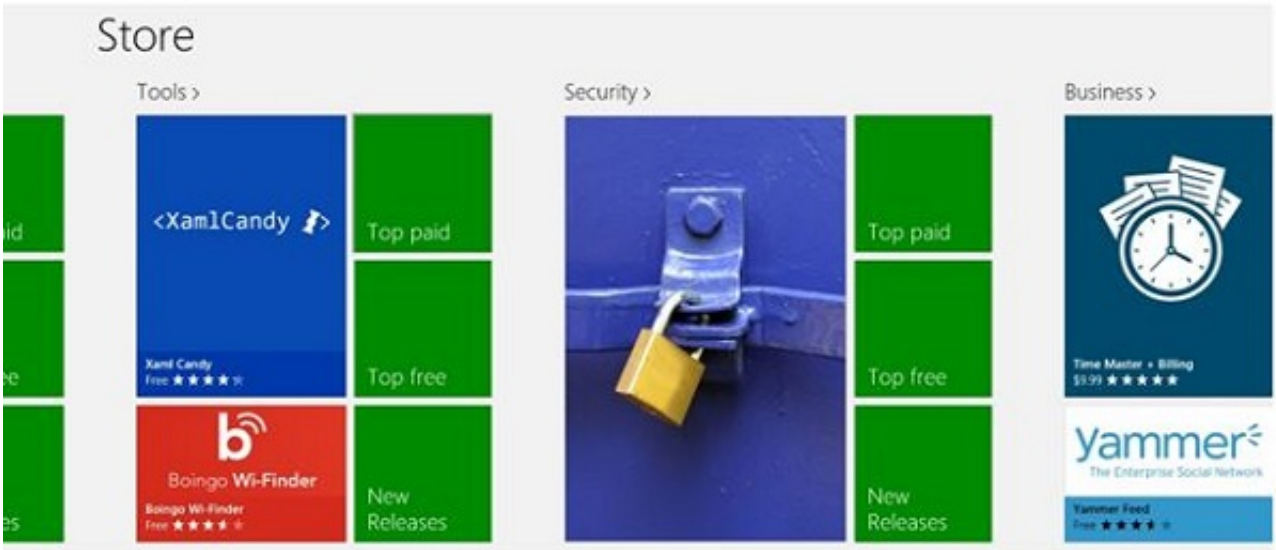
Aplicaţiile sunt cu siguranță cea mai importantă parte a oricărui sistem de operare și sunt necesare pentru o funcționarea normală. Însă, creșterea nivelului de securitate a sistemului de operare trebuie să includă şi aplicaţiile. Fiecare dintre ele poate aduce multe beneficii utilizatorilor, dar, cu siguranță, pot aduce şi o serie de probleme și riscuri.

Windows Store

Windows Store este o aplicație care vine cu sistemul de operare Windows 8 şi pe care o puteți folosi pentru căutarea și instalarea mai ușoară a aplicațiilor care sunt create pentru Windows 8 şi verificate de Microsoft. Aici puteți găsi destule aplicații gratuite și foarte utile, dar puteți găsi şi aplicaţii comerciale care costă peste 500 de dolari.

Windows Store este instalată prin default, deci fiecare instalare a sistemului de operare Windows 8 va conţine şi această aplicație. Se porneşte din ecranul de start și vă oferă o listă lungă de aplicații și o descriere a fiecăreia dintre ele pentru a vă ajuta să alegeți mai uşor ceea ce aveți nevoie.



Imaginea 9.1 Windows Store

Pe lângă toate lucrurile bune pe care această aplicație le aduce, există şi unele părţi proaste. Mai exact, angajații companiei pot folosi această aplicație pentru a instala diferite aplicații sau jocuri. Pentru a preveni acest lucru, trebuie să interziceţi angajaților să folosească Store-ul.

Interzicerea utilizării o puteți face şi la nivel de calculator, și la nivel de utilizator, folosind instrumentul Group Policy Editor.

1. Poziţionaţi-vă pe primul ecran şi tastaţi gpedit.msc. Se va deschide instrumentul Group Policy Editor
2. Pe rând, deschideţi următoarele secţiuni:

    a. User Configuration \ Administrative Templates \ Windows Components \ Store
    b.

LINKgroup

se conectează cu calculatorul respectiv şi după dezinstalare nu o mai puteţi instala prea simplu pe un alt calculator. Va trebui să dezactivaţi un calculator din Store pentru a putea să activaţi altul și pe el să instalaţi aplicația respectivă.

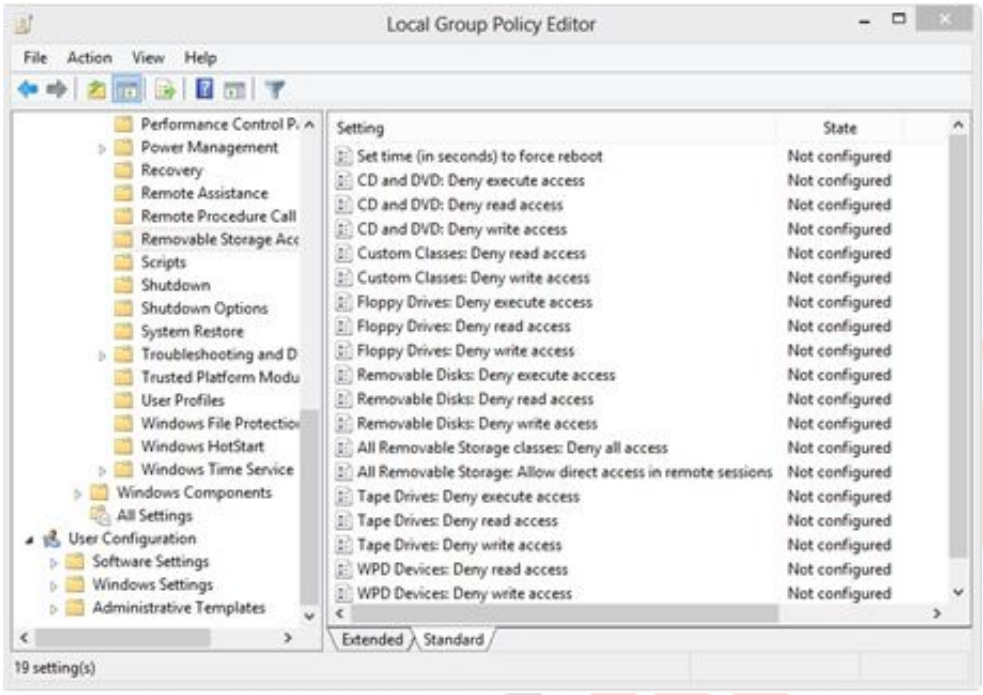
Blocarea accesului la dispozitive externe

Cel mai mare număr de scoateri neautorizate ale datelor din companie se referă la posibilitatea utilizatorilor de a conecta dispozitive externe private la calculatoarele companiei. Cea mai simplă și cea mai frecventă metodă de scurgere a datelor începe cu aducerea disk-urilor sau a USB-urilor externe de către angajaţi și copierea datelor pe ele. O alta, ce poate fi şi mai periculoasă şi care are legătură cu utilizarea disk-urilor externe, este transmiterea unui software maliţios. Dispozitivele externe sunt cunoscute prin faptul că virușii și viermii se lipesc rapid și ușor de ele şi, de fiecare dată când sunt conectate la calculator, se transferă şi se extind. Acest lucru vă obligă să interziceţi utilizarea dispozitivelor USB portabile în organizații și astfel să scăpaţi de o grijă și de eventualele probleme încă de la început.

Interzicerea utilizării dispozitivelor USB se face prin politica de grup. Instrumentul pentru crearea și gestionarea politicilor îl puteţi porni din ecranul de start, introducând gpedit.msc în câmpul de căutare.

Când se deschide instrumentul Group Policy Editor, găsiţi setarea Removable Storage Access. Calea până la aceasta este: Configuration/Administrative Templates/System/Removable Storage Access. Dacă doriți să faceţi setarea pentru utilizatori și nu pentru calculatoare, atunci aceeași setare căutaţi-o în User Configuration, în loc de Computer Configuration.

© Copyright Link group



Imaginea 9.2 Setarea politicii de grup

Această secțiune a politicilor de grup vă oferă posibilitatea de a interzice utilizarea unui număr mai mare de dispozitive externe şi aceasta nu numai prin setarea interdicţiei în totalitate, ci şi prin alegerea activităţilor de care se vor ocupa anumite dispozitive. Dați dublu clic pe opțiunea dorită și activaţi-o prin selectarea câmpului Enabled.

AppLocker

Dacă sunteţi unul dintre acei utilizatori care îşi împart des PC-ul cu alţi membri ai familiei sau cu alţi utilizatori dintr-un oarecare motiv, poate aţi vrea să limitaţi accesul acestora la programele, aplicațiile, fișierele sau documentele dvs. Folosind instrumentul AppLocker, veţi obține câteva opțiuni pentru a face acest lucru şi pentru a le interzice celorlaţi utilizatori să ruleze fișiere executabile, să instaleze aplicații Windows sau să ruleze anumite scripturi.

La fel precum blocarea dispozitivelor externe, și blocarea aplicaţiilor

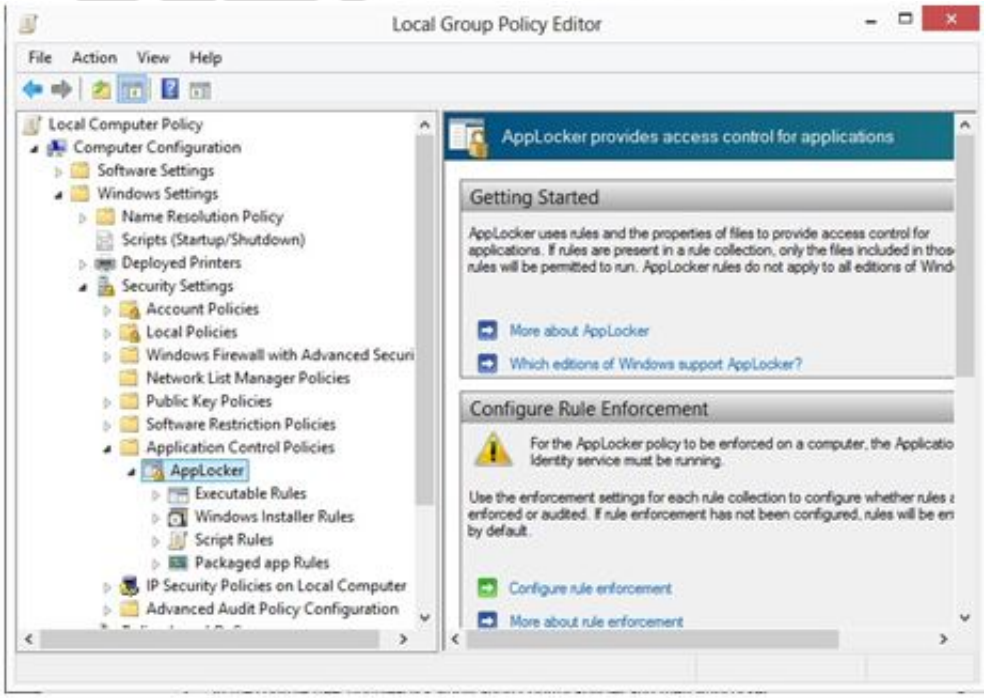
© Copyright Link group

are un rol important atunci când este vorba de ridicarea nivelului de siguranță. Aplicaţiile pot crea multe probleme în cadrul organizației. Utilizatorii care descarcă conținut de pe Internet pot sufoca traficul în reţea folosind torenţi și alte aplicații similare. Din greşeală, pot descărca şi soft-uri maliţioase pe care mai apoi le pot răspândi neintenţionat în întreaga rețea. Deseori, aplicaţiile de chat ocupă mult timp utilizatorilor şi îi distrag de la activitățile lor de lucru etc. Blocarea aplicaţiilor este încă una dintre activitățile pe care le puteţi face folosind politicile.

Aici vă sunt din nou necesare politicile de grup și instrumentul Group Policy Editor. Porniţi-l din ecranul de start, tastând gpedit.msc în câmpul de căutare.

Aveţi nevoie de secţiunea Application Control Policies. Calea până la ea este: Computer Configuration/Windows Settings/Security Settings/Application Control Policies.

Extindeţi acest câmp şi daţi clic pe AppLocker.

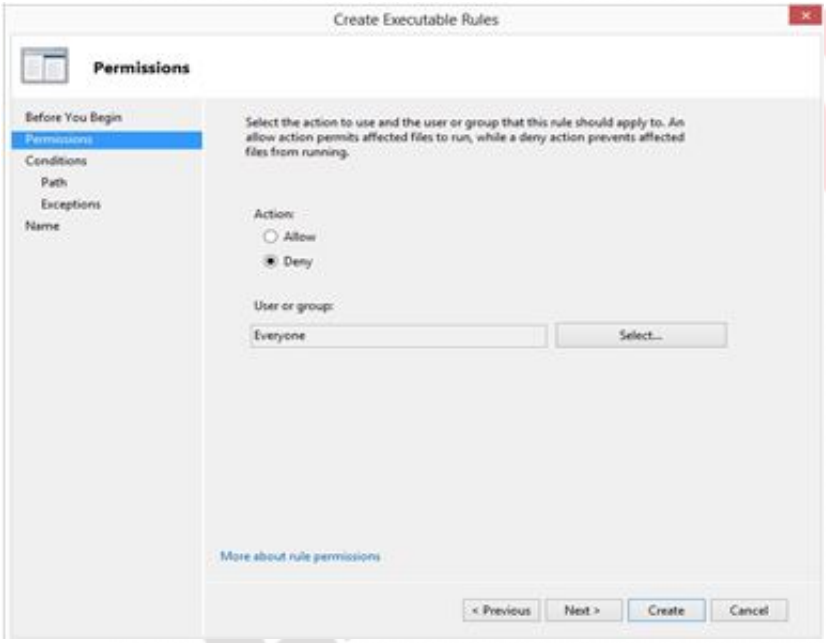


Imaginea 9.3 Setarea politicii AppLocker

© Copyright Link group

Aici puteți crea reguli prin care utilizatorilor individuali le va fi interzisă folosirea anumitor aplicații.

1. Daţi clic dreapta pe Executable Rules şi selectaţi Create Rule.
2. Pe primul ecran aveţi posibilitatea de a permite sau de a interzice utilizatorilor folosirea şi de a selecta grupul de utilizatori căruia îi veţi adăuga această regulă. Marcaţi deny şi selectaţi grupul Everyone, prin care veţi interzice folosirea unei aplicaţii tuturor utilizatorilor.

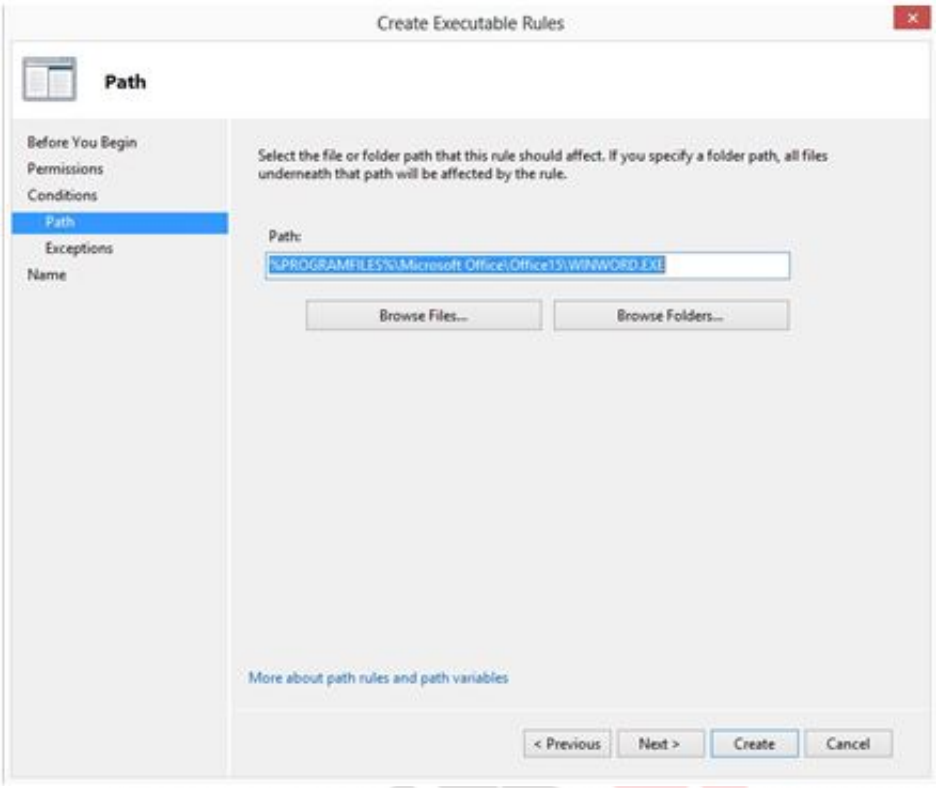


Imaginea 9.4 Crearea regulilor pentru politica AppLocker3.

3. Pe ecranul următor, selectați opţiunea Path pentru a alege una dintre aplicațiile instalate în funcţie de locaţia unde este instalată. În caz contrar, puteți selecta Publisher (pentru a selecta aplicaţia în funcţie de un anumit producător, o anumită versiune etc.) sau opţiunea File hash prin care puteţi separa aplicaţiile după valoarea hash a fișierului propriu-zis.

4. În etapa următoare introduceți locația, respectiv calea până la folderul în care aţi instalat aplicația pe care vreţi să o interziceţi.

© Copyright Link group

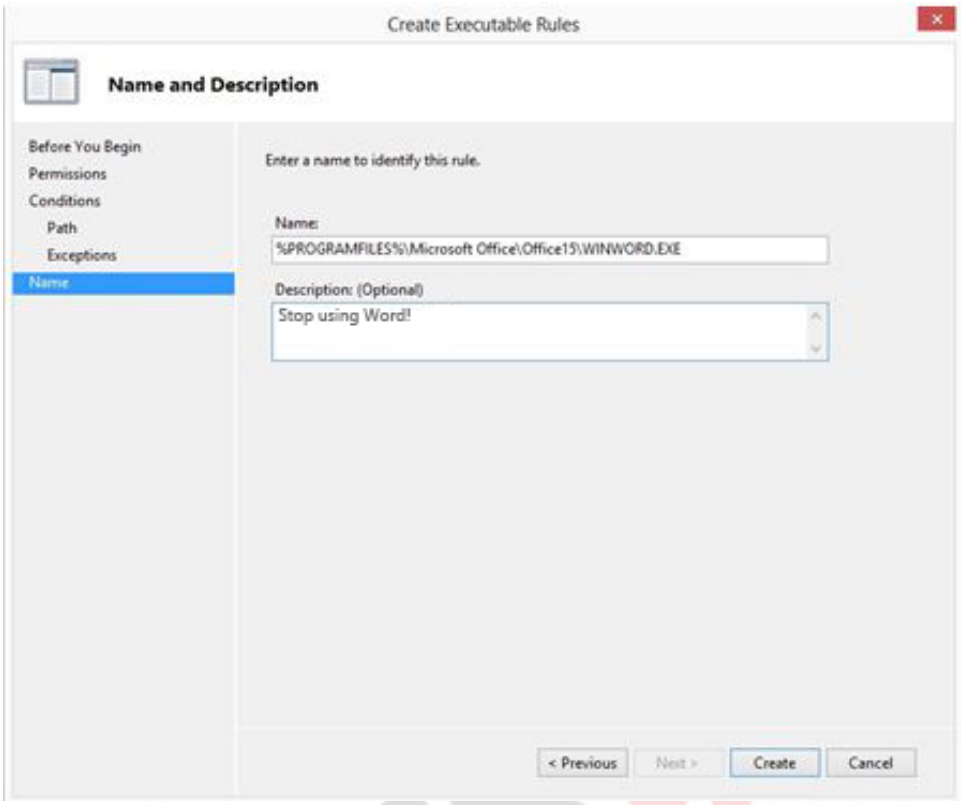


Imaginea 9.5 Crearea regulilor pentru politica AppLocker

5. Următoarea etapă vă oferă posibilitatea de a extrage și de a elimina pe cineva din regulă. În cazul nostru, am interzis utilizarea aplicaţiei Word pentru toți utilizatorii. Acum este momentul potrivit să-l separăm pe unul dintre utilizatori care ar trebui totuşi să utilizeze Word-ul. Puteți face acest lucru cu un clic pe Add din secțiunea Exceptions.

6. În ultima etapă, daţi un nume semnificativ pentru regula pe care o creaţi şi introduceţi-i o descriere pentru a vă descurca mai uşor ulterior. Apoi creaţi-o.

© Copyright Link group



Imaginea 9.6 Crearea regulilor pentru politica AppLocker

Pe lângă crearea unor noi reguli, aveţi şi posibilitatea de a crea reguli predefinite dând un clic dreapta pe Executable Rules și selectând Create Default Rules. Prin selectarea opţiunii Automaticly Generate Rules din acelaşi meniu, permiteţi crearea automată a regulilor pentru toate aplicațiile pe care le instalați mai târziu.

AppLocker funcționează pe principiul structurii regulilor definite cu care se permite sau se interzice efectuarea anumitor acțiuni.

AppLocker se foloseşte pe scară largă în companii și în mediul de afaceri, şi nu doar pe calculatoarele utilizatorilor de acasă.

Acțiunea "Allow" reprezintă o regulă prin care se permite rularea doar a aplicațiilor care se află în lista programelor a căror executare este permisă pe calculator. Rularea programelor care nu se află pe această listă va fi interzisă. Acțiunea "Deny" funcţionează în sens opus, fiind permisă rularea tuturor programelor, cu excepția celor care sunt pe lista de interdicţie.

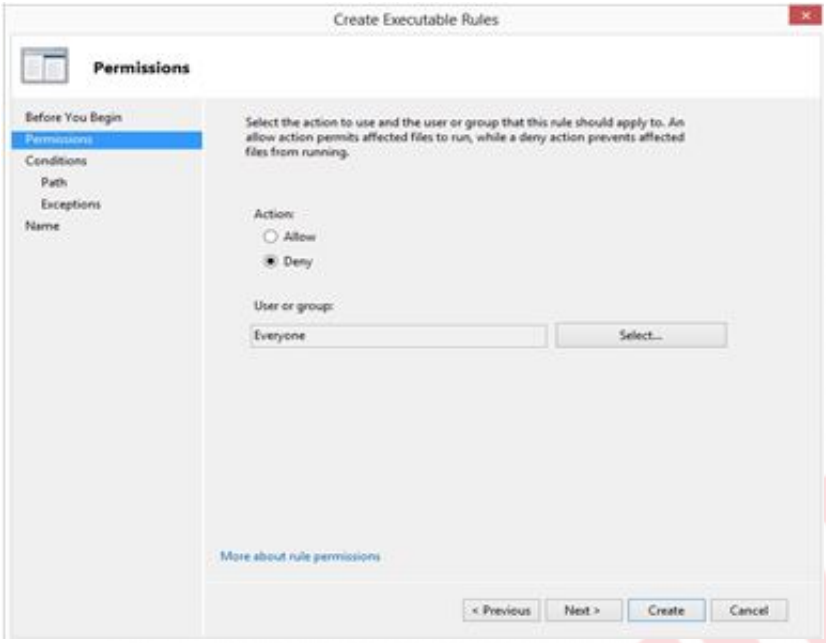
© Copyright Link group

- Să prevină executarea unui software fără licență
- Să prevină pornirea programelor care conțin un cod malițios
- Să împiedice utilizatorul în intenţia de a porni un software care încarcă inutil resursele rețelei
- Să împiedice executarea unor programe care destabilizează mediul desktop și care, în acest fel, creează costuri ridicate pentru suportul tehnic
- Să asigure numeroase posibilităţi de gestionare eficientă a mediului desktop
- Să permită utilizatorilor un upgrade periodic al aplicaţiei fără a fi nevoie ca acest lucru să fie făcut doar de un cerc restrâns de persoane autorizate
- Să ajute la asigurarea unui mediu desktop care este în concordanță cu politicile corporative și cu reglementările din industrie.

AppLocker este un mecanism simplu și flexibil, care permite administrarea și definirea exactă a ceea ce se poate rula sau nu în mediul desktop. Acest mecanism nu doar sporeşte securitatea, ci asigură şi anumite beneficii operative, permiţându-i administratorului:

În acest fel, vă veţi scuti atât pe dvs., cât şi compania de foarte multe probleme!

© Copyright Link group



Imaginea 9.4 Crearea regulilor pentru politica AppLocker

LINK group

WIN8_09 - Windows 8

1. Windows Store trebuie instalată manual pe toate ediţiile sistemului de operare Windows 8, în afară de Windows 8 Enterprise, în care această aplicaţie vine împreună cu sistemul de operare.

- ◯ a) adevărat
- ◯ b) fals

2. Pentru a dezactiva utilizarea aplicaţiei Windows Store, veţi configura opțiunea Store în cadrul politicilor de grup. Această opțiune se află pe locaţia:

- ☐ a) User Configuration \ Administrative Templates \ Windows Components \ Store
- ☐ b) Computer Configuration \ Administrative Templates \ Windows Components \ Store
- ☐ c) Computer Configuration \ Windows Components \ Store
- ☐ d) User Configuration \ Windows Components \ Store

3. Pentru a interzice utilizatorilor să conecteze dispozitive USB şi să lucreze cu ele, veţi folosi:

- ◯ a) Group Policy Editor
- ◯ b) Control Panel
- ◯ c) USB Disabler
- ◯ d) niciuna dintre variantele enumerate nu este corectă

4. Ați observat că utilizatorii folosesc în mod constant una dintre aplicațiile chat. Acestea sunt aplicații prin care se pot transfera și documente, astfel încât pot submina securitatea rețelei. Doriţi să interziceţi utilizarea acestor aplicații. Veţi configura:

- ◯ a) BitLocker
- ◯ b) AppLocker
- ◯ c) Windows Store

© Copyright Link group

- ◯ d) Windows Backup

5. Secțiunea politicilor de grup, referitoare la interzicerea utilizării dispozitivelor mobile, se numeşte Removable Storage Access şi se află în locaţia:

- ◯ a) Computer Configuration / Administrative Templates / System
- ◯ b) User Configuration / Administrative Templates / System
- ◯ c) Computer Configuration / Administrative Templates / Services
- ◯ d) User Configuration / Administrative Templates / Services

6. Când instalaţi o aplicaţie folosind Windows Store nu sunteţi limitaţi la un anumit număr de calculatoare pe care veţi instala aplicaţia.

- ◯ a) adevărat
- ◯ b) fals

7. Folosind politicile de grup şi secţiunea Removable Storage Access, aveţi posibilitatea de a interzice citirea datelor de pe discurile CD/DVD.

- ◯ a) adevărat
- ◯ b) fals

© Copyright Link group

1. Windows Store trebuie instalată manual pe toate ediţiile sistemului de operare Windows 8, în afară de Windows 8 Enterprise, în care această aplicaţie vine împreună cu sistemul de operare.

b

2. Pentru a dezactiva utilizarea aplicaţiei Windows Store, veţi configura opțiunea Store în cadrul politicilor de grup. Această opțiune se află pe locaţia:

a, b

3. Pentru a interzice utilizatorilor să conecteze dispozitive USB şi să lucreze cu ele, veţi folosi:

a

4. Ați observat că utilizatorii folosesc în mod constant una dintre aplicațiile chat. Acestea sunt aplicații prin care se pot transfera și documente, astfel încât pot submina securitatea rețelei. Doriţi să interziceţi utilizarea acestor aplicații. Veţi configura:

b

5. Secțiunea politicilor de grup, referitoare la interzicerea utilizării dispozitivelor mobile, se numeşte Removable Storage Access şi se află în locaţia:

a

6. Când instalaţi o aplicaţie folosind Windows Store nu sunteţi limitaţi la un anumit număr de calculatoare pe care veţi instala aplicaţia.

b

7. Folosind politicile de grup şi secţiunea Removable Storage Access, aveţi posibilitatea de a interzice citirea datelor de pe discurile CD/DVD.

a

© Copyright Link group