# PRZEWODNIK ZABEZPIECZEŃ SYSTEMU WINDOWS 8 ORAZ WINDOWS 8.1 WRAZ Z ZAŁĄCZNIKIEM SCM

**WERSJA 1.0**

Opracowanie powstało w ramach programu współpracy w obszarze bezpieczeństwa

Security Cooperation Program (SCP)

Spis treści

# 1. Wstęp

Przewodnik Zabezpieczeń systemu Windows 8 zawiera instrukcje i rekomendacje, które pomogą wzmocnić poziom zabezpieczenia komputerów stacjonarnych i komputerów przenośnych pracujących pod kontrolą systemu Windows 8 w domenie Active Directory Domain Services (AD DS).

Dodatkowo w podręczniku tym zostaną zaprezentowane narzędzia, szczegółowe instrukcje, rekomendacje oraz procesy, które usprawnią w znacznym stopniu proces wdrożenia systemu Windows 8.

Kolejnym elementem będzie wprowadzenie do procesu zarządzania zgodnością wraz z dodatkowymi informacjami i odsyłaczami na temat narzędzi zapewniających zgodność IT oraz zaleceniami Microsoft.

Kluczowym rekomendowanym narzędziem jest Security Compliance Manager[1] (SCM), który w połączeniu z Przewodnikiem Zabezpieczeń systemu Windows 8, zapewnia możliwości eksportowania wszystkich ustawień zasad grupowych, w celu wykorzystania wytycznych bezpieczeństwa w praktyczny sposób we własnym środowisku.

Autorzy dokumentu starali się uczynić ten przewodnik:

- **Sprawdzonym** – bazującym na zebranym doświadczeniu w tej dziedzinie
- **Autorytatywnym** – oferując najlepsze dostępne dobre praktyki w tym zakresie
- **Dokładnym** – przekazując rozwiązanie sprawdzone i przetestowane od strony technicznej
- **Gotowym do użycia** – zapewniając niezbędne kroki do wdrożenia zakończonego sukcesem
- **Użytecznym** – obejmującym rzeczywiste problemy związane z bezpieczeństwem

W dokumencie zamieszczono najlepsze praktyki stosowane w celu implementacji Windows 8, Windows 7 SP1, Windows Vista SP2, Windows Server 2003 SP2, Windows Server 2008 SP2, and Windows Server 2008 R2 SP1 oraz Windows Server 2012 w różnorodnych środowiskach.

W przypadku procesu oszacowania wdrożenia Windows 8 we własnym środowisku można skorzystać z pomocy oferowanej przez narzędzie Microsoft Assessment and Planning Toolkit[2] , które wspomoże określenie gotowości infrastruktury na uruchomienie systemu Windows 8 dla organizacji średniej wielkości, poprzez dokonanie inwentaryzacji sprzętu, określenie scenariusza wsparcia oraz uzyskanie informacji i wskazanie komputerów wymagających aktualizacji sprzętu.

Niniejszy przewodnik przedstawia funkcjonalności, zwiększające poziom zabezpieczeń systemu Windows 8. Zawarte informacje zostały sprawdzone i przetestowane z wykorzystaniem komputerów pracujących w domenie jak i również komputerów autonomicznych, niepracujących w domenie.

**Uwaga:** Wszystkie odniesienia do systemu Windows XP w niniejszym przewodniku dotyczą systemu Windows XP Professional SP3, a odniesienia dotyczące systemu Windows Vista dotyczą systemu Windows Vista SP2.

## 1.1. Streszczenie wykonawcze

Niezależnie od wielkości środowiska organizacji, należy sprawy bezpieczeństwa teleinformatycznego traktować bardzo poważanie, wiele organizacji nie zawsze docenia wartość i znaczenie, jaką stanowią

[1] http://go.microsoft.com/fwlink/?LinkId=113940
[2] http://go.microsoft.com/fwlink/?LinkId=105520

nowoczesne technologie informatyczne. W przypadku skutecznego przeprowadzonego ataku na serwery organizacji, może okazać się, iż skutki takiego działania odczuwalne będą dla normalnego funkcjonowania organizacji, a kluczowe procesy biznesowe zostaną zakłócone. Na przykład: W przypadku zainfekowania komputerów klienckich przez oprogramowanie złośliwe we własnej sieci, organizacja może utracić dane wrażliwe i ponieść określone koszty na przywrócenie stanu sprzed ataku. Przeprowadzenie ataku na firmową witrynę internetową, może przyczynić się do jej niedostępności oraz narazić organizację na straty finansowe oraz utratę zaufania przez klientów, łącznie z utratą reputacji.

Zgodność z przepisami i standardami staje się kluczową kwestią dla działania organizacji, a organy urzędowe zalecają lub nakazują stosowanie się do wytycznych i zaleceń dla zapewnienia zgodności ze standardami. Audytorzy wykonując ocenę dojrzałości organizacji przeważnie wymagają od organizacji potwierdzenia podjętych działań i weryfikują działania określne w wymaganiach i wytycznych zawartych w regulacjach. Brak podjętych działań w kierunku zapewnienia zgodności z obowiązującymi wytycznymi i regulacjami, może narazić organizację na straty finansowe, utarte reputacji lub nałożenia kary grzywny lub innych kar przewidzianych w obowiązującym prawie.

Przeprowadzenie analizy podatności pod kątem bezpieczeństwa, występujących ryzyk i występowania zagrożeń pozwala na znalezienie kompromisu pomiędzy zapewnieniem bezpieczeństwa a funkcjonalnością dla wszystkich systemów informatycznych pracujących w organizacji. Przewodnik niniejszy przedstawi najważniejsze środki zaradcze odnoszące się do aspektów bezpieczeństwa i jednocześnie omówi dostępne funkcjonalności systemu Windows 8, wskazując na potencjalne niebezpieczeństwa i negatywny wpływ, (jeśli taki występuje) podczas wdrażania omawianych środków zaradczych w celu podniesienia poziomu bezpieczeństwa w organizacji.

Przewodnik bezpieczeństwa prezentuje w dostępny sposób niezbędne informacje oraz wspomagające narzędzia zapewniając:

- Wdrożenie i zastosowanie ustawień bazowych zapewniających wyższy poziom bezpieczeństwa w środowisku organizacji.
- Zapoznanie i wykorzystanie funkcjonalności związanych z bezpieczeństwem systemu Windows 8 w najbardziej popularnych scenariuszach.
- Zapoznanie i omówienie poszczególnych ustawień zabezpieczeń wraz z określeniem ich znaczenia

W celu przeprowadzenia testów i wdrożenia ustawień zabezpieczeń, należy skorzystać z narzędzia Security Compliance Manager (SCM). Narzędzie to ułatwi w znacznym stopniu i zautomatyzuje proces wdrażania bazowych ustawień bezpieczeństwa. Szczegółowy poradnik jak korzystać z narzędzia SCM został przedstawiony, jako dodatek **„Narzędzie Security Compliance Manager (SCM) w praktyce”.**

Pomimo, iż przewodnik ten kierowany jest do dużych organizacji, to większość z zawartych tutaj informacji jest odpowiednia dla każdej organizacji bez względu na jej wielkość. Najlepszy efekt można osiągnąć zapoznając się z całym przewodnikiem, jednakże możliwe jest zapoznanie się z poszczególnymi i wybranymi częściami materiału, aby osiągnąć postawiony cel zapewnienia zapewnienie odpowiedniego poziomu bezpieczeństwa dla organizacji i towarzyszących jej celom biznesowym.

## 1.2. Zarządzanie bezpieczeństwem i zgodnością ze standardami z zastosowaniem technologii

Organizacje wymagają od swoich działów IT dostarczenia bezpiecznej infrastruktury w sprawny i podlegający kontroli sposób, a jednocześnie takiej, która będzie zgodna z obowiązującymi regulacjami, standardami oraz najlepszymi praktykami. Dział IT musi dokonywać ciągłej kontroli zgodności, aby zapewnić i sprostać wymaganiom stawianym organizacjom przez obowiązujące regulacje, stosowane standardy certyfikacji oraz najlepsze praktyki branżowe zgodne z bieżącą polityką bezpieczeństwa. Zapewnienie zgodności wymaga ciągłego procesu dostosowywania się do pojawiających się nowych technologii wraz z ich złożonością, którym działy IT muszą sprostać poprzez ciągły nadzór, kontrolę oraz raportowanie. W celu dostarczenia zgodnej ze standardami infrastruktury, działy IT muszą zabezpieczać organizacje, poprzez wdrożenia efektywnej metody aktualizacji systemów, utwardzania i procesu automatyzacji zapewnienia zgodności IT. Niniejszy przewodnik stanowi doskonały punkt wyjściowy dla zwiększenia i zapewnienia bezpieczeństwa informacji dla zarządzanych systemów. Firma Microsoft opracowała zbiór przewodników i narzędzi, które wspomagają organizacje niezależnie od jej wielkości. Przewodniki te wspomagają zespoły IT w procesie implementacji, wsparcia i weryfikacji bazowych ustawień systemów wykorzystujących różnorodne produkty Microsoft w swoim środowisku.

Ustawienia bazowe są kluczowym pojęciem określającym zbiór rekomendowanych i zalecanych ustawień wykorzystywanych w całym przewodniku i innych powiązanych dokumentach oraz narzędziach wydanych przez Microsoft.

**Co oznacza termin ustawienia bazowe (ang. baseline)?**

Ustawienia bazowe to zbiór rekomendowanych ustawień konfiguracji elementów dla poszczególnych produktów Microsoft, które dostarczają zalecane wartości ustawień do minimalizacji określonego ryzyka, poprzez określone czynności kontrolne.

Czynności kontrolne są w obszarze zainteresowania szczególnie osób na stanowisku Compliance Manager oraz każdej osoby odpowiedzialnej za bezpieczeństwo w organizacji z uwagi na podejmowane działania związane z występującym ryzykiem w organizacjach, co, do których muszą zostać określone zasady jak zarządzać danym ryzykiem i w jaki sposób je minimalizować, korzystając z określonych technologii. Firma Microsoft przez wiele lat publikowała zbiory ustawień bazowych zwracając szczególną uwagę na ustawienia konfiguracji dotyczącej zabezpieczeń komputerów w celu podniesienia poziomu produktów Microsoft. Zbiory te zawierały gotowe rekomendowane ustawienia do bezpośredniego zastosowania i wykorzystania przez administratorów IT we własnym środowisku produkcyjnym.

Po wprowadzeniu produktu IT GRC Process Management Pack dla Manager 2012·, zostały opublikowane bazowe ustawienia konfiguracji dla zapewnienia zgodności ze standardami (ang. compliance baselines).

Na potrzeby wytycznych opisanych w przewodniku, bazowe ustawienia konfiguracji zawierają następujące elementy:

1. Lista rekomendowanych środków zaradczych mających na celu zwiększenie poziomu zabezpieczeń produktów Microsoft.

2. Informacje techniczne niezbędne do implementacji każdego środka zaradczego minimalizującego ryzyko.
3. Informacje techniczne niezbędne do oszacowania stanu każdego środka zaradczego minimalizującego ryzyko, które pozwolą na automatyczne skanowanie stanu zgodności wraz utworzeniem raportu z przeprowadzonej czynności.
4. Uporządkowane ustawienia zgrupowane zostały w elementy konfiguracji (ang. Configuration Item (CI)) stanowiące istotny element powiązania IT Governance, Risk, and Compliance (IT GRC) Process Management Pack (PMP) z czynnościami kontrolnymi.

**W jaki sposób osiągnąć korzyści ze stosowania bazowych ustawień konfiguracji?**

W pierwszej kolejności rekomendowane są identyfikacje systemów operacyjnych i aplikacji wykorzystywanych we własnej sieci komputerowej w celu określenia właściwych ustawień bazowych konfiguracji, które zostaną zaimplementowane, czynności te można przeprowadzić w kilku krokach:

- Przeprowadzenie inwentaryzacji posiadanych zasobów w sieci można wykonać korzystając z bezpłatnego i automatycznego narzędzia Microsoft Assessment and Planning Toolkit[3], które upraszcza i zautomatyzuje proces inwentaryzacji obniżając nakłady pracy na wykonanie tej czynności.
- Dokonanie wyboru właściwych bazowych ustawień konfiguracji korzystając z przygotowanych rozwiązań Microsoft lub innych upoważnionych organizacji, jako punkt wyjścia.
- Analiza i skorygowanie bazowych ustawień konfiguracji, tak, aby spełniały wymagania potrzeb biznesowych organizacji oraz organów wydających regulacje, korzystając z informacji udostępnionych w narzędziu SCM, przewodników zabezpieczeń, oraz Information Technology Governance, Risk, and Compliance (IT GRC) Process Management Pack for System Center Service Manager[4].
- Zastosowanie celów kontrolnych i czynności kontrolnych w połączeniu z ustawieniami bazowymi w celu właściwej konfiguracji i utrzymania stanu zgodności IT zarządzanych systemów.

Konfiguracja ustawień dla produktów Microsoft takich jak systemy Windows, Microsoft Office, oraz Internet Explorer może być zarządzana poprzez wykorzystanie zasad grupowych (Group Policy), korzystając z narzędzia SCM w celu dopasowania ustawień bazowych do własnych potrzeb. Po przygotowaniu ustawień należy je wyeksportować w postaci arkusza Excel w celu przeprowadzenia rozmów ze stronami zainteresowanymi całej organizacji. Po zatwierdzeniu ustawień, należy je wyeksportować w postaci kopi zapasowej zasad grupowych, i wdrożyć je w środowisku testowym wykorzystując mechanizm zasad grupowych usług katalogowych Active Directory. W przypadku komputerów niepracujących w domenie, należy zastosować narzędzie Local Policy Tool, które dostępne jest w narzędziu SCM (narzędzie to będzie omówione rozdziale 2.5).

[3] http://go.microsoft.com/fwlink/?LinkId=105520
[4] http://go.microsoft.com/fwlink/?LinkId=201578

## 1.3. Praca z rekomendowanymi bazowymi ustawieniami konfiguracji (baseline)

Narzędzie SCM zawiera rekomendowane bazowe ustawienia konfiguracji dla produktów Microsoft, które mogą być zarządzane i dostosowywane do własnych potrzeb. Po wprowadzeniu zmian spełniających wymagania organizacji do bazowych ustawień konfiguracji, można przeprowadzić proces weryfikacji ustawień zasad grupowych dla każdego komputera poprzez wygenerowanie dostosowanych ustawień bazowych w narzędziu SCM. W celu osiągnięcia standaryzacji i zgodności ze standardami można osiągnąć poprzez utworzenie pakietów Desired Configuration Management (DCM) dla bazowych ustawień a następnie zaimportowanie tych ustawień do rozwiązania System Center Configuration Manager. Zastosowanie funkcjonalności DCM dla System Center Configuration Manager zautomatyzuje proces wdrożenia ustawień zapewniających zgodność ze standardami. Dodatkowo narzędzie SCM pozwala na wykonanie eksportu bazowych ustawień konfiguracji w formacie Security Content Automation Protocol (SCAP). Format SCAP jest wspierany przez wiele narzędzi służących do zarządzania zabezpieczeniami i konfiguracją dostarczonych przez Microsoft oraz firmy trzecie. W celu uzyskania dodatkowych informacji na temat formatu SCAP, należy zapoznać się informacjami umieszczonymi stronie National Institute of Standards and Technology (NIST) [5].

Kontrolę podjętych czynności mających na celu zapewnienie zgodności można wykonać poprzez zastsoowanie i integrację produktów Microsoft System Center Service Manager i IT GRC Process Management Pack. Czynność ta wspomaga organizacje w osiągnięciu celu implementacji procesu ładu korporacyjnego, zarządzania ryzykiem i zgodności ze standardami IT (IT GRC). Produkt System Center Service Manager umożliwia przygotowanie automatycznych raportów przeznaczonych dla kard kierowniczych, audytorów IT oraz innych osób biorących udział w projekcie. Proces IT GRC zostanie omówiony szerzej w rozdziale drugim „Ład korporacyjny, zarządzanie ryzykiem oraz zgodność ze standardami w IT (IT GRC)".

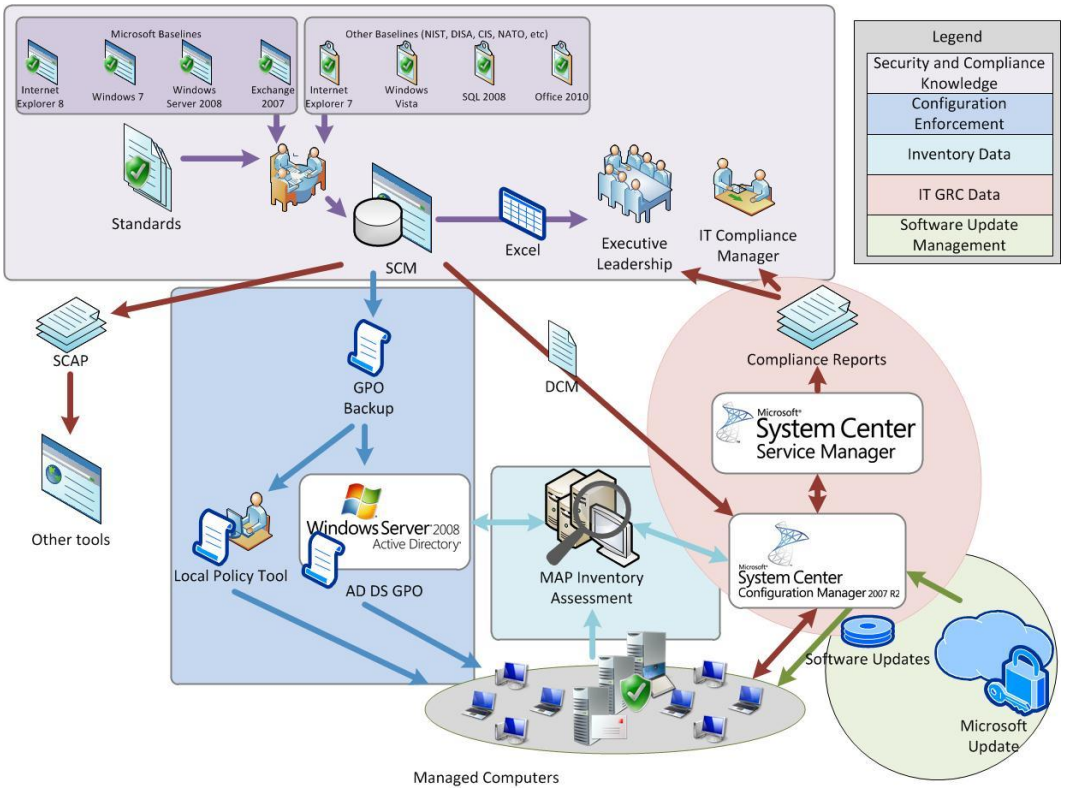
Narzędzie SCM wspomaga zarządzania bazowymi ustawieniami konfiguracji dla produktów Microsoft, których nie można konfigurować poprzez zasady grupowe (Group Policy), takie jak serwer Microsoft Exchange. SCM zawiera zestaw skryptów PowerShell dla tego typu produktów, które umożliwią wdrożenie bazowych ustawień konfiguracji dla jednego lub wielu serwerów korzystając z procesu automatyzacji, który poprzez wykorzystanie skryptów (programów) ułatwiających wykonanie zadań powtarzających się ograniczając w tym procesie czynności wykonywane przez ludzi.

Ten sam zestaw skryptów można również wykorzystać w celu przeskanowania komputerów pod kątem zgodności, możliwe jest również skorzystanie z funkcji eksportowania pakietów konfiguracyjnych DCM w narzędziu SCM. W celu uzyskania dodatkowych informacji należy zapoznać się dokumentem „Exchange Server PowerShell Script Kit User Guide", który dostępny jest wewnątrz narzędzia SCM w obszarze **Attachments \ Guides.**

Na Rys. 1.3.1. przedstawiono proces zarządzania bezpieczeństwem i zgodnością ze standardami z zastosowaniem technologii dla potrzeb organizacji.

[5] http://scap.nist.gov/

Więcej informacji na temat narzędzia SCM, znajduje się na stronie Microsoft Security Compliance Manager[6]. Warto również odwiedzić witrynę SCM Wiki[7] na stronach TechNet.




Rys. 1.3.1. Zarządzanie bezpieczeństwem i zgodnością ze standardami z zastosowaniem technologii dla potrzeb organizacji

## 1.4. Dla kogo przeznaczony jest ten podręcznik?

Podręcznik przeznaczony jest w głównej mierze dla specjalistów zarządzających bezpieczeństwem, architektów sieciowych, Administratorów IT, specjalistów IT oraz konsultantów planujących wdrożenie infrastruktury IT, wdrożenie systemu Windows 8 na komputerach klienckich w środowisku domenowym jak i poza domenowym.

## 1.5. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe zasoby zawierające informacje na tematy związane z bezpieczeństwem systemu Microsoft Windows 8:

- Federal Desktop Core Configuration (FDCC)[8].
- Microsoft Assessment and Planning Toolkit[9].
- Microsoft Security Compliance Manager[10].
- SCM Wiki[11].

[6] http://go.microsoft.com/fwlink/?LinkId=113940
[7] http://social.technet.microsoft.com/wiki/contents/articles/microsoft-security-compliance-manager-scm.aspx#comment-2585
[8] http://fdcc.nist.gov/
[9] http://go.microsoft.com/fwlink/?LinkId=105520
[10] http://go.microsoft.com/fwlink/?LinkId=113940

Security and Compliance Management Forum[12].

[11] http://social.technet.microsoft.com/wiki/contents/articles/microsoft-security-compliance-manager-scm.aspx#comment-2585
[12] http://social.technet.microsoft.com/Forums/en-us/compliancemanagement/threads

# 2. Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 8

## 2.1. Wprowadzenie

Firma Microsoft wraz z każdym nowo udostępnianym systemem operacyjnym wprowadza nowe rozwiązania w zakresie bezpieczeństwa. Ich duża różnorodność w Windows 8 powoduje, że jest on aktualnie najlepiej zabezpieczonym systemem Windows, który został do tej pory wydany. Konfiguracja opcji zabezpieczeń – w odróżnieniu od wcześniejszych wersji Windows – odbywa się obecnie poprzez Zasady polityk grupowych GPO (z ang. Group Policy Object). Mechanizm GPO zapewnia centralną infrastrukturę umożliwiającą w oparciu o strukturę hierarchiczną zarządzanie ustawieniami komputerów i/lub użytkowników włączając w to ustawienia zabezpieczeń.

Znane poprzednio kategorie odniesienia dla ustawień bezpieczeństwa Specialized Security – Limited Functionality (SSLF) oraz Enterprise Client (EC) zostały zastąpione poziomami ważności (ang. severity level):

- Krytyczny
  Ustawienia na tym poziomie mają wysoki stopień wpływu na bezpieczeństwo komputera i/lub przechowywanych na nim danych. Zaleca się stosowanie wszystkich ustawień krytycznych w organizacji
- Istotny
  Ustawienia na tym poziomie mają znaczący wpływ na bezpieczeństwo komputera i/lub przechowywanych na nim danych. Są one konfigurowane w organizacjach, które przechowują wrażliwe dane a tym samym są one ukierunkowane na ochronę swoich systemów informatycznych.
- Opcjonalny
  Ustawienia na tym poziomie mają niewielki wpływ na bezpieczeństwo, przez co większość organizacji pomija je na etapie projektowania zasad bezpieczeństwa. Nie oznacza to jednak dowolności w zakresie ich stosowania. Dla przykładu - wiele ustawień dotyczących Windows, Internet Explorer czy Office ukrywa elementy interfejsu użytkownika, które upraszczają pracę a nie mają bezpośredniego wpływu na bezpieczeństwo.
- Niezdefiniowany
  Jest to domyślny poziom ważności w Security Compliance Manager. Ustawienia, które nie były dostępne wcześniej są oznaczone takim poziomem. Przyjmuje się, że ich znaczenie porównywalne jest z poziomem Opcjonalny, przez co mają bardzo mały lub zerowy wpływ na bezpieczeństwo.

W zależności od wybranego formatu eksportu dla reguł, poziomy ważności przyjmują nazwy zgodnie z poniższą tabelą:

| Security Compliance Manager (SCM) | Desired Configuration Management (DCM) | Security Content Automation Protocol (SCAP) |
|---|---|---|
| Krytyczny | Krytyczny | Wysoki |
| Istotny | Ostrzegawczy | Średni |
| Opcjonalny | Informacyjny | Niski |
| Niezdefiniowany | Inny | Nieznany |

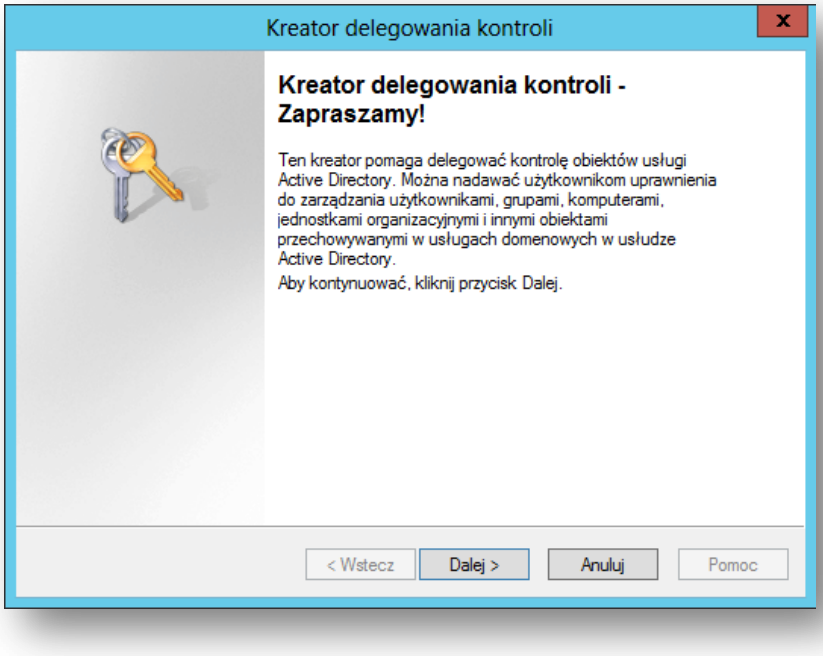
Tab. 2.1.1 Wykaz nazw poziomów ważności w zależności od wybranego formatu eksportu

## 2.2. Projektowanie struktur jednostek organizacyjnych (OU) ze szczególnym uwzględnieniem zasad bezpieczeństwa

Usługa katalogowa Active Directory umożliwia scentralizowane zarządzanie infrastrukturą przedsiębiorstwa. Dzięki hierarchicznej budowej można stworzyć model, który będzie uwzględniał narzucone i pożądane aspekty bezpieczeństwa organizacji.

Jednostka organizacyjna OU (z ang. Organizational Unit) jest kontenerem wewnątrz domeny Active Directory Domain Services (AD DS), który może zawierać użytkowników, grupy, komputery oraz inne jednostki organizacyjne. Wyróżniamy nadrzędne oraz podrzędne jednostki organizacyjne.

Jedną z ważnych cech jednostek organizacyjnych jest możliwość dołączania do nich zbiorów zasad grupowych GPO. Dzięki temu zadeklarowane ustawienia mogą być przekazywane do znajdujących się wewnątrz obiektów użytkowników i komputerów. Dodatkowo istnieje możliwość delegowania kontroli administracyjnej (rys. 2.2.1) nad jednostkami organizacyjnymi, dzięki czemu upraszcza się zarządzanie.

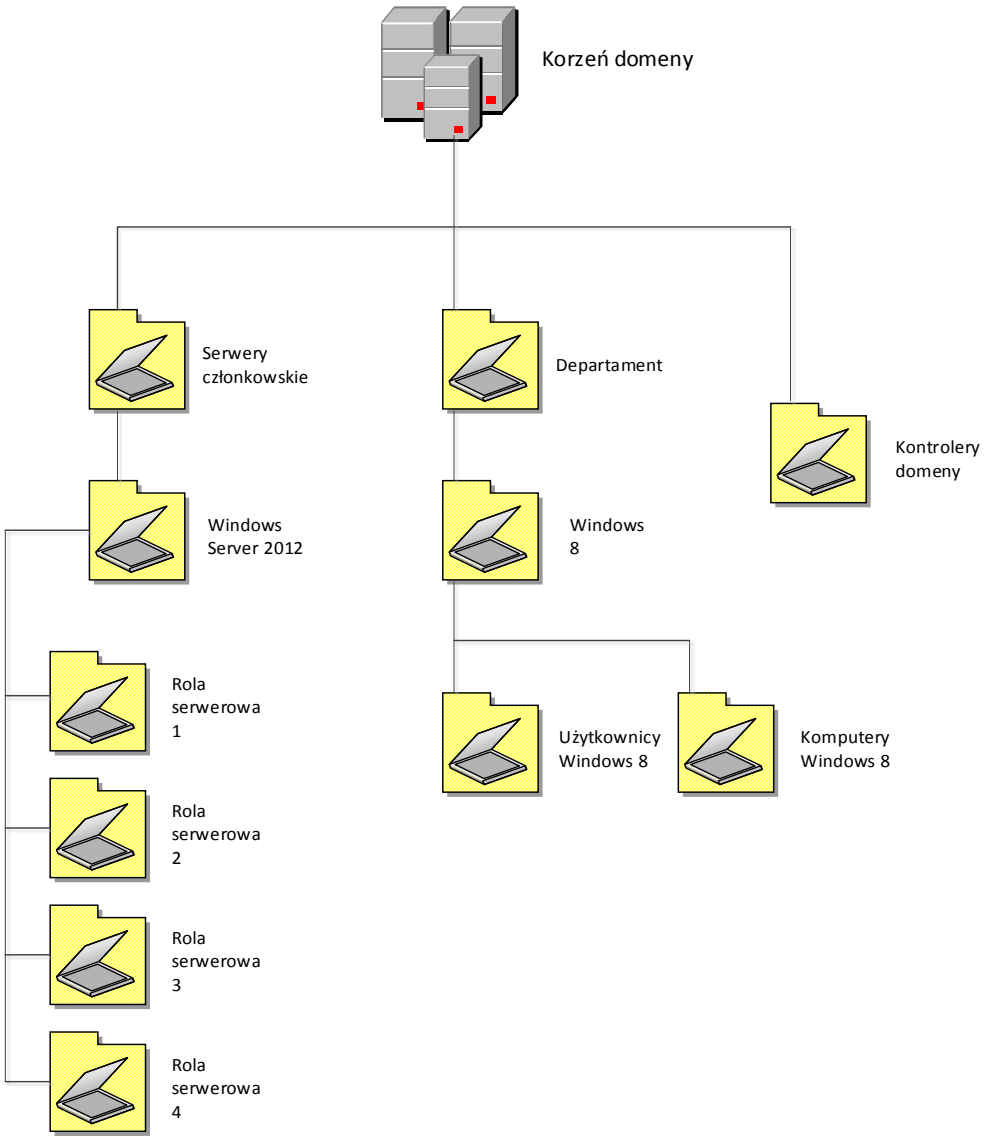



Rys. 2.2.1 Kreator delegowania kontroli w Użytkownicy i komputery Active Directory.

Dzięki jednostkom organizacyjnym można również tworzyć granice administracyjne oddzielające użytkowników od komputerów. Takie rozwiązanie idealnie sprawdza się w scenariuszach stosowania ustawień wyłącznie dedykowanych komputerom oraz wyłączenie dedykowanych użytkownikom.

Najważniejszym celem projektowania struktury jednostek organizacyjnych powinna być możliwość jednolitej implementacji zasad grupowych z uwzględnieniem spełnienia wszystkich standardów i zaleceń w zakresie bezpieczeństwa.

Na rysunku 2.2.2 zaprezentowana została przykładowa struktura uwzględniająca możliwe do zastosowania poziomy jednostek organizacyjnych w typowych rozwiązaniach usług katalogowych Active Directory.




Rys. 2.2.2 Przykładowa struktura jednostek organizacyjnych dla komputerów oraz użytkowników.

**Korzeń domeny**

Ustawienia, które dotyczą zabezpieczeń całej domeny można stosować w ramach GPO dołączonego do domeny. Na tym poziomie nie są zarządzane komputery oraz użytkownicy.

**Jednostki organizacyjne**

Serwery pełniące role kontrolerów domeny przechowują wiele wrażliwych danych, w tym dane, które kontrolują konfigurację zabezpieczeń ich samych. Stosowanie GPO na poziomie jednostki organizacyjnej Kontrolery domeny umożliwia konfigurację i ochronę kontrolerów domeny.

**Serwery członkowskie**

Stosowanie zasad GPO do pośredniej jednostki organizacyjnej Serwery członkowskie zapewnia możliwość konfiguracji stałych opcji dla wszystkich serwerów bez uwzględniania podziału na pełnione przez ni role.

**Role serwerowe**

Dobrą praktyką jest tworzenie dedykowanych jednostek organizacyjnych dla wszystkich ról serwerowych w organizacji. Dzięki temu zachowuje się ujednolicony model, który umożliwia stosowanie zasad GPO opartych na rolach serwerowych.

Dla serwerów utrzymujących wiele ról można tworzyć dodatkowe jednostki organizacyjne zgodnie z ich konfiguracją. W kolejnym kroku do takiej jednostki organizacyjnej dołącza się zbiory GPO dedykowane określonym rolom serwerowym. Należy zwrócić szczególną uwagę na mieszane konfiguracje, aby uwzględnić kolejność przetwarzania zasad GPO a tym samym uzyskiwane, wynikowe ustawienia.

**Departament**

Wymagania w zakresie zabezpieczeń są różne i często zależne są od struktury organizacyjnej. Tym samym tworzenie jednostek organizacyjnych dla poszczególnych komórek pozwala na stosowanie ustawień zabezpieczeń dla komputerów i użytkowników w zgodzie z przydziałem biznesowym.

**Użytkownicy Windows 8**

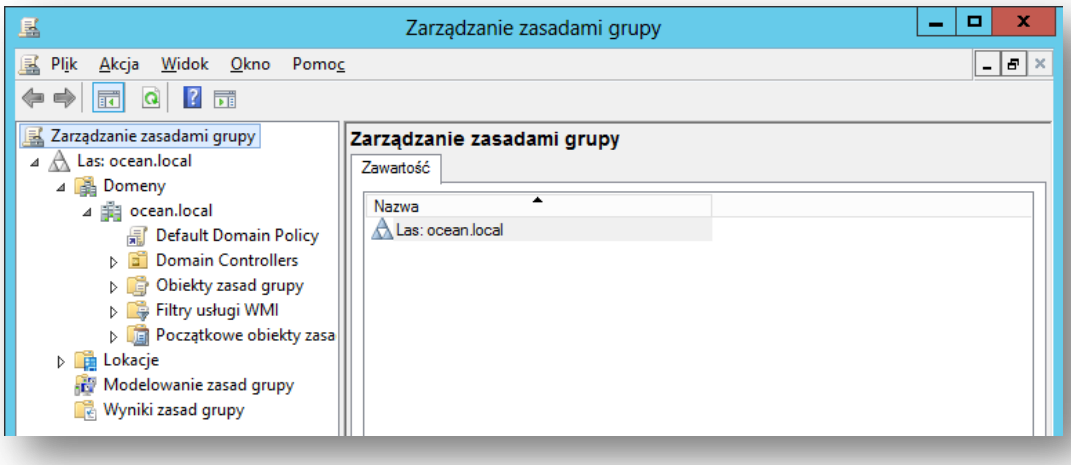
Stosowanie specjalnych jednostek organizacyjnych, w których przechowywane są konta użytkowników daje możliwość stosowania dedykowanych dla nich zasad zabezpieczeń.

**Komputery Windows 8**

Stosowanie dedykowanych jednostek organizacyjnych, w których przechowywane są konta komputerów pozwala na stosowanie ustawień zabezpieczeń zarówno dla komputerów stacjonarnych jak i mobilnych.

## 2.3. Projektowanie obiektów zasad grupowych (GPO) struktur jednostek organizacyjnych ze szczególnym uwzględnieniem zasad bezpieczeństwa

GPO jest zbiorem zawierającym ustawienia zasad grupowych, który definiuje się w przystawce Zarządzanie zasadami grupy (Rys. 2.3.1).




Rys. 2.3.1 Przystawka Zarządzanie zasadami grupy.

Ustawienia tam zawarte są przechowywane na poziomie domeny i mogą oddziaływać na użytkowników i/lub komputery znajdujące się w lokacji, domenach i jednostkach organizacyjnych.

Konfiguracja ręczna ustawień zapewniających identyczne efekty może prowadzić do niespójności. W konsekwencji może to wymusić zapewnienie odpowiedniej ilości osób, które będą odpowiadały za jednolite wdrożenie narzuconych zasad.

Wykorzystanie zasad grupowych w odróżnieniu od ręcznej konfiguracji ustawień upraszcza ponad to zarządzanie oraz zapewnia natychmiastową aktualizację zmian dla wielu komputerów i użytkowników. Zasady GPO zdefiniowane w obrębie domeny nadpisują ustawienia zasad lokalnych, co pozwala na utrzymanie centralnego modelu zarządzania konfiguracją.

Kolejność przetwarzania GPO przedstawiona została na rysunku 2.3.2.

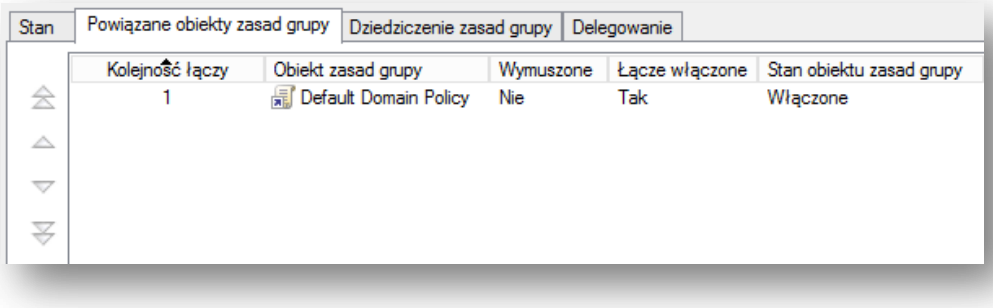

Rys.2.3.2 Kolejność przetwarzania zasad GPO.

Jako pierwsze przetwarzane są zasady lokalne, następnie na poziomie lokacji, domeny oraz jednostek organizacyjnych. Zbiory znajdujące się na poziomie jednostek organizacyjnych są przetwarzane hierarchicznie od najwyższego OU do najniżej położonego OU.

Tym samym ustawienia zdefiniowane dla komputerów znajdujące się na najniższym poziomie hierarchii jednostek organizacyjnych stosowane są, jako ostatnie i mają najwyższy priorytet. Takie działanie obowiązuje od systemów Windows Server 2003 SP2, Windows Server 2008, Windows XP SP3 oraz Windows Vista. Dla użytkowników model przetwarzania zasad jest identyczny.

Istnieje kilka zaleceń związanych z projektowaniem zasad grupowych, o których warto jest pamiętać.

- Administrator powinien ustalić kolejność dołączenia wielu GPO do jednostki organizacyjnej. Domyślnie są one stosowane zgodnie z kolejnością dołączania na etapie konfiguracji. Zasady znajdujące się wyżej na liście **Kolejność łączy** mają wyższy priorytet. Tym samym w przypadku zdefiniowania takiego samego ustawienia w dwóch zbiorach zasad grupowych efektywnym staje się to pochodzące od zbioru mającego wyższy priorytet.




Rys 2.3.3.. Zakładka Powiązane obiekty zasad grupy definiująca kolejność przetwarzania zasad grupowych.

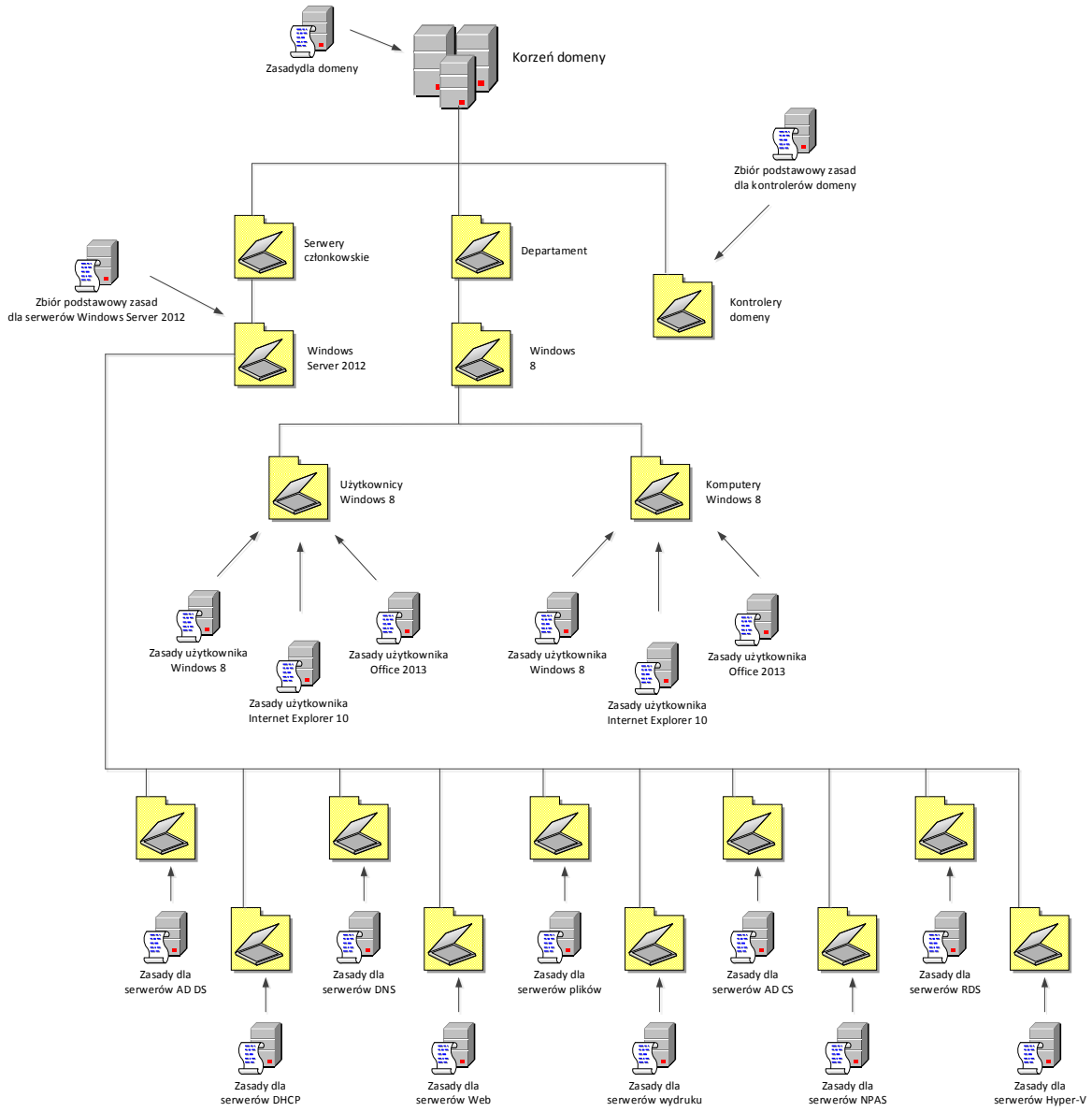
- W ramach konfiguracji GPO dostępna jest opcja **Wymuszone**. Jej zastosowanie powoduje, że zdefiniowane tam zasady nie będą nadpisywane przez inne zbiory – bez względu na ich poziom dołączenia.
- Stosowanie ustawień zasad grupowych ściśle związane jest z położeniem obiektów użytkownik i komputer w AD DS. W niektórych scenariuszach pożądane jest natomiast stosowanie ustawień dla użytkownika w oparciu o położenie obiektu komputer. W takich sytuacjach przydatna staje się opcja **Tryb przetwarzania sprzężenia zwrotnego zasad grupy użytkownika**. Umożliwia ona stosowanie ustawień konfiguracji użytkownika pochodzącego ze zbioru zawierającego ustawienia konfiguracji komputera.
- Na poziomie lokacji, domeny oraz jednostki organizacyjnej można stosować opcję **Zablokuj dziedziczenie**. Jej włączenie powoduje, że ustawienia pochodzące od nadrzędnych zbiorów GPO nie są przekazywane do obiektów podrzędnych. Przy konfiguracji zawierającej opcje **Wymuszone** oraz **Zablokuj dziedziczenie** ważniejszą jest opcja **Wymuszone**.

W odniesieniu do wcześniej zaproponowanej struktury jednostek organizacyjnych (rys. 3.3.2) projekt zakładający wykorzystanie zasad grupowych powinien uwzględnić zbiory GPO zapewniające:

- zasady dla domeny
- zasady dla kontrolerów domeny

- zasady dla serwerów członkowskich
- zasady dla każdej roli serwerowej w organizacji
- zasady dla użytkowników zgromadzonych w jednostce organizacyjnej **Windows 8**
- zasady dla komputerów znajdujących się w jednostce **organizacyjnej Komputery**

Struktura spełniające powyższe warunki została przedstawiona na rysunku 2.3.4.




Rys. 2.3.4 Przykładowa struktura jednostek organizacyjnych z dowiązaniami GPO dla infrastruktury Windows 8 oraz Windows Server 2012.

## 2.4. Zastosowanie filtrowania WMI w celu określenia dokładnej grupy docelowej odbiorców zasad GPO

Filtrowanie oparte o instrumentację zarządzania Windows WMI (z ang. Windows Management Instrumentation) dostępne jest od Windows XP i Windows Server 2003. Mechanizm WMI umożliwia dynamiczne sprawdzanie wartości atrybutów dotyczących komputerów, na które ma oddziaływać

określony zbiór GPO. Atrybuty mogą dotyczyć danych konfiguracyjnych sprzętu i/lub oprogramowania. Przykładowymi atrybutami mogą być:

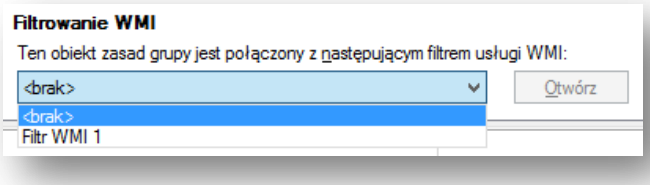
- rodzaj procesora,
- wersja Windows,
- producent komputera,
- wolne miejsce na dysku,
- liczba procesorów logicznych,
- dane odczytywane z rejestru,
- informacje o sterownikach,
- elementy systemu plików,
- konfiguracja sieciowa
- dane aplikacji.

Jeśli ze zbiorem GPO związany jest filtr WMI następuje jego przetwarzanie na stacji. Dzięki temu tylko w sytuacji spełnienia określonych filtrem WMI warunków, ustawienia GPO zostaną zastosowane.

Zapytania WMI tworzone są z wykorzystaniem języka WQL (z ang. WMI Query Language), który jest językiem podobnym do SQL (z ang. Structured Query Language). Zapytania mogą być łączone operatorami AND i OR w zależności od potrzeb.

Każde zapytanie WMI jest wykonywane w przestrzeni nazewniczej WMI. Domyślną przestrzenią jest root\CIMv2.

Filtry WMI są oddzielnymi obiektami od GPO. Aby zastosować filtr WMI należy go dołączyć do zbioru GPO (Rys. 2.4.1).




Rys. 2.4.1 Dołączenie filtru WMI do zbioru GPO.

Każdy zbiór GPO może posiadać tylko jeden filtr WMI. Natomiast pojedynczy filtr WMI może być dołączany do wielu GPO. Filtry WMI oraz powiązane zbiory GPO muszą znajdować się w tej samej domenie.

W tabeli 2.4.2 zawarte zostały przykłady filtrów WMI.

| Kryterium | Cel administracyjny | Filtr WMI |
|---|---|---|
| Konfiguracja | Zablokowanie włączania Microsoft Network Monitor (Netmon.exe) na stacjach, które mają włączony ruch grupowy. | SELECT * FROM Win32_NetworkProtocol WHERE SupportsMulticasting = true |

| | | |
|---|---|---|
| Strefa czasowa | Stosowanie zasad na wszystkich serwerach zlokalizowanych w Polsce. | Root\cimv2 ; SELECT * FROM win32_timezone WHERE bias =-60 |
| Poprawki | Stosowanie zasad na komputerach z zainstalowaną określoną poprawką. | Root\cimv2 ; SELECT * FROM Win32_QuickFixEngineering WHERE HotFixID = 'q147222' |
| Rodzaj komputera | Stlosowanie zasad tylko na komputerach mobilnych. | Root\CimV2; SELECT * FROM Win32_ComputerSystem WHERE PCSystemType = 2 |
| Rodzaj baterii | Stosowanie zasad tylko na komputerach z baterią litowo-jonową. | Root\CimV2; SELECT * FROM Win32_Battery WHERE Chemistry = '6' |
| Inwentaryzacja oprogramowania | Przypisanie oprogramowanie tylko do komputerów, które mają zainstalowany jeden lub więcej określonych pakietów oprogramowania. | Root\cimv2; SELECT * FROM Win32_Product WHERE name = "MSIPackage1" OR name = "MSIPackage2" |
| System operacyjny | Zastosowanie wyłącznie na komputerach z Windows 8. | Root\CimV2; SELECT * FROM Win32_OperatingSystem WHERE Version >=’6.2’ |
| Zasoby | Zastosowanie wyłącznie na komputerach, które mają, co najmniej 4GB wolnego miejsca na dyskach lokalnych. | Root\CimV2; SELECT * FROM Win32_LogicalDisk WHERE FreeSpace > 4294967296 AND MediaType = ‘12’ |

Tab 2.4.2. Przykłady filtrów WMI.

Tworzenie i zarządzanie filtrami WMI może być wykonane za pomocą dodatkowych narzędzi:

- WMI Administrative Tools
  http://www.microsoft.com/en-us/download/details.aspx?id=24045
- WMI Code Creator
  http://www.microsoft.com/en-us/download/details.aspx?id=8572
- Windows PowerShell Scriptomatic
  http://www.microsoft.com/en-us/download/details.aspx?id=24121

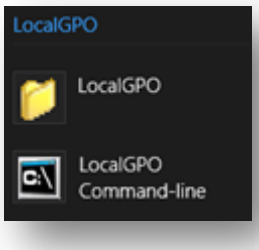
## 2.5. Omówienie narzędzia Local Policy Tool

W ramach Security Compliance Manager dostępne jest narzędzie tekstowe LocalGPO. Umożliwia ono wykonywanie wielu czynności obsługowych na zbiorach ustawień zasad grupowych, wśród nich:

- stosowanie ustawień zabezpieczeń w kontekście lokalnych ustawień zasad grupowych,
- eksport lokalnych ustawień zasad grupowych,
- tworzenie pakietów zawierających ustawienia, które można stosować na stacjach bez zainstalowanego narzędzie LocalGPO,
- centralizację lokalnych zbiorów zasad grupowych za pomocą Multiple Local GPO (MLGPO),
- aktualizację interfejsu graficznego do wyświetlania dodatkowych ustawień zbiorów zasad grupowych w ramach grupy MSS (z ang. Microsoft Solutions for Security).

Narzędzie LocalGPO nie jest automatycznie instalowane wraz z SCM. W celu instalacji należy uruchomić z lokalizacji **c:\Program Files (x86)\Microsoft Security Compliance Manager\LGPO** plik **LocalGPO.msi** i wykorzystując kreatora wybrać preferowane opcje instalacji.

Po pomyślnym zainstalowaniu LocalGPO w ramach Menu Start dostępny jest folder LocalGPO:




Rys.2.5.1 Folder LocalGPO w Menu Start.

## 2.6. Omówienie i praktyczne zastosowanie narzędzia Attack Surface Analyzer (ASA)

Firma Microsoft udostępniła narzędzie Attack Surface Analyzer (ASA), które umożliwia określenie zmian dokonywanych na systemie operacyjnym komputera podczas instalacji oprogramowania. Działanie narzędzia ASA poprzedzone jest każdorazowo wykonaniem migawki stanu komputera. Po instalacji żądanego oprogramowania wyświetlany jest raport o zmianach w zakresie:

- usług
- sterowników
- uruchomionych procesów
- kontrolek COM
- serwerów DCOM
- zmian dokonanych w zakresie uprawnień domyślnych DCOM
- skojarzeń rozszerzeń plików
- kontrolek Microsoft ActiveX
- Internet Explorer Pluggable Protocol Handlers
- Internet Explorer Silent Elevation Entries
- Internet Explorer Preapproved Controls
- portów
- strumieni nazw
- reguł zapory
- punktów końcowych wywołań RPC
- wpisów ścieżek
- grup i członkostwa w nich
- zasobów sieciowych

Dzięki raportowi, który dostarcza ASA można łatwo określić wpływ instalacji oprogramowania na funkcje Windows oraz można w łatwy sposób je zweryfikować.

## 2.7. Omówienie mechanizmu kont MSA

Jedną z nowych funkcji w Windows 7 SP1 oraz Windows Server 2008 R2 są konta MSA (z ang. Managed Service Accounts), które pozwalają zmniejszyć ryzyko kompromitacji kont używanych do

zarządzania usługami. Na stacjach lokalnych administrator może konfigurować aplikacje do uruchamiania w kontekście kont Usługa lokalna, Usługa sieciowe lub System lokalny. W przypadku domeny zasięg działania uniemożliwia jednak ich wykorzystanie.

Stosując standardowe konta użytkowników do uruchamiania aplikacji należy zadbać o politykę związaną z zarządzaniem hasłami. Konta MSA umożliwiają w tym zakresie pełną automatyzację. Dodatkowo zapewniają możliwość ustawiania dla nich nazwy głównej usługi SPN (z ang. Service Principal Name) oraz delegowanie zarządzania SPN.

Zarzadzanie kontami MSA odbywa się wyłącznie z poziomu PowerShell.

Kontrolery domeny działające pod kontrolą Windows Server 2008 i Windows Server 2003 posiadają wsparcie dla kont MSA.

W Windows 8 oraz Windows Server 2012 wprowadzono grupy MSA. Zapewniają one możliwość użycia kont MSA w środowisku, gdzie więcej niż jeden komputer wymaga uruchomienia usług za pomocą tego samego konta.

## 2.8. Ustawienia zasad domenowych

Domyślnie do obiektów usługi katalogowej Active Directory Domain Services stosowana jest ograniczona liczba ustawień zabezpieczeń. Są one konfigurowane w obrębie węzła Konfiguracja komputera, w ramach:

- Zasady haseł
- Zasady blokady konta

Poniżej omówione zostały szczegółowe ustawienia w zakresie tych gałęzi.

Zalecenia dotyczące ustawień w zależności od roli serwerowej znajdują się w narzędziu Security Compliance Manager (SCM).

### 2.8.1 Konfigurowanie ustawień dla zbioru Zasady haseł

Jednym z kluczowych założeń bezpieczeństwa systemów IT jest dobrze dobrana i ustalona polityka dotycząca haseł. Takie elementy jak złożoność haseł, cykliczność zmiany czy świadomość ich przechowywania składają się na ogólną politykę bezpieczeństwa stanowiąc kluczowy aspekt całości.

Zasady dotyczące haseł zorganizowane są w obrębie gałęzi

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady haseł**

**(Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy)**

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Wymuszaj tworzenie historii haseł | Krytyczny | 24 pamiętane hasła | 24 pamiętane hasła |
| Maksymalny okres ważności hasła | Krytyczny | 42 dni | 60 dni |

| | | | |
|---|---|---|---|
| Minimalny okres ważności hasła | Krytyczny | 0 dni | 1 dzień |
| Minimalna długość hasła | Krytyczny | 0 znaków | 14 znaków |
| Hasło musi spełniać wymagania, co do złożoności | Krytyczny | Wyłączone | Włączone |
| Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego | Krytyczny | Wyłączone | Wyłączone |

W hasłach mogą być stosowane znaki z czterech grup:

- Wielkie litery
- Małe litery
- Cyfry
- Znaki specjalne

Złożoność hasła (w kontekście zasady „Hasło musi spełniać wymagania co do złożoności") oznacza, że są w nim wykorzystane znaki z co najmniej trzech powyższych grup.

Zapewnienie zmiany haseł przez użytkowników tylko w ściśle określonym momencie wymaga ustalenia zasad dotyczących minimalnego i maksymalnego wieku hasła. Dla zasad „Minimalny okres ważności hasła" oraz „Maksymalny okres ważności hasła" obowiązują poniższe zależności.

- Minimalny okres ważności hasła
  Wartość minimalna – 0 – oznacza, że hasło może być zmieniane w dowolnym momencie.
  Wartość maksymalna – 998 – oznacza, że hasło może być zmienione po upływie 998 dni.
- Maksymalny okres ważności hasła
  Wartość minimalna – 0 – oznacza, że ważność hasła nigdy nie wygasa.
  Wartość maksymalna – 999 – oznacza, że ważność hasła wygasa po 999 dniach.

Między zasadami „Minimalny okres ważności hasła" a „Maksymalny okres ważności hasła" obowiązuje zależność:

Maksymalny okres ważności hasła = Minimalny okres ważności hasła + 1

Domyślnie użytkownicy mogą zmienić swoje hasło w interwale czasowym określonym parametrami minimalny i maksymalny okres ważności hasła. Jeśli istnieje potrzeba zablokowania możliwości zmiany hasła przez użytkownika w interwale narzuconym powyższymi ustawieniami można włączyć polityk Usuń opcję Zmień hasło (dostępną po wciśnięciu klawiszy Ctrl+Alt+Delete) w ramach ustawień zasad grupowych w:

**Konfiguracja użytkownika\Szablony administracyjne\System\Opcje klawiszy Ctrl+Alt+Delete**

## 2.9. Konfigurowanie ustawień haseł granularnych oraz dla zbioru Zasady blokady konta

Wśród ustawień związanych z hasłami użytkowników istotną rolę pełnią ustawienia haseł granularnych (ang. Fine-Grained Password) oraz Zasady blokady konta.

Hasła granularne to rozwiązanie, które umożliwia wdrożenie modelu ustawień zasad haseł dedykowanego określonym użytkownikom lub grupom użytkowników. Jest to możliwe w środowisku domenowym o poziomie funkcjonalności domeny od Windows Server 2008.

Zasady blokady konta zapewniają ochronę przed próbami odgadnięcia haseł użytkowników. Realizowane to jest przez zliczanie błędnych prób logowania i wykonanie określonej akcji związanej ze stanem konta użytkownika. Zasady blokady konta znajdują się w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady blokady konta**

**(Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy)**

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Czas trwania blokady konta | Krytyczny | Brak | 15 minut |
| Próg blokady konta | Krytyczny | 0 nieudanych prób zalogowania | 5 nieudanych prób zalogowania |
| Wyzeruj licznik blokady konta po | Krytyczny | Brak | 15 minut |

## 2.10. Ustawienia zasad Computer Policy Settings

Ustawienia zabezpieczeń stosowane dla obiektów Komputer są skupione wokół poniższych gałęzi:

- Zasady inspekcji
- Przypisywanie praw użytkownika
- Opcje zabezpieczeń
- Dziennik zdarzeń
- Zapora systemu Windows z zabezpieczeniami zaawansowanymi
- Szablony administracyjne

## 2.11. Konfigurowanie szczegółowych ustawień zbioru Zasady inspekcji

Zasady inspekcji umożliwiają gromadzenie szczegółowych informacji na temat aktywności użytkowników i systemu w określonych kategoriach.

W Windows 8 dostępnych jest 9 kategorii głównych oraz ustawienia podkategorii dostępne w gałęzi Inspekcja globalnego dostępu do obiektów.

Zasady inspekcji kategorii głównych znajdują się w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Zasady inspekcji**

**(Computer Configuration\Windows Settings\Security Settings\Local Policies\Reguły Audytu)**

- Przeprowadzanie inspekcji zdarzeń logowania na kontach
- Przeprowadź inspekcję dostępu do obiektów
- Przeprowadź inspekcję dostępu do usługi katalogowej

- Przeprowadź inspekcję śledzenia procesów
- Przeprowadź inspekcję użycia uprawnień
- Przeprowadź inspekcję zarządzania kontami
- Przeprowadź inspekcję zdarzeń logowania
- Przeprowadź inspekcję zdarzeń systemowych

Zasady inspekcji podkategorii znajdują się w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Konfiguracja zaawansowanych zasad inspekcji**

**(Computer Configuration\Windows Settings\Security Settings\Zaawansowana Konfiguracja Reguł Audytu)**

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Przeprowadź inspekcję weryfikacji poświadczeń | Krytyczny | Nie skonfigurowano | Sukces i Niepowodzenie |
| Przeprowadź inspekcję usługi uwierzytelniania Kerberos | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję operacji biletów usługi Kerberos | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję innych zdarzeń logowania na kontach | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zarządzania grupami aplikacji | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zarządzania kontami komputerów | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zarządzania grupami dystrybucyjnymi | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję innych zdarzeń zarządzania kontami | Krytyczny | Nie skonfigurowano | Sukces i Niepowodzenie |
| Przeprowadź inspekcję zarządzania grupami zabezpieczeń | Krytyczny | Sukces | Sukces i Niepowodzenie |
| Przeprowadź inspekcję zarządzania kontami użytkowników | Krytyczny | Sukces | Sukces i Niepowodzenie |
| Przeprowadź inspekcję działania DPAPI | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję tworzenia procesu | Krytyczny | Nie skonfigurowano | Sukces |

| | | | |
|---|---|---|---|
| Przeprowadź inspekcję zakończenia procesu | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zdarzeń RPC | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję szczegółowej replikacji usługi katalogowej | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję dostępu do usługi katalogowej | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zmian usługi katalogowej | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję replikacji usługi katalogowej | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję blokady konta | Krytyczny | Sukces | Nie skonfigurowano |
| Przeprowadź inspekcję trybu rozszerzonego protokołu IPsec | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję trybu głównego protokołu IPsec | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję trybu szybkiego protokołu IPsec | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję wylogowywania | Krytyczny | Sukces | Sukces |
| Przeprowadź inspekcję logowania | Krytyczny | Sukces | Sukces i Niepowodzenie |
| Przeprowadź inspekcję serwera zasad sieciowych | Krytyczny | Sukces i niepowodzenie | Nie skonfigurowano |
| Przeprowadź inspekcję innych zdarzeń logowania/wylogowywania | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję logowania specjalnego | Krytyczny | Sukces | Sukces |
| Przeprowadź inspekcję wygenerowanych przez aplikację | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję przemieszczania centralnych zasad dostępu | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję usług certyfikacji | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję szczegółowego udziału plików | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję udziału plików | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |

| | | | |
|---|---|---|---|
| Przeprowadź inspekcję systemu plików | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję połączenia platformy filtrowania | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję porzucania pakietów platformy filtrowania | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję manipulowania dojściem | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję obiektu jądra | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję innych zdarzeń dostępu do obiektów | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję rejestru | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję magazynu wymiennego | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję SAM | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zmiany zasad inspekcji | Krytyczny | Sukces | Sukces i Niepowodzenie |
| Przeprowadź inspekcję zmiany zasad uwierzytelniania | Krytyczny | Sukces | Sukces |
| Przeprowadź inspekcję zmiany zasad autoryzacji | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zmiany zasad platformy filtrowania | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję zmiany zasad na poziomie reguły MPSSVC | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję innych zdarzeń zmiany zasad | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję niepoufnego użycia uprawnień | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję innych zdarzeń użycia uprawnień | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Przeprowadź inspekcję poufnego użycia uprawnień | Krytyczny | Nie skonfigurowano | Sukces i Niepowodzenie |

| | | | |
|---|---|---|---|
| Przeprowadź inspekcję sterownika IPsec | Krytyczny | Nie skonfigurowano | Sukces i Niepowodzenie |
| Przeprowadź inspekcję innych zdarzeń systemowych | Krytyczny | Sukces i niepowodzenie | Nie skonfigurowano |
| Przeprowadź inspekcję zmiany stanu zabezpieczeń | Krytyczny | Sukces | Sukces i Niepowodzenie |
| Przeprowadź inspekcję rozszerzenia systemu zabezpieczeń | Krytyczny | Nie skonfigurowano | Sukces i Niepowodzenie |
| Przeprowadź inspekcję integralności systemu | Krytyczny | Sukces i niepowodzenie | Sukces i Niepowodzenie |
| System plików | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |
| Rejestr | Krytyczny | Nie skonfigurowano | Nie skonfigurowano |

## 2.12. Konfigurowanie szczegółowych zasad zbioru Przypisywanie praw użytkownika

Przypisywanie praw użytkownika jest zbiorem ustawień, który można definiować zapewniając użytkownikom delegowanie ściśle określonych czynności na systemie operacyjnym.

Zbiór Przypisywanie praw użytkownika znajduje się w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Przypisywanie praw użytkownika**

**(Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment)**

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Blokuj strony w pamięci | Istotny | - | - |
| Debuguj programy | Krytyczny | Administratorzy | Administratorzy |
| Dodaj stacje robocze do domeny | Istotny | - | - |
| Dostosuj przydziały pamięci dla procesów | Istotny | Administratorzy, Usługa lokalna, Usługa sieciowa | Administratorzy, Usługa lokalna, Usługa sieciowa |
| Działanie jako część systemu operacyjnego | Krytyczny | - | - |

| | | | |
|---|---|---|---|
| Generuj inspekcje zabezpieczeń | Krytyczny | Usługa lokalna, Usługa sieciowa | Usługa lokalna, Usługa sieciowa |
| Logowanie w trybie usługi | Krytyczny | NT Services\All services | - |
| Logowanie w trybie wsadowym | Istotny | Administratorzy, Operatorzy kopii zapasowych, Użytkownicy dzienników wydajności | - |
| Ładuj i zwalniaj sterowniki urządzeń | Istotny | Administratorzy | Administratorzy |
| Modyfikuj etykietę obiektu | Istotny | - | - |
| Modyfikuj wartości środowiskowe oprogramowania układowego | Istotny | Administratorzy | Administratorzy |
| Obejdź sprawdzanie przy przechodzeniu | Krytyczny | Administratorzy, Operatorzy kopii zapasowych, Usługa lokalna, Usługa sieciowa, Użytkownicy, Wszyscy | Administratorzy, Usługa sieciowa, Usługa lokalna, Użytkownicy |
| Odmawiaj logowania za pomocą usług pulpitu zdalnego | Opcjonalny | - | Goście |
| Odmowa dostępu do tego komputera z sieci | Krytyczny | Gość | Goście |
| Odmowa logowania lokalnego | Krytyczny | Gość | Goście |
| Odmowa logowania w trybie usługi | Krytyczny | - | - |
| Odmowa logowania w trybie wsadowym | Krytyczny | - | Goście |
| Określ konta komputerów i użytkowników jako zaufane w kwestii delegowania | Krytyczny | - | - |
| Personifikuj klienta po uwierzytelnieniu | Istotny | Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa | Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa |
| Profiluj pojedynczy proces | Istotny | Administratorzy | Administratorzy |

| | | | |
|---|---|---|---|
| Profiluj wydajność systemu | Istotny | Administratorzy, NT Service\WdiServiceHost | Administratorzy, NT Service\WdiServiceHost |
| Przejmij na własność pliki lub inne obiekty | Istotny | Administratorzy | Administratorzy |
| Przywracaj pliki i katalogi | Istotny | Administratorzy, Operatorzy kopii zapasowych | Administratorzy |
| Synchronizuj dane usługi katalogowej | Istotny | - | - |
| Usuń komputer ze stacji dokującej | Opcjonalny | Administratorzy, Użytkownicy | - |
| Utwórz łącza symboliczne | Istotny | Administratorzy | Administratorzy |
| Utwórz obiekt tokenu | Istotny | - | - |
| Utwórz obiekty globalne | Istotny | Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa | Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa |
| Utwórz plik stronicowania | Krytyczny | Administratorzy | Administratorzy |
| Utwórz trwałe obiekty udostępnione | Istotny | - | - |
| Uzyskaj dostęp do Menedżera poświadczeń jako zaufany obiekt wywołujący | Istotny | - | - |
| Uzyskiwanie dostępu do tego komputera z sieci | Krytyczny | Administratorzy, Operatorzy kopii zapasowych, Użytkownicy, Wszyscy | Administratorzy, Użytkownicy |
| Wykonuj kopie zapasowe plików i katalogów | Istotny | Administratorzy, Operatorzy kopii zapasowych | Administratorzy |
| Wykonuj zadania konserwacji woluminów | Krytyczny | Administratorzy | Administratorzy |
| Wymuszaj zamknięcie z systemu zdalnego | Krytyczny | Administratorzy | Administratorzy |
| Zamień token na poziomie procesu | Istotny | Usługa lokalna, Usługa sieciowa | Usługa lokalna, Usługa sieciowa |
| Zamknij system | Istotny | Administratorzy, Operatorzy kopii zapasowych, Użytkownicy | Administratorzy, Użytkownicy |
| Zarządzaj dziennikami inspekcji i zabezpieczeń | Krytyczny | Administratorzy | Administratorzy |

| | | | |
|---|---|---|---|
| Zezwalaj na logowanie lokalne | Krytyczny | Administratorzy, Goście, Operatorzy kopii zapasowych, Użytkownicy | Administratorzy, Użytkownicy |
| Zezwalaj na logowanie za pomocą usług pulpitu zdalnego | Istotny | Administratorzy, Użytkownicy pulpitu zdalnego | - |
| Zmień czas systemowy | Istotny | Administratorzy, Usługa lokalna | Administratorzy, Usługa lokalna |
| Zmień strefę czasową | Istotny | Administratorzy, Usługa lokalna, Użytkownicy | Administratorzy, Usługa lokalna, Użytkownicy |
| Zwiększ priorytet planowania | Istotny | Administratorzy | Administratorzy |
| Zwiększ zestaw roboczy procesu | Istotny | Użytkownicy | Administratorzy, Usługa lokalna |

## 2.13. Konfigurowanie szczegółowych zasad zbioru Opcje zabezpieczeń

Ustawienia w ramach gałęzi Opcje zabezpieczeń dostarczają szerokich możliwości konfiguracji zabezpieczeń, które są uporządkowane według grup.

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń**

**(Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)**

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Członek domeny: maksymalny wiek hasła konta komputera | Krytyczny | 30 dni | 30 dni |
| Członek domeny: podpisuj cyfrowo dane bezpiecznego kanału - gdy to możliwe | Krytyczny | Włączone | Włączone |
| Członek domeny: szyfruj cyfrowo dane bezpiecznego kanału - gdy to możliwe | Krytyczny | Włączone | Włączone |
| Członek domeny: szyfruj lub podpisuj cyfrowo dane bezpiecznego kanału - zawsze | Krytyczny | Włączone | Włączone |

| | | | |
|---|---|---|---|
| Członek domeny: wyłącz zmiany hasła konta komputera | Krytyczny | Wyłączone | Wyłączone |
| Członek domeny: wymagaj silnego klucza sesji (system Windows 2000 lub nowszy) | Krytyczny | Wyłączone | Włączone |
| DCOM: Ograniczenia dotyczące dostępu do komputera w składni języka SDDL (Security Descriptor Definition Language) | Opcjonalny | Niezdefiniowane | Niezdefiniowane |
| DCOM: Ograniczenia dotyczące uruchamiania komputera w składni języka SDDL (Security Descriptor Definition Language) | Opcjonalny | Niezdefiniowane | Niezdefiniowane |
| Dostęp sieciowy: nazwane potoki, do których można uzyskiwać dostęp anonimowo | Istotny | - | Niezdefiniowane |
| Dostęp sieciowy: nie zezwalaj na anonimowe wyliczanie kont SAM | Krytyczny | Włączone | Włączone |
| Dostęp sieciowy: nie zezwalaj na anonimowe wyliczanie kont SAM i udziałów | Krytyczny | Wyłączone | Włączone |
| Dostęp sieciowy: nie zezwalaj na przechowywanie haseł ani poświadczeń do uwierzytelniania sieciowego | Krytyczny | Wyłączone | Niezdefiniowane |
| Dostęp sieciowy: ogranicz anonimowy dostęp do nazwanych potoków i udziałów | Istotny | Włączone | Włączone |

| | | | |
|---|---|---|---|
| Dostęp sieciowy: ścieżki rejestru, do których można uzyskiwać dostęp anonimowo | Istotny | System\CurrentControlSet\Control\ProductOptions<br>System\CurrentControlSet\Control\Server Applications<br>Software\Microsoft\Windows NT\CurrentVersion | System\CurrentControlSet\Control\ProductOptions<br>System\CurrentControlSet\Control\Server Applications<br>Software\Microsoft\Windows NT\CurrentVersion |
| Dostęp sieciowy: ścieżki rejestru, do których można uzyskiwać dostęp anonimowo i ścieżki podrzędne | Istotny | System\CurrentControlSet\Control\Print\Printers<br>System\CurrentControlSet\Services\Eventlog<br>Software\Microsoft\OLAP Server<br>Software\Microsoft\Windows NT\CurrentVersion\Print<br>Software\Microsoft\Windows NT\CurrentVersion\Windows<br>System\CurrentControlSet\Control\ContentIndex<br>System\CurrentControlSet\Control\Terminal Server<br>System\CurrentControlSet\Control\Terminal Server\UserConfig<br>System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration<br>Software\Microsoft\Windows NT\CurrentVersion\Perflib<br>System\CurrentControlSet\Services\SysmonLog | System\CurrentControlSet\Control\Print\Printers<br>System\CurrentControlSet\Services\Eventlog<br>Software\Microsoft\OLAP Server<br>Software\Microsoft\Windows NT\CurrentVersion\Print<br>Software\Microsoft\Windows NT\CurrentVersion\Windows<br>System\CurrentControlSet\Control\ContentIndex<br>System\CurrentControlSet\Control\Terminal Server<br>System\CurrentControlSet\Control\Terminal Server\UserConfig<br>System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration<br>Software\Microsoft\Windows NT\CurrentVersion\Perflib<br>System\CurrentControlSet\Services\SysmonLog |
| Dostęp sieciowy: udostępnianie i model zabezpieczeń dla kont lokalnych | Krytyczny | Klasyczny – uwierzytelnianie użytkowników lokalnych, jako samych siebie | Klasyczny – uwierzytelnianie użytkowników lokalnych, jako samych siebie |

| | | | |
|---|---|---|---|
| Dostęp sieciowy: udziały, do których można uzyskiwać dostęp anonimowo | Istotny | Niezdefiniowane | Niezdefiniowane |
| Dostęp sieciowy: zezwalaj na anonimową translację identyfikatorów SID/nazw | Krytyczny | Wyłączone | Wyłączone |
| Dostęp sieciowy: zezwalaj na stosowanie uprawnień Wszyscy do anonimowych użytkowników | Krytyczny | Wyłączone | Wyłączone |
| Inspekcja: inspekcjonuj dostęp do globalnych obiektów systemu | Krytyczny | Wyłączone | Niezdefiniowane |
| Inspekcja: inspekcjonuj użycie prawa do wykonywania kopii zapasowych i przywracania | Krytyczny | Wyłączone | Niezdefiniowane |
| Inspekcja: wymuś ustawienia podkategorii zasad inspekcji (system Windows Vista lub nowszy), aby zastąpić ustawienia kategorii zasad inspekcji | Krytyczny | Niezdefiniowane | Włączone |
| Inspekcja: zamknij system natychmiast, jeśli nie można rejestrować wyników inspekcji | Krytyczny | Wyłączone | Wyłączone |
| Klient sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą serwera) | Krytyczny | Włączone | Włączone |
| Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze) | Krytyczny | Wyłączone | Włączone |

| | | | |
|---|---|---|---|
| Klient sieci Microsoft: wyślij niezaszyfrowane hasło w celu nawiązania połączenia z innymi serwerami SMB | Krytyczny | Wyłączone | Wyłączone |
| Konsola odzyskiwania: zezwalaj na automatyczne logowanie administracyjne | Krytyczny | Wyłączone | Wyłączone |
| Konsola odzyskiwania: zezwalaj na kopiowanie na dyskietkę oraz dostęp do wszystkich dysków i folderów | Istotny | Wyłączone | Wyłączone |
| Konta: blokuj konta Microsoft | Krytyczny | Niezdefiniowane | Użytkownicy nie mogą dodawać kont Microsoft ani logować się za ich pomocą |
| Konta: ogranicz używanie pustych haseł przez konta lokalne tylko do logowania do konsoli | Krytyczny | Włączone | Włączone |
| Konta: Stan konta administratora | Krytyczny | Wyłączone | Wyłączone |
| Konta: Stan konta gościa | Krytyczny | Wyłączone | Wyłączone |
| Konta: Zmienianie nazwy konta administratora | Krytyczny | Administrator | Niezdefiniowane |
| Konta: Zmienianie nazwy konta gościa | Istotny | Gość | Niezdefiniowane |
| Kontrola konta użytkownika: podnoszenie uprawnień tylko tych aplikacji z poziomem UIAccess, które są zainstalowane w bezpiecznych lokalizacjach | Krytyczny | Włączone | Włączone |

| | | | |
|---|---|---|---|
| Kontrola konta użytkownika: podnoszenie uprawnień tylko tych plików wykonywalnych, które są podpisane i mają sprawdzoną poprawność | Krytyczny | Wyłączone | Wyłączone |
| Kontrola konta użytkownika: przełącz na bezpieczny pulpit przy monitowaniu o podniesienie uprawnień | Krytyczny | Włączone | Włączone |
| Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora | Krytyczny | Wyłączone | Włączone |
| Kontrola konta użytkownika: uruchamianie wszystkich administratorów w trybie zatwierdzania przez administratora | Krytyczny | Włączone | Włączone |
| Kontrola konta użytkownika: wirtualizuj błędy zapisu plików i rejestru w lokalizacjach poszczególnych użytkowników | Krytyczny | Włączone | Włączone |
| Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie uprawnień | Krytyczny | Włączone | Włączone |
| Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora | Krytyczny | Monituj o zgodę na pliki binarne niepochodzące z systemu Windows | Monituj o zgodę na bezpiecznym pulpicie |

| | | | |
|---|---|---|---|
| Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych | Krytyczny | Monituj o poświadczenia | Automatycznie odrzucaj żądania podniesienia |
| Kontrola konta użytkownika: zezwalaj aplikacjom z poziomem UIAccess na monitowanie o podniesienie uprawnień bez używania bezpiecznego pulpitu | Krytyczny | Wyłączone | Wyłączone |
| Kryptografia systemu: użyj zgodnych algorytmów FIPS dla celów szyfrowania, tworzenia skrótu i podpisywania | Istotny | Wyłączone | Włączone |
| Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze | Istotny | Wyłączone | Niezdefiniowane |
| Logowanie interakcyjne: liczba poprzednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny) | Krytyczny | 10 logowań | 4 logowania |
| Logowanie interakcyjne: Limit nieaktywności komputera | Krytyczny | Niezdefiniowane | 900 sekund |
| Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem | Krytyczny | 14 dni | 14 dni |
| Logowanie interakcyjne: nie wymagaj naciśnięcia klawiszy CTRL+ALT+DEL | Krytyczny | Niezdefiniowane | Wyłączone |
| Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika | Krytyczny | Wyłączone | Włączone |
| Logowanie interakcyjne: próg blokady konta komputera | Krytyczny | Niezdefiniowane | 10 nieprawidłowych prób logowania |

| | | | |
|---|---|---|---|
| Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Logowanie interakcyjne: wymagaj karty inteligentnej | Istotny | Wyłączone | Niezdefiniowane |
| Logowanie interakcyjne: wymagaj uwierzytelnienia kontrolera domeny do odblokowania stacji roboczej | Krytyczny | Wyłączone | Wyłączone |
| Logowanie interakcyjne: wyświetlaj informacje o użytkowniku, gdy sesja jest zablokowana | Istotny | Niezdefiniowane | Niezdefiniowane |
| Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej | Istotny | Brak akcji | Zablokuj stację roboczą |
| Obiekty systemu: wymagaj nierozróżniania wielkości liter dla podsystemów innych niż Windows | Istotny | Włączone | Włączone |
| Obiekty systemu: wzmocnij uprawnienia domyślne wewnętrznych obiektów systemu (np. łączy symbolicznych) | Krytyczny | Włączone | Włączone |
| Serwer sieci Microsoft: okres bezczynności wymagany dla wstrzymania sesji | Krytyczny | 15 minut | 15 minut |
| Serwer sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą klienta) | Krytyczny | Wyłączone | Włączone |
| Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze) | Krytyczny | Wyłączone | Włączone |

| | | | |
|---|---|---|---|
| Serwer sieci Microsoft: poziom sprawdzania poprawności docelowej głównej nazwy usługi serwera | Krytyczny | Niezdefiniowane | Zaakceptuj, jeśli dostarczone przez klienta |
| Serwer sieci Microsoft: rozłączaj klientów po upływie limitu czasu logowania | Krytyczny | Włączone | Włączone |
| Urządzenia: ogranicz dostęp do stacji CD-ROM tylko do użytkownika zalogowanego lokalnie | Opcjonalny | Niezdefiniowane | Niezdefiniowane |
| Urządzenia: ogranicz dostęp do stacji dyskietek tylko do użytkownika zalogowanego lokalnie | Opcjonalny | Niezdefiniowane | Niezdefiniowane |
| Urządzenia: zapobiegaj instalacji sterowników drukarek przez użytkowników | Istotny | Wyłączone | Niezdefiniowane |
| Urządzenia: zezwalaj na oddokowywanie bez potrzeby logowania się | Opcjonalny | Włączone | Niezdefiniowane |
| Urządzenia: zezwolono na formatowanie i wysunięcie wymiennego nośnika | Istotny | Niezdefiniowane | Administratorzy i użytkownicy interakcyjni |
| Ustawienia systemowe: opcjonalne podsystemy | Opcjonalny | Posix | Niezdefiniowane |
| Ustawienia systemowe: użyj reguł certyfikatów do plików wykonywalnych systemu Windows dla Zasad ograniczeń oprogramowania | Istotny | Wyłączone | Niezdefiniowane |
| Zabezpieczenia sieci: minimalne zabezpieczenia sesji dla klientów opartych na NTLM SSP (włączając secure RPC) | Krytyczny | Wymagaj szyfrowania 128-bitowego | Wymaga zabezpieczeń sesji NTLMv2, Wymagaj szyfrowania 128-bitowego |
| Zabezpieczenia sieci: minimalne zabezpieczenia sesji dla serwerów opartych na NTLM SSP (włączając secure RPC) | Krytyczny | Wymagaj szyfrowania 128-bitowego | Wymaga zabezpieczeń sesji NTLMv2, Wymagaj szyfrowania 128-bitowego |

| | | | |
|---|---|---|---|
| Zabezpieczenia sieci: nie przechowuj wartości skrótu (hash) programu LAN Manager dla następnej zmiany hasła | Krytyczny | Włączone | Włączone |
| Zabezpieczenia sieci: poziom uwierzytelniania LAN Manager | Krytyczny | Wyślij tylko odpowiedź NTLMv2 | Wyślij tylko odpowiedź NTLMv2. Odmów LM i NTLM. |
| Zabezpieczenia sieci: wymagania podpisywania klienta LDAP | Krytyczny | Negocjuj podpisywanie | Negocjuj podpisywanie |
| Zabezpieczenia sieciowe: konfigurowanie typów szyfrowania dozwolonych dla protokołu Kerberos | Istotny | Niezdefiniowane | RC4/AES128/AES256/przyszłe typy szyfrowania |
| Zabezpieczenia sieciowe: Ograniczania ruchu NTLM: Dodaj wyjątki dla serwerów z tej domeny | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Dodaj wyjątki dla serwerów zdalnych w celu uwierzytelniania NTLM | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję przychodzącego ruchu NTLM | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję uwierzytelniania NTLM w tej domenie | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przychodzący ruch NTLM | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Uwierzytelnianie NTLM w tej domenie | Krytyczny | Niezdefiniowane | Niezdefiniowane |

| | | | |
|---|---|---|---|
| Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Wychodzący ruch NTLM do serwerów zdalnych | Krytyczny | Niezdefiniowane | Niezdefiniowane |
| Zabezpieczenia sieciowe: Wymuś wylogowanie użytkowników po upłynięciu czasu logowania | Istotny | Wyłączone | Niezdefiniowane |
| Zabezpieczenia sieciowe: Zezwalaj kontu systemowi lokalnemu na używanie pustych sesji | Istotny | Niezdefiniowane | Wyłączone |
| Zabezpieczenia sieciowe: Zezwalaj lokalnemu systemowi na uwierzytelnianie NTLM przy użyciu tożsamości komputera | Istotny | Niezdefiniowane | Włączone |
| Zabezpieczenia sieciowe: Zezwalaj na wysyłanie żądań uwierzytelniania PKU2U do tego komputera w celu używania tożsamości online | Istotny | Niezdefiniowane | Wyłączone |
| Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej | Krytyczny | Wyłączone | Wyłączone |
| Zamknięcie: zezwalaj na zamykanie systemu bez konieczności zalogowania | Istotny | Włączone | Włączone |

## 2.14. Konfigurowanie ustawień MSS

Wśród wielu ustawień zabezpieczeń istnieją takie, które nie mają reprezentacji w postaci zasad GPO. Można je za to definiować poprzez bezpośrednie wpisy w rejestrze. Ustawienia tego typu posiadają prefiks MSS (z ang. Microsoft Solutions for Security).

Ważnym aspektem zarządzania ustawieniami MSS jest, że nie są usuwane wraz z usuwaniem szablonów zabezpieczeń. To wymusza ich ręczną konfigurację z poziomu rejestru systemu (regedit32.exe).

## 2.15. Potencjalne zagrożenia związane z zasadami podpisywania cyfrowego pakietów SMB

Protokół SMB (z ang. Server Message Block) znany również, jako CIFS (z ang. Common Internet File System) zapewnia metody udostępniania zasobów komputerowych takich jak pliki, drukarki czy porty szeregowe.

W sytuacji nawiązywania przez klienta wykorzystującego SMB w wersji 1 połączenia w sesji konta innego niż konto Gość lub logowania nie anonimowego, kiedy zasady podpisywania SMB są włączone klient włącza podpisywanie cyfrowe komunikacji dla serwera, a kolejne nawiązane sesje będą dziedziczyły i stosowały podpisaną cyfrowo komunikację SMB. W Windows 8 w celu zwiększenia zasad bezpieczeństwa połączenia uwierzytelnione przez serwer są chronione przed degradacją do poziomu sesji Gość lub Anonimowe.

Powyższa zasada nie dotyczy scenariusza, w którym kontrolery domeny pracują pod kontrolą Windows Server 2003 a stacjami klienckimi są Windows Vista SP2 lub Windows Server 2008.

Mając to na uwadze, aby zachować jednolite zachowanie zasad podpisywania pakietów SMB należy skonfigurować poniższe ustawienia znajdujące się w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń**

**(Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)**

- W zakresie kontrolera domeny pracującego pod kontrolą Windows Server 2003:

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Serwer sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą klienta) | Krytyczny | Włączony | Włączony |
| Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze) | Krytyczny | Włączony | Włączony |

- W zakresie komputerów będących członkami domeny pracującymi pod kontrolą Windows Vista SP1 lub Windows Server 2008

| Zasada | Poziom ważności | Ustawienie domyślne | Ustawienie zalecane przez Microsoft |
|---|---|---|---|
| Serwer sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą klienta) | Krytyczny | Wyłączone | Włączony |
| Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze) | Krytyczny | Wyłączone | Włączony |

Omawiane problemy zostały rozwiązane w Windows Server 2008 SP2 oraz Windows Vista SP2.

## 2.16. Ograniczenie stosowania mechanizmu uwierzytelnienia NTLM

Uwierzytelnianie NT LAN Manager (NTLM) jest wszechobecne w wielu sieciach komputerowych nawet, jeśli dostępne są bardziej bezpieczne protokoły uwierzytelniania Windows. W Windows 8 pojawiły się nowe zasady zabezpieczeń pozwalające na analizę i ograniczanie wykorzystania NTLM w środowisku IT. Funkcje te obejmują zbieranie danych, analizę ruchu NTLM oraz proces metodyczny, który wprowadza ograniczenia w ruchu NTLM na rzecz silniejszych protokołów uwierzytelniania takich jak Kerberos. Ograniczenie użycia protokołu NTLM wymaga wiedzy na temat wykorzystania go przez aplikację oraz strategii i kroków potrzebnych do konfiguracji infrastruktury do pracy z innymi protokołami.

Zasady umożliwiające audyt oraz ograniczenie wykorzystania ruchu NTLM znajdują się w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń**

**(Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)**

i obejmują:

- w zakresie audytu:
    - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję przychodzącego ruchu NTLM
    - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję uwierzytelniania NTLM w tej domenie
- w zakresie ograniczania
    - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przychodzący ruch NTLM
    - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Uwierzytelnianie NTLM w tej domenie
    - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Wychodzący ruch NTLM do serwerów zdalnych

## 2.17. Konfigurowanie szczegółowych zasad zbioru Dziennik zdarzeń

Rejestrowanie zdarzeń należy do najważniejszych zadań realizowanych w obszarze bezpieczeństwa Windows, które można przeglądać z poziomu Dziennika zdarzeń. Istotnym aspektem konfiguracji są atrybuty dzienników związane z ich rozmiarem, prawami dostępu oraz metodą nadpisywania zdarzeń.

Zasady umożliwiające konfigurację wymienionych atrybutów znajdują się gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Dziennik zdarzeń**

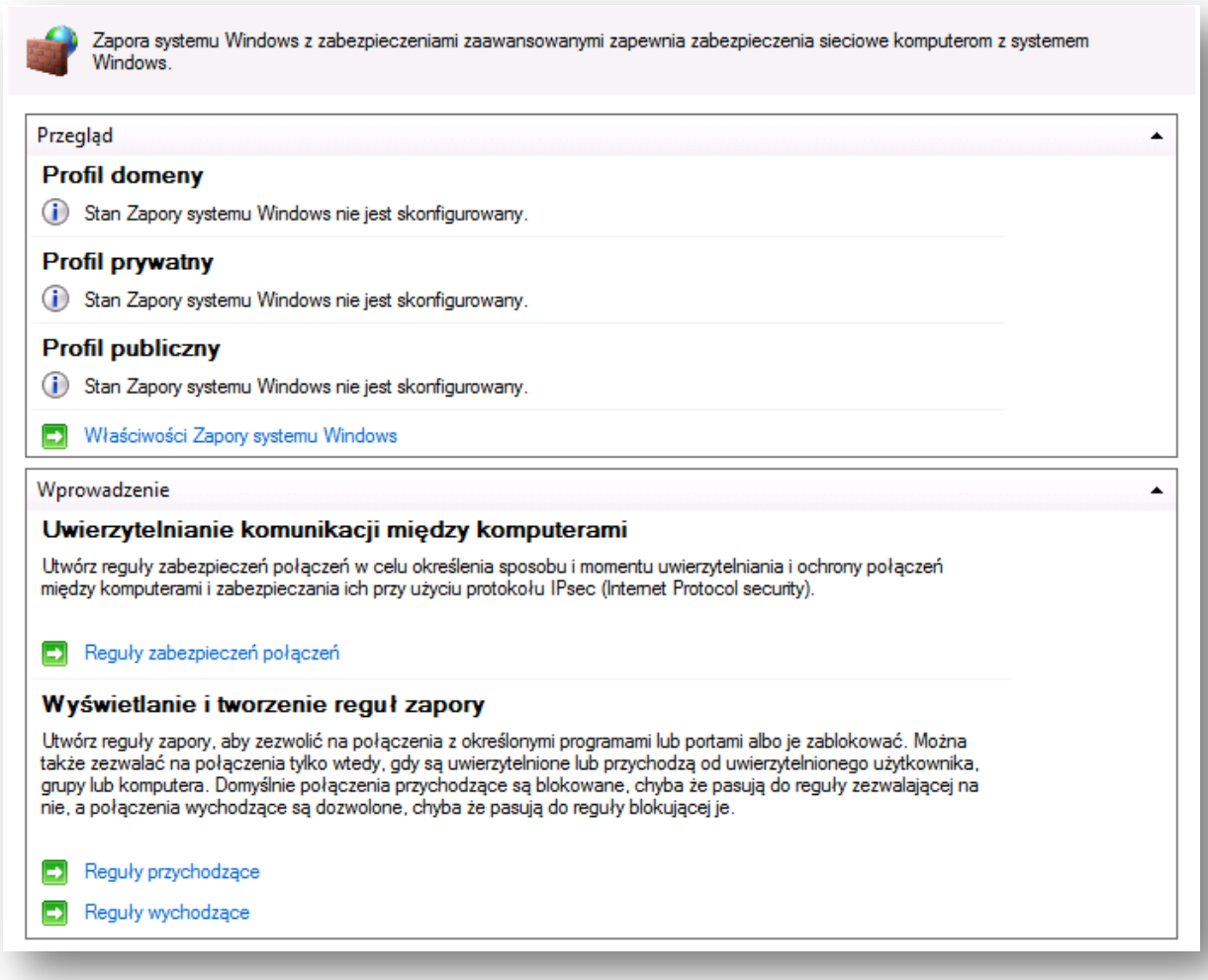
**(Computer Configuration\Windows Settings\Security Settings\Event Log)**

- Maksymalny rozmiar dziennika aplikacji
- Maksymalny rozmiar dziennika systemu
- Maksymalny rozmiar dziennika zabezpieczeń
- Metoda przechowywania dziennika aplikacji
- Metoda przechowywania dziennika systemu
- Metoda przechowywania dziennika zabezpieczeń
- Odmawiaj dostępu lokalnej grupie gości do dziennika aplikacji
- Odmawiaj dostępu lokalnej grupie gości do dziennika systemu
- Odmawiaj dostępu lokalnej grupie gości do dziennika zabezpieczeń
- Przechowuj dziennik aplikacji przez
- Przechowuj dziennik systemu przez
- Przechowuj dziennik zabezpieczeń przez

## 2.18. Szczegółowa konfiguracja zapory systemu Windows Firewall with Advanced Security

Precyzyjna konfiguracja narzędzia Zapora systemu Windows z zabezpieczeniami zaawansowanymi jest możliwa z poziomu zasad grupowych w ramach gałęzi
**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi**

**(Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security)**




Rys. 2.18.1 Ustawienia zasad grupowych dla Zapory systemu Windows z ustawieniami zaawansowanymi.

W ramach dostępnych ustawień można dokonywać zmian w zakresie:

- Ustawień ogólnych zapory dostępnych we właściwościach narzędzia Zapora systemu Windows z zabezpieczeniami zaawansowanymi
- Wyświetlanie i tworzenie reguł wchodzących i wychodzących zapory
- Wyświetlanie i tworzenie reguł w zakresie uwierzytelniania komunikacji między komputerami

Przystępując do konfiguracji ustawień należy sprecyzować profil sieciowy, dla którego będą definiowane ustawienia.

W ramach narzędzia Zapora systemu Windows z zabezpieczeniami zaawansowanymi dostępne są poniżej opisane profile sieciowe.

**Profil domenowy**

Profil stosowany jest, kiedy komputer został podłączony do sieci oraz nastąpiło uwierzytelnienie do kontrolera domeny, do którego należy komputer. Domyślna konfiguracja profilu umożliwia nawiązywanie sesji Pulpitu zdalnego oraz Pomocy zdalnej.

**Profil prywatny**
Profil stosowany jest, jeśli użytkownik posiadających poświadczenia lokalnego administratora przypisze go w ramach bieżącego połączenia sieciowego. Zaleca się, aby używać profilu prywatnego w sieciach zaufanych.

**Profil publiczny**
Jest to domyślny profil i stosowany jest w scenariuszach, kiedy komputer nie jest dołączony do domeny. Stanowi on zbiór najbardziej restrykcyjnych ustawień, w których wyłączona jest komunikacja wchodząca.

## 2.19. Usługa Windows Update

Usługa Windows Update umożliwia systematyczne sprawdzanie komputera pod kątem wymaganych aktualizacji. Wszystkie poprawki domyślnie dystrybuowane są poprzez witrynę Windows Update. Alternatywnie można utworzyć infrastrukturę, która będzie umożliwiała lokalną dystrybucję poprawek z centralną synchronizacją do witryny Windows Update. Realizuje się to za pomocą serwera WSUS (z ang. Windows Server Update Services)[13]. Zastosowanie serwera WSUS zapewnia:

- Administracyjną kontrolę nad synchronizacją poprawek z witryny Windows Update, które będą dystrybuowane lokalnie,
- Lokalny serwer Windows Update,
- Administracyjną kontrolę nad poprawkami,
- Automatyczną aktualizację komputerów (stacji roboczych i/lub serwerów).

Konfiguracja klientów serwera WSUS realizowana jest poprzez ustawienia zasad grupowych dostępne w gałęzi:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Update**

**(Computer Configuration\Administrative Templates\Windows Components\Windows Update)**

- Nie wyświetlaj opcji „Zainstaluj aktualizacje i zamknij system” w oknie dialogowym Zamykanie systemu Windows
- Nie ustawiaj opcji domyślnej na „Zainstaluj aktualizacje i zamknij system” w oknie dialogowym Zamykanie systemu Windows Nie skonfigurowano
- Włączanie Opcji zasilania, aby funkcja Windows Update automatycznie wznawiała system w celu zainstalowania zaplanowanych aktualizacji
- Konfigurowanie aktualizacji automatycznych
- Określ lokalizację intranetowej usługi aktualizującej firmy Microsoft
- Częstotliwość wykrywania aktualizacji automatycznych
- Zezwalaj, aby użytkownicy inni niż administratorzy otrzymywali powiadomienia aktualizacji
- Włącz powiadomienia o oprogramowaniu
- Zezwalaj na natychmiastową instalację aktualizacji automatycznych
- Włącz zalecane aktualizacje za pomocą aktualizacji automatycznych

[13] http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

- Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych przy zalogowanych użytkownikach
- Ponów monit o ponowne uruchomienie komputera z zaplanowanymi instalacjami
- Opóźniaj ponowne uruchomienie komputera dla zaplanowanych instalacji
- Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznych
- Włącz konfigurowanie docelowej strony klienta
- Zezwalaj na podpisane aktualizacje z intranetowej lokalizacji usługi aktualizacji firmy Microsoft

Do prawidłowego działania klienta z serwerem WSUS należy skonfigurować minimum cztery zasady:

- Określ lokalizację intranetowej usługi aktualizującej firmy Microsoft
- Konfigurowanie aktualizacji automatycznych
- Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych przy zalogowanych użytkownikach
- Zaplanuj ponownie zaplanowane instalacji aktualizacji automatycznych

## 2.20. Ataki na usługę zintegrowanego uwierzytelniania systemu Windows polegające na przekazywaniu poświadczeń

Poradniki Bezpieczeństwa Microsoft MSA (z ang. Microsoft Security Advisory) zawierają informację na temat ryzyka ataków związanych z przechwyceniem poświadczeń użytkownika wykorzystującego usługę zintegrowanego uwierzytelniania systemu Windows IWA (z ang. Integrated Windows Authentication). Tego typu naruszenia bezpieczeństwa mogą wystąpić poprzez ataki typu człowiek pośrodku (ang. man-in-the-middle) lub poprzez sprowokowanie uruchomienia przez użytkownika konkretnego odnośnika.

Poniżej przedstawione zostały dwa przykłady tego typu ataków:

- Przekazanie poświadczeń
  W tym scenariuszu atak następuje, kiedy przechwycone poświadczenia są wykorzystywane do logowania się do innych usług niż ofiara miała dostęp.
- Odbicie poświadczeń
  Tego typu atak zakłada wykorzystanie przechwyconych poświadczeń do ponownego logowania się na komputerze ofiary.

W celu zmniejszenia ryzyka tego typu ataków udostępniona została funkcja EPA (z ang. Extended Protection for Authentication) zawarta w Windows 8 oraz w Windows Server 2012. Dla poprzednich wersji Windows EPA jest dostępna, często jako aktualizacja.

Szczegółowe informacje o konfiguracji EPA dla wcześniejszych wersji Windows znajdują się w KB968389 (http://support.microsoft.com/kb/976918).

W założeniach zintegrowanego uwierzytelniania Windows przyjęto, że niektóre odpowiedzi uwierzytelniania są uniwersalne, co umożliwia ich łatwe powtórne użycie lub przekazanie. Stąd zaleca się, jako minimum konstrukcję, w której konstrukcja odpowiedzi w komunikacji zawiera określne informacje o kanale komunikacji. Dzięki temu usługi mają zapewnioną rozszerzoną ochronę w

zakresie odpowiedzi uwierzytelniania zawierających określone informacje dotyczące usług, takie jak SPN (z ang. Service Principal Name).

# 3. Sposoby ochrony przed złośliwym oprogramowaniem

Oprogramowaniem złośliwym, malware (ang. **mal**icious soft**ware**) określany jest każdy program komputerowy lub skrypt, mający szkodliwe lub złośliwe działanie w stosunku do użytkownika komputera. Przykładami oprogramowania złośliwego są: wirusy, robaki, konie trojańskie, rootkit'y oraz oprogramowanie szpiegujące( ang. Spyware), które gromadzą informacje na temat działalności użytkownika bez uprzedniej zgody użytkownika systemu.

Windows 8 został zbudowany w oparciu o technologie wprowadzone w systemach Windows Vista i Windows 7. Technologie te zawierają kilka nowych rozwiązań, które mogą zostać wykorzystane w celu zapewnienia ochrony przed oprogramowaniem złośliwym dla komputerów pracujących pod kontrolą systemu Windows 8.

W systemie Windows 8 dostępna jest nowa wersja przeglądarki internetowej Windows Internet Explorer 10, zawierająca kilka znaczących i ulepszonych funkcji pod kątem bezpieczeństwa, które pomagają zapobiec instalacji niechcianego oprogramowania. Funkcje te również zwiększają bezpieczeństwo przeglądarki i zapewniają ochronę prywatności danych zapobiegając nieautoryzowanym transmisjom prywatnych danych. W systemie Windows 8 użytkownik posiada możliwość kompletnego usunięcia przeglądarki Internet Explorer 10, jeśli tylko taka sytuacja jest wymagana. Narzędzie Microsoft Security Compliance Manager (SCM) zawiera rekomendowane ustawienia bazowe dedykowane przeglądarce Internet Explorer 10 ułatwiające implementację bezpiecznej konfiguracji przeglądarki internetowej.

Implementacje rekomendowanych ustawień nowych funkcji zabezpieczeń wprowadzonych w systemie Windows 8 może zostać wdrożona poprzez zastosowanie zasad grupowych, opisanych w rozdziale „Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 8".

Jednakże należy zauważyć, iż wiele z tych ustawień dla nowych funkcji zabezpieczeń wymaga informacji charakterystycznych dla danego środowiska systemu komputerowego, mającego wpływ na wybór funkcji i ustawień. Z tego powodu, większość rekomendowanych wartości dla dodatkowych ustawień nie zostało zawarte w niniejszym przewodniku.

Wszystkie opisane funkcje z ustawionymi wartościami domyślnymi zapewniają dodatkowy poziom ochrony komputerów pracujących pod kontrolą systemów Windows 8. Dostępne są jednak nowe ustawienia zasad grupowych, które poprzez dostosowanie zachowania i funkcjonalności tych technologii, mogą zapewnić jeszcze lepszą ochronę przed złośliwym oprogramowaniem dla własnego środowiska.

## 3.1. Funkcje zabezpieczeń stosowane w systemie Windows 8

System Windows 8 zawiera następujące nowe i rozszerzone technologie, które zapewniają ochronę przed złośliwym oprogramowaniem:

- Konsola Centrum Akcji (ang. Action Center)
- Bezpieczny rozruch (ang. Secure Boot)
- Kontrola Konta Użytkownika (ang. User Account Control – UAC)

- Zabezpieczenia biometryczne (ang. Biometric Security)
- Windows Defender
- Narzędzie do usuwania złośliwego oprogramowania (ang. Malicious Software Removal Tool)
- Zapora systemu Windows
- AppLocker

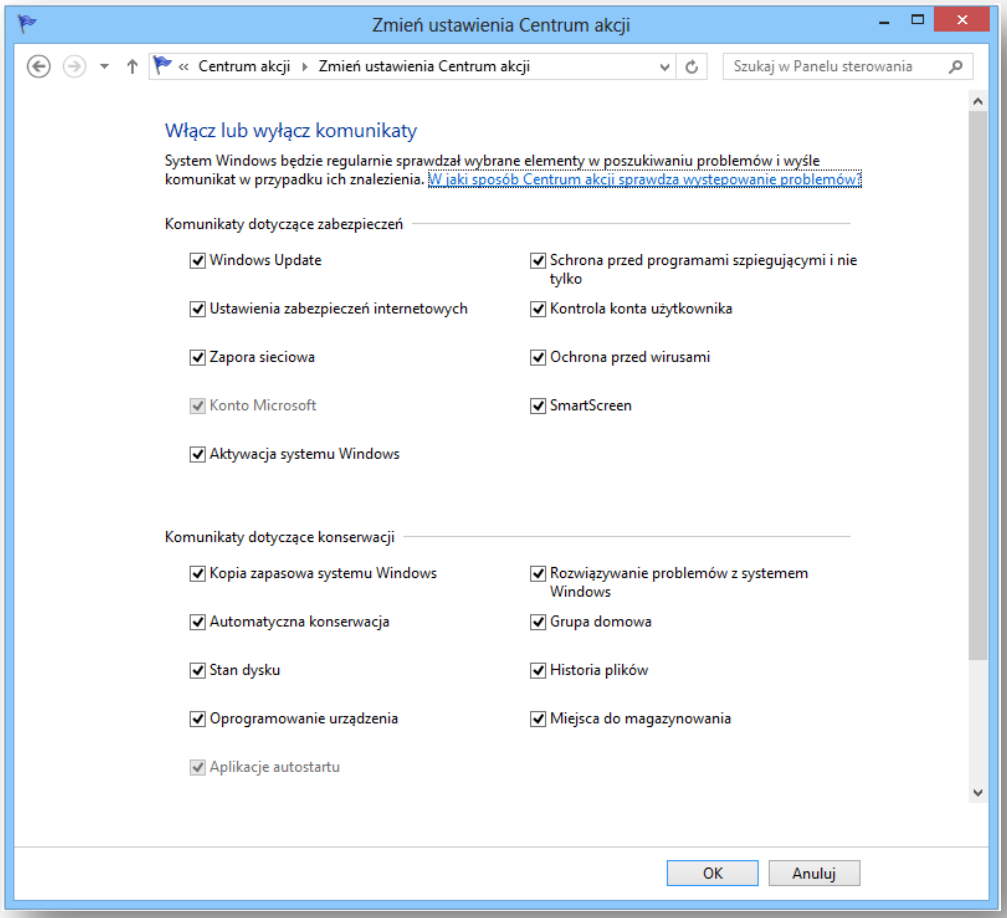
Ponadto, należy pamiętać, iż rekomendowaną praktyką zwiększającą bezpieczeństwo jest logowanie do systemu z wykorzystaniem konta zwykłego użytkownika (nieposiadającego uprawnień administracyjnych). Dodatkowo wysoce rekomendowane jest zainstalowanie programu antywirusowego, który zapewnia ochronę w czasie rzeczywistym przed nowymi zagrożeniami, które pojawiają się każdego dnia, przykładem takiego rozwiązania jest System Center 2012 Endpoint Protection [14]. Jeśli dana organizacja stosuje strategię defense-in-depth zaleca się określenie dodatkowych usług przeszukujących zasoby pod katem zagrożeń, Usługi te mogą być pobrane ze stron firmy Microsoft stanowiąc składnik systemu Windows 8 lub dodatkowy składnik pobrany, jako program lub usługa.

Należy podkreślić, iż nawet zastosowanie wszystkich możliwych technologii zabezpieczeń nie uchroni użytkowników komputerów przed narażeniem na niebezpieczeństwo, jeśli nie zabezpieczymy i nie będziemy kontrolowali w odpowiedni sposób dostępu do kont, które posiadają uprawnienia na poziomie administracyjnym do zabezpieczanych komputerów.

## 3.2. Konsola Centrum Akcji

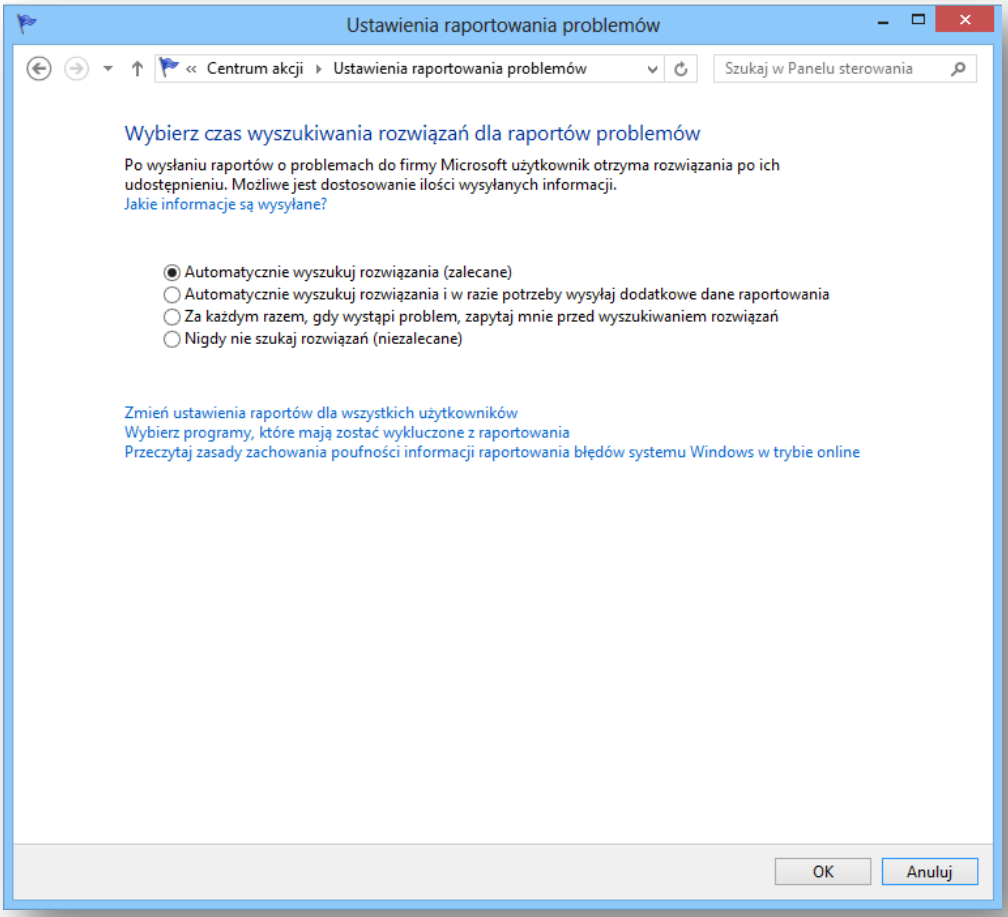
Centrum akcji to centralne miejsce, gdzie użytkownik może wyświetlać alerty i podejmować działania mające na celu zapewnienie sprawnego funkcjonowania systemu Windows. W Centrum Akcji wyświetlana jest lista ważnych komunikatów dotyczących ustawień zabezpieczeń oraz konserwacji, które wymagają uwagi użytkownika. Zakres wyświetlanych komunikatów, które mogą być wyłączone lub włączone został przedstawiony w ustawieniach konsoli **Zmień ustawienia Centrum Akcji** na rysunku 3.2.1

[14] http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx




Rys. 3.2.1 – Widok okna **Zmień ustawienia Centrum Akcji**

Konsola Centrum Akcji poza raportowaniem i powiadamianiem użytkowników systemu Windows 8 o występujących problemach, pozwala na kontrolowanie, jakie informacje są wysyłane do firmy Microsoft w celu wykrycia i rozwiązania problemów. Ustawienia raportowania problemów zostały przedstawione na rysunku 3.2.2.




Rys. 3.2.2 – Widok okna **Ustawienia raportowania problemów**

Każdy użytkownik może przejrzeć informacje dotyczące raportów problemów wysyłane do firmy Microsoft stosując następujące kroki:

1. Proszę otworzyć główne okno **Centrum Akcji**
2. Proszę kliknąć na opcję **Konserwacja**
3. Poniżej **Wyszukaj rozwiązania dotyczące raportów o problemach,** proszę kliknąć **Wyświetl historię niezawodności**
4. Na liście historii niezawodności, proszę kilknąć dwukrotnie na dowolnym zdarzeniu aby wyświetlić techniczne szczegóły dotyczące zdarzenia.
5. Zdarzenia wyświetlone w sekcji **Informacje** zwykle zawierają szczegóły zmian dokonanych w konfiguracji sprzętu lub oprogramowania.

W celu uzyskania dodatkowych informacji na temat raportowania problemów i zasada zachowania poufności informacji, należy odwiedzić witrynę Microsoft Usługa raportowania błędów firmy Microsoft — zasady zachowania poufności informacji[15]

**Zastosowanie ustawień zasad grup w celu minimalizacji ryzyka dla Centrum Akcji**

[15] http://oca.microsoft.com/pl/dcp20.asp

Konfiguracja tych ustawień dostępna jest dwóch lokalizacjach w gałęziach:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Raportowanie błędów systemu Windows**

**(Computer Configuration\Windows Components\Windows Error Reporting)**

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 8 dla omawianej technologii

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Wyłącz funkcję Raportowanie błędów systemu Windows | Jeżeli to ustawienie zostanie włączone, funkcja Raportowanie błędów systemu Windows nie będzie wysyłać do firmy Microsoft żadnych informacji o problemach. Ponadto w aplecie Centrum Akcji w Panelu sterowania nie będą dostępne informacje dotyczące rozwiązania. | Nie skonfigurowano |

Tabela 3.2.1 Ustawienia Centrum Akcji w systemie Windows

**Konfiguracja użytkownika\Szablony administracyjne\Menu Start i pasek zadań**

**(User Configuration\Start Menu and Taskbar\)**

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 8 dla omawianej technologii

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Usuń ikonę Centrum akcji | Zapobiega wyświetlaniu ikony Centrum akcji w obszarze kontroli systemu. Jeżeli to ustawienie zostanie włączone, ikona Centrum Akcji nie będzie wyświetlana w obszarze powiadomień systemu.<br><br>Jeżeli to ustawienie zostanie wyłączone lub nie zostanie skonfigurowane, ikona Centrum Akcji będzie wyświetlana w obszarze powiadomień systemu. | Nie skonfigurowano |

Tabela 3.2.2 Ustawienia Centrum Akcji w systemie Windows

## 3.3. Bezpieczny rozruch (Secure Boot)

System Windows 8 oferuje wsparcie dla protokołu bezpiecznego rozruchu (ang. secure boot protocol), który jest częścią specyfikacji Unified Extensible Firmware Interface (UEFI), która została

zaprojektowana, jako następca starszego systemu BIOS. System Windows 8 nadal wspiera starszy system BIOS, ale UEFI rozszerza możliwości systemu układowego (ang. firmware) włączając w to wsparcie dla większych dysków (możliwości rozruchu dysków większych niż 2 TB korzystających z GPT – GUID Partition Table), ulepszone mechanizmy bezpieczeństwa, grafiki oraz zwiększone możliwości zarządzania.

**Ocena ryzyka**

W nowoczesnych komputerach pracujących w oparciu o starszy system BIOS, środowisko rozruchu systemu operacyjnego może być narażone na podatności związane z atakiem przekierowania modułu ładującego rozruchu (ang. boot loader) systemu operacyjnego w taki sposób, aby kod złośliwy wykonał się przed właściwym startem systemu operacyjnego, umożliwiając wykonanie zaplanowanego ataku. W tym wypadku wektor ataku oznacza, iż złośliwy kod zostanie wykonany przed uruchomieniem systemu operacyjnego i stosowanego systemu zabezpieczeń, takich jak ochrona przed złośliwym oprogramowaniem, uniemożliwiając programom zapewniającym ochronę na ich wykrycie, usunięcie lub zablokowanie. Takie oprogramowanie złośliwe odnosi się czasem do oprogramowania określanego, jako ang. rootkit lub ang. bootkit i stanowi duże ryzyko dla użytkowników, którzy często czują się bezpieczni korzystając z oprogramowania do ochrony przez oprogramowaniem złośliwym, które w tym wypadku nie wykryje zagrożenia oraz nie ujawni podejrzanych plików, które powinny zostać usunięte z systemu.

**Minimalizacja ryzyka**

Standard UEFI wprowadził protokół bezpiecznego rozruchu (ang. secure boot protocol), który jest wspierany przez system Windows 8. Stosując bezpieczny rozruch system UEFI sprawdza podczas startu podpisany cyfrowo kod systemu układowego (ang. firmware), peryferia podłączone do komputera oraz moduł ładujący rozruch (ang. boot loader) w celu upewnienia się, iż dany kod może zostać wykonany jest podpisany cyfrowo. Bezpieczny rozruch jest włączony domyślne na komputerach pracujących w oparciu o system Windows 8, na których jest dostępny i skonfigurowany system jest UEFI.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Bezpieczny rozruch wymaga systemu układowego (ang. firmware), który zgodny jest ze specyfikacją UEFI w wersji, co najmniej 2.3.1 oraz wymaga skonfigurowania i włączenia bezpiecznego rozruchu w odpowiednich opcjach dla systemu układowego UEFI.

## 3.4. Mechanizm Kontrola Konta Użytkownika (User Account Control – UAC)

System Windows Vista wprowadził mechanizm kontroli konta użytkownika (ang. User Account Control – UAC) w celu ułatwienia wykorzystania konta użytkownika, który nie posiada uprawnień administracyjnych. Gdy na komputerze mają zostać dokonane zmiany wymagające uprawnień na poziomie administratora, funkcja Kontrola Konta Użytkownika powiadamia o tym. Mechanizm UAC składa się z kilku technologii:

- Konto Protected Administrator (PA)
- Podnoszenie uprawnień (ang. UAC elevation prompts)

- Wirtualizacja rejestru (ang. registry virtualization)
- Wirtualizacja systemu plików (ang. file system virtualization)
- Poziomy integralności Windows (ang. Windows Integrity levels)

Pomimo iż stosowanie konta skonfigurowanego w trybie Protected Administrator (PA) jest nieco bezpieczniejsze od trybu konta administratora niechronionego tym mechanizmem, to nadal wykorzystanie konta standardowego użytkownika do codziennej pracy jest zalecanym i najbardziej bezpiecznym rozwiązaniem. Ryzyko związane z oprogramowaniem złośliwym, które wykorzystując wysokie uprawnienia użytkownika potrafi zainstalować niechciane aplikacje lub dokonać nieautoryzowanych zmian w systemie Windows można zminimalizować poprzez zastosowanie konta zwykłego użytkownika do wykonywania codziennych czynności na komputerze.

W systemie Windows 8 można ustawić odpowiedni tryb i częstotliwość powiadamiania użytkownika. Poniżej przedstawiono cztery podstawowe poziomy powiadomień, które można odpowiednio skonfigurować w ustawieniach UAC w Centrum Akcji.

| Ustawienie | Opis | Wpływ na bezpieczeństwo |
|---|---|---|
| Powiadamiaj zawsze | Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze lub w systemie Windows wymagających uprawnień administratora.<br><br>Gdy zostanie wyświetlone powiadomienie, pulpit zostanie przyciemniony, a użytkownik będzie musieć zaakceptować lub odrzucić żądanie w oknie dialogowym funkcji Kontrola konta użytkownika, zanim będzie można zrobić na komputerze cokolwiek innego. Przyciemnienie pulpitu jest nazywane bezpiecznym pulpitem, ponieważ inne programy nie mogą działać, gdy pulpit jest przyciemniony. | Jest to najbezpieczniejsze ustawienie.<br><br>Po wyświetleniu powiadomienia użytkownik powinien starannie przeczytać zawartość każdego z okien dialogowych, nim zezwoli na wprowadzenie zmian na komputerze. |
| Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze – | Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze wymagających uprawnień administratora.<br><br>Użytkownik nie będzie powiadamiany, gdy sam będzie wprowadzać zmiany w ustawieniach systemu Windows wymagające uprawnień administratora.<br><br>Użytkownik będzie powiadamiany, gdy program spoza systemu Windows będzie próbował wprowadzić zmiany w ustawieniach systemu Windows. | Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze wymagających uprawnień administratora.<br><br>Użytkownik nie będzie powiadamiany, gdy sam będzie wprowadzać zmiany w ustawieniach systemu Windows wymagające uprawnień administratora.<br><br>Użytkownik będzie powiadamiany, gdy program spoza systemu Windows będzie próbował wprowadzić zmiany w ustawieniach systemu Windows.<br>**Ustawienie domyślne w systemie** |

| | | **Windows 8** |
|---|---|---|
| Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze (nie przyciemniaj pulpitu) | Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze wymagających uprawnień administratora.<br><br>Użytkownik nie będzie powiadamiany, gdy sam będzie wprowadzać zmiany w ustawieniach systemu Windows wymagające uprawnień administratora.<br><br>Użytkownik będzie powiadamiany, gdy program spoza systemu Windows będzie próbował wprowadzić zmiany w ustawieniach systemu Windows. | To ustawienie jest identyczne jak „Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze”, ale powiadomienia nie są wyświetlane na bezpiecznym pulpicie.<br><br>Ponieważ przy tym ustawieniu okno dialogowe funkcji Kontrola konta użytkownika nie znajduje się na bezpiecznym pulpicie, inne programy mogą wpływać na wygląd tego okna. Jest to małe zagrożenie dla bezpieczeństwa, jeśli złośliwy program już działa w komputerze. |
| Nie powiadamiaj nigdy | Użytkownik nie będzie powiadamiany przed wprowadzeniem jakichkolwiek zmian na komputerze. Jeśli użytkownik jest zalogowany jako administrator, programy mogą bez jego wiedzy wprowadzać zmiany na komputerze.<br><br>Jeśli użytkownik jest zalogowany jako użytkownik standardowy, wszelkie zmiany wymagające uprawnień administratora zostaną automatycznie odrzucone.<br><br>W przypadku wybrania tego ustawienia będzie konieczne ponowne uruchomienie komputera w celu ukończenia procesu wyłączania funkcji Kontrola konta użytkownika. Po wyłączeniu funkcji Kontrola konta użytkownika użytkownicy logujący się jako administrator zawsze będą mieć uprawnienia administratora. | Użytkownik nie będzie powiadamiany przed wprowadzeniem jakichkolwiek zmian na komputerze. Jeśli użytkownik jest zalogowany jako administrator, programy mogą bez jego wiedzy wprowadzać zmiany na komputerze.<br><br>Jeśli użytkownik jest zalogowany jako użytkownik standardowy, wszelkie zmiany wymagające uprawnień administratora zostaną automatycznie odrzucone.<br><br>W przypadku wybrania tego ustawienia będzie konieczne ponowne uruchomienie komputera w celu ukończenia procesu wyłączania funkcji Kontrola konta użytkownika. Po wyłączeniu funkcji Kontrola konta użytkownika użytkownicy logujący się jako administrator zawsze będą mieć uprawnienia administratora. **Ustawienie niezalecane.** |

Tabela. 3.3.1 - Opis ustawień funkcji Kontrola konta użytkownika

W momencie wprowadzenia technologii UAC, zbyt częste powiadomienia użytkownika systemu, powodowało, że większość użytkowników wyłączyło to ustawienie, zmniejszając w ten sposób poziom bezpieczeństwa komputera. W systemach Windows 7 SP1 oraz Windows 8, liczba pytań o podniesienie poświadczeń została obniżona, tak, aby użytkownik mógł wykonywać więcej zadań, jako standardowy użytkownik. Dodatkowo podczas wykorzystania konta PA niektóre programy zawarte w

systemie Windows 8, mogą automatycznie podnosić poziom uprawnień bez wyświetlenia powiadomienia.

Rekomendowanym minimalnym ustawieniem UAC jest domyślny poziom **Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze,** ale należy rozważyć ustawienie poziomu **Powiadamiaj zawsze** w środowiskach gdzie użytkownicy komputerów klienckich często podłączają się i korzystają z sieci publicznych lub kiedy wymagany jest wysoki poziom bezpieczeństwa. Zastosowanie pozostałych mniej bezpiecznych poziomów zwiększa prawdopodobieństwo dokonania nieautoryzowanych zmian w komputerze przez oprogramowanie złośliwe.

Funkcja zatwierdzania przez administratora (ang. Administrator Approval Mode) w technologii UAC zapewnia ograniczoną ochronę dla komputerów z systemem Windows 8, Windows 7 SP1 oraz Windows Vista Service Pack 1 (SP1) przed niektórymi typami oprogramowania złośliwego. Większość programów i czynności wykonywanych w systemie Windows 8 będzie poprawnie działało dla użytkownika standardowego, a w momencie, kiedy użytkownik będzie potrzebuje wykonać czynności administracyjne, takie jak instalacja oprogramowania lub modyfikacji ustawień systemu, to system powiadomi użytkownika i poprosi o udzielenie zgody na wykonanie tych czynności. Tryb ten jednak, nie zapewnia tego samego poziomu zabezpieczeń jak w przypadku konta standardowego użytkownika i nie gwarantuje, iż oprogramowanie złośliwe, które już znajduje się na komputerze, nie będzie mogło skorzystać z podniesienia uprawnień dla własnej aplikacji w celu wykonania czynności szkodliwych dla komputera, na którym się znajduje.

**Ocena ryzyka**

Użytkownicy posiadający uprawnienia administracyjne podczas normalnej pracy w systemie, narażeni są na wykonanie czynności administracyjnych w sposób przypadkowy lub szkodliwy bez ich wiedzy, poniżej przedstawiono kilka przykładów takiej sytuacji:

- Użytkownik pobrał i zainstalował oprogramowanie szkodliwe ze strony internetowej, która została specjalnie spreparowana lub zarażona wirusem lub oprogramowaniem złośliwym.
- Użytkownik został podstępnie zachęcony do otworzenia załącznika z poczty elektronicznej zawierającego oprogramowanie złośliwe, które zainstalowało się w sposób automatyczny i niezauważalny na komputerze użytkownika.
- Nośnik pamięci przenośnej został podłączony do komputera i funkcja auto odtwarzania samoczynnie uruchomiła i zainstalowała złośliwe oprogramowanie.
- Użytkownik zainstalował niewspieraną lub niesprawdzoną aplikację, która wpływa na wydajności komputera i jego niezawodność.

**Minimalizacja ryzyka**

Rekomendowane jest stosowane do codziennych czynności i działań w systemach kont użytkownika standardowego bez uprawnień administracyjnych. Podczas stosowania mechanizmu UAC w celu podniesienia uprawnień i wprowadzenia poświadczeń dla konta administratora zaleca się otworzenie innej sesji dla administratora stosując mechanizm szybkiego przełączania użytkowników.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Mechanizm UAC pomaga zminimalizować zagrożenie zdefiniowane w poprzedniej sekcji „Ocena ryzyka”, jednak przed zastosowaniem technologii UAC, ważne jest, aby wziąć pod uwagę następujące działania:

- Jeśli wewnętrzny dział programistów dostarcza aplikacje we własnym zakresie, rekomendowane jest zapoznanie się z artykułem "Windows Vista Application Development Requirements for User Account Control Compatibility"[16]. Dokument ten opisuje, w jaki sposób należy projektować i dostarczą aplikacje zgodne z mechanizmem UAC.
- Aplikacje nie kompatybilne z technologią UAC mogą spowodować problemy z domyślnie włączonym poziomem mechanizmu UAC. Z tej przyczyny ważne jest, aby przeprowadzić testy aplikacji na zgodność z technologią UAC zanim zostaną wdrożone w środowisku produkcyjnym. Więcej informacji na temat testów kompatybilności aplikacji znajduje się w rozdziale 6.
- Włączenie UAC w znaczny sposób zwiększa ilość żądań podniesienia uprawnień lub stosowania kont administracyjnych podczas normalnych czynności wykonywanych przez administratorów systemu. W przypadku, kiedy takie działanie wpływa w znacznym stopniu na wydajność pracy administratorów, można rozważyć skonfigurowanie ustawienia zasady grup **Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora** korzystając z opcji **Podnieś uprawnienia bez monitowania.** Jednakże, zmiana ta obniża poziom bezpieczeństwa konfiguracji komputerów i zwiększa ryzyko wystąpienia oprogramowania złośliwego.
- Użytkownik, który posiada uprawnienia administracyjne i posługuje się kontem Protected Administrator (PA) może wyłączyć funkcję zatwierdzania przez administratora (ang. Administrator Approval Mode), może także wyłączyć UAC tak, aby system nie powiadamiał o konieczności podnoszenia uprawnień podczas instalacji aplikacji lub dokonywania zmian w systemie. Z tego powodu nie można zagwarantować, iż stosowane zasady grup dotyczące mechanizmu UAC będą skuteczne, jeśli użytkownicy posiadają uprawnienia administracyjne na komputerach w organizacji.
- Rekomendowane jest stosowanie dwóch kont dla administratorów systemów. Pierwsze do wykonywania wszystkich normalnych czynności i zadań na komputerze, jako standardowy użytkownik nieposiadający uprawnień administracyjnych. W przypadku, kiedy wymagane jest zastosowanie uprawnień administracyjnych, administratorzy systemu powinni zalogować się korzystając z drugiego i wykonać określone czynności administracyjne. Po wykonaniu działań powinni wylogować się i powrócić do normalnej pracy korzystając z konta standardowego użytkownika.
- Ustawienia zasad grup wskazane w tym przewodniku wyłączają możliwość podnoszenia uprawnień standardowemu użytkownikowi, należy zauważyć, iż jest to normlane zachowanie komputerów, które korzystają z domeny Active Directory. Jest to rekomendowane ustawienie, które wymusza wykonywanie czynności administracyjnych tylko przez użytkowników posiadających konta z przypisanymi uprawnieniami administracyjnymi.
- Jeśli aplikacja zostanie niepoprawnie zidentyfikowana, jako aplikacja wymagająca uprawnień administracyjnych lub aplikacja użytkownika, to system Windows może uruchomić ta aplikację w złym kontekście zabezpieczeń.

[16] http://go.microsoft.com/fwlink/?linkid=104243

**Proces minimalizacji ryzyka**

Proces minimalizacji ryzyka należy rozpocząć od zbadania i przetestowania pełnych możliwości mechanizmu UAC. Dodatkowe informacje w tym zakresie można uzyskać na stronach Microsoft: Understanding and Configuring User Account Control in Windows Vista[17] oraz Getting Started with User Account Control on Windows Vista[18].

W celu minimalizacji ryzyka zaleca się zastosowanie działań:

1. Ustalenie liczby użytkowników, którzy wykonują zadania administracyjne.
2. Określenie jak często zadania administracyjne są wykonywane.
3. Określenie sposobu wykonywania czynności administracyjnych przez administratorów: prostszy poprzez powiadomienie UAC i wyrażanie zgody na wykonanie danej czynności lub wymagający wprowadzenia określonych poświadczeń w celu wykonania zadań administracyjnych.
4. Określenie czy standardowi użytkownicy powinni mieć możliwość podniesienia uprawnień w celu wykonania zadań administracyjnych. Zastosowane ustawienia zasad grupowych wskazane w tym przewodniku wyraźnie blokują możliwość podnoszenia uprawnień standardowym użytkownikom.
5. Zidentyfikowanie sposobu obsługi procesu instalacji aplikacji na komputerach.
6. Konfiguracja ustawień zasad grupowych dla UAC dopasowanych do własnych potrzeb i wymagań.

**Zastosowanie ustawień zasad grupowych w celu minimalizacji ryzyka dla UAC**

Konfiguracja tych ustawień dostępna jest w gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń**

**(Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options\)**

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 8 dla omawianej technologii

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora | To ustawienie zasad steruje sposobem działania trybu zatwierdzania przez administratora dla wbudowanego konta administratora. | Wyłączone |
| Kontrola konta użytkownika: zezwalaj aplikacjom z poziomem UIAccess na monitowanie o podniesienie uprawnień bez | To ustawienie zabezpieczeń kontroluje, czy programy z funkcją dostępności interfejsu użytkownika (UIAccess lub UIA, User Interface | Wyłączone |

[17] http://go.microsoft.com/fwlink/?linkid=148165
[18] http://go.microsoft.com/fwlink/?linkid=84129

| | | |
|---|---|---|
| używania bezpiecznego pulpitu | Accessibility) mogą automatycznie wyłączać bezpieczny pulpit na potrzeby monitowania o podniesienie uprawnień przez użytkownika standardowego. | |
| Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora | To ustawienie zabezpieczeń określa zachowanie monitu o podniesienie uprawnień dla administratorów. | Monituj o zgodę na pliki binarne niepochodzące z systemu Windows |
| Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych | To ustawienie zabezpieczeń określa zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych. | Monituj o poświadczenia |
| Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie uprawnień | To ustawienie zabezpieczeń steruje zachowaniem wykrywania instalacji aplikacji dla komputera. | Włączone |
| Kontrola konta użytkownika: podnoszenie uprawnień tylko tych plików wykonywalnych, które są podpisane i mają sprawdzoną poprawność | To ustawienie zabezpieczeń wymusza sprawdzanie podpisów infrastruktury kluczy publicznych (PKI) dla każdej aplikacji interakcyjnej, która żąda podniesienia uprawnień. Administratorzy przedsiębiorstwa mogą kontrolować listę dozwolonych aplikacji administratora przez dodanie certyfikatów znajdujących się w magazynie zaufanych wydawców na komputerach lokalnych. | Wyłączone |
| Kontrola konta użytkownika: Podnieś uprawnienia tylko tych aplikacji z poziomem UIAccess, które są zainstalowane w bezpiecznych lokalizacjach | To ustawienie zabezpieczeń kontroluje, czy aplikacje żądające wykonywania z poziomem integralności UIAccess muszą znajdować się w bezpiecznej lokalizacji w systemie plików. Bezpieczne lokalizacje ograniczają się do następujących katalogów:<br><br>- …\Program Files\ wraz z podkatalogami,<br>- …\Windows\system32,<br>- …\Program Files (x86)\ wraz z podkatalogami dla 64-bitowych wersji systemu Windows.<br><br>Uwaga: system Windows wymusza sprawdzanie podpisu infrastruktury kluczy publicznych (PKI) w każdej aplikacji interaktywnej, która żąda wykonywania z poziomem | Włączone |

| | | |
|---|---|---|
| | integralności UIAccess, niezależnie od stanu tego ustawienia zabezpieczeń. | |
| Kontrola konta użytkownika: uruchamianie wszystkich administratorów w trybie zatwierdzania przez administratora | To ustawienie zabezpieczeń kontroluje zachowanie wszystkich zasad funkcji Kontrola konta użytkownika dla komputera. | Włączone |
| Kontrola konta użytkownika: przełącz na bezpieczny pulpit przy monitowaniu o podniesienie uprawnień | To ustawienie zabezpieczeń kontroluje zachowanie wszystkich zasad funkcji Kontrola konta użytkownika dla komputera. | Włączone |
| Kontrola konta użytkownika: wirtualizuj błędy zapisu plików i rejestru w lokalizacjach poszczególnych użytkowników | To ustawienie zabezpieczeń kontroluje przekierowywanie błędów zapisu starszych aplikacji do zdefiniowanych lokalizacji zarówno w rejestrze, jak i w systemie plików. Ta funkcja ogranicza aplikacje, które wcześniej były uruchamiane z uprawnieniami administratora i zapisywały dane aplikacji w czasie wykonywania do katalogów %ProgramFiles%, %Windir%, %Windir%\system32 lub HKLM\Software\. | Włączone |

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

## 3.5. Zabezpieczenia biometryczne

Windows 8 zawiera strukturę biometryczną systemu Windows (ang. Windows Biometric Framework) obsługującą czytniki linii papilarnych oraz inne urządzenia biometryczne w sposób uniwersalny przez aplikacje wyższego poziomu. Wbudowane komponenty systemu Windows zapewniają wsparcie na poziomie systemu operacyjnego i ułatwiają obsługę rozpoznawania linii papilarnych przez aplikacje korzystające z rozwiązań biometrycznych. W poprzednich wersjach systemu Windows wydanych przed wersją Windows 7 obsługa rozpoznawania linii papilarnych wymagała sterowników i aplikacji firm trzecich do prawidłowej obsługi i logowania do systemu z zastosowaniem linii papilarnych. System Windows 7 i Windows 8 obsługuje natywnie rozwiązania biometryczne wymagając tylko instalacji sterownika do urządzenia czytnika biometrycznego.

W systemie Windows 8 wprowadzono dodatkowe rozszerzenia i wsparcie dla urządzeń biometrycznych. Funkcja szybkie przełączanie użytkownika (ang. fast user switching) jest w pełni obsługiwana i wspiera poprzez technologie rozpoznawania linii papilarnych, a dodatkowo wprowadzono ulepszone mechanizmy synchronizacji haseł i odcisków linii papilarnych.

**Ocena ryzyka**

Standardowe metody weryfikacji użytkownika z zastosowaniem hasła posiadają liczne słabości i podatności, które mogą stwarzać zagrożenia dla bezpieczeństwa zarządzanego środowiska informatycznego. Jeśli hasła są jedynym mechanizmem uwierzytelniającym użytkowników, to

mechanizm ten może powodować, że użytkownicy mogą zapisywać hasła na kartkach, mogą być często zapominane przez użytkowników lub mogą stać się łatwym celem ataku siłowego przeprowadzonym na systemie w celu ujawnienia i pozyskania haseł. W celu zwiększenia bezpieczeństwa ochrony kont użytkowników, należy stosować wieloczynnikowe metody uwierzytelnienia poprzez wdrożenie urządzeń takich jak karty inteligentne. Mechanizm ten wymaga od użytkownika wprowadzenia informacji, którą zna (PIN) oraz zastosowania czegoś, co posiada fizycznie (karta inteligenta). Metoda ta zwiększa poziom bezpieczeństwa uwierzytelnienia, ale nadal podatna jest na zgubienie lub w niewielkim stopniu na modyfikację.

**Minimalizacja ryzyka**

Zastosowane wsparcie dla urządzeń biometrycznych w systemie Windows 8 pozwala organizacjom na implementację dodatkowej warstwy weryfikacji tożsamości poprzez wymaganie przedstawienia czegoś, co jest częścią osoby, która jest weryfikowana. Proces ten minimalizuje ryzyko związane ze stosowaniem haseł oraz kart inteligentnych. Wbudowany mechanizm obsługi czytników biometrycznych w Windows 8 może współpracować z wieloma różnorodnymi typami uwierzytelnienia biometrycznego. Coraz większa dostępność i niska cena czynników linii papilarnych sprawiła, iż forma uwierzytelnienia biometrycznego może być skutecznie wdrożona w wielu organizacjach.

Identyfikacja na podstawie linii papilarnych oferuje następujące zalety:

- Odcisk palca pozostaje normalnie niezmienny przez całe życie
- Nie występują dwa identyczne odciski palca (nawet w przypadku bliźniaków)
- Czytniki linii papilarnych stały się tańsze i przez to dostępne w szerokim zakresie
- Proces skanowania linii papilarnych jest prosty i szybki
- Niezawodność skanowanych próbek jest wysoka i posiada niski poziom błędnych próbek biometrycznych (ang. false acceptance rate (FAR)) porównując do innych form biometrycznego skanowania, takich jak rozpoznawanie twarzy lub analiza głosu.

Identyfikacja na podstawie linii papilarnych posiada również wady:

- Użytkownicy z uszkodzonymi (poprzez obrażenia fizyczne naskórka) odciskami palców nie będą mogli się uwierzytelnić w sposób poprawny
- Zostało udowodnione naukowo, iż możliwe jest uzyskanie dostępu i oszukanie systemów rozpoznających odciski palców poprzez podstawienie spreparowanych odcisków palca, W celu uzyskania dodatkowych informacji należy odwiedzić witrynę Impact of Artificial "Gummy" Fingers on Fingerprint Systems[19].
- Wiek użytkownika oraz zakres wykonywanej pracy fizycznej może wpłynąć na niezawodność procesu skanowania linii papilarnych

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

W przypadku zastosowania mechanizmu weryfikacji biometrycznej, takiej jak odciski linii papilarnych, będącej częścią wdrożenia systemu Windows 8, należy rozważyć przed wdrożeniem następujące kwestie:

[19] http://cryptome.org/gummy.htm

- Systemy biometryczne zwykle wymagają odpowiedniego przetwarzania wrażliwych danych biometrycznych użytkowników, które przechowywane są na komputerach w celu dokonania uwierzytelnienia. Sytuacja ta może stanowić naruszenie prywatności oraz wymaga właściwego sposobu przetwarzania wrażliwych danych osobowych w organizacji.
- Większość nowoczesnych komputerów przenośnych posiada wbudowany czytnik linii papilarnych, przez co proces wdrożenia urządzeń biometrycznych może być prostszy, jednakże wbudowane czytniki mogą posiadać różnorodną precyzję skanowania i nie zawsze najwyższej, jakości, w stosunku do dedykowanych rozwiązań biometrycznych. Zaleca się przetestowanie i oszacowanie, jakości czytników na podstawie przeprowadzonych testów w zakresie biometrii: (FRR) - false rejection rate, (FAR) false acceptance rate, (CER) crossover error rate, (FTE/FER) - failure to enroll rate oraz wskaźnika wydajności.
- Jeśli środowisko pracy zawiera obszary, w których nie możliwe jest utrzymanie czystych rąk, z uwagi na rodzaj wykonywanej pracy, czytniki linii papilarnych nie mogą być stosowane. W tej sytuacji zaleca się rozważyć inne indywidualne cechy fizyczne, takie jak siatkówka oka, rozpoznanie twarzy lub geometria dłoni.
- Zaleca się, aby użytkownik wprowadzał dodatkowy czynnik podczas uwierzytelnienia, taki jak fraza kodująca, kod PIN lub karta inteligentna, z uwagi na fakt, iż, znane są sposoby oszukania czytników linii papilarnych przez podstawienie sztucznego odcisku palca wykonanego z żelu w celu ominięcia zabezpieczeń. W celu uzyskania dodatkowych informacji należy odwiedzić witrynę Impact of Artificial "Gummy" Fingers on Fingerprint Systems[20].

**Proces minimalizacji ryzyka**

Należy pamiętać, że każda organizacja posiada swoją specyfikę pracy, która jest unikalna z uwagi na środowisko, w którym funkcjonuje. Przed wdrożeniem należy dokładnie przeanalizować rozwiązanie i upewnić się, że planowane rozwiązanie spełni postawione wymaganie zapewnienie zwiększenia poziomu bezpieczeństwa procesu uwierzytelnienia.

W celu efektywnego wdrożenia zabezpieczeń biometrycznych oraz minimalizacji ryzyka zaleca się następujące działania:

1. Sprawdzenie i przeprowadzenie szeregu testów różnorodnych rozwiązań weryfikacji biometrycznych w celu wybrania najlepszego rozwiązania spełniającego wymagania i potrzeby organizacji.
2. Zapoznanie się z polityka prywatności obowiązującą w danej organizacji, ze szczególnym uwzględnieniem zasad przetwarzania wrażliwych danych osobowych.
3. Określenie wymagań technicznych stawianych urządzeniom biometrycznym oraz zaplanowanie w czasie wdrożenia fazy testowej, która sprawdzi zgodność urządzeń ze stawianymi wymaganiami dla tych urządzeń.
4. Określenie dodatkowych wymagań technicznych niezbędnych do wdrożenia rozwiązania biometrycznego, takich jak infrastruktura klucza publicznego lub instalacja oprogramowania klienckiego do obsługi biometrii.
5. Oszacowanie liczby pracowników, którzy mogą mieć trudności podczas korzystania z rozwiązania biometrycznego z uwagi na ich cechy fizyczne, wraz zaproponowaniem

[20] http://cryptome.org/gummy.htm

alternatywnego rozwiązania dla tych pracowników. Należy rozważyć alternatywny sposób uwierzytelnienia obejmujący korzystanie z haseł, lub kart inteligentnych wymagających podania kodu PIN.

6. Uświadomienie pracowników w zakresie stosowania uwierzytelnienia biometrycznego oraz poprawnego wykorzystania tego rozwiązania, a przypadku braku możliwości korzystania z tego systemu wskazanie alternatywnego procesu uwierzytelnienia.
7. Przeprowadzenie wdrożenia pilotażowego obejmującego dużą grupę osób w celu identyfikacji a następnie rozwiązania napotkanych problemów przed właściwym wdrożeniem rozwiązania w środowisku produkcyjnym.
8. Pobranie indywidualnych cech fizycznych do bazy rozwiązania biometrycznego od pracowników stosując się do instrukcji przekazanych przez dostawcę rozwiązania biometrycznego obejmującego proces skanowania i weryfikacji pobranych danych.
9. Przeszkolenie pracowników w zakresie korzystania z systemu biometrycznego, oraz zapewnienie wsparcia w przypadku napotkanych trudności.
10. Zaplanowanie wdrożenie alternatywnego sposobu uwierzytelnienia dla osób, które odmówią korzystania z systemu biometrycznego poprzez nie wyrażenie zgody na przetwarzanie wrażliwych danych osobowych lub innych czynników.

**Zastosowanie ustawień zasad grup w celu minimalizacji ryzyka dla rozwiązań biometrycznych**

Konfiguracja tych ustawień dostępna jest w gałęzi:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Biometria**

**(Computer Configuration\Administrative Templates\Windows Components\Biometrics)**

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 8 dla omawianej technologii:

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Zezwalaj na używanie biometrii | Jeżeli to ustawienie zasad zostanie włączone lub pozostanie nieskonfigurowane, Usługa biometryczna systemu Windows będzie dostępna, a użytkownicy będą mogli uruchamiać w systemie Windows aplikacje używające biometrii. | Nie skonfigurowano |
| Zezwalaj użytkownikom na logowanie przy użyciu biometrii | To ustawienie zasad określa, czy użytkownicy mogą logować się lub podwyższać poziom uprawnień Kontroli | Nie skonfigurowano |

| | | |
|---|---|---|
| | konta użytkownika przy użyciu biometrii.<br><br>Domyślnie użytkownicy lokalni będą mogli logować się do komputera lokalnego. | |
| Zezwalaj użytkownikom domeny na logowanie przy użyciu biometrii | To ustawienie zasad określa, czy użytkownicy z kontami w domenie mogą logować się lub podwyższać poziom uprawnień przy użyciu funkcji Kontrola konta użytkownika za pomocą biometrii.<br><br>Domyślnie użytkownicy domeny nie mogą używać biometrii w celu logowania. Jeśli to ustawienie zasad zostanie włączone, użytkownicy domeny będą mogli logować się do komputera z systemem Windows przyłączonego do domeny przy użyciu biometrii. W zależności od używanej biometrii włączenie tego ustawienia zasad może osłabić zabezpieczenia użytkowników logujących się przy użyciu biometrii. | Nie skonfigurowano |
| Określ limit czasu zdarzeń szybkiego przełączania użytkowników | To ustawienie zasad określa liczbę sekund, przez którą oczekujące zdarzenie szybkiego przełączania | Nie skonfigurowano |

| | | |
|---|---|---|
| | użytkowników pozostanie aktywne przed zainicjowaniem przełączenia. Domyślnie zdarzenie szybkiego przełączania użytkowników jest aktywne przez 10 sekund, a potem staje się nieaktywne. | |

Tabela 3.4.1 Ustawienia zasad grupowych dla rozwiązań biometrycznych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

## 3.6. Oprogramowanie Windows Defender

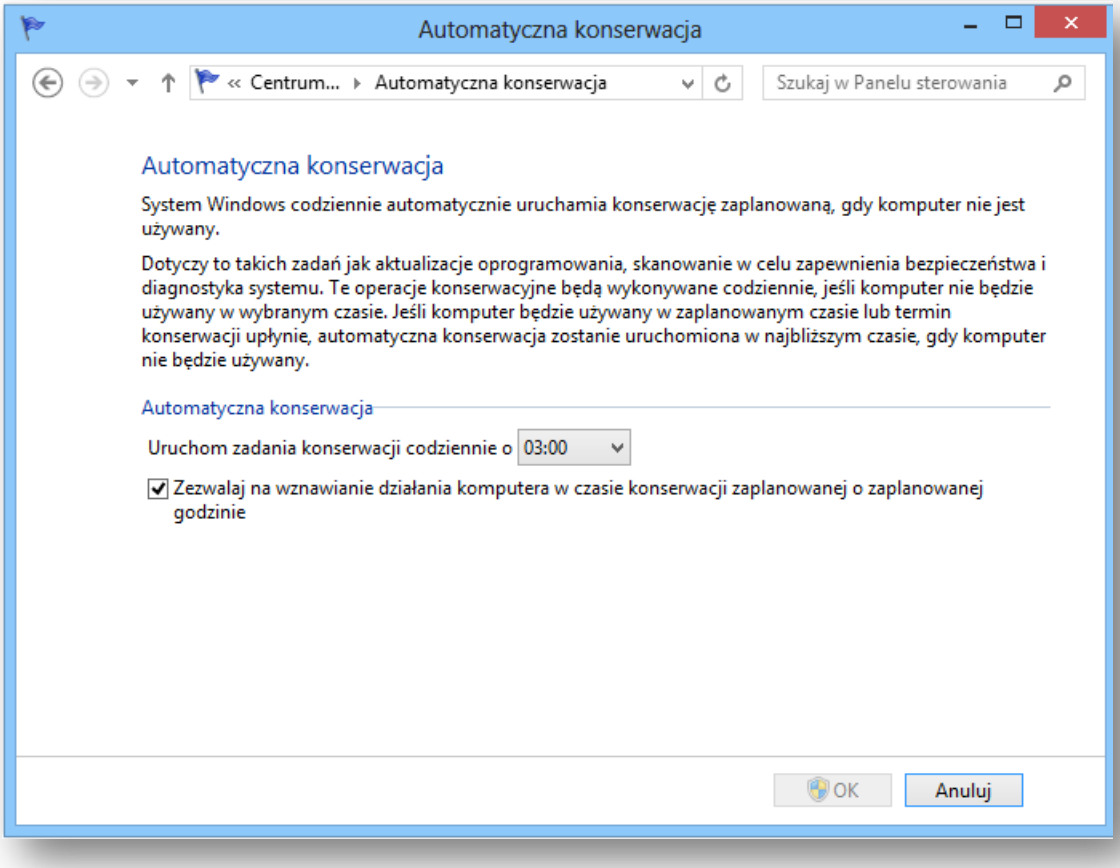
Usługa Windows Defender jest oprogramowaniem antyszpiegowskim dołączonym do systemu Windows 8 i uruchamianym automatycznie po włączeniu systemu, w poprzedniej wersji systemu Windows XP wymagała opcjonalnego pobrania i zainstalowania. Używanie oprogramowania antyszpiegowskiego może pomóc w zapewnieniu ochrony komputera przed programami szpiegującymi i innymi potencjalnie niechcianymi programami takimi jak wirusy, robaki, roboty (ang. bot) czy rootkit'y. Program szpiegujący może zostać zainstalowany na komputerze bez wiedzy użytkownika podczas każdego połączenia z Internetem, a ponadto komputer może zostać nim zainfekowany podczas instalowania niektórych programów przy użyciu nośników wymiennych. Usługa Windows Defender oferuje dwa sposoby ochrony komputera przed zainfekowaniem programami szpiegującymi: ochrona w czasie rzeczywistym oraz zaplanowane skanowanie w celu zapewnienia bezpieczeństwa, jako element automatycznej konserwacji.

W systemie Windows 8, skanowanie w celu zapewnienia bezpieczeństwa zostało przeniesione i stało się częścią **Automatycznej Konserwacji**, która zawiera również mechanizm sprawdzenia dostępnych aktualizacji oprogramowania oraz diagnostykę systemu.

W celu konfiguracji zaplanowanej automatycznej konserwacji należy wykonać czynności:

1. Proszę otworzyć główne okno **Centrum Akcji**
2. Proszę kliknąć w oknie **Centrum Akcji** na opcję **Konserwacja** a następnie należy wybrać **Zmień ustawienia konserwacji.**
3. W oknie **Automatyczna Konserwacja**, należy skonfigurować żądane ustawienia automatycznej konserwacji i zatiwerdzić klikając OK
4. Proszę zamknąć okno **Centrum Akcji.**

**Na rys. 3.5.1 przedstawiono rekomendowane ustawienia dla komputerów pracujących w systemie Windows 8 z włączoną usługą Windows Defender.**




Rys. 3.5.1 – Widok okna ustawień rekomendowanych automatycznego skanowania dla usługi Windows Defender

W momencie, kiedy aplikacja próbuje zmodyfikować chroniony obszar w systemie Windows 8, Windows Defender wyświetli powiadomienie w celu uzyskania potwierdzenia lub anulowania procesu zmiany, która ma wpływ na działanie systemu i zapobiega instalacji szkodliwego oprogramowania.

**Usługa Microsoft Active Protection (MAPS)**

Microsoft Active Protection Service to społeczność online, która może doradzić, jaki sposób reagowania na potencjalne zagrożenia należy wybrać. Społeczność pomaga też powstrzymać rozprzestrzenianie się nowych infekcji. Można zdecydować się na wysyłanie podstawowych lub dodatkowych informacji o wykrytym oprogramowaniu. Dodatkowe informacje pomagają firmie Microsoft w tworzeniu nowych definicji oraz ochronie komputerów przez aplikację Windows Defender. Wysyłane informacje mogą obejmować dane dotyczące lokalizacji wykrytych elementów na komputerze w przypadku usunięcia wirusa, programu szpiegującego lub potencjalnie szkodliwego oprogramowania. Informacje będą gromadzone i wysyłane automatycznie. W celu uzyskania

dodatkowej informacji na temat zasad zachowania poufności informacji należy przeczytać dokument Zasady zachowania poufności informacji w systemach Windows 8 i Windows Server 2012 [21]

**Ocena ryzyka**

Oprogramowanie złośliwe stwarza liczne zagrożenia dla organizacji, które muszą je minimalizować w celu zapewnienia bezpieczeństwa danych poprzez niedopuszczenie do ujawnienia danych przechowywanych na komputerach. Najbardziej zauważalne ryzyka, które stwarza oprogramowanie szpiegujące zawierają:

- Wrażliwe dane organizacji mogą zostać narażone na ryzyko ujawnienia przez osoby nieupoważnione
- Dane osobiste pracowników mogą zostać narażone na ryzyko ujawnienia przez osoby nieupoważnione
- Komputery mogą zostać narażone na utratę kontroli nad systemem poprzez zewnętrzne osoby atakujące
- Ryzyko dotyczące przestojów z powodu oprogramowania szpiegującego wynikające z obniżenia wydajności i stabilności systemów komputerowych.
- Ryzyko dotyczące wzrost kosztów utrzymania i zapewnienia ochrony z powodu oprogramowania szpiegującego
- Potencjalne ryzyko szantażu organizacji i w przypadku, kiedy zainfekowany system ujawni wrażliwe dane

**Minimalizacja ryzyka**

Usługa Windows Defender została zaprojektowana w celu minimalizacji ryzyka związanego z oprogramowaniem złośliwym. Należy regularne i automatycznie pobierać aktualizacje definicji korzystając z usługi Windows Update lub poprzez usługę Windows Server Update Services (WSUS).

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Usługa Windows Defender domyślnie jest włączona i uruchamiana automatycznie po włączeniu komputera z systemem Windows 8, technologia ta została zaprojektowana w taki sposób, aby nie przeszkadzać zwykłym użytkownikom w ich codziennej pracy. W celu efektywnego wdrożenia Windows Defender w organizacji, należy rozważyć następujące rekomendowane działania:

- Przeprowadzenie testów interoperacyjności przed wdrożeniem rozwiązania firm trzecich oprogramowania zapewniającego ochronę antywirusową i antyszpiegowską w czasie rzeczywistym
- Zaprojektowanie systemu wspomagającego zarządzanie aktualizacją sygnatur i definicji w przypadku zarządzania duża ilością komputerów.
- Przeszkolenie użytkowników z możliwych ataków dokonywanych przez oprogramowanie złośliwe oraz zapoznanie z metodami ataków socjotechnicznych
- Dostosowanie zaplanowanego czasu wykonywania automatycznego skanowania do potrzeb danej organizacji. Domyślny czas uruchomienia skanowania codziennego to godzina 3:00 w

[21] http://go.microsoft.com/fwlink/?LinkId=190175, http://windows.microsoft.com/pl-PL/windows-8/windows-8-privacy-statement?ocid=W8_UI

nocy, komputer automatycznie wybudzi się się ze stanu uśpienia w celu przeprowadzenia zaplanowanych zadań automatycznej konserwacji. Jeśli komputer nie będzie mógł przeprowadzić skanowania w zaplanowanym czasie, to użytkownik zostanie poinformowany i zapytany o zgodę na uruchomienie skanowania. Natomiast, jeśli skanowanie nie odbędzie si w ciągu 2 następnych dni, to zostanie przeprowadzone automatycznie po okresie 10 minut od startu komputera. W systemie Windows 8 proces skanowania uruchamiany jest z niskim priorytetem w sposób minimalizujący obciążenie pracującego komputera.

- Windows Defender nie został zaprojektowany, jako aplikacja klasy Enterpise skierowana dla dużych organizacji. Rozwiązanie to nie zapewnia pełnego centralnego raportowania, monitorowania i mechanizmów kontroli konfiguracji. W przypadku potrzeby wykorzystania dodatkowego elementu centralnego zarządzania i raportowania należy rozważyć wdrożenie produktów zaawansowanych takich jak Microsoft System Center 2012 Endpoint Protection.
- Określenie polityki poufności dla organizacji w zakresie wysyłania i raportowania ujawnionego oprogramowania złośliwego do programu społeczności MAPS.

**Proces minimalizacji ryzyka**

Windows Defender jest domyślnym składnikiem systemu Windows 8 i nie wymaga dodatkowych czynności w celu aktywacji tego produktu. Należy rozważyć kilka dodatkowych rekomendowanych czynnośći które zapewnią stałą ochronę organizacji poprzez rekomednowane działania:

1. Sprawdzenie i przeprowadzenie testów możliwości usługi Windows Defender działającego pod kontrolą systemu Windows 8.
2. Sprawdzenie i przeprowadzenie testów konfiguracji Windows Defender poprzez zastosowanie zasad grup.
3. Oszacowanie i przetestowanie dodatkowej ochrony antywirusowej, wraz z określeniem czy oferowana ochrona zapewnia zabezpieczenie przed oprogramowaniem szpiegującym wraz ochroną antywirusową.
4. Zaplanowanie optymalnych regularnych aktualizacji sygnatur i definicji dla wszystkich komputerów, należy pamiętać, iż komputery przenośne mogą wymagać innej konfiguracji niż komputery stacjonarne.
5. Przeprowadzić szkolenia użytkowników w zakresie, który umożliwi samodzielne identyfikowanie podejrzanych działań komputera i możliwych infekcji poprzez oprogramowanie złośliwe.
6. Przeprowadzić szkolenia pracowników działu technicznego zapewniającego wsparcie dla użytkowników z zakresu działania i dostępnych narzędzi wspomagających proces udzielania wsparcia użytkownikom w zakresie usługi Windows Defender.

**Zastosowanie ustawień zasad grupowych w celu minimalizacji ryzyka dla Widnows Defender**

Konfiguracja tych ustawień dostępna jest w następującej lokalizacji w narzędziu Edytor obiektów zasad grupowych:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Defender**

**(Computer Configuration\Administrative Templates\Windows Components\Windows Defender)**

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 8 oraz Windows 8.1 dla omawianej technologii:

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows |
|---|---|---|
| Sprawdzaj przed zaplanowanym skanowaniem, czy są nowe sygnatury | Powoduje, że przed uruchomieniem zaplanowanego skanowania następuje sprawdzenie, czy są nowe sygnatury.<br><br>Włączenie tego ustawienia zasad spowoduje sprawdzanie dostępności nowych sygnatur przed rozpoczęciem każdego zaplanowanego skanowania.<br><br>Jeśli to ustawienie zasad zostanie **wyłączone** lub **nie zostanie skonfigurowane**, zaplanowane skanowania będą inicjowanie bez pobierania nowych sygnatur. | Nie skonfigurowano |
| Wyłącz usługę Windows Defender | To ustawienie zasad powoduje wyłączenie usługi Windows Defender. Jeśli to ustawienie zasad zostanie włączone, usługa Windows Defender nie będzie uruchamiana, a komputery nie będą skanowane w poszukiwaniu złośliwego oprogramowania lub innego potencjalnie niechcianego oprogramowania. | Nie skonfigurowano |
| Wyłącz monitorowanie w czasie rzeczywistym | To ustawienie zasad umożliwia wyłączenie monitów ochrony w czasie rzeczywistym dotyczących wykrywania znanego złośliwego oprogramowania. | Nie skonfigurowano |
| Wyłącz rutynowo podejmowaną akcję | To ustawienie zasad umożliwia określenie, czy usługa Windows Defender ma automatycznie podejmować akcję dla wszystkich wykrytych zagrożeń. Akcja podejmowana w przypadku określonego zagrożenia jest ustalana na podstawie kombinacji akcji zdefiniowanej przez zasady, akcji zdefiniowanej przez użytkownika i akcji zdefiniowanej przez sygnaturę.<br><br>Jeśli to ustawienie zasad zostanie włączone, usługa Windows Defender nie będzie automatycznie podejmować akcji dla wykrytych zagrożeń, ale będzie monitować użytkowników o wybranie jednej z | Nie skonfigurowano |

| | | |
|---|---|---|
| | akcji dostępnych dla danego zagrożenia.<br><br>Jeśli to ustawienie zasad zostanie wyłączone lub pozostanie nieskonfigurowane, usługa Windows Defender będzie automatycznie podejmować akcję dla wszystkich wykrytych zagrożeń po około dziesięciu minutach (tego czasu nie można zmienić). | |
| Skonfiguruj raportowanie społeczności Microsoft Active Protection Service | To ustawienie zasad pozwala skonfigurować członkostwo w społeczności Microsoft Active Protection Service. | Nie skonfigurowano |

Tabela 4.5.1 Ustawienia zasad grupowych dla usługi Windows Defender

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

## 3.7. Narzędzie do usuwania złośliwego oprogramowania

Narzędzie do usuwania złośliwego oprogramowania (ang. MSRT - Malicious Software Removal Tool) jest programem wykonywalnym o niewielkim rozmiarze, który ułatwia usuwanie określonych najbardziej rozpowszechnionych rodzajów złośliwego oprogramowania z komputerów z systemami Windows.

Firma Microsoft dostarcza, co miesiąc nową wersję programu MSRT poprzez usługi aktualizacji: Microsoft Update, Windows Updates, WSUS oraz Centrum Pobierania Microsoft. Narzędzie do usuwania złośliwego oprogramowania jest uruchamiane w trybie cichym i po zakończeniu wyświetli raport, jeśli zostanie wykryte oprogramowanie złośliwe. Narzędzie to nie jest instalowane w systemie operacyjnym i nie posiada ustawień zasad grupowych. Domyślnie plik z raportem z przeprowadzonego skanowania jest umieszczony w miejscu **%SystemRoot%\Debug\mrt.log**.

Program MSRT nie został zaprojektowany, jako program antywirusowy klasy Enterpise skierowana do dużych organizacji. Rozwiązanie to nie zapewnia pełnego centralnego raportowania, monitorowania i mechanizmów kontroli konfiguracji. W przypadku potrzeby dodatkowego elementu centralnego zarządzania i raportowania należy rozważyć wdrożenie produktów zaawansowanych takich jak Microsoft System Center 2012 Endpoint Protection[22].

**Ocena ryzyka**

Rekomendowanym rozwiązaniem jest stosowanie programu antywirusowego zainstalowanego na każdym komputerze w organizacji, jako uzupełnienie usług zapewniających bezpieczeństwo dostępnych w systemach Windows 8. Pomimo instalacji właściwej ochrony antywirusowej należy pamiętać, iż istnieją dodatkowe ryzyka, które mogą mieć wpływ na bezpieczeństwo organizacji:

[22] http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx

- Zdarzenie, w którym program antywirusowy nie wykryje specyficznego rodzaju wystąpienia oprogramowania złośliwego
- Oprogramowanie złośliwe wyłączy lub zablokuje ochronę antywirusową na atakowanym komputerze

W sytuacji przedstawionej powyżej, oprogramowanie MSRT dostarczy dodatkową warstwę ochrony w celu wykrycia i usunięcia najbardziej rozpowszechnionych rodzajów złośliwego oprogramowania. Pełna lista złośliwego oprogramowania, które jest wykrywane i usuwane przez MSRT jest aktualizowana na bieżąco i została umieszczona na stronie internetowej: Rodziny programów usuwane przez narzędzie do usuwania złośliwego oprogramowania[23]

**Minimalizacja ryzyka**

W celu minimalizacji ryzyka rekomenduje się włączenie funkcji aktualizacje automatyczne na komputerach klienckich. Włączenie funkcji „Aktualizacje automatyczne" gwarantuje automatyczne otrzymywanie narzędzia MSRT, co miesiąc i możliwość uruchomienia tak szybko jak tylko ukażę się nowa wersja tego narzędzia. MSRT została zaprojektowany w celu minimalizacji ryzyka związanego z oprogramowaniem złośliwym, które firma Microsoft zidentyfikowała i zakwalifikowała, jako wysokie zagrożenie i jednocześnie rozpowszechniające się na szeroką skalę stanowiące zagrożenie dla bezpieczeństwa użytkowników systemu Windows.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

W przypadku rozważania zastosowanie omawianego narzędzia MSRT we własnym środowisku, przedstawiono poniżej listę najważniejszych czynników ułatwiających prawidłowe wdrożenie:

- Program MSRT zajmuje około 9 MB, równoczesne pobieranie tego programu przez dużą liczbę użytkowników, może wpłynąć niekorzystnie na wydajność połączenia internetowego
- Narzędzie MSRT pierwotnie zostało zaprojektowane dla użytkowników niekorporacyjnych, którzy nie posiadają zainstalowanych aktualnych rozwiązań antywirusowych. Jednakże, może stanowić uzupełnienie istniejącego rozwiązania ochrony antywirusowej, stanowiącej dodatkowy element strategii defense-in-depth. W celu wdrożenia narzędzia MSRT w środowisku organizacji, można wykorzystać następujące sposoby instalacji:
    - Windows Server Update Services
    - Pakiet instalacyjny SMS / SCCM
    - Poprzez skrypt startowy komputera uruchamiany przez zasady grupowe
    - Poprzez skrypt startowy użytkownika uruchamiany przez zasady grupowe

  W przypadku dużych środowisk, rekomendowane jest zapoznanie się z dokumentem Wdrażanie Narzędzia Microsoft Windows do usuwania złośliwego oprogramowania w środowisku przedsiębiorstwa[24], Numer ID artykułu: 891716 bazy wiedzy Microsoft Knowledge Base

- Program MSRT nie zapewnia ochrony w czasie rzeczywistym, w związku z powyższym wysoce rekomendowane jest zainstalowanie programu antywirusowego, który zapewnia ochronę w

[23] http://www.microsoft.com/pl-pl/security/pc-security/malware-families.aspx
[24] http://support.microsoft.com/Default.aspx?kbid=891716

czasie rzeczywistym przed nowymi zagrożeniami, które pojawiają się każdego dnia, przykładem takiego rozwiązania jest Microsoft System Center 2012 Endpoint Protection zapewniający uniwersalną ochronę przed oprogramowaniem złośliwym, stosowaną na komputerach przenośnych, stacjonarnych oraz serwerach.

- W trakcie uruchomienia programu MSRT, program tworzy tymczasowy katalog o losowej nazwie wewnątrz głównego dysku napędu posiadającego największą możliwą przestrzeń do zapisu, który przeważnie jest głównym dyskiem systemu operacyjnego. Katalog ten zawiera kilka plików włączając w to Mrtstub.exe, w większości przypadków katalog ten zostanie usunięty automatycznie po zakończeniu procesu skanowania lub ponownym uruchomieniu komputera. Ale może zdarzyć się sytuacja, w której folder ten nie zostanie usunięty automatycznie, w takim przypadku należy usunąć folder ręcznie bez obawy o skutki uboczne dla komputera.

**Proces minimalizacji ryzyka**

W celu efektywnego wykorzystania narzędzia MSRT i minimalizacji ryzyka zaleca się zastosować działania:

- Sprawdzenie i przeprowadzenie testów możliwości narzędzia MSRT, W celu uzyskania dodatkowych informacji należy odwiedzić witrynę: Narzędzie do usuwania złośliwego oprogramowania- Malicious Software Removal Tool[25]
- Oszacowanie potrzeby wdrożenia narzędzia MSRT we własnym środowisku
- Określenie najbardziej odpowiedniego sposobu wdrożenia narzędzia MSRT w organizacji.
- Dokonanie identyfikacji systemów w organizacji, na których wdrożenie narzędzia MSRT zapewni dodatkowy stopień ochrony.
- Wdrożenie narzędzia z zastosowaniem określonej i właściwej metody wdrożenia

## 3.8. Zapora systemu Windows 8 oraz Windows 8.1

Zapora osobista jest krytycznym elementem obrony przed wieloma rodzajami oprogramowania złośliwego. Tak jak w przypadku poprzednich wersji systemu Windows od czasu wydania Windows XP SP2 zapora osobista jest domyślnie włączona w systemie Windows, w celu zapewnienia ochrony komputera użytkownika od momentu jak tylko system operacyjny jest gotowy do pracy.

Zapora osobista w systemie Windows 8 oraz Windows 8.1 wykorzystuje ten sam mechanizm ochrony jak w przypadku Windows Vista włączając w to filtrowanie ruchu wchodzącego i wychodzącego dla zapewnienia ochrony poprzez ograniczenie dostępu sieciowego do zasobów systemu operacyjnego. W rozwiązaniu tym została zastosowana ta sama konsola interfejsu użytkownika zapory systemu Windows z zabezpieczeniami zaawansowanymi, znana już z poprzedniego systemu Windows Vista. Konsola ta jest centralnym miejscem upraszczającym zarządzanie. Z poziomu tej konsoli możemy zarządzać filtrowaniem ruchu sieciowego przychodzącego i wychodzącego z interfejsów sieciowych oraz ustawieniami protokołu IPsec zapewniającymi bezpieczeństwo połączenia dzięki zastosowaniu wymiany kluczy, uwierzytelniania, integralności danych i opcjonalnie szyfrowania danych.

[25] http://www.microsoft.com/pl-pl/security/pc-security/malware-removal.aspx

W systemie Windows 8 istnieją trzy profile aplikacji Zapora systemu Windows z zabezpieczeniami zaawansowanymi:

**Profil domenowy**
Profil stosowany jest, wtedy, kiedy komputer został podłączony do sieci oraz nastąpiło uwierzytelnienie do kontrolera domeny, do którego należy komputer.

**Profil publiczny**
Jest to domyślny profil i stosowany jest w scenariuszach, kiedy komputer nie jest dołączony do domeny. Ustawienia profilu publicznego powinny być najbardziej restrykcyjne, ponieważ komputer jest połączony z siecią publiczną, w której nie można kontrolować bezpieczeństwa.

**Profil prywatny**
Profil stosowany jest, jeśli użytkownik posiadający poświadczenia lokalnego administratora przypisze go w ramach bieżącego połączenia sieciowego do sieci wcześniej zdefiniowanej, jako sieć publiczna. Zaleca się, aby używać profilu prywatnego w sieciach zaufanych.

W systemach Windows Vista w danej chwili może być aktywny na komputerze tylko jeden profil. System Windows 8 zapewnia wsparcie dla wielu aktywnych profili na poziomie kart sieciowych. Jeśli istnieje wiele kart sieciowych połączonych z różnymi sieciami, dla wszystkich kart na komputerze jest stosowany profil o najbardziej odpowiednich ustawieniach dla typu sieci, do której został przyłączony. Na przykład:, jeśli znajdujemy się w kawiarence i korzystamy z darmowego punktu dostępowego sieci bezprzewodowej w celu połączenia się z siecią naszej organizacji stosując połączenie VPN, to profil publiczny w dalszym ciągu zapewnia nam ochronę ruchu sieciowego, który nie jest transmitowany przez zestawiony tunel połączenia VPN. To samo odnosi się do karty sieciowej niepodłączonej do sieci lub do nierozpoznanej sieci, w tym przypadku zostanie przypisany profil publiczny, a pozostałe karty sieciowe będą używały odpowiednich profili dla typu sieci, do której zostały przyłączone.

**Ocena ryzyka**

Połączenie sieciowe jest niezbędnym elementem w nowoczesnym biznesie, które umożliwia z jednej strony łączność z całym światem, a z drugiej strony to samo połączenie może stać się głównym celem osób atakujących. To zagrożenie towarzyszące nawiązywanym połączeniom musi być minimalizowane, aby zapewnić bezpieczeństwo i nie dopuścić do ujawnienia ważnych danych oraz infekcji komputerów. Najczęściej zidentyfikowane zagrożenia dla organizacji występujące w przypadku ataków z sieci obejmują:

- Zainfekowanie komputera oraz przejęcie kontroli nad komputerem łącznie z uzyskaniem uprawnień administracyjnych przez nieupoważnioną osobę atakującą.
- Zastosowanie skanerów sieciowych przez osobę atakująca w celu zdalnego ustalenia otwartych portów (niezbędnych do działania usług w sieci internet), które mogą zostać wykorzystane do przeprowadzenia ataku z zewnątrz.
- Wrażliwe dane organizacji mogą zostać narażone na ryzyko ujawnienia przez osoby nieupoważnione, w przypadku, kiedy aplikacja typu koń trojański zainicjuje i nawiąże połączenie sieciowe z wewnątrz sieci bezpośrednio ze stacji roboczej wprost to komputera atakującego.

- Komputery przenośne mogą zostać narażone na zewnętrzne ataki sieciowe pracując z sieci niezaufanych poza kontrolą firmowej zapory sieciowej.
- Komputery pracujące w sieci wewnętrznej mogą zostać narażone na ataki sieciowej pochodzące z zainfekowanych komputerów podłączonych to tej samej sieci wewnętrznej.
- Potencjalne ryzyko szantażu organizacji w przypadku, kiedy atakujący zainfekuje komputery pracujące w sieci wewnętrznej.

**Minimalizacja ryzyka**

Zapora systemu Windows 8 zapewnia ochronę komputera i jest dostępna bezpośrednio „po wyjęciu z pudełka". Zapora sieciowa blokuje niechciane połączenia przychodzące do czasu, kiedy stosowanych zmian nie dokona administrator lub odpowiednia zasada grupowa.

Zapora sieciowa zawiera również funkcjonalność filtrowania ruchu wychodzącego z komputera i jest dostępna bezpośrednio „po wyjęciu z pudełka", reguła ta domyślnie ustawiona jest na „zezwalaj" dla całego ruchu wychodzącego. Zastosowanie odpowiednich ustawień zasad grupowych pozwala na konfigurację tych reguł dostępnych w zaporze sieciowej, tak, aby pozostawić ustawienia zabezpieczeń komputera klienckiego w stanie niezmiennym.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

W przypadku rozważania zastosowania zapory sieciowej, przedstawiono poniżej listę najważniejszych czynników ułatwiających prawidłowe planowanie wdrożenia zapory sieciowej:

- Przeprowadzenie testów interoperacyjności aplikacji niezbędnych do pracy na komputerach w organizacji. Każda z aplikacji powinna posiadać określone i zanotowane niezbędne porty do prawidłowej pracy, tak, aby zapora sieciowa umożliwiła ich otwarcie.
- Identycznie jak w przypadku Windows 7, zapora sieciowa systemu Windows 8 obsługuje trzy profile: domenowy, publiczny i prywatny, po to, aby zapewnić odpowiedni poziom ochrony komputerów klienckich, które pracują w sieciach niezaufanych poza siecią wewnętrzną organizacji.
- Określenie odpowiedniego poziomu zbierania logów generowanych przez zaporę sieciową, w celu dostosowania ich do istniejących rozwiązań raportowania i monitorowania w organizacji.
- Domyślnie zapora sieciowa blokuje połączenia zdalnego sterowania oraz zdalnego zarządzania komputerów opartych o system Windows 8. Wewnątrz zapory znajdują się zdefiniowane wbudowane reguły umożliwiające wykonywanie zdalnych zadań. W przypadku potrzeby zdalnej kontroli wystarczy te reguły włączyć w odpowiednich profilach zapory. Na przykład: można włączyć regułę „Pulpit zdalny" dla profilu domenowego, aby zezwolić pracownikom działu wsparcia na zdalne połączenia w celu świadczenia usług pomocy zdalnej użytkownikom. A w przypadku profili publicznego i prywatnego można te reguły pozostawić wyłączone, aby zminimalizować ryzyko ataku sieciowego na komputery znajdujące się poza siecią wewnętrzną.

**Proces minimalizacji ryzyka**

System Windows 8 zawiera ustawienia zasad grupowych jak i również odpowiednie narzędzia graficzne, które wspomagają administratorów w celu przeprowadzenia odpowiedniej konfiguracji

funkcjonalności zapory sieciowej. Zaawansowane ustawienia zabezpieczeń dostępne dla systemów Windows 8 można zastosować również dla komputerów pracujących pod kontrolą systemu Windows 7 SP1 oraz Windows Vista, ale nie można z nich skorzystać w przypadku komputerów klienckich lub obrazów systemów wirtualnych trybu XP Mode pracujących pod kontrolą systemu Windows XP.

W przypadku modyfikacji domyślnej konfiguracji zapory sieciowej, rekomendowane jest wykorzystanie ustawień zasad grupowych dla Zapory systemu Windows z zabezpieczeniami zaawansowanymi w celu zarządzania komputerami pracującymi po kontrolą systemów Windows 8, Windows 7 SP1 oraz Windows Vista.

Zasady dotyczące Zapory systemu Windows z zabezpieczeniami zaawansowanymi zorganizowane są w obrębie gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi**

**(Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security)**

Rekomendowane jest włączenie Zapory systemu Windows z zabezpieczeniami zaawansowanymi dla wszystkich trzech profili. Dodatkowo zapora systemu Windows z zabezpieczeniami zaawansowanymi wspiera i obsługuje „Reguły zabezpieczeń połączeń" (ang. Connection security rules). Zabezpieczenia połączeń obejmują uwierzytelnianie dwu komputerów przed rozpoczęciem komunikacji i zabezpieczanie informacji wysyłanych między dwoma komputerami. Aplikacja Zapora systemu Windows z zabezpieczeniami zaawansowanymi używa zabezpieczeń protokołu internetowego (IPsec), aby uzyskać bezpieczeństwo połączenia dzięki zastosowaniu wymiany kluczy, uwierzytelniania, integralności danych i opcjonalnie szyfrowania danych.

Więcej informacji na temat IPSec[26] można uzyskać odwiedzając witrynę Microsoft Technet.

Zbiór ustawień bazowych opisujący zalecane ustawienia zapory systemu Windows z zabezpieczeniami zaawansowanymi dla systemu Windows 8 oraz Windows 8.1 wraz z wskazaniem zalecanych ustawień dostępny jest w narzędziu Security Compliance Manager[27] (SCM), narzędzie SCM zostanie opisane w dodatku do niniejszego dokumentu.

## 3.9. Ograniczanie dostępu do aplikacji - AppLocker

Windows 8 zawiera uaktualnioną i ulepszoną wersję zasad ograniczeń oprogramowania (ang. Software Restriction Policies) nazywaną AppLocker, która zastępuje funkcję Zasady ograniczania oprogramowania. Funkcja AppLocker udostępnia nowe możliwości i rozszerzenia, które zmniejszają ilość pracy związanej z administracją i ułatwiają administratorom kontrolowanie sposobu uzyskiwania przez użytkowników dostępu i używania plików, takich jak pliki wykonywalne, skrypty, pliki Instalatora Windows i pliki DLL. Konfiguracja funkcji AppLocker może zostać przeprowadzona z zastosowaniem zasad grupowych w obrębie domeny Active Directory lub lokalnie na komputerze z zastosowaniem konsoli Zasady Zabezpieczeń Lokalnych.

**Ocena ryzyka**

[26] http://go.microsoft.com/fwlink/?LinkId=69843
[27] http://go.microsoft.com/fwlink/?LinkId=156033

Każdorazowa próba instalacji nieautoryzowanej aplikacji stwarza ryzyko nieuprawnionych zmian w systemie. Proces instalacyjny dokonuje zmian w systemie operacyjnym komputera oraz powstaje ryzyko uruchomienia dodatkowych usług lub otworzenia dodatkowych portów zapory systemu Windows. Ale nawet, jeśli obawy te nie potwierdzą się, to w systemie pozostaje zainstalowana aplikacja, która wymaga sprawdzenia pod katem możliwego celu ataku, oraz wykorzystania podatności tej aplikacji do przeprowadzenia ataku na tą aplikację. Nieautoryzowana aplikacja może być szkodliwa (niebezpieczna) w zamierzeniu twórców i została zainstalowana omyłkowo lub celowo przez użytkownika, a następnie może przeprowadzić atak na systemy wewnętrzne po podłączeniu komputera do sieci organizacji.

W systemie Windows 8 oraz Windows 8.1, Applocker może również kontrolować nowe aplikacje systemu Windows 8 oraz Windows 8.1. Z uwagi na fakt, iż aplikacje Windows 8.x (nazywane spakowanymi aplikacjami – ang. packaged apps) powiązane są z plikami instalacyjnymi i współdzielone są pod wspólna nazwą wydawcy, nazwy aplikacji wraz z jej numerem wersji, co oznacza, że można tworzyć tylko regułę wydawcy w AppLocker w celu kontrolowania instalacji i uruchomienia aplikacji systemu Windows 8.x.

**Minimalizacja ryzyka**

AppLocker umożliwia administratorom implementację zestawu zasad sterowania aplikacjami, które w znacznym stopniu zredukują w organizacji ryzyko ataku, który może być efektem instalacji nieautoryzowanego oprogramowania na komputerach w organizacji. AppLocker pozwala na minimalizację ryzyka związanego z instalacją oprogramowania poprzez działania:

1. Definiowanie reguł na podstawie atrybutów plików uzyskanych z podpisu cyfrowego, w tym wydawcy, nazwy produktu, nazwy pliku i wersji pliku. Można na przykładu utworzyć reguły na podstawie atrybutu wydawcy, który zachowuje trwałość po dokonaniu aktualizacji, lub utworzyć reguły dotyczące określonej wersji pliku.
2. Przypisywanie reguły do grupy zabezpieczeń lub użytkownika.
3. Tworzenie wyjątków od reguł. Można na przykład utworzyć regułę zezwalającą na uruchamianie wszystkich procesów systemu Windows z wyjątkiem Edytora rejestru (Regedit.exe).
4. Użycie trybu Tylko inspekcja w celu wdrożenia i poznania wpływu zasady przed jej wymuszeniem.
5. Importowanie i eksportowanie reguł. Importowanie i eksportowanie wpływa na całą zasadę. Jeśli na przykład zasada zostanie wyeksportowana, zostaną wyeksportowane wszystkie reguły ze wszystkich kolekcji reguł, w tym ustawienia wymuszania dla kolekcji reguł. Zaimportowanie zasady powoduje zastąpienie istniejącej zasady.
6. Prostsze tworzenie i zarządzanie regułami zasad ograniczeń oprogramowania dzięki zastosowaniu apletów poleceń programu PowerShell dla zasad ograniczeń oprogramowania.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

W przypadku rozważania zastosowanie omawianej funkcji AppLocker we własnym środowisku, przedstawiono poniżej listę najważniejszych czynników ułatwiających prawidłowe wdrożenie:

- Przeprowadzenie dokładnych testów zasad sterowania aplikacjami przed wdrożeniem ich w środowisku produkcyjnym. Wszelkie błędy popełnione podczas procesu projektowania i implementacji tej funkcjonalności mogą spowodować poważne utrudnienia i wpłynąć znacząco na wydajność pracy użytkownika.
- Zaplanowanie czasu na przeprowadzenie procesu oszacowania użytkowanych aplikacji w organizacji poprzez użycie trybu **„Tylko inspekcja”** funkcji AppLocker mający na celu zapoznanie się z zakresem aplikacji wykorzystywanych przez użytkowników przed wdrożeniem ograniczeń.
- Rozważenie stopniowego wdrożenia ograniczeń, rozpoczynając od użytkowników gdzie instalacja oprogramowania stanowi duże zagrożenie dla bezpieczeństwa lub komputerów zawierających wrażliwe dane.

**Proces minimalizacji ryzyka**

Konfiguracja funkcji AppLocker dostępna jest w gałęzi Zasady sterowania aplikacjami w zasadach grupowych. System Windows 8 nadal wspiera zasady ograniczeń oprogramowania (SRP).

**Uwaga:** Funkcja AppLocker nie jest dostępna w wersjach przeznaczonych dla użytkownika indywidualnego systemach Windows 8 ( wersja Windows 8).

**Zastosowanie zasad grupowych w celu minimalizacji ryzyka stosując funkcję AppLocker**

Konfiguracja ustawień funkcji AppLocker znajduje się gałęzi:

**Konfiguracja komputera\Ustawienia systemu Windows\Ustawienie zabezpieczeń\Zasady sterowania aplikacjami**

**(Computer Configuration\Windows Settings\Security Settings\Application Control Policies)**

Przewodnik ten nie zawiera rekomendacji, jakie aplikacje warto zablokować na stacjach klienckich, z uwagi na specyficzne wymagania każdej organizacji. W celu uzyskania dodatkowych informacji na temat planowania i wdrażania zasad AppLocker, należy zapoznać się z dokumentami AppLocker Technical Documentation for Windows 7 and Windows Server 2008 R2[28].

## 3.10. Zasady ograniczeń oprogramowania

Zasady ograniczeń oprogramowania (ang. Software Restriction Policies (SRP)) wprowadzone w systemach Windows Vista, Windows XP, Windows Server 2003 oraz Windows Server 2008 nadal są dostępne i wspierane w systemie Windows 8. Administratorzy nadal mogą stosować te zasady, jako sposób określania i sterowania aplikacjami pracującymi na lokalnych komputerach. Jednakże, firma Microsoft rekomenduje zastąpienie zasad ograniczeń oprogramowania nowymi zasadami sterowania aplikacjami oferującymi nowe możliwości i rozszerzenia wprowadzone w funkcji AppLocker systemu Windows 8.

## 3.11. Bezpieczne uwierzytelnianie za pomocą kart inteligentnych

W systemach Windows, karty inteligentne (ang. smart card) oferują potencjalnie najlepszą metodę uwierzytelnienie i logowania użytkowników do komputerów, stron internetowych oraz aplikacji. Karty inteligentne wspierane są w kilku poprzednich edycjach systemu Windows, ale zmiany

[28] http://go.microsoft.com/fwlink/?LinkId=154902

wprowadzone w systemie Windows 8 sprawiły, iż karty inteligentne są bardziej przystępne do celów uwierzytelnienia w określonych typach dostępu.

Karta inteligentna w znacznym stopniu zwiększa bezpieczeństwo poprzez włączenie mechanizmu dwu-czynnikowego uwierzytelnia (ang. two-factor authentication). Pojęcie dwu-czynnikowego uwierzytelnienia odnosi się do faktu logowania się do komputera lub witryny internetowej, która wymaga posiadania fizycznego elementu, jakim jest fizyczna karta inteligentna (coś co użytkownik posiada – ang. something you have) oraz posiadania informacji przeważnie jest to kod PIN ( coś co jest znane użytkownikowi – ang. something you know). Dlatego, jeśli intruz posiada tylko jeden element z dwóch wymienionych, np. intruz odgadnie kod PIN, to osoba atakująca nadal nie może uwierzytelnić się w systemie bez posiadania fizycznej karty.

W systemie Windows 8, można wykorzystać wirtualne karty inteligentne, które zastępują fizyczne karty wykorzystywane do uwierzytelnienia w witrynach internetowych lub aplikacjach. Wirtualne karty inteligentne używają podobnych mechanizmów bezpieczeństwa, ale magazyn, w którym przechowywane są certyfikaty stanowi moduł TPM (ang. Trusted Platform Module) znajdujący się w komputerze. W tym wypadku komputer zastępuje nam karty inteligentne, jako fizyczne elementy wymagane do uwierzytelnienia (logowania). Wirtualne katy inteligentne oferują adekwatny poziom bezpieczeństwa w stosunku do fizycznych kart inteligentnych bez dodatkowych nakładów finansowych w zakup czytników kart inteligentnych jak i samych kart.

**Ocena ryzyka**

Zdalny dostęp sieciowy oraz dostęp do danych jest poważnym zagrożeniem w przypadku, kiedy konto danego użytkownika zostanie skompromitowane (przejęte) przez atakującego intruza, niezależnie od tego czy zostało to wykonane zdalnie czy lokalnie. Osoba atakująca może wykorzystać dostęp do komputera lub usługi poprzez odgadnięcie nazwy użytkownika (np. drogą dedukcji lub socjotechniki) oraz odgadnięcia hasła lub przeprowadzenia ataku siłowego na hasło użytkownika.

**Minimalizacja ryzyka**

Wdrożenie mechanizmu uwierzytelnienia za pomocą kart inteligentnych lub wirtualnych kart inteligentnych wprowadza silny proces dwu-składnikowego uwierzytelnienia. Poświadczenia użytkowników (ang. credentials) stają się trudniejszym celem atakujących z uwagi na brak dostępu do fizycznego elementu. Implementacja kart inteligentnych wymaga technologii infrastruktury klucza publicznego PKI ( ang. Public Key Infrastructure). Wdrożenie konfiguracji PKI jest zadaniem złożonym, które powinno być starannie zaplanowane przed wdrożeniem. Technologia PKI może zostać wdrożona w oparciu o rolę serwera Windows Server 2012 Usługi certyfikatów Active Directory (ang. Active Directory Certificate Services (AD CS)). Więcej informacji na ten temat można uzyskać pod adresem Active Directory Certificate Services Overview[29].

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

W przypadku rozważania wdrożenia kart inteligentnych lub wirtualnych kart inteligentnych w należy wziąć pod uwagę następujące działania:

[29] http://technet.microsoft.com/en-us/library/hh831740

- Wdrożenie fizycznych kart inteligentnych może wymagać znaczących nakładów finansowych w nowe wyposażenie. Należy zauważyć, iż każdy komputer będzie wymagał czytnika kart inteligentnych (część z dostępnych na rynku komputerów może posiadać takie czytniki) i fizycznej karty inteligentnej dla każdego użytkownika. Dodatkowo wymagane jest posiadanie odpowiedniej ilości karta zapasowych, dla nowych użytkowników lub użytkowników, którzy utracili swoje karty poprzez zgubienie lub zniszczenie.
- Jeśli użytkownik utraci lub zapomni swojej karty, nie będzie wstanie się zalogować do systemu, co wpłynie negatywnie na jego wydajność, szczególnie podczas wdrożenia. Wirtualne karty inteligentne mogą zmniejszyć ten problem w przypadku logowanie się do witryn internetowych, ale należy pamiętać, iż karty wirtualne nie mogą być wykorzystane do interaktywnego logowania się użytkownika do systemu Windows.
- Karty inteligentne nie ochronią organizacji przed błędami ludzkimi wynikającymi ze słabej świadomości zagrożeń. Karty inteligentne nie są panaceum na problemy wynikające z faktu, zapisywania przez użytkowników swoich kodów PIN, a szczególnie na kartach. Karty mogą zostać skradzione i mogą stanowić podatność. Należy szczególnie zwrócić uwagę na dobre praktyki, które muszą stosować użytkownicy ze szczególnym uwzględnieniem ochrony kodów PIN oraz nie pozostawiania kart bez opieki.
- Wirtualne karty inteligentne wymagają modułu TPM w komputerze. W zależności od dostawcy komputera, narzędzia niezbędne do konfiguracji modułu TPM mogą wymagać ręcznych czynności konfiguracyjnych związanych z urządzeniem TPM. Takich jak włączenie TPM w BIOS'ie lub zainicjowanie modułu i ustalenia hasła administratora podczas inicjacji urządzenia, który może uniemożliwić proces automatycznego lub wykorzystującego automatyczne skrypty wdrożenia albo aktualizacji.

W celu uzyskania dodatkowych informacji należy zapoznać się dokumentacją The Secure Access Using Smart Cards Planning Guide[30] oraz Understanding and Evaluating Virtual Smart Cards[31].

## 3.12. Odświeżanie i przywracanie komputera do stanu pierwotnego

System Windows 8 oferuje dwa nowe sposoby na przywrócenie komputera do poprzedniego stanu z określonego poprzedniego punktu w czasie.

- **Przywróć swój komputer (ang. Reset your PC)** - Proces przywracania komputera uruchamia komputer w trybie Windows Recovery Environment (Windows RE), wykasowuje i formatuje partycje zawierające dane systemu Windows oraz dane użytkownika, instaluje świeżą kopię systemu Windows i na koniec restartuje komputer.
- **Odśwież swój komputer (ang. Refresh your PC)** - Proces odświeżania komputera uruchamia komputer w trybie Windows Recovery Environment (Windows RE), skanuje i zbiera (zabezpiecza) dane i pliki użytkownika, konfigurację ustawień i aplikacji Windows 8, następnie instaluje świeżą kopię systemu Windows i przywraca dane i pliki użytkownika, konfigurację ustawień i aplikacji Windows 8. I na koniec restartuje komputer.

Zastosowanie opcji odświeżania systemu może zachować ustawienia komputera, włączając w to: konfigurację sieci bezprzewodowych i połączeń mobilnych, ustawień mechanizmu szyfrowania BitLocker i BitLocker To Go, przypisanych liter dysków, personalizacji, takich jak tapeta.

[30] http://technet.microsoft.com/en-us/library/cc170941.aspx
[31] http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=29076

Administratorzy mogą utworzyć własny obraz odświeżania komputera zawierający popularne oprogramowanie, narzędzia lub odpowiednie sterowniki, które są wykorzystywane podczas procesu odświeżania lub przywracania komputera. Korzystając z opcji przywracania komputera po wykryciu zarażenia i obecności oprogramowania złośliwego, dostarczamy czysty komputer bez obecności oprogramowania złośliwego. Opcja odświeżania komputera wspomaga proces odtworzenia komputera po wykryciu ataku oprogramowania złośliwego.

W przypadku, kiedy wystąpi atak lub zarażenie komputera, za pomocą procesu odświeżania komputera będziemy wstanie odtworzyć dane z komputera lub przywrócić komputer do punktu stanu sprzed ataku.

Z kolei proces przywracania komputera wspomoże proces odtworzenia systemu operacyjnego komputera po ataku lub zarażeniu przez oprogramowanie złośliwe wspomoże przywrócić komputer do stanu niezainfekowanego. Proces przywracania nie odtworzy danych użytkownika, ale pozwoli upewnić się, że przywrócony komputer jest czysty i nie posiada niechcianego oprogramowania.

## 3.13. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na temat bezpieczeństwa systemu Windows 8 opublikowanych na stronach Microsoft.com

- Active Directory Certificate Services Overview[32].
- "Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment[33]": Knowledge Base article 891716.
- Impact of Artificial "Gummy" Fingers on Fingerprint Systems[34].
- Install the latest Windows Defender definition updates[35].
- Protecting you from malware.[36]
- IPsec[37].
- System Center 2012 Endpoint Protection[38]
- Getting Started with User Account Control on Windows Vista[39].
- Malicious Software Removal Tool[40].
- Malware Families Cleaned by the Malicious Software Removal Tool[41].
- Microsoft Security Compliance Manager[42].
- Privacy Statement for the Microsoft Error Reporting Service[43].

[32] http://technet.microsoft.com/en-us/library/hh831740

[33] http://support.microsoft.com/Default.aspx?kbid=891716
[34] http://cryptome.org/gummy.htm
[35] http://www.microsoft.com/security/portal/Definitions/HowToWD.aspx
[36] http://blogs.msdn.com/b/b8/archive/2011/09/15/protecting-you-from-malware.aspx
[37] http://go.microsoft.com/fwlink/?LinkId=69843
[38] http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx
[39] http://go.microsoft.com/fwlink/?linkid=84129
[40] http://go.microsoft.com/fwlink/?LinkId=51307
[41] http://www.microsoft.com/security/malwareremove/families.aspx
[42] http://go.microsoft.com/fwlink/?LinkId=113940
[43] http://go.microsoft.com/fwlink/?linkid=62936

- "The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows Vista, Windows Server 2003, Windows Server 2008, Windows XP, or Windows 2000": Knowledge Base article 890830.
- Windows Defender Privacy Policy.
- Windows Firewall.
- Windows Server Group Policy.
- Windows Server Update Services (WSUS).
- "Windows Vista Application Development Requirements for User Account Control Compatibility" article.
- Understanding and Configuring User Account Control in Windows Vista.
- User Account Control.
- Using Software Restriction Policies to Protect Against Unauthorized Software.

## 4. Ochrona wrażliwych danych

Firma Microsoft dostarczyła nowe i rozszerzone funkcje oraz usługi zapewniające organizacjom ochronę danych przechowywanych na komputerach klienckich wraz z mechanizmami zabezpieczenia ich przed ryzykiem kradzieży oraz ujawnienia danych.

W rozdziale tym zostaną omówione rekomendowane ustawienia, które zostały zaprojektowane w celu podwyższenia stopnia ochrony danych przechowywanych na komputerach klienckich pracujących po kontrolą systemu Windows 8 oraz Windows 8.1. Konfiguracja poszczególnych funkcji ochrony zależy od wymagań i poziomu zabezpieczeń stawianych własnemu środowisku informatycznemu. Rozdział ten dostarczy niezbędnych informacji w celu identyfikacji, zaprojektowania oraz dostosowania konfiguracji właściwej ochronny danych w organizacjach następujących funkcji i usług:

- Szyfrowanie dysków funkcją BitLocker
    - Ochrona plików przechowywanych na woluminie, na którym zainstalowany jest system Windows (dysk systemu operacyjnego) oraz stałych dyskach z danymi
    - Ochrona danych znajdujących się na dyskach wymiennych (zewnętrzne dyski danych lub dyski flash USB) z zastosowaniem funkcji BitLocker To Go.
- System szyfrowania plików (EFS)
- Usługi zarządzania prawami dostępu (RMS)
- Mechanizm instalacji i zarządzania urządzeniami w systemie Windows

W celu zapewnienia ochrony wrażliwych danych w organizacji możemy skorzystać z funkcji Bitlocker, EFS, RMS oraz mechanizmu instalacji i zarządzania urządzeniami. Każda z tych technologii spełnia określone zadania w różnych scenariuszach zastosowania. Zaprezentowane tutaj wbudowane mechanizmy ochrony danych powinny być częścią strategii bezpieczeństwa organizacji a ich stosowanie jest wysoce rekomendowane. Przedstawione w tabeli przykłady pokazują, w jakich scenariuszach poszczególne funkcje mogą być wykorzystane odnosząc się do najczęściej spotykanych konfiguracji w organizacjach.

| Scenariusz | BitLocker | EFS | RMS | Zarządzanie urządzeniami |
|---|---|---|---|---|
| Ochrona danych komputerów przenośnych | ☑ | ☑ | | ☑ |
| Ochrona danych serwera biura oddziału | ☑ | | | ☑ |
| Ochrona lokalnych plików i folderów użytkownika | | ☑ | | |
| Ochrona komputerów stacjonarnych | ☑ | ☑ | | ☑ |
| Ochrona danych dysków wymiennych | ☑ | | | ☑ |
| Ochrona plików i folderów współużytkowanych komputerów | | ☑ | | |
| Ochrona plików i folderów | | ☑ | | |

| | | | | |
|---|---|---|---|---|
| zdalnych | | | | |
| Ochrona administratora pracującego w niezaufanej sieci | | ☑ | | |
| Egzekwowanie zasad ochrony dokumentów zdalnych | | | ☑ | |
| Ochrona treści podczas przesyłania przez sieć | | | ☑ | |
| Ochrona treści podczas współpracy grupowej | | | ☑ | |
| Ochrona danych przed kradzieżą | ☑ | | | ☑ |

Tabela 4.1 - Porównanie mechanizmów ochrony danych stosowanych w systemie Windows 8.

Ustawienia bazowe konfiguracji zaprezentowano w narzędziu **Security Compliance Manager (SCM)** w arkuszach programu Excel, w których wskazano różne powierzchnie ataków dla wybranych produktów Microsoft. Skoroszyty zawierające ustawienia wybranych produktów dostępne są w sekcji **Attachments\Guides** po wybraniu i wskazaniu właściwego produktu w narzędziu SCM.

**Uwaga:** Dla każdego z obszarów wskazanych w tym rozdziale wraz z ustawieniami dla zasad grupowych są uwydatnione w domyślnej konfiguracji dla nowych instalacji systemu Windows 8. Zalecane lub rekomendowane ustawienia zasad grupowych są oznaczone za pomocą symbolu „‡”. Więcej informacji na temat podstawowych ustawień bazowych i ich wartości umieszczono w tabelach dokumentu „Windows 8 Security Baseline settings” dostępnych w narzędziu Security Compliance Manager[44] (SCM).

## 4.1. Szyfrowanie i ochrona dysków z zastosowaniem funkcji BitLocker

Szyfrowanie dysków funkcją BitLocker jest mechanizmem szyfrowania całych woluminów, a nie tylko poszczególnych plików, zapewniając ochronę danych przechowywanych na dyskach pracujących pod kontrolą systemu Windows 8 oraz Windows 8.1. Mechanizm ten zapewnia bezpieczeństwo danych również w przypadku, kiedy dysk zostanie wymontowany i zainstalowany w innym komputerze. Technologia BitLocker w systemie Windows 8 zapewnia ochronę danych znajdujących się na dyskach twardych komputerów użytkowników, włączając w to ochronę dysków wymiennych, pamięci przenośnych USB oraz dysków podłączonych poprzez interfejs IEEE 1394.

W momencie uruchomienia ochrony dysków systemu operacyjnego BitLocker chroni sekwencję rozruchu aż do momentu wprowadzenia właściwych i uprawnionych danych uwierzytelniających wymaganych przez mechanizm BitLocker. Funkcja BitLocker zezwala na zastosowanie pamięci flash USB do przechowywania kluczy deszyfrujących, ale najwyższy stopień bezpieczeństwa uzyskuje się przy wykorzystaniu modułu TPM 1.2 (ang. Trusted Platform Module), który zapewnia sprzętową ochronę kluczy szyfrujących i zapobiega atakom programowym na bezpieczeństwo i integralność danych przechowywanych na dyskach. Funkcja BitLocker może korzystać z modułu TPM do weryfikowania integralności składników biorących udział we wczesnej fazie uruchamiania oraz do weryfikowania danych konfiguracji rozruchu. Dzięki temu funkcja BitLocker umożliwia uzyskanie dostępu do zaszyfrowanego dysku tylko wtedy, gdy te składniki nie zostały naruszone, a zaszyfrowany dysk znajduje się w oryginalnym komputerze.

[44] http://go.microsoft.com/fwlink/?LinkId=156033

Usługa BitLocker w systemie Windows 8 oraz Windows 8.1 wprowadziła następujące nowe funkcjonalności w celu zwiększenia poziomu bezpieczeństwa:

- **Szyfrowanie tylko zajętego miejsce na dysku** – w systemie Windows 8, użytkownik może dokonać wyboru czy szyfrować tylko zajęte miejsce na dysku czy cały wolumin. Szyfrowanie tylko zajętego miejsca na dysku znacznie przyśpiesza proces szyfrowania.
- **Obsługa BitLocker - (ang. BitLocker provisioning)** - w systemie Windows 8, możliwe jest włączenie usługi BitLocker przed instalacją systemu. W przypadku wykorzystania opcji szyfrowania tylko zajętego miejsca na dysku, obsługa BitLocker staje się szybsza i stanowi nieprzerywany proces instalacji nowych komputerów. Jednakże, należy pamiętać, że po zakończeniu procesu instalacji nowego systemu bezpieczny klucz zostanie dodany do chronionego wolumenu.
- **Odblokowywanie funkcją BitLocker przez sieć (ang. Network unlock)** – włączona funkcja BitLocker w systemie Windows 8 wykorzystująca ochronę poprzez stosowanie modułu TPM+PIN, może uruchomić system w zaufanej kablowej sieci komputerowej bez wymagania wprowadzenie kodu PIN przez użytkownika. Funkcja odblokowywanie funkcją BitLocker przez sieć pozwala administratorom na uruchomienie zaszyfrowanego systemu i chronionego za pomocą modułu TPM+PIN w celu wykonania nienadzorowanego procesu aktualizacji lub zadań konserwacji. Funkcja ta wymaga, aby sprzęt kliencki zawierał sterownik Dynamic Host Configuration Protocol (DHCP) zaimplementowany w oprogramowaniu UEFI (Unified Extensible Firmware Interface).
- **Wsparcie dla systemu Windows dysków sprzętowo szyfrowanych** – w systemie Windows 8, Bitlocker dostarcza wsparcia dla mechanizmu Full Disk Encryption (FDE) wykorzystującego specjalne dyski zapewniające sprzętowe szyfrowanie dysków (Encrypted Hard Drive). Szyfrowane dyski sprzętowo mogą być wykorzystane do przeprowadzenia szyfrowania na poziomie bloków dysków. Operacje szyfrowania i deszyfrowania są przeprowadzane przez kontroler dysków, zmniejszając w ten sposób obciążenie procesora komputera.
- **Zmiana kodu PIN lub hasła przez standardowego użytkownika (ang. - Standard user PIN and password change)** – w systemie Windows 8 użytkownik nieposiadający uprawnień administracyjnych nie może wykonywać konfiguracji funkcji BitLocker. Jednakże, wprowadzona została możliwość zmiany kodu PIN lub hasła dla wolumenów zawierających system operacyjny lub dysków stałych. Funkcja ta włącza możliwość standardowym użytkownikom wyboru własnego kodu PIN lub hasła w celu łatwiejszego zapamiętania. Niemniej należy pamiętać, iż funkcja ta może narazić organizacje na ryzyko odgadnięcia przez atakującego hasła. Opcja ta może być kontrolowana przez zasady grupy.
- **Szyfrowanie urządzeń** – w Windows 8.1 BitLocker dostarcza funkcjonalność szyfrowania urządzeń bazujących na procesorach x86 oraz x64 wspierających technologię Connected Standby, czyli możliwość pracy urządzenia w trybie uśpienia (np. komputer będzie w stanie wzbudzić się co jakiś określony czas aby ściągnąć pocztę) – wcześniej było to dostępne tylko dla urządzeń z Windows RT
-

## 4.2. Tryby pracy BitLocker oraz zarządzanie układem TPM

Funkcja BitLocker zawiera kilka trybów pracy, które można skonfigurować i dostosować do własnych wymagań. Tryb pracy, który zostanie wybrany i zastosowany w dużym stopniu zależy od dostępności modułu TPM na chronionych komputerach oraz przyjętego stopnia ochrony, który ma zostać wyegzekwowany. Tryb pracy obejmuje stosowanie modułu TPM, numeru PIN oraz klucza uruchomienia (ang. startup key). Klucz uruchomienia jest plikiem wygenerowanym w sposób kryptograficzny i umieszczonym na oddzielnym nośniku pamięci flash USB.

Tryby pracy funkcji BitLocker:

- **Tylko moduł TPM**. Używanie weryfikacji Tylko moduł TPM nie wymaga żadnej interakcji z użytkownikiem w celu odszyfrowania i udostępnienia dysku, do startu systemu nie jest potrzebne hasło, numer PIN lub klucz uruchomienia. Jeśli weryfikacja przy użyciu modułu TPM powiedzie się, przebieg logowania jest z punktu widzenia użytkownika taki sam, jak podczas logowania standardowego. Jeśli brakuje modułu TPM lub został on zmieniony, lub moduł TPM wykryje zmiany w plikach startowych systemu operacyjnego o znaczeniu krytycznym, lub nastąpi próba uruchomienia dysku w innym komputerze, to funkcja BitLocker przejdzie do trybu odzyskiwania i do odzyskania dostępu do danych będzie potrzebne hasło odzyskiwania. Tryb ten zapewnia ochronę środowiska rozruchowego dla systemu Windows 8 poprzez moduł TPM. Sposób ten jest przykładem najsłabszej implementacji funkcji BitLocker z uwagi na fakt, iż nie wymaga dodatkowego uwierzytelnienia do uruchomienia systemu Windows.
- **Moduł TPM z kluczem uruchomienia**. Oprócz ochrony zapewnianej przez moduł TPM część klucza szyfrowania jest przechowywana na dysku flash USB. Dostępu do danych na zaszyfrowanym woluminie nie można uzyskać bez klucza uruchomienia. Tryb ten wymaga urządzenia USB zawierającego klucz uruchomienia podłączonego do komputera podczas procesu uruchomienia systemu Windows. Kiedy system nie odczyta poprawnie klucza startującego komputer przejdzie w tryb odzyskiwania (ang. Recovery mode). Tryb ten również zapewnia ochronę środowiska rozruchowego dla systemu Windows 8 poprzez moduł TPM.
- **Moduł TPM z kodem PIN**. Oprócz ochrony zapewnianej przez moduł TPM funkcja BitLocker wymaga od użytkownika wprowadzenia osobistego numeru identyfikacyjnego (PIN). Dostępu do danych na zaszyfrowanym woluminie nie można uzyskać bez podania kodu PIN. Dodatkowo można wymusić za pomocą zasad grup używanie hasła złożonego zamiast prostego numeru PIN. Jeśli użytkownik nie wprowadzi prawidłowego kodu PIN podczas uruchomienia systemu, to komputer przejdzie w tryb odzyskiwania. Tryb ten zapewnia ochronę środowiska rozruchowego dla systemu Windows 8 poprzez moduł TPM.
- **Moduł TPM z kluczem uruchomienia i kodem PIN**. Opcję tę można skonfigurować wyłącznie przy użyciu narzędzia wiersza polecenia **Manage-bde.exe** oraz zasad grupowych. Oprócz ochrony podstawowych składników, którą zapewnia sprzętowy moduł TPM, część klucza szyfrowania jest przechowywana na dysku flash USB, a w celu uwierzytelnienia użytkownika w module TPM jest wymagane podanie kodu PIN. Uzyskane w ten sposób uwierzytelnianie wieloczynnikowe gwarantuje, że nawet, jeśli klucz USB zostanie zgubiony lub skradziony, nie będzie można go użyć w celu uzyskania dostępu do dysku, ponieważ jest również wymagany poprawny numer PIN. Tryb ten zapewnia ochronę środowiska rozruchowego dla systemu

Windows 8 poprzez moduł TPM. Ustawienie tego trybu zalecane jest dla środowisk gdzie wymagany jest bardzo wysoki poziom bezpieczeństwa i zapewnia najwyższy stopnień ochrony danych w organizacji.

- **Tryb pracy funkcji BitLocker bez modułu TPM.** Tryb ten zapewnia pełne szyfrowanie całego dysku, ale nie zapewnia ochrony środowiska rozruchowego dla systemu Windows 8. To ustawienie zalecane jest dla komputerów nieposiadających sprzętowego modułu TPM. W celu ustawienia tego trybu pracy niezbędna jest konfiguracja ustawień zasad grupowych: **Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Dyski z systemem operacyjnym\Wymagaj dodatkowego uwierzytelniania przy uruchamianiu.**
  **(Computer Configuration\Administrative Templates\WindowsComponents\BitLocker Drive Encryption\Operating System Drives\Require Additional Authentication At Startup)**
  W przypadku uruchomienia trybu pracy bez modułu TPM niezbędne jest urządzenie pamięci flash USB z kluczem uruchomienia do startu systemu Windows.

Większość implementacji funkcji BitLocker przechowuje klucze szyfrujące w pamięci (bezpieczny magazyn danych) modułu TPM. W momencie włączenia i konfiguracji modułu TPM, system Windows 8 będzie korzystał z niewielkiej informacji (ziarna - ang. seed) dostarczanej do generatora liczb losowych systemu Windows (RNG- ang. Random Number Generator). System RNG odpowiada za generowanie kluczy kryptograficznych dla różnych aplikacji w systemie Windows. Przypadkowość kluczy kryptograficznych będzie znacznie lepsza w przypadku stosowania TPM niż w sposób wyłącznie programowy, w tym celu rekomendowane jest włączenie i skonfigurowanie sprzętowego modułu TPM w ustawieniach BIOS komputera.

Domyślnie w systemach Windows 8 generator liczb losowych (RNG) pobiera wartość startową z modułu TPM podczas startu systemu oraz następnie, co 40 minut. W systemie dostępne są trzy konfiguracje tego mechanizmu służące do kontroli tego ustawienia. Parametry domyślne są idealne dla większości scenariuszy zastosowań.

Ustawienie TPMBOOTENTROPY jest konfigurowalne przez mechanizm danych konfiguracji rozruchu (ang. Boot Configuration Data – BCD). W sytuacji, kiedy ustawienie to jest skonfigurowane na fałsz (ang. false), to mechanizm wyłącza pobieranie entropii z modułu TPM, dla komputerów z włączonym układem TPM. Wartość domyślna tego parametru ustawiona jest na prawdę (ang. True) podczas startu systemu a w trybie awaryjnym oraz trybie awaryjnym z obsługa sieci na fałsz. Więcej informacji na temat zarządzania ustawieniami przechowywanymi w BCD można przeczytać w dokumentach: Boot Configuration Data in Windows Vista[45] and BCDEdit Commands for Boot Environment[46].

Parametr opisujący częstotliwość odświeżania (ang. refresh interval) określa jak często (w minutach) entropia danych jest pobierana z układu TPM. W momencie, kiedy ustawienie to wskazuje na zero, entropia nie jest pobierana, w ten sposób, wartość ta nie wpływa na ilość danych (entropię) pobieranych podczas startu systemu. Należy zwrócić szczególna uwagę podczas zmiany tego parametru z uwagi na fakt, iż nawet najmniejsza zmiana tego parametru może wpłynąć na ustawienie „Mean Time To Failure" w poszczególnych implementacjach różnych dostawców układu TPM.

[45] http://go.microsoft.com/fwlink/?LinkId=93005
[46] http://go.microsoft.com/fwlink/?LinkId=113151

Wartość tego parametru przechowana jest gałęzi rejestru **HKey_Local_Machine**, jako wartość DWORD o nazwie **TpmRefreshEntropyIntervalInMinutes** i umieszczona w **\Software\Policies\Microsoft\Cryptography\RNG**, domyślną wartością tego ustawienia jest liczba 40 i konfigurowalna w zakresie od 0 do 40. Dodatkowo możemy skonfigurować liczbę milibitów (ang. millibits) ilości danych (entropię) na każdy bajt wychodzący z generatora liczb losowych układu TPM. Wartość tego parametru przechowana jest gałęzi rejestru **HKey_Local_Machine**, jako wartość DWORD o nazwie **TpmEntropyDensityInMillibitsPerByte** i umieszczona w **\System\CurrentControlSet\Control\Cryptography\RNG**, domyślną wartością tego ustawienia jest liczba 8000 i konfigurowalna w zakresie od 1 do 8000. Więcej informacji na temat technologii TPM oraz jej specyfikacji można uzyskać na stronie Trusted Computing Group[47].
Należy podkreślić, iż w przypadku niedostępności modułu TPM funkcja BitLocker może nadal zabezpieczać dane, ale nie można zapewnić ochrony integralności systemu oraz ochrony środowiska rozruchowego, można osiągnąć ten cel w następujących scenariuszach:

- Ochrona danych znajdujących się dyskach systemowych oraz dyskach stałych
- Ochrona danych przechowywanych na wymiennych dyskach danych z zastosowaniem funkcji BitLocker To Go
- Szczegóły wskazanych scenariuszu opisane są w dalszej części niniejszego rozdziału

**Uwaga:** Funkcja BitLocker umożliwia zabezpieczenie danych w systemie Windows Server 2008, ale scenariusz ten nie został opisany w niniejszym przewodniku.

**Uwaga:** Pomimo, że możliwe jest zapisywanie danych w programie Windows Virtual PC, jako wirtualne dyski (VHD) wewnątrz chronionego systemu plików przez mechanizm BitLocker, to nie ma możliwości wykorzystania chronionych przez funkcję BitLocker wirtualnych dysków (VHD) do uruchomienia systemu Windows z pliku VHD (native VHD boot) oraz nie ma możliwości uruchomienia funkcji BitLocker na wolumenach, które zawarte są wewnątrz plików VHD.

## 4.3. Ochrona danych znajdujących się dyskach systemowych oraz dyskach stałych

W tym scenariuszu zastosowanie funkcji BitLocker umożliwi ochronę wszystkich stałych dysków z danymi (wewnętrzne dyski twarde), które zawierają pliki systemu operacyjnego a także inne dane. Jest to zalecana konfiguracja w celu zapewnienia, iż wszystkie dane w systemie są chronione przez funkcję BitLocker.

**Ocena ryzyka**

Głównym zagrożeniem bezpieczeństwa jest utrata danych z komputerów przenośnych, które zostały utracone lub skradzione. Funkcja BitLocker została zaprojektowana właśnie w celu zmniejszenia tego zagrożenia. Sytuacja ta ma miejsce wtedy, kiedy atakujący uzyska fizyczny dostęp do niezabezpieczonego komputera, potencjalne konsekwencje takiego czynu obejmują następujące działania:

Atakujący może się zalogować do komputera z systemem Windows 8 i skopiować dane

[47] http://www.trustedcomputinggroup.org/

- Atakujący może uruchomić komputer z alternatywnego systemu operacyjnego w celu:
    - Przejrzenia listy plików
    - Skopiowania plików
    - Odczytu danych z plików hibernacji lub pliku stronicowania w celu odczytu informacji przechowywanych jawnym tekstem lub dokumentów związanych z uruchomionym procesem.
    - Odczytu danych z pliku hibernacji w celu ujawnienia i pozyskania kopii kluczy prywatnych przechowywanych w postaci tekstowej.

Nawet, jeśli pliki są w postaci zaszyfrowanej z wykorzystaniem systemu szyfrowania plików EFS, to istnieje zagrożenie, iż nieostrożny użytkownik systemu może przenieść lub skopiować pliki z zaszyfrowanego folderu do katalogu, na którym nie jest włączona funkcja EFS (np. katalogi tymczasowe lub ukryte), co może skutkować pozostawieniem kopii plików w postaci niezaszyfrowanej i dostępnej dla atakującego. Nieświadomi pracownicy działów IT mogą dopuścić się zaniedbania poprzez nieszyfrowanie katalogów ukrytych, w których mogą być przechowywane kopie plików wykonywanie przez aplikacje podczas normalnej pracy systemu i aplikacji. Istnieje również ryzyko operacyjne, w którym nieupoważnione osoby dokonają modyfikacji plików systemowych lub rozruchowych, które uniemożliwią normalną pracę systemu operacyjnego.

**Minimalizacja ryzyka**

W celu zmniejszenia zagrożenia związanego z powyższym ryzykiem, zaleca się skonfigurować komputery i włączyć funkcję BitLocker, która wykryje zmiany w plikach startowych systemu operacyjnego o znaczeniu krytycznym oraz zapewnia ochronę środowiska rozruchowego dla systemu Windows 8 wraz z wymuszeniem dodatkowego procesu uwierzytelnienia przed uruchomieniem systemu i uzyskania dostępu do w pełni zaszyfrowanego dysku. Co w rezultacie zapewni pełną ochronę systemu operacyjnego oraz zabezpieczy dane przed nieautoryzowanym dostępem.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Funkcja BitLocker stosowana na dyskach, na których zainstalowany jest system Windows (dysk systemu operacyjnego) oraz stałych dyskach z danymi (wewnętrzne dyski twarde) może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji „Ocena ryzyka”, jednak przed zastosowaniem funkcji BitLocker, ważne jest, aby wziąć pod uwagę następujące wymagania i najlepsze praktyki dla tej funkcji ochrony danych:

- W przypadku zastosowania optymalnej konfiguracji, płyta główna komputera powinna posiadać moduł TPM 1.2 lub nowszy, obsługiwać system BIOS zgodny z wytycznymi Trusted Computing Group. Zalecana konfiguracja wymaga stosowania kodu PIN nadanego przez użytkownika w celu odblokowania systemu. Dodatkowo, opcjonalnie warto zastosować klucz uruchomienia umieszczony na nośniku pamięci flash USB.
- Dysk twardy chronionego komputera powinien zawierać minimum 2 partycje: partycję z systemem operacyjnym i aktywna partycję systemową. Partycja systemowa to miejsce gdzie zostaną zainstalowane pliki systemu operacyjnego w postaci zaszyfrowanej a aktywna partycja systemowa w postaci niezaszyfrowanej musi posiadać rozmiar minimalny o wielkość 350 MB i jest przeznaczona na pliki umożlwiające start systemu. Domyślnie podczas instalacji systemu Windows 8, instalator systemu Windows tworzy automatycznie partycję

systemową, do której nie jest przypisana żadna litera dysku i jest ona ukryta przed użytkownikami. Jeśli system nie posiada oddzielnej aktywnej partycji systemowej, układ partycji zostanie zmodyfikowany w sposób automatyczny podczas włączania i inicjacji funkcji BitLocker.

- W przypadku, kiedy BitLocker będzie wymagał nośnika pamięci USB lub kodu PIN, konieczne jest ustalenie i wprowadzenie procedury, która przewiduje sytuacje awaryjne utraconych kluczy uruchomienia lub zapomnianych kodów PIN i jednocześnie pozwoli na ich odzyskanie przez użytkowników.
- Należy wziąć pod uwagę, iż funkcja BitLocker ma niewielki wpływ na wydajność komputera, przeważanie jest to niedogodność niezauważalna przez większość użytkowników. Jednakże, jeśli wydajność systemu jest krytycznym elementem systemu komputerowego warto sprawdzić w fazie testów przedwdrożeniowych czy BitLocker nie wpływa znacząco na wydajność pracy użytkownika.
- W zależności od producenta komputerów, narzędzia służące do zarządzania modułem TPM mogą wymagać ręcznej konfiguracji komputera lub ustawień BIOS, należy to wziąć pod uwagę podczas planowania w pełni zautomatyzowanego lub wykorzystującego skrypty procesu wdrożenia funkcjonalności BitLocker w organizacji, zarówno podczas nowych instalacji jak i aktualizacji z poprzednich systemów Windows.
- W celu zastosowania klucza USB z kluczem uruchomienia do odblokowania procedury startu i rozruchu systemu, BIOS komputera musi umożliwić odczyt danych z dysku USB w środowisku przed zainicjowaniem systemu operacyjnego.
- BitLocker może mieć wpływ na proces dystrybucji oprogramowania, który został zautomatyzowany i przewiduje zdalne instalacje lub aktualizacje aplikacji zaplanowane w nocy lub poza godzinami pracy, podczas kiedy wymagany jest ponowny rozruch komputera bez obecności użytkownika. Poniższe przykłady ilustrują opisaną sytuację:
    - Konfiguracja komputera przewiduje ochronę wykorzystująca moduł TPM wraz z kodem PIN lub zastosowanie modułu TPM wraz z kluczem uruchomienia na nośniku USB, a czynności zaplanowana jest na godzinę 2.00 w nocy. Kiedy proces wdrożenia aplikacji wymaga restartu komputera, to komputer nie zostanie poprawnie zrestartowany z uwagi na wymaganie wprowadzenia kodu PIN lub obecności klucza uruchomienia na nośniku pamięci USB.
    - Jeśli w organizacji wykorzystywana jest technologia Wake-on-LAN lub funkcja automatycznego uruchomienia komputera poprzez BIOS w celu wykonania czynności serwisowych, to takie komputery również nie zostaną automatycznie uruchomione z powodu zastosowania modułu TPM z dodatkowym elementem uwierzytelniającym w postaci czynności wprowadzenia kodu PIN lub braku obecności klucza uruchomienia na nośniku pamięci USB.
- Wszelkie aktualizacje oprogramowania układowego (ang. firmware) mogą wpłynąć niekorzystnie na komputery z włączoną funkcją BitLocker. Aktualizacja oprogramowania BIOS, może zostać wykryta przez BitLocker, jako modyfikacja środowiska, co w efekcie spowoduje, iż komputer przejdzie w tryb odzyskiwania (ang. Recovery mode). Jeśli funkcja BitLocker jest już włączona i zachodzi konieczność zaktualizowania systemu BIOS, należy tymczasowo wstrzymać działanie funkcji BitLocker przed zaktualizowaniem systemu BIOS, a następnie wznowić działanie funkcji BitLocker po zakończeniu aktualizacji.

- Chociaż jest mało prawdopodobne, że aktualizacje aplikacji mogą mieć wpływ na działanie komputerów z włączoną funkcją BitLocker, to należy zwrócić szczególna uwagę na wprowadzane zmiany do systemu przez aktualizacje a szczególnie na zmiany wprowadzone do menadżera rozruchu (ang. boot manager), które mogą spowodować błędy podczas rozruchu systemu i spowodują przejście komputera w tryb odzyskiwania. Przed przystąpieniem do instalacji lub aktualizacji aplikacji, które moją wpływ na funkcje rozruchu systemu Windows 8 zaleca się przetestowanie tych czynności na komputerze z włączoną funkcja BitLocker.
- Wszystkie kontrolery domenowe musza pracować pod systemem Windows Server 2003 z dodatkiem service pack 2 (SP2) lub wyższym.

**Uwaga:** Windows serwer 2003 wymaga rozszerzenia schematu usługi katalogowej (Active Directory) w celu poprawnej obsługi i przechowywania kopii zapasowej informacji odzyskiwania funkcji BitLocker w usługach domenowych w usłudze Active Directory (AD DS).

**Proces minimalizacji ryzyka**

Poniżej przedstawiono proces minimalizacji ryzyka w celu oszacowania i wdrożenia najlepszych praktyk konfiguracji funkcji BitLocker, aby zapewnić ochronę wrażliwych danych znajdujących się na komputerach klienckich zarządzanych w organizacji:

W celu minimalizacji ryzyka zaleca się zastosowanie czynności:

1. Sprawdzenie i przeprowadzenie testów technologii BitLocker
   **Uwaga:** W celu uzyskania dodatkowych informacji na temat BitLocker, należy zapoznać się z dokumentami: BitLocker Drive Encryption Deployment Guide for Windows 7[48] i Windows BitLocker Drive Encryption Design and Deployment Guides[49] umieszczonych na stronach witryny Microsoft TechNet
2. Oszacowanie potrzeby wdrożenia funkcji BitLocker w organizacji.
3. Sprawdzenie i oszacowanie niezbędnych wymagań do zastosowania ochrony BitLocker pod kątem sprzętu, oprogramowania oraz oprogramowania firmware.
4. Dokonanie identyfikacji i wskazanie komputerów, które wymagają zapewnienia ochrony przez funkcję BitLocker.
5. Dokonanie identyfikacji i oszacowania odpowiedniego poziomu ochrony wymaganego w organizacji, mając na uwadze możliwość zastosowania kodów PIN lub nośników pamięci USB z kluczem uruchomienia, biorąc pod uwagę, fakt, iż system nie uruchomi się poprawnie bez dodatkowych zabezpieczeń.
6. Instalacja niezbędnych sterowników w systemie testowym.
7. Wykorzystanie obiektów zasad grup (GPO) w celu skonfigurowania funkcji BitLocker w systemach testowych.
8. Po przeprowadzeniu testów należy wdrożyć funkcjonalność BitLocker w środowisku produkcyjnym.
9. Stosowanie zasad grup w celu kontrolowania opcji włączenia i zarządzania poprawną konfiguracją funkcji BitLocker.

[48] http://go.microsoft.com/fwlink/?LinkId=140286
[49] http://go.microsoft.com/fwlink/?LinkId=134201

## 4.4. Zastosowanie ustawień zasad grup do wdrożenia BitLocker w celu minimalizacji ryzyka

Poniżej przedstawione zostaną dwa szablony ustawień zasad grup, które zaleca się stosować do zarządzania konfiguracją funkcji BitLocker. Szablony te umożliwiają zarządzanie konfiguracją modułu TPM oddzielnie od reszty funkcji BitLocker. Poniższa tabela przedstawia ustawienia zasad grup dostępne dla funkcji BitLocker w szablonie **VolumeEncryption.admx**. Konfiguracja tych ustawień dostępna jest w następującej lokalizacji w narzędziu Edytor obiektów zasad grupy:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker**

**(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption)**

W systemie Windows 8 dostępne są trzy poziomy ustawień zasady grupowych uporządkowanych w ramach tej ścieżki:

- Dyski z systemem operacyjnym
- Stałe dyski danych
- Wymienne dyski danych

Na poziomie globalnym ustawień następujące ustawienia zasad grupowych są dostępne:

§ - Oznacza ustawienia zasad grupowych, które są nowością w Windows 8.

| Zasada | Poziom ważności | Opis | Domyślne ustawienie w systemie Windows 8 | Ustawienie zalecane przez Microsoft |
|---|---|---|---|---|
| Zapisuj informacje umożliwiające odzyskiwanie dla funkcji BitLocker w usługach domenowych w usłudze Active Directory (systemy Windows Server 2008 i Windows Vista) | | To ustawienie zasad umożliwia zarządzanie kopią zapasową informacji odzyskiwania szyfrowania dysków funkcją BitLocker w usługach domenowych w usłudze Active Directory (AD DS, Active Directory Domain Services) Ta zasada dotyczy tylko komputerów z systemem Windows Server 2008 lub Windows Vista. | Nie skonfigurowano | |
| Wybierz folder | Opcjonalny | To ustawienie zasad | Nie | Nie |

| | | | | |
|---|---|---|---|---|
| domyślny dla hasła odzyskiwania | | umożliwia określenie domyślnej ścieżki wyświetlanej w monicie Kreatora instalacji szyfrowania dysków funkcją BitLocker o wprowadzenie lokalizacji folderu, w którym ma zostać zapisane hasło odzyskiwania. | skonfigurowano | skonfigurowano |
| Określ, jak użytkownicy mogą odzyskiwać dyski chronione funkcją BitLocker (systemy Windows Server 2008 i Windows Vista) | | To ustawienie zasad umożliwia określenie, czy w Kreatorze instalacji szyfrowania dysków funkcją BitLocker będzie można wyświetlić i określić opcje odzyskiwania funkcji BitLocker. | Nie skonfigurowano | |
| Wybierz metodę szyfrowania dysków i siłę szyfrowania | Istotny | To ustawienie zasad umożliwia skonfigurowanie algorytmu i siły szyfrowania używanych przez szyfrowanie dysków funkcją BitLocker. Funkcja BitLocker będzie używać domyślnej metody szyfrowania — AES 128 | Nie skonfigurowano | Włączone AES 256 |
| § Podaj unikatowe identyfikatory dla organizacji | Opcjonalny | To ustawienie zasad umożliwia skojarzenie unikatowych identyfikatorów organizacyjnych z nowym dyskiem, dla którego włączono funkcję BitLocker. | Nie skonfigurowano | Nie skonfigurowano |
| Zapobiegaj zastępowaniu pamięci podczas ponownego uruchamiania komputera | Opcjonalny | To ustawienie zasad steruje wydajnością ponownego uruchamiania komputera przy narażeniu na ryzyko ujawnienia tajnych kluczy funkcji | Nie skonfigurowano | Nie skonfigurowano |

| | | | | |
|---|---|---|---|---|
| | | BitLocker. | | |
| § Sprawdzaj zgodność użycia certyfikatu karty inteligentnej z regułami | Opcjonalny | To ustawienie zasad umożliwia skojarzenie identyfikatora obiektu pochodzącego z certyfikatu karty inteligentnej z dyskiem chronionym funkcją BitLocker. | Nie skonfigurowano | Nie skonfigurowano |

Tabela 4.4.1 Ustawienia globalne szyfrowania dysków funkcją BitLocker

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

Tabela poniżej przedstawia ustawienia zasad grupowych dostępne dla modułu TPM w szablonie **TPM.admx**. Konfiguracja tych ustawień dostępna jest w następującej lokalizacji w narzędziu Edytor obiektów zasad grupy:

**Konfiguracja komputera\Szablony administracyjne\System\Usługi modułu TPM**

**(Computer Configuration\Administrative Templates\System\Trusted Platform Module Services)**

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Włącz tworzenie kopii zapasowej modułu TPM w usługach domenowych Active Directory | To ustawienie zasad umożliwia zarządzanie kopiami zapasowymi informacji o właścicielu zgodnego sprzętowego modułu zabezpieczającego TPM (Trusted Platform Module) w usługach domenowych usługi Active Directory (AD DS). | Nie skonfigurowano |
| Konfigurowanie listy blokowanych poleceń modułu TPM | To ustawienie zasad umożliwia zarządzanie listą zasad grupy poleceń modułu TPM (Trusted Platform Module) blokowanych w systemie Windows. | Nie skonfigurowano |
| Ignorowanie listy domyślnej blokowanych poleceń modułu TPM | To ustawienie zasad umożliwia wymuszanie lub ignorowanie domyślnej listy poleceń modułu TPM (Trusted Platform Module) zablokowanych na komputerze. | Nie skonfigurowano |
| Ignorowanie listy lokalnej blokowanych poleceń modułu TPM | To ustawienie zasad umożliwia wymuszanie lub ignorowanie lokalnej listy poleceń modułu TPM (Trusted Platform Module) zablokowanych na komputerze. | Nie skonfigurowano |

Tabela 4.4.2 Ustawienia modułu Trusted Platform Module

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

**Dostępne opcje dla ustawień: Stałe dyski danych**

Ustawienia charakterystyczne dla dysków stałych (wewnętrzne dyski twarde) zawierających dane użytkownika lub aplikacji, ale nie są to dyski, na których zainstalowany jest system Windows (dysk systemu operacyjnego) zawarte są w następującej lokalizacji w Edytorze obiektów zasad grupy:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Stałe dyski danych**

**(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives)**

Poniższa tabela przedstawia ustawienia zasad grupowych, które są dostępne dla funkcji BitLocker w szablonie **VolumeEncryption.admx**. Na poziomie **Stałe dyski danych** następujące ustawienia zasad grupowych są dostępne:

§ - Oznacza ustawienia zasad grupowych, które są nowością w Windows 8.

| Zasada | Poziom ważności | Opis | Domyślne ustawienie w systemie Windows 8 | Ustawienie zalecane przez Microsoft |
|---|---|---|---|---|
| §Wymuś typ szyfrowania dysków na stałych dyskach twardych | Istotny | To ustawienie zasad umożliwia skonfigurowanie typu szyfrowania używanego przez szyfrowanie dysków funkcją BitLocker. Jest ono stosowane po włączeniu funkcji BitLocker. Wybranie opcji pełnego szyfrowania powoduje szyfrowanie całego dysku po włączeniu funkcji BitLocker. Wybranie opcji szyfrowania tylko zajętego miejsca powoduje po włączeniu funkcji BitLocker szyfrowanie tylko tej części dysku, na której są przechowywane dane. | Nie skonfigurowano | Nie skonfigurowano |

| | | | | |
|---|---|---|---|---|
| Konfiguruj użycie kart inteligentnych na stałych dyskach danych | Krytyczny | To ustawienie zasad umożliwia określenie, czy można używać kart inteligentnych do uwierzytelniania dostępu użytkownika do stałych dysków danych w komputerze, które są chronione funkcją BitLocker. | Nie skonfigurowano | Włączone Wymagaj użycia kart inteligentnych na stałych dyskach twardych |
| Odmawiaj dostępu do zapisu do dysków stałych niechronionych funkcją BitLocker | Istotny | To ustawienie zasad określa, czy ochrona funkcją BitLocker jest wymagana, aby komputer umożliwiał zapisywanie na stałych dyskach danych. To ustawienie zasad jest stosowane po włączeniu funkcji BitLocker. | Nie skonfigurowano | Nie skonfigurowano |
| Zezwalaj na dostęp do stałych dysków danych chronionych funkcją BitLocker ze starszych wersji systemu Windows | Krytyczny | To ustawienie zasad określa, czy stałe dyski danych sformatowane za pomocą systemu plików FAT można odblokowywać i przeglądać na komputerach z systemem operacyjnym Windows Server 2008, Windows Vista, Windows XP z dodatkiem Service Pack 3 (SP3) lub Windows XP z dodatkiem Service Pack 2 (SP2). | Nie skonfigurowano | Wyłączone |
| Konfiguruj używanie haseł dla stałych dysków danych | Istotny | To ustawienie zasad określa, czy do odblokowania stałych dysków z danymi chronionych funkcją BitLocker jest wymagane hasło. Jeśli zostanie wybrana opcja zezwalania na używanie hasła, będzie można wymagać używania hasła, wymuszać | Nie skonfigurowano | Wyłączone |

| | | | | |
|---|---|---|---|---|
| | | przestrzeganie wymagań dotyczących złożoności hasła oraz skonfigurować minimalną długość hasła. | | |
| Określ, jak mogą być odzyskiwane dyski stałe chronione funkcją BitLocker | Krytyczny | To ustawienie zasad umożliwia określenie, w jaki sposób będą odzyskiwane stałe dyski danych chronione funkcją BitLocker w przypadku braku wymaganych poświadczeń. | Nie skonfigurowano | Włączone<br><br>Zezwalaj na używanie agenta odzyskiwania danych<br><br>Zezwalaj na używanie 48-cyfrowego hasła odzyskiwania<br><br>Zezwalaj na używanie 256-bitowego klucza odzyskiwania<br><br>Zapisz informacje odzyskiwania funkcji BitLocker w usługach AD DS |

Tabela 4.4.3 Ustawienia Stałe dyski danych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

**Dostępne opcje dla ustawień: Dyski z systemem operacyjnym**

Ustawienia charakterystyczne dla woluminów, na których zainstalowany jest system Windows (dysk systemu operacyjnego) zawarte są w następującej lokalizacji w Edytorze obiektów zasad grupy:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Dyski z systemem operacyjnym**

**(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives)**

Poniższa tabela przedstawia ustawienia zasad grupowych, które są dostępne dla funkcji BitLocker w szablonie **VolumeEncryption.admx**. Na poziomie **Dyski z systemem operacyjnym** następujące ustawienia zasad grupowych są dostępne:

§ - Oznacza ustawienia zasad grupowych, które są nowością w Windows 8.

| Zasada | Poziom ważności | Opis | Domyślne ustawienie w systemie Windows 8 | Ustawienie zalecane przez Microsoft |
|---|---|---|---|---|
| § Wymuś typ szyfrowania dysków na dyskach z systemem operacyjnym | | To ustawienie zasad umożliwia skonfigurowanie typu szyfrowania używanego przez szyfrowanie dysków funkcją BitLocker. Jest ono stosowane po włączeniu funkcji BitLocker. Jeśli dysk został już zaszyfrowany lub trwa proces szyfrowania, zmiana typu szyfrowania nie przyniesie efektu. Wybranie opcji pełnego szyfrowania powoduje szyfrowanie całego dysku po włączeniu funkcji BitLocker. Wybranie opcji szyfrowania tylko zajętego miejsca powoduje po włączeniu funkcji BitLocker szyfrowanie tylko tej części dysku, na której są przechowywane dane. | Nie skonfigurowano | Nie skonfigurowano |
| Wymagaj dodatkowego uwierzytelniania przy uruchamianiu | Krytyczny | To ustawienie zasad umożliwia określenie, czy funkcja BitLocker będzie wymagać dodatkowego uwierzytelniania przy każdym uruchomieniu komputera i czy funkcja BitLocker ma być używana wraz z modułem TPM, czy | Nie skonfigurowano | Włączone<br><br>Konfiguruj uruchomienia modułu TPM: Nie zezwalaj na używanie modułu TPM<br><br>Konfiguruj numer PIN |

| | | | | |
|---|---|---|---|---|
| | | bez niego. | | uruchomienia modułu TPM: Wymagaj startowego kodu PIN z modułem TPM<br><br>Nie zezwalają na używanie klucza uruchomienia z modułem TPM<br><br>Nie zezwalaj na używania klucza i numeru PIN uruchomienia z modułem TPM |
| Wymagaj dodatkowego uwierzytelniania przy uruchamianiu (systemy Windows Server 2008 i Windows Vista) | | To ustawienie zasad umożliwia określenie, czy Kreator instalacji szyfrowania dysków funkcją BitLocker będzie mieć możliwość skonfigurowania dodatkowej metody uwierzytelniania, której użycie będzie wymagane przy każdym uruchomieniu komputera. | Nie skonfigurowano | |
| Zezwalaj na używanie rozszerzonych numerów PIN przy uruchamianiu | Istotny | To ustawienie zasad umożliwia określenie, czy rozszerzone numery PIN uruchomienia będą używane z funkcją BitLocker. | Nie skonfigurowano | Włączone |
| Konfiguruj minimalną długość numeru PIN uruchomienia | Krytyczny | To ustawienie zasad umożliwia skonfigurowanie minimalnej długości numeru PIN uruchomienia modułu TPM. To ustawienie zasad jest stosowane po włączeniu funkcji BitLocker. Minimalna długość numeru PIN | Nie skonfigurowano | Włączone<br><br>Minimalna liczba znaków: 7<br>Włączone |

| | | | | |
|---|---|---|---|---|
| | | uruchomienia to 4 cyfry, a maksymalna to 20 cyfr. | | |
| Określ, jak mogą być odzyskiwane dyski z systemem operacyjnym chronione funkcją BitLocker | Krytyczny | To ustawienie zasad umożliwia określenie, w jaki sposób będą odzyskiwane dyski z systemem operacyjnym chronione funkcją BitLocker przy braku wymaganych informacji o kluczu uruchomienia. | Nie skonfigurowano | Włączone<br><br>Zezwalaj na używanie 48-cyfrowego hasła odzyskiwania<br><br>Nie zezwalaj na używanie 256-bitowego klucza odzyskiwania<br><br>Usuń opcje odzyskiwania z Kreatora instalacji funkcji BitLocker<br><br>Zapisz informacje odzyskiwania funkcji BiLocker w usługach AD DS. dla dysków z systemem operacyjnym<br><br>Konfiguruj magazyn informacji odzyskiwania funkcji BitLocker w usługach AS DS.<br>Przechowuj hasła odzyskiwania i pakiety kluczy<br><br>Nie włączaj funkcji BitLocker, dopóki informacje odzyskowania dla dysków z systemem |

| | | | | |
|---|---|---|---|---|
| | | | | operacyjnym nie będą przechowywane w usługach AD DS. |
| Konfiguruj profil sprawdzania poprawności platformy modułu TPM (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008R2) | Istotny | To ustawienie zasad umożliwia skonfigurowanie sposobu zabezpieczenia klucza szyfrowania funkcji BitLocker przez zabezpieczenia sprzętowe modułu TPM. To ustawienie zasad nie jest stosowane, gdy komputer nie ma zgodnego modułu TPM ani gdy funkcja BitLocker została już włączona z ochroną za pomocą modułu TPM. | Nie skonfigurowano | Nie skonfigurowano |

Tabela 4.4.4 Ustawienia dyski z systemem operacyjnym

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

Polityka bezpieczeństwa powinna skutecznie wspierać procedury dotyczące haseł i procedury zarządzania kluczami stosowane dla funkcji BitLocker. Polityka ta powinna być na tyle wszechstronna, aby wystarczająco zabezpieczyć informacje, i jednocześnie nie utrudniać wsparcia normalnej pracy funkcji BitLocker. Poniższa lista zawiera przykłady takich zasad:

- Zalecane jest wymaganie stosowania kopii zapasowej informacji odzyskiwania szyfrowania dysków funkcją BitLocker w usługach domenowych w usłudze Active Directory
- Zalecane jest wymaganie stosowania kopii zapasowej informacji o właścicielu zgodnego sprzętowego modułu zabezpieczającego TPM (Trusted Platform Module) w usługach domenowych usługi Active Directory (AD DS).
- Zalecane jest stosowanie kluczy odzyskiwania danych oraz haseł odzyskiwania, jako metody dostępu do zaszyfrowanych danych na wypadek awarii.
- W przypadku korzystania z modułu TPM w połączeniu z numerem PIN lub nośnikiem USB zawierającym klucz uruchomienia, należy zmieniać hasła i numery PIN w regularnych odstępach czasu.
- Dla komputerów z włączonym i skonfigurowanym modułem TPM, zalecane jest założenie hasła administratora dla BIOS w celu zapobiegania modyfikacji ustawień BIOS przez nieupoważnione osoby.

- Zalecane jest stosowanie procedur, które zabraniają przechowywania nośników pamięci USB zawierających klucz uruchomienia wraz komputerem ( np. wspólna torba, czy pozostawienie klucza USB w pobliżu komputera)
- Zalecane jest stosowanie bezpiecznej centralnej lokalizacji do przechowywania kluczy odzyskiwania BitLocker w przypadku odzyskiwania danych po awarii.
- Zalecane jest przechowywanie kopii materiałów zawierających informacje niezbędne do odzyskiwania danych zaszyfrowanych w bezpiecznym miejscu poza główną lokalizacją organizacji.

Dodatkowym narzędziem wspomagającym funkcję BitLocker jest MBAM (ang. BitLocker Administration and Monitoring). Narzędzie to pozwala na łatwiejsze wdrażanie i odzyskiwaniu kluczy, centralizację zapewniania dostępu, monitorowanie i raportowanie stanu szyfrowania dysków stałych i wymiennych oraz minimalizacji kosztów obsługi. MBAM jest cześcią częścią pakietu Microsoft Desktop Optimization Pack dla Software Assurance[50]. Więcej informacji na temat MBAM można uzyskać odwiedzając stronę dokumentacji produktu MBAM[51].

## 4.5. Ochrona danych przechowywanych na wymiennych dyskach danych z zastosowaniem funkcji BitLocker To Go

Funkcja BitLocker To Go dostępna jest tylko w edycjach Professional i Enterprise systemów Windows 8. Na komputerach pracujących pod kontrolą systemów operacyjnych Windows 8 możliwe jest skonfigurowanie urządzeń USB, tak, aby wspierały funkcję BitLocker To Go. Pozostałe edycje systemu Windows 8, mogą odczytać dane z zaszyfrowanego dysku USB i zapisać dane poza tym dyskiem USB, ale nie mogą skonfigurować nowych urządzeń USB do obsługi funkcji BitLocker To Go. Funkcja BitLocker To Go pozwala na szyfrowanie dysków przenośnych i umożliwia korzystanie z tych urządzeń na innych komputerach, pod warunkiem posiadania odpowiedniego hasła. W tym scenariuszu możliwe jest zastosowanie BitLocker To Go w celu ochrony danych na wymiennych dyskach, takich jak zewnętrzne dyski IEEE 1394, karty pamięci, lub pamięci flash USB. Funkcja BitLocker To Go pomaga organizacjom na zabezpieczenie danych przechowywanych na tych nośnikach przed nieautoryzowanym dostępem nawet, jeśli nośnik zostanie zgubiony lub skradziony.

**Ocena ryzyka**

Przenośne nośniki danych stanowią istotne i kluczowe zagrożenie dla ważnych i wrażliwych danych w organizacji. Urządzenia te szybko stały się powszechne z uwagi na cenę i prostotę stosowania umożliwiając jednocześnie możliwość kopiowania i przenoszenia bardzo dużych ilości danych w bardzo krótkim czasie. Dodatkowo komputery przenośne i urządzenia pamięci flash USB są często narażone na zagrożenia związane z utratą i kradzieżą podczas ich przewożenia. Scenariusze te powodują, że dane wrażliwe mogą trafić do rąk niepowołanych osób i na razić organizację na ogromne straty.

**Minimalizacja Ryzyka**

W celu zmniejszenia zagrożenia związanego z powyższym ryzykiem, organizacje stosują różne ograniczenia związane z zakazem stosowania urządzeń, wyłączaniem portów i urządzeń USB oraz

[50] http://www.microsoft.com/pl-pl/windows/enterprise/products-and-technologies/mdop/mbam.aspx
[51] http://onlinehelp.microsoft.com/en-us/mdop/gg703313.aspx

IEEE 1394, a także konfigurowanie komputerów chroniąc sekwencję startową w taki sposób, że system będzie się uruchamiać tylko, gdy będzie to autoryzowany start wymagający dodatkowego uwierzytelnienia. Ponadto, podejmowane są kroki w celu zapewnienia ochrony plików systemu operacyjnego i plików danych. BitLocker To Go zapewnia skuteczną warstwę ochronną, co oznacza, że nawet, jeśli atakujący uzyska fizyczny dostęp do dysku, to taka sytuacja nie musi jednoznacznie oznaczać, że atakujący ma dostęp do danych zapisanych na dysku. Korzystając z zasad grupowych, organizacje mogą wymusić, aby dyski wymienne korzystały z funkcji BitLocker To Go, przed tym zanim dane zostaną skopiowane na urządzenie, wszystko po to, aby chronić dysk przed nieautoryzowanym dostępem.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

BitLocker To Go może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji „Ocena ryzyka", jednak przed zastosowaniem funkcji BitLocker na wymiennych dyskach danych, ważne jest, aby wziąć pod uwagę następujące wymagania i najlepsze praktyki dla tej funkcji ochrony danych:

- Funkcja BitLocker To Go nie wymaga modułu TPM.
- Dyski wymienne zaszyfrowane przy pomocy BitLocker To Go można skonfigurować tak, aby wymagały podania hasła lub zastosowania karty inteligentnej z odpowiednim certyfikatem w celu dostępu do danych. W przypadku zastosowania kart inteligentnych należy pamiętać o wyposażeniu komputerów w odpowiednie czytniki kart inteligentnych, na których będą odczytywane dane z nośników wymiennych.
- Funkcja BitLocker ma niewielki wpływ na wydajność komputera, przeważanie jest to niedogodność niezauważalna przez większość użytkowników. Jednakże, jeśli wydajność systemu jest krytycznym elementem systemu komputerowego warto sprawdzić w fazie testów przedwdrożeniowych czy BitLocker nie wpływa znacząco na wydajność pracy użytkownika.
- Należy pamiętać, że dyski mogą być dostępne, jako urządzenia tylko do odczytu w komputerach z systemem Windows XP lub Windows Vista. Użytkownicy starszych wersji systemu Windows będą widzieć drugą partycję na urządzeniu, która zazwyczaj jest ukryta w systemach Windows 8. Funkcjonalność ta jest znana, jako dysk odnajdywalny (ang. discovery drive), dysk ten zawiera aplikację BitLocker To Go Reader. Użytkownicy mogą odblokować zaszyfrowany dysk za pomocą tej aplikacji poprzez podanie hasła lub hasła odzyskiwania. Możliwe jest również skonfigurowanie zasad grupowych **Zezwalaj na dostęp do wymiennych dysków danych chronionych funkcją BitLocker ze starszych wersji systemu Windows** w celu kontroli czy dysk odnajdywalny jest utworzony i czy na nim zostanie umieszczona aplikacja BitLocker To Go podczas włączenia obsługi ochrony BitLocker dla dysku wymiennego, więcej informacji na ten temat można przeczytać w dokumencie Best Practices for BitLocker in Windows 7[52].
- Wszystkie kontrolery domenowe w domenie muszą pracować pod kontrolą systemu Windows Server 2003 SP2 lub wyższy.
  **Uwaga:** Windows serwer 2003 wymaga rozszerzenia schematu usługi katalogowej (Active Directory) w celu poprawnej obsługi i przechowywania kopii zapasowej informacji odzyskiwania funkcji BitLocker w usługach domenowych w usłudze Active Directory (AD DS).

[52] http://technet.microsoft.com/en-us/library/dd875532(WS.10).aspx

**Proces minimalizacji ryzyka**

Poniżej przedstawiono proces minimalizacji ryzyka w celu oszacowania i wdrożenia najlepszych praktyk konfiguracji funkcji BitLocker, aby zapewnić ochronę wrażliwych danych przechowywanych na wymiennych dyskach danych w komputerach klienckich zarządzanych w organizacji:

W celu minimalizacji ryzyka zaleca się stosować czynności:

1. Sprawdzenie i przeprowadzenie testów technologii BitLocker To Go
   **Uwaga:** W celu uzyskania dodatkowych informacji na temat BitLocker, należy zapoznać się z dokumentami: BitLocker Drive Encryption Deployment Guide for Windows 7[53] i Windows BitLocker Drive Encryption Design and Deployment Guides[54] umieszczonych na stronach witryny Microsoft TechNet
2. Oszacowanie potrzeby wdrożenia funkcji BitLocker To Go na wymiennych dyskach danych w organizacji.
3. Sprawdzenie i oszacowanie niezbędnych wymagań do zastosowania ochrony BitLocker To Go na wymiennych dyskach danych pod kątem sprzętu i oprogramowania.
4. Dokonanie identyfikacji i wskazanie komputerów, które wymagają zapewnienia ochrony przez funkcję BitLocker To Go na wymiennych dyskach danych.
5. Przeprowadzenie niezbędnych testów urządzeń wymiennych dysków włączając w to wszelkie nośniki pamięci flash USB.
6. Wykorzystanie obiektów zasad grupowych (GPO) w celu skonfigurowania funkcji BitLocker na wymiennych dyskach w systemach testowych.
7. Przeszkolenie użytkowników w zakresie prawidłowego użytkowania funkcji BitLocker To Go na dyskach wymiennych w ich własnym środowisku.
8. Po przeprowadzeniu testów należy wdrożyć funkcjonalność BitLocker na wymiennych dyskach danych w środowisku produkcyjnym.

W celu wyłączenia ochrony BitLocker na dyskach wymiennych należy skorzystać z opcji **Szyfrowanie dysków funkcją BitLocker** dostępną w **Panelu Sterowania**.

## 4.6. Zastosowanie ustawień zasad grup do wdrożenia BitLocker To Go w celu minimalizacji ryzyka

Poniższa tabela przedstawia ustawienia zasad grup dostępne dla funkcji BitLocker To Go w szablonie **VolumeEncryption.admx**. Konfiguracja tych ustawień dostępna jest w następującej lokalizacji w narzędziu Edytor obiektów zasad grupy:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Wymienne dyski danych**

**(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives)**

Na poziomie globalnym ustawień następujące ustawienia zasad grupowych są dostępne:

[53] http://go.microsoft.com/fwlink/?LinkId=140286
[54] http://go.microsoft.com/fwlink/?LinkId=134201

§ - Oznacza ustawienia zasad grupowych, które są nowością w Windows 8.

| Zasada | Poziom ważności | Opis | Domyślne ustawienie w systemie Windows 8 | Ustawienie zalecane przez Microsoft |
|---|---|---|---|---|
| § Wymuś typ szyfrowania dysków na wymiennych dyskach danych | Istotny | To ustawienie zasad umożliwia skonfigurowanie typu szyfrowania używanego przez szyfrowanie dysków funkcją BitLocker. Jest ono stosowane po włączeniu funkcji BitLocker. Jeśli dysk został już zaszyfrowany lub trwa proces szyfrowania, zmiana typu szyfrowania nie przyniesie efektu. Wybranie opcji pełnego szyfrowania powoduje szyfrowanie całego dysku po włączeniu funkcji BitLocker. Wybranie opcji szyfrowania tylko zajętego miejsca powoduje po włączeniu funkcji BitLocker szyfrowanie tylko tej części dysku, na której są przechowywane dane. | Nie skonfigurowano | Nie skonfigurowano |
| Kontroluj użycie funkcji BitLocker na dyskach wymiennych | Istotny | To ustawienie zasad kontroluje użycie funkcji BitLocker na wymiennych dyskach danych. | Nie skonfigurowano | Nie skonfigurowano |
| Konfiguruj użycie kart inteligentnych na wymiennych dyskach danych | Krytyczny | To ustawienie zasad umożliwia określenie, czy można używać kart inteligentnych do uwierzytelniania dostępu użytkownika do wymiennych dysków danych w komputerze, które są | Nie skonfigurowano | Włączone<br><br>Wymagaj użycia kart inteligentnych na wymiennych dyskach danych |

| | | | | |
|---|---|---|---|---|
| | | chronione funkcją BitLocker. | | |
| Odmawiaj dostępu do zapisu do dysków wymiennych niechronionych funkcją BitLocker | Istotny | To ustawienie zasad określa, czy ochrona funkcją BitLocker jest wymagana, aby komputer umożliwiał zapisywanie danych na wymiennym dysku danych. | Nie skonfigurowano | Włączone<br><br>Nie zezwalaj na dostęp do zapisu do urządzeń skonfigurowanych w innej organizacji |
| Zezwalaj na dostęp do wymiennych dysków danych chronionych funkcją BitLocker ze starszych wersji systemu Windows | Istotny | To ustawienie zasad określa, czy wymienne dyski danych sformatowane za pomocą systemu plików FAT można odblokowywać i przeglądać na komputerach z systemem operacyjnym Windows Server 2008, Windows Vista, Windows XP z dodatkiem Service Pack 3 (SP3) lub Windows XP z dodatkiem Service Pack 2 (SP2). | Nie skonfigurowano | Wyłączone |
| Konfiguruj użycie haseł dla wymiennych dysków danych | Istotny | To ustawienie zasad określa, czy do odblokowania wymiennych dysków z danymi chronionych funkcją BitLocker jest wymagane hasło. Jeśli zostanie wybrana opcja zezwalania na używanie hasła, będzie można wymagać używania hasła, wymuszać przestrzeganie wymagań dotyczących złożoności hasła oraz skonfigurować jego minimalną długość. | Nie skonfigurowano | Wyłączone |
| Określ, jak mogą być odzyskiwane dyski wymienne chronione | Krytyczny | To ustawienie zasad umożliwia określenie, w jaki sposób będą | Nie skonfigurowano | Włączone<br><br>Zezwalaj na |

| | | | | |
|---|---|---|---|---|
| funkcją BitLocker | | odzyskiwane wymienne dyski danych chronione funkcją BitLocker w przypadku braku wymaganych poświadczeń. | | używanie agenta odzyskiwania danych<br><br>Nie zezwalaj na używanie 48-cyfrowego hasła odzyskiwania<br><br>Nie zezwalają na używanie 256-bitowego klucza odzyskiwania<br><br>Usuń opcje odzyskiwania z Kreatora instalacji funkcji bitlocker<br><br>Wykonaj kopie zapasowe haseł odzyskiwania i pakietów kluczy |

Tabela 4.6.1 Ustawienia funkcji BitLocker dla Wymienne dyski danych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

## 4.7. BitLocker a Connected StandBy

Szyfrowanie urządzenia pozwala ochronić dane na komputerze użytkownika. Pozwala na blokowanie dostępu do plików poprzez np. fizyczne wyjęcie dysku z komputera i instalację w innym urządzeniu. Szyfrowanie urządzenia chroni dysk systemu operacyjnego oraz pozostałe dyski za pomocą AES-128. Szyfrowanie to może być uzyte z kontem domenowym oraz kontem Microsoft. Aby możliwe było uruchomienie szyfrowania urządzeń system musi spełniać technologie Connected Standby i spełniać wymagania Windows Hardware Certification Kit (HCK).

Wymagania są dostępne w następujących sekcjach:

**System.Fundamentals.Security.DeviceEncryption** – Ogólne wymagania do szyfrowania urządzeń.

**System.Fundamentals** – Wymagania systemów dla Connected Standby.

**System.Fundamentals.Firmware.CS.UEFISecureBoot.ConnectedStandby** - Wymagania dla TPM 2.0 oraz Secure Boot systemów z technologią Connected StandBy.

W przeciwieństwie do standardowego BitLocker'a szyfrowanie urządzenia jest włączone automatycznie, dlatego też urządzenie jest zawsze chronione.

**Włączenie lub wyłączenie szyfrowania urządzenia.**

Po wykonaniu czystej instalacji Windows 8.1 szyfrowanie urządzenia jest włączone automatycznie. Jeśli system był aktualizowany do wersji 8.1 możliwe jest włączenie szyfrowania urządzenia używając opcji PC Info (opcja dostępna w ustawieniach komputera).

**Wyłączenie automatycznego szyfrowania**

Jeśli podczas instalacji nie chcemy automatycznie chronić systemu szyfrowaniem urządzenia to należy przygotować plik unattend z następującymi ustawieniami rejestru:

Ścieżka: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BitLocker

Wartość: PreventDeviceEncryption równe True (1)

Typw: REG_DWORD

**Konflikty z ustawieniami Group Policy**

Szyfrowanie urządzenia jest elementem ustawień BitLocker'a w Group Policy. Jednak standardowe ustawienia mogą kolidować z ustawieniami Group Policy. Poniższa lista przedstawia ustawienia, które powinny być ustawione jako „nie konfigurowane/not configured" a w przypadku konfiguracji powinniśmy mieć pewność, że nasze urządzenie wspiera szyfrowanie urządzenia.

- Computer Configuration\Administrative Templates\Składniki systemu Windows\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup:
- Computer Configuration\Administrative Templates\Składniki systemu Windows\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered
- Computer Configuration\Administrative Templates\Składniki systemu Windows\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed data drives can be recovered

## 4.8. Wsparcie FIPS do ochrony odzyskiwania hasła.

Standard FIPS 140-1 określa wymagania, które muszą spełniać sprzętowe i programowe moduły kryptograficzne służące do szyfrowania danych, które są ważne, ale nie poufne (SBU).

Standard FIPS dostępny był w poprzedniej wersji systemu – zmiany Windows 8.1 zawierają między innymi:

Ochrona odzyskiwania haseł zgodna z FIPS może być utworzona w momencie, gdy Windows pracuje w trybie FIPS, kiedy możliwe jest potwierdzenie jego algorytmów.

Odzyskane hasła utworzone w trybie FIPS w Windows 8.1 mogą być rozróżniane od odzyskanych haseł w innych systemach.

Kiedy odzyskane hasło zgodne z FIPS odblokuje dyski, to pozwalają one na pracę w trybie zapis/odczyt nawet, jeśli pracują w trybie FIPS.

Możliwe jest eksportowanie i przechowywanie w AD odzyskanych haseł zgodnych z FIPS jeśli pracujemy w trybie FIPS.

## 4.9. System szyfrowania plików EFS

System szyfrowania plików (EFS) pozwala na zaszyfrowanie plików i folderów w celu zabezpieczenia ich przed nieautoryzowanym dostępem. Funkcjonalność ta jest jednym z elementów systemu plików NTFS i jest całkowicie przezroczysta dla użytkownika i aplikacji. Podczas normalnej pracy, kiedy użytkownik lub aplikacja próbuje uzyskać dostęp do zaszyfrowanego pliku, system operacyjny w sposób automatyczny uzyskuje dostęp do klucza deszyfrującego zawartość pliku, operacja szyfrowania i deszyfrowania odbywa się w tle a system wykonuje te działania w imieniu użytkownika. Użytkownicy, którzy posiadają dostęp do właściwych kluczy szyfrujących pracują z plikami zaszyfrowanymi tak samo jak z innymi plikami, podczas gdy inni użytkownicy otrzymują odmowę dostępu do plików zaszyfrowanych.

W systemie Windows 8 wprowadzono zmiany w architekturze, które w chwili obecnej wspierają kryptografię oparta na krzywych eliptycznych ( ECC – ang. Eliptic Curve Cryptography). Funkcjonalność ta jest zgodna z wymaganiami SUITE B, zestawem algorytmów kryptograficznych zdefiniowanych przez NSA (National Security Agency) na potrzeby amerykańskich agencji rządowych w celu zapewnienie ochrony informacji niejawnych. Zdefiniowany zestaw Suite B wymaga zastosowania kryptograficznych algorytmów AES, SHA oraz ECC w celu zapewnienia najwyższego stopnia ochrony i nie zezwala na stosowanie algorytmów kryptografii RSA, ale system szyfrowania plików (EFS) w systemie Windows 8 wspiera i obsługuje nowy „tryb mieszany" obsługujący algorytmy ECC i RSA. Tryb ten zapewnia zgodność plików zaszyfrowanych utworzonych przy zastosowaniu algorytmów dostępnych w poprzednich wersjach systemów Windows. Funkcjonalność ta może być bardzo użyteczna dla organizacji, które stosują kryptograficzne algorytmy RSA i jednocześnie zamierzają już wykorzystywać algorytmy ECC w celu przygotowania własnego środowiska do zapewnienia zgodności z zestawem Suite B.

**Uwaga:** Zaleca się stosowanie równoczesne mechanizmów BitLocker oraz EFS w celu zapewnienia najwyższego stopnia ochrony danych.

**Ocena ryzyka**

Nieautoryzowany dostęp do danych może wpłynąć negatywnie na procesy w organizacji, zwłaszcza w tam, gdzie wielu użytkowników ma dostęp do tego samego systemu lub korzysta z przenośnych systemów komputerowych, co w rezultacie powoduje duże ryzyko ujawnienia danych. EFS został zaprojektowany w celu minimalizacji ryzyka kradzieży danych oraz ujawnienia wrażliwych danych w

przypadku zgubienia lub kradzieży komputerów przenośnych a w szczególności ryzyka ujawnienia danych wrażliwych przez pracowników wewnętrznych posiadających do nich dostęp. Komputery ogólnodostępne i współdzielone są również narażone na powyższe ryzyko.

Sytuacja ta ma miejsce wtedy, kiedy atakujący uzyska fizyczny dostęp do niezabezpieczonego komputera, potencjalne konsekwencje takiego czynu obejmują następujące działania:

- Atakujący może uruchomić ponownie komputer i podwyższyć swoje uprawnienia do poziomu lokalnego administratora w celu uzyskania dostępu do danych użytkownika. Atakujący może również pobrać programy narzędziowe i wykonać atak siłowy w celu uzyskania hasła użytkownika. Po skutecznym ataku będzie możliwe zalogowanie się do systemu korzystając z konta i ujawnionego hasła użytkownika, a w konsekwencji uzyskanie dostępu do danych użytkownika.
- Atakujący może zalogować się do komputera z systemem Windows 8 w celu przekopiowania dostępnych danych na nośniki przenośne, przesłania ich poprzez wiadomość pocztową (email) lub przekopiowania ich przez sieć komputerową lub przetransferować je do zdalnego serwera z wykorzystaniem protokołu FTP.
- Atakujący może ponownie uruchomić komputer z alternatywnego systemu operacyjnego i przekopiować je bezpośrednio z lokalnego dysku twardego.
- Atakujący może połączyć komputer do innej sieci komputerowej, uruchomić skradziony komputer i następnie zalogować się do niego zdalnie.
- Jeśli użytkownik buforuje swoje pliki sieciowe w trybie offline, atakujący może wykorzystać je do podwyższenia swoich uprawnień do poziomu lokalnego administratora / systemu lokalnego a następnie sprawdzić zawartość plików buforowanych w trybie offline.
- Atakujący może ponownie uruchomić komputer z alternatywnego systemu operacyjnego i dokonać odczytu zawartości pliku stronicowania w celu odczytu informacji przechowywanych jawnym tekstem lub kopii dokumentów w postaci otwartego tekstu zintegrowanych z uruchomionym procesem.
- Ciekawski współpracownik może otworzyć wrażliwe pliki należące do innych użytkowników ogólnodostępnego i współdzielonego komputera.

**Minimalizacja Ryzyka**

W celu zmniejszenia zagrożenia związanego z powyższym ryzykiem, zaleca się zaszyfrowanie danych przechowywanych na dyskach twardych. Ulepszenia w technologii EFS zastosowane w systemie Windows 8 pozwolą na zmniejszenie następującego ryzyka i wymuszą zwiększenie bezpieczeństwa:

- Należy stosować szyfrowanie (EFS) plików i folderów, aby uniemożliwić atakującemu odczyt plików za pośrednictwem innego systemu operacyjnego, który wymaga uzyskania stosownego klucza deszyfrującego w celu odszyfrowania zawartości pliku. Klucz taki może zostać umieszczony na karcie inteligentnej w celu zapewnienia zwiększenia bezpieczeństwa.
- Należy wymuszać silne mechanizmy szyfrowania stosowane przez EFS poprzez zastosowanie zasad grup.
- Należy udaremnić działania atakującej osoby, która próbuje uzyskać dostęp do danych użytkownika poprzez przeprowadzenie ataku siłowego na hasło użytkownika stosując karty inteligentne, jako magazyn dla kluczy szyfrujących EFS lub stosując połączenie obu

technologii szyfrowania jednocześnie Bitlocker i EFS w celu uniemożliwienia dostępu do skrótu (ang. hash) hasła użytkownika i buforowanych poświadczeń użytkownika.

- Należy uniemożliwić atakującemu dostęp do wrażliwych danych użytkowników poprzez wymuszenia szyfrowania folderu „moje dokumenty" użytkownika stosując zasady grupowe. Alternatywnie można wymusić szyfrowanie innych lokalizacji zawierających dane użytkownika lub szyfrując całą partycję z danymi użytkownika poprzez skrypty logowania.
- Należy stosować system szyfrowania plików EFS, aby zapewnić szyfrowanie na wielu dyskach i udziałach sieciowych.
- Należy stosować system szyfrowania plików EFS, aby zapewnić ochronę pliku stronicowania i buforowanych podręcznych plików sieciowych trybu offline.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Szyfrowany system plików (EFS) może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji „Ocena ryzyka", jednak przed zastosowaniem funkcji EFS, ważne jest, aby wziąć pod uwagę następujące wymagania:

- Należy wdrożyć sprawdzone procedury zarządzania kluczami stosowanych do odzyskiwania danych oraz procedur odzyskiwania danych. W przypadku braku niezawodnych i poprawnie zdefiniowanych procedur, krytyczne dane organizacji mogą być niedostępne i nie możliwe do odszyfrowania w momencie utraty kluczy deszyfrujących.
- Funkcjonalność EFS ma niewielki wpływ na wydajność komputera, przeważanie jest to niedogodność niezauważalna przez większość użytkowników podczas normalnej pracy. Jednakże, jeśli wydajność systemu jest krytycznym elementem systemu komputerowego warto sprawdzić w fazie testów przedwdrożeniowych czy EFS nie wpływa znacząco na wydajność pracy użytkownika.
- W przypadku konieczności zapewnienia zgodności z zestawem Suite B w organizacji, należy wdrożyć algorytm ECC w celu przygotowania systemu komputerowego do spełnienia wymagań wdrożenia poziomu standardu szyfrowania.
- W przypadku włączenia szyfrowania plików EFS nie jest możliwe równoczesne kompresowanie plików na tym samym wolumenie, funkcja kompresji wbudowana jest w system plików NTFS.
- Użytkownicy i pracownicy działu IT muszą być odpowiednio przeszkoleni, aby uniknąć możliwych problemów, takich jak:
    - Kopiowanie oraz przenoszenie plików z miejsc zaszyfrowanych do miejsc niezaszyfrowanych, operacje, które mogą pozostawić pliku w postaci jawnej.
    - Niezastosowanie szyfrowania plików ukrytych folderów, w których aplikacje przechowują i zarządzają swoje własne kopie zapasowe.
- Należy bardzo dokładnie przetestować konfigurację EFS w celu sprawdzenia, czy szyfrowanie EFS zostało wdrożone na wszystkich lokalizacjach plików wrażliwych danych, wliczając w to „moje dokumenty", pulpit oraz foldery z plikami tymczasowymi.

**Proces minimalizacji ryzyka**

Poniżej przedstawiono proces minimalizacji ryzyka w celu oszacowania i wdrożenia najlepszych praktyk konfiguracji funkcji EFS, aby zapewnić ochronę wrażliwych danych znajdujących się na komputerach klienckich zarządzanych w organizacji:

W celu minimalizacji ryzyka zaleca się zastosowanie czynności:

1. Sprawdzenie i przeprowadzenie testów technologii szyfrowania EFS
   **Uwaga:** W celu uzyskania dodatkowych informacji na temat EFS, należy zapoznać się z artykułem: „Best practices for the Encrypting File System"[55] umieszczonym na stronach firmy Microsoft.
2. Oszacowanie potrzeby wdrożenia funkcji szyfrowania EFS.
3. Sprawdzenie i przeprowadzenie testów konfiguracji EFS poprzez zastosowanie zasad grup.
4. Dokonanie identyfikacji i wskazanie komputerów, które wymagają zapewnienia ochrony przez szyfrowanie EFS.
5. Dokonanie identyfikacji i oszacowania odpowiedniego wymaganego poziomu ochrony, np. Czy organizacja wymaga stosowania kart inteligentnych w połączeniu z systemem EFS.
6. Konfiguracja szyfrowania EFS w sposób odpowiedni dla środowiska z wykorzystaniem zasad grupowych.

## 4.10. Szczegółowe ustawienia systemu EFS zapewniające ochronę wrażliwych danych

W celu zarządzania konfiguracją systemu szyfrowania plików EFS poprzez mechanizm zasad grup, dostępne jest kilka ustawień konfiguracyjnych. Konfiguracja ustawień dostępna jest w następującej lokalizacji:

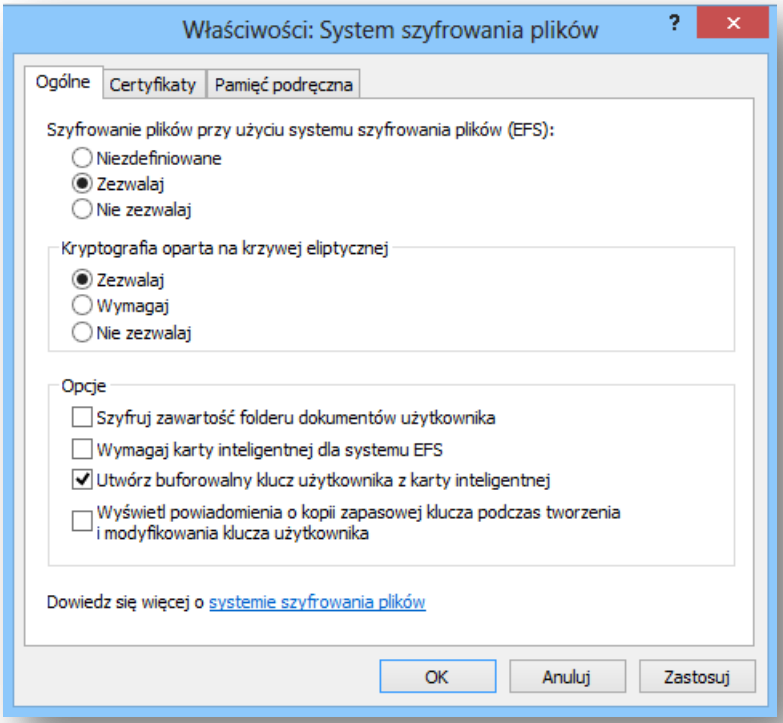
**Konfiguracja Komputera\Ustawienia systemu Windows\Ustawienie zabezpieczeń\Zasady kluczy publicznych\System szyfrowania plików**

**(Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System)**

W celu dodania lub utworzenia agenta odzyskiwania danych (DRA – ang. Data Recovery Agent) należy kliknąć prawym przyciskiem myszki **System szyfrowania plików** a następnie wybrać **Dodaj agenta odzyskiwania danych …**

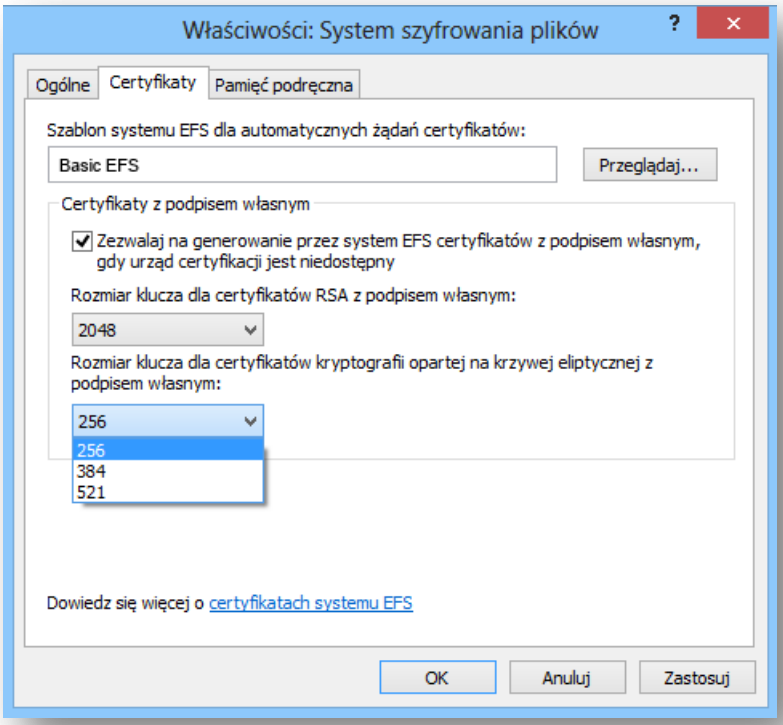
W celu wyświetlenia ustawień dotyczących EFS należy prawym przyciskiem myszki **System szyfrowania plików** a następnie kliknąć na opcję **Właściwości** w celu otworzenia okna **Właściwości: System szyfrowania plików.**

[55] http://support.microsoft.com/default.aspx?scid=kb;en-us;223316




Rys. 4.8.1 – Właściwości System Szyfrowania plików widok zakładka Ogólne

Ustawienie opcji „**Kryptografia oparta na krzywej eliptycznej" (ECC)** w tryb **Zezwalaj** pokazanej na rysunku 4.8.1 ustawia system szyfrowania plików (EFS) w tryb „mieszany", który pozwoli komputerom na stosowanie algorytmów RSA lub ECC. W przypadku kiedy środowisko wymaga zgodności z wymaganiami zestawu Suite B należy ustawić opcję **Wymagaj** przy ustawieniu „**Kryptografia oparta na krzywej eliptycznej" (ECC)** a następnie należy wybrać odpowiedni **rozmiar klucza dla certyfikatów kryptografii opartej na krzywej eliptycznej z podpisem własnym** pokazany na Rys. 4.8.2.




Rys. 4.8.2 – Właściwości System Szyfrowania plików widok zakładka Certyfikaty

Ważna uwaga –należy pamiętać, że przedstawione ustawienie zasad grupowych zostanie zastosowane tylko wtedy, kiedy plik lub folder będzie zaszyfrowany po włączeniu tej opcji. A w przypadku, kiedy plik lub folder został zaszyfrowany zanim przedstawiona opcja została skonfigurowana, użytkownik będzie korzystał z algorytmu, który został wybrany przy szyfrowaniu. Opcja **Wymagaj** przy ustawieniu „**Kryptografia oparta na krzywej eliptycznej" (ECC)** nie wymusza stosowania algorytmu AES dla toworzonych kluczy szyfrujących, opcja ta wymusza tylko zastosowanie algorytmu ECC

Rys.4.8.3 – Właściwości System Szyfrowania plików widok zakładka Pamieć podręczna

Poniższa tabela przedstawia 4 szablony ustawień zasad grup dla funkcji Systemu szyfrowania plików EFS.

| **Szablon oraz ustawienia** | **Ścieżka oraz opis** | **Domyślne ustawienie w systemie Windows 8** |
|---|---|---|
| GroupPolicy.admx<br><br>**Konfiguruj przetwarzanie zasad odzyskiwania systemu** | Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy<br>Ustawienia te określają, kiedy zasady dotyczące szyfrowania są | Nie skonfigurowano |

| | | |
|---|---|---|
| **szyfrowania plików** | aktualizowane. | |
| EncryptFilesonMove.admx<br><br>**Nie szyfruj automatycznie plików przenoszonych do zaszyfrowanych folderów.** | Konfiguracja komputera \ Szablony administracyjne \ System<br><br>To ustawienie zasad zapobiega szyfrowaniu przez Eksploratora plików tych plików, które są przenoszone do zaszyfrowanego folderu. | Nie skonfigurowano |
| OfflineFiles.admx<br><br>**Szyfruj pamięć podręczną plików offline** | Konfiguracja komputera \ Szablony administracyjne \ Sieć \Pliki trybu offline\<br><br>To ustawienie zasad określa, czy pliki trybu offline są szyfrowane.<br>Uwaga W systemach Windows XP SP3, pliki są szyfrowane za pomocą klucza systemu a wprzypadku Windows Vista SP1 lub późniejszy ,, pliki są szyfrowane kluczem użytkownika. | Nie skonfigurowano |
| Search.admx<br><br>**Zezwalaj na indeksowanie zaszyfrowanych plików** | Konfiguracja komputera \ Szablony administracyjne \ Składniki system Windows \Wyszukaj\<br><br>To ustawienie zasad umożliwia indeksowanie zaszyfrowanych elementów | Nie skonfigurowano |

Tabela 4.8.1 Ustawienia systemu szyfrowania plików EFS

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

## 4.11. Usługi zarządzania prawami do informacji (RMS)

Usługi zarządzania prawami do informacji (RMS – ang. Rights Management Services) zostały zaprojektowane w celu zapewnienia ochrony i egzekwowania zasad użytkowania zawartości wrażliwych treści informacji przechowywanych w wiadomościach poczty elektronicznej, dokumentów, zawartości stron internetowych oraz innych rodzajów informacji. RMS zapewnia bezpieczeństwo zawartości dokumentów przez trwały mechanizm szyfrowania informacji i przypisania praw użytkowania zawartości. Zawartość każdej wiadomości pocztowej oraz pliku podczas przesyłania jej przez sieć w organizacji lub sieć internet z zastosowaniem rozwiązania RMS, dostępna jest tylko i wyłącznie dla użytkowników uwierzytelnionych i upoważnionych poprzez nadanie uprawnień. Każda nieuprawniona osoba pomimo dostępu do pliku nie będzie wstanie odczytać treści tej informacji, która jest chroniona poprzez odpowiednio nadane uprawnienia i mechanizm szyfrowania. RMS składa się trzech głównych komponentów:

- **Serwer RMS** – system Windows 8 wymaga Usługi zarządzania prawami dostępu w systemie Windows dla systemu Windows Server 2003 lub nowszy.

- **Oprogramowanie klienta RMS** – oprogramowanie to wbudowane jest w system Windows 8 i nie wymaga dodatkowej instalacji.
- **Platforma lub aplikacja RMS** – jest to platforma lub aplikacja zaprojektowana w celu obsługi RMS poprzez mechanizm szyfrowania i kontroli dostępu do treści informacji zarządzanych przez ten mechanizm.

**Uwaga:** Pomimo, iż oprogramowanie klienta usług zarządzania prawami (RMS) wbudowane jest w systemie Windows 8, to wymaga zakupienia oddzielnej licencji dostępowej RMS CAL, aby móc skorzystać z tego oprogramowania.

**Ocena ryzyka**

Usługi zarządzania prawami (RMS) pozwalają na zmniejszenie ryzyka w organizacjach, w których nieuprawnione osoby mogą zapoznać się i przejrzeć dane wrażliwe. Informacje wrażliwe mogą zostać rozpowszechnione lub udostępnione osobom nieuprawnionym w wyniku pomyłki lub zaplanowanych działań złośliwych. Kilka przykładów zawierających możliwe scenariusze ryzyka opisano poniżej:

- Nieuprawnieni użytkownicy mogą uzyskać dostęp do informacji poprzez podsłuchanie ruchu sieciowego, uzyskanie fizycznego dostępu do urządzeń przenośnych pamięci flash lub dysków twardych lub uzyskują dostęp do niewłaściwie zabezpieczonych udziałów sieciowych serwerów lub magazynów danych.
- Uprawnieni użytkownicy mogą wysłać informacje wrażliwe to nieuprawnionych odbiorców wewnątrz lub na zewnątrz organizacji.
- Uprawnieni użytkownicy mogą skopiować lub przenieść dane wrażliwe do nieautoryzowanych lokalizacji lub aplikacji, a także mogą wykonać kopie danych z autoryzowanego miejsca przechowywania danych do nieautoryzowanych pamięci przenośnych flash lub dysków twardych (nośniki zewnętrzne).
- Uprawnieni użytkownicy, którzy przypadkowo udzielili dostępu do wrażliwych informacji nieuprawnionym użytkownikom poprzez sieci P2P (peer-to-peer) lub komunikatory internetowe.
- Uprawnieni użytkownicy, którzy wydrukowali wrażliwe informacje, i nie zabezpieczyli ich w sposób właściwy, przez co na razili na ryzyko pozyskania wydruków przez nieuprawnione osoby, które mogą te informacje skopiować, przefaksować lub przesłać je poprzez wiadomości poczty elektronicznej (email).

**Minimalizacja Ryzyka**

W celu skutecznej ochrony danych współdzielonych poprzez współpracowników poprzez zasoby sieciowe niezależnie od mechanizmu ich wykorzystania, zaleca się zabezpieczenie zawartości informacji korzystając z usługi zarządzania prawami do informacji (RMS). Mechanizm RMS doskonale chroni treść informacji, które są przesyłane pomiędzy serwerami, urządzeniami oraz współdzielonymi zasobami sieciowymi. Informacja, która została pozyskana w sposób nieautoryzowany nadal pozostaje w postaci zabezpieczonej i zaszyfrowanej przez mechanizm RMS.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Usługi zarządzania prawami do informacji (RMS) mogą zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji „Ocena ryzyka", jednak przed zastosowaniem i wdrożeniem usługi zarządzania prawami do informacji (RMS), ważne jest, aby wziąć pod uwagę następujące wymagania i najlepsze praktyki dla tej funkcji ochrony danych:

- RMS wymaga zainstalowanej usługi zarządzania prawami dostępu na serwerze RMS w systemie Windows dla systemu Windows Server 2003 lub nowszym, a także zainstalowania aplikacji obsługujących technologię RMS zainstalowanych na stacjach klienckich użytkowników.
- Microsoft® Office SharePoint® Server lub nowszy wymagany jest w przypadku zastosowania komponentu SharePoint-RMS integration ( mechanizm RMS chroni dokumenty i informacje przed nieupoważnionym dostępem przechowywane w witrynach programu SharePoint
- W przypadku zastosowania opcjonalnej integracji kart inteligentnych (SMART CARD) , należy upewnić się i sprawdzić czy każda stacja kliencka, która będzie korzystała z chronionej zawartości informacji jest w pełni kompatybilna ze stosowanymi kartami inteligentnymi.
- W przypadku zastosowania aplikacji internetowych (ang. web based) takich jak Microsoft Outlook® Web Access (OWA) z komponentem RMS, należy pamiętać, iż wymagany jest dodatek do programu Internet Explorer, który umożliwi korzystanie z RMS.
- Zalecane jest przeszkolenie osób działu IT z zakresu wdrożenia, wsparcia technicznego oraz rozwiązywania problemów związanych z technologią RMS.

**Proces minimalizacji ryzyka**

Poniżej przedstawiono proces minimalizacji ryzyka w celu oszacowania i wdrożenia najlepszych praktyk konfiguracji usługi zarządzania prawami (RMS), aby zapewnić ochronę wrażliwych danych przechowywanych w komputerach klienckich zarządzanych w organizacji:

- Sprawdzenie i przeprowadzenie testów technologii usługi zarządzania prawami (RMS)
  **Uwaga:** W celu uzyskania dodatkowych informacji na temat RMS, należy zapoznać się z artykułem: „Active Directory Rights Management Services"[56] umieszczonym na stronach firmy Microsoft.
- Oszacowanie potrzeby wdrożenia usługi zarządzania prawami (RMS).
- Przeprowadzić identyfikację aplikacji i usług wspieranych przez RMS.
- Określić i oszacować scenariusze wdrożenia usługi zarządzania prawami (RMS), takie jak:
  - Pojedynczy serwer RMS (lub pojedynczy klaster) - Single server (or single cluster)
  - Single certification, single license
  - Single certification, multiple license
  - Multiple certification, single license
  - Multiple certification, multiple license
- Dokonanie identyfikacji i oszacowania zakresu chronionych informacji korzystając z technologii RMS

[56] w języku polskim - http://technet.microsoft.com/pl-pl/library/cc771234(v=ws.10).aspx ,
w języku angielskim http://go.microsoft.com/fwlink/?LinkId=153465

- Dokonanie identyfikacji i oszacowania grup użytkowników, którzy wymagają dostępu do określonych i chronionych informacji.
- Konfiguracja usługi zarządzania prawami (RMS) w sposób, który zezwala na dostęp do określonych informacji tylko osobom uprawnionym.

## 4.12. Zastosowanie ustawień zasad grup do wdrożenia usługi RMS

Ustawienia zasad grup do konfigurowania usługi zarządzania prawami (RMS) nie są częścią instalacji systemu Windows 8. RMS to przede wszystkim rozwiązanie oparte na konfiguracji serwera, w związku z powyższym konfiguracja usługi zarządzania prawami (RMS) powinna być wykonana na serwerze pełniącego rolę serwera RMS. Ponadto aplikacje współpracujące z rozwiązaniem usługi zarządzania prawami (RMS) mogą posiadać indywidulane ustawienia, które określają, w jaki sposób zarządzać chronioną zawartością informacji.

## 4.13. Instalacja i zarządzanie urządzeniami w systemie Windows 8

Technologia urządzeń Plug and Play (PnP) daje użytkownikom dużą swobodę w użytkowaniu wszelkich urządzeń w tym również przenośnych na ich stacjach roboczych. Z drugiej strony urządzenia takie jak pamięci przenośne USB lub przenośne dyski twarde stanowią poważne problemy i wyzwania w utrzymaniu właściwego poziomu bezpieczeństwa dla administratorów i pracowników IT. Zagrożenie to, to nie tylko trudność w utrzymaniu i zarządzaniu instalacji niekompatybilnego i nieautoryzowanego sprzętu na stacji klienckich, ale również sytuacja ta stwarza poważne zagrożenie dla bezpieczeństwa przetwarzanych danych. W systemie Windows 8 wprowadzono szereg zmian w zasadach grup, które mają pomóc administratorom IT w zarządzaniu i kontroli każdej próby instalacji nieobsługiwanych i nieautoryzowanych urządzeń. Ważne jest jednak, aby mieć świadomość, iż każde urządzenie zainstalowane w systemie, dostępne jest dla każdego użytkownika tego systemu a nie tylko dla konkretnego użytkownika. System Windows 8, Windows 7 oraz Windows Vista zapewniają wsparcie na poziomie użytkownika w zapewnieniu kontroli dostępu w trybie do odczytu lub zapisu dla urządzenia zainstalowanego w systemie. Na przykład, można zapewnić pełny dostęp do zapisu i odczytu do zainstalowanego urządzenia, takiego, jako przenośna pamięć USB dla specyficznego użytkownika, a dla innych użytkowników już tylko dostęp do odczytu dla tego urządzenia na tym samym komputerze. Więcej informacji na temat zarządzania i instalacji urządzeń oraz w jaki sposób ustawienia zasad grupowych mogą pomóc w utrzymaniu i zarządzaniu urządzeń, można przeczytać w artykule „Step-By-Step Guide to Controlling Device Installation Using Group Policy[57]”

**Ocena ryzyka**

Nieautoryzowane dodawanie lub usuwanie urządzeń do komputerów stanowi bardzo wysokie zagrożenie dla bezpieczeństwa organizacji, ponieważ działania takie mogą pozwolić atakującemu na uruchomienie szkodliwego oprogramowania, usunięcie danych oraz zainstalowanie oprogramowania lub innych danych. Urządzenia te stanowią główne źródło wycieku danych. Kilka przykładów zawierających możliwe scenariusze ryzyka przedstawiono poniżej:

- Uprawnieni użytkownicy mogą skopiować lub przenieść dane wrażliwe zawarte na autoryzowanych nośnikach lub urządzeniach do nieautoryzowanych pamięci masowych lub

[57] http://go.microsoft.com/fwlink/?LinkId=130390

dysków twardych (nośniki zewnętrzne), czynności te mogą zostać wykonane w sposób świadomy lub nieświadomy przez użytkowników. Sytuacja taka może obejmować kopiowanie danych z zaszyfrowanych nośników danych lub lokalizacji do nieautoryzowanych i nieszyfrowanych ogólnodostępnych pamięci przenośnych.

- Atakujący może zalogować się do komputerów autoryzowanych użytkowników, a następnie skopiować dane na nośniki pamięci przenośnych.
- Atakujący może wykorzystać nośniki pamięci przenośnych lub udziały sieciowe zawierające oprogramowanie szkodliwe w celu automatycznego uruchomienia skryptu wykorzystując mechanizm auto uruchomienia (ang. AutoRun) w celu instalacji oprogramowania złośliwego na nienadzorowanych komputerach klienckich.
- Atakujący może zainstalować nieautoryzowane oprogramowanie lub urządzenie przechwytujące wszystkie wprowadzane dane z klawiatury (ang. Keyloger), które mogą zostać wykorzystane do przechwycenia nazwy konta, hasła lub innych danych wrażliwych w celu przeprowadzenia późniejszego ataku.

**Minimalizacja Ryzyka**

W celu zmniejszenia zagrożenia związanego z powyższym ryzykiem, zaleca się ochronę systemów komputerowych ze szczególnym uwzględnieniem kontroli i nadzoru instalacji oraz użytkowania nieautoryzowanych urządzeń podłączanych do komputerów. Do kontroli i nadzoru urządzeń PnP, takich jak pamięci przenośne USB lub przenośne dyski twarde można wykorzystać ustawienia zasad grup.

**Zagadnienia minimalizacji ryzyka wymagające rozważenia**

Zastosowanie ustawień zasad grup dotyczących instalacji urządzeń w systemie Windows 8 może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji „Ocena ryzyka”. Jednak przed wdrożeniem ustawień dotyczących instalacji i zarządzania urządzeń w komputerach klienckich, ważne jest, aby wziąć pod uwagę następujące zagadnienia związane z minimalizacją ryzyka:

- Ograniczenie korzystania z urządzeń może zablokować możliwość korzystania z udostępniania danych uprawnionym użytkownikom lub zmniejszyć efektywność użytkowników mobilnych poprzez zablokowanie dostępu do urządzeń przenośnych.
- Ograniczenie korzystania z urządzeń przenośnych może uniemożliwić zastosowanie klucza USB, jako części procesu wdrożenia szyfrowania dysków korzystając z technologii BitLocker. Na przykład, jeśli zastosujemy ustawienie zasad grupowych: „**Dyski wymienne: Odmowa prawa do zapisu**”, pomimo, iż ustawienie to przeznaczone jest dla użytkowników, to będzie obowiązywało ono również w przypadku użytkownika z prawami administratora, co w efekcie spowoduje, że program instalacyjny BitLocker nie będzie mógł zapisać, klucza uruchomienia na dysku przenośnym USB.
- Pewna cześć urządzeń, jest identyfikowana podwójnie w systemie, jako urządzenie magazynu wymiennego (ang. removable storage ID) oraz jako urządzenie magazynu lokalnego (ang. local storage ID). Na przykład, takiej identyfikacji dokonają niektóre typy dysków przenośnych USB uruchamianych podczas startu systemu w zależności od momentu podłączenia urządzenia, przed startem systemu lub w czasie, kiedy system jest już uruchomiony. Dlatego ważne jest, aby dokładnie przetestować ustawienia zasad grupowych (GPO), aby zapewnić właściwą ochronę dla

odpowiednich typów urządzeń i określić czy wykorzystanie tych urządzeń jest zabronione czy zezwolone w środowisku organizacji.

**Proces minimalizacji ryzyka**

Poniżej przedstawiono proces minimalizacji ryzyka w celu oszacowania i wdrożenia najlepszych praktyk dla instalacji i zarządzania urządzeniami w systemie Windows 8, aby zapewnić ochronę wrażliwych danych znajdujących się zarządzanych na komputerach:

W celu minimalizacji ryzyka zaleca się zastosowanie czynności:

1. Sprawdzenie i przeprowadzenie testów dotyczących zagadnienia instalacji i zarządzania urządzeniami w systemie Windows 8
   **Uwaga:** W celu uzyskania dodatkowych informacji na ten temat, należy zapoznać się z dokumentami: Step-By-Step Guide to Controlling Device Installation Using Group Policy[58] umieszczonych na stronach witryny Microsoft.
2. Oszacowanie potrzeby wdrożenia mechanizmu instalacja i zarządzanie urządzeniami w systemie Windows 8.
3. Sprawdzenie i przeprowadzenie testów dotyczących ustawień zasad grup dla mechanizmu instalacja i zarządzanie urządzeniami w systemie Windows 8.
4. Dokonanie identyfikacji niezbędnych urządzeń przenośnych pracujących w środowisku organizacji, i przygotowanie listy ustawień dla tych urządzeń ze szczególnym uwzględnieniem identyfikatorów sprzętu (ang. Hardware ID) oraz identyfikatorów zgodnych(ang. Compatible ID).
5. Dokonanie identyfikacji i wskazanie komputerów oraz użytkowników, którzy wymagają codziennej pracy z urządzeniami przenośnymi.
6. Wdrożenie i zastosowanie ustawień zasad grupowych w celu włączenia możliwości instalacji niezbędnych i odpowiednich klas urządzeń.
7. Wdrożenie i zastosowanie ustawień zasad grupowych w celu włączenia możliwości instalacji na wybranych komputerach, na których jest to niezbędne do codziennej pracy.

## 4.14. Zastosowanie ustawień zasad grupowych do nadzorowania instalacji urządzeń

W celu nadzorowania instalacji i zarządzania urządzeń rekomendowane jest zastosowanie ustawień zasad grupowych dostępnych w szablonie zasad grupowych **Deviceinstallation.admx**. Tabela poniżej przedstawia zasady grupowe dostępne w tym szablonie**.** Konfiguracja tych ustawień dostępna jest w gałęzi:

**Konfiguracja komputera\Szablony administracyjne\System\Instalacja urządzenia\Ograniczenia dotyczące instalacji urządzeń**

**(Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions)**

[58] http://go.microsoft.com/fwlink/?LinkId=130390

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Zezwalaj administratorom na zastępowanie zasad ograniczających instalację urządzeń | To ustawienie zasad umożliwia określenie, czy członkowie grupy Administratorzy mogą instalować i aktualizować sterowniki dowolnego urządzenia, bez względu na inne ustawienia zasad. | Nie skonfigurowano |
| Zezwalaj na instalację urządzeń za pomocą sterowników odpowiadających tym klasom konfiguracji urządzeń | To ustawienie zasad umożliwia określenie listy unikatowych identyfikatorów globalnych (GUID) klasy konfiguracji urządzeń dla sterowników urządzeń, których instalacja w systemie Windows ma być dozwolona.<br>Jeśli to ustawienie zasad zostanie włączone, w systemie Windows będzie dozwolona instalacja lub aktualizacja sterowników urządzeń, których identyfikatory GUID klasy konfiguracji urządzeń znajdują się na utworzonej liście, chyba że inne ustawienie zasad zapobiega instalacji (np. ustawienie zasad „Zapobiegaj instalacji urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń”, „Zapobiegaj instalacji urządzeń tych klas” lub „Zapobiegaj instalacji urządzeń wymiennych”). | Nie skonfigurowano |
| Nie zezwalaj na instalację urządzeń za pomocą sterowników odpowiadających tym klasom konfiguracji urządzeń | To ustawienie zasad umożliwia określenie listy unikatowych identyfikatorów globalnych (GUID) klasy konfiguracji urządzeń dla sterowników urządzeń, których instalacja w systemie Windows ma być niedozwolona. To ustawienie zasad ma pierwszeństwo przed każdym innym ustawieniem zasad, które zezwala na instalację urządzenia w systemie Windows. | Nie skonfigurowano |
| Wyświetl niestandardowy komunikat, jeśli ustawienie zasad uniemożliwia instalację | To ustawienie zasad umożliwia wyświetlanie użytkownikom niestandardowego komunikatu w powiadomieniu w sytuacji, gdy podjęto próbę instalacji urządzenia, a jakieś ustawienie zasad uniemożliwia instalację.<br>Jeśli to ustawienie zasad zostanie | Nie skonfigurowano |

| | | |
|---|---|---|
| | włączone, wówczas w przypadku gdy jakieś ustawienie zasad uniemożliwi instalację urządzenia, w systemie Windows będzie wyświetlany tekst wpisany przez użytkownika w polu Szczegóły. | |
| Wyświetl niestandardowy tytuł komunikatu, jeśli ustawienie zasad uniemożliwia instalację | To ustawienie zasad umożliwia wyświetlanie powiadomienia niestandardowego tytułu komunikatu w sytuacji, gdy podjęto próbę instalacji urządzenia i jakieś ustawienie zasad uniemożliwia instalację.<br><br>Jeśli to ustawienie zasad zostanie włączone, wówczas w przypadku gdy jakieś ustawienie zasad uniemożliwi instalację urządzenia, w systemie Windows jako tytuł powiadomienia będzie wyświetlany tekst wpisany przez użytkownika w polu Treść. | Nie skonfigurowano |
| Zezwalaj na instalację urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń | To ustawienie zasad umożliwia wyświetlanie powiadomienia niestandardowego tytułu komunikatu w sytuacji, gdy podjęto próbę instalacji urządzenia i jakieś ustawienie zasad uniemożliwia instalację.<br><br>Jeśli to ustawienie zasad zostanie włączone, wówczas w przypadku gdy jakieś ustawienie zasad uniemożliwi instalację urządzenia, w systemie Windows jako tytuł powiadomienia będzie wyświetlany tekst wpisany przez użytkownika w polu Treść. | Nie skonfigurowano |
| Zapobiegaj instalacji urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń | To ustawienie zasad umożliwia określenie listy identyfikatorów sprzętu typu Plug and Play oraz zgodnych identyfikatorów urządzeń, których instalacja w systemie Windows ma być niedozwolona. To ustawienie zasad ma pierwszeństwo przed każdym innym ustawieniem zasad, które zezwala na instalację urządzenia w systemie Windows.<br><br>Jeśli to ustawienie zasad zostanie włączone, w systemie Windows nie | Nie skonfigurowano |

| | | |
|---|---|---|
| | będzie dozwolona instalacja urządzeń, których identyfikatory sprzętu lub zgodne identyfikatory znajdują się na utworzonej liście. | |
| Czas (w sekundach), po jakim jest wymuszany ponowny rozruch, jeśli jest on wymagany do zastosowania zmian zasad | To ustawienie zasad umożliwia określenie listy identyfikatorów sprzętu typu Plug and Play oraz zgodnych identyfikatorów urządzeń, których instalacja w systemie Windows ma być niedozwolona. To ustawienie zasad ma pierwszeństwo przed każdym innym ustawieniem zasad, które zezwala na instalację urządzenia w systemie Windows.<br><br>Jeśli to ustawienie zasad zostanie włączone, w systemie Windows nie będzie dozwolona instalacja urządzeń, których identyfikatory sprzętu lub zgodne identyfikatory znajdują się na utworzonej liście. | Nie skonfigurowano |
| Zapobiegaj instalacji urządzeń wymiennych | Za pomocą tego ustawienia zasad można zapobiec instalowaniu w systemie Windows urządzeń wymiennych. Urządzenie jest uważane za wymienne, jeśli sterownik urządzenia, do którego jest ono podłączone, wskazuje, że urządzenie jest wymienne. Na przykład urządzenie USB jest zgłaszane jako wymienne przez sterowniki koncentratora USB, do którego jest ono podłączone. To ustawienie zasad ma pierwszeństwo przed każdym innym ustawieniem zasad, które zezwala na instalację urządzenia w systemie Windows. | Nie skonfigurowano |
| Zapobiegaj instalacji urządzeń nieopisanych w innych ustawieniach zasad | To ustawienie zasad pozwala zapobiec instalacji urządzeń, które nie są w sposób wyraźny opisane w żadnym innym ustawieniu zasad.<br><br>Jeśli to ustawienie zostanie włączone, w systemie Windows nie będzie możliwe zainstalowanie ani zaktualizowanie sterownika żadnego urządzenia, które nie jest opisane w ustawieniu zasad „Zezwalaj na instalację urządzeń o identyfikatorach | Nie skonfigurowano |

| | | |
|---|---|---|
| | odpowiadających tym identyfikatorom urządzeń” lub „Zezwalaj na instalację urządzeń tych klas”. | |

Tabela 4.12.1 Ustawienia zasad grupowych do nadzorowania instalacji urządzeń

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia, znajduje się w zakładce **POMOC** w ustawieniach w Edytorze obiektów zasad grupy.

## 4.15. Zastosowanie ustawień zasad grupowych do kontroli obsługi urządzeń

Dodatkowo w celu zapewnienia nadzorowania instalacji urządzeń, system Windows 8 pozwala na nadzorowanie poziomu dostępu użytkowników do poszczególnych klas urządzeń, które uprzednio zostały zainstalowane. Szablon **RemovableStorage.admx** zawiera ustawienia dla urządzeń magazynu wymiennego, konfiguracja tych ustawień dostępna jest w gałęzi:

**Konfiguracja komputera\Szablony administracyjne\System\Dostęp do magazynu wymiennego**

**(Computer Configuration\Administrative Templates\System\Removable Storage Access)**

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Czas (w sekundach) do wymuszenia ponownego uruchomienia | To ustawienie zasad pozwala zapobiec instalacji urządzeń, które nie są w sposób wyraźny opisane w żadnym innym ustawieniu zasad.<br><br>Jeśli to ustawienie zostanie włączone, w systemie Windows nie będzie możliwe zainstalowanie ani zaktualizowanie sterownika żadnego urządzenia, które nie jest opisane w ustawieniu zasad „Zezwalaj na instalację urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń” lub „Zezwalaj na instalację urządzeń tych klas”. | Nie skonfigurowano |
| Dysk CD i DVD: odmowa dostępu do wykonywania | To ustawienie zasad powoduje odmowę dostępu do wykonywania w przypadku klasy magazynów wymiennych CD i DVD. | Nie skonfigurowano |
| Dysk CD i DVD: odmowa dostępu do odczytu | To ustawienie zasad powoduje odmowę dostępu do odczytu w przypadku klasy magazynów wymiennych CD i DVD. | Nie skonfigurowano |
| Dysk CD i DVD: odmowa prawa do zapisu | To ustawienie zasad powoduje odmowę prawa do zapisu w przypadku klasy magazynów | Nie skonfigurowano |

| | | |
|---|---|---|
| | wymiennych CD i DVD. | |
| Klasy niestandardowe: odmowa dostępu do odczytu | To ustawienie zasad powoduje odmowę dostępu do odczytu w przypadku niestandardowych klas magazynów wymiennych. | Nie skonfigurowano |
| Klasy niestandardowe: odmowa prawa do zapisu | To ustawienie zasad powoduje odmowę prawa do zapisu w przypadku niestandardowych klas magazynów wymiennych. | Nie skonfigurowano |
| Stacje dyskietek: odmowa dostępu do wykonywania | To ustawienie zasad powoduje odmowę dostępu do wykonywania w przypadku klasy magazynów wymiennych Stacje dyskietek, obejmującej też stacje dyskietek USB. | Nie skonfigurowano |
| Stacje dyskietek: odmowa dostępu do odczytu | To ustawienie zasad powoduje odmowę dostępu do odczytu w przypadku klasy magazynu wymiennego „stacje dyskietek”, obejmującej też stacje dyskietek USB. | Nie skonfigurowano |
| Stacje dyskietek: odmowa dostępu do zapisu | To ustawienie zasad powoduje odmowę prawa do zapisu w przypadku klasy magazynu wymiennego „stacje dyskietek”, obejmującej też stacje dyskietek USB. | Nie skonfigurowano |
| Dyski wymienne: odmowa dostępu do wykonywania | To ustawienie zasad powoduje odmowę dostępu do wykonywania do dysków wymiennych. | Nie skonfigurowano |
| Dyski wymienne: odmowa dostępu do odczytu | To ustawienie zasad powoduje odmowę dostępu do odczytu dysków wymiennych. | Nie skonfigurowano |
| Dyski wymienne: odmowa prawa do zapisu | To ustawienie zasad powoduje odmowę dostępu do zapisu do dysków wymiennych. | Nie skonfigurowano |
| Wszystkie klasy magazynów wymiennych: odmowa dostępu | Konfiguruje dostęp do wszystkich klas magazynów wymiennych.<br><br>To ustawienie zasad ma pierwszeństwo przed wszystkimi ustawieniami zasad dla poszczególnych magazynów wymiennych. Aby zarządzać poszczególnymi klasami, należy użyć ustawień zasad dla każdej klasy. | Nie skonfigurowano |
| Wszystkie magazyny wymienne: Zezwalaj na dostęp bezpośredni w sesjach zdalnych | To ustawienie zasad zapewnia zwykłym użytkownikom bezpośredni dostęp do wymiennych urządzeń | Nie skonfigurowano |

| | | |
|---|---|---|
| | pamięci masowej w sesjach zdalnych. | |
| Stacje taśm: odmowa dostępu do wykonywania | To ustawienie zasad powoduje odmowę dostępu do wykonywania w przypadku klasy magazynów wymiennych Stacja taśm. | Nie skonfigurowano |
| Stacje taśm: odmowa dostępu do odczytu | To ustawienie zasad powoduje odmowę dostępu do odczytu w przypadku klasy magazynu wymiennego „stacja taśm”. | Nie skonfigurowano |
| Stacje taśm: odmowa dostępu do odczytu | To ustawienie zasad powoduje odmowę prawa do zapisu w przypadku klasy magazynu wymiennego „stacja taśm”. | Nie skonfigurowano |
| Urządzenia WPD: odmowa prawa do zapisu | To ustawienie zasad powoduje odmowę dostępu do odczytu dysków wymiennych, które mogą obejmować odtwarzacze multimedialne, telefony komórkowe, wyświetlacze pomocnicze i urządzenia z systemem Windows CE. | Nie skonfigurowano |
| Urzadzenia WPD: odmowa prawa do zapisu | To ustawienie zasad powoduje odmowę dostępu do odczytu dysków wymiennych, które mogą obejmować odtwarzacze multimedialne, telefony komórkowe, wyświetlacze pomocnicze i urządzenia z systemem Windows CE. | |

## 4.16. Zastosowanie ustawień zasad grup do kontroli i blokowania funkcji autostartu i autoodtwarzania

Szablon **Autoplay.admx** zawiera następujące ustawienia mające wpływ na zachowanie funkcji autoodtwarzania i autouruchamiania dla wymiennych urządzeń magazynujących oraz nośników wymiennych w systemie Windows 8. Konfiguracja tych ustawień dostępna jest w gałęzi:

**Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Zasady funkcji Autoodtwarzanie**

**(Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies)**

| Ustawienie zasad | Opis | Domyślne ustawienie w systemie Windows 8 |
|---|---|---|
| Wyłącz funkcję Autoodtwarzanie | To ustawienie zasad umożliwia | Nie skonfigurowano |

| | | |
|---|---|---|
| | wyłączenie funkcji Autoodtwarzanie. | |
| Wyłącz zapamiętywanie wyborów użytkownika przez funkcję Autoodtwarzanie | To ustawienie zasad umożliwia wyłączenie funkcji Autoodtwarzanie. | Nie skonfigurowano |
| Wyłącz funkcję Autoodtwarzanie dla urządzeń niezawierających woluminów | To ustawienie zasad umożliwia wyłączenie funkcji Autoodtwarzanie dla urządzeń MTP, takich jak aparaty fotograficzne lub telefony. | Nie skonfigurowano |
| Ustaw domyślne zachowanie autouruchamiania | To ustawienie zasad określa domyślne zachowanie poleceń autouruchamiania. | Nie skonfigurowano |

Ustawienia powyższe dostępne są również w gałęzi:

**Konfiguracja użytkownika\Szablony Administracyjne\Składniki systemu Windows\Zasady funkcji Autoodtwarzanie**

**(User Configuration\Administrative Templates\Windows Components\AutoPlay Policies)**

Jeśli ustawienia dotyczące nadzorowania instalacji urządzeń powodują konflikt, to ustawienie dla konfiguracji komputera zastąpi ustawienie konfiguracji użytkownika.

## 4.17. Windows To Go

Obszar roboczy Windows To Go umożliwia utworzenie rozruchowej kopii systemu Windows 8 na dysku USB i uruchomienie jej z dysku USB na dowolnym komputerze. Windows To Go pozwala użytkownikom systemu Windows otwierać wszystkie niezbędne aplikacje oraz pliki i korzystać z tych elementów przy pomocy przenośnej wersji Windows umieszczonej na dysku USB razem z możliwością pracy zdalnej.

**Ocena ryzyka**

W pewnych organizacjach, praca zdalna lub z domu jest atrakcyjną i elastyczną metodą współpracy pracownika z organizacją, która zwiększa satysfakcję użytkownika z wykonywanej pracy oraz redukuje koszty. Jednakże w scenariuszu pracy zdalnej z domu, podczas kiedy użytkownik z własnego domowego komputera łączy się z firmowa siecią za pomocą VPN, to takie rozwiązanie niesie ze sobą pewne niebezpieczeństwa i zwiększa ryzyko zarażenie oprogramowaniem złośliwym. Dodatkowo jakiekolwiek wrażliwe dane zapisane na domowym komputerze pozostają niezabezpieczone.

**Minimalizacja Ryzyka**

Korzystając z systemu Windows 8 administratorzy mogą utworzyć rozruchowy obraz systemu Windows To Go na dysku USB i dostarczyć użytkownikom korzystającym z pracy zdalnej. Użytkownik będzie musiał tylko uruchomić system z dostarczonego dysku USB na domowym komputerze. Tak przygotowany system będzie zbliżonym systemem, z którego korzysta użytkownik na co dzień w swojej organizacji, dodatkowo system ten może posiadać zainstalowane niezbędne aplikacje oraz

narzędzia do bezpiecznego połączenia zdalnego. W scenariuszu tym Windows To Go posiada następujące korzyści:

- Lokalne dyski twarde na komputerze domowym nie są dostępne w uruchomionym obrazie systemu Windows To Go.
- Przenośny system Windows To Go może zostać zabezpieczony i zaszyfrowany za pomocą funkcji BitLocker. System ten pozostaje nie dostępny dla użytkownika dopóki nie wprowadzi on niezbędnego hasła lub innych elementów zabezpieczeń.
- Najnowsza wersja systemu Windows pozostaje skonfigurowana w sposób zbliżony do domowego komputera i nie wymaga dodatkowego sprzętu oraz dodatkowym nakładów finansowych.
- Windows To Go pozwala na pełen dostęp do lokalnych urządzeń peryferyjnych, takich jak drukarka albo elementy dotykowe.

W celu uzyskania informacji na temat Windows To Go, należy zapoznać się informacjami umieszczonymi Windows To Go: Scenario Overview[59].

## 4.18. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na temat bezpieczeństwa systemu Windows 8 opublikowanych na stronach Microsoft.com:

- Active Directory Rights Management Services[60]
- BCDEdit Commands for Boot Environment[61].
- Best Practices for BitLocker in Windows 7[62].
- Best practices for the Encrypting File System[63].
- BitLocker Drive Encryption Deployment Guide for Windows 7[64].
- BitLocker Drive Encryption Overview[65].
- Boot Configuration Data in Windows Vista[66].
- First Look: New Security Features in Windows Vista[67] for general information about security features in Windows Vista SP1.
- How Setup Selects Drivers[68].
- Microsoft Security Compliance Manager[69].
- Office 2003 Policy Template Files and Deployment Planning Tools[70].

[59] http://technet.microsoft.com/library/hh831833.aspx
[60] http://go.microsoft.com/fwlink/?LinkId=153465
[61] http://go.microsoft.com/fwlink/?LinkId=113151
[62] http://technet.microsoft.com/en-us/library/dd875532(WS.10).aspx
[63] http://support.microsoft.com/default.aspx?scid=kb;en-us;223316
[64] http://go.microsoft.com/fwlink/?LinkId=140286
[65] http://technet.microsoft.com/en-us/library/cc732774.aspx
[66] http://go.microsoft.com/fwlink/?LinkId=93005
[67] https://www.microsoft.com/technet/technetmag/issues/2006/05/FirstLook/default.aspx
[68] http://msdn.microsoft.com/en-us/library/ff546228.aspx
[69] http://go.microsoft.com/fwlink/?LinkId=113940

- Step-By-Step Guide to Controlling Device Installation Using Group Policy[71].
- The Encrypting File System[72].
- Trusted Computing Group[73].
- Windows BitLocker Drive Encryption Design and Deployment Guides[74].
- Active Directory Rights Management Services[75].
- Windows Vista Security and Data Protection Improvements[76]: "Data Protection."

[70] http://office.microsoft.com/en-us/assistance/HA011513711033.aspx
[71] http://go.microsoft.com/fwlink/?LinkId=130390
[72] http://www.microsoft.com/technet/security/topics/cryptographyetc/efs.mspx
[73] http://www.trustedcomputinggroup.org/
[74] http://go.microsoft.com/fwlink/?LinkId=134201
[75] http://go.microsoft.com/fwlink/?LinkId=153465
[76] http://technet.microsoft.com/en-us/library/cc507844.aspx

# 5. Zapewnienie kompatybilności aplikacji w kontekście bezpieczeństwa stacji z Windows 8

Od wprowadzenia Windows Vista zaszło wiele zmian w zakresie ochrony współpracy na linii aplikacja – jądro systemu. Z tego powodu pojawiły się problemy z kompatybilnością aplikacji.

Mimo wprowadzenia w Windows 8 nowego rodzaju aplikacji skupionych wokół AppContainer model architektury aplikacji Win32 pozostaje taki sam. To z kolei wymusza skupienie się na weryfikacji planowanego do wykorzystania oprogramowania w organizacji pod kątem możliwości pracy w środowisku Windows 8.

Funkcjonalności takie jak Kontrola konta użytkownika UAC (z ang. User Account Control) czy Ochrona zasobów system Windows WRP (z ang. Windows Resource Protection) mogą powodować, że aplikacje zaprojektowane dla starszych systemów nie będą prawidłowo funkcjonowały w Windows 8.

## 5.1. Testowanie zgodności aplikacji z systemem Windows 8

Testowanie zgodności stanowi podstawową czynność, którą należy wykonać przed wdrożeniem oprogramowania w środowisku Windows 8.

Testowanie zgodności aplikacji z Windows 8 powinno obejmować następujące kroki.

1. Instalację Windows 8 na komputerze testowym i zalogowanie się na konto z uprawnieniami administracyjnymi.
2. Uruchomienie instalacji oprogramowania.
3. W przypadku błędów instalatora należy go uruchomić w trybie „Uruchom jako administrator”. Jeśli nie są zgłaszane błędy kolejnym krokiem jest czynność w punkcie 5.
4. W przypadku kolejnych błędów należy we właściwościach instalatora ustawić tryb kompatybilności na Windows XP Professional SP3 i powtórzyć czynność w punkcie 2. W przypadku dalszych błędów należy wykonać czynność w punkcie 7.
5. Zalogowanie się na konto bez uprawnień administracyjnych.
6. Uruchomienie aplikacji. Jeśli wyświetlane są błędy należy włączyć tryb kompatybilności Windows XP Professional SP3 i ponownie uruchomić aplikację.
7. Jeśli aplikacja uruchomiła się prawidłowo należy wykonać szereg testów związanych z czynnościami obsługowymi wykonywanymi w ramach testowanego oprogramowania. Po przejściu wszystkich testów aplikacja jest gotowa do prawidłowego działania w systemie Windows 8.
8. Jeśli aplikacja nie zainstalowała się lub nie uruchomiła prawidłowo, przestaje odpowiadać, wyświetla błędy oznacza problemy z kompatybilnością i należy przeprowadzić dodatkową analizę działania oprogramowania.

## 5.2. Znane problemy zgodności aplikacji w kontekście rozszerzonych mechanizmów ochrony

Istnieje kilka znanych powodów, dla których kompatybilność aplikacji nie jest zachowana. Mogą one wynikać z wbudowanych w Windows 8 mechanizmów ochrony, które opisane zostały poniżej.

**Kontrola konta użytkownika**

Funkcja dostępna w Windows Vista, Windows 7 SP1 oraz Windows 8 zapewnia separację standardowych uprawnień użytkownika i zadań od tych, które wymagają dostępu administracyjnego. Dzięki kontroli konta użytkownika podnoszony jest poziom bezpieczeństwa, co pozwala wykonywać standardowym użytkownikom więcej czynności bez konieczności korzystania z kont posiadających uprawnienia administracyjne. Jedną z cech mechanizmu jest również możliwość wirtualizacji na poziomie rejestru i systemu plików. Dzięki temu można zapewnić kompatybilność aplikacji, które zaprojektowane zostały do korzystania z chronionych obecnie obszarów w rejestrze i systemie plików.

**Ochrona zasobów systemu Windows**

Dostępny od Windows Vista mechanizm ochrony zasobów systemu Windows zapewnia ochronę kluczy rejestru i folderów na tych samych zasadach, w jaki zabezpieczane są kluczowe pliki systemowe. Aplikacje, które próbują uzyskać dostęp do chronionych przez mechanizm plików mogą nieprawidłowo funkcjonować w Windows 8, dlatego wymagana jest w takiej sytuacji modyfikacja sposobu działania aplikacji.

**Tryb chroniony**

Funkcja Internet Explorer 10 ułatwia ochronę komputerów pracujących pod kontrolą Windows przed instalacją złośliwego oprogramowania i innych aplikacji powodujących niestabilność. Jeśli Internet Explorer pracuje w trybie chronionym przeglądarka współpracuje wyłącznie z określonymi obszarami systemu plików i rejestru. Domyślnie tryb chroniony jest włączony od Internet Explorer 8, kiedy odbywa się próba dostępu do witryn zlokalizowanych w strefie Intranet i/lub strefie witryn zaufanych.

## 5.3. Zmiany i ulepszenia systemu operacyjnego Windows 8 oraz Windows 8.1

W Windows 8 oraz Windows 8.1 wprowadzone zostały zmiany, które mogą powodować brak kompatybilności aplikacji firm trzecich. Należą do nich:

- Nowy interfejs programowania aplikacji API (z ang. Application Programming Interface) Dostępny od Windows Vista interfejs programowania aplikacji w odmienny sposób zapewnia komunikację między programami. Przykładami są oprogramowanie antywirusowe oraz zapora ogniowa, które opierając się na nowym API zapewniają lepszą ochronę, ale wymuszają jednocześnie uwzględnienie ich istnienia dla działających w Windows 8 aplikacji.
- 64-bitowa wersja Windows
  Aplikacje 16-bitowe oraz sterowniki 32-bitowe nie są wspierane w środowisku 64-bitowym Windows 8. Automatyczne przekierowanie rejestru i plików systemowych jest dostępne wyłącznie dla aplikacji 32-bitowych. Z tego powodu aplikacje 64-bitowe muszą być napisane w pełnej zgodzie ze standardami aplikacji Windows Vista, Windows 7 SP1 oraz Windows 8.
- Wersje systemu operacyjnego
  Zdarza się, że starsze aplikacje sprawdzają wersje Windows. W przypadku wykrycia innej wersji niż ta, dla której są dedykowane zatrzymywane jest ich działanie. Jednym z rozwiązań jest uruchomienie w trybie kompatybilności z wcześniejszymi systemami.

## 5.4. Omówienie stosowanych narzędzi w celu zapewnienia zgodności aplikacji z systemem Windows 8 oraz Windows 8.1

W ramach Windows 8 oraz Windows 8.1 dostępnych jest wiele narzędzi, które przeznaczone są do zapewnienia kompatybilności aplikacji.

**Asystent zgodności programów**

Funkcja Asystent zgodności programów stworzona została w celu umożliwienia uruchamiania aplikacji zaprojektowanych dla wcześniejszych wersji Windows. W sytuacji, kiedy Windows 8 wykryje aplikację, która wymaga trybu kompatybilności dla Windows 2000, Windows XP Professional SP3 bądź innych Windows automatycznie ustawia odpowiedni tryb działania aplikacji. Asystent zgodności programów uruchamia się automatycznie.

**Kreator kompatybilności programów**

Funkcja ta umożliwia w ramach dostępnego kreatora określić problemy kompatybilności wybranej aplikacji i wykryć powody z jednoczesnym zaproponowanej rozwiązania. Uruchomienie kreatora kompatybilności programów jest możliwe z poziomu **Panelu sterowania**, w sekcji **Programy** po kliknięciu opcji **Uruchom programy napisane dla starszych wersji systemu Windows**.

**Application Compatibility Toolkit (ACT)**

Pakiet ACT jest zbiorem narzędzi oraz dokumentacji umożliwiający określanie i zarządzanie aplikacjami w organizacji pod kątem zapewnienia ich kompatybilności w środowisku Windows 8. ACT umożliwia inwentaryzację oprogramowania, zarządzanie aplikacjami krytycznymi oraz wskazywania rozwiązań, które zapewnią prawidłowe wdrożenie Windows 8. Pakiet jest dostępny bezpłatnie ze stron Microsoft.

**Wirtualizacja Windows**

Szereg rozwiązań wirtualizacji dostępny w i dla rodziny Windows umożliwia uruchamianie aplikacji wewnątrz maszyny wirtualnej. Dzięki przeniesieniu jej działania na platformę wirtualną zapewniana jest pełna kompatybilność działania.

# 6. Klient Hyper-V

Windows 8 zawiera Hyper-V, który jest technologią wirtualizacji klasy Enterprise stanowiącą integralną część środowiska Windows Server 2012. Wirtualizacja stanowi rozwiązanie umożliwiające uruchomienie dodatkowego systemu operacyjnego pracującego w izolacji, ale z zapewnieniem dostępu do elementów sprzętowych takich jak karty sieciowej czy dyski. Hyper-V sprawdza się w wielu scenariuszach umożliwiając testowanie aplikacji, rozwiązań IT oraz zapewniając kompatybilność.

## 6.1 Konfiguracja funkcji zabezpieczeń

Po zainstalowaniu roli Hyper-V wszystkie instancje systemu operacyjnego na komputerze fizycznym uruchamiane są jako maszyny wirtualne. Dotyczy to również instancji Windows 8, która została użyta do utworzenia i zarządzania maszynami wirtualnym. Ta instancja nazywa się systemem operacyjnym zarządzania.

Hypervisor będący głównym elementem funkcji Hyper-V stanowi cienką warstwę programową między sprzętem a systemem operacyjnym. Hypervisor umożliwia pracę wielu systemom operacyjnym na fizycznym komputerze w tym samym czasie.

Istnieją dwa obszary obejmujące tematykę ochrony środowisk wirtualnych:

- zabezpieczenia systemów operacyjnych zarządzania,
- zabezpieczenia maszyn wirtualnych.

### 6.1.1 Zabezpieczanie systemów operacyjnych zarządzania

Dostarczając komputer każdorazowo wykonujemy czynności, które mają zwiększyć jego ogólne bezpieczeństwo. Przykładowo - instalacja oddzielnych kart sieciowych w celu separacji czynności zarządzania systemem operacyjnym i maszynami wirtualnymi od zapewnienia dostępu maszynom wirtualnym do logicznych magazynów danych.

Funkcja Hyper-V zawiera narzędzia zarządzania Hyper-V, na które składają się:

- konsola Menedżera funkcji Hyper-V,
- moduł Hyper-V dla Windows PowerShell.

Dzięki modułowi Hyper-V dla Windows PowerShell uprawnieni administratorzy mają możliwość zdalnego zarządzania serwerami z funkcją Hyper-V.

**Sieci Hyper-V**

Klient Hyper-V umożliwia konfigurację różnego rodzaju przełączników wirtualnych, dzięki czemu można osiągnąć pożądane rozwiązanie zapewniające komunikację między maszynami wirtualnymi.

W ramach klienta Hyper-V można użyć następujących typów przełączników wirtualnych:

- Zewnętrzny
  Przełączniki tego typu umożliwiają komunikację poprzez fizyczną kartę sieciową, dzięki czemu każda maszyna wirtualna ma zapewniony dostęp do sieci fizycznej.
- Wewnętrzny

Wewnętrzny przełącznik wirtualny może być używany tylko przez maszyny wirtualne uruchomione na tym komputerze fizycznym oraz do komunikacji między maszynami wirtualnymi a komputerem fizycznym. Wewnętrzny przełącznik wirtualny nie zapewnia łączności z siecią fizyczną.

- Prywatny
  Ten typ przełącznika może być używany tylko przez maszyny wirtualne uruchomione na tym komputerze fizycznym.

**Ochrona dedykowanych magazynów danych**

Pliki, które zawierają informacje konfiguracyjne na temat każdej maszyny wirtualnej są przechowywane domyślnie w lokalizacji:

**%ProgramData%\Microsoft\Windows\Hyper-V**

Pliki konfiguracyjne maszyn wirtualnych są relatywnie małe i dlatego domyślna lokalizacja jest akceptowalna dla większości scenariuszy. Pliki VHD mogą być rodzaju dynamicznego lub o stałym rozmiarze.

Rozmiar plików dynamicznych ***.vhdx** zwiększa się wraz ze zmianą danych. Pliki o stałym rozmiarze mają od samego początku dostęp do całkowitego, zadeklarowanego przy ich tworzeniu rozmiaru. Przykładowo dysk o rozmiarze 80GB w przypadku dysków dynamicznych będzie zajmował tylko tyle miejsca, ile potrzebują dane. Natomiast dysk o stałym rozmiarze od samego początku będzie miał taki rozmiar na dysku fizycznym.

Rekomendowane jest wykorzystywanie dysków o stałym rozmiarze dla zapewnienia wysokiej wydajności oraz zapobieganiu niespodziewanemu wyczerpaniu miejsca.

Domyślnie pliki **.vhdx** są przechowywane w lokalizacji **%users%\Public\Documents\Hyper-V\Virtual Hard Disks**. Powyższa ścieżka może być zmieniona w ramach ustawień z poziomu Menedżera funkcji Hyper-V. Wybierając inną lokalizację należy upewnić się, że do folderu zostały nadane uprawnienia zgodnie z poniższą tabelą.

| Obiekt | Uprawnienia | Dotyczy |
|---|---|---|
| Administratorzy<br>System | Pełna kontrola | Ten folder, podfoldery i pliki |
| Twórca-Właściciel | Pełna kontrola | Tylko podfoldery i pliki |
| Maszyny wirtualne | Tworzenie plików/Zapis danych<br>Tworzenie folderów/Dołączanie danych<br>Wyświetlanie zawartości folderu//Odczyt danych<br>Odczyt atrybutów<br>Odczyt atrybutów rozszerzonych<br>Odczyt uprawnień | Ten folder, podfoldery i pliki |

W celu uproszczenia zarządzania można przechowywać wszystkie pliki konfiguracyjne, pliki dysków wirtualnych, pliki VFD oraz pliki ISO w oddzielnych folderach na tym samym woluminie. Przykładowa struktura reprezentująca takie rozwiązanie może przedstawiać się następująco:

- **V:\Virtualization Resources\Virtual Machines**
- **V:\Virtualization Resources\Virtual Hard Disks**
- **V:\Virtualization Resources\Virtual Floppy Disks**
- **V:\Virtualization Resources\ISO files**

Instalując oprogramowanie antywirusowe w systemie operacyjnym z rolą Hyper-V należy skonfigurować wykluczenie skanowania w czasie rzeczywistym dla folderów przechowujących pliki maszyn wirtualnych oraz programów **vmms.exe** i **vmwp.exe** znajdujących się w lokalizacji **C:\Windows\System32**. Nie wykonanie powyższej czynności może powodować błędy przy tworzeniu i uruchamianiu maszyn wirtualnych.

### 6.1.2 Zabezpieczenia maszyn wirtualnych

Utrzymywanie wielu maszyn wirtualnych powoduje pewne konsekwencje w zakresie bezpieczeństwa narzucając konieczność dodatkowej konfiguracji ustawień. Część z nich można zrealizować na poziomie maszyny wirtualnej, inne z poziomu Menedżera Hyper-V.

**Konfiguracja maszyn wirtualnych**

Poniżej przedstawiono zalecenia i rekomendacje w kontekście konfiguracji maszyn wirtualnych na komputerach Windows 8 z uruchomionym Hyper-V.

- Określenie miejsca przechowywania plików maszyn wirtualnych oraz plików VHD.
  Miejsce, w którym będą przechowywane pliki maszyn wirtualnych oraz pliki VHD powinno być wybrane z największą starannością o ich bezpieczeństwo. Należy pamiętać, że dostęp do tych danych jest praktycznie równoważny dostępowi do konfiguracji i zawartości maszyn wirtualnych.
- Określenie ilości pamięci operacyjnej oraz procentowy limit użycia procesora, które zostaną przyznane maszynom wirtualnym.
  Wprowadzenie limitów w zakresie ilości pamięci operacyjnej oraz możliwego użycia procesora(-ów) przez maszyny wirtualne zapewnia zachowanie wysokiej dostępności i wydajności środowiska.
- Konfiguracja dostępu wyłącznie do potrzebnych urządzeń masowych.
  Należy zapewnić dostęp maszynom wirtualnym tylko do wymaganych urządzeń masowych, aby nie stanowiły one źródła dostępu do danych, które mogą być użyte np. do instalacji niepożądanego oprogramowania.
- Włączenie wsparcia w zakresie synchronizacji czasu.
  Synchronizacja czasu stanowi jeden w podstawowych elementów poprawnej i bezpiecznej konfiguracji środowiska, wymaganym na przykład przy wdrażaniu polityk kontroli. Z tego powodu należy zapewnić instalację usług integracji w obrębie maszyn wirtualnych.
- Konfiguracja maszyn wirtualnych na zbliżonym poziomie zabezpieczeń w obrębie tego samego komputera fizycznego.

Maszyny wirtualne są tak samo narażone na niebezpieczeństwo jak komputery fizyczne. Z tego powodu należy zadbać o zbliżony poziom zabezpieczeń maszyn wirtualnych w obrębie komputera, na którym są one uruchomione.

- Usunięcie zbędnych plików VHD zawierających poufne dane.
  Dla maszyn wirtualnych, które przechowują ważne i poufne dane należy ustalić proces kasowania plików VHD kiedy już nie będą one potrzebne. W tym celu można użyć narzędzie SDelete v.1.61 (http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx).
- Bezpieczne przechowywanie plików migawek.
  Migawka (ang. snapshot) jest obrazem maszyny wirtualnej wykonanym w określonej chwili czasu pozwalającym na powrócenie do jej stanu w przyszłości.

# 7. Ład korporacyjny, zarządzanie ryzykiem oraz zgodność ze standardami w IT (IT GRC)

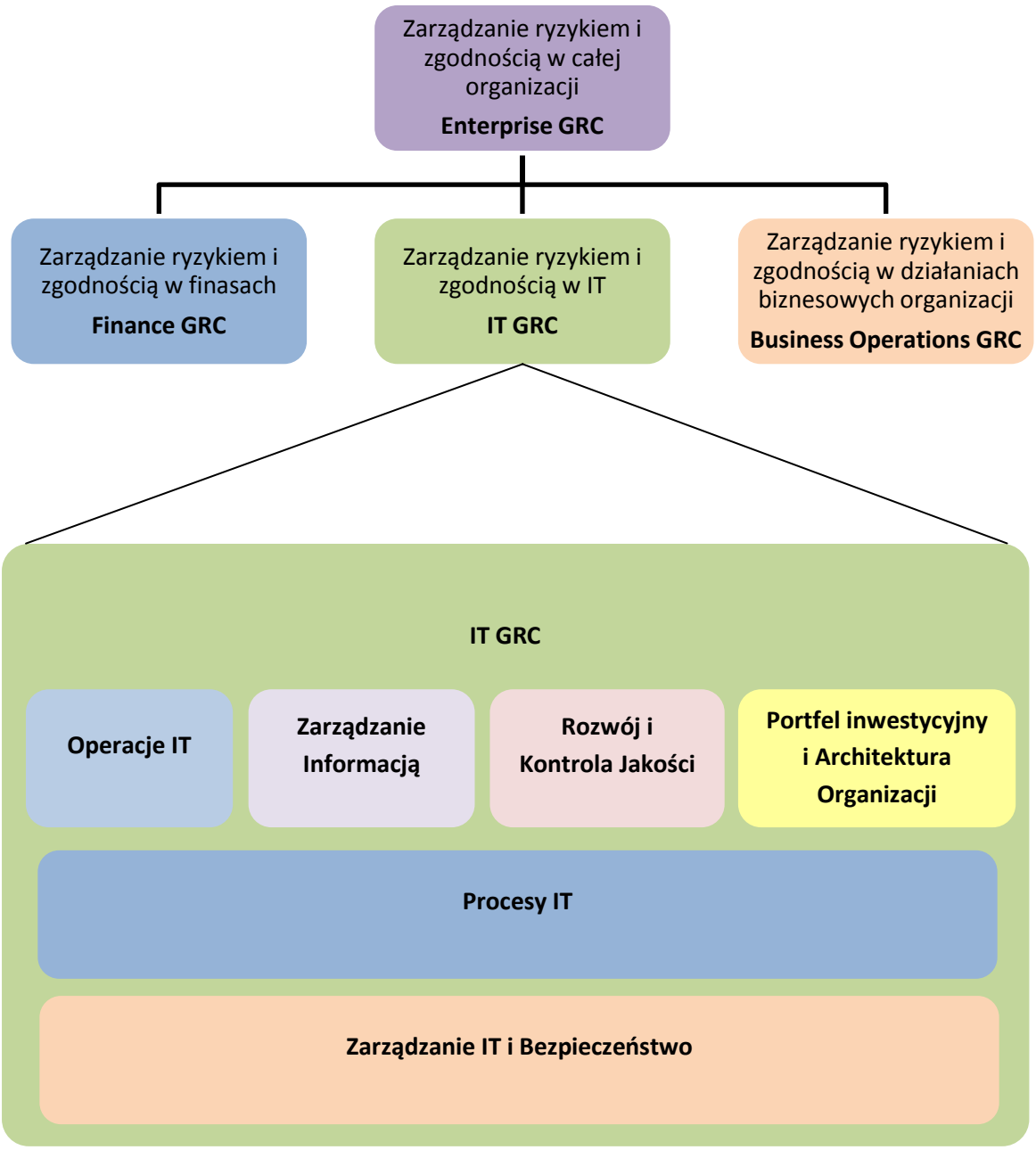
System ładu korporacyjnego, zarządzania ryzykiem i zgodności ze standardami - GRC (ang. Governance, Risk, and Compliance), to system, na który składają się ludzie, procesy i technologie w ramach całej infrastruktury, przynoszący danej organizacji następujące korzyści:

- Ograniczenie ryzyka
- Ujednolicenie procesów biznesowych
- Poprawa efektywności
- Uwolnienie zasobów
- Usprawnienie zarządzania zmianami

W poniższym rozdziale zostały przedstawione zastosowania produktów Microsoft w kontekście bazowych ustawień systemu korzystając z IT Governance, Risk, and Compliance (IT GRC) Process Management Pack (PMP) dla systemu Microsoft System Center Service Manager 2012, w taki sposób, aby utrzymanie ładu korporacyjnego, zarządzania ryzykiem i zgodności ze standardami w IT przyniosło korzyści organizacji wspierających system IT GRC. Process management pack jest pakietem administracyjnym dla produktu System Center Service Manager, który wspomaga proces zarządzania IT bazując na regulacjach, międzynarodowych standardach oraz najlepszych praktykach, takich jak Microsoft Operations Framework (MOF) oraz Information Technology Infrastructure Library (ITIL). IT GRC Process Management Pack wraz z ustawieniami bazowymi systemu pomaga zapewnić automatyczny proces zgodności dla komputerów klienckich oraz serwerów. W celu uzyskania dodatkowych informacji na temat rozwiązań Microsoft wspierających system GRC, należy zapoznać się z przewodnikami Compliance Solution Accelerators[77] opisanymi na stronach przewodników Microsoft Solution Accelerators.

Poniższy rysunek przedstawia umiejscowienie IT GRC w strukturze zarządzania ryzykiem i zgodnością całej organizacji. IT GRC Process Management Pack skupia się wyłącznie na systemie IT GRC bez uwzględniania innych aspektów zarządzania ryzykiem i zgodnością całej organizacji.

[77] http://go.microsoft.com/fwlink/?LinkId=199861




Rys. 7.1 Umiejscowienie IT GRC w strukturze zarządzania ryzykiem i zgodnością całej organizacji

## 7.1. Wprowadzenie

W rozdziale tym zostały opisane procesy oraz wskazane dodatkowe zasoby opisujące wykorzystanie IT GRC Process Management Pack dla produktu System Center Service Manager. W celu uzyskania dodatkowych informacji należy zapoznać się z przewodnikami:

- IT GRC Process Management Pack Deployment Guide. Przewodnik ten opisuje proces wdrożenia IT GRC Process Management Pack.

- IT GRC Process Management Pack Operations Guide. Przewodnik ten zawiera informacje na temat wykorzystania IT GRC Process Management Pack oraz budowania własnych pakietów.

- IT GRC Process Management Pack Developers Guide. Przewodnik ten opisuje proces dostosowania i konfiguracji do własnych potrzeb IT GRC Process Management Pack.

Wymienione przewodniki dostępne są do pobrania ze strony IT GRC Process Management Pack SP1 for System Center Service Manager[78] w dziale Centrum Pobierania Microsoft. W celu uzyskania dodatkowych informacji należy zapoznać się z dodatkowymi zasobami:

- IT Compliance Management Library Deployment Guide, który zawarty jest w każdej bibliotece obejmującej zarządzanie zgodnością ze standardami IT. Przewodnik ten zawiera informacje na temat wdrożenia IT GRC Process Management Pack oraz pakietów konfiguracyjnych Microsoft System Center Configuration Manager.
- Microsoft System Center Service Manager[79].
- Microsoft System Center Configuration Manager[80].

## 7.2. Omówienie i budowa IT GRC PMP

IT GRC Process Management Pack dostarcza informacji na temat możliwości i sposobu zarządzania procesem IT GRC w obrębie całej organizacji oraz określa możliwości automatyzacji tego procesu. IT GRC Process Management Pack dostarcza możliwości wykorzystania poprzez importowanie gotowych bibliotek zgodności ze standardami, które mogą być zastosowane w celu określenie punktów kontrolnych niezbędnych dla wymagań stawianych systemowi IT GRC w organizacjach.

Biblioteki zgodności przeznaczone dla IT GRC Process Management Pack określają punkty kontrolne wykorzystywane do zapewnienia zgodności z dokumentami organów nadrzędnych IT GRC, powołując się na wytyczne określone przez międzynarodowe, rządowe oraz branżowe instytucje opracowujące ogólne wytyczne IT GRC. Dokumenty te zawierają wytyczne oraz określają wymagania szczegółowe stawiane procesom biznesowym oraz technologiom różnych sektorów organizacji i instytucji.

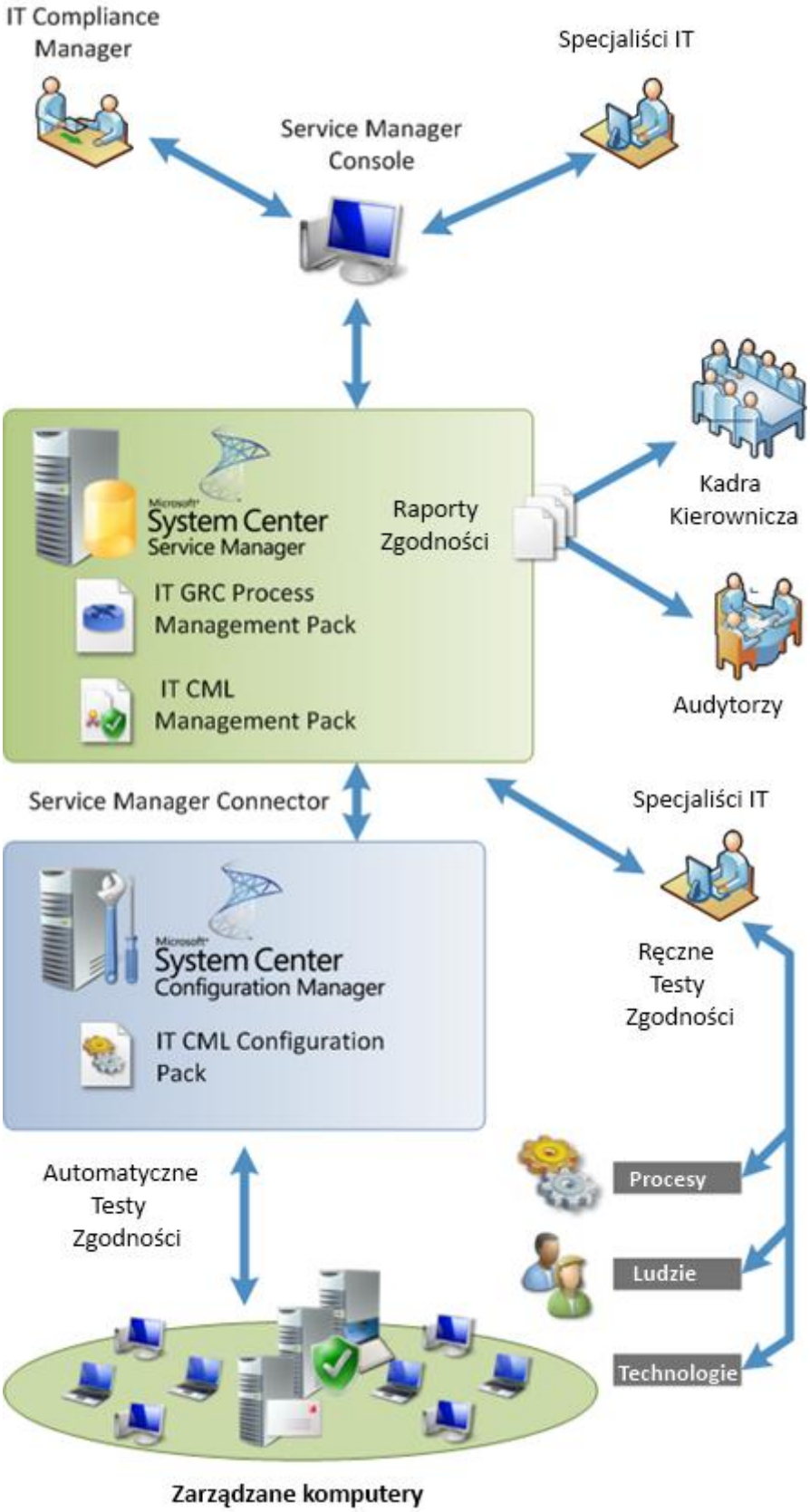
Dodatkowe pakiety administracyjne i informacje dla produktów System Center dostępne są Microsoft System Center Marketplace [81] oferują zintegrowane rozwiązania i automatyzację, pomagając organizacjom w sprawnym spełnieniu wymagań GRC.

Korzyści wynikające ze stosowania integracji produktów System Center Service Manager, System Center Configuration Manager oraz System Center Operations Manager:

- Efektywny sposób na monitorowanie, sprawdzenie oraz raportowanie stanu zgodności wdrożonych produktów Microsoft.
- Stosowanie jednoczesne wymienionych rozwiązań wspomaga zrozumienie i połączenie złożonych celów biznesowych, którym musi sprostać infrastruktura organizacji.

Przedstawiony rysunek poniżej ilustruje rozwiązanie IT GRC Process Management Pack.

[78] http://go.microsoft.com/fwlink/?LinkId=201578
[79] http://go.microsoft.com/fwlink/?LinkId=155958
[80] http://go.microsoft.com/fwlink/?LinkId=206193
[81] http://go.microsoft.com/fwlink/?LinkId=82105




Rys.7.2.1 - Ilustracja rozwiązania IT GRC Process Management Pack

Kadra kierownicza oraz audytorzy wykorzystują raporty IT GRC Process Management Pack w celu przeanalizowania pod kątem zgodności i poddania ocenie procesów IT GRC organizacji. Ta grupa użytkowników przeważnie wymaga dostępu tylko do odczytu oraz możliwości wykonania raportów dotyczących informacji zarządzanych przez proces GRC Process Management Pack.

W przedstawionym rozwiązaniu, IT Compliance Manager oraz specjaliści IT sterują scentralizowanym procesem zapewnienia zgodności IT GRC korzystając z narzędzia Service Manager Console. Narzędzie to zapewnia osobie pełniącej rolę IT Compliance Manager możliwość zarządzania wieloma programami IT GRC oraz postawionymi celami kontrolnymi, które odnoszą się do wytycznych oraz wymagań szczegółowych przedstawionych w dokumentach wydanych przez organy nadrzędne.

Specjaliści IT korzystając z centralnego narzędzia mogą dokonać oszacowania wyników zgodności IT GRC dla wszystkich celów kontrolnych określonych w systemie IT GRC. Wyniki z przeprowadzonych testów zgodności mogą być osiągnięte w następujący sposób:

- **Automatycznie.** Funkcjonalność zarządzania docelową konfiguracją – (ang. Desired Configuration Management (DCM)) zawarta w System Center Configuration Manager oraz IT CML Configuration Packs, wspomaga osiągnąć rezultaty zgodności dla zautomatyzowanych celów kontrolnych. Automatyczne cele kontrolne w znacznym stopniu redukują nakład pracy wymagany do osiągnięcia zgodności IT GRC.
- **Ręcznie** – specjaliści IT mogą w sposób ręczny ocenić wyniki zgodności:
    - **Technologia –** zawiera ustawienia zgodności IT GRC, które nie mogą być oszacowanie metodami automatycznymi
    - **Procesy –** zawiera procesy zgodności stosowane w organizacji i powiązane z IT GRC, takie jak właściwe i bezpieczne usuwanie danych z systemów wycofywanych z organizacji a zawierających informacje wrażliwe.
    - **Ludzie –** zawiera aspekty ergonomii pracy w zakresie zgodności z IT GRC, takie jak dokładne sprawdzenie pracownika przed udzieleniem dostępu do informacji wrażliwych

Zastosowanie integracji opartej na produktach System Center Service Manager oraz System Center Configuration Manager zapewnia następujące funkcjonalności i korzyści:

- System Center Configuration Manager analizuje docelową oczekiwaną konfigurację z aktualną konfiguracją zarządzanych zasobów wykorzystując pakiety DCM, które zostały umieszczone poziomie konfiguracji elementu, aby zapewnić obsługę celów kontrolnych.
- Element konfiguracji znajdujący się w Service Manager CMDB (baza danych zarządzania konfiguracją) może być automatycznie wypełniony informacjami dostarczonymi przez System Center Configuration Manager.
- Przeprowadzone testy zgodności dla zautomatyzowanych celów kontrolnych mogą być aktualizowane w Service Manager CMDB

Produkt System Center Service Manager umożliwia tworzenie i wykorzystanie własnych łączników (ang. connector), za pomocą, których można zdefiniować połączenia z innymi systemami, umożliwiając zebranie informacji na temat zgodności z innych systemów stosowanych w organizacji. Funkcjonalność ta rozszerza proces automatyzacji testów i zbierania wyników z wcześniej zdefiniowanych celów kontrolnych.

## 7.3. Korzyści wynikające ze stosowania IT GRC PMP

Rozwiązanie zarządzania procesem zgodności oraz zarządzania ryzykiem oferowane przez IT GRC Process Management Pack, IT Compliance Management Libraries, System Center Service Manager, oraz System Center Configuration Manager oferuje następujące możliwości i korzyści:

- **Mapowanie celów biznesowych bezpośrednio na cele i działania IT GRC.** Mechanizm ten w łatwy sposób odwzorowuje cele biznesowe określone przez kadrę zarządzającą na cele i działania dla programu zgodności działu IT. Rozwiązanie to:
    - Zawiera bibliotekę tysięcy dokumentów zgodności cytowanych dokumentów urzędowych pochodzących z setek dokumentów urzędowych, które zostały dostosowane w ujednolicony zestaw celów kontrolnych.
    - Tworzy bibliotekę zgodności zawierające cele kontrolne, działania i ustawienia dla kluczowych produktów Microsoft oraz nowych systemów Windows 8 oraz Windows Server 2012 w postaci zbioru zaktualizowanych ustawień bazowych dla konfiguracji.
- **Zauważalne zwiększenie zgodności ze standardami –** użytkownicy w łatwy sposób mogą zidentyfikować niezgodności korzystając z raportów IT GRC Process Management Pack.
- **Utworzenie pojedynczego punktu sterowania zarządzaniem programów IT GRC** - organizacje mogą zarządzać wieloma programami zgodności IT GRC spełniając jednocześnie wymagania wielu złożonych dokumentów urzędowych. IT GRC Process Management Pack wprowadza kontrolę obejmującą wszystkie źródła dokumentów urzędowych, redukując problemy małej wydajności w przypadku regulacji wzajemnie się pokrywających.
- **Wykorzystanie najlepszych branżowych praktyk do zarządzania procesami** – Procesy zaimplementowane w IT GRC PMP zostały utworzone w oparciu o najlepsze praktyki wykorzystywane do zarządzania incydentami i zarządzania zmianami bazując na MOG oraz ITIL.
- **Redukcja nakładu pracy** – Proces automatyzacji testów uwzględniający integrację funkcjonalności DCM w System Center Configuration Manager redukuje ręczny nakład pracy, który jest wymagany do przeprowadzanie testów sprawdzających zgodność ze standardami.
- **Obniżenie kosztów kontroli i raportowania** – Redukcja nakładu pracy poświęconego na przygotowanie i wykonywania czynności kontrolujących stan zgodności ze standardami wpływa na obniżenie kosztów związanych z przygotowaniem audytów.
- **Minimalizacja ryzyka** – Użytkownicy mogą w łatwy sposób zidentyfikować niezgodności, a co za tym idzie mogą kontrolować na bieżąco występujące ryzyko, co w konsekwencji prowadzi do zmniejszenia ryzyka związanego z zapewnieniem zgodności.
- **Ułatwienie zmian zachodzących w biznesie** – Biznes wymaga ciągłych zmian, w związku z tym opisywane rozwiązanie zarządzania zgodnością wykrywa zachodzące zmiany z zarządzanej infrastrukturze i stosuje odpowiednie mechanizmy kontroli zgodności.
- **Przygotowanie do audytów zewnętrznych** - Przygotowane predefiniowane raporty IT Compliance Management Pack odzwierciedlają większość informacji na temat zgodności ze standardami wymaganych przez audytorów. Wykorzystując te raporty organizacje mogą w szybki i łatwy sposób przedstawić stan zgodności ze standardami na prośbę audytorów, konsultantów lub Zarządu organizacji.

- **Podejmowanie czynności korygujących w celu wyeliminowania niezgodności -** Osoby pełniące funkcje IT GRC Manager mogą zidentyfikować niezgodne ze standardami ustawienia konfiguracji i korzystając z procesu zarządzania i śledzenie incydentów, w łatwy sposób mogą zlecić specjalistom IT zadanie przywrócenia ustawień konfiguracji do stanu zapewniającego zgodność ze standardami.

## 7.4. Terminy i definicje

W poniższej tabeli przedstawiono podstawowe terminy i pojęcia związane z wykorzystaniem IT GRC Process Management Pack.

| Termin lub pojęcie | Opis |
|---|---|
| Regulacje dotyczące ładu korporacyjnego, zarządzania ryzykiem oraz zgodności ze standardami (GRC) (ang. GRC authority document) | Dokumenty obejmujące regulacje w zakresie GRC zawierają wymagania opublikowane przez organy urzędowe w postaci rozporządzeń lub wytycznych, opisanych standardów lub polityki organizacji. Regulacje GRC mogą obejmować wymagania dotyczące procesów minimalizacji ryzyka, które określają specyficzne bądź ogólne opisy konfiguracji, użytkowania lub inne parametry obsługi, które dotyczą organizacji, personelu, procesów biznesowych oraz technologii. Różnorodne regulacje zwracają uwagę na te same aspekty ryzyka zgodności, pomimo to, dokumenty te pozwalają na spojrzenie z różnych perspektyw często odmiennych strategii minimalizacji ryzyka oraz stawianych wymagań. Wymagania wskazane przez regulacje GRC przekształcone na cele kontrolne i odnoszą się do czynności kontrolnych zaprojektowanych w celu zapewnienia, iż towarzyszące ryzyka są minimalizowane w odpowiedni i uzasadniony sposób.<br>IT GRC Process Management Pack zawiera cele kontrolne, przytoczone z odpowiednich regulacji i spełniających stawiane im wymagania. Regulacje obejmują swoim zakresem ustawy dotyczące finansów, polityki prywatności oraz ochrony zdrowia, takie jak Sarbanes–Oxley (SOX), European Union Data Protection Directive (EUDPD), oraz Health Insurance Portability and Accountability Act (HIPAA).<br>Pełna lista regulacji zawarta w produkcie IT GRC Process Management Pack, znajduje się w sekcji **Library,** konsoli Service Manager - Library **\| Authority Documents** . |
| Program | Definiuje zbiór ryzyk, celów kontrolnych, działań oraz wyników zgodności. Programy definiują również role użytkownika i towarzyszących mu praw w obrębie określonego zakresu, poprzez zdefiniowanie użytkownikowi odpowiednich uprawień. Zdefiniowane zakresy zezwalają osobie pełniącego role menadżera programu na zarządzanie ryzykiem i kontrolę w obrębie tego programu.<br>Programy zostały utworzone w celu określenia zgodności z jednym lub wieloma dokumentami regulacji oraz ryzyk towarzyszących programowi zarządzania IT GRC. |
| Cele Kontrolne (ang. Control objectives) | Sprecyzowane określenie wymagań i wytycznych zawartych w regulacjach GRC. Cele kontrolne mogą być wymagane przez jeden lub wiele zbiorów regulacji w celu spełnienia jednego lub wielu czynności kontrolnych. |

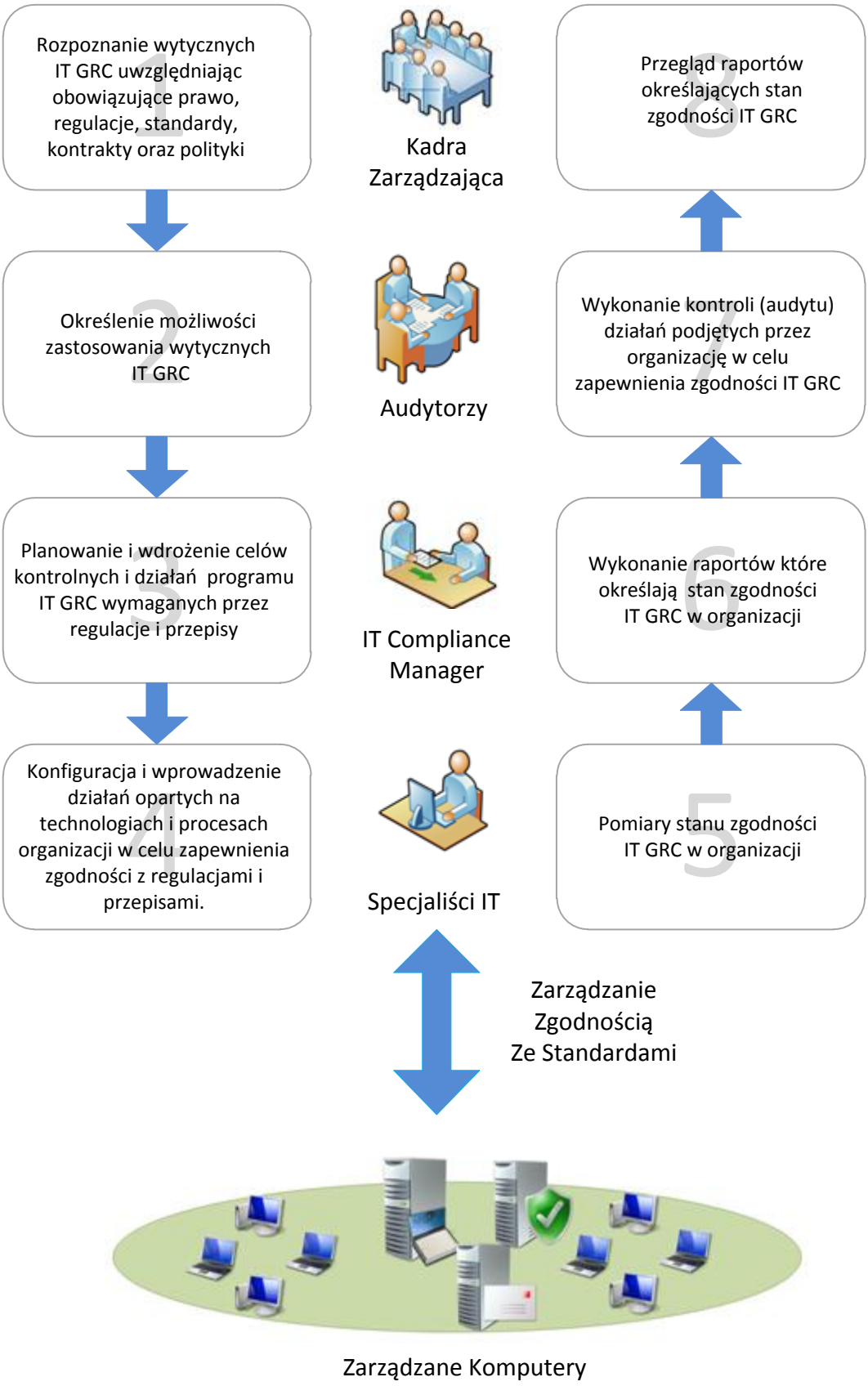
| | |
|---|---|
| Powoływanie się na dokumenty organów w zakresie regulacji (ang. Authority dokument citation) | Odniesienie w obrębie celów kontrolnych do jednego lub wielu szczegółowych wymagań w obrębie obowiązujących przepisów i regulacji. |
| Czynności kontrolne (ang. Control Activities) | Szczegółowe, podlegające zaskarżeniu stopnie konfigurowania i obsługi produktu poprzez określenie zgodności z wymaganiami celów kontrolnych. Działania kontrolne mogą obejmować jeden lub wiele celów kontrolnych. |
| Ryzyko (ang. Risk) | Możliwość wystąpienia szansy lub zagrożenia, mającego wpływ na osiągnięcie wyznaczonych celów biznesowych lub celów IT danej organizacji. Ryzyko jest mierzone z wykorzystaniem określeń wpływ lub prawdopodobieństwo. Pojęcie ryzyka związane jest celami kontrolnymi, czynnościami kontrolnymi lub innymi ryzykami. |
| Próg (ang. Threshold) | Minimalny udział procentowy obowiązujący dla zarządzanych jednostek w zakresie programu, który musi być zgodny dla czynności kontrolnych, aby został uznany za zgodny. |
| Zatwierdzanie przepływu pracy (ang. Approval workflow) | Proces, w którym wszystkie zmiany zachodzące dla jednostek zarządzanych przez IT GRC PMP są zatwierdzone. Zazwyczaj zmiany wykonuje ten sam proces zatwierdzania jak w przypadku żądania zmiany przez System Center Service Manager. |
| Automatyzacja (ang. Automation) | Zastosowanie komponentów IT w celu wykonania zadań lub kroków wymaganych do rozwiązania jednego lub wielu celów kontrolnych, które zawierają automatycznie zgormadzone wyniki zgodności IT GRC. |
| Rezultaty testów kontroli (ang. Managed entity result) | Rezultaty testów zgodności, które zostały wykonane na zarządzanej jednostce, takiej jak pojedynczy komputer. |

Tabela 7.4.1 Terminy i definicje związane z IT GRC

## 7.5. Cykl życia procesu zgodności w oparciu o IT GRC PMP

Narzędzia IT GRC Process Management Pack, System Center Service Manager, oraz System Center Configuration Manager dostarczają zamknięty i pełny cykl życia zarządzania dla procesu zgodności IT. Cykl życia zgodności integruje procesy oraz wiedzę poprzez mechanizm mapowania szczegółowych wymagań w obrębie obowiązujących przepisów i regulacji na konfigurację i działania dla określonych produktów a następnie śledzenie zachodzących tam zmian poprzez raporty kontrolne.

Poniższy rysunek ilustruje główne zadania i obowiązki osób zaangażowanych w cykl życia zgodności IT w obrębie każdego kroku procesu.




Rys. 7.5.1 - Główne zadania i obowiązki osób zaangażowanych w cykl życia procesu zgodności IT

Należy zwrócić uwagę, że przepływ cyklu życia zgodności IT zaprezentowany na rysunku 2.5.1 Jest ściśle określony na wysokim szczeblu kadry zarządzającej oraz wskazuje precyzyjny przepływ procesów pomiędzy rolami, ale celowo został uproszczony. Każdy osoba wykonująca swoją pracę, musi komunikować się z innymi na temat następujących cech wymagań stawianych przez IT GRC:

**Zastosowanie** – cecha ta zawiera proces rozpoznania wymagań w obrębie obowiązujących przepisów i regulacji, które są znaczące i pełnią istotną rolę dla organizacji. Na przykład Payment Card Industry Data Security Standard (PCI DSS) będzie dotyczyło organizacji prowadzących działalność biznesową z użytkownikami kart kredytowych przetwarzających ich dane zawarte na kartach kredytowych w ramach utrzymywanej infrastruktury IT.

**Wystarczalność** – cecha ta zawiera proces rozpoznania wymagań w obrębie obowiązujących regulacji i rozpoznanie czy przedstawione regulacje są wystarczające i pozwolą na zapewnienie zgodności. Na przykład: ustawienie minimalnej długości hasła na wartość 8 znaków dla wszystkich użytkowników jest elementem wystarczającym dla wszystkich obowiązujących i stosowanych regulacji.

**Zasadność** – cecha ta zawiera proces rozpoznania wymagań w obrębie obowiązujących regulacji i rozpoznanie czy przedstawione regulacje są rozsądne, racjonalne i praktyczne do wdrożenia. Na przykład, decyzja o wymaganiu minimalnej długości hasła o wartości 16 znaków, może być technicznie wykonalna, ale nie praktyczna do wdrożenia z uwagi na fakt, iż użytkownicy mogą nie zapamiętać swoich haseł.

Dodatkowe informacje na temat stosowanie IT GRC w kontekście cyklu życia usług IT oraz innych ról użytkowników działu IT, należy zapoznać się z dokumentem Governance, Risk, and Compliance Service Management Function[82] w kontekście MOF 4.0.

## 7.6. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na temat bezpieczeństwa systemu Windows 8 opublikowanych na stronach Microsoft.com

- Compliance Solution Accelerators[83]
- Governance, Risk, and Compliance Service Management Function[84] w oparciu o MOF 4.0.
- IT GRC Process Management Pack SP1 for System Center Service Manager[85].
- Microsoft System Center Marketplace.[86]
- System Center Configuration Manager.[87]
- System Center Service Manager.[88]
- System Center Service Manager team blog.[89]

[82] http://go.microsoft.com/fwlink/?LinkId=115630
[83] http://go.microsoft.com/fwlink/?LinkId=199861
[84] http://go.microsoft.com/fwlink/?LinkId=115630
[85] http://go.microsoft.com/fwlink/?LinkId=201578
[86] http://go.microsoft.com/fwlink/?LinkId=82105
[87] http://go.microsoft.com/fwlink/?LinkId=206193
[88] http://go.microsoft.com/fwlink/?LinkId=155958
[89] http://blogs.technet.com/servicemanager/

## 8. Narzędzie Security Compliance Manager (SCM) w praktyce

Microsoft Security Compliance Manager (SCM)[90] jest bezpłatnym narzędziem udostępnionym przez zespół Microsoft Solution Accelerators, pozwalającym na szybką konfigurację i zarządzanie ustawieniami komputerów przez zasady grupowe GPO oraz produkt System Center Configuration Manager. SCM udostępnia gotowe zasady grupowe do wdrożenia w organizacji oraz paczki konfiguracyjne DCM, w pełni przetestowane i wspierane. Elementy te oparte są na rekomendacjach zawartych w dokumencie zawartych w niniejszym przewodniku i najlepszych praktykach w środowiskach produkcyjnych, pozwalają także na ich konfigurację.

**Korzyści wynikające z zastosowania narzędzia SCM**

**Integracja z systemem System Center 2012 Process Pack for IT GRC:** Konfiguracje ustawień dla produktów są zintegrowane w paczkach Process Pack for IT GRC zapewniając monitorowanie i raportowanie czynności zapewniających zgodność z zaleceniami.

**Główne źródło wsparcia:** Funkcja importowania ustawień zapewnia maksymalne korzyści wykorzystania zasad grupy w celu utworzenia wzorcowego komputera zapewniającego maksymalną ochronę.

**Konfiguracja komputerów autonomicznych (ang. standalone):** Proces wdrożenia dostosowanych konfiguracji ustawień dla komputerów nieprzyłączonych do domeny korzystając z nowej funkcjonalności GPO Pack.

**Aktualne wytyczne z zakresu bezpieczeństwa:** Osiągnięcie korzyści poprzez zastosowanie dogłębnej znajomości aspektów bezpieczeństwa oraz najlepszych praktyk umieszczonych w najnowszych wytycznych przewodnika bezpieczeństwa. Zastosowując asystowaną pomoc w zmniejszaniu obszaru ataków dla systemów Windows w celu minimalizacji ryzyka związanego z bezpieczeństwem teleinformatycznym.

**Zcentralizowane zarządzanie ustawieniami bazowych konfiguracji dla pełnej gamy produktów Microsoft** – Zcentralizowana konsola programu SCM dostarcza ujednolicone i kompleksowe środowisko pozwalające na planowanie, dostosowywanie oraz eksport ustawień bazowych konfiguracji. Narzędzie to zapewnia pełny dostęp do rekomendowanych ustawień bazowych konfiguracji dla systemów klienckich oraz serwerów Windows oraz aplikacji. SCM dodatkowo pozwala na szybkie uaktualnienie najnowszych wytycznych i rekomendacji w zakresie bazowych ustawień konfiguracji stosując kontrole wydawanych wersji ustawień bazowych (baselines).

**Dostosowanie bazowych ustawień konfiguracji do własnych potrzeb i wytycznych**: Proces dostosowywania, porównywania, łączenia i pełny wgląd w bazowe ustawienie konfiguracji został uproszczony i ulepszony. Możliwość dostosowanie ustawień bazowych konfiguracji dla własnych potrzeb korzystając z narzędzia SCM zapewnia szybkie wykonanie duplikatu danego zbioru ustawień zawierającego rekomendowane ustawienia a następnie modyfikację tych ustawień według wytycznych i standardów obowiązujących w danej organizacji.

[90] http://social.technet.microsoft.com/wiki/contents/articles/774.microsoft-security-compliance-manager-scm-en-us.aspx

**Możliwości eksportu ustawień do wielu formatów:** Proces eksportu ustawień bazowych konfiguracji pozwala na wykorzystywanie formatów, takich jak: XLS, Group Policy objects (GPO), Desired Configuration Management (DCM) packs, oraz Security Content Automation Protocol (SCAP) w celu zapewnienia procesu automatyzacji wdrożenia tych ustawień a także monitorowania zgodności z rekomendowanymi ustawieniami.

**Dostępne zbiory ustawień bazowych konfiguracji (ang. Baselines) zapewniają wsparcie dla produktów**: Windows Server 2012, Windows 8, Windows Server 2008 R2 SP1, Windows Server 2008 SP2, Windows Server 2003 SP2, Hyper-V, Windows 7 SP1, Windows Vista SP2, Windows XP SP3, BitLocker Drive Encryption, Internet Explorer 10, Internet Explorer 9, Internet Explorer 8, Microsoft Office 2010 SP1, Microsoft Office 2007 SP2, Exchange Server 2010 SP2 oraz Exchange Server 2007 SP3

**Przyjęte definicje pojęć w programie SCM:**

**Baseline**. Program SCM pracuje na zbiorach ustawień bazowych konfiguracji, które stanowią kolekcje ustawień dla programów zwanych elementami konfiguracji (ang. configuration items (CIs)). Każdy element konfiguracji został stworzony z myślą o zapewnieniu najwyższego poziomu bezpieczeństwa w organizacji.

**CCE-ID (Common Configuration Enumeration) -** CCE-ID – numer identyfikacyjny, unikalny i powiązany bezpośrednio z danym opisem problemu konfiguracji systemu. Opis ten zawiera szczegółowe informacje na temat sposobu zmiany konfiguracji oraz wskazuje na preferowane lub wymagane ustawienie systemu dotyczące kluczy rejestru, plików lub ustawień zasad grupy.

**DCM Configuration Pack** – zbiór ustawień (ang. Configuration Items (CIs)) wykorzystywanych i stosowanych w funkcjonalności Desired Configuration Management (DCM) w systemie Microsoft System Center Configuration Manager w celu zapewnienia skanowania oraz monitorowania komputerów pod katem zapewnienia zgodności z wytycznymi.

**Excel workbook.** Arkusz programu Excel – stosowany do zapoznania się i porównania zbioru ustawień bazowych konfiguracji z innymi zbiorami ustawień bazowych konfiguracji.

**GPO backup folder** - folder zasad grupy (GPO) zawierający obiekty GPO, które można w szybki i elastyczny sposób importować bezpośrednio do usługi katalogowej (Active Directory) w celu dostarczenia żądnych ustawień konfiguracji dla grup komputerów i użytkowników.

**SCAP data file** – pliki w formacie Security Content Automation Protocol (SCAP) spełniające wymagania dla standardów dostarczonych przez National Institute of Standards and Technology (NIST).

**Setting** – ustawienie - najniższy poziom kontroli technicznej odpowiedzialny za stan systemu operacyjnego lub aplikacji. Np. Minimalna długość hasła jest ustawieniem zawiera liczbę całkowitą w celu wymuszenia ustawień specyficznych dla funkcjonalności logowania. Ustawienie posiada 2 rodzaje przechowywanej informacji: definicja ustawienia oraz wartość ustawienia zasady.

**Setting definition**. Definicja ustawienia – zestaw właściwości powiązany z ustawieniami danego systemu operacyjnego lub aplikacji zdefiniowane przez właściciela tworzącego dane ustawienie. Np. gałąź z ustawieniem rejestru, ścieżka lub dane określone przez definicję. Definicja ustawienia nie zmienia swojej wartości po opublikowaniu.

**Setting policy** – ustawienia zasady, jest to zbiór właściwości powiązanych z określonych ustawieniem i zdefiniowanym przez danego użytkownika, dla którego zostało zastosowane to ustawienie zasady. Np. minimalna długość hasła musi być większa lub równa 8.

**Minimalne wymagania systemowe dla instalacji SCM:**

- Windows Vista Service Pack 2 (SP2), Windows Server 2008 R2, Windows Server 2012, Windows 7, Windows 8
- Microsoft .NET Framework 3.5
- SQL Server® 2008 Express edition uruchomiony na komputerze zawierającym instalację programu SCM*
- Uprawnienia administracyjne do uruchomienia z linii komend narzędzia LocalGPO
- 500 MB pamięci RAM lub więcej.
- 40 MB wolnej przestrzeni na dysku twardym.
- Windows® Installer w wersji 4.5.
- Microsoft Visual® C++ 2010 (zawarty w instalatorze programu SCM).
- Microsoft Word lub Microsoft Word Viewer do przeglądania dokumentów.
- Microsoft Excel® 2007 lub nowszy (opcjonalnie do wykonania exportu ustawień w formacie arkusza programu Excel).
- Połączenie internetowe do pobrania ze strony Microsoft aktualnych ustawień bazowych konfiguracji (baselines)

*** Uwaga:** Do poprawnego działania wymagane jest posiadanie przynajmniej Microsoft SQL Server Express. Jeśli nie mamy zainstalowanego serwera SQL, to instalator Microsoft Security Compliance Manager automatycznie go pobierze i zainstaluje.

**Instalacja programu SCM (Security Compliance Manager):**

Program SCM należy pobrać z witryny: Microsoft Security Compliance Manager[91] a następnie uruchomić plik **Security_Compliance_Manager_Setup.exe.**

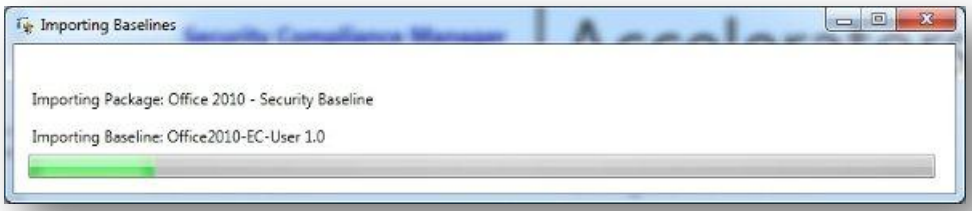
Instalator sprawdzi wymagania wstępne dla produktu SCM i w przypadku braku danego komponentu, zaproponuje instalację tego komponentu lub poinformuje o jego braku, w dalszej kolejności instalator pobierze program Microsoft SQL Server Express i zainstaluje ten produkt na lokalnym komputerze. Po zakończeniu instalacji otrzymamy komunikat o poprawnej instalacji produktu SCM.

[91] http://www.microsoft.com/en-us/download/details.aspx?id=16776

**Uwaga**: **Aktualna wersja programu w chwili tworzenia dokumentu to wersja 3.0.60**. - przed instalacją należy sprawdzić czy dostępna jest nowsza wersja produktu, w przypadku wystąpienia nowszej wersji, zaleca się dokonanie instalacji najnowszej wersji produktu SCM.

## 8.1 Wprowadzenie

Podczas pierwszego uruchomienia SCM, narzędzie przechodzi w tryb „pierwszego użycia" i próbuje połączyć się z witryną Centrum Pobierania Microsoft (ang. Microsoft Download Center), aby pobrać dostępne najnowsze bazowe ustawienia (ang. Baseline). W trybie tym SCM zainstaluje najnowsze gotowe bazowe ustawienia (baseline) przygotowane przez firmę Microsoft do lokalnego folderu komputera, na którym uruchomione zostało narzędzie SCM.



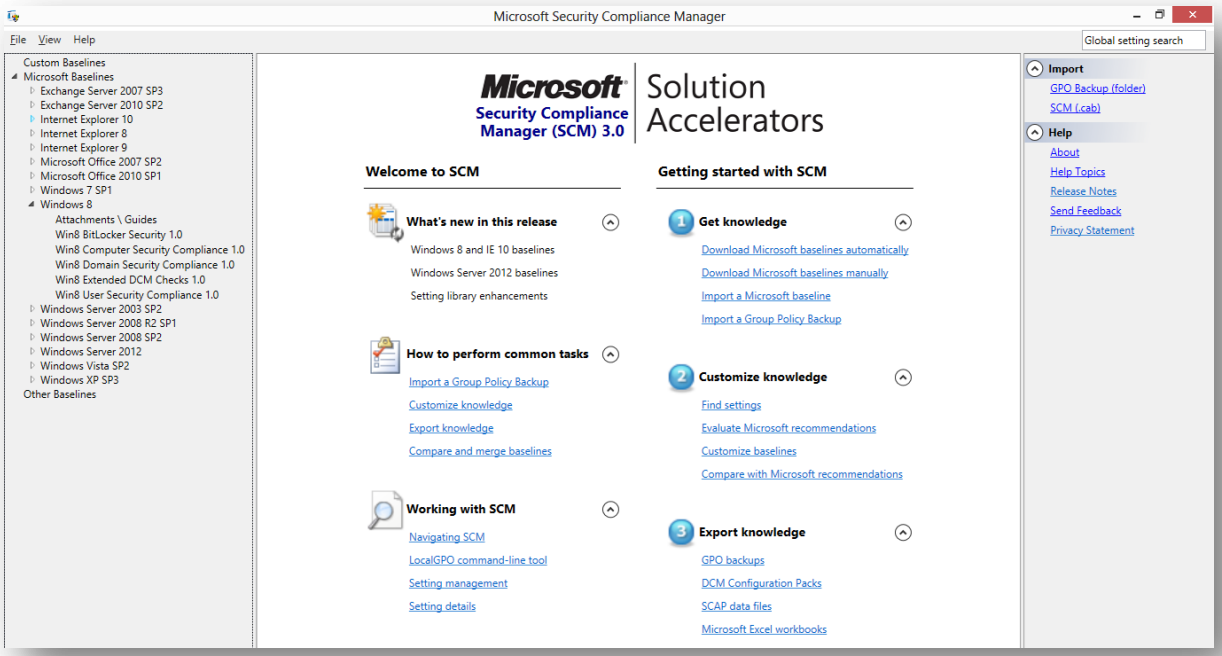

Rys. 8.1.1 - Widok pasku postępu podczas procesu importu ustawień bazowych.

**Uwaga:** Należy upewnić się, że proces importu zakończył się pomyślnie.

## 8.2 Praca z programem SCM

Widok konsoli programu SCM zawiera kilka kluczowych elementów:

- **Bibliotekę ustawień bazowych (ang. Baseline Library)** zlokalizowaną w lewym okienku konsoli programu. Biblioteka wyświetla zawartość zbioru dostępnych lokalnie ustawień bazowych w postaci drzewa z dokonanym podziałem na sekcje:
  - **Custom Baselines** – zbiór własnych indywidulanie dostosowanych ustawień bazowych
  - **Microsoft Baselines** – zbiór gotowych ustawień bazowych – pobranych z witryny Microsoft Dowload Center
  - **Other Baselines** – zbiór innych ustawień bazowych
- **Informacja na temat poszczególnych ustawień bazowych (ang. Baseline Information) –** informacje umieszczone w środkowym okienku konsoli. Wyświetlane w tym miejscu informacje zależą od kontekstu. Na przykład podczas uruchomienia programu pojawi się ekran powitalny, ale w momencie wybrania z lewego okienka określonego zbioru ustawień bazowych, w okienku centralnym ukażą się informacje szczegółowe na temat wybranego zbioru ustawień bazowych.
- **Okienko akcji (ang. Action Pane)** – umieszczone w prawym okienku konsoli wyświetla listę poleceń oraz czynności możliwych do wykonania.



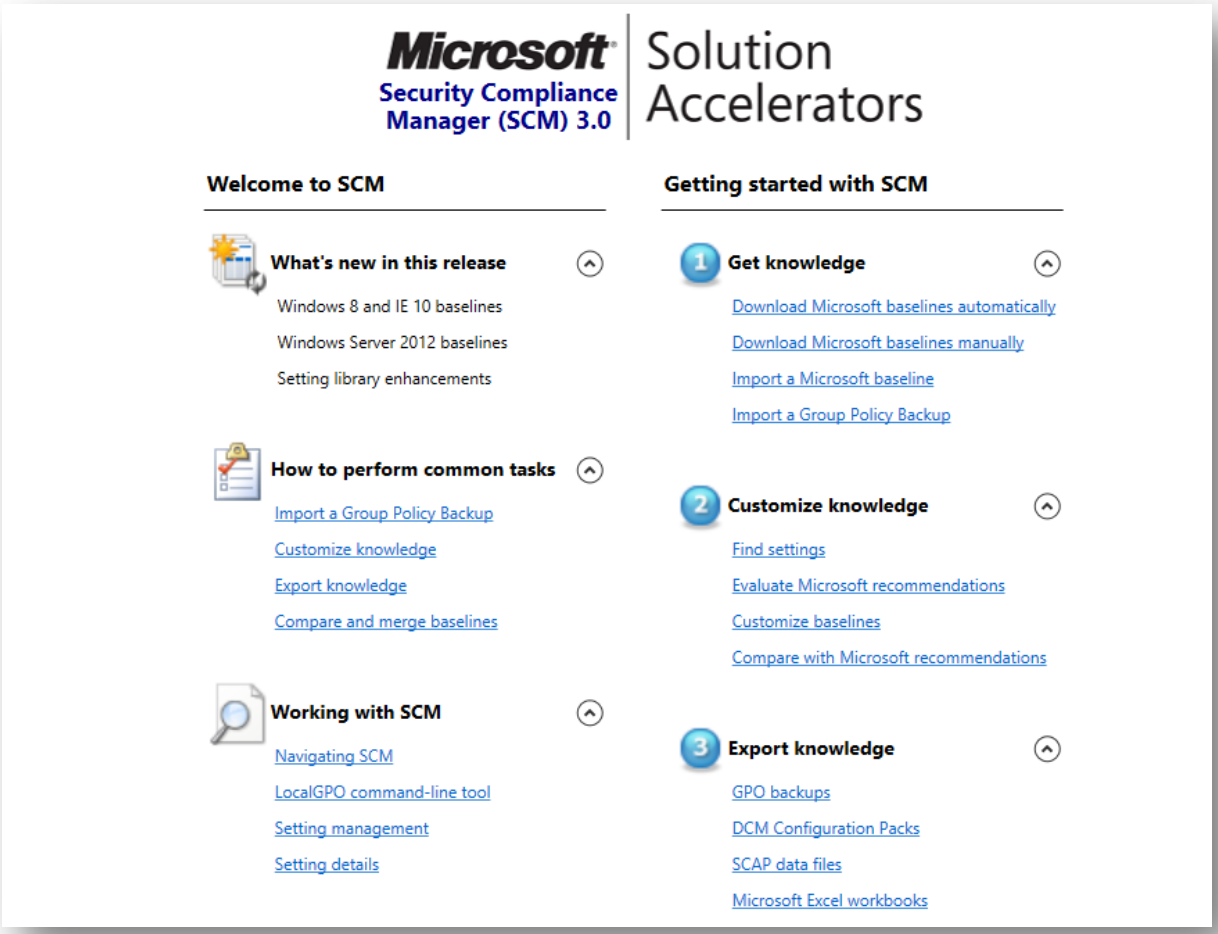

Rys. 8.2.1 - Widok konsoli programu SCM – ekran startowy

Konsola programu SCM wyświetla znaczną ilość informacji na temat poszczególnych opcji ustawień bazowych konfiguracji po wybraniu określnego ustawienia bazowego, z tego powodu zaleca się wybranie opcji maksymalizacji widoku okna na ekranach o dużych rozdzielczościach, szerokość okien można dostosować do własnych potrzeb. Widok konsoli SCM można uprościć poprzez ukrycie lewego oraz prawego okna. Za pomocą skrótów klawiaturowych można ukrywać lub wyświetlać zawartość okna:
**Ctrl+L** – wyświetlenie/ukrycie lewego okna (Baseline Library).
**Ctrl+R** – wyświetlenie/ukrycie prawego okna (Action Pane).

Pozostałe przydatne skróty klawiaturowe:

**Ctrl+O** – otwiera okienko **Options** z dostępnymi opcjami, w którym można zarządzać ustawieniem automatycznego sprawdzenia czy istnieją nowe zbiory ustawień bazowych podczas uruchomienia programu.
**Ctrl+U** – otwiera okienko **Download Updates**, w którym można wykonać ręczne sprawdzenie dostępności nowych zbiorów ustawień bazowych.
**Ctrl+I –** otwiera okienko **Import Baselines Wizard**, które umożliwia ręczne zaimportowanie własnych ustawień bazowych.
**Delete** – usuwa wybrane i zaznaczone przez użytkownika ustawienie bazowe (baseline).
**Ctrl+Delete** - usuwa wybrane i zaznaczone przez użytkownika ustawienie bazowe (baseline).
**Shift+Delete** - usuwa wybraną i zaznaczoną przez użytkownika grupę wszystkich ustawień bazowych (baseline) dotyczących danego produktu, np. „Windows 7 SP1”.

## 8.3 Rozpoczęcie pracy z programem SCM




Rys. 8.3.1 - Widok głównego ekranu programu SCM

Główny ekran programu SCM – środkowe okno zawiera dwie sekcje:

- **Welcome to SCM**:
    1. **What's new in this release** - sekcja informacyjna, z której dowiemy się, co nowego w tej wersji narzędzia SCM
    2. **How to perform common tasks** – sekcja omawiająca jak wykonywać typowe zadania w programie SCM
    3. **Working with SCM** - pomoc na temat pracy z programem SCM i dodatkowych narzędzi
- **Getting started with SCM**:
    1. **Get knowledge** – obsługa i zarządzanie zbiorami udostępnionych zestawów ustawień bazowych (Baseline).
    2. **Customize knowledge** – sekcja, która pozwoli na dostosowanie ustawień bazowych do własnych potrzeb oraz porównanie własnych ustawień do rekomendowanych ustawień zawartych w zestawach ustawień bazowych.

3. **Export knowledge** – sekcja, w której można wyeksportować przygotowane ustawienia bazowe konfiguracji do formatu kopii zapasowej zasady grupowej (Group Policy Backup), paczki SCAP oraz DCM a także utworzyć pliki SCM .cab.

## 8.4 Kluczowe elementy sekcji „Welcome to SCM”

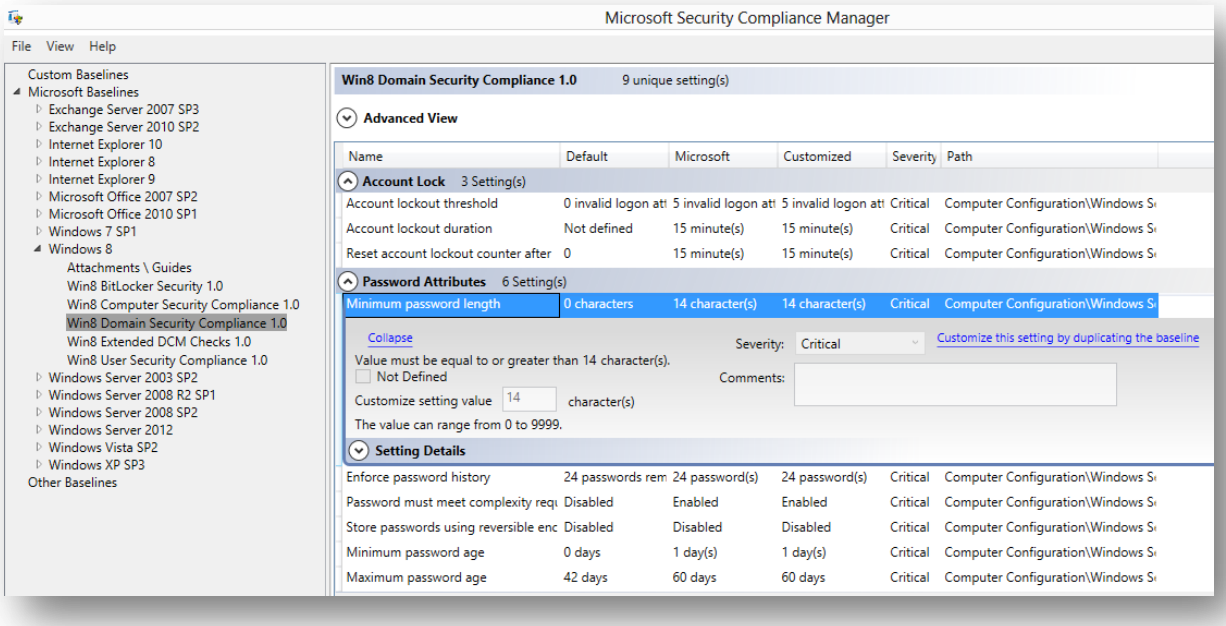
### 8.4.1 Zarządzanie ustawieniami (Setting management)

Ustawienia bazowe zawierają liczne opcje konfiguracji ustawień. Narzędzie SCM upraszcza w znaczny sposób proces przeglądania i zarządzania tymi ustawieniami poprzez pogrupowanie ich w poszczególne kategorie.

W celu zapoznania się z ustawieniami bazowymi wraz z ich szczegółowymi ustawieniami oraz dodatkową informacją należy:

1. Wybrać z okna **Baseline Information** określony zestaw ustawień bazowych (produkt), po wybraniu w centralnym oknie zostaną wyświetlone szczegółowe informacje na temat ustawień dostępnych w danym zestawie ustawień bazowych. Na górze okna zostanie wyświetlona całkowita liczba dostępnych ustawień w danym zestawie.
   Uwaga: Aby uzyskać więcej informacji na temat zabezpieczeń oraz zapewnienia zgodności na temat wszystkich ustawień, w oknie **Baseline Information,** poniżej nazwy wybranego produktu, należy przejść do sekcji **Attachments \ Guides** i otworzyć właściwy dokument.

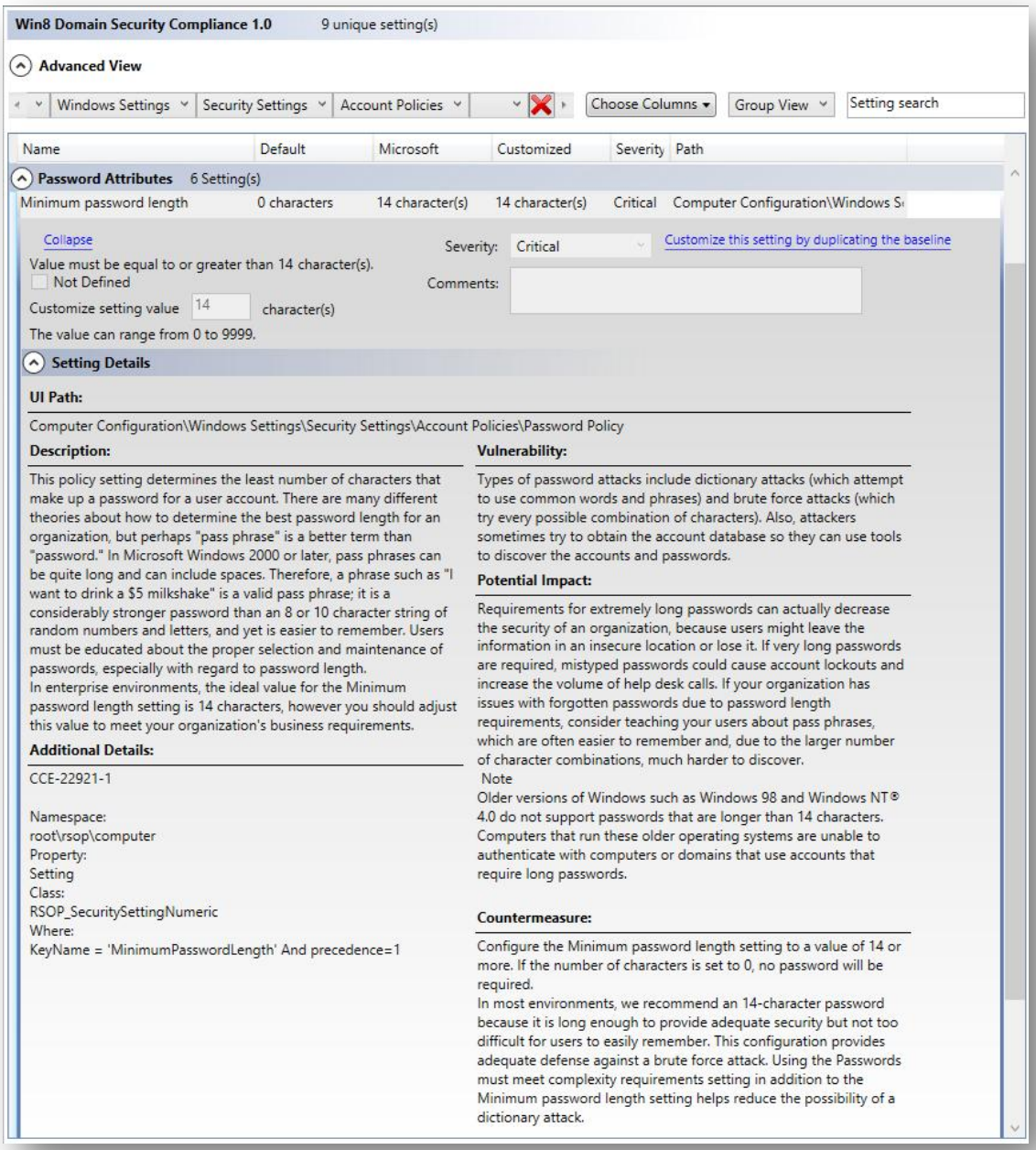
2. W oknie wybranej grupy ustawień bazowych, poniżej **Advanced View** należy wybrać właściwe ustawienie klikając w nazwę określonego ustawienia, po wybraniu ustawienia zostaną wyświetlone rekomendowane przez Microsoft domyślne ustawienia zabezpieczeń.




Rys. 8.4.1.1 – widok wybranego ustawienia „Minimum password length” wraz z rekomendowanymi wartościami

3. W celu wyświetlenia dodatkowych informacji na temat danego ustawienia należy wybrać i kliknąć w **Setting Details**, dodatkowe informacje na temat wybranego ustawienia:

- **UI Path:** Określa dokładną gałąź zasady, w której znajduje się ustawienie.
- **Additional Details:** Dostarcza dodatkowych informacji na temat klucza rejestru lub CCE-ID.
- **Vulnerability:** Wyjaśnia, w jaki sposób atakujący może przeprowadzić atak w przypadku, kiedy ustawienie jest skonfigurowane w mniej bezpieczny sposób.
- **Potential Impact:** Określa potencjalne negatywny wpływ zastosowanych ustawień zapobiegających podatności w systemie.
- **Countermeasure:** Określa, w jaki sposób należy implementować środki zaradcze.



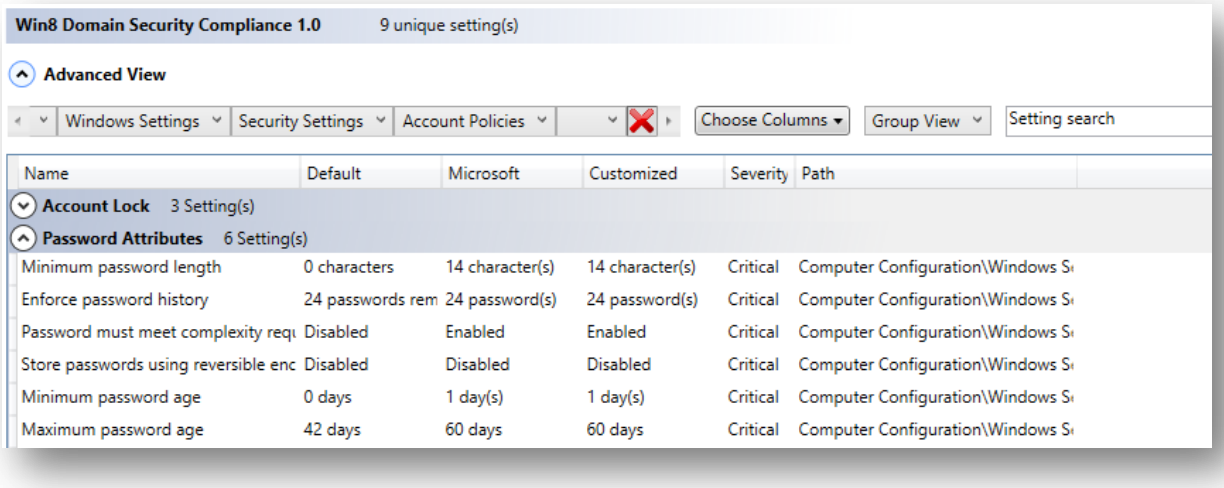
Rys. 8.4.1.2 – widok wybranego ustawienia „Minimum password length” wraz z dodatkowymi informacjami

4. Aby powrócić na najwyższy poziom, do widoku wszystkich ustawień w danym zbiorze, należy kliknąć opcję **Collapse**.

   **Wskazówka**:, Aby przyśpieszyć wyszukiwanie określonego ustawienia, wystarczy wprowadzić część nazwy ustawienia w polu **Settings search** w widoku **Advanced View** w prawym górnym rogu okienka **Baseline Information.**

## Zastosowanie widoku zaawansowanego Advanced View

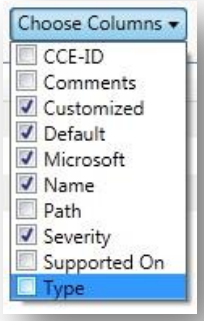
Domyślny widok wyświetla ustawienia pogrupowane według nazwy ustawienia, widok można pogrupować klikając w nazwę kolumny nagłówka tabeli. Dodatkowo można skorzystać z opcji filtrowania ustawień korzystając z widoku zaawansowanego **Advanced View.**




Rys. 8.4.1.3 - Widok zaawansowany **Advanced View**

Korzystając z **Advanced** możemy skorzystać następujących możliwości filtrowania:

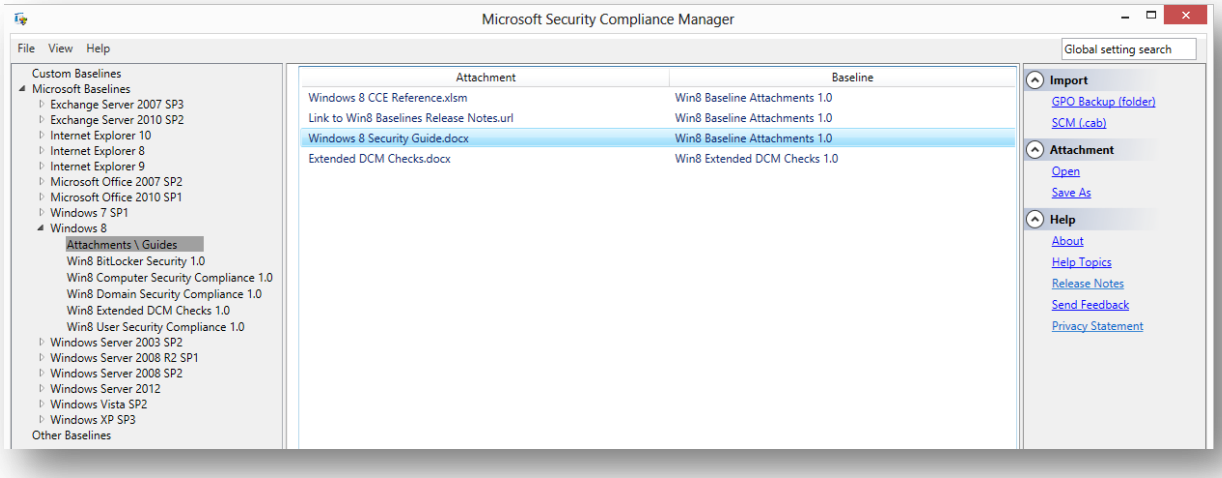
- **Setting search** - pozwala na filtrowanie ustawień tabeli według wprowadzonego słowa kluczowego będącego nazwą ustawienia w polu wyszukiwania.
  **Uwaga:** Nie można stosować równocześnie filtru **Setting Search** oraz **Path filter.**
- **Group View** - opcja ta pozwala na wybór trybu wyświetlenia ustawień stosując sortowanie ustawień według grupy ustawień (domyślny widok) lub **Simple View** w przypadku widoku prostego wyświetlane są wszystkie ustawienia bez grupowania.
- **Path** - Kolumna wyświetla pełną ścieżkę lokalizacji ustawienia w systemie operacyjnym Windows lub nazwę aplikacji Microsoft ustawienia bazowego (baseline), do którego się odwołuje w narzędziu SCM.
- **Choose Columns** – opcja ta pozwala na modyfikację widoku wyświetlanych kolumn poprzez usuwanie lub dodawanie kolumn według własnego wyboru.




Aby powrócić do widoku domyślnych kolumn w widoku zaawansowanych należy nacisnąć czerwony krzyżyk -

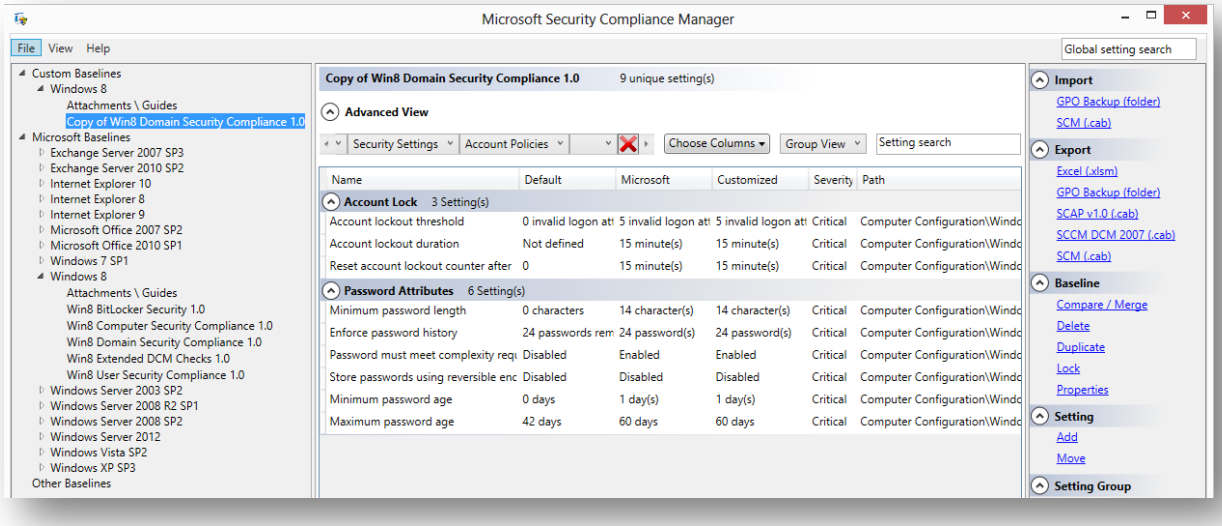
## Zarządzanie plikami załączników (Attachments) ustawień bazowych

W narzędziu SCM można zarządzać różnorodnymi załącznikami dołączonymi do ustawień bazowych (Baseline), które dostarczają dodatkowych informacji, jako uzupełnienie i rozszerzenie wiedzy na temat ustawień bazowych. Korzystając z SCM można wyszczególnione dokumenty można otwierać, edytować, tworzyć kopię lub wydrukować. Wspierane formaty załączników: **.cab, .doc, .docx, .mp, .rtf, .txt, .url, .xls, .xlsx, .xlsm, .zip**




Rys. 8.4.1.4 – Widok sekcji zarządzania załącznikami przypisanymi do grupy produktu ustawień bazowych

SCM zezwala również na umieszczanie również własnych dodatkowych informacji na temat stosowanych lub niestosowanych ustawień wraz z ich objaśnieniem. Operacje dodawania lub usuwania plików załączników można wykonać tylko dla plików umieszczonych we własnej bibliotece ustawień - sekcja **Baselines Library**, podsekcja **Custom Baselines.**



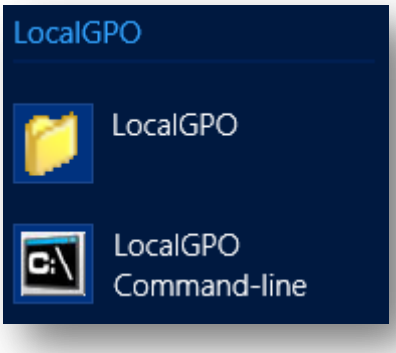

Rys. 8.4.1.5 – Widok sekcji zarządzania załącznikami przypisanymi do biblioteki własnych ustawień bazowych.

### 8.4.2 Narzędzie wiersza polecenia LocalGPO

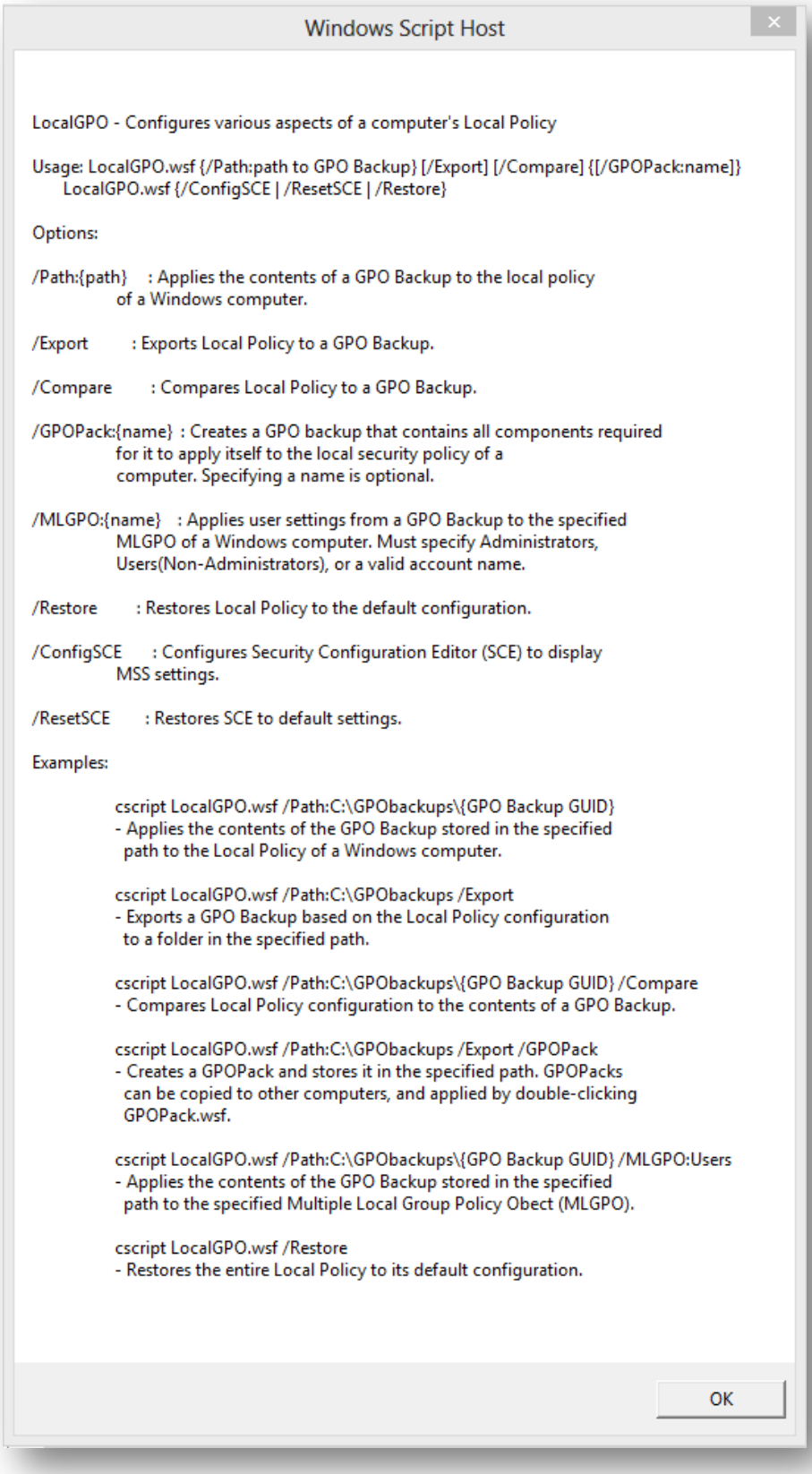
Po zainstalowaniu narzędzia SCM, dostępne jest narzędzie wiersza polecenia **LocalGPO**, które pozwala na zarządzanie i stosowanie ustawień dla komputerów nieprzyłączonych do domeny. **LocalGPO** pozwala na wykonanie kopii zapasowej ustawień zasad grupowych przeznaczonych dla środowisk domenowych a następnie implementację tych ustawień w środowiskach komputerów nieprzyłączonych do domeny.

Uwaga: SCM zawiera narzędzie **LocalGPO**, ale wymaga ono dodatkowego procesu instalacji.

W celu instalacji narzędzia wiersza polecenia **LocalGPO** należy uruchomić plik **LocalGPO.msi** zlokalizowany w folderze **C:\Program Files (x86)\Microsoft Security Compliance Manager\LGPO.** Po poprawnej instalacji narzędzia LocalGPO , należy zweryfikować pojawienie się narzędzia na liście programów.




Rys. 8.4.2.1 – widok narzędzia **LocalGPO** po poprawnej instalacji w systemie




Rys. 8.4.2.2 – Widok ekranu powitalnego po uruchomieniu narzędzia LocalGPO

Narzędzie LocalGPO pozwala na wykonanie określonych zadań:

- **Zastosowanie bazowych ustawień zabezpieczeń do lokalnych zasad grupy komputera**

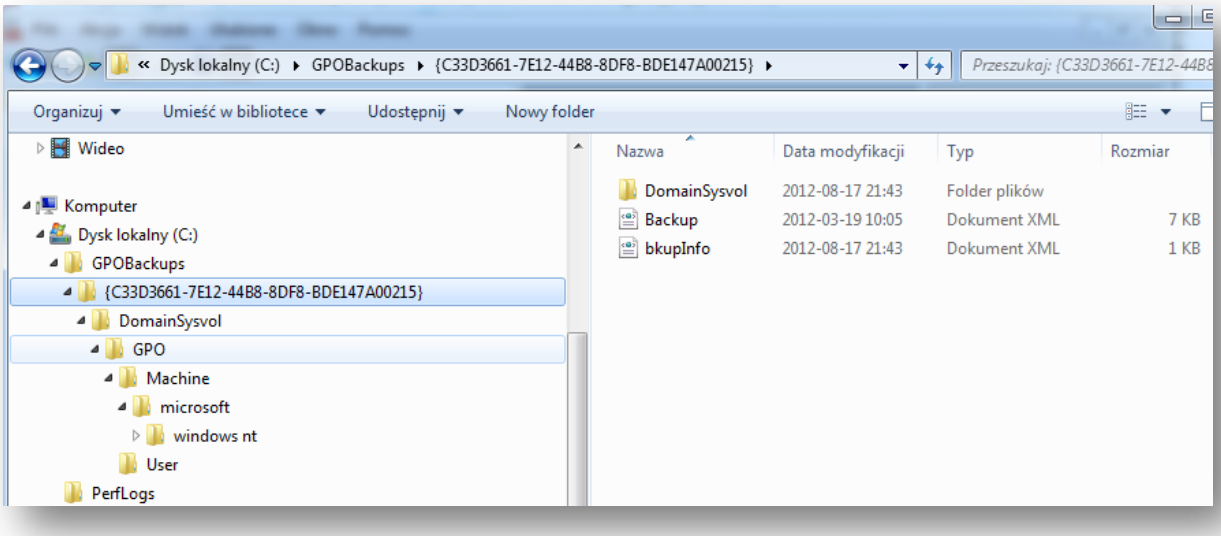
  LocalGPO wykonuje import ustawień przygotowanych w pliku kopii zapasowej ustawień zasad grupy (GPO backup) przez SCM. Plik kopii należy przygotować korzystając z narzędzia SCM.
  W celu wyeksportowania kopii zapasowej ustawień zasad grupy (GPO backup) do lokalnych zasad grupy komputera należy:
  - Zalogować się do komputera, jako Administrator
  - Uruchomić narzędzie **LocalGPO** stosując opcję **Uruchom jako administrator**
  - Wykonać polecenie z linii poleceń:
    **`cscript LocalGPO.wsf /Path:<ścieżka>`** - gdzie <ścieżka> to ścieżka do pliku GPO backup

  Aby przywrócić ustawienia lokalnych zasad grupy należy wykonać polecenie w kolejności jak wyżej: **`cscript LocalGPO.wsf /Restore`**

- **Eksport lokalnych zasad grupy komputera do pliku kopii zapasowej zasad grupy (Group Policy backup)**

  Korzystając z narzędzia LocalGPO możemy wykonać eksport ustawień lokalnych zasad komputera w celu zaimplementowania tych ustawień w innym komputerze lub w celu wykonania importu do usługi katalogowej.

  W celu wykonania eksportu lokalnych zasad grupy komputera, należy wykonać czynności:
  - Zalogować się do komputera, jako Administrator
  - Uruchomić narzędzie **LocalGPO** stosując opcję **Uruchom jako administrator**
  - Wykonać polecenie z linii poleceń:
    **`cscript LocalGPO.wsf /Path:"c:\GPOBackups" /Export`**

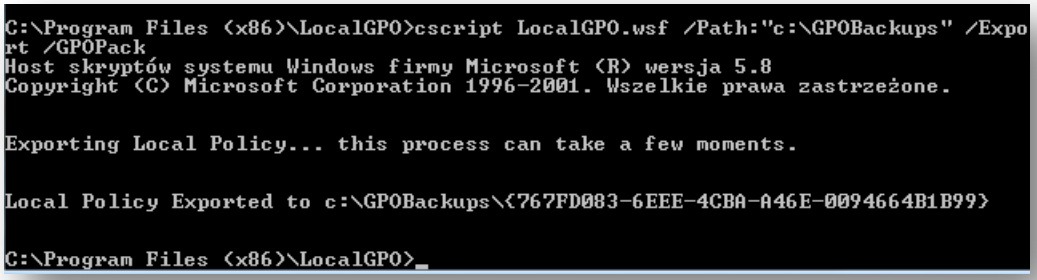


- **Utworzenie paczki GPOPack do zastosowania tych samych ustawień bazowych zabezpieczeń bez instalacji narzędzia LocalGPO**

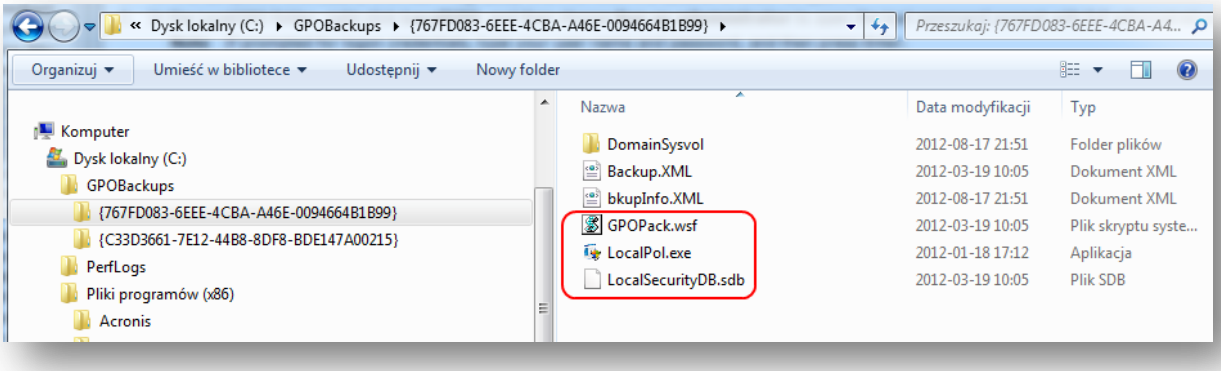
  W celu utworzenia paczki GPOPack, należy wykonać czynności:
  - Zalogować się do komputera, jako Administrator
  - Uruchomić narzędzie **LocalGPO** stosując opcję **Uruchom jako administrator**
  - Wykonać polecenie z linii poleceń:

  **`cscript LocalGPO.wsf /Path:"c:\GPOBackups" /Export /GPOPack`**

  Uwaga: W przypadku zastosowania przełącznika /GPOPack z podaną nazwą, np. /GPOPack:GPONazwa, nie będzie możliwe dokonanie importu wyniku korzystając z edytora zasad grupy (GPMC). Podanie nazwy w tym wypadku nie usprawni wykonania polecenia, ponieważ nie jest wymagane wprowadzenie identyfikatora GUID.




W wyniku działania utworzenia GPOPack zostaną utworzone 3 pliki przedstawione poniżej:




Dodatkowe informacje na temat wykorzystania i stosowania GPOPack uzyskać można na stronie bloga "SCM: LocalGPO Rocks!"[92]

Wskazówka: Możliwe jest wykorzystanie nowej funkcjonalności **LocalGPO** aby zintegrować skrypty wynikowe stosując narzędzie Microsoft Deployment Toolkit (MDT) aby przyśpieszyć i zautomatyzować

[92] http://blogs.technet.com/b/secguide/archive/2011/07/05/scm-v2-beta-localgpo-rocks.aspx.

proces wdrożenia systemów Windows 8 oraz Windows Server 2012. Aby uzyskać więcej informacji na ten temat należy odwiedzić witrynę produktu Microsoft Deployment Toolkit (MDT)[93]

- Zastosowanie Multiple local GPO w celu edycji kolekcji ustawień lokalnych zasad komputera. Funkcjonalność ta została zaprojektowana w celu ulepszenia procesu zarządzanie komputerami nieprzyłączonymi do domeny. Wykorzystanie przełącznika **/MLGPO** pozwoli zastosować ustawienia użytkownika korzystając z pliku GPOBackup lub paczki GPOPack do określonego MLGPO na komputerze z systemem Windows. Aby skorzystać z tej funkcjonalności należy określić grupę lokalnych **Administratorów** lub **Użytkowników**, ale można również określić grupę **Inni niż administratorzy** (Non-Administrators) lub dowolną nazwę użytkownika lokalnego.

  W celu utworzenia edycji kolekcji ustawień lokalnych zasad komputera, należy wykonać czynności:
  - Zalogować się do komputera, jako Administrator
  - Uruchomić narzędzie **LocalGPO** stosując opcję **Uruchom jako administrator**
  - Wykonać polecenia z linii poleceń:

```
cscript LocalGPO.wsf /Path:"c:\GPO Backups\GPO Backup 1"
/MLGPO:<nazwa lokalnego użytkownika lub lokalnej grupy>

cscript GPOPack.wsf /MLGPO:<nazwa lokalnego użytkownika lub
lokalnej grupy>
```

- Aktualizacja interfejsu użytkownika w narzędziu Edytor obiektów zasad grupy. Ustawienia posiadające prefiks MSS (Microsoft Solutions for Security), które zostały dostarczone przez grupę Microsoft Solutions nie są standardowo wyświetlanie w narzędziach GPMC oraz Security Configuration Editor (SCE). W celu poprawnego wyświetlenia ustawień MSS należy rozszerzyć funkcjonalność wspomnianych narzędzi. Poniższa procedura prezentuje sposób aktualizacji narzędzia SCE na komputerach, w których planowane jest zarządzanie zasadami grupy utworzonych narzędziem SCM.

  W celu aktualizacji narzędzia SCE do poprawnego wyświetlania ustawień MSS, należy wykonać czynności, wcześniej upewniając się, iż komputer jest przyłączony do domeny oraz narzędzie SCM jest zainstalowane:

  - Zalogować się do komputera, jako Administrator
  - Uruchomić narzędzie **LocalGPO** stosując opcję **Uruchom jako administrator**
  - Wykonać polecenia z linii poleceń:

```
cscript LocalGPO.wsf /ConfigSCE
```

  W celu przywrócenia domyślnych ustawień należy wykonać:

  - Zalogować się do komputera, jako Administrator
  - Uruchomić narzędzie **LocalGPO** stosując opcję **Uruchom jako administrator**

[93] Microsoft Deployment Toolkit (MDT) - http://go.microsoft.com/fwlink/?LinkId=105753

- Wykonać polecenia z linii poleceń:
  **`cscript LocalGPO.wsf /ResetSCE`**

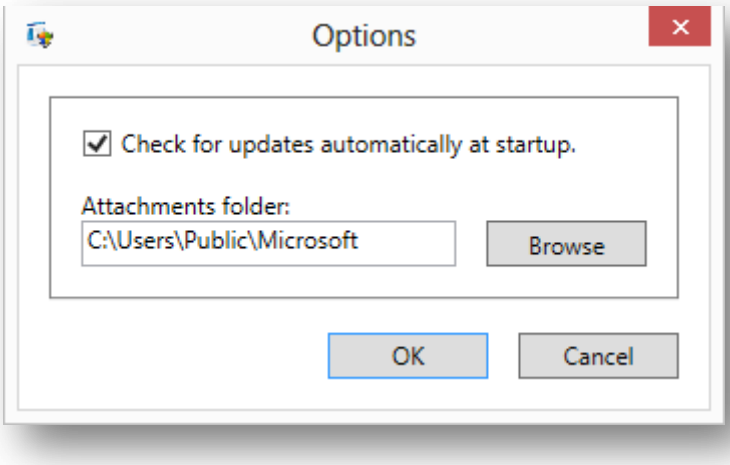
## 8.5 Kluczowe elementy sekcji „Getting started with SCM”

### 8.5.1 Zarządzaj ustawieniami bazowymi konfiguracji - Get knowledge

- **Download Microsoft baselines automatically** - Automatyczne pobieranie ustawień bazowych Microsoft

Po uruchomieniu opcji **Download Microsoft baselines automatically** widocznej w ekranie powitalnym programu SCM, system pobierze nowe ustawienia bazowe konfiguracji lub aktualizacje dla już istniejących ustawień.

W celu automatycznego pobierania nowych ustawień bazowych lub ich aktualizacji podczas startu programu SCM można skonfigurować to ustawienie wybierając opcję **File -> Options** lub posługując się skrótem klawiszowym **(Ctrl+O).**




- **Download Microsoft baselines manually** - Ręczne pobieranie ustawień bazowych Microsoft

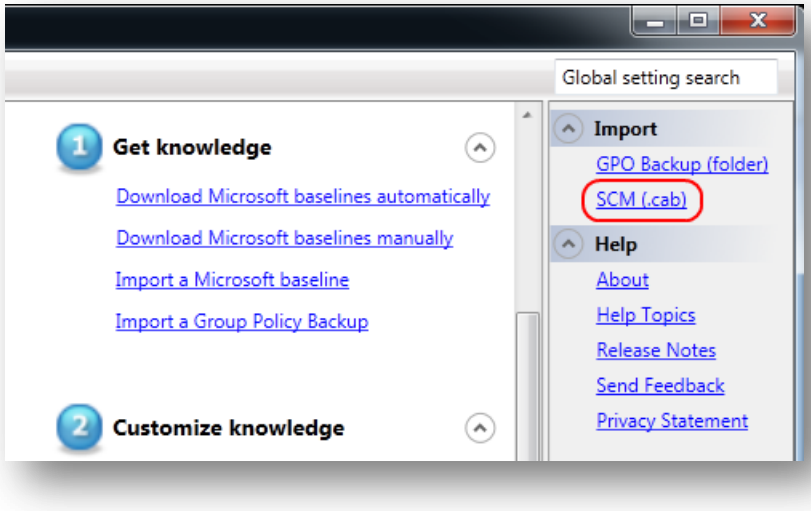
Po uruchomieniu opcji **Download Microsoft baselines manually** widocznej w ekranie powitalnym programu SCM, program otworzy dedykowaną stronę dla ustawień bazowych, z której będzie można pobrać najnowsze ustawienia bazowe dla produktów (Microsoft Baselines). Proces ten można uruchomić również ręcznie, wybierając opcję **File -> Check for Updates** lub posługując się skrótem klawiszowym **(Ctrl+U).**

- **Import a baseline** - importowanie ustawień bazowych Microsoft

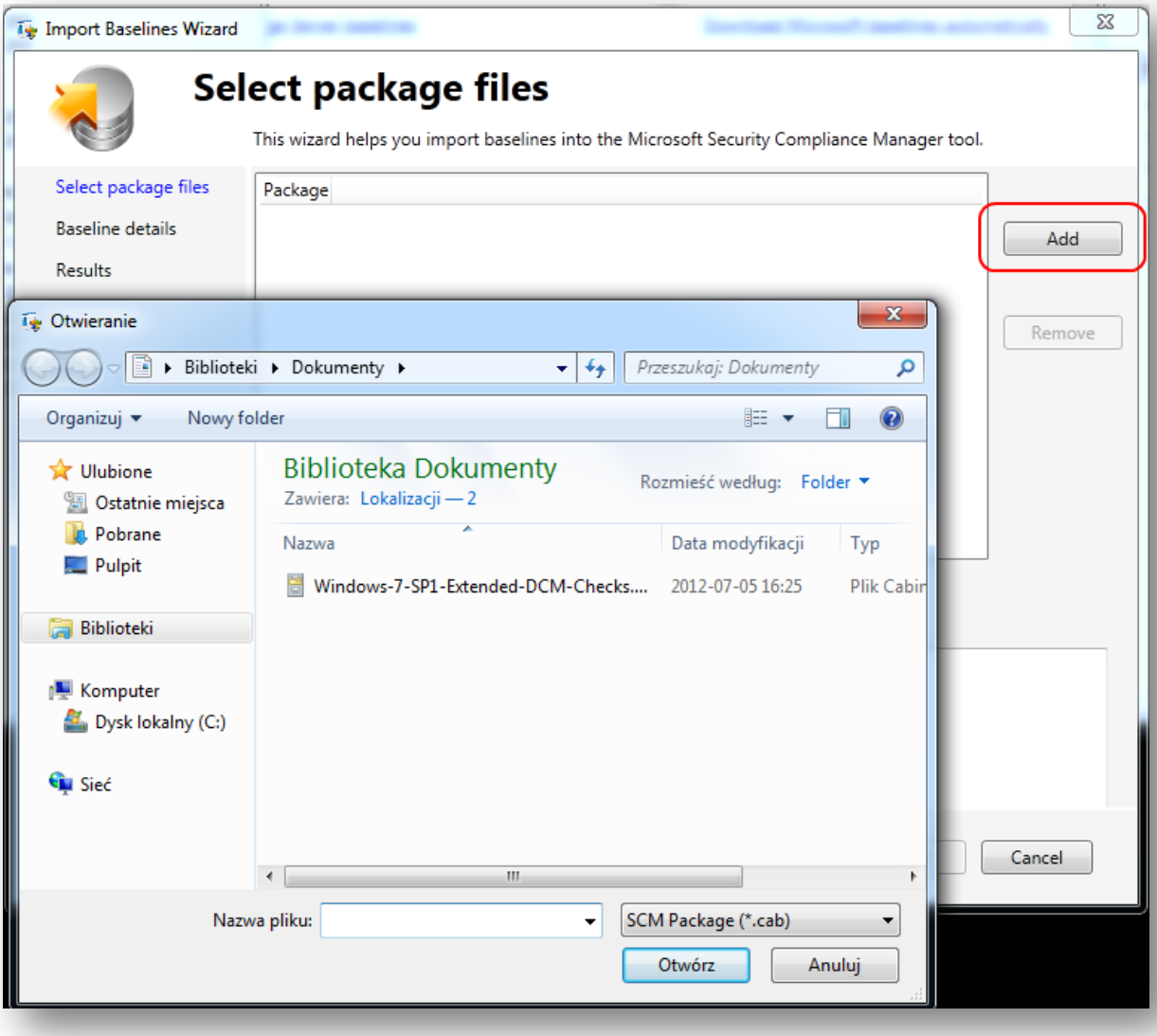
Narzędzie SCM pozwala na automatyczne pobieranie ustawień bazowych ze strony Microsoft Download Center, ale pozwala również na wykonanie importu w sposób ręczny bezpośrednio z plików.

W celu wykonania importu korzystając z kreatora **Import Baselines Wizard**, należy wykonać czynności:

- Należy uruchomić kreator opcję wybierać **Import** z prawego okna **Action** klikając w **SCM (.cab)** lub posługując się skrótem klawiszowym **(Ctrl+I)**.




- W kreatorze należy wybrać opcję **Select package files** a następnie kliknąć w opcję **Add** w celu wyświetlenia okna pozwalającego na wskazanie wybranego pliku przeznaczonego do importu.

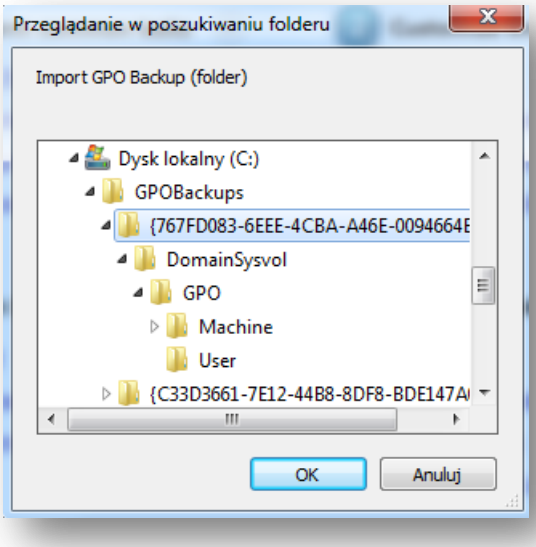



Dodatkowo można zaznaczyć opcję **Create modifiable copies of each baseline to be imported**, która umożliwi jednoczesne wykonanej kopii przeznaczonej do modyfikacji ustawień bazowych a następnie dokonać importu ustawień bazowych do programu SCM.

- **Import a Group Policy Backup** – importowanie pliku kopi zapasowej ustawień zasad grupy

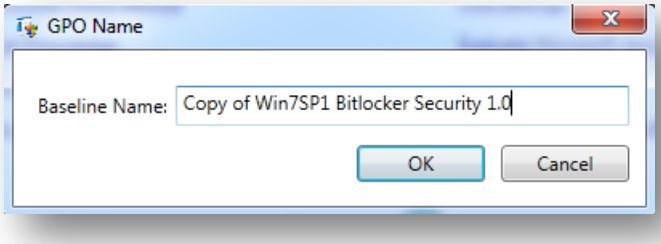
W celu wykonania importu pliku kopii zapasowej ustawień zasad grupy, należy wykonać czynności:

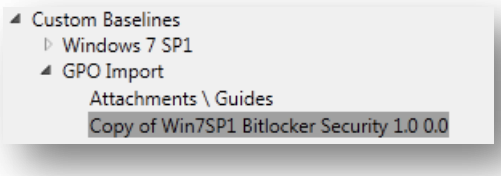
  - W prawym oknie **Action**, należy kliknąć w opcję **GPO Backup (folder)**, następnie w oknie **Przeglądanie w poszukiwaniu folderu** (**Browse for folder)** należy wybrać folder zawierający plik kopii zapasowej ustawień grupy i kliknąć **OK**.




- W oknie **GPO Name** należy wprowadzić nazwę dla kopii ustawień zasad grupy

- Po poprawnym imporcie zostanie wyświetlony komunikat **Import GPO completed successfully**, należy kliknąć **OK.**
- Plik kopii ustawień zasad grupy dostępny będzie w bibliotece ustawień bazowych **Baselines Library** w gałęzi **Custom Baselines**.



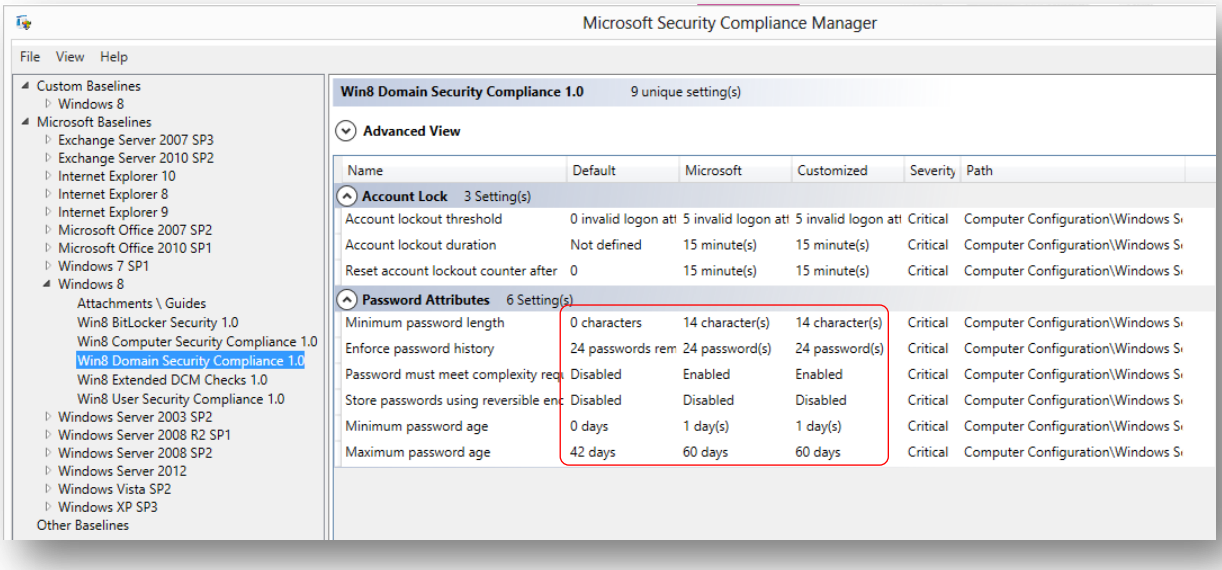

### 8.5.2 Dostosuj ustawienia bazowe konfiguracji do własnych potrzeb - Customize knowledge

Program SCM pozwala na pracę z gotowymi ustawieniami bazowymi dostarczonymi przez Microsoft bez możliwości dokonywania żadnych zmian, ale przypuszczalnie pojawi się wymóg dostosowania rekomendowanych ustawień dla wymogów stawianych własnym organizacjom. Pracując w programie SCM nie ma możliwości modyfikacji ustawień bazowych Microsoft zawartych w SCM, ale dla

własnych celów można wykonać kopię danego ustawienia bazowego wraz z możliwością edycji i modyfikacji według własnych wytycznych. Sekcja **Customize knowledge** pozwoli nam na wykonanie dostosowania ustawień bazowych do własnych celów.

- **Find settings** – opcja to pozwoli nam na szybkie przeszukanie określonych ustawień, informacje na ten temat opisano w rozdziale 8.5.1.

- **Evaluate Microsoft recommendations** – analiza ustawień domyślnych, rekomendowanych oraz własnych każdego ustawienia.
  SCM dostarcza rekomendowane ustawienia bazowe konfiguracji dla poszczególnych produktów, które są prezentowane w każdym ustawieniu bazowym konfiguracji (**Baseline**), wyświetlane są one w oknie zawierającym szczegółowe ustawienia. Każde z tych ustawień zawiera informacje o domyślnej konfiguracji, rekomendowanej przez Microsoft oraz ustawienia własne wraz z określeniem poziomu ważności danego ustawienia.

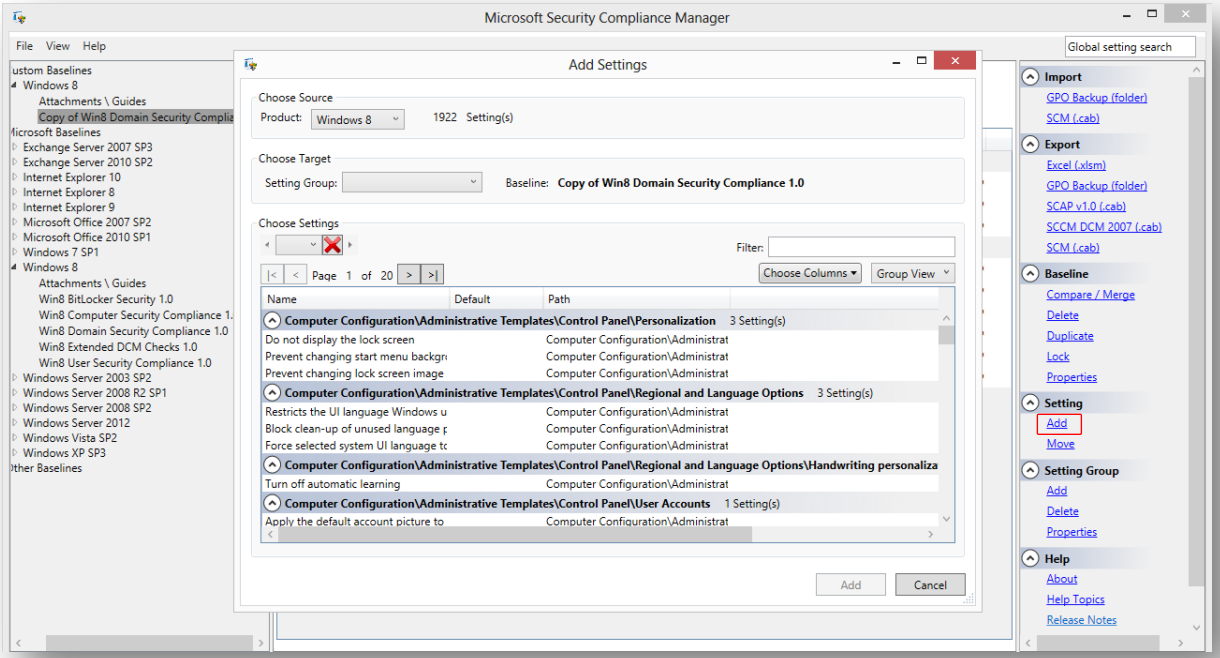



- **Customize baselines** – dostosowanie ustawień szczegółowych dla bazowych konfiguracji dla własnych potrzeb
  Ustawienia szczegółowe dla bazowych ustawień konfiguracji uporządkowane są według grup zbliżonych do ustawień zasad grupy znane z narzędzia Edytor obiektów zasad grupy, ale dla własnych potrzeb można dodawać, przenosić, kasować ustawienia oraz tworzyć własne grupy. Wszystkie te operacje dostępne są dla ustawień bazowych konfiguracji utworzonych w sekcji **Custom Baselines** umieszczonej w bibliotece **Baselines Library**.

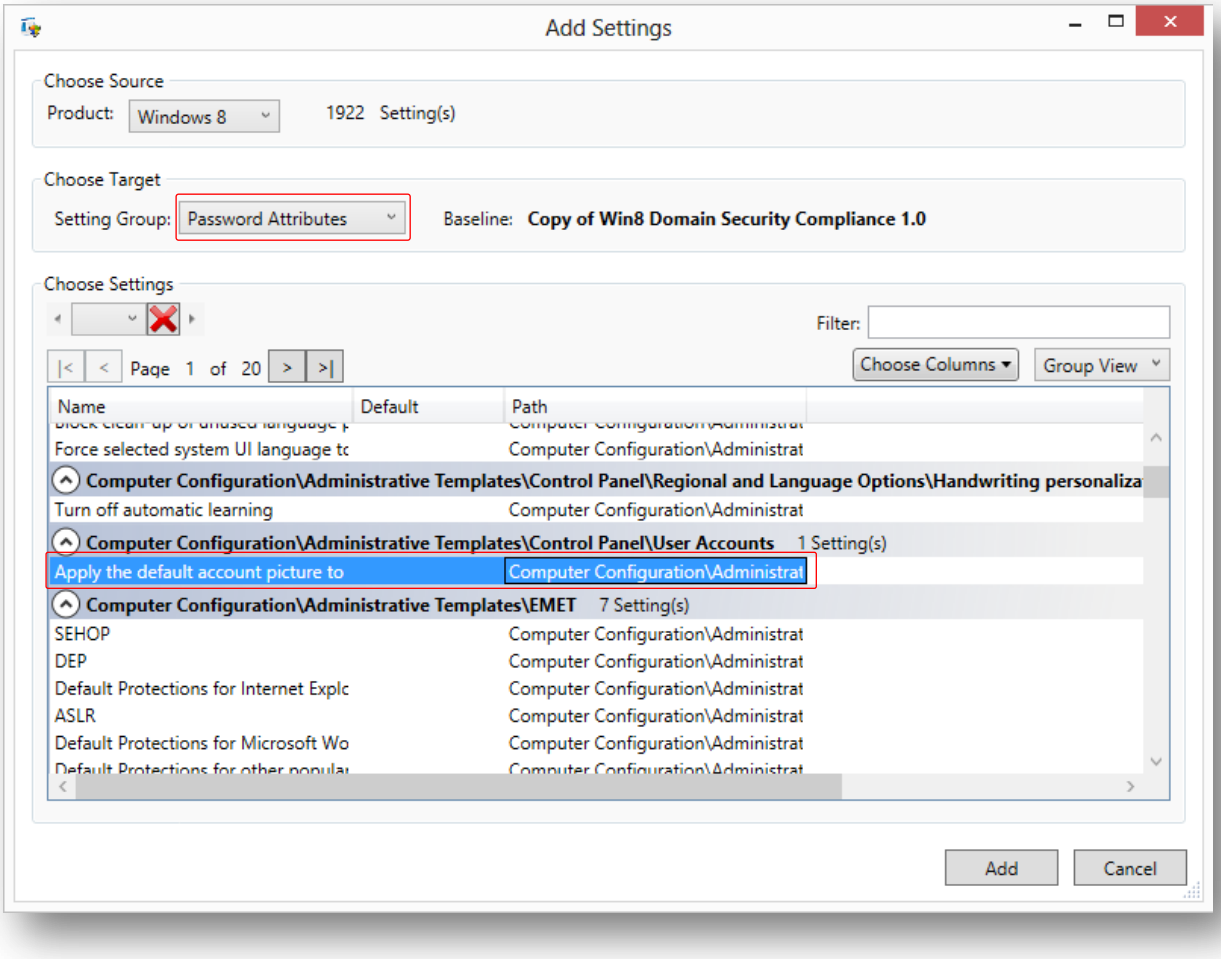
**Dodawanie szczegółowych ustawień**

W celu wykonania operacji dodawania szczegółowych ustawień dla własnych ustawień bazowych - **Add a setting**, należy wykonać czynności:

- Po wybraniu odpowiedniego własnego szablonu ustawień bazowych w sekcji **Custom Baselines** umieszczonej w bibliotece **Baselines Library** W prawym oknie **Action** w obszarze **Setting** należy kliknąć opcję **Add.**



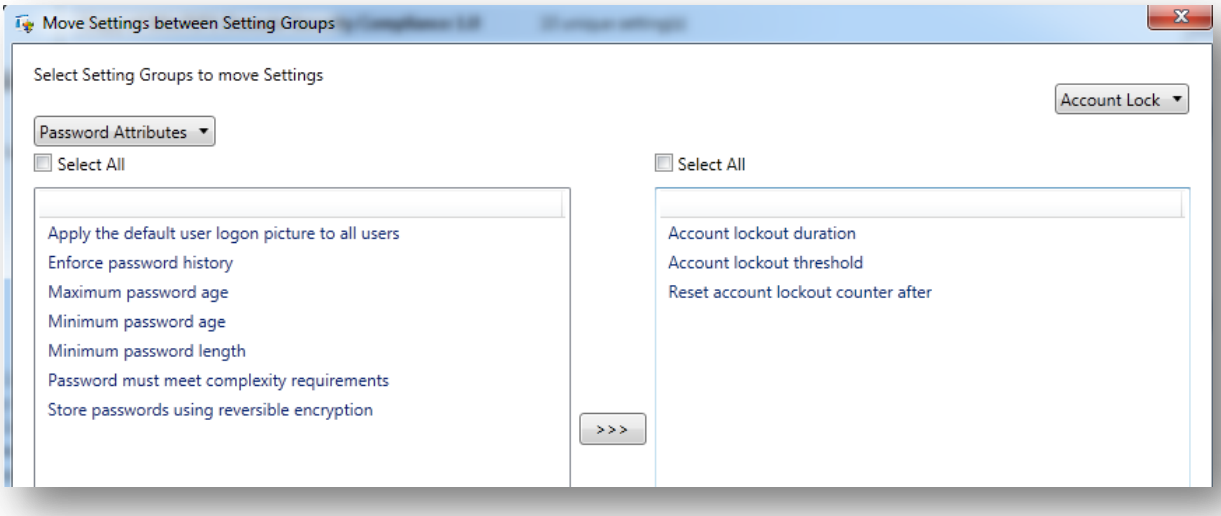

- Domyślnie okno znajduje się w szablonie ustawień bazowych, do którego dodajemy nowe ustawienie, w przedstawionym przykładzie jest to Windows 7 SP1, produkt określony jest w polu wyboru **Choose Source**.
- W następnej kolejności należy określić obszar docelowy **Choose Target** w oknie **Add Settings**, po rozwinięciu listy **Setting Group** należy wybrać właściwą grupę, w której zostanie dodane ustawienie. Następnie za pomocą strzałek w razie konieczności można rozwinąć grupy w celu identyfikacji właściwego ustawienia, które chcemy dodać.
- Kolejno należy wskazać ustawienie, które chcemy dodać i je wybrać, na zakończenie należy kliknąć opcję **Add**.



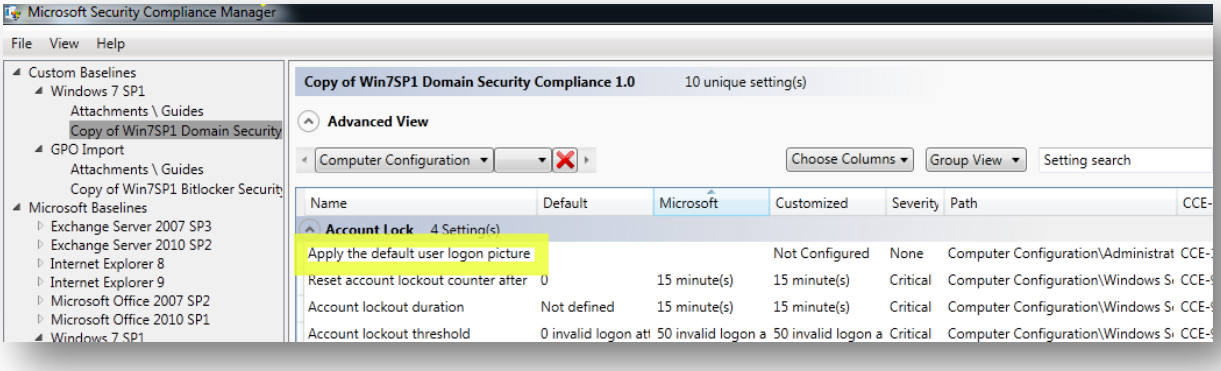

**Przenoszenie jednego lub wielu szczegółowych ustawień**

W celu wykonania operacji przenoszenia jednego lub wielu szczegółowych ustawień dla własnych ustawień bazowych - **Move a setting**, należy wykonać czynności:

- Po wybraniu odpowiedniego własnego szablonu ustawień bazowych w sekcji **Custom Baselines** umieszczonej w bibliotece **Baselines Library** W prawym oknie **Action** w obszarze **Setting** należy kliknąć opcję **Move.** Wyświetli się okno **Move Settings between Setting Groups.**



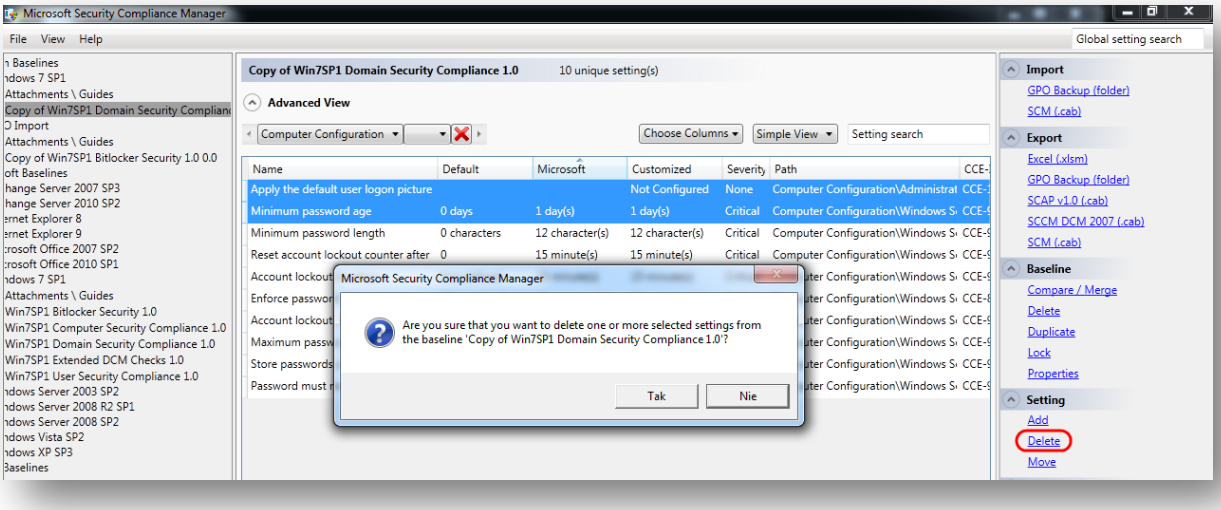

- Następnie należy wybrać po prawej stronie grupę docelową, do które ma zostać przeniesione jedno lub wiele ustawień i wybrać OK. SCM wykona operację przenoszenia i wyświetli ustawienie w nowej grupie, tak jak na przykładzie poniżej.




**Usunięcia jednego lub wielu szczegółowych ustawień**

W celu wykonania operacji usunięcia jednego lub wielu szczegółowych ustawień dla własnych ustawień bazowych - **Delete a setting**, należy wykonać czynności:

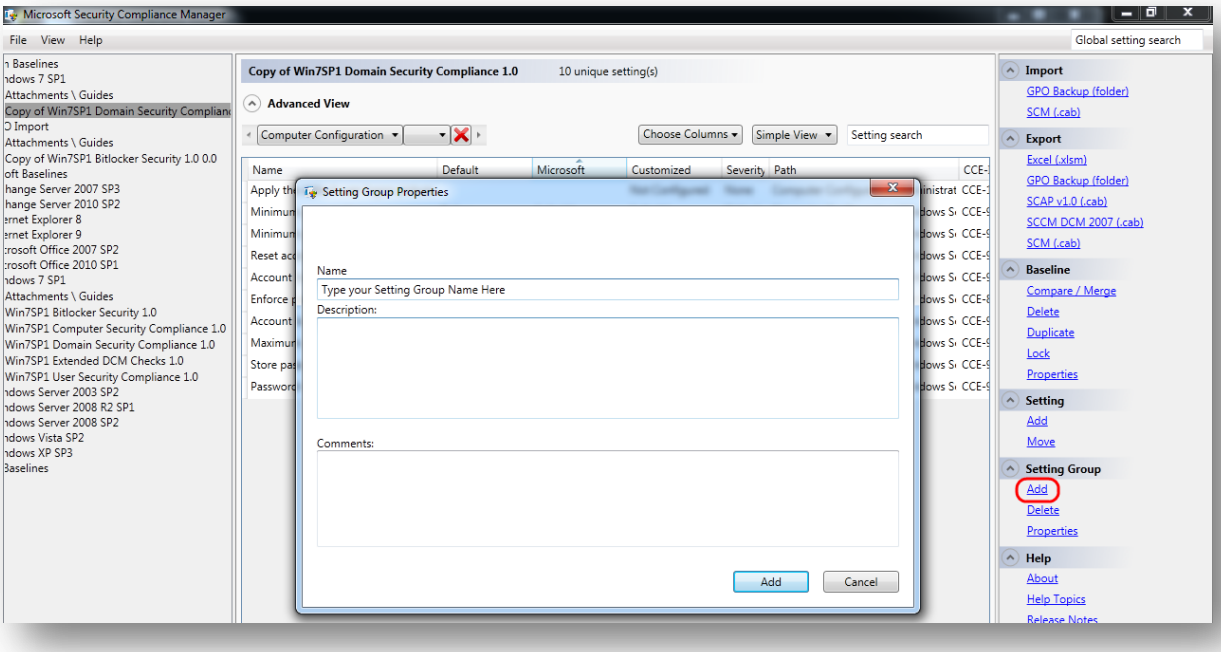
- Po wybraniu odpowiedniego własnego szablonu ustawień bazowych w sekcji **Custom Baselines** umieszczonej w bibliotece **Baselines Library** należy wybrać jedno lub wiele ustawień do usuniecia
- Następnie w prawym oknie **Action** w obszarze **Setting** należy kliknąć opcję **Delete.**




**Dodanie grupy ustawień**

W celu wykonania operacji dodania grupy ustawień dla własnych ustawień bazowych – **Add a setting group**, należy wykonać czynności:

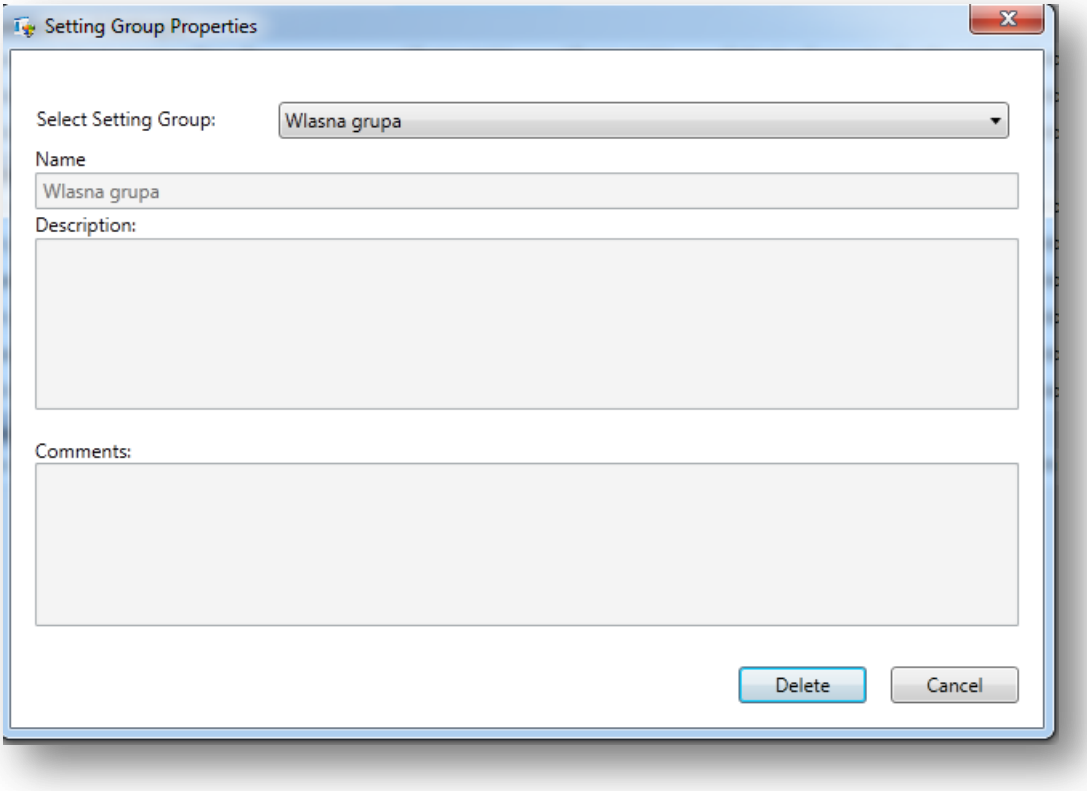
- Po wybraniu odpowiedniego własnego szablonu ustawień bazowych w sekcji **Custom Baselines** umieszczonej w bibliotece **Baselines Library**, należy w prawym oknie **Action** w obszarze **Setting Group** należy kliknąć opcję **Add.**




**Usuwanie grupy ustawień**

W celu wykonania operacji usunięcia grupy ustawień dla własnych ustawień bazowych – **Delete a setting group**, należy wykonać czynności:

- Po wybraniu odpowiedniego własnego szablonu ustawień bazowych w sekcji **Custom Baselines** umieszczonej w bibliotece **Baselines Library**, należy w prawym oknie **Action** w obszarze **Setting Group** należy kliknąć opcję **Delete** w celu wyświetlenia ona przedstawionego poniżej.
- Następnie po rozwinięciu listy grup należy wybrać grupę do usunięcia i zatwierdzić operację klikając w przycisk **Delete**.



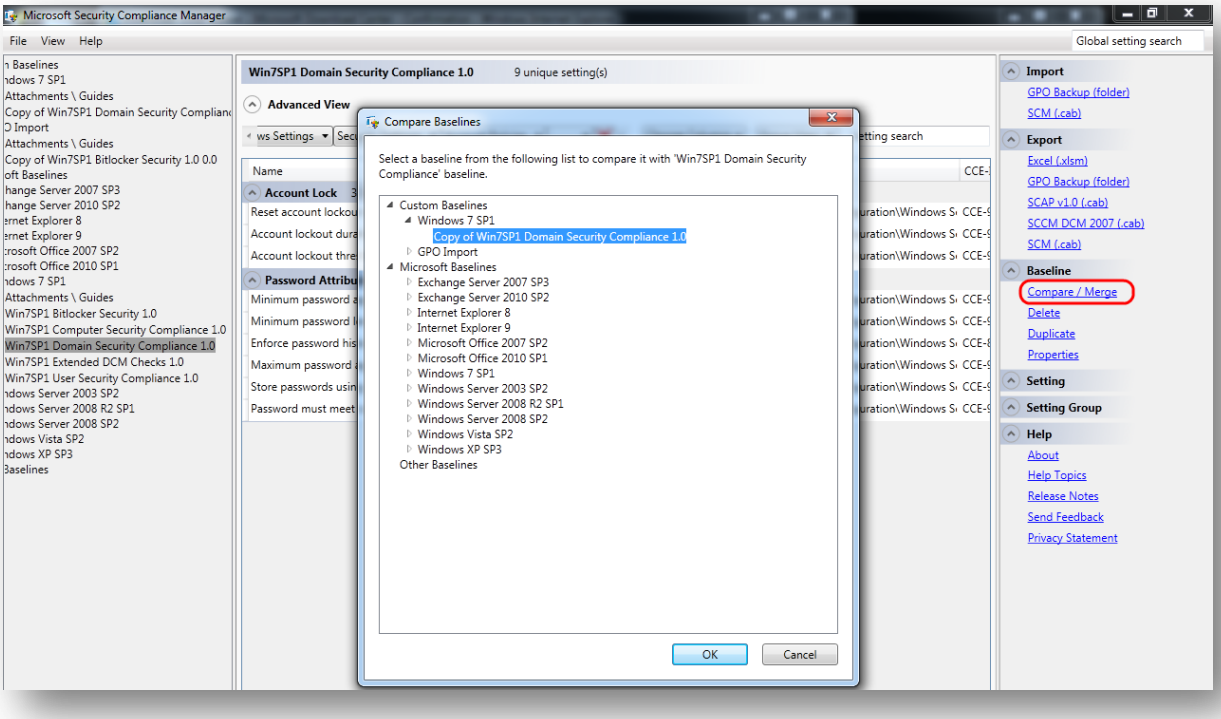

- **Compare with Microsoft recommendations** – porównanie ustawień bazowych z rekomendowanymi ustawieniami Microsoft

Funkcjonalność porównania ustawień bazowych pozwala na szybkie uzyskanie wyników porównania, które mogą zostać zapisane w arkuszu programu Microsoft Excel.

**Porównanie / połącznie dwóch ustawień bazowych konfiguracji w celu przejrzenia różnic pomiędzy ustawieniami bazowymi konfiguracji.**

W celu wykonania operacji porównania ustawień bazowych – **Delete a setting group**, należy wykonać czynności:

- Po wybraniu odpowiedniego szablonu ustawień bazowych do porównania należy w prawym oknie **Action** w obszarze **Baseline** należy kliknąć opcję **Compare / Merge.**

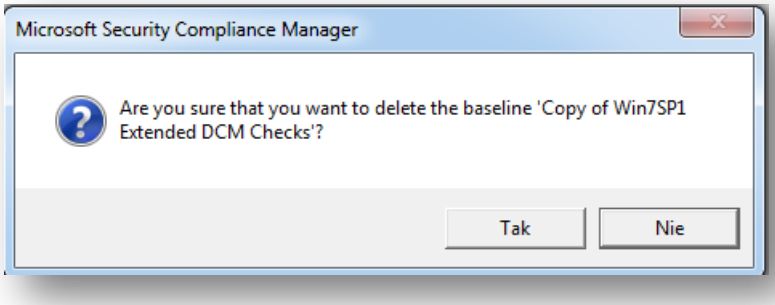



- Raport **Compare Baselines Summary** wyświetli wynik porównania Baseline A wybranego, jako pierwszy, z Baseline B wybranym, jako drugim.
- Raport będzie zawierał:
  - Całkowitą liczbę porównanych unikalnych ustawień
  - Całkowitą liczbę wspólnych ustawień
  - Całkowitą liczbę ustawień występujących tylko w jednym z porównywalnych ustawień bazowych

**Usunięcie ustawień bazowych konfiguracji.**

W celu wykonania operacji usunięcia jednego lub wielu ustawień bazowych, należy wykonać czynności:

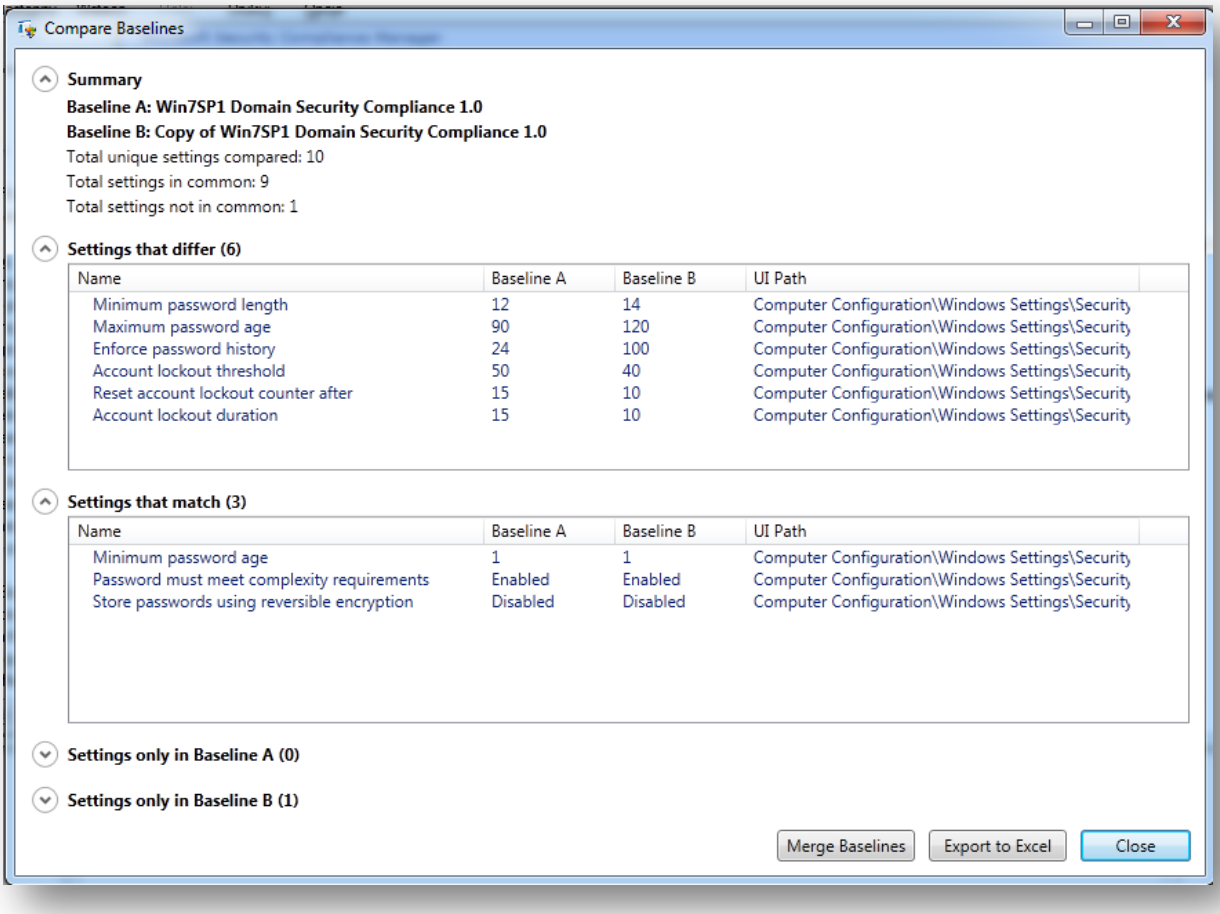
- Po wybraniu odpowiedniego szablonu/ów ustawień bazowych należy w prawym oknie **Action** wybrać opcję **Delete** i potwierdzić wykonanie operacji usunięcia.



**Usunięcie ustawień bazowych konfiguracji.**

W celu wykonania operacji usunięcia jednego lub wielu ustawień bazowych, należy wykonać czynności:

- Po wybraniu odpowiedniego szablonu/ów ustawień bazowych należy w prawym oknie **Action** wybrać opcję **Delete** i potwierdzić wykonanie operacji usunięcia.

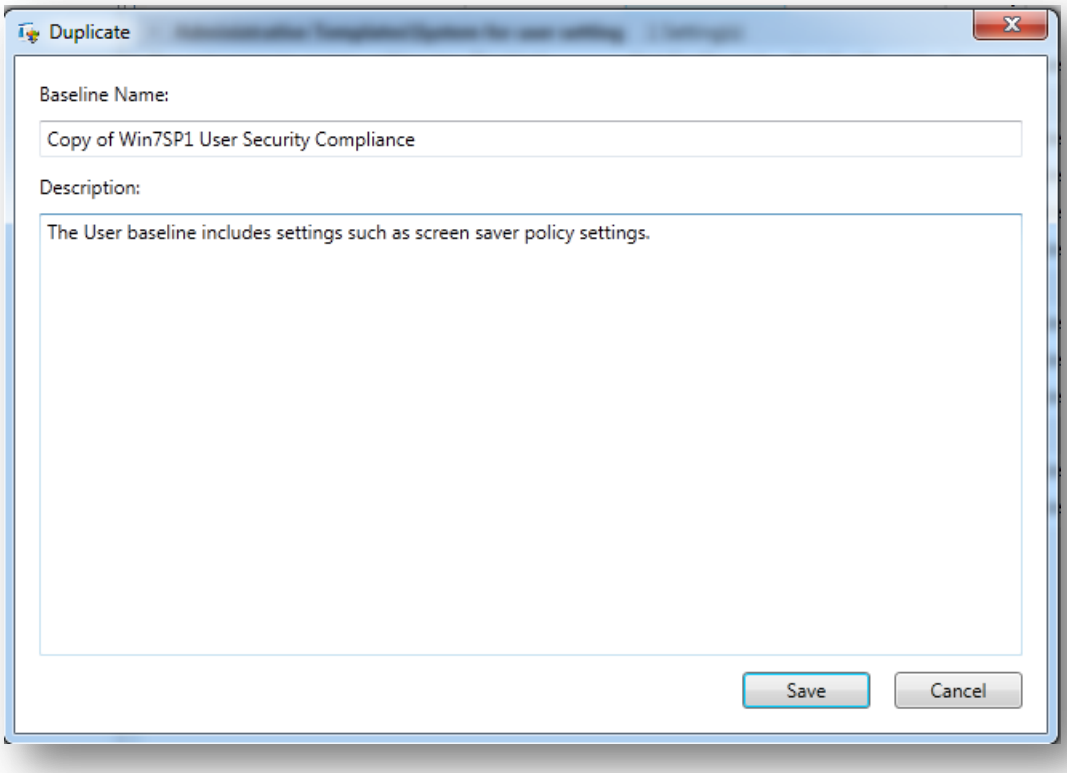



- W dalszej kolejności można dokonać połączenia ustawień bazowych lub wyeksportować wynik do formatu arkusza Microsoft Excel. (opcja wymaga zainstalowanego programu Microsoft Excel)

**Duplikacja ustawień bazowych konfiguracji.**

W celu wykonania operacji duplikacji ustawień bazowych, należy wykonać czynności:

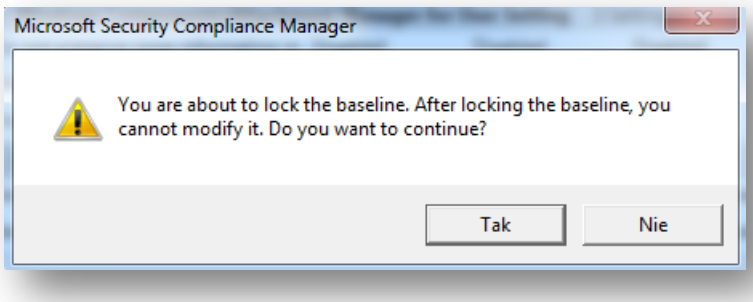
- Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** wybrać opcję **Duplicate** i potwierdzić lub wprowadzić nową nazwę ustawień bazowych.




**Zablokowanie ustawień bazowych konfiguracji.**

W celu wykonania operacji zablokowanie zduplikowanego szablonu ustawień bazowych, należy wykonać czynności:

- Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** wybrać opcję **Lock** i potwierdzić operację.



### 8.5.3 Eksportuj ustawienia bazowe konfiguracji- Export knowledge

- **Export a GPO backup** – opcja ta pozwala na wyeksportowanie ustawień bazowych konfiguracji do postaci GPO backup, który pozwoli na szybką implementację ustawień w środowisku usługi katalogowej.

W celu wykonania operacji wyeksportowanie ustawień bazowych konfiguracji do postaci GPO backup, należy wykonać czynności:

- Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** w obszarze **Export** wybrać opcję **GPO Backup (folder)** i wskazać istniejący folder lub utworzyć nowy w docelowym miejscu na dysku i potwierdzić **OK.**

- **Export DCM Configuration Packs**

Desired Configuration Management (DCM) jest funkcjonalnością Microsoft System Center Configuration Manager. Configuration Packs dostarczają danych w formacie DCM, które pozwalają na przeskanowanie pod katem zgodności zarządzanych komputerów.

W celu wykonania operacji wyeksportowanie ustawień bazowych konfiguracji do formatu Configuration Pack, należy wykonać czynności:

- Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** w obszarze **Export** wybrać opcję **SCCM DCM 2007 (.cab)** i wskazać istniejący folder lub utworzyć nowy w docelowym miejscu na dysku, następnie wprowadzić nazwę pliku .cab i potwierdzić klikając na przycisk **Save.**
  Nazwa utworzonego pliku będzie zawierała dołączoną informacje **_DCM.**

- **Export SCAP data files**

The Security Content Automation Protocol (SCAP) jest standardem wprowadzonym przez National Institute of Standards and Technology (NIST). SCAP składa się z danych w formacie XML i opisuje podatności programów oraz elementy konfiguracji configuration items (CIs). W celu uzyskania dodatkowych informacji na temat SCAP oraz formatu danych należy odwiedzić witrynę http://scap.nist.gov/[94].

W celu wykonania operacji wyeksportowanie ustawień bazowych konfiguracji do formatu SCAP, należy wykonać czynności:

- Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** w obszarze **Export** wybrać opcję **SCAP v1.0 (.cab)** i wskazać istniejący folder lub utworzyć nowy w docelowym miejscu na dysku, następnie wprowadzić nazwę pliku .cab i potwierdzić klikając na przycisk **Save.**
  Nazwa utworzonego pliku będzie zawierała dołączoną informacje **_SCAP.**

[94] http://scap.nist.gov/.

- **Export SCM .cab files**

SCM pozwala na eksportowanie ustawień bazowych konfiguracji w tym samym formacie, z którego sam korzysta. Format SCM może pozwala na współdzielenie i wymianę plików ustawień bazowych konfiguracji z innymi administratorami.

W celu wykonania operacji wyeksportowanie ustawień bazowych konfiguracji do formatu SCAP, należy wykonać czynności:

  - Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** w obszarze **Export** wybrać opcję **SCM (.cab)** i wskazać istniejący folder lub utworzyć nowy w docelowym miejscu na dysku, następnie wprowadzić nazwę pliku .cab i potwierdzić klikając na przycisk **Save.**

- **Export Microsoft Excel workbooks**

Ustawienia bazowe konfiguracji mogą zostać wyeksportowane do formatu Microsoft Excel (opcja wymaga zainstalowanego programu Microsoft Excel)

W celu wykonania operacji wyeksportowanie ustawień bazowych konfiguracji do formatu Microsoft Excel, należy wykonać czynności:

  - Po wybraniu odpowiedniego szablonu ustawień bazowych należy w prawym oknie **Action** w obszarze **Export** wybrać opcję **Excel (.xslm)** i wskazać istniejący folder lub utworzyć nowy w docelowym miejscu na dysku, następnie wprowadzić nazwę pliku dla arkusza Excel i potwierdzić klikając na przycisk **Save.**

## 9. Zarządzanie urządzeniami

Dzięki wsparciu dla protokołu Simple Certificate Enrollment Protocol (SCEP), który wykorzystuje protokół Open Mobile Alliance Device Management (OMA DM) możliwe jest zarządzanie urządzeniami w bezpieczny sposób.

SCEP jest protokołem, który został zaprojektowany do zarządzania urządzeniami mobilnymi takimi jak telefony czy tablety. SCEP jest również protokołem wdrażania certyfikatów, który został przewidziany dla ruterów a którego to nie wspiera system Windows 8. Windows 8.1 udostępnia protokół DM OMA dla rozwiązań zarządzania urządzeniami mobilnymi, które są dostarczane przez innych dostawców niż Microsoft.

Device encryption was introduced in Windows RT as an automatic data protection mechanism for consumer devices. In enterprise editions of Windows 8, device encryption was limited to BitLocker. In Windows 8.1, device encryption is available in all editions of Windows that are InstantGo certified to support a connected standby state.

Some benefits of device encryption include:

Encryption of the operating system volume is automatic and configured by default.

Protection is enabled once an administrator uses a Microsoft Account to sign in.

If encryption is unmanaged, the key recovery password is stored in SkyDrive.

In Professional and Enterprise editions of Windows 8.1, device encryption can be reconfiguration to use BitLocker features.

Device encryption in Windows 8.1 permits greater flexibility of personal device use within an organization because it helps protect corporate data across a variety of Windows editions so that:

Data on a device in a connected standby state is always protected through encryption.

User data on all fixed volumes on a device in a connected standby state is always protected through encryption.

When the device in a connected standby state is joined to the domain, it can comply with enterprise security policies.

## 10.Ochrona przed złośliwym oprogramowaniem

Systemy Windows 8 oraz Windows 8.1 pracują bezpośrednie z platformą sprzętową, która zaprojektowana jest w taki sposób, aby ulepszyć sposoby łagodzenia działania szkodliwego oprogramowania a dokładnie przekłada się to na następujące elementy:

**Platforma TPM** – opisywana wcześniej

**Losowej przestrzeni adresowej**

Address space layout randomization (ASLR) jest technologią, która chroni przed bezpośrednim zapisem w pamięci systemu poprzez losowanie (randomizację) jak i gdzie będą trzymane istotne dane w pamięci. Wraz z ASLR jest trudniejsze dla złośliwego oprogramowania odnalezienie specyficznej lokalizacji do zaatakowania.

W systemie Windows 8.1 pamięć losowana przez ASLR może być unikalna na poziomie różnych urządzeń czyniąc ją jeszcze bardziej chronioną i trudną do zaatakowania przez różnego rodzaju exploity.

**Zapobieganie wykonywania danych**

Zapobieganie wykonywania danych (Data execution prevention - DEP) znacznie ogranicza zakres pamięci, której złośliwy kod może wykorzystać na swój użytek. DEP używa bitu Never eXecute (NX) na wspieranych procesorach w celu oznaczenia bloków pamięci, w których dane nie powinny być uruchamiane jako kod. Nawet jeśli złośliwe oprogramowanie umieści fragment kodu w takim obszarze pamięci to nigdy nie zostanie on wykonany.

Systemy Windows 8 oraz Windows 8.1 są pierwszymi, które wymagają procesorów zgodnych sprzętowo z DEP. Te systemy operacyjne nie powinny być instalowane na komputerach, na których nie jest uruchomiony DEP.

## 11. Bezpieczny rozruch systemu

Systemy Windows 8 oraz Windows 8.1 mogą być uruchomione tylko na certyfikowanych komputerach PC. Certyfikacji częściowo podlega również UEFI.

Interfejs UEFI (Unified Extensible Firmware Interface) to standardowy interfejs oprogramowania układowego komputerów, zaprojektowany w celu zastąpienia systemu BIOS. Standard ten opracowało konsorcjum UEFI obejmujące ponad 140 firm technologicznych. Zaprojektowano go z myślą o zapewnieniu lepszej współpracy oprogramowania i rozwiązaniu problemów spowodowanych ograniczeniami systemu BIOS. Oto niektóre zalety oprogramowania układowego UEFI:

- Większe bezpieczeństwo dzięki łatwiejszej ochronie procesu poprzedzającego uruchomienie (rozruch) przed atakami programów typu bootkit.
- Szybsze uruchamianie i wznawianie pracy po hibernacji.
- Obsługa dysków o rozmiarze przekraczającym 2,2 terabajtów (TB).
- Obsługa nowoczesnych, 64-bitowych sterowników urządzeń w oprogramowaniu układowym, przy użyciu których system może zaadresować ponad 17,2 miliardów gigabajtów (GB) pamięci podczas uruchamiania.
- Możliwość używania systemu BIOS ze sprzętem UEFI.

Bootkity są najgroźniejszą formą złośliwego oprogramowania. Uruchamiają się tuż przed startem systemu Windows i kryją się między sprzętem a systemem operacyjnym gdzie są właściwie niewykrywalne i mają nieograniczony dostęp do zasobów systemu.

Wcześniejsze implementacje UEFI były w stanie uruchomić sprawdzenie wewnętrznej integralności, która weryfikowała cyfrowy podpis firmware przed uruchomieniem go. Ponieważ tylko producenci sprzętu PC mogą kontrolować, które certyfikaty mają możliwość tworzyć prawidłowe podpisy dla firmware UEFI oferuję ochronę od rootkitów firmware'u. Dlatego też UEFI jest pierwszym łączem w łańcuchu zaufania.

Wraz z usługa Secure Boot UEFI komputera weryfikuje czy bootloader Windowsa jest bezpieczny przez załadowaniem go. Jeśli bootloader został zmodyfikowany (np. przez instalację bootkita) lub zamieniony to Secure Boot nie pozwoli na jego uruchomienie.

### 11.1 Trusted Boot

System Windows 8.1 zawiera również funkcję Trusted Boot, która weryfikuje czy wszystkie komponenty ładowania system Windows zawierają integralność i mogą być zaufane. Bootloader weryfikuje podpis cyfrowy kernela przed załadowaniem go. Kernel w trakcie uruchamiania weryfikuje każdy komponent na liście startowej procesu Windows, włączając w to sterowniki, pliki startowe oraz komponenty ELAM.

W systemie Windows 8.1 funkcja Measured Boot została dodana do procesu startu dla sytemów zgodnych z ELAM. Measured Boot pozwala na zdalnym serwerze systemom niebazującym na Windows na weryfikację bezpieczeństwa każdego ładowanego komponentu w sposób trudny do obejścia przez złośliwe oprogramowanie. Jeśli zostanie wykryta próba ładowania złośliwego oprogramowania Trusted Boot naprawi system poprzez odtworzenie oryginalnego pliku.

## 12 Model kontroli dostępu do systemu Windows

### 12.1 Dynamic Access Control

Dynamic Access Control wykorzystuje dynamiczne polisy bazujące na rolach w celu ochrony folderów, plików oraz udostępnionych zasobów. Polisy te mogą pozwolić na dostęp lub zabronić dostępu bazując na kombinacji użytkownika, urządzenia, właściwości danych niż na statycznych listach użytkowników oraz grupach bezpieczeństwa.

Używajac Dynamic Access Control administratorzy mogą tworzyć szczegółowe polisy audytowe, np. do dokumentów zawierających dane podlegające ochronie, aby możliwe było spełnienie zgodności raportowej oraz wymagań analizy kryminalistycznej. W przeciwieństwie do tradycyjnych możliwości audytowych, w których gromadzone są ogromne ilości danych priorytetyzowanych, DAC oraz jego reguły bazujące na rolach pozwalają na zbieranie wszystkich danych lub tylko tych, które nas interesują pod kątem audytu.

### 12.2 Ochrona publicznych certyfikatów i kluczy

W systemie Windows 8.1 poświadczenie certyfikatu dotyczy publicznych certyfikatów oraz kluczy. Funkcjonalność SmartScreen dostępna w Internet Explorer jest zgodna z usługa Web Service, która dostarcza wczesne ostrzeżenia dla użytkownika na temat podejrzanej strony WWW, która

może być wykorzystana do ataków lub dystrybucji złośliwego oprogramowania. Usługa ta jest w stanie wykryć kiedy certyfikat jest wystawiony przez niespodziewane źródło a następnie może sprawdzić różnice które mogą rozpocząć zaradcze akcje lub zasugerować cofnięcie certyfikatu.

## 12.3 Tryb Restricted Admin dla połączeń pulpitu zdalnego

Klient usługi Remote Desktop może połączyć się w trybie Restricted Admin. Używając tego trybu z uprawnieniami administratora RDS próbuje połączyć się interaktywnie do serwera, który również wspiera ten tryb bez wysyłania poświadczeń. W momencie, kiedy host zweryfikuje, że konto łączącego się użytkownika ma uprawnienia administratora oraz wspiera tryb Restricted Admin to połączenie będzie udane. W trybie tym w żadnym punkcie nie jest wysyłane czystym tekstem lub innych form połączenia do zdanych komputerów.

## 12.4 Schowek dla poświadczeń - Credential Locker

Schowek dla poświadczeń jest usługą, która tworzy i zarządza bezpiecznym magazynem, na lokalnym komputerze, przechowującym nazwy użytkowników i hasła, które zostały zapisane dla stron internetowych oraz aplikacji ze sklepu Windows. W Windows 8 został zaprezentowany Web Authentication Broker aby wspierać połączenie aplikacji z zasobami dostępnymi w Internecie i aby zarządzać uprawnieniami.

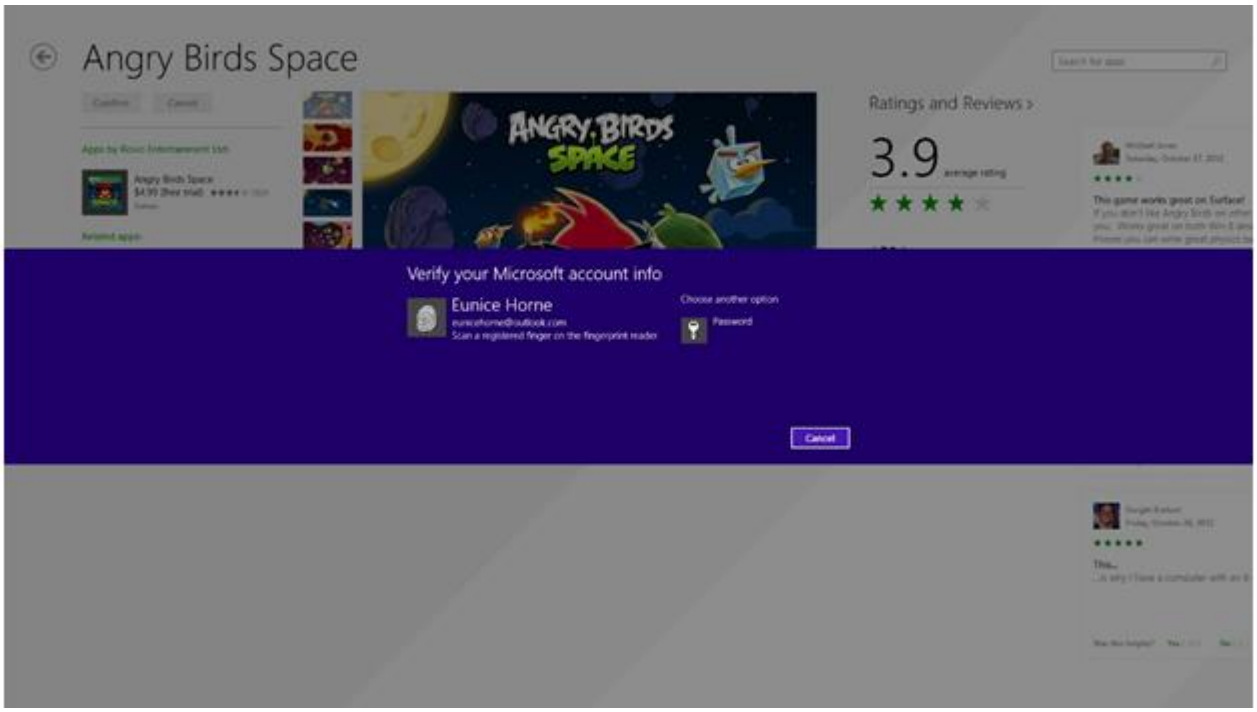
Credential Locker wspiera jednolite logowanie przez użycie aplikacji z Windows Store, które korzystają z usługi Web Authentication Broker. Usługa ta pamięta hasła dla takich serwisów jak Facebook czy Twitter, dlatego też użytkownik nie musi podawać hasła wielokrotnie. Takie jednolite logowanie zostało rozszerzone również o urządzenia korzystające z Windows 8.1.

W przypadku, kiedy wiele uprawnień jest przechowywanych dla tego samego zasobu nie ma możliwości określenia, który z nich jest podstawowym. W Windows 8.1 użytkownik może zdecydować i określić podstawowe uprawnienia dla zasobu.

# 13 Biometria

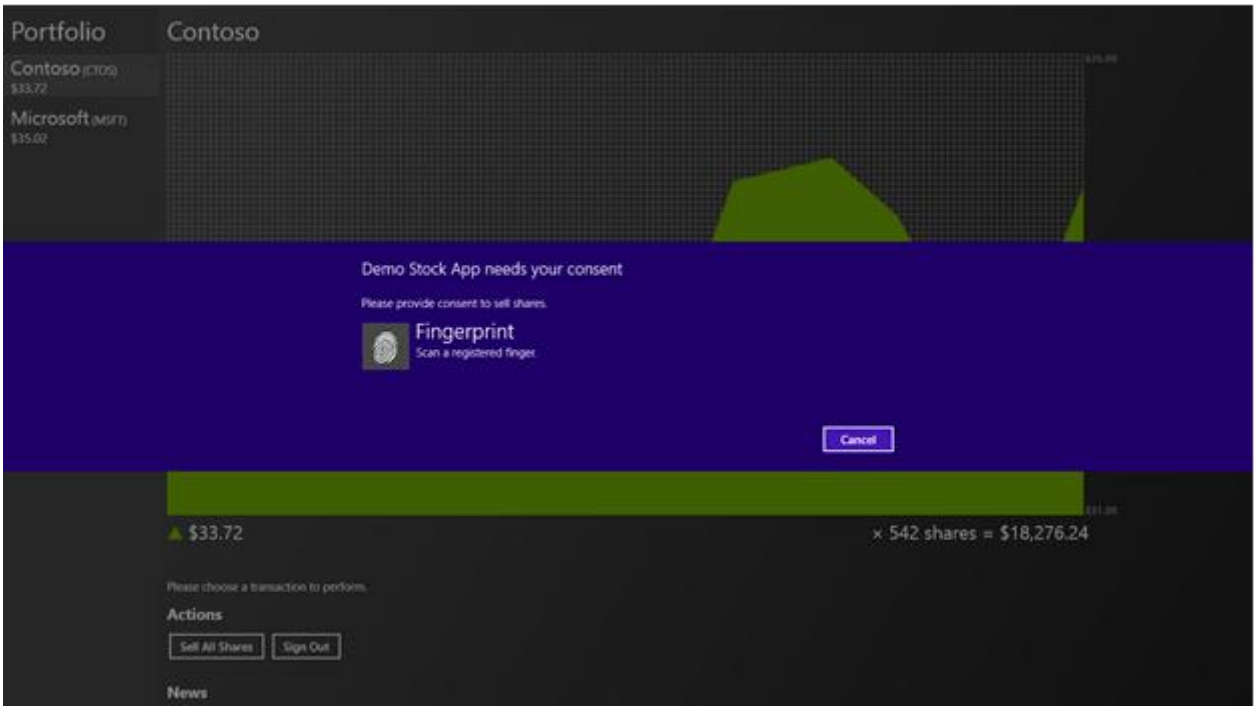
Rozszerzenia dodane do platformy Windows Biometrics Framework (WBF) w Windows 8.1 pozwalają na działania w nowych scenariuszach. Wśród scenariuszy możemy wyróżnić między innymi API dla programistów do autoryzowania użytkowników w aplikacjach udostępnionych w Windows Store. Kolejną nowością w Windows 8.1 jest wydzielenie z platformy WBF klasy sterowników USB dla linii papilarnych Biometric Input Device (BID).

W Windows 8.1 możliwe jest zintegrowanie czytnika linii ze sklepem Windows Store do zakupu aplikacji




W ten sam sposób możliwy jest zakup różnych treści multimedialnych.

Windows 8.1 udostepnia również platformę dla Windows 8.1 RT i wykorzystanie jej we własnych aplikacjach




Dodatkowo możliwe jest użycie Group Policy do ustawień użycia biometrii w systemie Windows 8.1

# 14 Dodatek – ustawienia bezpieczeństwa w Group Policy dla Windows 8.1 oraz Windows Server 2012 R2

W poniższej tabeli przedstawione są nowe oraz sugerowane ustawienia dla Windows 8.1 oraz Windows Server 2012 R2 dla Group Policy zgodne z przewodnikiem bezpieczeństwa.

| ***Ścieżka*** | ***Nazwa reguły*** | ***Poprzednia wartość*** | ***Nowa wartość*** |
|---|---|---|---|
| Konfiguracja komputera\Szablony administracyjne\Panel Sterowania\Personalizacja | Chroń przed włączeniem kamery na ekranie blokady | N/D | Włączone |
| Konfiguracja komputera\Szablony administracyjne\Panel Sterowania\Personalizacja | Chroń przed włączeniem pokazu slajdów na ekranie blokady | N/D | Włączone |
| Konfiguracja komputera\Szablony administracyjne\System\Logowanie | Nie wyświetlaj interfejsu użytkownika wyboru sieci | N/D | Włączone |
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\App runtime | Zezwalaj aby konto Micrsoft było opcjoanlne | N/D | Włączone |
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Opcje logowania Windows | Loguj automatycznie ostatnio działającego użytkownika po restarcie systemu | N/D | Wyłączone |
| Konfiguracja komputera\Ustawienia Systemu Windows\Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa dostępu do komputera z sieci | Goście | Goście, konta lokalne<br><br>(dla członków grup: Goście, Konto lokalne oraz członków grupy Administratorzy) |
| Konfiguracja komputera\Ustawienia Systemu Windows\Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa logowania poprzez usługę Remote Desktop | Goście | Goście, konta lokalne |

| *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|
| Konfiguracja Użytkownika\Szablony Administracyjne\Menu Start I Pasek Zadań\Notyfikacje | Wyłącz powiadomienia typu toast na ekranie blokady | N/D | Włączone |

**Nowe ustawienia dla Internet Explorer 11**

Poniżej znajduje się lista zalecanych ustawień dla Internet Explorer 11

| *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zaawansowane | Włącz tryb 64 bity dla zakładek podczas pracy w trybie zaawansowanej ochrony w 64 bitowym systemie Windows | N/D | Włączone |
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Strefa Internet | Nie uruchamiaj oprogramowania antymalware na kontrolkach ActiveX | N/D | Wyłączone |
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Lokalny Intranet | Nie uruchamiaj oprogramowania antymalware na kontrolkach ActiveX | N/D | Wyłączone |
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Strefa Lokalny komputer | Nie uruchamiaj oprogramowania antymalware na kontrolkach ActiveX | N/D | Wyłączone |

| *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Strefa Witryny z ograniczeniami | Nie uruchamiaj oprogramowania antymalware na kontrolkach ActiveX | N/D | Wyłączone |
| Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Strefa Zaufane Witryny | Nie uruchamiaj oprogramowania antymalware na kontrolkach ActiveX | N/D | Wyłączone |

## 14.2. Zmiany w ustawieniach zaleceń

**Ataki typu Pass the Hash**

Poniższe zalecenia rekomendowane są przed mitygowaniem zagrożeń ataków typu Pass the Hash oraz podobnych ataków.

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Security Settings\Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa dostępu do komputera z sieci | Goście | Goście, konta lokalne<br><br>(dla członków grup: Goście, Konto lokalne oraz członków grupy Administratorzy) |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Security Settings\Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa logowania poprzez usługę Remote Desktop | Goście | Goście, Konto lokalne |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Security Settings\Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa logowania jako praca wsadowa | Goście | Goście |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa logowania jako usługa | Goście | Goście |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\ Ustawienia Bezpieczeństwa \Zasady Lokalne\Przypisywanie praw użytkownika | Odmowa logowania lokalnego | Goście | Goście |

**Blokowanie użycia przeglądarek Web na kontrolerach domeny.**

Powszechnie wiadomo, że ze względów bezpieczeństwa użycie przeglądarki internetowej na serwerach z krytycznymi systemami, np. kontrolerem domeny nie jest wskazane. Poniżej przedstawione są zalecenia do ochrony takiego zachowania przez użycie AppLocker. Wiadomo również, że nie ma możliwości ochrony przed tym, aby administratorzy nie omijali tego zabezpieczenia, dlatego też reguła ta ma chronić przed przypadkowym użyciem i uczynić przeglądarkę niedostępną na serwerach kontrolera domeny.

Ustawienia te mogą być również użyte na serwerach z innymi krytycznymi systemami takimi jak przykładowo serwery bazodanowe.

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Nowa wartość* |
|---|---|---|---|
| Wszystkie Serwery Windows „Kontrolery Domeny” | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Kontroli Aplikacji\AppLocker | Włącz wymuszanie wykonywania raguł | Włączone |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Nowa wartość* |
|---|---|---|---|
| Wszystkie Serwery Windows „Kontrolery Domeny” | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Kontroli Aplikacji\AppLocker\Reguły uruchamiania | Blokowanie IE | FilePublisherRule: Deny Everyone PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="WINDOWS® INTERNET EXPLORER" BinaryName="IEXPLORE.EXE" |
| Wszystkie Serwery Windows „Kontrolery Domeny” | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Kontroli Aplikacji\AppLocker\ Reguły uruchamiania | Blokowanie Chrome.exe | FilePublisherRule: Deny Everyone PublisherName="O=GOOGLE INC, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US" ProductName="GOOGLE CHROME" BinaryName="CHROME.EXE" |
| Wszystkie Serwery Windows „Kontrolery Domeny” | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Kontroli Aplikacji\AppLocker\ Reguły uruchamiania | Blokowanie Firefox | FilePublisherRule: Deny Everyone PublisherName="O=MOZILLA CORPORATION, L=MOUNTAIN VIEW, S=CA, C=US" ProductName="FIREFOX" BinaryName="FIREFOX.EXE" |
| Wszystkie Serwery Windows „Kontrolery Domeny” | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Kontroli Aplikacji\AppLocker\ Reguły uruchamiania | Reguły podstawowe | Allow non-admins to run executables in Program Files<br>Allow non-admins to run executables in Windir<br>Allow admins to run executables anywhere |
| Wszystkie Serwery Windows „Kontrolery Domeny” | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Usługi Systemu | Identyfikator aplikacji (AppIDSvc) | Service startup mode = Automatic |

**EMET**

Rekomendowane jest instalowanie EMET na wszystkich stacjach roboczych oraz serwerach wraz z poniższymi ustawieniami Group Policy.

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\EMET | Podstawowa ochrona dla Internet Explorer | N/D | Włączone |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\EMET | Podstawowa ochrona dla Popular Software | N/D | Włączone |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\EMET | Podstawowa ochrona dla Recommended Software | N/D | Włączone |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\EMET | System ASLR | N/D | Włączone: Application Opt-In |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\EMET | System DEP | N/D | Włączone: Application Opt-Out |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\EMET | System SEHOP | N/D | Włączone: Application Opt-Out |

**Zaktualizowany przewodnik**

Poniżej przedstawione są ustawienia, które powinny zostać dodane lub zmienione, aby być zgodnym z innymi liniami bazowymi.

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Składniki systemu Windows\Usługa Dziennika Zdarzeń\Aplikacje | Określ maksymalny rozmiar pliku log (KB) | 20480 | 32768 |
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Składniki systemu Windows\Usługa Dziennika Zdarzeń\Bezpieczeństwo | Określ maksymalny rozmiar pliku log (KB) | 20480 | 196608 |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Składniki systemu Windows\Usługa Dziennika Zdarzeń\System | Określ maksymalny rozmiar pliku log (KB) | 20480 | 32768 |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Wyszukiwanie | Pozwól na indeksowanie szyfrowanych plików | Nie skonfigurowano | Wyłączone |
| Wszystkie systemy operacyjne | Konfiguracja komputera\ Ustawienia Systemu Windows\ Ustawienia Bezpieczeństwa \Reguły Kont\Reguły blokowania konta | Ilość prób logowań | 50 prób błędnego logowania | 10 prób błędnego logowania |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Opcje Bezpieczeństwa | Bezpieczeństwo sieci: Wymuś wylogowanie, kiedy wygasną godziny logowania | Nie skonfigurowano | Włączone |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Opcje Bezpieczeństwa | Kontrola konta użytkownika: Zachowanie podczas żądania elewacji uprawnień dla standardowych użytkowników. | Zapytaj o uprawnienia | Automatycznie blokuj żądania elewacji uprawnień |
| Wszystkie Serwery w członkowstwie | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Opcje Bezpieczeństwa | Bezpieczeństwo sieci: Pozwól aby Lokalny System używał identyfikatora komputera dla NTLM | Nie zdefiniowane | Włączone |
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Przypisywanie praw użytkownika | Dostęp do komputera z sieci | Użytkownicy, Administratorzy | Uwierzytelnieni użytkownicy, Administratorzy |

**Zaawansowane audytowanie**

W przewodniku bezpieczeństwa dla Windows 8 oraz Windows Server 2012 rekomendowane było ustawienie „Brak audytowania”. Pozwalało ono użytkownikowi na decyzję. W Windows 8.1 oraz Windows Server 2012 rekomenduje się użycie wartości “Nie zdefiniowane”.

| ***Baseline*** | ***Ścieżka*** | ***Nazwa reguły*** | ***Poprzednia wartość*** | ***Nowa wartość*** |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logowanie | Audytuj usługę autentykacji Kerberos | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logowanie | Audytuj usługę operacji zgłoszeń Kerberos | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logowanie | Audytuj inne zdarzenia logowania konta | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Zarządzanie kontem | Audytuj zarządzanie grupą aplikacji | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\ Zarządzanie kontem | Audytuj zarządzanie konta komputera | Brak audytowania | Nie zdefiniowane |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\ Zarządzanie kontem | Audytu zarządzanie Grupami Dystrybucji | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Śledzenie szczegółowe | Audytuj aktywności DPAPI | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowane Reguły Audytu\Konfiguracja\ Reguły Audytu\Śledzenie szczegółowe | Audytuj wygaśnięcie procesu | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Śledzenie szczegółowe | Audytuj zdarzenia RPC | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp Usługa Katalogu | Audytuj usługę szczegółowej replikacji katalogu | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\ Dostęp Usługa Katalogu | Audytuj dostęp usługi katalogu | Brak audytowania | Nie zdefiniowane |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne klienckie | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\ Dostęp Usługa Katalogu | Audytuj zmiany usługi katalogu | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\ Dostęp Usługa Katalogu | Audytuj replikację usługi katalogu | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logon/Logoff | Audytuj blokowanie konta | Brak audytowania | Sukces |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logon/Logoff | Audytuj rozszerzony tryb IPSec | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logon/Logoff | Audytuj główny tryb IPSec | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logon/Logoff | Audytuj szybki tryb IPSec | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logon/Logoff | Audit Network Policy Server | Brak audytowania | Nie zdefiniowane |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Logon/Logoff | Audytuj inne zdarzenia Logowania i wylogowania | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audit Certification Services | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj szczegółowe udostępnianie plików | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj udostępnianie plików | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj system plików | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj manipulację uchwytem | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj obiekty jądra | Brak audytowania | Nie zdefiniowane |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj inne zadarzenia dostępu obiektów | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj rejestr | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj Magazyny Wymienne | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Dostęp obiektów | Audytuj SAM | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Zmiana reguły | Audytuj zmiany reguł autoryzacji | Brak audytowania | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Zaawansowana Konfiguracja Reguł Audytu\Reguły Audytu\Zmiana reguły | Audit inne zdarzenia zmiany reguły | Brak audytowania | Nie zdefiniowane |

**Usunięte rekomendacje dla Windows**

Sekcja ta zawiera listę ustawień, która powinna być usunięta z rekomendacji dla Windows.

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Opcje Bezpieczeństwa | Kryptografia system: Używaj algorytmów zgodnych z FIPS do szyfrowania, hashowania oraz podpisywania | Włączone | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Opcje Bezpieczeństwa | Interaktywne logowanie: Wymagaj autentykacji kontrolera domeny do odblokowania stacji roboczej | Włączone | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Opcje Bezpieczeństwa | Kontrola konta użytkownika: Podnoś uprawnienia tylko dla podpisanych i walidowanych plików wykonywalnych | Wyłączone | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Przypisywanie praw użytkownika | Pomijanie sprawdzania omijania | Administratorzy, Użytkownicy, Lokalny Serwis, Usługa Sieciowa | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Dziennika Zdarzeń\Aplikacja | Kontrola zachowania Dziennika Zdarzeń kiedy osiągnie maksymalny rozmiar | Wyłączone | Nie zdefiniowane |
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Dziennika Zdarzeń\Bezpieczeństwo | Kontrola zachowania Dziennika Zdarzeń kiedy osiągnie maksymalny rozmiar | Wyłączone | Nie zdefiniowane |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie systemy operacyjne | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Dziennika Zdarzeń\System | Kontrola zachowania Dziennika Zdarzeń kiedy osiągnie maksymalny rozmiar | Wyłączone | Nie zdefiniowane |
| Wszystkie kontrolery domen | Konfiguracja komputera\Ustawienia Systemu Windows\Ustawienia Bezpieczeństwa\Zasady Lokalne\Przypisywanie praw użytkownika | Zaloguj jako zadanie wsadowe | Administratorzy | Nie zdefiniowane |

**Usunięte rekomendacje dla Internet Explorer**

W tej części zawiera listę ustawień, które powinny być usunięte z rekomendacji dla Internet Explorer. W wielu przypadkach dostarczają niewielką lub znikomą wartość dla bezpieczeństwa.

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie IE | Konfiguracja użytkownika\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\menu przeglądarki | Wyłącz opcję zapisz ten program na dysk | Włączone | Nie skonfigurowano |
| Wszystkie IE | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień | Wyłącz zakładkę zaawansowane | Włączone | Nie skonfigurowano |
| Wszystkie IE | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień | Wyłącz zakładkę Bezpieczeństwo | Włączone | Nie skonfigurowano |

| *Baseline* | *Ścieżka* | *Nazwa reguły* | *Poprzednia wartość* | *Nowa wartość* |
|---|---|---|---|---|
| Wszystkie IE | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Strefa Internet | Kanał uprawnień oprogramowania | Wysokie bezpieczeństwo | Nie skonfigurowano |
| Wszystkie IE | Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Internet Explorer\Panel Ustawień\Zakładka Bezpieczeństwo\Strefa Witryny z ograniczeniami | Kanał uprawnień oprogramowania | Wysokie bezpieczeństwo | Nie skonfigurowano |