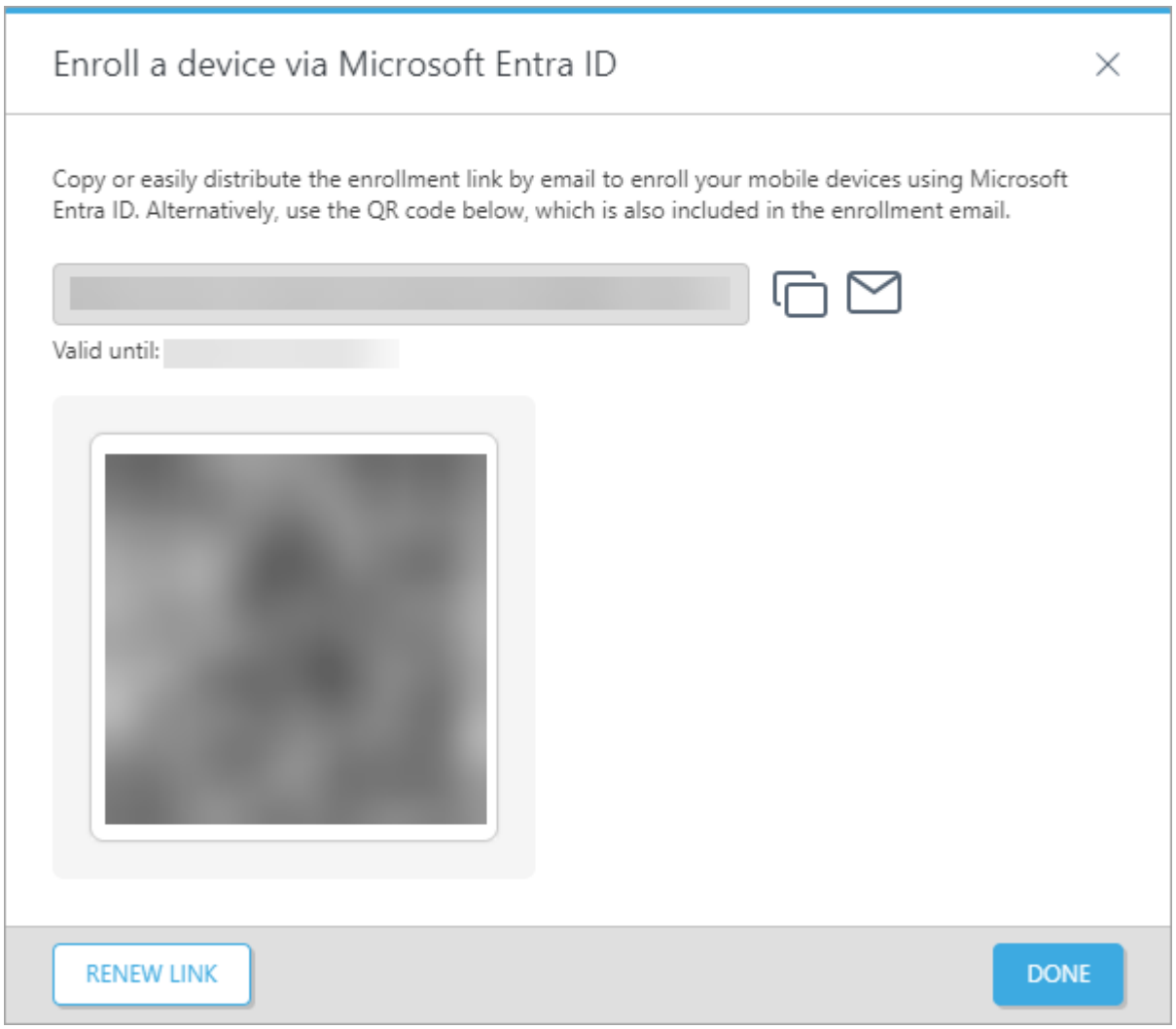
8. Po kliknutí na **Aplikovat nastavení** se uloží a aplikují všechny vybrané parametry registrace. Mobilní zařízení s Microsoft Entra ID se zobrazí ve webové konzoli ESET PROTECT v sekci **Počítače** se stejnými názvy. Zařízení lze přejmenovat v Detailech zařízení.



9. Pro zobrazení registračního odkazu klikněte na **Registrační odkaz**:

• Odkaz můžete zkopírovat, naskenovat pomocí kódu QR nebo odeslat e-mailem. Existuje jeden registrační odkaz, a ten není vázaný na specifického uživatele.

• Odkaz pro registraci je platný po dobu jednoho roku. Pro obnovení registračního odkazu klikněte na **Obnovit odkaz**.



10. Otevřete odkaz pro registraci na mobilním zařízení, přihlaste se ke svému účtu Microsoft Entra ID a přijměte požadované povolení. Poté postupujte podle pokynů pro registraci Android nebo iOS.

> Registrace Android zařízení s omezenými možnosti vstupu:
> 1.Na počítači si ve webovém prohlížeči otevřete odkaz pro registraci.
> 2.Vložte bezpečnostní kód vygenerovaný v ESET Endpoint Security pro Android aplikaci do mobilního zařízení, které chcete zaregistrovat.
> 3.Dokončete registraci.

11. Nyní můžete v ESET PROTECT spravovat mobilní zařízení s Microsoft Entra ID.

Všechna mobilní zařízení s Microsoft Entra ID jsou ve vyhrazených dynamických skupinách – **Registrace Microsoft Entra ID** (Android zařízení) a Zařízení **Microsoft Entra ID** (iOS zařízení).

Synchronizace s Microsoft Intune (Android)

V případě, že používáte Microsoft Intune, můžete svůj účet synchronizovat s ESET PROTECT, a jeho prostřednictvím spravovat vaše zařízení s Androidem, která v Microsoft Intune máte.

Požadavky

- Registrace zařízení s Androidem.
- Připojení svému účtu Intune ke spravovanému účtu Google Play.
- Zaregistrujte zařízení jako Android Enterprise.
- Před registrací proveďte migraci zařízení zaregistrovaných jako **administrátor zařízení se systémem Android**.

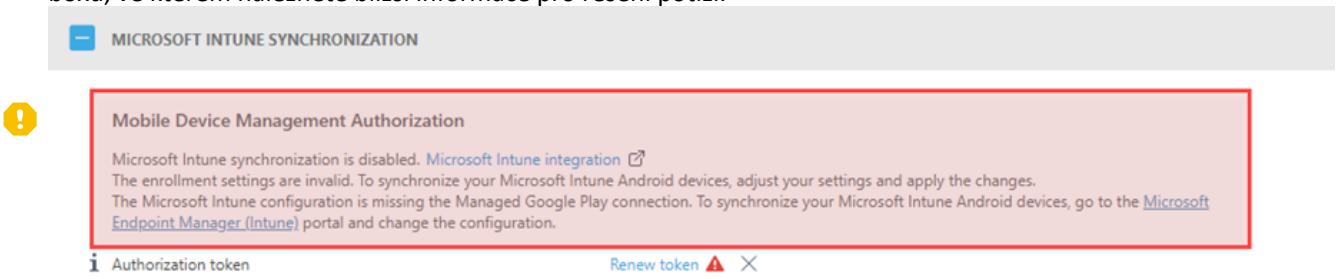
1. V hlavním menu ESET PROTECT Web Console přejděte do sekce **Další** > **Nastavení** > **Synchronizace s Microsoft Intune**.

2. Klikněte na **Získat token**.

3. Přihlaste se ke svému účtu Microsoft Intune.

4. Po úspěšném přihlášení se zobrazí **Žádost o přidělení oprávnění** pro aplikaci ESET PROTECT. Zkontrolujte poskytnuté informace a po kliknutí na **Přijmout** přidejte platný autentizační token k instanci ESET PROTECT.

Pokud se v průběhu importování autorizačního tokenu vyskytne nějaký problém, podívejte se do informačního boxu, ve kterém naleznete bližší informace pro řešení potíží.



5. V části **Nastavení registrace** si vyberte jeden ze způsobů:

- **Registrovat všechna Android zařízení** – do ESET PROTECT se automaticky zaregistrují všechny Android zařízení, která máte v Microsoft Intune.
- **Registrovat Android zařízení všech uživatelů** – do ESET PROTECT se zaregistrují se pouze Android zařízení, která mají v Microsoft Intune přiřazeného uživatele.
- **Registrace Android zařízení ze skupin Microsoft Intune** – do ESET PROTECT se zaregistrují pouze Android zařízení z vámi vybraných skupin v Microsoft Intune.

6. Vyberte **licenci**, kterou chcete použít pro aktivaci registrovaných Android zařízení.

7. Vyberte **nadřazenou skupinu**, do které se registrovaná zařízení s Androidem zařadí.

8. **Oznámení** (ve výchozím nastavení povoleno) – automatické zasílání oznámení na každé zařízení, pokud ochrana nebyla aktivována. Oznámení informují uživatele o tom, že jsou v jejich zařízeních nainstalovaná bezpečnostní řešení, která je třeba aktivovat otevřením ESET Endpoint Security v jejich pracovním profilu. Zařízení může obdržet až tři oznámení: pět dní, sedm dní a devět dní po registraci. Kliknutím na **Přizpůsobit** můžete zprávu upravit oznámení přizpůsobit.

9. Pro uložení a aplikování vybraných parametrů registrace klikněte na **Aplikovat možnosti registrace**.

Nyní můžete svá Microsoft Intune zařízení spravovat prostřednictvím Microsoft Intune i ESET PROTECT zároveň.

Při registraci zařízení s OS Android verze 9 a novější prostřednictvím Microsoft Intune nebo VMware Workspace ONE, ESET Endpoint Security pro Android verze 3.5 a novější budou ignorována následující nastavení politik:

- Správa zařízení
- Správa aplikací
- Anti-Theft

Synchronizace s VMware Workspace ONE (Android)

Pokud spravujete zařízení se systémem Android pomocí VMware Workspace ONE (viz Registering Android with VMware Workspace ONE), můžete svůj VMware Workspace ONE účet synchronizovat s ESET PROTECT a chránit tak zařízení VMware Workspace ONE se systémem Android. Tuto synchronizaci nakonfigurujte podle následujících kroků:

I. Povolte přístup k REST API v VMware Workspace ONE

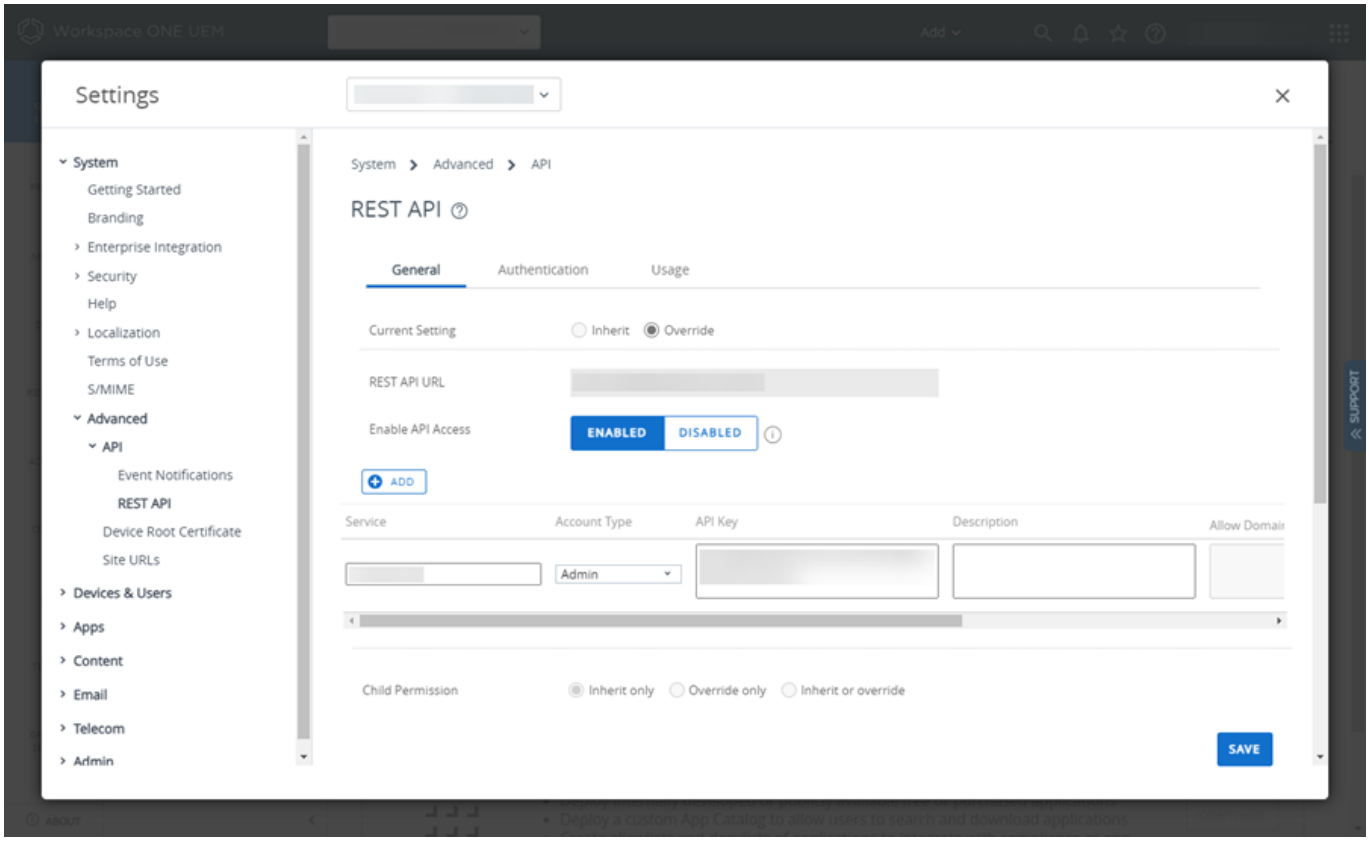
II. Vytvořte klienta OAuth v VMware Workspace ONE

III. Synchronizace ESET PROTECT s VMware Workspace ONE

I. Povolení přístupu k REST API v VMware Workspace ONE

1. Přihlaste se do VMware Workspace ONE.
2. Klikněte na **Začínáme** > **Nastavení**.
3. Klikněte na **Pokročilé** > **API** > **REST API**.
4. Zkopírujte **URL adresu REST API**.
5. Vyberte **Povoleno** vedle položky **Povolit přístup API**.
6. Klikněte na **Přidat**, zadejte název **Služby** a zkopírujte **API klíč**.
7. Klikněte na **Uložit**.

Další informace o REST API pro VMware Workspace ONE.



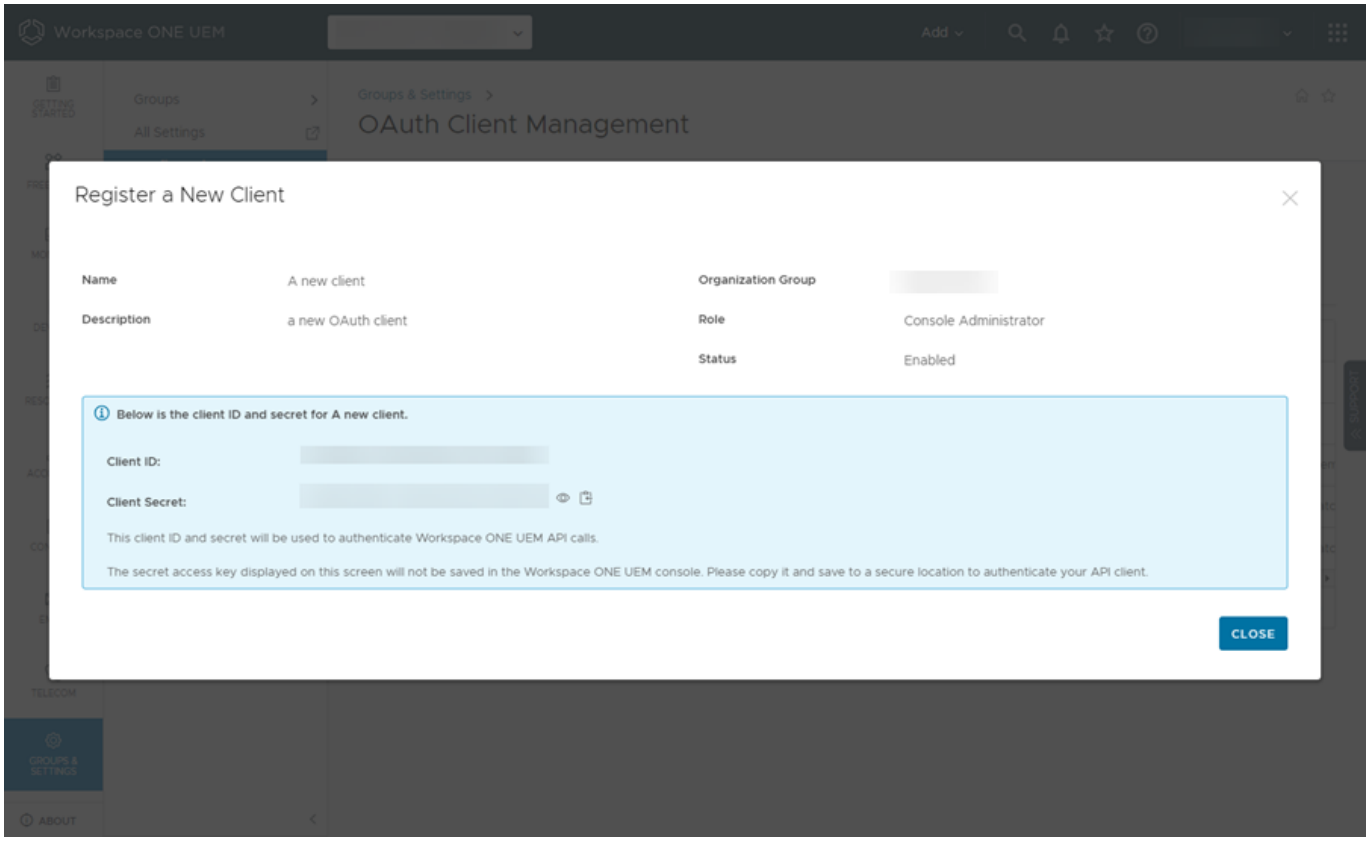
II. Vytvoření klienta OAuth v VMware Workspace ONE

1. Klikněte na **Skupiny a nastavení** > **Konfigurace**.
2. Do vyhledávacího pole **Zadejte název nebo kategorii** napište **OAuth**.
3. Klikněte na **Správa klientů OAuth**.
4. Klikněte na **Přidat**.
5. V okně **Registrace nového klienta**:
   a. Zadejte **jméno**, **popis** a **organizační skupinu**.
   b. V rozbalovacím menu **Role** vyberte možnost **Správce konzole**.
   c. Ujistěte se, že přepínač **Stavu** je v poloze **Zapnuto**.
   d. Klikněte na **Uložit**.
6. Zkopírujte **ID klienta** a **tajný klíč**.

> Před zavřením okna se ujistěte, že jste zkopírovali a uložili **ID klienta** a **tajný klíčí**. Po kliknutí na **Zavřít** už nelze načíst **ID klienta** a **tajný klíč**.

7. Klikněte na tlačítko **Zavřít**.

> Další informace o správě klientů OAuth najdete v dokumentaci k VMware Workspace ONE.



III. Synchronizace ESET PROTECT s VMware Workspace ONE

1. Detailní informace o analyzovaných souborech naleznete v ESET PROTECT Web Console v sekci **Další** > **Nastavení**.

2. Rozšiřte **synchronizace s VMware Workspace ONE**.

3. Klikněte na **Nastavit** vedle **Autorizace**.

4. Zadejte nebo vložte požadované nastavení autorizace:

   a. **URL adresa REST API** – zadejte nebo vložte odkaz, který jste zkopírovali v kroku 4 v části I výše.

   b. **REST API KEY** – zadejte nebo vložte **API klíč**, který jste zkopírovali v kroku 6 v části I výše.

   c. **ID klienta OAuth** – zadejte nebo vložte **ID klienta**, které jste zkopírovali v kroku 6 v části II výše.

   d. **Tajný klíč klienta OAuth** – zadejte nebo vložte **Tajný klíč**, který jste zkopírovali v kroku 6 v části II výše.

5. Klikněte na tlačítko **Nastavit**. Pokud je nastavení autorizace správné, zobrazí se zpráva **Aktualizovat ✔** se zeleným zaškrtnutím vedle pole **Autorizace**.

6. V části **Přiřazení** vyberte zařízení se systémem Android, která chcete synchronizovat:

   a. **Registrovat všechna Android zařízení** – synchronizovat všechna zařízení se systémem Android z VMware Workspace ONE.

Volba **Registrovat všechna Android zařízení** vytvoří VMware Workspace ONE smart skupinu **Všechna Android zařízení chráněná ESET**. **Přiřazení ochrany ESET** nainstaluje ESET Endpoint Security pro Android na mobilní zařízení v této skupině. Pokud později vyberete možnost **Registrovat pouze zařízení s OS Android z konkrétní skupiny**, bude smazána smart skupina **Všechna Android zařízení chráněná ESET**.

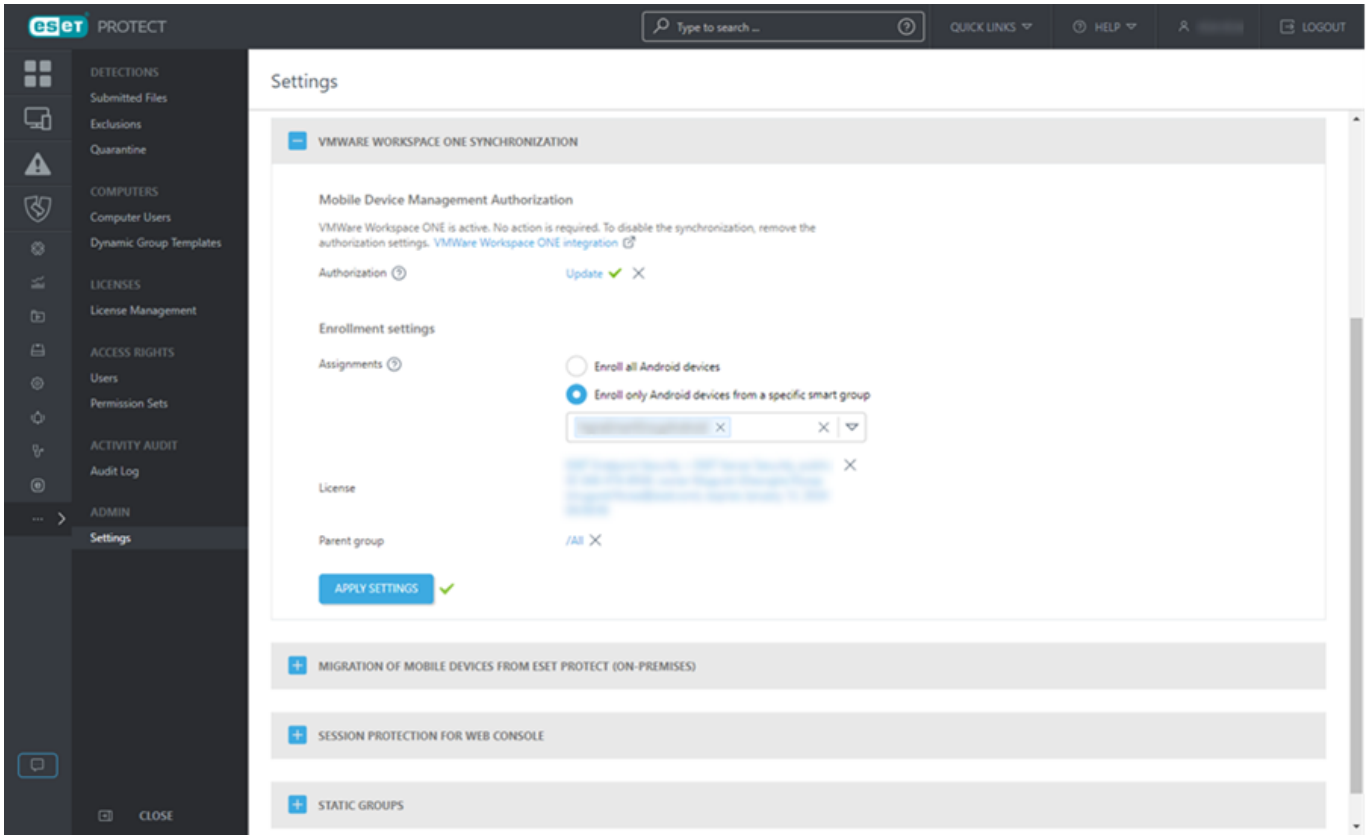
b. **Registrovat pouze zařízení se systémem Android z konkrétní smart skupiny** – synchronizuje Android zařízení z VMware Workspace ONE smart skupin vybraných z rozbalovacího menu.

7. **Licence** – příslušná licence je předem vybrána. Můžete si vybrat jinou licenci. Licence během instalace aktivuje ESET Endpoint Security pro Android.

8. **Nadřazená skupina** – vyberte nadřazenou skupinu ESET PROTECT, podle které se budou zařízení se systémem Android synchronizovat.

9. **Oznámení** (ve výchozím nastavení povoleno) – automatické zasílání oznámení na každé zařízení, pokud ochrana nebyla aktivována. Oznámení informují uživatele o tom, že jsou v jejich zařízeních nainstalovaná bezpečnostní řešení, která je třeba aktivovat otevřením ESET Endpoint Security v jejich pracovním profilu nebo ťuknutím na odkaz v oznámení. Zařízení může obdržet až tři oznámení: pět dní, sedm dní a devět dní po registraci. Kliknutím na **Přizpůsobit** můžete zprávu upravit oznámení přizpůsobit.

10. Klikněte na **Aplikovat nastavení**.



Android zařízení z VMware Workspace ONE se zobrazí v sekci Počítače pod vybranou nadřazenou skupinou a prostřednictvím politiky můžete spravovat nainstalovaný ESET Endpoint Security pro Android.

Při registraci zařízení s OS Android verze 9 a novější prostřednictvím Microsoft Intune nebo VMware Workspace ONE, ESET Endpoint Security pro Android verze 3.5 a novější budou ignorována následující nastavení politik:

- Správa zařízení
- Správa aplikací
- Anti-Theft

Synchronizace (iOS) s Apple Business Manager (ABM)

Apple Device Enrollment Program (DEP) je nový způsob, který společnost Apple nabízí pro registraci firemních iOS zařízení. Prostřednictvím ABM nemusíte mít k zařízení fyzický přístup a tento způsob vyžaduje minimální interakci uživatele. Při registraci ABM si můžete jako administrátor přizpůsobit proces prvotní konfigurace zařízení. Dále nabízí možnost pro zabránění uživateli v odebrání MDM profilu ze zařízení. Do ABM můžete zařadit stávající iOS zařízení (splňují-li podmínky pro registraci) a všechna iOS zařízení, která si v budoucnu zakoupíte. Více informací naleznete v Apple ABM příručce a Apple ABM dokumentaci.

Před provedením registrace iOS zařízení v AMB povolte synchronizaci s ABM ve webové konzoli ESET PROTECT. V hlavním menu přejděte do sekce **Další** > **Nastavení** > **Synchronizace s Apple Business Manager (ABM)**.

Synchronizujte ESET PROTECT MDM s Apple ABM serverem

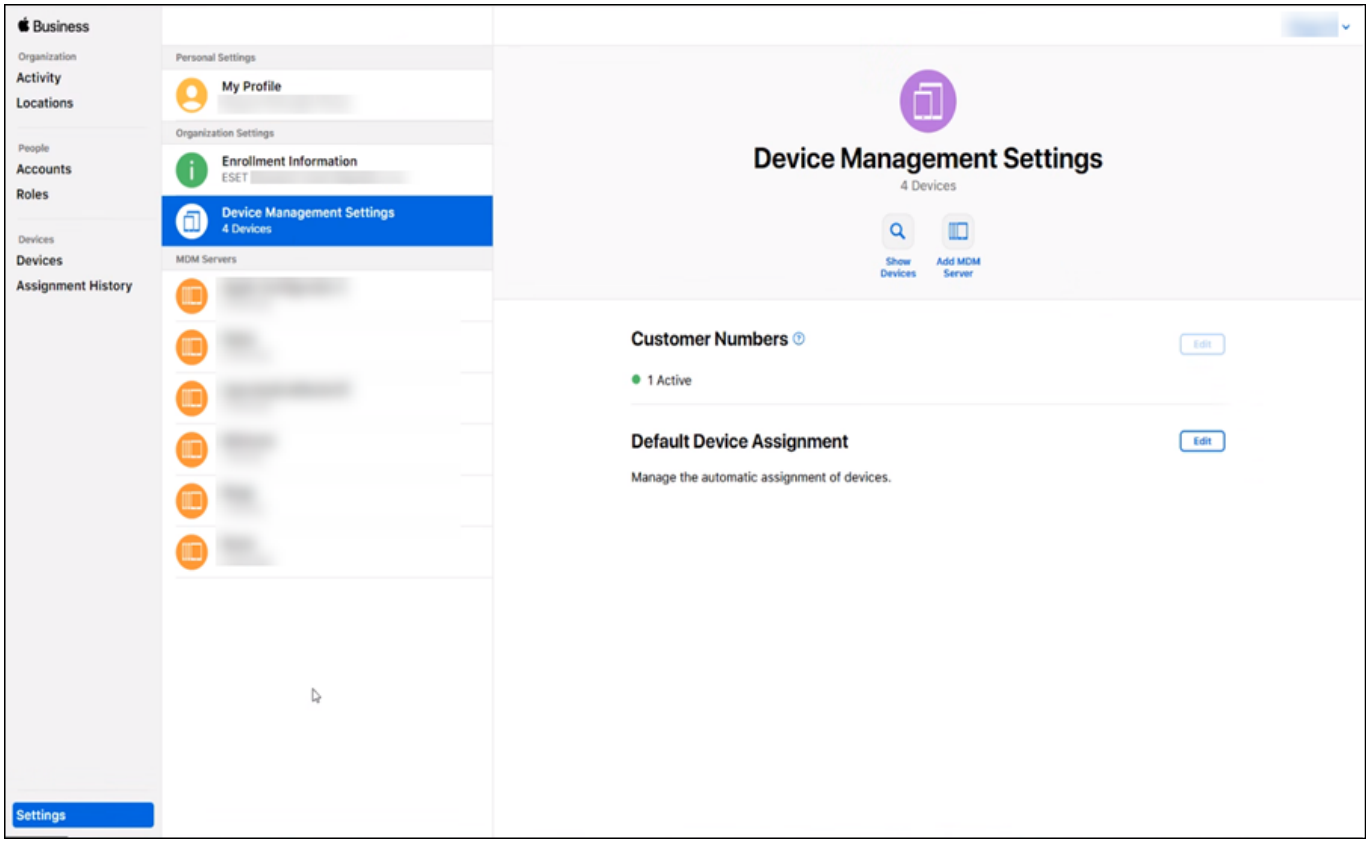
1. Ověřte, zda váš účet a iOS zařízení splňují podmínky pro Apple ABM.

ABM účet:

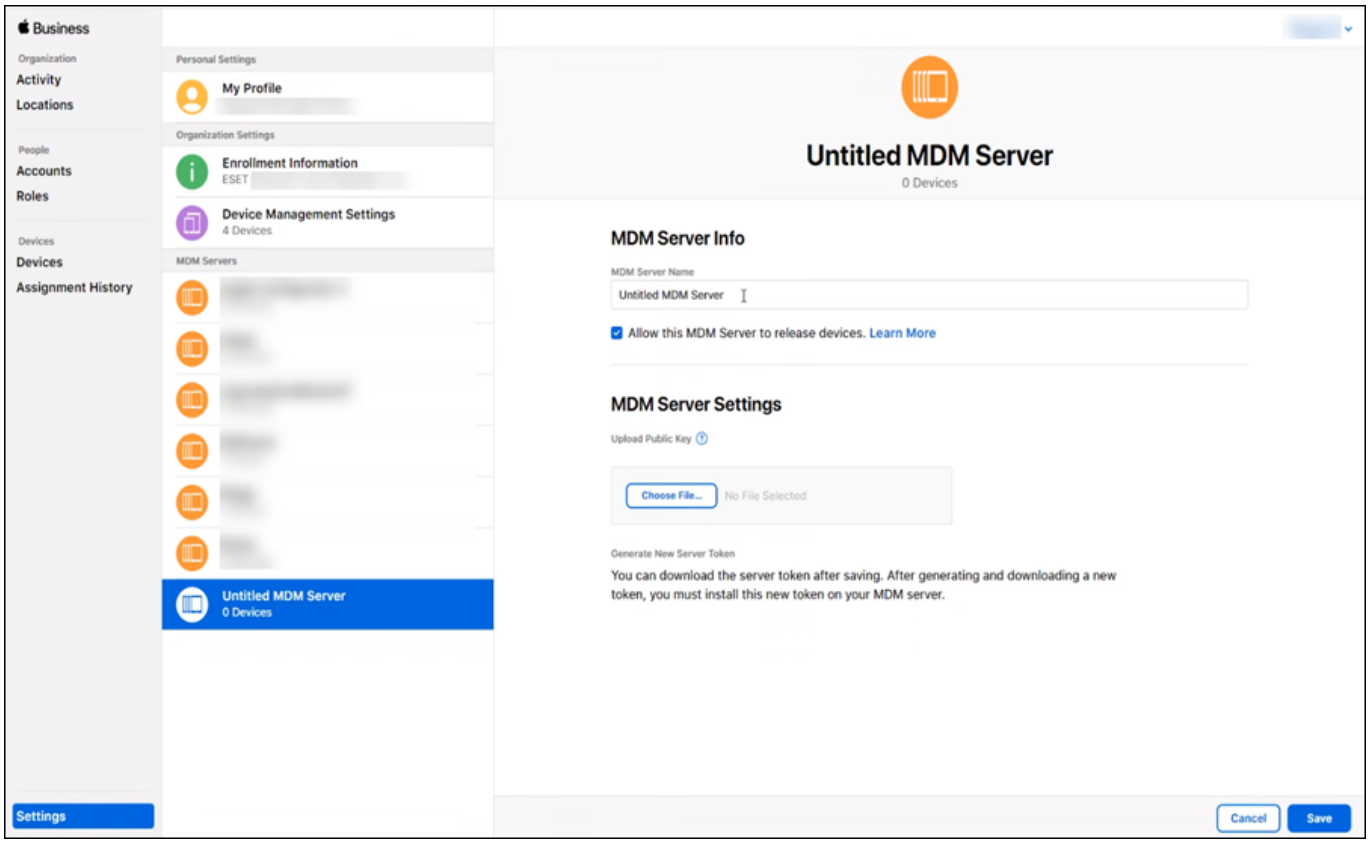
- Program je dostupný pouze v některých zemích. Zda je dostupný také ve vaší zemi ověřte na webových stránkách Apple ABM.
- Detailní informace o požadavcích na Apple ABM účet naleznete na webových stránkách společnosti Apple: Apple deployment program requirements a Apple Device Enrollment Program requirements.
- Detailní informace o požadavcích na zařízení v programu ABM naleznete na webových stránkách společnosti Apple.

2. Přihlaste se ke svému Apple ABM účtu. Pokud jej nemáte, vytvořte si jej.

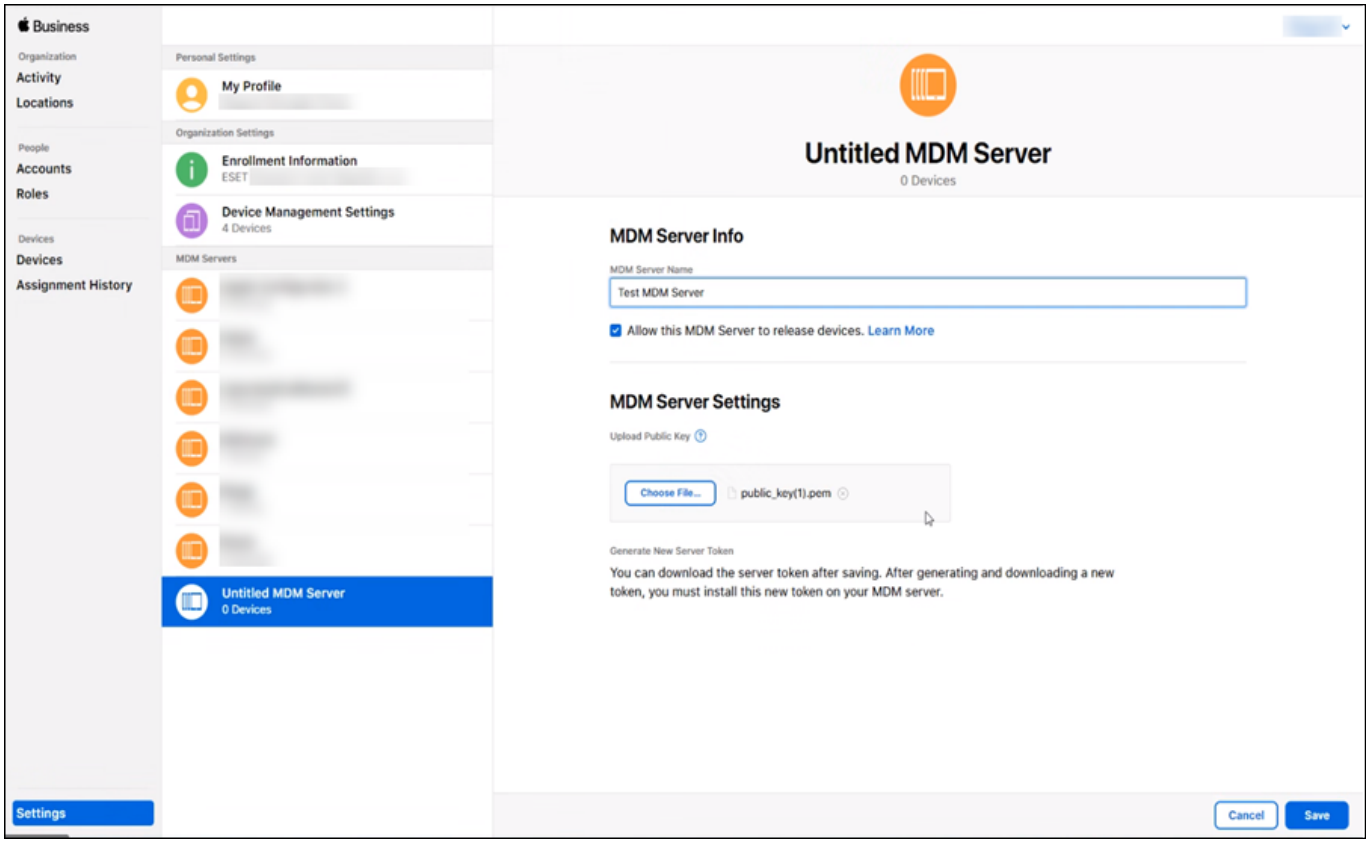
3. V sekci **Device Management Settings** vyberte možnost **Add MDM Server**.



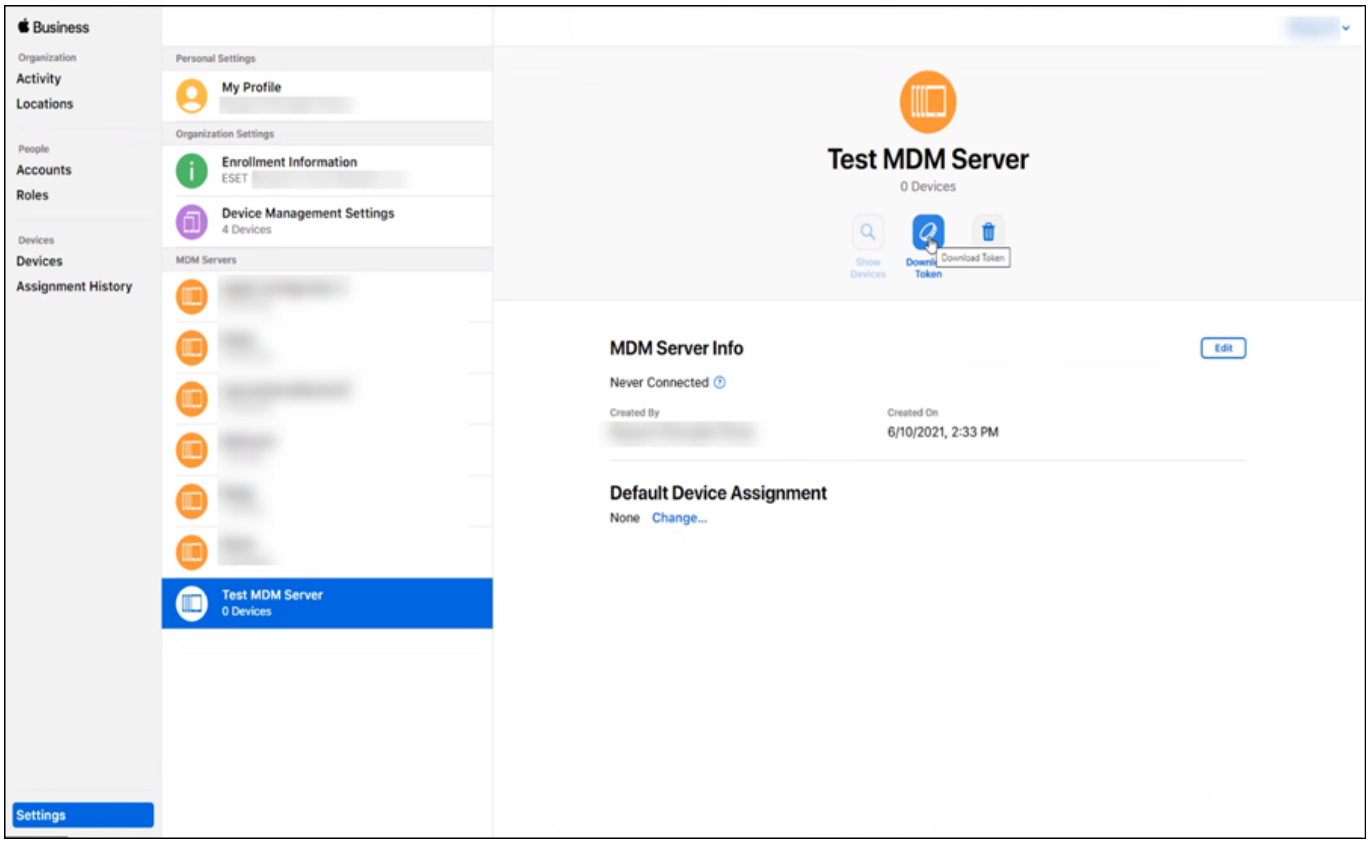
4. Zadejte **název MDM serveru**, například: "MDM_Server".



5. Na ABM portál nahrajte svůj veřejný klíč. Klikněte na **Choose file** a vyberte soubor s veřejným klíčem (soubor, který jste si stáhli z ESET PROTECT v sekci konfigurace ABM) a pokračujte kliknutím na tlačítko **Save**.



6. Následně si **stáhněte** vygenerovaný Apple ABM Token. Tento soubor nahrajte do Nastavení ESET PROTECT v sekci **ABM Server token** > **Nahrát**.

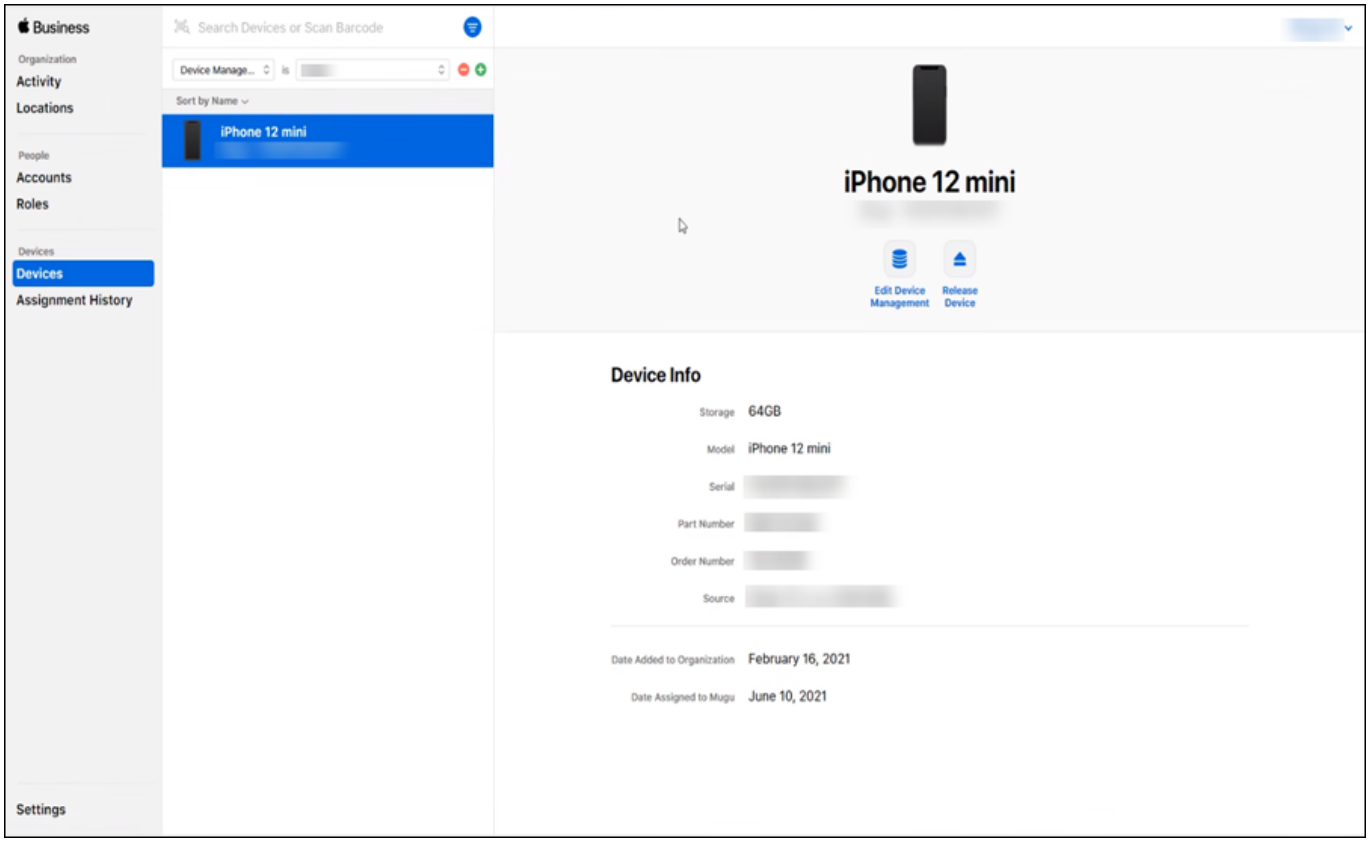


Přidejte iOS zařízení do Apple ABM:

V dalším kroku na Apple ABM portále přiřaďte iOS zařízení virtuálnímu MDM serveru. Zařízení přidejte ručně

zadáním sériového čísla nebo čísla objednávky (zákaznické číslo), případně můžete hromadně importovat CSV soubor se seznamem sériových čísel. V obou případech musíte přiřadit iOS zařízení virtuálnímu MDM serveru vytvořeném v předchozím kroku.

1. Na ABM portále přejděte do sekce **Devices** a vyberte zařízení, které chcete k serveru přiřadit. Dále pokračujte kliknutím na **Edit Device Management**.



2. Ze seznamu vyberte svůj MDM server a po potvrzení výběru dojde k přiřazení zařízení k MDM serveru.

Odebráním zařízení z ABM portálu dojde k jeho trvalému odstranění a již jej nebude možné znovu do portálu přidat.

Nyní můžete opustit Apple ABM portál a vrátit se zpět do webové konzole ESET PROTECT.

Pokud provedete registraci již používaného iOS zařízení (a splňuje všechny požadavky), nové nastavení bude vynuceno až po obnovením zařízení do továrního nastavení.

Interval synchronizace Cloud MDM je nastaven na 30 minut. To znamená, že se Apple zařízení v ESET PROTECT objeví až po uplynutí této doby.

Řešení problémů – opětovné přidání odebraného zařízení v programu ABM

Pokud jste odebrali zařízení v programu ABM ze seznamu zařízení ve webové konzoli ESET PROTECT, můžete jej znovu přidat do webové konzole ESET PROTECT následujícím postupem:

1. Odeberte zařízení z MDM Serveru v programu ABM. Neodebírejte zařízení v portálu ABM.

2. Počkejte 30 minut.

3. Znovu přiřaďte zařízení k MDM Serveru.

Spravovaná mobilní zařízení

Po registraci mobilních zařízení se systémem Android je můžete začít spravovat.

Kromě standardních možností pro správy všech koncových zařízení máte k dispozici další funkce, které jsou dostupné výhradně pro spravovaná mobilní zařízení.

Správa mobilních zařízení prostřednictvím klientských úloh

Úlohy Anti-Theft (platí pro zařízení se systémem Android a iOS) – úlohy lze provádět pouze u spravovaných mobilních zařízeních. Zařízení můžete např.: Najít, Zamknout nebo Obnovit jeho tovární nastavení. Administrátor je může použít ke vzdálenému zjištění polohy mobilního zařízení, stejně tak v situacích, kdy je vyžadováno smazání obsahu.

Podívejte se na všechny klientské úlohy pro mobilní zařízení.

> **Podmínky spuštění klientské úlohy na mobilních zařízeních**
> Pro klientské úlohy na mobilních zařízeních můžete použít pouze tyto podmínky spuštění:
> • Ihned
> • Při připojení do dynamické skupiny
> Klientské úlohy s jinými než výše uvedenými podmínkami spuštění skončí chybovou zprávou **Nepodporovaný typ podmínky spuštění**.

Správa zařízení se systémem Android prostřednictvím politik

Přiřaďte zařízení politiku **ESET Endpoint Security for Android**. V politice si upravte jednotlivá dostupná nastavení správy Androidu dle svých potřeb. Příklad:

- Filtrování obsahu webu
- Správa aktualizací operačního systému
- Vzdálená instalace aplikací – prostřednictvím politiky můžete vynutit vzdálenou instalaci aplikace na zařízení tím, že ji přidáte do seznamu vyžadovaných aplikací.

    1.K tomu si otevřete stávající nebo vytvořte novou politiku pro produkt **ESET Endpoint Security for Android**.

    2.V konfigurační šabloně přejděte do sekce **Správa aplikací** a aktivujte pomocí přepínače možnost **Zapnout správu aplikací**.

    3.Klikněte na **Seznam aplikací** a do seznamu přidejte aplikaci, kterou chcete po aplikaci politik instalovat vzdáleně na mobilním zařízení.

Při registraci zařízení s OS Android verze 9 a novější prostřednictvím Microsoft Intune nebo VMware Workspace ONE, ESET Endpoint Security pro Android verze 3.5 a novější budou ignorována následující nastavení politik:

- Správa zařízení
- Správa aplikací
- Anti-Theft

Správa iOS zařízení prostřednictvím politik

Prostřednictvím Cloud MDM do ESET PROTECT můžete zaregistrovat svá iOS zařízení a následně je spravovat, a to jak v běžném režimu, tak ABM.

Zařízením můžete přiřadit **ESET MDM for iOS / iPadOS** politiku, prostřednictvím které dokážete vynutit firemní politiku a konfigurovat samotné zařízení. Příklad:

- Konfigurace účtu Exchange ActiveSync
- Vynucení omezení používání iOS

Filtrování obsahu webu pro Android zařízení

Prostřednictvím ESET Endpoint Security pro Android nainstalovaným na spravovaných Android zařízeních můžete regulovat přístup k webovým stránkám. Filtrování obsahu webu můžete využít k zamezení přístupu na webové stránky, které mohou porušovat práva duševního vlastnictví, a chránit tak vaši společnost před rizikem právní odpovědnosti. Cílem je zabránit zaměstnancům v přístupu na stránky s nevhodným nebo škodlivým obsahem, případně stránky, které mohou mít negativní vliv na produktivitu práce.

Filtrování obsahu webu pro Android zařízení je dostupný v ESET Endpoint Security pro Android 3.0 a novější.

Filtrování obsahu webu je ve výchozím nastavení vypnuté. Pro zapnutí této funkce si vytvořte novou politiku:

1. V hlavním menu klikněte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.

2. V okně **Nová politika** přejděte do **Nastavení** a vyberte **ESET Endpoint Security for Android**.

3. V politikách v části **Webová ochrana** > rozbalte nabídku Filtrování obsahu webu a klikněte na přepínač **Filtrování obsahu webu**.

4. Definujte seznam povolených nebo blokovaných stránek či kategorií. Pomocí politiky pro filtrování obsahu webu můžete definovat seznam adres pro tři různé kategorie:

- **Seznam blokovaných URL** – přístup na tyto URL bude blokován
- **Seznam povolených URL** – přístup na tyto URL bude povolen
- **Seznam výstražných URL** – při přístupu na URL bude uživatel upozorněn, ale bude mít možnost pokračovat

V každé ze sekcí máte k dispozici následující možnosti pro správu:

- **Přidat** – kliknutím přidáte nový záznam s konkrétní URL adresou

- **Změnit** – po kliknutí můžete upravit existující záznam
- **Odstranit** – kliknutím odstraníte existující záznam ze seznamu
- **Importovat** – po kliknutí importujete seznam URL do dané kategorie
- **Exportovat** – kliknutím exportujete seznam URL z dané kategorie

> Při definováním pravidla, která má regulovat přístup na konkrétní webovou stránku, zadejte do pole **URL** úplnou adresu.
> V poli URL můžete používat zástupné znaky – * (hvězdička) a ? (otazník).
> Při zadání domény bude na základě definované akce přístup povolen nebo blokován k veškerému obsahu na této doméně a všech subdoménách (například `subdomain.domain.com`).

Další možností je povolení/blokování celé sady URL adres na základě kategorie definovaných v části **Pravidla kategorií**.

V dialogovém okně **Pravidla kategorií** vyberte akci platnou pro všechny URL z dané kategorie a dále se rozhodněte, zda se má akce aplikovat též na podkategorie.

- **Povolit** – po vybrání této možnosti povolíte přístup na URL z dané kategorie
- **Blokovat** – po vybrání této možnosti zablokujete přístup na URL z dané kategorie
- **Upozornit** – po vybrání této možnosti bude uživatel upozorněn, že přistupuje na URL z dané kategorie

Správa aktualizací operačního systému

Prostřednictvím ESET Endpoint Security pro Android nainstalovaným na spravovaných Android zařízeních můžete mít pod kontrolou správu aktualizací operačního systému.

> Tato funkce vyžaduje ESET Endpoint Security pro Android verze 3.0, Android verze 8.x a novější. Zařízení s Androidem musí být zaregistrováno v režimu Vlastníka zařízení.

Správu aktualizací operačního systému je možné řídit pomocí politiky:

1. V hlavním menu klikněte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.
2. V sekci **Nastavení** vyberte z rozbalovacího menu jako produkt **ESET Endpoint Security for Android**.
3. V konfigurační šabloně přejděte do sekce **Správa zařízení**, rozbalte část **Správa zařízení** a pomocí přepínače zapněte možnost **Zapnout správu zařízení**.
4. Pro aktivaci správy operačního systému přejděte do sekce **Správa aktualizací systému** a zapněte možnost **Spravovat aktualizace systému**.

V této části můžete definovat různá pravidla týkající se aktualizací operačního systému Android na vámi spravovaných zařízeních:

- **Politika aktualizací systému**:
  - **Automaticky** – aktualizace operačního systému Android se provede bez prodlení.

- **V definovaném intervalu** – aktualizace operačního systému Android se spustí pouze v časovém intervalu nastaveném v části **Interval denní údržby**.
- **Odložené o 30 dní** – aktualizace operačního systému Android se spustí až 30 dní po jejím vydání.

- **Interval denní údržby** – umožňuje nastavit časový interval během kterého se provede aktualizace operačního systému na spravovaném zařízení se systémem Android.
- **Období pozastavené údržby** – umožňuje zadat několik časových období, kdy nelze zařízení aktualizovat.

Vytvoření politiky pro nastavení Exchange ActiveSync účtu v iOS zařízení

Prostřednictvím politik dokážete změnit, přepsat nebo doplnit nastavení iOS zařízení. Tato nastavení platí pro ABM i non-ABM iOS zařízení.

- Nastavení platná pro ABM zařízení jsou označena ikonou 

. Tato nastavení se aplikují pouze na iOS zařízeních zaregistrovaných na Apple ABM portále. V politikách určených pro non-ABM zařízení nedoporučujeme konfigurovat možnosti určené výhradně pro ABM zařízení.
- Některá nastavení se aplikují pouze v případě, že je na zařízení konkrétní verze operačního systému iOS. Tato nastavení jsou označena ikonou představující verzi systému iOS, například iOS verze 11.0 a novější 

.
- Pokud je u nastavení zobrazena ABM ikona a ikona s minimální vyžadovanou verzí iOS, aby se nastavení uplatnilo, musí dojít ke splnění obou podmínek. V opačném případě se nastavení na zařízení nepropíše.

V níže uvedeném příkladu vám vysvětlíme použití iOS MDM politiky pro konfiguraci Microsoft Exchange poštovního účtu:

Prostřednictvím této politiky pro iOS zařízení můžete vzdáleně uživatelům na jejich zařízení nastavit přístup k firemní poště, kontaktů a kalendáři. Přitom není potřeba vytvářet politiku pro každého uživatele, ale stačí vytvořit jednu obecnou, a aplikovat ji iOS zařízení. Stačí k tomu využít uživatelské atributy z Active Directory. V politice je nutné definovat proměnné, například `${exchange_login/exchange}`, které budou následně nahrazeny hodnotami z AD pro daného uživatele zařízení.

Pokud ve své sítě neprovozujete Microsoft Exchange, můžete ručně nastavit přístup k jednotlivým službám jako je **e-mail**, **kalendář**, **databáze kontaktů**, **LDAP účet** nebo **odebíraný kalendář**.

Níže uvádíme příklad, jak vytvořit politiku pro automatické nastavení poštovního účtu na iOS zařízení a s tím souvisejících služeb prostřednictvím Exchange ActiveSync (EAS) protokolu.

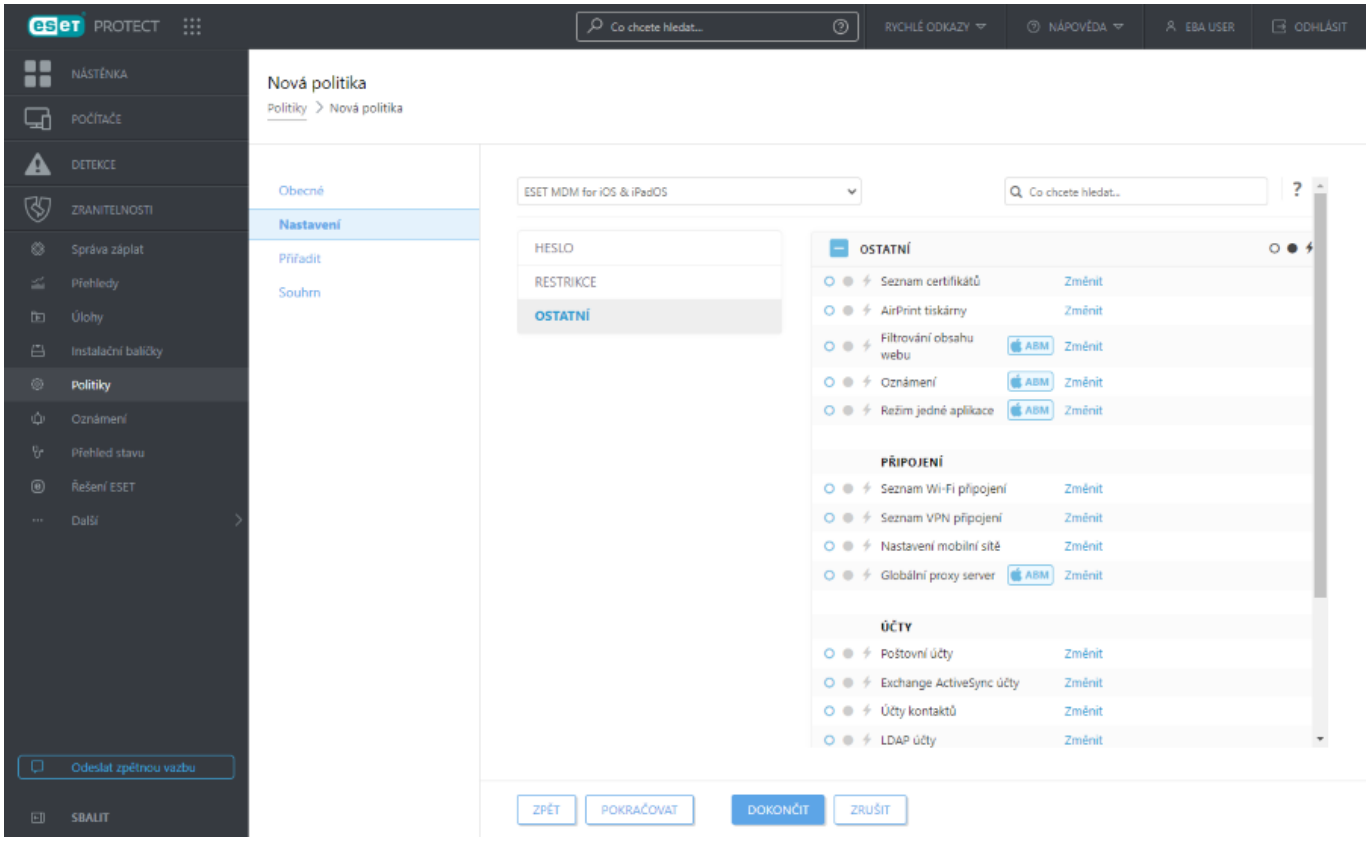
> Než začnete tuto politiku nastavovat, ujistěte se, že jste již provedli kroky popsané v části Registrace mobilních zařízení.

Obecné

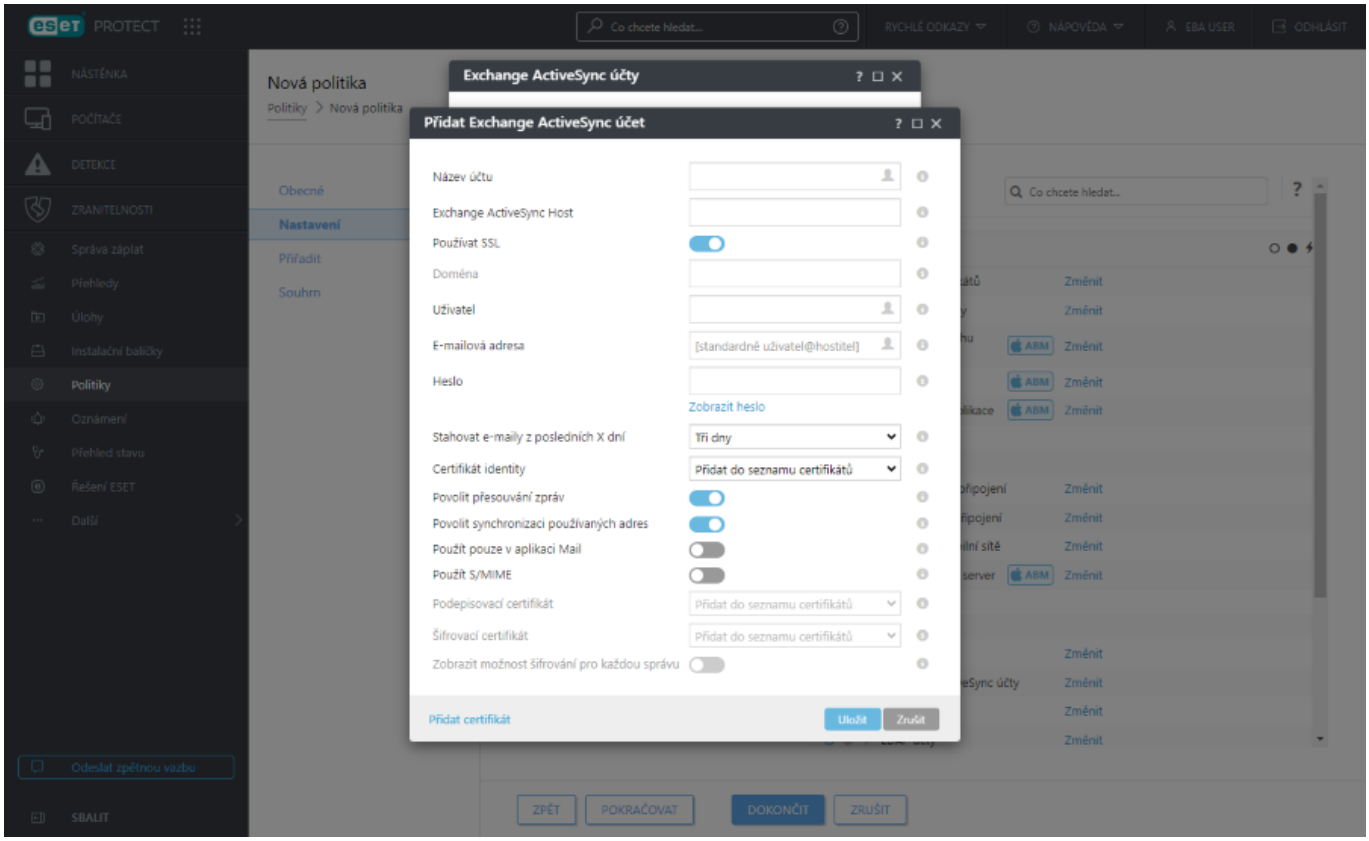
Zadejte **název** nové politiky. Pole **Popis** je nepovinné.

Nastavení

Dále z rozbalovacího menu vyberte **ESET MDM for iOS & iPadOS**, klikněte na **Ostatní** a rozbalte kategorie. Poté klikněte na **Upravit** vedle položky **Exchange ActiveSync účty**.



V zobrazeném dialogovém okně klikněte na tlačítko **Přidat** a vyplňte zobrazená pole. V polích můžete používat proměnné (po kliknutí do pole se zobrazí menu se seznamem formátů), například při definování pro jména uživatele nebo e-mailové adresy. Tyto proměnné budou při aplikování politiky nahrazeny odpovídajícími hodnotami definovanými ve vlastnostech uživatele.



• **Název účtu** – zadejte název Exchange účtu.

• **Exchange ActiveSync Host** – zadejte IP adresu nebo název Exchange serveru.

• **Používat SSL –** tato možnost je standardně zapnutá. Prostřednictvím ní definujte, zda Exchange Server používá při autentifikaci Secure Sockets Layer (SSL).

• **Doména** – toto pole je nepovinné. V případě potřeby můžete specifikovat doménu, do které uživatelský účet patří.

• **Uživatel** – uživatelské jméno Exchange účtu. Z rozbalovacího menu vyberte formát, který bude následně doplněn z atributů uživatele v Active Directory.

• **E-mailová adresa** – z rozbalovacího menu vyberte formát e-mailové adresy, který bude následně doplněn z atributů uživatele v Active Directory.

• **Heslo** – toto pole je nepovinné. Doporučujeme jej ponechat prázdné. V takovém případě bude k zadání hesla vyzván uživatel.

• **Stahovat e-maily za posledních X dní** – z rozbalovacího menu vyberte počet dní, jak dlouho se mají e-maily zůstávat v zařízení.

• **Certifikát identity** – rozhodněte, zda se mají údaje pro připojení do ActiveSync uložit.

• **Povolit přesouvání zpráv** – pokud je tato možnost aktivní, uživatel může zprávy přesouvat z jednoho účtu do druhého.

• **Povolit synchronizaci používaných adres** – pokud je tato možnost aktivní, uživatel může synchronizovat mezi svými zařízeními naposledy použité e-mailové adresy.

• **Použít pouze v aplikaci Mail** – pokud je tato možnost aktivní, zprávy prostřednictvím tohoto poštovního účtu je možné odesílat výhradně z aplikace Mail.

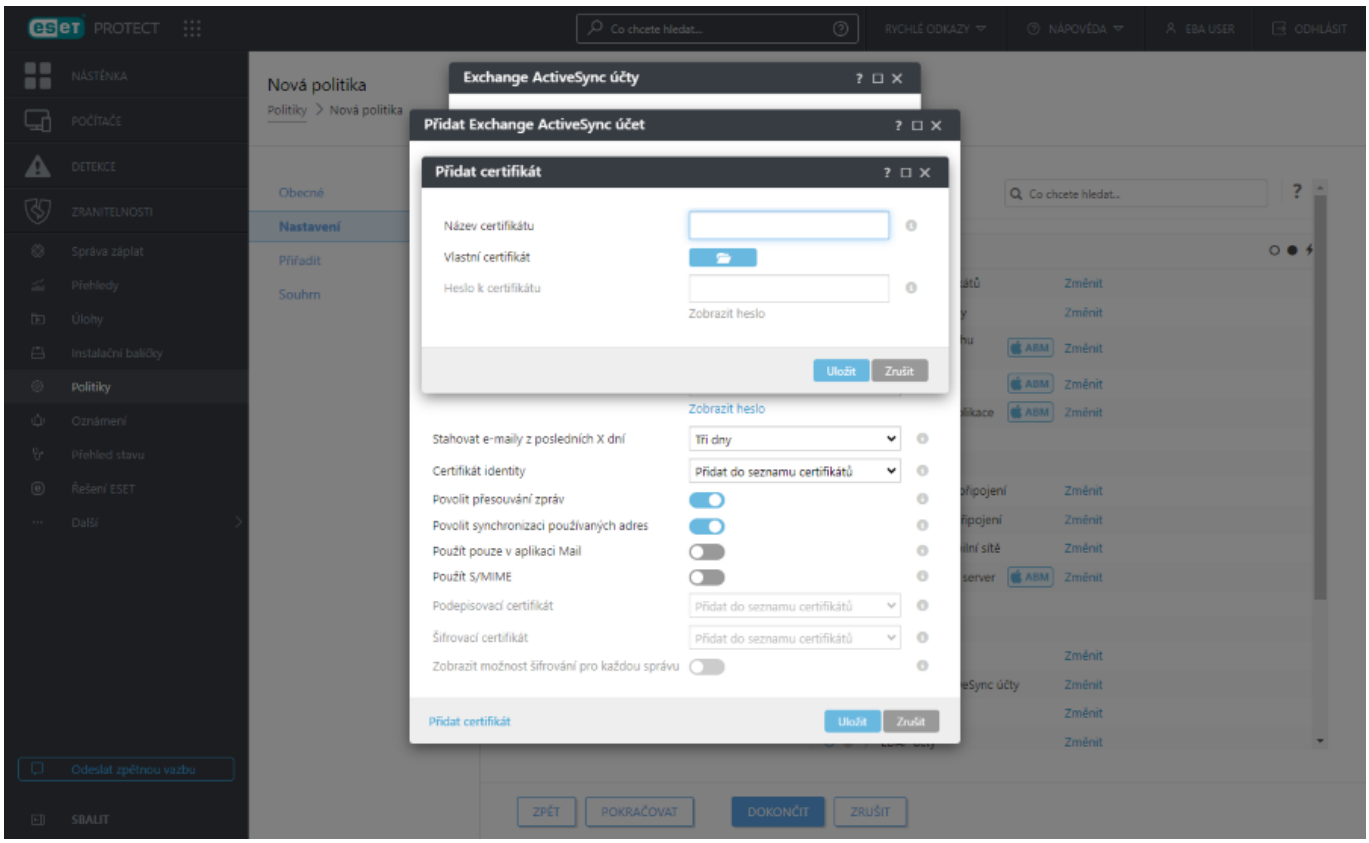
• **Použít S/MIME** – pokud je tato možnost aktivní, odesílané zprávy budou šifrovány prostřednictvím S/MIME.

• **Podepisovací certifikát** – rozhodněte, zda se mají údaje pro podepsání MIME dat uložit.

• **Šifrovací certifikát** – rozhodněte, zda se mají údaje pro zašifrování MIME dat uložit

• **Zobrazit možnost šifrování pro každou zprávu** – pomocí této možnosti můžete ponechat rozhodnutí o šifrování zprávy na uživateli.

Pokud nechcete hodnotu definovat a ponecháte pole prázdné, mobilní zařízení vyzve uživatele k zadání této hodnoty. To je vhodné například v případě **hesla**.

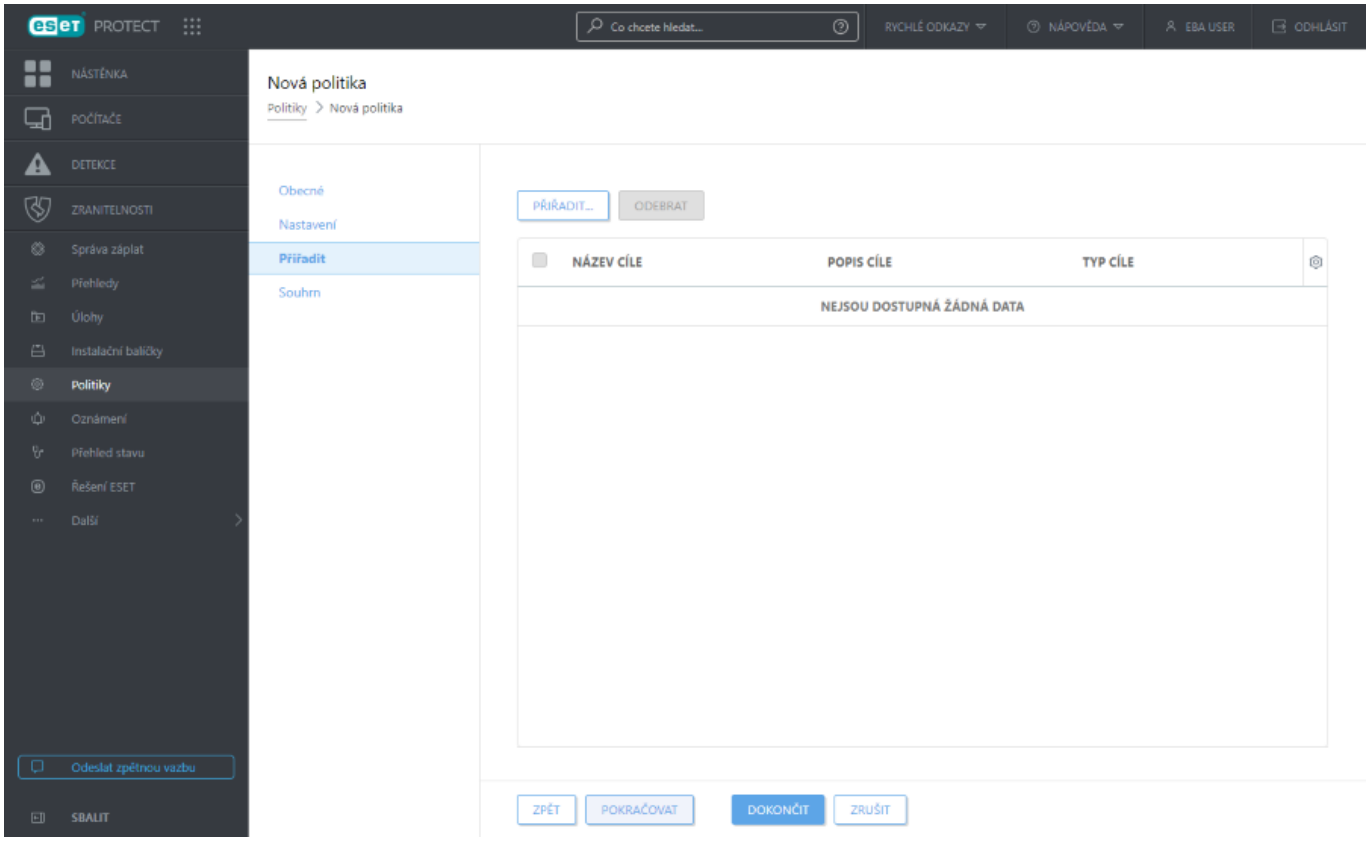


• **Přidat certifikát** – pokud pro ověření identity používáte certifikáty, definujte je v této části.

Pomocí výše uvedených kroků můžete do zařízení přidat více Exchange ActiveSync účtů. To znamená, že na mobilním zařízení bude nakonfigurováno více účtu. Konfiguraci účtu můžete kdykoli upravit.

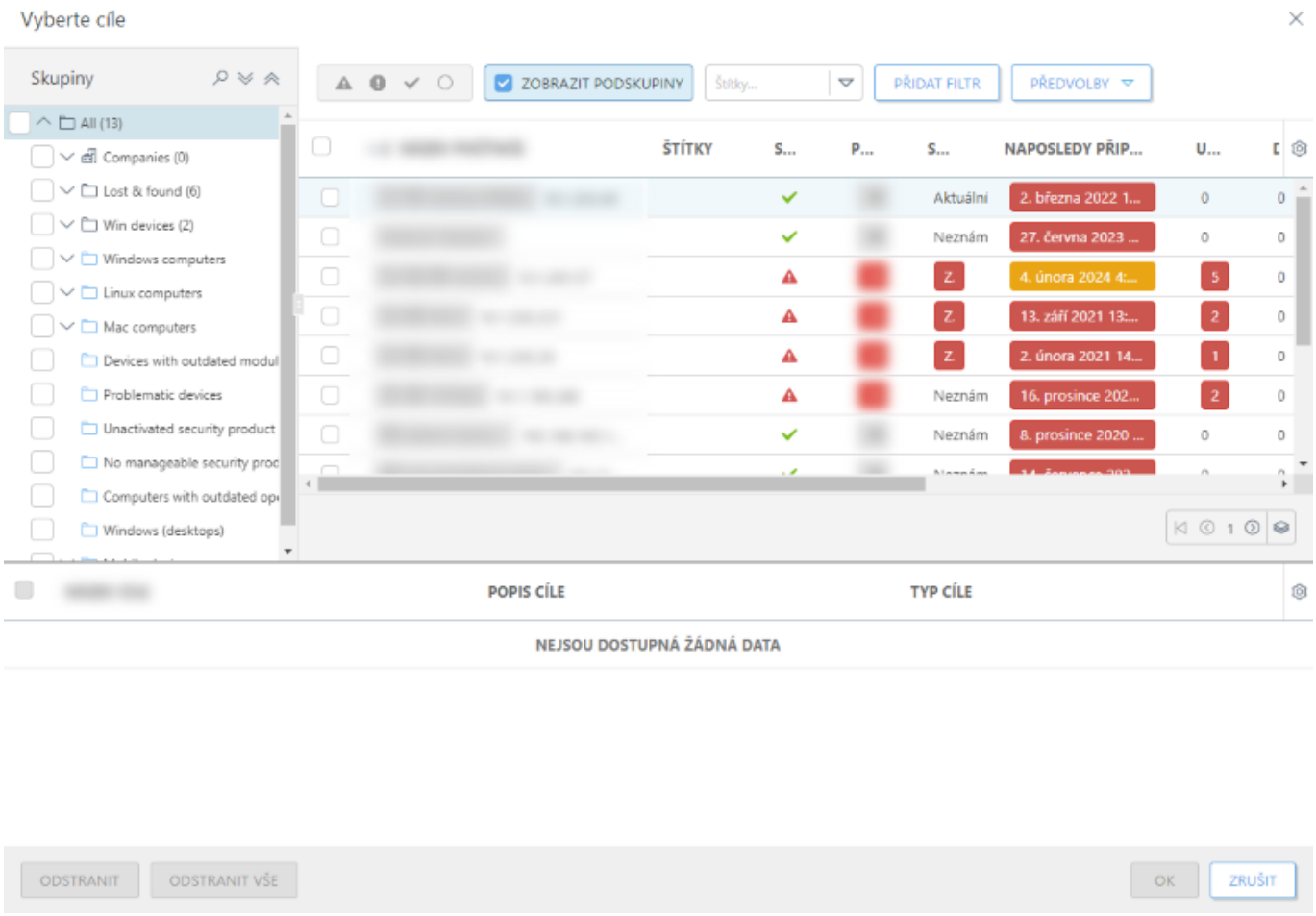
Přiřadit

V této části vyberte cíl (počítač nebo skupinu), kterému chcete danou politiku přiřadit.



Po kliknutí na tlačítko **Přiřadit** se zobrazí dialogové okno se všemi statickými i dynamickými skupinami. Vyberte požadovaný cíl (zařízení nebo skupina) a klikněte na tlačítko **OK**.

Pro zajištění, že se objekt aplikuje na všechna zařízení ve skupině, místo výběru jednotlivých stanic vyberte jako cíl celou skupinu. Zabráníte tím zároveň zpomalení Web Console.
Pokud vyberte velké množství počítačů, Web Console zobrazí varování.



Souhrn

Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**. Politika se na cíl aplikuje při jeho příštím připojení k ESET PROTECT.

Vytvoření politiky pro restrikci iOS zařízení a nastavení Wi-Fi sítě

Prostřednictvím politiky pro iOS mobilní zařízení můžete vynutit restrikce a firemní politiku. Prostřednictvím politiky pro iOS zařízení můžete vzdáleně vynutit jeho konfiguraci a omezit používání některých funkcí. Nastavit můžete například, to znamená, že se zařízení automaticky připojí k firemní bezdrátové sítě. Totéž platí pro VPN připojení.

Pro tvorbu politik určených pro iOS zařízení platí níže uvedená pravidla a doporučení. Zakázat můžete například FaceTime a používání fotoaparátu, stejně tak konkrétní funkce iCloud, případně přizpůsobit možnosti zabezpečení a ochrany soukromí vašim potřebám nebo deaktivovat vybrané aplikace.

> Mějte na paměti, že některé restrikce se nemusí uplatnit na starších verzích iOS. Všechny možnosti podporuje iOS 8 a novější.

Na následujícím příkladu si ukážeme, jak vytvořit politiku, která zabrání uživatelům používání **fotoaparátu**, aplikace **FaceTime**, a nastaví parametry Wi-Fi pro automatické připojení k firemní bezdrátové síti, pokud je v dosahu. Vybráním možnosti Automaticky připojit zajistíte automatické připojení iOS zařízení k této síti. Mějte na

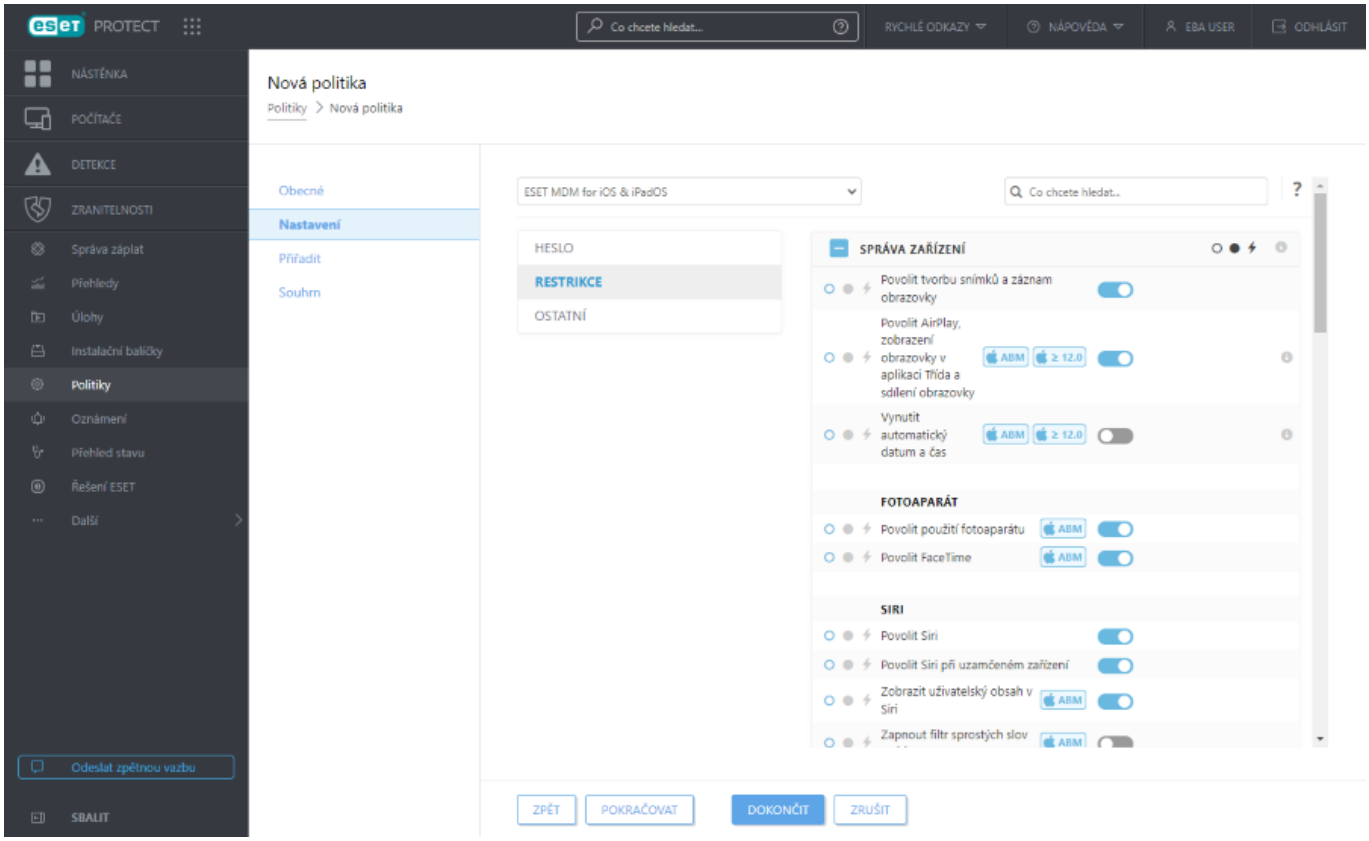
paměti, že politika je vždy nadřazena uživatelskému nastavení.

Obecné

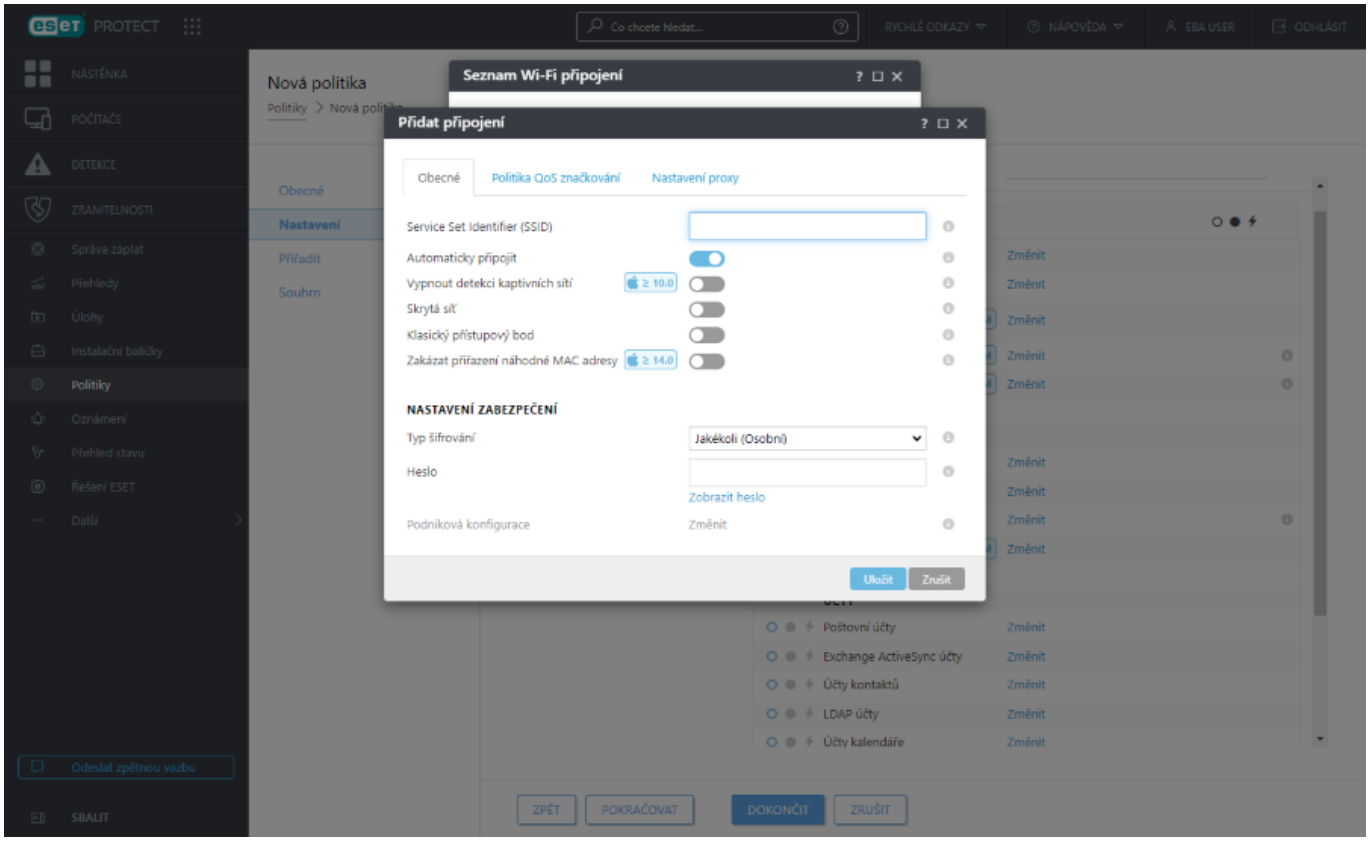
Zadejte **název** nové politiky. Pole **Popis** je nepovinné.

Nastavení

Vyberte **ESET MDM for iOS & iPadOS**, klikněte na **Restrikce** a zobrazte kategorie. Pro vypnutí klikněte na přepínač vedle **Povolit použití fotoaparátu**. Všimněte si, že se zároveň deaktivovala možnost pro aktivaci aplikace FaceTime, protože ta nemůže fungovat bez fotoaparátu. Pokud chcete zakázat pouze FaceTime, ponechte zapnutou možnost pro použití fotoaparátu a pomocí přepínače vypněte pouze možnost **Povolit FaceTime**.



Pro konfiguraci **restrikcí** přejděte do části **Ostatní** a klikněte na **Změnit** u položky **Seznam Wi-Fi připojení**. Následně se zobrazí seznam Wi-Fi připojení. Klikněte na tlačítko **Přidat** a definujte detaily Wi-Fi sítě. Konfiguraci uložte kliknutím na tlačítko **Uložit**.



- **Service Set Identifier (SSID)** – zadejte SSID bezdrátové sítě.

- **Automaticky připojovat** – pokud je tato možnost aktivní (standardně zapnuta), zařízení se automaticky připojí k této síti, pokud je v dosahu.

Nastavení zabezpečení

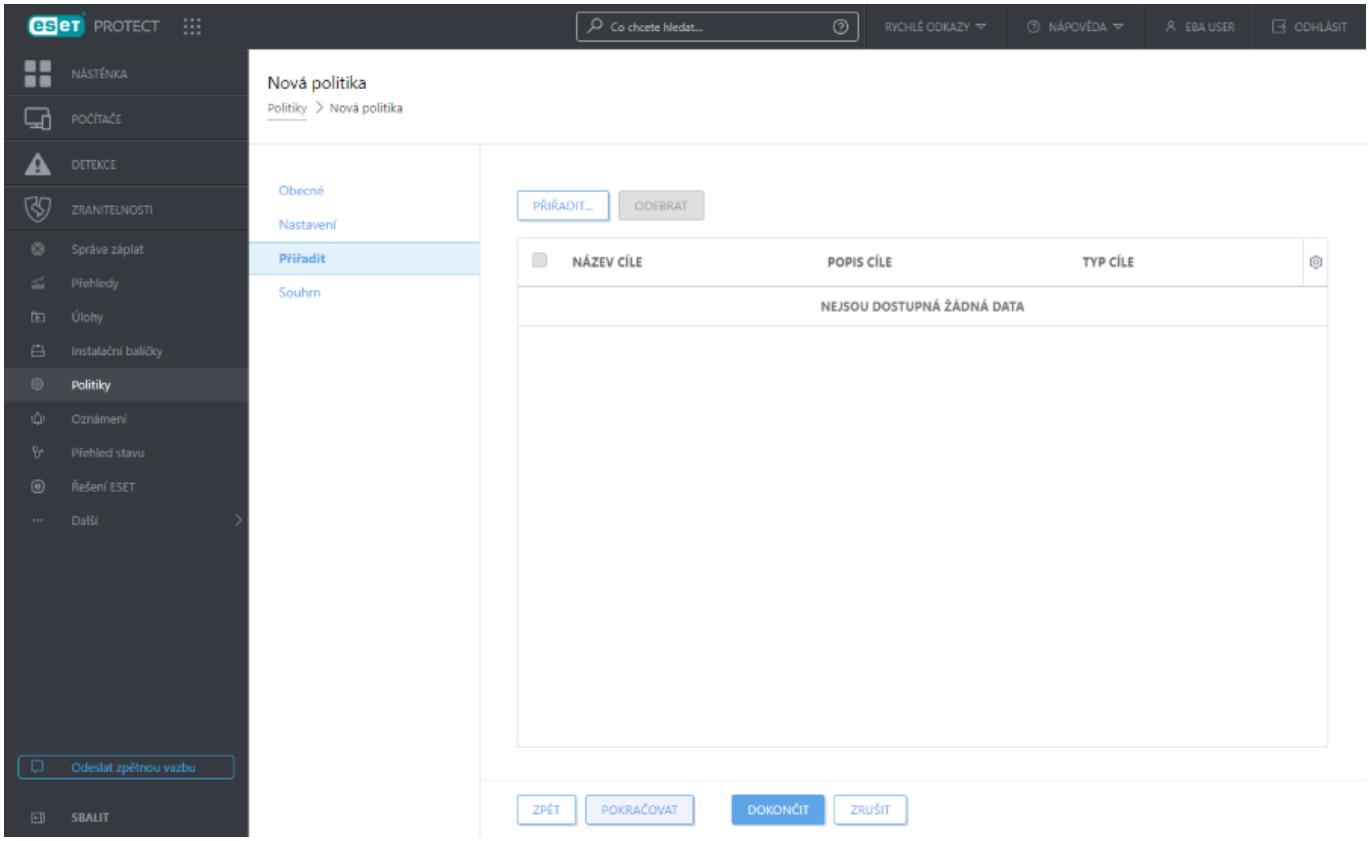
- **Typ šifrování** – z rozbalovacího menu vyberte způsob šifrování a ujistěte se, že odpovídá parametrům Wi-Fi sítě.

- **Heslo** – do tohoto pole zadejte heslo pro přístup do sítě.

Nastavení proxy – nepovinné. Pokud ve své síti používáte pro přístup do internetu proxy, nastavte ji v této části.

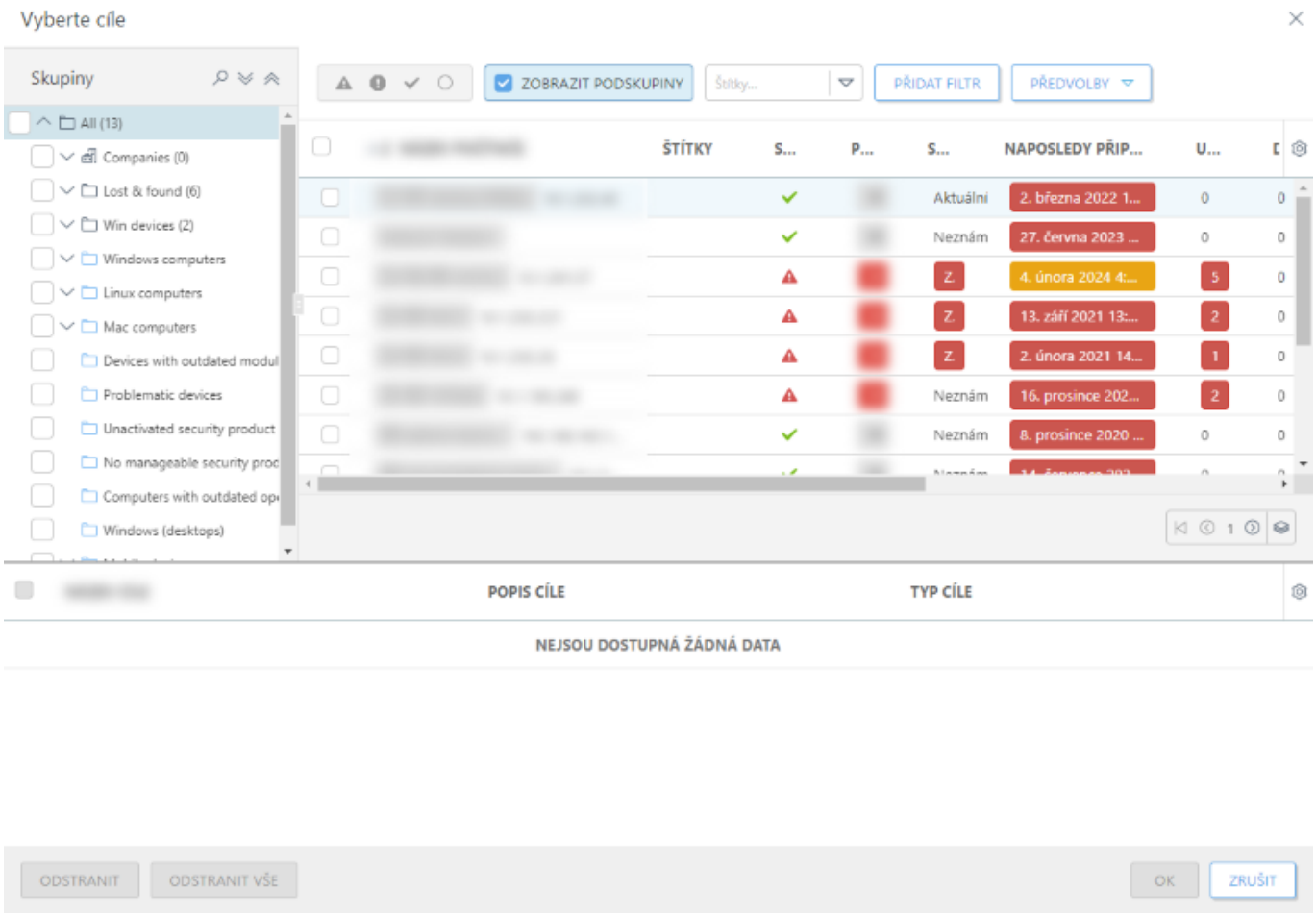
Přiřadit

V této části vyberte cíl (počítač nebo skupinu), kterému chcete danou politiku přiřadit.



Po kliknutí na tlačítko **Přiřadit** se zobrazí dialogové okno se všemi statickými i dynamickými skupinami. Vyberte požadovaný cíl (zařízení nebo skupina) a klikněte na tlačítko **OK**.

Pro zajištění, že se objekt aplikuje na všechna zařízení ve skupině, místo výběru jednotlivých stanic vyberte jako cíl celou skupinu. Zabráníte tím zároveň zpomalení Web Console.
Pokud vyberte velké množství počítačů, Web Console zobrazí varování.



Souhrn

Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**. Politika se na cíl aplikuje při jeho příštím připojení k ESET PROTECT.

Konfigurační profily Cloud MDM

Prostřednictvím profilů můžete vzdáleně vynutit konfiguraci mobilního iOS zařízení a uživateli automaticky nastavit přístup k e-mailům atp.

Název profilu	Krátký popis
Heslo	V této části můžete definovat bezpečnostní politiku pro zámek obrazovky. Tím zajistíte ochranu firemních dat uložených ve spravovaném zařízení. Pokud uplatňujete více politik na heslo, použije se nejrestriktivnější z nich.
Restrikce	Uživatelům můžete omezit používání aplikací jako je iTunes nebo naopak vynutit zálohování či šifrování obsahu zařízení. Mějte na paměti, že některé možnosti se aplikují pouze na iOS 8 a novější.
Seznam Wi-Fi připojení	Profily Wi-Fi přenášejí firemní nastavení Wi-Fi přímo do spravovaných zařízení pro okamžitý přístup.

Název profilu	Krátký popis
Seznam VPN připojení	Uživatelům můžete do jejich zařízení nakonfigurovat VPN profil pro vzdálený zabezpečený přístup do vaší firemní sítě. **Název připojení** – zadejte název profilu, jak jej uvidí uživatel na zařízení. **Typ připojení** – nejprve vyberte způsob připojení. Následně v závislosti na vybraném typu vyplňte potřebné parametry. **Server** – zadejte IP adresu nebo název VPN serveru.
Poštovní účty	V této části můžete uživateli nastavit jeho IMAP/POP3 poštovní účet.
Exchange ActiveSync účty	ProfilyExchange ActiveSync umožňují koncovým uživatelům přístup ke své firemní poště. Mějte na paměti, že existují předvyplněná pole pro vyhledávání a možnosti, které platí pouze pro iOS 5+.
CalDAV – účty kalendářů	Uživatelům můžete nastavit přístup ke CalDAV kalendáři a zajistit jeho automatickou synchronizaci.
CardDAV – účty kontaktů	V této části můžete konfigurovat CardDAV služby.
Odebírané kalendáře	Pokud uživatelům nadefinujete CalDAV kalendáře, v této části můžete specifikovat úroveň oprávnění.

Migrace do Cloud MDM (z ESET PROTECT On-Prem)

Následující kroky vám pomohou s migrací mobilních zařízení z ESET PROTECT On-Prem do prostředí ESET PROTECT:

Předpoklady

- Pracovní prostředí ESET PROTECT On-Prem s komponentou Správa mobilních zařízení
- Jak pracovat s prostředím ESET PROTECT
- Účet ESET PROTECT s oprávněním **superuživatele**

Omezení

- Migrace je možná pouze u zařízení s OS Android
- Tato migrace vyžaduje ESET Endpoint Security pro Android ve verzi 3.5 a vyšší a ESET PROTECT On-Prem ve verzi 10.0 a vyšší
- Migrace spravovaných zařízení s iOS vyžaduje ruční zrušení registrace v ESET PROTECT On-Prem a novou registraci v ESET PROTECT

1. Otevřete webovou konzoli ESET PROTECT.
2. Klikněte na **Více** > **Nastavení** > **Migrace mobilních zařízení z ESET PROTECT On-Prem**.
3. Po dokončení migrace vyberte **licenci**, kterou chcete použít pro aktivaci spravovaných mobilních zařízení.
4. Zároveň po dokončení vyberte **nadřazenou skupinu** pro počáteční umístění zařízení.
5. **Limit použití tokenu** – pomocí migračního tokenu můžete omezit počet migrovaných zařízení.

Pokud spravujete velké množství mobilních zařízení, doporučujeme vám, abyste si nejprve vyzkoušeli proces migrace na malém počtu zařízení. Díky tomu zjistíte, zda migrace probíhá bez problémů. Navázat pak můžete migrací zbývajících mobilních zařízení.

6. Výběrem možnosti **Generovat token** vygenerujete migrační token s nastavenými parametry procesu

migrace.

Vygenerovaný token platí 14 dní. K dispozici je do doby, než opustíte stránku. Dokud si token nezkopírujete, stránku neopouštějte, ani ji neobnovujte.

7. Migrační token se zobrazí v poli níže jako řetězec znaků. Zkopírujte si jej do textového editoru.

8. Otevřete webovou konzoli ESET PROTECT On-Prem.

9. V hlavním menu klikněte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.

10. V sekci **Obecné** vyplňte **název** a **popis** politiky. Na základě této politiky dojde k migraci aktuálně spravovaných mobilních zařízení z on-premises prostředí do prostředí cloudu.

11. V sekci **Nastavení** vyberte **ESET Mobile Device Connector**.

12. V sekci **Obecné** > **Migrace do ESET PROTECT** > vložte migrační token do textového pole **Token pro migraci**.

13. V sekci **Přiřadit** vyberte zařízení, na kterém je spuštěn Mobile Device Connector.

14. Jakmile dojde k aplikaci politiky, zahájí se proces migrace.

Server použije migrační politiku na každé spravované mobilní zařízení, které se od tohoto okamžiku připojí. Zajistěte, aby se všechna spravovaná mobilní zařízení připojila k serveru po dobu platnosti migračního tokenu (po dobu následujících 14 dní). Pokud se zařízení v tomto období nepřipojí, nedojde k migraci a bude nutné ji opakovat.

15. Migrační proces můžete sledovat ve webové konzoli ESET PROTECT. Po migraci se mobilní zařízení připojí k ESET PROTECT a bude viditelné v sekci **Počítače** ve webové konzoli ESET PROTECT.

16. Po úspěšné migraci zařízení do prostředí ESET PROTECT jej můžete bezpečně odebrat z webové konzole ESET PROTECT On-Prem.

17. Po úspěšné migraci všech mobilních zařízení do prostředí ESET PROTECT můžete bezpečně vypnout komponentu Správa mobilních zařízení.

Migrační scénáře ESET PROTECT

Scénáře pro přechod na ESET PROTECT.

V této kapitole se podíváme na možné scénáře zahrnující přechod z jiných řešení ESET na ESET PROTECT. Klikněte na odkaz, který nejlépe vystihuje váš případ.

1. Mám ve své síti nespravované produkty ESET Endpoint a chci je začít spravovat prostřednictvím ESET PROTECT.

2. Aktuálně používám ve své síti ESET PROTECT On-Prem a chci přejít na ESET PROTECT.

3. V současné době spravuji svou síť pomocí ESET PROTECT a chci přejít na ESET PROTECT.

Pokud máte spravovaná zařízení zašifrovaná prostřednictvím ESET Full Disk Encryption, postupujte podle následujících kroků, abyste zabránili ztrátě dat pro obnovení šifrování.
1.Před zahájením migrace přejděte do sekce **Stav serveru** > **Šifrování**. Naleznete zde možnost pro **exportování dat pro obnovení šifrování**.
2.Po dokončení migrace tento soubor s **daty pro obnovení šifrování** následně **importujte** do nové konzole pro vzdálenou správu.
V případě, že tyto kroky nemůžete provést, dešifrujte stanice před zahájením migrace. Po dokončení migrace je následně zašifrujte z webové konzole ESET PROTECT.

Mám ve své síti nespravované produkty ESET Endpoint a chci je začít spravovat prostřednictvím ESET PROTECT.

Prostřednictvím Live Installer není možné aktualizovat serverové produkty ESET ve verzi 4.5 a starší. Pro aktualizaci při přechodu na ESET PROTECT musíte mít nainstalovány produkty ve verzi 6 a novější.

Podle níže uvedených kroků identifikujte a přidejte nespravované stanice do ESET PROTECT:

1. Vytvořte si svou ESET PROTECT instanci.

2. Vytvořte si nový instalační balíček s ESET Endpoint produktem, který již používáte ve své síti.

3. V případě potřeby do balíčku přidejte politiku a definovat můžete také skupinu, do které zařízení přidá po připojení k serveru. Pokud součástí balíčku nebude žádná politika, a ani není žádná aplikovaná na skupinu v ESET PROTECT, aktuální konfigurace produktu ESET Endpoint zůstane beze změny. Později si ji můžete exportovat a následně převést do politiky.

4. Nasaďte instalační balíček na stanice ve vaší síti. Live Installer na ně nainstaluje ESET Management Agenta a aktualizuje existující produkt ESET Endpoint.

Live Installer vyžaduje přímý přístup k internetu pro stažení vyžadovaných komponent. Po dokončení instalace můžete produkt nastavit tak, aby komunikoval prostřednictvím proxy serveru.

5. Po úspěšném dokončení instalace a připojení zařízení k ESET PROTECT můžete začít spravovat tato zařízení pomocí ESET PROTECT.

6. Pokud součástí instalačního balíčku nebyla žádná politika, případně není v ESET PROTECT přiřazena skupině či zařízení, můžete nyní ji vytvořit na základě konfigurace právě nainstalovaného produktu.

7. Pro provedení této akce přejděte do sekce **Úlohy** a vytvořte novou úlohu z kategorie Export spravovaného produkt.

8. V sekci **Nastavení** vyberte z rozbalovacího menu **Produkt: Vše**. Jako **Cíl** úlohy vyberte všechna zařízení, ze kterých chcete exportovat konfiguraci.

9. Vyčkejte na spuštění úlohy na všech vybraných zařízeních.

10. Na konkrétním zařízení přejděte do sekce **Detaily** > **Konfigurace** a otevřete konfiguraci požadovaného produktu.

11. Následně uvidíte exportované nastavení produktu. Pokud vám vyhovuje, klikněte na tlačítko **Převést do**

politiky.

12. Otevře se průvodce vytvořením politiky, ve kterém upravte **název** politiky, případně upravte některá nastavení, a politiku uložte kliknutím na tlačítko **Dokončit**.

13. Tento postup opakujte pro každý bezpečnostní produkt.

14. Po převedení konfigurací všech produktů do politiky můžete pokračovat jejich přiřazením odpovídajícím klientům. Tím vynutíte stejné nastavení a uživatelům zabráníte v jeho modifikaci.

Částečná migrace z ESET PROTECT On-Prem na ESET PROTECT

Migrace z on-premise serveru ESET PROTECT na ESET PROTECT je pouze částečná – viz tabulka níže:

Můžete migrovat:	Migrovat nelze:
• ESET Management Agenty (spravované počítače) • statické skupiny • politiky • šablony dynamických skupin • šablony přehledů • mobilní zařízení (pouze Android)	• celou databázi • dynamické skupiny (můžete však migrovat šablony dynamických skupin) • detekce • audit log • oznámení • úlohy a podmínky spuštění • instalační balíčky • naplánované/vygenerované přehledy (můžete však migrovat šablony přehledů) • štítky • mobilní zařízení s iOS

ESET PROTECT nepodporuje ESET Inspect On-Prem, podporuje však ESET Inspect. Při migraci z ESET PROTECT On-Prem do ESET PROTECT nebudete moci spravovat ESET Inspect On-Prem z ESET PROTECT, můžete však spravovat ESET Inspect z ESET PROTECT.

Při migraci z on-premise serveru ESET PROTECT na ESET PROTECT postupujte podle následujících kroků:

Pokud máte účet MSP, postupujte podle kroků uvedených v návodu Migrace MSP do cloudu.

I. Vytvoření nové instance ESET PROTECT

II. Migrace politik z ESET PROTECT On-Prem do ESET PROTECT

III. Migrace šablon dynamických šablon skupin z ESET PROTECT On-Prem do ESET PROTECT

IV. Migrace šablon přehledů z ESET PROTECTOn-Prem do ESET PROTECT

V. Migrace spravovaných počítačů z ESET PROTECT On-Prem do ESET PROTECT

V.I. Migrace struktury statický skupin pomocí nástroje pro export počítačů

V.II. Migrace spravovaných počítačů (ESET Management Agentů) pomocí politiky pro migraci

VI. Migrace mobilních zařízení

VII. Vytvoření ESET PROTECT uživatelů v ESET Business Account

VIII. Namapování ESET Business Account uživatelů ve webové konzoli ESET PROTECT

IX. Vyřazení on-premise serveru ESET PROTECT z provozu

Řešení problémů po migraci

Pokud máte spravovaná zařízení zašifrovaná prostřednictvím ESET Full Disk Encryption, postupujte podle následujících kroků, abyste zabránili ztrátě dat pro obnovení šifrování.
1.Před zahájením migrace přejděte do sekce **Stav serveru** > **Šifrování**. Naleznete zde možnost pro **exportování dat pro obnovení šifrování**.
2.Po dokončení migrace tento soubor s **daty pro obnovení šifrování** následně **importujte** do nové konzole pro vzdálenou správu.
V případě, že tyto kroky nemůžete provést, dešifrujte stanice před zahájením migrace. Po dokončení migrace je následně zašifrujte z webové konzole ESET PROTECT.

Neexportujte žádné politiky pro ESET Management Agenta.
Před migrací se ujistěte, že jste pro Agenta zcela zrušili přiřazení všech aktivních politik.

I. Vytvoření nové instance ESET PROTECT

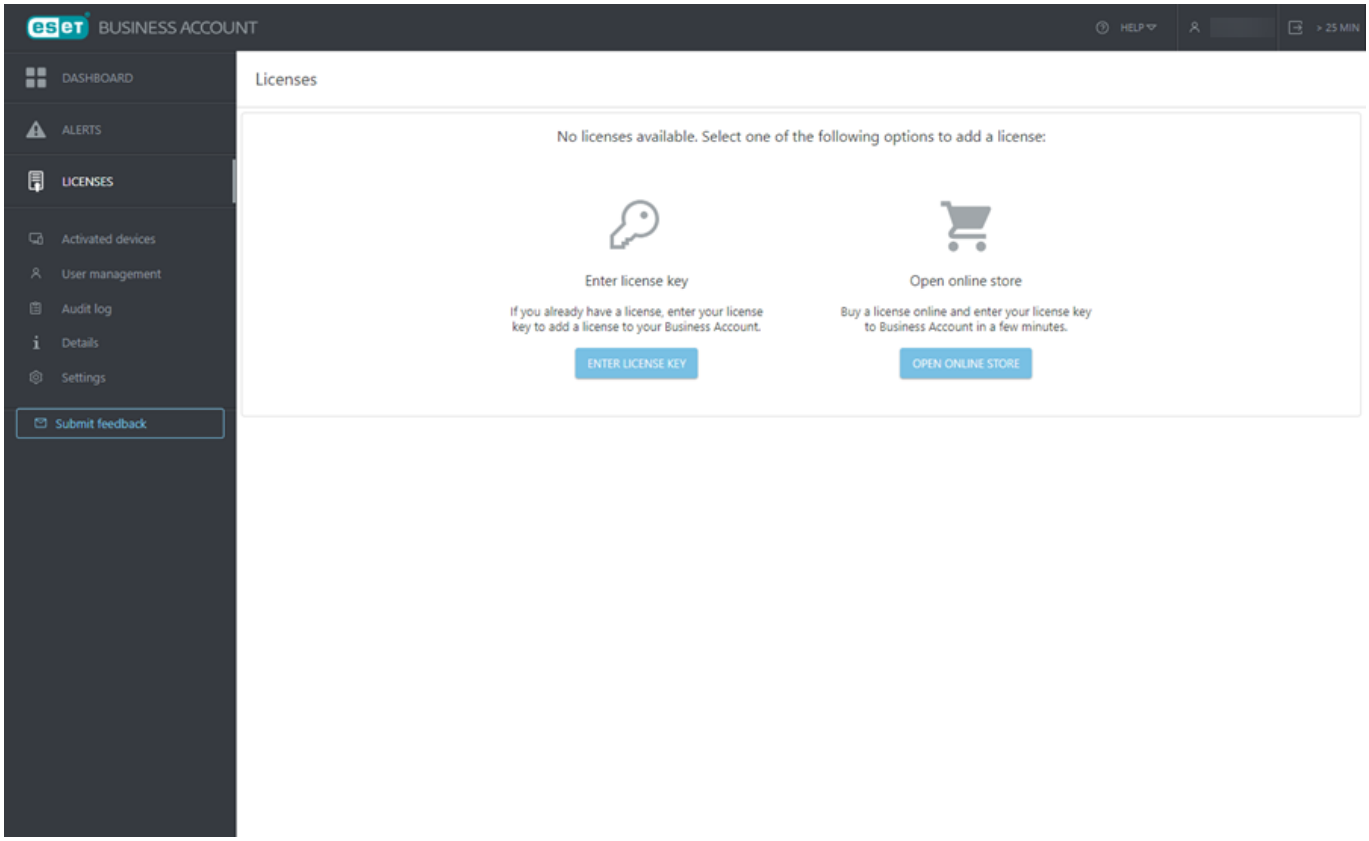
Požadavky

- Vytvořený účet superuživatele na portále ESET Business Account.
- Přidaná vhodná licence pro ESET PROTECT.

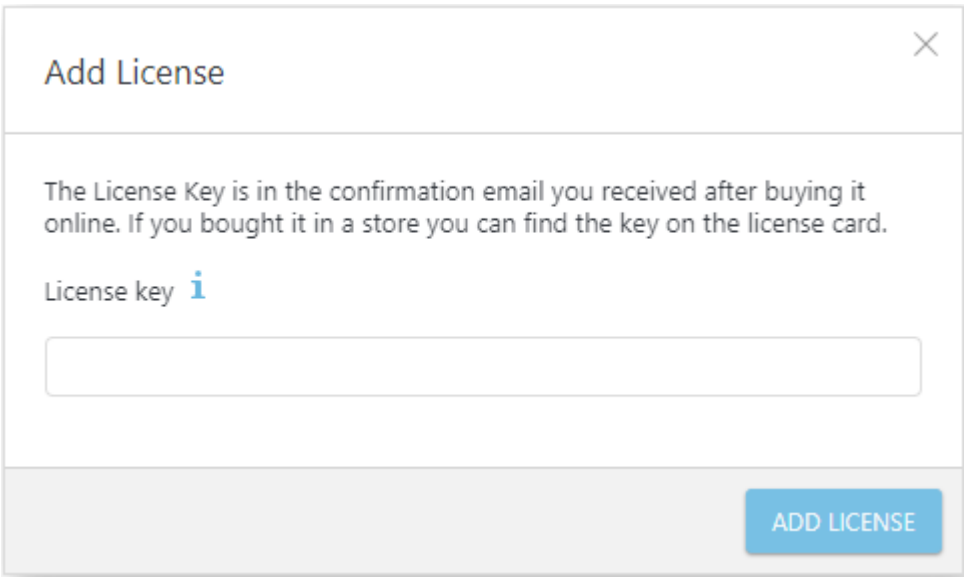
Pokud máte na stejnou e-mailovou adresu založen EBA i EMA2 účet, ESET PROTECT je možné aktivovat pouze z jednoho účtu. Aktivovat nebo odstranit instanci budete schopni výhradně prostřednictvím účtu (EBA nebo EMA2), který si vyberete pro vytvoření ESET PROTECT instance.

Vytvoření nové instance ESET PROTECT

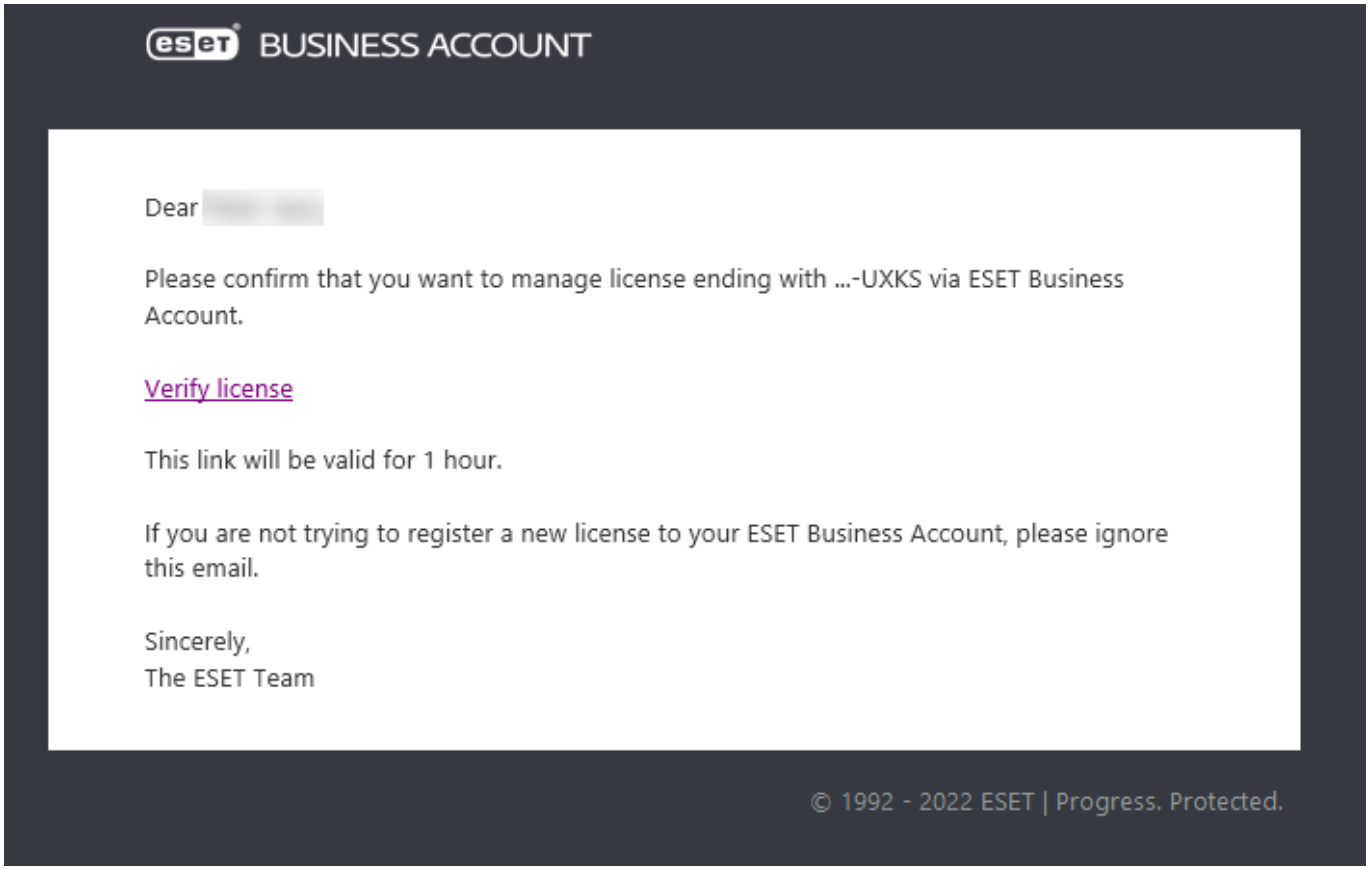
1. Přihlaste na portál ESET Business Account. Pokud zatím účet nemáte, vytvořte si jej.
2. V hlavním menu přejděte na záložku **Licence** a klikněte na tlačítko **Zadat licenční klíč**.



3. V dialogovém okně **Přidat licenci** zadejte **licenční klíč** pro ESET PROTECT a klikněte na tlačítko **Přidat licenci**.



4. Následně obdržíte ověřovací e-mail. V případě, že vám nedorazí, postupujte podle kroků uvedených v Databázi znalostí. V e-mailu klikněte na odkaz **Ověřit licenci**.



5. Na **Nástěnce** se vám následně zpřístupní možnost pro **aktivaci ESET PROTECT**. Pokračujte kliknutím na **Aktivovat**.

⚠ Ověřte nastavení vašeho jazyka ve vašem účtu na portále ESET Business Account. Některé části produktu a předdefinované objekty ESET PROTECT se vytvoří v jazyce, který máte nastaven v ESET Business Account, a není možné jej později změnit.

6. Zobrazí se dialogové okno pro **aktivaci ESET PROTECT**. Přečtěte si a odsouhlaste podmínky použití.

7. Vyberte datové centrum nejbližší vámi spravované síti, ve kterém chcete vytvořit instanci, a klikněte na tlačítko **Pokračovat**.

⚠ Jakmile provedete potvrzení, nebude možné změnit datové centrum vaší instance.

8. Instance ESET PROTECT bude vytvořena. Vyčkejte několik minut, případně se můžete i odhlásit. Jakmile bude uvedena do provozu, zašleme vám upozornění e-mailem.

9. Klikněte na tlačítko **Pokračovat**. Může také na **Nástěnce** kliknout na tlačítko **Otevřít**. V nové záložce prohlížeče se otevře ESET PROTECT Web Console.

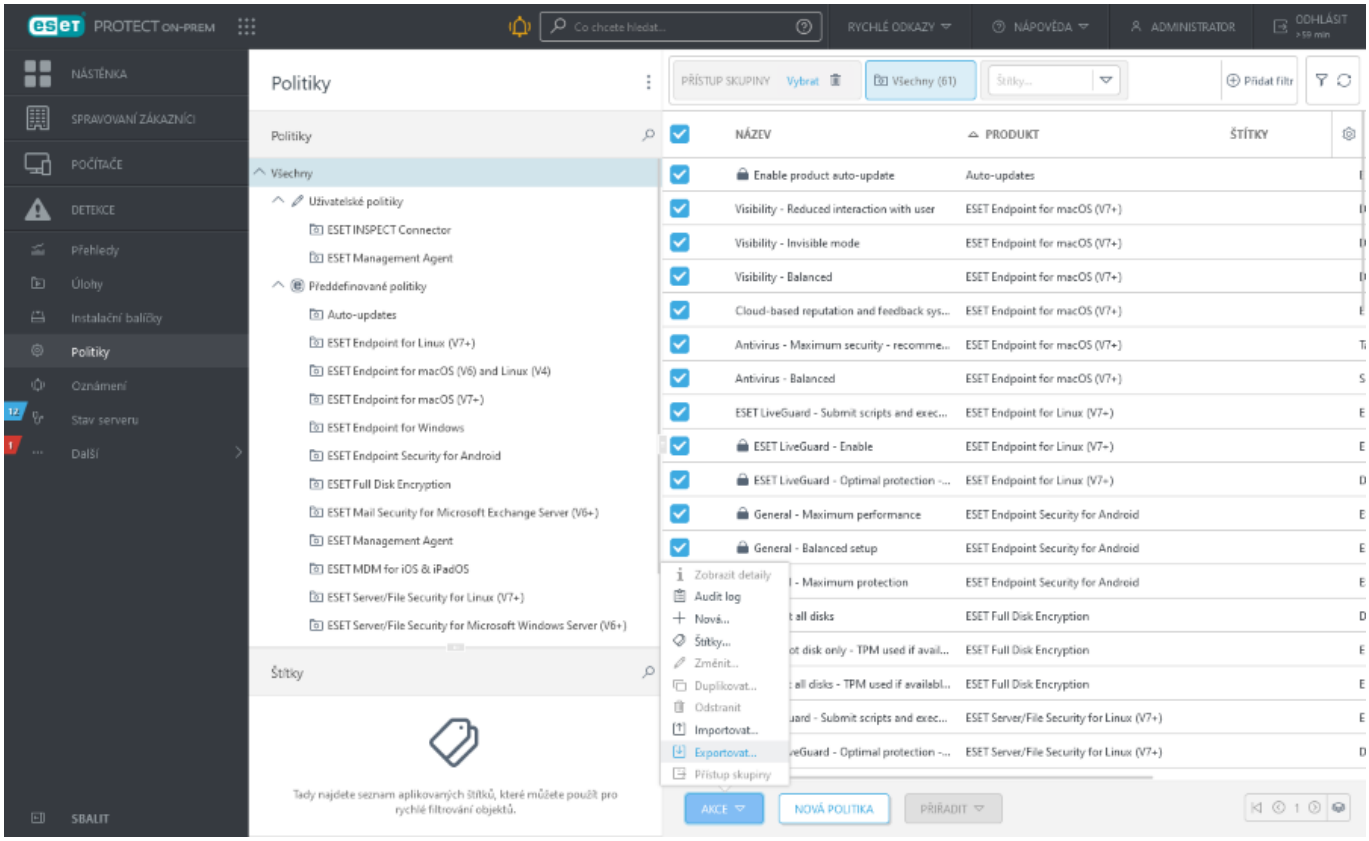
ESET PROTECT synchronizuje strukturu z ESET Business Account a ve Web Console je v sekci **Počítače** reprezentována jako strom statických skupin.

II. Migrace politik z ESET PROTECT On-Prem do ESET PROTECT

1. Přihlaste se ke svému účtu ESET PROTECT On-Prem.

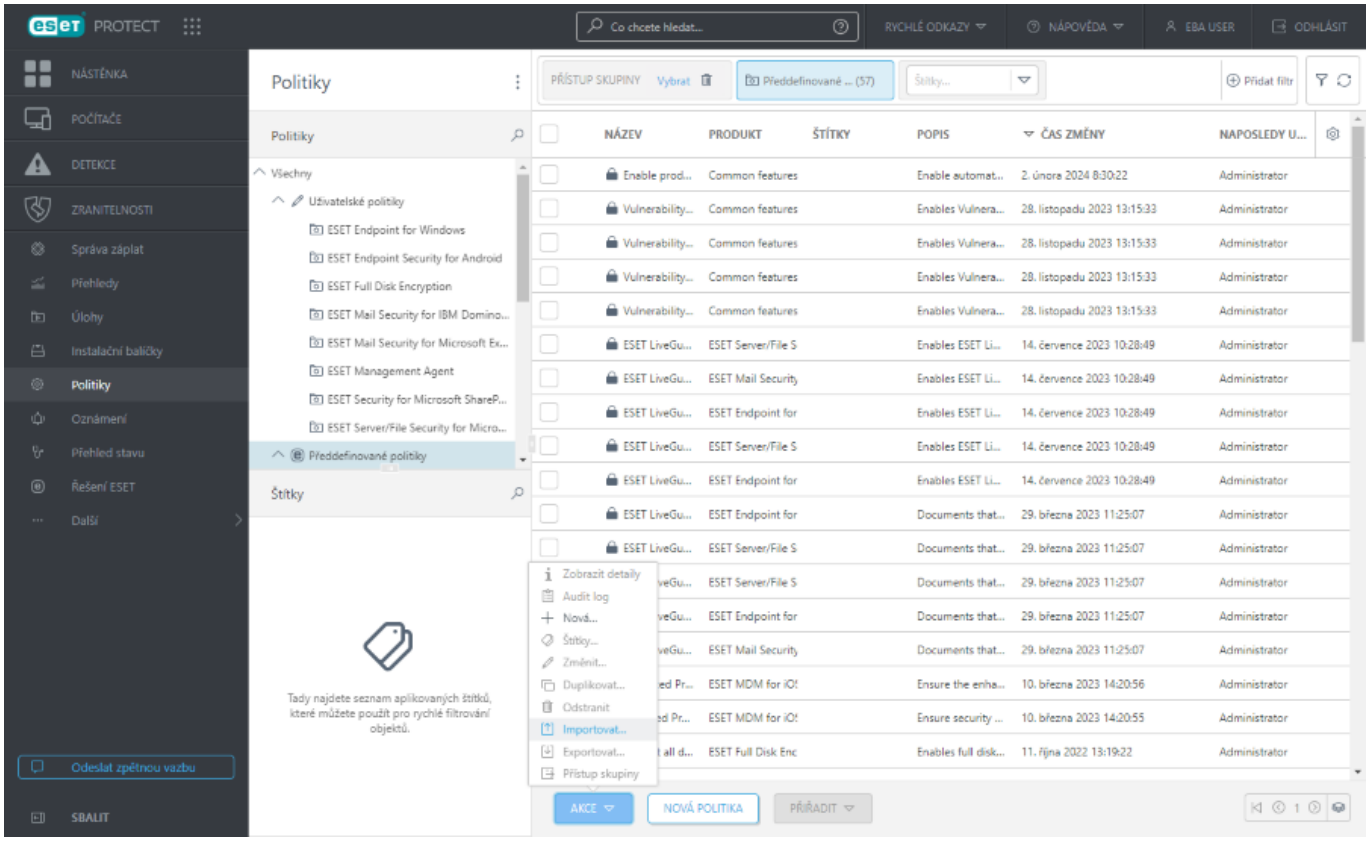
2. V ESET PROTECTOn-Prem zvolte **Politiky** > **Všechny** > zaškrtněte políčko v záhlaví tabulky (nebo zaškrtněte políčka u politik, které chcete exportovat, a klikněte na **Akce** > **Exportovat**.

> Neexportujte žádné politiky pro ESET Management Agenta.
> Před migrací se ujistěte, že jste zcela zrušili přiřazení všech aktivních politik pro Agenta.



3. Uložte si *.dat* soubor obsahující politiky.

4. V ESET PROTECT zvolte **Politiky** > **Akce** > **Importovat** a vyberte soubor *.dat* se seznamem politik exportovaných z ESET PROTECTOn-Prem v kroku číslo 2 a kliknutím na **Importovat** je naimportujte do ESET PROTECT.



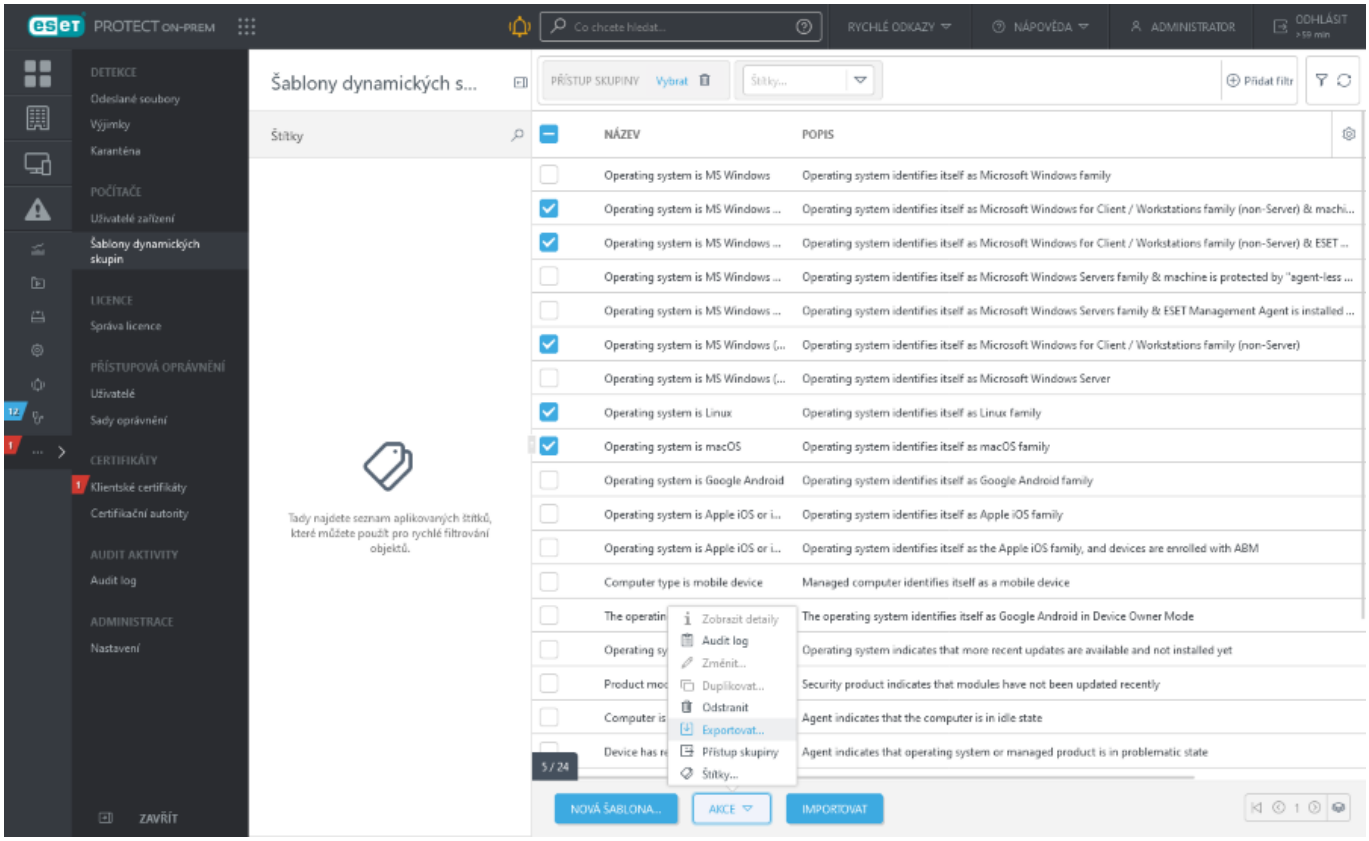
5. Importované politiky se zobrazí v sekci **Uživatelské politiky**. Po migraci zařízení z ESET PROTECT On-Prem do ESET PROTECT nebudou zachovány politiky, které byly přiřazeny zařízením v ESET PROTECT On-Prem. Po importování politik do ESET PROTECT je ručně přiřaďte počítačům v ESET PROTECT.

Při aplikování politik buďte opatrní:
a)V ESET PROTECT On-Prem: Pro každý počítači si vytvořte seznam aplikovaných politik a jejich pořadí.
b)V ESET PROTECT: Aplikujte politiky na jednotlivá zařízení na základě nastavení politiky v ESET PROTECTOn-Prem.

III. Migrace šablon dynamických šablon skupin z ESET PROTECT On-Prem do ESET PROTECT

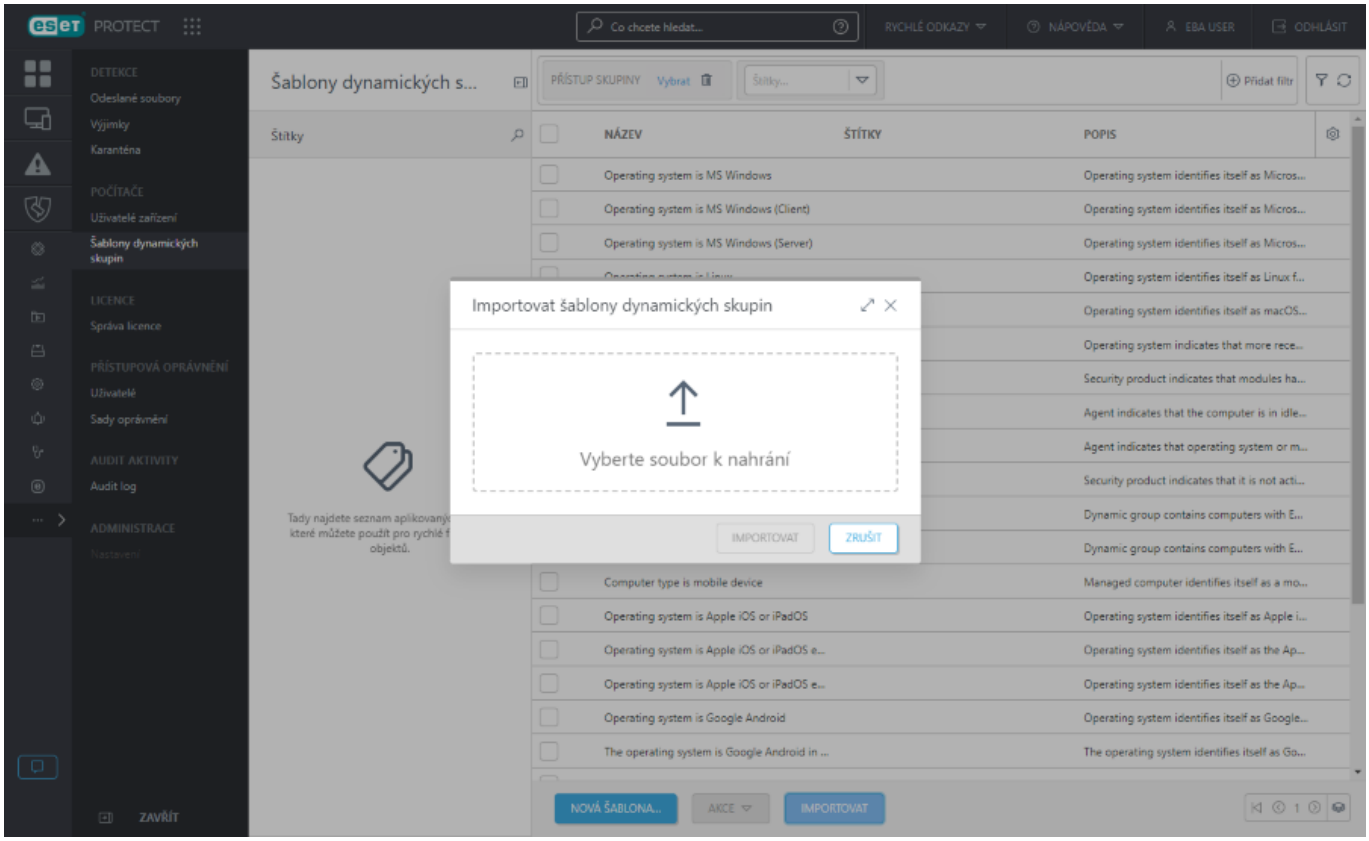
1. V ESET PROTECT On-Prem vyberte možnost **Další** > **Šablony dynamických skupin**.

2. U šablon dynamických skupin, které chcete exportovat, klikněte na políčko pro označení příslušné šablony > klikněte na tlačítko **Akce** > **Exportovat…**



3. Uložte soubor *.dg* s exportovanými šablonami dynamickými šablonami skupin.

4. V ESET PROTECT klikněte na **Další** > **Šablony dynamických skupin** > **Importovat** a vyberte soubor *.dg* se šablonami dynamických skupin vyexportovanými z ESET PROTECT On-Prem a kliknutím na **Importovat** je naimportujte do ESET PROTECT.



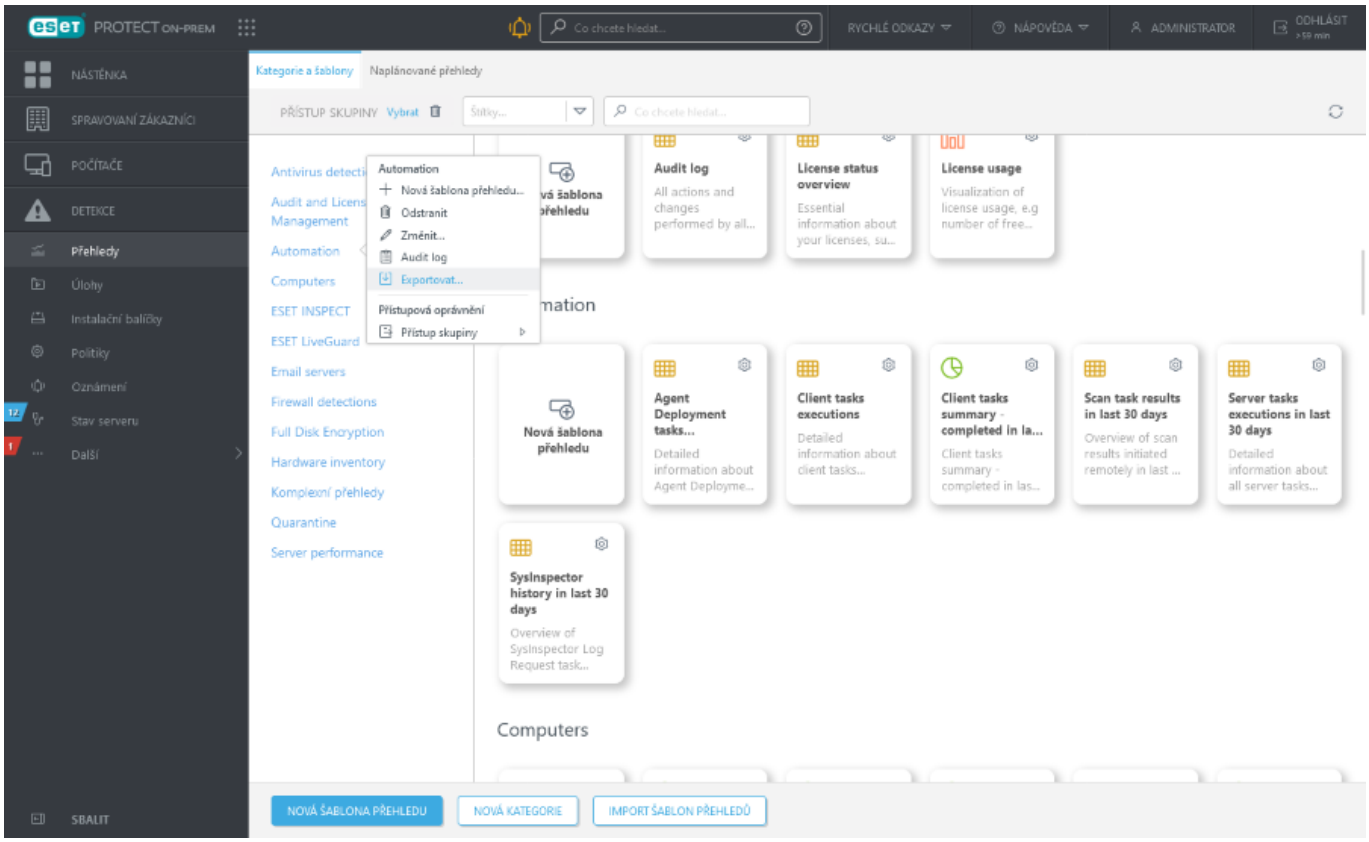
5. Importované šablony dynamických skupin se následně zobrazí v seznamu šablon a můžete je využít při

vytváření dynamických skupin (dynamické skupiny nelze migrovat).

IV. Migrace šablon přehledů z ESET PROTECTOn-Prem do ESET PROTECT

1. V ESET PROTECT On-Prem vyberte možnost **Přehledy**.

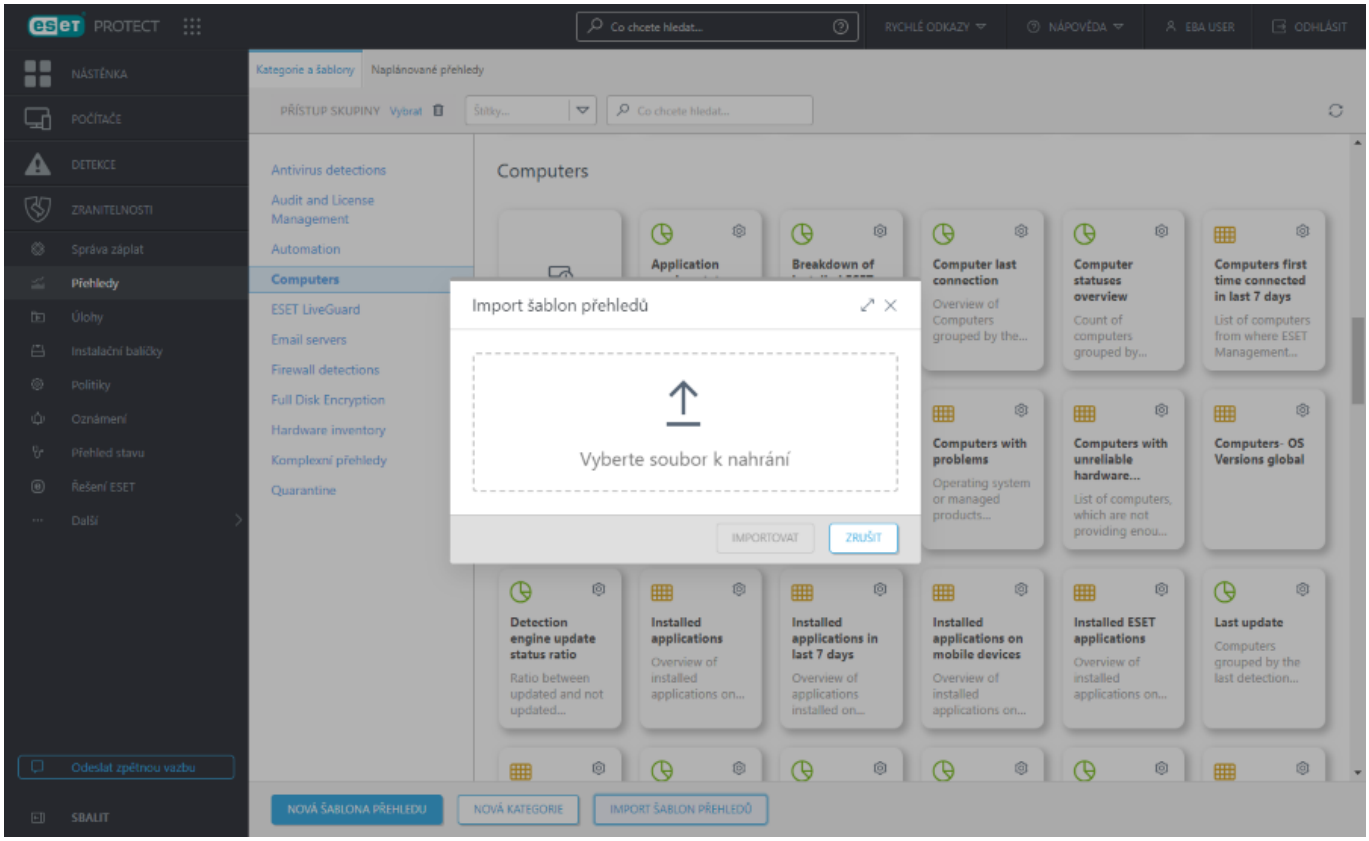
2. Klikněte na ikonu ozubeného kola vedle kategorie přehledu nebo přímo na šabloně přehledu > klikněte na **Exportovat**.



3. Uložte soubor *.dat* s exportovanými šablonami.

4. V ESET PROTECT klikněte na **Přehledy** >**Import šablon přehledů** > nahrajte soubor *.dat* se šablonami přehledů vyexportovanými z ESET PROTECT On-Prem a kliknutím na **Importovat** je naimportujte do ESET PROTECT.

Pokud si přejete migrovat více samostatných přehledů, postupujte opět dle výše uvedených kroků.



5. Importované šablony přehledů se zobrazí v části **Přehledy**. Šablony přehledů můžete využít k plánování a generování přehledů.

V. Migrace spravovaných počítačů z ESET PROTECT On-Prem do ESET PROTECT

V.I. Migrace struktury statický skupin pomocí nástroje pro export počítačů

Nástroj pro export počítačů dokáže exportovat strukturu statických skupin (MSP nebo jiné než MSP) z ESET PROTECT On-Prem. Následně můžete importovat strukturu statických skupin do ESET PROTECT.

Pokud se rozhodnete nepoužít nástroj pro export počítačů:
- Pokračujte v migraci pomocí politiky pro migraci.
- Po dokončení migrace do ESET PROTECT naleznete všechna zařízení ve statické skupině **Ztráty a nálezy**.

Požadavky pro spuštění nástroje určeného k exportu počítačů:

- 64-bit Windows nebo Linux
- Python (verze 3.9 a novější) – zda je Python nainstalován a jaká je jeho verze můžete zjistit spuštěním následujícího příkazu:
  - Příkaz v systému Windows: `python --version`
  - Příkaz v systému Linux: `python3 --version`

Python můžete stáhnout ze stránek https://www.python.org/. Ujistěte se, že jste během instalace v systému

Windows zaškrtli políčko **Add python.exe to PATH**.

- Zkontrolujte, zda je v síti přístupný port webové konzole (port 2223 nebo vlastní).

1. Stáhněte si nástroj pro export počítačů.

2. Rozbalte stažený archiv *computers_export_tool.zip*.

3. Otevřete složku *computers_export_tool* pomocí příkazové řádku systému Windows nebo Linux.

4. Spusťte následující příkaz:

   - Windows: `python computers_export_tool.py`
   - Linux: `python3 computers_export_tool.py`

5. V **Hostname [localhost]** zadejte název ESET PROTECT On-Prem a stiskněte klávesu Enter. Pokud na ESET PROTECT Serveru spustíte nástroj pro export počítačů, po stisknutí klávesy Enter se použije výchozí hodnota `localhost`.

6. V části **Port [2223]** stiskněte Enter pokud ESET PROTECT On-Prem používá výchozí port webové konzole (2223), nebo zadejte vlastní port webové konzole a stiskněte Enter.

7. Do pole **Username** zadejte jméno uživatele webové konzole a stiskněte klávesu Enter.

Použijte uživatele webové konzole s právy administrátora, který má přístup ke všem statickým skupinám ESET PROTECT On-Prem, abyste zajistili export všech statických skupin.

8. V části **Password** zadejte heslo uživatele webové konzole (zadané znaky se nezobrazí) a stiskněte Enter.

9. Nástroj vygeneruje soubor *computers.csv* (umístěný ve stejné složce – *computers_export_tool*). Soubor *computers.csv* obsahuje strukturu statických skupin ESET PROTECT On-Prem s názvy počítačů. Poznámka: Pokud nástroj spustíte znovu, přepíše se *computers.csv* soubor.

Velký počet spravovaných stanic

Import velkého počtu počítačů může trvat delší čas. Pokud je v ESET PROTECT On-Prem více než 30 000 spravovaných počítačů, postupujte podle následujících kroků:
1.Pomocí jednoduchého textového editoru rozdělte *computers.csv* na několik *.csv* souborů s maximálně 30 000 řádky v každém souboru.
2.Do ESET PROTECT importujte každý *.csv* soubor opakováním níže uvedených kroků.

10. Ve webové konzoli ESET PROTECT klikněte na položku **Počítače** > klikněte na ikonu ozubeného kola v řádku **Všechny** statické skupiny > **Importovat**.

11. Klikněte na **Vyberte soubor** > vyberte soubor *computers.csv* a klikněte na **Otevřít**.

12. Klikněte na **Importovat** a ESET PROTECT začne importovat strukturu statických skupin ESET PROTECT On-Prem ze souboru *computers.csv*. Okno pro importování můžete zavřít a pokračovat v práci s ESET PROTECT.

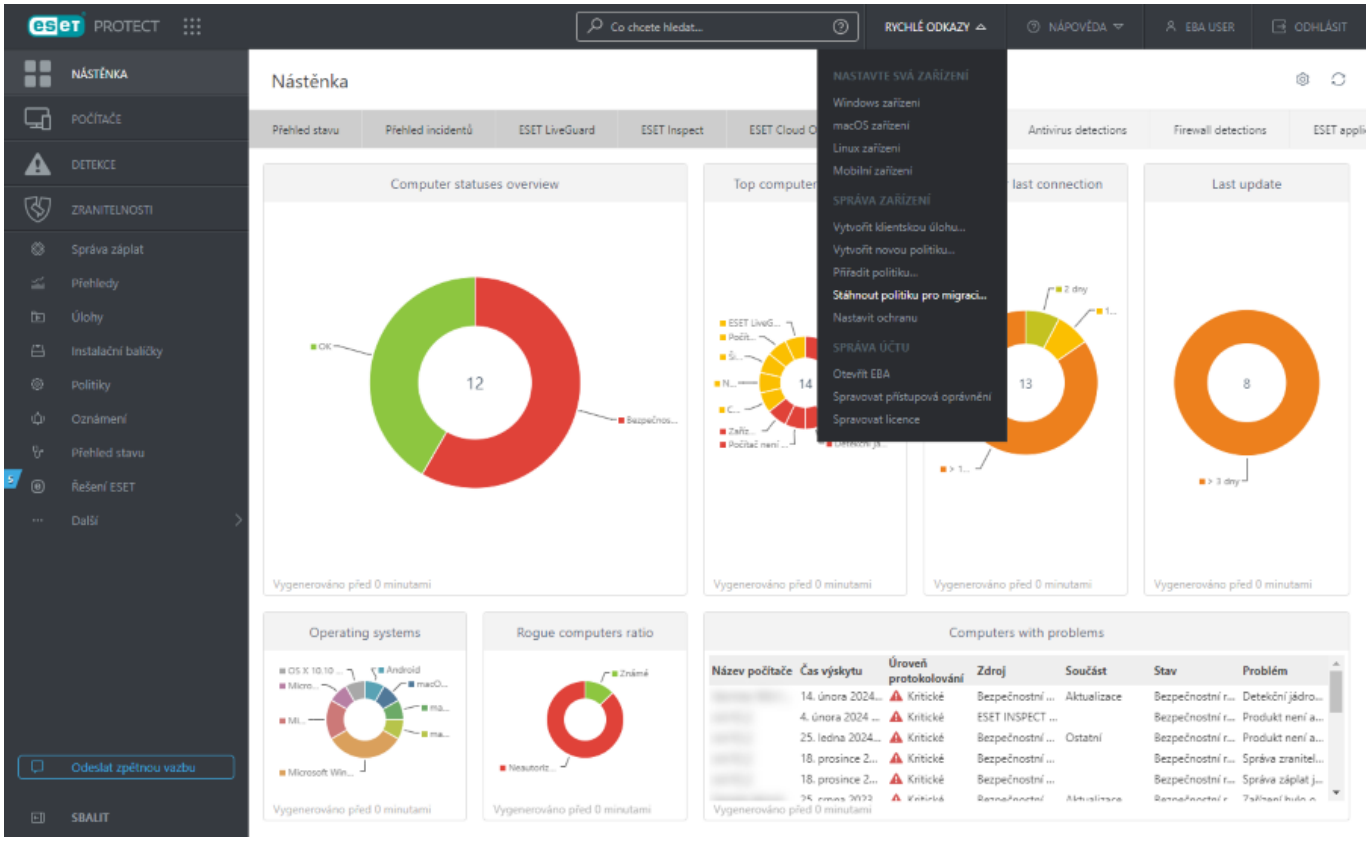
13. Po dokončení importu se struktura statických skupin s názvy počítačů z ESET PROTECT On-Prem objeví v sekci **Počítače** v cloudové webové konzoli ESET PROTECT. Postupujte podle níže uvedených kroků – použijte

politiku pro migraci spravovaných počítačů (ESET Management Agentů).

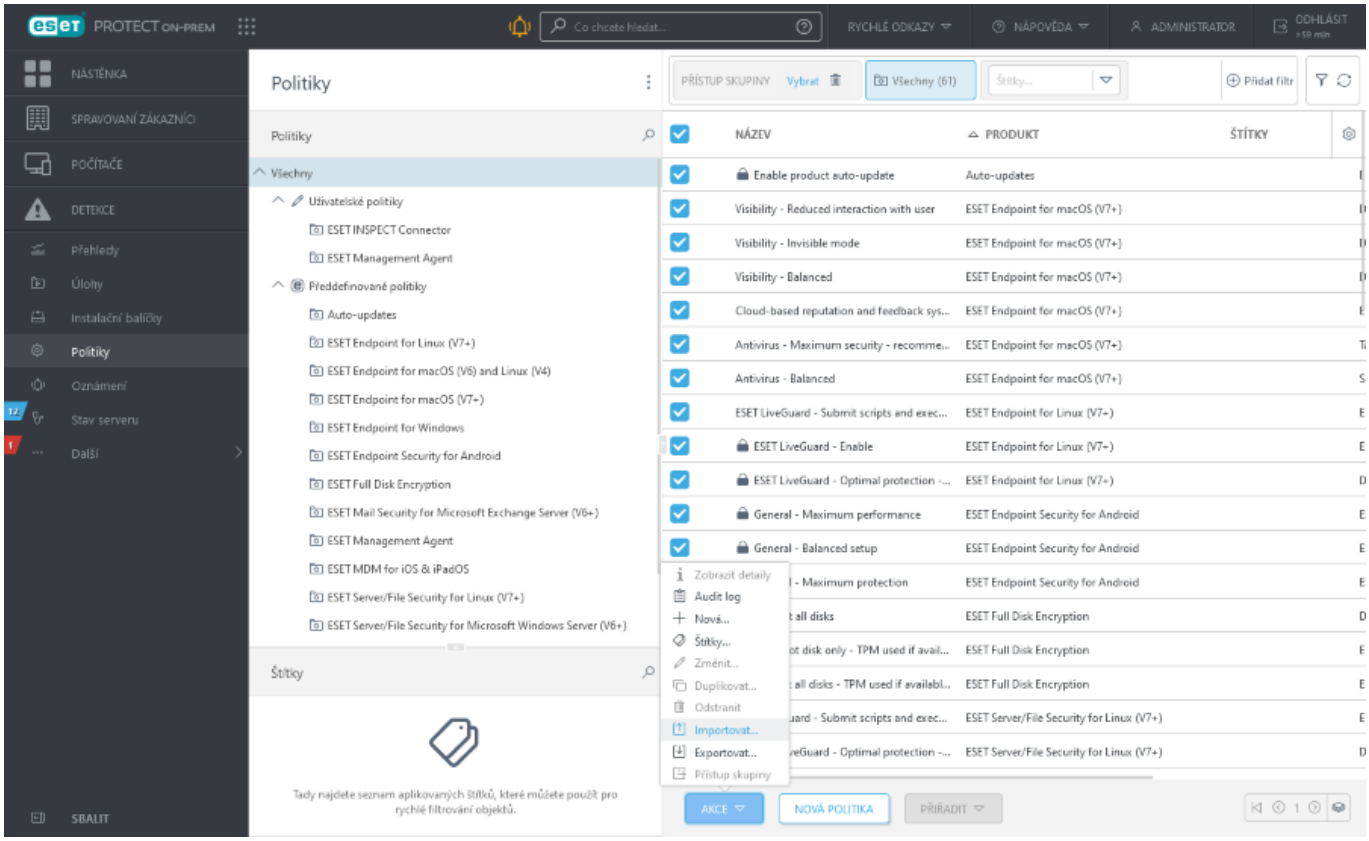
V.II. Migrace spravovaných počítačů (ESET Management Agentů) pomocí politiky pro migraci

Před migrací agentů se ujistěte, že nastavení firewallu splňují síťové požadavky ESET PROTECT.

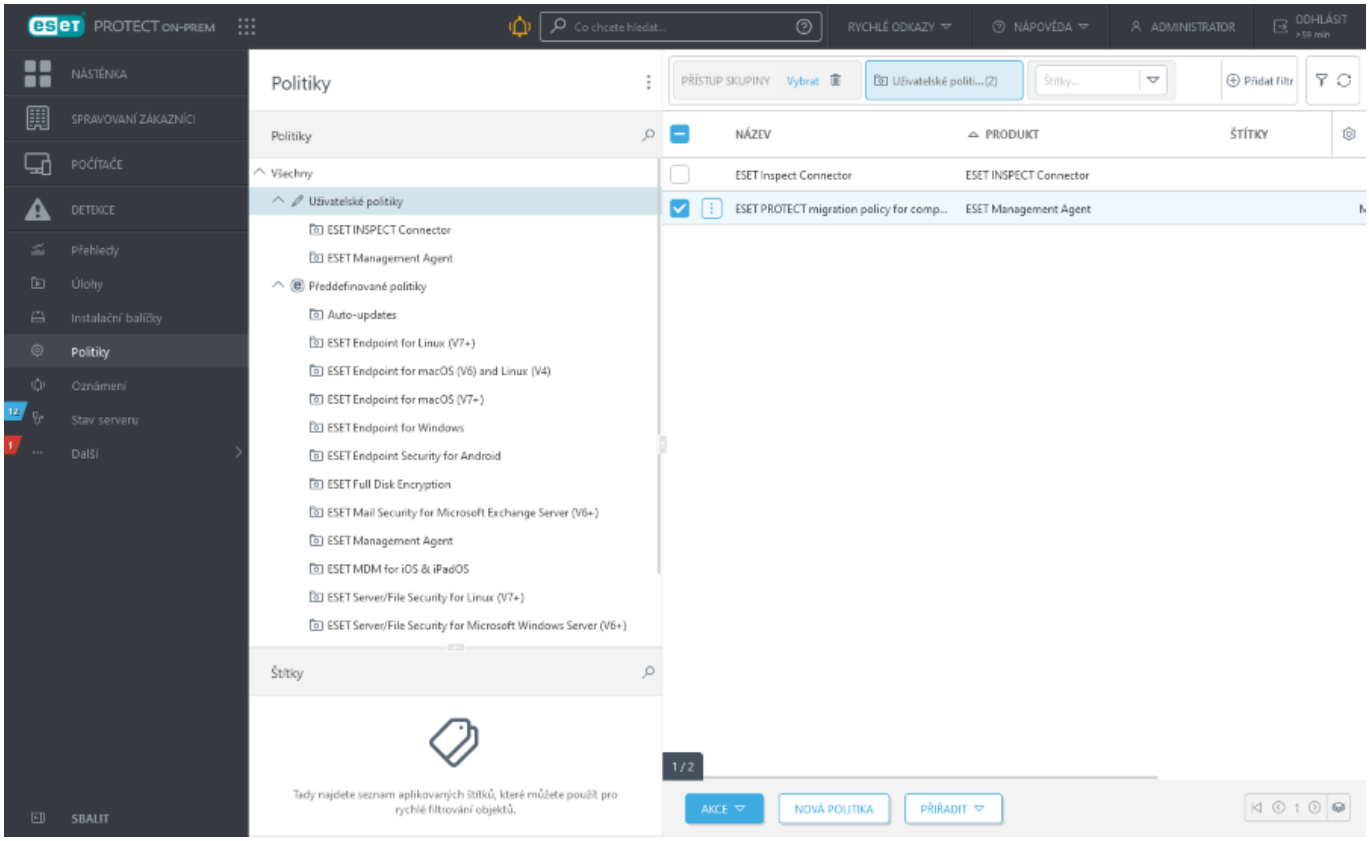
1. V horní části ESET PROTECT Web Console klikněte na **Rychlé odkazy** > **Stáhnout politiku pro migraci** a uložte si *.dat* soubor.



2. V ESET PROTECT On-Prem vyberte možnost **Politiky** > **Importovat**. Vyberte stažený *.dat* soubor z předchozího kroku a akci potvrďte kliknutím na tlačítko **Importovat**.



3. Přejděte do sekce **Uživatelské politiky** a vyberte importovanou politiku pro migraci.



4. Klikněte na migraci politik > **Upravit**.

5. V **Nastavení** > **Připojení** nastavte příznak **Vynutit** pro **Připojovat se k těmto serverům** a **Certifikát**.

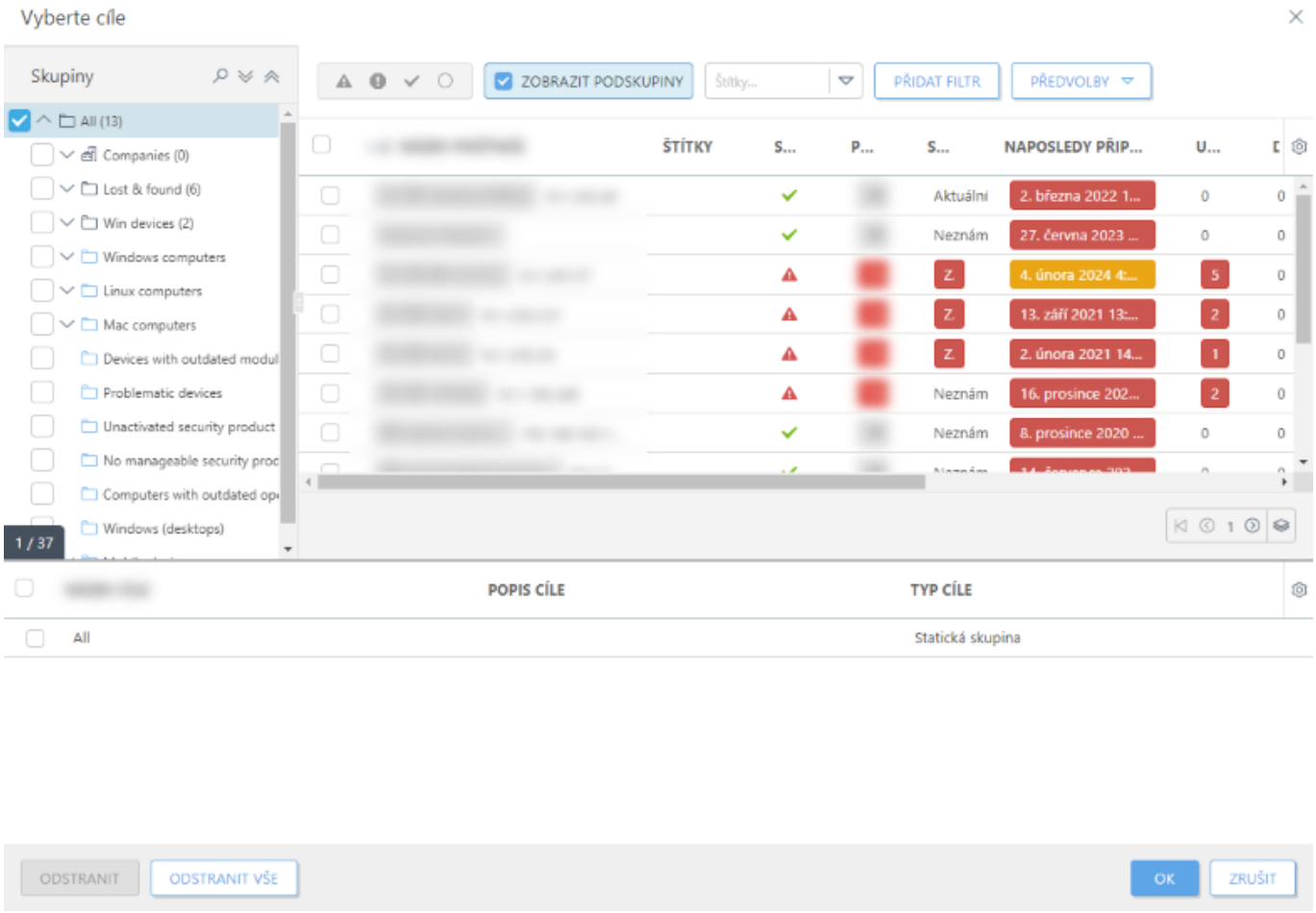
6. Klikněte na tlačítko **Dokončit**.

Otestujte si migraci na malém vzorku stanic
Doporučujeme nejprve přemigrovat několik počítačů, ke kterým máte fyzický přístup. Ujistěte se, že se mohou připojit k ESET PROTECT a poté všechny počítače migrujte.

7. V zobrazeném kontextovém menu vyberte možnost **Přiřadit skupině**.

8. Vyberte statickou skupinu **Všechna zařízení** a klikněte na tlačítko **OK**.

Přiřazením politiky pro migraci statické skupině **Všechna zařízení** zajistíte migraci všech spravovaných počítačů.

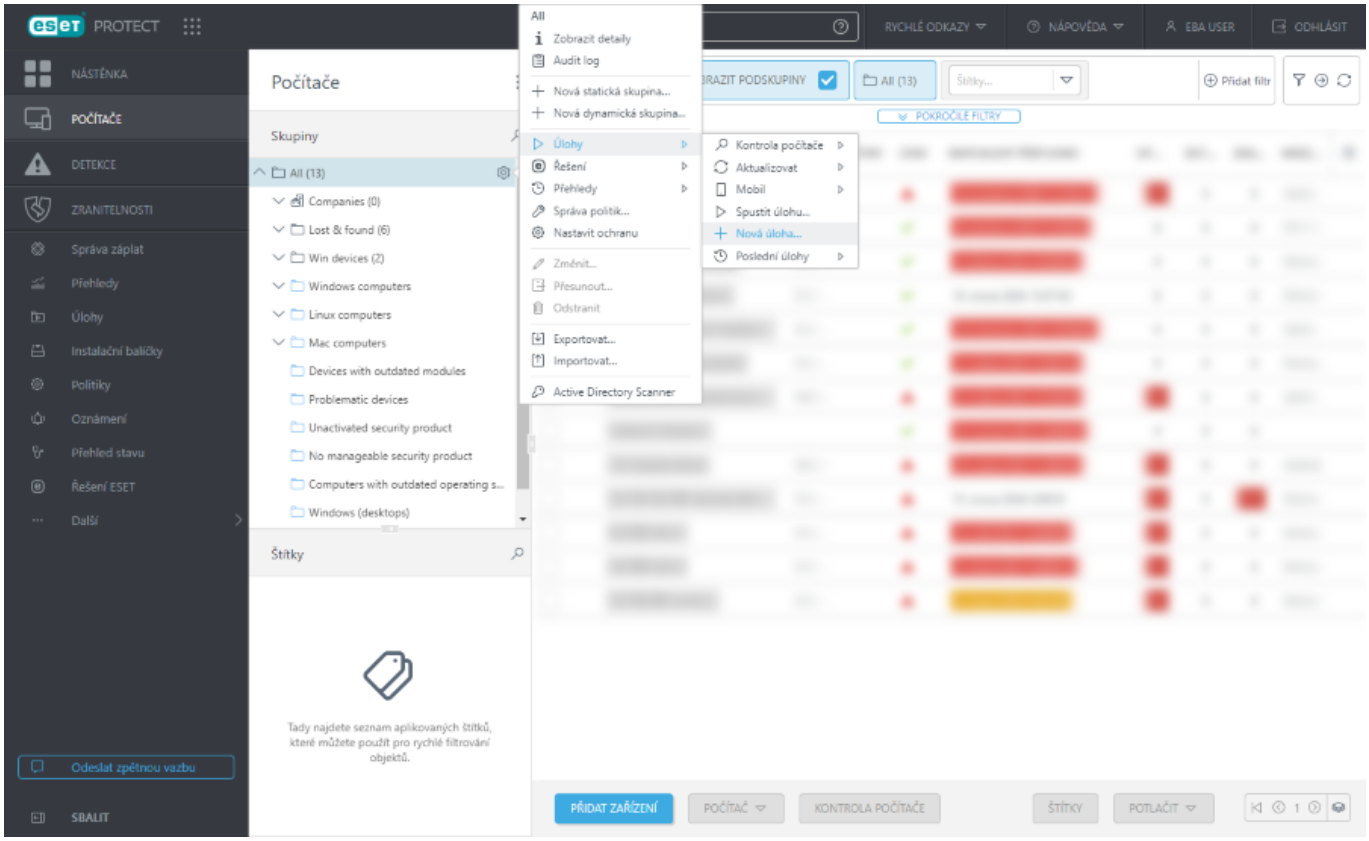


9. Politiku uložte kliknutím na tlačítko **Dokončit**.

10. Přihlaste se do ESET PROTECT Web Console. V části **Počítače** si zobrazíte počítače přemigrované z ESET PROTECT On-Prem. Může trvat několik minut, než se všechny počítače z ESET PROTECT On-Prem začnou připojovat k ESET PROTECT.

11. Po migraci počítačů z ESET PROTECT On-Prem do ESET PROTECT je nutné znovu aktivovat bezpečnostní produkty ESET na spravovaných počítačích pomocí cloudových licencí spravovaných v ESET PROTECT:

a. Ve webové konzoli ESET PROTECT klikněte na **Počítače** > klikněte na ikonu ozubeného kola v řádku **Všechny** statické skupiny > vyberte **Úlohy** > **Nová úloha**.



b.V rozbalovací nabídce **Úloha** vyberte možnost **Aktivace produktu**.

c.V sekci **Nastavení** vyberte licenci, kterou chcete aktivovat bezpečnostní produkt ESET, v sekci **Cíle** zkontrolujte cílové počítače a klikněte na tlačítko **Dokončit**.

Pokud používáte více bezpečnostních řešení (například ESET Endpoint a řešení pro ochranu serverů), bude nutné kroky pro aktivaci opakovat pro každou kategorii řešení.

d.Vyčkejte několik minut, než dojde k aktivaci bezpečnostních produktů ESET.

VI. Migrace mobilních zařízení

VII. Vytvoření ESET PROTECT uživatelů v ESET Business Account

VIII. Namapování ESET Business Account uživatelů ve webové konzoli ESET PROTECT

IX. Vyřazení on-premise serveru ESET PROTECT z provozu

Po úspěšné migraci na ESET PROTECT, vyřaďte z provozu server ESET PROTECT.

Pokud si ponecháte on-premise server ESET PROTECT, vypněte úlohu Odstranění nepřipojujících se počítačů, abyste zabránili možné deaktivaci bezpečnostních řešení ESET na počítačích spravovaných serverem ESET PROTECT.

Řešení problémů po migraci

Informace o upozornění **Zařízení používá připojení s podporou převzetí služeb při selhání** najdete v článku naší Databáze znalostí.

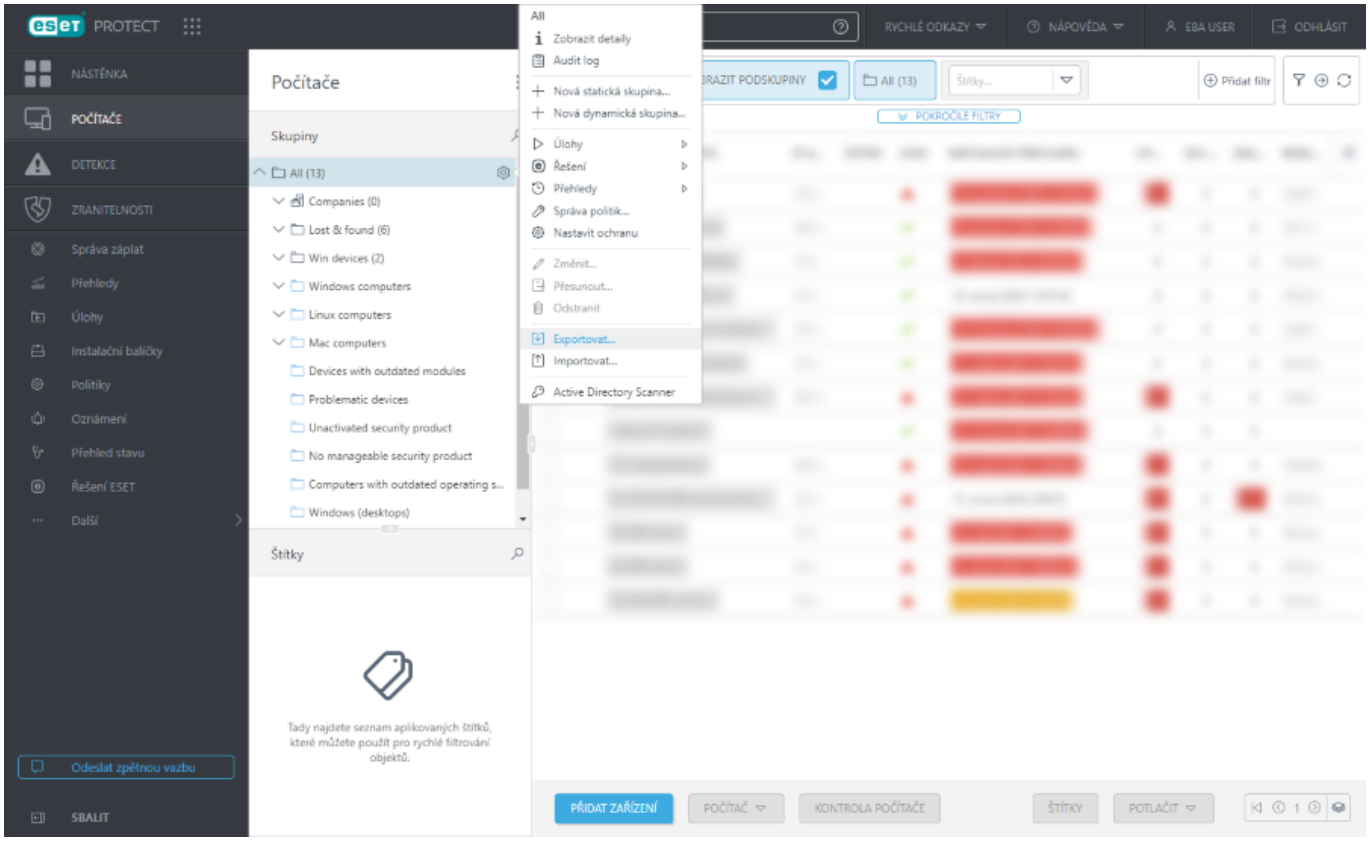
Migrace v rámci cloudu – z ESET PROTECT na jiný ESET PROTECT

Podle níže uvedených kroků poveďte migraci z ESET PROTECT (níže jako **ESET PROTECT 1**) na jiný ESET PROTECT (níže jako **ESET PROTECT 2**) pomocí politiky pro migraci:

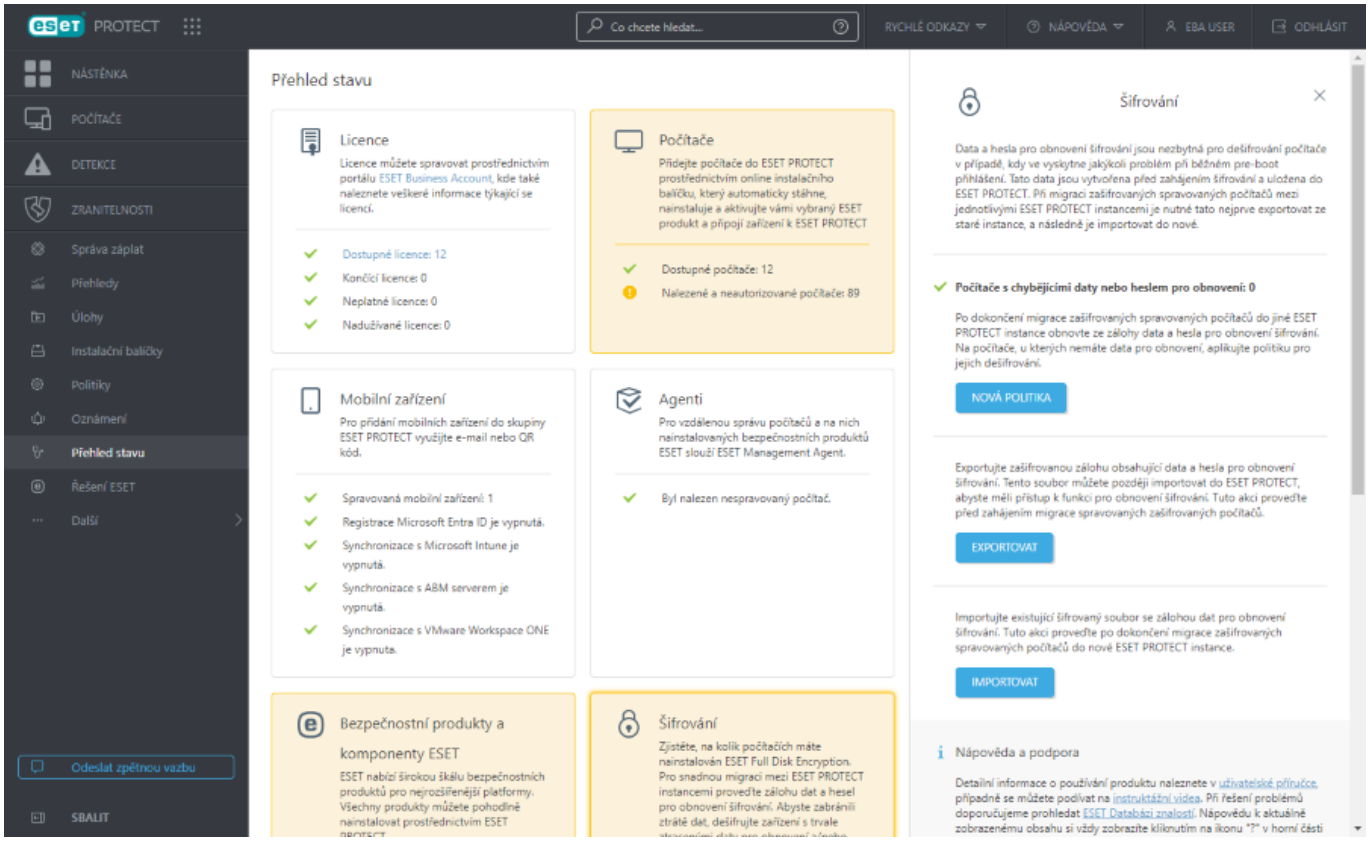
ESET PROTECT 1 obsahuje vlastní statické skupiny, připojující se ESET Management Agenty, spravovaná zařízení s nainstalovanými a aktivovanými bezpečnostními produkty ESET a šifrovaná zařízení.

Můžete migrovat:	Migrovat nelze:
• spravovaná zařízení (ESET Management Agenty a ESET Inspect Connectory) • statické skupiny • politiky • šablony dynamických skupin • šablony přehledů	• celou databázi • dynamické skupiny (můžete však migrovat šablony dynamických skupin) • detekce • audit log • oznámení • úlohy a podmínky spuštění • instalační balíčky • naplánované/vygenerované přehledy (můžete však migrovat šablony přehledů) • štítky • mobilních zařízení (můžete je ale přeregistrovat)

1. **ESET PROTECT 1** – klikněte na **Počítače** > klikněte na ikonu ozubeného kola vedle statické skupiny pro **všechna zařízení** > vyberte **Exportovat** > klikněte na **Ano** a vyexportujete zařízení z podskupin > uložte *TXT* soubor.

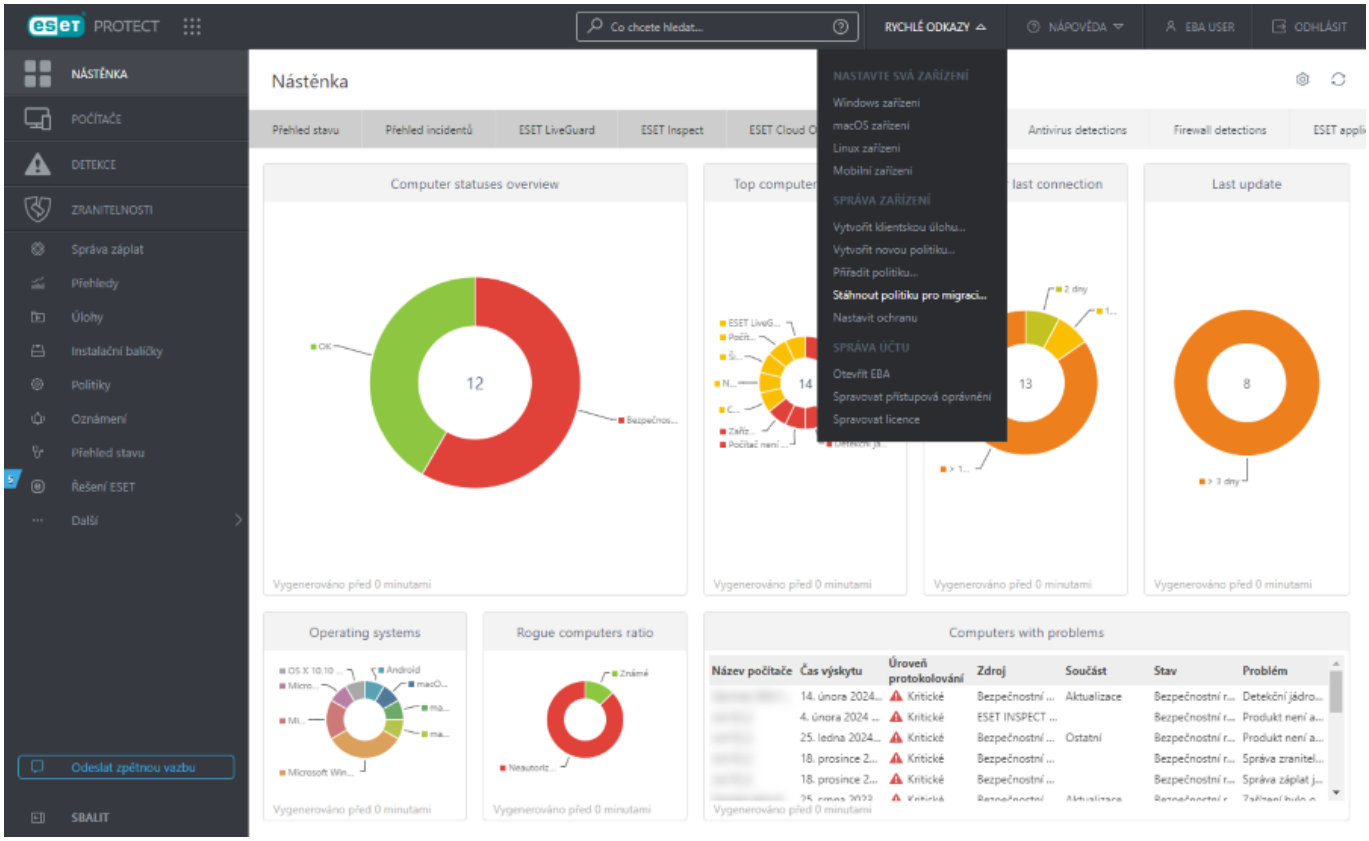


2. **ESET PROTECT 1 –** klikněte na **Přehled stavu** > klikněte na dlaždici **Šifrování** > klikněte na **Exportovat** pro export šifrovacích dat a hesel > uložte soubor **efdeRecoveryExport.dat.**

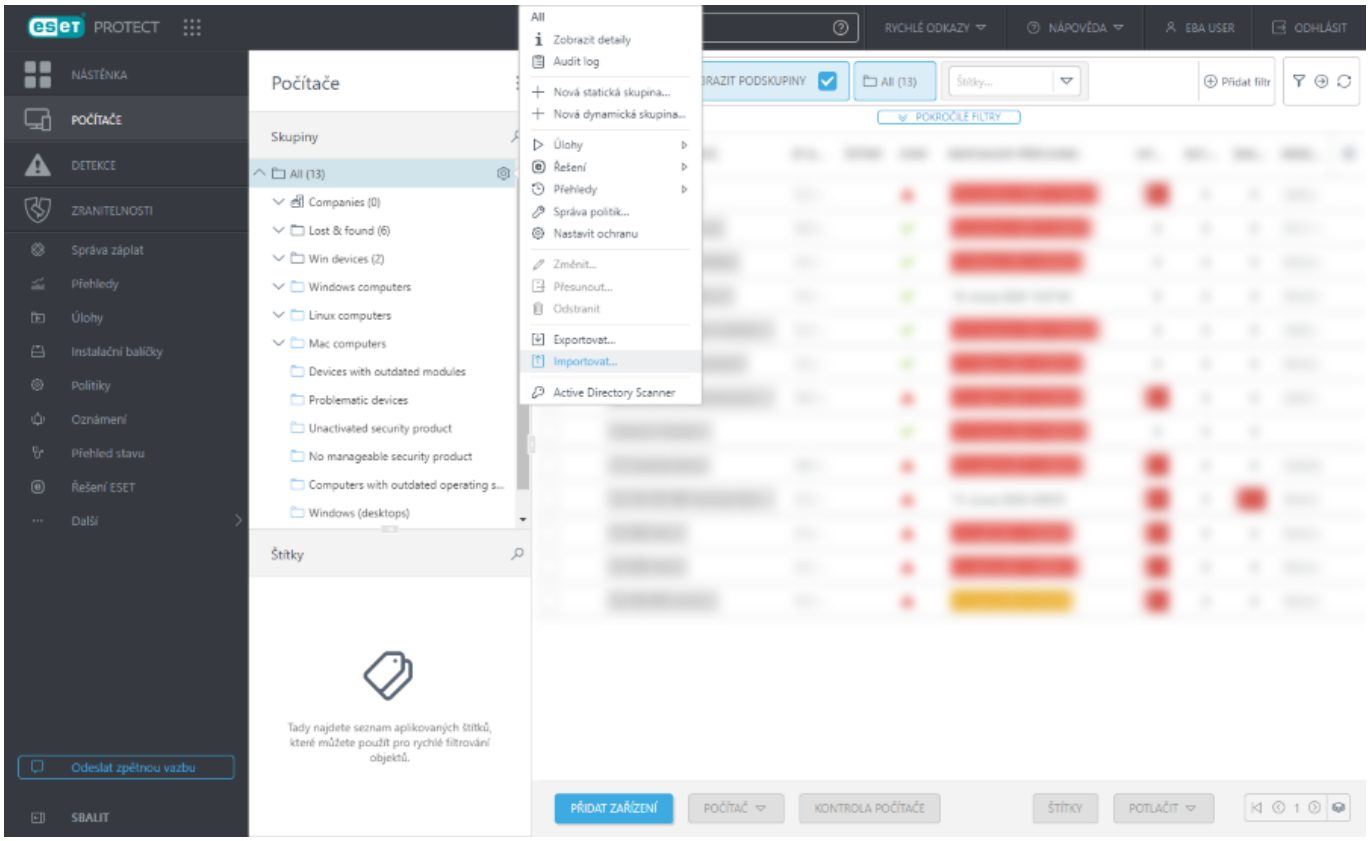


3. Vytvořte nový ESET PROTECT (**ESET PROTECT 2**).

4. **ESET PROTECT 2 –** klikněte na **Rychlé odkazy** > **Stáhnout politiku pro migraci** > uložte soubor *CloudMigrationPolicy {timestamp}* s příponou *.dat.*



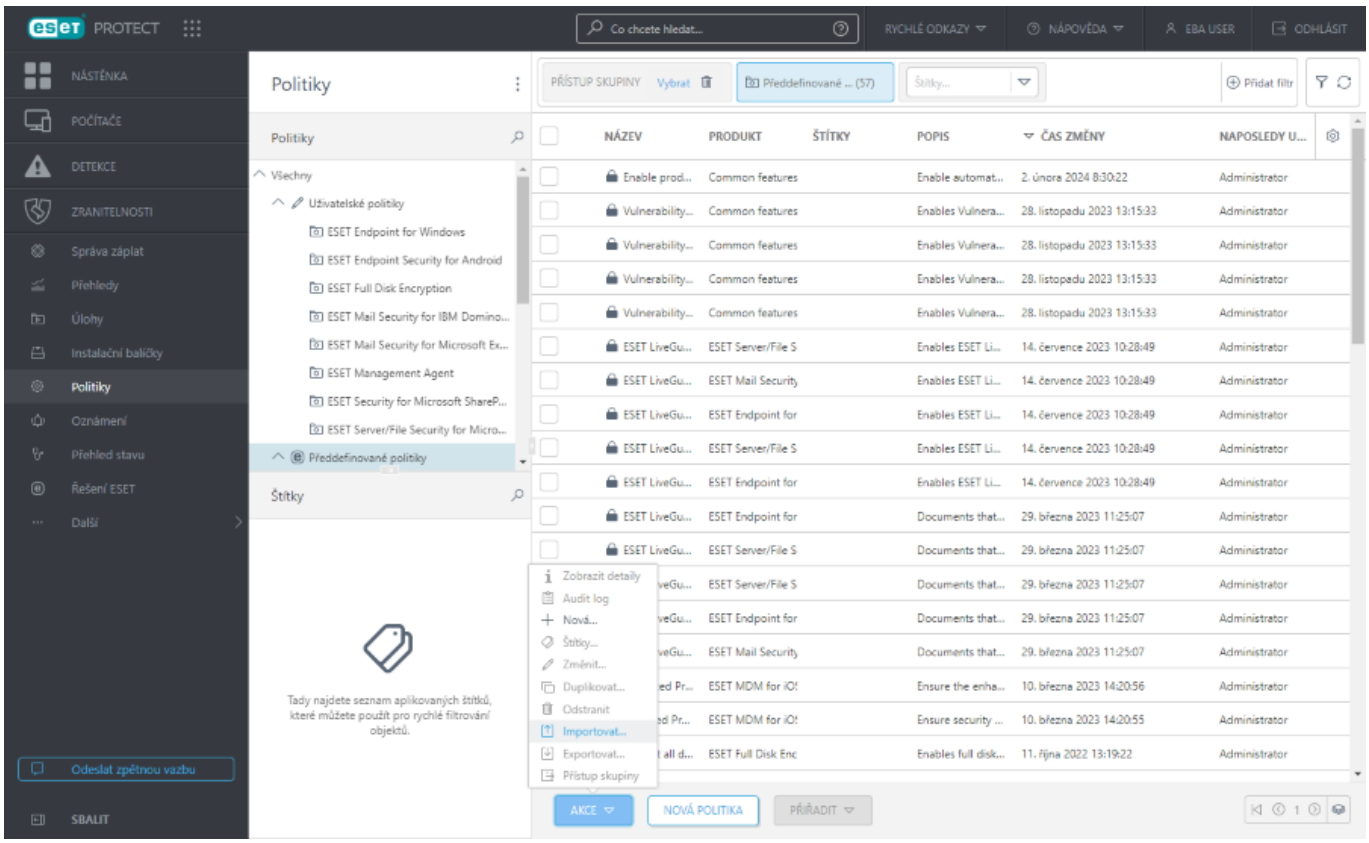
5. **ESET PROTECT 2** – klikněte na **Počítače** > klikněte na ikonu ozubeného kolečka vedle statické skupiny pro **všechna zařízení** > vyberte **Importovat** > naimportujte statické skupiny pomocí *TXT* souboru exportovaného z **ESET PROTECT 1** v kroku 1 výše.



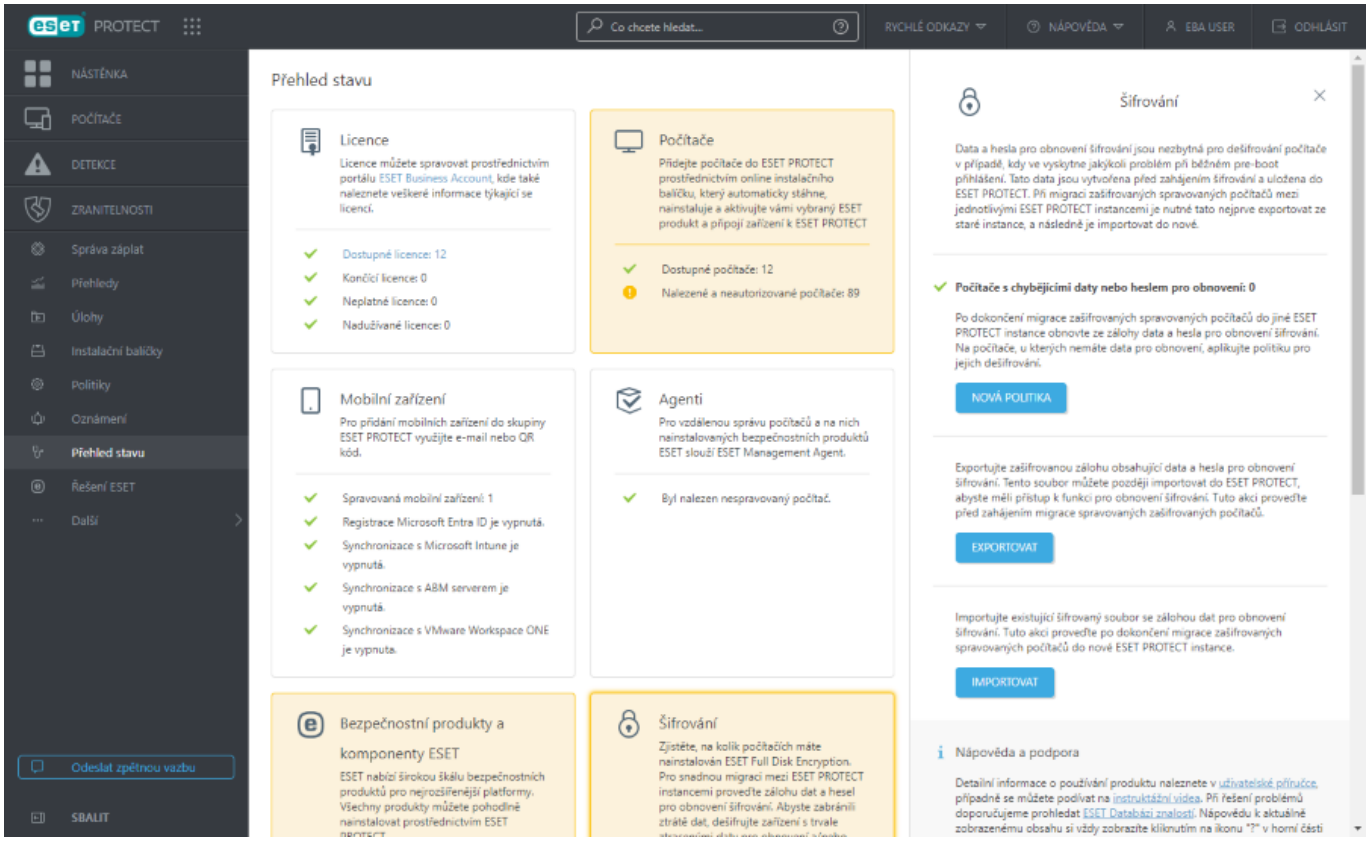
6. **ESET PROTECT 1** – klikněte na **Politiky** > **Akce** > **Importovat** > naimportujte politiku pro migraci pomocí *DAT* souboru exportovaného z **ESET PROTECT 2** v kroku 4 výše > přiřaďte politiku pro migraci statické skupině pro

všechna zařízení. Spravovaná zařízení se připojí k **ESET PROTECT 2**.

> Pokud použijete ESET Inspect, konektory ESET Inspect na spravovaných zařízeních se připojí k novému ESET Inspect.



7. **ESET PROTECT 2** – klikněte na **Přehled stavu** > klikněte na dlaždici **Šifrování** > klikněte na **Importovat** a naimportujte šifrovací data a hesla z *DAT* souboru vyexportovaného z **ESET PROTECT 1** v kroku 2 výše.



8. Podobně jako při migraci z ESET PROTECT On-Prem na ESET PROTECT, proveďte migraci z **ESET PROTECT** 1 na **ESET PROTECT 2** pro:

   - politiky
   - šablony dynamických skupin
   - šablony přehledů

> **Migrace mobilních zařízení**
> Chcete-li migrovat spravovaná mobilní zařízení, odregistrujte je z **ESET PROTECT 1** a zaregistrujte je do **ESET PROTECT 2**.

Jak odstranit ESET PROTECT ze sítě

Existují dva korektní scénáře, jak můžete ukončit správu své sítě prostřednictvím ESET PROTECT:

a) Kompletně odinstalujete všechny bezpečnostní produkty ESET, ESET Management Agenty a zahodíte ESET PROTECT instanci.

b) Pokračovat v používání bezpečnostních produktů, pouze odinstalujete ESET Management Agenty a zahodíte ESET PROTECT instanci. (V tomto scénáři přeskočte na krok Odebrání ESET Management Agenta).

Odebrání bezpečnostních produktů ESET z vaší sítě

1. Obnovte výchozí nastavení produktu nebo umožněte jeho lokální změnu.

   a.Smažte všechny **Uživatelské politiky**, které jsou aplikovány na klienty.

b.Projděte **Předdefinované politiky** a na záložce **Přiřazeno k** se podívejte, zda nejsou přiřazeny nějakým zařízením ve vaší síti.

2. Odstraňte vámi definované heslo pro přístup do nastavení produktu.

a.Vytvořte novou politiku pro konkrétní bezpečnostní produkt a v konfigurační šabloně přejděte do sekce **Uživatelské rozhraní** > **Přístup k nastavení**.

b.Ponechte možnost **Chránit nastavení heslem** neaktivní a aplikujte příznak **Vynutit** u možnosti **Nastavit heslo**.

c.Přiřaďte tuto politiku všem zařízením ve vaší síti. Tím odstraníte heslo, které brání neautorizovanému přístupu do rozšířeného nastavení produktu a v jeho odinstalování.

3. Dešifrujte všechny stanice zašifrované prostřednictvím produktu ESET Full Disk Encryption.

Pokud po smazání ESET PROTECT instance zůstanou některé stanice zašifrované, neexistuje způsob pro jejich dešifrování (pokud jste si předem nestáhli data pro obnovení). V takovém případě vám nemůže technická podpora ESET pomoci.

4. V případě potřeby můžete bezpečnostní produkt odinstalovat. Můžete jej ponechat nainstalovaný. V takovém případě poběží nepřetržitě dále, jen nebude centrálně spravovaný.

Pro hromadné odinstalování bezpečnostních produktů můžete použít úlohu Odinstalace aplikace.

a.V hlavním menu přejděte na záložku **Úlohy** a klikněte na tlačítko **Nová**.

b.V průvodci vytvořením úlohy v sekci **Obecné** zadejte název a popis úlohy. Z rozbalovacího menu **Úloha** vyberte možnost **Odinstalace aplikace**.

c.V sekci **Nastavení** vyberte z rozbalovacího menu **Odinstalovat** možnost Aplikaci ze seznamu. V sekci **Název balíčku** klikněte na **Vyberte balíček, který chcete odinstalovat**, ze seznamu vyberte balíček, který chcete odinstalovat a pokračujte kliknutím na tlačítko **OK**.

d.V sekci **Verze balíčku** klikněte na možnost **Odinstalovat všechny verze balíčku**. Tím zabráníte komplikacím při odinstalování, pokud máte v síti nasazeny rozdílné verze bezpečnostních produktů.

e.Pro zajištění korektního procesu odinstalace aktivujte možnost **Automaticky restartovat, když je potřeba** a vytvoření úlohy potvrďte kliknutím na tlačítko **Dokončit**.

f.Klikněte na tlačítko **Vytvořit podmínku spuštění** pro definování cílů úlohy. Klikněte na tlačítko **Přidat skupiny** a vyberte nejnadřazenější skupinu **Všechna zařízení**. Vyberte si pro vás vhodnou podmínku spuštění a spuštění úlohy naplánujte kliknutím na tlačítko **Dokončit**.

Ověřte, zda úloha doběhla úspěšně na všech zařízeních a následně proces opakujte pro další bezpečnostní produkty ve vaší síti.

Odstranění ESET Management Agenta z vaší sítě

Pro nejefektivnější odstranění všech ESET Management Agentů z vaší sítě se ujistěte, že jsou všechna zařízení zapnutá a připojují se k ESET PROTECT.

1. Odstraňte ochranu heslem (platné pouze pro Windows)

   a.Vytvořte novou politiku pro ESET Management Agenta.

   b.V konfigurační šabloně přejděte v sekci **Rozšířená nastavení** > **Nastavení** aplikujte příznak Vynutit u možnosti **Chránit nastavení heslem**.

   c.Přiřaďte politiku nejnadřazenější skupině **Všechna zařízení** a uložte ji kliknutím na tlačítko **Dokončit**.

2. Ověřte, že se politika aplikovala. Po úspěšném aplikování politiky odeberte ESET Management Agenty ze zařízení ve vaší síti. Využít k tomu můžete úlohu Ukončit správu (odinstalovat ESET Management Agenta. Naplánujte její spuštění na všech zařízeních ve své síti.

3. Vyčkejte na spuštění úlohy na všech zařízeních ve své síti.

4. V hlavním menu ESET PROTECT přejděte na záložku **Počítače** a odstraňte všechna zařízení .

Pokud se žádné zařízení po uplynutí 10 minut neobjeví zpět v konzoli, úspěšně jste odinstalovali všechny ESET Management Agenty ve své síti.

Odstranění instance ESET PROTECT

1. Přihlaste ke svému účtu na portále ESET Business Account.

2. Na **Nástěnce** přejděte na dlaždici ESET PROTECT.

3. Klikněte na ikonu ozubeného kolečka > z kontextového menu vyberte možnost **Odstranit ESET PROTECT**.

4. Zadejte heslo a klikněte na tlačítko **Odstranit**. Následně dojde ke smazání vaší instance ESET PROTECT.

Vypršela platnost poslední ESET PROTECT licence

V této kapitole si popíšeme následující scénáře související s licencí:

- Co se stane s ESET PROTECT instancí před a po vypršení platnosti poslední vhodné ESET PROTECT licence.
- Co se stane po odebrání poslední vhodné ESET PROTECT licence z vašeho účtu na portále ESET Business Account.

Co se stane s ESET PROTECT instancí před a po vypršení platnosti poslední vhodné ESET PROTECT licence?

Před blížícím se koncem platnosti licence se v ESET Business Account zobrazí upozornění.

- Pokud do doby konce platnosti licenci neprodloužíte nebo neaktivujete novým klíčem, v ESET Business Account se zobrazí upozornění, že platnost licence vypršela.

- Pokud po vypršení platnosti licence nebudete mít v ESET Business Account žádnou další vhodnou licenci, zobrazí se vám upozornění, že za 14 dní vaši instanci pozastavíme. Tuto informaci zašleme zároveň na e-mailovou adresu uvedenou u administrátorského účtu.

Máte 14 dní na prodloužení platnosti vaší propadlé licence. Na to, že již uplynula polovina této doby vás upozorníme v ESET Business Account, a také e-mailem. Po uplynutí 14 dní vaši ESET PROTECT instanci pozastavíme.

Instance bude nedostupná a nebude funkční. Pozastavenou ESET PROTECT instanci uložíme, a zpřístupníme vám ji ve chvíli, kdy do ESET PROTECT nahrajete vhodnou ESET Business Account licenci. **Vaši ESET PROTECT instanci ponecháme pozastavenou 30 dní. Po uplynutí této doby ji trvale smažeme včetně všech souvisejících dat.**

Ve chvíli, kdy dojde k pozastavení instance, se tato informace zobrazí v ESET Business Account. Až bude zbývat 14 dní do smazání instance, obdržíte upozornění rovněž e-mailem. Pro obnovení své ESET PROTECT instance je nutné do EBA přidat novou vhodnou ESET PROTECT licenci.

Co se stane po odebrání poslední vhodné ESET PROTECT licence z vašeho účtu na portále ESET Business Account?

Pokud ve svém účtu na portále ESET PROTECT nemáte žádnou vhodnou ESET Business Account licenci, vaši ESET PROTECT instanci pozastavíme.

Instance bude nedostupná a nebude funkční. Pozastavenou ESET PROTECT instanci uložíme, a zpřístupníme vám ji ve chvíli, kdy do ESET PROTECT nahrajete vhodnou ESET Business Account licenci. **Vaši ESET PROTECT instanci ponecháme pozastavenou 30 dní. Po uplynutí této doby ji trvale smažeme včetně všech souvisejících dat.**

Ve chvíli, kdy dojde k pozastavení instance, se tato informace zobrazí v ESET Business Account. Až bude zbývat 14 dní do smazání instance, obdržíte upozornění rovněž e-mailem. Pro obnovení své ESET PROTECT instance je nutné do EBA přidat novou vhodnou ESET PROTECT licenci.

Automatické aktualizace

Existuje několik typů automatických aktualizací produktů ESET:

- Automatická aktualizace ESET Management Agenta
- Automatická aktualizace bezpečnostních produktů ESET

Doporučujeme se seznámit s životním cyklem firemních produktů.
Další informace naleznete v článku Jaké jsou rozdíly mezi jednotlivými typy aktualizací produktu?
Automatické aktualizace nebudou funkční v prostředích s vytvořeným offline repozitářem, ve kterém nejsou potřebná metadata (například pokud jste zkopírovali instalační balíčky na sdílenou síťovou jednotku). Pro vytvoření offline repozitáře s podporou funkce pro automatickou aktualizaci produktu využijte Mirror Tool. Mějte na paměti, že z offline repozitáře vytvořeného prostřednictvím Mirror Tool se automatické aktualizace distribuují současně po celé síti (v případě online repozitáře dochází k distribuci automatických aktualizací postupně).

Automatická aktualizace ESET Management Agenta

ESET PROTECT zajišťuje automatickou aktualizaci ESET Management Agentů nainstalovaných na spravovaných zařízeních.

Jak funguje automatická aktualizace ESET Management Agenta

- Automatická aktualizace agenta je ve výchozím nastavení zapnutá, a není možné ji vypnout.

- K automatické aktualizaci ESET Management agenta dojde po dvou týdnech od uvolnění nové verze do repozitáře, pokud aktualizaci mezitím administrátor neinicioval ručně.

Pokud je k dispozici novější verze ESET Management Agenta a k automatické aktualizaci zatím nedošlo, můžete ji inicializovat ručně přímo na Nástěnce > **Stav verze komponent**.
Případně můžete použít klientskou úlohu Aktualizace Agenta.

- Proces automatické aktualizace je navržen tak, aby se zajistila její postupná distribuce za účelem minimalizování dopadu na síť a spravované stanice.

- Automatické aktualizace nebudou funkční v prostředích s vytvořeným offline repozitářem, ve kterém nejsou potřebná metadata (například pokud jste zkopírovali instalační balíčky na sdílenou síťovou jednotku). Pro vytvoření offline repozitáře s podporou funkce pro automatickou aktualizaci produktu využijte Mirror Tool. Mějte na paměti, že z offline repozitáře vytvořeného prostřednictvím Mirror Tool se automatické aktualizace distribuují současně po celé síti (v případě online repozitáře dochází k distribuci automatických aktualizací postupně).

Automatická aktualizace bezpečnostních produktů ESET

ESET PROTECT disponuje funkcí, která udržuje bezpečnostní produkty ESET na spravovaných počítačích aktualizované na nejnovější verzi.

Automatické aktualizace produktu jsou po nově nasazené instanci ESET PROTECT automaticky povoleny.

- Pro použití musíte vlastnit vhodnou licenci na bezpečnostní produkty ESET. Podívejte se, jaké produkty ESET určené pro firemní uživatele podporují automatické aktualizace. Ostatní bezpečnostní produkty ESET nepodporují automatické aktualizace. Tuto funkci budeme implementovat v budoucnu.
- Automatické aktualizace můžete konfigurovat prostřednictvím politiky.
- Další informace naleznete v kapitole často kladené dotazy týkající se automatické aktualizace. K první automatické aktualizaci produktu dojde po vydání nové verze původního sestavení 9.x (například verze 9.1 nebo 9.0.xxxx.y, kde verze xxxx je vyšší než první 9.x). Pro zajištění maximální stability aktualizací je distribuce automatické aktualizace zahájena se zpožděním po globálním vydání nové verze bezpečnostního produktu ESET. Během této doby může Web Console hlásit, že je daný bezpečnostní produkt zastaralý.
- Další informace naleznete v článku Jaké jsou rozdíly mezi jednotlivými typy aktualizací produktu?
- Automatické aktualizace nebudou funkční v prostředích s vytvořeným offline repozitářem, ve kterém nejsou potřebná metadata (například pokud jste zkopírovali instalační balíčky na sdílenou síťovou jednotku). Pro vytvoření offline repozitáře s podporou funkce pro automatickou aktualizaci produktu využijte Mirror Tool. Mějte na paměti, že z offline repozitáře vytvořeného prostřednictvím Mirror Tool se automatické aktualizace distribuují současně po celé síti (v případě online repozitáře dochází k distribuci automatických aktualizací postupně).

Pro přechod na bezpečnostní produkty ESET, které podporují automatické aktualizace, využijte jednu z níže uvedených možností:

- Použijte akci jedním kliknutím: na **Nástěnce** > **Přehled** > **Stav verze komponent** klikněte na sloupcový graf a z kontextového menu vyberte možnost **Aktualizovat nainstalované ESET produkty**.
- V hlavním menu přejděte do sekce **Počítače**, vyberte nejnadřazenější statickou skupinu **Všechna zařízení**, klikněte na ikonu ozubeného kolečka a vyberte možnost **Úlohy** > **Aktualizovat** > **Aktualizovat ESET produkty**.
- Použijte klientskou úlohu pro instalaci aplikace.

V tomto případě máte dvě možnosti, jak bezpečnostní produkty ESET aktualizovat na nejnovější verzi:

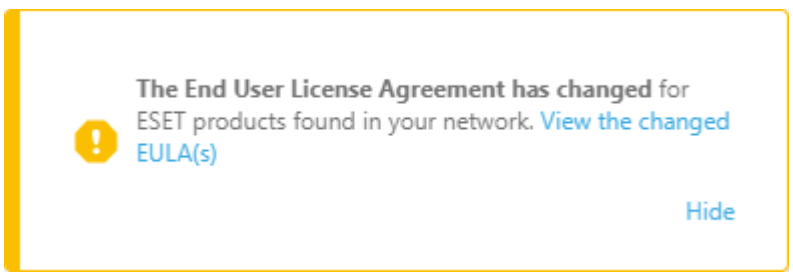
- Klientská úloha pro instalaci aplikace
- Funkce Automatické aktualizace

Rozdíly mezi klientskou úlohou pro instalaci aplikace a funkcí pro automatickou aktualizaci

	Proces aktualizace	Restart počítače po dokončení aktualizace	Budoucí aktualizace
Klientská úloha pro instalaci aplikace	V průběhu aktualizace dojde k přeinstalování bezpečnostního produktu ESET.	Z bezpečnostních důvodů je po dokončení aktualizace bezpečnostního produktu ESET vyžadován okamžitý restart počítače (pro zajištění plné funkčnosti aktualizovaného produktu).	Ručně – administrátor musí po vydání každé verze ručně zahájit aktualizaci spuštěním klientské úlohy – viz dostupné možnosti výše.
Automatické aktualizace	V průběhu aktualizace nedojde k přeinstalování bezpečnostního produktu ESET.	Aktualizace bezpečnostního řešení ESET vyžaduje restart zařízení, ale ne ihned (restart není vynucen). Správce ESET PROTECT může ovšem vynutit aktualizaci a restart počítače vzdáleně z webové konzole pomocí klientské úlohy Vypnout počítač u které zaškrtne políčko **Restartovat počítač(e)**.	Automaticky – podporované bezpečnostní produkty ESET se automaticky aktualizují po vydání nové verze (z důvodu zajištění stability jsou aktualizace distribuovány se zpožděním). Kontrolu aktualizací bezpečnostních produktů ESET můžete vynutit ručně pomocí úlohy Kontrola aktualizace produktu.

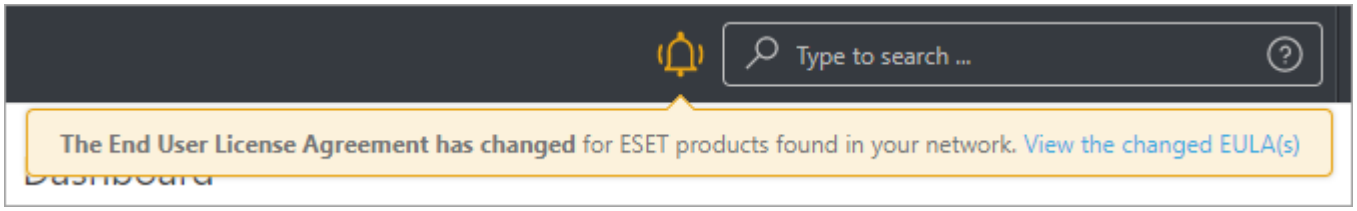
Aktualizovaná Licenční ujednání s koncovým uživatelem (EULA) u spravovaného bezpečnostního produktu ESET

ESET PROTECT Web Console upozorní správce, pokud je k dispozici aktualizované Licenční ujednání s koncovým uživatelem (EULA) spravovaného bezpečnostního řešení ESET.



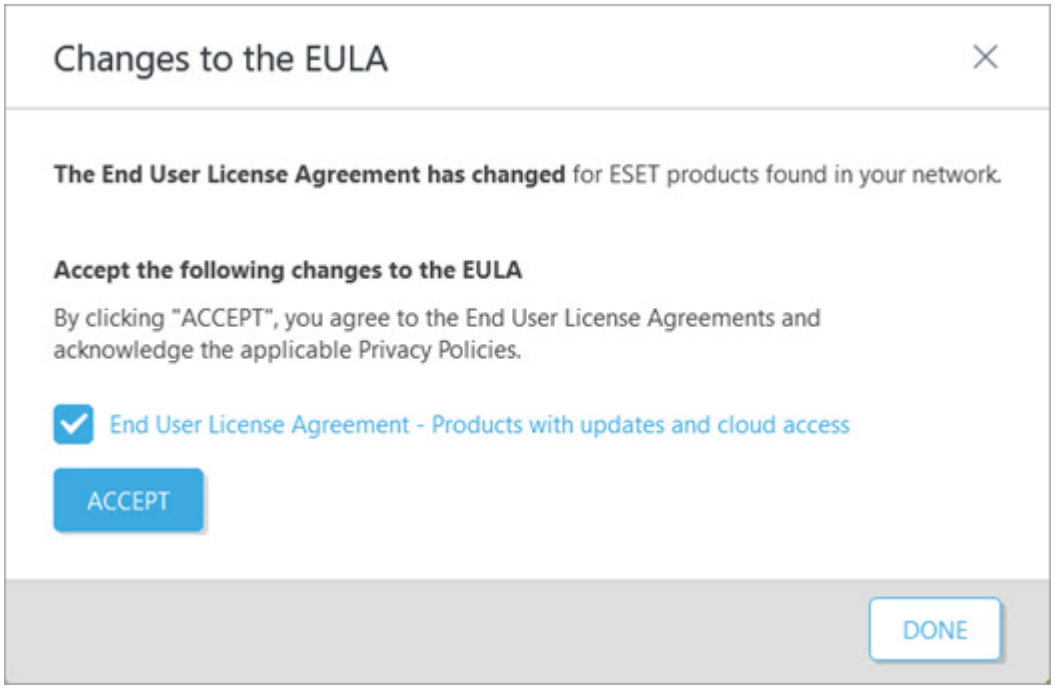
Kliknutím na **Zobrazit změněné licenční ujednání s koncovým uživatelem (EULA)** si přečtete podrobnosti o

změnách, nebo klikněte na možnost **Skrýt** a přesunete oznámení pod žlutou ikonu v horním panelu nástrojů.

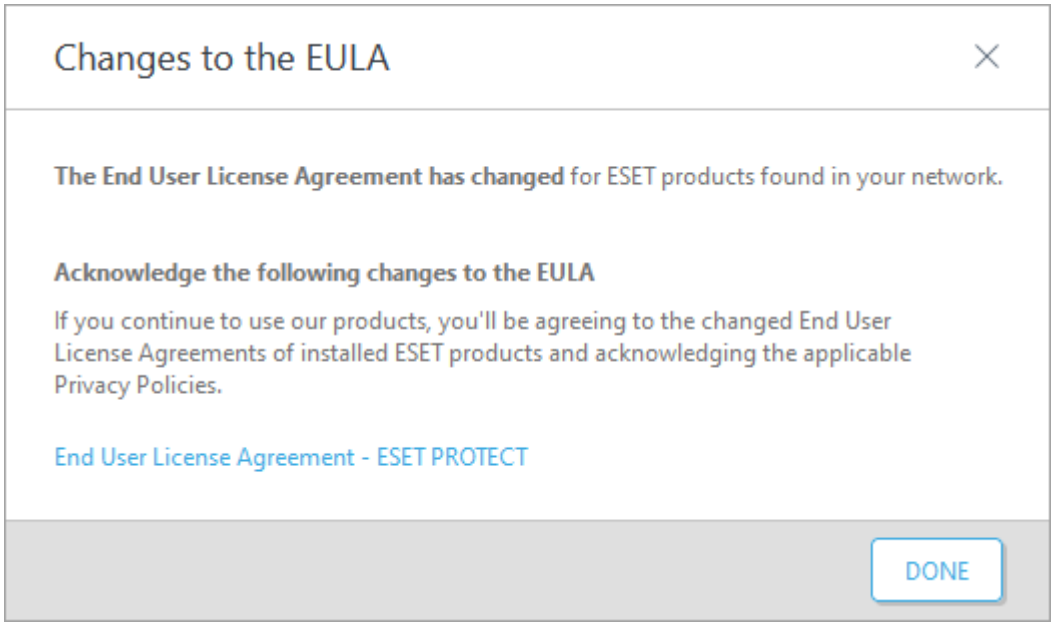


Pokud kliknete na **Zobrazit změněné licenční ujednání s koncovým uživatelem (EULA)**, zobrazí se vám nové okno s podrobnostmi o bezpečnostním produktu ESET a změnách v EULA:

- Pokud máte starší verze bezpečnostních produktů ESET, které nepodporují automatické aktualizace (například ESET Endpoint verze 8.x a starší), klikněte na tlačítko **Přijmout**, čímž schválíte aktualizované licenční ujednání a zapnete aktualizace na verze, které podporují automatické aktualizace.



- V případě, že máte firemní produkty ESET, které podporují automatické aktualizace (například ESET Endpoint verze 9 a novější), nebude nutné při aktualizaci bezpečnostních produktů ESET na nejnovější verzi aktualizaci EULA přijímat. Tlačítko **Přijmout** totiž nebude v takovém oznámení k dispozici.



Konfigurace automatické aktualizace produktů

Automatické aktualizace můžete konfigurovat pomocí politiky, která je platná pro všechny kompatibilní bezpečnostní produkty ESET, kdy její cíl jejím výchozím cílem je nejnadřazenější statická skupina **Všechna zařízení**.

Změna cílů předdefinované politiky pro automatickou aktualizaci

V hlavním menu ESET PROTECT Web Console přejděte na záložku **Politiky**. Rozbalte sekci **Předdefinované politiky** > klikněte na politiku a z rozbalovacího menu vyberte možnost **Změnit přiřazení**. Po změně cílů klikněte na tlačítko **Dokončit**.

Konfigurace automatických aktualizací

Pro konfiguraci automatických aktualizací si vytvořte **novou politiku**.

1. V hlavním menu ESET PROTECT Web Console přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika** > **Nastavení**.

2. Z rozbalovacího menu vyberte **Obecné funkce** > **Aktualizace** a nakonfigurujte politiku:

   - **Automatické přepínání profilů** – klikněte na **Upravit** a přiřaďte profil aktualizace podle profilů síťových připojení.

   - **Automatické aktualizace** – tato možnost je standardně zapnutá.

> Pro zakázání automatických aktualizací použijte přepínač na řádku **Automatické aktualizace**. Více informací, týkajících se zrušení automatických aktualizací naleznete v naší Databázi znalostí.

   - **Aktualizovat do verze** > **Vyberte verzi** – volitelně můžete definovat verzi bezpečnostního produktu ESET,

na které se má automatická aktualizace zastavit.

- Po kliknutí na možnost **Vybrat z repozitáře** vyberte požadovanou verzi.
- Při definování verze můžete použít * jako zástupný znak. Příklad: 9.*/9.0.*/9.0.2028.*.

✓ Pokud například zadáte 9.0.*, nainstalují se všechny hotfix minoritní verze 9.0.

ℹ Toto nastavení se nevztahuje na aktualizace zajišťující bezpečnost a stabilitu, které se instalují automaticky bez ohledu na definovanou verzi nebo nastavení automatických aktualizací. Další informace naleznete v článku Jaké jsou rozdíly mezi jednotlivými typy aktualizací produktu?

3. V sekci **Přiřadit** vyberte cíl (skupiny nebo jednotlivé počítače).

⚠ Ujistěte se, že předdefinovaná politika pro automatickou aktualizaci nepřepíše vaši vlastní politiku pro automatickou aktualizaci. Pro více informací přejděte do kapitoly Jak se aplikují politiky na klienta.

4. Klikněte na tlačítko **Dokončit**.

O ESET PROTECT

Pro zobrazení dialogového okna **O programu** klikněte v menu na **Nápověda** > **O programu**. V tomto okně jsou uvedeny podrobnosti o vámi používané verzi ESET PROTECT. Dále je zde uveden počet připojujících se klientů a aktivních licencí.

ℹ Při kontaktování ESET technické podpory identifikujte vaší ESET PROTECT instanci poskytnutím UUID identifikátoru. UUID své instance naleznete v menu **Nápověda** > **O programu** > **ID**, stejně tak ve svém účtu na portále **ESET Business Account** nebo **ESET MSP Administrator** v sekci **Nápověda** > **O programu** > **ID ESET PROTECT**.

ESET Connect API

ESET Connect je brána REST API mezi klientem a souborem backendových služeb ESET. ESET Connect funguje jako reverzní proxy, přijímá volání všech aplikačních programových rozhraní (API) a agreguje služby potřebné k jejich splnění a vrací příslušný výsledek.

Vytvořené integrace ESET API a API nad API bránou umožňují automatizaci monitorování, zabezpečení a správy.

ℹ Seznam změn v ESET Connnect je dostupný pouze v angličtině. Další informace naleznete v online nápovědě k ESET Connnect.

Často kladené dotazy ke Správa zranitelností a záplat

Níže naleznete nejčastější dotazy týkající se Správy zranitelností a záplat (V&PM):

Seznam aplikací

Jak často se aktualizuje seznam aplikací, na které se vztahují zranitelnosti?	• V&PM dokáže detekovat nově přidaný software na základě databáze aktualizované několikrát týdně. • Seznam je denně aktualizován na základě údajů od poskytovatele.
Jsou kontrolovány zranitelnosti aplikací, které nejsou uvedeny v seznamu podporovaných aplikací?	Ne, seznam je definitivní a aplikace, které nejsou v databázi zahrnuty, nebudou detekovány.
Zobrazuje a opravuje V&PM pouze starší zranitelné verze aplikací, nebo lze instalovat i záplaty pro zastaralé nezranitelné verze aplikací?	V&PM neprovádí instalace záplat aplikací bez CVE (identifikačního čísla zranitelnosti).

Politiky

Jsou **Povolené aplikace** a **Vyloučené aplikace** v sekci **Obecné funkce** V&PM seřazeny podle toho, zda je lze záplatovat automaticky?	Jde o seznamy povolených a zakázaných aplikací v automatické správě záplat na základě nastavení strategie **Automatického záplatování**.

Plánovač Správy zranitelností a záplat

Jak přesně se spouští kontrola V&PM?	Kontrola V&PM se spouští jednou denně pomocí plánovače V&PM na základě nastavení, které provedl administrátor v politice.
Co se stane během vybraného časového intervalu?	Kontrola se provádí jednou denně v daném časovém rozmezí. Kontrola se spustí, když se zařízení během tohoto času zapne.
Jsou úkoly kontroly a instalace záplat vzájemně propojené? V 15:50 nastavím plánovač na spuštění v čase mezi 16:00 a 19:00; spustí se pouze úloha kontroly, nebo i úloha instalace záplat? Pokud je v 16:00 spuštěna pouze úloha kontroly, kdy bude spuštěna další úloha instalace záplat?	Kontrola a instalace záplat nejsou vzájemně propojeny. Pokud je 15:50 a vy aplikujete tuto politiku, pak se kontrola spustí v 16:00 a instalace záplat se spustí v náhodném čase mezi 16:30 a 18:30. Pokud se však nacházíte mimo stanovený časový interval, bude automatická instalace záplat provedena příště. Správa záplat neprovádí instalace záplat mimo tyto hodiny.
Pokud se počítač zapne v 19:00, spustí se úloha kontroly/záplatování okamžitě, nebo se počká do 9:00? Je v plánovači nastaveno, že pokud se úloha neprovede v naplánovaném čase, instalace záplat se spustí ihned poté?	Pokud je politice nastaveno, že tyto úlohy se mají provádět mezi 17:00 a 9:00 a vy otevřete počítač v 19:00, pak se kontrola provede co nejdříve. Záplaty budou také nainstalovány, ale pouze v případě, že byl při vytváření úlohy náhodně vybrán čas spuštění před 19:00; pokud ne, počká se na zvolenou hodinu.
Pokud není v politice nastaven plánovač, kdy se spustí kontrola a instalace záplat? Výchozí interval v politice je od 17:00 do 09:00. Znamená to, že se kontrola/záplatování spustí v 17:00 + 30 minut nebo v 9:00 - 30 minut, pokud není nastavena žádná politika?	Ano, naplánovaný časový interval je stejný jako v přednastavené politice – od 17:00 do 09:00.

Jak přesně a kdy se spustí aktualizace aplikací (když jsou v plánovači nastaveny všechny dny a celý 24hodinový cyklus)?	Automatická instalace záplat je úloha, kterou plánovač provede, ale čas provedení je náhodná hodnota mezi **časem zahájení** + 30 min a **časem ukončení** - 30 min. Příklad: Administrátor nastaví v plánovači čas zahájení na pondělí v 1:00 h a čas ukončení v 11:00 h. Při aplikaci této politiky na koncovém zařízení se použije algoritmus, který vytvoří úlohu automatické instalace záplat naplánovanou na náhodný čas mezi 1:30 h a 10:30 h, například 4:21 h. To znamená, že automatická instalace záplat bude spuštěna každé pondělí ve 4:21. Stejný postup se použije také v případě, že jsou vybrány všechny dny a čas spuštění je mezi 0:00 a 24:00. (24h). Je zvolena hodnota mezi těmito časy, například 13:23. Následně se automatická instalace záplat spustí každý den ve 13:23.
Závisí doba kontroly na nastavení v plánovači V&PM (lze například kontrolu vynutit ručně úpravou nastavení plánovače), nebo o čase instalace záplaty rozhoduje pouze plánovač?	Kontrolu nelze vynutit ručně, spouští ji pouze plánovač.
Je pro kontrolu nastaven nějaký čas, nebo je časový interval náhodný?	Úloha kontroly se spustí ve vybrané dny v týdnu v zadaném čase. Například v pondělí a v pátek je **čas zahájení** 1:00. **Čas ukončení** je 11:00, což znamená, že kontrola se spustí v pondělí v 1:00 a v pátek v 1:00.

Proces

Zobrazují se na stránce Zranitelnosti také zranitelnosti operačního systému?	V&PM dokáže odhalit zranitelnosti aplikací i zranitelnosti operačního systému.
Jak se kontrola provádí?	Neprovádějí se žádné aktivní kontroly zneužitelnosti. Verze nainstalovaného softwaru se porovnávají s verzemi uvedenými v databázi jako zranitelné.
Co to znamená, že je úloha instalace záplat dokončená? Provede instalaci záplat na zařízení nebo odešle požadavek pro záplatování? Proč se aktualizační úloha zobrazuje jako úspěšně dokončená, ačkoli nebyla instalována žádná záplata?	Bezpečnostní řešení ESET pro ochranu koncových zařízení spustí příkaz v operačním systému. Neexistuje žádný jiný způsob sledování výsledků operace msiexec. Pokud je tedy příkaz úspěšně předán, je úloha ukončena s úspěšným výsledkem.
ELC a diagnostické protokoly?	Shromažďování pokročilých protokolů V&PM: 1.Stiskněte klávesu F5 > klikněte na Nástroje > Diagnostika > Zapnout rozšířené protokolování Správy zranitelností a záplat a zapněte diagnostické protokolování V&PM. 2.Reprodukujte problém. 3.Zakažte rozšířené protokolování (jinak se shromážděná data nebudou zapisovat do protokolu). 4.Sesbírejte protokoly ELC + SysInspector s ELC 4.9.0 a novějšími verzemi.
Kde najdu přehled aplikovaných a neúspěšných záplat?	Můžete vytvořit přehled se seznamem zařízení s číslem CVE a nasazenou záplatou, ale v současné době nelze vytvořit přehled s neúspěšnými úlohami, a to ani pro zobrazení výsledků úloh, kdy se záplatování provádí i zaznamenává v OS.
Jak dlouho trvá, než se příkaz k ruční aktualizaci aplikace aplikuje na koncové zařízení?	Ruční záplata se provede ihned po připojení Agenta. Příkaz pro aktualizaci vytvoří úlohu provedení záplaty aplikace, která se spustí okamžitě.

Pokud dojde k restartu, když nebyly aplikovány všechny záplaty, bude proces po restartu pokračovat?	Je pouze jedna úloha instalace záplat, která prochází všechny aplikace a instaluje záplaty jednu po druhé. Pokud některá z aplikací vyžaduje restart, zobrazí se po dokončení všech instalací zpráva o restartu. K restartu nedojde bez oznámení, ani během procházení seznamu aplikací určených k záplatování. Ačkoli se některé aplikace restartují přímo po nasazení záplat, aniž by byl uživatel informován o nutnosti restartu, nemělo by k tomu docházet. Na řešení tohoto problému již pracujeme. Pokud však zařízení restartujeme, záplatování nebude pokračovat tam, kde skončilo (i když jsme ve správném časovém intervalu), ale provede se až příště.
Je možné nainstalovat konkrétní verzi aplikace (nejen nejnovější verzi)?	Podporovaný software můžete záplatovat pouze na nejnovější verzi.
Jak bude probíhat stahování instalačních balíčků záplat? Budou umístěny na serverech společností ESET nebo jen uloženy v cache?	Přímé stahování pouze z koncového zařízení.
Má restart zařízení nějaký vliv na aktualizaci aplikací nebo správu záplat?	Ne, restart je nutný pouze v případě, že je přímo vyžadován po instalaci záplat pro konkrétní aplikaci. V takovém případě uživatele upozorníme, že je nutný restart.

Bezpečnostní dokumentace pro ESET PROTECT

Úvod

Účelem tohoto dokumentu je shrnout bezpečnostní zásady a postupy uplatňované v rámci služby ESET PROTECT Cloud. Bezpečnostní zásady a postupy jsou navrženy tak, aby byla zajištěna důvěrnost, integrita a dostupnost dat zákazníků. Mějte na paměti, že se bezpečnostní zásady a postupy mohou kdykoli změnit.

Rozsah

Účelem tohoto dokumentu je shrnout bezpečnostní postupy a zásady uplatňované v ESET PROTECT Cloud infrastruktuře, stejně tak infrastruktuře, organizaci, personálních a provozních procesech souvisejících s ESET Business Account (dále jen "EBA"), ESET MSP Administrator (dále jen "EMA"). Mezi bezpečnostní zásady a postupy patří:

1. Politiky bezpečnosti informací
2. Organizace bezpečnosti informací
3. Bezpečnost lidských zdrojů
4. Řízení aktiv
5. Řízení přístupu
6. Kryptografie
7. Fyzická bezpečnost a bezpečnost prostředí
8. Bezpečnost provozu
9. Bezpečnost komunikací
10. Akvizice, vývoj a údržba systému
11. Vztah s dodavateli
12. Řízení incidentů bezpečnosti informací
13. Aspekty řízení kontinuity organizace z hlediska bezpečnosti informací
14. Soulad s požadavky

Bezpečnostní koncept

Společnost ESET s.r.o. je držitelem certifikátu ISO 27001:2013 s integrovaným systémem správy, který pokrývá službu ESET PROTECT Cloud, EBA a EMA.

Koncept informační bezpečnosti proto používá standard ISO 27001 k implementaci bezpečnostní strategie vícevrstvé ochrany při aplikování bezpečnostních zásad na vrstvě sítové, operačních systémů, databází, aplikací, zaměstnanců a provozních procesů. Použité bezpečnostní postupy a zásady se mají vzájemně překrývat a doplňovat.

Bezpečnostní zásady a postupy

1. Politiky bezpečnosti informací

Společnost ESET uplatňuje politiky informační bezpečnosti, které pokrývají všechny aspekty standardu ISO 27001, včetně řízení bezpečnosti informací a bezpečnostní zásady a postupy. Politiky jsou každoročně revidovány a po významných změnách aktualizovány, aby byla zajištěna jejich kontinuální vhodnost, přiměřenost a účinnost.

Společnost ESET provádí každoroční revize těchto politik a kontroly interní bezpečnosti za účelem zajištění souladu s jejich ustanoveními. V případě nedodržování politik informační bezpečnosti jsou zaměstnancům společnosti ESET uložena disciplinární opatření a dodavatelům smluvní sankce, které mohou vést až k ukončení smlouvy.

2. Organizace bezpečnosti informací

Organizace informační bezpečnosti služby ESET PROTECT Cloud se skládá z více týmů a jednotlivců zapojených do informační bezpečnosti a IT, včetně:

- výkonného managementu společnosti ESET,
- týmů interní bezpečnosti společnosti ESET,
- IT týmů podnikových aplikací,
- dalších podpůrných týmů.

Odpovědnost za informační bezpečnost je přidělována v souladu se zavedenými politikami informační bezpečnosti. Interní procesy jsou identifikovány a posuzovány z hlediska rizik vyplývajících z neoprávněné nebo neúmyslné modifikace nebo zneužití aktiv společnosti ESET. Při rizikových nebo citlivých činnostech souvisejících s interními procesy je za účelem snížení rizika uplatňován princip oddělení odpovědností.

Právní tým společnosti ESET je zodpovědný za kontakt s orgány státní správy, včetně regulačních orgánů v oblasti kybernetické bezpečnosti a ochrany osobních údajů. Tým interní bezpečnosti společnosti ESET je zodpovědný za kontakt se zájmovými skupinami, jako je například ISACA. Výzkumné týmy společnosti ESET jsou zodpovědné za komunikaci s dalšími společnostmi zabývajícími se bezpečností a širší komunitou pro kybernetickou bezpečnosti.

Informační bezpečnost je zohledněna v projektovém řízení pomocí aplikovaného rámce řízení projektů od koncepce až po dokončení projektu.

Práci na dálku a práci z domova pokrývají politiky implementované na mobilních zařízeních, které zahrnují použití silné kryptografické ochrany dat na mobilních zařízeních při pohybu mezi nedůvěryhodnými sítěmi. Bezpečnostní kontroly na mobilních zařízeních jsou navrženy tak, aby fungovaly nezávisle na interních sítích a interních systémech společnosti ESET.

3. Bezpečnost lidských zdrojů

Společnost ESET používá standardní postupy v oblasti lidských zdrojů, včetně politik určených k dodržování informační bezpečnosti. Tyto postupy jsou platné po celý životní cyklus zaměstnance a vztahují se na všechny týmy, které mají přístup k prostředí služby ESET PROTECT Cloud.

4. Řízení aktiv

Infrastruktura služby ESET PROTECT Cloud je součástí katalogu aktiv společnosti ESET s určeným vlastnictvím a pravidly aplikovanými podle typu a citlivosti aktiv. Společnost ESET má definované interní klasifikační schéma. Veškerá data a konfigurace související se službou ESET PROTECT Cloud jsou klasifikována jako důvěrná.

5. Řízení přístupu

Politika řízení přístupu společnosti ESET upravuje každý přístup v rámci služby ESET PROTECT Cloud. Řízení přístupu se nastavuje na úrovni infrastruktury, síťových služeb, operačního systému, databáze a aplikace. Správa úplného přístupu uživatelů na úrovni aplikace je autonomní. Jednotné přihlášení (SSO) v rámci služby ESET PROTECT Cloud a ESET Business Account řídí centrální poskytovatel identity, který zajišťuje, že uživatel má přístup pouze oprávněnému tenantu. Aplikace používá standardní oprávnění služby ESET PROTECT Cloud za účelem zajištění kontroly přístupu k tenantu na základě rolí.

Přístup k backendu je výhradně omezen na oprávněné osoby a role. Při správě přístupu zaměstnanců společnosti ESET k infrastruktuře a sítím služby ESET PROTECT Cloud se využívají standardní procesy společnosti ESET pro (de)registraci uživatelů, (de)provisioning, správu oprávnění a kontrolu přístupových oprávnění uživatelů.

Pro ochranu přístupu ke všem datům souvisejícím se službou ESET PROTECT Cloud se používá silné ověřování.

6. Kryptografie

Za účelem ochrany dat souvisejících se službou ESET PROTECT Cloud se používá silná kryptografie k šifrování uložených a přenášených dat. Certifikáty pro veřejné služby vydává všeobecně uznávaná certifikační autorita. Klíče používané v rámci ESET PROTECT Cloud infrastruktury jsou spravovány prostřednictvím interní infrastruktury veřejných klíčů společnosti ESET. Data uložená v databázi jsou chráněna šifrovacími klíči generovanými v cloudu. Všechna zálohovaná data jsou chráněna klíči spravovanými společností ESET.

7. Fyzická bezpečnost a bezpečnost prostředí

Vzhledem k tomu, že ESET PROTECT Cloud a ESET Business Account jsou cloudové služby, spoléháme se na environmentální a fyzické zabezpečení platformy Microsoft Azure. Microsoft Azure využívá certifikovaná datová centra s efektivními fyzickými bezpečnostními opatřeními. Fyzické umístění datového centra závisí na zákazníkem vybrané lokalitě. Data zákazníků jsou při svém přenosu z cloudového prostřední chráněna silnou kryptografií. (například při přenosu na fyzické záložní úložiště dat).

8. Bezpečnost provozu

Služba ESET PROTECT Cloud je provozována automatizovanými prostředky na základě přísných provozních postupů a konfiguračních šablon. Všechny změny, včetně změn v konfiguraci a nasazení nového balíčku, se nasazením do produkčního prostředí schvalují a testují ve vyhrazeném testovacím prostředí. Vývojová, testovací a produkční prostředí jsou od sebe oddělená. Data služby ESET PROTECT Cloud se nacházejí výhradně v produkčním prostředí.

Prostředí služby ESET PROTECT Cloud je sledováno prostřednictvím monitorování provozu za účelem rychlé

identifikace problémů a zajištění dostatečné kapacity všem službám na úrovni sítě a hostitele.

Veškerá konfigurační data jsou uložena v našich pravidelně zálohovaných úložištích, aby bylo možné automaticky obnovit konfiguraci prostředí. Zálohovaná data služby ESET PROTECT Cloud jsou ukládána on-site i off-site.

Zálohy jsou šifrovány a v rámci testování kontinuity je pravidelně ověřována jejich obnovitelnost.

Audit systémů je prováděn dle interních standardů a směrnic. Protokoly a auditní záznamy z infrastruktury, operačního systému, databáze, aplikačních serverů a prvků zabezpečení se shromažďují nepřetržitě. Auditní záznamy jsou dále zpracovávány týmy IT a interní bezpečností za účelem identifikace provozních a bezpečnostních anomálií a incidentů informační bezpečnosti.

Společnost ESET se řídí všeobecným technickým procesem pro správu zranitelností k řízení zranitelností v infrastruktuře ESET, včetně služby ESET PROTECT Cloud a dalších produktech ESET. Součástí tohoto procesu je proaktivní skenování zranitelností a opakované penetrační testování infrastruktury, produktů a aplikací.

Společnost ESET má zavedené interní směrnice pro bezpečnost interní infrastruktury, sítí, operačních systémů, databází, aplikačních serverů a aplikací. Jejich dodržování je kontrolováno prostřednictvím monitorování technického souladu a našeho programu interního auditu informační bezpečnosti.

9. Bezpečnost komunikací

Prostředí služby ESET PROTECT Cloud je segmentováno pomocí nativních možností dostupných v cloudu, kdy přístup k síti je omezen pouze na nezbytné služby v rámci síťových segmentů. Dostupnost síťových služeb je dosaženo pomocí nativních možností dostupných v cloudu, jako jsou zóny dostupnosti, vyrovnávání zátěže a redundance. Komponenty vyhrazené pro vyrovnávání zátěže jsou nasazeny za účelem ověřování a směrování koncových zařízení k instanci služby ESET PROTECT Cloud. Síťový provoz je nepřetržitě monitorován na výskyt provozních a bezpečnostních anomálií. Potenciální útoky lze vyřešit pomocí nativních možností dostupných v cloudu nebo nasazených bezpečnostních řešení. Veškerá síťová komunikace je šifrována pomocí obecně dostupných technik, včetně protokolů IPsec a TLS.

10. Akvizice, vývoj a údržba systému

Vývoj systémů služby ESET PROTECT Cloud probíhá v souladu s politikou pro vývoj bezpečného softwaru společnosti ESET. Týmy interní bezpečnosti se na vývoji služby ESET PROTECT Cloud podílejí již od počáteční fáze a dohlížejí na všechny aspekty vývoje a údržby. Tým interní bezpečnosti definuje a kontroluje plnění bezpečnostních požadavků v různých fázích vývoje softwaru. Bezpečnost všech služeb, včetně nově vyvinutých, je od jejich vydání průběžně testována.

11. Vztah s dodavateli

Relevantní dodavatelský vztah je veden podle platných směrnic společnosti ESET, které upravují řízení vztahů se zákazníky a smluvní požadavky z hlediska informační bezpečnosti a ochrany osobních údajů. Kvalita a bezpečnost služeb poskytovaných poskytovatelem kritických služeb podléhá pravidelnému hodnocení.

Dále společnost ESET u služby ESET PROTECT Cloud uplatňuje princip přenositelnosti, aby se zabránilo závislosti na konkrétním dodavateli.

12. Řízení incidentů bezpečnosti informací

Správa incidentů v oblasti informační bezpečnosti souvisejících se službou ESET PROTECT Cloud je řízena podobně jako u jiných infrastruktur společnosti ESET a opírá se o definované postupy řešení incidentů. Role v rámci reakce na incidenty jsou definovány a rozděleny mezi více týmů, nejen z oblasti IT, bezpečnosti, právní, lidských zdrojů,

vztahů s veřejností a výkonného managementu. Incidenty třídí tým interní bezpečnosti, které si následně přebírá sestavený tým zodpovědný za řešení incidentu. Tento tým zajistí další koordinaci ostatních týmů, které se podílejí na řešení incidentu. Tým interní bezpečnost je rovněž zodpovědný za shromažďování důkazů a získaných poznatků. Vznik incidentu a jeho řešení je sděleno dotčeným stranám. Právní tým společnosti ESET je v případě potřeby zodpovědný za informování regulačních orgánů v souladu se všeobecným nařízení o ochraně osobních údajů (GDPR) a aktem EU o kybernetické bezpečnosti EU transponujícím směrnici o bezpečnosti sítí a informačních systémů (NIS).

13. Aspekty řízení kontinuity organizace z hlediska bezpečnosti informací

Kontinuita provozu služby ESET PROTECT Cloud je zakódována v robustní architektuře, která maximalizuje dostupnosti poskytovaných služeb. V případě katastrofického selhání všech redundantních uzlů komponent služby ESET PROTECT Cloud, nebo služby ESET PROTECT Cloud samotné, je možné provést kompletní obnovení z externích záloh a konfiguračních dat. Proces obnovy je pravidelně testován.

14. Soulad s požadavky

Dodržování regulačních a smluvních požadavků souvisejících se službou ESET PROTECT Cloud je pravidelně posuzováno a přezkoumáváno podobně jako jiná infrastruktura a procesy společnosti ESET. Provádějí se nezbytná opatření k zajištění soustavného dodržování požadavků. Společnost ESET je registrována jako poskytovatel digitálních služeb v oblasti cloud computingu, mezi které spadají další služby společnosti ESET včetně ESET PROTECT Cloud. Mějte na paměti, že aktivity společnost ESET týkající se dodržování předpisů nemusí nutně znamenat, že jsou splněny celkové požadavky zákazníků na dodržování předpisů.

Podmínky použití

Platné od 29. září 2023 | Zobrazit předchozí verzi Podmínek použití | Porovnat změny

Tyto podmínky použití (dále jen „Podmínky“) představují zvláštní smlouvu mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 85101 Bratislava, Slovak Republic, s obchodním registračním číslem 31333532 (dále jen „ESET“ nebo „Poskytovatel“) a vámi, fyzickou anebo právnickou osobou (dále jen „Vy“ nebo „Uživatel”) přistupující k účtu pro správu, ESET PROTECT Cloud, a používající online služby, které vlastní a řídí společnost ESET (dále jen „Účet“), které jsou všechny specifikovány v příslušné dokumentaci přístupné prostřednictvím ESET Online nápovědy (dále jen „dokumentace“). Pokud využíváte Účet jménem organizace, souhlasíte s těmito Podmínkami jménem dané organizace a zaručujete se, že máte oprávnění zavázat tuto organizaci těmito Podmínkami. V takovém případě se pojmy „Uživatel“ a „Vy“ budou vztahovat na tuto organizaci. Tyto Podmínky použití si pozorně přečtěte. Tyto Podmínky použití si pozorně přečtěte. Vztahují se také na služby poskytované společností ESET prostřednictvím nebo ve vztahu k tomuto Účtu. Konkrétní podmínky používání jednotlivých služeb nad rámec těchto Podmínek jsou uváděny u jednotlivých služeb, přičemž jejich přijetí je součástí procesu aktivace služeb.

Zabezpečení a ochrana dat

Účet zajišťuje přístup ke službám poskytovaným společností ESET. Pro vytvoření a používání Účtu je vyžadováno úplné jméno uživatele, název společnosti, země, platná e-mailová adresa, telefonní číslo, informace o licenci a statistická data, stejně tak z důvodu zajištění a údržby služeb, které jsou prostřednictvím Účtu dostupné. Souhlasíte s tím, že na servery Poskytovatele anebo jeho obchodních partnerů mohou být shromažďovány a přenášeny údaje, které mají za účel zabezpečit funkčnost a oprávněnost používání Softwaru a ochranu práv Poskytovatele. V souvislosti s uzavřením těchto Podmínek jsou Poskytovatel nebo obchodní partneři oprávněni pro účely poskytování podpory a plnění těchto Podmínek přenášet, zpracovávat a uchovávat údaje, které Vás

umožní identifikovat v nevyhnutelném rozsahu. Jste oprávněni používat Účet výhradně za účelem a způsobem, pro který je určen podle těchto Podmínek, podmínek jednotlivých služeb a dokumentace.

Za zabezpečení vašeho Účtu a přihlašovacích údajů zodpovídáte vy. Společnost ESET není zodpovědná za žádné ztráty ani škody v důsledku nedodržení této vaší povinnosti zajišťovat bezpečnost. Uživatel je dále zodpovědný za jakoukoli aktivitu související s Účtem, ať již k nim má nebo nemá povolení. V případě napadení či zneužití Účtu neprodleně oznamte tuto skutečnost Poskytovateli.

Za účelem zajištění služby pro správu Účtu, je vyžadován sběr dat z připojených spravovaných zařízení společně s informacemi o správě (dále jako "Data"). Data poskytujete společnosti ESET výhradně za účelem zajištění služby pro správu Účtu. Data jsou zpracovávána a uchovávána v souladu s bezpečnostními politikami a postupy společnosti ESET, stejně tak v souladu se Zásadami ochrany osobních údajů.

Údaje i další protokoly týkající se Účtu budou uloženy v souladu s politikou uchovávání protokolů.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů.

Zabezpečení dat API

Používáním rozhraní pro programování aplikací (dále jen "API") berete na vědomí a souhlasíte s tím, že jakákoli data nebo informace přenášené do API nebo přijaté z API mohou opustit zabezpečenou infrastrukturu společnosti ESET nebo do ní vstoupit. To zahrnuje mimo jiné pokyny, požadavky, příkazy nebo směrnice přijaté ze systémů nebo sítí třetích stran. Jste srozuměni s tím, že společnost ESET nemůže zaručit bezpečnost nebo důvěrnost dat nebo informací přenášených do API nebo přijatých API, a že společnost ESET nenese odpovědnost za neoprávněný přístup, zveřejnění, ztrátu, poškození nebo zneužití těchto dat nebo informací.

Prohlašujete a zaručujete, že jste zavedli vhodná bezpečnostní opatření k ochraně údajů a informací přenášených do rozhraní API a veškerých příkazů obdržených od třetích stran prostřednictvím rozhraní API. Souhlasíte s tím, že nesete výhradní odpovědnost za bezpečnost a důvěrnost dat a informací poté, co opustí nebo vstoupí do infrastruktury společnosti ESET, jakož i za interpretaci a provedení jakýchkoli příkazů obdržených prostřednictvím API. Berete na vědomí, že přebíráte veškerá rizika spojená s interakcí API se systémy nebo sítěmi třetích stran, mimo jiné včetně rizika škodlivé interference.

Fair Use Policy

Jste povinni dodržovat technická omezení stanovená v dokumentaci. Souhlasíte s tím, že budete Účet a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Uživatelů, aby mohl služby využívat nejvyšší možný počet Uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Účtu a odstranění dat a informací.

Poskytovatel si dále vyhrazuje právo omezit počet zařízení spravovaných Účtem. Nemůžete přidat a spravovat více než 50000 koncových zařízení.

Omezení používání

Použití Účtu je striktně omezeno na správu produktů aktivovaných pomocí licencí vhodných pro cloud. ESET Full Disk Encryption se smí používat pouze na koncových zařízeních s bezpečnostními produkty pro koncová zařízení nainstalovanými a aktivovanými pomocí licencí vhodných pro cloud nebo samostatně, aniž by byl překročen celkový počet získaných jednotek licencí vhodných pro cloud. Poskytovatel si dále vyhrazuje právo omezit počet produktů spravovaných Účtem v případě Vašeho nesouladu s tímto omezením.

Poloha

Poskytovatel Vám může umožnit výběr lokality pro hostování vašeho Účtu, zahrnující Poskytovatelem doporučenou lokalitu. Berete na vědomí, že výběr jiné než doporučené lokality může ovlivnit Váš uživatelský zážitek. Na základě zvolené polohy může platit Smlouva o ochraně údajů uvedená v dodatku č. 2 této Dohody a Standardní smluvní body uvedené v Dodatku č. 3 této Dohody. ESET si vyhrazuje právo kdykoli změnit konkrétní lokalitu bez předchozího upozornění za účelem vylepšení poskytovaných služeb poskytovaných společností ESET v souladu s Vašimi preferencemi na lokalitu (například Evropská unie).

Software

Společnost ESET nebo její příslušní dodavatelé vlastní nebo mohou uplatňovat autorská práva na veškerý software, který je k dispozici stránkách účtu (dále jako „Software“). Software je možné používat jen v souladu s licenční smlouvou s koncovým uživatelem (dále jako „EULA“). Smlouva EULA se poskytuje spolu se Softwarem nebo je jeho součástí. Software dodaný se smlouvou EULA nelze nainstalovat bez souhlasu uživatele se smlouvou EULA. Další informace týkající se licencování, autorských práv, dokumentace a ochranných známek se nacházejí v Právních informacích.

Restrikce

Nesmíte Účet kopírovat, šířit, oddělovat jeho části anebo vytvářet od Účtu odvozená díla. Při používání Účtu jste povinný dodržovat následovné omezení:

(a) Účet nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Účtu anebo kopií Účtu jinak, než je výslovně uvedené v této Dohodě.

(b) Účet nesmíte prodat, sublicencovat, pronajmout anebo pronajmout si, vypůjčit si ho anebo používat na poskytování komerčních služeb.

(c) Účet nesmíte zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusit získat zdrojový kód Účtu s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

(d) Souhlasíte s tím, že budete používat Účet jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Účet používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

Vyloučení odpovědnosti

JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE ÚČET A SLUŽBY JSOU POSKYTOVÁNY „TAK JAK JSOU", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ PLATNÝMI PRÁVNÍMI PŘEDPISY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE ÚČET NEBO SLUŽBY NEPORUŠUJÍ ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. POSKYTOVATEL ANI ŽÁDNÁ JINÁ STRANA NEPOSKYTUJE ŽÁDNOU ZÁRUKU, ŽE ÚČET NEBO SLUŽBY BUDOU SPLŇOVAT VAŠE POŽADAVKY ANI ŽE ÚČET NEBO SLUŽBY BUDOU FUNGOVAT NEPŘERUŠENĚ NEBO BEZCHYBNĚ. VEŠKEROU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR A POUŽÍVÁNÍ ÚČTU A SLUŽEB NA DOSAŽENÍ ZAMYŠLENÝCH VÝSLEDKŮ A ZA VÝSLEDKY Z NICH ZÍSKANÉ PŘEBÍRÁTE VY.

Tyto Podmínky nezakládají na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v těchto Podmínkách žádné jiné závazky.

Omezení zodpovědnosti

V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ ZÁKONY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO DODAVATELÉ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ ČINNOSTI, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, POJISTNÉ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, AŤ UŽ NA ZÁKLADĚ SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT ÚČET, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL, JEHO DODAVATELÉ ANEBO PŘIDRUŽENÉ SPOLEČNOSTI BYLI UVĚDOMĚNÍ O MOŽNOSTI VZNIKU TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ, DODAVATEŮ ANEBO PŘIDRUŽENÝCH SPOLEČNOSTÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA DANOU SLUŽBU NEBO ÚČET.

Soulad se zákony o kontrole obchodu

(a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z těchto Podmínek, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z těchto Podmínek, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována (právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

(b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení oddílu (a) bodu Soulad se zákony o kontrole obchodu těchto Podmínek; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z těchto Podmínek mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

(c) Nic v těchto Podmínkách není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

Rozhodné právo a jazyk

Tyto Podmínky se řídí a musí být vykládány v souladu se zákony Slovenské republiky. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Jste-li spotřebitelem s obvyklým bydlištěm v EU, vztahuje se na vás také další ochrana, kterou vám poskytují závazná ustanovení právních předpisů platných v zemi vašeho bydliště.

Výslovně souhlasíte, že řešením jakýchkoli sporů nebo nároků vůči Poskytovateli nebo sporů a nároků souvisejících s vaším používáním Softwaru, Účtu nebo Služeb nebo sporů vyplývající z těchto Podmínek nebo Zvláštních podmínek (pokud jsou k dispozici) bude pověřen příslušný Obvodní soud v Bratislavě I. (Slovenská republika) a výslovně souhlasíte s výkonem jurisdikce tímto soudem. Jste-li spotřebitelem s obvyklým bydlištěm v EU, můžete také uplatnit nárok na vymáhání svých spotřebitelských práv v místě příslušné jurisdikce nebo v zemi EU, ve které žijete. Kromě toho můžete také použít online platformu pro řešení sporů, kterou naleznete zde: https://ec.europa.eu/consumers/odr/. Před oficiálním uplatněním nároku nás však prosím nejprve kontaktujte.

V případě jakýchkoli rozporů mezi jazykovými verzemi těchto Podmínek bude vždy rozhodující anglická verze, která je dostupná zde.

Všeobecná ustanovení

Společnost ESET si vyhrazuje právo kdykoli upravit tyto Podmínky a dokumentaci nebo jakékoli jejich části, a to aktualizací příslušného dokumentu tak, aby se do něj promítly změny zákonů nebo změny týkající se účtu. O jakékoli změně Podmínek v rámci účtu budete informováni. Pokud s danými změnami Podmínek nebudete souhlasit, můžete účet zrušit. Pokud po upozornění na tyto změny svůj účet nezrušíte, jste vázáni případnými dodatky nebo úpravami těchto Podmínek. Doporučujeme vám pravidelně navštěvovat tuto stránku a přečíst si aktuální Podmínky, které se vztahují k používání účtu.

Oznámení

Všechna oznámení je třeba doručit na následující adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Dodatek č.1

ESET Management Agent EULA

Dodatek č.2

Smlouva o zpracování údajů

Dodatek č.3

Standardní smluvní body

ESET Management Agent EULA

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH**

ÚDAJŮ.

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 („ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou („Vy“ anebo „Koncový uživatel”) Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do

paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro fungování Softwaru a pro jeho aktualizaci a upgrade. Poskytovatel je oprávněn vydávat aktualizace nebo upgrade Softwaru („Aktualizace“), avšak není povinen Aktualizace poskytovat. Tato funkce je při standardním nastavení Softwaru zapnutá, proto se Aktualizace nainstalují automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Aktualizací zakázal. Pro poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

Poskytování jakýchkoli aktualizací může podléhat „Zásadám konce životnosti“, které jsou k dispozici na webu https://go.eset.com/eol_business. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody.** Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ INSTALACÍ, POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI

TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu,

zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované

změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

DODATEK K DOHODĚ

Komunikace a Správa dat. Na komunikaci a správu údajů se vztahují následující dodatečná ustanovení:

Tento Software obsahuje funkci, která umožňuje přenos informací mezi počítačem a softwarem pro vzdálenou správu. Informace, které jsou předmětem přenosu, obsahují data o správě, jako jsou informace o hardwaru a softwaru na spravovaném počítači, a pokyny pro správu ze softwaru pro vzdálenou správu. Další obsah dat přenášených z počítače je určen nastavením softwaru nainstalovaného v počítači. Obsah pokynů ze softwaru pro správu je určen nastavením softwaru pro vzdálenou správu.

EULAID: EULA-PRODUCT-AGENT; 3537.0

Smlouva o zpracování údajů

Podle požadavků Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen GDPR) vstupujete vy (dále jen správce) a poskytovatel (dále jen zpracovatel) do smluvního vztahu zpracování dat, abyste definovali podmínky a ujednání pro zpracování osobních údajů, způsob jejich ochrany, jakož i vymezení dalších práv a povinností obou stran při zpracovávání osobních údajů subjektů údajů jménem správce v průběhu provádění předmětu těchto podmínek jako hlavní smlouvy.

1. **Zpracování osobních údajů.** Služby poskytované v souladu s těmito podmínkami zahrnují zpracování informací týkajících se identifikované nebo identifikovatelné fyzické osoby uvedené v zásadách ochrany osobních údajů (dále jen osobní údaje).

2. **Oprávnění.** Správce opravňuje zpracovatele zpracovávat osobní údaje, což zahrnuje následující:

(i) Účelem zpracování se rozumí poskytování služeb v souladu s těmito podmínkami. Zpracovatel je oprávněn zpracovávat osobní údaje jménem správce pouze v souvislosti s poskytováním služeb požadovaných správcem. Veškeré informace shromážděné pro další účely jsou zpracovávány mimo smluvní vztah mezi správcem a zpracovatelem.

(ii) Obdobím zpracování se rozumí období od vstupu do spolupráce za těchto podmínek do ukončení služeb.

(iii) Rozsah a kategorie osobních údajů. Služby jsou určeny pouze ke zpracování obecných osobních údajů. Za určení rozsahu osobních údajů však odpovídá výhradně správce.

(iv) Subjektem údajů se rozumí fyzická osoba jako oprávněný uživatel zařízení správce.

(v) Operacemi zpracování se rozumějí všechny operace nezbytné pro zpracování.

(vi) Doloženými pokyny se rozumějí instrukce popsané v těchto podmínkách, jejich přílohách, zásadách ochrany osobních údajů a dokumentaci služeb. Správce odpovídá za právní přípustnost zpracování osobních údajů zpracovatelem z hlediska příslušných platných ustanovení právních předpisů o ochraně osobních údajů.

3. **Povinnosti zpracovatele**. Zpracovatel je povinen:

(i) zpracovávat osobní údaje pouze na základě doložených pokynů a pro účely definované v podmínkách, jejich přílohách, zásadách ochrany osobních údajů a dokumentaci služeb,

(ii) poučit osoby oprávněné zpracovávat osobní údaje (dále označované jako „autorizované osoby“) o jejich právech a povinnostech podle nařízení GDPR a o jejich odpovědnosti v případě porušení povinností a zajistit, aby se autorizované osoby zavázaly k zachovávání důvěrnosti a dodržování zdokumentovaných pokynů.

(iii) implementovat a dodržovat opatření popsaná v podmínkách, jejich přílohách, zásadách ochrany osobních údajů a dokumentaci služeb,

(iv) pomáhat správci při vyřizování žádostí subjektů údajů týkající se jejich práv. Zpracovatel nesmí opravit, vymazat nebo omezit zpracování osobních údajů bez pokynu správce. Veškeré žádosti subjektu údajů týkající se osobních údajů zpracovávaných jménem správce budou neprodleně předány správci.

(v) pomáhat správci s oznamováním porušení zabezpečení osobních údajů dozorčímu orgánu a subjektu údajů, Zpracovatel je povinen upozornit správce na jakýkoli problém při zpracování osobních údajů nebo se zabezpečením osobních údajů ihned po jeho zjištění. Zpracovatel bude v přiměřeném rozsahu spolupracovat při vyšetřování a nápravě takového problému a přijme přiměřená opatření k omezení dalších negativních dopadů.

(vi) na základě volby správce vymazat nebo vrátit všechny osobní údaje správci po skončení období zpracování. Správce se zavazuje informovat zpracovatele o svém rozhodnutí do deseti (10) dnů od konce období zpracování. Tímto ustanovením není dotčeno právo zpracovatele uchovávat osobní údaje v nezbytném rozsahu pro účely archivace ve veřejném zájmu, pro účely vědeckého výzkumu, pro statistické účely nebo pro účely stanovení, výkonu nebo obrany právních nároků.

(vii) vést aktuální registr všech kategorií zpracovatelských činností, které zpracovatel provedl jménem správce;

(viii) zpřístupnit správci všechny informace nezbytné k prokázání dodržování těchto podmínek, jejich příloh, zásad ochrany osobních údajů a dokumentace služeb. V případě auditu nebo kontroly zpracování osobních údajů ze strany správce je správce povinen informovat zpracovatele písemně nejméně třicet (30) dnů před plánovaným auditem nebo kontrolou.

4. **Zapojení dalšího zpracovatele.** Zpracovatel je oprávněn zapojit jiného zpracovatele za účelem provádění zvláštních zpracovatelských činností, jako je poskytování cloudového úložiště a infrastruktury pro služby v souladu s těmito podmínkami, jejich přílohami, zásadami ochrany osobních údajů a dokumentací služeb. V současné době společnost Microsoft poskytuje cloudové úložiště a infrastrukturu jako součást cloudové služby Azure. I v tomto případě musí být zpracovatel jediným kontaktním subjektem a stranou, která je odpovědná za dodržování pravidel. Zpracovatel se tímto zavazuje informovat správce o jakémkoli přidání dalšího zpracovatele nebo nahrazení zpracovatele, aby bylo možné vznést proti takové změně námitku.

5. **Území zpracování.** Zpracovatel zajišťuje, že se zpracování uskuteční v Evropském hospodářském prostoru nebo na základě rozhodnutí správce v zemi označené rozhodnutím Evropské komise jako bezpečné. V případě převodů a zpracování umístěných mimo Evropský hospodářský prostor nebo v zemi, která byla rozhodnutím Evropské komise na žádost správce označena jako bezpečná, platí standardní smluvní doložky.

6. **Zabezpečení.** Zpracovatel je certifikován na ISO 27001:2013 a používá soustavu ISO 27001 k implementaci bezpečnostní strategie vrstvené obrany při použití prvků zabezpečení ve vrstvě sítě, operačních systémů, databází, aplikací, zaměstnanců a provozních procesů. Dodržování regulačních a smluvních požadavků je pravidelně posuzováno a přezkoumáváno podobně jako jiná infrastruktura a operace zpracovatele. Provádějí se nezbytná opatření k zajištění soustavného dodržování požadavků. Zpracovatel zajistil zabezpečení údajů pomocí systému řízení bezpečnosti (ISMS) na základě ISO 27001. Bezpečnostní dokumentace zahrnuje především dokumenty zásad pro bezpečnost informací, fyzickou bezpečnost a bezpečnost zařízení, správu incidentů, postupy při úniku dat a bezpečnostních incidentech atd.

7. **Technická a organizační opatření**. Zpracovatel bude chránit osobní údaje před neúmyslným nebo nezákonným poškozením či zničením, neúmyslnou ztrátou, změnou, neoprávněným přístupem a vyzrazením. Za tímto účelem zpracovatel přijme adekvátní technická a organizační opatření odpovídající režimu zpracování a riziku, které zpracování představuje pro práva subjektů údajů, v souladu s požadavky GDPR. Podrobný popis technických a organizačních opatření je uveden v zásadách zabezpečení.

8. **Kontaktní informace zpracovatele.** Všechna oznámení, žádosti, požadavky a jiná sdělení týkající se ochrany osobních údajů je třeba adresovat společnosti ESET, spol. s.r.o.: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standardní smluvní body

ODDÍL I

Doložka 1 Účel a rozsah působnosti

(a) Účelem těchto standardních smluvních doložek je zajistit dodržování požadavků uvedených v nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) (1), pokud jde o předávání osobních údajů do třetí země.

b) Smluvní strany:

(i) fyzická nebo právnická osoba či osoby, orgán či orgány veřejné moci, agentura či agentury nebo jiný subjekt či jiné subjekty (dále jen "subjekt" či "subjekty") předávající osobní údaje, uvedené v příloze I části A (dále jen "vývozce údajů"), a

(ii) subjekt či subjekty ve třetí zemi, přijímající přímo nebo nepřímo prostřednictvím jiného subjektu, jenž je rovněž stranou těchto doložek, osobní údaje od vývozce údajů, uvedené v příloze I části A (dále jen "dovozce údajů"),

se dohodly na těchto standardních smluvních doložkách (dále jen "Doložky").

(c) Tyto doložky se použijí s ohledem na předávání osobních údajů podle přílohy I části B.

(d) Dodatek k těmto doložkám obsahující přílohy, na něž se v těchto doložkách odkazuje, tvoří nedílnou součást těchto doložek.

Doložka 2 Účinek a neměnnost doložek

Tyto doložky stanoví vhodné záruky, včetně vymahatelných práv subjektu údajů a účinné právní ochrany, podle čl. 46 odst. 1 a čl. 46 odst. 2 písm. c) nařízení (EU) 2016/679 a s ohledem na předávání údajů od správců zpracovatelům a/nebo od zpracovatelů zpracovatelům, standardní smluvní doložky podle čl. 28 odst. 7 nařízení (EU) 2016/679, pokud nebudou změněny, s výjimkou výběru vhodného modulu (vhodných modulů) nebo za účelem přidání nebo aktualizace informací v dodatku. To smluvním stranám nebrání v tom, aby zahrnuly standardní smluvní doložky stanovené v těchto doložkách do širší smlouvy a/nebo přidaly další doložky nebo dodatečné záruky, pokud nebudou přímo nebo nepřímo v rozporu s těmito doložkami nebo nebudou dotčena základní práva nebo svobody subjektů údajů.

(b) Těmito doložkami nejsou dotčeny povinnosti, které se vztahují na vývozce údajů na základě nařízení (EU)

2016/679.

Doložka 3 Oprávněné třetí strany

(a) Subjekty údajů se mohou jako oprávněné třetí strany ve vztahu k vývozci a/nebo dovozci údajů dovolávat těchto doložek a vymáhat je, a to s následujícími výjimkami:

i) Doložka 1, Doložka 2, Doložka 3, Doložka 6, Doložka 7;

ii) Doložka 8 – Modul 1: Doložka 8.5. písm. e) a Doložka 8.9. písm. b); Modul 2: Doložka 8.1. písm. b), Doložka 8.9. písm. a), c), d) a e); Modul 3: Doložka 8.1. písm. a), c) a d) a Doložka 8.9. písm. a), c), d), e), f) a g); Modul 4: Doložka 8.1. písm. b) a Doložka 8.3 písm. b);

(iii) Doložka 9 – Modul dva: Doložka 9 písm. a), c), d) a e); Modul 3: Doložka 9 písm. a), c), d) a e);

(iv) Doložka 12 – Modul 1: Doložka 12 písm. a) a d); Moduly 2 a 3: Doložka 12 písm. a), d) a f);

(v) Doložka 13;

(vi) Doložka 15.1 písm. c), d) a e);

(vii) Doložka 16 písm. e);

(viii) Doložka 18 – Moduly 1, 2 a 3: Doložka 18 písm. a) a b); Modul 4: Doložka 18.

(b) Písmenem a) nejsou dotčena práva subjektů údajů podle nařízení (EU) 2016/679.

Doložka 4 Výklad

(a) Pokud tyto doložky používají pojmy, které jsou vymezeny v nařízení (EU) 2016/679, mají tyto pojmy stejný význam jako v uvedeném nařízení.

(b) Tyto doložky je třeba číst a vykládat s ohledem na ustanovení nařízení (EU) 2016/679.

(c) Tyto doložky nebudou vykládány žádným způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679.

Doložka 5 Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod mezi stranami, které existovaly v době sjednání těchto doložek, nebo které byly uzavřeny až po jejich sjednání, mají tyto doložky přednost.

Doložka 6 Popis předávání

Podrobnosti týkající se předávání, zejména kategorie osobních údajů, které jsou předávány, a účel nebo účely, pro které jsou předávány, jsou uvedeny v příloze I části B.

Doložka 7 – volitelná Doložka o přistoupení

(a) Subjekt, který není stranou těchto doložek, může se souhlasem stran k těmto doložkám kdykoli přistoupit, buď jako vývozce údajů, nebo jako dovozce údajů, a to vyplněním dodatku a podepsáním přílohy I části A.

(b) Poté, co přistupující subjekt vyplní dodatek a podepíše přílohu I část A, stane se stranou těchto doložek a má práva a povinnosti vývozce údajů nebo dovozce údajů v souladu se svým určením v příloze I části A.

(c) Přistupující subjekt nemá žádná práva ani povinnosti na základě těchto doložek plynoucí z období před tím, než se stal stranou.

ODDÍL II – POVINNOSTI STRAN

Doložka 8 Záruky ochrany údajů

Vývozce údajů zaručuje, že vynaložil přiměřené úsilí, aby mohl stanovit, zda je dovozce údajů schopen – zavedením vhodných technických a organizačních opatření – plnit své povinnosti podle těchto doložek.

MODUL 1: Předání od správce správci

8.1. Omezení účelu

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání v souladu s přílohou I částí B. Osobní údaje může zpracovávat pro jiný účel pouze tehdy, pokud:

i) získal předchozí souhlas subjektu údajů;

(ii) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

(iii) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

8.2. Transparentnost

(a) Aby subjekty údajů mohly účinně vykonávat svá práva podle doložky 10, dovozce údajů je informuje přímo nebo prostřednictvím vývozce údajů:

i) o své totožnosti a kontaktních údajích;

(ii) o kategoriích zpracovávaných osobních údajů;

(iii) o právu získat kopii těchto doložek;

(iv) pokud má v úmyslu osobní údaje dále předat jakékoli třetí straně nebo stranám, o příjemci nebo kategoriích příjemců (podle potřeby za účelem poskytnutí smysluplných informací), o účelu takového dalšího předávání a o důvodu pro další předávání podle doložky 8.7.

(b) Písmeno a) se nepoužije, pokud subjekt údajů již tyto informace má, a to i v případě, že tyto informace již poskytl vývozce údajů, nebo pokud je poskytnutí těchto informací nemožné nebo by to pro dovozce údajů znamenalo nepřiměřené úsilí. V druhém případě dovozce údajů informace v maximální možné míře zveřejní.

(c) Strany poskytnou subjektu údajů na požádání a bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, mohou strany před sdílením kopie upravit část znění dodatku, ale poskytnou smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny.

(d) Písmeny a) až c) nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.3. Přesnost a minimalizace údajů

(a) Každá strana zajistí, aby osobní údaje byly přesné a v případě potřeby aktualizovány. Dovozce údajů přijme veškerá smysluplná opatření, aby zajistil, že osobní údaje, které jsou nepřesné, budou s ohledem na účel nebo účely zpracování bezodkladně vymazány nebo opraveny.

(b) Pokud se jedna ze stran dozví, že osobní údaje, které předala nebo přijala, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje druhou stranu.

(c) Dovozce údajů zajistí, aby osobní údaje byly přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelu nebo účelů, pro které jsou zpracovávány.

8.4. Minimalizace uchovávání

Dovozce údajů uchová osobní údaje pouze po dobu nezbytnou pro účel nebo účely, pro který (které) jsou zpracovávány. Přijme vhodná technická nebo organizační opatření k zajištění dodržování této povinnosti, včetně vymazání nebo anonymizace údajů (2) a všech záloh na konci doby uchovávání.

8.5. Bezpečnost zpracování

a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení osobních údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení oni řádně zohlední aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování.

(b) Strany se dohodly na technických a organizačních opatřeních stanovených v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

(c) Dovozce údajů zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

(d) V případě porušení zabezpečení osobních údajů týkajících se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení osobních údajů, včetně opatření ke zmírnění jeho možných nepříznivých účinků.

(e) V případě porušení zabezpečení osobních údajů, které by mohlo vést k ohrožení práv a svobod fyzických osob, dovozce údajů bez zbytečného odkladu informuje vývozce údajů i příslušný dozorový úřad v souladu s doložkou 13. Toto ohlášení obsahuje i) popis povahy daného případu porušení zabezpečení osobních údajů (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů), ii) jeho pravděpodobných důsledků, iii) popis opatření, která byla přijata nebo byla navržena s cílem vyřešit dané porušení zabezpečení, a iv) údaje kontaktního místa, kde lze získat více informací. Není-li možné, aby dovozce údajů veškeré informace poskytl současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

(f) V případě porušení zabezpečení osobních údajů, které pravděpodobně bude představovat vysoké riziko pro práva a svobody fyzických osob, dovozce údajů rovněž bez zbytečného odkladu podá hlášení dotčeným subjektům údajů o porušení zabezpečení osobních údajů a jeho povaze – v případě potřeby ve spolupráci s vývozcem údajů – a sdělí jim také informace uvedené v písm. e) bodu ii) až iv), pokud dovozce údajů nezavedl opatření za účelem

značného snížení rizika pro práva a svobody fyzických osob nebo pokud dané hlášení nevyžaduje nepřiměřené úsilí. V posledně uvedeném případě dovozce údajů místo toho vydá veřejné oznámení nebo zajistí obdobné opatření, kterým veřejnost o porušení zabezpečení osobních údajů informuje.

(g) Dovozce údajů dokumentuje veškeré relevantní skutečnosti týkající se porušení zabezpečení osobních údajů, včetně jeho účinků a přijatých nápravných opatření, a vede si o tom záznamy.

8.6. Citlivé údaje

Jestliže předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech nebo trestných činů (dále jen "citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky přizpůsobené zvláštní povaze údajů a souvisejícím rizikům. To může zahrnovat omezení personálu, který má povolen přístup k osobním údajům, dodatečná bezpečnostní opatření (jako je pseudonymizace) a/nebo dodatečná omezení s ohledem na další zpřístupnění.

8.7. Další předávání

Dovozce údajů nezpřístupní osobní údaje třetí straně se sídlem mimo Evropskou unii (3) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen "další předávání"), ledaže by tato třetí strana byla podle příslušného modulu těmito doložkami vázána nebo by souhlasila s tím, že jimi bude vázána. K dalšímu předání dovozcem údajů jinak může dojít pouze tehdy, pokud:

(i) se provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679, jenž upravuje další předávání;

(ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dotčené zpracování;

(iii) třetí strana uzavře s dovozcem údajů závazný instrument zajišťující stejnou úroveň ochrany údajů jako podle těchto doložek a dovozce údajů poskytne kopii těchto záruk vývozci údajů;

(iv) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení;

(v) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, nebo

(vi) pokud neplatí žádná z dalších podmínek, dovozce údajů získal výslovný souhlas subjektu údajů s dalším předáváním v konkrétní situaci poté, co jej informoval o jeho účelu nebo účelech, totožnosti příjemce a možných rizicích, která pro něj vyplývají z takového předávání vzhledem k nedostatku vhodných záruk ochrany údajů. V takovém případě dovozce údajů informuje vývozce údajů a na žádost vývozce údajů mu předá kopii informací poskytnutých subjektu údajů.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.8. Zpracování z pověření dovozce údajů

Dovozce údajů zajistí, aby jakákoli osoba, která jedná z jeho pověření, včetně zpracovatele, zpracovávala údaje pouze na základě jeho pokynů.

8.9. Dokumentace a plnění povinností

(a) Každá strana musí být schopna prokázat plnění svých povinností podle těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování, za jejichž provádění odpovídá.

(b) Dovozce údajů tuto dokumentaci na požádání zpřístupní příslušnému dozorovému úřadu.

MODUL 2: Předání od správce zpracovateli

8.1. Pokyny

(a) Dovozce údajů zpracovává osobní údaje pouze na základě doložených pokynů od vývozce údajů. Vývozce údajů může takové pokyny vydávat po celou dobu trvání smlouvy.

(b) Dovozce údajů okamžitě informuje vývozce údajů, pokud není schopen tyto pokyny dodržet.

8.2. Omezení účelu

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání uvedené v příloze I části B, ledaže vývozce údajů vydá další pokyny.

8.3. Transparentnost

Na požádání poskytne vývozce údajů subjektu údajů bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně opatření popsaných v příloze II a osobních údajů, může vývozce údajů před sdílením kopie upravit část znění dodatku k těmto doložkám, ale poskytne smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny. Touto doložkou nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.4. Přesnost

Pokud se dovozce údajů dozví, že osobní údaje, které přijal, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje vývozce údajů. V takovém případě dovozce údajů spolupracuje s vývozcem údajů na jejich vymazání nebo opravě.

8.5. Doba zpracování a vymazání nebo vrácení údajů

Dovozce údajů zpracovává údaje pouze po dobu uvedenou v příloze I části B. Po skončení poskytování zpracovatelských služeb dovozce údajů v souladu s volbou vývozce údajů vymaže všechny osobní údaje zpracovávané jménem vývozce údajů a potvrdí vývozci údajů, že tak učinil, nebo vývozci údajů vrátí všechny osobní údaje zpracovávané jeho jménem a vymaže existující kopie. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a že bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to místní právo vyžaduje. Tím není dotčena doložka 14, zejména požadavek, aby dovozce údajů podle doložky 14 písm. e) informoval vývozce údajů po celou dobu trvání smlouvy, pokud má důvod se domnívat, že se na něj vztahují nebo se na něj začaly vztahovat právní předpisy nebo postupy, jež nejsou v souladu s požadavky podle doložky 14 písm. a).

8.6. Bezpečnost zpracování

(a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění uvedených údajů (dále

jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení strany řádně zohlední aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování. V případě pseudonymizace zůstanou dodatečné informace pro přiřazení osobních údajů konkrétnímu subjektu údajů, pokud je to možné, pod výlučnou kontrolou vývozce údajů. Za účelem dodržení svých povinností podle tohoto odstavce musí dovozce údajů přinejmenším zavést technická a organizační opatření uvedená v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

(b) Dovozce údajů poskytne přístup k osobním údajům svým zaměstnancům pouze v rozsahu nezbytně nutném pro provádění, správu a monitorování smlouvy. Zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

(c) V případě porušení zabezpečení osobních údajů týkajících se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení, včetně opatření ke zmírnění jeho nepříznivých dopadů. Dovozce údajů rovněž bez zbytečného odkladu poté, co se o porušení dozvěděl, podá hlášení vývozci údajů. Takové hlášení obsahuje podrobnosti o kontaktním místě, které může poskytnout bližší informace, popis povahy daného případu porušení zabezpečení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a přibližného množství záznamů osobních údajů), jeho pravděpodobných důsledků a opatření přijatých nebo navržených s cílem vyřešit dané porušení zabezpečení, včetně případných opatření ke zmírnění jeho možných nepříznivých dopadů. Není-li možné poskytnout všechny informace současně, původní hlášení obsahuje informace, které byly v danou dobu k dispozici, a další informace, jakmile budou k dispozici, budou následně poskytovány bez zbytečného odkladu.

(d) Dovozce údajů spolupracuje s vývozcem údajů a pomáhá mu tak, aby mu umožnil plnit jeho povinnosti podle nařízení (EU) 2016/679, zejména povinnost podávat hlášení příslušnému dozorovému úřadu a dotčeným subjektům údajů, s přihlédnutím k povaze zpracování a informacím, které jsou dovozci údajů dostupné.

8.7. Citlivé údaje

Pokud předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech a trestných činů (dále jen "citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky popsané v příloze I části B.

8.8. Další předávání

Dovozce údajů zpřístupní osobní údaje třetí straně pouze na základě doložených pokynů od vývozce údajů. Údaje mohou být navíc zpřístupněny třetí straně se sídlem mimo Evropskou unii (4) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen "další předávání"), pokud je tato třetí strana podle příslušného modulu vázána těmito doložkami nebo souhlasí s tím, že jimi bude vázána, nebo pokud:

(i) se další předávání provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679, jenž upravuje další předávání;

(ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dotčené zpracování;

(iii) je další předávání nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

(iv) je další předávání nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.9. Dokumentace a plnění povinností

(a) Dovozce údajů neprodleně a odpovídajícím způsobem vyřídí dotazy vývozce údajů, které se týkají zpracování podle těchto doložek.

b) Strany musí být schopny prokázat dodržování těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování prováděných za vývozce údajů.

(c) Dovozce údajů poskytne vývozci údajů veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v těchto doložkách, a na žádost vývozce údajů umožní audity činností zpracování, na které se tyto doložky vztahují, a bude k nim přispívat, a to v přiměřených intervalech, nebo pokud existují okolnosti nasvědčující tomu, že doložky nejsou dodržovány. Při rozhodování o přezkumu nebo auditu může vývozce údajů vzít v úvahu příslušná osvědčení, kterými disponuje dovozce údajů.

(d) Vývozce údajů se může rozhodnout provést audit sám nebo pověřit nezávislého auditora. Audity mohou zahrnovat inspekce v prostorách nebo ve fyzických zařízeních dovozce údajů a v příslušných případech se provádějí na základě přiměřeně včasného oznámení.

(e) Strany na požádání příslušnému dozorovému úřadu poskytnou informace uvedené v písmenech b) a c), včetně výsledků jakýchkoli auditů.

MODUL 3: Předání od zpracovatele zpracovateli

8.1. Pokyny

(a) Vývozce údajů informoval dovozce údajů, že jedná jako zpracovatel na základě pokynů svého správce nebo správců, a tyto pokyny vývozce údajů před zpracováním zpřístupní dovozci údajů.

(b) Dovozce údajů zpracovává osobní údaje pouze na základě dokumentovaných pokynů správce, které byly vývozcem údajů sděleny dovozci údajů, a na základě jakýchkoli dodatečných dokumentovaných pokynů od vývozce údajů. Tyto dodatečné pokyny nesmí být v rozporu s pokyny správce. Správce nebo vývozce údajů může po dobu trvání smlouvy vydat další dokumentované pokyny týkající se zpracování údajů.

(c) Dovozce údajů okamžitě informuje vývozce údajů, pokud není schopen tyto pokyny dodržet. Jestliže dovozce údajů není schopen postupovat podle pokynů správce, vývozce údajů o tom správce neprodleně uvědomí.

(d) Vývozce údajů zaručuje, že uložil dovozci údajů stejné povinnosti v oblasti ochrany údajů, jaké stanoví smlouva nebo jiný právní akt podle práva Unie nebo členského státu mezi správcem a vývozcem údajů (5).

8.2. Omezení účelu

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání v souladu s přílohou I částí B, pokud neexistují další pokyny ze strany správce, které dovozci údajů sdělil vývozce údajů, ani další pokyny ze strany vývozce údajů.

8.3. Transparentnost

Na požádání poskytne vývozce údajů subjektu údajů bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, může vývozce údajů před sdílením kopie upravit část znění dodatku, ale poskytne smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany

poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny.

8.4. Přesnost

Pokud se dovozce údajů dozví, že osobní údaje, které přijal, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje vývozce údajů. V takovém případě dovozce údajů spolupracuje s vývozcem údajů na jejich opravě nebo vymazání.

8.5. Doba zpracování a vymazání nebo vrácení údajů

Dovozce údajů zpracovává údaje pouze po dobu uvedenou v příloze I části B. Po skončení poskytování zpracovatelských služeb dovozce údajů v souladu s volbou vývozce údajů vymaže všechny osobní údaje zpracovávané jménem správce a potvrdí vývozci údajů, že tak učinil, nebo vývozci údajů vrátí všechny osobní údaje zpracovávané jeho jménem a vymaže všechny existující kopie. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a že bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to místní právo vyžaduje. Tím není dotčena doložka 14, zejména požadavek, aby dovozce údajů podle doložky 14 písm. e) informoval vývozce údajů po celou dobu trvání smlouvy, pokud má důvod se domnívat, že se na něj vztahují nebo se na něj začaly vztahovat právní předpisy nebo postupy, jež nejsou v souladu s požadavky podle doložky 14 písm. a).

8.6. Bezpečnost zpracování

(a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění uvedených údajů (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení oni řádně zohlední aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování. V případě pseudonymizace zůstanou dodatečné informace pro přiřazení osobních údajů konkrétnímu subjektu údajů, pokud je to možné, pod výlučnou kontrolou vývozce údajů nebo správce. Za účelem dodržení svých povinností podle tohoto odstavce musí dovozce údajů přinejmenším zavést technická a organizační opatření uvedená v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

(b) Dovozce údajů poskytne přístup k údajům svým zaměstnancům pouze v rozsahu nezbytně nutném pro provádění, správu a monitorování smlouvy. Zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

(c) V případě porušení zabezpečení osobních údajů týkajících se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení, včetně opatření ke zmírnění jeho nepříznivých dopadů. Dovozce údajů rovněž bez zbytečného odkladu poté, co se o porušení zabezpečení dozvěděl, podá hlášení vývozci údajů, a je-li to vhodné a proveditelné, také správci. Takové hlášení obsahuje podrobnosti o kontaktním místě, které může poskytnout bližší informace, popis povahy daného případu porušení zabezpečení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a přibližného množství záznamů osobních údajů), jeho pravděpodobných důsledků a opatření přijatých nebo navržených s cílem vyřešit dané porušení zabezpečení údajů, včetně opatření ke zmírnění jeho možných nepříznivých dopadů. Není-li možné poskytnout všechny informace současně, původní hlášení obsahuje informace, které byly v danou dobu k dispozici, a další informace, jakmile budou k dispozici, budou následně poskytovány bez zbytečného odkladu.

(d) Dovozce údajů spolupracuje s vývozcem údajů a pomáhá mu tak, aby mu umožnil plnit jeho povinnosti podle nařízení (EU) 2016/679, zejména povinnost podávat hlášení svému správci, aby tento správce mohl informovat příslušný dozorový úřad a dotčené subjekty údajů, s přihlédnutím k povaze zpracování a informacím, které jsou dovozci údajů dostupné.

8.7. Citlivé údaje

Pokud předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech a trestných činů (dále jen "citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky stanovené v příloze I části B.

8.8. Další předávání

Dovozce údajů zpřístupní osobní údaje třetí straně pouze na základě doložených pokynů od správce, které dovozci údajů sdělil vývozce údajů. Údaje mohou být navíc zpřístupněny třetí straně se sídlem mimo Evropskou unii (6) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen "další předávání"), pokud je tato třetí strana podle příslušného modulu vázána těmito doložkami nebo souhlasí s tím, že jimi bude vázána, nebo pokud:

(i) se další předávání provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679, jenž upravuje další předávání;

(ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679;

(iii) je další předávání nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

(iv) je další předávání nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.9. Dokumentace a plnění povinností

(a) Dovozce údajů neprodleně a odpovídajícím způsobem vyřídí dotazy vývozce údajů nebo správce, které se týkají zpracování podle těchto doložek.

b) Strany musí být schopny prokázat dodržování těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování prováděných za správce.

(c) Dovozce údajů poskytne vývozci údajů veškeré informace nezbytné k prokázání dodržování povinností stanovených v těchto doložkách, přičemž vývozce údajů je pak poskytne správci.

(d) Dovozce údajů umožní audity ze strany vývozce údajů, které se týkají činností zpracování, na něž se tyto doložky vztahují, a k těmto auditům přispívá, a to v přiměřených intervalech, nebo pokud existují okolnosti nasvědčující tomu, že doložky nejsou dodržovány. Totéž platí, pokud vývozce údajů požaduje audit na základě pokynů správce. Při rozhodování o auditu může vývozce údajů zohlednit příslušná osvědčení, kterými disponuje dovozce údajů.

(e) Pokud je audit prováděn na základě pokynů od správce, bude správce o jeho výsledcích informován vývozcem údajů.

(f) Vývozce údajů se může rozhodnout provést audit sám nebo pověřit nezávislého auditora. Audity mohou

zahrnovat inspekce v prostorách nebo ve fyzických zařízeních dovozce údajů a v příslušných případech se provádějí na základě přiměřeně včasného oznámení.

(g) Strany na požádání příslušnému dozorovému úřadu poskytnou informace uvedené v písmenech b) a c), včetně výsledků jakýchkoli auditů.

MODUL 4: Předání od zpracovatele správci

8.1. Pokyny

(a) Vývozce údajů zpracovává osobní údaje pouze na základě doložených pokynů od dovozce údajů, který jedná jako jeho správce.

(b) Vývozce údajů neprodleně informuje dovozce údajů, pokud není schopen tyto pokyny dodržovat, včetně případů, kdy tyto pokyny porušují nařízení (EU) 2016/679 nebo jiné právní předpisy Unie nebo členského státu v oblasti ochrany údajů.

(c) Dovozce údajů se zdrží přijímání jakýchkoli opatření, která by vývozci údajů bránila v plnění jeho povinností podle nařízení (EU) 2016/679, mimo jiné v kontextu dílčího zpracování, nebo pokud se jedná o spolupráci s příslušnými dozorovými úřady.

(d) Po skončení poskytování zpracovatelských služeb vývozce údajů v souladu s volbou dovozce údajů vymaže všechny osobní údaje zpracovávané jménem dovozce údajů a potvrdí dovozci údajů, že tak učinil, nebo dovozci údajů vrátí všechny osobní údaje zpracovávané jeho jménem a vymaže všechny existující kopie.

8.2. Bezpečnost zpracování

a) Strany zavedou vhodná technická a organizační opatření k zajištění zabezpečení údajů, a to i během předávání, a zajistí ochranu před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému poskytnutí nebo zpřístupnění (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení strany náležitě zohlední aktuální stav techniky, náklady na provedení, povahu osobních údajů (7), povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním, a zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování.

(b) Vývozce údajů pomáhá dovozci údajů při zajišťování odpovídajícího zabezpečení údajů v souladu s písmenem a). V případě porušení zabezpečení osobních údajů týkajícího se osobních údajů zpracovávaných vývozcem údajů podle těchto doložek vývozce údajů podá hlášení dovozci údajů bez zbytečného odkladu poté, co se o něm dozvěděl, a dovozci údajů bude při řešení uvedeného porušení nápomocen.

(c) Vývozce údajů zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

8.3. Dokumentace a plnění povinností

(a) Strany musí být schopny prokázat dodržování těchto doložek.

(b) Vývozce údajů poskytne dovozci údajů veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v těchto doložkách, umožní provedení auditů a bude k nim přispívat.

Doložka 9 Využití dílčích zpracovatelů

MODUL 2: Předání od správce zpracovateli

(a) Dovozce údajů má obecné povolení vývozce údajů pro zapojení dílčího zpracovatele nebo dílčích zpracovatelů ze schváleného seznamu. Dovozce údajů výslovně písemně informuje vývozce údajů o veškerých zamýšlených změnách uvedeného seznamu, které spočívají v přidání nebo nahrazení dílčích zpracovatelů nejméně [uveďte časové období] předem, čímž poskytne vývozci údajů dostatek času, aby mohl proti takovým změnám vznést námitky před zapojením dílčího zpracovatele nebo zpracovatelů. Dovozce údajů poskytne vývozci údajů informace nezbytné k tomu, aby vývozce údajů mohl uplatnit své právo vznést námitku.

Pokud dovozce údajů pro výkon konkrétních činností zpracování zapojí dílčího zpracovatele (jménem vývozce údajů), učiní tak prostřednictvím písemné smlouvy, která v zásadě stanoví stejné povinnosti v oblasti ochrany údajů jako ty, které jsou závazné pro dovozce údajů na základě těchto doložek, a to i pokud jde o práva náležející oprávněné třetí straně v případě subjektů údajů. (8) Strany se dohodly, že dodržováním této doložky dovozce údajů plní své povinnosti podle doložky 8.8. Dovozce údajů zajistí, aby dílčí zpracovatel dodržoval povinnosti, které se v souladu s těmito doložkami vztahují na dovozce údajů.

(c) Dovozce údajů poskytne vývozci údajů na jeho žádost kopii takové dohody s dílčím zpracovatelem a veškeré její následné změny. V rozsahu nezbytném k ochraně obchodních tajemství nebo jiných důvěrných informací, včetně osobních údajů, může dovozce údajů před sdílením kopie znění této dohody upravit.

(d) Dovozce údajů je i nadále vývozci údajů plně odpovědný za plnění povinností dílčího zpracovatele na základě smlouvy, kterou s dovozcem údajů uzavřel. Dovozce údajů informuje vývozce údajů o každém případu, kdy dílčí zpracovatel nesplnil svou povinnost, jež z uvedené smlouvy vyplývá.

(e) Dovozce údajů sjedná s dílčím zpracovatelem doložku ve prospěch oprávněné třetí strany, přičemž – v případě, že dovozce údajů fakticky zmizel, z právního hlediska zanikl nebo se dostal do platební neschopnosti – má vývozce údajů právo smlouvu s dílčím zpracovatelem vypovědět a dát dílčímu zpracovateli pokyn, aby osobní údaje vymazal nebo vrátil.

MODUL 3: Předání od zpracovatele zpracovateli

(a) Dovozce údajů má obecné povolení správce pro zapojení dílčího zpracovatele nebo dílčích zpracovatelů ze schváleného seznamu. Dovozce údajů výslovně písemně informuje správce o veškerých zamýšlených změnách uvedeného seznamu, které spočívají v přidání nebo nahrazení dílčích zpracovatelů nejméně [uveďte časové období] předem, čímž poskytne správci dostatek času, aby mohl proti takovým změnám vznést námitky před zapojením dílčího zpracovatele nebo zpracovatelů. Dovozce údajů poskytne správci informace nezbytné k tomu, aby správce mohl uplatnit své právo vznést námitku. Dovozce údajů o zapojení dílčího zpracovatele nebo dílčích zpracovatelů informuje vývozce údajů.

(b) Pokud dovozce údajů pro výkon konkrétních činností zpracování zapojí dílčího zpracovatele (jménem správce), učiní tak prostřednictvím písemné smlouvy, která v zásadě stanoví stejné povinnosti v oblasti ochrany údajů jako ty, které jsou závazné pro dovozce údajů na základě těchto doložek, a to i pokud jde o práva náležející oprávněné třetí straně v případě subjektů údajů. (9) Strany se dohodly, že dodržováním této doložky dovozce údajů plní své povinnosti podle doložky 8.8. Dovozce údajů zajistí, aby dílčí zpracovatel dodržoval povinnosti, které se v souladu s těmito doložkami vztahují na dovozce údajů.

(c) Dovozce údajů poskytne na žádost vývozce údajů nebo správce kopii takové dohody s dílčím zpracovatelem a veškeré její následné změny. V rozsahu nezbytném k ochraně obchodních tajemství nebo jiných důvěrných informací, včetně osobních údajů, může dovozce údajů před sdílením kopie znění této dohody upravit.

(d) Dovozce údajů je i nadále vývozci údajů plně odpovědný za plnění povinností dílčího zpracovatele na základě smlouvy, kterou s dovozcem údajů uzavřel. Dovozce údajů informuje vývozce údajů o každém případu, kdy dílčí zpracovatel nesplnil svou povinnost, jež z uvedené smlouvy vyplývá.

(e) Dovozce údajů sjedná s dílčím zpracovatelem doložku ve prospěch oprávněné třetí strany, přičemž – v případě,

že dovozce údajů fakticky zmizel, z právního hlediska zanikl nebo se dostal do platební neschopnosti – má vývozce údajů právo smlouvu s dílčím zpracovatelem vypovědět a dát dílčímu zpracovateli pokyn, aby osobní údaje vymazal nebo vrátil.

Doložka 10 Práva subjektu údajů

MODUL 1: Předání od správce správci

(a) Dovozce údajů, případně za pomoci vývozce údajů, vyřizuje veškeré dotazy a žádosti, které obdrží od subjektu údajů, týkající se zpracování jeho osobních údajů a výkonu jeho práv podle těchto doložek, a to bez zbytečného odkladu a nejpozději do jednoho měsíce od obdržení dotazu nebo žádosti. (10) Dovozce údajů přijme vhodná opatření k usnadnění vyřizování těchto dotazů, žádostí a výkonu práv subjektu údajů. Veškeré informace poskytované subjektu údajů musí být ve srozumitelném a snadno přístupném znění za použití jasných a jednoduchých jazykových prostředků.

(b) Na žádost subjektu údajů dovozce údajů zejména bezplatně:

(i) poskytne subjektu údajů potvrzení o tom, zda se zpracovávají osobní údaje, které se ho týkají, a v takovém případě mu poskytne kopii údajů, které se ho týkají, a informace uvedené v příloze I; pokud osobní údaje byly nebo budou dále předávány, poskytne informace o příjemcích nebo kategoriích příjemců (podle potřeby za účelem poskytnutí smysluplných informací), kterým osobní údaje byly nebo budou dále předávány, účel těchto dalších předání a jejich důvod v souladu s doložkou 8.7.; a poskytne informace o právu podat stížnost u dozorového úřadu v souladu s doložkou 12 písm. c) bodem i);

ii) opraví nepřesné nebo neúplné údaje týkající se subjektu údajů;

(ii) vymaže osobní údaje týkající se subjektu údajů, pokud tyto údaje jsou nebo byly zpracovávány v rozporu s kteroukoli z těchto doložek, která zajišťuje práva náležející oprávněné třetí straně, nebo pokud subjekt údajů odvolá souhlas, na kterém je zpracování založeno.

(c) Pokud dovozce údajů zpracovává osobní údaje pro účely přímého marketingu, přestane je pro tyto účely zpracovávat, vznese-li proti tomu subjekt údajů námitky.

(d) Dovozce údajů nepřijme rozhodnutí založené výhradně na automatizovaném zpracování předávaných osobních údajů (dále jen "automatizované rozhodnutí"), které by mělo právní účinky týkající se subjektu údajů nebo by ho obdobně významně ovlivnilo, ledaže by k tomu subjekt údajů dal výslovný souhlas, nebo pokud by mu to bylo na základě právních předpisů země určení povoleno, za předpokladu, že takové právní předpisy stanoví vhodná opatření na ochranu práv a oprávněných zájmů subjektu údajů. V tomto případě dovozce údajů, v případě potřeby ve spolupráci s vývozcem údajů:

(i) informuje subjekt údajů o předpokládaném automatizovaném rozhodnutí, předpokládaných důsledcích a použitém postupu a

(ii) zavede vhodná ochranná opatření, přinejmenším tím, že umožní subjektu údajů napadnout rozhodnutí, vyjádřit svůj názor a dosáhnout přezkumu prováděného člověkem.

(e) Jestliže jsou žádosti subjektu údajů nepřiměřené, zejména proto, že se opakují, může dovozce údajů buď uložit přiměřený poplatek, v němž budou zohledněny administrativní náklady související s vyhověním dané žádosti, nebo může odmítnout žádosti vyhovět.

(f) Dovozce údajů může žádost subjektu údajů odmítnout, pokud je takové odmítnutí umožněno podle práva země určení a je v demokratické společnosti nezbytné a přiměřené za účelem ochrany jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679.

(g) Pokud má dovozce údajů v úmyslu žádost subjektu údajů odmítnout, informuje subjekt údajů o důvodech odmítnutí a možnosti podat stížnost u příslušného dozorového úřadu a/nebo požádat o soudní ochranu.

MODUL 2: Předání od správce zpracovateli

(a) Dovozce údajů neprodleně informuje vývozce údajů o každé žádosti, kterou od subjektu údajů přijal. Na tuto žádost sám neodpoví, pokud k tomu nedostal povolení od vývozce údajů.

(b) Dovozce údajů vývozci údajů pomáhá při plnění jeho povinností reagovat na žádosti subjektů údajů týkající se výkonu jejich práv podle nařízení (EU) 2016/679. V tomto ohledu stanoví strany v příloze II příslušná technická a organizační opatření s přihlédnutím k povaze zpracování, prostřednictvím něhož bude pomoc poskytována, a stanoví i rozsah a dosah požadované pomoci.

(c) Při plnění svých povinností podle písmen a) a b) musí dovozce údajů dodržovat pokyny vývozce údajů.

MODUL 3: Předání od zpracovatele zpracovateli

(a) Dovozce údajů neprodleně informuje vývozce údajů a v příslušném případě i správce o každé žádosti, kterou od subjektu údajů přijal, aniž by na tuto žádost reagoval, ledaže by k tomu dostal od správce povolení.

(b) Dovozce údajů, případně ve spolupráci s vývozcem údajů, pomáhá správci při plnění jeho povinností reagovat na žádosti subjektů údajů týkající se výkonu jejich práv podle nařízení (EU) 2016/679 nebo v příslušném případě nařízení (EU) 2018/1725. V tomto ohledu stanoví strany v příloze II příslušná technická a organizační opatření s přihlédnutím k povaze zpracování, prostřednictvím něhož bude pomoc poskytována, a stanoví i rozsah a dosah požadované pomoci.

(c) Při plnění svých povinností podle písmen a) a b) musí dovozce údajů dodržovat pokyny správce, které mu jsou sděleny vývozcem údajů.

MODUL 4: Předání od zpracovatele správci

Strany si vzájemně pomáhají při odpovídání na dotazy a žádosti subjektů údajů podle místního práva použitelného na dovozce údajů nebo v případě zpracování údajů dovozcem údajů v EU podle nařízení (EU) 2016/679.

Doložka 11 Náprava

(a) Dovozce údajů transparentně a ve snadno přístupném formátu informuje subjekty údajů prostřednictvím individuálního oznámení nebo na svých internetových stránkách o kontaktním místě oprávněném vyřizovat stížnosti. Takové místo neprodleně vyřídí jakékoli stížnosti, které od subjektu údajů přijme.

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(b) V případě sporu mezi subjektem údajů a jednou ze smluvních stran týkajícího se dodržování těchto doložek vyvine tato strana veškeré úsilí k tomu, aby takovou záležitost vyřešila smírně a včas. Strany se o těchto sporech navzájem informují a v příslušných případech při jejich řešení spolupracují.

(c) Pokud se subjekt údajů dovolává práva ve prospěch oprávněné třetí strany podle doložky 3, dovozce údajů akceptuje rozhodnutí subjektu údajů:

(i) podat stížnost u dozorového úřadu v členském státě svého obvyklého bydliště nebo místa výkonu práce nebo u

příslušného dozorového úřadu podle doložky 13;

(ii) postoupit spor příslušným soudům ve smyslu doložky 18.

(d) Strany jsou srozuměny, že subjekt údajů může být zastoupen neziskovým subjektem, organizací nebo sdružením za podmínek stanovených v čl. 80 odst. 1 nařízení (EU) 2016/679.

(e) Dovozce údajů dodržuje rozhodnutí závazné podle platného práva EU nebo členského státu.

(f) Dovozce údajů souhlasí s tím, že výběr provedený subjektem údajů nebude mít vliv na jeho hmotná a procesní práva požadovat nápravu v souladu s platnými právními předpisy.

Doložka 12 Odpovědnost

MODUL 1: Předání od správce správci

MODUL 4: Předání od zpracovatele správci

(a) Každá strana je vůči druhé straně/ostatním stranám odpovědná za jakoukoli újmu, kterou druhé straně/ostatním stranám při porušení těchto doložek způsobí.

(b) Každá strana je odpovědná vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou strana způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek. Tím není dotčena odpovědnost vývozce údajů podle nařízení (EU) 2016/679.

(c) Pokud je za újmu způsobenou subjektu údajů v důsledku porušení těchto doložek odpovědná více než jedna strana, nesou společnou a nerozdílnou odpovědnost všechny odpovědné strany a subjekt údajů je oprávněn proti kterékoli z těchto stran podat žalobu u soudu.

(d) Smluvní strany se dohodly, že pokud je jedna ze smluvních stran odpovědná podle písmene c), je oprávněna požadovat od druhé smluvní strany/ostatních smluvních stran zpět část náhrady újmy odpovídající její odpovědnosti za újmu.

(e) Dovozce údajů se nemůže dovolávat jednání zpracovatele nebo dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(a) Každá strana je vůči druhé straně/ostatním stranám odpovědná za jakoukoli újmu, kterou druhé straně/ostatním stranám při porušení těchto doložek způsobí.

(b) Dovozce údajů je odpovědný vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou dovozce údajů nebo jeho dílčí zpracovatel způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek.

(c) Aniž by bylo dotčeno písmeno b), vývozce údajů je odpovědný vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou vývozce údajů nebo dovozce údajů (nebo jeho dílčí zpracovatel) způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek. Tím není dotčena odpovědnost vývozce údajů, a pokud je vývozcem údajů zpracovatel jednající jménem správce, odpovědnost správce podle nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.

(d) Strany se dohodly, že pokud je vývozce údajů odpovědný podle písmene c) za újmu způsobenou dovozcem

údajů (nebo jeho dílčím zpracovatelem), je oprávněn požadovat od dovozce údajů část náhrady újmy odpovídající odpovědnosti dovozce údajů za újmu.

(e) Pokud je za újmu způsobenou subjektu údajů v důsledku porušení těchto doložek odpovědná více než jedna strana, nesou společnou a nerozdílnou odpovědnost všechny odpovědné strany a subjekt údajů je oprávněn proti kterékoli z těchto stran podat žalobu u soudu.

(f) Smluvní strany se dohodly, že pokud je jedna ze smluvních stran odpovědná podle písmene e), je oprávněna požadovat od druhé smluvní strany/ostatních smluvních stran zpět část náhrady újmy odpovídající její odpovědnosti za újmu.

(g) Dovozce údajů se nemůže dovolávat jednání dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

Doložka 13 Dohled

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(a) [Pokud je vývozce údajů usazen v členském státě EU:] Dozorový úřad uvedený v příloze I části C, který je odpovědný za zajištění, že vývozce údajů dodržuje nařízení (EU) 2016/679, pokud jde o předávání údajů, jedná jako příslušný dozorový úřad.

[Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2 a jmenoval zástupce podle čl. 27 odst. 1 nařízení (EU) 2016/679:] Dozorový úřad členského státu – uvedený v příloze I části C–, v němž je usazen zástupce ve smyslu čl. 27 odst. 1 nařízení (EU) 2016/679, jedná jako příslušný dozorový úřad.

[Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2, aniž by však musel jmenovat zástupce podle čl. 27 odst. 2 nařízení (EU) 2016/679:] Dozorový úřad jednoho z členských států, v nichž se nacházejí subjekty údajů, jejichž osobní údaje jsou předávány podle těchto doložek v souvislosti se zbožím nebo službami jim nabízenými, nebo jejichž chování je monitorováno, uvedený v příloze I části C, jedná jako příslušný dozorový úřad.

(b) Dovozce údajů souhlasí, že se podřídí pravomoci příslušného dozorového úřadu a bude s ním spolupracovat v rámci všech postupů zaměřených na zajištění dodržování těchto doložek. Dovozce údajů zejména souhlasí, že bude reagovat na dotazy, podrobovat se auditům a dodržovat opatření přijatá dozorovým úřadem, včetně nápravných a kompenzačních opatření. Dozorovému úřadu poskytne písemné potvrzení, že byla přijata nezbytná opatření.

ODDÍL III – MÍSTNÍ PRÁVNÍ PŘEDPISY A POVINNOSTI V PŘÍPADĚ PŘÍSTUPU ORGÁNŮ VEŘEJNÉ MOCI

Doložka 14 Místní právní předpisy a postupy mající dopad na dodržování doložek

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci (pokud zpracovatel z EU kombinuje osobní údaje přijaté od správce ve třetí zemi s osobními údaji shromážděnými zpracovatelem v EU)

(a) Strany zaručují, že nemají důvod se domnívat, že právní předpisy a postupy ve třetí zemi určení, které se vztahují na zpracování osobních údajů dovozcem údajů, včetně jakýchkoli požadavků na zpřístupnění osobních údajů nebo opatření, kterými se povoluje přístup orgánům veřejné moci, brání dovozci údajů při plnění svých povinností podle těchto doložek. To je založeno na předpokladu, že právní předpisy a postupy, které respektují podstatu základních práv a svobod a nepřekračují to, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679, nejsou v rozporu s těmito doložkami.

(b) Smluvní strany prohlašují, že při poskytování záruky uvedené v písmenu a) náležitě zohlednily zejména následující prvky:

(i) konkrétní okolnosti předání, včetně délky zpracovatelského řetězce, počtu zapojených subjektů a použitých kanálů pro přenos údajů, zamýšlené další předání, druh příjemce, účely zpracování, kategorie a formát předávaných osobních údajů, hospodářské odvětví, v němž se předávání uskutečňuje, místo, kde se předané údaje uchovávají;

(ii) právní předpisy a postupy třetí země určení – včetně těch, které vyžadují zpřístupnění údajů orgánům veřejné moci nebo povolují přístup těchto orgánů – relevantní s ohledem na konkrétní okolnosti předání, jakož i použitelná omezení a záruky (12);

(iii) veškeré příslušné smluvní, technické nebo organizační záruky zavedené za účelem doplnění záruk podle těchto doložek, včetně opatření uplatňovaných během předání a zpracování osobních údajů v zemi určení.

(c) Dovozce údajů zaručuje, že při provádění posouzení podle písmene b) vynaložil maximální úsilí, aby poskytl vývozci údajů relevantní informace, a souhlasí s tím, že bude při zajišťování dodržování těchto doložek s vývozcem údajů i nadále spolupracovat.

(d) Strany souhlasí, že posouzení podle písmene b) zdokumentují a na požádání zpřístupní příslušnému dozorovému úřadu.

(e) Dovozce údajů souhlasí s tím, že neprodleně uvědomí vývozce údajů, pokud má po vyjádření souhlasu s těmito ustanoveními a po dobu trvání smlouvy důvod se domnívat, že se na něj vztahují, nebo se začaly vztahovat právní předpisy nebo postupy, které nejsou v souladu s požadavky podle písmene a), a to i po změně v právních předpisech třetí země nebo opatření (jako je například žádost o poskytnutí údajů), jež svědčí o tom, že uplatňování těchto právních předpisů v praxi není v souladu s požadavky uvedenými v písmeni a). [Pokud jde o modul 3: Vývozce údajů předá oznámení správci.]

(f) Po oznámení podle písmene e), nebo pokud má vývozce údajů jinak důvod se domnívat, že dovozce údajů již nemůže plnit své povinnosti na základě těchto doložek, vývozce údajů neprodleně určí vhodná opatření (např. technická nebo organizační opatření k zajištění bezpečnosti a důvěrnosti), která má přijmout vývozce údajů a/nebo dovozce údajů k řešení situace [pokud jde o modul 3: případně po konzultaci se správcem]. Vývozce údajů pozastaví předávání údajů, pokud se domnívá, že pro toto předávání nemohou být zajištěny žádné vhodné záruky, nebo pokud mu dá pokyn [pokud jde o modul 3: správce nebo] příslušný dozorový úřad. V tomto případě je vývozce údajů oprávněn vypovědět smlouvu, pokud jde o zpracování osobních údajů podle těchto doložek. Pokud smlouva zahrnuje více než dvě smluvní strany, může vývozce údajů toto právo na vypovězení uplatnit pouze ve vztahu k příslušné straně, pokud se strany nedohodly jinak. Jestliže je smlouva vypovězena podle této doložky, použije se doložka 16 písm. d) a e).

Doložka 15 Povinnost dovozce údajů v případě přístupu orgánů veřejné moci

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci (pokud zpracovatel z EU kombinuje osobní údaje přijaté od správce ve třetí zemi s osobními údaji shromážděnými zpracovatelem v EU)

15.1. Oznámení

(a) Dovozce údajů souhlasí s tím, že neprodleně uvědomí vývozce údajů, a je-li to možné, subjekt údajů (v případě potřeby s pomocí vývozce údajů), pokud:

/i) na základě právních předpisů země určení obdrží právně závaznou žádost od orgánu veřejné moci, včetně soudních orgánů, o zpřístupnění osobních údajů předaných podle těchto doložek; takové oznámení obsahuje informace o požadovaných osobních údajích, dožadujícím orgánu, právním základu žádosti a poskytnuté odpovědi, nebo

(ii) se dozví o jakémkoli přímém přístupu orgánů veřejné moci k osobním údajům předávaným podle těchto doložek v souladu s právními předpisy země určení; takové oznámení obsahuje všechny informace dostupné dovozci.

[Pokud jde o modul 3: Vývozce údajů předá oznámení správci.]

(b) Pokud je podle právních předpisů země určení dovozci údajů zakázáno informovat vývozce údajů a/nebo subjekt údajů, souhlasí dovozce údajů s tím, že za účelem co nejrychlejšího sdělení co největšího množství informací vynaloží maximální úsilí, aby od tohoto zákazu bylo upuštěno. Dovozce údajů souhlasí, že zdokumentuje své maximální úsilí, aby je mohl na žádost vývozce údajů prokázat.

(c) Je-li to povoleno právními předpisy země určení, dovozce údajů souhlasí, že bude poskytovat vývozci údajů v pravidelných intervalech po dobu trvání smlouvy co nejrelevantnější informace o přijatých žádostech (zejména informace o počtu žádostí, druhu požadovaných údajů, dožadujícím orgánu nebo orgánech, zda byly tyto žádosti napadeny a výsledek takového napadení atd.). [Pokud jde o modul 3: Vývozce údajů předá informace správci.]

(d) Dovozce údajů souhlasí s tím, že po dobu trvání smlouvy bude informace podle písmene a) až c) uchovávat a na vyžádání je poskytne příslušnému dozorovému úřadu.

(e) Písmeny a) až c) není dotčena povinnost dovozce údajů podle doložky 14 písm. e) a doložky 16 neprodleně informovat vývozce údajů, pokud není schopen tyto doložky dodržovat.

15.2. Přezkum zákonnosti a minimalizace údajů

(a) Dovozce údajů souhlasí s tím, že přezkoumá zákonnost žádosti o poskytnutí údajů, zejména zda nepřekročila meze pravomocí udělených dožadujícímu orgánu veřejné moci, a že žádost napadne, pokud po pečlivém posouzení dojde k závěru, že existují opodstatněné důvody se domnívat, že žádost je podle právních předpisů země určení, platných závazků podle mezinárodního práva a zásad mezinárodní zdvořilosti protiprávní. Dovozce údajů za stejných podmínek využívá možností odvolání. Při napadení žádosti dovozce údajů přijme předběžná opatření s cílem pozastavit účinky žádosti, dokud příslušný soudní orgán nerozhodne o její opodstatněnosti. Nezpřístupní požadované osobní údaje, dokud mu taková povinnost nebude stanovena na základě platných

procesních pravidel. Těmito požadavky nejsou dotčeny povinnosti dovozce údajů podle doložky 14 písm. e).

(b) Dovozce údajů souhlasí, že zdokumentuje své právní posouzení i jakékoli napadení žádosti o poskytnutí údajů a v rozsahu povoleném právními předpisy země určení zpřístupní dokumentaci vývozci údajů. Na požádání ji rovněž zpřístupní příslušnému dozorovému úřadu. [Pokud jde o modul 3: Vývozce údajů posouzení zpřístupní správci.]

(c) Dovozce údajů souhlasí s poskytnutím minimálního přípustného množství informací při odpovědi na žádost o zpřístupnění, a to na základě přiměřeného výkladu žádosti.

ODDÍL IV – ZÁVĚREČNÁ USTANOVENÍ

Doložka 16 Nedodržení doložek a vypovězení

(a) Dovozce údajů neprodleně informuje vývozce údajů, pokud není z jakéhokoli důvodu schopen tyto doložky dodržet.

(b) Pokud dovozce údajů poruší tyto doložky nebo není schopen tyto doložky dodržet, vývozce údajů pozastaví předávání osobních údajů dovozci údajů, dokud není dodržování opět zajištěno nebo smlouva vypovězena. Tímto není dotčena doložka 14 písm. f).

(c) Vývozce údajů je oprávněn vypovědět smlouvu v rozsahu, v němž se jedná o zpracování osobních údajů podle těchto doložek, pokud:

(i) vývozce údajů pozastavil předávání osobních údajů dovozci údajů podle písm. b) a dodržování těchto doložek není v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení obnoveno;

(ii) dovozce údajů tyto doložky podstatně nebo trvale porušuje nebo

(iii) dovozce údajů nedodrží závazné rozhodnutí příslušného soudu nebo dozorového úřadu týkajícího se jeho povinností podle těchto doložek.

V takových případech o nedodržení informuje příslušný dozorový úřad [pokud jde o modul 3: a správce]. Jestliže smlouva zahrnuje více než dvě smluvní strany, může vývozce údajů toto právo na vypovězení uplatnit pouze ve vztahu k příslušné straně, pokud se strany nedohodly jinak.

d) [Pokud jde o modul 1, 2 a 3: Osobní údaje, které byly předány před vypovězením smlouvy podle písmene c), musí být podle volby vývozce údajů neprodleně vráceny vývozci údajů nebo vymazány v celém rozsahu. To samé se uplatní ve vztahu k veškerým kopiím údajů.] [Pokud jde o modul 4: Osobní údaje shromážděné vývozcem údajů v EU, které byly předány před vypovězením smlouvy podle písmene c), musí být neprodleně vymazány v celém rozsahu, včetně veškerých jejich kopií.] Dovozce údajů potvrdí vývozci údajů, že byly údaje vymazány. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují předané osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to uvedené místní právo vyžaduje.

(e) Kterákoli ze stran může odvolat svůj souhlas s tím, že bude vázána těmito doložkami, pokud i) Evropská komise přijme rozhodnutí podle čl. 45 odst. 3 nařízení (EU) 2016/679 týkající se předávání osobních údajů, na které se tyto doložky vztahují, nebo ii) se nařízení (EU) 2016/679 stane součástí právního rámce země, do které jsou osobní údaje předávány. Tím nejsou dotčeny další povinnosti vztahující se na dotčené zpracování podle nařízení (EU) 2016/679.

Doložka 17 Rozhodné právo

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

Tyto doložky se řídí právem jednoho z členských států EU, pokud takové právo umožňuje uplatňovat práva náležející oprávněné třetí straně. Strany se dohodly, že se budou řídit právem definovaným v Podmínkách.

MODUL 4: Předání od zpracovatele správci

Tyto doložky se řídí právem země, jež umožňuje uplatňovat práva náležející oprávněné třetí straně. Strany se dohodly, že se budou řídit právem definovaným v Podmínkách.

Doložka 18 Volba soudu a příslušnost

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(a) Veškeré spory vyplývající z těchto doložek budou řešeny soudy členského státu EU.

(b) Strany se dohodly, že se budou řídit soudy definovanými v Podmínkách.

(c) Subjekt údajů může rovněž zahájit soudní řízení proti vývozci údajů a/nebo dovozci údajů před soudy členského státu, v němž má subjekt údajů své obvyklé bydliště.

(d) Smluvní strany se dohodly, že se příslušnosti těchto soudů podřídí.

MODUL 4: Předání od zpracovatele správci

Veškeré spory vyplývající z těchto doložek budou řešeny soudy jak je definováno v Podmínkách.

DODATEK

VYSVĚTLIVKY: Musí být možné jasně rozlišit informace, které se vztahují na každé předání nebo každou kategorii předání, a v tomto ohledu určit příslušnou úlohu/příslušné úlohy stran v postavení vývozce/vývozců údajů a/nebo dovozce/dovozců údajů. To nemusí nutně vyžadovat vyplnění a podepsání samostatných dodatků pro každé předání/kategorii předání a/nebo smluvní vztah, pokud lze této transparentnosti dosáhnout prostřednictvím jednoho dodatku. Pokud je to však nutné k zajištění dostatečné srozumitelnosti, měly by se použít samostatné dodatky.

PŘÍLOHA I

A. SEZNAM SMLUVNÍCH STRAN

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci

Vývozce (vývozci) údajů: [Totožnost a kontaktní údaje vývozce/vývozců údajů a v příslušném případě jeho/jejich pověřence pro ochranu osobních údajů a/nebo zástupce v Evropské unii]

1. Správce, jak je definován ve Smlouvě o zpracování údajů

2. Zpracovatel, jak je definován ve Smlouvě o zpracování údajů

(na základě toku dat)

Dovozce nebo dovozci údajů: [Totožnost a kontaktní údaje dovozce/dovozců údajů, včetně jakékoli kontaktní osoby, která je odpovědná za ochranu údajů]

1. Správce, jak je definován ve Smlouvě o zpracování údajů

2. Zpracovatel, jak je definován ve Smlouvě o zpracování údajů

(na základě toku dat)

B. POPIS PŘEDÁNÍ

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci

Kategorie subjektů údajů, jejichž osobní údaje se předávají: Jak je definováno ve Smlouvě o zpracování údajů.

Kategorie předávaných osobních údajů: Jak je definováno ve Smlouvě o zpracování údajů a Zásadách ochrany osobních údajů.

Citlivé údaje, které se předávají (v příslušných případech), a uplatněná omezení nebo záruky, jež plně zohledňují povahu údajů a související rizika, například přísné účelové omezení, omezení přístupu (včetně přístupu pouze pro zaměstnance, kteří absolvovali specializované školení), vedení záznamu o přístupu k údajům, omezení pro další předávání nebo dodatečná bezpečnostní opatření: Jak je definováno ve Smlouvě o zpracování údajů a Zásadách ochrany osobních údajů.

Četnost předávání (např. zda jsou údaje předávány jednorázově nebo průběžně): Průběžně.

Povaha zpracování: Automatizovaně.

Účel nebo účely předání údajů a další zpracování: Poskytování služeb, jak je definováno v Podmínkách, jejich Přílohách, Zásadách ochrany osobních údajů a servisní dokumentaci.

Doba, po kterou budou osobní údaje uchovávány, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby: Jak je definováno ve Smlouvě o zpracování údajů.

Pokud jde o předávání (dílčím) zpracovatelům, rovněž uveďte předmět, povahu a trvání zpracování: Jak je definováno ve Smlouvě o zpracování údajů.

C. PŘÍSLUŠNÝ DOZOROVÝ ÚŘAD

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

V souladu s doložkou 13 určete příslušný dozorový úřad nebo příslušné dozorové úřady: Jak je definováno v Zásadách ochrany osobních údajů

PŘÍLOHA II TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K ZAJIŠTĚNÍ ZABEZPEČENÍ ÚDAJŮ

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

VYSVĚTLIVKY: Technická a organizační opatření musí být popsána konkrétně (nikoli obecně). Viz také obecnou poznámku na první stránce dodatku, týkající se zejména potřeby jasně uvést, která opatření se vztahují na každé jednorázové nebo souborné předání.

Popis technických a organizačních opatření zavedených dovozcem nebo dovozci údajů (včetně veškerých příslušných certifikací) za účelem zajištění vhodné úrovně zabezpečení s přihlédnutím k povaze, rozsahu, kontextu a účelu zpracování a rizikům pro práva a svobody fyzických osob: Jak je definováno v Bezpečnostní dokumentaci

Pokud jde o předávání údajů (dílčím) zpracovatelům, popište také konkrétní technická a organizační opatření, která má (dílčí) zpracovatel přijmout, aby mohl poskytnout pomoc správci; a – v případě předávání od zpracovatele dílčímu zpracovateli – vývozci údajů.

PŘÍLOHA III SEZNAM DÍLČÍCH ZPRACOVATELŮ

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

VYSVĚTLIVKY: Tuto přílohu je třeba vyplnit pro moduly 2 a 3 pro případ zvláštního povolení dílčích zpracovatelů (doložka 9 písm. a), varianta 1).

Správce udělil povolení pro zapojení následujících dílčích zpracovatelů: Jak je definováno ve Smlouvě o zpracování údajů

Odkazy:

(1) Pokud je vývozcem údajů zpracovatel, na nějž se vztahuje nařízení (EU) 2016/679 a který jedná jménem orgánu nebo subjektu Unie jako správce, spoléhání se na tyto doložky při zapojení jiného zpracovatele (dílčí zpracování), na kterého se nařízení (EU) 2016/679 nevztahuje, rovněž zajišťuje soulad s čl. 29 odst. 4 nařízení

Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie, a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí 1247/2002/ES (Úř. věst. L 295 ze dne 21.11.2018, s. 39), v rozsahu, v němž jsou tyto doložky a povinnosti týkající se ochrany údajů stanovené ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle čl. 29 odst. 3 nařízení (EU) 2018/1725 sladěny. To bude zejména případ, kdy se správce a zpracovatel spoléhají na standardní smluvní doložky obsažené v rozhodnutí 2021/915.

(2) To vyžaduje anonymizaci údajů takovým způsobem, aby již nikdo nemohl být nikým identifikovatelný, v souladu s 26. bodem odůvodnění nařízení (EU) 2016/679, a aby byl tento proces nevratný.

(3) Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, které jsou začleněny do přílohy XI uvedené dohody. Jakékoli zpřístupnění dovozcem údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další předávání.

(4) Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, které jsou začleněny do přílohy XI uvedené dohody. Jakékoli zpřístupnění dovozcem údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další předávání.

(5) 28 odst. 4 nařízení (EU) 2016/679, a pokud je správcem orgán nebo jiný subjekt EU, čl. 29 odst. 4 nařízení (EU) 2018/1725.

(6) Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, které jsou začleněny do přílohy XI uvedené dohody. Jakékoli zpřístupnění dovozcem údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další předávání.

(7) Mimo jiné se jedná o to, zda se předávání a další zpracování týká i osobních údajů vypovídajících o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetických údajů nebo biometrických údajů za účelem jedinečné identifikace fyzické osoby, údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údajů týkajících se rozsudků v trestních věcech nebo trestných činů.

(8) Tento požadavek může být splněn dílčím zpracovatelem přistupujícím k těmto doložkám v rámci příslušného modulu v souladu s doložkou 7.

(9) Tento požadavek může být splněn dílčím zpracovatelem přistupujícím k těmto doložkám v rámci příslušného modulu v souladu s doložkou 7.

(10) Tuto lhůtu lze v nezbytném rozsahu s přihlédnutím ke složitosti a počtu žádostí prodloužit nejvýše o další dva měsíce. Dovozce údajů o takovém prodloužení řádně a neprodleně informuje subjekt údajů.

(11) Dovozce údajů může nabídnout nezávislé řešení sporů prostřednictvím rozhodčího orgánu pouze v případě, že je usazen v zemi, která ratifikovala Newyorskou úmluvu o výkonu rozhodčích nálezů.

(12) Pokud jde o dopad takových právních předpisů a postupů na dodržování těchto doložek, za součást celkového posouzení lze považovat různé prvky. Mezi tyto prvky mohou patřit relevantní a zdokumentované praktické zkušenosti s předchozími případy žádostí o zpřístupnění od orgánů veřejné moci nebo neexistence takových žádostí, které pokrývají dostatečně reprezentativní časový rámec. Týká se to zejména interních záznamů nebo jiné dokumentace, vypracovávané průběžně v souladu s náležitou péčí a certifikované na úrovni vrcholového vedení, za předpokladu, že tyto informace lze v souladu s právními předpisy sdílet se třetími stranami. Pokud se na základě této praktické zkušenosti dospěje k závěru, že dovozci údajů nebude bráněno v dodržování těchto

doložek, je třeba to podpořit dalšími relevantními, objektivními prvky a je na smluvních stranách, aby pečlivě zvážily, zda tyto prvky mají společně dostatečnou váhu na podporu tohoto závěru, pokud jde o jejich spolehlivost a reprezentativnost. Smluvní strany musí zejména zohlednit, zda jsou jejich praktické zkušenosti potvrzeny veřejně dostupnými nebo jinak přístupnými spolehlivými informacemi o existenci či neexistenci žádostí ve stejném odvětví a/nebo o uplatňování práva v praxi, jako je například judikatura a zprávy nezávislých orgánů dohledu, a nejsou s nimi v rozporu.

Zásady ochrany osobních údajů

Platí od 19. července 2023 | Zobrazit předchozí verzi Zásad ochrany osobních údajů | Porovnat změny

Ochrana osobních údajů je pro společnost ESET, spol. s r. o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, která je zapsaná v Obchodním registru vedeném Okresním soudem Bratislava I, oddíl Sro, vložka číslo 3586/B, IČO: 31333532, jako pro správce údajů („ESET“ nebo „My“) obzvlášť důležitá. Snažíme se dodržovat požadavky na transparentnost, které jsou právně standardizovány v rámci Obecného nařízení EU o ochraně osobních údajů („GDPR“). Abychom dosáhli tohoto cíle, zveřejňujeme tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků („Koncový uživatel“ nebo „Vy“) jako subjektů údajů o následujících tématech týkajících se ochrany osobních údajů:

- Právní základ pro zpracování osobních údajů
- Sdílení a důvěrnost dat
- Zabezpečení dat
- Vaše práva jako subjektu údajů
- Zpracování vašich osobních údajů
- Kontaktní informace.

Právní základ pro zpracování osobních údajů

Při zpracování dat používáme v souladu s příslušným legislativním rámcem v souvislosti s ochranou osobních údajů jen několik právních základů. Zpracování osobních údajů ve společnosti ESET je potřebné zejména za účelem plnění dokumentu Podmínky použití („Podmínky“) odsouhlaseného s koncovým uživatelem (dle článku 6 (1) (b) nařízení GDPR), který je platný pro poskytování produktů nebo služeb společnosti ESET, pokud není výslovně uvedeno jinak, například:

- Oprávněný zájem: Právní základ (dle článku 6 (1) (f) nařízení GDPR), který nám umožňuje zpracovávat údaje o tom, jak naši zákazníci využívají naše služby a jak jsou s nimi spokojeni, abychom jim mohli poskytnout nejlepší možnou ochranu, podporu a služby. Podle platných právních předpisů je za oprávněný zájem považován i marketing, proto se při marketingové komunikaci s našimi zákazníky obvykle spoléháme na tento koncept.
- Souhlas (dle článku 6 (1) (a) nařízení GDPR): Můžeme jej od vás vyžadovat v konkrétních situacích, kdy považujeme tento právní základ za nejvhodnější, nebo pokud to vyžaduje zákon.
- Splnění zákonné povinnosti (dle článku 6 (1) (c) nařízení GDPR): Například specifikace požadavků na elektronickou komunikaci nebo uchovávání dokumentů souvisejících s fakturací.

Sdílení a důvěrnost dat

Vaše data nesdílíme se třetími stranami. ESET je ale společnost s celosvětovou působností a v rámci naší prodejní, servisní a podpůrné sítě využíváme přidružené firmy a partnery. Informace o licencování, fakturaci a technické podpoře, které společnost ESET zpracovává, mohou být přenášeny k přidruženým firmám nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb nebo podpora.

Společnost ESET upřednostňuje zpracování svých dat v Evropské unii (EU). V závislosti na vaší poloze (používání našich produktů a/nebo služeb mimo EU) a/nebo službě, kterou jste si zvolili, ovšem může být nutné přenést vaše data do země mimo EU. Služby třetích stran využíváme například ve spojení s cloudovým computingem. V těchto případech si naše poskytovatele služeb pečlivě vybíráme a zajišťujeme příslušnou úroveň ochrany dat prostřednictvím smluvních, ale i technických a organizačních opatření. Je pravidlem, že uzavíráme standardní smluvní klauzule pro EU, ke kterým v případě potřeby přijímáme doplňková smluvní omezení.

U některých zemí mimo EU, jako jsou Spojené království nebo Švýcarsko, již EU uznala srovnatelnou úroveň ochrany dat. Vzhledem ke srovnatelné úrovni ochrany dat nevyžaduje přenos dat do těchto zemí žádnou speciální autorizaci nebo smluvní dohodu.

Spoléháme se na služby třetích stran související s cloud computingem, které poskytuje společnost Microsoft jako poskytovatel cloudových služeb.

Zabezpečení dat

Společnost ESET implementuje příslušná technická a organizační opatření k zajištění úrovně bezpečnosti, která odpovídá potenciálním rizikům. Děláme vše, co je v našich silách, abychom zajistili nepřetržitou důvěrnost, integritu, dostupnost a odolnost zpracovatelských systémů a služeb. Pokud však dojde k narušení ochrany údajů, které ohrožuje vaše práva a svobody, jsme připraveni informovat příslušné dozorčí orgány i ohrožené koncové uživatele jakožto subjekty údajů.

Práva subjektu údajů

Práva každého koncového uživatele jsou důležitá a rádi bychom vás informovali, že všichni koncoví uživatelé (z libovolné země v EU nebo mimo ni) mají společností ESET garantována následující práva. Pokud chcete uplatnit svá práva subjektu údajů, můžete nás kontaktovat prostřednictvím formuláře podpory nebo e-mailem na adrese dpo@eset.sk. Za účelem identifikace po vás budeme požadovat následující údaje: Jméno, e-mailová adresa a – pokud jsou k dispozici – licenční klíč nebo číslo zákazníka a afilace společnosti. Neposílejte nám prosím žádné jiné osobní údaje, jako je datum narození. Rádi bychom vás upozornili, že v zájmu zpracování vaší žádosti a za účelem identifikace budeme zpracovávat vaše osobní údaje.

Právo odvolat souhlas. Právo odvolat souhlas lze uplatnit pouze v případě zpracování založeného výhradně na souhlasu. Pokud zpracováváme vaše osobní údaje na základě vašeho souhlasu, máte právo svůj souhlas kdykoli odvolat i bez uvedení důvodu. Vaše odvolání souhlasu bude platné pouze do budoucna a nebude mít vliv na legálnost údajů zpracovaných před odvoláním.

Právo vznést námitku. Právo vznést námitku proti zpracování lze uplatnit v případě zpracování založeného na oprávněném zájmu společnosti ESET nebo třetí strany. Pokud zpracováváme vaše osobní údaje v zájmu ochrany oprávněného zájmu, máte jako subjekt údajů právo kdykoli vznést námitku vůči námi uvedenému oprávněnému zájmu a vůči zpracování vašich osobních údajů. Vaše námitka bude platná pouze do budoucna a nebude mít vliv na zákonnost údajů zpracovaných před vznesením námitky. Pokud vaše osobní údaje zpracováváme pro účely přímého marketingu, není nutné u námitky uvádět důvody. Platí to rovněž pro profilování, pokud je spojeno s přímým marketingem. Ve všech ostatních případech vás žádáme, abyste nás stručně informovali o svých stížnostech vůči oprávněnému zájmu společnosti ESET na zpracování vašich osobních údajů.

Upozorňujeme vás, že v některých případech jsme i přes odvolání vašeho souhlasu oprávněni dále zpracovávat vaše osobní údaje na jiném právním základě, například za účelem plnění smlouvy.

Právo na přístup. Jako subjekt údajů máte právo kdykoli bezplatně získat informace o vašich údajích, které má společnost ESET uloženy.

Právo na opravu. Pokud si o vás omylem uložíme nesprávné osobní údaje, máte právo na jejich opravu.

Právo na výmaz a právo na omezení zpracování. Jako subjekt údajů máte právo požádat o výmaz nebo o omezení zpracování vašich osobních údajů. Pokud například zpracováváme vaše osobní údaje s vaším souhlasem a vy tento souhlas odvoláte, přičemž neexistuje žádný jiný právní základ (například smlouva), vymažeme vaše osobní údaje okamžitě. Vaše osobní údaje budou rovněž vymazány, jakmile nebudou dále vyžadovány pro uvedené účely na konci období uchovávání.

Pokud vaše údaje využíváme pouze za účelem přímého marketingu a vy odvoláte svůj souhlas nebo vznesete námitku vůči uvedenému oprávněnému zájmu společnosti ESET, omezíme zpracování vašich osobních údajů do té míry, že vaše kontaktní údaje přidáme na naši interní černou listinu, abychom předešli nevyžádanému kontaktování. V ostatních případech budou vaše osobní údaje vymazány.

Upozorňujeme, že může být potřebné, abychom vaše údaje měly uloženy do konce platnosti povinností na uchovávání a období stanovených legislativou nebo dozorčími úřady. Povinnosti na uchovávání a příslušná období mohou také vyplývat ze zákonů Slovenské republiky. Po uplynutí daných lhůt budou příslušné údaje rutinně vymazány.

Právo na přenositelnost dat. Jako subjektu dat vám rádi poskytneme osobní údaje, které o vás společnost ESET zpracovává, ve formátu xls.

Právo podat stížnost. Jako subjekt údajů máte právo kdykoli podat stížnost u dozorčího orgánu. Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Příslušným dozorčím orgánem pro ochranu osobních údajů je Úrad na ochranu osobných údajov Slovenskej republiky, který sídlí na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Zpracování vašich osobních údajů

Služby poskytované společností ESET implementované v našem webovém produktu jsou poskytovány za podmínek uvedených v Podmínkách použití, ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o zpracování údajů spojených s poskytováním našich produktů a služeb. Poskytujeme různé služby s přihlédnutím k podmínkám a produktové dokumentaci. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

- Pro účely správy bezpečnostních produktů ESET jsou vyžadovány ID licence a jméno, název produktu, informace o licenci, informace o aktivaci a vypršení platnosti a informace o hardwaru a softwaru týkající se spravovaného zařízení s nainstalovaným bezpečnostním produktem ESET. Kvůli usnadnění správy a dohledu nad funkcemi a službami jsou shromažďovány a uchovávány záznamy týkající se aktivit spravovaných bezpečnostních produktů ESET a spravovaných zařízení.
- Dále jsou zpracovávány informace o procesu instalace, včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů nebo spravovaných zařízení, jako jsou údaje o hardwaru, ID instalace, ID licencí, IP adresa, MAC adresa, použité e-mailové adresy, souřadnice GPS mobilního zařízení a nastavení konfigurace produktu.
- Kvůli zajištění bezpečnosti infrastruktury a pro účely vykazování je třeba zpracovávat telemetrická data včetně počtu uživatelů, zásad, přihlašovacích údajů, úloh, oznámení, spravovaných zařízení, hrozeb atd a také hlavičky protokolu HTTP.
- Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb.
- Za účelem poskytování podpory mohou být vyžadovány kontaktní informace a údaje obsažené ve vašich požadavcích na podporu. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí

podpory, jako jsou například vygenerované soubory protokolů.

- Pro funkce analýzy zranitelnosti a správy záplat budou zpracovávány další informace. Pro analýzu zranitelnosti budou shromážděny a zpracovány informace týkající se názvu a identifikátoru zranitelnosti, závažnosti a skóre dopadu pro spravovaná zařízení. Funkce správy záplat vyžaduje také název, verzi a dodavatele aplikace, verzi záplaty chybějící v zařízení a identifikátor chybějící záplaty.
- Údaje o využívání naší služby jsou na konci relace zcela anonymizovány. Po ukončení relace nejsou ukládány žádné osobní údaje, na jejichž základě by vás bylo možné identifikovat.
- Zpětnou vazbu nám můžete poskytnout prostřednictvím našich webových formulářů. Pro účely následných kroků může být vyžadována vaše e-mailová adresa a informace o licenci a počtu spravovaných zařízení.

Upozorňujeme, že pokud osoba používající naše produkty a služby není koncový uživatel, který si zakoupil produkt nebo službu a přijal smluvní podmínky (například zaměstnanec koncového uživatele, člen rodiny nebo osoba, která od koncového uživatele jiným způsobem dostala oprávnění používat produkt nebo službu v souladu s podmínkami), je zpracování údajů prováděno na základě oprávněného zájmu společnosti ESET, jak je definován v článku 6 (1) f) nařízení GDPR, abychom mohli uživateli autorizovanému koncovým uživatelem umožnit používání námi poskytovaných produktů a služeb v souladu s podmínkami.

Kontaktní informace

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk