Panda Managed Office Protection

Wdrożenie systemu w 5 krokach

Wstęp

Panda Managed Office Protection jest rozwiązaniem dedykowanym dla małych oraz średnich przedsiębiorstw. Produkt składa się z aplikacji ochronnych zapewniających kompleksową ochronę firmowych komputerów stacjonarnych, mobilnych stacji roboczych oraz serwerów, a także z systemu pozwalającego na zcentralizowane zarządzanie.

System zarządzania oparty jest o nowoczesny mechanizm, który uwzględnia potrzeby oraz możliwości małych i średnich przedsiębiorstw eliminując konieczność inwestycji w infrastrukturę sieciową oraz ograniczając zaangażowanie personelu IT w zadania implementacji oraz późniejszej administracji systemem zabezpieczającym.

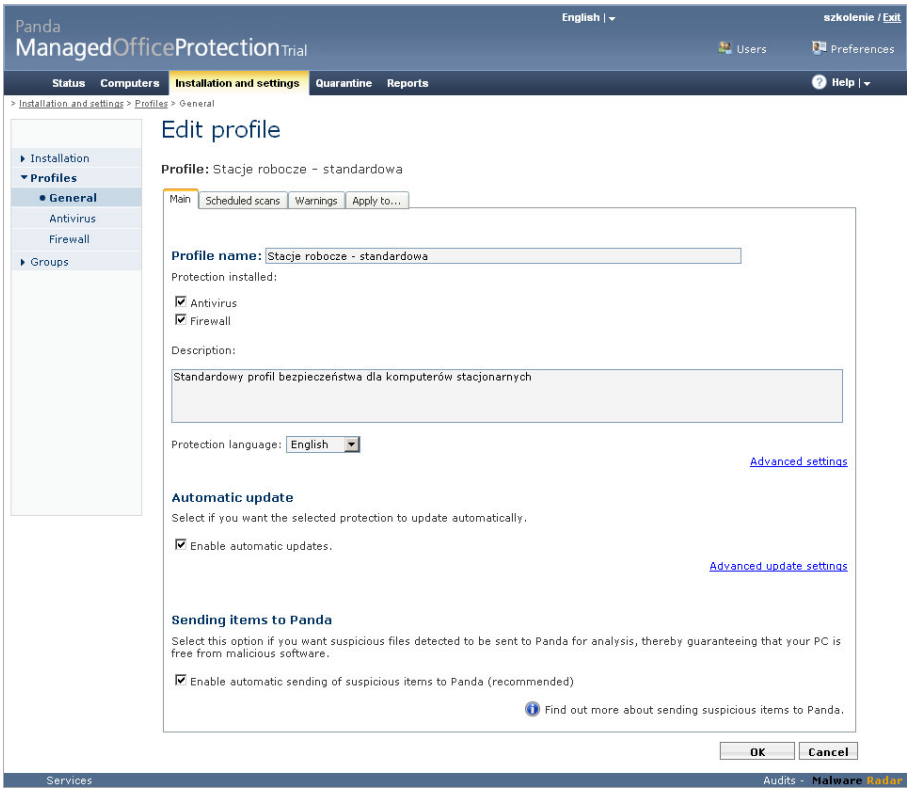
W przypadku tradycyjnego modelu centralnego zarządzania aby uzyskać możliwość zdalnej administracji aplikacjami ochronnymi administrator zmuszony jest do instalacji wewnątrz własnej organizacji złożonego systemu, który składa się z kilku modułów (np. serwera administracyjnego, bazy danych, serwera aktualizacyjnego, konsoli zarządzającej). Instalacja musi zostać poprzedzona etapem planowania gdyż nieprawidłowo wdrożony system może powodował problemów w sieci np. ograniczając jej wydajność. Zakupione oraz odpowiednio przygotowane muszą zostać także serwery utrzymujące poszczególne moduły. Dopiero po skomplikowanym procesie przygotowań możliwe jest przystąpienie do instalacji systemu oraz wprowadzenia odpowiedniej jego konfiguracji. Po wykonaniu powyższych czynności należy przystąpić do etapu instalacji aplikacji ochronnych. Ze względu na złożoność całego procesu wdrożenie takiego systemu jest czasochłonne i często powoduje liczne problemy. Komplikacje w połączeniu z koniecznością inwestycji w lokalną infrastrukturę (zakup, modernizacja lub rekonfiguracja serwerów) powodują wzrost kosztów wdrożenia sytemu ochronnego.

System zcentralizowanego zarządzania wykorzystany w rozwiązaniu Panda Managed Office Protection opiera się o mechanizmy utrzymywane na dedykowanych do tego celu serwerach producenta rozwiązania. Aby uzyskać możliwość zdalnej administracji klient wykorzystujący rozwiązanie Panda Managed Office Protection nie musi implementować wewnątrz własnej infrastruktury żadnych elementów systemu zarządzania. W ten sposób koszt wdrożenia rozwiązania oraz czas potrzebny na jego przeprowadzenie jest zminimalizowany. Brak ingerencji w lokalną infrastrukturę sieciową eliminuje również dodatkowe komplikacje oraz problemy wynikające z braku kompatybilności.

Po zakupie rozwiązania lub zarejestrowaniu wersji demo na wskazany adres e-mail wysyłana jest wiadomość zawierającą dane pozwalające na dostęp do systemu zcentralizowanego zarządzania.

1. Tworzenie profili bezpieczeństwa - konfiguracja aplikacji ochronnych

Zarządzanie aplikacjami zabezpieczającymi oparte jest o grupy oraz profile konfiguracyjne. Pozwala to na wprowadzenie wielopoziomowej polityki bezpieczeństwa. Administrator ma więc możliwość określenie odpowiedniego poziomu bezpieczeństwa, a następnie łatwego przypisania go do wybranej grupy komputerów. Opcję tworzenia oraz edycji profili konfiguracyjnych odnajdziemy w zakładce ***„Installation and settings - Profiles".***



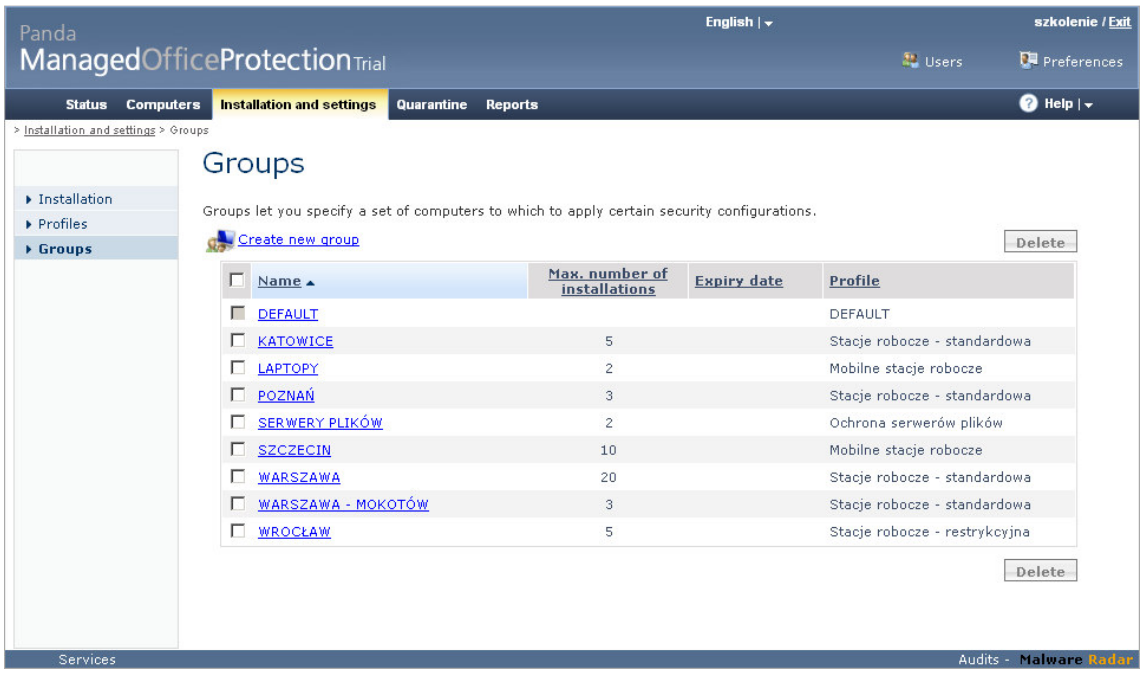
Profile konfiguracyjne określają jakie moduły ochronne powinny zostać zainstalowane oraz jaka powinna być ich konfiguracja. Możliwe jest wykorzystanie domyślnego profilu bezpieczeństwa i przejść do dalszej części instrukcji lub utworzyć i skonfigurować własny profili poprzez:

- nadanie nazwy oraz komentarza przypisanego do tworzonego profilu,
- określenie język instalowanych aplikacji ochronnych,
- ustanowienie poziom ochrony określając aktywne moduły ochronne,
- skonfigurowanie modułów ochronnych dostosowując je do specyfiki własnej firmy,
- określenie częstotliwość aktualizacji oraz komunikacji aplikacji ochronnych.

2. Tworzenie grup komputerów - organizowanie struktury sieci

Złożoność struktury sieci komputerowej, specyfika pracy poszczególnych pracowników, a także rozróżnienie komputerów stacjonarnych oraz mobilnych wymaga od systemu zabezpieczającego możliwości wprowadzenie odmiennych konfiguracji dla określonych grup stacji oraz serwerów. Zarządzanie oparte o grupy pozwala na efektywne przypisywanie określonych ustawień aplikacji zabezpieczających nawet w przypadku złożonych sieci komputerowych. Możliwe jest więc wprowadzenie podziału np. na stacje robocze stacjonarne, stacje robocze mobilne oraz serwery, a następnie dla każdej z tych grup możliwe jest określenie innego poziomu ochrony.

Poprzez utworzenie kilku nowych grup istnieje możliwość dokładnego odwzorowania aktualnej struktury firmy.

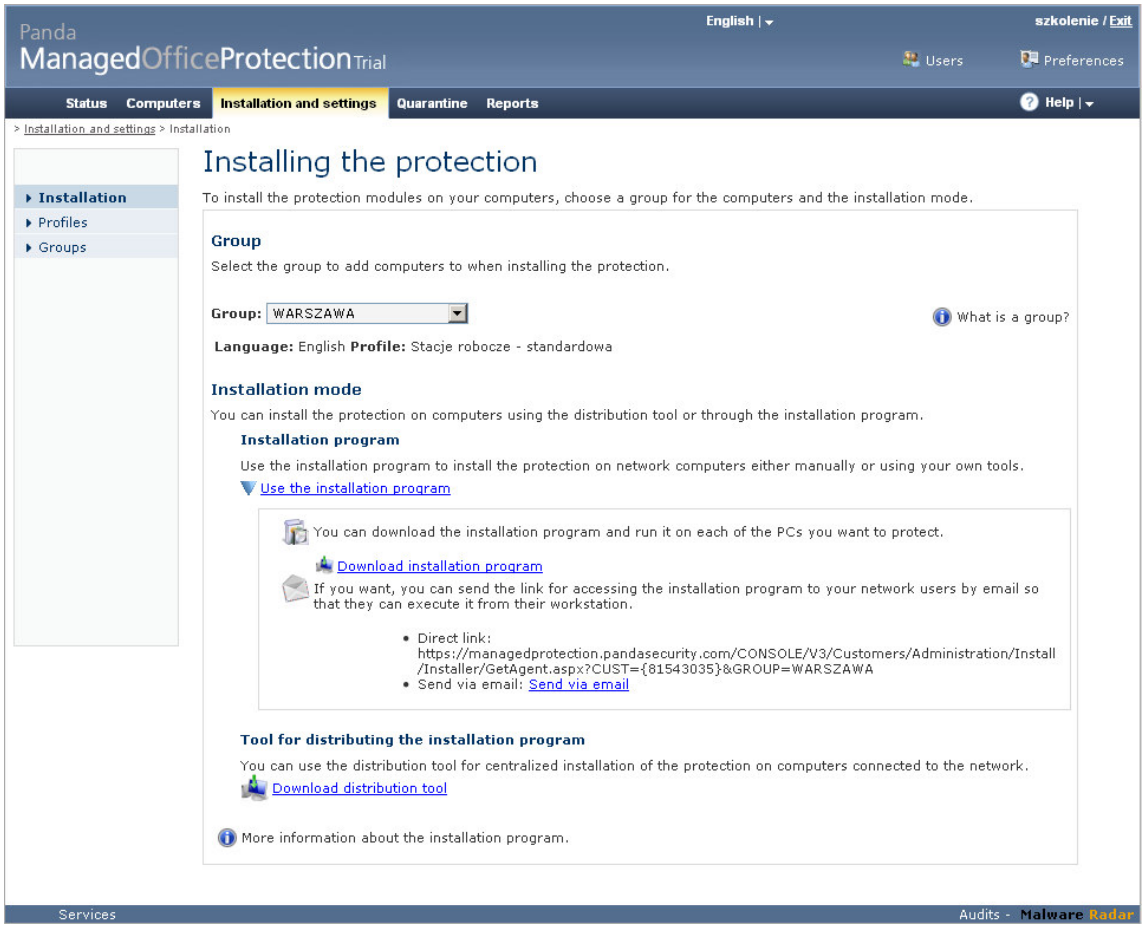


W zakładce ***„Installation and settings – Groups”*** możliwe jest utworzenie nowej grupy poprze:

- nadanie jej na nazwy,
- przypisanie dla niej odpowiedniego profilu konfiguracyjnego (polityki bezpieczeństwa
- określenie dodatkowych parametrów grupy np. ilości stacji jakie dana grupa może obejmować.

3. Instalacja aplikacji zabezpieczających

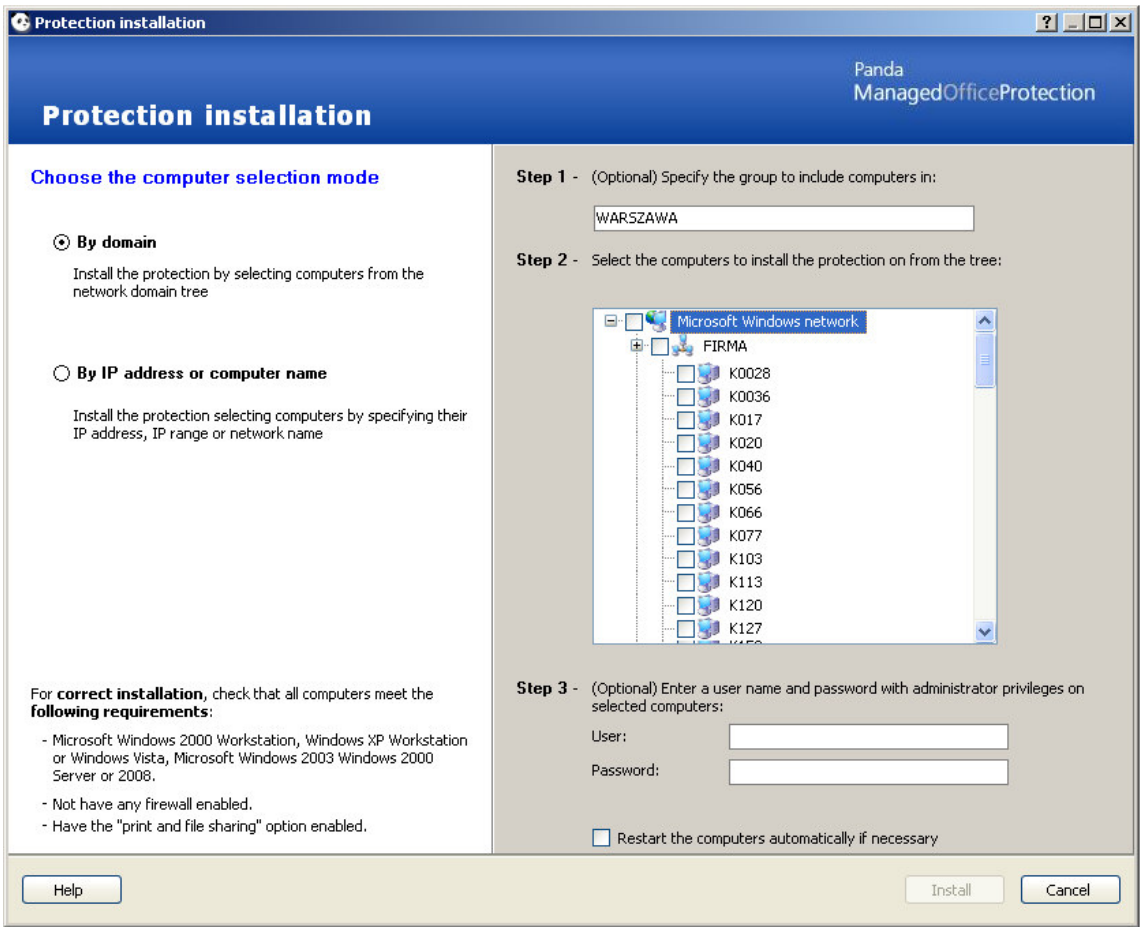
Kolejnym etapem procesu wdrożenia rozwiązania Panda Managed Office Protection jest instalacja aplikacji zabezpieczających. W pierwszej kolejności w zakładce ***„Installation and settings - Installation”*** należy wybrać grupę dla której przeprowadzamy dany proces instalacji. Na stacjach roboczych automatycznie wprowadzone zostaną ustawienia określone przez profil konfiguracyjny powiązany z daną grupą. Po instalacji aplikacji ochronnych nie jest więc konieczne dodatkowe ich konfigurowanie.



Dostępne są dwie metody instalacji aplikacji ochronnych.

W przypadku mobilnych stacji roboczych lub sieci o rozproszonej strukturze bezpośrednio z konsoli WWW istnieje możliwość pobrania paczki w postaci pliku instalacyjnego - *„Download installation program”.* Plik ten, o wielkości 5 MB należy rozesłać do użytkowników stacji roboczej. Bezpośrednio z konsoli zarządzającej może zostać także wygenerowana wiadomość e-mail zawierająca bezpośredni odnośnik do pliku instalacyjnego – *„Send via email”*. Użytkownik końcowy po uruchomieniu otrzymanego pliku inicjuje proces instalacji aplikacji ochronnej.

W przypadku gdy procesem instalacji objęta ma zostać większa grupa komputerów zalecane jest wykorzystanie dedykowanej konsoli instalacyjnej – *„Download distribution tool”* .
Konsola pozwala zdalnie wymusić instalację aplikacji ochronnych na wybranej grupie komputerów. Grupę tą możemy definiować wybierając określoną domenę, grupę roboczą lub określoną nazwę komputera. Możliwe jest także wskazanie zakresu adresów IP lub kilku pojedynczych adresów.



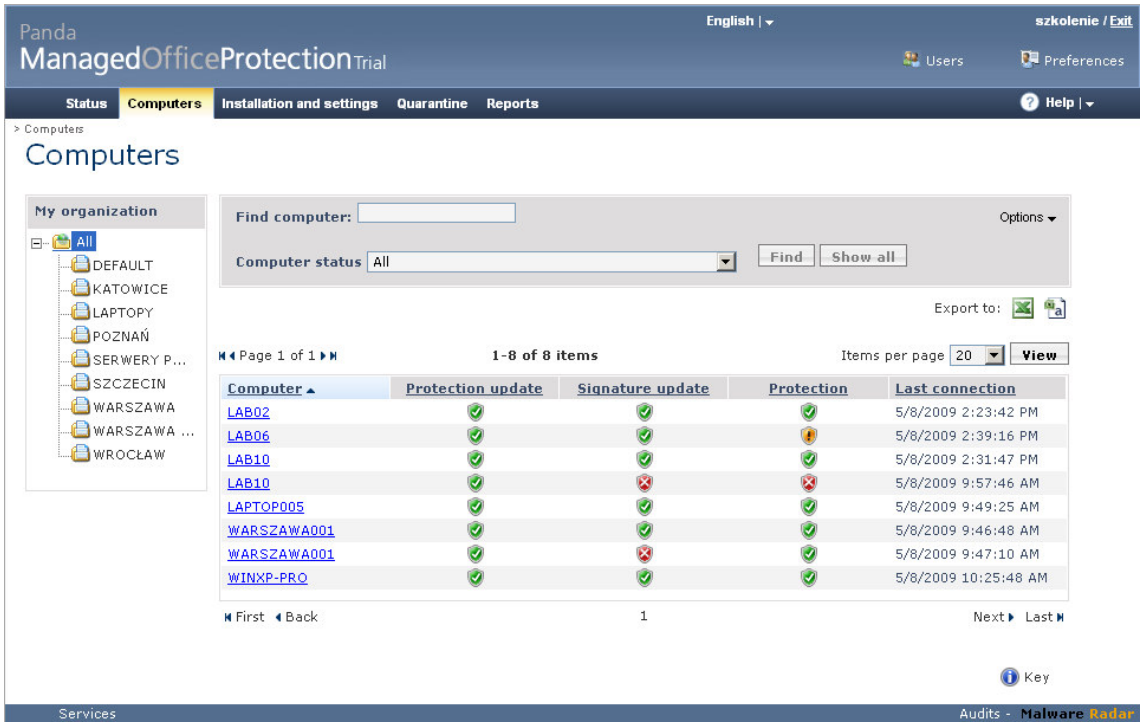
Po zainicjowaniu procesu instalacji dalszy jej ciąg przebiega całkowicie bezobsługowo.
Paczka instalacyjna automatycznie wykrywa aktualnie zainstalowane aplikacje ochronne i dokonuje ich deinstalacji. Następnie łączy się z konsolą zarządzającą, implementuje odpowiednie moduły ochronne i wprowadza ich ustawienia zgodnie z określonym dla grupy profilem konfiguracyjnym. Po zakończeniu procesu raportuje status ochrony danej stacji do konsoli zarządzającej.

Podczas operacja instalacji zachowana jest ciągłość ochrony stacji. Po instalacji nie zachodzi również konieczność wykonywania dodatkowych działań takich jak rekonfiguracja lub aktywacja produktu.

4. Monitorowanie procesu instalacji

Aplikacje zabezpieczające zostały przygotowane tak aby cyklicznie raportować do konsoli centralnego zarządzania zarówno status modułów ochronnych jak i poszczególne zdarzenia związane z daną stacją np. informacje o wykryciu zagrożenia, przeprowadzonej aktualizacji itp.

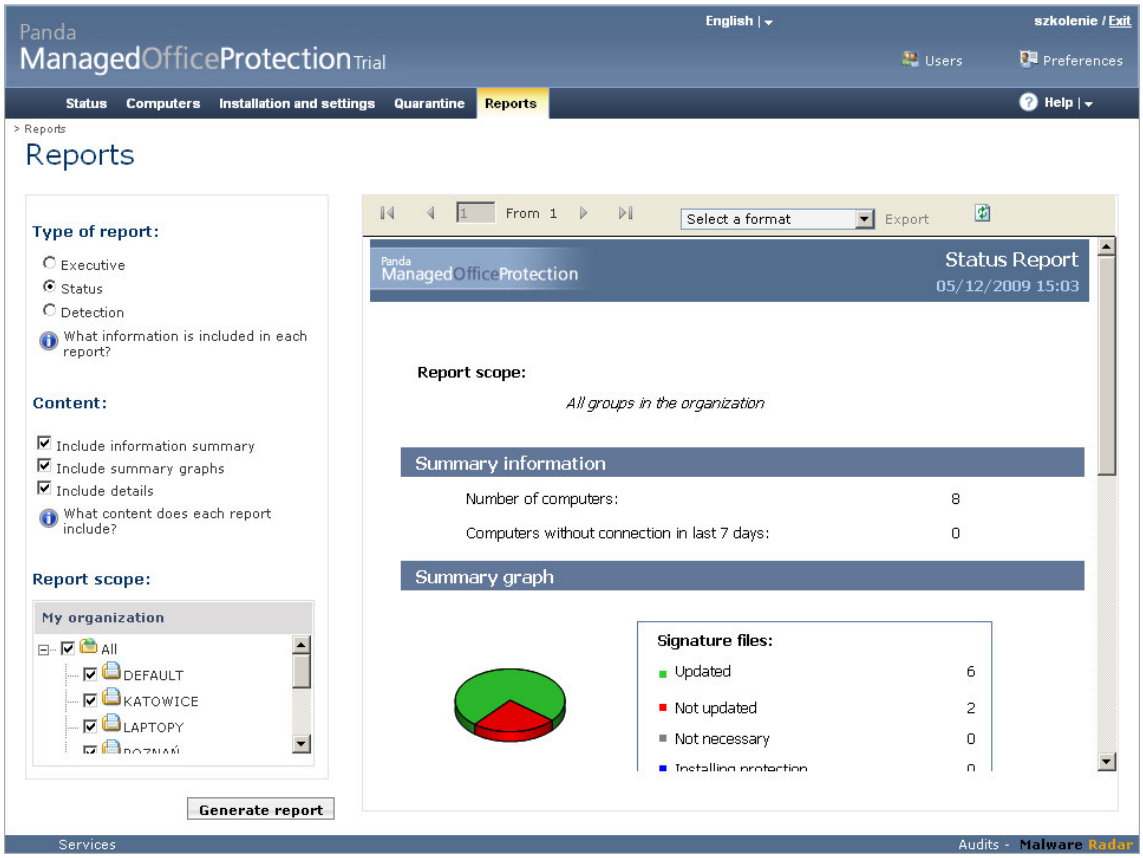
Już w trakcie procesu instalacji modułów ochronnych stacja raportuje do konsoli centralnej aktualny status ochrony. W zakładce ***„Computers”*** przedstawiany jest status poszczególnych komputerów objętych ochroną.



Po kilku minutach od rozpoczęcia instalacji aplikacji ochronnych możliwe jest już zweryfikowanie w konsoli zarządzającej, które komputery zakończyły instalację, a na których proces ten nadal trwa. Na tym etapie procesu implementacji rozwiązania Panda ManagedOffice Protection należy zweryfikować czy komputery objęte procesem instalacji zostały wyświetlone w zakładce ***„Computers”*** konsoli administracyjnej oraz jaki jest postęp instalacji oraz status ich ochrony.

5. Raportowanie statusu wprowadzonego systemu zabezpieczającego

Po zakończeniu procesu instalacji w zakładce ***„Reports”*** istnieje możliwość wygenerowania zbiorczego raportu prezentującego aktualny status ochrony całej organizacji.



Raport prezentuje informacje dotyczące zainstalowanych modułów ochronnych, stanu ich aktualizacji, daty posiadanej bazy sygnatur oraz daty ostatniego połączenia z serwerem centralnym. Dane prezentowane w sposób graficzny lub opisowy przedstawiać mogą status wybranej grupy komputerów lub całej organizacji. Istnieje możliwość zapisania wygenerowanego raportu w postaci pliku PDF, XLS, XML lub TIFF.

Informacje dodatkowe:

Minimalne wymagania instalacyjne:

- **Ochrona stacji roboczych:**

  Procesor: *Pentium 300Mhz*

  RAM: *Pełen pakiet ochronny 128MB (Antimalware: 64MB)*

  DYSK: *130 MB*

  System Operacyjny: *Windows 2000 Professional, Windows XP (32 & 64 bits), Windows Vista (32 & 64 bits)*

- **Ochrona serwerów:**

  Procesor: *Pentium 300 Mhz*

  RAM: *256MB*

  DYSK: *130 MB*

  System Operacyjny: *Windows 2000 Server, Windows Server 2003 (32 & 64 bits), Windows Server 2008 (32 &64 bits)*

Wymagania związane z procesem zdalnej dystrybucji ochrony:

- **Narzędzie zdalnej dystrybucji:**

  Procesor: *Pentium 266Mhz*

  RAM: 64*MB*

  DYSK: 2*0 MB*

  System Operacyjny: *Windows 2000 Professional, Windows XP (32 & 64-bit), Windows Vista (32 & 64-bit), Windows Server 2000, Windows Server 2003 (32 & 64-bit), Windows Server 2008 (32 & 64-bit).*

- **Stacje komputerowe objęte procesem zdalnej dystrybucji:**
  - system operacyjny musi posiadać funkcję zezwalającą na zdalne wykonywanie poleceń: Windows 2000, Windows XP Professional, Windows Vista, Windows 2003, Windows 2008,
  - wyłączona lokalna zapora sieciowa lub wprowadzony wyjątek zezwalający na udostępnianie zasobów sieciowych/drukarek,
  - system Windows XP musi posiadać wyłączoną opcję *Prostego Udostępniania Plików*,
  - system Windows Vista musi posiadać wyłączoną opcję *Kontroli Konta Użytkownika*,
  - należy posiadać login oraz hasło Administratora komputera.