Prezentuje status programu, stałej ochrony oraz ostrzeżeń.

Umożliwia wybór skanowanych obszarów komputera oraz konfigurowanie zaplanowanych zadań skanowania.

Skanuje wybrany element.

Umożliwia konfigurację różnych opcji skanowania w ramach ochrony antywirusowej , gwarantując maksymalną elastyczność.

Skanuje wszystkie skompresowane pliki, do których próbowano uzyskać dostęp.

Skanuje pliki systemowe w trakcie każdego zadania skanowania.

Skanuje wszystkie pliki e-mail odnalezione w trakcie skanowania.

Skanuje wszystkie pliki na komputerze.

Skanowane są tylko pliki z wybranymi rozszerzeniami.

Umożliwia wybór rozszerzeń plików, które chcesz poddać skanowaniu.

Uaktywnia dźwięki dla konfigurowanego zadania skanowania.

Po zaznaczeniu tej opcji wszystkie zdarzenia zachodzące w trakcie skanowania uwzględniane są w raporcie.

Wybór tej opcji umożliwia skanowanie większej liczby dyskietek jedna po drugiej.

Okno prezentujące przebieg skanowania zostało zminimalizowane.

Konfiguruje skanowanie heurystyczne.

Przywraca ustawienia domyślne.

Klawisz ten umożliwia dodawanie katalogów do listy katalogów nie poddawanych skanowaniu.

Klawisz ten umożliwia usuwanie katalogów z listy katalogów nie poddawanych skanowaniu.

Klawisz ten umożliwia dodawanie plików do listy plików nie poddawanych skanowaniu.

Klawisz ten umożliwia usuwanie plików z listy plików nie poddawanych skanowaniu.

Wprowadź w tym polu wszelkie nowe rozszerzenia, które zostaną dodane do listy rozszerzeń nie poddawanych skanowaniu.

Klawisz ten umożliwia dodawanie rozszerzenia wprowadzonego w polu do listy rozszerzeń nie poddawanych skanowaniu.

Klawisz ten umożliwia usuwanie rozszerzenia z listy rozszerzeń nie poddawanych skanowaniu.

Po zaznaczeniu tej opcji ostrzeżenia przesyłane będą do stacji roboczej z chwilą wykrycia wirusa.

Klawisz ten umożliwia konfigurację ostrzeżeń wysyłanych do stacji roboczej.

Umożliwia ustawienie sygnałów dźwiękowych w razie wykrycia wirusa. Sygnały te mogą mieć zarówno prostą postać, jak i wykorzystywać dowolny plik WAV.

Umożliwia wybór pliku Wav.

Umożliwia ustawienie wyświetlania komunikatów w razie wykrycia wirusa.

Po zaznaczeniu tej opcji ostrzeżenia przesyłane będą pocztą z chwilą wykrycia wirusa.

Umożliwia edycję komunikatu ostrzegawczego wysyłanego pocztą.

Umożliwia wskazanie, by komunikat ostrzegawczy przesyłany był do wybranej stacji roboczej w sieci. Komunikat ten można konfigurować.

Umożliwia edycję komunikatu ostrzegawczego wysyłanego do stacji roboczej.

Umożliwia edycję komunikatu ostrzegawczego wysyłanego do domeny.

Umożliwia tworzenie nowego zadania skanowania z pomocą kreatora.

Umożliwia edycję elementów poddawanych skanowaniu, konfigurację zadania skanowania oraz wybór częstotliwości jego przeprowadzania.

Usuwa wybrane zadanie skanowania.

Umożliwia aktualizację ochrony antywirusowej z wykorzystaniem kreatora.

Wskazuje, że pliki aktualizacji znajdują się na dyskietce, dysku CD-ROM lub dysku sieciowym w sieci lokalnej. Umożliwia również wskazanie określonej lokalizacji plików aktualizacji.

Wskazuje, że aktualizacje przeprowadzić należy przez Internet. W celu prawidłowej identyfikacji należy podać adres oraz nazwę użytkownika i hasło.

Opcja ta umożliwia przeprowadzenie pełnego skanowania komputera.

Umożliwia tworzenie dysków ratunkowych w celu uruchomienia komputera w środowisku pozbawionym wirusów.

Umożliwia konfigurację stałego skanowania plików oraz Internetu.

Umożliwia ustawianie częstotliwości przeprowadzania zadań skanowania.

Prezentuje informacje dotyczące różnych aspektów stałego skanowania: zdarzenia, przeprowadzone działania, liczba wiadomości poddanych skanowaniu lub zneutralizowanych itd.

Umożliwia konfigurację wszelkich aspektów stałego skanowania: typy plików poddawane skanowaniu lub usuwane z listy zadań stałego skanowania, przeprowadzane działania oraz ostrzeżenia wysyłane w razie wykrycia wirusa.

Umożliwia aktywację lub dezaktywację stałej ochrony.

Skanuje wszystkie skompresowane pliki, do których próbowano uzyskać dostęp.

Po zaznaczeniu tej opcji wszystkie zdarzenia, do których dochodzi w trakcie skanowania, zapisywane są w raporcie.

Wszystkie pliki na komputerze są skanowane.

Skanowane są jedynie pliki z wybranymi rozszerzeniami.

Umożliwia wybór rozszerzeń plików poddawanych skanowaniu.

Zainfekowany plik jest usuwany, gdy jego wyleczenie nie jest możliwe.

Zainfekowany plik jest przenoszony do określonej lokalizacji. W ten sposób utworzyć można obszar, w którym przechowywane są wirusy „w kwarantannie".

Po zaznaczeniu tej opcji tworzona jest kopia zapasowa pliku, w którym wykryto wirusa.

Po zaznaczeniu tej opcji wszystkie odebrane wiadomości e-mail są skanowane.

Po zaznaczeniu tej opcji wszystkie wysyłane wiadomości e-mail są skanowane.

Skanuje wszystkie skompresowane pliki powiązane z dowolną skanowaną wiadomością.

Skanuje wszystkie wiadomości zawarte wewnątrz innych wiadomości.

Po wybraniu tej opcji dane dotyczące skanowania zapisywane są w raporcie.

Wybór tej opcji umożliwia skanowanie wszystkich plików niezależnie od rozszerzenia.

Po wybraniu tej opcji skanowane są jedynie pliki z rozszerzeniem EXE lub COM.

Skanowane są jedynie pliki z wybranymi rozszerzeniami.

Umożliwia wybór rozszerzeń plików poddawanych skanowaniu.

Skanowane są aplikacje otrzymane w załącznikach wiadomości e-mail.

Skanowane są rysunki otrzymane w załącznikach wiadomości e-mail.

Skanowane są pliki wideo otrzymane w załącznikach wiadomości e-mail.

Skanowane są pliki audio otrzymane w załącznikach wiadomości e-mail.

Skanowane są pliki tekstowe otrzymane w załącznikach wiadomości e-mail.

Skanowane są pliki HTML otrzymane w załącznikach wiadomości e-mail.

Skanowane są inne typy plików, których nie wymieniono wyżej.

Po wybraniu tej opcji zmieniona zostaje nazwa zainfekowanego pliku, o ile niemożliwe jest jego wyleczenie.

Usuwa zainfekowane pliki, gdy nie można ich wyleczyć.

Przenosi zainfekowany plik do wyznaczonej lokalizacji. W ten sposób utworzyć można obszar, w którym przechowywane są wirusy „w kwarantannie".

Po zaznaczeniu tej opcji aktywowana jest blokada adresu, by uniemożliwić doń dostęp.

Po zaznaczeniu tej opcji aktywowana jest blokada usług internetowych, by uniemożliwić korzystanie z nich.

Po zaznaczeniu tej opcji skanowane są dostępne dyski sieciowe.

Po zaznaczeniu tej opcji blokowany jest dostęp do dysków sieciowych w przypadku infekcji, by uniemożliwić rozprzestrzenianie się wirusów tą drogą.

Wyświetla informacje na temat plików poddanych kwarantannie.

Wyświetla informacje na temat zainfekowanych plików, w przypadku których wykonano kopie zapasowe.

Wyświetla informacje na temat plików przesłanych do Panda Software.

Wyświetla informacje i umożliwia przeprowadzenie różnych działań dotyczących plików poddawanych kwarantannie, plików przesłanych do Panda Software lub tych, które posiadają kopię zapasową.

Skanuje tylko pliki poddawane kwarantannie.

Umożliwia wysyłanie plików poddawanych kwarantannie do Panda Software.

Umożliwia przemieszczanie pliku poddawanego kwarantannie do pierwotnej lokalizacji.

Umożliwia usuwanie wybranych plików poddawanych kwarantannie.

Umożliwia dodawanie zainfekowanego pliku lub pliku podejrzanego do listy plików „w kwarantannie".

Umożliwia przywracanie kopii zapasowych plików, które usunięto z wykorzystaniem ochrony antywirusowej.

Umożliwia usunięcie na stałe kopii zapasowych plików, usuniętych z wykorzystaniem ochrony antywirusowej.

Skanuje pliki przesłane do Panda Software.

Przemieszcza pliki przesłane do Panda Software w celu ich sprawdzenia do ich pierwotnej lokalizacji.

Usuwa wybrane pliki przesłane do Panda Software.

Umożliwia ponowne przesłanie wybranych plików.

Wyświetla usługi udostępniane zarejestrowanym użytkownikom Panda Software.

Umożliwia wysyłanie podejrzanych plików do Panda Software.

W tej części znalazły się odpowiedzi na pytania zadawane najczęściej przez użytkowników.

Wyświetla asystenta wykorzystywanego przez użytkowników do wysłania własnych uwag.

Umożliwia dodawanie plików, które chcesz przesłać do Panda Software.

Po wybraniu tej opcji wyświetlone zostaną informacje na temat ochrony antywirusowej dla przedsiębiorstw.

Po wybraniu tej opcji wyświetlone zostaną informacje na temat Panda Invent.

Po wybraniu tej opcji wyświetlone zostaną informacje na temat Panda PerimeterScan.

Umożliwia określenie lokalizacji, z której przeprowadzona zostanie aktualizacja: Internet, dyskietki, dysk CD-ROM itd.

Wyświetla raport zdarzeń sporządzany z wykorzystaniem ochrony antywirusowej.

Drukuje cały raport.

Umożliwia wyszukiwanie słów w wybranych polach.

Wyszukiwanie odbywa się w polu Zdarzenie.

Wyszukiwanie odbywa się w polu Zadanie.

Wyszukiwanie odbywa się w polu Ścieżka.

Wyszukiwanie odbywa się w polu Działanie.

Dokonuje konwersji raportu na plik tekstowy.

Usuwa plik raportu.

Filtruje informacje, które chcesz uwzględnić w raporcie.

Wyświetla listę wirusów z podaniem istotnych informacji na temat wybranych wirusów wykrytych przez program.

Drukuje informacje na temat wybranych wirusów.

Wskazuje, że profil domyślny skonfigurowany w Panelu sterowania powinien być zawsze wykorzystywany do prezentowania poczty w skanerze antywirusowym z możliwością jej skanowania.

Z chwilą uruchomienia ochrony antywirusowej zostaniesz zapytany, z jakiego profilu pocztowego chcesz korzystać.

Umożliwia wskazanie określonego profilu pocztowego, by był on zawsze wykorzystywany w skanerze antywirusowym.

Wskazuje, że napędy CD-ROM powinny być wyświetlane jako obszary skanowane w różnych zadaniach skanowania.

Wskazuje, że dyski sieciowe powinny być wyświetlane jako obszary skanowane w różnych zadaniach skanowania.

Wskazuje, że foldery e-mail powinny być wyświetlane jako obszary skanowane w różnych zadaniach skanowania.

Wskazuje, że bazy danych Lotus Notes na komputerze, na którym zainstalowano program antywirusowy, powinny być wyświetlane jako obszary skanowane.

Wskazuje, że bazy danych Lotus Notes na serwerze powinny być wyświetlane jako obszary skanowane.

Umożliwia wskazanie maksymalnego rozmiaru raportu, w którym zapisywane jest działanie ochrony antywirusowej, by nie okazał się on zbyt duży.

Po zaznaczeniu tej opcji bootsektor dyskietki pozostawionej w stacji w chwili ponownego uruchamiania lub wyłączania komputera jest automatycznie skanowany.

Umożliwia skonfigurowanie aktualizacji w taki sposób, by ochrona antywirusowa aktualizowała się automatycznie w określonych odstępach czasu.

Wyświetla komunikat z informacją, że aktualizacja została przeprowadzona prawidłowo.

Klawisz umożliwia odtworzenie wybranego dźwięku, co pozwala na jego sprawdzenie.

Umożliwia wskazanie określonego dźwięku przyporządkowanego do zdarzenia.

Umożliwia dezaktywację opcji odtwarzania dźwięków przyporządkowanych do poszczególnych zdarzeń.

Tutaj należy wpisać hasło dla wybranych obszarów.

Umożliwia zmianę hasła.

Hasło zabezpiecza dostęp do konfiguracji Panda Antivirus.

Hasło zabezpiecza dostęp do konfiguracji zadań skanowania stałego.

Hasło zabezpiecza dostęp do aktualizacji ochrony antywirusowej.

Hasło zabezpiecza dostęp do konfiguracji zadań stałego skanowania.

Hasło zabezpiecza dostęp do konfiguracji aktualizacji.

Umożliwia wybór elementów poddawanych skanowaniu.

Usuwa element wybrany z listy.

Umożliwia zaznaczenie częstotliwości, z jaką przeprowadzane będą operacje skanowania.

Umożliwia konfigurację stałego skanowania: poczty, portów, blokady adresów internetowych itd.

Otwiera asystenta wykorzystywanego przez użytkowników do wysłania zapytań technicznych.

Konfiguruje skanowanie heurystyczne w taki sposób, by użytkownik ostrzegany był przed plikami, które mogą być zainfekowane przez nowego wirusa. Nawet na tym poziomie istnieje bardzo niewielkie prawdopodobieństwo, że program antywirusowy wygeneruje fałszywy alarm.

Konfiguruje skanowanie heurystyczne w taki sposób, by skanowanie przebiegało szybko przy jednoczesnym sprawdzaniu wszystkich plików, które mogą być zainfekowane przez nowego wirusa.

Konfiguruje skanowanie heurystyczne w taki sposób, by przebiegało szybciej. W trybie tym skanowanie heurystyczne wykrywa jedynie te pliki, w przypadku których istnieje wysokie prawdopodobieństwo zainfekowania przez nieznane wirusy.

Po zaznaczeniu tej opcji w razie wykrycia wirusa zainfekowany plik przenoszony jest do określonej lokalizacji.

Po zaznaczeniu tej opcji w razie wykrycia wirusa zainfekowany plik jest usuwany.

Po zaznaczeniu tej opcji w razie wykrycia wirusa zainfekowany plik jest leczony.

Po zaznaczeniu tej opcji w razie wykrycia wirusa zmieniana jest nazwa zainfekowanego pliku.

Po zaznaczeniu tej opcji w razie wykrycia wirusa prezentowana jest informacja na temat zainfekowanego pliku.

Skanowanie zostaje wstrzymane w razie wystąpienia nieoczekiwanego błędu. Po potwierdzeniu ostrzeżenia możesz kontynuować skanowanie.

Przywraca listę w taki sposób, by obejmowała pierwotną listę rozszerzeń.

Usuwa wybrane rozszerzenie z listy.

Usuwa wszystkie rozszerzenia z listy.

Po zaznaczeniu tej opcji pliki bez rozszerzenia również są skanowane.

Dodaje wybrane nowe rozszerzenie do listy rozszerzeń.

Po zaznaczeniu tej opcji tworzona jest kopia zapasowa wyleczonego pliku.

Po zaznaczeniu tej opcji w razie wykrycia wirusa emitowany jest sygnał dźwiękowy.

Po zaznaczeniu tej opcji w razie wykrycia wirusa odtwarzany jest wybrany plik .Wav.

Umożliwia zaznaczenie, że do nadawcy zainfekowanej wiadomości należy wysłać komunikat ostrzegawczy.

Umożliwia zaznaczenie, że do innych odbiorców zainfekowanej wiadomości należy wysłać komunikat ostrzegawczy.

Umożliwia wysłanie komunikatu do wybranej stacji roboczej.

Wprowadź komunikat, który przesłany zostanie do stacji roboczej.

Umożliwia wysyłanie komunikatu do wybranej domeny.

Wprowadź komunikat, który przesłany zostanie do domeny.

Wprowadź nazwę stacji roboczej, która odbierze komunikat.

Wprowadź nazwę domeny, która odbierze komunikat.

Adres IP proxy wykorzystywany do połączeń z Internetem.

Liczba portów komunikacyjnych proxy wykorzystywanych do połączeń z Internetem.

Nazwa użytkownika, która będzie uwierzytelniana przed połączeniem z Internetem za pośrednictwem serwera proxy.

Hasło użytkownika, które będzie uwierzytelniane przed połączeniem z Internetem za pośrednictwem serwera proxy.

Prezentuje liczbę dni, jakie upłynęły od chwili ostatniej aktualizacji pliku zawierającego sygnatury wirusów.

Przyspiesza inne działania, w trakcie gdy skanowanie jest w toku.

Po zaznaczeniu tej opcji uzyskujesz opcję dostępu do zablokowanych stron, z chwilą gdy próbujesz uzyskać do nich dostęp.

Dodaje adres w tym polu do listy adresów blokowanych.

Po zaznaczeniu tej opcji uzyskujesz opcję dostępu do zablokowanych usług, z chwilą gdy próbujesz uzyskać do nich dostęp.

Umożliwia zaznaczenie częstotliwości, z jaką odbywać się będzie skanowanie: raz, co godzinę, codziennie, co tydzień, co miesiąc lub co rok.

Umożliwia wskazanie czasu rozpoczęcia skanowania.

Umożliwia wskazanie czasu, do jakiego najpóźniej musi się zakończyć skanowanie. Jeśli do tego czasu nie zostanie ukończone, zostanie przerwane.

Umożliwia aktywację lub dezaktywację zaplanowanego zadania skanowania.

Skanowanie przeprowadzane jest przy każdym uruchomieniu komputera.

Skanowanie przeprowadzane jest co określoną liczbę razy, gdy uruchomiono komputer, przy czym liczba ta może się zmieniać.

Skanowanie przeprowadzane jest co określoną liczbę dni, przy czym liczbę tę można ustalić.

Skanowanie przeprowadzane jest jedynie w wybrane dni tygodnia.

Wraz z opcją umożliwiającą zaznaczenie, czy skanowanie odbywać się ma co tydzień, co miesiąc itd., opcja ta umożliwia określenie częstotliwości przeprowadzania skanowania.

Usuwa wybrany element z listy elementów wykluczonych.

Usuwa wszystkie elementy z listy elementów wykluczonych.

Dodaje wybrany element do listy elementów wykluczonych.

Umożliwia wprowadzenie nazwy użytkownika podawanej z chwilą rejestracji.

Umożliwia wprowadzenie hasła podawanego z chwilą rejestracji.

Opcję należy wybrać w przypadku połączeń z Internetem poprzez serwer proxy.

Umożliwia określenie ścieżki, z której przeprowadzona zostanie aktualizacja.

Umożliwia wybór konfiguracji dostępu do Internetu poprzez serwer proxy.

Zmiany wprowadzone w konfiguracji zostaną zapisane i wdrożone.

Zmiany wprowadzone w konfiguracji nie zostaną zapisane, ani wdrożone.

Umożliwia wybór konfiguracji domyślnej.

Prezentuje nazwę wybranego pliku dźwiękowego.

Umożliwia wprowadzenie hasła.

Umożliwia wprowadzenie hasła.

Umożliwia wprowadzenie hasła.

Umożliwia wprowadzenie hasła.

Umożliwia dostęp do pomocy technicznej na witrynie Panda Software.

Po wybraniu tej opcji wyświetlane są informacje dotyczące Panda PerimeterScan.

Kliknięcie tego łącza przenosi do obszaru rejestracji online na witrynie Panda Software.

Zaznaczenie tej opcji aktywuje stałą ochronę z pomocą firewalla.

Umożliwia konfigurację firewalla.

Umożliwia konfigurację firewalla.

Po wybraniu tej opcji pliki skryptów nie będą wykonywane.

Po wybraniu tej opcji pliki skryptów nie będą wykonywane.

Po wybraniu tej opcji pliki skryptów nie będą wykonywane.

Umożliwia wybór działania, które przeprowadzane będzie w razie wykrycia wirusa.

Umożliwia konfigurację ostrzeżeń przesyłanych pocztą.

Umożliwia określenie adresu e-mail, na jaki przesyłane będą ostrzeżenia.

Umożliwia wybór protokołu wykorzystywanego do przesyłania ostrzeżeń pocztą.

Umożliwia wybór serwera, przez który przesłane zostanie ostrzeżenie.

Umożliwia wybór typu plików uznawanych za niebezpieczne.

Po wybraniu tej opcji załączniki potencjalnie niebezpieczne będą blokowane.

Po wybraniu tej opcji, pliki z podwójnym rozszerzeniem zostaną zablokowane.

Po wybraniu tej opcji, pliki z wybranymi rozszerzeniami zostaną zablokowane.

Umożliwia wybór rozszerzeń plików, które chcesz blokować.

Umożliwia dodawanie nowego rozszerzenia.

Umożliwia wybór działania, które zostanie przeprowadzone w razie wykrycia niebezpiecznego załącznika.

Umożliwia wybór programów, które łączyć się będą z Internetem.

Umożliwia konfigurację zaawansowanych reguł konfiguracji.

Rozwijając to menu, możesz określić, czy chcesz zezwolić wybranemu programowi na dostęp do Internetu. Możesz również określić, czy chcesz być pytany, ilekroć program próbuje uzyskać dostęp do Internetu.

Po wybraniu tej opcji programy systemu operacyjnego wyświetlone zostaną na liście.

Umożliwia dodanie nowego programu do listy.

Umożliwia określenie adresów, z którymi komunikować się mogą programy, oraz konfigurowanie portów.

Umożliwia usunięcie wybranego programu z listy.

Po zaznaczeniu tej opcji wszelkie wprowadzone zmiany zaprezentowane zostaną w raporcie.

Umożliwia wprowadzenie ścieżki do programu, który chcesz dodać do listy.

Umożliwia wyszukiwanie programu, który chcesz dodać do listy.

Umożliwia komunikację ze wszystkimi adresami IP.

Umożliwia komunikację ze wszystkimi adresami IP.

Umożliwia komunikację ze wszystkimi adresami IP.

Po zaznaczeniu tej opcji wybrany program uzyska możliwość łączenia się z Internetem. Będziesz miał również możliwość określić porty, przez które nawiązywane będzie to połączenie.

Umożliwia wybór protokołu lub określenie portów TCP, przez które łączyć się będzie program.

Umożliwia wybór protokołu lub określenie portów UPD, przez które łączyć się będzie program.

Po zaznaczeniu tej opcji inne komputery będą mogły łączyć się z wybranym programem z sieci.

Umożliwia dodawanie nowych reguł połączeń.

Umożliwia zmianę wybranych parametrów reguły.

Umożliwia usuwanie z listy zaznaczonej reguły.

Po zaznaczeniu tej opcji zastosowane nowe reguły prezentowane będą w raporcie.

Umożliwia wprowadzenie nazwy, którą chcesz przypisać do nowej reguły.

Rozwijając to menu, możesz wybrać działanie, jakie przeprowadzać będzie nowa reguła.

Rozwijając to menu, możesz wybrać kartę sieciową, do której odnosić się będzie reguła.

Umożliwia wybór protokołu, do którego odnosić się będzie reguła.

Umożliwia określenie, czy reguła odnosić się będzie do połączeń przychodzących, połączeń wychodzących, czy obu ich rodzajów.

Po zaznaczeniu tej opcji reguła odnosić się będzie do wszystkich adresów zdalnych.

Umożliwia określenie adresu karty sieciowej, do którego odnosić się będzie reguła.

Umożliwia określenie adresów IP, do których odnosić się będzie reguła.

Umożliwia określenie adresów IP, do których odnosić się będzie reguła. Możesz wprowadzić pełne adresy lub zakresy adresów oddzielone przecinkami.

Umożliwia wybór urządzenia sieciowego, przez które chcesz zezwalać lub odmawiać dostępu do folderów udostępnianych.

Umożliwia wybór urządzenia sieciowego, przez które chcesz zezwalać lub odmawiać dostępu do folderów udostępnianych.

Umożliwia dostęp do folderów udostępnianych na innych komputerach.

Po zaznaczeniu tej opcji wyświetlane jest ostrzeżenie za każdym razem, gdy zablokowana zostanie próba włamania.

Umożliwia skonfigurowanie profilu pocztowego, opcji aktualizacji, ograniczeń z hasłem, dźwięków, elementów, które można skanować itd.