O mare parte din configurarea sistemului de operare Windows 8 se poate face utilizând instrumente graficeclasice, precum Control Panel şi toate instrumentele din cadrul său. Aceste instrumente sunt destinate utilizatorilor finali şi sunt făcute în aşa fel încât să se poate folosi fără foarte mult efort. Însă, există şi situaţii când trebuie configurate anumite lucruri care nu sunt disponibile prin instrumentele grafice clasice sau când trebuie să interziceţi sau să le permiteţi utilizatorilor să utilizeze anumite instrumente din Control Panel pentru a-i împiedica să facă modificări ce pot influenţa funcţionarea sistemului de operare.

Politicile reprezintă setări care nu sunt disponibile utilizatorilor obişnuiţi, dar pe care le puteţi folosi pentru a-i convinge pe utilizatori să facă anumite lucruri într-un anumit fel sau pentru a le interzice unele lucruri. De exemlu:

- Să-i convingeţi pe utilizatori să creeze parole complexe pentru logare.
- Să-i convingeţi pe utilizatori să-şi schimbe parola o dată la 90 de zile.
- Să dezactivaţi UAC-ul pentru administratori.
- Să porniţi monitorizarea accesului şi a utilizării resurselor partajate.

Pentru a accesa politicile locale şi pentru a le manipula trebuie să vă logaţi pe Windows 8 ca administrator local, iar în ecranul de strat să căutaţi Secpol.msc.

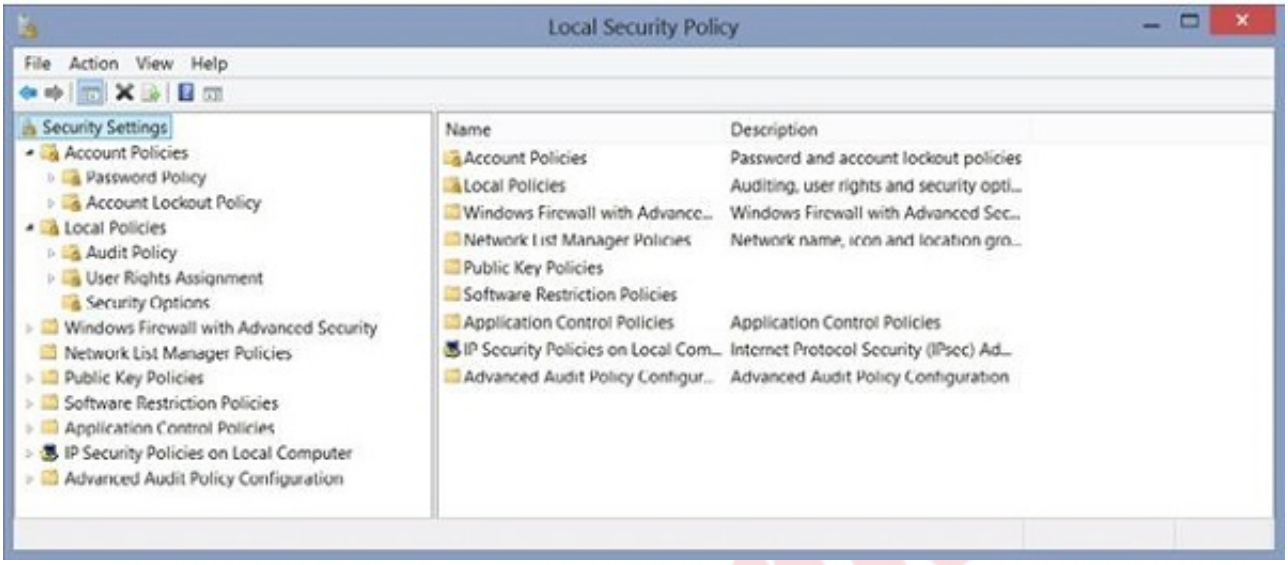

Figura 18.1 Politici locale de securitate

- Account Policiesinclude setările legate de parole şi blocarea conturilor de utilizator. Vă permite să setaţi cererile pentru lungimea şi complexitatea parolei, numărul încercărilor eşuate de logare etc. Se referă doar la conturi create local.
- Local Policies – include setările legate de monitorizare (audit), drepturile utilizatorilor pe calculator şi nivelul de securitate. Vă permite să monitorizaţii comportamentul utilizatorului, să setaţi anumite interdicţii, de exemplu, pentru accesul la calculator prin intermediul reţelei, închiderea calculatorului etc.
- Windows Firewall With Advanced Settings – vă permite să activaţi şi să dezactivaţi firewall-ul şi să îl setaţi în detaliu, iar la final să interziceţi utilizatorilor să schimbe setările pe care le-aţi introdus dvs.
- Network List Manager Policies – vă permite să permiteţi sau să interziceţi utilizatorilor să adauge noi locaţii în reţea, respectiv noi foldere partajate.
- comportamentului calculatoarelor client cu certificate, în mediile unde sunt atribuite certificate clienţilor pentru lucrul în reţea.

- Software Restriction Policies – vă permite să controlaţi ce aplicaţii vor putea să se folosească şi care nu.
- Application Control Policies – reprezintă setarea instrumentului AppLocker.
- IP Security Policies – vă permite să creaţi şi să gestionaţi setările IPSec în reţea.
- Advanced Audit Policy Configuriation – reprezintă setări mai aprofundate ale regulilor pentru monitorizarea comportamentului şi a activităţiloe utilizatorilor.

Prima politică ce ar trebui setată este cea pentru gestionarea parolelor de utilizator: cât de lungă trebuie să fie, când trebuie schimbată sau dacă trebuie să fie complexă.

1. Deschideţi fereastra Local Security Policy şi extindeţi secţiunea Account Policies, apoi Password Policy.

2. Daţi dublu clic pe Enforce Password History. Această setare descrie numărul de parole unice care trebuie să existe, respectiv numărul de parole care nu trebuie să se repete cu ocazia schimbării. Deci, dacă puneţi aici 5, atunci când utilizatorul va schimba parolele va trebui să aibă cinci parole unice şi abia la a 6-a modificare va putea să-şi introducă prima parolă, dacă doreşte acest lucru.

3. Daţi dublu clic pe Maximum Password Age – Valoarea standard de 42 de zile spune că după 42 de zile este necesar ca utilizatorul să-şi schimbe parola, altfel nu va putea să se logheze la calculator.

4. Daţi dublu clic pe Minimum Password Age. Schimbaţi valoarea standard 0 la 10 zile. În acest fel, i-aţi intezis utilizatorului să-şi schimbe parola în primele 10 zile după schimbarea parolei. Deci,

după ce îşi schimbă parola, va trebui să aştepte cel puţin 10 zile pentru a o schimba din nou şi cel mult 42 de zile, deoarece atunci va trebui obligatoriu să o schimbe.

5. Daţi dublu clic pe Minimum Password Lenght. Valoarea standard este 0. Introduceţi 7. Cu aceasta îi obligaţi pe utilizatori ca parola pe care o creează să conţină cel puţin 7 caractere.

6. Daţi dublu clic pe Password Must Meet Complexity Requirements. Daţi un clic pe Enable. Cu aceasta i-aţi obligat pe utilizatori să creeze parole complexe. Parola complexă trebuie să conţină cel puţin trei din următoarele patru tipuri de caractere:

   a. Litere mici

   b. Majuscule

   c. Cifre

   d. Caractere speciale (!“#$%&/()=)

7. Cu aceasta, parola complexă nu poate să conţină trei caractere unite din prenumele, numele utilizatorului şi username.

8. Daţi dublu clic pe Store Password Using Reversible Encriptyon. Dacă activaţi aceeastă opţiune, parolele vor putea fi preluate şi returnate dacă vor fi pierdute, însă această opţiune îi ajută şi pe hackeri să le obţină.

Setările pe care le-aţi făcut în cadrul politicilor locale sunt aplicate imediat, însă parolele pe care le au utilizatorii rămân valabile şi nu se suprapun cu politica decât după 42 de zile.

O altă setare destul de importantă în cadrul politicilor locale, în ceea ce priveşte creşterea nivelului de securitate, este blocarea contului. Aceasta se referă la faptul că, în cazul în care un utilizator îşi introduce greşit parola de mai multe ori, contul acestuia va fi blocat şi nu îl va putea utiliza pentru o anumită perioadă de timp. Setarea acestei politici ajută la apărarea împotriva hackerilor şi a atacurilor lor. Atacul în care un hacker încearcă să ghicească parola utilizatorului încercând să introducă foarte multe parole într-un interval scurt de timp se numeşte „brute-force“. Politica pentru blocarea contului este cea mai bună formă de apărare împotriva acestor atacuri.

1. Deschideţi fereastra Local Security Policy.

2. Extindeţi Account Policy, apoi Account Lockout Policy.

3. Daţi dublu clic pe Account Lockout Threshold. Această setare defineşte câte încercări greşite de logare sunt permise, respectiv câte parole greşite poate să intoducă utilizatorul înainte de a i se bloca contul.

4. Introduceţi 3 şi daţi un clic pe OK.

5. Veţi avea posibilitatea să introduceţi valori pentru Account Lockout Duration şi Reset Account Lockout Counter After. Aceste setări arată pentru cât timp va fi contul inutilizabil după blocare şi după cât timp counter-ul se va întoarce la zero şi îi va permite utilizatorului să încerce să se logheze din nou.

Toate setările pe care le faceţi în cadrul politicii locale le puteţi

împacheta şi exporta pentru a nu fi nevoiţi să faceţi aceleaşi setări pe alte calculatoare din reţea. Este sufient să introduceţi doar politica şi să o importaţi.

1. Deschideţi fereastra Local Security Policy şi daţi clic dreapta pe Security Settings.

2. Selectaţi opţiunea Export Policy.

3. Introduceţii numele sub care veţi salva politica. Politica se salvează în formatul .inf.

4. Copiaţi acest fişier .inf pe un alt calculator.

5. Deschideţi fereastra Local Security Policy pe acesta şi daţi un clic dreapta pe Security Settings.

6. Selectaţi Import Policy şi găsiţi fişierul .inf.

În acest mod, veţi avea aceleaşi setări Security pe ambele calculatoare.

Acum când i-aţi obligat pe utilizatori să-şi aleagă parole puternice şi aţi setat primul nivel de protecţie împotriva atacurilor hackeri-lor, este momentul să vă ocupaţi de restricţionarea utilizatorilor. Utilizatorii obişnuiţi trebuie ţinuţi la distanţă de la setările se sistem şi de opţiunile care pot dăuna sistemului de operare.

User Rights Assignement este secţiunea politicii locale care vă va permite acest lucru. Windows cunoaşte două tipuri de drepturi de utilizator:

- Privilegii – de exemplu, dreptul de a face copii de rezervă pentru fişiere şi foldere.

- Drepturi de logare – de exemplu, dreptul de a se loga pe sistem.

Dacă vă uitaţi cu atenţie peste toate opţiunile care se află în secţiunea User Rights Assignement, veţi vedea că aici aveţi de toate. Utilizatorii sau grupurile de utilzatori care sunt adăugate în cadrul unei opţiuni vor avea dreptul de a face lucrurile pe care le defineşte opţiunea respectivă.

Change The System Time and Change The Time Zone este opţiunea care permite utilizatorilor să acceseze instrumentul Date And Time din Control Panel şi să schimbe ora şi data sau fusul orar.

Allow log on localy este opţiunea care permite utilizatorilor să se logheze local pe calculator.

Deny log on through Remote Desktop Serivces interzice grupului de utilizatori să se conecteze pe calculatorul local de pe o locaţie aflată la distanţă folosind instrumentul Remote Desktop.

Managementul acreditărilor

Credential Manager este parte constitutivă a sistemelor de operare Windows de ceva vremedeja. Acesta se ocupă cu stocarea acreditărilor de utilizator, respectiv a numelor de utilizator şi a parolelor. De fiecare dată când se conectează pe o locaţie sau pe site de pe Internet, utilizatorii îşi introduc numele de utilizator şi parola. Toate aceste acreditări sunt salvate în Credential Manager. Noutatea pe care o aduce sistemul de operare Windows 8 în ceea ce priveşte Credential Manager este Credential Locker. Credential Lockerreprezintă o parte separată a hard disk-ului care este blocată şi în care sunt stocate acum acreditările de utilizator. O altă funcţionalitate importantă pe

care o au utilizatorii sistemului de operare Windows 8 este Credential Locker „traveling“. Toţi utilizatorii care folosesc contul Microsoft pentru logarea pe Windows 8 pot să-şi sincronizeze acreditări pe mai multe dispozitive pentru a putea accesa fără probleme conţinutul de pe Internet de pe oricare dintre ele.

Setarea lui Credential Manager o puteţi face folosind instrumentul din Control Panel. Acest instrument se poate accesa şi prin căutare în ecranul de start.

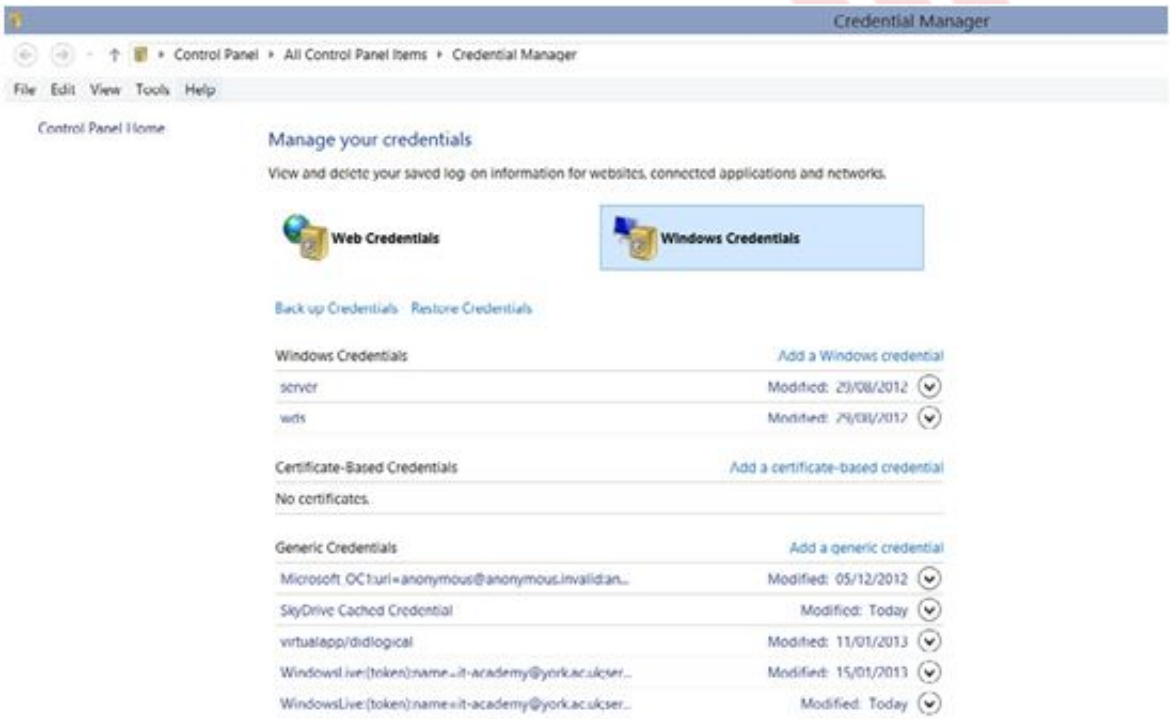

Figura 18.2 Credential Manager

Credential Manager poate colecta acreditările de utilizator pentru aplicaţiile Windows 8 care susţin Credential Manager şi pentru site-urile web pentru care utilizatorul optează să salveze acreditările. Având în vedere acest lucru, Credential Manager împarte acreditările colectate în două categorii:

- Web Credentials

- Windows Credentials

Parolele introduse în Credential Manager le puteţi sincroniza pe fiecare dispozitiv Windows 8. Parolele le puteţi vedea în orice moment printr-o simplă introducere a parolei pentru logare.

Picture password

Având în vedere că Windows 8 nu este destinat doar pentru utilizatorii de calculatoare tradiţionale, ci şi pentru utilizatorii unor dispozitive cu ecrane sensibile la atingere, precum tabletele, Microsoft a creat o nouă posibilitate de logare. Parola sub forma de imagine.

Pentru a permite şi pentru a seta o parolă sub formă de imagine, aveţi nevoie de opţiunea Change PC Settings.

- Apăsaţi tastele Win şi I simultan şi selectaţi Change PC Settings.
- Selectaţi Users.
- Daţi clic pe Create a Picture Password. Trebuie să vă introduceţi parola actuală care va fi ascunsă sub parola sub formă de imagine.
- Selectaţi imaginea pe care vreţi să o setaţi şi să o folosiţi pentru logare.

Figura 18.3 Parola sub formă de imagine

- Desenaţi trei forme pe care le veţi repeta de fiecare dată când doriţi să vă logaţi pe calculator. Puteţi folosi săgeţi, cercuri şi puncte pe imagine.
- Puneţi formele astfel încât să vă amintiţi uşor de locaţia şi dimensiunea lor. Repetaţi procesul încă o dată şi setarea va fi gata. În continuare vă veţi loga folosind imaginea.

Folosirea parolei sub forma de imagine nu este mai puţin sigură decât utilizarea parolei obişnuite sau a PIN-urilor, prin urmare nu trebuie să o ocoliţi dacă vi se pare interesantă.

Pe aceeaşi locaţie unde se află setarea parolei sub formă de imagine, deci în Change PC Settings/Users, se află şi setarea PIN-ului. Personal Identifier Number sau PIN-ul este o "parolă" din patru cifre. Lungimea PIN-ului ne spune că securitatea sa este mult mai slabă decât cea obţinută prin utilizarea parolelor complexe.

Pentru a seta PIN-ul daţi clic pe Create a PIN în cadrul secţiunii Users. Introduceţi parola pe care aţi folosit-o până acum pentru logare. Introduceţi şi repetaţi PIN-ul dorit şi asta este tot.

Ultima metodă, dar poate cea mai importantă pentru pentru logare este logarea pe calculator folosind contul Microsoft. Uneori cunoscut sub denumirea de Windows Live ID, Microsoft Account validează acum acreditările dvs. pe serverele Microsoft în cloud. Îl puteţi folosi pentru logare pe calculator, pe SkyDrive sau pe Skype.

Cel mai mare avantaj în utilizarea contului Microsoft pentru logare constă în faptul că, în acest caz, unele setări se transmit în Cloud şi se salvează în cadrul contului dvs., ceea ce înseamnă că se pot folosi pe fiecare dispozitiv Windows 8 pe care vă logaţi cu acelaşi cont.

Contul dvs. Windows curent îl puteţi transforma în cont Microsoft prin Change PC Settings. În cadrul secţiunii Users, selectaţi Switch To Microsoft Account. Introduceţi parola curentă, apoi numele de utilizator şi parola pentru contul Microsoft.

WIN8_18 - Windows 8

1. Fereastra Local Security Policy o puteţi deschide tastând:

- a) Polsec.msc
- b) Secpol.msc
- c) Secedit.msc
- d) Poledit.msc

2. Setarea lungimii minime şi a complexităţii parolei de utilizator se află în cadrul:

- a) Account Policies
- b) Local Policies
- c) Application COntrol Policies
- d) Advanced Policies

3. Setările, în cadrul politicilor, care vă oferă posibilitatea de a controla ce aplicaţii vor putea fi folosite în sistem se află în:

- a) Account Policies
- b) Account Policies
- c) Application COntrol Policies
- d) Software Restriction Policies

4. Atunci când setaţi o politică conform căreia utilizatorii trebuie să folosească parole complexe, de cel puţin 7 caractere, toti utilizatorii ale căror parole nu îndeplinesc noile condiţii vor fi nevoiţi să-şi schimbe parola imediat.

- a) adevărat
- b) fals

5. Instrumentul care salvează şi memorează toate acreditările de utilizator folosite în timpul lucrului pe sistemul de operare Windows 8 se numeşte:

- a) Credential Manager
- b) Credential Harvester

- c) System Manager
- d) Services Manager

6. Care este numărul maxim de forme pe care le puteţi defini cu ocazia creării parolei sub formă de imagine?

- a) 1
- b) 2
- c) 3
- d) 4

7. PIN este prescurtarea de la:

- a) Personal Identifier Number
- b) Personal Identifier Name
- c) Perspective Identifier Number
- d) Perspective Identifier Name

1. Fereastra Local Security Policy o puteţi deschide tastând:

b

2. Setarea lungimii minime şi a complexităţii parolei de utilizator se află în cadrul:

a

3. Setările, în cadrul politicilor, care vă oferă posibilitatea de a controla ce aplicaţii vor putea fi folosite în sistem se află în:

d

4. Atunci când setaţi o politică conform căreia utilizatorii trebuie să folosească parole complexe, de cel puţin 7 caractere, toti utilizatorii ale căror parole nu îndeplinesc noile condiţii vor fi nevoiţi să-şi schimbe parola imediat.

b

5. Instrumentul care salvează şi memorează toate acreditările de utilizator folosite în timpul lucrului pe sistemul de operare Windows 8 se numeşte:

a

6. Care este numărul maxim de forme pe care le puteţi defini cu ocazia creării parolei sub formă de imagine?

c

7. PIN este prescurtarea de la:

a