G DATA Business 14

Podręcznik użytkownika

ISBN 978-83-61624-23-3

G DATA Software Sp. z o.o.
ul. 28 Lutego 2, 78-400 Szczecinek
tel. 094 3729 650
faks 094 3729 659
e-mail: biuro@gdata.pl
Raiffeisen Bank Polska S.A.
78 1750 1396 0000 0000 2014 8837

Spis treści

1 Wstęp

Rozwój usług internetowych i samego Internetu pociąga za sobą także drastyczny wzrost zagrożeń. Tematyka ochrony antywirusowej zaczyna być popularna nie tylko w gronie fachowców. Problem ten dotyczy obecnie każdego użytkownika komputera.

Ataki wirusów są najdotkliwsze dla firm i instytucji działających w oparciu o wewnętrzne sieci komputerowe połączone z Internetem. Skutki mogą być rozmaite: utrata danych, zawieszanie systemów operacyjnych, czasem wręcz utrata kluczowych kanałów komunikacyjnych. Wirusy są w stanie wyrządzić szkody, których czasem nie da się naprawić. Oprogramowanie oferuje wysokiej klasy ochronę przed wirusami. W testach wykrywalności produkt od lat zajmuje czołowe miejsca.

Działanie programu nastawione jest konsekwentnie na centralną konfigurację i zarządzanie oraz szeroko pojętą automatyzację ochrony. Procesy przebiegają w tle, a użytkownicy nie mogą wyłączyć ochrony bez zgody administratora. Automatyczne aktualizacje internetowe umożliwiają opanowanie infekcji najnowszych wirusów. Zdalne sterowanie przy pomocy modułu G DATA ManagementServer umożliwia instalację, konfigurację, aktualizację oraz automatyzację ochrony sieci.

G DATA Software

1.1 Dokumentacja techniczna

Szczegółowe informacje dotyczące obsługi oprogramowania znajdziesz w pomocy programu dostępnej kontekstowo po wciśnięciu klawisza F1. Dokumentacja dostępna jest również w pliku PDF - do pobrania ze strony G DATA:

www.gdata.pl

1.2 Pomoc techniczna

Pomoc techniczna przysługuje wszystkim zarejestrowanym użytkownikom przez rok czasu od rejestracji programu lub wykupienia abonamentu. Zgłoszenia problemów z programem przyjmujemy telefonicznie, pocztą elektroniczną i faksem.

telefon: 94 3729 650

e-mail: b2b-support@gdata.pl

W rozwiązaniu wielu problemów pomoże konfrontacja z tekstami pomocy lub podręcznikiem, prosimy więc najpierw tam poszukać odpowiedzi na pytania. Wiele odpowiedzi można znaleźć na stronie pomocy technicznej: http://www.gdata.pl/pomoc.

Przed rozmową prosimy o przygotowanie danych na temat sieci i komputerów ze zwróceniem szczególnej uwagi na:

- Numery wersji modułów G DATA ManagementServer i G DATA Security Client,
- Numer klienta (symbol) lub numer rejestracyjny,
- Wersje systemów operacyjnych,
- Dodatkowo zainstalowane oprogramowanie i sprzęt.
- Teksty ew. komunikatów błędów w pełnym brzmieniu lub ich zrzuty ekranowe.

Przygotowanie powyższych informacji ułatwi i przyspieszy korespondencję lub rozmowę z serwisantem.

1.3 G DATA Security Labs

Program G DATA ManagementServer ma możliwość wysyłania wykrytych wirusów drogą poczty elektronicznej do G DATA Security Labs. Gwarantujemy pełną dyskrecję i przestrzeganie zasad przechowywania danych osobowych dotyczących przesyłanych plików.

Przed wysłaniem pliku niezbędne jest skonfigurowanie ustawień poczty elektronicznej. Szczegółowy opis znajdziesz w rozdziale Ustawienia e-mail.

1.4 Rozwiązania biznesowe G DATA

Rozwiązania G DATA przystosowane są do ochrony sieci dowolnych rozmiarów - od klientów indywidualnych, przez małe i średnie firmy po duże przedsiębiorstwa. Zastosowanie najnowocześniejszych technologii gwarantuje użytkownikom najwyższy poziom bezpieczeństwa połączony z wysoką wydajnością oraz optymalną wygodę użytkowania. Wybierz pakiet oprogramowania odpowiadający Twoim potrzebom.

2 Instalacja

Instalacja wszystkich modułów programu jest prosta nawet dla początkujących administratorów. W uruchomionym systemie Windows włóż do napędu nośnik z oprogramowaniem.

Uwaga: Przed zainstalowaniem programu należy zweryfikować sprzętowe i programowe zabezpieczenia sieci i komputerów. Szczególnie ważne jest uaktualnienie wszystkich systemów operacyjnych w sieci.

Przed zainstalowaniem składników zamknij wszystkie inne aplikacje systemu Windows.

Wybierz w oknie instalacji element, który chcesz zainstalować na tym komputerze:

- G DATA ManagementServer: Pierwszy krok to instalacja składnika ManagementServer. Ten składnik zdalnie steruje ochroną stacji roboczych i przekazuje im sygnatury wirusów pobierane przez Internet z serwera aktualizacji. Razem z nim instaluje się automatycznie składnik Administrator, interfejs graficzny obsługi składnika ManagementServer.
- G DATA AntiVirus Administrator: Jest to moduł sterujący modułem ManagementServer. Osoba znająca hasło dostępu może uruchomić program z każdej stacji roboczej.
- G DATA AntiVirus Client: Jest to oprogramowanie chroniące stacje robocze i wykonujące zadania składnika ManagementServer.
- Kreator płyt startowych: Aplikacja umożliwiająca tworzenie startowych płyt CD służących do wstępnego skanowania dysków komputera. Szczegóły w rozdziale Nośnik startowy.
- G DATA AntiVirus WebAdministrator: Aplikacja umożliwiająca sterowanie modułem ManagementServer przez przeglądarkę internetową.

- G DATA MobileAdministrator: Aplikacja umożliwiająca sterowanie modułem ManagementServer przez mobilne przeglądarki internetowe. Umożliwia wykonywanie jedynie podstawowych czynności obsługowych.
- G DATA MailSecurity: G DATA MailSecurity to oprogramowanie pełniące funkcję bramy poczty elektronicznej (SMTP proxy) i filtruje ruch SMTP/POP3 przechodzący przez serwer poczty. Program jest dostępny w odsłonach Enterprise produktów G DATA Software dla przedsiębiorstw.

2.1 Przed instalacją

- Przed zainstalowaniem programu należy zweryfikować sprzętowe i programowe zabezpieczenia sieci i komputerów. Szczególnie ważne jest uaktualnienie wszystkich systemów operacyjnych w sieci. Jeśli istnieje podejrzenie, że dany komputer jest zainfekowany, warto rozważyć przeprowadzenie skanowania wstępnego przy użyciu płyty startowej G DATA.
- Pierwszy krok to instalacja składnika ManagementServer. Komputer obsługujący serwer zarządzający G DATA musi spełniać wymagania programu G DATA ManagementServer. Ten składnik zdalnie steruje ochroną stacji roboczych i przekazuje im sygnatury wirusów pobierane przez Internet z serwera aktualizacji. Razem z nim instaluje się automatycznie składnik Administrator, interfejs graficzny obsługi składnika ManagementServer.
- Po zainstalowaniu serwera zarządzającego przeprowadź rejestrację online. Zarejestrowanie produktu online umożliwia pobieranie aktualizacji oprogramowania i sygnatur wirusów przez Internet.
- Pierwsze uruchomienie składnika Administrator na komputerze z zainstalowanym składnikiem ManagementServer odbywa się pod nadzorem asystenta konfiguracji. Asystent umożliwia zainstalowanie oprogramowania klienckiego na stacjach roboczych sieci, a także konfigurację podstawowych ustawień ochrony.

2.1.1 Wymagania programu

Poniżej lista wymagań poszczególnych wersji i modułów oprogramowania G DATA dla firm:

Wymagania minimalne

G DATA ManagementServer

- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2,

Windows Server 2008, Windows 2003 Server
- 1 GB RAM

G DATA Administrator/G DATA WebAdministrator/G DATA MailSecurity Administrator

- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bit), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003

G DATA MobileAdministrator

- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

G DATA Security Client

- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bit), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003
- 1 GB RAM

G DATA Security Client for Linux

- Wersje 32/64-bit Debian 6.0, 7, 8, OpenSUSE 11.4, 12.2, 12.3, 13.1, 13.2 Suse Linux Enterprise Server 10 SP4, 11 SP3 i 12, Red Hat Enterprise Linux 5.11, 6.6 i 7.0, Ubuntu 10.04.4 LTS, 12.04.5 LTS, 14.04.1 LTS, 14.10, 15.04, CentOS 5.11, 6.6 i 7.0, Fedora 19, 20, 21 i 22

G DATA Security Client for Mac

- Mac OS X 10.6 lub wyższy

G DATA Internet Security for Android

- Android 4.0 lub wyższy

G DATA MailSecurity

- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bit), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 2003 Server
- 1 GB RAM

G DATA MailSecurity for Exchange (64-bit Exchange plugin)

- Microsoft Exchange Server 2016, Microsoft Exchange Server 2013, Microsoft Exchange Server 2010, Microsoft Exchange Server 2007 SP1

Do komunikacji client/server oprogramowanie G DATA wykorzystuje protokół TCP/IP.

W przypadku stosowania serwera G DATA lub bramy MailSecurity z lokalną bazą SQL lub innymi zasobożernymi aplikacjami na tej samej maszynie, zaleca się dodatkowo:

- 4 GB RAM
- Wielordzeniowy procesor

2.1.2 Konfiguracja portów

Produkty G DATA wykorzystują różne porty TCP w celu zapewnienia bezpiecznej komunikacji w sieci. Zadbaj o udostępnienie ruchu na poniższych portach w zaporach programowych i sprzętowych:

Główny i zapasowy serwer zarządzający (MMS)

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)
- Port 7182 (TCP)
- Port 7183 (TCP)

Serwer podrzędny

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)

Klient

- Port 7169 (TCP)

MailSecurity

- Port 7182 (TCP)

MailSecurity Exchange plugin

- Port 7171 (TCP)
- Port 7185...7195 (TCP)

Modyfikacja ustawień portów

Porty komunikacyjne ustawione są w taki sposób, aby nie powodować konfliktów ze standardowymi aplikacjami sieciowymi. Jeśli zajdzie konieczność, można zmodyfikować ustawienia niektórych portów poprzez

edycję pliku konfiguracyjnego serwera zarządzającego G DATA. Przed edycją pliku zatrzymaj działanie usługi G DATA ManagementServer (**Start, Uruchom, services.msc**). Plik konfiguracyjny znajduje się w folderze serwera zarządzającego (domyślnie C:\Program Filesx86\G DATA\G DATA ManagementServer). Edycji pliku konfiguracyjnego **config.xml** można dokonać w dowolnym edytorze tekstu (np. notatnik systemu Windows). W razie konieczności zmień ustawienia portów zgodnie z poniższym opisem:

- AdminPort: Wpisz wybrany numer portu. Wartość domyślna to "0" (tzn. stosowany jest standardowy port - 7182).
- ClientHttpsPort: Wpisz wybrany numer portu. Wartość domyślna to "0" (tzn. stosowany jest standardowy port - 443). Nie zaleca się modyfikowania wartości ClientHttpsPort, ponieważ mobilny klient nie będzie akceptować połączeń z innych portów.
- ClientHttpPort: Wpisz wybrany numer portu. Wartość domyślna to "0" (tzn. stosowany jest standardowy port - 80).

Jeśli zmodyfikujesz ustawienia ClientHttpPort lub ClientHttpsPort, musisz ponownie zainicjować konfigurację zabezpieczeń HTTP. Otwórz wiersz poleceń z prawami administratora i uruchom polecenie C:\Program Files\G DATA\G DATA ManagementServer\gdmmsconfig.exe /installcert.

Po dokonaniu edycji portów uruchom ponownie usługę G DATA ManagementServer.

Uwaga: Jeśli zmienisz parametr AdminPort, musisz wskazać nowo ustawiony port podczas logowania do G DATA Administrator. Wskazanie realizuje składnia: *nazwa serwera:port*.

2.1.3 Konfiguracja URL

Jeśli wykorzystujesz sladnik G DATA PatchManager, serwer G DATA pobiera pliki konfiguracyjne oraz poprawki z zewnętrznych źródeł. Zadbaj o udostępnienie poniższych adresów do ruchu w zaporach programowych i sprzętowych:

- gdata.cdn.heatsoftware.com

W zależności od oprogramowania, dla którego pobierane będą poprawki, należy również umożliwić ruch z następujących adresów URL:

- 7-Zip: http://downloads.sourceforge.net
- Adobe: ardownload.adobe.com, armdl.adobe.com, download.adobe.com, swupdl.adobe.com, www.adobe.com
- Microsoft: go.microsoft.com, download.windowsupdate.com, www.download.windowsupdate.com, download.skype.com, download.microsoft.com

- Mozilla: http://ftp.mozilla.org
- UltraVNC: http://support1.uvnc.com
- VideoLAN: http://download.videolan.org

2.1.4 Nośnik startowy

Dzięki nośnikowi startowemu można przeprowadzić skanowanie lokalnych napędów, wykazujące ewentualną obecność wirusa na dysku lub w pamięci. Skanowanie odbywa się bez udziału systemu Windows.

W tym celu należy uruchomić komputer z nośnika instalacyjnego lub z nośnika sporządzonego przez moduł Kreator Nosników startowych.

- Włóż płytę lub pendrive do odpowiedniego napędu.
- Wyłącz komputer na około 5 sekund. Istnieją wirusy, które są w stanie przetrwać tzw. miękki reset komputera (CTRL+ALT+DEL).
- Uruchom komputer. Komputer sam odnajdzie na płycie startowej moduł skanujący oparty na systemie Linux.

Wskazówka: Skanowanie wstępne odbywa się przy pomocy specjalnego modułu antywirusowego opartego na systemie operacyjnym Linux.

- Usuń wszystkie znalezione wirusy używając opcji oferowanych przez program.
- Po zakończeniu skanowania uruchom komputer ponownie z dysku twardego wybierając przycisk Zakończ.

2.1.4.1 Kreator nośników startowych

Możesz sporządzić nośnik startowy z aktualnymi bazami wirusów przy pomocy modułu Kreator nośników startowych. Moduł należy zainstalować z obrazu płyty instalacyjnej lub z pobranego pliku instalatora. Program nagra na płytę lub pendrive obraz nośnika zawierający bazy wirusów jakimi w danej chwili dysponuje składnik kliencki zainstalowany w systemie operacyjnym. Obraz może również zostać zapisany na dysku w postaci pliku w celu późniejszego wykorzystania.

Do przeprowadzenia skanowania wstępnego nie jest potrzebny zainstalowany program. Po uruchomieniu komputera z nośnika startowego uruchomi się osobny system operacyjny, w którym zostanie przeprowadzone skanowanie lokalnych dysków.

Do utworzenia nośnika startowego potrzebny jest czysty pendrive lub płyta CD/DVD.

2.1.4.2 Ustawienia BIOS

Upewnij się, że komputer automatycznie startuje z płyty CD/DVD-ROM. Jeśli nie, zmień kolejność uruchamiania urządzeń w menu BIOS. Jako pierwsze urządzenie bootujące (1st Boot Device) należy ustawić napęd CD/DVD-ROM, dysk twardy z systemem operacyjnym jako drugie (2nd Boot Device). Jeżeli płyta startowa znajduje się w napędzie, uruchomiona zostanie wersja programu oparta o system Linux. Jeżeli płyty nie ma w napędzie, komputer uruchomi automatycznie system Windows z dysku twardego.

Wskazówka: Niektóre płyty główne umożliwiają zmianę kolejności uruchamiania urządzeń po wciśnięciu klawisza F11, F8 lub F2. W przypadku wątpliwości dotyczących sposobu zmiany kolejności uruchamiania, zapoznaj się z dokumentacją dołączoną do płyty głównej. Po przeprowadzeniu skanowania wstępnego i zainstalowaniu programu, zaleca się przywrócenie pierwotnej kolejności uruchamiania.

2.1.5 Instalacja składnika ManagementServer

Włóż do napędu płytę z zakupionym oprogramowaniem lub uruchom plik instalacyjny pobrany z Internetu. W celu rozpoczęcia instalacji kliknij przycisk Instaluj w menu automatycznego startu. Wybierz do instalacji składnik G DATA ManagementServer.

Przed rozpoczęciem instalacji zamknij wszystkie inne aplikacje. Przeczytaj i zatwierdź akceptację warunków licencji i przystąp do instalacji.

2.1.5.1 Rodzaj serwera

Do wyboru masz trzy rodzaje instalacji składnika ManagementServer:

- Serwer główny: W przypadku pierwszej instalacji tego składnika należy zainstalować go jako serwer główny. Będzie to centralna instancja konfiguracyjna i zarządzająca sieciowej architektury ochrony antywirusowej. Wszystkie pozostałe serwery, zarówno zapasowe, jak i podrzędne korzystają z bazy danych serwera głównego.
- Serwer zapasowy: W przypadku zastosowania bazy danych typu SQL, program umożliwia zainstalowanie drugiej, awaryjnej instancji serwera. W razie awarii serwera głównego lub segmentu sieci zawierającego serwer główny, stacje robocze łączą się automatycznie i synchronizują z serwerem

zapasowym. W momencie przywrócenia działania serwera głównego, stacje znów się z nim łączą. Serwer zapasowy tworzą osobne repozytorium baz wirusów.

- Serwer podrzędny: W przypadku dużych sieci, warto rozważyć zainstalowanie serwerów podrzędnych w mniejszych segmentach lub podsieciach. Spowoduje to rozłożenie obciążenia sieci powodowanego przez użytkowanie oprogramowania. Do danego serwera podrzędnego można przyporządkować konkretne stacje robocze w celu odciążenia serwera głównego. Serwery podrzędne pozostają w pełni funkcjonalne nawet w momencie, kiedy serwer główny i serwer zapasowy nie są dostępne.

Dzięki wprowadzeniu hierarchizacji serwerów, można dostosować architekturę ochrony do logicznej topografii sieci. Serwery podrzędne mogą grupować stacje robocze w podsieciach i synchronizować ustawienia i aktualizacje z serwerem głównym. W razie awarii lub potrzeby konserwacji serwera głównego, jego funkcję przejmuje automatycznie serwer zapasowy.

2.1.5.2 Rodzaj bazy danych

Wybierz rodzaj bazy danych, w której chcesz przechowywać ustawienia składnika ManagementServer. Możesz podłączyć się do istniejącej w sieci instancji serwera SQL lub pozwolić automatycznie zainstalować i skonfigurować program Microsoft SQL Server 2014 Express (np. dla sieci poniżej 1000 stacji roboczych). Ta wersja serwera SQL nie obsługuje systemów Windows XP, Vista, 2003 Server oraz Server 2008. Jeśli chcesz zastosować starszy system operacyjny jako serwer bazy danych aplikacji G DATA, zainstaluj w nim wcześniej ręcznie Microsofty SQL Server 2008 R2 Express. Więcej informacji znajdziesz w dokumencie Reference Guide.

Do zainstalowania serwera zarządzającego nie jest wymagany typowo serwerowy system operacyjny. Dla sieci powyżej 1000 stacji roboczych zaleca się stosowanie pełnych wersji serwerów Microsoft SQL.

2.1.5.3 Aktywacja produktu

Podczas instalacji program zapyta o metodę aktywacji produktu. Program będzie aktualizował się przez Internet po dokonaniu aktywacji.

- Chcę wprowadzić nowy numer rejestracyjny: Jeśli chcesz zarejestrować zakupiony numer rejestracyjny produktu G DATA, wybierz tę opcję. Wypełnij formularz i kliknij przycisk Rejestracja.

Po zarejestrowaniu dane dostępu do aktualizacji zostaną automatycznie wprowadzone do programu, a także wysłane na wskazany w formularzu adres e-mail.

W przypadku problemów z rejestracją, sprawdź, czy wpisujesz numer rejestracyjny poprawnie. Łatwo pomylić duże "I" (jak Irena) z cyfrą"1" lub małym "l" (jak lebioda). Podobnie: "B" i "8", "G" i 6, "O" i "0" czy "Z" i "2".

- Chcę wprowadzić dane dostępu: Jeśli Twój numer został wcześniej zarejestrowany, możesz od razu wprowadzić dane dostępu (użytkownik i hasło).

Dane dostępu znajdziesz w wiadomości e-mail potwierdzającej rejestrację.

Jeśli nie masz danych w zasięgu ręki, lub nie masz dostępu do wiadomości z potwierdzeniem rejestracji, kliknij przycisk Nie pamiętasz danych dostępu? Zostaniesz przeniesiony na stronę internetową umożliwiającą ponowne wysłanie danych dostępu po wpisaniu adresu e-mail wskazanego w procesie rejestracji. W razie problemów z odzyskaniem danych skontaktuj się z Pomocą techniczną.

- Wersja testowa: Jeśli chcesz wypróbować oprogramowanie G DATA, zarejestruj się bezpłatnie wypełniając formularz wersji trial nie wymagający wpisania numeru rejestracyjnego. Wpisz prawidłowy adres e-mail. Na ten adres zostaną wysłane dane do aktualizacji produktu.

- Uaktywnię później: Jeśli nie chcesz uaktywniać oprogramowania, lub chcesz to zrobić później, wybierz tę opcję. Produkt będzie w pełni funkcjonalny, ale nie będzie pobierał aktualizacji z Internetu. Opis ręcznej aktywacji znajdziesz w rozdziale Jak później uaktywnić program?

Oprogramowanie G DATA skutecznie chroni Twoją sieć dopiero po dokonaniu aktywacji i przeprowadzeniu uaktualnienia. Korzystanie z oprogramowania bez aktualizacji nie gwarantuje skutecznej ochrony.

2.1.5.4 Jak później uaktywnić program?

Jeśli chcesz ręcznie uaktywnić zainstalowany program, uruchom aplikację Start > (Wszystkie) programy > G DATA > G DATA ManagementServer > Internet Update i kliknij przycisk Rejestracja online...

Wypełnij formularz i kliknij przycisk Rejestracja. Po zarejestrowaniu dane dostępu do aktualizacji zostaną automatycznie wprowadzone do programu, a także wysłane na wskazany w formularzu adres e-mail.

Dopóki nie dokonasz aktywacji produktu G DATA ClientSecurity lub G DATA EndpointProtection, program będzie funkcjonował w wersji G DATA AntiVirus Business, bez funkcji oferowanych przez wyższe pakiety biznesowe.

2.1.5.5 Zakończenie instalacji

Po zainstalowaniu usługa systemowa G DATA ManagementServer będzie uruchamiać się automatycznie przy każdym uruchomieniu komputera. Aby dokonać zmian w ustawieniach programu G DATA ManagementServer, uruchom składnik Administrator poleceniem menu Start > (Wszystkie) Programy > G DATA > G DATA Administrator > G DATA Administrator.

2.2 Instalacja składnika Administrator

Administrator instaluje się automatycznie podczas instalacji składnika ManagementServer. Nie jest wymagana dodatkowa ręczna instalacja Administratora. Aby zainstalować ręcznie moduł administrujący na końcówce sieci, włóż do napędu końcówki płytę z programem i uruchom instalację składnika Administrator.

Przed rozpoczęciem instalacji zamknij wszystkie aplikacje Windows.

Składnik Administrator uruchamia się poleceniem menu Start > (Wszystkie) Programy > G DATA > G DATA Administrator.

2.3 Instalacja składnika WebAdministrator

Aby zainstalować moduł administrujący na końcówce sieci, włóż do napędu końcówki płytę z programem i uruchom instalację składnika WebAdministrator.

Po zatwierdzeniu warunków umowy licencyjnej masz możliwość wybrania folderu instalacji. Zaleca się stosowanie domyślnego folderu (\inetpub\wwwroot).

Zainstalowanie składnika WebAdministrator wymaga obecności/aktywowania następujących komponentów programowych:

- **Microsoft Internet Information Services (IIS):** Ponieważ WebAdministrator to produkt bazujący na serwerze WWW, komputer musi być wyposażony w składnik Microsoft Internet Information Services (IIS).
- **Zgodność metabazy usług IIS z konfiguracją usług IIS w wersji 6:** Przed zainstalowaniem programu G DATA WebAdministrator niezbędne jest włączenie tej funkcji. Jeśli nie będzie aktywna, instalator automatycznie przerwie działanie. Można ją włączyć w oknie Włącz lub wyłącz funkcje systemu Windows w aplecie Programy i funkcje Panelu sterowania. Aby dotrzeć do tej funkcji rozwiń w drzewie ustawień **Internetowe usługi informacyjne > Narzędzia zarządzania siecią Web > Zgodność z narzędziami zarządzania usługami IIS w wersji 6**. Poza tym wymagane

jest włączenie (jeśli nie jest włączona) funkcji o nazwie **Usługi WWW**. Jest to również jedna z gałęzi drzewa Internetowe usługi informacyjne. W systemach serwerowych można sterować tymi opcjami w sekcji **Role serwera** w oknie zarządzania serwerem.

- **Microsoft .NET Framework:** Program WebAdministrator działa w oparciu o platformę .NET Framework firmy Microsoft. Jeśli tego składnika nie będzie w systemie, instalator WebAdministratora wymusi instalację. Po zainstalowaniu platformy .NET niezbędne będzie ponowne uruchomienie komputera przed kontynuowaniem instalacji programu WebAdministrator.
- **Microsoft Silverlight:** Program G DATA WebAdministrator wymaga do uruchomienia obecności oprogramowania Microsoft Silverlight. Jeśli nie jest zainstalowane, program WebAdministrator wyświetli stosowny komunikat przy próbie uruchomienia.

Po zainstalowaniu program G DATA WebAdministrator jest gotowy do użycia. Okno informujące o zakończeniu instalacji wyświetla również link, który można zastosować do uruchomienia programu z innych komputerów. Lokalnie, można korzystać również ze skrótu umieszczonego przez instalator na pulpicie.

Stosowanie składnika WebAdministrator przez Internet bez szyfrowanego połączenia nie jest całkowicie bezpieczne. Zaleca się zastosowanie certyfikatu SSL w serwerze IIS w celu podniesienia bezpieczeństwa połączeń.

2.4 Instalacja składnika MobileAdministrator

Aby zainstalować moduł administrujący na końcówce sieci, włóż do napędu końcówki płytę z programem i uruchom instalację składnika G DATA MobileAdministrator.

Instalacja składnika G DATA MobileAdministrator jest porównywalna z instalacją składnika WebAdministrator. Po zatwierdzeniu warunków umowy licencyjnej masz możliwość wybrania folderu instalacji. Zaleca się stosowanie domyślnego folderu (\inetpub\wwwroot).

Zainstalowanie składnika WebAdministrator wymaga obecności/aktywowania następujących komponentów programowych::

- **Microsoft Internet Information Services (IIS):** Ponieważ WebAdministrator to produkt bazujący na serwerze WWW, komputer musi być wyposażony w składnik Microsoft Internet Information Services (IIS).
- **Microsoft .NET Framework:** Program WebAdministrator działa w oparciu o platformę .NET Framework firmy Microsoft. Jeśli tego składnika nie będzie w systemie, instalator WebAdministratora wymusi instalację. Po zainstalowaniu platformy .NET niezbędne będzie ponowne uruchomienie komputera przed kontynuowaniem instalacji programu WebAdministrator.

Po zainstalowaniu program jest gotowy do użycia. Okno informujące o zakończeniu instalacji wyświetla również link, który można zastosować do uruchomienia programu z innych komputerów. Lokalnie, można korzystać również ze skrótu umieszczonego przez instalator na pulpicie.

Stosowanie składnika WebAdministrator przez Internet bez szyfrowanego połączenia nie jest całkowicie bezpieczne. Zaleca się zastosowanie certyfikatu SSL w serwerze IIS w celu podniesienia bezpieczeństwa połączeń.

2.5 Instalacja G DATA Security Client (Windows)

Jeśli nie jest to pożądane lub możliwe, można zainstalować oprogramowanie klienckie ręcznie, bezpośrednio na stacjach roboczych. Aby zainstalować klienta ręcznie, włóż do napędu komputera płytę z zakupionym oprogramowaniem i uruchom instalację składnika Klient. Administrator umożliwia także utworzenie pakietu cichej instalacji do rozdzielenia np. przy pomocy skryptów logowania.

W trakcie instalacji ręcznej program zapyta o nazwę lub adres IP komputera, na którym zainstalowany jest składnik ManagementServer. Wskazanie komputera z serwerem zarządzającym jest niezbędne do uzyskania komunikacji między składnikami Security Client i ManagementServer.

W przypadku instalacji klienta G DATA w systemie serwerowym, może zaistnieć potrzeba dostosowania ustawień programu w celu uniknięcia konfliktów. Przykładem mogą być serwery baz danych, serwery pocztowe lub bramy HTTP. Szczegóły znajdziesz w dokumencie Reference Guide.

2.5.1 Instalacja zdalna

Najwygodniejszą formą dystrybucji klienta na stacje robocze i serwery jest zdalna instalacja z okna programu G DATA Administrator.

Oprócz skonfigurowania wymaganych portów komunikacyjnych w zaporach sieciowych, do instalacji zdalnej wymagane jest wykonanie następujących kroków umożliwiających wykonanie instalacji:

- Wyjątek dla pliku gdmms.exe w zaporze komputera z serwerem G DATA.
- W przypadku instalacji w grupie roboczej, w systemach Windows XP trzeba wyłączyć proste udostępnianie plików (wymagany również wyjątek dla udostępniania plików i drukarek w zaporze), a w systemach Windows Vista oraz Windows 7 wymagane jest włączenie funkcji Odnajdywanie sieci i Udostępnianie plików i drukarek.

- W przypadku instalacji w grupie roboczej wymagana jest zgodność haseł konta stosowanego do instalacji na serwerze zarządzającym G DATA oraz stacji roboczej - najlepiej zastosować wbudowane konto Administrator. Konto Administrator można włączyć w opcjach zarządzania komputerem (w systemach Vista i 7 konto jest wyłączone).
- Systemy Windows Vista lub nowsze mogą wymagać również drobnej interwencji w rejestrze Windows. Otwórz edytor rejestru i przejdź do klucza **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**. Utwórz zmienną DWORD o nazwie **LocalAccountTokenFilterPolicy**. Następnie przypisz zmiennej wartość **1**.

Spełnienie tych warunków zapewnia dostęp do udziałów administracyjnych C$ oraz Admin$, do rejestru stacji, a także do zapisu w bazie danych serwera zarządzającego G DATA.

Po automatycznym wyświetleniu stacji roboczych w drzewie (lista pobierana jest z serwera DNS) można uaktywnić stacje i zainstalować oprogramowanie klienta zdalnie. W razie potrzeby można wyszukać stacje po adresach IP korzystając z polecenia Wyszukaj stacje robocze w menu Organizacja. Aby zainstalować oprogramowanie Security Client zdalnie, przejdź do zakładki Stacje robocze w prawej części okna, zaznacz wybrane stacje i kliknij zaznaczenie prawym klawiszem myszy. Instalację inicjuje polecenie Instaluj składnik G DATA Security Client. Instalacja będzie wymagała uwierzytelnienia poświadczeniami Windows. Po uwierzytelnieniu program zapyta, czy wraz z klientem zainstalować również oprogramowanie G DATA Firewall. Ta opcja jest dostępna w wersjach programu G DATA Client Security, G DATA EndpointProtection, oraz G DATA SmallBusiness Security. Po zainstalowaniu klienta wymagane będzie ponowne uruchomienie stacji, aby wszystkie składniki ochrony zaczęły funkcjonować.

Możesz również skorzystać z możliwości zintegrowania programu z usługą Active Directory, jeśli stacje robocze są członkami domeny Windows.

Jeśli instalacja zdalna nie jest możliwa, istnieje również opcja zainstalowania klienta na stacji metodą ręczną - z płyty, z pliku pobranego przez Internet, lub też przy wykorzystaniu pakietu instalacyjnego.

2.5.2 Instalacja lokalna

Jeśli instalacja zdalna nie jest możliwa, istnieje również opcja zainstalowania klienta na stacji metodą ręczną - z płyty, z pliku pobranego przez internet, lub też przy wykorzystaniu pakietu cichej instalacji.

2.5.2.1 Nośnik/plik instalacyjny

Włóż płytę z programem G DATA do napędu i uruchom instalację składnika G DATA Security Client. Alternatywnie możesz uruchomić na stacji plik instalacyjny klienta pobrany przez internet.

W trakcie instalacji niezbędne jest wskazanie nazwy lub adresu IP komputera z zainstalowanym programem G DATA ManagementServer. Dzięki temu zapewniona zostanie komunikacja sieciowa między stacją, a serwerem zarządzającym G DATA.

2.5.2.2 Instalacja z pakietu instalacyjnego

Pakiet cichej instalacji klienta to pojedynczy plik wykonywalny (GDClientPck.exe), który umożliwia zainstalowanie oprogramowania G DATA Security Client bez interakcji z użytkownikiem. Można wykorzystać pakiet do dystrybucji poprzez skrypt startowy w domenie Windows.

Aby utworzyć aktualny pakiet cichej instalacji, uruchom polecenie Utwórz pakiet cichej instalacji G DATA Security Client z menu Organizacja programu G DATA Administrator. Przed utworzeniem pakietu można zdefiniować wstępne ustawienia pakietu:

- ManagementServer: Serwer zarządzający, do którego ma się podłączyć instalowany klient.
- Język: Język instalacji klienta.
- Grupa: Grupa, do której ma zostać dodany klient po zakończeniu instalacji.

Zastosuj znak "/", aby oddzielić nazwy grup i podgrup w celu odwzorowania hierarchii (grupa"/"podgrupa). Wszystkie znaki specjalne muszą być oznaczone, aby składnia została prawidłowo zinterpretowana: Każdy cudzysłów należy podwoić, a jeżeli nazwa grupy zawiera znak "/", sama nazwa grupy również musi być w cudzysłowie.

- Ogranicz ważność: Utworzony pakiet instalacyjny będzie miał termin ważności. Ważność pakietu dotyczy tylko mechanizmu autoryzacji klienta w serwerze zarządzającym. Jeśli pakiet zostanie zainstalowany na stacji/serwerze po terminie ważności, będzie wymagał ręcznego zatwierdzenia klienta do autoryzacji przez administratora w aplikacji G DATA Administrator > Stacje robocze > Ustawienia.

Kliknij OK i wskaż miejsce zapisu pakietu. G DATA Administrator utworzy w tle. Pakiet trzeba następnie skopiować na stację docelową i uruchomić z uprawnieniami administratora. Składnik G DATA Security Client zostanie zainstalowany po zatwierdzeniu stosownych komunikatów. Jeśli instalacja ma przebiegać w trybie nienadzorowanym (np. przy użyciu skryptów startowych), pakiet należy uruchomić z parametrem /§_QuietInstallation="true":

GDClientPck.exe /§_QuietInstallation="true".

2.6 Instalacja G DATA Security Client (Linux)

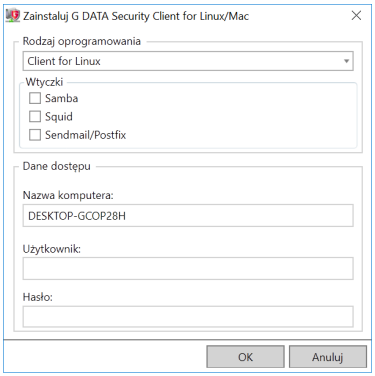
Produkt umożliwia zainstalowanie ochrony antywirusowej G DATA na stacjach roboczych z różnymi dystrybucjami systemu Linux. Podobnie jak klient dla systemu Windows, linuksowe oprogramowanie klienckie może być zarządzane i aktualizowane zdalnie przez składnik G DATA ManagementServer.

Klient dla systemów Linux może również zostać zainstalowany z opcją wtyczki dla serwera **Samba**, serwerów poczty **Sendmail/Postfix** oraz serwera **Squid**.

2.6.1 Instalacja zdalna

Najwygodniejszą formą dystrybucji klienta na stacje robocze i serwery linux jest zdalna instalacja z okna programu G DATA Administrator. Wymagania instalacji zdalnej w systemiach Linux:

- W systemie Linux musi być zainstalowany i włączony serwer SSH.
- Użytkownik instalujący oprogramowanie musi mieć możliwość logowania do serwera SSH za pomocą hasła.
- Nazwy serwera zarządzającego i klienta muszą być rozwiązywane przez DNS.



1. W widoku Stacje robocze zaznacz komputer z systemem Linux i uruchom polecenie Instaluj G DATA Security Client for Linux/Mac....

2. Jako rodzaj oprogramowania wybierz pozycję **Client for Linux**.
3. Wybierz wtyczki jakie chcesz zainstalować wraz z klientem (Samba, Squid, Sendmail/Postfix) w zależności od potrzeb.
4. Wpisz nazwę użytkownika i hasło. Zdalna instalacja wymaga zastosowania hasła konta root.
5. Kliknij przycisk OK. Przebieg instalacji możesz śledzić w oknie Przegląd instalacji.

2.6.2 Instalacja lokalna

Jeśli instalacja zdalna nie jest możliwa, składnik G DATA Security Client for Linux można zainstalować również lokalnie.

1. Utwórz skrypt instalacyjny dla systemu Linux/Mac odpowiednim poleceniem w oknie G DATA Administrator > menu **Organizacja** wskazując pożądaną lokalizację do jego zapisania.
2. Skopiuj utworzony skrypt instalacyjny do dowolnego folderu w systemie docelowym i nadaj uprawnienia do uruchamiania (np. poleceniem terminala: **chmod +x install-client.sh**).
3. Skorzystaj z okna terminala aby uaktywnić uprawnienia konta root, wpisując polecenie **su** i potwierdzając hasłem konta root. Ten sam efekt uzyskasz przy wykorzystaniu polecenia **sudo** w punkcie czwartym.
4. Przejdź do folderu zawierającego skopiowany wcześniej skrypt i uruchom go poleceniem: ./install-client.sh -t <produkt>

   Parametr produkt określa moduły programu do zainstalowania:

   ALL: G DATA Security Client for Linux i wszystkie dodatkowe moduły

   WS: G DATA Security Client for Linux

   SMB: moduł dla serwera **Samba**

   AMAVIS: moduł dla serwerów **Sendmail/Postfix**

   WEB: moduł dla serwera **Squid**
5. Po zainstalowaniu klient będzie wymagał ręcznego zatwierdzenia do autoryzacji przez administratora w aplikacji G DATA Administrator > Stacje robocze > Ustawienia.

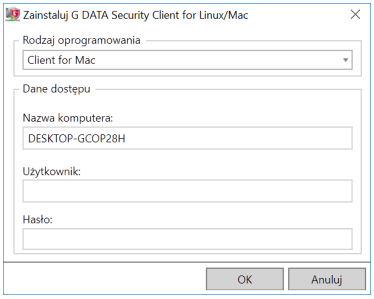
2.7 Instalacja G DATA Security Client (Mac)

G DATA Security Client for Mac umożliwia zainstalowanie ochrony antywirusowej G DATA w komputerach Mac. Podobnie jak klient dla systemu Windows i Linux oprogramowanie klienckie może być zarządzane i aktualizowane zdalnie przez składnik G DATA ManagementServer.

2.7.1 Instalacja zdalna

Najwygodniejszą formą dystrybucji klienta jest zdalna instalacja z okna programu G DATA Administrator. Wymagania instalacji zdalnej w systemiach Mac są identyczne jak wymagania dla systemów Linux.

1. W widoku Stacje robocze zaznacz komputer z systemem Linux i uruchom polecenie Instaluj G DATA Security Client for Linux/Mac....
2. Jako rodzaj oprogramowania wybierz pozycję **Client for Mac**.
3. Wpisz nazwę użytkownika i hasło. Zdalna instalacja wymaga zastosowania hasła konta root.
4. Kliknij przycisk OK. Przebieg instalacji możesz śledzić w oknie Przegląd instalacji.



2.7.2 Instalacja lokalna

Jeśli instalacja zdalna nie jest możliwa, składnik G DATA Security Client for Mac można zainstalować również lokalnie.

1. Utwórz skrypt instalacyjny dla systemu Linux/Mac odpowiednim poleceniem w oknie G DATA Administrator > menu **Organizacja** wskazując pożądaną lokalizację do jego zapisania.

2. Skopiuj utworzony skrypt instalacyjny do dowolnego folderu w systemie docelowym.
3. Skorzystaj z okna terminala aby uaktywnić uprawnienia konta root, wpisując polecenie **su** i potwierdzając hasłem konta root. Ten sam efekt uzyskasz przy wykorzystaniu polecenia **sudo** w punkcie czwartym.
4. Przejdź do folderu zawierającego skopiowany wcześniej skrypt i uruchom go poleceniem: ./install-client.sh -t WS
5. Po zainstalowaniu klient będzie wymagał ręcznego zatwierdzenia do autoryzacji przez administratora w aplikacji G DATA Administrator > Stacje robocze > Ustawienia.

2.8 Instalacja składnika MailSecurity

Jeśli korzystasz z serwera Microsoft Exchange Server 2007 SP1/2010/2013 lub 2016 z architekturą 64-bit, możesz zastosować wtyczkę G DATA dla serwerów Exchange instalując ją bezpośrednio na serwerze Exchange. Wtyczka jest obsługiwana przez składnik G DATA ManagementServer i można ją obsługiwać za pomocą aplikacji G DATA Administrator.

Wtyczka jest jednocześnie narzędziem antywirusowym i filtrem spamu.

Oprogramowanie MailSecurity w postaci antywirusowej i antyspamowej bramy SMTP proxy może obsługiwać dowolny serwer poczty. Instalacja wtyczki możliwa jest tylko w systemach Windows. Obsługę serwerów poczty działających w innych systemach operacyjnych uzyskujemy poprzez przekierowanie strumienia poczty na bramę stosując odpowiednie numery portów.

2.8.1 MailSecurity for Exchange

Przed zainstalowaniem programu zamknij wszystkie aplikacje Windows. Instalacja programu podczas pracy innych aplikacji może powodować problemy. Upewnij się także czy dysponujesz odpowiednią ilością wolnego miejsca na dysku twardym. Jeśli zabraknie miejsca program wyświetli podczas instalacji stosowny komunikat.

Instalacja programu jest zupełnie prosta. Po uruchomieniu Windows włóż płytę z programem do napędu. Instalator uruchomi się automatycznie i zaoferuje następujące opcje:

- **Instaluj**: Rozpoczęcie instalacji programu na komputerze.

- **Przeglądaj**: Uruchomienie Eksploratora Windows co umożliwia przeglądanie zawartości płyty CD-ROM z programem.
- **Anuluj**: Zamknięcie okna autostartu.

Wybierz przycisk **Instaluj**. W oknie wyboru składnika wybierz z sekcji Instalacja w postaci wtyczki do MS Exchange pozycję G DATA MailSecurity (Exchange).

Ponieważ aplikacja wymaga obecności serwera zarządzającego G DATA Business, program oferuje możliwość zdalnego podłączenia się do istniejącej instancji serwera zarządzającego G DATA poprzez wskazanie komputera z serwerem zarządzającym. Można także zainstalować lokalnie wersję serwera zarządzającego tylko wtyczką dla serwera Exchange.

Jeśli na komputerze jest już zainstalowany serwer zarządzający G DATA Business, instalator go wykryje i automatycznie się do niego podłączy.

Po zainstalowaniu wtyczka jest gotowa do pracy. Obsługa wtyczki odbywa się z program G DATA Administrator.

2.8.2 Brama MailSecurity

Przed instalacją programu G DATA MailSecurity należy zastanowić się gdzie go umiejscowić w sieci. Moduł sterujący programem - Administrator można zainstalować na dowolnym komputerze podłączonym do sieci. Sam program wymaga zainstalowania w odpowiednim miejscu topologii sieci.

Generalnie zaleca się instalację programu bezpośrednio za zaporą sprzętową (o ile jest stosowana), lub na komputerze funkcjonującym jako brama pocztowa w przedsiębiorstwie. W przypadku stosowania Windowsowego serwera poczty Exchange, aplikację można zainstalować bezpośrednio na komputerze z serwerem poczty. W przypadku serwera działającego w innym systemie operacyjnym, potrzebna będzie dodatkowa maszyna z systemem Windows.

Pamiętaj o dostosowaniu konfiguracji firewalla (adres IP i/lub port) tak, aby umożliwić kontrolę przepływu strumienia danych przez program.

Instalacja programu na serwerze poczty Windows

Jeśli Twój serwer SMTP zezwala na zmianę numerów portów, możesz zainstalować G DATA MailSecurity na tym samym komputerze co serwer SMTP. W takim przypadku nadaj nowy numer portu dla serwera pocztowego (np. 7100 lub wyższy). MailSecurity stosuje do edycji poczty przychodzącej port o numerze 25.

Jeśli zainstalujesz MailSecurity na komputerze z programem Microsoft Exchange, program przestawi port wiadomości wychodzących.

W tym celu należy zmodyfikować wpis SMTP w pliku \winnt\system32 \drivers\etc\services, i ponownie uruchomić usługę Internet Mail Service programu Microsoft Exchange.

Instalacja programu na osobnym komputerze

W tym przypadku poczta przychodząca muszą być odbierane najpierw przez G DATA MailSecurity, a nie bezpośrednio przez serwer poczty.

Można to zrobić na klika różnych sposobów:

a) dopasować rekord MX w DNS danej domeny

b) zdefiniować obejście w firewallu (jeśli jest stosowany)

c) zmienić adres IP serwera poczty, a oryginalny adres serwera poczty przyporządkować komputerowi z programem MailSecurity

Proces instalacji

Przed zainstalowaniem programu zamknij wszystkie aplikacje Windows. Instalacja programu podczas pracy innych aplikacji może powodować problemy. Upewnij się także czy dysponujesz odpowiednią ilością wolnego miejsca na dysku twardym. Jeśli zabraknie miejsca program wyświetli podczas instalacji stosowny komunikat.

Instalacja programu jest zupełnie prosta. Po uruchomieniu Windows włóż płytę z programem do napędu. Instalator uruchomi się automatycznie i zaoferuje następujące opcje:

- **Instaluj**: Rozpoczęcie instalacji programu na komputerze.
- **Przeglądaj**: Uruchomienie Eksploratora Windows co umożliwia przeglądanie zawartości płyty CD-ROM z programem.
- **Anuluj**: Zamknięcie okna autostartu.

Instaluj program zgodnie ze wskazówkami kreatora instalacji. W oknie wyboru modułu wybierz program G DATA MailSecurity i rozpocznij instalację na wybranym komputerze. Najlepiej, jeśli jest to brama będąca przed serwerem pocztowym, ale możliwa jest także instalacja programu na tym samym komputerze co serwer pocztowy. Komputer ten musi oczywiście spełniać wymagania oprogramowania G DATA MailSecurity.

Podczas instalacji programu, możesz zdecydować, czy chcesz zainstalować składnik prowadzący szczegółowe statystyki strumienia poczty. Statystyki poczty dostępne są do wglądu po kliknięciu przycisku Statystyki w widoku Statusu. Opcje statystyk można modyfikować w zakładce Opcji o nazwie Rejestrowanie.

2.9 Instalacja składnika Internet Security for Android

Aby skorzystać z możliwości zdalnego zarządzania aplikacją G DATA MobileSecurity w urządzeniach przenośnych, najpierw trzeba zainstalować specjalnie w tym celu spreparowaną wersję oprogramowania na urządzeniach z systemem Android. Program G DATA Administrator umożliwia zlecenie instalacji aplikacji na urządzeniu mobilnym poprzez wysłania linku do zasobu w na serwerze IIS. Kliknięcie ikonki z telefonem w pasku narzędzi drzewa sieci powoduje otwarcia okna umożliwiającego wprowadzenie adresu mailowego do wysyłki odnośnika do aplikacji MobileSecurity. Możliwa jest również wysyłka na większą ilość adresów mailowych oddzielonych przecinkami lub średnikami. Program G DATA Administrator umożliwia również ustawienie hasła dla uwierzytelniania mobilnej aplikacji.

Po wysyłce użytkownik urządzenia mobilnego może zainstalować program klikając link do pliku APK zawierającego instalkę. Do zainstalowania programu niezbędne jest włączenie zezwolenia na instalację aplikacji spoza sklepu Google Play w ustawieniach systemu Android (najczęściej Ustawienia > Zabezpieczenia > Nieznane źródła.

Po uruchomieniu pliku APK przez dotknięcie linku, instalator zażąda potwierdzenia uprawnień i zainstaluje program G DATA MobileSecurity. Aby program MobileSecurity mógł korzystać z serwera zarządzającego, należy włączyć funkcję Zezwól na zdalne zarządzanie w ustawieniach aplikacji. W wyświetlonym oknie wpisz nazwę lub adres IP składnika ManagementServer. W polu nazwa urządzenia możesz wpisać nazwę, która będzie wyświetlana w oknie G DATA Administrator. W polu hasło wpisz wcześniej ustawione hasło do uwierzytelniania (hasło jest wysłane w wiadomości mailowej wraz z linkiem do aplikacji).

Jeśli urządzenie nie pojawi się automatycznie na liście stacji roboczych w oknie G DATA Administrators, uruchom urządzenie ponownie aby wymusić zarejestrowanie klienta mobilnego w programie G DATA ManagementServer.

3 G DATA ManagementServer

G DATA ManagementServer to serce całego systemu ochrony. Serwer pobiera aktualizacje i przekazuje je automatycznie na stacje robocze. Służy do sterowania ochroną antywirusową w sieci. Serwer zarządzający komunikuje się ze stacjami roboczymi używając protokołu TCP/IP. Dla mobilnych stacji roboczych, którzy są często odłączeni od sieci zadania są gromadzone i synchronizowane podczas kolejnej sesji online. Serwer zarządza też centralnym katalogiem Kwarantanny. Pliki Kwarantanny przechowywane są w postaci zaszyfrowanej. Moduł Administrator umożliwia wysłanie plików do Ambulansu G DATA za pomocą poczty elektronicznej. Składnikiem G DATA

ManagementServer administruje się za pomocą modułu Administrator.

Zamknięcie modułu Administrator nie powoduje wyłączenia składnika ManagementServer. Pozostaje on aktywny w tle i steruje ochroną stacji roboczych.

3.1 Internet Update

Aplikacja Internet Update umożliwia uaktualnienie sygnatur wirusów i plików składnika G DATA Client w repozytorium serwera zarządzającego oraz w szczególności aktualizację samego składnika ManagementServer.

Składnik ManagementServer, nie aktualizuje się automatycznie. Aby uaktualnić pliki serwera zarządzającego uruchom polecenie menu Start > (Wszystkie) programy > G DATA > G DATA ManagementServer > Internet Update i wciśnij przycisk Uaktualnij pliki Serwera.

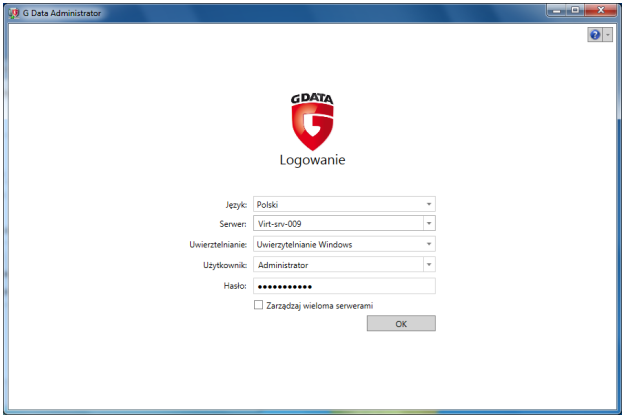
Uwaga: Jest to jedyna metoda aktualizacji plików serwera zarządzającego.

4 G DATA Administrator

Składnik Administrator to graficzny interfejs obsługi składnika ManagementServer. Instaluje się automatycznie podczas instalacji składnika ManagementServer. Umożliwia sterowanie procesami zdalnych instalacji i aktualizacji oprogramowania klienckiego na stacjach roboczych, a także planowanie procesów aktualizacji i skanowania. Z poziomu okna Administratora można modyfikować ustawienia ochrony stacji roboczych.

4.1 Uruchamianie G DATA Administrator

Po uruchomieniu składnika G DATA Administrator program zapyta o nazwę (adres IP) serwera, metodę uwierzytelniania, użytkownika oraz hasło.



Wpisz w polu Serwer nazwę lub adres IP komputera z zainstalowanym składnikiem G DATA ManagementServer (program automatycznie podkłada w tym polu nazwę lokalnego komputera).

Następnie wybierz metodę uwierzytelniania:

Uwierzytelnianie Windows

Ta metoda uwierzytelniania pozwala na zalogowanie się do składnika G DATA Administrator przy pomocy poświadczeń konta administratora systemu Windows.

Zintegrowanie uwierzytelnianie

Ta metoda umożliwia utworzenie wbudowanych kont użytkowników programu G DATA Administrator. Możliwe jest utworzenie konta bez uprawnień do modyfikacji ustawień programu. Tworzenie i modyfikowanie kont użytkowników możliwe jest dzięki poleceniu Zarządzanie użytkownikami w menu Plik.

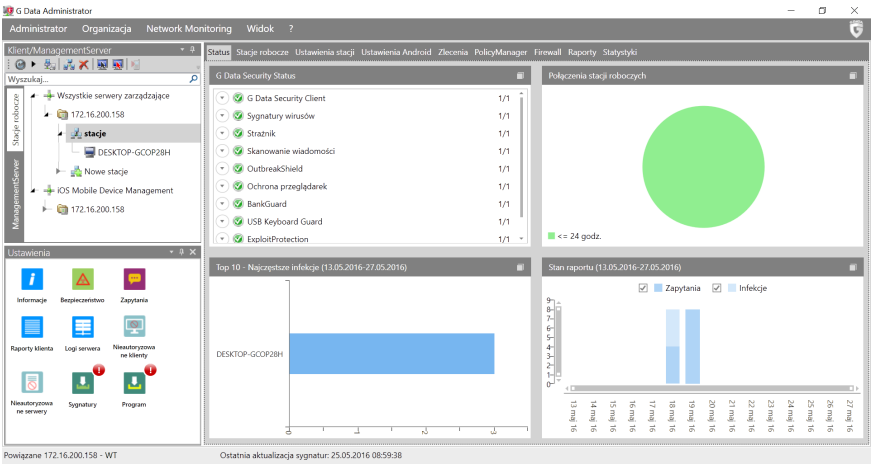
Uwaga: Pierwsze logowanie do składnika Administrator musi odbyć się przy zastosowaniu uwierzytelniania Windows, ponieważ w bazie ustawień oprogramowania nie ma założonych żadnych kont zintegrowanego uwierzytelniania.

Opcja **Zarządzaj wieloma serwerami** pozwala na zarządzanie w jednym oknie różnymi serwerami G DATA ManagementServer. Do jej uaktywnienia wymagany jest klucz odblokowujący generowany na żądanie. Jeśli potrzebujesz klucza, skontaktuj się z pomocą techniczną G DATA.

Kliknięcie ikony strzałki obok znaku zapytania w prawym, górnym rogu ekranu otwiera menu umożliwiające podejrzenie bieżącej wersji programu G DATA Administrator oraz przywrócenie ustawień okna logowania (np. rozmiar).

4.2 Obsługa składnika Administrator

Okno programu G DATA Administrator podzielone jest na 4 obszary.

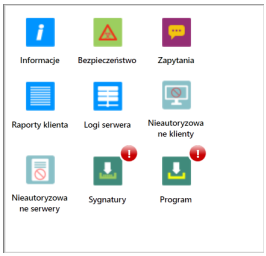


- Obszar Powiadomienia wyświetla informacje o statusie powiadomień oferując jednocześnie skróty do odpowiednich okien z raportami.
- Obszar Klient/ManagementServer umożliwia wyświetlanie klientów i serwerów zarządzanych z poziomu aplikacji G DATA Administrator.
- Prawa część okna przedstawia widok roboczy zawierający szereg kart. Bieżący widok i skład okna zależy od tego, co zaznaczone jest w obszarze Klient/ManagementServer, a także od posiadanej licencji na konkretne rozwiązanie.
- Pasek menu umożliwia dostęp do funkcji globalnych oraz do funkcji poszczególnych modułów programu:
  - Administrator: Uruchamianie kreatora kretora ustawień i wyłączanie aplikacji G DATA Administrator.
  - Organizacja (patrz rozdział Klient/ManagementServer > Stacje robocze > Organizacja)

- Stacje robocze (patrz rozdział Stacje robocze > Ustawienia)
- Zlecenia (patrz rozdział Zakładka Zlecenia)
- Firewall (patrz rozdział Zakładka Firewall > Ustawienia)
- Network Monitoring: Otwiera witrynę G DATA ActionCenter, umożliwiającą obsługę opcjonalnego modułu Network Monitoring.
- Widok: Wyświetlanie/ukrywanie obszaru Powiadomienia.
- ?: Wyświetlanie pliku pomocy lub informacji o wersji programu.

4.2.1 Powiadomienia

W obszarze powiadomień wyświetlane są informacje o ilości nieprzeczytanych raportów i statusów informujących o działaniu programu. Klikając w poszczególne ikony możemy szybko przeskoczyć do okna raportów zawierającego odfiltrowane informacje. Ilość ikon zależy od posiadanej licencji na produkt.



- **Informacje**: Ogólne informacje i raporty o błędach.
- **Bezpieczeństwo**: Raporty dotyczące zagrożeń.
- **Zapytania**: Zapytania użytkowników modułów PolicyManager, PatchManager, Firewall oraz kontroli aplikacji w klientach Android.
- **Poprawki**: Nieprzydzielone do instalacji poprawki o wysokim priorytecie.
- **Raporty klienta**: Raporty dotyczące pracy klientów (np. zmiana ustawień, status zleceń skanowania).
- **Logi serwera**: Logi i raporty błędów składnika ManagementServer.
- **Postfix**: Raporty modułu dla serwerów Sendmail/Postfix.

- **Squid**: Raporty modułu Squid.
- **Exchange**: Raporty wtyczki MailSecurity for Exchange.
- **Nieautoryzowane klienty**: Podłączone do serwera instancje klienta, które wymagają ręcznego autoryzowania przez administratora.
- **Nieautoryzowane serwery**: Serwery podrzędne powiązane z instancją ManagementServer, które wymagają ręcznego autoryzowania przez administratora.
- **Nieautoryzowane klienty Exchange**: Podłączone do serwera wtyczki Exchange, które wymagają ręcznego autoryzowania przez administratora.
- **Sygnatury**: Informacje o wersji sygnatur zagrożeń w repozytorium składnika ManagementServer.
- **Program**: Informacje o wersji składnika ManagementServer.

4.2.2 Klient/ManagementServer

Ten obszar wyświetla klientów i serwerów zarządzanych z poziomu aplikacji G DATA Administrator. Karta Stacje robocze wyświetli drzewo podłączonych instancje klienta oraz moduły do zarządzania klientami. Karta ManagementServer wyświetli drzewo serwerów zarządzających (serwery główne, podrzędne i zapasowe).

Grupy podzielone na podgrupy wyświetlone są ze znakiem + znanym z Eksploratora Windows. Aby rozwinąć grupę należy kliknąć znak +. Aby zwinąć daną gałąź kliknij znak -. W zależności od zaznaczonego węzła dostępne są różne grupy menu i ustawień programu.

Nad drzewkiem umieszczony został pasek narzędzi zawierający narzędzia umożliwiające zarządzanie klientami, dostępne również w postaci poleceń menu Organizacja:

Odśwież widok

Rozwiń/zwiń wszystko: Powoduje rozwinięcie lub zwinięcie wszystkich gałęzi drzewa.

Pokaż nieaktywne stacje

Utwórz nową grupę...

Usuń...

Uaktywnij stację: Po uaktywnienie stacji serwer sprawdza, czy na stacji zainstalowany jest klient G DATA.

Przegląd instalacji: Otwiera okno historii instalacji i samoaktywacji klientów G DATA.

Wyślij link instalacyjny do urządzenia mobilnego: Umożliwia wysłanie linku instalacyjnego do uzytkowników systemów Androidi iOS.

4.2.2.1 Stacje robocze

Drzewo stacji przedstawia widok obejmujący wszystkie jednostki komputerowe zarządzane z poziomu aplikacji G DATA Administrator. Sieć podzielona jest na 5 węzłów głównych (dostępność w zależności od posiadanej licencji):

- Wszystkie serwery zarządzające: Wszystkie podłączone serwery zarządzające G DATA wraz z klientami Windows/Android.
- Exchange: Wszystkie podłączone serwery Exchange wyposażone we wtyczkę G DATA MailSecurity for Exchange.
- Sendmail/Postfix: Systemy Linux z zainstalowanym klientem Sendmail/ Postfix.
- Squid: Systemy Linux z zainstalowanym klientem Squid.
- iOS Mobile Device Management: Zarządzane urządzenia iOS.

Aby zarządzać końcówkami za pomocą składnika G DATA Administrator, niezbędne jest ich dodanie/uaktywnienie w widoku drzewa oraz instalacja odpowiedniej wersji klienta G DATA:

- Windows: Aby wyszukać stacje użyj Asystenta konfiguracji, polecenia Wyszukaj stacje robocze, lub skojarz utworzoną grupę z serwerm Active Directory. Następnie rozpocznij instalację składnika G DATA Security Client.
- Linux: Skorzystaj z polecenia Wyszukaj stacje robocze aby dodać komputery do drzewa. Następnie rozpocznij instalację składnika G DATA Security Client w systemie Linux.
- Mac: Skorzystaj z opcji Uaktywnij klienta. Następnie przeprowadź procedurę Instalacja G DATA Security Clients (Mac).
- MailSecurity for Exchange: Wykonaj instalację G DATA MailSecurity dla Exchange. Wtyczka automatycznie pojawi się w widoku drzewa.
- Android: Skorzystaj z polecenia Wyślij link instalacyjny do urządzenia mobilnego. Po wysłaniu linku użytkownik musi zainicjować instalację i konfigurację bezpośrednio z odebranej wiadomości. Po skomunikowaniu się urządzenia mobilnego z serwerem zarządzającym (urządzenia muszą się "widzieć" w sieci), klient mobilny automatycznie pojawi się w drzewku, w węźle Wszystkie serwery zarządzające.

- iOS: Wprowadź dane do usługi G DATA ActionCenter w oknie Opcje > Ustawienia serwera > G_DATA_ActionCenter. Skorzystaj z polecenia Wyślij link instalacyjny do urządzenia mobilnego. Po zatwierdzeniu zgody na zarządzanie urządzeniem przez użytkownika klient mobilny iOS automatycznie pojawi się w drzewku, w węźle iOS MDM.

Objaśnienia symboli węzłów i końcówek:

 Cała sieć

 G DATA ManagementServer

 Grupa robocza

 Grupa (Active Directory)

 Serwer

 Serwer podrzędny

 Klient desktop

 Klient (nieaktywny)

 Klient laptop

 Klient mobilny

 Serwer Linux

 Klient Linux

 Klient MailSecurity for Exchange

 Nieobsługiwane urządzenia: np. drukarki sieciowe

Okno drzewka umożliwia wygodne eksportowanie i importowanie ustawień danego klienta do pliku. Polecenie prawego klawisza myszy **Eksport ustawień...**, spowoduje zapisanie ustawień zaznaczonego klienta oraz ustawień PolicyManager do pliku .dbdat. Ustawienia można zaimportować dla konkretnego klienta lub grupy w ten sam sposób, wybierając z menu kontekstowego polecenie **Import ustawień...** i wskazując zapisany wcześniej plik .dbdat.

Organizacja

Menu i lista przycisków Organizacja to zestaw poleceń umożliwiających zarządzanie ochroną stacji roboczych lub grup.

Odśwież

Polecenie odświeża widok drzewa sieci.

Pokaż nieaktywne stacje

Za pomocą tego polecenia możesz ujawnić nieaktywne lub usunięte z listy stacje robocze. Ich ikony są półprzezroczyste.

Dodaj grupę

Za pomocą tego polecenia możesz utworzyć nową grupę ustawień stacji roboczych. Grupowanie ustawień ułatwia zarządzanie procesami ochrony. Po kliknięciu polecenia w drzewie sieci pojawi się nowa grupa, której można nadać dowolną nazwę.

Aby przypisać daną stację roboczą do grupy, kliknij jej nazwę myszką i przeciągnij na folder grupy.

Edytuj grupę

Klikając to polecenie otworzysz okno, w którym za pomocą przycisków Dodaj i Usuń można dowolnie grupować stacje robocze. Funkcja jest aktywna po zaznaczeniu dowolnej grupy. Aby przypisać daną stację roboczą do grupy, kliknij jej nazwę myszką i przeciągnij na folder grupy.

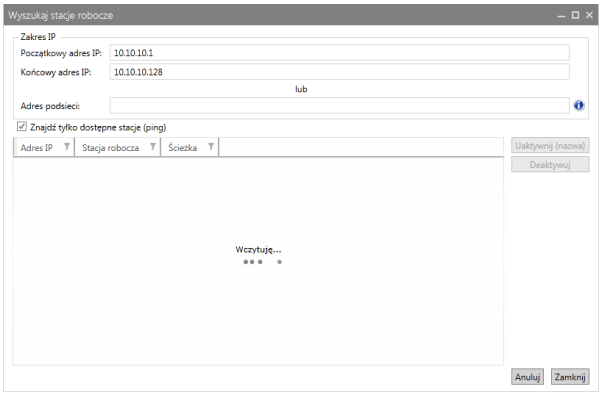
Usuń

Polecenie Usuń z menu Plik usuwa stację roboczą z drzewka (końcówka będzie nieaktywna). Nie oznacza to jednak odinstalowania składnika Klient. Usuwając grupy przywrócisz pierwotną hierarchię stacji roboczych.

To polecenie umożliwia również usunięcie grupy, pod warunkiem, że jest pusta. Stacje należy przed usunięciem przenieść do innej grupy.

Wyszukaj stacje robocze

Funkcja ta umożliwia wyszukiwanie komputerów w sieci po ich adresach IP. Można zastosować początkowy i końcowy adres IP (192.168.0.1 i 192.168.0.255), lub posłużyć się notacją **CIDR** (192.168.0.0/24). Po odnalezieniu stacji można je od razu uaktywnić po nazwie używając przycisku po prawej stronie. Wyszukiwanie można ograniczyć do dostępnych stacji przy pomocy wbudowanej funkcjonalności **ping**.



W razie potrzeby można zastosować wyszukiwarkę aby odnaleźć i zdeaktywować wybrane stacje przyciskim **Deaktywuj**.

Kreator reguł

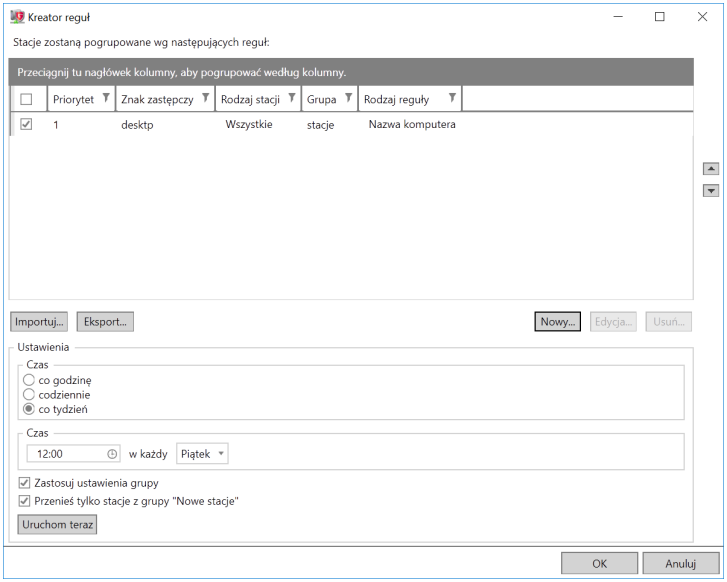
W momencie pierwszego połączenia zainstalowanego klienta ze składnikiem ManagementServer, trafia on zawsze automatycznie do grupy o nazwie **Nowe stacje**. Wyjątkiem będą klienty zainstalowane za pomocą pakietu instalacyjnego Windows skonfigurowane ze wskazaniem grupy docelowej. Kreator reguł umożliwia automatycznie przydzielanie klientów do wybranych grup na podstawie określonych parametrów.

Edycji reguł dokonujemy za pomocą przycisków Nowy..., **Edycja...** i **Usuń...**. Przyciski **Importuj...** i **Exportuj...** umożliwiają zapisywanie reguł w postaci plików **.json** oraz przenoszenie ich do innych serwerów zarządzających w celu zaimportowania.

W sekcji ustawienia możemy skonfigurować parametry uruchamiania reguł:

- **Czas:** Częstotliwość uruchamiania reguł.
- **Zastosuj ustawienia grupy:** Zaznaczenie tej opcji spowoduje dziedziczenie ustawień grupy w momencie przenoszenia klienta przez regułę.

- **Przenieś tylko stacje z grupy "Nowe stacje"**: Reguły zostaną zastosowane tylko do klientów znajdujących się w grupie inicjalnej o nazwie **Nowe stacje**. Jeśli ta opcja nie jest zaznaczona, reguły będą dotyczyć wszystkich klientów. Może to spowodować wielokrotne przenoszenie stacji z grupy do grupy, więc ta opcja domyślnie jest wyłączona.
- **Uruchom teraz**: Przycisk powoduje automatyczne uruchomienie reguły.



Dostępne są następujące kryteria przenoszenia klientów do pożądanych grup:

- **Rodzaj reguły**: Reguły mogą funkcjonować na podstawie nazwy komputera, adresu IP, nazwy domeny lub adresu bramy domyślnej.
- **Znak zastępczy**: Maska filtrowania klientów według ciągów znaków. Dozwolone jest stosowanie znaków zastępczych:

  produkcja_* spowoduje zastosowanie reguły dla wszystkich klientów o nazwie rozpoczynającej się od tego ciągu (dla reguł nazwy komputera),

  192.168.0.[1-100] spowoduje zastosowanie reguły dla wszystkich klientów z adresami IP z przedziału 192.168.0.1-192.168.0.100 (dla reguł adresu IP).
- **Rodzaj stacji**: Reguły mogą być stosowane do wszystkich rodzajów klientów

lub np. tylko dla serwerów, urządzeń android czy laptopów.

- **Grupy**: Wprowadź nazwy grup docelowych ręcznie lub klikając dwukrotnie pozycje drzewka poniżej. Jeśli wybierzesz więcej niż jedną grupę, klienty zostaną rozdzielone równomiernie pomiędzy wszystkie z nich.

Utwórz pakiet instalacji klienta Windows

Dzięki tej funkcji można utworzyć instalacyjny plik .exe, pozwalający na nienadzorowaną instalację oprogramowania klienckiego na stacjach roboczych bez potrzeby ingerencji użytkowników.

Pakiet zawiera zawsze aktualną wersję oprogramowania klienckiego. Opis instalacji znajdziesz w rozdziale Instalacja z pakietu instalacyjnego.

Utwórz skrypt instalacyjny klienta Linux/Mac

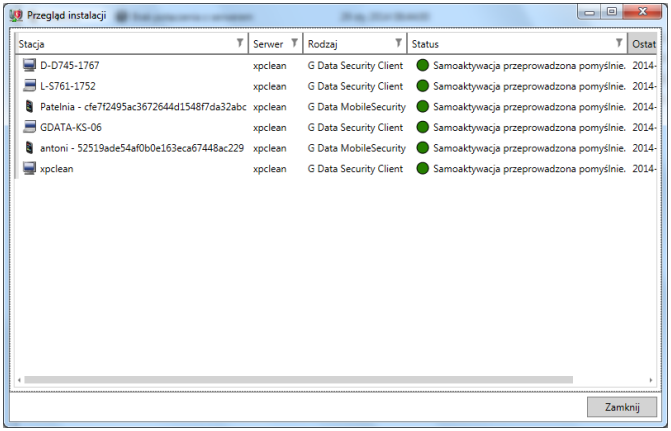
Dzięki tej funkcji można skrypt instalacyjny plik pozwalający na lokalną instalację oprogramowania klienckiego w systemach Linux/Mac.

Pakiet zawiera zawsze aktualną wersję oprogramowania klienckiego. Opis instalacji znajdziesz w rozdziałach Instalacja lokalna (Linux) i Instalacja lokalna (Mac).

Przegląd instalacji

To polecenie otwiera okno zawierające informacje na temat przebiegu i postępu instalacji zdalnych. Otwiera się automatycznie w momencie zlecenia zdalnej instalacji. Można je otworzyć również przy pomocy ikonki ponad drzewem sieci.

Okno przedstawia listę zakończonych i trwających zleceń zdalnej instalacji. Kolumna Rodzaj określa co konkretnie jest instalowane (G DATA Security Client/G DATA Firewall/serwer podrzędny). Po zakończeniu instalacji, kolumna statusu uaktualnia się automatycznie. W większości przypadków instalacja klienta wymaga restartu stacji roboczej. W zakładce Raporty powstaje w takim przypadku odpowiednia adnotacja przypominająca o potrzebie restartu..



Wyślij link instalacyjny do urządzenia mobilnego

Ta funkcjonalność umożliwia wysłanie do użytkowników urządzeń mobilnych linku instalacyjnego umożliwiającego uruchomienie instalację aplikacji G DATA. W zależności od zaznaczonego w drzewie węzła, w oknie pojawi się opcja wysyłki wiadomości do użytkowników systemu Android lub iOS.

Po wykonaniu przez użytkownika czynności instalacyjnych instalacja odpowiedniego klienta zostanie sfinalizowana, a urządzenie pojawi się w drzewie.

Przed wysłaniem wiadomości upewnij się, że w oknie Opcje > Ustawienia serwera > e-mail wprowadzone zostały dane dostępowe Twojego serwera SMTP.

System Android

Wprowadź adresy mailowe użytkowników urządzeń z systemem Android (oddzielone przecinkami lub średnikami). Kliknij **OK** aby wysłać wiadomości.

Przed wysłaniem wiadomości do użytkowników systemu Android wprowadź hasło dostępowe, które zostanie wysłane w treści wiadomości. Opcje > Ustawienia serwera > Ustawienia mobilne.

System iOS

W przypadku systemów iOS możesz uzupełnić pola decydujące o prezentacji urządzenia w aplikacji G DATA Administrator:

- Nazwa: Przyjazna nazwa urządzenia.
- Opis: Opis urządzenia.
- Organizacja: Nazwa organizacji.
- End User License Agreement: Treść umowy licencyjnej.
- Odbiorca: Adresy mailowe użytkowników urządzeń iOS (oddzielone przecinkami lub średnikami).

Przed wysłaniem wiadomości należy wprowadzić dane dostępu do usługi G DATA ActionCenter w oknie Opcje > Ustawienia serwera > G DATA ActionCenter. Zarządzanie urządzeniami mobilnymi iOS wymaga połączenia aplikacji G DATA Administrator z usługą G DATA ActionCenter. Wprowadź nazwę użytkownika i hasło do usługi. Jeśli nie masz konta w usłudze G DATA ActionCenter, zarejestruj się.

Kliknij **OK**, aby wysłać wiadomości.

Integracja z Active Directory

Od wersji 11 programy biznesowe G DATA Software mają możliwość integracji z Active Directory. Import skutkuje zaimportowaniem wybranych jednostek organizacyjnych (OU) i wszystkich stacji roboczych z katalogu Active Directory kontrolera domeny Windows. W celu zintegrowania z AD należy założyć nową grupę w drzewie komputerów. Opcja integracji można znaleźć w menu kontekstowym prawego klawisza myszy po kliknięciu założonej grupy stacji roboczych - Skojarz grupę z Active Directory.

W oknie wyboru domeny wskaż lokalizację serwera LDAP. Kliknij przycisk Wybierz... aby wyświetlić widoczne w sieci serwery. Istnieje również możliwość podłączenia się do innej domeny niż bieżąca.

Zaznaczenie opcji Automatycznie instaluj składnik G DATA Client na dodanych stacjach spowoduje automatyczne instalowanie programu G DATA Client na stacjach podłączanych i dodawanych do Active Directory, które spełniają formalne wymogi zdalnej instalacji. G DATA ManagementServer synchronizuje dane z serwerem AD co 6 godzin. Ten parametr można modyfikować w oknie Opcje > Ustawienia serwera > Synchronizacja.

4.2.2.2 ManagementServer

Drzewo serwerów przedstawia strukturę serwerów zarządzających G DATA.

 Węzeł główny (wszystkie serwery)

 Serwer główny

 Serwer zapasowy

 Serwer podrzędny

Po zaznaczeniu węzła lub danego serwera, w oknie roboczym wyświetlą się odpowiednie dla rodzaju serwera opcje i moduły.

4.2.3 Sekcja Stacje robocze

Wybierz sekcję stacje robocze aby wyświetlić moduły i opcje dla klientów w obszarze roboczym.

4.2.3.1 Zakładka Status

Zakładka **Status** przedstawia zestawienie najważniejszych informacji dotyczących ochrony antywirusowej stacji roboczych.

G DATA Security Status
Zestawienie podstawowych ustawień ochrony dla zaznaczonej grupy lub stacji roboczej.

Zielony kolor oznacza, że ustawienia ochrony skonfigurowane są optymalnie.

Czerwony wykrzyknik oznacza, że wskazana lub możliwa jest Twoja ingerencja w ustawienia oprogramowania.

W momencie uruchamiania składnika Administrator, wszystkie ikony pokazują przez moment znaj ostrzeżenia. Nie oznacza to, że program G DATA nie działa prawidłowo. W tym momencie mechanizm kontrolny automatycznie sprawdza poprawność ustawień ochrony.

Kliknięcie danego elementu powoduje otwarcie odpowiedniego okna z

ustawieniami, gdzie można dokonać korekty, lub przeprowadzić czynności związane z ochroną antywirusową.

Połączenia stacji roboczych
Sekcja zawiera informacje o połączeniach nawiązywanych przez serwer ze stacjami roboczymi. Stacje powinny regularnie łączyć się z serwerem. Jeśli tak nie jest, może to wskazywać na problemy z połączeniem, siecią, lub aplikacją G DATA Client na stacji roboczej.

Najczęściej infekowane stacje
Jeśli stacja jest często atakowana przez wirusy, warto zwrócić na nią uwagę lub uczulić użytkownika na przestrzeganie zasad bezpiecznego użytkowania komputera. W razie konieczności można zastosować opcje dostępne w zakładce PolicyManager (dostępne w wersjach G DATA EndpointProtection) w celu ograniczenia użytkownikom dostępu do niebezpiecznych zasobów Internetowych, lub np. zablokowania stosowania pendrive'ów i dysków przenośnych.

Stan raportu
Przejrzysty wykres przedstawiający ilość infekcji, zapytań i błędów zgłaszanych przez stacje robocze w zadanym czasie. Ramy czasowe można zmienić klikając ikonkę kalendarza.

4.2.3.2 Zakładka Stacje robocze

Widok **Ustawienia** przedstawia listę komputerów uaktywnionych przez konsolę administracyjną. Dostępne są tu informacje o wersji klienta G DATA, jego stanie, aktualności sygnatur wirusów, data ostatniego zgłoszenia się stacji do serwera, i inne.

Ustawienia

Po kliknięciu nazwy stacji roboczej, grupy lub ikony Cała sieć w drzewie po lewej stronie, w widoku Ustawienia zakładki Klienci pojawi się spis wszystkich stacji roboczej danej grupy.

Wyjaśnienie ikon paska narzędzi i poleceń menu kontekstowego w widoku stacji:

- **Odśwież:** Odświeża widok okna. Wczytuje aktualne ustawienia z serwera.
- **Usuń:** Przycisk ten usuwa zaznaczoną stację z grupy.
- **Drukuj**: Funkcja ta umożliwia wydruk ustawień. Przed wydrukiem można wybrać elementy do wydruku.

- **Widok strony**: Funkcja ta umożliwia podgląd układu strony przed wydrukiem.
- **Zainstaluj składnik Security Client**: Instaluje moduł Security Client. Instalacja jest możliwa tylko wtedy, kiedy komputery spełniają określone wymagania.
- **Odinstaluj składnik G DATA Security Client**: Polecenie powoduje odinstalowanie składnika klienta z komputera.
- **Teraz uaktualnij sygnatury wirusów**: Aktualizuje bazy wirusów Klienta.
- **Automatycznie uaktualniaj sygnatury wirusów**: Uruchamia automatyczną aktualizację baz wirusów klienta.
- **Teraz uaktualnij pliki programu**: Aktualizuje pliki składnika Security Client. Po aktualizacji może być wymagane ponowne uruchomienie komputera.
- **Automatycznie aktualizuj pliki programu**: Uruchamia automatyczną aktualizację plików klienta.
- **Przyznaj autoryzację**: Autoryzuje połączenie klienta zainstalowanego ręcznie lub z pakietu instalacyjnego.

Zawartość okna widoku Ustawienia można sortować widok klikając nagłówki poszczególnych kolumn.

Instalacja G DATA Security Client

Wybierz polecenie Instaluj składnik G DATA Security Client, aby przeprowadzić instalację zdalną programu G DATA Security Clients na wybranych komputerach.

Jeśli niektóre stacje widoczne są z wyszarzonymi ikonkami, uaktywnij je klikając prawym klawiszem ich nazwy w drzewie sieci po lewej stronie i wybierając polecenie Uaktywnij stację.

Jeśli nie masz możliwości przeprowadzenia zdalnej instalacji, lub nie chcesz w ten sposób instalować oprogramowania, możesz wykonać instalację ręcznie.

Deinstalacja G DATA Security Client

Wybierz polecenie Odinstaluj składnik G DATA Security Client, jeśli chcesz odinstalować klienta z wybranych komputerów. W oknie wyświetlonym po kliknięciu tego polecenia wybierz, czy chcesz usunąć również raporty stacji, kopie zapasowe i inne zasoby powiązane z komputerem.

Istnieje również możliwość odinstalowania klienta lokalnie poprzez wiersz

poleceń systemu Windows (cmd) uruchomiony w trybie administratora. W tym celu uruchom wiersz polecenia jako administrator i przejdź do folderu C:\Program Files (x86)\G DATA\AVKClient i wpisz polecenie unclient /AVKUninst. Deinstalacja przebiegnie w tle. Po ok. 10 minutach można uruchomić komputer ponownie aby system mógł sfinalizować process.

Zarządzanie EULA

Okno EULA (End User Licence Agreement) umożliwia zarządzanie informacjami o licencjonowaniu ochrony na urządzenia mobilne. Mamy możliwość tworzenia, edytowania i usuwania treści licencji, które możemy następnie przydzielić urządzeniom poprzez widok Stacje robocze. Dzięki temu zyskujemy pewność, że użytkownicy urządzeń mobilnych zostaną powiadomieni o objęciu urządzenia ochroną i że zgadzają się na zastosowanie rozwiązania zabezpieczającego G DATA.

Dodając nową licencję do listy, możemy określić jej nazwę, język oraz treść warunków.

W dowolnej chwili możemy zmodyfikować lub usunąć dowolną pozycję z listy.

Software

W tej zakładce można dokonać przeglądu oprogramowania zainstalowanego w komputerach. W celu ułatwienia zarządzania zasobami oprogramowania zakładka umożliwia tworzenie globalnych list dozwolonego i niedozwolonego oprogramowania.

Widok wyświetla aplikacje zainstalowane w systemach klienckich. Można dodawać wybrane aplikacje do białych i czarnych list za pomocą przycisków paska narzędzi. W widoku globalnej czarnej i białej listy jest również przycisk Dodaj, który umożliwia automatyczne dodawanie aplikacji na podstawie wybranych parametrów. Parametry można konfigurować ręcznie, lub odczytać automatycznie z wskazanego pliku (przycisk Ustalanie właściwości).

Sprzęt

Widok **Sprzęt** wyświetla zestawienie wybranych parametrów sprzętowych stacji.

Aby rozszerzyć widok o dodatkowe informacje, kliknij nagłówek dowolnej kolumny prawym przyciskiem myszy i wybierz polecenie Wybierz kolumny. Dostępne są informacje dotyczące procesora, pamięci, wolnego miejsca na dysku i inne.

Wiadomości

Zakładka **Stacje robocze**, oprócz standardowego widoku Ustawienia, wyposażona jest w widok Wiadomości umożliwiający przesłanie dowolnej wiadomości do użytkownika stacji roboczej.

Administrator programu może wyświetlać na ekranach stacji roboczych dowolne informacje tekstowe kierowane do użytkowników. Wiadomości można wysyłać do pojedynczych stacji, grup komputerów lub do całej sieci. Wiadomości wyświetlane są podobnie jak powiadomienia systemu Windows jako okienka w prawym, dolnym rogu ekranu.

Aby utworzyć nową wiadomość kliknij przycisk Nowy. Zaznacz stacje robocze, do których chcesz ją wysłać i wpisz treść wiadomości, a następnie kliknij przycisk Wyślij.

Jeśli chcesz wysłać wiadomość tylko do konkretnego użytkownika stacji roboczej, wpisz jego nazwę w polu **Użytkownik**.

4.2.3.3 Stacje robocze (iOS)

W widoku stacji roboczych, po zaznaczeniu w drzewie węzła iOS MDM pojawi się lista podłączonych do serwera urządzeń Apple:

- Stacja robocza: Nazwa urządzenia.
- Status zabezpieczeń: Bieżący stan zabezpieczeń. Jeśli do urządzenia nie został przypisany żaden profil ustawień, w tej kolumnie będzie widoczne ostrzeżenie.
- Profil: Profil ustawień przypisany do urządzenia. Wybierz profil z listy aby go przypisać. Możesz również usunąć profil urządzenia wybierając pozycję **Brak profilu**.
- Ostatnie logowanie: Dokładny czas ostatniego zameldowania się urządzenia iOS w usłudze G DATA ActionCenter.
- IMEI: Numer IMEI urządzenia.
- Pojemność: Ilość pamięci urządzenia (w GB).
- Wersja: Wersja systemu iOS.
- Numer telefonu urządzenia.
- E-mail: Adres e-mail, na który została wysłana wiadomość z linkiem instalacyjnym.
- Nazwa produktu: Nazwa produktu urządzenia.

Kliknij nazwę urządzenia prawym klawiszem i wybierz polecenie **Usuń** jeśli chcesz wyłączyć zarządzanie urządzeniem i usunać je z listy.

4.2.3.4 Zakładka Ustawienia stacji

Zakładka **Ustawienia** umożliwia modyfikowanie wszystkich opcji ochrony antywirusowej dla konkretnych stacji roboczych, grup lub całej sieci.

Rozwijana lista znajdująca się u góry okna ustawień umożliwia przełączanie między dostępnymi zestawami opcji. Ustawienia dotyczą zawsze stacji roboczej lub grupy zaznaczonej w drzewie sieci, z lewej strony. Po zakończeniu konfiguracji opcji w danym zestawie kliknij przycisk Zastosuj, aby przekazać ustawienia do stacji roboczych.

Ogólne

Sekcje ustawień zawarte w zakładce ogólne opisane są w następnych rozdziałach.

G DATA Security Client

Pierwsza sekcja zawiera następujące ustawienia:

- **Komentarz**: Jeżeli stacje robocze nie mają komentarzy przypisanych w ustawieniach systemu, możesz przypisać własne komentarze ułatwiające identyfikację komputerów (np. komputer szefa, księgowość, itp.)
- **Ikonka w zasobniku**: Dzięki tej opcji możesz ukryć ikonkę oprogramowania klienckiego na stacji roboczej, jeśli np. nie chcesz aby użytkownik miał świadomość, że program antywirusowy jest zainstalowany. Ustawienie Tylko w pierwszej sesji spowoduje, że ikonka nie będzie widoczna dla kolejnych użytkowników, którzy zalogują się jednocześnie do komputera. Jeżeli planujesz nadanie użytkownikom uprawnień do podglądu lub modyfikowania opcji, ukrywanie ikonki nie ma sensu, gdyż obsługa programu z poziomu stacji roboczej możliwa jest tylko poprzez menu kontekstowe ikonki.
- **Konto użytkownika**: Oprogramowanie klienckie funkcjonuje w kontekście systemu Windows. Jeżeli chcesz wpisać inne konto użytkownika, zastosuj konto z uprawnieniami administratora na stacjach roboczych, aby umożliwić skanowanie.

Aktualizacje

Sekcja aktualizacje umożliwia ustawienie następujących parametrów:

- **Uaktualniaj sygnatury wirusów automatycznie**: Włączenie tej opcji spowoduje automatyczne przekazywanie bieżących aktualizacji z serwera zarządzającego do stacji roboczych.
- **Uaktualniaj pliki programu automatycznie**: Ta opcja umożliwia automatyczne aktualizowanie plików oprogramowania klienckiego na stacjach roboczych.
- **Ponowne uruchomienie po aktualizacji**: Zdarza się, że po uaktualnieniu lub odinstalowaniu oprogramowania klienckiego niezbędne jest ponowne uruchomienie systemu operacyjnego stacji roboczej. Można wymusić ponowne uruchomienie bez ostrzeżenia, wyświetlić komunikat o potrzebie restartu lub tylko utworzyć raport.

Uprawnienia stacji

Ta sekcja umożliwia ustawienie uprawnień dla użytkownika oprogramowania klienckiego zainstalowanego na stacji roboczej:

- **Użytkownik może przeprowadzać skanowanie**: Jeżeli ta opcja jest włączona, użytkownik może uruchomić skanowanie dowolnych zasobów lokalnych komputera, a także modyfikować opcje skanowania. W menu kontekstowym pojawiają się pozycje Skanuj i Opcje.
- **Użytkownik może aktualizować sygnatury wirusów**: Jeżeli to uprawnienie jest włączone, użytkownik może aktualizować sygnatury wirusów oprogramowania klienckiego nawet, jeśli komputer nie ma połączenia ze składnikiem ManagementServer. Opcja jest bardzo przydatna w przypadku komputerów przenośnych, które nie zawsze mają połączenie z lokalna siecią przedsiębiorstwa.
- **Użytkownik może modyfikować opcje Strażnika:** Użytkownik z tym uprawnieniem jest w stanie całkowicie wyłączyć ochronę dostępową stacji roboczej. Ustawienie zalecane tylko dla doświadczonych i zaufanych użytkowników stacji roboczych.
- **Użytkownik może modyfikować opcje ochrony poczty:** Użytkownik może włączać i wyłączać ochronę poczty elektronicznej POP3/IMAP/SMTP.
- **Użytkownik może modyfikować opcje HTTP**: Użytkownik może włączać i wyłączać ochronę przeglądarek.
- **Użytkownik może przeglądać lokalną Kwarantannę**: Użytkownik z nadanym uprawnieniem do lokalnej Kwarantanny może samodzielnie usuwać, dezynfekować lub przywracać do systemu zarażone pliki

odizolowane w zaszyfrowanym folderze Kwarantanny. Ustawienie zalecane tylko dla doświadczonych i zaufanych użytkowników stacji roboczych.

- **Zabezpieczenie ustawień hasłem**: Jeżeli do stacji roboczej ma dostęp więcej niż jeden zaufany użytkownik, można zabezpieczyć dostęp do ustawień hasłem, znanym tylko tej osobie. Dzięki temu inni użytkownicy komputera nie będą mogli modyfikować ustawień narażając system na infekcję.
- **Ustawienia aktualizacji**: Stacja robocza może uaktualniać sygnatury wirusów z repozytorium serwera zarządzającego, lub bezpośrednio z Internetu. Można również ustawić trzecią opcję, czyli kombinację dwóch pierwszych. W takim przypadku stacja (lub komputer przenośny) pobiera sygnatury z serwera, jeżeli jest w sieci przedsiębiorstwa, a bezpośrednio z Internetu, jeżeli jest poza firmą.

Zlecenia

W sekcji Wyjątki można zdefiniować pomijane przy skanowaniu pliki, foldery i napędy sieciowe. Kliknięcie przycisku Edycja, a następnie ..., otwiera okno struktury katalogów stacji roboczej.

Wyjątki można definiować dla konkretnych stacji roboczych, grup lub całej sieci. Istnieje też możliwość eksportowania i importowania zestawów wyjątków do pliku tekstowego.

Niezależnie od zleceń skanowania możesz włączyć funkcjonalność **Skanowania w trybie bezczynności**. Jest to specjalny, bezobsługowy tryb skanowania wykonujący skanowanie stacji w czasie, kiedy nie jest używana. Skanowanie bezczynne wstrzymuje się automatycznie, jeśli wykryta zostanie aktywność systemu lub użytkownika. Po ponownym przejściu w stan bezczynności skanowanie wznawia się.

Strażnik

W tym widoku można dostosować ustawienia Strażnika dla wybranych stacji roboczych lub grup. Aby zmienić ustawienia dla całej grupy, należy zaznaczyć grupę na liście komputerów. Strażnik kontroluje wszystkie próby odczytu i zapisu plików zgodnie z ustawieniami. Działanie Strażnika odbywa się w tle, praktycznie niezauważalnie dla użytkownika.

Można skonfigurować Strażnika indywidualnie dla każdej stacji roboczej, grupy komputerów lub całej sieci. Zmiany w ustawieniach zatwierdza się przyciskiem Zastosuj. Przycisk Anuluj przywróci poprzednie ustawienia.

Jeśli w obrębie grupy zmienione zostaną ustawienia niektórych stacji, w ustawieniach grupy będzie to uwidocznione wypełnionymi kwadracikami przy

opisach opcji, które nie są jednolite dla całej grupy lub sieci

Bez ważnej przyczyny, nie powinno się wyłączać Strażnika na żadnym ze stanowisk.

Strażnik może spowolnienie działania niektórych programów lub ich komponentów. Aby tego uniknąć, można dodać foldery lub niektóre pliki tych aplikacji do wyjątków Strażnika.

Ustawienia

Sekcja Ustawienia umożliwia modyfikację następujących parametrów:

- **Status**: Strażnik może być włączony, wyłączony. Nie zaleca się wyłączania monitora bez ważnego powodu.
- **Skanery**: Klient stosuje dwa niezależne skanery antywirusowe. Zalecamy ustawienie Dwa skanery - optymalna wydajność. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor.
- **W razie infekcji**: Wybierz reakcję programu na wykrycie infekcji.

  Zablokuj dostęp: Program uniemożliwi zapis oraz odczyt danego pliku.

  Dezynfekcja (jeśli niemożliwa: zablokuj dostęp): Jeżeli nie uda się zdezynfekować pliku, program zablokuje do niego dostęp.

  Dezynfekcja (jeśli niemożliwa: do Kwarantanny): Jeśli nie uda się zdezynfekować pliku, program przeniesie go do Kwarantanny.

  Dezynfekcja (jeśli niemożliwa: usuń plik): Jeśli nie uda się zdezynfekować pliku, program spróbuje go usunąć.

  Przenieś plik do Kwarantanny: Plik zostanie umieszczony w zaszyfrowanym folderze.

  Usuń zarażony plik: Funkcja ta umożliwia usunięcie pliku wraz z wirusem.
- **Zainfekowane archiwa**: Można ustalić osobną reakcje na wykrycie wirusa w spakowanym pliku.
- **Skanuj**: Zdecyduj, czy chcesz skanować pliki w trakcie odczytu, zapisu i odczytu, czy tylko w trakcie uruchamiania.
- **Skanuj napędy sieciowe**: Przy włączonej opcji Strażnik kontroluje także zamapowane napędy sieciowe. Jeśli cała sieć jest chroniona przez moduły klienckie, opcja ta może być wyłączona.
- **Heurystyka**: Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując kody plików z kodami stale aktualizowanej bazy znanych wirusów, ale rozpoznaje je po typowych

cechach spotykanych u tego typu programów. Ta metoda, z jednej strony wzmaga skuteczność skanowania, ale jest bardzo czasochłonna i może powodować fałszywe alarmy.

- **Skanuj archiwa**: Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne dopóki włączony jest Strażnik. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się. Aby zminimalizować obciążenie procesora rozpakowywaniem dużych plików, można ograniczyć rozmiar kontrolowanych archiwów.
- **Skanuj pliki e-mail**: Jeśli opcja jest włączona, skanowane są także foldery programów pocztowych zawierające wiadomości. Nierozważne użycie tej funkcji może spowodować utratę wiadomości pocztowych.
- **Skanuj obszary systemowe przy starcie komputera**: Włączenie tej opcji powoduje skanowane sektorów rozruchowych dysku twardego oraz dyskietki przy każdym uruchomieniu komputera.
- **Skanuj obszary systemowe przy zmianie nośnika**: Można kontrolować obszary systemowe przy starcie komputera lub przy zmianie nośnika (np. włożenie do napędu nowej płytki CD-ROM). Zaleca się pozostawienie włączonej przynajmniej jednej z tych dwóch opcji.
- **Wykrywaj dialery/adware/spyware/riskware**: Strażnik wykrywa także programy wysokiego ryzyka, które niekoniecznie są wirusami. W ten sposób wykrywane są np. dialery, programy do zdalnego administrowania (np. RealVNC).

Jeśli chcesz, aby użytkownik otrzymywał komunikaty o wykryciu wirusa w systemie, zaznacz opcję Powiadamiaj użytkownika o wykryciu wirusa. Powiadomienie odbywa się poprzez wyświetlenia okna z komunikatem.

Wyjątki

W razie potrzeby można skonfigurować działanie Strażnika tak, aby kontrolując dostęp do plików pomijał określone napędy, katalogi lub pliki.

Możliwe jest definiowanie następujących rodzajów wyjątków:

- **Napęd**: Kliknij przycisk ..., a następnie wybierz literę napędu (partycji, dysku, napędu CD/DVD), który chcesz wyjąć spod ochrony monitora.
- **Katalog**: Kliknij przycisk ..., a następnie wybierz folder, który chcesz wyjąć spod ochrony monitora wraz z podfolderami.
- **Plik**: Wpisz nazwę pliku, który chcesz wyjąć spod ochrony. Dozwolone jest stosowanie znaków specjalnych (? jako dowolny znak, * jako dowolny ciąg znaków).

- **Proces**: Kliknij przycisk ..., a następnie wybierz plik wykonywalny (EXE), którego proces chcesz wyjąć spod ochrony monitora.

W ten sposób możesz utworzyć dowolną ilość wyjątków, które później można zmodyfikować lub usunąć.

Aby wybrać np. wszystkie pliki z rozszerzeniem .exe, wpisz *.exe. Aby wybrać np. wszystkie pliki o formacie arkuszy kalkulacyjnych (np. *.xlr, *.xls), wpisz *.xl?. Jeśli chcesz sprawdzać pliki o takim samym początku nazwy wpisz np. tekst*.*

Kontrola zachowania

Mechanizm kontroli zachowania nie działa w oparciu o wzorce wirusów, ale o wzorce zachowań. Program rejestruje zachowania aplikacji typowe dla szkodników (np. próby zapisu i tworzenie wpisów w rejestrze). Jeśli ilość podejrzanych zachowań przekroczy dopuszczalną normę, program zareaguje zgodnie z przewidzianą w ustawieniach reakcją. Może być to samo utworzenie raportu, zatrzymanie podejrzanej aplikacji lub przeniesienie podejrzanego programu do Kwarantanny.

ExploitProtection

Exploit to technologia ataku wykorzystująca słabe punkty oprogramowania zainstalowanego w komputerze. Moduł ExploitProtection weryfikuje na bieżąco zachowanie zainstalowanych programów i wykrywa podejrzane działania. W przypadku stwierdzenia w systemie wykorzystania luk w zabezpieczeniach programów aplikacja G DATA reaguje zgodnie z ustawieniami: **Tylko protokół** lub **Zapobiegaj uruchomieniu**.

Wszystkie działania moduły raportują do serwera zarządzającego, a raporty dostępne są w widoku raportów i w oknie powiadomień. Fałszywe detekcje można wyeliminować tworząc wyjątki kontekstowo, bezpośrednio z okna raportów. Wyjątki można przeglądać i edytować po kliknięciu przycisku **Edytuj globalną listę wyjątków...**.

USB Keyboard Guard

Moduł USB Keyboard Guard chroni stacje przed atakami typu BadUSB. Zmanipulowane urządzenia USB - np. kamery, pendrive'y lub drukarki mogą przedstawiać się w systemach oepracyjnych jako klawiatury. Aby zapobiec wyłudzeniu danych lub wykonaniu niekontrolowanych automatycznych poleceń w obrębie systemum składnik USB Keyboard Guard blokuje automatycznie wszystkie nowopodłączone urządzenia, które przedstawiają się jako

klawiatury. Użytkownik sam może zdecydować o dopuszczeniu klawiatury do użytku postępując zgodnie z wytycznymi wyświetlanymi w interaktywnym oknie. Jeśli podpięte urządzenie nie jest klawiaturą, może zablokować jego użycie.

Niezależnie od decyzji użytkownika, w oknie Raporty programu G DATA Administrator pojawi się odpowiedni raport. Pomimo dopuszczenia urządzenia przez użytkownika, administrator może je zablokować cofając autoryzację.

e-mail

Składnik klient wyposażony jest w narzędzie umożliwiające ochronę poczty wychodzącej i przychodzącej dowolnego programu pocztowego korzystającego z protokołów POP3, IMAP i SMTP, czyli Outlook Express, Mozilla Thunderbird, The Bat! i inne. Konta programu MS Office Outlook chronione są przez specjalny dodatek.

Ustawienia można skonfigurować indywidualnie dla każdej stacji roboczej, dla grupy komputerów lub też dla całej sieci:

Wiadomości przychodzące

Ta sekcja umożliwia modyfikowanie następujących ustawień:

- **W razie infekcji**: Wybierz reakcję programu na wykrycie wirusa w wiadomości.
- **Skanuj wiadomości przychodzące**: Włączenie tej opcji spowoduje sprawdzenie każdej przychodzącej wiadomości pod kątem wirusów i innych zagrożeń.
- **Skanuj nieprzeczytane wiadomości podczas uruchamiania Microsoft Outlook**: Włączenie tej opcji spowoduje przeskanowanie wszystkich nie przeczytanych wiadomości we wszystkich folderach programu MS Office Outlook.
- **Dołącz raport do zarażonych wiadomości przychodzących**: Jeśli program wykryje wirusa w wiadomości, dołączy do tematu słowo WIRUS w nawiasie kwadratowym, a do treści maila komunikat o infekcji.

Wiadomości wychodzące

Sekcja Wiadomości wychodzące umożliwia modyfikowanie następujących ustawień:

- **Skanuj wiadomości wychodzące**: Włączenie tej opcji może zapobiec przypadkowemu wysłaniu wirusa lub zarażonego załącznika. Jeżeli program wykryje wirusa w przesyłce, pojawi się stosowny komunikat, a wiadomość nie zostanie wysłana przez program pocztowy.
- **Dołącz stopkę do wiadomości wychodzących**: Jeżeli opcja Skanuj wiadomości wychodzące, program dołączy do treści wiadomości stopkę informującą o przeprowadzeniu skanowania maila. Dodatkowo można wymusić umieszczenie w podpisie informacji o wersji programu oraz linku do strony G DATA Software.

Opcje skanowania

Do dyspozycji masz następujące opcje skanowania wiadomości:

- **Skanery**: Zalecamy stosowanie dwóch skanerów. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor.
- **OutbreakShield**: Jest to dodatkowy skaner poczty, który działa niezależnie od tradycyjnych sygnatur wirusów. Jest w stanie wykryć niebezpieczną wiadomość jeszcze przed sklasyfikowaniem wirusa i dostarczeniem odpowiedniej sygnatury wirusów. Kliknij przycisk Zmień, jeśli chcesz dodatkowo użyć specjalnych sygnatur wirusów tworzonych na potrzeby skanera OutbreakShield. W takim przypadku program będzie próbował automatycznie nawiązać połączenie z Internetem. Jeżeli połączenie z Internetem wymaga skonfigurowana serwera proxy, skorzystaj z ustawień w sekcjach Serwer proxy i Uwierzytelnianie proxy.

Komunikaty ostrzegawcze

Jeśli chcesz, aby użytkownik otrzymywał komunikaty o wykryciu wirusa w wiadomości, zaznacz opcję Powiadamiaj użytkownika o wykryciu wirusa. Powiadomienie odbywa się poprzez wyświetlenia okna z komunikatem.

Wtyczka w Microsoft Outlook

Chroń konta Microsoft Office Outlook zintegrowaną wtyczką: Włączenie tej opcji, oprócz skanowania wiadomości podczas wysyłania/odbierania, umożliwia dodatkowo skanowanie wiadomości oraz folderów na żądanie, bezpośrednio w programie MS Office Outlook. Skanowanie można wykonać przez zaznaczenie folderu i uruchomienie polecenia Narzędzia > Skanuj folder programem G DATA AntiVirus.... Polecenie dostępne jest również jako ostatnia ikonka standardowego paska narzędzi programu MS Office Outlook.

Nasłuch na portach

Kliknij przycisk **Zmień...** aby otworzyć okno ustawień nasłuchu na portach. Programy pocztowe takie jak Outlook Express, Mozilla Thunderbird, TheBat! korzystające z protokołów POP3, IMAP oraz SMTP chronione są w standardowy sposób. Ochronę poszczególnych protokołów można włączać/wyłączać po kliknięciu przycisku Zmień.

HTTP

Składnik klient oferuje funkcje skanowania stron internetowych przed otwarciem, a także ochronę komunikatorów.

Skanowanie HTTP

- Skanuj zawartość HTTP: Filtr działa już w trakcie otwierania stron przy pomocy przeglądarki internetowej. Jeśli chcesz użyć tej funkcjonalności, włącz sprawdzanie zawartości stron i wpisz numer lub oddzielone przecinkiem numery portów HTTP (domyślnie 80).
- Ignoruj przekroczenie limitu czasu w przeglądarkach: Skanowanie zawartości strony odbywa się przed otwarciem strony. Może to spowodować błąd w przeglądarce, z powodu niedostarczenia treści strony do przeglądarki w czasie ustawionym w przeglądarce. Włączając tę opcję spowodujesz zignorowanie przekroczenia limitu czasu, dzięki czemu przeglądarka nie wyświetli komunikatu błędu.
- Ograniczenie rozmiaru: Ta opcja pozwala uniknąć długotrwałego skanowania dużych plików zawartych na sprawdzanej stronie internetowej. Skanowanie wszystkich plików w niewielkim stopniu spowalnia czas otwierania obszernych witryn internetowych.
- Globalne wyjątki skanowania HTTP: Możliwość skonfigurowania listy stron pomijanych podczas skanowania HTTP. Opcja działa globalnie, dla wszystkich stacji roboczych.

BankGuard

Szkodniki nastawione na atakowanie sesji zakupów oraz bankowości online to zagrożenie, którego nie można bagatelizować. Rewolucyjna technologia G DATA o nazwie BankGuard weryfikuje integralność bibliotek przeglądarki internetowej w czasie rzeczywistym. Zapobiegając i neutralizując próby manipulacji danych w pamięci operacyjnej mechanizm jest w stanie uchronić 99% sesji online przed kompromitacją nawet ze strony nieznanych szkodników. Zalecamy pozostawienie tej opcji włączonej dla użytkowników korzystających z przeglądarek Internet Explorer, Firefox i Chrome.

AntiSpam

Składnik klient ma wbudowany filtr antyspamowy.

Jeżeli chcesz uruchomić filtr spamu dla poczty elektronicznej, włącz opcję **Zastosuj filtr spamu**. Po wykryciu podejrzanej, lub potwierdzonej wysyłki masowej, program automatycznie doda zdefiniowany poniżej komunikat do tematu wiadomości.

Dzięki oznaczaniu niechcianych wiadomości w temacie, możesz zdefiniować w aplikacjach pocztowych poszczególnych stacji roboczych reguły przenoszące wiadomości do utworzonych folderów poczty np. Spam, Prawdopodobnie spam.

4.2.3.5 Zakładka Ustawienia Exchange

Ten rozdział opisuje konfigurację wtyczki G DATA MailSecurity dla serwerów Microsoft Exchange 2007/2010/2013/2016. Wtyczka jest modułem opcjonalnym dla wszystkich wersji aplikacji G DATA dla firm.

Ogólne

Automatyczne skanowanie obiektów podczas każdej próby dostępu jest domyślnie włączone. Nie zaleca się wyłączania tej opcji, choć program to umożliwia.

Podobnie jak oprogramowanie klienckie na stacje robocze, wtyczka do serwerów poczty Microsoft Exchange wyposażona jest w mechanizm skanowania w trybie bezczynności, włączający się automatycznie w momencie minimalnego obciążenia procesora serwera poczty. Skanowanie obejmuje wszystkie obiekty Microsoft Information Store.

Istnieje możliwość wyłączenia wykonywania skanowania w trybie bezczynności w konkretnych godzinach dnia, lub określonych dni. Dzięki temu można skonfigurować skaner do działania poza godzinami pracy w dni robocze, ale przez cały czas w weekend.

Istnieje również możliwość ustawienia maksymalnego wieku skanowanych plików (w dniach). Pliki starsze niż zadana wartość nie będą skanowane przez skaner trybu bezczynności.

Skanowanie

- **Skanery**: Klient stosuje dwa niezależne skanery antywirusowe. Zalecamy ustawienie Dwa skanery - optymalna wydajność. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor.
- **W razie infekcji**: Wybierz reakcję programu na wykrycie infekcji.
- **Zainfekowane archiwa**: Można ustalić osobną reakcje na wykrycie wirusa w spakowanym pliku.
- **Rodzaje plików**: Można skanować wszytkie pliki lub jedynie programy i dokumenty. Skanowanie wszystkich plików może zająć więcej czasu.
- **Heurystyka**: Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując kody plików z kodami stale aktualizowanej bazy znanych wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, z jednej strony wzmaga skuteczność skanowania, ale jest bardzo czasochłonna i może powodować fałszywe alarmy.
- **Archiwa**: Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne dopóki włączony jest Strażnik. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się. Aby zminimalizować obciążenie procesora rozpakowywaniem dużych plików, można ograniczyć rozmiar kontrolowanych archiwów.

Status

Program wyświetla listę serwerów Exchange chronionych wtyczką G DATA MailSecurity. W poszczególnych kolumnach znajdują się następujące informacje:

- **Komputer**: Nazwa serwera poczty.
- **Skaner A/Skaner B**: Numery wersji skanerów antywirusowych.
- **Stan danych**: Data i godzina przeprowadzenia ostatniej aktualizacji

sygnatur wirusów G DATA MailSecurity. Data może być inna niż sama data sygnatur wirusów.

- **Wersja G DATA Client**: Numer wersji oprogramowania klienckiego dla serwera poczty.
- **Ostatnie logowanie**: Data ostatniego połączenia wtyczki G DATA MailSecurity ze składnikiem G DATA ManagementServer.
- **Aktualizacja sygnatur wirusów / Czas**: Informacja na temat terminu i stanu wykonania ostatniego zlecenia aktualizacji sygnatur wirusów.
- **Aktualizacja plików / Czas**: Informacja na temat terminu i stanu wykonania ostatniego zlecenia aktualizacji plików wtyczki.

Sortowanie danych w kolumnach można wymusić klikając nagłówek wybranej kolumny.

AntiSpam

Moduł antyspamowy pozwala na odfiltrowanie niechcianych wiadomości przed przekazaniem ich do użytkowników. Moduł AntiSpam dostępny jest tylko dla serwerów Exchange pełniących rolę Hub Transport.

Wiadomości klasyfikowane są przez system antyspamowy z podziałem na trzy kategorie: **Podejrzenie o spam**, **Wysokie prawdopodobieństwo spamu** i **Bardzo wysokie prawdopodobieństwo spamu**. Filtr umożliwia wybór osobnej reakcji sytemu dla każdej z kategorii:

- Reakcja:
  - Dostarcz wiadomość: Wiadomość trafi do użytkownika.
  - Przenieś wiadomość do Kwarantanny: Wiadomość zostanie przeniesiona do folderu Kwarantanny.
  - Odrzuć wiadomość: Wiadomość zostanie odrzucona.
  - Przenieś wiadomość do spamu: Wiadomość zostanie przeniesiona do folderu spam.
- Prefiks w temacie: Do tematu wiadomości zostanie dodany przedrostek (np. [SPAM?]).
- Komunikat w treści: W treści wiadomości zostanie dodany komunikat.
- Twórz raporty: System utworzy raport w widoku Raporty aplikacji G DATA Administrator

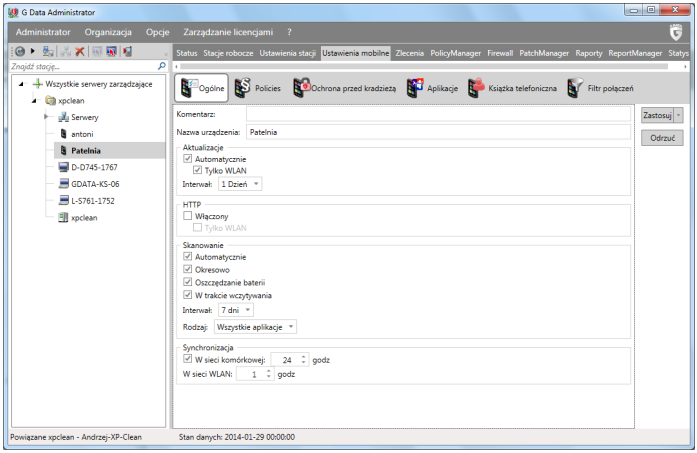
Ponadto istnieje możliwość tworzenia i edytowania białych i czarnych list domen i adresów e-mail. Wiadomości pochodzące z adresów i domen z białej listy nie będą badane pod kątem spamu. Wiadomości pochodzące z adresów i domen z czarnej listy oznaczane będą jako **Bardzo wysokie prawdopodobieństwo spamu**.

4.2.3.6 Zakładka Ustawienia Android

Ta zakładka umożliwia zarządzanie klientami mobilnymi. Po zainstalowaniu i skonfigurowaniu składnika G DATA Internet Security for Android, mobilne urządzenia pojawią się automatycznie w drzewie sieci.

Ogólne

Ustawienia w tej zakładce dotyczą urządzeń mobilnych z systemem Android, z zainstalowanym klientem mobilnym.



- **Komentarz**: Pole tekstowe na wprowadzenie dowolnego komentarza.
- **Nazwa urządzenia**: Pole ułatwiające identyfikację urządzenia.

Aktualizacje

- **Automatycznie**: Włączenie tej opcji powoduje automatyczne aktualizowanie klienta mobilnego w urządzeniu. Jeśli włączysz tę opcję, możesz również wymusić aktualizowanie urządzenia tylko poprzez sieć bezprzewodową (Tylko WLAN).

HTTP

- **Włączony**: Włącza/wyłącza filtr HTTP w przeglądarkach mobilnych urządzenia.

Skanowanie

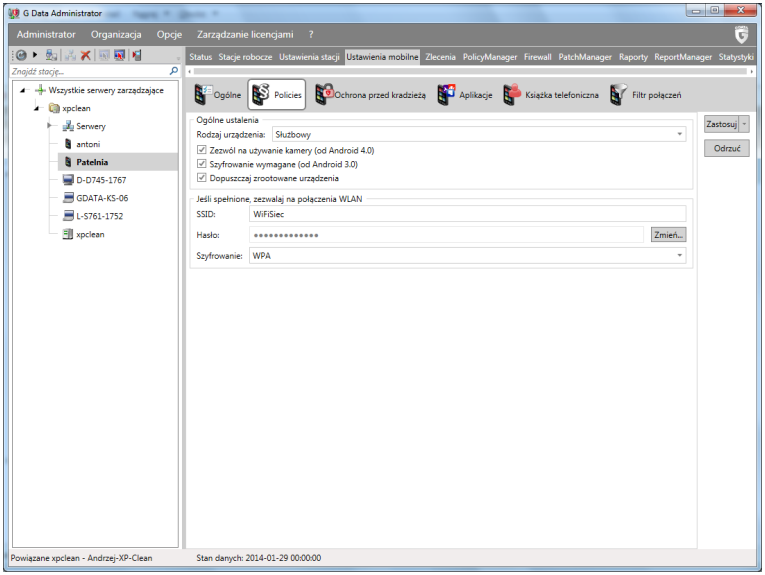
- **Automatycznie**: Skanowanie uruchamiane jest automatycznie, bez potrzeby ingerencji użytkownika.
- **Okresowo**: Umożliwia zastosowanie harmonogramu automatycznego skanowania. Poniżej można wybrać z listy Interwał częstotliwość skanowania, oraz jego zakres (lista Rodzaj).
- **Oszczędzanie baterii**: Włącz tę funkcję, jeśli chcesz zezwolić na skanowanie w trybie oszczędzania energii.
- **W trakcie ładowania**: Włącz tę funkcję, jeśli chcesz zezwolić na skanowanie tylko podczas ładowania urządzenia.
- **Rodzaj**: Wybierz, czy chcesz skanować wszystkie aplikacje, czy tylko te zainstalowane przez użytkownika.

Synchronizacja

Określ częstotliwość synchronizacji danych aplikacji mobilnych z serwerem poprzez sieci komórkowe i WLAN.

Policies

Widok **Policies** umożliwia zarządzanie istotniejszymi uprawnieniami korzystania z urządzeń mobilnych.



Ustawienia ogólne

Wskazując **Służbowe** jako rodzaj urządzenia mobilnego automatycznie zablokujemy użytkownikowi możliwość modyfikowania kluczowych ustawień systemu Android. Niezależnie od powyższego możemy wymusić następujące zachowania urządzeń:

- **Zezwól na używanie kamery (od Android 4.0)**
- **Szyfrowanie wymagane (OD Android 3.0)**
- **Dopuszczaj zrootowane urządzenia** (spowoduje pominięcie uwierzytelniania klienta hasłem w przypadku zrootowanego systemu Android)

Warunkowe połączenia WLAN

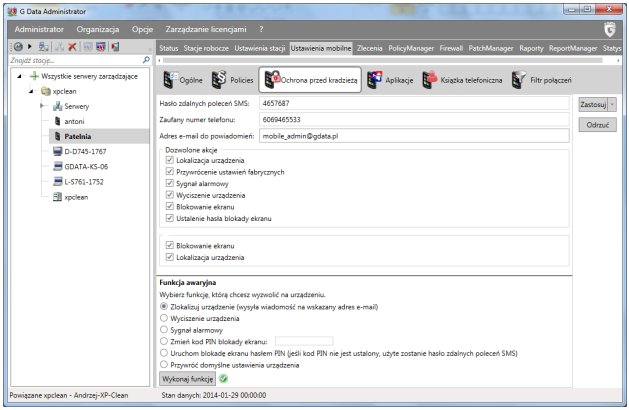
Jeśli urządzenie mobilne spełnia polityki bezpieczeństwa ustawione powyżej, możemy automatycznie przydzielić mu dostęp do określonej sieci bezprzewodowej.

Wprowadź identyfiaktor sieci (SSID), wybierz rodzaj szyfrowania i w razie potrzeby wprowadź hasło.

Ochrona przed kradzieżą

Zarządzanie ochroną urządzeń mobilnych obejmuje również funkcjonalność ochrony przed utratą urządzenia z możliwością sterowania urządzeniem zdalnie za pomocą spreparowanych poleceń SMS z telefonu, lub przy użyciu protokołu Google Cloud Messaging - bezpośrednio z konsoli G DATA Administrator. Jeśli urządzenie zaginie, można je dzięki temu zdalnie zablokować, zlokalizować lub wymusić usunięcie danych.

Do wysyłki zdalnych poleceń SMS z telefonu, niezbędne jest ustalenie specjalnego hasła, stosowanego później w składni zdalnych poleceń. Kolejnym zabezpieczeniem jest możliwość zdefiniowania zaufanego numeru telefonu. Tylko z tego numeru będzie można zdalnie zmodyfikować wcześniej wspomniane hasło do składni zdalnych poleceń. Urządzenia mobilne reagują na zdalne polecenia SMS raportując zwrotnym SMS-em. Po wprowadzeniu do konfiguracji adresu mailowego do powiadomień, odpowiedzi będą również wędrować na wskazany adres e-mail.



Dozwolone akcje

Sekcja dozwolonych akcji określa, jakie zdalne polecenia można będzie wykonywać na danym urządzeniu lub ich grupie. Zaznacz polecenia, które chcesz włączyć:

- **Lokalizacja urządzenia**: Po włączeniu tej akcji będzie można zlokalizować urządzenie na żądanie poleceniem SMS. Lokalizacja zostanie wysłana na skonfigurowany wcześniej adres mailowy. Składnia polecenia SMS: hasło locate.
- **Przywrócenie ustawień fabrycznych**: Ta opcja umożliwia usuwanie prywatnych danych z urządzenia poprzez zdalne wymuszenie przywrócenia ustawień fabrycznych. Składnia polecenia SMS: hasło wipe.
- **Sygnał alarmowy**: Umożliwia wysłanie do urządzenia polecenia wywołującego głośny sygnał dźwiękowy trwający do momentu uruchomienia aplikacji G DATA Internet Security. Ułatwia to zlokalizowanie urządzenia po zgubieniu lub kradzieży. Składnia polecenia SMS: hasło ring.
- **Wyciszenie urządzenia**: Ta opcja umożliwia zdalne wyciszenie urządzenia, np. aby nie zwracało na siebie uwagi. Oczywiście nie wpłynie to na możliwość wywołania sygnału alarmowego. Składnia polecenia SMS: hasło mute.
- **Blokowanie ekranu**: Ta opcja otwiera możliwość zdalnego zablokowania ekranu urządzenia przywracając wcześniej ustawione hasło blokady ekranu. Składnia polecenia SMS: hasło lock. Jeśli urządzenie nie ma ustalonego hasła blokady, zostanie zastosowane hasło zdalnych poleceń SMS.
- **Ustalenie hasła blokady ekranu**: W przypadku zapomnienia hasła blokady telefonu, możemy dzięki tej funkcjonalności wymusić zdalne ustawienie hasła. Składnia polecenia SMS: hasło set device password: hasło.

Można również wymusić zmianę hasła zdalnych poleceń SMS. Musi się to odbyć przy użyciu ustawionego wcześniej zaufanego telefonu. Składnia polecenia SMS: remote password reset: hasło.

Po wymianie SIM

W trakcie instalacji aplikacji G DATA Internet Security rejestrowana jest obecność kary SIM. Jeśli aplikacja wykryje wyjęcie karty z urządzenia, mamy możliwość automatycznego wywołania następujących akcji:

- **Blokowanie ekranu**: Analogicznie jak w opisie Dozwolone akcje.
- **Lokalizacja urządzenia**: Analogicznie jak w opisie Dozwolone akcje.

Funkcje awaryjne

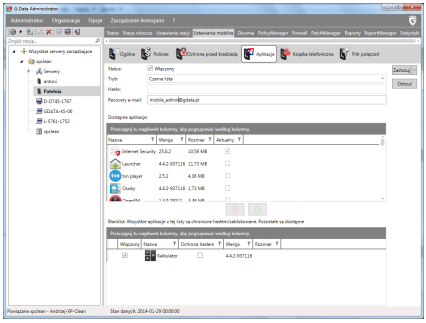
Oprócz możliwość wysyłania zdalnych poleceń SMS, konsola G DATA Administrator umożliwia wywoływanie zdalnych działań na chronionych urządzeniach za pomocą Google Cloud Messaging. Ta funkcjonalność nie wymaga obecności karty SIM w telefonie. Wystarczy połączenie z internetem. Przed użyciem funkcji awaryjnych niezbędne jest przeprowadzenie konfiguracji protokołu Google Cloud Messaging: W oknie menu Opcje > Ustawienia serwera> Ustawienia mobilne trzeba wprowadzić parametry Sender ID oraz API Key.

Aby wywołać funkcję awaryjną, zaznacz ją i kliknij przycisk **Wywołaj funkcję**. Funkcjonalność jest identyczna jak w przypadku zdalnych poleceń SMS opisanych w rozdziele Dozwolone akcje.

- Zlokalizuj urządzenie
- Wyciszenie urządzenia
- Sygnał alarmowy
- Zmień kod PIN blokady ekranu
- Uruchom blokadę ekranu
- Przywróć domyślne ustawienia urządzenia

Aplikacje

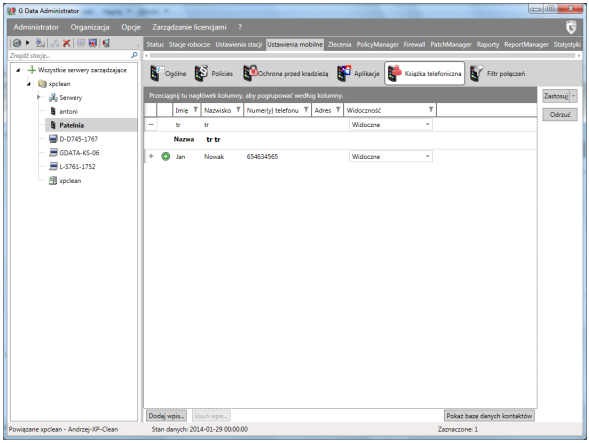
Ten widok umożliwia zarządzanie dostępem do aplikacji na urządzeniach mobilnych. Filtr może działać w trybie białej lub czarnej listy. W trybie czarnej listy, widniejące na niej aplikacje zostaną zablokowane, lub udostępnione po podaniu hasła. W trybie białej listy dozwolone jest stosowanie wszystkich widniejących na niej aplikacji. Do uruchomienia pozostałych niezbędne jest hasło (PIN). Skonfigurowanie adresu recovery e-mail umożliwi wysłanie przypomnienia hasła.



List dostępnych aplikacji zawiera wszystkie programy zainstalowane w urządzeniu mobilnym. Umieszczanie wybranych aplikacji na białej lub czarnej liście odbywa się przy użyciu ikon strzałek.

Książka adresowa

Ten widok umożliwia zarządzanie kontaktami w urządzeniach mobilnych. Można umieszczać wybrane kontakty w wewnętrznej książce adresowej aplikacji Internet Security i w ten sposób ukryć je wraz z listą połączeń i wiadomości wymienianych z adresatami.



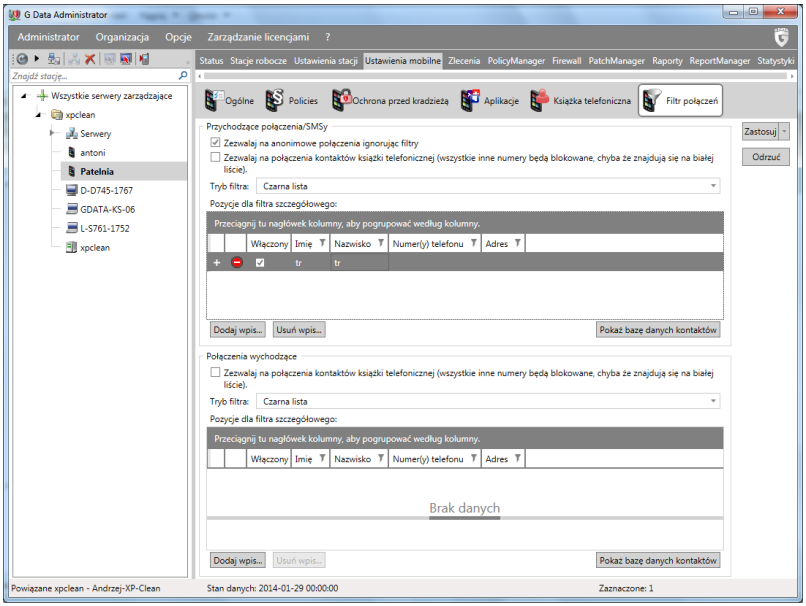
Lista przedstawia pozycje wprowadzone do książki telefonicznej aplikacji Internet Security. Kolumna widoczność umożliwia ustalenie, czy kontakt ma być widoczny w standardowych kontaktach Android. Ukrywając kontakt ukrywamy również komunikację (historię połaczeń i wiadomości SMS) z adresatem. Przycisk **Dodaj wpis...** pozwala na dodanie kontaktu do książki.

Okno bazy danych kontaktów zawiera listę wszystkich zdefiniowanych wcześniej kontaktów. Można dodawać do listy lub usuwać dowolne kontakty z bazy danych.

Lista bazy danych kontaktów umożliwia wprowadzanie nowych pozycji w bazie kontaktów. Można również zaimportować kontakty z Active Directory Organizational Unit (OU). Usunięcie kontaktu możliwe jest po jego zaznaczeniu i wybraniu odpowiedniego polecenia z paska menu lub menu kontekstowego prawego klawisza.

Filtr połączeń

Filtr połączeń umożliwia blokowanie określonych połaczeń i SMS-ów przychodzących, a także połączeń wychodzących. Korzystając z bazy kontaków opisanej w rozdziale Ksiazka adresowa, można w prosty sposób edytować czarną lub białą listę kontaktów.



Przychodzące połączenia/SMS

W tej sekcji można zdefiniować kontakty, które będą pomijane przy próbie wysłania wiadomości SMS lub wykonania telefonu na urządzenie mobilne. Osobno można również zablokować komunikację z anonimowych numerów lub ograniczyć filtr tylko do kontaktów z książki telefonicznej.

Tryb filtra określa, czy filtrowanie następuje wg czarnej, czy białej listy. Przyciski Dodaj wpis... oraz Usuń wpis... umożliwiają zarządzanie książką adresową.

Połączenia przychodzące

Sekcja połączeń wychodzących umożliwia ograniczenie wykonywania połączeń wg skonfigurowanego filtra. Filtr może działać w trybie białej lub czarnej listy

W momencie próby wykonania niedozwolonego połączenia, użytkownik otrzymuje stosowny komunikat z możliwością zażądania dostępu do wybieranego numeru. Żądanie pojawi się administratorowi w sekcji Raporty, gdzie można kontekstowo dodać numer bezpośrednio do białej lub czarnej listy.

4.2.3.7 Zakładka Ustawienia iOS

W tej zakładce dostępne są wszystkie opcje konfiguracyjne dotyczące zarządzania systemami iOS.

Ogólne

Widok Ogólne umożliwia wprowadzenie dodatkowego opisu urządzenia oraz przypisanie profilu ustawień.

- Opis: Można wprowadzić opis charakteryzujący urządzenie lub jego konfigurację. Opis będzie widoczny tylko w aplikacji G DATA Administrator.
- Bieżący profil: Profil ustawień przypisany aktualnie do urządzenia iOS. Wybierz profil z listy lub wybierz pozycję **Brak profilu** aby usunąć profil z urządzenia.

Po niżej, w sekcji **Informacje o instalacji** wyświetlony jest zestaw informacji wprowadzony w trakcie wysyłki wiadomości instalacyjnej do użytkownika wraz z przypisaną treścią umowy licencyjnej - **End User License Agreement**.

Profil

Profil umożliwia skonfigurowanie zestawów polityk bezpieczeństwa dla urządzeń lub grup urządzeń iOS. Użyj przycisku **Dodaj profil...** aby utworzyć nowy profil nadając mu nazwę i ewentualnie opatrując go opisem. Każdy profil może zawierać do **pięciu** predefiniowanych polityk. Każda z nich zawiera ustawienia związane z konkretnymi kategoriami ustawień.

Po utworzeniu profilu należy dodać minimum jedną z polityk aby go zapisać. Wybierz kategorię polityki i kliknij ikonę plusa, aby dodać ją do profilu:

- Ograniczenia funkcjonalności: Blokowanie specyficznych funkcjonalności systemów iOS (np. użycie kamery, Siri czy też Cloud).
- Ograniczenia aplikacji: Blokowanie działania aplikacji (np. YouTube, iTunes Store lub Safari).
- Ograniczenia treści: Blokowanie aplikacji, treści medialnych ze względu na wiek i region.
- Ustawienia kodu: Wymuszanie polityk kodu dostęu do urządzeń iOS (np. złożoność, długość czy maksymalna ilość pomyłek).
- WLAN: Zdalna konfiguracja sieci bezprzewodowej w urządzeniach iOS.

Wybierz dodaną politykę, aby skonfigurować jej szczegółowe ustawienia. Kliknij przycisk **Zastosuj** aby zapisać polityki i profil. Po przypisaniu profilu do urządzenia ustawienia zostaną zsynchronizowane. Po zastosowaniu profilu w oknie Raporty (iOS) pojawi się odpowiedni zapis.

Istnieje możliwość eksportowania importowania profili za pomocą przycisków paska narzędzi. Ustawienia zapisywane są w plikach JSON.

AntiTheft

Wodok AntiTheft umożliwia podjęcie działań antykradzieżowych na urządzeniach z systemami iOS:

- Zablokuj urządzenie: Włącza ekran blokady na urządzeniu (jeśli kod jest ustawione, do zdjęcia blokady będzie wymagane jego podanie).
- Przywróć ustawienia domyślne urządzenia: Wymusza przywrócenie ustawień fabrycznych urządzenia. Uwaga: Ta funkcja usuwa wszystkie dane i wyłącza zdalne zarządzenie urządzeniem.
- Zdejmij hasło: Usuwa kod blokady urządzenia.

Zaznacz wybrane polecenie i kliknij przycisk **Wykonaj funkcję...** aby zlecić jej wykonanie. Stan zlecenie widoczny będzie w widoku Raporty (iOS).

4.2.3.8 Zakładka Sendmail/Postfix

Moduł dla serwerów poczty Sendmail/Postfix jest dostępny jako opcja przy zakupie.

Zakładka **Sendmail/Postfix** służy konfigurowania ustawień wtyczek.

Ustawienia

Ustawienia wtyczki obejmują konfigurację parametrów ochrony antywirusowej:

- Reakcja: Ustala reakcję programu na wykrycie zagrożenia w wiadomości (usuwanie załącznika lub przenoszenie wiadomości do Kwarantanny).
- Prefix w temacie: Określa przedrostek dodawany do tematu niebezpiecznej wiadomości (np. [VIRUS]).
- Komunikat w treści: Określa tekst dodawany do treści wiadomości (np. Wiadomość zawiera wirusa).

AntiSpam

Wtyczka dla serwerów Sendmail/Postfix wykrywa również niechciane wiadomości. Widok AntiSpam umożliwia konfigurację ustawień antyspamowych.

Wiadomości niechciane kategoryzowane automatycznie jako **podejrzane o spam**, **wysokie prawdopodobieństwo spamu** oraz **bardzo wysokie prawdopodobieństwo spamu**. Dla każdej z kategorii istnieje możliwość ustawienia odrębnej reakcji programu:

- **Reakcja**:
  - **Dostarcz wiadomość**: Wiadomość zostanie dostarczona do użytkownika.
  - **Usuń wiadomość**: Wiadomość zostanie usunięta.
- **Prefix w temacie**: Do tematu wiadomości zostanie dodany przedrostek (np. [SPAM?]).
- **Komunikat w treści**: Do treści wiadomości zostanie dodany komunikat.
- **Utwórz raport**: Reakcja programu zostanie zaraportowana do serwera zarządzającego.

Można również dla każdej z kategorii ustawić czarne i białe listy adresów lub

domen. Wiadomości z adresów i domen na białej liście nie będą filtrowane; wiadomości z adresów i domen na czarnej liście zawsze będą kategoryzowane jako bardzo wysokie prawdopodobieństwo spamu. Białe i czarne listy można eksportować i importować w postaci plików .json.

4.2.3.9 Zakładka Squid

Moduł dla serwerów Squid jest dostępny jako opcja przy zakupie.

Zakładka Squid umożliwia konfigurowanie ustawień wtyczki dla serwerów proxy Squid:

- **Włączony**: Ochrona antywirusowa serwera Squid jest włączona.
- **Zastosuj AntiPhishing**: Uruchamia system weryfikacji w chmurze dla poprawy skuteczności ochrony.
- **Twórz raporty**: Reakcje programu są raportowane do serwera zarządzającego.

Dodatkowo Sekcja **Czarna lista** umożliwia konfigurowanie domen i adresów IP, które mają być blokowane przez wtyczkę.

4.2.3.10 Zakładka Zlecenia

W tym widoku definiuje się zlecenia skanowania komputerów z zainstalowanym oprogramowaniem klienckim. Istnieją dwa rodzaje zleceń: jednorazowe i periodyczne. Jednorazowe skanowanie uruchamiane jest natychmiastowo, dla zleceń periodycznych planuje się czas wykonania zlecenia na określony dzień i godzinę.

W widoku Zlecenia widoczne są wszystkie zlecone skanowania. Można je sortować klikając opisy w nagłówkach kolumn:

- **Nazwa**: Nazwa zlecenia nadana przez w trakcie tworzenia zlecenia.
- **Komputer**: To nazwa stacji roboczej. Zlecenia można przydzielać tylko aktywnym stacjom roboczym.
- **Grupa**: Stacje robocze można łączyć w grupy. Jeśli przydzielisz zlecenie grupie, w oknie widoku nie pojawią się nazwy wszystkich stacji roboczych, lecz tylko nazwa grupy.
- **Status**: Informacja o stanie lub wyniku wykonywanego zlecenia. Dowiesz się tu, czy zlecenie jest już wykonane i czy podczas skanowania zostały wykryte wirusy.
- **Ostatnie uruchomienie**: Stąd dowiesz się kiedy ostatnio uruchomione

zostało dane zlecenie.

- **Interwał**: Kolumna informuje jak często ma być wykonywane skanowanie.
- **Zakres skanowania**: Zawiera informacje na temat zasobów wybranych do przeskanowania (np. wszystkie dyski lokalne).

Polecenia paska zadań

- **Odśwież**: To polecenie odświeża widok okna Zlecenia.
- **Jednorazowe zlecenie skanowanie**: Ta funkcja umożliwia przeprowadzenie jednorazowego skanowania wybranych zasobów na żądanie. Przed uruchomieniem zlecenia można zdefiniować nazwę zlecenie, parametry skanowania i zasoby, które mają zostać objęte zleceniem. Kliknij dwukrotnie nazwę zlecenia, jeżeli chcesz przejrzeć lub zmodyfikować ustawienia zlecenia. Ten sam efekt uzyskasz klikając nazwę zlecenia prawym klawiszem myszki i wybierając polecenie Właściwości...
- **Periodyczne zlecenie skanowania**: Ta funkcja umożliwia przeprowadzenie skanowania periodycznego wybranych zasobów. W zakładce Planowanie istnieje możliwość określenia częstotliwości przeprowadzania skanowania. Kliknij dwukrotnie nazwę zlecenia, jeżeli chcesz przejrzeć lub zmodyfikować ustawienia zlecenia. Ten sam efekt uzyskasz klikając nazwę zlecenia prawym klawiszem myszki i wybierając polecenie Właściwości...
- **Zlecenie kopii**: Tworzenie codziennych kopii zapasowych umożliwi szybkie odzyskanie danych w przypadku awarii. Najlepiej odizolować lokalizację kopii fizycznie i logicznie od sieci produkcyjnej. Umożliwi to odzyskanie danych nawet w przypadku rozleglejszej awarii.
- **Zlecenie przywracania**: Zlecenia przywracania umożliwiają odzyskiwanie danych z utworzonych wcześniej kopii.
- **Zlecenie wykrywania oprogramowania**: To polecenie uruchamia skanowanie stacji lub grupy komputerów pod kątem zainstalowanego oprogramowania. Szczegóły znajdziesz w następnych rozdziałach.
- **Zlecenie dystrybucji oprogramowania**: To polecenie umożliwia zastosowanie w stacji lub grupie komputerów poprawek wykrytych przez zlecenie wykrywania oprogramowania. Szczegóły znajdziesz w następnych rozdziałach
- **Uruchom teraz**: Użycie tego polecenia wymusza natychmiastowe wykonanie zaznaczonego zlecenia niezależnie od ustawionego harmonogramu.
- **Raporty**: To polecenie otwiera okno raportów dotyczących zleceń dla danej stacji roboczej.

Po kliknięciu zakładki **Zlecenia**, w pasku menu pojawi się dodatkowa pozycja o tej samej nazwie. Menu umożliwia przeprowadzenie następujących działań:

- **Widok**: Jeżeli nie chcesz wyświetlać wszystkich zleceń, wybierz z menu Widok pożądaną opcję. Możesz ograniczyć widok do zleceń periodycznych, jednorazowych, rozpoczętych oraz zakończonych. Dodatkowo można włączyć wyświetlanie szczegółów zleceń grupowych.
- **Uruchom teraz**: To polecenie wymusza natychmiastowe uruchomienie dowolnego istniejącego zlecenia, niezależnie od ustalonego harmonogramu.
- **Anuluj**: Użyj tej funkcji w celu przerwania trwającego skanowania.
- **Usuń**: To polecenie usuwa skonfigurowane zlecenie.
- **Nowy**: Polecenie umożliwia utworzenie nowego zlecenia jednorazowego lub periodycznego.

Możesz utworzyć dowolną ilość różnych zleceń skanowania. Ze względu na obciążenie powodowane przez proces skanowania, najlepiej unikać zleceń zachodzących na siebie w czasie.

Zlecenie skanowania

Ta funkcja umożliwia przeprowadzenie skanowania periodycznego wybranych zasobów. W zakładce Planowanie istnieje możliwość określenia częstotliwości przeprowadzania skanowania.

Ta funkcja umożliwia przeprowadzenie jednorazowego skanowania wybranych zasobów na żądanie. Przed uruchomieniem zlecenia można zdefiniować nazwę zlecenie, parametry skanowania i zasoby, które mają zostać objęte zleceniem.

Kliknij dwukrotnie nazwę zlecenia, jeżeli chcesz przejrzeć lub zmodyfikować ustawienia zlecenia.

Kliknij dwukrotnie nazwę zlecenia, jeżeli chcesz przejrzeć lub zmodyfikować ustawienia zlecenia. Ten sam efekt uzyskasz klikając nazwę zlecenia prawym klawiszem myszki i wybierając polecenie Właściwości...

Okna ustawień zlecenia jednorazowego i periodycznego wyglądają bardzo podobnie. W przypadku zlecenia jednorazowego nie ma zakładki umożliwiającej planowanie skanowania. Opcje zlecenia są intuicyjne i przejrzyste, nie powinny sprawiać większego kłopotu. Ustawiamy zakres skanowania, opcje skanerów i ewentualnie harmonogram wykonywania.

Przydatne może być ustawienie umożliwiające użytkownikom wstrzymanie/

przerwanie skanowania.

Wyłącz komputer po zakończeniu skanowania, jeżeli żaden użytkownik nie jest zalogowany to ciekawa opcja umożliwiająca pozostawienie włączonych komputerów np. na noc w celu przeskanowania zasobów bez niepotrzebnego obciążania maszyn w trakcie pracy.

Domyślnie zaznaczona jest opcja Uruchom zlecenie później, jeśli komputer jest wyłączony w dane chwili.

W zakładce **Skaner** warto zwrócić uwagę na priorytet (im wyższy, tym bardziej obciążony komputer) i możliwość zredukowania ilości procesorów użytej do procesu skanowania.

Zlecenie kopii zapasowej

Widok zlecenia umożliwia tworzenie zleceń kopii zapasowych w wersjach produktu wyposażonych w tę funkcjonalność. Program umożliwia tworzenie pełnych i częściowych (różnicowych) kopii zapasowych.

Tworzenie codziennych kopii zapasowych umożliwi szybkie odzyskanie danych w przypadku awarii. Najlepiej odizolować lokalizację kopii fizycznie i logicznie od sieci produkcyjnej. Umożliwi to odzyskanie danych nawet w przypadku rozleglejszej awarii.

G DATA Backup jest rozwiązaniem kopiującym wskazane pliki i foldery. Nie umożliwia tworzenia obrazów całych systemów stacji roboczych.

W celu zmodyfikowania ustawień kliknij dwukrotnie wiersz z nazwą zlecenia, lub skorzystaj z polecenia Właściwości menu prawego klawisza myszy.

Źródło kopii

Nadaj jednoznaczną nazwę dla zlecenia kopii i wskaż foldery, które mają zostać uwzględnione w kopii zapasowej. Możesz przeglądać foldery lokalnego komputera lub włączonych stacji roboczych. Foldery dodaje się i usuwa z listy przyciskami Dodaj i usuń. Opcja Foldery użytkownika automatycznie dodaje do listy wszystkie foldery użytkowników komputera (C:\Users lub C:\Dokumenty i ustawienia.

Istnieje możliwość eksportowania list folderów do pliku tekstowego i importowania ich do programu. Służą do tego przyciski Import i Eksport. Podczas przeglądania drzewa folderów, w polu Aktualna ścieżka pojawia się nazwa klikniętego foldera. Pole umożliwia ręczne wpisanie ścieżki dostępu do folderu w celu dodania go do listy źródeł kopii.

Planowanie

Ta zakładka umożliwia określenie harmonogramu przeprowadzania kopii zapasowej. Można ustawić osobny harmonogram dla kopii pełnej i osobny dla kopii częściowych. Opcja Nie uruchamiaj na zasilaniu bateryjnym umożliwia

wykrywanie stacji roboczych zasilanych bateryjnie. Zaległa kopia zostanie wykonana w momencie podłączenia stacji do stałego źródła zasilania. Ta opcja zapobiega rozładowaniu baterii przez większe obciążenie stacji podczas wykonywania kopii. Jeśli w momencie przewidzianym w harmonogramie dana stacja robocza nie jest podłączona do serwera zarządzającego, kopia zostanie sporządzona tymczasowo lokalnie, na stacji roboczej i przeniesiona na serwer zarządzający w momencie podłączenia stacji do sieci z serwerem zarządzającym. Kopia tymczasowa zostanie zapisana na partycji stacji, na której jest najwięcej miejsca. Podczas następnego kontaktu z serwerem zarządzającym, kopia zostanie przeniesiona na serwer.

Jeśli w momencie przewidzianym w harmonogramie stacja robocza jest wyłączona, zlecenie zostanie nadrobione po włączeniu komputera.

Domyślnie kopie zapasowe przechowywane są w następujących folderach serwera zarządzającego:

C:\ProgramData\G DATA\ManagementServer\Backup.

lub C:\Documents and settings\All Users\Dane aplikacji\G DATA\ManagementServer\Backup.

Lokalizację kopii można zmienić w oknie menu Opcje > Ustawienia serwera > Backup

Jeśli w trakcie tworzenia kopii zabraknie wolnego miejsca, program G DATA Administrator wyświetli odpowiedni komunikat błędu.

Opcje

Zakładka opcji pozwala na wykluczenie predefiniowanych rodzajów folderów z kopii zapasowych (np. foldery plików tymczasowych, plików z określonym atrybutem) a także na określenie rozszerzeń plików, które ma ją zostać pomijane przy tworzeniu kopii.

Przed przekazaniem do serwera, kopie zapasowe są zapisywane w folderze tymczasowym na stacji roboczej. Domyślnie kopie tymczasowe zapisywane są w folderze G DATA\Backup tworzonym na partycji dysponującej największą ilością wolnego miejsca. Jeśli chcesz zmienić domyślny folder kopii tymczasowej, wyłącz opcję dynamicznego ustalania lokalizacji i wskaż własny folder.

Zlecenie przywracania

Zlecenia przywracania można konfigurować na różne sposoby. Można wywołać okno wyboru gotowych kopii do przywrócenia z menu **Zlecenia > Nowe > Zlecenie przywracania** lub też poprzez kliknięcie odpowiedniej ikony z paska narzędzi menu **Zlecenia**. Można również kliknąć prawym klawiszem konkretne zlecenie kopii, aby przywrócić zabezpieczone za jego pomocą zasoby.

Okno przywracania może zawierać jeden lub więcej wierszy zleceń kopii

zapasowych do przywrócenia. Dla każdego zlecenia może być dostępnych kilka wykonanych kopii. Z tego punktu można zdecydować o przywróceniu danego stanu kopii na konkretną stację roboczą (niekoniecznie tę, z której pochodzą dane). Kliknij OK, aby przejść do ustawień.

Okno ustawień przywracania kopii pozwala na wgląd do archiwów kopii w celu przejrzenia plików. Umożliwia to wybranie do przywrócenia konkretnych plików, zamiast całej struktury archiwum.

Karta opcji zlecenia umożliwia skonfigurowanie parametrów zlecenia przywracania kopii. Można określić nazwę zgłoszenia, miejsce docelowe przywracania, a także co ma się dziać w przypadku wykrycia konfliktów wersji przywracanych plików. Po zatwierdzeniu zlecenie trafia na listę zleceń i jest natychmiast uruchamiane.

Zlecenie wykrywania oprogramowania

Wykrywanie oprogramowania jest możliwe, jeśli dysponujesz wersją programu wyposażoną w opcjonalny składnik PatchManager.

Ta funkcja pozwala na zgromadzenie informacji oraz sporządzenie listy zainstalowanych i dostępnych dla stacji poprawek. Zlecenie może zostać wykonane niezwłocznie, lub we wskazanym terminie, także zgodnie z harmonogramem. Można zawęzić zlecenie do konkretnych poprawek, tylko krytycznych lub ustalanych na podstawie zdefiniowanych kryteriów.

Aby wyszukać tylko poprawki o zdefiniowanych parametrach (producent, nazwa, priorytet, język), zaznacz pole wyboru przy nazwie parametru. Parametry można konfigurować w oparciu o znaki specjalne "?" i "*".

Zlecenie dystrybucji oprogramowania

Zdalne instalowanie poprawek i oprogramowania jest możliwe, jeśli dysponujesz wersją programu wyposażoną w opcjonalny składnik PatchManager.

Za pomocą tej funkcji można określić, kiedy i gdzie serwer zarządzający ma zainstalować wybrane poprawki. Implementacja oprogramowania może nastąpić natychmiast, bezpośrednio po uruchomieniu komputerów lub bezpośrednio po zalogowaniu. Opcja Zastosuj z opóźnieniem spowoduje wstrzymanie implementacji poprawek do chwili, kiedy minie zadany czas.

Do usuwania zainstalowanych poprawek służy osobne Zlecenie cofania dostępne również w widoku PatchManager.

Zlecenie cofania zmian

Zlecenie cofania zmian służy do deinstalowania aktualizacji zainstalowanych przy użyciu modułu G DATA PatchManager. Kliknij **Zlecenie dystrybucji oprogramowania** w widoku Zlecenia prawym klawiszem myszy i wybierz polecenie **Cofnij**. Zlecenie cofania można również zaplanować w zakładce Widok składnik PatchManager, poprzez wybranie stacji i konkretnej poprawki.

Okno konfiguracji zlecenia cofania umożliwia opatrzenie zlecenia nazwą w celu łatwej identyfikacji. Po wprowadzeniu nazwy kliknij **OK** aby zatwierdzić zlecenie. Realizacja zlecenia nastąpi niezwłocznie.

4.2.3.11 Zakładka PolicyManager

PolicyManager umożliwia zarządzanie kontrolą urządzeń, aplikacji, filtrem treści, a także czasem dostępu użytkowników do Internetu. Jest to elastyczne narzędzie, przydatne w planowaniu polityki bezpieczeństwa i wydajności pracy w przedsiębiorstwie. Zdefiniuj dostęp określonych użytkowników do zasobów firmy i zorganizuj ich czas pracy. Teraz decydujesz, czy, i z jakich aplikacji i nośników danych korzystają Twoi pracownicy.

W każdej z zakładek składnika PolicyManager po prawej stronie otwiera okno umożliwiające włączenie lub wyłączenie użytkownikom możliwości wysyłania próśb o włączenie dostępu do zablokowanego urządzenia, strony internetowej lub aplikacji poprzez. Komunikacja odbywa się poprzez okienko dialogowe z przyciskami, pojawiające się w momencie zablokowania danego zasobu.

Raporty składnika PolicyManager mogą być również przesyłane na adres mailowy skonfigurowany wraz z serwerem poczty w oknie Powiadomień.

Kontrola aplikacji

Ta funkcjonalność umożliwia blokowanie lub udostępnianie użytkownikom konkretnych programów, plików lub folderów. Obostrzenia mogą dotyczyć użytkowników z ograniczonym dostępem lub zarówno użytkowników jak i administratorów komputerów. Rozwijana lista Tryb pozwala aplikacji określić, czy ma działać w trybie białej, czy czarnej listy.

- **Whitelist**: Dostępne będą tylko aplikacje, pliki i foldery znajdujące się na białej liście.
- **Blacklist**: Programy, pliki i foldery znajdujące się na czarnej liście będą zablokowane.

Jeśli użytkownik uruchomi aplikację, do której nie ma dostępu, system pokaże mu odpowiedni komunikat.

Jeżeli administrator włączy możliwość zgłaszania próśb o odblokowanie aplikacji, użytkownik dodatkowo zobaczy okno dialogowe umożliwiające wysłanie prośby o odblokowanie konkretnej aplikacji/pliku/folderu. Administrator może odmówić dostępu lub na niego zezwolić jednocześnie przesyłając do użytkownika komunikat, którego treść może każdorazowo modyfikować.

Raporty składnika PolicyManager mogą być również przesyłane na adres mailowy skonfigurowany wraz z serwerem poczty w oknie Powiadomień.

Tworzenie nowych reguł

Aby utworzyć nową regułę dostępu kliknij przycisk Nowy... Wybierz rodzaj reguły z dostępnych w oknie dialogowym.

- **Producent**: Reguła tego typu będzie dotyczyła wszystkich aplikacji i plików podpisanych cyfrowo przez konkretnego producenta. Kliknij przycisk ... i wskaż plik, z którego program automatycznie odczyta informacje o producencie, lub wpisz nazwę producenta ręcznie. Znak * zastępuje dowolny znak lub ciąg znaków.
- **Plik**: Inną metodą blokowania zasobów jest blokowanie konkretnych plików. Program oferuje szeroką gamę kryteriów stosowanych do identyfikacji i zarządzania dostępem do plików. Oprócz nazw, można wykorzystać nazwę producenta, sumy kontrolne, wersję, prawa autorskie lub komentarz. Przycisk Określ właściwości pliku umożliwia wskazanie pliku w celu odczytania wszystkich wymienionych cech charakterystycznych. Cechy można wpisywać również ręcznie w przygotowane pola edycyjne. Dozwolone jest stosowanie znaku *, zastępującego dowolny ciąg znaków.
- **Folder**: Istnieje również możliwość udostępnienia lub zablokowania całego folderu (opcjonalnie z uwzględnieniem podfolderów.

Kontrola urządzeń

Funkcja kontroli urządzeń umożliwia zarządzanie dostępem użytkowników do pendrive'ów, dysków zewnętrznych, kamer internetowych, stacji dyskietek i napędów optycznych. Oprócz zablokowania danego urządzenia lub nośnika, można ograniczyć użytkownikom prawo do zapisywania danych.

Obostrzenia mogą dotyczyć użytkowników z ograniczonym dostępem lub zarówno użytkowników jak i administratorów komputerów.

Program wyświetla domyślną listę urządzeń do zablokowania (nie zawsze te urządzenia są podłączone lub obecne w komputerze). Można zablokować dostęp do kamer internetowych w grupie komputerów, pomimo faktu że nie w każdym komputerze zainstalowana jest kamera.

Dla każdego urządzenia dostępne są następujące ustawienia uprawnień:

Odczyt/zapis: Pełny dostęp do urządzenia.

Odczyt: Urządzenie nie może zapisywać danych na nośnikach.

Zablokuj dostęp: Zablokowany jest zapis, a także odczyt danych. Urządzenie nie będzie dostępne dla użytkownika.

Jeśli użytkownik uruchomi urządzenie/nośnik, do którego nie ma dostępu, system pokaże mu odpowiedni komunikat.

Jeżeli administrator włączy możliwość zgłaszania próśb o odblokowanie urządzenia, użytkownik dodatkowo zobaczy okno dialogowe umożliwiające wysłanie prośby o odblokowanie konkretnego urządzenia/nośnika. Administrator może odmówić dostępu lub na niego zezwolić jednocześnie przesyłając do użytkownika komunikat, którego treść może każdorazowo modyfikować.

Raporty składnika PolicyManager mogą być również przesyłane na adres mailowy skonfigurowany wraz z serwerem poczty w oknie Powiadomień.

Wyjątki

Istnieje możliwość skonfigurowania listy uprzywilejowanych urządzeń i nośników, które będą działać w komputerach przedsiębiorstwa pomimo ogólnych obostrzeń. Wyjątki mogą być oparte o jedno z poniższych kryteriów.

- **Zastosuj identyfikator nośnika**: Program może wygenerować identyfikator konkretnego nośnika danych (np. pendrive'a lub dysku zewnętrznego) i stosować go jako cechę rozpoznawczą.
- **Zastosuj identyfikator urządzenia**: Inna możliwość to skonfigurowanie jako wyjątek urządzenia w oparciu o jego identyfikator sprzętowy.

Aby skonfigurować wyjątek kliknij przycisk nowy pod oknem wyjątków. Aby wyszukać urządzenie, kliknij przycisk **...**, wskaż, czy chcesz wyszukać urządzenie w lokalnym, czy innym komputerze i wybierz rodzaj wyjątku.

Kontrola treści

Filtr treści internetowych umożliwia zarządzanie dostępem do stron internetowych. Gotowe zestawy kategorii stron w połączeniu z białą i czarną listą to elastyczne narzędzie kontroli treści stron przeglądanych przez Twoich pracowników. Zestaw kategorii działa w trybie białej listy, czyli zaznaczenie danej pozycji odblokowuje dostęp do stron internetowych tej kategorii.

Poniżej dostępne są przyciski umożliwiające skonfigurowanie dodatkowych dozwolonych i niedozwolonych stron poprzez ręczne wprowadzanie adresów.

Obostrzenia mogą dotyczyć użytkowników z ograniczonym dostępem lub zarówno użytkowników jak i administratorów komputerów.

Jeśli użytkownik spróbuje otworzyć stronę, do której nie ma dostępu, system pokaże mu odpowiedni komunikat.

Jeżeli administrator włączy możliwość zgłaszania próśb o odblokowanie stron, użytkownik dodatkowo zobaczy okno dialogowe umożliwiające wysłanie prośby o odblokowanie konkretnej strony internetowej. Administrator może odmówić dostępu lub na niego zezwolić jednocześnie przesyłając do użytkownika komunikat, którego treść może każdorazowo modyfikować.

Raporty składnika PolicyManager mogą być również przesyłane na adres mailowy skonfigurowany wraz z serwerem poczty w oknie Powiadomień.

Biała lista

Za pomocą białej listy stron internetowych można zdefiniować listę dozwolonych stron, niezależnie od ustawień blokowania stron według kategorii. Kliknij przycisk Dozwolone..., i wpisz ręcznie adresy URL stron, które chcesz odblokować.

Czarna lista

Przy użyciu czarnej listy stron internetowych można zdefiniować listę blokowanych stron, niezależnie od ustawień kategorii. Kliknij przycisk Niedozwolone..., i wpisz ręcznie adresy URL stron, które chcesz zablokować.

Dostęp do internetu

To narzędzie pozwala określić precyzyjnie, kiedy i jak długo pracownicy mogą korzystać z internetu w celu przeglądania stron. Okno po lewej stronie umożliwia precyzyjne określenie w jakich godzinach których dni tygodnia chcesz udostępnić internet pracownikom. Zaznacz myszą wybrany obszar i z menu kontekstowego wybierz opcję, którą chcesz zastosować dla zaznaczonego przedziału czasowego.

Zaznaczając opcję Kontroluj czas dostępu do internetu po prawej stronie włączasz licznik czasu sumujący całkowity czas spędzany w internecie w danym dniu, tygodniu, czy miesiącu. Przesuwając suwaki możesz określić limity na korzystanie z przeglądarek w danych przedziałach czasowych.

Uwaga: Zawsze obowiązuje najbardziej restrykcyjny limit. Jeśli ograniczysz czas korzystania z przeglądarek do 4 dni w miesiącu i jednocześnie do 5 dni w tygodniu, zastosowany zostanie tylko limit 4 dni w miesiącu, jako bardziej restrykcyjny.

Jeśli użytkownik komputera spróbuje otworzyć przeglądarkę w czasie, kiedy internet nie jest udostępniony, zamiast strony internetowej zobaczy komunikat o zablokowaniu dostępu do Internetu.

4.2.3.12 Zakładka Firewall

Ta zakładka umożliwia zarządzanie ustawieniami zapory połączeń sieciowych na poszczególnych stacjach roboczych lub w ich grupach. Do wyboru są dwa widoki z rozwijanej listy. Pierwszy z nich przedstawia ogólne ustawienia zapory zaznaczonej stacji roboczej, drugi zaś umożliwia zarządzanie zestawami reguł zapory.

Ustawienia

Okno ustawień zapory umożliwia modyfikację kluczowych opcji dla wybranej stacji roboczej:

- **Zapora włączona**: Wyłączenie tej opcji spowoduje wyłączenie zapory na stacji roboczej.
- **Zgłaszaj zablokowane aplikacje**: Ta opcja włącza automatyczne raportowanie administratorowi o aplikacjach zablokowanych przez zaporę na danej stacji roboczej.
- **Użytkownik może włączać/wyłączać Firewalla**: Ta opcja nadaje/odbiera użytkownikowi stacji roboczej uprawnienie do wyłączania/włączania zapory. Jest to możliwe dopóki stacja robocza jest podłączona do sieci przedsiębiorstwa z działającym składnikiem G DATA ManagementServer.
- **Zastosuj konfigurację offsite dla mobilnych komputerów**: W trybie offsite, zestawy reguł skonfigurowane administracyjnie zostają automatycznie zastąpione predefiniowanymi zestawami reguł wbudowanymi w zaporę po stronie stacji roboczej. Tryb offsite włącza się w momencie odłączenia stacji roboczej od sieci przedsiębiorstwa. Po ponownym połączeniu z siecią, w której funkcjonuje składnik G DATA ManagementServer, zastosowane zostaną ponownie zdalnie dystrybuowane zestawy reguł.
- **Użytkownik może modyfikować konfigurację offsite**: Zaawansowanym użytkownikom można nadać uprawnienie do samodzielnej modyfikacji i konfiguracji ustawień zapory podczas gdy stacja nie jest połączona z siecią przedsiębiorstwa. Po ponownym połączeniu z siecią, w której funkcjonuje składnik G DATA ManagementServer, zastosowane zostaną ponownie zdalnie dystrybuowane zestawy reguł.

Konfigurację offsite można włączyć tylko na stacjach roboczych, które działają w trybie zestawów reguł. Nie da się z niej skorzystać przy włączonym autopilocie. Jeśli autopilot jest włączony, będzie funkcjonować nadal także po odłączeniu od sieci przedsiębiorstwa.

Poniżej znajduje się zestawienie stacji roboczych zaznaczonych w drzewku po lewej stronie wraz z podstawowymi informacjami na temat stanu zapory i stacji w następujących kolumnach:

- **Komputer**: Nazwa stacji roboczej.
- **Firewall**: Stan zapory, czyli czy jest ona zainstalowana, włączona lub wyłączona.
- **Autopilot/Zestawy reguł**: W tej kolumnie znajdziesz informację, czy dla wskazanej stacji zastosowane jest tryb autopilota, czy też indywidualnie konfigurowany tryb zestawów reguł.
- **Konfiguracja offsite**: W trybie offsite użytkownik stacji roboczej może samodzielnie zarządzać ustawieniami zapory, o ile stacja (np. komputer przenośny) znajduje się poza siecią przedsiębiorstwa.

Uwaga: Konfiguracja offsite może zostać włączona w momencie, kiedy na danej stacji wyłączony jest tryb autopilota.

Zestawy reguł czy autopilot?
Istnieją dwa różne tryby pracy zapory.

- **Autopilot**: Zapora działa automatycznie. Podstawowe aplikacje są skonfigurowane domyślnie jako uprawnione do łączenia się z Internetem. Użytkownik nie musi zatwierdzać uciążliwych pytań o pozwolenie dla każdej aplikacji. W tym trybie nie działa opcja konfiguracji offsite.
- **Zestawy reguł**: Administrator może włączyć tryb zestawów reguł i skonfigurować zestaw aplikacji na podstawie listy najczęściej używanych programów i portów. Można utworzyć więcej zestawów reguł na potrzeby różnych sieci, podsieci, czy użytkowników.

Menu kontekstowe wyświetlane po kliknięciu danej stacji prawym klawiszem umożliwia wykonanie dodatkowych poleceń:

- **Utwórz zastaw reguł**: Polecenie wyświetla widok zestawów reguł z otwartym oknem kreatora zestawu.
- **Edytuj zestaw reguł**: Polecenie wyświetla widok zestawów reguł, gdzie możliwe jest modyfikowanie utworzonych wcześniej zestawów.
- **Wybierz zestaw reguł**: Otwiera okno umożliwiające wybranie i zastosowanie zestawu reguł z listy gotowych zestawów. Dodatkowo okno umożliwia przełączenie trybu działania zapory z zestawów reguł na autopilota.
- **Zainstaluj zaporę**: Polecenie umożliwia zainstalowanie zapory na zdalnym komputerze.
- **Odinstaluj Firewall**: Ta funkcja zdalnie odinstalowuje zaporę ze stacji roboczej.

Zestawy reguł

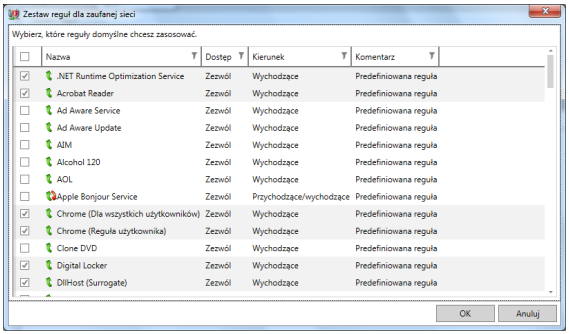
Widok Zestawy reguł umożliwia tworzenie, modyfikowanie i usuwanie zestawów reguł. Po zainstalowaniu składnika ManagementServer na liście nie ma żadnych zestawów. Edytowanie i tworzenie zestawów możliwe jest poprzez użycie przycisków **Nowy...**, **Edycja...**, **Usuń...**, **Import...** i **Export...**.

Nowy zestaw reguł

Aby utworzyć nowy zestaw kliknij przycisk **Nowy...** w sekcji **Zestaw reguł**. W oknie kreatora zestawów reguł wpisz nazwę dla zestawu i komentarz. Możesz też użyć opcji **Tryb ukrycia**, jeśli nie chcesz, aby adres IP stacji roboczej był widoczny w sieci.

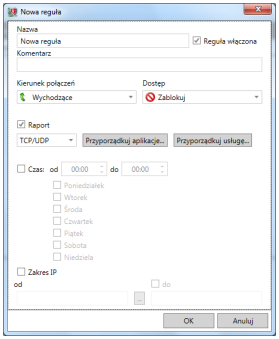
W następnym oknie kreatora możesz zaznaczyć dodatkowe reguły dla aplikacji, które mogą łączyć się z Internetem. Domyślnie zaznaczone są najbardziej popularne aplikacje i porty niezbędne do pracy w sieci.

Każdy utworzony zestaw reguł można dowolnie edytować, zmieniając ustawienia lub wyłączając i włączając reguły. Można także modyfikować poszczególne reguły za pomocą przycisków po prawej stronie. W razie potrzeby można modyfikować również kolejność stosowania reguł.



Tworzenie/edycja reguł

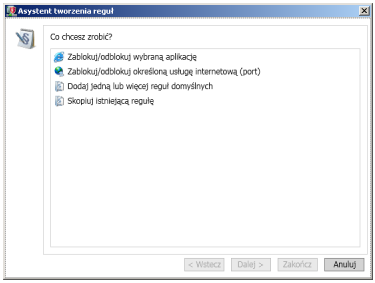
Okno edycji reguły zawiera następujące pola, przyciski i rozwijane listy umożliwiające utworzenie nowej lub zmodyfikowanie istniejącej reguły:



- **Nazwa:** W regułach predefiniowanych jest to nazwa aplikacji której dotyczy reguła. Nazwę można zmieniać i uzupełniać.
- **Reguła włączona:** Można wyłączyć działanie reguły poprzez odznaczenie tego pola.
- **Komentarz:** Pole informuje w jaki sposób reguła została utworzona. Reguły predefiniowane oznaczone są komentarzem Domyślna reguła, natomiast w przypadku reguł tworzonych na podstawie zapytań w tej rubryce widnieje tekst Generowane poprzez zapytanie. Wprowadź własny komentarz dla reguł generowanych ręcznie.
- **Kierunek połączeń:** To ustawienie definiuje, czy chodzi w danym przypadku o regułę dla połączeń wychodzących, przychodzących czy dla obydwu rodzajów.
- **Dostęp:** To pole określa, czy reguła ma blokować, czy akceptować połączenia.
- **Protokół:** Wybór protokołu umożliwia zdefiniowanie ogólnej reguły dla całego protokołu, bez względu na aplikację, czy port.
- **Czas:** Reguły mogą być także aktywne tylko w czasie określonym w tej sekcji. W ten sposób można ograniczyć dostęp konkretnych aplikacji do sieci np. tylko do czasu pracy.
- **Zakres IP:** Reglamentacja dostępu do sieci staje się prostsza szczególnie w przypadku sieci z przydzielonymi stałymi adresami IP.

Asystent tworzenia reguł

Przy pomocy Asystenta tworzenia reguł użytkownik może zdefiniować określone dodatkowe reguły danego zestawu reguł lub zmodyfikować istniejące reguły. Asystent tworzenia reguł umożliwia podjęcie następujących działań:



- **Akceptuj lub blokuj dostęp wybranej aplikacji**: Możesz wskazać program (plik) i zezwolić lub zablokować jej dostęp do sieci. W polu Kierunek połączenia wskazać czy wybrany program ma zostać zablokowany dla połączeń wychodzących, przychodzących czy w obydwu kierunkach. W ten sposób użytkownik zapory może np. uniemożliwić aplikacji do odtwarzania muzyki łączenie się ze zdalnym serwerem i pobieranie aktualizacji.
- **Udostępnij lub zablokuj usługę (port)**: Porty przekazują aplikacjom dane za pośrednictwem określonych protokołów. Przesyłanie danych ze stron internetowych odbywa się poprzez port 80, wysyłanie poczty elektronicznej przez port 25, odbieranie poczty elektronicznej przez port 110 itd. W komputerze bez zapory wszystkie porty używane przez aplikacje są generalnie otwarte, chociaż zazwyczaj zwykli użytkownicy ich nie wykorzystują. Blokując jeden lub kilka portów, można w szybki sposób zamknąć luki bezpieczeństwa, które mogłyby być wykorzystane przez hakerów lub wirusy. Przy pomocy Asystenta tworzenia reguł można zablokować wszystkie lub tylko niektóre porty (np. tylko dla wybranych programów).
- **Dodaj reguły domyślne**: Umożliwia dodanie reguł z ogólnej listy do domyślnego zestawu stosowanego podczas tworzenia zestawu reguł.
- **Skopiuj istniejącą regułę**: Umożliwia wykonanie kopii istniejącej reguły.

4.2.3.13 Zakładka PatchManager

Składnik PatchManager służy do zarządzania poprawkami związanymi z bezpieczeństwem stacji. Poza aktualizacjami Windows umożliwia aktualizowanie przeglądarek internetowych, a także oprogramowania Java i Flash Player. Program umożliwia weryfikację, czy w danym systemie poprawki

mają zastosowanie. Można stosować czarne listy poprawek, instalować/ deinstalować je zdalnie na stacjach i grupach stacji.

Widok

Tu znajdziesz zestawienie wszystkich poprawek wraz z szczegółowymi informacjami. Można się z zestawienia dowiedzieć, czy komputery dysponują dostępnymi poprawkami. Z tego miejsca możliwe jest zaplanowanie dystrybucji poprawek.

Lista poprawek wyświetlana jest w porządku alfabetycznym. Opcje filtrowania pomagają w efektywnym zarządzaniu poprawkami:


Odśwież: Odświeża listę poprawek i informacji.


Ukryj poprawki na czarnej liście: Ukrywa poprawki, które zostały przeniesione na czarną listę w widoku Poprawki.


Pokaż tylko poprawki: Domyślnie wyświetlane są zarówno aktualizacje jak pełne wersje programów. Zastosuj tę funkcję, jeśli chcesz ukryć pełne wersje.

Przy pomocy funkcji dostępnych w menu kontekstowym prawego klawisza, możesz sprawdzić, czy poprawki mają zastosowanie na konkretnej stacji, a także uruchomić i zaplanować zlecenie dystrybucji lub deinstalacji poprawek. Polecenie właściwości wyświetla dostępne informacje o poprawce.

Kolumna Status informuje o stanie poprawki oraz o zaplanowanych dla niej zleceniach.

Ustawienia

Zakładka Ustawienia umożliwia włączenie i wyłączenie składnika PatchManager na stacjach.

Uprawnienia stacji

Ta sekcja umożliwia zarządzaniem uprawnieniami użytkownika.

- **Użytkownik może wyświetlać i żądać instalacji poprawek**: Umożliwia zgłaszanie potrzeby instalacji danych poprawek do składnika Administrator.
- **Użytkownik może odrzucać poprawki**: Umożliwia opóźnienie instalacji poprawek przez użytkownika, ale tylko do pewnego momentu. Użytkownik nie ma możliwości całkowitego zablokowania implementacji poprawek.

Poprawki

W tej zakładce masz możliwość podejrzenia większej ilości informacji na temat dostępnych poprawek.

Lista jest podobna do tej w zakładce Widok, ale nie pokazuje kolumny statusu.

 Odśwież: Odświeża listę poprawek i informacji.

 Ukryj poprawki na czarnej liście: Ukrywa poprawki, które zostały przeniesione na czarną listę w widoku Poprawki.

 Pokaż tylko poprawki: Domyślnie wyświetlane są zarówno aktualizacje jak pełne wersje programów. Zastosuj tę funkcję, jeśli chcesz ukryć pełne wersje.

Przy pomocy funkcji dostępnych w menu kontekstowym prawego klawisza, możesz sprawdzić, czy poprawki mają zastosowanie na konkretnej stacji, a także uruchomić i zaplanować zlecenie dystrybucji lub deinstalacji poprawek. Polecenie właściwości wyświetla dostępne informacje o poprawce.

W tej zakładce możesz również oznaczać poprawki jako przeniesione na czarną listę, oraz usuwać je z czarnej listy. Funkcja Właściwości spod prawego klawisza myszy pokazuje szczegółowe informacje o poprawce - licencja, suma kontrolna MD5, link do opisu poprawki na stronie producenta, itp.

W razie potrzeby można zmodyfikować priorytet stosowania poprawek w kolumnie o nazwie Priorytet.

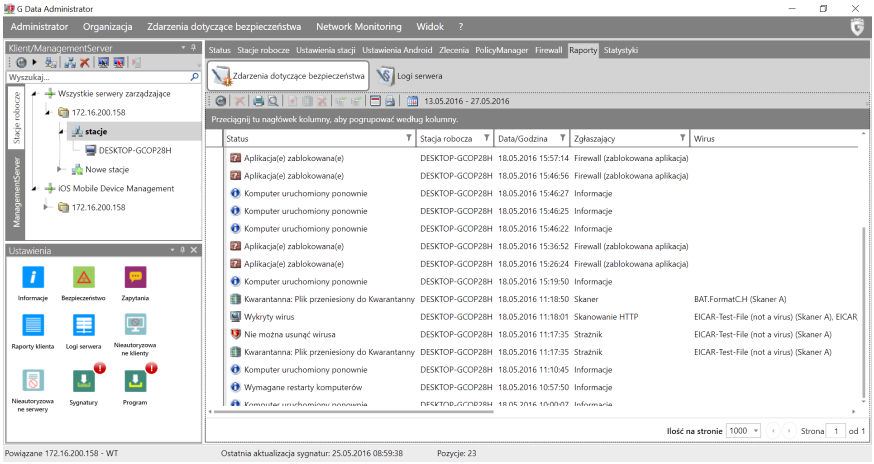
4.2.3.14 Zakładka Raporty

Zakładka raporty udostępnia widok zdarzeń dotyczących bezpieczeństwa oraz widok logów serwera.

Zdarzenia dotyczące bezpieczeństwa

W tym widoku wyświetlane są zdarzenia dotyczące wykrytych zagrożeń, a także zapytań składników PolicyManager, PatchManager i Firewall. Ponadto do wglądu mamy też raporty dotyczące instalacji, restartów komputerów i problemów z działaniem klienta na chronionych komputerach.

Z poziomu okna raportów możliwe również kontekstowe reagowanie na zagrożenia i zapytania. Zaznacz jeden lub więcej raportów i kliknij zaznaczenie prawym klawiszem myszy aby zastosować bezpośrednio reakcję z menu kontekstowego.



Opcje menu kontekstowego dostepne są również przez pasek ikon lub polecenia menu ponad obszarem roboczym:

- **Widok**: Umożliwia ukrywanie/wyświetlanie powiazanych i przeczytanych raportów.
- **Usuń wirusa z pliku**: Program spróbuje usunąć ciało wirusa z zarażonego pliku.
- **Przenieś plik do Kwarantanny**: Przenosi zarażony plik do zaszyfrowanego folderu Kwarantanny. Raporty są powiązane z plikami w Kwarantannie. Usunięcie raportu powoduje jednocześnie usunięcie pliku z Kwarantanny.
- **Usuń plik**: Powoduje usunięcie zarażonego pliku.
- **Zdefiniuj jako wyjątek Strażnika...**: Tworzy wyjątek ochrony rezydentnej na podstawie zarażonego pliku (lista wyjątków jest dostępna w ustawieniach stacji > Strażnik > wyjątki Strażnika).
- **Zdefiniuj jako wyjątek ExploitProtection**: Tworzy wyjątek ochrony przed exploitami na podstawie zarażonego pliku (lista wyjątków jest dostępna w ustawieniach stacji > Strażnik > wyjątki ExploitProtection.
- **Cofnij zezwolenie na klawiaturę**: Wycofuje zgodę na stosowanie klawiatury zgłoszonej przez moduł USB Keyboard Guard i odblokowanej wcześniej przez użytkownika.
- **Kwarantanna: Oczyść i przywróć**: Próbuje usunąć zagrożenie z pliku. Jeśli to się uda, przywraca plik do pierwotnej lokalizacji. Jeżeli nie da się oczyścić pliku, plik nie zostanie przywrócony.
- **Kwarantanna: Przywróć**: Przywraca plik do pierwotnej lokalizacji. Uwaga:

Pliki są przywracane w oryginalnym stanie i mogą zawierać niebezpieczny kod.

- **Kwarantanna: Wyślij do G DATA Security Labs**: Polecenie umożliwia dyskretne przekazanie wykrytego zagrożenia do zbadania w naszych laboratoriach. Opcja może być przydatna w przypadku podejrzenia o fałszywą detekcję.
- **Kwarantanna: Usuń plik i raport:** Usuwa zaznaczone raporty wraz z przynależnymi plikami w Kwarantannie.
- **URL na białą listę**: Dodaje adres URL z raportu do białej listy.
- **URL na czarną listę**: Dodaje adres URL z raportu do czarnej listy.
- **Usuń raport...**: Usuwa zaznaczone raporty. Jeśli zaznaczony raport dotyczy Kwarantanny i powiązanego z nim pliku, program zażąda potwierdzenia usunięcia raportu.
- **Porządkuj raporty...**: Usuwa duplikaty raportów (bazując na polach klient, zgłaszający oraz plik/wiadomość/treść).

Opcja porządkowania bieże pod uwagę jedynie raporty wyświetlone w bieżacym widoku. Raporty ukryte przez filtrowanie nie zostaną usunięte. Bez zmian pozostaną również raporty znajdujące się na kolejnych stronach obszaru roboczego.

- **Eksportuj raporty...**: Eksportuje raporty do pliku XML.
- **Zaznacz jako przeczytane**: Oznacza raporty jako przeczytane zmieniając pogrubienie czcionki.
- **Zaznacz jako nieprzeczytane**: Oznacza raporty jako nieprzeczytane zmieniając pogrubienie czcionki.
- **Szczegóły/Działania**: Otwiera okno działań kontekstowych dostępnych dla danego typu raportu (żadania PolicyManager, Firewall, PatchManager).

Objaśnienia ikon paska zadań:

 Odśwież

 Usuń

 Drukuj

 Widok strony

 Usuń wirusa

 Przenieś do Kwarantanny

 Usuń plik

 Przywróć plik z Kwarantanny

 Oczyść plik i przywróć z Kwarantanny

 Ukryj powiązane raporty

 Ukryj przeczytane raporty

 Przedział czasowy

Logi serwera

Widok logów serwera udostępnia przegląd zdarzeń powiazanych z działaniem serwerów zarządzających (aktualizacje, statusy zleceń, zmiany ustawień, błędy).

Objaśnienia ikon paska zadań:

 Odśwież

 Usuń

 Drukuj

 Widok strony

 Ukryj przeczytane raporty

 Przedział czasowy

4.2.3.15 Zakładka Raporty (iOS)

Widok raportów przedstawia pozycje dotyczące stanu zarządzania profilami oraz akcji antykradzieżowych.

- Status: Status raportu.
- Stacja robocza: Nazwa urządzenia.
- Data/Godzina: Czas utworzenia raportu.

Raport można usunąć za pomocą odpowiedniego polecenia z menu kontekstowego prawego klawisza myszy.

4.2.3.16 Zakładka statystyki

Widok zawiera statystyki dotyczące ataków wirusów. Można przejrzeć ogólne informacje dotyczące relacji składnika ManagementServer i klientów, a także dane o najczęściej występujących wirusach i najczęściej atakowanych komputerach. Istnieje możliwość graficznego przedstawienia statystyk w postaci wykresów. W tym celu należy kliknąć ostatni przycisk w pasku narzędzi.

4.2.4 Sekcja ManagementServer

Wybierz sekcję ManagementServer aby wyświetlić moduły i opcje dostępne dla serwerów w obszarze roboczym.

4.2.4.1 Zakładka Serwer

Zakładka Serwer umożliwia przegladanie ogólnych informacji o serwerach, zarządzanie dostępem do konsoli G DATA Administrator oraz przeglądanie logów serwerów.

Ustawienia

Widok ustawień zawiera zestaw ogólnych informacji o serwerach zarządzających. Dostępne są parametry ujawniające nazwy serwerów, ich rodzaj, ilość podłączonych klientów, nr wersji i wiele innych.

Objaśnienie ikon paska narzędzi i poleceń menu:

- **Odśwież**: Odświeża bieżący widok
- **Asystent konfiguracji serwera**: Uruchamia kreator ustawień pierwszego uruchomienia.
- **Usuń**: Usuwa z listy zaznaczony serwer. Ta operacja nie powoduje odinstalowania oprogramowania z komputera.
- **Synchronizacja**: Wymusza uzgodnienie ustawień i transfer danych między serwerem głównym a serwerami podrzędnymi.
- **Przyporządkuj stacje**: Umożliwia przydzielanie klientów do serwerów podrzędnych. Przyporządkowanie jest faktem niezależnym od przynależności klientów do grup w drzewach poszczególnych serwerów.
- **Zainstaluj serwer podrzędny**: Umożliwia zdalne zainstalowanie serwera

podrzędnego. Wybierz komputer z listy i wprowadź poświadczenia z uprawnieniami administratora. Zatwierdź przyciskiem OK, aby rozpocząć zdalną instalację. Proces instalacji można śledzić w oknie Przegląd instalacji. Wymagania zdalnej instalacji są identyczne jak w przypadku wymagań dla zdalnej instalacji klienta. Do zdalnej instalacji stosowany jest instalator serwera Microsoft SQL Server 2014 Express, który nie obsługuje systemów operacyjnych Windows Vista i Windows Server 2008/2003. W starszych systemach operacyjnych zalecana jest ręczna instalacja instancji serwera podrzędnego po uprzednim zainstalowaniu odpowiedniej wersji serwera SQL.

- **Odinstaluj serwer**: Umożliwia zdalne odinstalowanie serwera podrzędnego. Proces można śledzić w oknie Przegląd instalacji. Deinstalacja będzie funkcjonować tylko w odniesieniu do serwerów podrzędnych, które zostały autoryzowane w konsoli G DATA Administrator serwera głównego.
- **Przyznaj autoryzację**: Serwery podrzędne zainstalowane ręcznie wymagają przeprowadzenia ręcznej autoryzacji przez administratora.

  Serwery podrzędne instalowane zdalnie są automatycznie autoryzowane.
- **Zezwól na aktualizowanie plików programu**: Serwery podrzędne w wersji 12 wymagają ręcznego doinstalowania serwera baz danych przed podniesieniem do wersji 14. Najpierw zainstaluj w serwerach podrzędnych serwer Microsoft SQL Server 2014 Express (Windows Server 2008 R2/ Windows 7 i nowsze) ew. Microsoft SQL Server 2008 R2 Express (Windows Server 2003/2008/Windows Vista). Zezwól na aktualizowanie plików programu. Bezpośrednio po dokonaniu aktualizacji skonfiguruj dostęp serwerów podrzędnych do bazy danych za pomocą narzędzia **GdmmsConfig.exe**. Więcej informacji znajdziesz w dokumencie Reference Guide.
- **Właściwości**: Właściwości serwera zarządzającego, np. wersja oprogramowania, sygnatur wirusów i plików klienta w repozytorium.

Asystent konfiguracji

Przy pierwszym uruchomieniu programu automatycznie otwiera się okno asystenta. Asystent pomaga w instalacji i konfiguracji klienta. Można go wywołać także później z menu Administrator > Asystent konfiguracji serwera.

Aktywacja

W pierwszej kolejności należy uaktywnić wszystkie komputery, które mają zostać objęte ochroną. Zaznacz stację roboczą na liście i kliknij przycisk Uaktywnij. Jeśli jakiegoś komputera nie ma na liście, np. mógł przez dłuższy czas pozostawać wyłączony, wpisz w polu Komputer jego nazwę i kliknij przycisk Uaktywnij (nazwa). Komputer zostanie wciągnięty na listę. Kiedy wszystkie końcówki są już aktywne, kliknij Dalej.

Instalacja

Zaznacz opcję instalacji, jeśli chcesz automatycznie instalować moduł kliencki na aktywowanych stacjach.

Aktualizacja

ManagementServer może pobierać aktualizacje plików i sygnatur wirusów z Internetu. Proces aktualizacji można zautomatyzować. Wpisz w odpowiednie pola dane dostępu otrzymane po zarejestrowaniu programu. Szczegółowy opis planowania aktualizacji i ustawień z nią związanych znajdziesz w rozdziale Aktualizacja.

Powiadomienia

ManagementServer może powiadamiać wskazanych adresatów o różnych zdarzeniach za pomocą poczty elektronicznej. Można ograniczyć ilość wysyłanych wiadomości, żeby nie przepełniać skrzynki pocztowej w przypadku infekcji większej ilości plików.

Zarządzanie użytkownikami

Za pomocą tego polecenia, administrator systemu może utworzyć lub zmodyfikować zintegrowane konta dostępu do interfejsu obsługi programu ManagementServer. Aby utworzyć nowe konto kliknij przycisk Nowe, wpisz nazwę użytkownika i hasło, a następnie określ poziom dostępu użytkownika (odczyt/zapis lub tylko odczyt).

Logi serwera

Widok logów serwera udostępnia przegląd zdarzeń powiazanych z działaniem serwerów zarządzających (aktualizacje, statusy zleceń, zmiany ustawień, błędy). Widok jest identyczny jak ten z sekcji Stacje robocze.

4.2.4.2 Zakładka Ogólne ustawiania

Ogólne ustawienia umożliwiają m. in. zarządzanie automatycznym usuwaniem logów i raportów, synchronizacją i ograniczeniem obciążenia sieci w większych jednostkach. Widok **e-mail** pozwala na skonfigurowanie ustawień poczty niezbędnych do wysyłki powiadomień z programu G DATA.

Oczyszczanie

Wszystkie raporty i logi programu G DATA są przechowywane w bazie danych. Istnieje możliwość ustawienia automatu usuwającego przestarzałe raporty po upływie określonego czasu. W widoku **Oczyszczanie** można ustawić parametry automatycznego usuwania raportów oraz interwały czasowy.

- **Automatycznie usuwaj logi serwera**: Włącz opcję, jeśli chcesz usuwać automatycznie pozycje szczegółowego protokołu serwera zarządzającego.
- **Automatycznie usuwaj raporty skanowania**: Ta opcja powoduje automatyczne usuwanie raportów od klientów dotyczących skanowania.
- **Automatycznie usuwaj zdarzenia dot. bezpieczeństwa**: Automatyczne usuwanie powiadomień dotyczących zagrożeń i problemów z klientami.
- **Automatycznie usuwaj historię raportów**: Automatyczne usuwanie historii raportów składnika **RaportManager**.
- **Usuwaj stacje po okresie braku aktywności**: Usuwa stacje, które nie logują się do serwera przez określony czas z drzewa sieci.
- **Automatycznie usuwaj pliki poprawek**: Usuwa nieużywane pliki poprawek modułu PatchManager.

Synchronizacja

Ta zakładka umożliwia zdefiniowanie parametrów dotyczących komunikacji między stacjami, serwerami podrzędnymi i serwerem głównym programu:

- **Stacje robocze:** W tej sekcji można określić regularność synchronizacji stacji roboczych z serwerem zarządzającym. Po zaznaczeniu opcji Powiadamiaj stacje robocze o modyfikacjach ustawień, użytkownik stacji będzie informowany komunikatem o każdej zmianie ustawień wykonanej zdalnie.
- **Serwery podrzędne:** W tej sekcji określone są interwały czasowe synchronizacji ustawień i sygnatur wirusów między Serwerem głównym, a Serwerami podrzędnymi. Zaznaczenie opcji Przenoś na bieżąco nowe raporty na serwer główny, spowoduje zsynchronizowanie nowych raportów w momencie ich powstawania, niezależnie od powyższych ustawień.
- **Active Directory:** W tej sekcji możesz odczytać informację o czasie ostatniej synchronizacji serwera z usługą Active Directory, a także skonfigurować interwał czasowy tego procesu. Synchronizacja z Active Directory odbywa się tylko wtedy, kiedy przynajmniej jedna grupa stacji została skojarzona z usługą Active Directory.

Ograniczanie obciążenia

Opcja **Włącz ograniczenie obciążenia** umożliwia skonfigurowanie progowej ilości połączeń do serwera zarządzającego w zależności od rodzaju połączenia.

Backup

Sekcja przydział miejsca pozwala zdefiniować wartości progowe dla ostrzeżeń i komunikatów błędów wyświetlanych w momencie wykrycia, że wolne miejsce na dysku się kończy lub jego ilość jest mniejsza niż zadana wartość.

Jeśli ilość wolnego miejsca osiągnie zadaną wartość np. dla komunikatów błędów na stacji roboczej, starsze kopie będą usuwane, żeby zrobić miejsca dla nowszych. Usuwana zawsze jest najstarsza kopia zapasowa (zasada FIFO).

W sekcji foldery kopii na serwerze można ustalić folder lub foldery, w których mają być przechowywane kopie zapasowe danych ze stacji roboczych. Jeśli folder nie zostanie wskazany, domyślnie ustawiona jest wartość C:\ProgramData\G DATA\ManagementServer\Backup lub C:\Documents and settings\All Users\Dane Aplikacji\G DATA\ManagementServer\Backup.

Ponieważ wszystkie kopie zapasowe są szyfrowane, program umożliwia wyeksportowanie hasła szyfrującego do zapisania.

Okno ustawień kopii umożliwia również zaimportowanie do programu kopii zapasowych przechowywanych w innych lokalizacjach.

e-mail

W przypadku wykrycia wirusa serwer zarządzający może automatycznie wysyłać powiadomienia za pomocą poczty elektronicznej. Niezbędnych w tym celu ustawień dokonujemy w oknie Powiadomienia.

Uaktywnij opcję powiadamiania przez e-mail w dolnej części okna i wpisz adres odbiorcy komunikatów. Warto ustalić ograniczenie ilościowe, aby skrzynka nie przepełniła się w przypadku dużej ilości zarażonych plików.

Aby skonfigurować serwer poczty do wysyłki powiadomień, kliknij przycisk otwierający okno edycji ustawień poczty ( ).

Ustawienia e-mail

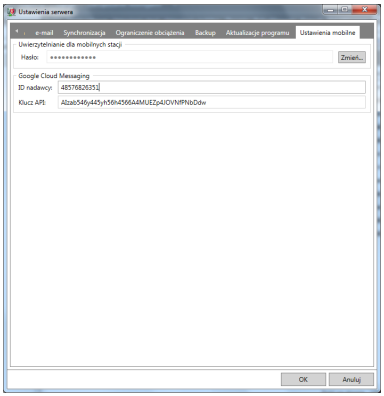
Wpisz nazwę serwera poczty oraz numer portu SMTP (zazwyczaj 25). Kliknij przycisk Uwierzytelnianie SMTP aby wpisać dane dostępu do serwera SMTP. Wybierz metodę uwierzytelniania i wpisz dane dostępu. Następnie potrzebny będzie działający adres poczty elektronicznej, aby można było z niego przesyłać wiadomości. Na ten adres będą nadchodzić odpowiedzi na zgłoszenia plików do Ambulansu. Na ten adres będą nadchodzić odpowiedzi na zgłoszenia plików do Ambulansu.

Możesz skonfigurować grupy odbiorców powiadomień mailowych, którzy będą otrzymywać informacje na temat zdarzeń dotyczących działania programu.

Android

Zakładka globalnych ustawień dla urządzeń mobilnych umożliwia wprowadzenia hasła uwierzytelniania klientów mobilnych zainstalowanych w urządzeniach. To samo hasło należy wprowadzić ręcznie w każdym urządzeniu po zainstalowaniu klienta G DATA Internet Security for Android. Instalacja opisana jest w rozdziale Instalacja składnika Internet Security for Android.

Ponadto w tym miejscu można wprowadzić dane konfiguracyjne usługi **Google Cloud Messaging** niezbędne do komunikacji z urządzeniami poza siecią lokalną.



Aby umożliwić wysyłanie do urządzeń poleceń awaryjnych związanych z ochroną przed kradzieżą, niezbędne jest wprowadzenie parametrów Sender ID oraz API Key z Twojego konta Google Cloud Messaging.

Wskazówka: Konto można założyć bezpłatnie na stronie code.google.com/apis/console. Szczegółowe informacje dostępne są w dokumencie Reference Guide.

4.2.4.3 Zakładka Aktualizacje

To okno umożliwia dokonanie ustawień dotyczących aktualizacji plików składnika Security Client oraz sygnatur wirusów. W zakładce Dane dostępu i ustawienia wpisz dane dostępu do aktualizacji otrzymane w potwierdzeniu rejestracji programu. Aktualizacje pobierane są z serwera aktualizacji i przechowywane lokalnie przez moduł ManagementServer. Aktualizowanie baz sygnatur wirusów oraz plików programu to podstawa ochrony antywirusowej. Oddzielnym tematem jest aktualizacja plików składnika ManagementServer. Możliwe jest to tylko metodą ręczną poprzez aplikację Internet Update.

Sygnatury wirusów

Klienci wyposażeni są własne kopie baz sygnatur wirusów. Aktualizacja baz wirusów przebiega w dwóch etapach, oba z nich można zautomatyzować. Pierwszy krok to pobranie plików z serwera aktualizacji do repozytorium składnika ManagementServer. Potem pliki są przekazywane do stacji roboczych (patrz zakładka Stacje robocze).

- **Odśwież status:** Przycisk odświeża widok okna. Wczytuje bieżące ustawienia z serwera zarządzającego.
- **Uaktualnij teraz...:** To polecenie wymusza ręczne pobranie aktualizacji sygnatur wirusów do repozytorium składnika ManagementServer.
- **Automatyczne aktualizacje...:** Podobnie jak skanowanie, proces aktualizacji sygnatur wirusów można zautomatyzować. W tym celu kliknij przycisk Automatyczne aktualizacje.

Aby program mógł pobierać aktualizacje serwer musi być połączony z Internetem. Jeżeli jest to konieczne, wprowadź w zakładce Dane dostępu i ustawienia dane konta użytkownika i ustawienia proxy.

Pliki programu

Aktualizacja plików składnika Security Client również przebiega w dwóch etapach, i także w tym przypadku oba z nich można zautomatyzować.

Pierwszy krok to pobranie plików z serwera aktualizacji do repozytorium składnika ManagementServer. Drugi krok to przekazanie aktualizacji do stacji roboczych.

- **Odśwież:** Przycisk odświeża widok okna. Wczytuje bieżące ustawienia z serwera zarządzającego.
- **Uaktualnij teraz...:** To polecenie wymusza ręczne pobranie aktualizacji plików klienta do repozytorium składnika ManagementServer.

- **Automatyczne aktualizacje...:** Podobnie jak skanowanie, proces aktualizacji plików klienta można zautomatyzować. W tym celu kliknij przycisk Automatyczne aktualizacje.

Aby program mógł pobierać aktualizacje serwer musi być połączony z Internetem. Jeżeli jest to konieczne, wprowadź w zakładce Dane dostępu i ustawienia dane konta użytkownika i ustawienia proxy.

Uwaga: Aby przeprowadzić aktualizację plików programowych składnika ManagementServer uruchom aplikację Internet Update z grupie programowej składnika ManagementServer w menu Start. Jest to jedyna metoda aktualizacji serwera zarządzającego.

Stopniowe rozdzielanie

Ta zakładka umożliwia modyfikowanie konfiguracji stopniowej dystrybucji aktualizacji plików klienta na stacje robocze. Dzięki opóźnieniu instalacji aktualizacji plików klienta na części komputerów redukuje się obciążenie sieci oraz chwilowy spadek wydajności wszystkich komputerów. Program może sam zdecydować o podziale stacji na grupy. W razie potrzeby można ustalić ręcznie jedynie skład pierwszej grupy aktualizowanych komputerów. W dolnej części okna można zdecydować ile ma być grup stacji i w jakich odstępach czasu ma następować instalacja na kolejnych grupach.

Dane dostępu i ustawienia

Dane dostępu do aktualizacji baz wirusów i plików programu, czyli użytkownika i hasło otrzymasz pocztą elektroniczną po wykonaniu rejestracji online. Jeżeli bazy wirusów lub pliki programu uległy uszkodzeniu poprzez przerwanie pobierania, wyłącz na czas jednej aktualizacji opcję Kontrola wersji (zalecane) w celu pobrania wszystkich plików. Program pobierze wtedy nie uszkodzone bazy wirusów lub pliki składnika Security Client.

Uwaga: Wprowadzanie zmian w oknie ustawień serwera proxy zalecane jest tylko w przypadku problemów z połączeniem przy standardowych ustawieniach.

Aby sprawdzić dostępność połączenia z serwerem aktualizacji, wpisz w przeglądarce adres http://ieupdate.gdata.de/test.htm, i sprawdź, czy strona zwraca stosowny komunikat.

Jeżeli używasz urządzenia sieciowego wymagającego autoryzacji lub serwera proxy, kliknij przycisk Ustawienia proxy... i zaznacz opcję Skorzystaj z serwera proxy. Wpisz adres serwera i port w odpowiednich polach. Jeżeli wymagana jest autoryzacja, wpisz również nazwę użytkownika oraz hasło.

Cofnij skaner A/B

Serwer zarządzający przechowuje zadaną ilość wersji aktualizacji sygnatur wirusów. W przypadku wystąpienia fałszywych alarmów lub innych problemów z sygnaturami wirusów, jest możliwość zablokowania bieżącej aktualizacji i cofnięcia plików sygnatur do wcześniejszej, poprawnie działającej wersji.

Aby cofnąć stan danego skanera do wcześniejszej wersji, zaznacz w oknie Cofanie aktualizacji bieżącą wersję sygnatur. Jeżeli chcesz cofnąć dany skaner o 2 wersje wstecz, zaznacz bieżącą i poprzednią wersję sygnatur itd.

Jeśli komputer przenośny jest odłączony od sieci z serwerem zarządzającym, operacja cofnięcia sygnatur nie zostanie na nim wykonana. Podobnie nie będzie można anulować cofnięcia sygnatur po odłączeniu komputera od sieci.

4.2.4.4 Zakładka ReportManager

Składnik ReportManager umożliwia skonfigurowanie automatycznego generowania raportów o stanie ochrony sieci z możliwością przesyłania ich na wybrane adresy e-mail.

Odśwież: Wczytuje aktualne informacje z bazy danych serwera zarządzającego G DATA ManagementServer.

Usuń: Usuwa zaznaczone definicje raportów.

Dodaj nową definicję raportu...: Otwiera okno konfiguracji nowego raportu. Szczegóły w rozdziale Nowy raport.

Import/Eksport: Umożliwia zapisanie i wczytanie raportu do/z pliku.

Menu kontekstowe prawego klawisza myszy umożliwia usunięcie lub natychmiastowe uruchomienie zaznaczonych raportów. Edycja raportu możliwa jest poprzez dwukrotne kliknięcie pozycji lub polecenie Właściwości. Polecenie Historia umożliwia wgląd do wcześniej wygenerowanych raportów, a także ich usuwanie.

Nowy raport

Okno konfiguracji raportu umożliwia zdefiniowanie jego nazwy, języka i wybór grupy adresatów, do których ma być kierowany. Konfiguracji grup i ustawień serwera SMTP do wysyłki można dokonać bezpośrednio z tego okna, lub poprzez uruchomienie polecenia Opcje > Ustawienia serwera > Ustawienia e-mail. Pole Dodatkowi odbiorcy umożliwia ręczne wprowadzenie dodatkowych adresów wysyłkowych (większą ilość adresów oddzielamy przecinkami).

W przypadku jednorazowego raportu istnieje możliwość ustalenia terminu jego wygenerowania. W przypadku raportów periodycznych można zdefiniować harmonogram powtórzeń.

Wybrane moduły

W celu dodania składnika raportu kliknij przycisk Nowy.... Wybierz kategorię z listy rozwijanej i wskaż moduł, który chcesz dodać do definicji raportu. Każda pozycja raportu może być wyświetlona w wybranej formie. Wybierz z listy Format wyjściowy pożądaną formę raportowania. Lista dostępnych formatów zależy od rodzaju wybranego wcześniej modułu. Niektóre moduły umożliwiają ustalenie limitu wyświetlanych pozycji w celu zmniejszenia rozmiaru raportu. Kliknij OK aby dodać składnik raportu. Składniki można dowolnie usuwać i edytować. Można również podejrzeć przykładowy raport - przycisk Podgląd.

Po wygenerowaniu raportu pojawi się on w widoku zakładki ReportManager i zostanie wysłany do zdefiniowanych adresatów e-mail.

4.2.4.5 Zakładka Zarządzanie licencjami

Polecenie Zestawienie licencji wyświetli ilość wszystkich wykorzystanych licencji na podstawie zainstalowanych instancji klienta. W widoku rozszerzonym dodana zostanie kolumna o nazwie Serwer zarządzający, na potrzeby podzielenia zestawienia na podłączone serwery, jeśli program jest wykorzystywany w trybie logowania MasterAdmin (zarządzanie wieloma serwerami).

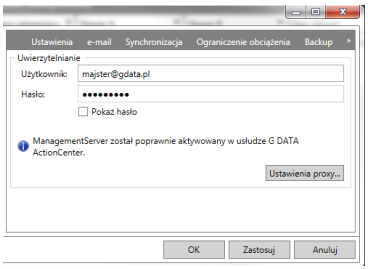
Przycisk **Eksport...** umożliwia zapisanie zestawienia w pliku tekstowym.

Polecenie **Rozszerz licencję...** otwiera stronę internetową umożliwiającą nawiązanie kontaktu w celu dokonania zamówienia dodatkowych licencji.

4.2.4.6 Zakładka ActionCenter

Zarządzanie urządzeniami mobilnymi iOS wymaga połączenia aplikacji G DATA Administrator z usługą G DATA ActionCenter. Wprowadź nazwę użytkownika i hasło do usługi. Jeśli nie masz konta w usłudze G DATA ActionCenter, zarejestruj się.

Do poprawnego działania usługi G DATA ActionCenter wymagana jest ważna licencja na produkt G DATA. Sprawdź dane dostępu do aktualizacji w oknie Opcje > Aktualizacja... > Dane dostępu i ustawienia.



5 G DATA WebAdministrator

WebAdministrator to oprogramowanie umożliwiające zarządzanie składnikiem ManagementServer przez przeglądarkę internetową

5.1 Uruchamianie G DATA WebAdministrator

Aby uruchomić składnik, kliknij ikonkę skrótu na pulpicie. Otworzy się strona przeglądarki z oknem logowania do składnika WebAdministrator.

Wpisz te same dane dostępu, których używasz do logowania do standardowego składnika Administrator.

5.2 Obsługa składnika WebAdministrator

Obsługa WebAdministratora nie różni się od obsługi tradycyjnego składnika G DATA Administrator.

6 G DATA MobileAdministrator

G DATA MobileAdministrator to ograniczona wersja konsoli zarządzającej dla urządzeń przenośnych. Umożliwia wykonywanie podstawowych czynności obsługowych i przeglądanie ustawień.

6.1 Uruchamianie G DATA MobileAdministrator

Po zakończeniu instalacji składnika G DATA MobileAdministrator, można go uruchomić z dowolnej przeglądarki. Wpisz w przeglądarce adres URL wyświetlony pod koniec instalacji. Link składa się z adresu IP lub nazwy komputera z zainstalowanym serwerem ISS i składnikiem MobileAdministrator i nazwy folderu strony (np. http://10.0.2.150/GDMobileAdmin/).

Ekran logowania jest niemal identyczny z ekranem logowania składników G DATA Administrator i G DATA WebAdministrator. Wymaga wskazania nazwy lub adresu IP serwera zarządzającego, rodzaju uwierzytelniania, użytkownika i hasła. Umożliwia również wybór wersji językowej składnika. Istnieje możliwość zapamiętania nazwy użytkownika po zaznaczeniu pola Zapamiętaj nazwę użytkownika w formularzu logowania.

6.2 Obsługa składnika MobileAdministrator

Okno główne programu zawiera 4 przyciski umożliwiające przejście do następujących modułów programu: Status, Raporty, Stacje robocze i ReportManager. Aby zakończyć program dotknij polecenie Wyloguj w prawym, górnym rogu ekranu.

6.2.1 Status

Status składnika G DATA MobileAdministrator przedstawia najważniejsze informacje o stanie ochrony.

Rozwiń pozycję G DATA Security Status aby uzyskać szczegóły na temat serwera i klientów programu G DATA. MobileAdministrator umożliwia podejrzenie statystyk dotyczących ilości zainstalowanych klientów oraz stanu aktualizacji, czy też aktywności podstawowych ustawień (Strażnik, filtr HTTP itp.). Zagłębiając się w widok Sygnatury wirusów mamy możliwość bezpośredniego wymuszania aktualizacji lub też cofania wersji skanerów.

Dostępne są również dane statystyczne na temat połączeń stacji z serwerem, najczęstszych infekcji oraz raportów.

6.2.2 Raporty

Widok raportów zawiera informacje o istotnych zdarzeniach zarejestrowanych przez klienta na stacjach - infekcje, raporty zapory, błędy oraz zdarzenia związane z obsługą składnika PolicyManager. Jest to uproszczona wersja widoku raportów składnika G DATA Administrator.

Możesz operować w widoku zdarzeń z danego dnia, 7 ostatnich dni lub z ostatniego miesiąca. Program wyświetla kategorie zdarzeń, w których dostępne są raporty. Dotknij wybraną kategorię, aby wyświetlić listę raportów. Raporty posortowane są alfabetycznie.

6.2.3 Stacje robocze

Widok zawiera listę stacji zarządzanych z poziomu serwera G DATA. Dla każdej stacji dostępne są najważniejsze ustawienia i informacje. Możliwe jest dokonywanie zmian w wyświetlonych ustawieniach.

Domyślnie wyświetlona jest lista stacji lub grup zarządzanych z programu G DATA ManagementServer. Listę można odfiltrować po nazwach. Po wybraniu konkretnej stacji, program wyświetla widok podsumowania informacji o oprogramowaniu i aktualizacjach. Mamy możliwość zmodyfikowania najważniejszych opcji dotyczących zabezpieczeń. Można np. włączyć/wyłączyć ochronę trybu rzeczywistego, filtrowanie HTTP, skanowanie w trybie bezczynności, czy też zaporę G DATA.

Można również włączyć/wyłączyć funkcjonowanie elementów składnika PolicyManager, czyli Kontrolę aplikacji, urządzeń, treści oraz Dostęp do Internetu.

6.2.4 ReportManager

Mobilna wersja modułu ReportManager umożliwia konfigurowanie, planowanie i podgląd automatycznie generowanych raportów.

Można przeglądać i edytować istniejące raporty lub tworzyć nowe za pomocą przycisku Dodaj harmonogram. Możliwości modułu są porównywalne z wersją modułu dostępną z poziomu komputera.

7 G DATA Security Client (Windows)

Składnik klient chroni stacje robocze w tle i generalnie nie wymaga ingerencji użytkowników. Stacje robocze wyposażone są we własne sygnatury wirusów i mają możliwość samodzielnej aktualizacji (przydatne w przypadku komputerów mobilnych).

Po zainstalowaniu klienta na stacji roboczej, w zasobniku systemowym Windows pojawi się ikona klienta pozwalająca użytkownikowi na wykonywanie zadań określonych w ustawieniach składnika Administrator.

Kliknij prawym klawiszem ikonę Klienta, aby otworzyć menu kontekstowe. Ilość i skład pozycji menu kontekstowego zależy od uprawnień stacji roboczej przydzielonych w zakładce Ustawienia > Ogólne konsoli zarządzającej. Użytkownik może samodzielnie skanować zasoby komputera, aktualizować sygnatury wirusów i zarządzać niektórymi opcjami ochrony - włączać/wyłączać Strażnika, ochronę poczty, czy skanowanie HTTP.

7.1 Skanowanie

Użytkownik stacji roboczej ma możliwość ręcznego uruchomienia skanowania komputera, napędu, pamięci lub określonych zasobów, o ile w module Administrator włączone jest uprawnienie do samodzielnego skanowania.

Możliwe jest także skanowanie obiektów z menu kontekstowego Eksploratora Windows przy użyciu prawego klawisza myszy.

W trakcie trwanie skanowania menu ikonki Klienta powiększa się o następujące pozycje:

- **Priorytet**: Im wyższy priorytet, tym skanowanie trwa krócej, i tym bardziej obciążony jest system i działanie innych programów. Skanowanie z niskim priorytetem trwa najdłużej, ale w jego trakcie można pracować na stacji bez większych utrudnień.
- **Zatrzymaj skanowanie**: Po wstrzymaniu skanowania można je wznowić w dowolnym momencie.
- **Anuluj skanowanie**: Jeżeli w module Administrator włączone jest uprawnienie do modyfikacji ustawień, użytkownik może przerwać periodyczne lub jednorazowe skanowanie uruchomione zdalnie.
- **Pokaż okno skanowania**: Ta opcja otwiera okno skanowania. Okno wyświetla informacje o przebiegu i postępie skanowania.

7.2 Wyłącz Strażnika

To polecenie umożliwia czasowe wyłączenie Strażnika składnika G DATA Client (maksymalnie do kolejnego uruchomienia komputera). Jest to możliwe tylko wtedy, gdy w składniku Administrator ustawione jest odpowiednie uprawnienie użytkowników tej stacji roboczej. Zaleca się nadawanie tego uprawnienia tylko zaufanym i odpowiednio przeszkolonym użytkownikom.

7.3 Opcje

W zależności od ustawień administratora dla danego komputera, użytkownik ma dostęp do maksymalnie pięciu zakładek okna opcji programu Klient.

Uwaga: Nadanie użytkownikom pełnych uprawnień, umożliwi wyłączenie Strażnika i zatrzymanie procesu skanowania. Zalecamy nadawanie pełnych uprawnień do obsługi oprogramowania Klienckiego tylko zaufanym i przeszkolonym użytkownikom.

Jeżeli do stacji roboczej ma dostęp więcej niż jeden zaufany użytkownik, można zabezpieczyć dostęp do ustawień hasłem, znanym tylko tej osobie. Dzięki temu inni użytkownicy komputera nie będą mogli modyfikować ustawień narażając system na infekcję.

Ustawianie uprawnień możliwe jest w oknie składnika Administrator, w zakładce Ustawienia > Ogólne. Opis poszczególnych uprawnień znajdziesz w rozdziale Uprawnienia stacji.

Opisy poszczególnych zakładek opcji Klienta znajdziesz w rozdziale Zakładka Ustawienia.

7.4 Kwarantanna

W oknie lokalnej Kwarantanny wyświetlone są wszystkie pliki przeniesione do Kwarantanny przez monitor antywirusowy i procesy skanowania. Użytkownik może dokonać próby dezynfekcji i przywrócenia pliku, a także usunąć plik z folderu Kwarantanny.

Uwaga: Przywrócenie zainfekowanego pliku może wywołać wtórną infekcję stacji roboczej. Zaleca się stosowanie tej funkcji tylko w przypadku, kiedy chodzi o potwierdzony fałszywy alarm, lub jeśli system operacyjny wymaga danego pliku do działania.

7.5 Aktualizacje/poprawki

Po włączeniu uprawnienia przeglądania i instalacji poprawek dla stacji, użytkownik ma możliwość przeglądania i wysyłania żądań zainstalowania poprawek w oknie uruchamianym z menu kontekstowego ikony klienta w pasku zadań systemu Windows poleceniem **Aktualizacje/Poprawki....**

Mamy do dyspozycji osobne widoki zainstalowanych oraz dostępnych poprawek. Dwukrotne kliknięcie wiersza danej poprawki wyświetla szczegółowe informacje na jej temat.

Poprawki widoczne na liście zainstalowanych można zgłaszać do odinstalowania korzystając z przycisku **Odinstaluj...**. Status poprawki odpowiednio się zmieni, a administrator otrzyma stosowny raport z żądaniem odinstalowania poprawki. Przycisk Znajdź aktualizacje... spowoduje odczytanie aktualnej listy poprawek z systemu.

Lista dostępnych poprawek umożliwia także podgląd szczegółów o poprawkach przez podwójne kliknięcie. Przycisk Zainstaluj... spowoduje wysłanie żądania instalacji poprawki do administratora. Zatwierdzanie żądań odbywa się podobnie jak w przypadku deinstalacji w widoku Raporty.

7.6 Aktualizacja

To okno umożliwia przeprowadzenie aktualizacji baz wirusów, nawet gdy komputer (np. laptop) nie jest podłączony do sieci ze składnikiem ManagementServer. Jest to przydatne w przypadku komputerów mobilnych, przebywających czasem dłuższy czas poza firmą.

Przycisk **Ustawienia i planowanie** umożliwia skonfigurowanie harmonogramu automatycznych aktualizacji sygnatur wirusów.

7.7 Firewall

Klient Firewall jest oprogramowaniem pełniącym funkcje zapory internetowej przeznaczonym na stacje robocze. Zapora chroni komputery działające pod kontrolą systemu operacyjnego Windows przed nieautoryzowanym dostępem do danych oraz przed atakami hakerów działających w sieci lokalnej oraz w Internecie.

Domyślnie program ma włączony tryb autopilota, dzięki czemu funkcjonuje bez potrzeby ingerencji ze strony użytkownika i administratora. Możesz przełączyć zaporę w tryb zestawów reguł, umożliwiający interakcję z użytkownikiem.

Składnik G DATA Firewall instaluje się na stacji roboczej wraz z oprogramowaniem klienckim podczas instalacji zdalnej. Zaporę można zainstalować również w zakładce Firewall z menu kontekstowego prawego klawisza myszki, po kliknięciu wybranej stacji roboczej.

W każdej chwili można odinstalować oprogramowanie zapory poprzez opcję menu kontekstowego prawego klawisza myszy.

Po odłączeniu komputera od sieci przedsiębiorstwa, użytkownik z uprawnieniami do edycji ustawień zapory może tym poleceniem otworzyć interfejs użytkownika składnika Firewall.

7.7.1 Obsługa składnika Firewall

Zapora sieciowa instaluje się w trybie autopilota i nie wymaga ingerencji użytkownika w ustawienia. Tryb zestawów reguł wymaga skonfigurowania przez administratora przynajmniej jednego zestawu reguł przy wykorzystaniu listy najczęściej stosowanych aplikacji. Dostosowanie pozostałych i nowych aplikacji może przebiegać zdalnie dzięki możliwości interakcji użytkownika z administratorem. Ręczna konfiguracja programu nie jest możliwa, chyba że program funkcjonuje w trybie offsite, po odłączeniu od sieci przedsiębiorstwa z dostępem do składnika ManagementServer. W trybie offsite użytkownik ma dostęp do zaawansowanych ustawień zapory poprzez menu ikonki w zasobniku systemowym, pod warunkiem, że administrator zezwoli na to odpowiednim uprawnieniem.

7.7.1.1 Widok Status

Widok Status programu Firewall zawiera podstawowe informacje na temat aktualnego stanu zapory. Symbol ostrzeżenia oznacza, że ustawienia zapory wymagają interwencji użytkownika.

Przez podwójne kliknięcie (lub przez zaznaczenie wpisu i kliknięcie przycisku Edycja) można przejść do okna umożliwiającego modyfikację danego ustawienia programu. Po usunięciu przyczyny ostrzeżenia symbol ostrzeżenia zniknie.

- Skuteczność: Ten wiersz widoku Status informuje o zastosowanym trybie skuteczności zapory. Domyślnie zapora ma ustawioną normalną skuteczność działania.
- Tryb: Ten wiersz informuje o ustawionym trybie pracy zapory. Domyślnie włączony jest tryb Automatyczny (autopilot).

  Tryb autopilota: Zapora działa automatycznie i nie wymaga ingerencji użytkownika. Odpowiednie

reguły dostępu są tworzone automatycznie.

Ręczne tworzenie reguł: Możliwe tylko w trybie offsite.

- Połączenia: Zapora kontroluje wszystkie połączenia sieciowe komputera. Jeśli przynajmniej jedno połączenie nie jest niechronione, np. po ręcznym wyłączeniu ochrony połączenia, przy pozycji Sieci widoku Status pojawi się symbol ostrzegawczy.
- Zarejestrowane ataki: Jeżeli zapora zablokuje atak przeprowadzony z sieci lokalnej lub internetu, w wierszu Zarejestrowane ataki pojawi się odpowiednia adnotacja. Dwukrotne kliknięcie wiersza otworzy okno zawierające szczegóły na temat zablokowanych ataków.
- Radar aplikacji: Ta pozycja okna Status pokazuje ilość aplikacji zablokowanych automatycznie przez zaporę. Jeżeli przy pozycji Radar aplikacji pojawi się symbol ostrzeżenia, kliknij dwukrotnie wiersz Radar aplikacji aby otworzyć okno z listą zablokowanych programów. Aby odblokować dany program, zaznacz go i kliknij przycisk Zezwól.

7.7.1.2 Widok Połączenia

Widok sieci przedstawia połączenia sieciowe (np. LAN, dial-up) Twojego komputera. Okno informuje również o zestawie reguł stosowanym dla każdego połączenia oraz o adresach IP aktywnych połączeń. Dwukrotne kliknięcie wiersza danego połączenia otwiera okno właściwości umożliwiające modyfikację ustawień zapory dla tego połączenia. Szczegóły na temat modyfikacji i tworzenia zestawów reguł znajdziesz w rozdziale Firewall > Zestaw reguł.

Właściwości połączenia

W oknie właściwości wyświetlone są szczegóły połączenia. Można tutaj również modyfikować ustawienia zapory dla wybranego połączenia sieciowego, a także uruchomić asystenta tworzenia reguł.

- Informacje o sieci: Szczegółowe informacje na temat danego połączenia: Adres IP, Maska podsieci, Brama domyślna, Serwer DNS oraz Serwer WINS.
- To połączenie jest chronione przez Firewall: Wyłączenie tej opcji spowoduje wyłączenie zapory dla danego połączenia. Należy to robić tylko w uzasadnionych przypadkach.
- Pozwól na automatyczną konfigurację (DHCP): To ustawienie musi być włączone w sieciach dynamicznie przydzielających adresy IP poprzez serwer

DHCP (Dynamic Host Configuration Protocol).

- Zestaw reguł: Możesz wybrać jeden z gotowych zestawów reguł z przewijanej listy, lub kliknąć przycisk Edytuj zestaw reguł aby zmodyfikować zaawansowane ustawienia zaznaczonego na liście zestawu reguł. Szczegóły znajdziesz w rozdziale Firewall > Zestaw reguł.

7.7.1.3 Widok Zestaw reguł

Widok Zestaw reguł przedstawia listę predefiniowanych zestawów, gotowych do użycia po zainstalowaniu programu. Można modyfikować ustawienia istniejących zestawów reguł, lub tworzyć nowe zestawy dla specjalnych potrzeb.

Tryb ukrycia to ustawienie ukrywające adres IP komputera. Ma to na celu utrudnienie potencjalnym hakerom uzyskania informacji o portach otwartych w systemie. Uzyskanie takich informacji umożliwia przeprowadzanie bardziej zaawansowanych ataków na komputer.

Podstawowych czterech zestawów reguł dla sieci zaufanych, niezaufanych, blokowanych i bezpośredniego połączenia z Internetem nie da się usunąć. Zestawy reguł, które stworzysz sam, można będzie usunąć.

Modyfikacja i tworzenie zestawów reguł

Do każdego połączenia można przyporządkować wybrany zestaw reguł. Poszczególne sieci mogą być chronione przez zaporę w konkretny sposób. Domowa sieć chroniona przez router wyposażony w sprzętową zaporę wymaga niższego poziomu zabezpieczeń niż komputer podłączony bezpośrednio do Internetu.

Zapora proponuje cztery gotowe zestawy reguł dla różnych typów sieci:

- Bezpośrednie połączenia z Internetem: Dla komputerów połączonych bezpośrednio z Internetem.
- Niezaufane sieci: Sieci otwarte, np. hot-spoty lub inne sieci publiczne o nieznanych ustawieniach.
- Zaufane sieci: Do zaufanych można zaliczyć np. prawidłowo zabezpieczone sieci domowe oraz korporacyjne.
- Blokowane sieci: Tego zestawu można użyć, jeśli połączenie komputera z Internetem ma być czasowo lub trwale zablokowane. Ten zestaw reguł jest pusty, więc cały ruch połączeń objętych tym zestawem jest blokowany. Można udostępnić część usług lub aplikacji tego zestawu przez ręczne dodawanie reguł.

Za pomocą przycisku Nowy, możesz stworzyć własny zestaw reguł dla wybranej sieci. Wpisz nazwę dla tworzonego zestawu reguł i wybierz, czy chcesz utworzyć pusty zestaw reguł, czy skorzystać z jednego z dostępnych zestawów reguł.

W widoku Zestaw reguł pod nadaną przez użytkownika nazwą zestawu pojawi się nowy zestaw reguł. Po naciśnięciu przycisku Edytuj w zależności od ustawień, otworzy się Asystent tworzenia reguł lub dialog zaawansowany umożliwiający szczegółową konfigurację poszczególnych reguł.

Więcej na temat reguł i zestawów znajdziesz w rozdziałach Asystent tworzenia reguł i Tryb zaawansowany.

Opis działania automatycznego generowania zapytań opisany jest w rozdziale Firewall > Zestaw reguł > Półautomatyczne tworzenie reguł.

Asystent tworzenia reguł

Przy pomocy Asystenta tworzenia reguł użytkownik może zdefiniować określone dodatkowe reguły danego zestawu reguł lub zmodyfikować istniejące reguły. Początkującym użytkownikom zalecamy stosowanie Asystenta tworzenia reguł do ręcznej konfiguracji zapory lub zdanie się na tryb autopilota.

Za pośrednictwem Asystenta tworzenia reguł użytkownik może zmienić jedną lub kilka reguł w wybranym zestawie.

W zależności od tego, który zestaw reguł został wybrany dla danej sieci, może mieć miejsce sytuacja, że jedna i ta sama aplikacja w zestawie reguł (np. dla niezaufanych sieci) będzie zablokowana, a w drugim zestawie reguł (np. dla sieci zaufanych) będzie mieć pełen dostęp. W ten sposób użytkownik jest w stanie ograniczyć np. przeglądarkę internetową przyporządkowując jej odpowiednio zróżnicowane reguły, aby mieć dostęp na strony znajdujące się na sieci wewnętrznej (np. domowej) ale blokować połączenie w sieci zewnętrznej.

Asystent tworzenia reguł umożliwia podjęcie następujących działań:

- Akceptuj lub blokuj dostęp wybranej aplikacji: Możesz wskazać program (plik) i zezwolić lub zablokować jej dostęp do sieci. W polu Kierunek połączenia wskazać czy wybrany program ma zostać zablokowany dla połączeń wychodzących, przychodzących czy w obydwu kierunkach. W ten sposób użytkownik zapory może np. uniemożliwić aplikacji do odtwarzania muzyki łączenie się ze zdalnym serwerem i pobieranie aktualizacji.
- Udostępnij lub zablokuj określoną usługę internetową (port): Porty przekazują aplikacjom dane za pośrednictwem określonych protokołów. Przesyłanie danych ze stron internetowych odbywa się poprzez port 80, wysyłanie poczty elektronicznej przez port 25, odbieranie poczty elektronicznej przez port 110 itd. W komputerze bez zapory wszystkie porty

używane przez aplikacje są generalnie otwarte, chociaż zazwyczaj zwykli użytkownicy ich nie wykorzystują. Blokując jeden lub kilka portów, można w szybki sposób zamknąć luki bezpieczeństwa, które mogłyby być wykorzystane przez hakerów lub wirusy. Przy pomocy Asystenta tworzenia reguł można zablokować wszystkie lub tylko niektóre porty (np. tylko dla wybranych programów).

- Akceptuj lub blokuj dostęp do plików i drukarek (NetBIOS): NetBIOS to specjalny interfejs w sieciach komputerowych, który może być wykorzystywany np. do akceptacji dostępu do plików i drukarek bezpośrednio z komputera do komputera, bez wykorzystywania przy tym protokołu TCP/IP. Jako że nie jest to konieczne w sieciach domowych, a NetBIOS może być wykorzystywany przez hakerów do ataków na komputer użytkownika, zaleca się zablokowanie portów NetBIOS w sieciach niezaufanych.
- Akceptuj lub blokuj usługi domen: Domena umożliwia scentralizowane zarządzanie komputerami w sieci wyposażonej w kontroler domeny. Dlatego też dostęp do usług domen w sieciach niezaufanych powinien być z reguły zablokowany.
- Zezwól na współdzielenie połączenia internetowego: Ta funkcjonalność dotyczy jedynie połączeń typu dialup (np. Neostrada, GPRS, UMTS itp.). Po udostępnieniu danego połączenia, konkretne komputery w sieci lokalnej również mogą z niego korzystać.
- Przełącz na tryb zaawansowany: W ten sposób użytkownik może przejść z trybu Asystenta tworzenia reguł do trybu zaawansowanego.

Wyłączenie opcji Uruchamiaj Asystenta reguł również w przyszłości, spowoduje, że program będzie wyświetlał okno zaawansowanej konfiguracji reguł zamiast Asystenta tworzenia reguł.

Tryb zaawansowany

W trybie zaawansowanym można skonfigurować reguły dla poszczególnych zestawów reguł. Tworzenie może przebiegać przy użyciu Asystenta tworzenia reguł lub ręcznie.

Dostępne są następujące ustawienia:

- Nazwa: Tu w zależności od potrzeb można zmieniać nazwę aktualnego zestawu reguł. Pod tą nazwą zestaw będzie wyświetlony w liście w widoku Zestaw reguł.
- Tryb ukrycia: W trybie ukrycia system nie odpowiada na zapytania wysyłane do komputera, w celu sprawdzenia dostępności portów. Utrudnia to hakerom uzyskanie informacji o systemie.
- Określ reakcję, jeśli żadna reguła nie pasuje: To pole określa reakcję na

połączenie aplikacji, które nie jest regulowane przez żadną regułę.

- Tryb konfiguracji: Tryb konfiguracji przydatny jest w przypadku stosowania aplikacjach, które wykorzystują technikę kanałów zwrotnych (np. FTP, gry sieciowe). Aplikacje te łączą się ze zdalnym komputerem i negocjują z nim kanał zwrotny, poprzez który zdalny komputer łączy się następnie ponownie z aplikacją użytkownika. Jeśli tryb konfiguracji jest aktywny, zapora rozpoznaje kanał zwrotny i udziela mu dostępu bez dodatkowych zapytań.
- Szczegóły ICMP: Internet Control Message Protocol (ICMP) to protokół internetowy umożliwiający przekazywanie informacji o błędach, pakietach testowych oraz o transferze danych. Pakiety ICMP mogą być wykorzystywane do inwigilowania komputera. Z tego powodu pakiety ICMP powinny być filtrowane przez zaporę.

Lista zawiera wszystkie reguły stosowane w danym zestawie. Reguły umożliwiają blokowanie lub akceptowanie połączeń wywoływanych zdalnie i lokalnie przez usługi i aplikacje. Metody tworzenia reguł:

- Zastosowanie Asystenta tworzenia reguł.
- Ręcznie, poprzez kliknięcie przycisku Nowy w widoku trybu zaawansowanego .
- W oknie zapytania wyświetlanym automatycznie podczas próby nawiązania połączenia.

Kolejność reguł może mieć znaczenie. Może dojść np. do zablokowania usługi zaakceptowanej na poziomie portu przez regułę blokującą dostęp dla całego protokołu. Kolejność reguł można zmieniać poprzez przeciąganie ich nazw myszą lub przy użyciu przycisków strzałek w sekcji Pozycja.

Okno Edytuj regułę zawiera następujące pola, przyciski i rozwijane listy umożliwiające utworzenie nowej lub zmodyfikowanie istniejącej reguły:

- Nazwa: W regułach predefiniowanych jest to nazwa aplikacji której dotyczy reguła. Nazwę można zmieniać i uzupełniać.
- Reguła aktywna: Można wyłączyć działanie reguły poprzez odznaczenie tego pola.
- Komentarz: Pole informuje w jaki sposób reguła została utworzona. Reguły predefiniowane oznaczone są komentarzem Domyślna reguła, natomiast w przypadku reguł tworzonych na podstawie zapytań w tej rubryce widnieje tekst Generowane poprzez zapytanie. Wprowadź własny komentarz dla reguł generowanych ręcznie.
- Kierunek połączenia: To ustawienie definiuje, czy chodzi w danym przypadku o regułę dla połączeń wychodzących, przychodzących czy dla obydwu rodzajów.

- Reakcja: To pole określa, czy reguła ma blokować, czy akceptować połączenia.
- Protokół: Wybór protokołu umożliwia zdefiniowanie ogólnej reguły dla całego protokołu, bez względu na aplikację, czy port.
- Przedział czasowy: Reguły mogą być także aktywne tylko w czasie określonym w tej sekcji. W ten sposób można ograniczyć dostęp konkretnych aplikacji do sieci np. tylko do czasu pracy.
- Zakres adresów IP: Reglamentacja dostępu do sieci staje się prostsza szczególnie w przypadku sieci z przydzielonymi stałymi adresami IP.

Półautomatyczne tworzenie reguł

Jeżeli zapora przełączona jest w tryb ręczny, przy każdej próbie połączenia się aplikacji sieciowej z siecią lokalną lub Internetem program prosi o utworzenie reguły. Okno automatycznego tworzenia reguł umożliwia podgląd szczegółów na temat danej aplikacji lub procesu. W zależności od wybranej reakcji program utworzy regułę blokującą lub akceptującą aktywność sieciową aplikacji lub procesu.

Okno z zapytaniem oferuje do wyboru następujące przyciski:

- Zawsze akceptuj: Tworzy dla danej aplikacji (np. Opera.exe, Explorer.exe czy WINWORD.exe) regułę, która danej aplikacji na stałe zezwala na aktywność sieciową. Ta reguła znajdzie się w aktywnym Zestawie reguł jako reguła generowana przez zapytanie.
- Akceptuj teraz: Przycisk zezwala danej aplikacji tylko jednorazowe połączenie. Przy następnej próbie dostępu do sieci, np. po ponownym uruchomieniu komputera, zapora zapyta ponownie o pozwolenie.
- Zawsze blokuj: Tworzy regułę dla danej aplikacji, która blokuje na stałe aktywność sieciową aplikacji. Reguła ta znajdzie się aktywnym Zestawie reguł jako generowana przez zapytanie.
- Blokuj teraz: Przycisk zablokuje jednorazowo aktywność sieciową danej aplikacji. Przy następnej próbie dostępu do sieci, np. po ponownym uruchomieniu komputera, zapora zapyta ponownie o pozwolenie.

Kliknij przycisk Szczegóły aby wyświetlić dodatkowe informacje na temat protokołu, portu i adresu IP lub nazwy serwera.

7.7.1.4 Widok Protokół

Widok Protokół zawiera listę wszystkich połączeń komputera z Internetem i siecią lokalną. Można sortować listę klikając nagłówki kolumn. Kliknij przycisk Szczegóły... aby zobaczyć szczegółowe informacje na temat przesyłanych pakietów danych.

7.7.1.5 Ustawienia zapory

Widok Opcje służy do modyfikowania zaawansowanych ustawień funkcji zapory. Jeżeli korzystasz z trybu autopilota, zapora działa w pełni automatycznie i nie wymaga zaawansowanej konfiguracji.

Tryb automatyczny

Zapora może automatycznie reagować na zagrożenia. Jeśli tryb autopilota zostanie wyłączony, możliwe jest ręczne tworzenie reguł, a zapora będzie zadawać użytkownikowi pytania odnośnie połączeń z Internetem nawiązywanych przez aplikacje.

Tryb autopilota: Zapora działa automatycznie i nie wymaga ingerencji użytkownika. Odpowiednie reguły dostępu są tworzone automatycznie.

Ręczne tworzenie reguł: Możliwe tylko w trybie offsite.

7.8 Wyłącz Firewall

To polecenia pozwala na wyłączenie zapory G DATA, nawet jeśli stacja znajduje się w sieci z dostępnym serwerem zarządzającym G DATA. Jeśli zapora zostanie wyłączona, można ją ponownie włączyć poleceniem **Włącz Firewall**.

Aby polecenie wyłączania zapory było aktywne z poziomu stacji, należy je włączyć w oknie Administrator, w zakładce Firewall > Ustawienia (Użytkownik może włączać/wyłączać zaporę).

7.9 Informacje

Polecenie **Informacje** pozwala sprawdzić datę sygnatur wirusów i numer wersji klienta G DATA.

8 G DATA Security Client (Linux)

G DATA Security Client dla systemów Linux to usługa działająca w tle umożliwiająca funkcjonalność skanowania na obecność wirusów. Dla systemów Linux działających jako serwery plików SAMBA dostępny jest specjalny moduł klienta G DATA dla serwerów SAMBA (patrz rozdział Instalacja G DATA Security Client (Linux)). Moduł kontroluje wszystkie próby dostępu do plików zapisanych na udziałach SMB zapobiegając przedostawaniu się zagrożeń między systemami Windows i Linux.

G DATA Security Client dla systemów Linux to dwa działające w tle daemony **gdavserver** i **gdavclientd**, a także interfejs graficzny i interfejs wiersza poleceń.

8.1 Interfejs graficzny

Skrót do okienkowego interfejsu aplikacji G DATA Security Clients dla systemów Linux można znaleźć w oknie wyboru aplikacji lub innym pokrewnym menu, w zależności od stosowanej dystrybucji. Alternatywnie interfejs można uruchomić ręcznie za pomocą polecenia **/opt/gdata/bin/gdavclient-qt**.

Po uruchomieniu interfejsu okno aplikacji można uruchomić klikając ikonę klienta G DATA. Zestaw dostępnych opcji zależy od ustawień podjętych w oknie G DATA Administrator > Ustawienia stacji > Ogólne > Uprawienia stacji.

Za pomocą menu kontekstowego interfejsu ikonki w zasobniku można uruchomić następujące polecenia programu:

- Skanowanie
- Kwarantanna
- Aktualizacja
- Pomoc
- Otwórz G DATA Security Client: Uruchamia interfejs graficzny G DATA Security Clients for Linux i wyświetla widok **Status**.

- Informacje

Wszystkie moduły chronione są przed niezamierzonym wprowadzaniem zmian. Kliknij obszar kłódki w dolnej części okna aby umożliwić wprowadzanie zmian w ustawieniach. Jeśli wymagane będzie podniesienie uprawnień, wprowadź dane dostępu konta **root**.

8.1.1 Status

Widok statusu wyświetla podstawowe informacje na temat stanu ochrony klienta.

- **Ostatnie skanowanie**: Data ostatniego skanowania systemu. Kliknij przycisk **Skanuj komputer** aby uruchomić procedurę skanowania.
- **Ostatnia aktualizacja**: Data i czas ostatniej aktualizacji sygnatur zagrożeń. Kliknij przycisk **Uaktualnij teraz** aby uruchomić procedurę aktualizacji.

8.1.2 Skanowanie

Wybierz rodzaj skanowania lokalnego, jakie chcesz przeprowadzić. Możliwe jest przeskanowanie wybranych folderów i plików, obszarów systemowych lub całego systemu plików komputera. W przypadku wykrycia zagrożenia aplikacja wykona automatycznie działanie skonfigurowane poniżej. Ponadto o infekcji informowany jest serwer zarządzający G DATA, a w widoku **Raportów** pojawi się odpowiedni wpis zawierający szczegóły zdarzenia.

Sekcja **Ustawienia** umożliwia modyfikowanie parametrów skanowania:

Do wyboru są następujące reakcje na wykrycie zagrożenia:

  - Tylko raport
  - Dezynfekcja
  - Usunięcie pliku
  - Przeniesienie pliku do Kwarantanny
  - Przekazanie decyzji o podjęciu reakcji użytkownikowi.

- **Jeśli dezynfekcja nie jest możliwa**: Reakcja wtórna na wypadek problemu z oczyszczaniem zarażonego pliku.
- **Zainfekowane archiwa**: Odrębna reakcja dla spakowanych i skompresowanych plików.

- **Rodzaje plików**

W sekcji **Zaawanasowane** możemy dokonać ustawień kolejnych parametrów:

- **Heurystyka**
- **Skanuj obszary systemowe**
- **Skanuj archiwa**
- **Maksymalny rozmiar skanowanych archiwów**: Archiwa powyżej zadanego rozmiaru nie będą skanowane.
- **Maksymalny rozmiar skanowanych plików**: Pliki powyżej zadanego rozmiaru nie będą skanowane.

Sekcja **Wyjątki** umożliwia wykluczenie ze skanowania listy plików, folderów.

Możliwość samodzielnego skanowania systemu przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

8.1.3 Aktualizacja

Widok umożliwia zarządzanie procesem aktualizowania sygnatur zagrożeń. Okno wyświetla czas ostatniej aktualizacji oraz numery wersji obu skanerów.

Opis parametrów aktualizacji:

- **Źródło aktualizacji**: Klient może pobierać aktualizacje z serwera zarządzającego lub bezpośrednio z internetu.
- **Planowanie**: Aktualizowanie może się odbywać ręcznie lub automatycznie wg harmonogramu.
- **Serwer proxy**: Jeśli komputer łączy się z internetem przez serwer proxu, niezbędne jest wprowadzenie ustawień w tej sekcji.
- **Dane dostępu**: W tym miejscu można wprowadzić dane dostępu do usługi aktualizacji G DATA.

Ustawienia dotyczące planowania, serwera proxy oraz danych dostepu mają znaczenie tylko w przypadku pobierania aktualizacji bezpośrednio z internetu.

Możliwość samodzielnego aktualizowania programu przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

8.1.4 Kwarantanna

Widok Kwarantanny umożliwia przeglądanie plików przeniesionych do zaszyfrowanego folderu w wyniku zastosowania takiej reakcji na wykrycie zagrożenia.

Zaznacz jeden lub więcej plików aby skorzystać z przycisków dostępnych poniżej:

- **Dezynfekuj i przywróć**: Nastąpi próba oczyszczenia pliku i przywrócenia go do pierwotnej lokalizacji.
- **Przywróć**: Plik zostanie przywrócony do pierwotnej lokalizacji. Plik nadal może stanowić zagrożenie!
- **Usuń**: Plik zostanie bezpowrotnie usunięty z Kwarantanny.

Możliwość obsługi modułu Kwarantanny przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

8.1.5 Informacje

Okno informacji o kliencie wyświetla następujące dane:

- **Wersja**: Numer wersji zainstalowanago klienta.
- **ManagementServer**: Status połaczenia ze składnikiem ManagementServer.
- **Status**: Status procesów działających w tle

8.2 Interfejs wiersza poleceń

Klientem dla systemów Linux można alternatywnie zarządzać za pomocą interfejsu wiersza poleceń systemu Linux. Polecenie gdavclientc umożliwia konfigurowanie i wykonywanie skanowania, wyświetlanie informacji o wersji, przetwarzania aktualizacji i zarządzanie usługą serwera skanowania działającą w tle. Polecenie gdavupdate służy do pobierania aktualizacji z serwerów aktualizacji G DATA. Oba narzędzia ,uszą być uruchamiane na uprawnieniach root ze względu na wymagane pełne uprawnienia do systemu.

8.2.1 gdavclient-cli

Domyślna lokalizacja gdavclient-cli to folder /usr/bin. Składnia polecenia gdavclient-cli wygląda następująco: gdavclient-cli [<opcje>] <pliki/ścieżka>. Dostępne są następujące opcje:

- --status: Wyświetla status usług działających w tle: gdavclientc, gdavserver.
- --version: Wyświetla informacje o wersji.
- --mmsconnection: Informacje na temat połączenia z instancją ManagementServer.
- --lastscan: Wyświetla ostatni raport skanowania.
- --lastupdate: Wyświetla informacje o ostatniej aktualizacji sygnatur zagrożeń.
- --update: Uruchamia aktualizację sygnatur zagrożeń.
- --sysinfo: Tworzy plik gdatahwinfo-<data>.tar.gz. Plik zawiera log debugowania oraz np. raporty i pliki konfiguracyjnne.

Jeśli zostaną wskazane pliki lub ścieżki, proces gdavclient-cli rozpocznie ich skanowanie.

8.2.2 gdavclientc

Domyślna lokalizacja gdavclientc to folder /usr/bin. Narzędzie działa niezależnie od składnika G DATA ManagementServer i wczytuje konfigurację z pliku /etc/gdata/gdav.ini. Składnia polecenia gdavclientc wygląda następująco: gdavclientc [<opcje>] <polecenie>. Dostępne są następujące polecenia:

scan:<ścieżka>: Uruchamia skanowanie plików w folderze <ścieżka>. <ścieżka> może być w formacie uniwersalnym lub względnym i może wskazywać plik lub folder. Foldery są skanowane rekursywnie. Dozwolone jest stosowanie znaków zastępczych (*, ?).

scanboot: Uruchamia skanowanie sektorów rozruchowych. Skanowanie obejmie sektory startowe wszystkich nieoptycznych nośników danych obecnych w /proc/partitions.

abort: Anuluje bieżące skanowanie.

start: Uruchamia usługę gdavserver.

stop: Zatrzymuje usługę gdavserver.

restart: Zatrzymuje i wznawia usługę gdavserver.

updateVDB<:engine>: Uruchamia aktualizację sygnatur wirusów skanera EngineA lub skanera EngineB. Po zakończeniu aktualizacji, serwer skanowania musi zostać uruchomiony ponownie poleceniem restart.

dump: Wyświetla bieżącą konfigurację gdavserver.

set:<klucz>=<wartość>: Dodaje lub modyfikuje klucz i wartość w konfiguracji gdavserver. Ustawienie obowiązuje tylko przez czas bieżącego działania usługi. Aby wprowadzić ustawienia na stałe, należy je wprowadzić i zapisać w pliku konfiguracyjnym /etc/gdata/gdav.ini przed uruchomieniem serwera.

get:<klucz>: Zwraca wartość klucza <klucz>.

reload: Wczytuje konfigurację z pliku /etc/gdata/gdav.ini.

engines: Wyświetla listę silników używanych przez gdavserver.

baseinfo: Wyświetla informacje o wersji.

coreinfo: Wyświetla informacje o wersach silników.

pid: Wyświetla PID usługi gdavserver.

Zastosowanie polecenia scan: umożliwia wykorzystanie następujących opcji:

-s: Oprócz wyniku skanowania, wyświetla również podsumowanie wyników.

-x: Oprócz wyniku skanowania, wyświetla również podsumowanie wyników (w formacie XML).

8.3 Procesy

W celu sprawdzenia działania obu procesów klienta G DATA w systemie Linux wpisz w terminalu polecenie:

linux:~# ps ax|grep av

Spodziewany jest następujący wynik:

/usr/sbin/gdavserver
/usr/sbin/gdavclientd

Procesy można uruchomić następującymi poleceniami:

linux:~# /etc/init.d/gdavserver start
linux:~# /etc/init.d/gdavclient start

Procesy można zatrzymać następującymi poleceniami:

linux:~# /etc/init.d/gdavserver stop
linux:~# /etc/init.d/gdavclient stop

Do wykonania poleceń niezbędne są uprawnienia poziomu root.

8.4 Logi

Zdalna instalacja składnika G DATA Security Clients w systemi Linux logowana jest w pliku **/var/log/gdata_install.log**.

Proces gdavclientd protokołuje informacje i błędy w pliku **/var/log/gdata/avclient.log**.

Proces gdavserver protokołuje informacje i błędy w pliku **/var/log/gdata/gdavserver.log**. Ten plik może być pomocny w diagnostyce połączenia ze składnikiem G DATA ManagementServer.

Jeśli potrzebujesz bardziej szczegółowych informacji w logach, zmień w plikach konfiguracyjnych **/etc/gdata/gdav.ini** i **/etc/gdata/avclient.cfg** wartość dla parametru **LogLevel** na **7** setzen (jeśli parametru nie ma, po prostu dodaj go w osobnym wierszu). Uwaga: Wysoki poziom logowania generuje duże ilości komunikatów i powoduje szybki przyrost rozmiaru plików **.log**. W czasie normalnej obsługi obniż poziom logowania do niższej wartości.

8.5 Test serwera skanowania

Narzędzie **gdavclientc** umożliwia weryfikację pracy serwera skanowania. Informacje o wersji można wywołać poleceniami **baseinfo** i **coreinfo**. Uruchom testowe skanowanie poleceniem **scan:<ścieżka>**. Więcej informacji znajdziesz w rozdziale gdavclient-cli.

8.6 Połączenie z serwerem G DATA

Konfiguracja komunikacji z serwerem G DATA ManagementServer znajduje się w pliku **/etc/gdata/avclient.cfg**. Sprawdź czy adres IP składnika ManagementServer wprowadzony jest poprawnie. Jeśli adres nie jest poprawny, wprowadź prawidłową wartość i zapisz plik.

9 G DATA Security Client (Mac)

Aplikacja G DATA Security Clients dla systemów Mac OS X chroni system operacyjny za pomocą skanera dostępowego. Umożliwia również wykonywanie skanowania na żądanie lub z harmonogramu.

Po uruchomieniu interfejsu okno aplikacji można uruchomić klikając ikonę klienta G DATA. Zestaw dostępnych opcji zależy od ustawień podjętych w oknie G DATA Administrator > Ustawienia stacji > Ogólne > Uprawienia stacji.

Za pomocą menu kontekstowego interfejsu ikonki w zasobniku można uruchomić następujące polecenia programu:

- Włącz/wyłącz Strażnika
- Skanowanie
- Kwarantanna
- Aktualizacja
- Pomoc
- Otwórz G DATA Security Client: Uruchamia interfejs graficzny G DATA Security Clients for Mac i wyświetla widok **Status**.
- Informacje

Wszystkie moduły chronione są przed niezamierzonym wprowadzaniem zmian. Kliknij obszar kłódki w dolnej części okna aby umożliwić wprowadzanie zmian w ustawieniach. Jeśli wymagane będzie podniesienie uprawnień, wprowadź dane dostępu konta **root**.

9.1 Status

Widok statusu wyświetla podstawowe informacje na temat stanu ochrony klienta.

- **Strażnik**: Stan ochrony rezydentnej. Możliwe jest czasowe wyłączenie Strażnika.
- **Ostatnie skanowanie**: Data ostatniego skanowania systemu. Kliknij przycisk **Skanuj komputer** aby uruchomić procedurę skanowania.
- **Ostatnia aktualizacja**: Data i czas ostatniej aktualizacji sygnatur zagrożeń.

Kliknij przycisk **Uaktualnij teraz** aby uruchomić procedurę aktualizacji.

9.2 Strażnik

Sekcja Ustawienia umożliwia modyfikację następujących parametrów:

- **Status**: Strażnik może być włączony, wyłączony, lub wyłączony czasowo. Czasowe wyłączenie można ustawić na określoną ilość minut, lub do następnego uruchomienia komputera.
- Do wyboru są następujące reakcje na wykrycie zagrożenia:
  - Tylko raport
  - Dezynfekcja
  - Usunięcie pliku
  - Przeniesienie pliku do Kwarantanny
  - Przekazanie decyzji o podjęciu reakcji użytkownikowi.
- **Jeśli dezynfekcja nie jest możliwa**: Reakcja wtórna na wypadek problemu z oczyszczaniem zarażonego pliku.
- **Zainfekowane archiwa**: Odrębna reakcja dla spakowanych i skompresowanych plików.
- **Rodzaje plików**

W sekcji **Zaawanasowane** możemy dokonać ustawień kolejnych parametrów:

- **Heurystyka**
- **Skanuj obszary systemowe**
- **Skanuj archiwa**
- **Maksymalny rozmiar skanowanych archiwów**: Archiwa powyżej zadanego rozmiaru nie będą skanowane.
- **Maksymalny rozmiar skanowanych plików**: Pliki powyżej zadanego rozmiaru nie będą skanowane.

Sekcja **Wyjątki** umożliwia wykluczenie ze skanowania listy plików, folderów.

Możliwość obsługi Strażnika przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

9.3 Skanowanie

Wybierz rodzaj skanowania lokalnego, jakie chcesz przeprowadzić. Możliwe jest przeskanowanie wybranych folderów i plików, obszarów systemowych lub całego systemu plików komputera. W przypadku wykrycia zagrożenia aplikacja wykona automatycznie działanie skonfigurowane poniżej. Ponadto o infekcji informowany jest serwer zarządzający G DATA, a w widoku **Raportów** pojawi się odpowiedni wpis zawierający szczegóły zdarzenia.

Sekcja **Ustawienia** umożliwia modyfikowanie parametrów skanowania.

Możliwość samodzielnego skanowania systemu przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

9.4 Aktualizacja

Widok umożliwia zarządzanie procesem aktualizowania sygnatur zagrożeń. Okno wyświetla czas ostatniej aktualizacji oraz numery wersji obu skanerów.

Opis parametrów aktualizacji:

- **Źródło aktualizacji**: Klient może pobierać aktualizacje z serwera zarządzającego lub bezpośrednio z internetu.
- **Planowanie**: Aktualizowanie może się odbywać ręcznie lub automatycznie wg harmonogramu.
- **Serwer proxy**: Jeśli komputer łączy się z internetem przez serwer proxu, niezbędne jest wprowadzenie ustawień w tej sekcji.
- **Dane dostępu**: W tym miejscu można wprowadzić dane dostępu do usługi aktualizacji G DATA.

Ustawienia dotyczące planowania, serwera proxy oraz danych dostepu mają znaczenie tylko w przypadku pobierania aktualizacji bezpośrednio z internetu.

Możliwość samodzielnego aktualizowania programu przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

9.5 Kwarantanna

Widok Kwarantanny umożliwia przeglądanie plików przeniesionych do zaszyfrowanego folderu w wyniku zastosowania takiej reakcji na wykrycie zagrożenia.

Zaznacz jeden lub więcej plików aby skorzystać z przycisków dostępnych poniżej:

- **Dezynfekuj i przywróć**: Nastąpi próba oczyszczenia pliku i przywrócenia go do pierwotnej lokalizacji.
- **Przywróć**: Plik zostanie przywrócony do pierwotnej lokalizacji. Plik nadal może stanowić zagrożenie!
- **Usuń**: Plik zostanie bezpowrotnie usunięty z Kwarantanny.

Możliwość obsługi modułu Kwarantanny przez użytkownika można zablokować z poziomu aplikacji G DATA Administrator w oknie Ustawienia stacji > Ogólne > Uprawnienia stacji.

9.6 Informacje

Okno informacji o kliencie wyświetla następujące dane:

- **Wersja**: Numer wersji zainstalowanago klienta.
- **ManagementServer**: Status połaczenia ze składnikiem ManagementServer.
- **Status**: Status procesów działających w tle

10 G DATA ActionCenter

G DATA ActionCenter to witryna internetowa oferująca dostęp do obsługi chmurowych usług G DATA. Do skorzystania z serwisu niezbędne jest utworzenie konta w witrynie:

https://ac.gdata.de

Po zalogowaniu dostepne są następujące obszary usług do zarządzania

- **Urządzenia mobilne**: Mobile Device Management dla użytkowników domowych.
- **Network monitoring**: Nadzór nad infrastrukturą sieciową.

Dodatkowe elementy ActionCenter:

- **Uprawnienia**: Zarządzanie przekazywaniem uprawnień innym użytkownikom usługi ActionCenter, np. udostępnienie wglądu do odczytu w aplikacji Network monitoring.
- **Grupy e-mail**: Dzięki konfiguracji tej opcji usługa ActionCenter będzie w stanie dostarczać raporty i powiadomienia alarmowe aplikacji Network Monitoring.

Skonfigurowanie usługi ActionCenter jest również wymagana do skorzystania z opcji iOS Mobile Device Management, zapewnia bowiem komunikację między urządzeniami iOS a składnikiem G DATA ManagementServer. Zarządzanie opcjami iOS Mobile Device Management odbywa się bezpośrednio z konsoli G DATA Administrator, poprzez dedykowany węzeł drzewa sieci.

10.1 Tworzenie konta i konfiguracja

Witryna ActionCenter umożliwia zarejestrowanie nowego konta. Wprowadź adres e-mail oraz hasło i zatwierdź zgodę na warunki korzystania z usługi. Następnie potwierdź tożsamość klikając link aktywacyjny wysłany na wskazany adres mailowy.

Po zatwierdzeniu tożsamości konto jest gotowe do użytkowania.

Ważne: W celu powiązania serwera zarządzającego z kontem G DATA ActionCenter niezbędne jest wprowadzenie danych do serwisu również w programie G DATA Administrator > Sekcja ManagementServer > Zakładka ActionCenter.

10.2 Moduły

G DATA ActionCenter obsługujemy za pomocą modułów aplikacji. Dla rozwiązań G DATA Business powstał odrębny moduł serwisu ActionCenter - Network Monitoring.

10.2.1 Network Monitoring

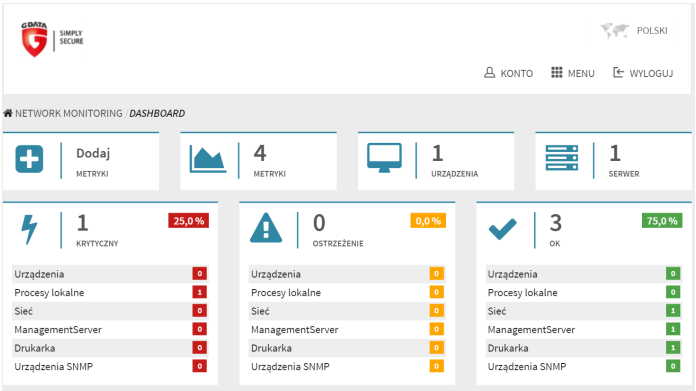
Network Monitoring jest opcją programów G DATA Business dostępną za dodatkową opłatą.

Ten moduł umożliwia administratorowi monitorowanie stanu infrastruktury

sieciowej. Poprzez utworzenie odpowiednich metryk możemy uzyskać paletę pożądanych statystyk wyświetlanych w obszarze Dashboard.

10.2.1.1 Dashboard

Widok Dashboard przedstawia zestawienie statystyk wszystkich ustawionych metryk, a także zarządzanych serwerów i urządzeń. Jeśli dodamy metrykę do ulubionych, widok Dashboard zaprezentuje odrębny widget zawierający podsumowanie informacji (nazwa, ostatnia wartość i wykres tendencji).



Środkowa część widoku prezentuje statystyki wszystkich metryk podzielone na 3 grupy wg stanu metryki w odniesieniu do wartości progowych - krytyczne, ostrzeżenia i OK. Po pierwszym przekroczeniu wartości progowej dana metryka trafia na listę ostrzeżeń. Po kolejnych dwóch przekroczeniach zadanego progu stan metryki zmienia się na krytyczny.

Poniżej wyświetlane są logi metryk. Wpis w logu tworzony jest przy pierwszym kontakcie metryki z serwerem lub w momencie zmiany stanu metryki na ostrzeżenie lub krytyczny. Klikajac dany wiersz loga przenosimy się do ustawień metryki.

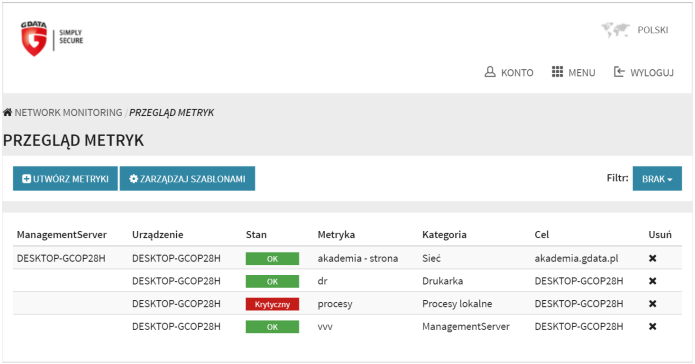
Jeśli do usługi podłaczymy więcej niż jeden serwer zarządzający, możemy utworzyć więcej niż jeden widok Dashboard - polecenie Utwórz Dashboard umożliwia utworzenie widoku i powiązania go z jednym lub kilkoma serwerami zarządzającymi.

10.2.1.2 Przegląd metryk

Utworzenie nowej metryki polega na przypisaniu do urządzenia lub kilku urządzeń szablonu metryki. Na podstawie parametrów szablonu metryka regularnie raportuje do usługi ActionCenter przekazując statystyki dotyczące urządzenia. Kliknij przycisk **Utwórz metryki** aby utworzyć nową metrykę.

Widok Przegląd metryk przedstawia listę wszystkich utworzonych punktów pomiarowych. Kliknij metrykę aby przejść do okna ustawień danej metryki. Listę metryk można filtrować ze względu na stan metryk lub ich kategorie. Objaśnienie kolumn:

- **ManagementServer**: Składnik ManagementServer, do którego przyporządkowane jest urządzenie.
- **Urządzenie**: Urządzenie, z którym powiązany jest szablon metryki.
- **Stan**: Bieżący stan metryki (OK, ostrzeżenie, krytyczny lub nieznany).
- **Metryka**: Nazwa szablonu metryki, na podstawie którego została utworzona.
- **Kategoria**: Kategoria szablonu metryki.
- **Cel**: Docelowe urządzenie szablonu metryki.

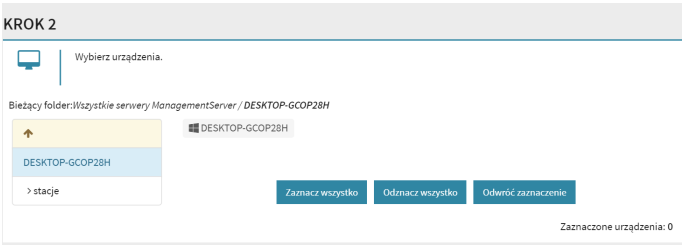


Utwórz metryki

Tworzenie metryki polega na powiązaniu jednego lub więcej szablonów metryk z jednym lub wieloma urządzeniami. Proces podzielony jest na 4 kroki:

1. Wybór szablonów. Wybierz jeden lub kilka szablonów metryk. Szablony wyświetlane są według kategorii.

2. Wybór urządzeń. Zaznacz jedno lub więcej urządzeń. Urządzenia wyświetlane są w strukturze drzewa zgodnej z powiązanym składnikiem ManagementServer. Najwyższy poziom struktury umożliwia wybranie serwera zarządzającego (o ile w pierwszym kroku jako szablon wskazana została kategoria ManagementServer).



3. Weryfikacja wybranych urządzeń. Upewnij się, czy zaznaczone są wszystkie urządzenia do których przypisany są wybrane szablony metryk.

4. Podsumowanie. Kliknij przycisk **Utwórz metryki**, aby sfinalizować proces i przejść do widoku przeglądu metryk.

Metryka

Widok strony metryki wyświetla szczegóły punktu pomiaru (nazwa szablonu, powiązany składnik ManagementServer, a także aktualny status). Kliknij przycisk **Ulubiony**, aby wyświetlić metrykę jako widget widoku Dashboard.

Pod szczegółami metryki mamy do dyspozycji widok wykresu punktu pomiaru. Widok można modyfikować zmieniając jego przedział czasowy. Domyślne ustawienie to wykres ostatnich sześciu godzin pomiaru.

W sekcji przegląd dostepne są następujące informacji:

- **Interwał pomiaru**: Częstotliwość przesyłania danych do usługi ActionCenter.

- **Ostatnia wartość**: Wartość ostatniego pomiaru z datą i godziną.
- **Minimum**: Najniższa zmieżona wartość.
- **Maksymalnie**: Najwyższa zmierzona wartość.
- **Próg** (jeśli próg jest ustawiony): Bieżąca wartość progowa.
- **Ponad próg** (jeśli próg jest ustawiony): Procentowe przekroczenie progu.
- **Poniżej progu** (jeśli próg jest ustawiony): Procentowe ujęcie wartości w odniesieniu do progu.

Wpis w logu tworzony jest przy pierwszym kontakcie metryki z serwerem lub w momencie zmiany stanu metryki na ostrzeżenie lub krytyczny.

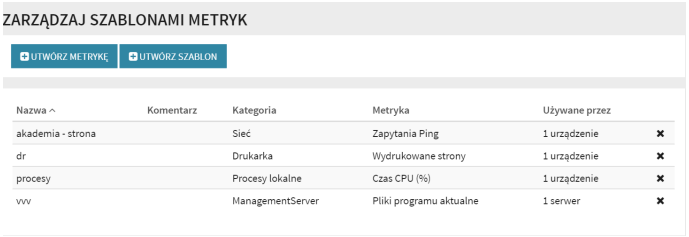
Zarządzaj szablonami

Szablony metryk do zestawy parametrów umożliwiające elastyczne stosowanie aplikacji Network Monitoring. Na podstawie szablonów można tworzyć metryki przypisane do konkretnych urządzeń. Kliknij przycisk Utwórz szablon aby otworzyć stronę kreatora szablonów.

Widok zarządzania szablonami metryk przedstawia listę wszystkich utworzony szablonów. Klikając wybrany wiersz szablonu otwieramy okno umożliwiające jego edycję. Opis kolumn:

- **Nazwa**: Nazwa szablonu.
- **Komentarz**: Informacje ułatwiające identyfikację szablonu.
- **Kategoria**: Kategoria szablonu (urządzenia, procesy, sieć, ManagementServer, drukarka lub urządzenie SNMP).

- **Metryka**: Opisuje gromadzone dane w zależności od wybranej kategorii.
- **Używane przez**: Ilość urządzeń/serwerów do których przypisany jest szablon.



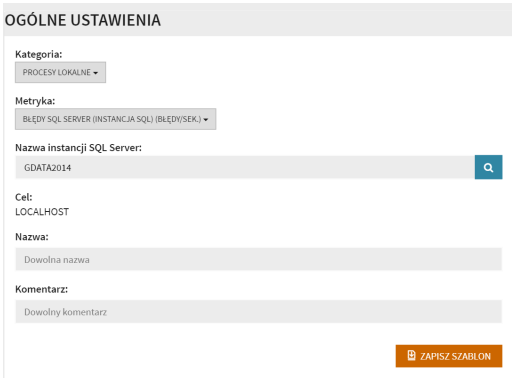
Utwórz szablon

Utworzenie szabonu metryki wymaga wprowadzenia następujących parametrów:

- **Kategoria**: Wybór kategorii szablonu (urządzenia, procesy, sieć, ManagementServer, drukarka lub urządzenie SNMP).
- **Metryka**: W zależności od kategorii pole wyboru oferuje różne statystyki dla szablonu metryk.
- **Nazwa**: Nazwa szablonu.
- **Komentarz**: Informacje ułatwiające identyfikację szablonu.

W zależności od wybranej kategorii i rodzaju metryki mogą być potrzebne dodatkowe informacje:

- **Cel**: Urządzenie docelowe, na którym gromadzone będą dane pomiarowe. Tej wartości nie można zmodyfikować i zazwyczaj ustawiona jest domyślnie na **localhost**. Oznacza to, że pomiar zapisywany jest na urządzeniu powiązanym z szablonem.
- **Nazwa hosta**: Nazwa urządzenia, na którym dokonywany jest pomiar. Nie musi być to urządzenie powiązane z szablonem. Można ustawić tu więcej niż jedno urządzenie, aby rozszerzyć horyzont pomiaru; dla każdego hosta zostanie utworzona odrębna metryka.
- **URL**: Adres URL dla którego będą gromadzone statystyki. Można ustawić tu więcej niż jeden adres URL - w takim przypadku utworzonych zostanie więcej metryk.
- **Instancja SQL Server**: Metryka do pomiaru statystyk serwerów SQL. Kliknij ikonę lupy, aby otworzyć okno z listą dostępnych serwerów SQL.



- **Wartość progowa**: Wartość odniesienia dla metryki. Metryka może alarmować o osiągnięciu wartości wyższej lub niższej niż próg.
- **Indeks CPU**: Umożliwia określenie jednego lub wszystkich procesorów do nadzorowania.
- **Napęd**: Umożliwia określenie jednego lub wszystkich napędów do nadzorowania.
- **Nazwa procesu**: Umożliwia określenie jednego lub wszystkich procesów do nadzorowania.
- **Karta sieciowa**: Określ, którą kartę chcesz nadzorować lub wprowadź ***** aby objąć pomiarem wszystkie interfejsy.
- **Baza SQL Server**: Umożliwia określenie jednej lub wszystkich baz danych do nadzorowania.
- **Timeout**: Określ parametr przekroczenia czasu dla zapytań **ping**.
- **Rozszerzony kod status HTTP**: Jeśli metryka stwierdzi inny niż ustawiony kod statusu HTTP, odpowiednio zmieni się jej stan - potraktuje go jak wartość progową.
- **SNMP Community**: Wprowadź wartość odpowiednią dla urządzenia SNMP. Wartości określane są przez producentów urządzeń i można je zazwyczaj znaleźć w dokumentacji.

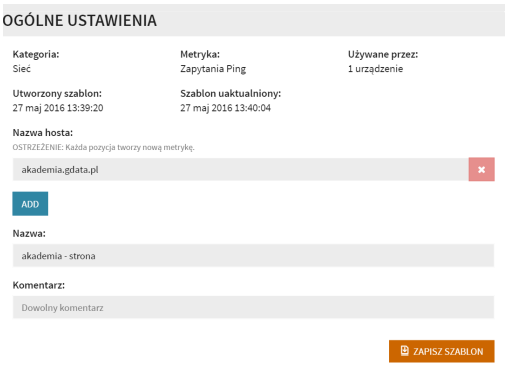
Sekcja Ustawienia powiadomień umożliwia konfigurację wyzwalaczy i wybór grup docelowych adresatów powiadomień mailowych:

- **Warunek powiadomienia**: Powiadomienie może być wysyłane po przejściu metryki w stan krytyczny lub po zmianie stanu na ostrzeżenie.
- **Powiadamiaj tylko zaznaczone grupy e-mail**: Jeśli utworzone zostaną

różne grupy odbiorców powiadomień, można w tym miejscu wskazać grupy odpowiednie dla skonfigurowanego szablonu.

Edytuj szablon

Niektóre parametry szablonu możemy zmodyfikować po jego utworzeniu.



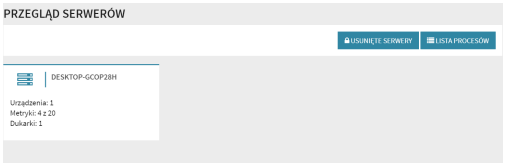
Tych parametrów nie da się zmienić:

- **Kategoria**
- **Metryka**
- **Używane przez**
- **Cel**
- **Nazwa hosta**
- **URL**

Pozostałe ustawienia można edytować. Po dokonaniu edycji kliknij przycisk **Zapisz szablon**. Zmiany zostaną zastosowane dla wszystkich metryk utworzonych na podstawie szablonu.

10.2.1.3 Przegląd serwerów

Ten widok przedstawia listę wszystkich serwerów zarządzających powiązanych z kontem w usłudze ActionCenter. Wyświetlone są tu również informacje o ilości nadzorowanych urządzeń, metryk i drukarek.



Po kiknięciu nazwy serwera otwiera się okno zawierające szczegóły na jego temat. Dostępne informacje:

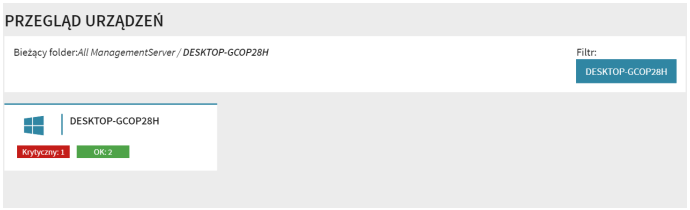
- **Nazwa hosta**: Nazwa hosta składnika ManagemetServer.
- **Wersja**: Numer wersji składnika ManagemetServer.
- **Ostatnia próba dostępu**: Moment ostatniej synchronizacji danych serwera z usługą ActionCenter.
- **Metryki**: Ilość zastosowanych metryk.
- **Urządzenia**: Ilość powiązanych urządzeń.
- **Drukarki**: Ilość powiązanych drukarek.
- **Komentarz**: Informacje ułatwiające identyfikację serwera.
- **Dostęp API**: Domyślnie włączony. Jeśli wyłączysz dostęp API, serwer pozostanie widoczny w ActionCenter, ale nie będzie przekazywał wartości pomiarowych.
- **Tagi**: Tagi umożliwiają identyfikację serwerów oraz filtrowanie ich w innych widokach.

Przycisk **Ustaw uprawnienia** umożliwia delegowanie uprawnień do danego serwera zarządzającego innym użytkownikom usługi ActionCenter. Wprowadź adres mailowy konta i kliknij przycisk **Wyślij zaproszenie** aby wydelegować uprawnienia. Po ponownym zalogowaniu do ActionCenter odbiorca zaproszenia uzyska dostęp do odczytu danych pomiarowych delegowanego serwera. Za pomocą przycisku **Usuń** można usunąć delegację uprawnień dla danego konta.

Jeśli użytkownik, który otrzymał zaproszenie nie ma konta w usłudze ActionCenter, może je założyć. Po założeniu konta może akceptować zaproszenie aby uzyskać dostęp do danych.

10.2.1.4 Przegląd urządzeń

Widok **Przegląd urządzeń** umożliwia zarządzanie wszystkimi urządzeniami powiązanymi z serwerami zarządzającymi zgłoszonymi w usłudze ActionCenter.



Pod każdym urządzeniem widnieje lista przypisanych do niego metryk. Klikając wybraną nazwę metryki przenosimy się bezpośrednio do okna szczegółów metryki.

10.2.2 Uprawnienia

Aplikacja **Uprawnienia** przedstawia listę kont, które otrzymały delegację uprawnień do aplikacji Network Monitoring. Aby usunąć delegację dla konta, kliknij przycisk **Usuń** po prawej stronie.

10.2.3 Grupy e-mail

Aplikacja **Grupy e-mail** umożliwia tworzenie i edytowanie grup adresów mailowych wykorzystywanych do automatycznych powiadomień aplikacji Network Monitoring.

Kliknij przycisk **Dodaj grupę e-mail**, aby utworzyć nową grupę dystrybucyjną. Wprowadź nazwę grupy aby przejść dalej. Edycja grupy umożliwia dodawanie dowolnej ilości adresów mailowych a także wybór języka obsługi.

Utwórz więcej grup, jeśli potrzebujesz zdywersyfikować wysyłanie powiadomień modułu Network Monitoring.

11 G DATA MailSecurity

G DATA MailSecurity to pakiet oprogramowania służącego do ochrony strumienia poczty elektronicznej.

- **G DATA MailSecurity**: Brama poczty (SMTP proxy) filtrująca ruch POP3 i SMTP pod kątem spamu i szkodliwego oprogramowania. Działa niezależnie od rodzaju serwera poczty, potrafi filtrować ruch również generowany przez serwery poczty działające w innych niż Windows systemach operacyjnych.
- **G DATA MailSecurity Administrator**: Konsola zarządzająca bramą.

Konfiguracja programu

Po zainstalowaniu program jest gotowy do konfiguracji. Program kontroluje przychodzące i wychodzące wiadomości SMTP i POP3 na obecność spamu, wirusów, złośliwych programów oraz niechcianych treści. Poza tym program pobiera automatycznie najnowsze sygnatury wirusów i aktualizacje programu przez Internet. Wraz z pośrednikiem poczty w systemie instalowany jest automatycznie składnik G DATA MailSecurity Administrator, czyli jego graficzny interfejs. Administrator umożliwia modyfikowanie ustawień programu i podgląd statystyk.

Możesz dodatkowo zainstalować składnik G DATA MailSecurity Administrator na dowolnym komputerze w sieci spełniającym wymagania programu. Umożliwi to zarządzanie ochroną bezpośrednio z tego komputera.

Protokoły poczty elektronicznej

Odbiór i wysyłka wiadomości elektronicznych zachodzi z reguły przy użyciu protokołów SMTP i POP3. SMTP (Simple Mail Transfer Protocol) służy do wysyłania wiadomości, podczas gdy POP3 (Post Office Protocol 3) odbiera i przechowuje wiadomości w specjalnej skrzynce pocztowej zabezpieczonej hasłem przez użytkownika.

W zależności od budowy Twojej sieci, MailSecurity chroni strumień wiadomości w różnych jej miejscach:

- Jeśli korzystasz z serwera SMTP, MailSecurity ma możliwość kontroli wiadomości jeszcze zanim wpłyną do serwera pocztowego. Konfiguracja tej opcji dostępna jest w zakładce **Przychodzące (SMTP)**.
- Jeżeli odbierasz pocztę elektroniczną bezpośrednio przez protokół POP3 (np. poprzez zbiorcze konto POP3), MailSecurity może skanować maile zanim zostaną otwarte przez użytkownika. Konfiguracja tej opcji dostępna jest w zakładce **Przychodzące (POP3)**.

Program może także dokonywać kontroli wychodzących wiadomości przed wysłaniem do adresata. Konfiguracja tej opcji dostępna jest w zakładce **Wychodzące (SMTP)**.

11.1 G DATA MailSecurity Administrator

Składnik G DATA MailSecurity Administrator jest graficznym interfejsem programu G DATA MailSecurity, umożliwiającym zarządzenie kompleksową ochroną protokołów SMTP i POP3. Jeżeli składnik Administrator zainstalowany jest na innym komputerze niż główny składnik G DATA MailSecurity, w oknie logowania należy wpisać nazwę komputera z zainstalowaną bramą poczty. Dostęp do G DATA MailSecurity można zabezpieczyć hasłem.

11.1.1 Uruchamianie programu (logowanie)

Aby uruchomić moduł sterujący programem G DATA MailSecurity Administrator, kliknij skrót na pulpicie lub uruchom polecenie G DATA MailSecurity w grupie programowej menu Start > Wszystkie programy > G DATA MailSecurity. Przy pierwszym uruchomieniu program zapyta o nazwę serwera oraz hasło.

W polu **Serwer** wpisz nazwę lub adres IP komputera, na którym zainstalowany jest program G DATA MailSecurity. Jeżeli nie chcesz ustawiać hasła dostępu do programu, po prostu kliknij przycisk OK bez wpisywania hasła, a następnie kliknij klawisz **Anuluj**.

Hasło można ustawić lub zmodyfikować w oknie Opcje > Inne klikając przycisk Zmień hasło.

11.2 Konfiguracja G DATA MailSecurity Administrator

Pasek menu programu G DATA MailSecurity Administrator oferuje następujące polecenia:

- Opcje: Możliwość dostosowania podstawowych ustawień sterowania programem oraz dopasowania ich do własnych potrzeb.
- Filtr spamu: Filtr spamu umożliwia skuteczne blokowanie wiadomości o określonych treściach

lub pochodzące od niepożądanych nadawców.

- Aktualizacja: Opcje i ustawienia związane z pobieraniem aktualizacji baz wirusów oraz plików programowych przez Internet. Istnieje możliwość zaplanowania automatycznych aktualizacji programu MailSecurity.
- Pomoc: Wywołanie pliku pomocy.
- Informacje: Informacje o wersji programu.

11.2.1 Opcje

Ustawienia zawarte w zakładkach okna **Opcje** pozwalają na optymalne dostosowanie pracy programu MailSecurity do warunków panujących w Twojej sieci. Wszystkie opcje pogrupowane są tematycznie w zakładkach. Kliknij wybraną zakładkę aby otworzyć grupę opcji.

Po kliknięciu przycisku OK zmiany zostaną zatwierdzone, a okno opcji zamknięte. Przycisk Anuluj spowoduje powrót do poprzednich ustawień i zamknięcie okna opcji. Przycisk **Zastosuj** zatwierdza zmiany i pozostawia okno otwarte. Poszczególne ustawienia wyjaśnione zostały w następnych rozdziałach.

11.2.1.1 Przychodzące (SMTP)

W tej zakładce można dokonać ustawień związanych z przepływem oraz kontrolą wysyłanych wiadomości SMTP przed wysłaniem na serwer.

Odbiór

W polu **Port poczty przychodzącej** wpisz numer portu, używanego do odbierania poczty w Twojej sieci. Zazwyczaj stosowany jest port 25 i tak domyślnie ustawiony jest port odbioru w programie. Jeśli jest to wymagane, można zmodyfikować numer portu oraz inne ustawienia protokołu klikając przycisk **Konfiguracja....**

Przesyłanie

Aby przesyłać wiadomości do serwera pocztowego, wyłącz opcję Użyj serwera DNS do wysyłania wiadomości i w polu **Przekazuj wiadomości na ten serwer SMTP** wpisz nazwę serwera poczty. Należy wskazać również port, po którym poczta będzie wysyłana. Jeśli masz do dyspozycji więcej niż jedną kartę sieciową, możesz wskazać pożądane urządzenie w polu IP nadawcy.

Ochrona przed przesyłaniem

Aby zapobiec wysyłaniu spamu z Twojego serwera poczty, możesz ograniczyć przesyłanie wiadomości wysyłanych do nieznanych domen. W polu Akceptuj przychodzące wiadomości tylko dla następujących domen oraz adresów wpisz nazwy domen, do których serwer poczty może przesyłać wiadomości.

Uwaga: Jeśli nie dodasz żadnej domeny, program nie będzie odbierał wiadomości. Jak chcesz odbierać wiadomości dla wszystkich domen, wpisz wartość *.*.

Ochronę przed przesyłaniem można realizować również poprzez listę adresów e-mail. Wiadomości nie będą przesyłane do odbiorców, których nie ma na liście. Przydatnym narzędziem jest możliwość automatycznego pobierania adresów z Active Directory. Do połączenia z usługą Active Directory wymagana jest platforma .NET Framework w wersji 1.1 lub nowszej.

11.2.1.2 Wychodzące (SMTP)

W tej zakładce można dokonać ustawień związanych z przepływem oraz kontrolą wiadomości wychodzących SMTP.

Odbiór

Zaznacz opcję **Edycja poczty wychodzącej** aby uruchomić kontrolę poczty wychodzącej na obecność wirusów. W polu Adresy IP lub podsieci komputerów wysyłających wiadomości wpisz adresy IP komputerów, z których wysyłane będą maile. Dane te są niezbędne w celu odróżnienia poczty przychodzącej od wychodzącej. Zazwyczaj stosowany jest port 25 i tak domyślnie ustawiony jest port odbioru w programie. Jeśli jest to wymagane, można zmodyfikować numer portu oraz inne ustawienia protokołu klikając przycisk Konfiguracja...

Przesyłanie

Aby wiadomości były przesyłane bezpośrednio do domeny docelowej, należy włączyć opcję **Użyj serwera DNS do wysyłania wiadomości**. Jeśli strumień wiadomości ma przechodzić przez inny serwer (np providera), należy wyłączyć opcję używania serwera DNS i wpisać nazwę serwera w polu Przekazuj wiadomości na ten serwer SMTP. Jeśli masz do dyspozycji więcej niż jedną kartę sieciową, możesz wskazać pożądane urządzenie w polu IP nadawcy.

11.2.1.3 Przychodzące (POP3)

W tej zakładce można dokonać ustawień związanych z przepływem oraz kontrolą wiadomości przychodzących POP3.

Zapytania

Uruchom opcję **Edycja poczty przychodzącej POP3** aby włączyć ochronę antywirusową wiadomości przychodzących. Po skanowaniu poczta jest przesyłana do odbiorców. Należy wskazać port wykorzystywany przez Twój program pocztowy do komunikacji z serwerem POP3 (zazwyczaj 110), a w polu Odbieraj pocztę z tego serwera POP3, nazwę serwera poczty POP3 (np. pop3.mojapoczta.pl). Funkcja Ignoruj limit czasu połączenia w programie pocztowym daje klientowi poczty więcej czasu na odbiór wiadomości podczas gdy MailSecurity je skanuje.

Wskazówka: Programy pocztowe oparte o protokół POP3 można skonfigurować ręcznie. Jako nazwę serwera POP3 należy wpisać 127.0.0.1 lub adres komputera z programem MailSecurity, a nazwę użytkownika trzeba poprzedzić nazwą zewnętrznego serwera poczty i dwukropkiem.

Czyli zamiast

POP3:poczta.xxx.pl / Użytkownik:Jan Nowak

należy wpisać

POP3:127.0.0.1 / Użytkownik:poczta.xxx.pl:Jan Nowak.

Dokładny opis ręcznej konfiguracji znajdziesz w dokumentacji technicznej danego programu pocztowego.

Odbieranie

W polu **Odbieraj pocztę z tego serwera POP3** wprowadź serwer POP3, z którego chcesz odbierać pocztę (np. pop3.dostawca.pl).

Filtr

Jeżeli wiadomość POP3 zostanie zatrzymana przez filtr treści lub skaner antywirusowy, nadawca wiadomości może zostać o tym powiadomiony. Treść standardowego powiadomienia brzmi: Wiadomość odrzucona przez administratora.

Aby zmienić treść powiadomienia, należy kliknąć przycisk ••• obok opcji powiadomienia i skonstruować nową treść. Dozwolone jest używanie znaków specjalnych zastępujących parametry wiadomości:

- %v Wirus
- %s Nadawca
- %r Odbiorca
- %c DW
- %d Data
- %u Temat
- %h Nagłówek
- %i IP nadawcy

11.2.1.4 Skanowanie

Opcje w tej zakładce dotyczą ustawień kontroli antywirusowej wiadomości przychodzących i wychodzących.

Przychodzące

Zaleca się uruchomienie opcji Szukaj wirusów w przychodzących wiadomościach oraz wybór reakcji na wykrycie wirusa:

- Tylko protokół
- Dezynfekuj (Jeśli się nie da: tylko protokół)

- Dezynfekuj (Jeśli się nie da: zmień nazwę pliku)
- Dezynfekuj (Jeśli się nie da: usuń plik)
- Zmień nazwy zarażonych załączników
- Usuń zarażone załączniki
- Usuń wiadomość

Ustawienie Tylko protokół ma sens tylko wtedy, gdy system jest chroniony przed wirusami w inny sposób (np. programem G DATA AntiVirus Business).

Do dyspozycji jest szereg możliwości konstruowania powiadomień o wykryciu wirusa. Do powiadomienia adresata można dołączyć m.in. temat oraz treść zarażonej przesyłki. Powiadomić daje się także nadawcę zarażonego maila, a także wybrane osoby, np. administratora systemu. Adresy odbiorców powiadomień oddziel przy wpisywaniu średnikami.

Aby zmienić treść powiadomienia, należy kliknąć przycisk ••• obok opcji powiadomienia i skonstruować nową treść. Dozwolone jest używanie znaków specjalnych zastępujących parametry wiadomości:

- %v Wirus
- %s Nadawca
- %r Odbiorca
- %c DW
- %d Data
- %u Temat
- %h Nagłówek
- %i IP nadawcy

Wychodzące

Funkcja **Szukaj wirusów w wychodzących wiadomościach** oraz **Nie przesyłaj zainfekowanych wiadomości** powinny być stale włączone. Dzięki temu żaden wirus nie zostanie wysłany z Twojej sieci.

Do dyspozycji jest szereg możliwości konstruowania powiadomień o wykryciu wirusa. Do powiadomienia adresata można dołączyć m.in. temat oraz treść zarażonej przesyłki. Powiadomić daje się także nadawcę zarażonego maila, a także wybrane osoby, np. administratora systemu. Adresy odbiorców powiadomień oddziel przy wpisywaniu średnikami. Aby zmienić treść powiadomienia, należy kliknąć przycisk ••• obok opcji powiadomienia i

skonstruować nową treść. Dozwolone jest używanie znaków specjalnych zastępujących parametry wiadomości:

- %v Wirus
- %s Nadawca
- %r Odbiorca
- %c DW
- %d Data
- %u Temat
- %h Nagłówek
- %i IP nadawcy

Dodatkowo można uruchomić opcję dołączania raportu o dokonanej kontroli przez MailSecurity do wysyłanych, niezawirusowanych wiadomości. Oczywiście istnieje możliwość modyfikacji lub wyłączenia komunikatu powiadomienia.

G DATA ManagemenServer

Jeśli stosujesz program G DATA ManagementServer, możesz uaktywnić opcję Powiadom o infekcji program G DATA. Komunikacja między tymi programami zwiększy bezpieczeństwo Twojej sieci.

11.2.1.5 Parametry skanowania

W tym oknie można dopasować parametry skanowania wiadomości do potrzeb Twojej sieci. Zwiększenie wydajności skanowania powoduje nieznaczne spowolnienie strumienia wiadomości.

Program MailSecurity pracuje przy użyciu dwóch niezależnych skanerów antywirusowych, odpowiedzialnych za różne partie analizy antywirusowej. Optymalne efekty daje oczywiście zastosowanie dwóch skanerów. Przy użyciu tylko jednego z nich, proces trwa krócej. Zalecamy ustawienie Dwa skanery. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor.

Dzięki tej opcji istnieje możliwość wskazania rodzajów skanowanych plików. Z reguły nie ma potrzeby kontroli plików, które się nie uruchamiają, kontrola całego systemu plików może zająć dość dużo czasu. Zaleca się ustawienie Automatyczne rozpoznanie plików – sprawdzone zostaną tylko pliki mogące teoretycznie zawierać wirusa.

Możesz samodzielnie zdefiniować rodzaje plików, które mają być uwzględnione podczas skanowania. W tym celu wybierz opcję Pliki użytkownika. Kliknij przycisk ... aby otworzyć okno, wyboru plików. Wpisane rozszerzenia zatwierdza przycisk Dodaj.

Możliwe jest stosowanie masek plików z wykorzystaniem następujących znaków zastępczych:

? zastępuje pojedynczy znak

* zastępuje ciąg znaków

Aby wybrać np. wszystkie pliki z rozszerzeniem .exe, wpisz *.exe. Aby wybrać np. wszystkie pliki o formacie arkuszy kalkulacyjnych (jak np. *.xlr, *.xls), wpisz *.xl?. Jeśli chcesz sprawdzać pliki o takim samym początku nazwy wpisz np. tekst*.*.

Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując kody plików z kodami stale aktualizowanej bazy znanych wirusów, lecz rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, z jednej strony wzmaga skuteczność skanowania, ale jest bardzo czasochłonna, a w niektórych przypadkach może powodować fałszywe alarmy.

Zalecamy również pozostawienie włączonej opcji skanowania spakowanych plików.

OutbreakShield

Moduł OutbreakShield umożliwia rozpoznanie i zwalczanie wirusów jeszcze przed opracowaniem odpowiednich sygnatur wirusów. Moduł OutbreakShield łącząc się z odpowiednim serwerem ustala czy wiadomość stanowi zagrożenie na podstawie jej cech charakterystycznych. Dzięki temu jest w stanie zareagować na zagrożenie dużo wcześniej przed stworzeniem i dostarczeniem odpowiednich sygnatur wirusów. Moduł jest zintegrowany z ochroną poczty elektronicznej.

Ze względu na specyficzną budowę, moduł OutbreakShield nie potrafi dezynfekować wiadomości, przenosić ich do Kwarantanny ani też zmieniać nazw załączników. Użytkownik informowany jest o infekcji przez tekst zastępczy. Jeśli w oknie Kontrola antywirusowa wybrana zostanie opcja Usuń wiadomość, OutbreakShield nie ma możliwości poinformowania użytkownika o wykryciu wirusa.

11.2.1.6 Kolejka

Ta zakładka pozwala ustalić w jakich odstępach czasowych zachodzić ma proces ponownego wysyłania wiadomości czekających w kolejce. Wiadomości zatrzymywane są w kolejce z różnych przyczyn. Np. dlatego, że adresat (albo serwer poczty) w danej chwili jest niedostępny.

Wiadomości umieszczane są w kolejce po przeprowadzeniu kontroli antywirusowej przez program MailSecurity.

Niedoręczone wiadomości

W polu **Interwał czasowy** wpisz, w jakich odstępach czasu program ma podejmować kolejne próby wysłania wiadomości przetrzymywanych w kolejce. Np. wpis 1, 1, 1, 4 spowoduje, że program podejmie próbę wysłania trzykrotnie co godzinę, a następnie będzie próbował co 4 godziny. W polu **Czas oczekiwania na błąd (h)** zdefiniuj czas, który upłynie zanim program ostatecznie usunie wiadomość z kolejki.

Istnieje również opcja powiadamiania nadawców wiadomości w określonych w polu numerycznym odstępach czasu. Jeśli nie chcesz regularnie powiadamiać nadawców, wpisz w pole wartość zero. Nawet jeśli powiadamianie zostanie wyłączone, nadawca zostanie i tak powiadomiony o nie doręczeniu wiadomości i jej usunięciu z serwera.

Przywrócenie standardowych ustawień kolejki uzyskuje się przez kliknięcie przycisku Przywróć domyślne.

Ograniczenie rozmiaru

Program umożliwia ograniczenie rozmiaru kolejki. Dzięki temu można uniknąć przepełniania kolejki w momencie przetwarzania dużych ilości wiadomości - np. w razie ataku typu Denial of Service.

11.2.1.7 Zaawansowane

W tej zakładce znajdziesz globalne ustawienia programu MailSecurity.

Banner SMTP

W polu **Domena** możesz wprowadzić nazwę komputera lub w pełni kwalifikowaną nazwę z rozszerzeniem domeny (FQDN). Jest to niezbędne w przypadku wysyłania wiadomości za pomocą serwera DNS w celu umożliwienia wykonania reverse lookup.

Włącz funkcję **Pokaż tylko domenę**, aby ukryć wyświetlanie wersji serwera podczas komunikacji z innymi serwerami.

Ograniczenie

Włącz tę opcję, jeśli chcesz ograniczyć liczbę połączeń SMTP obsługiwanych przez MailSecurity. W ten sposób możesz dopasować filtrowanie wiadomości do wydajności sprzętu, na którym pracuje program.

Komunikaty systemowe

Adres nadawcy wiadomości systemowych wykorzystywany jest np. przy wysyłaniu powiadomień do nadawców i odbiorców zarażonych wiadomości. Program wysyła także niezależne od powiadomień komunikaty wiążące się z potencjalnymi zagrożeniami ze strony wirusów. Użytkownicy są także ostrzegani, jeśli ochrona antywirusowa przestaje działać z jakichkolwiek powodów. Adresy odbiorców ostrzeżeń systemowych mogą się np. pokrywać z adresami używanymi przez protokoły SMTP i POP3.

Ustawienia

Przyciski dostępne w tej zakładce umożliwiają import oraz eksport wszystkich ustawień programu do pliku XML.

Zmień hasło

Ta opcja pozwala zmienić hasło ustalone przy pierwszym uruchomieniu programu MailSecurity. Wystarczy podać aktualne hasło, w polu poniżej nowe, a na samym dole potwierdzić nowe hasło.

11.2.1.8 Rejestrowanie

Opcje w zakładce Rejestrowanie dotyczą przechowywania raportów usługi statystyk poczty. Ustawienia pozwalają ograniczyć rozmiary bazy danych z raportami. Podgląd okna statystyk dostępny jest poprzez kliknięcie przycisku Statystyki w widoku Status. Opcja zapisywania w pliku log uruchamia dodatkowo zapis raportów w pliku tekstowym. Rozmiar pliku tekstowego można ograniczyć za pomocą opcji Tylko spam lub poprzez wprowadzenie limitu ilości przechowywanych wiadomości.

11.2.2 Aktualizacja

W oknie aktualizacji można dokonać ustawień dotyczących pobierania aktualizacji sygnatur wirusów oraz plików programowych przez Internet.

11.2.2.1 Sekcja Ustawienia

Jeśli równocześnie z programem G DATA MailSecurity używasz programu G DATA Business, możesz wykorzystywać w programie funkcję Zastosuj bazy wirusów programu G DATA Security Client. Dzięki temu unikniesz podwójnego pobierania aktualizacji baz z Internetu. Oczywiście możliwe jest też pobieranie baz wirusów bezpośrednio z serwera aktualizacji.

Przycisk **Ustawienia i planowanie** otwiera okno podstawowych ustawień ręcznej i automatycznej aktualizacji programu.

Dane dostępu do aktualizacji

W polach zakładki Dane dostępu wpisz nazwę użytkownika i hasło otrzymane na potwierdzeniu rejestracji programu. Jeżeli zamierzasz teraz zarejestrować program, kliknij przycisk Rejestracja online....

Do zarejestrowania programu potrzeby jest numer rejestracyjny. Znajdziesz go w opakowaniu z zakupionym programem lub w wiadomości z realizacją zamówienia w przypadku dokonania zakupu online. Po zarejestrowaniu produktu, dane dostępu zostaną automatycznie zastosowane w programie, a także wysłane na wpisany w formularzu adres mailowy.

Planowanie

Zakładka Planowanie umożliwia ustalenie częstotliwości przeprowadzania automatycznych aktualizacji. W sekcji Wykonaj zaznacz pożądany interwał czasowy i uzupełnij szczegóły, np. godzinę i dni tygodnia, w które ma przebiegać proces aktualizacji.

Ustawienia

Jeżeli używasz urządzenia sieciowego wymagającego autoryzacji lub serwera proxy, zaznacz opcję Skorzystaj z serwera proxy. Wpisz adres serwera i port w odpowiednich polach. Jeżeli niezbędna jest autoryzacja, wpisz również nazwę użytkownika oraz hasło.

Konto użytkownika

Jeśli jest to wymagane, w polu Konto użytkownika wpisz nazwę użytkownika z dostępem do Internetu na komputerze z zainstalowanym programem G DATA MailSecurity.

11.2.2.2 Sekcja sygnatury wirusów

Za pomocą przycisków **Aktualizacja baz wirusów** i **Odśwież status** możesz przeprowadzić aktualizację niezależnie od zaplanowanych aktualizacji automatycznych.

11.2.2.3 Sekcja pliki programu

Przyciskiem **Aktualizacja plików** możesz uruchomić aktualizację plików programu G DATA MailSecurity, oczywiście jeśli udostępniona jest nowsza wersja.

11.2.3 Widoki składnika Administrator

Interfejs programu jest skonstruowany przejrzyście i intuicyjnie. Całość podzielona jest na tematyczne okna widoków, przełączane w panelu po lewej stronie:

 Status

 Filtr

 Kolejki

 Działanie

 Wykryte wirusy

11.2.3.1 Widok Status

W oknie statusu znajduje się spis podstawowych informacji o stanie systemu komputera oraz MailSecurity.

Taki symbol widnieje z lewej strony pozycji listy spełniającej optimum wymogów bezpieczeństwa komputera.

Jeśli któryś ze składników nie jest zoptymalizowany (np. nieaktualne sygnatury wirusów), obok jego opisu pojawia się symbol ostrzeżenia.

Aby dokonać zmian w ustawieniach, kliknij dwukrotnie opis pożądanego składnika lub przejdź do odpowiedniego okna programu (ewentualnie wybierz składnik i kliknij przycisk Edycja).

Lista okna statusu obejmuje pozycje:

- **Edycja poczty przychodzącej**: Jeśli opcja jest aktywna, program ma dostęp do poczty przychodzącej zanim dostanie się ona do użytkownika. Klikając dwukrotnie opis otworzysz okno ustawień. Patrz też rozdział Opcje > Przychodzące (SMTP).
- **Kontrola poczty przychodzącej**: Skanowanie przychodzących wiadomości zapobiega przedostaniu się zawartych w nich wirusów do Twojej sieci. Klikając dwukrotnie opis otworzysz okno ustawień.
- **Edycja poczty wychodzącej**: Jeśli opcja jest aktywna, program ma dostęp do poczty wychodzącej zanim zostanie ona wysłana do odbiorcy. Klikając dwukrotnie opis otworzysz okno ustawień. Patrz też rozdział Opcje > Wychodzące (SMTP).
- **Kontrola poczty wychodzącej**: Skanowanie przychodzących wiadomości zapobiega wysyłaniu wirusów. Klikając dwukrotnie opis otworzysz okno ustawień.
- OutbreakShield umożliwia rozpoznanie i zwalczanie wirusów jeszcze przed opracowaniem odpowiednich sygnatur wirusów. Moduł OutbreakShield łącząc się z odpowiednim serwerem ustala czy wiadomość stanowi zagrożenie na podstawie jej cech charakterystycznych. Dzięki temu jest w stanie zareagować na zagrożenie dużo wcześniej przed stworzeniem i dostarczeniem odpowiednich sygnatur wirusów. Moduł jest zintegrowany z ochroną poczty elektronicznej.
- **Automatyczna aktualizacja**: Generalnie zaleca się włączenie opcji automatycznej aktualizacji. Klikając dwukrotnie opis otworzysz okno ustawień. Patrz też rozdział Aktualizacja.
- **Data ostatniej aktualizacji**: Im nowsze bazy wirusów, tym skuteczniejsza ochrona przed wirusami. Należy przeprowadzać aktualizacje tak często jak się da. Klikając dwukrotnie opis otworzysz okno ustawień. Patrz też rozdział Aktualizacja.
- Filtr spamu umożliwia skuteczne wykrywanie i blokowanie wiadomości zawierających niepożądane treści lub pochodzące od niechcianych nadawców.

- **Spam-OutbreakShield**: Jest to moduł, który skutecznie wykrywa i blokuje wiadomości masowe. Łącząc się z odpowiednim serwerem ustala czy wiadomość jest powiązana z wysyłką masową.

Podczas instalacji programu, możesz zdecydować, czy chcesz zainstalować składnik prowadzący szczegółowe statystyki strumienia poczty. Statystyki poczty dostępne są do wglądu po kliknięciu przycisku **Statystyki** w widoku **Statusu**. Opcje statystyk można modyfikować w zakładce Opcji o nazwie Baza danych.

11.2.3.2 Widok Filtr

Widok **Filtr** umożliwia definiowanie kryteriów filtrowania, zatrzymywania i usuwania wiadomości przychodzących i wychodzących. Kliknij przycisk Nowy... aby utworzyć nowy filtr lub Edycja aby zmodyfikować zapisane ustawienia.

Lista zdefiniowanych filtrów znajduje się w środkowej części okna. Aktywne filtry oznaczone są haczykami w polach przed ich nazwami. Klikając pole przed nazwą filtra możesz go włączyć lub wyłączyć.

W dolnej części okna znajduje się szereg przycisków ułatwiających zarządzanie filtrami.

- **Import**: Przycisk umożliwia wczytanie zapisanego wcześniej zestawu filtrów z pliku XML.
- **Eksport**: Przycisk służy do eksportowania zdefiniowanych filtrów do pliku w formacie XML. Zaznacz filtry, które chcesz wyeksportować i kliknij przycisk Eksport. Aby zaznaczyć więcej niż jeden filtr, przytrzymaj klawisz Ctrl lub Shift.
- **Nowy**: Kliknij ten przycisk aby utworzyć nowy filtr. W oknie wyboru zaznacz pożądany szablon, na podstawie którego chcesz utworzyć nowy filtr. Informacje o poszczególnych szablonach i objaśnienia ustawień znajdziesz kolejnych rozdziałach.
- **Edycja**: Zaznacz filtr, który chcesz zmodyfikować i kliknij przycisk Edycja, aby zmienić ustawienia filtra.
- **Usuń**: Ten przycisk umożliwia usunięcie zaznaczonego filtra.
- **Statystyki**: Zaznacz jeden filtr i kliknij ten przycisk, aby wyświetlić okno statystyk dotyczących stosowania filtra.
- **Protokół**: Wbudowany filtr (Filtr spamu) wyposażony jest w narzędzie raportujące wydarzenia związane z filtrowaniem wiadomości. Protokołowane są wiadomości zaindeksowane przez program jako niechciane. Z okna protokołu można dowiedzieć się, jakie kryteria wykrywania spamu zadecydowały o detekcji (wartości indeksów spamu). To okno umożliwia zgłoszenie fałszywego wykrycia wysyłki masowej do serwera OutbreakShield. Wiadomość zostanie w takim przypadku powtórnie przeskanowana. W

przypadku potwierdzenia błędu, program zakwalifikuje wiadomość jako niegroźną. Uwaga: Do serwera przykazywana jest tylko suma kontrolna wiadomości, nie zaś jej treść.

Niezależnie od stosowanych filtrów program G DATA MailSecurity skanuje pocztę elektroniczną na obecność złośliwego oprogramowania. Filtry dodatkowo minimalizują prawdopodobieństwo przedostania się do skrzynek pocztowych spamu, podejrzanych skryptów i reklam.

Nazwa i komentarz

Zalecamy stosowanie wymownych i jednoznacznych nazw podczas tworzenia filtrów. Można również skorzystać z opcji dodania komentarza, co pozwoli na łatwiejszą identyfikację filtrów w przyszłości

Reakcja

W sekcji Reakcja można ustalić, co program ma zrobić w momencie nadejścia wiadomości spełniającej regułę filtra.

Istnieje możliwość powiadomienia nadawcy wiadomości lub dowolnego użytkownika poczty o wykryciu anomalii w mailu.

Wiadomość z powiadomieniem można dowolnie skonstruować korzystając z oferowanych przez program zmiennych:

%s Nadawca

%r Odbiorca

%c DW

%d Data

%u Temat

%h Nagłówek

%i IP nadawcy

Filtr potwierdzeń odbioru

Ten filtr automatycznie usuwa uciążliwe żądania potwierdzenia odczytu wiadomości. Żądanie potwierdzenia odczytu wiadomości można wymusić za pomocą większości stosowanych programów do odbioru poczty.

Filtr skryptów HTML

Filtr wykrywa w wiadomościach HTML aktywne skrypty, które mogą pobierać i uruchamiać złośliwe programy.

Filtr zewnętrznych referencji

Bardzo często wiadomości w formacie HTML zawierają linki do danych, które uruchamiają się lub ukazują dopiero po otwarciu wiadomości. Mogą to być np. zdjęcia, nie wysyłane bezpośrednio w wiadomości, a pobierane w momencie jej otwarcia. Zdarza się też, że wiadomość zawiera link do złośliwego programu, strony lub nawet wirusa. Właśnie z tego względu zaleca się wyłączenie zewnętrznych referencji. Tekst wiadomości pozostaje bez zmian.

Filtr Greylist

Technologia zwana greylisting to wydajna metoda obniżania ilości niechcianych wiadomości. Wiadomości od nieznanych nadawców nie są dostarczane do adresatów przez serwer SMTP natychmiast po wysłaniu. Serwer dostarcza wiadomość dopiero po automatycznej próbie ponownego dostarczenia tej samej wiadomości. Jako że nadawcy spamu nie stosują zarządzania kolejkami, wiadomości nie są wysyłane powtórnie. Standardowe serwery pocztowe przetrzymują wiadomości przez określony czas i regularnie powtarzają próby wysłania.

- **Czas oczekiwania (w minutach)**: To ustawienie określa, jak długo serwer ma zwlekać z odebraniem wiadomości od nowego odbiorcy. Po upływie określonego czasu, ponowna próba dostarczenia wiadomości zakończy się sukcesem. Ostatecznie nadawca zostaje usunięty z listy Greylist i umieszczony na liście zaufanych nadawców - Whitelist. Wiadomości od nadawcy nie będą więcej blokowane. Dostarczanie wiadomości nie będzie opóźniane.
- **Czas życia (w dniach)**: Można określić czas, po upłynięciu którego adresat zostanie usunięty z zaufanej listy i znów trafi na "szarą listę". Licznik jest cofany do wskazanej wartości dla konkretnego nadawcy w momencie wysłania kolejnej wiadomości. Przykładowo, w przypadku comiesięcznych biuletynów informacyjnych, ustawienie wartości czasu życia powyżej 30 dni spowoduje, że nadawca biuletynu nigdy nie zostanie usunięty z zaufanej listy.

Z filtra **Greylist** można skorzystać tylko wtedy, gdy włączony jest również filtr spamu programu G DATA MailSecurity. Niezbędna jest również obecność bazy danych SQL na komputerze pełniącym rolę bramy poczty.

Filtr załączników

Opcja filtrowania załączników wiadomości oferuje wachlarz możliwości filtrowania załączników poczty oraz dokumentów. Większość wirusów rozprzestrzenia się właśnie przez pliki załącznika, zawierające ukryte pliki wykonywalne. Może to być zwykły plik EXE, lub też skrypt VBS ukryty w grafice, filmie lub pliku muzycznym. Podczas otwierania załączników należy zachować szczególną ostrożność. W wątpliwych przypadkach lepiej zwrócić się przed otwarciem pliku do nadawcy z pytaniem, czy naprawdę go wysyłał.

W polu Rozszerzenia plików można zdefiniować filtrowane typy plików. Najbardziej niebezpieczne są pliki wykonywalne (EXE oraz COM), można także uwzględnić duże formaty (MPEG, AVI, MP3, JPEG, ZIP) obciążające serwer pocztowy ze względu na swój rozmiar. Wszystkie rozszerzenia należy wpisywać oddzielając je średnikami: np. *.exe; *.dll.

Włączenie opcji Filtruj także zagnieżdżone wiadomości spowoduje filtrowanie wiadomości załączonych w innych wiadomościach. Zaleca się, aby opcja była zawsze włączona.

Jeśli zaznaczona zostanie opcja Zmień nazwy załączników, filtr nie będzie automatycznie usuwał wiadomości spełniających kryteria. Zmieniona zostanie nazwa pliku (przez dodanie rozszerzenia), co zapobiegnie jego uruchomieniu. Przed uruchomieniem załącznika, użytkownik będzie musiał zapisać go na dysku i zmienić nazwę na pierwotną. Jeśli natomiast opcja nie będzie zaznaczona, załączniki będą usuwane.

W polu **Dodaj** wpisz tekst, który ma zostać dodany do nazwy pliku (np. *.exe. danger). W polu Dodaj komunikat do w treści wiadomości można ustalić treść komunikatu dodawanego przez program do zmodyfikowanej wiadomości.

Filtr treści

Za pomocą tego narzędzia można odfiltrować i zablokować wiadomości zawierające w treści lub temacie określone ciągi znaków. Zdefiniuj regularne wyrażenie wpisując słowa kluczowe i ciągi znaków, na które program MailSecurity ma reagować, i określ Zakres wyszukiwania w odpowiednim polu. Następnie trzeba ustalić reakcję programu na wykrycie zdefiniowanego ciągu znaków (powiadomienie nadawcy, odrzucenie wiadomości, powiadamianie innych osób o uruchomieniu filtra zawartości).

Obok pola **Regularne wyrażenie** znajduje się przycisk Nowy.... Kliknij aby otworzyć edytor wyrażenia logicznego. Tekst można dowolnie skonfigurować dzięki zastosowaniu funkcji logicznych **I** oraz **LUB**. Wyrażenia oddzielone parametrem **I** muszą wystąpić jednocześnie, aby filtr zadziałał, parametr **LUB**

uruchomi filtr także jeśli tylko jedno z wyrażeń zostanie odnalezione.

W oknie Wyrażenie logiczne można ręcznie skonstruować dowolne wyrażenie logiczne przy użyciu znaków zastępujących funkcje logiczne:

LUB - znak rozdzielający |

I - (Shift + 7) &

Filtr nadawców

Filtr ten pozwala na zablokowanie wiadomości pochodzących od konkretnych nadawców lub z konkretnych domen. W polu **Adresy/Domeny** wystarczy wpisać adresy lub domeny oddzielone średnikiem. MailSecurity nie przepuści wiadomości pochodzących z wpisanych domen i kont.

Dzięki tej funkcji można odfiltrować również wiadomości wysłane bez wypełnionego pola nadawcy.

Filtr odbiorców

Filtr ten pozwala na zablokowanie wiadomości wysyłanych do konkretnych osób lub domen. W polu **Adresy/Domeny** wystarczy wpisać adresy lub domeny oddzielone średnikiem. MailSecurity nie przepuści wiadomości wychodzących, zaadresowanych do wpisanych domen i kont.

Dzięki tej funkcji można odfiltrować również wiadomości wysłane bez wypełnionego pola odbiorcy (np. wiadomości z wypełnionym jedynie polem DW (do wiadomości).

Filtr spamu

Filtr spamu umożliwia skuteczne i elastyczne blokowanie wiadomości o niepożądanych treściach lub pochodzących od niechcianych nadawców (np. konkretnych serwerów wysyłających spam). Program jest wyczulony na wszystkie cechy wiadomości typowe dla wysyłek masowych. Na podstawie wykrytych właściwości tworzony jest indeks spamu odzwierciedlający prawdopodobieństwo, że dana wiadomość jest spamem. Do dyspozycji jest szereg zakładek zawierających tematycznie pogrupowane funkcje filtra.

Filtr

Reakcja filtra spamu na stwierdzenie niechcianej wiadomości może zależeć od oszacowanego indeksu prawdopodobieństwa spamu. Program umożliwia trzy różne reakcje dla trzech progowych wartości indeksu.

W zależności od wysokości indeksu prawdopodobieństwa spamu szacowanego na podstawie określonych kryteriów, program dzieli wiadomości na 3 grupy. Reakcję dla każdej z nich można określić po kliknięciu przycisku Zmień.

Program może odrzucić wiadomość lub tylko dołączyć komunikaty w temacie i treści wiadomości. Dodatkowo można powiadomić nadawcę wiadomości o wysłaniu niechcianej przesyłki, a także powiadomić określone osoby, np. administratora o fakcie nadejścia niechcianej wiadomości. Program umożliwia modyfikację tekstu wszelkich komunikatów dołączanych do wiadomości i wysyłanych do konkretnych adresatów.

Zaufana lista

Lista zaufanych nadawców pozwala na utworzenie wyjątków programu w postaci adresów e-mail lub całych domen. Wprowadź zaufany adres e-mail lub domenę i kliknij przycisk Dodaj aby utworzyć wyjątek. Listę wyjątków można także wyeksportować i zaimportować z pliku *.txt.

Czarna lista

Ta zakładka umożliwia stworzenie listy blokowanych adresów e-mail i domen. Wpisz adres e-mail lub domenę, z której nie chcesz otrzymywać wiadomości i kliknij przycisk Dodaj. Listę blokowanych domen można wyeksportować a także zaimportować z pliku w formacie *.txt.

Realtime Blacklists

W Internecie istnieją strony publikujące listy adresów serwerów wysyłających spam. Zalecamy stosowanie standardowych adresów list Realtime Blacklists. To okno umożliwia również utworzenie wyjątków od reguły. Wpisz w oknie Nie używaj "czarnych list" dla następujących domen domenę, którą chcesz wyjąć spod ochrony programem i kliknij przycisk Dodaj.

Słowa kluczowe (temat)

W tej zakładce można zdefiniować słowa kluczowe, na które program ma zwrócić szczególną uwagę kontrolując tematy wiadomości. Jeśli w temacie wykryte zostanie choć jedno słowo zawarte na liście, program podniesie indeks prawdopodobieństwa spamu dla danej wiadomości. Listę można modyfikować za pomocą przycisków **Dodaj**, **Zmień** i **Usuń**. Listę wyrażeń kluczowych można importować i eksportować do pliku *.txt. Opcja **Znajdź tylko całe wyrazy** spowoduje, że program nie będzie reagował jeśli wykryje słowo kluczowe zawarte w innym wyrazie, np. "dick" w "dickens".

Słowa kluczowe (treść)

W tej zakładce można zdefiniować słowa kluczowe, na które program ma zwrócić szczególną uwagę kontrolując treść wiadomości. Jeśli w treści wykryte zostanie choć jedno słowo zawarte na liście, program podniesie indeks prawdopodobieństwa spamu dla danej wiadomości. Listę można modyfikować za pomocą przycisków **Dodaj**, **Zmień** i **Usuń**. Listę wyrażeń kluczowych można importować i eksportować do pliku *.txt. **Opcja Znajdź tylko całe wyrazy** spowoduje, że program nie będzie reagował jeśli wykryje słowo kluczowe zawarte w innym wyrazie, np. "dick" w "dickens".

Filtr treści

Jest to samouczący się mechanizm wykorzystujący inteligenty filtr treści Bayesa. Wraz z upływem czasu program uczy się nowych słów kluczowych dodając je automatycznie do listy. Przycisk **Sprawdź w tabeli** wyświetla listę wyuczonych wyrażeń. Aby usunąć z listy wszystkie wyuczone wyrażenia kliknij przycisk **Wyczyść tabelę**. Proces gromadzenia wyrażeń kluczowych rozpocznie się od nowa.

Zaawansowane

Okno umożliwia szczegółowe ustawienia kryteriów kwalifikowania wiadomości. Zalecamy jednak pozostawienie domyślnych ustawień programu. Przycisk **Indeksy prawdopodobieństwa** umożliwia modyfikację wartości indeksów przyznawanych za spełnianie konkretnych kryteriów. Nierozważne modyfikowanie wartości indeksów może spowodować nieprawidłowe działanie programu.

Filtr adresów

Umożliwia blokowanie wiadomości wysłanych przez konkretne komputery. Aby dodać adres IP do listy blokowanych serwerów, wpisz go w polu **Odrzucaj wiadomości od następujących adresów** i kliknij przycisk **Dodaj**.

Można importować i eksportować listę adresów IP z/do pliku *.txt.

Filtr języków

Filtr języków umożliwia rozpoznawanie języka, w którym napisana jest wiadomość. Duża część niechcianych wiadomości to spam obcojęzyczny, zazwyczaj w języku angielskim. Zaznaczenie na liście języka angielskiego spowoduje odfiltrowanie wszystkich wiadomości w języku angielskim.

11.2.3.3 Widok Kolejki

W oknie kolejek można obserwować przychodzące i wychodzące wiadomości czekające na kontrolę antywirusową, lub na ponowne przesłanie, jeśli adresat nie jest w danej chwili dostępny. Kontrola antywirusowa przebiega na bieżąco, MailSecurity powoduje jedynie nieznaczne opóźnienie ruchu. Po przesłaniu wiadomości zostają usunięte z listy. Jeśli któryś z serwerów (adresatów) jest niedostępny, przy wiadomości pojawi się odpowiada adnotacja. Program ponawia próbę wysłania w regulowanych przez użytkownika odstępach czasowych (Opcje > Kolejka). Każde nieudana próba wysłania zostanie udokumentowana.

Przycisk Przychodzące/Wychodzące przełącza między kolejkami wiadomości przychodzących a wychodzących. Można nakazać programowi natychmiastowe wysłanie wiadomości klikając przycisk **Powtórz teraz**. Częstotliwość wysyłania plików ustala się w polu **Interwał czasowy** w zakładce Opcje > Kolejka. Przycisk **Usuń** powoduje usunięcie zaznaczonej wiadomości z kolejki.

11.2.3.4 Widok Działanie

W tym oknie protokołowane są wszystkie procesy wykonywane przez program MailSecurity, z określeniem godziny, numeru identyfikacyjnego oraz opisem. Za pomocą przycisku Wyczyść można usunąć wszystkie pozycje i rozpocząć protokołowanie na nowo.

Numery ID pozwalają skojarzyć procesy z konkretnymi wiadomościami. Raporty o tym samym numerze ID dotyczą jednej wiadomości (np. 12345 wczytuję wiadomość, 12345 edytuję wiadomość, 12345 wysyłam wiadomość).

Uwaga: Bufor widoku Działanie jest czyszczony w momencie zamknięcia okna programu. Po ponownym uruchomieniu aplikacji, okno widoku Działanie jest puste, a gromadzenie danych rozpoczyna się od nowa.

11.2.3.5 Widok Wykryte wirusy

W tym oknie można znaleźć szczegółowe informacje na temat wszystkich przypadków wykrycia wirusa, włącznie z podjętymi środkami (np. Status: usunięto zawirusowany fragment, usunięto załącznik, wiadomość odrzucona) oraz adresy nadawcy i odbiorcy zawirusowanej wiadomości.

12 G DATA Internet Security for Android

Pakiety biznesowe G DATA wyposażone są w specjalną wersję klienta mobilnego dla systemów Android umożliwiającą zdalne zarządzanie. Instalację oprogramowania na urządzeniach wymusza się poprzez specjalną funkcję w pasku narzędzi drzewa sieci składnika G DATA Administrator. Umożliwia ona wysłanie linku do zasobu APK udostępnionego automatycznie na serwerze IIS drogą mailową.

Po zainstalowaniu aplikacja z pomocą konsoli zarządzającej (opis w rozdziale Instalacja składnika Internet Security) klient wymaga wstępnego skonfigurowania połączenia z serwerem zarządzającym w oknie **Ustawienia**, w sekcji **Zdalna administracja**.

Po podłączeniu się aplikacji do serwera, ustawienia zdalnej administracji blokują się automatycznie. Klient zyskuje możliwość pobierania aktualizacji i można zarządzać jego funkcjami z konsoli Administrator.

Po włączeniu zezwolenia na zdalną administrację wprowadzamy niezbędne parametry: **Adres serwera**, **Nazwa urządzenia**, **Hasło** autoryzacji do serwera G DATA.

12.1 Widoki menu

Dotknij przycisk menu Internet Security aby wysunąć pasek umożliwiający przełączanie między widokami. Dotknięcie nazwy wybranego widoku spowoduje pojawienie się odpowiedniej karty ustawień.

12.1.1 Centrum zabezpieczeń

Sekcja **Centrum zabezpieczeń** przedstawia ogólny stan zabezpieczeń programu Internet Security.

Sekcja **Wiadomości** przedstawia chronologiczną listę zdarzeń i działań programu Internet Security for Android. Dotknij raport aby wyświetlić szczegóły. Przesuń raport w prawo lub w lewo aby usunąć wiersz.

W pasku narzędzi widoczne jest przycisk umożliwiający wymuszenie aktualizacji oraz ikona przedstawiająca kosz służąca do usuwania wszystkich raportów z sekcji wiadomości.

12.1.2 Skanowanie

Okno skanowania umożliwia wybór trybu skanowania.

- **Zainstalowane aplikacje**: Ten tryb obejmuje wszystkie zainstalowane aplikacje systemu Android. Jeśli skanowanie wykaże zagrożenie, program umożliwi bezpośrednie odinstalowanie szkodliwej aplikacji.
- **System (pełne skanowanie)**: Skanowanie obejmuje cały system plików urządzenia włączając w to pliki na kartach SD.

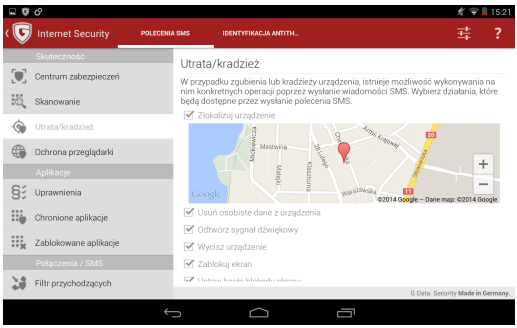
Dotknij przycisk ustawień w prawym, górnym rogu okna aby zmodyfikować ustawienia dotyczące automatycznego skanowania:

- **Automatyczne skanowanie**: Włącza/wyłącza możliwość automatycznego skanowania tylko instalowanych aplikacji.
- **Skanowanie zaplanowane**: Włącza/wyłącza skanowanie według harmonogramu.
- **Oszczędność energii**: Powoduje, że skanowanie nie będzie odbywać się jeśli bateria będzie słaba.

- **Skanuj podczas ładowania**: Powoduje, że urządzenie będzie skanowane tylko podczas ładowania.
- **Częstotliwość skanowania**: Umożliwia ustalenie interwału harmonogramu (1, 3, 7, 14 lub 30 dni).
- **Rodzaj skanowania**: Przełącza między skanowaniem tylko zainstalowanych aplikacji, a skanowaniem całego systemu.

12.1.3 Utrata/kradzież

Konfiguracja tej funkcji umożliwia zarządzanie telefonem w przypadku jego kradzieży lub zagubienia. Możliwe jest zdalne uruchamianie określonych poleceń poprzez wysłanie wiadomości SMS.



Dotknij przycisk ustawień w pasku menu aby ustalić lub zmienić hasło dla zdalnych poleceń SMS, numeru telefonu innego urządzenia do zdalnego modyfikowania hasła poleceń SMS oraz adresu e-mail do powiadomień o zdarzeniach związanych z działaniem modułu.

Hasło (kod PIN) będzie niezbędne do wysyłki wiadomości SMS umożliwiających zablokowanie urządzenia, usunięcie danych, uruchomienie sygnału dźwiękowego itp. Hasło będzie można zmienić zdalnie, ale tylko z telefonu o numerze skonfigurowanym w ustawieniach. Na adres mailowy są wysyłane informacje o lokalizacji GPS urządzenia, a także powiadomienia o skutku wykonania poleceń SMS. Dotknij przycisk paska menu zatwierdzający zmiany aby zapisać ustawienia. Jeśli program poprosi zatwierdź dodanie aplikacji G DATA do listy administratorów urządzenia.

Polecenia SMS

Ustawienia modułu można dowolnie modyfikować. W karcie **Polecenia SMS** możesz ustalić, które polecenia SMS będą funkcjonować:

- **Zlokalizuj urządzenie**: Po wysłaniu na numer urządzenia SMSa o treści

password ***locate*** urządzenie wyśle na zdefiniowany adres mailowy lokalizację GPS urządzenia.

- **Usuń osobiste dane z urządzenia**: Po wysłaniu na numer urządzenia SMSa o treści *password* ***wipe*** urządzenie zostanie przywrócone do stanu fabrycznego wraz z usunięciem prywatnych informacji.
- **Odtwórz sygnał dźwiękowy**: Po wysłaniu na numer urządzenia SMSa o treści *password* ***ring*** urządzenie włączy sygnał dźwiękowy, który może umożliwić odnalezienie zgubionego urządzenia.
- **Wycisz urządzenie**: Po wysłaniu na numer urządzenia SMSa o treści *password* ***mute*** spowoduje wyłączenie dźwięku w urządzeniu, dzięki czemu nie będzie na siebie zwracało uwagi.
- **Zablokuj ekran**: Po wysłaniu na numer urządzenia SMSa o treści *password lock* spowoduje zablokowanie ekranu urządzenia.
- **Ustaw hasło blokady ekranu**: Aby odzyskać dostęp do urządzenia po odzyskaniu go, może być potrzebna zdalna zmiana hasła blokady (nieużywane hasło można zapomnieć. Po wysłaniu na numer urządzenia SMSa o treści *password* ***set device password***: *devicepassword*

Indentyfikacja AntiTheft

Jeśli złodziej wymieni w urządzeniu kartę SIM, nie będzie można wysłać na nie poleceń SMS. Zabezpiecz się przed tym korzystając z opcji karty **Indentyfikacja AntiTheft**:

- **Zablokuj urządzenie po zmianie karty SIM**: Po wyjęciu karty SIM telefon zostanie zablokowany do chwili włożenia oryginalnej karty.
- **Zlokalizuj urządzenie po zmianie karty SIM**: Po wyjęciu karty SIM urządzenie wyśle na ustalony wcześniej adres e-mail lokalizację GPS urządzenia.

Aby zmienić hasło poleceń SMS, wyślij z numeru telefonu ustalonego wcześniej SMS o treści: ***remote password reset:*** *password*.

Jeśli chcesz, aby program powiadamiał Cię o niskim stanie baterii Twojego telefonu, zaznacz opcję

12.1.4 Ochrona przeglądarek

Moduł ochrony zapewnia ochronę przed stronami wyłudzającymi informacje. Ponieważ moduł zwiększa w niewielkim stopniu ilość pobieranych danych, istnieje możliwość skonfigurowania opcji działania ochrony przeglądarek tylko przy wykorzystywaniu połączeń WLAN w widoku Ustawienia. Opcja nie działa w

trybie incognito przeglądarek mobilnych.

12.1.5 Uprawnienia

Widok uprawnienia wyświetla podsumowanie uprawnień nadanych zainstalowanym aplikacjom. Zwróćmy szczególne uwagę na darmowe aplikacje, które mają dostęp do książki adresowej i wysyłki wiadomości SMS. Bezpośrednio z listy aplikacji dysponującej wybranym uprawnieniem masz możliwość odinstalowania danej aplikacji.

12.1.6 Ochrona aplikacji

Moduł ochrony aplikacji umożliwia zablokowanie dostępu do dowolnie wybranych aplikacji. Dostęp zostanie przyznany po wpisaniu hasła (kod PIN), adresu e-mail (reset hasła) lub podaniu odpowiedzi na tajne pytanie (wyświetlenie hasła).

Skonfiguruj hasło, adres mailowy do przypomnień oraz tajne pytanie/ odpowiedź i dotknij przycisk **Zmiana danych** w pasku menu.

Pokaże się główny widok **Ochrona aplikacji** przedstawiający na razie pustą listę aplikacji objętych ochroną. Dotknij ikonę + aby dokonać wyboru aplikacji, które chcesz chronić hasłem.

12.1.7 Filtr przychodzących

Ten moduł umożliwia filtrowanie SMS-ów i połączeń od wybranych kontaktów:

- **Biała lista:** Akceptowane będą tylko numery z listy
- **Czarna lista:** Blokowane będą tylko numery z listy
- **Kontakty:** Akceptowane będą tylko numery z książki kontaktów.

Tryb **Kontakty** można łączyć z trybem białej lub czarnej listy. Program umożliwia akceptowanie połączeń anonimowych bez względu na filtry.

Po włączeniu trybu białej lub czarnej listy możesz dotknąć ikonę kłódki u góry aby edytować listę. W celu dodania numeru do listy dotknij ikonę z plusem. Możesz wyszukiwać numery w książce kontaktów lub na liście historii połączeń.

12.1.8 Filtr wychodzących

Ten moduł umożliwia filtrowanie SMS-ów i połączeń do wybranych kontaktów:

- **Biała lista:** Akceptowane będą tylko numery z listy
- **Czarna lista:** Blokowane będą tylko numery z listy
- **Kontakty:** Akceptowane będą tylko numery z książki kontaktów.

Wskazówka: Dozwolone jest stosowanie znaku zastępczego *****, zastępującego dowolny ciąg cyfr. Składnią 0800* można w ten sposób zablokować wszystkie połączenia wychodzące do numerów **0800** itd.

Tryb **Kontakty** można łączyć z trybem białej lub czarnej listy.

Po włączeniu trybu białej lub czarnej listy możesz dotknąć ikonę kłódki u góry aby edytować listę. W celu dodania numeru do listy dotknij ikonę z plusem. Możesz wyszukiwać numery w książce kontaktów lub na liście historii połączeń.

12.1.9 Ukrywanie kontaktów

Ta funkcja umożliwia ukrywanie wybranych kontaktów wraz z historią połączeń i przesłanych wiadomości. W tym celu kontakty są przenoszone do zablokowanego konta G DATA.

Dostęp do ukrytych kontaktów jest możliwy tylko poprzez program Internet Security for Android, po dotknięciu nazwy funkcji **Ukrywanie kontaktów**. W celu dodania kontaktu do listy dotknij ikonę z plusem. Możesz wyszukiwać numery w książce kontaktów lub na liście historii połączeń. Aby edytować ustawienia kontaktu, dotknij jego nazwę. Możesz zablokować tylko widoczność komunikacji z kontaktem (połączenia i SMSy), a dodatkowo również widoczność kontaktu w książce adresowej. Jeśli usuniesz kontakt z listy, zostanie z powrotem przeniesiony do oficjalnej książki adresów.

12.1.10 Ustawienia

Ten widok pozwala na modyfikowanie globalnych ustawień aplikacji. Ustawienia pogrupowane są w następujących sekcjach.

Ogólne

Ikona powiadomienia: Umożliwia ukrycie ikonki G DATA Internet Security for Android w obszarze powiadomień.

Zapisz raporty: Umożliwia lokalny zapis raportów skanowania systemu.

Aktualizacja

Automatyczna aktualizacja: Włącza automatyczne aktualizowanie sygnatur wirusów w tle.

Częstotliwość aktualizacji: Umożliwia ustawienie interwału aktualizacji (1, 3, 7, 14, lub 30 dni).

Tylko poprzez WLAN: Spowoduje, że aktualizacje będą pobierane jedynie przez sieci WiFi.

Region aktualizacji: Umożliwia wybór regionu aktualizacji (automatycznie ustawiony poprzez wersję językową).

Skanowanie

Skanowanie zaplanowane: Otwiera okno ustawień skanowania.

Ochrona przeglądarki

Tylko WLAN: Przeglądarki będą chronione tylko podczas połączeń z sieciami WiFi.

Zdalna administracja

Po podłączeniu się aplikacji do serwera, ustawienia zdalnej administracji blokują się automatycznie. Klient zyskuje możliwość pobierania aktualizacji i można zarządzać jego funkcjami z konsoli Administrator.

Po włączeniu zezwolenia na zdalną administrację wprowadzamy niezbędne parametry: **Adres serwera**, **Nazwa urządzenia**, **Hasło** autoryzacji do serwera G DATA.

13 Licencje

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Polenter - Software Solutions nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Json.NET

Json.NET is distributed under The MIT License (MIT). Copyright © 2007 James Newton-King.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DotNetZip

DotNetZip is distributed under the Microsoft Public License (Ms-PL).

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license

cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

PhoneNumbers.dll / PushSharp

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of

this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the

Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/ or rights consistent with this License. However, in accepting such obligations,

You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.