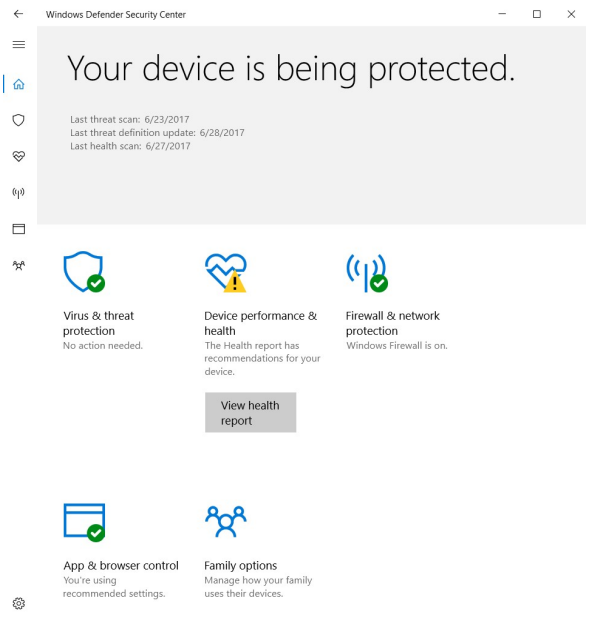
Tema: Securitatea sistemelor de operare Windows

Sistemele de operare asigurară securitatea și integritatea sistemului de calcul. Permite interacțiunea cu mai mulți utilizatori, rularea mai multor aplicații și modificarea strategiilor de răspuns la o anumită problemă.

Sistemul de operare controlează accesul utilizatorilor și proceselor la resursele hadware și software ale sistemului și previne execuția de instrucțiuni invalide, malițioase sau privilegiate.

1.1. Centrul de securitate Windows Defender, figura ,1 oferă zona Protecție împotriva virușilor și amenințărilor, pentru a proteja sistemul de calcul. Sunt disponibile următoarele soluții de securitate:

- *Protecția împotriva virușilor și amenințărilor*, prin scanarea după amenințări și actualizarea la cea mai recentă protecție oferită de Antivirus Windows Defender, vizualizarea scanărilor anterioare împotriva virușilor și amenințărilor.
- *Urmărirea stării de bună funcționare a sistemului și performanță*. Consultantul monitorizează sistemul de calcul și oferă informații, recomandări într-un raport privind starea de bună funcționare pentru a adresa problemele uzuale cu capacitatea de stocare, driverele de dispozitiv, autonomia bateriei, Windows Update sau Fresh Start.
- *Firewall și protecție în rețea*. Se poate vedea starea Firewallului Windows și rețelele la care este conectat sistemul de calcul. Pot fi accesate și setate opțiunile de filtrare a datelor transmise prin rețea în/din sistem.
- *Controlul aplicațiilor și browserului.* SmartScreen contribuie la protejarea dispozitivului dvs. împotriva aplicațiilor, fișierelor, site-urilor web și descărcărilor potențial periculoase.
- *Protejarea familiei* dvs. în mediul online. Opțiunile pentru familie oferă acces ușor la instrumente utile pentru gestionarea vieții digitale a copiilor sau altor membri ai familiei în sistemul de calcul.



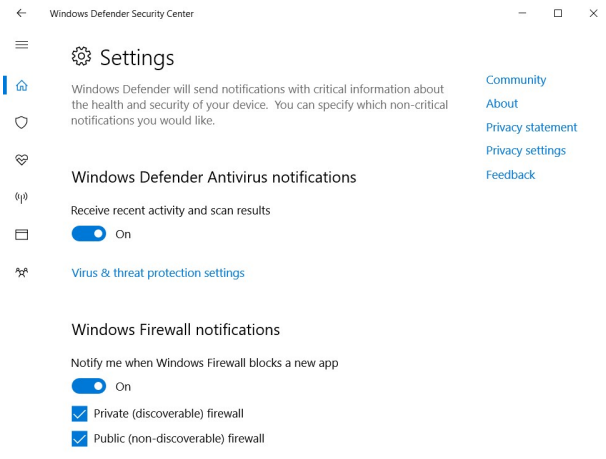


Figura 1. Windows Defender Security Center

1.2. Conturi de utilizator

Conturile de utilizator permit mai multor utilizatori să folosească același sistem de calcul, fiecare având propriul folder privat de *Documente*, poștă electronică, setări, etc. De asemenea, este îmbunătățită securitatea și sunt reduse probleme ce pot apărea la partajarea de fișiere.

Un nou cont de utilizator ar trebui creat atunci când există o altă persoană care lucrează pe același calculator cu tine.

În Windows 10 există două tipuri principale de conturi: administrator și standard (utilizator standard).

Administratorul are acces complet la toate conturile de utilizator de pe calculator. Poate crea și șterge conturi de utilizator, poate crea parole pentru ceilalți utilizatori, le poate schimba numele contului, parola, imaginea sau tipul de cont. Ca regulă, trebuie să existe cel puțin un cont de administrator pe calculator. Implicit, la instalarea sistemului de operare, se creează un cont de administrator.

Utilizatorul standard este configurat de către un administrator. Un utilizator standard poate instala aplicații și poate schimba configurări pentru uzul propriu. Utilizatorii standard nu pot adăuga alți utilizatori și nu pot modifica configurările altor utilizatori.

Își poate modifica imaginea contului și poate crea, modifica sau șterge parola, dar nu poate schimba numele sau tipul contului său. De asemenea, unele programe (mai ales programe vechi) este posibil să nu funcționeze corect pe acest tip de cont. Este posibil ca ele să solicite modificarea temporară sau permanentă a contului utilizator într-unul de administrator.

În plus față de alegerea unuia dintre aceste tipuri de conturi, se poate alege, de asemenea, o metodă de conectare pentru fiecare tip: persoanele se pot conecta la Windows cu un **cont Microsoft** sau cu un **cont local** (figura 2-4).

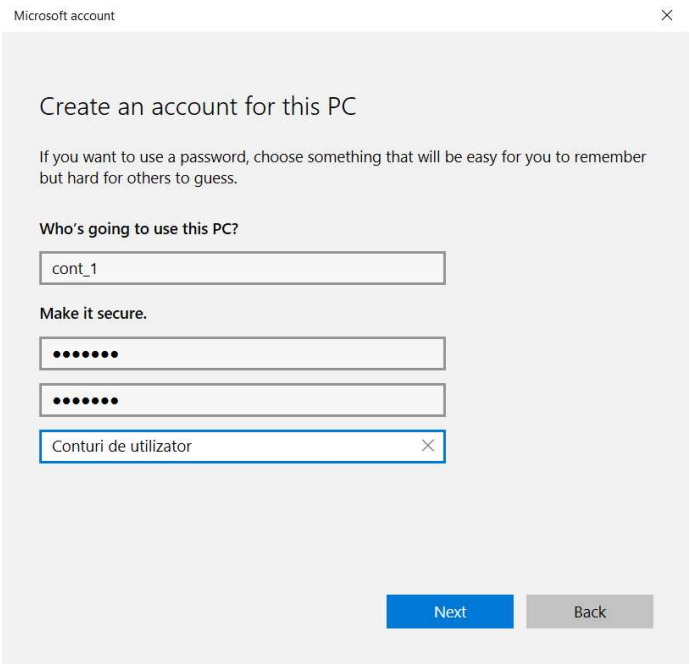


Figura 2. Crearea unui cont în Windows 10

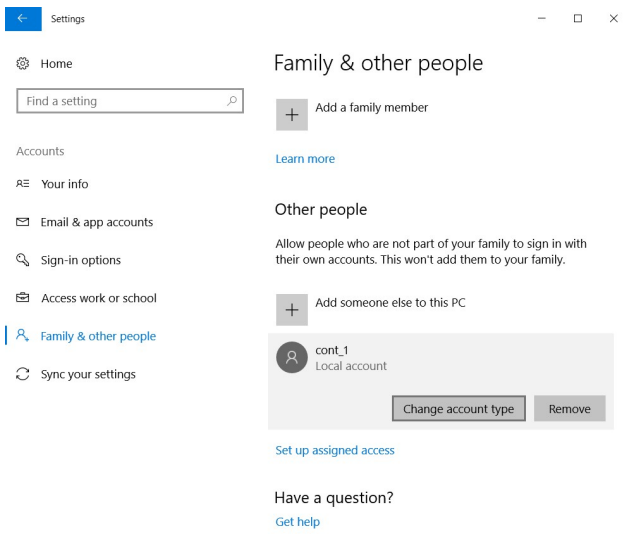


Figura 3. Setările unui cont în Windows 10

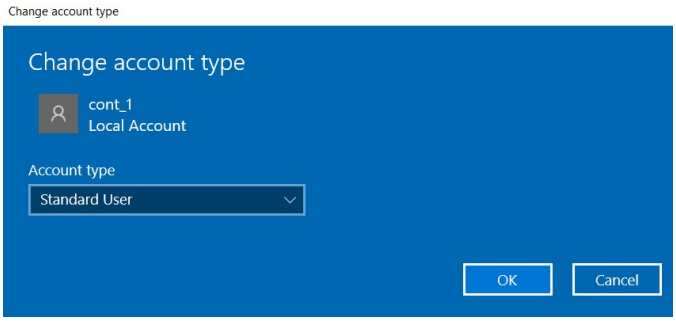


Figura 4. Schimbarea tipului unui cont în Windows 10

RISCURI ȘI RECOMANDĂRI

Accesarea servicilor Web de pe un cont de administrator crează premise de infectare cu programe malițioase, de aceea se recomandă să se utilizeze contul standard. Contul de administrator se utilizează doar în cazul speciale.

Orice activitate din sistem trebuie să poată fi identificată prin contul de utilizator sau adresa IP (să nu fie utilizate instrumente de anonimat în sistemele informatice, cum ar fi de exemplu proxy server-e, anonymizer-r etc.).

Alte tipuri de conturi:

Utilizator administrat. Utilizatorii care sunt administrați cu controale parentale pot accesa doar aplicațiile și conținutul specificat de administratorul care se ocupă de utilizator. Administratorul poate restricționa contactele utilizatorului și accesul la site-uri web și poate aplica limite temporale pentru utilizarea computerului.

Utilizator doar cu drepturi de partajare. Pot accesa de la distanță fișiere partajate, însă nu pot face login și nu pot schimba configurările computerului.

Un *grup* permite mai multor utilizatori să aibă aceleași privilegii de acces. De exemplu, se poate acorda unui grup anumite privilegii de acces la un dosar sau fișier și toți membrii grupului vor avea acces. Se poate aloca privilegii de acces specifice unui grup pentru fiecare din dosarele partajate.

Utilizator vizitator. Poate utiliza temporar computerul dvs., fără a trebui să îi adăugați ca utilizatori individuali. Se poate configura restricții astfel încât vizitatorii să poată accesa doar articolele pe care doriți să le partajați. Fișierele create de un vizitator sunt stocate într-un dosar temporar, dar acest dosar și conținutul său sunt șterse când vizitatorul face logout. Vizitatorii nu au nevoie de o parolă pentru a face login, nu pot schimba configurările pentru utilizator sau computer.

1.3. Gestionarea drepturilor de acces

Utilizatorii (atât de domeniu, cît și locali), grupuri de utilizatori și calculatoare (numite entități) au identificatoare de securitate unice - SID. Cu ajutorul acestui identificator sistemul "știe" entitatea. SID are o valoare unică în domeniu și se formează în timpul creării unui utilizator sau grup, sau atunci când calculatorul este înregistrat în domeniu.

Atunci când un utilizator la conectare introduce numele de utilizator și parola , sistemul de operare verifică dacă parola este corectă și creează un token de acces pentru utilizator. Token-ul include SID și toate SID-urile grupurilor utilizatorului din care utilizatorul face parte.

Pentru obiectele care urmează să fie protejate (cum ar fi fișiere, foldere, registru Windows) se creează un descriptor de securitate. Cu el se asociază ACL (Access Control List - ACL), care conține informații despre modul în care subiecților le sunt date anumite drepturi de acces la obiect. Pentru a determina dacă să se acorde tipul solicitat de acces la obiect, sistemul de operare compară SID în token-ul de acces al subiectului cu SID cuprins în ACL (figura 5).

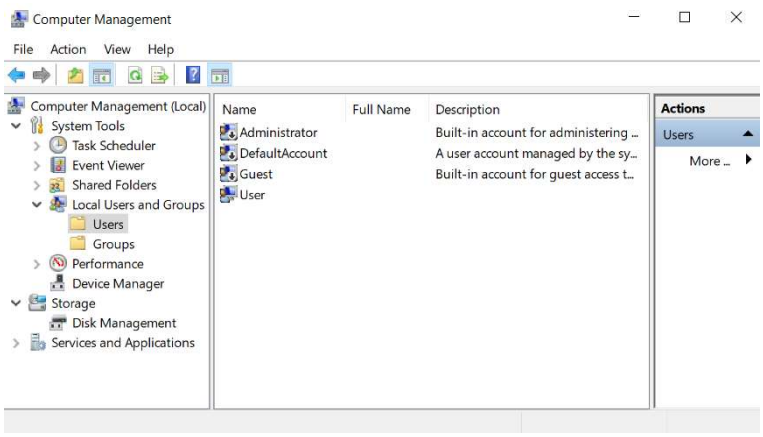


Figura 5. Utilizatorii locali și grupurile de utilizatori

Permisiunile sunt sumate, iar interdicția este o prioritate mai mare decât permisiunea. De exemplu, în cazul în care utilizatorul are permisiunea de a citi dosarul, și în grupul din care face parte - de a scrie, ca urmare utilizatorul poate citi și scrie. În cazul în care utilizatorul are permisiunea de a citi, și grupul din care face parte, citirea este interzisă, utilizatorul nu poate citi fișierul.

Dacă vorbim despre fișiere și foldere, mecanismele de securitate din sistemele de fișiere sunt acceptate numai pe discuri cu sistem de fișiere NTFS. Sistemul de fișiere FAT (și varianta sa - FAT32) nu implică posibilitatea de a stoca ACL, asociat cu fișierul (figura 6,7).

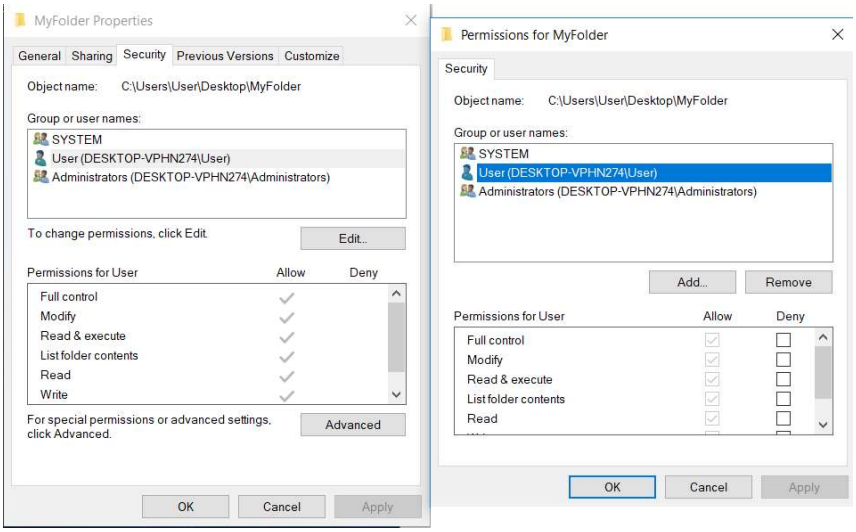


Figura 6. Drepturile de acces la fișiere și foldere

Următorul tabel descrie permisiunile speciale pentru fișiere și foldere.

Permisiuni speciale	Control total	Modificare	Citire și executare	Listare conținut folder	Citire	Scriere
Parcurgere folder / Executare fișier	da	da	da	da	nu	nu
Listare folder / Citire date	da	da	da	da	da	nu
Citire atribute	da	da	da	da	da	nu
Citire atribute extinse	da	da	da	da	da	nu
Creare fișiere / Scriere date	da	da	nu	nu	nu	da
Creare foldere / Adăugare date	da	da	nu	nu	nu	da
Scriere atribute	da	da	nu	nu	nu	da
Scriere atribute extinse	da	da	nu	nu	nu	da
Ștergere subfoldere și fișiere	da	nu	nu	nu	nu	nu
Ștergere	da	da	nu	nu	nu	nu
Citire permisiuni	da	da	da	da	da	da
Modificare permisiuni	da	nu	nu	nu	nu	nu
Preluare în proprietate	da	nu	nu	nu	nu	nu
Sincronizare	da	da	da	da	da	da

Figura 7. Permisiuni speciale pentru fișiere și foldere

RISCURI ȘI RECOMANDĂRI

Fiecărui utilizator trebuie să-i fie comunicat, într-o formă stabilită de responsabilul de securitate cibernetică sau de către persoana responsabilă de proces (administratorul), drepturile, obligațiile, restricțiile și responsabilitățile privind utilizarea mijloacelor TIC în activitatea de serviciu;

Să-i fie asociat un cont de utilizator specific atribuțiilor de serviciu, cu funcții de administrare sau cu funcții de utilizator. Să fie utilizate în sistem mijloacele tehnice speciale, care să interzică utilizarea acestor conturi de către persoane terțe.

1.4. Politicile de securitate

Politicile de securitate Windows sunt foarte eficiente în protejarea mașinilor Windows prin asigurarea accesului restricționat la utilizatori. Dacă politicile de securitate Windows nu sunt configurate corect, utilizatorii pot manipula ușor registrul, applet-urile panoului de control, și alte setări de sistem critice, ceea ce poate duce la blocarea sistemului. Prin urmare, configurarea în mod corespunzător a politicilor de securitate pentru Windows în fiecare mașină windows din rețea este foarte important (figura 8).

Politica de securitate locală a unui sistem este un set de informații cu privire la securitatea unui calculator local. Informațiile politicii de securitate locale include următoarele:

1. Domeniile de încredere pentru a autentifica încercări de conectare.
2. Care conturi de utilizator pot accesa sistemul și cum. De exemplu, interactiv, printr-o rețea, sau ca un serviciu.
3. Drepturile și privilegiile atribuite conturilor.
4. Politica de audit de securitate.

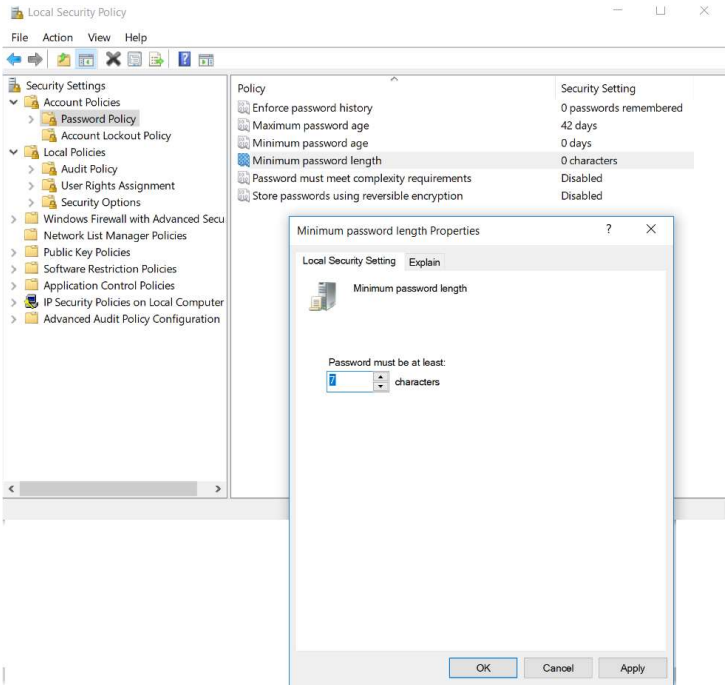


Figura 8. Politici de securitate privind utilizarea parolelor