Příručka aplikace Symantec™ Endpoint Protection 14.3 RU1 pro klienta Mac

Listopad 2020

Ochrana počítače Mac pomocí aplikace Symantec Endpoint Protection

Aplikace Symantec Endpoint Protection kombinuje několik vrstev ochrany, aby zabezpečila počítač proti útokům v podobě virů a spywaru a také proti pokusům o narušení.

Typy ochrany popisují jednotlivé vrstvy ochrany.

Table 1: Typy ochrany

Ochrana	Popis
Ochrana před viry a spywarem	Aplikace Symantec Endpoint Protection nabízí plánovaná prověřování výskytu virů, prověřování na požádání a funkci Auto-Protect, která je spuštěna na pozadí a sleduje viry. Pokud je nalezen virus, aplikace Symantec Endpoint Protection jej odstraní. Ochrana počítače Mac pomocí ochrany před viry a spywarem
Ochrana před síťovými hrozbami	Aplikace Symantec Endpoint Protection umožňuje zachytit data v síťové vrstvě. Využívá signatury k prověřování paketů nebo jejich proudů. Při prověřování jednotlivých paketů vyhledává vzory, které odpovídají specifikacím útoku v síti nebo v prohlížeči. Ochrana před síťovými hrozbami zahrnuje následující: • Prevence narušení, která zjišťuje útoky na součásti operačního systému a na aplikační vrstvu. Když aplikace Symantec Endpoint Protection zjistí síťovou hrozbu, zablokuje ji. • Bránu firewall, která povoluje nebo blokuje síťový provoz na základě zásad a pravidel brány firewall. (od verze 14.2.) Ochrana počítače Mac pomocí ochrany před síťovými hrozbami
Řízení zařízení	Správci aplikace Symantec Endpoint Protection Manager mohou konfigurovat zásady řízení zařízení. Pomocí zásady lze blokovat nebo povolit zařízení na základě názvu, výrobce, modelu nebo sériového čísla. V případě spravovaných klientů se nastavení řízení zařízení zobrazují na kartě **Pokročilé**. U nespravovaných klientů není řízení zařízení k dispozici. Řízení zařízení v klientovi aplikace Symantec Endpoint Protection pro systém Mac
Endpoint Detection and Response	Správci aplikace Symantec Endpoint Protection Manager nakonfigurují zásady zapisovače aktivit, které poskytují prostředky ke zjišťování a odhalování podezřelé síťové aktivity.

Klient do počítače automaticky stáhne definice virů, definice IPS a aktualizace produktu.

Aktualizace definic virů, definic prevence narušení a klientského softwaru

Ochrana počítače Mac pomocí ochrany před viry a spywarem

Aplikace Symantec Endpoint Protection pomocí definic virů zjišťuje známé viry během plánovaných prověřování a ručních prověřování. Funkce Auto-Protect pomocí definic virů neustále prověřuje činnost počítače.

Pokud aplikace Symantec Endpoint Protection zjistí virus nebo jiné bezpečností riziko, zobrazí upozornění. Virus nebo jiné bezpečnostní riziko jsou zjištěny, když nastane některá z těchto situací:

- Funkce Auto-Protect nalezne virus při sledování počítače.
- Funkce Auto-Protect nalezne virus při plánovaném nebo ručně spuštěném prověření.

Ve výchozím nastavení se aplikace Symantec Endpoint Protection automaticky pokusí opravit jakýkoli virus, který nalezne. Pokud nedokáže soubor opravit, klient bezpečně přesune soubor do karantény, aby nemohl poškodit počítač.

Klient tyto opravy obvykle provede bez nutnosti jakékoli akce z vaší strany. Když počítač nalezne virus, můžete se rozhodnout odeslat informace o něm společnosti Symantec.

Za určitých okolností vás klient požádá, abyste vybrali, zda chcete nalezený infikovaný soubor opravit, odstranit nebo obnovit. Na základě vašich reakcí bude určena akce, kterou klient s infikovaným souborem provede.

Reakce na zprávy o infekcích a zjištění rizik

Zapnutí nebo vypnutí odesílání informací o zabezpečení společnosti Symantec

Ochrana počítače Mac pomocí ochrany před síťovými hrozbami

Ochrana před hrozbami sítě zahrnuje následující technologie ochrany:

- Prevence narušení
- Brána firewall

Prevence narušení

Funkce prevence narušení automaticky zjišťuje a blokuje pokusy o napadení ze sítě. Prevence narušení představuje vnitřní vrstvu zabezpečení klientských počítačů. Prevence narušení je někdy také označována jako systém IPS (Intrusion Prevention System).

Prevence narušení umožňuje zachytit data v síťové vrstvě. Využívá signatury k prověřování paketů nebo jejich proudů. Při prověřování jednotlivých paketů vyhledává vzory, které odpovídají specifikacím útoku v síti nebo v prohlížeči. Prevence narušení odhaluje útoky na komponenty operačního systému a na aplikační vrstvu.

Prevence narušení zjišťuje útoky na klientské počítače na základě signatur. U známých útoků prevence narušení automaticky odstraňuje pakety, které odpovídají dané signatuře.

Brána firewall

Brána firewall sleduje síťový provoz a blokuje potenciálně škodlivý provoz, aby ochránila váš počítač Mac. Brána firewall aplikace Symantec Endpoint Protection není v nespravovaném klientovi k dispozici.

Brána firewall aplikace Symantec Endpoint Protection sleduje provoz ve vrstvě Transport a Internet. Vestavěná brána firewall počítače Mac sleduje provoz ve vyšší aplikační vrstvě, poté, co ji sleduje brána firewall aplikace Symantec Endpoint Protection. Proto můžete obě brány firewall povolit najednou, aby běžely vedle sebe.

K povolování a blokování síťového provozu používá brána firewall následující typy pravidel:

- Výchozí pravidla
- Vlastní pravidla
- Integrovaná pravidla
- Pravidla ochrany

Mezi tato pravidla patří zjišťování prověřování portů, zjišťování odepření služby, ochrana proti falšování adres MAC, služba Smart DHCP a Smart DNS. Nastavení brány firewall je řízeno výhradně správcem aplikace Symantec Endpoint Protection Manager. Bránu firewall můžete povolit nebo zakázat pouze v případě, že správce uživatelskému klientovi povolí řízení počítače Mac.

Ochrana pomocí brány firewall byla přidána ve verzi 14.2.

Správa prevence narušení

Správa ochrany pomocí brány firewall pro klienta systému Mac

Kompatibilita operačního systému s aplikací Symantec Endpoint Protection pro systém Mac

Aplikace Symantec Endpoint Protection pro systém Mac podporuje následující verze operačního systému:

- macOS 10.15 až 10.15.5
- macOS 10.14
- macOS 10.13

Další informace o podpoře starších verzí operačního systému Mac naleznete v tématu Kompatibilita systému Mac s klientem aplikace Endpoint Protection.

Autorizace rozšíření jádra pro aplikaci Symantec Endpoint Protection v systému macOS 10.13 nebo novějším

Poznámky k verzi, nové opravy a systémové požadavky pro všechny verze aplikace Endpoint Protection

Instalace klienta Symantec Endpoint Protection pro systém Mac

Můžete přímo nainstalovat klienta Symantec Endpoint Protection na počítač Mac, pokud nemůžete použít nebo nechcete použít vzdálenou instalaci bez vyžádání. Kroky instalace jsou u spravovaného i nespravovaného klienta podobné.

Jediný způsob, jak nainstalovat spravovaného klienta, je pomocí balíčku vytvořeného aplikací Symantec Endpoint Protection Manager. Nespravovaného klienta můžete kdykoli konvertovat na spravovaného klienta, a to importem nastavení komunikace klient-server do klienta Mac.

NOTE
Chcete-li připravit klienta Symantec Endpoint Protection pro Mac k použití třetími stranami, přečtěte si Export a použití klienta Symantec Endpoint Protection přes Apple Remote Desktop or Casper.

Table 2: Metody instalace klienta systému Mac

Pokud jste stáhli instalační soubor.	1. Extrahujte obsah do složky v počítači Mac a otevřete složku. 2. Otevřete `SEP_MAC`. 3. Zkopírujte `Symantec Endpoint Protection.dmg` na plochu počítače Mac. 4. Dvakrát klikněte na `Symantec Endpoint Protection.dmg` a ze souboru vytvořte virtuální disk. Potom můžete nainstalovat klienta Symantec Endpoint Protection pro systém Mac
Pokud máte klientský instalační balíček ZIP z portálu podpory Broadcom.	1. Zkopírujte soubor na plochu počítače Mac. Soubor může mít název `Symantec Endpoint Protection.zip` nebo `Symantec_Endpoint_Protection_verze_Mac_Client.zip`, kdeverzeje verzí produktu. 2. Klikněte pravým tlačítkem myši na položku **Otevřít s > Nástroj Archiv** a extrahujte obsah souboru. 3. Otevřete výslednou složku. Potom můžete nainstalovat klienta Symantec Endpoint Protection pro systém Mac.

Výsledná virtuální bitová kopie disku nebo složka obsahuje instalační program aplikace a složku nazvanou Další zdroje. Aby byla instalace úspěšná, obě položky musí být ve stejném umístění. Pokud instalační program zkopírujete z jiného umístění, je nutné také zkopírovat složku Další zdroje.

Instalace klienta Symantec Endpoint Protection pro systém Mac:

1. Dvakrát klikněte na možnost `InstalovatSymantec Endpoint Protection`.
2. Pokud chcete instalaci spustit, klikněte na možnost **Instalovat**.
3. Pokud chcete nainstalovat pomocný nástroj potřebný k instalaci klienta Symantec Endpoint Protection, zadejte uživatelské jméno a heslo pro správce systému Mac a klikněte na tlačítko **Install Helper**.
4. Po instalaci klikněte na tlačítko **Pokračovat** a dokončete nastavení klienta Symantec Endpoint Protection.
5. Pokud chcete klienta Symantec Endpoint Protection nastavit, postupujte takto:

Schvalte rozšíření systému Symantec Endpoint Protection.	V dialogovém okně **Zabezpečení a ochrana osobních údajů** na kartě **Obecné** v části **Načítání systémového softwaru z aplikace „Symantec Endpoint Protection“ bylo zablokováno** klikněte na tlačítko **Povolit**. V případě potřeby klikněte na ikonu zámku a proveďte změny. Aby aplikace Symantec Endpoint Protection zcela fungovala, je nutné povolit rozšíření systému. Autorizace rozšíření systému pro aplikaci Symantec Endpoint Protection v systému macOS 10.15 a novějším
Povolte úplný přístup k disku.	V dialogovém okně **Zabezpečení a ochrana osobních údajů** na kartě **Ochrana osobních údajů** zkontrolujte, zda má aplikace **Symantec System Extension** povolený přístup k datům a nastavení správy pro všechny uživatele zařízení Mac. V případě potřeby klikněte na ikonu zámku a proveďte změny.
Povolte změny profilu sítě.	Po zobrazení výzvy **Aplikace Symantec Endpoint Protection chce filtrovat obsah sítě** klikněte na tlačítko **Povolit**.

6. Klikněte na tlačítko **Dokončit**.

Autorizace rozšíření systému pro aplikaci Symantec Endpoint Protection v systému macOS 10.15 a novějším

Požadování schválení rozšíření systému je nová funkce zabezpečení počínaje verzí systému macOS 10.15. Aby aplikace Symantec Endpoint Protection zcela fungovala, je nutné povolit rozšíření systému.

Pokud chcete schválit rozšíření systému pro aplikaci Symantec Endpoint Protection během nastavování klienta aplikace Symantec Endpoint Protection, klikněte v dialogovém okně **Zabezpečení a ochrana osobních údajů,** na kartě **Obecné** v možnosti **Načítání systémového softwaru z aplikace „Symantec Endpoint Protection“ bylo zablokováno** na položku **Povolit**.

Instalace klienta Symantec Endpoint Protection pro systém Mac

Výzva k upgradu klienta aplikace Symantec Endpoint Protection pro systém Mac

Správci aplikace Symantec Endpoint Protection Manager mohou nastavit, aby instalační balíček klienta automaticky upgradoval spravované klientské počítače pomocí nastavení pro instalaci klienta.

Pokud jste přihlášeni k počítači se systémem Mac, může se zobrazit výzva k restartu, po jehož provedení bude dokončena instalace. Restart můžete odložit na základě nastavení instalace klienta.

Pokud nejste přihlášeni k počítači se systémem Mac, při instalaci bude počítač se systémem Mac automaticky restartován.

Začínáme s klientem aplikace Symantec Endpoint Protection

Při otevření klienta aplikace Symantec Endpoint Protection se v horní části stránky zobrazí zpráva **You Are Protected**, dokud se neobjeví problém, který bude potřeba vyřešit. Kliknutím na tlačítko **Opravit** vyřešíte jakékoli potíže.

Klient aplikace Symantec Endpoint Protection zobrazí hlavní úkoly, které můžete provést.

Table 3: Stránky klienta aplikace Symantec Endpoint Protection

Možnost	Popis
Zabezpečení	Zobrazuje stav ochrany počítače.
Prověřuje	Umožňuje prověření počítače. Můžete si vybrat, zda spustíte rychlé prověření nebo úplné prověření. Můžete také přetáhnout soubor nebo složku a nechat je prověřit. Spuštění ručního prověřování
LiveUpdate	Spustí aktualizaci LiveUpdate, pomocí které aktualizuje definice a soubory produktu v aplikaci Symantec Endpoint Protection. Okamžitá aktualizace obsahu aplikace Symantec Endpoint Protection
Rozšířené	Poskytuje podrobnější možnosti ochrany před viry a spywarem, ochrany před síťovými hrozbami a aktualizací LiveUpdate.

Správa ochrany počítače Mac pomocí aplikace Symantec Endpoint Protection

Výchozí nastavení aplikace Symantec Endpoint Protection chrání počítač Mac před mnoha typy malwaru. Klient může zjištění malwaru zpracovat automaticky nebo vám může dát na výběr z několika způsobů, jak s malwarem naložit.

V závislosti na nastaveních zvolených správcem byste měli provádět následující akce k zajištění ochrany.

NOTE
Je možné, že správce vám provádění těchto akcí nepovolil.

Table 4: Ochrana počítače

Kroky	Popis
Krok 1: Zkontrolujte, že je povolena ochrana před viry a spywarem i ochrana před síťovými hrozbami.	Pokud je ochrana zapnutá, zobrazí se na stránce **Zabezpečení** zelený symbol zaškrtnutí a zpráva **Jste chráněni**. Zapnutí a vypnutí ochrany před viry a spywarem Zapnutí nebo vypnutí ochrany před síťovými hrozbami
Krok 2: Přesvědčte se, že jsou software i definice aktuální.	Na stránce **Zabezpečení** je zobrazen čas poslední aktualizace definic ochrany před viry a spywarem a ochrany před síťovými hrozbami. V části **LiveUpdate** je uvedeno datum poslední aktualizace produktu. Pokud chcete zobrazit číslo verze softwaru, klikněte na možnost **Nápověda > O aplikaci**.
Krok 3: V případě potřeby software a definice aktualizujte.	V klientovi Symantec Endpoint Protection klikněte na možnost **LiveUpdate** a spusťte okamžitou aktualizaci softwaru a definicí. Aktualizace definic virů, definic prevence narušení a klientského softwaru
Krok 4: Spusťte prověřování.	Můžete naplánovat prověřování v pravidelných časových intervalech nebo jej spustit ručně. Nastavení plánovaných prověřování Spuštění ručního prověřování

Správa nastavení ochrana před viry a spywarem

Obnovení licence k produktu

Pod ikonou klienta aplikace Symantec Endpoint Protection se na řádku nabídek může zobrazit zpráva, že vypršela platnost licence aplikace Symantec Endpoint Protection. Klient aplikace Symantec Endpoint Protection používá licenci k aktualizaci následujících položek:

- Klientský software
- Soubory definice ochrany k prověřování virů a spywaru a prevenci narušení

Klient může používat zkušební licenci nebo placenou licenci. Pokud jakákoli z nich vypršela, klient neaktualizuje žádné definice ani klientský software.

Pokud chcete licenci aktualizovat nebo obnovit, je třeba se u jakéhokoli typu licence obrátit na správce.

Reakce na zprávy o infekcích a zjištění rizik

Povolení nebo zakázání řízení zařízení v klientovi Symantec Endpoint Protection pro systém Mac

Správci aplikace Symantec Endpoint Protection Manager mohou pro spravované klienty nakonfigurovat zásadu řízení zařízení. Pomocí zásady lze blokovat nebo povolit zařízení na základě názvu, výrobce, modelu nebo sériového čísla.

Aktivity řízení zařízení můžete zobrazit na stránce **Pokročilé** po kliknutí na možnost **Aktivita > Security History**.

Pomocí nastavení **Řízení zařízení** v klientovi aplikace Symantec Endpoint Protection lze povolit nebo zakázat řízení zařízení. Pokud je řízení zařízení povoleno, můžete volitelně povolit nebo zakázat zobrazování oznámení při blokování nebo odblokování zařízení.

Chcete-li nastavení změnit, je potřeba se přihlásit pomocí přihlašovacích údajů správce systému Mac. Pokud jsou tato nastavení zobrazena šedě, byla uzamknuta správcem, takže tuto funkci nemůžete povolit ani zakázat.

Pomocí rozhraní klienta aplikace Symantec Endpoint Protection nemůžete přidat ani odebrat zařízení, která chcete blokovat nebo odblokovat.

> **NOTE**
> Nastavení řízení zařízení se řídí zásadou řízení zařízení aplikace Symantec Endpoint Protection Manager. Při dalším prezenčním signálu se provedené změny nastavení vrátí zpět na hodnoty určené zásadou.

U nespravovaných klientů není řízení zařízení k dispozici.

Přesměrování přenosů služby WSS u klienta pro systém Mac

Přesměrování přenosů služby WSS (WTR) umožňuje automatizovat přesměrování webového provozu na službu Symantec Web Security Service a zabezpečit webový provoz v každém koncovém počítači, který používá aplikaci Symantec Endpoint Protection.

Správce řídí nastavení, která používá přesměrování přenosů služby WSS, včetně adresy URL pro konfiguraci proxy serveru a volitelného kořenového certifikátu služby Symantec Web Security Service. Tato nastavení smí konfigurovat pouze správce aplikace Symantec Endpoint Protection Manager a tato nastavení se nezobrazují v uživatelském rozhraní klienta Symantec Endpoint Protection. Adresu URL konfiguračního souboru proxy serveru můžete zobrazit v počítači Mac pomocí možností **Systémové předvolby > Síť**, v části **Servery proxy**. Certifikát cloudových služeb je zobrazen v části **Svazek klíčů**.

Webové prohlížeče Safari, Chrome a Firefox verze 65 a novější podporují přesměrování přenosů služby WSS. Verze Symantec Endpoint Protection starší než 14.2 RU1 podporují pouze prohlížeče Safari a Chrome.

Odinstalování klienta aplikace Symantec Endpoint Protection pro systém Mac

Klienta aplikace Symantec Endpoint Protection pro systém Mac můžete odinstalovat pomocí ikony klienta v řádku nabídek. K odinstalaci klienta aplikace Symantec Endpoint Protection pro systém Mac jsou nutné přihlašovací údaje správce.

> **NOTE**
> Po odinstalaci klienta aplikace Symantec Endpoint Protection budete vyzváni, abyste restartovali klientský počítač a dokončili tak odinstalaci. Než začnete, uložte si veškerou rozdělanou práci a zavřete všechny otevřené aplikace.

Odinstalace klienta aplikace Symantec Endpoint Protection pro systém Mac:

1. V klientském počítači Mac otevřete klienta Symantec Endpoint Protection a poté klikněte na možnosti **Symantec Endpoint Protection > Odinstalovat Symantec Endpoint Protection**.
2. Opětovným kliknutím na možnost **Odinstalovat** zahajte odinstalaci.
3. Pokud chcete nainstalovat pomocný nástroj potřebný k odinstalaci klienta Symantec Endpoint Protection, zadejte uživatelské jméno a heslo pro správce systému Mac a klikněte na tlačítko **Nainstalovat pomocný nástroj**.
4. V dialogovém okně **Aplikace Symantec Endpoint Protection se pokouší upravit systémové rozšíření** zadejte uživatelské jméno a heslo k počítači Mac a poté klikněte na tlačítko **OK**.

   Můžete být vyzváni také k zadání hesla pro odinstalaci klienta. Toto heslo může být jiné než heslo správce systému Mac.
5. Po dokončení odinstalace klikněte na možnost **Restartovat**.

Pokud se odinstalace nezdaří, může být potřeba odinstalovat klienta jiným způsobem. Viz:

Odinstalace aplikace Symantec Endpoint Protection

Aktualizace definic virů, definic prevence narušení a klientského softwaru

Produkty společnosti Symantec při ochraně počítače před nově zjištěnými hrozbami vycházejí z aktuálních informací. Společnost Symantec tyto informace předává aplikaci Symantec Endpoint Protection prostřednictvím služby LiveUpdate. Služba LiveUpdate do počítače stahuje aktualizace produktu a definic prostřednictvím připojení k internetu.

Aktualizace definic jsou soubory, díky nimž mohou produkty Symantec využívat aktuální technologie ochrany před hrozbami. Služba LiveUpdate stáhne nové soubory signatur prevence narušení nebo definic virů z webu společnosti Symantec a následně jimi nahradí původní soubory.

Aktualizace produktu jsou vylepšení již nainstalovaného klienta. Aktualizace produktu obvykle slouží k rozšíření operačního systému nebo kompatibility hardwaru, k vyladění potíží s výkonem nebo k opravám chyb produktu. Aktualizace produktu jsou vydávány podle potřeby. Klient získává aktualizace produktu přímo ze serveru LiveUpdate. Aktualizace produktu a aktualizace definic jsou souhrnně označovány jako aktualizace obsahu.

Table 5: Způsoby aktualizace obsahu na počítači

Úloha	Popis
Okamžitá aktualizace obsahu	Aktualizaci LiveUpdate můžete spustit okamžitě. Okamžitá aktualizace obsahu aplikace Symantec Endpoint Protection

Správa ochrany počítače Mac pomocí aplikace Symantec Endpoint Protection

Okamžitá aktualizace obsahu aplikace Symantec Endpoint Protection

Definice a soubory produktu můžete okamžitě aktualizovat pomocí služby LiveUpdate. Ruční spuštění služby LiveUpdate se doporučuje v následujících případech:

- Klientský software byl nainstalován nedávno.
- Uběhla dlouhá doba od posledního prověřování.
- Předpokládáte výskyt viru nebo jiného malwaru.

Okamžitá aktualizace obsahu aplikace Symantec Endpoint Protection:

Aktualizaci LiveUpdate můžete spustit jedním z následujících způsobů:

- V řádku nabídek klikněte pravým tlačítkem myši na ikonu Symantec Endpoint Protection a poté klikněte na možnost **LiveUpdate**.
- Otevřete klienta aplikace Symantec Endpoint Protection a poté klikněte na možnost **LiveUpdate**.

Služba LiveUpdate se připojí k nastavenému serveru služby LiveUpdate, zkontroluje dostupné aktualizace a následně je stáhne a automaticky nainstaluje. Ve stavovém řádku je zobrazen průběh stahování.

Aktualizace definic virů, definic prevence narušení a klientského softwaru

Aktualizace obsahu aplikace Symantec Endpoint Protection podle plánu

Plány na spravovaných klientech pro systém Mac

Ve výchozím nastavení převezmou klienti pro systém Mac plán od aplikace Symantec Endpoint Protection Manager, na základě kterého se spouští aktualizace LiveUpdate každé čtyři hodiny. Plán určuje správce aplikace Symantec Endpoint Protection Manager. Spravovaní klienti nemohou odstranit, upravit ani zobrazit plán vytvořený správcem ani vytvořit nový plán.

Plány na nespravovaných klientech pro systém Mac

Můžete vytvořit plán, aby byla aktualizace LiveUpdate spouštěna automaticky v naplánovaných intervalech. Můžete nastavit plán na spuštění služby LiveUpdate v době, kdy nepoužíváte počítač.

Aktualizace obsahu aplikace Symantec Endpoint Protection podle plánu:

1. V klientovi aplikace Symantec Endpoint Protection klikněte na stránce **Pokročilé** na možnost **Nastavení produktu** a poté klikněte na ikonu nastavení **Naplánovaná aktualizace LiveUpdate**.

   Zobrazí se aktuální plán.

2. V rozevírací nabídce Plán aktualizace LiveUpdate vyberte požadovaný interval.

   Ve výchozím nastavení se aktualizace spouští každé **4** hodiny. Můžete rovněž vybrat možnost **Denně** nebo **Týdně** a zvolit čas, případně den a čas.

3. Klikněte na tlačítko **Použít změny**.

Okamžitá aktualizace obsahu aplikace Symantec Endpoint Protection

Aktualizace definic virů, definic prevence narušení a klientského softwaru

Připojení k serveru pro správu přes proxy server

Můžete být vyzváni, abyste aplikaci Symantec Endpoint Protection povolili použití vašich přihlašovacích údajů při připojení k serveru pro správu přes proxy server. Zobrazí se zpráva s dotazem, zda chcete procesu `symdaemon` povolit přístup ke svým přihlašovacím údajům.

Je nutné kliknout na možnost **Vždy povolit**. V opačném případě se bude daná zpráva zobrazovat při každé komunikaci klienta se serverem LiveUpdate. Pokud kliknete na možnost **Odmítnout**, nebude mít klient k dispozici aktualizace softwaru ani definic.

Aktualizace definic virů, definic prevence narušení a klientského softwaru

Správa nastavení ochrana před viry a spywarem

Ve výchozím nastavení aplikace Symantec Endpoint Protection poskytuje ochranu před viry a bezpečnostními riziky, včetně síťových hrozeb, ihned po spuštění počítače. Součástí ochrany před viry a spywarem je funkce Auto-Protect, která při spuštění programů vyhledává v těchto programech viry. Sleduje také výskyt všech činností v počítači, které by mohly znamenat přítomnost viru nebo bezpečnostního rizika. Funkce Auto-Protect zachytává viry a brání jim v infikování počítače. Funkci Auto-Protect je vhodné ponechat zapnutou.

V případě spravovaných klientů závisí úroveň řízení těchto nastavení na způsobu, jakým správce nakonfiguroval klienta. Při dalším prezenčním signálu se navíc provedené změny nastavení mohou vrátit zpět na hodnoty určené zásadou.

Správa ochrany proti virům a spywaru popisuje úkoly, které lze provést při správě ochrany proti virům a spywaru na počítači Mac.

Table 6: Správa ochrany před viry a spywarem

Kroky	Popis
Krok 1: Zapnutí nebo vypnutí ochrany před viry a spywarem	Ochranu před viry a spywarem můžete snadno povolit a zakázat. Společnost Symantec ji doporučuje ponechat zapnutou. Zapnutí a vypnutí ochrany před viry a spywarem
Krok 2: Přizpůsobení nastavení funkce Auto-Protect	Funkce Auto-Protect je důležitou součástí ochrany před viry a spywarem. Tyto možnosti můžete konfigurovat na stránce **Pokročilé**. Konfigurace nastavení funkce Auto-Protect a zóny prověřování
Krok 3: Prověření výskytu virů v počítači	Prověření výskytu virů můžete nastavit tak, aby se spouštěla podle plánu nebo aby se spouštěla okamžitě. Nastavení plánovaných prověřování Pozastavení, odložení a ukončení prověřování Spuštění ručního prověřování
Krok 4: Reakce při zjištění viru aplikací Symantec Endpoint Protection	Když aplikace Symantec Endpoint Protection prověřuje počítač, může provést následující: • Upozornit na akce, které můžete podniknout. • Informovat o ochranných akcích, které pro vás provedla. Reakce na zprávy o infekcích a zjištění rizik

Zapnutí a vypnutí ochrany před viry a spywarem

Ve výchozím nastavení je ochrana před viry a spywarem zapnutá spolu s funkcí Auto-Protect.

U funkce Auto-Protect lze dále nastavit jednotlivé podrobnější možnosti.

Pokud je ochrana před viry a spywarem vypnutá, zobrazí se na stránce **Stav** červený symbol „x“ a zpráva **Ochrana před viry a spywarem – deaktivováno**. Pokud je ochrana zakázaná, měli byste ji co nejdříve opět povolit.

NOTE
Plánovaná prověření se provádí bez ohledu na to, zda je ochrana před viry a spywarem povolená či zakázaná. Správce může zakázat přístup k některým nastavením aplikace Symantec Endpoint Protection. Nemusí být možné tato nastavení zakázat, naplánovat prověřování nebo upravit možnosti ochrany. Ke změně těchto nastavení může být požadováno heslo správce systému Mac.

Zapnutí a vypnutí ochrany před viry a spywarem:

1. Pokud chcete zapnout ochranu proti virům a spywaru, klikněte v klientovi aplikace Symantec Endpoint Protection na stránce **Pokročilé** na možnost **Chránit můj Mac** a povolte možnost **Automatické prověřování**.
2. Pokud chcete ochranu proti virům a spywaru vypnout, klikněte v klientovi aplikace Symantec Endpoint Protection na stránce **Pokročilé** na možnost **Chránit můj Mac** a poté zakažte možnost **Automatické prověřování**.

Konfigurace nastavení funkce Auto-Protect a zóny prověřování

Správa nastavení ochrany před viry a spywarem

Reakce na zprávy o infekcích a zjištění rizik

Konfigurace nastavení funkce Auto-Protect a zóny prověřování

Pokud správce tuto možnost povolí, můžete ve spravovaných klientech upravit nastavení funkce Auto-Protect, která určují způsob sledování virů a opravy infikovaných souborů.

Nastavení funkce Auto-Protect se zobrazí jako možnosti v části **Protect My Mac**. Pokud chcete funkci Auto-Protect povolit, je nutné povolit funkci**Automatické prověření**.

V části **Scan Zone Settings** můžete určit soubory, které chcete do prověřování zahrnout nebo je z něj vyloučit.

Konfigurace nastavení funkce Auto-Protect:

1. V klientovi aplikace Symantec Endpoint Protection klikněte na stránce **Pokročilé** na příkaz **Chránit můj Mac** a poté klikněte na ikonu nastavení funkce **Automatic Scans**.
2. Upravte libovolné z následujících možností:

Auto Quarantine (Automaticky přesunout do karantény),	Je možné zvolit, jestli odeslat libovolné soubory, které není možné opravit, do karantény.
Auto Repair (Automaticky opravit),	Je možné zvolit, aby funkce Auto-Protect automaticky opravovala všechny infikované soubory, které najde.
Prověřit	Můžete zvolit možnost **Datové disky** nebo **Všechny ostatní disky**.
Prověřovat komprimované soubory	Je možné zvolit, jestli chcete do prověřování funkcí Auto-Protect zahrnout komprimované soubory. Do prověřování se zahrne komprimovaný soubor i soubory, které obsahuje.

WARNING
Pokud nezvolíte možnost **Auto Repair**, žádné infikované soubory nebudou přesunuty do karantény, i když vyberete možnost **Auto Quarantine**. Software vám položí otázku, jestli chcete infikovaný soubor opravit. Pokud soubor neopravíte, zůstane v počítači. Pokud zvolíte možnost **Auto Repair** a zároveň nevyberete možnost **Auto Quarantine**, budou všechny infikované soubory odstraněny.

3. Klikněte na tlačítko **Hotovo**.

Konfigurace nastavení zón prověřování:

1. V klientovi aplikace Symantec Endpoint Protection klikněte na stránce **Pokročilé** na příkaz **Chránit můj Mac** a poté klikněte na ikonu nastavení funkce **Scan zone Settings**.
2. Upravte libovolné z následujících možností:

Scan Everywhere (Prověřovat vše)	Všechny soubory a procesy v počítači jsou prověřovány vždy, když je použijete.
Scan Only (Prověřovat pouze)	Do prověřování jsou zahrnuty pouze soubory nebo složky, které určíte.
Don't Scan (Neprověřovat)	Jsou prověřovány všechny soubory s výjimkou souborů či složek, které z prověřování vyloučíte.
Použít výchozí hodnoty	Pokud zvolíte tuto možnost, prověřuje se vše.

3. Klikněte na tlačítko **OK**.

Ochrana počítače Mac pomocí ochrany před viry a spywarem

Zapnutí a vypnutí ochrany před viry a spywarem

Správa souborů umístěných do karantény

Nastavení plánovaných prověřování

Aplikace Symantec Endpoint Protection automaticky spustí výchozí prověřování, pokud máte spravovaného klienta. Pokud vám to správci umožní, můžete nastavit další plánovaná prověřování.

> **NOTE**
> V nespravovaném klientovi je nutné spustit vlastní prověřování. Společnost Symantec doporučuje co nejdříve spustit úplné ruční prověřování a poté nastavit pravidelné plánované prověřování. Plánované i ruční prověřování můžete pozastavit nebo odložit.

Ve spravovaném klientovi se výchozí prověřování spouští každý den ve 20:00, přičemž automatická oprava je povolena.

Spuštění ručního prověřování

Nastavení plánovaných prověřování:

1. V klientovi aplikace Symantec Endpoint Protection klikněte na stránce **Pokročilé** na možnost **Chránit můj Mac** a poté klikněte na ikonu nastavení **Plánovaná prověření**.
2. V dialogovém okně klikněte na možnost **Přidat plánované prověřování** nebo klikněte na aktuální plánované prověřování a poté klikněte na možnost **Upravit**, čímž upravíte jeho nastavení.
3. Na kartě **Položky prověření** můžete nastavit následující možnosti:

Jednotky	Můžete si vybrat, zda chcete nebo nechcete prověřit **pevné disky** a **vyměnitelné jednotky**.
Složky	Můžete si vybrat, zda chcete prověřit **domovskou složku (aktivní uživatel)**, **aplikace** a **soubory knihovny**. Pokud není v okamžiku plánovaného prověřování domovské složky přihlášen žádný uživatel, prověřování se nespustí.
Možnosti prověřování	Můžete si vybrat z následujících možností: • **Scan Compressed (Prověřovat komprimované soubory),** • **Auto Repair (Automaticky opravit),** • **Auto Quarantine (Automaticky přesunout do karantény),** • **Enable Idle Time Scan (Povolit prověřování v době nečinnosti).**

4. Na kartě **Naplánovat prověření** můžete nastavit následující možnosti:

Naplánovat prověření	Můžete nastavit spuštění prověřování v konkrétním intervalu v hodinách, denně, týdně nebo měsíčně. Při plánování nového prověřování je ve výchozím nastavení vybrána možnost **Spustit v konkrétním intervalu**.
Spouštět každou	Tato možnost je k dispozici, když je vybrána možnost **Spustit v konkrétním intervalu** u položky **Naplánovat prověření**.
Čas spuštění	Tato možnost je k dispozici, pokud u položky Naplánovat prověření vyberte možnost **Denně**, **Týdně** nebo **Měsíčně**. Můžete si vybrat dobu spuštění prověřování. Je vhodné vybrat dobu, kdy obvykle nepracujete, protože prověřování může zpomalit chod počítače.
Zapnuto	Tato možnost je k dispozici, pokud u položky Naplánovat prověření vyberte možnost **Týdně** nebo **Měsíčně**. Můžete si vybrat den v týdnu nebo měsíc, kdy bude spuštěno prověřování. Doporučujeme vybrat dobu, kdy obvykle nepracujete, protože prověřování může zpomalit chod počítače.

5. Na kartě **Ladění** můžete upravit způsob optimalizace výkonu prověřování.
6. Klikněte na tlačítko **OK**.
7. Klikněte na tlačítko **Hotovo**.

Pozastavení, odložení a ukončení prověřování

Správa ochrany počítače Mac pomocí aplikace Symantec Endpoint Protection

Reakce na zprávy o infekcích a zjištění rizik

Zapnutí nebo vypnutí odesílání informací o zabezpečení společnosti Symantec

Spuštění ručního prověřování

V některých případech může být potřeba provést ruční prověřování souborů, například pokud chcete prověřit soubory, které byly do počítače uloženy před instalací aplikace Symantec Endpoint Protection, nebo pokud chcete prověřit některé soubory vyloučené z plánovaného prověřování.

> **NOTE**
> Plánované i ruční prověřování můžete pozastavit nebo odložit.

Spuštění ručního prověřování:

V klientovi aplikace Symantec Endpoint Protection na stránce **Prověřování** proveďte jednu z následujících akcí:

- Pokud chcete spustit rychlé prověření, klikněte na možnost **Quick Scan** a poté klikněte na možnost **Start a Quick Scan**.
- Pokud chcete spustit úplné prověření, klikněte na možnost **Full Scan** a poté klikněte na možnost **Start a Full Scan**.
- Pokud chcete prověřit soubor nebo složku, klikněte na možnost **File Scan** a poté klikněte na možnost **Select a File**. Otevře se aplikace Finder a vy si budete moci vybrat mezi možností **Zobrazit skryté soubory** a **Prověřit komprimované soubory**. Budete také moci povolit možnost **Automaticky opravit** a **Automaticky přesunout do karantény**.

Pozastavení, odložení a ukončení prověřování

Nastavení plánovaných prověřování

Zapnutí nebo vypnutí odesílání informací o zabezpečení společnosti Symantec

Pozastavení, odložení a ukončení prověřování

Funkce pozastavení umožňuje prověřování zastavit a pokračovat v něm jindy (kdy si zvolíte). Každé prověřování také můžete kdykoli ukončit a zrušit. K použití těchto funkcí nepotřebujete oprávnění správce.

Když se prověřování obnoví, začne tam, kde bylo zastaveno.

> **NOTE**
> Pokud klient prověřuje komprimovaný soubor a vy prověřování pozastavíte, klient může zareagovat na pozastavení až po několika minutách.

Pokud je povoleno odložení, můžete prověřování odložit. Je však možné odložit pouze prověřování, které ještě nebylo zahájeno. Probíhající prověřování nelze odložit.

Pozastavení nebo ukončení probíhajícího plánovaného prověřování:

1. V dialogovém okně průběhu prověřování klikněte na tlačítko **Pozastavit**.
2. Chcete-li v prověřování pokračovat, klikněte v dialogovém okně průběhu prověřování na tlačítko **Pokračovat**. Kliknutím na tlačítko **Zastavit** prověřování ukončíte. Okno můžete také zavřít kliknutím na tlačítko **Hotovo**.

Pozastavení nebo ukončení probíhajícího ručního prověřování:

1. Chcete-li prověřování pozastavit, klikněte v dialogovém okně průběhu prověřování na tlačítko **Pozastavit**.
2. Chcete-li probíhající ruční prověřování ukončit, klikněte na tlačítko **Zrušit**. Jestliže chcete v prověřování pokračovat, klikněte na tlačítko **Pokračovat**.

Odložení nadcházejícího prověřování:

1. V zobrazeném okně klikněte na rozevírací nabídku a vyberte dobu odložení. Prověření můžete odložit pouze o 15 minut, ale také o celý den.
2. Kliknutím na tlačítko **OK** prověřování odložíte.

   Chcete-li prověřování spustit podle plánu, nemusíte provádět žádnou akci.

Nastavení plánovaných prověřování

Spuštění ručního prověřování

Reakce na zprávy o infekcích a zjištění rizik

Můžete zkontrolovat, zda je počítač infikovaný, a pokud vyžadujete lepší zabezpečení nebo výkon, můžete provést některé další úlohy.

Vašeho klienta může spravovat správce, nebo můžete spustit nespravovaného klienta. Úlohy ochrany, které můžete provést, závisí na právech, která správce klientovi udělí.

Pokud aplikace Symantec Endpoint Protection nalezne virus nebo bezpečnostní riziko, může se zobrazit výzva, abyste v souvislosti s rizikem provedli akci. Na základě nastavení vybraných správcem můžete být informováni o akci, kterou klient automaticky provedl.

Table 7: Reakce na zprávy o infekcích

Obsah zprávy	Požadovaná akce
Infikovaný soubor byl opraven.	Žádný
Požaduje schválení opravy infikovaného souboru.	Schvalte opravu. Tato možnost závisí na předvolbách funkce Auto-Protect. Správa nastavení ochrany před viry a spywarem Pokud není možnost automatické opravy infikovaných souborů zaškrtnutá, je nutné opravit soubor ručně. Oprava infikovaných souborů
Infikovaný soubor nelze opravit.	Proveďte správu infekce v karanténě. Správa souborů umístěných do karantény

Ochrana počítače Mac pomocí ochrany před viry a spywarem

Oprava infikovaných souborů

Pokud není infikovaný soubor automaticky opraven nebo přesunut do karantény, můžete jej opravit ze seznamu výsledků prověřování. Ručně můžete opravit soubory uložené na pevném disku počítače nebo na vyměnitelném médiu.

Oprava infikovaných souborů:

1. V seznamu výsledků prověřování vyberte soubor, který chcete opravit, a poté klikněte na možnost **Opravit**.

   Můžete také kliknout pravým tlačítkem na libovolný soubor v aplikaci **Finder** nebo nabídce **Hledat**.

2. Podle potřeby postup opakujte.
3. Spusťte další prověřování, abyste vyhledali případné další infikované soubory.
4. Zkontrolujte, zda opravené soubory fungují správně.

Správa nastavení ochrany před viry a spywarem

Správa souborů umístěných do karantény

Správa souborů umístěných do karantény

Pokud klient zjistí virus v souboru, ve výchozím nastavení se jej pokusí odstranit. Pokud virus nelze odstranit, soubor je umístěn do karantény v počítači. Pokud aplikace Symantec Endpoint Protection zjistí bezpečnostní riziko v souboru, nejprve umístí soubor do karantény. Poté opraví vedlejší účinky rizika.

Během aktualizace definic virů klient automaticky kontroluje karanténu. Položky v karanténě můžete znovu prověřit. Nejnovější definice mohou vyčistit nebo opravit soubory umístěné do karantény.

Správa souborů umístěných do karantény:

1. V klientovi aplikace Symantec Endpoint Protection klikněte na stránce **Pokročilé** na možnost **Aktivita > Historie zabezpečení > Karanténa**.
2. Vyberte soubor, který chcete spravovat, a poté vyberte příslušnou akci:

Opravit	Tuto možnost vyberte, pokud se chcete pokusit opravit soubor umístěný do karantény. Přesvědčte se, zda jsou definice virů aktuálnější, než je datum umístění souboru do karantény.
Odstranění	Tuto možnost vyberte, pokud chcete z karantény odstranit soubory, které již nepotřebujete.
Obnovit	Pokud si jste jisti, že soubor neobsahuje virus, můžete jej obnovit do původního umístění v počítači. Tato možnost neprovede prověření souboru ani se nepokusí jej opravit.

Reakce na zprávy o infekcích a zjištění rizik

Zapnutí nebo vypnutí odesílání informací o zabezpečení společnosti Symantec

Aplikace Symantec Endpoint Protection může odesílat pseudoanonymizované informace o zjištěných hrozbách společnosti Symantec. Společnost Symantec tyto informace využívá k ochraně klientských počítačů před novými, cílenými a měnícími se hrozbami. Veškerá data odeslaná společnosti Symantec umožňují lépe reagovat na hrozby a přizpůsobit ochranu ve vašem počítači.

Data shromažďovaná telemetrií společnosti Symantec mohou obsahovat anonymní prvky, které nejsou přímo identifikovatelné. Společnost Symantec nepotřebuje ani se nesnaží použít telemetrická data k identifikaci jakéhokoli jednotlivého uživatele.

Ve výchozím nastavení odesílá klientský počítač informace o zjištěných položkách společnosti Symantec. Odesílání můžete vypnout, i když společnost Symantec doporučuje ponechat toto nastavení zapnuté.

Tato možnost odešle pouze informace o zjišťování virů.

NOTE
Společnost Symantec doporučuje ponechat tuto možnost zapnutou.

Zapnutí nebo vypnutí odesílání anonymních informací o zabezpečení společnosti Symantec:

V klientovi aplikace Symantec Endpoint Protection na stránce **Pokročilé** klikněte na možnost **Product Settings** a poté zapněte nebo vypněte možnost **Security Info Submission**.

Nastavení plánovaných prověřování

Spuštění ručního prověřování

Správa prevence narušení

Výchozí nastavení prevence narušení chrání klienta systému Mac. Pokud však chcete spravovat vlastní ochranu, můžete spravovat prevenci narušení jako součást modulu Ochrany před síťovými hrozbami.

Table 8: Správa prevence narušení

Kroky	Popis
Krok 1: Zjistěte informace o prevenci narušení.	Zjistěte, jak funkce prevence narušení zjišťuje a blokuje síťové útoky. Ochrana počítače Mac pomocí ochrany před síťovými hrozbami
Krok 2: Stáhněte nejnovější signatury IPS.	Ve výchozím nastavení jsou nejnovější signatury stahovány do klientů. Nicméně někdy můžete chtít signatury stáhnout okamžitě. Okamžitá aktualizace obsahu aplikace Symantec Endpoint Protection
Krok 3: Povolte nebo zakažte prevenci narušení.	Prevenci narušení bude možná nutné zakázat při řešení potíží nebo v případě, že klientský počítač vykazuje příliš mnoho falešných poplachů. Prevenci narušení je běžně vhodné nechat spuštěnou. Zapnutí nebo vypnutí ochrany před síťovými hrozbami
Krok 4: Povolte upozornění prevence narušení.	Konfiguraci můžete upravit tak, aby aplikace Symantec Endpoint Protection zobrazila při odhalení útoku upozornění. Zapnutí a vypnutí oznámení ochrany před síťovými hrozbami

Správa ochrany pomocí brány firewall pro klienta systému Mac

Brána firewall aplikace Symantec Endpoint Protection pro systém Mac je plně integrována do aplikace Symantec Endpoint Protection, včetně událostí, zásad a příkazů. Brána firewall aplikace Symantec Endpoint Protection je k dispozici pouze u spravovaných klientů.

NOTE
Brána firewall aplikace Symantec Endpoint Protection pro systém Mac není integrována s vestavěnou bránou firewall operačního systému. Místo toho funguje souběžně. Brána firewall operačního systému provádí kontrolu na aplikační vrstvě, zatímco brána firewall aplikace Symantec Endpoint Protection provádí kontrolu na nižších úrovních (adresa IP a přenos). Brána firewall aplikace Symantec Endpoint Protection pro systém Mac nenabízí pravidla blokování peer-to-peer, i když je lze částečně vytvořit prostřednictvím vlastních pravidel brány firewall.

Table 9: Správa ochrany bránou firewall

Kroky	Popis
Krok 1: Přečtěte si informace o ochraně pomocí brány firewall.	Zjistěte, jak ochrana pomocí brány firewall sleduje provoz a chrání před běžnými způsoby útoku. Ochrana počítače Mac pomocí ochrany před síťovými hrozbami
Krok 2: Povolte nebo zakažte bránu firewall.	Možná bude potřeba zakázat bránu firewall kvůli řešení problémů, například pokud je blokován provoz, který by měl být povolený. Bránu firewall byste obvykle zakazovat neměli. Zapnutí nebo vypnutí ochrany před síťovými hrozbami

Zapnutí nebo vypnutí ochrany před síťovými hrozbami

Při vypnutí součástí ochrany před síťovými hrozbami v počítači je počítač obvykle méně zabezpečený. Můžete však vypnout prevenci narušení a zabránit zdánlivě pozitivním výsledkům, nebo můžete vypnout bránu firewall a vyřešit problémy s blokovaným provozem. Prevence narušení a brána firewall jsou součástí ochrany před síťovými hrozbami.

V případě spravovaných klientů závisí úroveň řízení těchto nastavení na způsobu, jakým správce nakonfiguroval klienta. Při dalším prezenčním signálu se navíc provedené změny nastavení mohou vrátit zpět na hodnoty určené zásadou.

U nespravovaných klientů není brána firewall k dispozici.

Zapnutí nebo vypnutí ochrany před síťovými hrozbami:

1. V klientovi aplikace Symantec Endpoint Protection na stránce **Pokročilé** klikněte na možnost **Ochrana před síťovými hrozbami**.
2. Pokud chcete povolit nebo zakázat prevenci narušení, zapněte nebo vypněte možnost **Prevence narušení**.
3. Pokud chcete povolit nebo zakázat bránu firewall, zapněte nebo vypněte možnost **Brána firewall**.
4. Pokud chcete povolit nebo zakázat oznámení týkající se prevence narušení a brány firewall, klikněte na ikonu nastavení **Vulnerability Protection** a v dialogovém okně zaškrtněte nebo zrušte zaškrtnutí políčka **Display Vulnerability Protection Notifications**.
5. Klikněte na tlačítko **Hotovo**.

Pokud tyto součásti vypnete, bude třeba je co nejdříve zapnout, aby byl počítač co nejlépe chráněn.

Správa prevence narušení

Správa ochrany pomocí brány firewall pro klienta systému Mac


Symantec
A Division of Broadcom