SOFTIDEA

SILOGON

Príručka administrátora

(AN232312)

Marec 2012

Obsah

Táto príručka popisuje nastavenie a prevádzku systému *SILOGON* administrátorom tak, aby sa dosiahla maximálna možná miera informačnej bezpečnosti. Za užívateľa systému *SILOGON* sa v tejto príručke považuje osoba, ktorá má v operačnom systéme chránenej pracovnej stanice vytvorené svoje užívateľské konto. Tu popísané operácie týkajúce sa *Tokenu* je potrebné vykonať najprv s *Tokenom* administrátora a potom s *Tokenmi* všetkých ostatných užívateľov systému. V danom čase majte v systéme vložený vždy len jeden *Token*.

1 Charakteristika

- Produkt ***SILOGON*** [1] od spoločnosti ***SoftIdea*** realizuje systém viacfaktorovej autentizácie užívateľov pre počítače s operačným systémom Windows Vista, Windows 7 a Windows 8.

- Užívateľ potvrdzuje svoju identitu súčasným splnením dvoch podmienok:
  - užívateľ vlastní príslušné hardvérové autentizačné zariadenie - ***GNT USB Token*** [2] a zároveň
  - užívateľ pozná informáciu známu len jemu (*heslo užívateľa Tokenu UPW*).

- *SILOGON* spĺňa požiadavky pre prácu s utajovanými skutočnosťami stupňov utajenia Prísne tajné, Tajné a Dôverné definované v § 5 ods. (3) písm. (a) vyhlášky 339/2004 Z.z..

2 Inštalácia

Prihláste sa k cieľovej pracovnej stanici ako administrátor. Pre nainštalovanie produktu *SILOGON* spustite inštalačný program *silogon_setup.exe*. Zvoľte plnú inštaláciu. Po úspešnom nainštalovaní vložte *Token* a zmeňte *heslo administrátora Tokenu APW*. Táto operácia sa vykoná pomocou programu *silogon_admin.exe*, voľba *Zmeniť APW* (pre prvé prihlásenie použite náhradné heslo "admin").

Nové heslo administrátora Tokenu APW uchovávajte bezpečným spôsobom. Budete ho možno potrebovať na odblokovanie hesla užívateľa Tokenu UPW v prípade jeho straty.

---

3 Vydanie Tokenu

Každý užívateľ systému *SILOGON* je držiteľom jedinečného, jemu vydaného, osobného hardvérového autentizačného zariadenia typu *GNT USB Token*. Predpokladajme, že užívateľ má v operačnom systéme pracovnej stanice vytvorené svoje konto, ktoré je asociované s *menom a heslom užívateľa v operačnom systéme*. Vydanie *Tokenu* spočíva v uložení *mena a hesla užívateľa v operačnom systéme* do chránenej pamäti *Tokenu*. Operáciu vykoná administrátor v spolupráci s užívateľom pomocou programu *silogon_admin.exe* nasledujúcim spôsobom:

- aktivuje sa voľba *Vytvoriť užívateľa*,
- užívateľ zadá platné *heslo užívateľa Tokenu* (pre prvé prihlásenie sa použije náhradné heslo "user"),
- zadá sa *meno a heslo užívateľa v operačnom systéme*,

Po vykonaní tejto operácie *Token* obsahuje vo svojej chránenej pamäti autentizačné údaje užívateľa: *meno a heslo užívateľa v operačnom systéme.* Následne je vhodné chránenú stanicu nastaviť tak, aby pri nasledujúcom prihlásení užívateľa bola požadovaná zmena hesla užívateľa. Toto nastavenie vykonajte podľa návodu v kapitole 4.1. Význam tohoto nastavenia pre bezpečnosť systému je vysvetlený v kapitole 4.

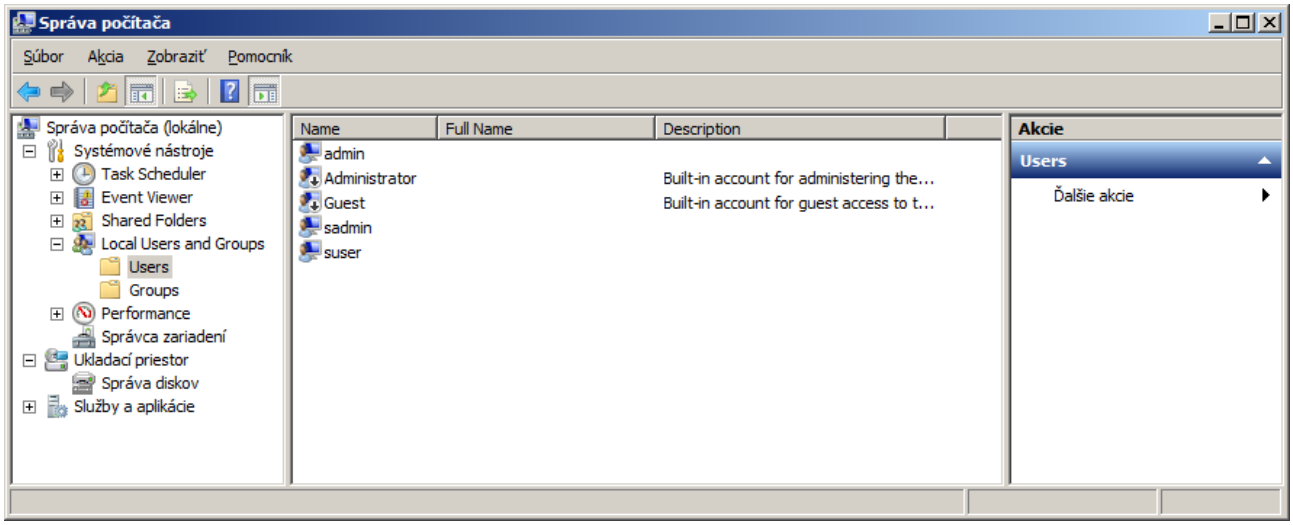
4 Administrátorom vynútená zmena hesiel

Dobrý systém zabezpečenia informačnej bezpečnosti vyžaduje od užívateľa pravidelnú zmenu prístupových hesiel. Systém *SILOGON* zahŕňa sofistikovanú podporu pre administrátorom vynútenú zmenu *hesla užívateľa Tokenu UPW* a zároveň *hesla užívateľa v operačnom systéme*.

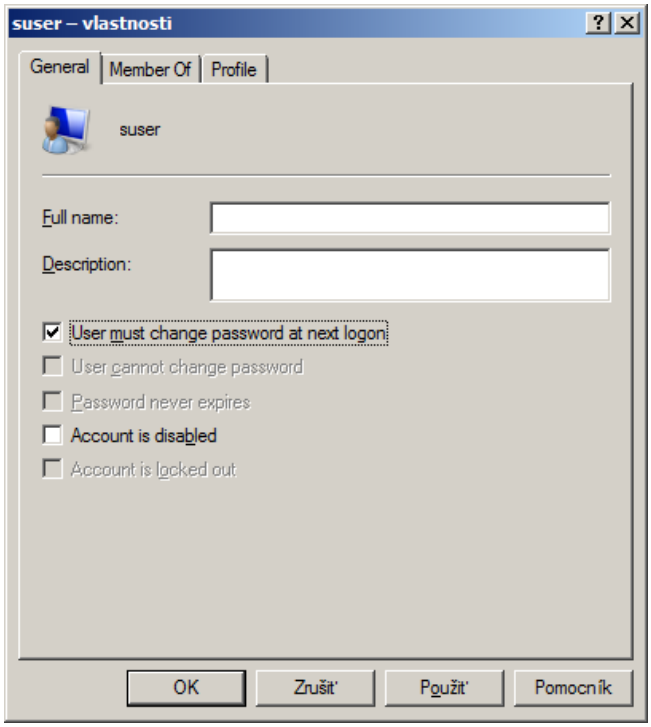
Administrátor vynúti zmenu hesiel jedným zo spôsobov popísaných v kapitolách 4.1 a 4.2:

4.1 Vynútenie zmeny hesla pri nasledujúcom prihlásení

Spustite konzolu pre správu počítača *compmgmt.msc* a aktivujte uzol *Users* tak, ako je to na nasledujúcom obrázku.

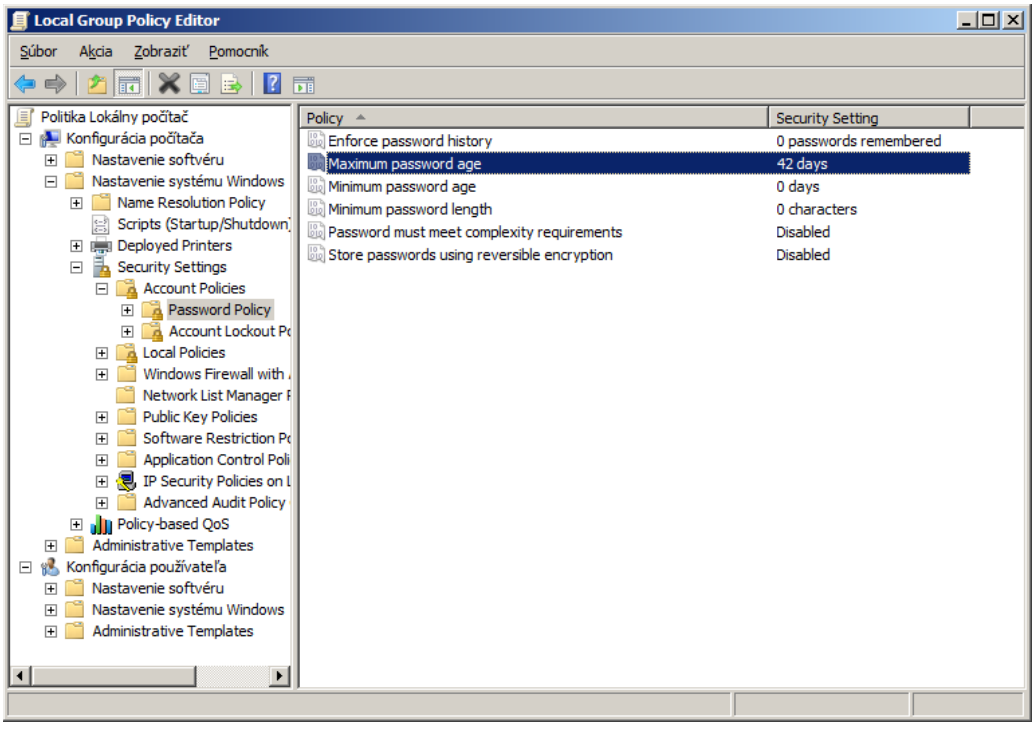


Aktivujte úpravu vlastností užívateľa, pre ktorého chcete nastaviť požadovaný parameter a označte voľbu "*User must change password at next logon*" tak, ako je to na nasledujúcom obrázku.



4.2 Nastavenie maximálnej doby platnosti hesla

Spustite konzolu *gpedit.msc* a nastavte požadovanú hodnotu parametra "*Security Settings/Password Policy/Maximum password age*" podľa nasledujúceho obrázku:



Po aktivácii vynútenej zmeny hesiel v systéme *SILOGON* sa vykonajú v poradí nasledujúce operácie:

- užívateľ je informovaný o povinnosti zmeniť heslo,
- užívateľ po vyzvaní zadá *nové heslo užívateľa Tokenu UPW*,
- *heslo užívateľa Tokenu UPW* sa zmení na *nové heslo užívateľa Tokenu UPW*,
- *heslo užívateľa v operačnom systéme* sa zmení na **náhodne vygenerované silné heslo s dĺžkou 127 znakov**,
- nové *heslo užívateľa v operačnom systéme* sa uloží do Tokenu užívateľa, kde nahradí jeho pôvodnú hodnotu.
- užívateľ je opätovne požiadaný o autentifikáciu s predvyplneným *novým heslom Tokenu UPW*.

Po úspešnej realizácii vynútenej zmeny hesiel v systéme *SILOGON* užívateľ nepozná svoje *nové heslo užívateľa v operačnom systéme*. Pre funkciu systému *SILOGON* táto znalosť nieje potrebná. V prípade potreby, napríklad za účelom zálohovania hesla, je možné za spolupráce užívateľa a administrátora zobraziť *heslo užívateľa v operačnom systéme* pomocou programu *silogon_admin.exe*, voľba *Vypísať zoznam*.

---

5 Vylúčenie štandardného spôsobu autentizácie

Ak administrátor plánuje vylúčiť štandardný spôsob autentizácie užívateľov, je potrebné, aby najprv podľa kapitoly 3 vydal sám sebe Token, ktorým sa bude k stanici prihlasovať.

Inštaláciou produktu *SILOGON* sprístupníte možnosť autentizácie do operačného systému pomocou *Tokenu*. Avšak užívatelia sa naďalej môže autentizovať i štandardným spôsobom - pomocou mena a hesla v operačnom systéme. Ak chcete nastaviť systém tak, aby sa užívatelia mohli prihlásiť výlučne len pomocou svojho *Tokenu*, postupujte podľa pokynov uvedených v tejto kapitole.

1. Spustite *regedit.exe*, zobrazte dostupné moduly *Credential Provider* v lokalite *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers]* . Štandardne sú k dispozícii moduly s nasledujúcimi identifikátormi:

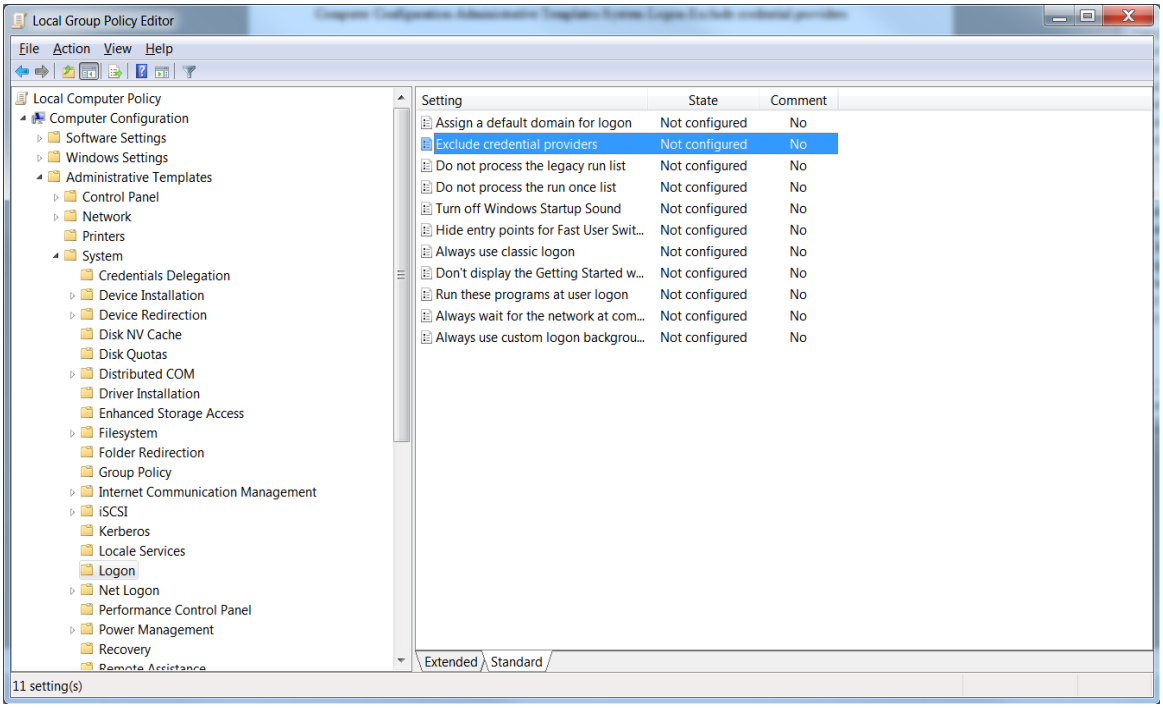
{25CBB996-92ED-457e-B28C-4774084BD562},{3dd6bec0-8193-4ffe-ae25-e08e39ea4063}, {503739d0-4c5e-4cfd-b3ba-d881334f0df2},{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}, {8841d728-1a76-4682-bb6f-a9ea53b4b3ba},{8bf9a910-a8ff-457f-999f-a5ca10b4a885},{94596c7e-3744-41ce-893e-bbf09122f76a},{AC3AC249-E820-4343-A65B-377AC634DC09},{e74e57b0-6c6d-44d5-9cda-fb2df5ed7435}

Identifikátor *{b82ca702-35a8-4e67-8d2a-6c2807b297d3}* identifikuje *Credential Provider* produktu *SILOGON*. Ak sú okrem vyššie uvedených modulov *Credential Providers* zobrazené i

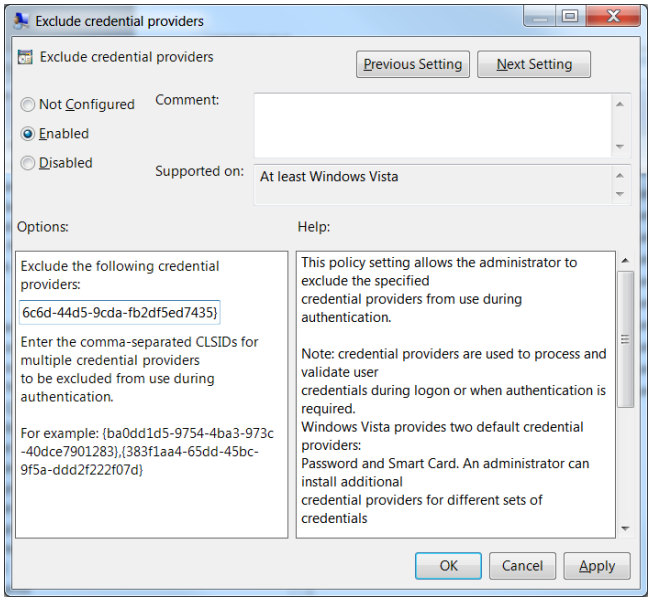
ďalšie, zaznamenajte si ich identifikátory - spolu so štandardnými identifikátormi budú tvoriť zoznam zakázaných identifikátorov.

2. Spustite gpedit.msc a zakážte všetky moduly *CredentialProvider* okrem *CredentialProvider* s identifikátorom *{b82ca702-35a8-4e67-8d2a-6c2807b297d3}*:

3. Prejdite k lokalite *Computer Configuration - Administrative Templates - System - Logon - Exclude credential providers.*



Aktivujte úpravu parametra *Exclude credential providers* a v nasledujúcom okne zvoľte "*Enabled*" a v poli "*Exclude the following credential providers*" vložte čiarkou oddelený zoznam zakázaných identifikátorov vytvorený podľa bodu 1. Kliknite na tlačidlo OK.



Upozornenie: Ak nastavíte systém podľa pokynov uvedených v tejto kapitole, nebude možné prihlásiť sa do operačného systému inak, ako pomocou Tokenu. Ak plánujete odinštalovať produkt SILOGON, budete musieť najprv zrušiť nastavenia podľa bodu 2 a uviesť parameter "Exclude credential providers" do pôvodného stavu (Not Configured).

6 Zmena autentizačných údajov uložených v *Tokene*

Ak sa zmení *meno alebo heslo užívateľa v operačnom systéme* pracovnej stanice inak ako jedným zo spôsobov administrátorom vynútenej zmeny hesiel popísaných v kapitole 4 (napríklad ak užívateľ zmení svoje *heslo v operačnom systéme* v lokalite "*Štart/Ovládací panel/Používateľské kontá a bezpečnosť rodiny/Používateľské kontá/Zmeniť heslo*"), je potrebné tieto údaje manuálne zmeniť i v chránenej pamäti príslušného *Tokenu*. Operáciu vykonajte pomocou programu *silogon_admin.exe* nasledujúcim spôsobom:

- aktivujte voľbu *Zmazať užívateľa* a zmažte z *Tokenu* staré autentizačné údaje užívateľa,
- aktivujte voľbu *Vytvoriť užívateľa* a uložte na *Token* aktuálne autentizačné údaje užívateľa.

7 Zmena hesla užívateľa UPW

Užívateľ môže kedykoľvek zmeniť svoje *heslo užívateľa Tokenu UPW* bez zmeny uložených autentizačných údajov pomocou programu *silogon_user.exe* aktivovaním voľby *Zmeniť UPW*.

8 Odblokovanie hesla užívateľa UPW

Odblokovať *heslo užívateľa Tokenu UPW* pomocou *hesla administrátora tokenu APW* môže byť potrebné napríklad pri strate *UPW* užívateľom. Operáciu vykoná administrátor v spolupráci s užívateľom pomocou programu *silogon_admin.exe* aktivovaním voľby *Odblokovať UPW*.

9 Odblokovanie Tokenu

Po viacnásobnom nesprávnom zadaní *hesla UPW* v súvislom slede *Token* automaticky zničí všetky v ňom uložené údaje a zablokuje sa[1]. V takom prípade sa užívateľ nemôže autentifikovať pomocou *Tokenu* a programy *silogon_admin.exe* a *silogon_user.exe* neregistrujú zablokovaný Token. Pre odblokovanie *Tokenu* vykonajte nasledujúce kroky:

- pomocou programu *Ginit.exe* konfigurujte (*Issue*) *Token* pre prácu s rozhraním *SIPKCS* (postupujte podľa príručky [3]). Funkciu automatického zničenia údajov po viacnásobnom nesprávnom zadaní *hesla UPW* konfigurujte podľa svojich požiadaviek.
- Token je teraz v stave ako po vyrobení. Môžete vydať Token užívateľovi (kapitola 3)

1 Ak je táto funkcia aktívna. Funkciu prvotne konfiguruje výrobca podľa požiadavky v objednávke - pozri [2].

10 Dokumentácia

[1] SILOGON - Katalógový list (AN232310), SoftIdea, s.r.o. , Marec 2012, http://www.softidea.sk/an232310_sk.pdf

[2] GNT USB Token - dátový list, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/gnt_datasheet_sk.pdf

[3] GINIT - užívateľský manuál, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/ginit_manual_sk.pdf

SoftIdea s.r.o.
Sliačska 10, 831 02 Bratislava
tel.: +421 2 444 60 444
fax.: +421 2 446 40 441
http://www.softidea.sk
info@softidea.sk