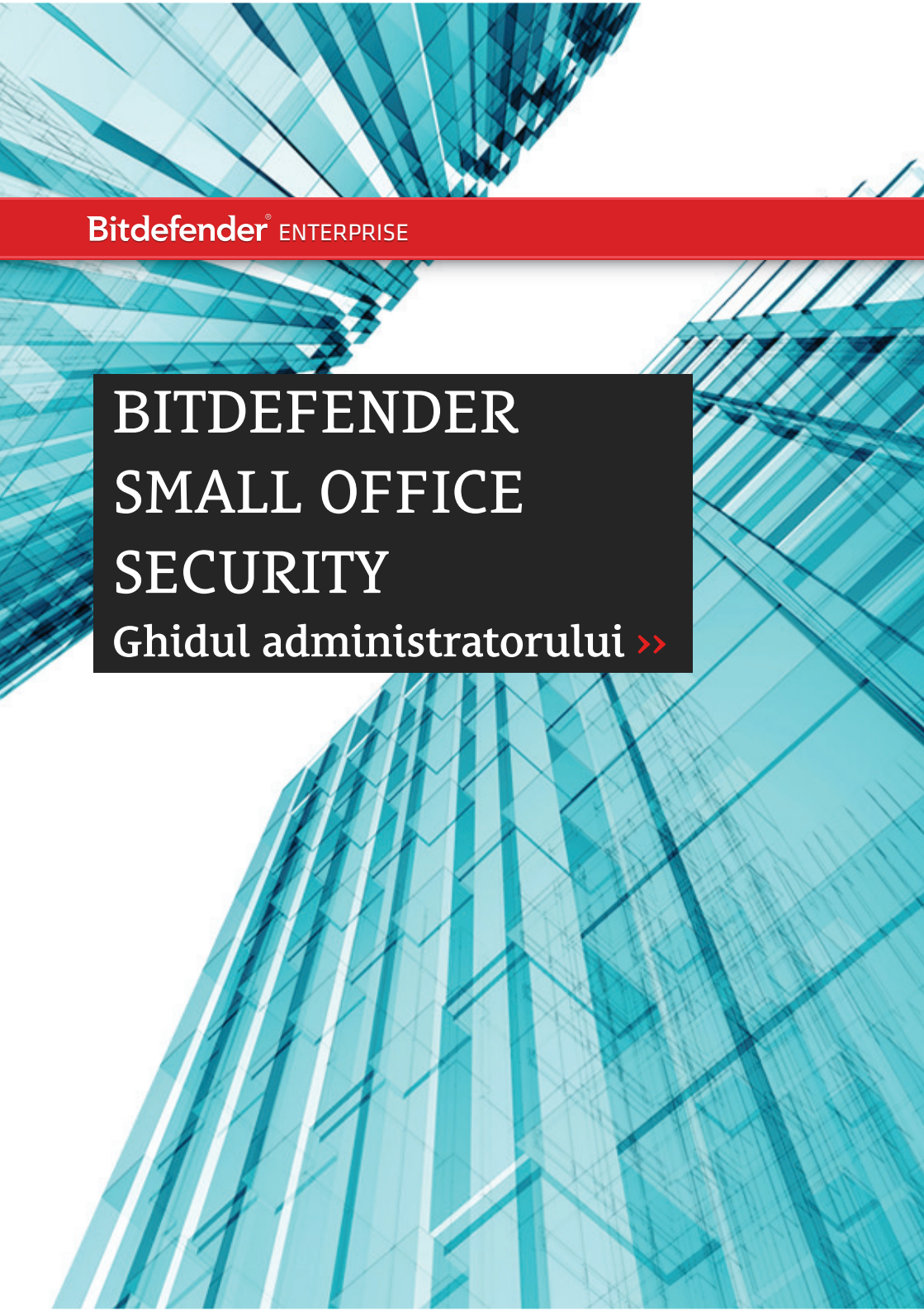

Bitdefender® ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Ghidul administratorului ››

Bitdefender Small Office Security
Ghidul administratorului

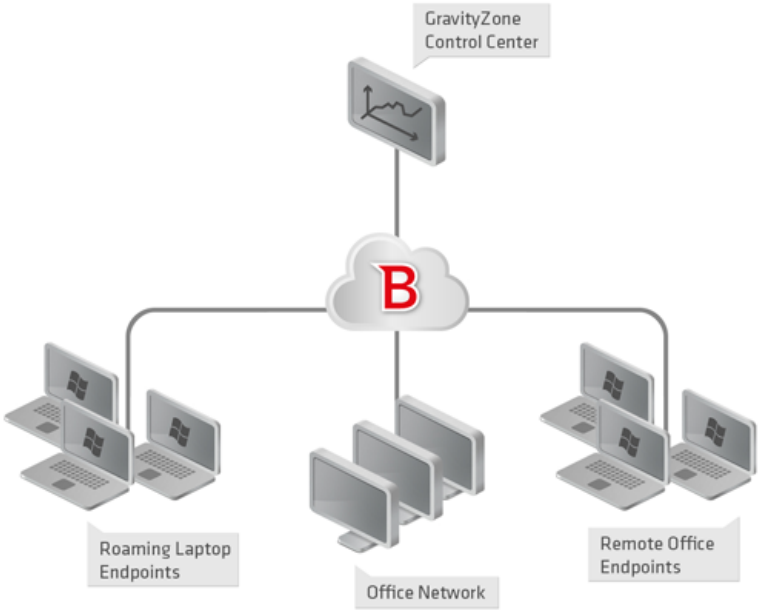
Publicat 2015.01.21


Bitdefender

Cuprins

1. Despre Small Office Security

Small Office Security este un serviciu de protecție împotriva programelor malware, găzduit în cloud, dezvoltat de Bitdefender pentru calculatoarele cu sistem de operare Microsoft Windows și Macintosh. Aceasta folosește un model centralizat de instalare multiplă de tip Software-as-a-Service potrivit pentru clienții de tip organizație, profitând în același timp de tehnologiile de protecție împotriva programelor malware dezvoltate de Bitdefender pentru piața de consum.



Arhitectura Small Office Security

Serviciul de securitate este găzduit în cloudul public al Bitdefender. Abonații au acces la interfața de administrare pe platformă web denumită **Control Center**. Prin această interfață, administratorii pot instala și administra de la distanță protecția antimalware pe calculatoarele Windows și Macintosh, cum ar fi: serverele și stațiile de lucru din cadrul rețelei interne, laptopurile conectate prin roaming sau stații de lucru ale companiei aflate la distanță.

Pe fiecare calculator protejat se instalează o aplicație locală denumită **Endpoint Security**. Utilizatorii locali au vizibilitate limitată și doar drept de vizualizare a setărilor de securitate,

care sunt administrate de către administrator din Control Center; în timp ce scanările, actualizările și modificările de configurație se realizează de obicei în fundal.

2. Introducere

Funcționalitățile Small Office Security pot fi configurate și administrate cu ajutorul unei platforme de control centralizată denumită Control Center. Consola Control Center are o interfață web, pe care o puteți accesa folosind numele de utilizator și parola.

2.1. Conectarea la Control Center

Accesul la Control Center se realizează prin conturile de utilizator. Veți primi informațiile dumneavoastră de autentificare prin e-mail odată ce contul dumneavoastră a fost creat.

Cerințe preliminare:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Rezoluție recomandată a ecranului: 1024x768 sau mai mare

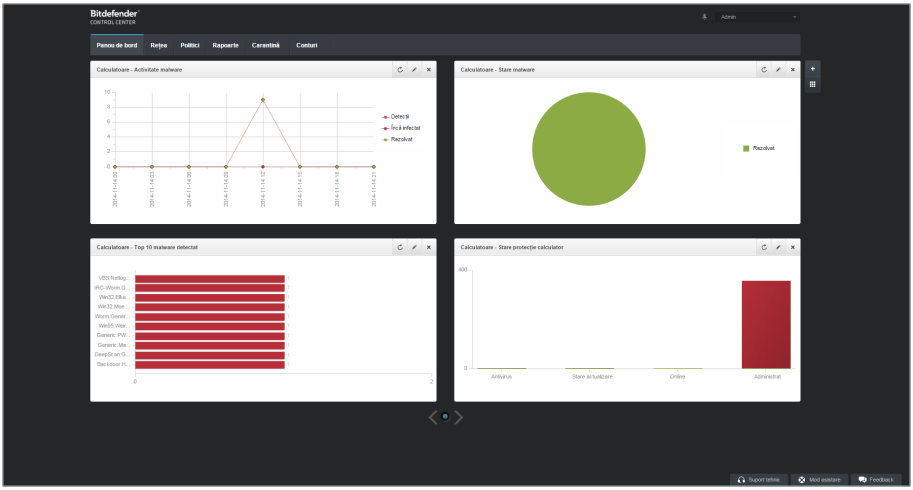
Pentru conectarea la Control Center:

1. Deschideți browser-ul web.
2. Accesați următoarea adresă: https://gravityzone.bitdefender.com
3. Introduceți adresa e-mail și parola contului dumneavoastră.
4. Faceți clic pe **Autentificare**.

Notă
Dacă ați uitat parola, utilizați legătura de recuperare a parolei pentru a solicita o nouă parolă. Trebuie să furnizați adresa e-mail a contului dumneavoastră.

2.2. Control Center dintr-o privire

Consola Control Center este organizată astfel încât permite accesul facil la toate funcțiile. Utilizați bara de meniu din zona superioară pentru a naviga prin consolă. Funcțiile disponibile depind de tipul de utilizator care accesează consola.



Panoul de bord

2.2.1. Vedere de ansamblu asupra Control Center

Utilizatorii care dețin rolul de administrator al companiei dețin drepturi depline asupra configurației Control Center și setărilor de securitate a rețelei, în timp ce utilizatorii cu rol de administrator au acces la funcțiile de securitate a rețelei, inclusiv administrarea utilizatorilor.

În funcție de rolul deținut, administratorii Small Office Security pot accesa următoarele secțiuni din bara de meniu:

Panou de bord

Vizualizați grafice ușor de citit care furnizează informații cheie despre securitatea rețelei dumneavoastră.

Rețea

Instalați protecția, aplicați politici pentru a administra setările de securitate, rulați sarcini de la distanță și generați rapid rapoarte.

Politici

Creați și administrați politici de securitate.

Rapoarte
Obțineți rapoarte de securitate referitoare la clienții administrați.

Carantină
Administrați de la distanță fișierele aflate în carantină.

Conturi
Administrați accesul la Control Center pentru alți angajați ai companiei.

Notă
Acest meniu este disponibil numai utilizatorilor care dețin drepturi de Administrare a utilizatorilor.

În plus, în colțul din dreapta sus al consolei, pictograma **Notificări** oferă acces facil la mesajele de notificare precum și la pagina **Notificări**.

Dacă apăsați pe numele de utilizator din colțul din dreapta sus al consolei, sunt disponibile opțiunile următoare:

- **Contul meu**. Faceți clic pe această opțiune pentru a administra detaliile și preferințele contului dumneavoastră de utilizator.
- **Compania mea**. Faceți clic pe această opțiune pentru a administra detaliile și preferințele contului dumneavoastră de companie.
- **Administrare date de autentificare**. Faceți clic pe această opțiune pentru adăugarea sau administrarea datelor de autentificare necesare pentru sarcinile de instalare de la distanță.
- **Deconectare**. Faceți clic pe această opțiune pentru a ieși din contul dumneavoastră.

În colțul din dreapta jos al consolei, sunt disponibile următoarele link-uri:

- **Suport tehnic**. Faceți clic pe acest buton pentru a obține asistență și informații de ajutor.
- **Mod asistare**. Faceți clic pe acest buton pentru a activa o funcție de ajutor care include casete extensibile cu sfaturi pe elementele din Control Center. Veți afla cu ușurință informații utile referitoare la funcțiile Control Center.
- **Trimiteți feedback**. Faceți clic pe acest buton pentru afișarea unui formular care vă permite să editați și să trimiteți mesaje de feedback referitoare la experiența cu Small Office Security.

2.2.2. Date tabelare

Tabelele sunt deseori utilizate în cadrul consolei, pentru organizarea datelor într-un format ușor de utilizat.

Pagina de Rapoarte - Tabel rapoarte

Navigarea prin pagini

Tabelele cu mai mult de 10 intrări au mai multe pagini. În mod implicit, se afișează numai 10 intrări/pagină. Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Puteți modifica numărul de intrări afișate pe pagină selectând o altă opțiune din meniul de lângă butoanele de navigație.

Căutarea anumitor intrări

Pentru a găsi cu ușurință anumite intrări, folosiți casetele de selectare de sub titlurile coloanelor.

Introduceți termenul căutarii în câmpul corespunzător. Elementele care corespund criteriilor de căutare sunt afișate în tabel pe măsură ce tastați. Pentru resetarea conținutului tabelului, ștergeți informațiile din câmpurile de căutare.

Sortarea datelor

Pentru a sorta datele dintr-o coloană, faceți clic pe titlul acesteia. Faceți clic pe titlul coloanei din nou pentru a inversa ordinea sortării.

Reîmprospătarea datelor tabelare

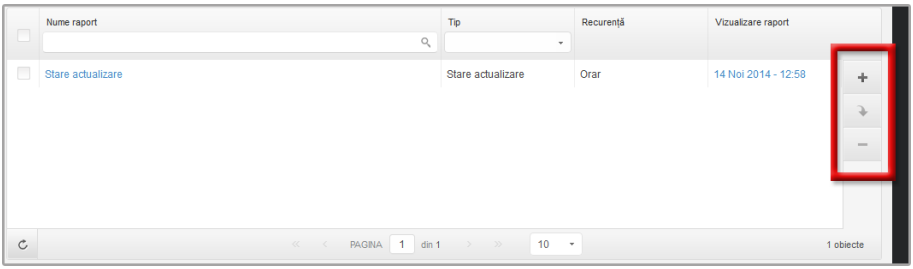
Pentru a vă asigura că în consolă se afișează cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din colțul din stânga jos al tabelului.

2.2.3. Bare de instrumente pentru acțiuni

În Control Center, barele de instrumente de acțiuni vă permit să efectuați anumite operațiuni aferente secțiunii în care vă aflați. Fiecare bară de instrumente include o serie de pictograme care se află în partea din dreapta tabelului. De exemplu, bara de instrumente de acțiuni din secțiunea **Rapoarte** vă permite să efectuați următoarele operații:

- Crearea unui nou raport.

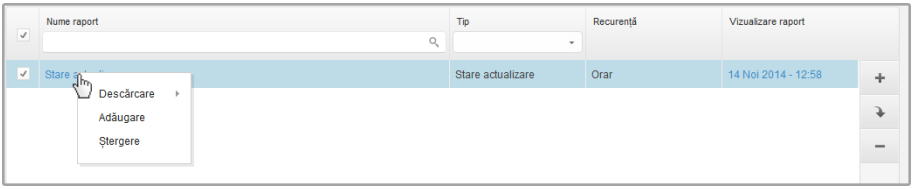
- Descărcare rapoarte generate de un raport programat.
- Ștergerea unui raport programat.



Pagina de Rapoarte - Bare de instrumente pentru acțiuni

2.2.4. Meniul contextual

Comenzile de pe bara de instrumente pentru acțiuni sunt, de asemenea, accesibile din meniul contextual. Faceți clic dreapta pe secțiunea Control Center pe care o utilizați și selectați comanda de care aveți nevoie din listă.

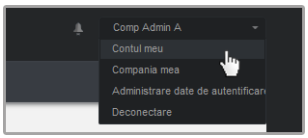


Pagina de Rapoarte - Meniu contextual

2.3. Administrarea contului dumneavoastră

Pentru a verifica sau modifica detaliile și setările contului dumneavoastră:

1. Îndreptați cursorul către numele de utilizatorul din colțul din dreapta sus al consolei și selectați **Contul meu**.



Meniul Cont de utilizator

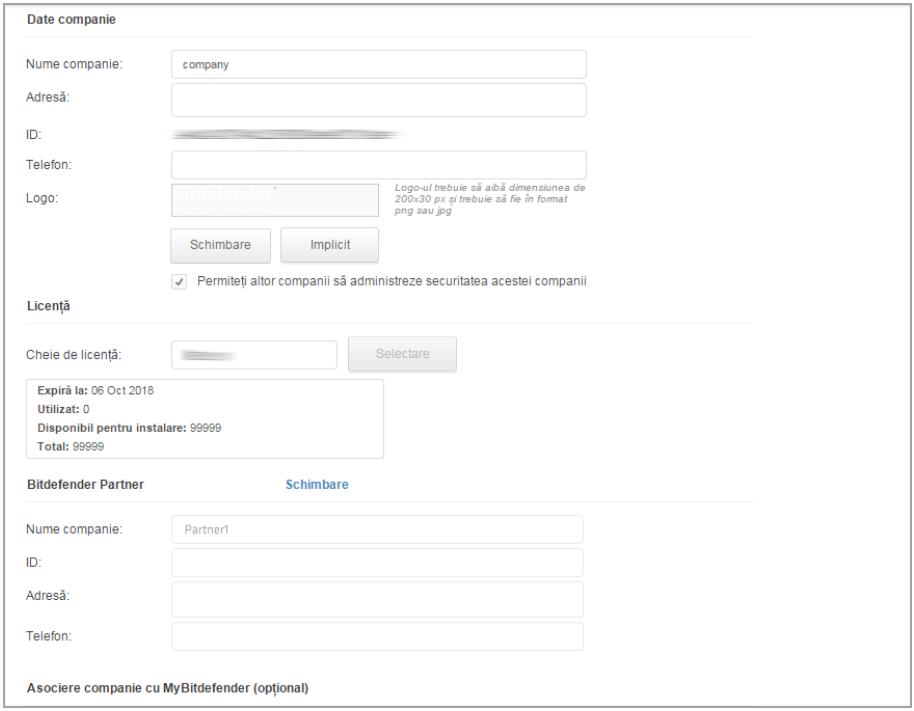
2. În secțiunea **Detalii cont**, corectați sau actualizați detaliile contului dumneavoastră.
   - **Nume complet.** Introduceți numele complet.
   - **E-mail.** Aceasta este adresa dumneavoastră e-mail pentru autentificare și contact. Rapoartele și notificările importante de securitate sunt expediate la această adresă. Notificările prin e-mail sunt expediate automat oricând sunt detectate situații de risc în rețea.
   - **Parolă.** Linkul **Modificare parolă** vă permite să schimbați parola de conectare.
3. În secțiunea **Setări**, configurați setările contului conform preferințelor dumneavoastră.
   - **Fus orar.** Selectați din meniu fusul orar al contului. Consola va afișa informațiile referitoare la oră conform fusului orar selectat.
   - **Limba.** Selectați din meniu limba de afișare a consolei.
   - **Expirare sesiune.** Selectați intervalul de inactivitate înainte ca sesiunea dvs. ca utilizator să expire.
4. Faceți clic pe **Salvare** pentru a aplica modificările.

Notă
Nu vă puteți șterge propriul cont.

2.4. Administrarea companiei dumneavoastră

Ca utilizator cu rol de Administrator al companiei, puteți verifica și modifica detaliile companiei și setările de licență:

1. Poziționați cursorul pe numele de utilizator din colțul din dreapta sus al consolei și selectați **Compania mea**.



Pagina Compania mea

2. La **Date companie**, completați cu informații despre companie, cum ar fi denumirea companiei, adresa și numărul de telefon.
3. Puteți modifica sigla afișată în Control Center, în rapoartele companiei și notificările prin e-mail astfel:
   - Faceți clic pe **Schimbare** pentru a selecta sigla din calculatorul dumneavoastră. Formatul fișierului de tip imagine trebuie să fie .png sau .jpg, iar dimensiunea imaginii trebuie să fie de 200x30 pixeli.
   - Faceți clic pe **Implicit** pentru a șterge imaginea și a reseta la imaginea furnizată de Bitdefender.
4. În mod implicit, compania dvs. poate fi gestionată de conturile de tip partener ale altor companii care ar putea avea compania dvs. afișată în propria consolă Bitdefender Control Center. Puteți bloca accesul acestor companii la rețeaua dvs. dezactivând opțiunea **Permiteți altor companii să administreze securitatea acestei companii**. Drept rezultat, rețeaua dvs. nu va mai fi vizibilă în consola Control Center a altor companii și acestea nu vor mai putea administra subscripția dvs.

5. La secțiunea **Licență**, puteți vizualiza și modifica detaliile licenței dumneavoastră.
   - Pentru a adăuga o cheie de licență nouă:
     a. Din meniul **Tip**, alegeți un tip de subscripție pentru **Licență**.
     b. Introduceți cheia în câmpul **Cheie de licență**.
     c. Faceți clic pe butonul **Verificare** și așteptați până când Control Center extrage informațiile despre cheia de licență introdusă.
   - Pentru a verifica detaliile cheii de licență, consultați informațiile afișate sub cheia de licență:
     – **Data expirării**: data până la care licența poate fi folosită licența.
     – **Utilizat**: numărul de utilizări folosite din numărul total de utilizări disponibile pe cheia de licență. O utilizare licențiată este folosită atunci când clientul Bitdefender a fost instalat pe o stație de lucru din rețeaua administrată de dumneavoastră.
     – **Disponibil pentru instalare**: numărul de utilizări libere din numărul total de utilizări aferente unei licențe lunare (excluzând utilizările folosite).
     – **Total**: numărul total de utilizări licențiate disponibile pentru subscripția dumneavoastră.
6. În secțiunea **Partener Bitdefender** puteți găsi informații despre compania care vă furnizează serviciile.

   Pentru a schimba furnizorul de servicii administrate:

   a. Faceți clic pe butonul **Modificare**.
   b. Introduceți în câmpul **ID partener** codul de companie al partenerului dvs.

   > **Notă**
   > Fiecare companie își poate găsi ID-ul în pagina **Compania mea**. Odată ce ați încheiat un acord cu o companie parteneră, reprezentantul acesteia trebuie să vă furnizeze ID-ul companiei respective din Control Center.

   c. Faceți clic pe **Salvare**.

   Drept rezultat, compania dvs. este mutată automat de la partenerul anterior la noul partener, în Control Center.
7. Opțional, vă puteți asocia compania cu contul dvs. MyBitdefender folosind câmpurile furnizate.
8. Faceți clic pe **Salvare** pentru a aplica modificările.

2.5. Schimbarea parolei de conectare

După ce contul dvs. a fost creat, veți primi un e-mail cu datele de autentificare.

- Modificați parola de autentificare implicită la prima accesare a Control Center.
- Modificați periodic parola dumneavoastră de autentificare.

Pentru a modifica parola de autentificare:

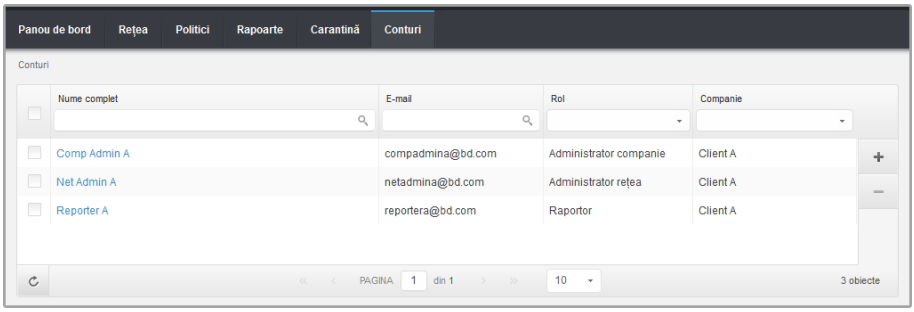
1. Îndreptați cursorul către numele de utilizatorul din colțul din dreapta sus al consolei și selectați **Contul meu**.
2. În **Detalii cont**, faceți clic pe **Modificare parolă**.
3. Introduceți parola actuală și noua parolă în câmpurile corespunzătoare.
4. Faceți clic pe **Salvare** pentru a aplica modificările.

3. Administrarea conturilor de utilizator

Serviciul Security for Endpoints poate fi configurat și administrat din Control Center folosind contul primit după abonarea la serviciul respectiv.

Ce trebuie să știți despre conturile de utilizator Small Office Security:

- Pentru a permite altor angajați ai companiei să acceseze Control Center, puteți crea conturi interne de utilizator. Puteți să atribuiți conturi de utilizator cu roluri diferite, în funcție de nivelul lor de acces în companie.
- Pentru fiecare cont de utilizator, puteți personaliza accesul la caracteristicile Small Office Security sau la anumite părți ale rețelei din care face parte.
- Toate conturile cu drept **Administrare utilizatori** pot crea, edita și șterge alte conturi de utilizator.
- Puteți administra doar conturile cu drepturi egale sau inferioare contului dumneavoastră.
- Puteți crea și gestiona conturile de utilizator pe pagina **Conturi**.



Pagina Conturi

Conturile existente sunt afișate în tabel. Pentru fiecare cont de utilizator, puteți vizualiza:

- Numele de utilizator al contului (utilizat pentru a vă conecta la Control Center).
- Adresa de e-mail a contului (folosită ca o adresă de contact). Rapoartele și notificările importante de securitate sunt expediate la această adresă. Notificările prin e-mail sunt expediate automat oricând sunt detectate situații de risc în rețea.
- Rolul utilizatorului (partener / administrator companie / administrator rețea / raportor / particularizat).

3.1. Roluri de utilizator

Rolul de utilizator constă într-o combinație specifică de drepturi de utilizator. La crearea unui cont de utilizator, puteți alege unul dintre rolurile predefinite sau puteți crea un rol personalizat, selectând doar anumite drepturi de utilizator.

Notă
Puteți atribui doar conturi de utilizator cu drepturi egale sau inferioare contului dumneavoastră.

Sunt disponibile următoarele roluri de utilizator:

1. **Administrator de companie** - Potrivit pentru administratorii companiilor care a achiziționat o licență Small Office Security de la un partener. Administratorul de companie gestionează licența, profilul companiei și întreaga instalare a Small Office Security, permițând controlul la cel mai ridicat nivel asupra tuturor setărilor de securitate (exceptând cazul în care este suprapus de contul de partener părinte în cadrul unui scenariu al furnizorului de servicii de securitate). Administratorii companiei pot partaja sau își pot delega responsabilitățile operaționale către administratorii subordonați și raportori.
2. **Administrator de rețea** - Pentru o companie, pot fi create mai multe conturi cu rol de Administrator de rețea, cu privilegii administrative asupra întregii instalări Security for Endpoints a companiei sau asupra unui anumit grup de calculatoare, inclusiv asupra administrării utilizatorilor. Administratorii de rețea sunt responsabili pentru gestionarea activă a setărilor de securitate ale rețelei.
3. **Raportor** - Conturile de raportor sunt conturi interne numai pentru consultare. Acestea permit accesul numai la rapoarte și jurnale. Astfel de conturi pot fi alocate personalului cu responsabilități de monitorizare sau altor angajați care trebuie să fie ținuți la curent cu starea de securitate.
4. **Particularizat** - Rolurile de utilizator predefinite includ o anumită combinație de drepturi de utilizator. În cazul în care un rol predefinit de utilizator nu este adecvat nevoilor dvs., puteți crea un cont personalizat prin selectarea drepturilor care vă interesează.

Tabelul de mai jos prezintă pe scurt relațiile dintre diferitele roluri de cont și drepturile lor. Pentru informații detaliate, consultați capitolul „Drepturile de utilizare” (p. 14).

Rol cont	Conturi subordonate permise	Drepturile de utilizare
Administrator companie	Administratori companie, Administratori rețea, Raportori	Administrare companie Administrare utilizatori Administrare rețele Administrare rapoarte
Administrator rețea	Administratori rețea, Raportori	Administrare utilizatori Administrare rețele

Rol cont	Conturi subordonate permise	Drepturile de utilizare
		Administrare rapoarte
Raportor	-	Administrare rapoarte

3.2. Drepturile de utilizare

Puteți atribui următoarele drepturi de utilizator conturilor de utilizator Small Office Security:

- **Administrare utilizatori**. Creați, modificați sau ștergeți conturi de utilizator.
- **Administrare companie**. Utilizatorii pot administra propria cheie de licență Small Office Security și pot modifica setările de profil ale companiei lor. Acest privilegiu este specific pentru conturile de administrator ale companiei.
- **Administrare rețele**. Oferă privilegii administrative asupra setărilor de securitate de rețea (inventar de rețea, politici, activități, pachete de instalare, carantină). Acest privilegiu este specific conturilor de administrator de rețea.
- **Administrare rapoarte**. Creați, modificați, ștergeți rapoarte și administrați panoul de bord.

3.3. Crearea de conturi de utilizator

Înainte de a crea un cont de utilizator, asigurați-vă că aveți la îndemână adresa de e-mail necesară. Adresa este obligatorie pentru crearea contului de utilizator Small Office Security. Utilizatorii vor primi datele de autentificare Small Office Security la adresa de e-mail furnizată. De asemenea, utilizatorii vor folosi adresa de e-mail pentru a se autentifica în Small Office Security.

Pentru a crea un cont de utilizator:

1. Mergeți la pagina **Conturi**.
2. Faceți clic pe butonul **+ Adăugare** din dreapta tabelului. Este afișată o fereastră de configurare.
3. La secțiunea **Detalii**, completați detaliile contului.
   - **Email**. Introduceți adresa de e-mail a utilizatorului. Informațiile de autentificare vor fi expediate către această adresă imediat după crearea contului.

     Notă
     Adresa de e-mail trebuie să fie unică. Nu puteți crea un alt cont de utilizator cu aceeași adresă e-mail.

   - **Nume complet**. Introduceți numele complet al titularului contului.
4. La secțiunea **Setări și privilegii**, configurați următoarele setări:

- **Fus orar**. Selectați din meniu fusul orar al contului. Consola va afișa informațiile referitoare la oră conform fusului orar selectat.
- **Limba**. Selectați din meniu limba de afișare a consolei.
- **Rol**. Selectați rolul utilizatorului. Pentru detalii cu privire la rolurile de utilizator, consultați „Roluri de utilizator” (p. 13).
- **Drepturi**. Fiecare rol de utilizator predefinit are o anumită configurație de drepturi. Cu toate acestea, puteți selecta doar drepturile de care aveți nevoie. În acest caz, rolul utilizatorului se modifică în **Personalizat**. Pentru detalii cu privire la drepturile de utilizator, consultați „Drepturile de utilizare” (p. 14).
- **Selectare ținte**. Derulați în jos în fereastra de configurare pentru a afișa secțiunea aferentă țintelor. Selectați grupurile de rețea la care va avea acces utilizatorul. Puteți restricționa accesul utilizatorilor la anumite zone din rețea.

5. Faceți clic pe **Salvare** pentru a adăuga utilizatorul. Noul cont va apărea în lista conturilor de utilizatori.

Notă
Parola pentru fiecare cont de utilizator este generată automat odată ce contul a fost creat și este trimisă la adresa de e-mail a utilizatorului împreună cu celelalte detalii de cont.
După crearea contului puteți schimba parola. Faceți clic pe numele contului în pagina **Conturi** pentru a modifica parola asociată acestuia. Odată ce parola a fost modificată, utilizatorul este notificat imediat prin e-mail.
Utilizatorii își pot schimba parola de autentificare din Control Center, accesând pagina **Contul meu**.

3.4. Conturi existente

Editați conturile pentru a păstra actualizate detaliile de cont sau pentru a modifica setările contului.

Pentru a edita un cont de utilizator:

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Faceți clic pe numele utilizatorului.
4. Modificați detaliile contului și setările după cum este necesar.
5. Faceți clic pe **Salvare** pentru a aplica modificările.

Notă
Toate conturile cu drept **Administrare utilizatori** pot crea, edita și șterge alte conturi de utilizator. Puteți administra doar conturile cu drepturi egale sau inferioare contului dumneavoastră.

3.5. Ştergerea conturilor

Ștergeți conturile, atunci când acestea nu mai sunt necesare. De exemplu, în cazul în care titularul de cont nu mai este angajat al companiei.

Pentru a șterge un cont:

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Selectați contul din listă.
4. Faceți clic pe butonul **– Ștergere** din dreapta tabelului.

3.6. Resetarea parolelor de conectare

Titularii conturilor care își uită parola o pot reseta folosind link-ul de recuperare a parolei de pe pagina de autentificare. De asemenea, puteți reseta o parolă de conectare uitată prin editarea contului corespunzător din consolă.

Pentru a reseta parola de conectare pentru un utilizator:

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Faceți clic pe numele utilizatorului.
4. Scrieți parola nouă în câmpurile corespunzătoare (în secțiunea **Detalii**).
5. Faceți clic pe **Salvare** pentru a aplica modificările. Titularul contului va primi un e-mail cu noua parolă.

4. Instalarea Security for Endpoints

Security for Endpoints este destinat calculatoarelor și laptopurilor care rulează cu sistemele de operare Windows și Mac OS X și cu serverele Windows. Pentru a proteja calculatoarele cu Security for Endpoints, trebuie să instalați Endpoint Security (software-ul client) pe fiecare dintre acestea. Endpoint Security administrează protecția pe calculatorul local. Comunică de asemenea cu Control Center pentru a primi comenzile administratorului și a expedia rezultatele acțiunilor sale.

Puteți instala Endpoint Security cu unul dintre următoarele roluri (disponibile în asistentul de instalare):

1. **Stație de lucru**, cand calculatorul corespunde unui unui terminal obișnuit din rețea.
2. **Endpoint Security Relay**, atunci când calculatorul respectiv este utilizat de către alte terminale din rețea pentru comunicarea cu Control Center. Rolul Endpoint Security Relay instalează Endpoint Security alături de un server de actualizări care poate fi utilizat pentru actualizarea tuturor celorlalți clienți din rețea. Terminalele din aceeași rețea pot fi configurate prin politică pentru comunicarea cu Control Center printr-unul sau mai multe calculatoare cu rol Endpoint Security Relay. Astfel, dacă nu este disponibil un rol Endpoint Security Relay, următorul este luat în considerare pentru asigurarea comunicării calculatorului cu Control Center.

Avertisment

- Primul calculator pe care instalați protecția trebuie să aibă rol de Endpoint Security Relay, altfel nu veți putea instala Endpoint Security pe celelalte calculatoare din rețea.
- Calculatorul cu rol de Endpoint Security Relay trebuie să fie pornit și online pentru ca sistemele client să comunice cu Control Center.

Puteți instala Endpoint Security pe calculatoare rulând pachetele de instalare local sau prin rularea sarcinilor de instalare de la distanță de pe Control Center.

Este foarte important să citiți cu atenție și să urmați instrucțiunile de pregătire a instalării.

Endpoint Security dispune de o interfață minimală pentru utilizator. Permite utilizatorilor doar să verifice starea de protecție și să ruleze sarcini de securitate de bază (actualizări și scanări), fără a oferi acces la setări.

Implicit, limba de afișare a interfeței pentru utilizator de pe calculatoarele protejate este setată la instalare în funcție de limba contului dumneavoastră.

Pentru a instala interfața pentru utilizator în altă limbă pe anumite calculatoare, puteți crea un pachet de instalare și seta limba preferată în opțiunile de configurare a pachetului. Pentru

mai multe informații cu privire la crearea pachetelor de instalare, consultați „Crearea pachetelor de instalare Endpoint Security” (p. 21).

4.1. Cerințe de sistem

4.1.1. Sisteme de operare suportate

În prezent, Security for Endpoints protejează următoarele sisteme de operare:

Sisteme de operare pentru stații de lucru:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista cu Service Pack 1
- Windows XP cu Service Pack 2 (64 biți)
- Windows XP cu Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Sisteme de operare embedded și pentru tablete:

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded cu Service Pack 2*
- Windows XP Tablet PC Edition*

*Anumite module ale sistemului de operare trebuie instalate pentru ca Security for Endpoints să funcționeze.

Sisteme de operare pentru servere:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 cu Service Pack 1

- Windows Home Server

4.1.2. Cerinţe hardware

- Procesor compatibil Intel® Pentium

  Sisteme de operare pentru staţii de lucru
  - 1 GHz sau superior pentru Microsoft Windows XP SP3, Windows XP SP2 64 biţi şi Windows 7 Enterprise (32 şi 64 biţi)
  - Viteze de 2 GHz sau mai mari pentru Microsoft Windows Vista SP1 sau mai recent (32 şi 64 biţi), Microsoft Windows 7 (32 şi 64 biţi), Microsoft Windows 7 SP1 (32 şi 64 biţi), Windows 8
  - 800 MHZ sau mai rapid pentru Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded cu Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Sisteme de operare pentru servere
  - Minim: 2.4 GHz single-core CPU
  - Se recomandă: CPU Intel Xeon multi-core cu viteze de 1,86 GHz sau mai mari
- **Memorie RAM disponibilă**:
  - Pentru Windows: minimum 512 MB, 1 GB recomandat
  - Pentru Mac: 1 GB minimum
- **Spaţiu HDD**:
  - 1.5 GB spaţiu liber pe hard-disk

Notă

Pentru entităţi cu rol Endpoint Security Relay este nevoie de un spaţiu disponibil pe disc de cel puţin 6 GB, întrucât acestea vor stoca toate actualizările şi pachetele de instalare.

4.1.3. Browsere compatibile

Securitatea pentru browser Endpoint este testată pentru compatibilitatea cu următoarele browsere:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

4.1.4. Porturile de comunicare Small Office Security

Tabelul de mai jos include informații cu privire la porturile folosite de componentele Small Office Security:

Port	Utilizare
80 (HTTP) / 443 (HTTPS)	Portul utilizat pentru accesarea consolei web Control Center.
80	Portul serverului de actualizare.
8443 (HTTPS)	Port utilizat de către software-ul client/agent pentru conectarea la Serverul de comunicații.
7074 (HTTP)	Comunicarea cu Endpoint Security Relay (dacă este disponibil)

Pentru informații detaliate privind porturile Small Office Security, consultați acest articol KB.

4.2. Pregătirea pentru instalare

Înainte de instalare, urmați pașii pregătitori de mai jos pentru a vă asigura că totul funcționează corect:

1. Asigurați-vă că toate calculatoarele îndeplinesc cerințele minime de sistem. Pentru unele calculatoare, se poate să fie necesară instalarea celui mai recent service pack disponibil sau eliberarea spațiului pe disc. Realizați o listă de calculatoare care nu îndeplinesc cerințele necesare, pentru a le putea exclude din administrare.
2. Dezinstalați (nu doar dezactivați) orice program antimalware, firewall sau software de securitate Internet existente pe calculatoare. Rularea simultană Endpoint Security cu alte software-uri de securitate pe un calculator le poate afecta funcționarea și cauza probleme majore în sistem.

   Multe dintre programele de securitate care sunt incompatibile cu Endpoint Security sunt detectate automat și șterse la instalare. Pentru a afla mai multe și a verifica lista software-urilor de securitate detectate, consultați acest articol KB.

   Important
   Nu este nevoie să vă îngrijorați pentru funcțiile de securitate Windows (Windows Defender, Windows Firewall), deoarece acestea vor fi oprite automat înainte de inițierea instalării.

3. Pentru instalare este necesară existența privilegiilor de administrare și a accesului la Internet. Asigurați-vă că aveți toate drepturile necesare la îndemână, pentru toate calculatoarele.
4. Calculatoarele trebuie să aibă conectivitate la Control Center.

4.3. Instalare locală

O modalitate în care puteți instala Endpoint Security pe un calculator este aceea de a rula local un pachet de instalare.

Puteți genera și administra pachetele de instalare, în funcție de necesități, de pe pagina **Rețea > Pachete**.

Meniu Rețea > Pachete

Avertisment

- Primul calculator pe care instalați protecția trebuie să aibă rol de Endpoint Security Relay, altfel nu veți putea instala Endpoint Security pe celelalte calculatoare din rețea.
- Calculatorul cu rol de Endpoint Security Relay trebuie să fie pornit și online pentru ca sistemele client să comunice cu Control Center.

Notă

După ce ați instalat primul client, acesta va fi utilizat pentru a detecta alte calculatoare din aceeași rețea, pe baza mecanismului de Descoperire rețea. Pentru informații detaliate referitoare la descoperirea rețelei, consultați „Cum funcționează opțiunea de descoperire a rețelei” (p. 30).

Pentru a instala local Endpoint Security pe un calculator, respectați următorii pași:

1. Creați un pachet de instalare conform necesităților dumneavoastră.

   Notă
   Pasul nu este obligatoriu dacă un pachet de instalare a fost deja creat pentru rețeaua de sub contul dumneavoastră.

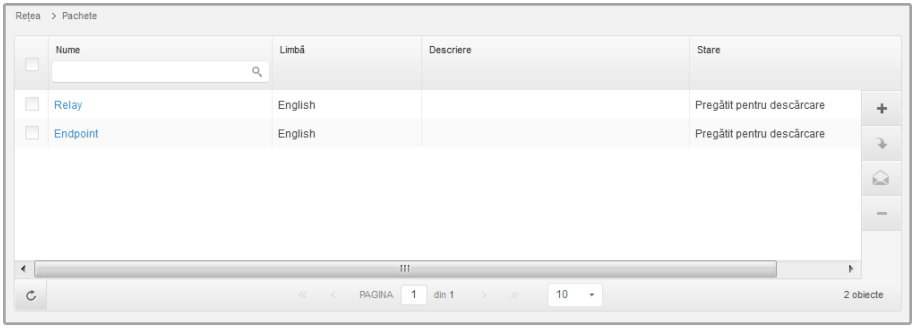
2. Descărcați pachetul de instalare pe calculator.
3. Rulați pachetul de instalare pe calculator.

4.3.1. Crearea pachetelor de instalare Endpoint Security

Pentru a crea un pachet de instalare Endpoint Security:

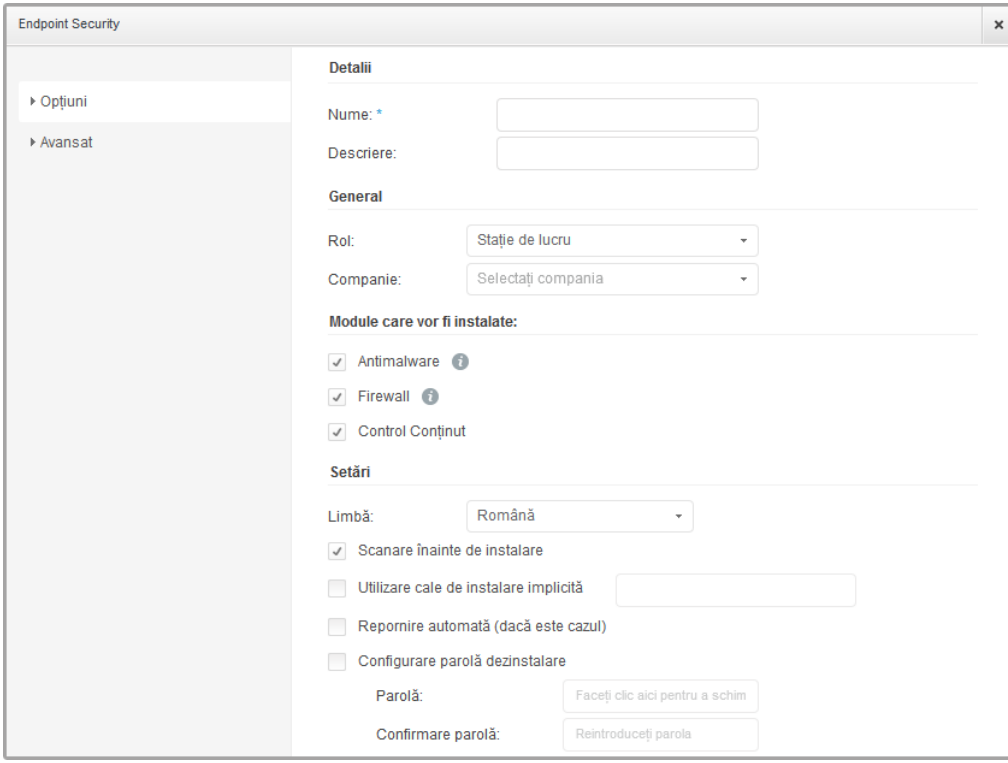
1. Conectați-vă și autentificați-vă la Control Center folosind propriul cont.

2. Mergeți la pagina **Rețea > Pachete**.



Pagina pachete

3. Faceți clic pe butonul + **Adăugare** din dreapta tabelului. Va apărea o fereastră de configurare.



Crearea pachetelor Endpoint Security - Opțiuni

4. Introduceți o denumire sugestivă și o descriere pentru pachetul de instalare pe care doriți să îl creați.
5. Selectați rolul calculatorului țintă:
   - **Stație de lucru**. Selectați această opțiune pentru a crea pachetul pentru un terminal obișnuit.
   - **Endpoint Security Relay**. Selectați această opțiune pentru a crea pachetul pentru un terminal cu rol Endpoint Security Relay. Endpoint Security Relay este un rol special care instalează un server de actualizări pe mașina țintă, alături de Endpoint Security, care poate fi utilizat pentru toți ceilalți clienți din rețea, diminuând gradul de utilizare a lățimii de bandă între mașinile client și Control Center.
6. Selectați compania unde se va utiliza pachetul de instalare.
7. Selectați modulele de protecție pe care doriți să le instalați.
8. Din câmpul **Limbă**, selectați limba dorită pentru interfața clientului.

9. Selectați **Scanare înainte de instalare** dacă doriți să vă asigurați că ați curățat calculatoarele, înainte de instalarea Endpoint Security pe acestea. Se va efectua o scanare rapidă prin cloud pe calculatoarele corespunzătoare, înainte de pornirea instalării.
10. Endpoint Security este instalat în directorul de configurare implicit pe calculatoarele selectate. Selectați **Utilizare cale de instalare implicită** dacă doriți să instalați Endpoint Security într-o altă locație. În acest caz, introduceți calea dorită în câmpul corespunzător. Folosiți convențiile Windows la introducerea căii (de exemplu, `D:\folder`). Dacă folderul specificat nu există, acesta va fi generat în timpul instalării.
11. Dacă doriți, puteți seta o parolă pentru a împiedica utilizatorii să șteargă protecția. Selectați **Configurare parolă dezinstalare** și introduceți parola dorită în câmpurile corespunzătoare.
12. Faceți clic pe **Înainte**.
13. În funcție de rolul pachetului de instalare (Endpoint sau Endpoint Security Relay), selectați entitatea la care se vor conecta periodic calculatoarele țintă, pentru actualizarea clientului:
    - **Bitdefender Cloud**, dacă doriți să actualizați clienții direct de pe internet.
    - **Endpoint Security Relay**, dacă doriți să conectați terminalele la un Endpoint Security Relay instalat în rețeaua dvs. Toate calculatoarele cu rolul de Endpoint Security Relay detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați Endpoint Security Relay dorit. Terminalele conectate vor comunica cu Control Center exclusiv prin Endpoint Security Relay specificat.

      Important
      Portul 7074 trebuie să fie deschis pentru ca instalarea prin Endpoint Security Relay să funcționeze.

14. Faceți clic pe **Salvare**.

Noul pachet de instalare va apărea în lista de pachete alte companiei țintă.

4.3.2. Descărcați pachetele de instalare

Pentru descărcarea pachetelor de instalare Endpoint Security:

1. Înregistrați-că în Control Center de pe calculatorul pe care doriți să instalați protecția.
2. Mergeți la pagina **Rețea > Pachete**.
3. Selectați pachetul de instalare Endpoint Security pe care doriți să îl descărcați.
4. Faceți clic pe butonul **Descărcare** din partea dreaptă a tabelului și selectați tipul de instalare pe care doriți să o utilizați. Există două tipuri de fișiere de instalare:
    - **Aplicație de descărcare**. Aplicația de descărcare descarcă mai întâi setul complet de instalare de pe serverele cloud ale Bitdefender și apoi demarează instalarea. Este de dimensiuni reduse și poate fi rulată atât pe sistemele de 32, cât și pe cele de 64

de biți (ceea ce ușurează distribuția). Dezavantajul este că necesită o conexiune activă la Internet.

- **Kit complet**. Setul complet va fi utilizat pentru a instala protecția pe calculatoare cu o conexiune slabă sau chiar inexistentă la internet. Descărcați acest fișier pe un calculator conectat la Internet și apoi distribuiți-l pe alte calculatoare folosind un mediu de stocare extern sau un director partajat în rețea.

Notă
Versiuni cu kit complet disponibile:

– **Windows OS:** sisteme pe 32 de biți și pe 64 de biți

– **Mac OS X:** numai sisteme pe de biți

Asigurați-vă că folosiți versiunea corectă pentru calculatorul pe care instalați.

5. Salvați fișierul în calculator.

4.3.3. Rularea pachetelor de instalare

Pentru ca instalarea să fie efectuată corect, pachetul trebuie să fie rulat folosind drepturile de administrator sau într-un cont de administrator.

1. Conectați-vă și autentificați-vă la Control Center.
2. Descărcați sau copiați fișierul de instalare în calculatorul țintă sau într-o formă partajată accesibilă în rețea, de pe calculatorul respectiv.
3. Rulați pachetul de instalare.
4. Urmați instrucțiunile de pe ecran.

După ce ați instalat Endpoint Security, calculatorul va apărea ca și administrat în Control Center (pagina **Rețea**), în câteva minute.

4.4. Instalare de la distanță

După ce ați efectuat instalarea locală pe primul client cu rol Endpoint Security Relay, este posibil să dureze câteva minute până când calculatoarele din rețea devin vizibile în Control Center. Din acest punct, puteți instala de la distanță Endpoint Security pe calculatoarele pe care le administrați folosind sarcinile de instalare din Control Center.

Endpoint Security include un mecanism automat de descoperire a rețelei care permite detectarea altor calculatoare din aceeași rețea. Calculatoarele detectate sunt afișate ca și **calculatoare neadministrate** din pagina **Rețea**.

Pentru informații detaliate referitoare la descoperirea rețelei, consultați „Cum funcționează opțiunea de descoperire a rețelei” (p. 30).

4.4.1. Cerinţe pentru instalarea Endpoint Security de la distanţă

Pentru ca instalarea de la distanță să funcționeze:

- Un Endpoint Security Relay trebuie să fie instalat în rețeaua dvs.
- Fiecare calculator țintă trebuie să aibă partajarea de administrare admin$ activată. Configurați fiecare stație de lucru țintă pentru utilizarea partajării avansate de fișiere (Advanced File Sharing).
- Dezactivați temporar User Account Control pe toate calculatoarele care rulează sisteme de operare Windows care includ această funcție de securitate (Windows Vista, Windows 7, Windows Server 2008 etc.). În cazul în care calculatoarele sunt într-un domeniu, puteți utiliza o politică de grup pentru a dezactiva User Account Control de la distanță.
- Dezactivați sau închideți firewall-ul de pe calculatoare. În cazul în care calculatoarele sunt într-un domeniu, puteți utiliza o politică de grup pentru a dezactiva firewall-ul Windows de la distanță.

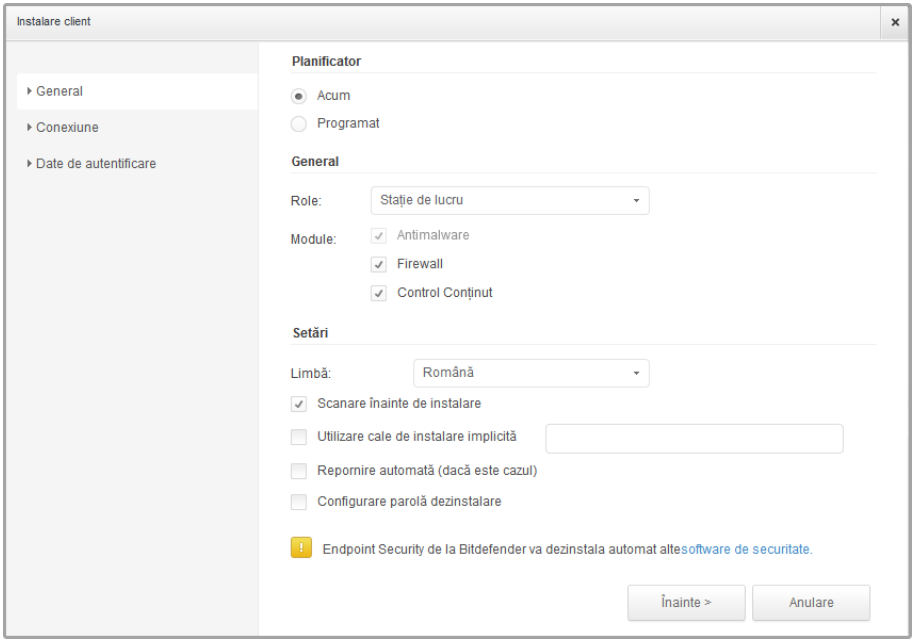
4.4.2. Rularea operaţiilor de instalare Endpoint Security de la distanţă

Pentru a rula o sarcină de instalare de la distanță:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați grupul dorit din rețea din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

Notă
Opțional, puteți aplica filtre pentru a afișa exclusiv calculatoarele neadministrate. Faceți clic pe butonul **Filtre** și selectați următoarele opțiuni: **Neadministrat** din categoria **Securitate** și **Toate obiectele recursiv** din categoria **Adâncime**.

4. Selectați entitățile (calculatoarele sau grupurile de calculatoare) pe care doriți să instalați protecția.
5. Faceți clic pe butonul **Sarcini** din partea dreaptă a tabelului și selectați **Instalare client**. Se afișează asistentul **Instalare client**.



Instalare Endpoint Security din meniul Sarcini

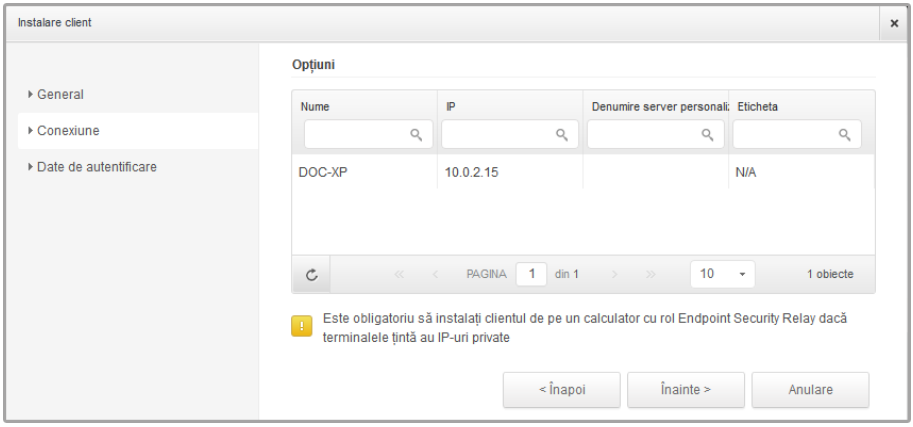
6. Configurați opțiunile de instalare:
   - Programați intervalul de instalare:
     - **Acum**, pentru a lansa instalarea imediat.
     - **Programat**, pentru a configura intervalul de recurență al instalării. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.

       Notă
       De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi dezinstalarea altor aplicații și repornirea sistemului de operare), puteți programa sarcina de instalare să ruleze la fiecare 2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes a instalării.

   - Selectați modulele de protecție pe care doriți să le instalați. Vă rugăm rețineți că pentru sistemele de operare pentru servere este disponibilă numai protecția împotriva malware.
   - Din câmpul **Limbă**, selectați limba dorită pentru interfața clientului.

- Selectați **Scanare înainte de instalare** dacă doriți să vă asigurați că ați curățat calculatoarele, înainte de instalarea Endpoint Security pe acestea. Se va efectua o scanare rapidă prin cloud pe calculatoarele corespunzătoare, înainte de pornirea instalării.
- Endpoint Security este instalat în directorul de configurare implicit pe calculatoarele selectate. Selectați **Utilizare cale de instalare implicită** dacă doriți să instalați Endpoint Security într-o altă locație. În acest caz, introduceți calea dorită în câmpul corespunzător. Folosiți convențiile Windows la introducerea căii (de exemplu, `D:\folder`). Dacă folderul specificat nu există, acesta va fi generat în timpul instalării.
- În timpul instalării silențioase, calculatorul este scanat pentru detectarea de malware. Uneori este necesară repornirea sistemului pentru a finaliza ștergerea malware-ului.

  Selectați **Restartare automată (dacă este necesară)** pentru a vă asigura că malware-ul detectat este șters complet înainte de instalare. Altfel, instalarea poate eșua.
- Dacă doriți, puteți seta o parolă pentru a împiedica utilizatorii să șteargă protecția. Selectați **Configurare parolă dezinstalare** și introduceți parola dorită în câmpurile corespunzătoare.
- Faceți clic pe **Înainte**.
- Fila **Conexiune** include lista terminalelor cu rol Endpoint Security Relay instalate în rețea. Fiecare client nou trebuie să fie conectat la cel puțin un Endpoint Security Relay din aceeași rețea, care va servi ca server de comunicații și actualizare. Selectați Endpoint Security Relay pe care doriți să îl asociați clienților noi.



7. Faceți clic pe **Înainte**.
8. În secțiunea **Administrare date de autentificare**, specificați drepturile de administrare necesare pentru autentificarea de la distanță pe terminalele selectate. Puteți adăuga

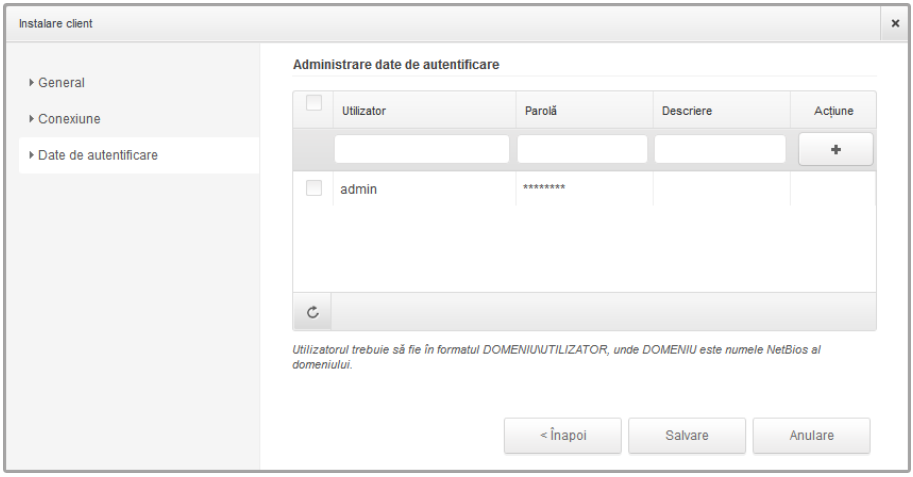
datele necesare introducând numele de utilizator și parola fiecărui sistem de operare țintă.

Important

Pentru stații de lucru cu sistem de operare Windows 8.1, este necesar să furnizați datele de autentificare ale contului de administrator încorporat sau ale unui cont de administrator de domeniu. Pentru mai multe informații, consultați acest articol KB.

Notă

Dacă nu ați selectat datele de autentificare, se va afișa un mesaj de avertizare. Acest pas este obligatoriu pentru instalarea de la distanță a Endpoint Security pe calculatoare.



Pentru a adăuga datele SO necesare:

a. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont. În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

   Folosiți convențiile Windows la introducerea numelui unui cont de utilizator de domeniu, de exemplu, `utilizator@domeniu.com` sau `domeniu\utilizator`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`utilizator@domeniu.com` și `domeniu\utilizator`).

   Notă

   Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

b. Faceți clic pe butonul + **Adăugare**. Contul este adăugat la lista de date de autentificare.

c. Selectați caseta corespunzătoare contului pe care doriți să îl folosiți.

9. Faceți clic pe **Salvare**. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

4.5. Cum funcționează opțiunea de descoperire a rețelei

Security for Endpoints include un mecanism de descoperire automată a rețelei proiectat pentru detectarea calculatoarelor din grupul de lucru.

Security for Endpoints se bazează pe **serviciul Microsoft Computer Browser** pentru descoperirea rețelei. Serviciul Computer Browser este o tehnologie de rețelistică utilizată de calculatoarele care rulează Windows pentru menținerea unei liste actualizate de domenii, grupuri de lucru și a calculatoarelor incluse în acestea și pentru furnizarea acestor liste către calculatoarele client, la cerere. Calculatoarele detectate în rețea de serviciul Computer Browser pot fi vizualizate prin rularea comenzii **net view** într-o fereastră de introducere a comenzii.

Comanda net view

Pentru a permite descoperirea rețelei, trebuie să aveți Endpoint Security instalat deja pe cel puțin un calculator din rețea. Acest calculator va fi utilizat pentru scanarea rețelei.

Important

Control Center nu utilizează informații de rețea din Active Directory sau din funcția de hartă rețea disponibilă în Windows Vista și versiunile mai recente. Harta rețelei se bazează pe o altă tehnologie de descoperire a rețelei: protocolul Link Layer Topology Discovery (LLTD).

Control Center nu este implicată activ în operațiunea serviciului Computer Browser. Endpoint Security interoghează serviciul Computer Browser numai pentru identificarea listelor de stații de lucru și servere vizibile în rețea (cunoscute ca și lista de navigare) și apoi o transmite către Control Center. Control Center procesează lista de parcurgere și include noile calculatoare detectate în lista **Calculatoare neadministrate**. Calculatoarele detectate anterior

nu sunt șterse după o nouă interogare de descoperire a rețelei; prin urmare, trebuie să excludeți și să ștergeți manual & calculatoarele care nu mai sunt în rețea.

Interogarea inițială aferentă listei de parcurgere este efectuată de primul Endpoint Security instalat în rețea.

- Dacă Endpoint Security este instalat pe un calculator aparținând unui grup de lucru, numai calculatoarele din acest grup vor fi vizibile în Control Center.
- Dacă Endpoint Security este instalat pe un calculator de domeniu, numai calculatoarele din domeniul respectiv vor fi vizibile în Control Center. Calculatoarele din alte domenii pot fi detectate dacă există o relație de încredere cu domeniul pe care este instalat Endpoint Security.

Interogările ulterioare pentru descoperirea rețelei sunt efectuate regulat, în fiecare oră. Pentru fiecare nouă interogare, Control Center împarte spațiul calculatoarelor administrate în zonele de vizibilitate și apoi identifică un Endpoint Security în fiecare zonă, pentru executarea sarcinii. O zonă de vizibilitate este un grup de calculatoare care se detectează reciproc. În general, o zonă de vizibilitate este definită de un grup de lucru sau domeniu, însă aceasta depinde de topologia și configurația rețelei. În anumite cazuri, o zonă de vizibilitate poate include mai multe domenii și grupuri de lucru.

Dacă un Endpoint Security selectat nu efectuează interogarea, Control Center așteaptă până la următoarea interogare programată, fără a alege un alt Endpoint Security pentru a relua încercarea.

Pentru vizibilitate completă a rețelei, Endpoint Security trebuie instalat pe cel puțin un calculator din fiecare grup de lucru sau domeniu din rețeaua dumneavoastră. Ideal, Endpoint Security trebuie instalat pe cel puțin un calculator din fiecare sub-rețea.

4.5.1. Mai multe despre serviciul Microsoft Computer Browser

Pe scurt despre serviciul Computer Browser:

- Operează independent de Active Directory.
- Rulează exclusiv pe rețelele IPv4 și operează independent în limitele unui grup LAN (grup de lucru sau domeniu). O listă de parcurgere este realizată și menținută pentru fiecare grup LAN.
- În mod tipic, utilizează pentru comunicarea între noduri transmisiile prin servere și nevalidate.
- Utilizează NetBIOS prin TCP/IP (NetBT).
- Necesită o rezoluție de nume NetBIOS. Se recomandă existența unei infrastructuri Windows Internet Name Service (WINS) care să ruleze în rețea.
- Nu este activată implicit pe Windows Server 2008 și 2008 R2.

Pentru informații detaliate privind serviciul Computer Browser, accesați Computer Browser Service Technical Reference de pe Microsoft Technet.

4.5.2. Cerinţe pentru aplicaţia de descoperire a reţelei

Pentru descoperirea cu succes a tuturor calculatoarelor (servere și stații de lucru) care vor fi administrate de pe Control Center, sunt necesare următoarele:

- Calculatoarele trebuie să fie asociate într-un grup de lucru sau domeniu și conectate printr-o rețea locală IPv4. Serviciul Computer Browser nu funcționează pe rețelele IPv6.
- Mai multe calculatoare din fiecare grup LAN (grup de lucru sau domeniu) rebuie să ruleze serviciul Computer Browser. Controlerele principale ale domeniului trebuie să ruleze de asemenea serviciul.
- NetBIOS prin TCP/IP (NetBT) trebuie să fie activată pe calculatoare. Firewall-ul local trebuie să permită traficul NetBT.
- Partajarea fișierelor trebuie să fie activată pe toate calculatoarele. Firewall-ul local trebuie să permită partajarea fișierelor.
- O infrastructură Windows Internet Name Service (WINS) trebuie să fie configurată și să funcționeze corespunzător.
- Pentru Windows Vista și versiuni ulterioare, trebuie activată funcția de descoperire a rețelei (**Control Panel > Network and Sharing Center > Change Advanced Sharing Settings**).

  Pentru a putea activa această funcție, trebuie inițiate următoarele servicii:
  - DNS Client
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- În medii cu mai multe domenii, se recomandă configurarea unor relații de încredere între domenii, pentru a permite calculatoarelor să acceseze listele de parcurgere din alte domenii.

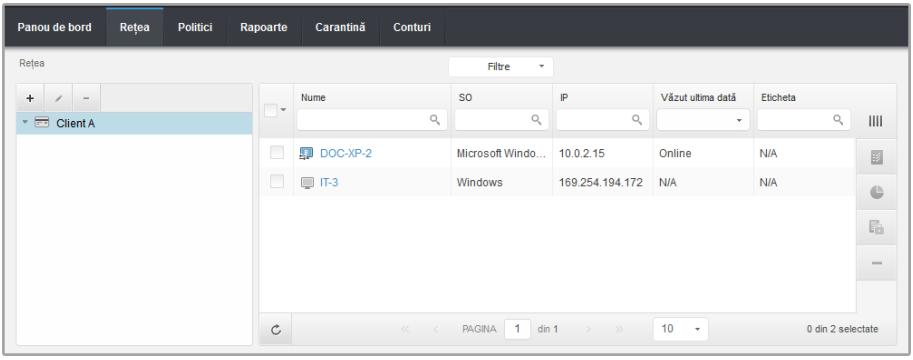
Calculatoarele de pe care Endpoint Security interoghează serviciul Computer Browser trebuie să poată identifica numele NetBIOS.

Notă

Mecanismul de descoperire a rețelei funcționează pentru toate sistemele de operare acceptate, inclusiv versiunile de Windows Embedded, cu condiția să fie îndeplinite cerințele.

5. Administrarea calculatoarelor

Pagina **Rețea** oferă mai multe caracteristici pentru explorarea și administrarea calculatoarelor disponibile. Modul de vizualizare **Rețea** constă într-o interfață alcătuită din două panouri ce afișează starea în timp real a tuturor obiectelor din rețea:



Pagina Rețea

1. În fereastra din stânga se afișează structura arborelui de rețea disponibilă.

   Notă
   Puteți vizualiza și gestiona numai grupurile pentru care dețineți drepturi de administrator.

2. În fereastra din dreapta se afișează conținutul grupului pe care i-ați selectat din arborele de rețea. Această fereastră include o grilă, în care rândurile includ obiecte de rețea și coloanele afișează informații specifice pentru fiecare tip de obiect.

   Din această fereastră, puteți face următoarele:

   - Vizualizați informațiile detaliate referitoare la fiecare obiect din rețea din contul dumneavoastră. Puteți vizualiza starea fiecărui obiect verificând pictograma de lângă denumirea corespunzătoare. Faceți clic pe denumirea obiectului pentru afișarea unei ferestre care include detalii specifice.
   - Folosiți Bara de instrumente pentru acțiune din partea dreaptă a tabelului pentru efectuarea unor operațiuni specifice pentru fiecare obiect din rețea (cum ar fi rularea sarcinilor, crearea rapoartelor, alocarea politicilor și ștergere).
   - Reîmprospătați datele tabelare.

Din secțiunea **Rețea**, puteți administra, de asemenea, pachetele de instalare și lista de sarcini pentru fiecare tip de obiect din rețea.

Pentru a vizualiza calculatoarele din contul dumneavoastră, mergeți în pagina **Rețea** și selectați grupul de rețea dorit din partea stângă a paginii.

Puteți vizualiza rețeaua de calculatoare disponibilă din fereastra din stânga, precum și detaliile referitoare la fiecare calculator, în fereastra din dreapta.

Pentru a personaliza detaliile calculatorului afișate în tabel:

1. Faceți clic pe butonul **Coloane** din partea dreaptă a capului de tabel.
2. Selectați denumirile coloanelor pe care doriți să le vizualizați.
3. Faceți clic pe butonul **Resetare** pentru a reveni la vizualizare implicită coloane.

Din secțiunea **Rețea**, puteți administra calculatoarele după cum urmează:

- Verificați starea calculatorului.
- Organizați calculatoarele în grupuri.
- Vizualizați detaliile calculatorului.
- Sortați, filtrați și căutați calculatoare.
- Rulați sarcinile pe calculatoare.
- Creați rapoarte rapide.
- Atribuiți politici.
- Ștergeți calculatoarele din inventarul rețelei.

5.1. Verificaţi starea calculatorului

Fiecare calculator este reprezentat în pagina de rețea prin intermediul unei pictograme specifice stării calculatorului. Vizualizați starea calculatoarelor și pictogramele corespunzătoare în tabelul de mai jos:

Pictogramă	Stare
	Calculator, Administrat, Nu există probleme, Online
	Calculator, Administrat, Cu probleme de securitate, Online,
	Calculator, Administrat, Nu există probleme, Offline
	Calculator, Administrat, Cu probleme de securitate, Offline
	Neadministrat(e)
	Șters

Pentru informații detaliate, consultați:

- „Calculatoare administrate, neadministrate, șterse” (p. 35)
- „Calculatoare online și offline” (p. 35)

- „Calculatoare cu probleme de securitate” (p. 36)

5.1.1. Calculatoare administrate, neadministrate, şterse

Calculatoarele pot avea diferite stări de administrare:

- **Administrat** - calculatoare pe care este instalată protecția Endpoint Security.
- **Neadministrat** - calculatoare detectate pe care nu s-a instalat încă protecția Endpoint Security.
- **Șters** - calculatoarele pe care le-ați șters din Control Center. Pentru mai multe informații, consultați capitolul „Ștergerea calculatoarelor din inventarul rețelei” (p. 59).

5.1.2. Calculatoare online şi offline

Starea de conectivitate se referă exclusiv la calculatoarele administrate. Din acest punct de vedere, calculatoarele administrate pot fi:

- **Online**. O pictogramă albastră indică faptul că un calculator este online.
- **Neconectat (offline)**. O pictogramă gri indică faptul că un calculator este offline.

Un calculator este considerat offline dacă Endpoint Security este inactiv mai mult de 5 minute. Posibile motive pentru care calculatoarele apar ca fiind offline:

- Calculatorul este oprit, în stare de așteptare sau de hibernare.

  Notă
  În mod normal, calculatoarele apar online chiar dacă sunt blocate sau utilizatorul este deconectat.

- Endpoint Security nu are conectivitate cu Bitdefender Control Center sau cu Endpoint Security Relay atribuit:
  - Calculatorul poate fi deconectat de la rețea.
  - Un firewall de rețea sau router poate obstrucționa comunicarea dintre Endpoint Security și Bitdefender Control Center sau Endpoint Security Relay atribuit.
- Endpoint Security a fost instalat manual de pe calculator, în timp calculatorul nu avea conectivitate la Bitdefender Control Center sauEndpoint Security Relay atribuit. În mod normal, atunci când Endpoint Security este dezinstalat manual de pe un calculator, Control Center este notificat cu privire la acest eveniment, iar calculatorul este marcat ca fiind neadministrat.
- Este posibil ca Endpoint Security să nu funcționeze corect.

Pentru a afla cât timp au fost inactive calculatoarele:

1. Se afișează doar calculatoarele administrate. Faceți clic pe meniul **Filtre** de deasupra tabelului, selectați **Administrate (Terminale)** și **Administrate (Endpoint Security Relay)** din categoria **Securitate** și faceți clic pe **Salvare**.
2. Faceți clic pe titlul coloanei **Văzut ultima dată** pentru sortarea calculatoarelor în funcție de perioada de inactivitate.

Puteți ignora perioadele de inactivitate mai scurte (minute, ore), deoarece este posibil ca acestea să fie rezultatul unei stări temporare. De exemplu, calculatorul este în prezent oprit.

Perioadele de inactivitate mai lungi (zile, săptămâni) indică, în general, o problemă cu calculatorul.

5.1.3. Calculatoare cu probleme de securitate

Starea de securitate se referă exclusiv la calculatoarele administrate. Verificați pictograma de stare care afișează un simbol de avertizare pentru a identifica calculatoarele cu probleme de securitate:

- Calculator administrat, probleme existente, online.
- Calculator administrat, probleme existente, offline.

Un calculator are probleme de securitate dacă se aplică cel puțin una dintre situațiile de mai jos:

- Protecția contra malware este dezactivată.
- Licența Endpoint Security a expirat.
- Endpoint Security a expirat.
- Semnăturile nu sunt la zi.
- S-a detectat malware.

Dacă identificați un calculator cu probleme de securitate, faceți clic pe denumire pentru afișarea paginii **Detalii calculator**. Puteți identifica aspectele de securitate printr-o pictogramă . Verificați informațiile oferite de pictogramă pentru detalii suplimentare. Este posibil să fie necesare investigații locale suplimentare.

5.2. Organizarea calculatoarelor în grupuri

Puteți gestiona grupurile de calculatoare din fereastra din partea stângă a paginii **Rețea**, în grupurile **Rețea**.

Beneficiul major este acela că puteți utiliza politicile de grup pentru a îndeplini diferite cerințe de securitate.

În grupul de **Rețea** aparținând companiei dumneavoastră puteți crea, șterge, redenumi și muta grupuri de calculatoare într-o structură de tip arbore predefinită.

Important
Vă rugăm să rețineți următoarele:

- Un grup poate include atât calculatoare, cât și alte grupuri.
- Dacă selectați un grup din fereastra din stânga, puteți vizualiza toate calculatoarele, cu excepția celor din sub-grupuri. Pentru a vizualiza toate calculatoarele din grup și din sub-grupurile acestuia, faceți clic pe meniul **Filtre** din partea de sus a tabelului și selectați **Toate obiectele recursiv** din secțiunea **Adâncime**.

Crearea unui nou grup

Înainte de a începe să creați grupuri, gândiți-vă la motivele pentru care aveți nevoie de ele și creați o schemă de grupare. De exemplu, puteți grupa calculatoarele pe baza unuia sau mai multora dintre următoarele criterii:

- Structura organizatorică (Vânzări, Marketing, Asigurarea calității, Dezvoltare software, Management etc.).
- Necesitățile de securitate (desktopuri, laptopuri, servere etc.).
- Locația (sediu central, birouri locale, personal la distanță, birouri de acasă etc.).

Pentru a organiza rețeaua în grupuri:

1. Selectați grupul **Rețea** din fereastra din stânga.
2. Faceți clic pe butonul **Adăugare grup** din partea de sus a ferestrei din stânga.
3. Introduceți o denumire sugestivă pentru grup și faceți clic pe **OK**.

Redenumirea unui grup

Pentru a redenumi un grup:

1. Selectați grupul din fereastra din stânga.
2. Faceți clic pe butonul **Editare grup** din partea de sus a ferestrei din stânga.
3. Introduceți noua denumire în câmpul corespunzător.
4. Faceți clic pe **OK** pentru confirmare.

Mutarea grupurilor şi calculatoarelor

Puteți muta grupurile și utilizatorii oriunde în ierarhia grupului **Rețea**. Pentru a muta un grup sau un utilizator, trageți-l și inserați-l din locația curentă în cea nouă.

Notă

Entitatea mutată va moșteni setările de politică ale noului grup părinte, cu excepția cazului în care i s-a atribuit o politică diferită. Pentru detalii privind preluarea politicii, consultați „Alocarea politicilor unor obiecte din rețea” (p. 72).

Ştergerea unui grup

Un grup nu poate fi șters dacă include cel puțin un calculator. Mutați toate calculatoarele din grup pe care doriți să le ștergeți într-un alt grup. Dacă grupul include sub-grupuri, puteți opta pentru mutarea tuturor sub-grupurilor mai degrabă decât a calculatoarelor individuale.

Pentru a șterge un grup:

1. Selectați grupul gol din partea dreaptă a **paginii Rețea**.
2. Faceți clic pe butonul **Ștergere grup** din partea de sus a ferestrei stânga. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

5.3. Vizualizarea detaliilor calculatorului

Puteți obține informații detaliate cu privire la fiecare calculator din pagina **Rețea**, inclusiv sistemul de operare, IP-ul, data și ora ultimei accesări etc.

Pentru a afla detalii despre un calculator:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din rețea din fereastra din stânga.

   Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Puteți detecta cu ușurință starea calculatorului, verificând pictograma corespunzătoare. Pentru informații detaliate, consultați capitolul „Verificați starea calculatorului” (p. 34).
4. Verificați informațiile afișate în coloane pentru fiecare calculator:
   - **Nume**: denumirea calculatorului.
   - **FQDN**: nume de domeniu calificat complet care include denumirea gazdei și numele de domeniu.
   - **SO**: sistemul de operare instalat pe calculator.
   - **IP**: adresa IP a calculatorului.
   - **Văzut ultima dată**: detalii privind starea de conectivitate a calculatorului.

     Notă

     Este important să monitorizați câmpul **Văzut ultima dată** deoarece intervalele lungi de inactivitate pot indica o problemă de comunicare sau un calculator deconectat.

   - **Eticheta**: eticheta adăugată calculatorului în fereastra **Detalii calculator**.

5. Faceți clic pe denumirea calculatorului administrat dorit. Se afișează fereastra **Detalii calculator**.

   - Mergeți la fila **Descriere generală** pentru următoarele detalii:

     – Informații generale referitoare la calculator, adresa IP, sistemul de operare, grupul mamă și starea curentă. De asemenea, puteți atribui calculatorului o etichetă. Prin urmare, puteți căuta și filtra calculatoarele după etichetă, prin intermediul câmpului de căutare al coloanei **Eticheta** din tabelul din partea dreaptă a paginii **Rețea**.

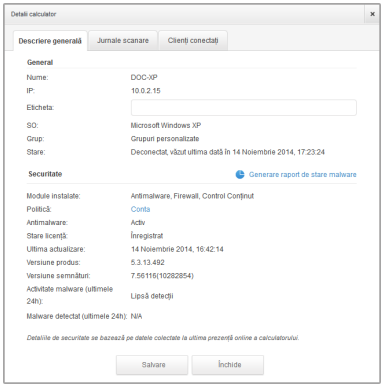
     – Detaliile de securitate referitoare la Endpoint Security instalat pe calculator, cum ar fi modulele instalate, politica atribuită, starea antimalware, starea licenței, ultima actualizare, produsul și versiunile de semnătură, precum și malware-ul detectat în ultimele 24 de ore. De asemenea, puteți obține o prezentare rapidă a numărului de programe malware detectate pe calculator în ziua curentă.

     – Faceți clic pe **Generare raport stare malware** pentru a accesa opțiunile referitoare la raportarea de malware pentru calculatorul selectat.

     Pentru mai multe informații, consultați capitolul „Crearea rapoartelor” (p. 124)

     Notă

     Fiecare proprietate care generează probleme de securitate este marcată prin pictograma . Verificați informațiile oferite de pictogramă pentru detalii suplimentare. Este posibil să fie necesare investigații locale suplimentare.



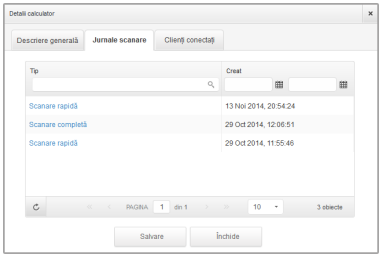
Detalii calculator - Prezentare generală

   – Secțiunea **Endpoint Security Relay** (disponibilă pentru clienții regulați ai terminalelor) afișează informații referitoare la Endpoint Security Relay la care este conectat calculatorul curent.

- Faceți clic pe fila **Jurnale de scanare** pentru a vizualiza informații detaliate referitoare la toate scanările efectuate pe calculator. Faceți clic pe raportul de scanare care vă interesează pentru a-l deschide într-o nouă pagină de browser.

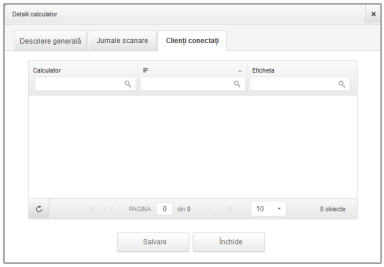
  Pentru a trece de la o pagină la alta, folosiți opțiunile de navigație din partea de jos a tabelului. Dacă există prea multe intrări, puteți folosi opțiunile de filtrare disponibile în partea de sus a tabelului.

  Faceți clic pe butonul **Reîmprospătare** din colțul din stânga jos al tabelului pentru a actualiza lista jurnalelor de scanări.



Detalii calculator - Jurnale de scanare

- Pentru calculatoarele cu rol de Endpoint Security Relay, este disponibilă și fila **Clienți conectați**, în car eputeți vedea o listă a terminalelor conectate.



Detalii calculator - Clienți conectați

5.4. Sortarea, filtrarea şi căutarea calculatoarelor

În funcție de numărul de calculatoare, tabelul cu calculatoare notificări se poate întinde pe mai multe pagini (implicit, sunt afișate doar 10 intrări pe pagină). Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă există prea multe intrări, puteți folosi casetele de căutare de sub titlurile coloanelor sau meniul **Filtre** din partea de sus a tabelului, pentru a filtra datele afișate. De exemplu, puteți modifica o căutarea unui anumit calculator sau selecta să vizualizați numai calculatoarele administrate.

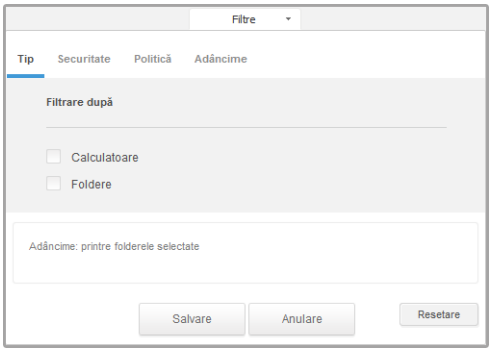
5.4.1. Sortarea calculatoarelor

Pentru a sorta datele după o anumită coloană, faceți clic pe titlurile coloanelor. De exemplu, dacă doriți să ordonați calculatoarele după nume, faceți clic pe titlul **Nume**. Dacă faceți din nou clic pe numele de coloană, calculatoarele vor fi afișate în ordine inversă.

Sortarea calculatoarelor

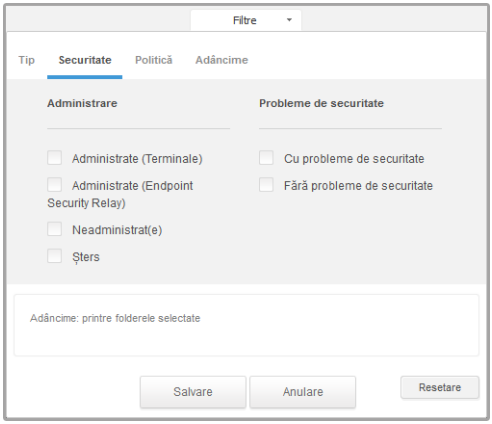
5.4.2. Filtrarea calculatoarelor

1. Selectați grupul dorit din fereastra din stânga.
2. Faceți clic pe meniul **Filtre** situat deasupra tabelului.
3. Selectați criteriile de filtrare după cum urmează:
   - **Tip**. Selectați tipul de entități care doriți să fie afișate (calculatoare, foldere sau ambele).



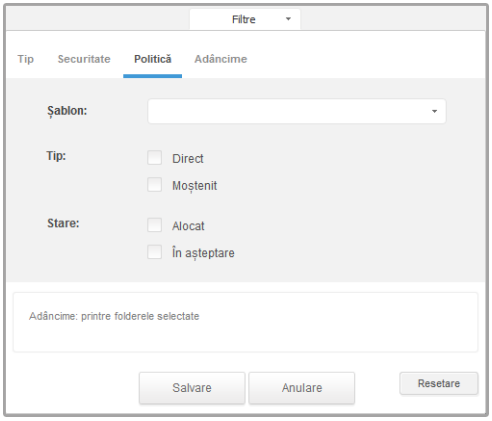
Calculatoare - Filtrare după tip

   - **Securitate**. Alegeți afișarea calculatoarelor după starea de administrare și securitate.



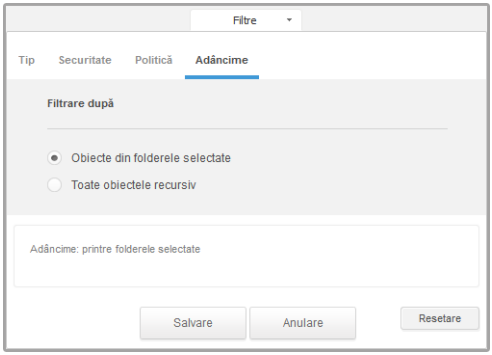
Calculatoare - Filtrare după securitate

- **Politică**. Selectați modelul de politică dorit pentru filtrarea calculatoarelor după tipul de atribuire a politicii (Directă sau Moștenită), precum și starea de atribuire a politicii (Atribuită sau În așteptare).



Calculatoare - Filtrare după politică

- **Adâncime**. Când administrați o rețea de calculatoare de tip arbore, calculatoarele din sub-grupuri nu sunt afișate la selectarea grupului rădăcină. Selectați opțiunea **toate obiectele recursiv** pentru a vedea toate calculatoarele din grupul curent și din sub-grupuri.



Calculatoare - Filtrare după adâncime

Notă
Puteți vizualiza toate criteriile de filtrare selectate din partea de jos a ferestrei **Filtre**. Dacă doriți să eliminați toate filtrele, faceți clic pe butonul **Resetare**.

4. Faceți clic pe **Salvare** pentru a filtra calculatoarele după criteriile selectate. Filtrul rămâne activ în pagina **Rețea** până când vă deconectați sau resetați filtrul.

5.4.3. Căutarea unui calculator

1. Selectați grupul dorit din fereastra din stânga.
2. Introduceți termenul de căutare în caseta corespunzătoare de sub titlurile coloanelor (Nume, SO sau IP) din fereastra din dreapta. De exemplu, introduceți IP-ul calculatorului pe care îl căutați în câmpul **IP**. În tabel se va afișa doar calculatorul care corespunde criteriilor de căutare.

   Ștergeți informațiile din caseta de căutare pentru afișarea unei liste a tuturor calculatoarelor.

Căutare calculatoare

5.5. Rularea sarcinilor pe calculatoare

De pe pagina **Rețea**, puteți rula de la distanță o serie de sarcini administrative pe calculatoare.

Iată ce puteți face:

- „Scanare” (p. 44)
- „Instalare client” (p. 51)
- „Modificare aplicație de instalare” (p. 54)
- „Dezinstalare client” (p. 55)
- „Actualizare” (p. 56)
- „Repornire calculator” (p. 56)
- „Descoperire rețea” (p. 57)

Puteți opta pentru generarea unor sarcini individual pentru fiecare calculator sau pentru grupuri de calculatoare. De exemplu, puteți instala de la distanță Endpoint Security pe un grup de calculatoare neadministrate. Ulterior, puteți crea o sarcină de scanare pentru un anumit calculator din același grup.

Pentru fiecare calculator puteți rula doar sarcini compatibile. De exemplu, dacă selectați un calculator neadministrat, nu puteți selecta decât **Instalare client**, toate celelalte sarcini fiind dezactivate.

Pentru un grup, sarcina selectată va fi creată exclusiv pentru calculatoarele compatibile. Dacă niciunul dintre calculatoarele din grup nu este compatibil cu sarcina selectată, veți fi informat că sarcina nu a putut fi generată.

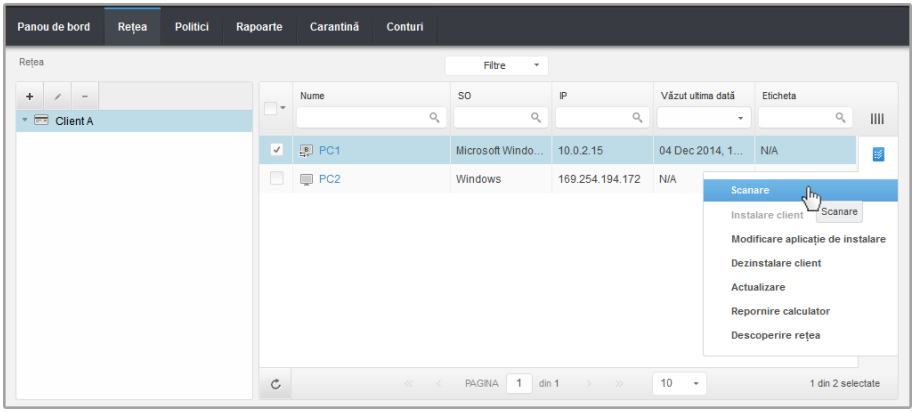
După ce a fost creată, sarcina va începe să ruleze imediat pe caculatoarele online. Dacă un calculator este offline, sarcina va rula imediat după ce calculatorul este din nou online.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.5.1. Scanare

Pentru a rula de la distanță o sarcină de scanare pe unul sau pe mai multe calculatoare:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați căsuțele corespunzătoare calculatoarelor pe care doriți să le scanați.
4. Faceți clic pe butonul **Sarcini** din dreapta tabelului și selectați **Scanare**.

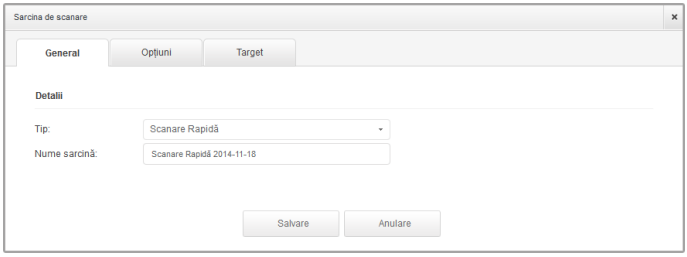


Sarcină de scanare calculatoare

Va apărea o fereastră de configurare.

5. Configurați opțiunile de scanare:

   - În secțiunea **General**, puteți selecta tipul de scanare și puteți introduce o denumire pentru sarcina de scanare. Scopul denumirii scanării este acela de a vă ajuta să identificați cu ușurință scanarea curentă pe pagina **Sarcini**.



Sarcină de scanare calculatoare - Configurarea setărilor generale

Selectați tipul unei scanări din meniul **Tip**:

– **Scanare rapidă** utilizează scanarea în cloud pentru a detecta malware-ul care rulează pe sistem. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Notă

Scanarea rapidă detectează doar malware-ul existent, fără a lua niciun fel de măsuri. Dacă în timpul unei operațiuni de Scanare rapidă este identificat malware, trebuie să rulați o sarcină de Scanare completă pentru ștergerea acestora.

– **Scanare completă** verifică întregul calculator pentru identificarea tuturor tipurilor de malware care îi amenință siguranța, cum ar fi virușii, aplicațiile spion, adware, rootkit-uri și altele.

– **Scanare personalizată** vă permite să selectați locațiile pe care doriți să le scanați și să configurați opțiunile de scanare. Pentru a defini o scanare personalizată:

  • Mergeți la secțiunea **Opțiuni** pentru a seta opțiunile de scanare. Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Folosiți descrierea din partea dreaptă a scalei, pentru a vă ghida alegerea.

    În funcție de profilul selectat, opțiunile de scanare din secțiunea **Setări** sunt configurate automat. Cu toate acestea, dacă doriți, le puteți configura detaliat. În acest scop, selectați caseta de bifare **Personalizat** și mergeți la secțiunea **Setări**.

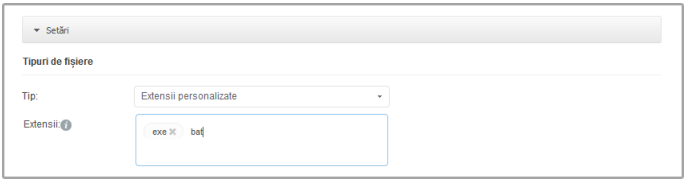
Sarcină de scanare calculatoare

Sunt disponibile următoarele opțiuni:

– **Tipuri de fișiere.** Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți seta Endpoint Security să scaneze toate fișierele (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

> **Notă**
>
> Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Lista de tipuri de fișiere de aplicații ” (p. 149).

Dacă doriți să scanați doar fișiere cu anumite extensii, selectați **Extensii definite de utilizator** din meniu și introduceți extensiile în câmpul de editare, apăsând `Enter` după fiecare.



Opțiuni sarcină de scanare calculatoare - Adăugarea extensiilor definite de utilizator

– **Arhive.** Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoase pot afecta sistemul numai dacă fișierul infestat este extras din arhivă și executat fără ca protecția în timp real să fie activată. Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

> **Notă**
> Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

  - **Scanare în arhive.** Selectați această opțiune dacă doriți să scanați fișierele arhivate, pentru identificarea de malware. Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:
    – **Limitare dimensiune arhivă la (MB).** Puteți seta o dimensiune limită acceptată pentru arhivele care vor fi scanate. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).
    – **Adâncime maximă arhivă (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.
  - **Scanare arhive de e-mail.** Selectați această opțiune dacă doriți să activați scanarea fișierelor atașate la mesajele e-mail și bazele de date e-mail, inclusiv format de fișiere de tipul .eml, .msg, .pst, .dbx, .mbx, .tbb și altele.

> **Notă**
> Scanarea arhivei e-mail necesită numeroase resurse și poate afecta performanțele sistemului.

– **Diverse.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.

- **Scanare sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
- **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
- **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.
- **Scanare după keyloggers.** Selectați această opțiune pentru a scana software-urile de tip keylogger.
- **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului.
- **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe calculator.
- **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Scanare pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.

– **Acțiuni.** În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

  - **La detectarea unui fișier infectat.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date a Bitdefender. În mod normal, Endpoint Security poate șterge codul malware din fișierul infestat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

În cazul în care este detectat un fișier infectat, Endpoint Security va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Important
Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

- **La detectarea unui fișier suspect.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice. Deoarece B-HAVE este o tehnologie euristică de analiză, Endpoint Security nu vă poate asigura dacă fișierul este într-adevăr virusat sau nu. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

  Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină. Fișierele sub carantină sunt transmise regulat spre analiză la Laboratoarele Bitdefender. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

- **La detectarea unui rootkit.** Rootkit-urile reprezintă aplicații specializate utilizate pentru ascunderea fișierelor de sistemul de operare. Deși nu sunt periculoase, rootkit-urile sunt adesea utilizate pentru ascunderea programelor periculoase sau pentru a disimula prezența unui intrus în sistem.

  Rootkit-urile și fișierele ascunse detectate sunt ignorate implicit.

Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți preciza o a doua acțiune de aplicat în cazul în care prim eșuează, precum și acțiuni diferite pentru fiecare categorie. Alegeți din meniurile corespunzătoare prima și a doua acțiune de aplicat pentru fiecare tip de fișier detectat. Următoarele acțiuni sunt disponibile:

Dezinfectează
Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Mută în carantină
Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

Ștergere
Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Ignoră
Nu se vor lua niciun fel de măsuri împotriva fișierelor detectate. Aceste fișiere vor fi doar afișate în jurnalul de scanare.

- Mergeți la secțiunea **Ținte**, pentru a adăuga locațiile pe care doriți să le scanați din calculatoarele țintă.

  În secțiunea **Țintă scanare**, puteți adăuga un fișier sau folder nou pentru a fi scanat:

  a. Selectați o locație predefinită din meniul derulant sau introduceți **Căi specifice** pe care doriți să le folosiți.

  b. Specificați calea către obiectul de scanat în câmpul de editare.

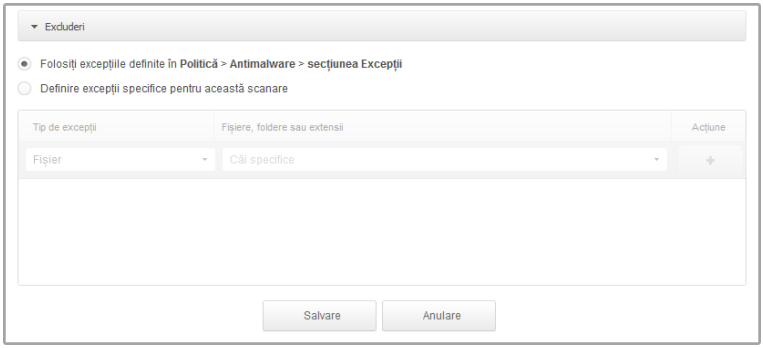
  – Dacă ați ales o locație predefinită, completați calea, după caz. De exemplu, pentru a scana integral folderul `Program Files`, este suficient să selectați locația predefinită corespunzătoare din meniul derulant. Pentru a scana un anumit folder din `Program Files`, trebuie să completați calea adăugând o bară oblică inversă (\) și denumirea folderului.

  – Dacă ați selectat **Căi specifice**, introduceți calea completă către obiectul de scanat. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă. Pentru informații suplimentare referitoare la variabilele de sistem, consultați„Utilizarea variabilelor de sistem” (p. 149)

  c. Faceți clic pe butonul ⁺ **Adăugare** corespunzător.

  Pentru a edita o locație existentă, faceți clic pe aceasta. Pentru a șterge o locație din listă, deplasați cursorul peste aceasta și faceți clic pe butonul ⁻ **Ștergere** corespunzător.

  Faceți clic pe secțiunile **Excluderi** dacă doriți să definiți excluderi pentru ținte.



Sarcină de scanare calculatoare - Definirea excepțiilor

Puteți utiliza excepții definite de politică sau puteți defini excluderi explicite pentru sarcina de scanare curentă. Pentru detalii referitoare la excepții, consultați „Excluderi” (p. 96).

6. Faceți clic pe **Salvare** pentru a crea sarcina de scanare. Va apărea un mesaj de confirmare.
7. Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.5.2. Instalare client

Pentru a vă proteja calculatoarele cu Security for Endpoints, trebuie să instalați Endpoint Security pe fiecare dintre acestea.

Avertisment

- Primul calculator pe care instalați protecția trebuie să aibă rol de Endpoint Security Relay, altfel nu veți putea instala Endpoint Security pe celelalte calculatoare din rețea.
- Calculatorul cu rol de Endpoint Security Relay trebuie să fie pornit și online pentru ca sistemele client să comunice cu Control Center.

După ce ați instalat un client Endpoint Security cu rol Endpoint Security Relay în rețea, acesta va detecta automat calculatoarele neprotejate din rețea.

Protecția Security for Endpoints poate fi apoi instalată pe aceste calculatoare de la distanță, de pe Control Center.

Instalarea la distanță este efectuată în fundal, fără ca utilizatorul să știe despre acest lucru.

Avertisment

Înainte de instalare, asigurați-vă că ați dezinstalat aplicația firewall contra programelor periculoase de pe calculatoare. Instalarea Security for Endpoints peste aplicațiile de securitate

existente poate afecta funcționarea acestora și cauza probleme majore cu sistemul. Windows Defender și Windows Firewall se dezactivează automat la demararea instalării.

Pentru a instala protecția Security for Endpoints de la distanță pe unul sau mai multe calculatoare:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din rețea din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

Notă
Opțional, puteți aplica filtre pentru a afișa exclusiv calculatoarele neadministrate. Faceți clic pe butonul **Filtre** și selectați următoarele opțiuni: **Neadministrat** din categoria **Securitate** și **Toate obiectele recursiv** din categoria **Adâncime**.

3. Selectați entitățile (calculatoarele sau grupurile de calculatoare) pe care doriți să instalați protecția.
4. Faceți clic pe butonul **Sarcini** din partea dreaptă a tabelului și selectați **Instalare client**. Se afișează asistentul **Instalare client**.
5. Configurați opțiunile de instalare:
   - Programați intervalul de instalare:
     - **Acum**, pentru a lansa instalarea imediat.
     - **Programat**, pentru a configura intervalul de recurență al instalării. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.

Notă
De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi dezinstalarea altor aplicații și repornirea sistemului de operare), puteți programa sarcina de instalare să ruleze la fiecare 2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes a instalării.

   - Selectați rolul pe care doriți să îl atribuiți clientului:
     - **Stație de lucru**. Selectați această opțiune dacă doriți să instalați clientul pe un terminal obișnuit.
     - **Endpoint Security Relay**. Selectați această opțiune pentru a instala clientul cu rol Endpoint Security Relay pe calculatorul țintă. Endpoint Security Relay este un rol special care instalează un server de actualizări pe mașina țintă, alături de Endpoint Security, care poate fi utilizat pentru toți ceilalți clienți din rețea, diminuând gradul de utilizare a lățimii de bandă între mașinile client și Control Center.

- Selectați modulele de protecție pe care doriți să le instalați. Vă rugăm rețineți că pentru sistemele de operare pentru servere este disponibilă numai protecția împotriva malware.
- Din câmpul **Limbă**, selectați limba dorită pentru interfața clientului.
- Selectați **Scanare înainte de instalare** dacă doriți să vă asigurați că ați curățat calculatoarele, înainte de instalarea Endpoint Security pe acestea. Se va efectua o scanare rapidă prin cloud pe calculatoarele corespunzătoare, înainte de pornirea instalării.
- Endpoint Security este instalat în directorul de configurare implicit pe calculatoarele selectate. Selectați **Utilizare cale de instalare implicită** dacă doriți să instalați Endpoint Security într-o altă locație. În acest caz, introduceți calea dorită în câmpul corespunzător. Folosiți convențiile Windows la introducerea căii (de exemplu, `D:\folder`). Dacă folderul specificat nu există, acesta va fi generat în timpul instalării.
- În timpul instalării silențioase, calculatorul este scanat pentru detectarea de malware. Uneori este necesară repornirea sistemului pentru a finaliza ștergerea malware-ului.

  Selectați **Restartare automată (dacă este necesară)** pentru a vă asigura că malware-ul detectat este șters complet înainte de instalare. Altfel, instalarea poate eșua.
- Dacă doriți, puteți seta o parolă pentru a împiedica utilizatorii să șteargă protecția. Selectați **Configurare parolă dezinstalare** și introduceți parola dorită în câmpurile corespunzătoare.
- Faceți clic pe **Înainte**.
- În funcție de rolul clientului (Endpoint sau Endpoint Security Relay), selectați entitatea prin care va comunica respectivul client:
  - **Bitdefender Cloud**, dacă doriți să actualizați clienții direct de pe internet.
  - **Endpoint Security Relay**, dacă doriți să conectați terminalele la un Endpoint Security Relay instalat în rețeaua dvs. Toate calculatoarele cu rolul de Endpoint Security Relay detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați Endpoint Security Relay dorit. Terminalele conectate vor comunica cu Control Center exclusiv prin Endpoint Security Relay specificat.

    Important
    Portul 7074 trebuie să fie deschis pentru ca instalarea prin Endpoint Security Relay să funcționeze.

6. Faceți clic pe **Înainte**.
7. În secțiunea **Administrare date de autentificare**, specificați drepturile de administrare necesare pentru autentificarea de la distanță pe terminalele selectate.

Puteți adăuga datele necesare introducând numele de utilizator și parola fiecărui sistem de operare țintă.

Notă

Dacă nu ați selectat datele de autentificare, se va afișa un mesaj de avertizare. Acest pas este obligatoriu pentru instalarea de la distanță a Endpoint Security pe calculatoare.

Pentru a adăuga datele SO necesare:

a. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont. În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

Folosiți convențiile Windows la introducerea numelui unui cont de utilizator de domeniu, de exemplu, `utilizator@domeniu.com` sau `domeniu\utilizator`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`utilizator@domeniu.com` și `domeniu\utilizator`).

Notă

Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

b. Faceți clic pe butonul **Adăugare**. Contul este adăugat la lista de date de autentificare.

c. Selectați caseta corespunzătoare contului pe care doriți să îl folosiți.

8. Faceți clic pe **Salvare**. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.5.3. Modificare aplicație de instalare

Pentru a modifica modulele de protecție instalate pe unul sau mai multe calculatoare:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați casetele de bifare corespunzătoare calculatoarelor administrate pe care doriți să schimbați modulele de protecție instalate.
4. Faceți clic pe butonul **Sarcini** din dreapta tabelului și selectați **Modificare aplicație de instalare**.
5. În secțiunea **Module**, selectați doar modulele de protecție pe care doriți să le instalați:

Antimalware
Modulul Antimalware protejează sistemul contra tuturor tipurilor de malware (viruși, troieni, aplicații spion, rootkit-uri, adware și așa mai departe).

Firewall
Firewallul vă protejează calculatorul de tentativele de conectare neautorizate, atât la intrare, cât și la ieșire.

Control Conținut
Modulul Control Conținut vă ajută să controlați accesul utilizatorilor la Internet și aplicații. Vă rugăm să rețineți că setările configurate pentru Control Conținut se aplică tuturor utilizatorilor care se autentifică pe calculatoarele țintă.

Notă
Vă rugăm rețineți că pentru sistemele de operare pentru servere este disponibilă numai protecția împotriva malware.

6. Bifați opțiunea **Rpornire dacă este cazul** pentru a permite calculatorului să repornească automat pentru finalizarea instalării.
7. Faceți clic pe **Salvare**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.5.4. Dezinstalare client

Pentru a dezinstala de la distanță întreaga protecție Security for Endpoints de pe unul sau mai multe calculatoare:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați casetele de bifare corespunzătoare calculatoarelor de pe care doriți să dezinstalați protecția Security for Endpoints.
4. Faceți clic pe butonul **Sarcini** din dreapta tabelului și selectați **Uninstall client**.
5. Se va afișa o fereastră de configurare, care vă va permite să optați pentru păstrarea obiectelor din carantină pe mașina client.
6. Faceți clic pe **Salvare** pentru a genera sarcina. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

Notă
Dacă doriți să reinstalați protecția, asigurați-vă mai întâi că ați repornit calculatorul.

5.5.5. Actualizare

Verificați periodic starea calculatoarelor administrate. Dacă identificați un calculator cu probleme de securitate, faceți clic pe denumire pentru afișarea paginii **Detalii calculator**. Pentru mai multe informații, consultați capitolul „Calculatoare cu probleme de securitate” (p. 36).

Clienții sau semnăturile care nu sunt la zi reprezintă o problemă de securitate. În aceste cazuri, trebuie să executați o actualizare pentru calculatorul corespunzător. Această sarcină poate fi efectuată local de pe calculator sau de la distanță din Control Center.

Pentru a actualiza de la distanță clientul și semnăturile pe calculatoarele administrate:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați casetele de bifare ale calculatoarelor pe care doriți să rulați o actualizare a clientului.
4. Faceți clic pe butonul **Sarcini** din dreapta tabelului și selectați **Actualizare**. Va apărea o fereastră de configurare.
5. Puteți opta pentru actualizarea produsului, doar a semnăturilor virușilor sau a amândurora.
6. Faceți clic pe **Actualizare** pentru a executa sarcina. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.5.6. Repornire calculator

Puteți opta pentru repornirea de la distanță a calculatoarelor administrate.

Notă

Verificați pagina **Rețea > Sarcini** înainte de a reporni anumite calculatoare. Este posibil ca sarcinile create anterior să fie în continuare în curs de procesare pe calculatoarele țintă.

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați casetele de bifare, în funcție de calculatoarele pe care doriți să le reporniți.
4. Faceți clic pe butonul **Sarini** din dreapta tabelului și selectați **Repornire calculator**.
5. Selectați opțiunea programului de repornire:
   - Selectați **Repornire imediată** pentru a reporni imediat calculatoarele.

- Selectați **Repornire la** și folosiți câmpurile de mai jos, pentru a programa repornirea la data și ora dorită.

6. Faceți clic pe **Salvare**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.5.7. Descoperire rețea

Această funcție este executată automat din oră în oră de către Endpoint Security cu rol Endpoint Security Relay. Cu toate acestea, puteți executa manual sarcina de descoperire rețea din Control Center oricând doriți, pornind de la orice mașină protejată de Endpoint Security.

Pentru a rula o sarcină de descoperire a rețelei în rețeaua dumneavoastră:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul de calculatoare dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați casetele de bifare corespunzătoare calculatoarelor cu care doriți să executați sarcina de descoperire a rețelei.
4. Faceți clic pe butonul **Sarcini** din dreapta tabelului și selectați **Descoperire rețea**.
5. Va apărea un mesaj de confirmare. Faceti clic pe **Da**.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**. Pentru mai multe informații, consultați capitolul Viewing and Managing Tasks.

5.6. Crearea de rapoarte rapide

Puteți opta pentru crearea de rapoarte rapide pe calculatoarele administrate, din pagina **Rețea**:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

   Opțional, puteți filtra conținutul grupului selectat numai după calculatoarele administrate.
3. Selectați casetele de bifare corespunzătoare calculatoarelor care vor fi incluse în raport.
4. Faceți clic pe butonul **Rapoarte** din partea dreaptă a tabelului și selectați tipul de raport din meniu. Rapoartele de activitate vor include doar datele pentru săptămâna anterioară. Pentru mai multe informații, consultați capitolul „Tipuri de rapoarte disponibile ” (p. 121).

5. Configurați opțiunile pentru raport. Pentru mai multe informații, consultați capitolul „Crearea rapoartelor” (p. 124)
6. Faceți clic pe **Generare**. Raportul este afișat imediat. Intervalul necesar pentru crearea rapoartelor poate varia în funcție de numărul de computere selectate.

5.7. Atribuirea unei politici

Setările de securitate se administrează folosind politici.

Din secțiunea **Rețea**, puteți vizualiza, modifica și atribui politici pentru fiecare calculator sau grup de calculatoare.

Notă

Puteți vizualiza sau modifica setările de securitate pentru calculatoarele administrate sau pentru grupuri. Pentru a facilita această sarcină, puteți filtra conținutul tabelului pentru a include doar calculatoarele administrate.

Pentru a vizualiza politica atribuită unui anumit calculator:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Faceți clic pe denumirea calculatorului administrat dorit. Se va afișa o fereastră cu detalii.
4. În secțiunea **Securitate**, faceți clic pe denumirea politicii curente, pentru vizualizarea setărilor.
5. Puteți modifica setările de securitate în funcție de necesități, cu condiția ca deținătorul politicii să fi permis celorlalți utilizatori să modifice politica respectivă. Vă rugăm să rețineți că orice modificare va afecta toate celelalte calculatoare cărora le este atribuită aceeași politică.

   Pentru informații suplimentare referitoare la modificarea politicilor calculatorului, consultați „Politicile pentru calculator” (p. 74).

Pentru atribuirea unei politici pentru un calculator sau un grup:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați caseta de bifare pentru calculatorul sau grupul dorit. Puteți selecta unul sau mai multe obiecte de același timp, numai dacă aparțin aceluiași nivel.
4. Faceți clic pe butonul **Atribuire politică** din dreapta tabelului.
5. Efectuați setările necesare în fereastra **Atribuire politică**. Pentru mai multe informații, consultați capitolul „Alocarea politicilor unor obiecte din rețea” (p. 72).

5.8. Ştergerea calculatoarelor din inventarul reţelei

Dacă nu doriți să administrați o parte dintre calculatoarele detectate, puteți opta pentru excluderea acestora din inventarul rețelei. De asemenea, puteți șterge permanent calculatoarele excluse din inventarul rețelei.

5.8.1. Excluderea calculatoarelor din inventarul reţelei

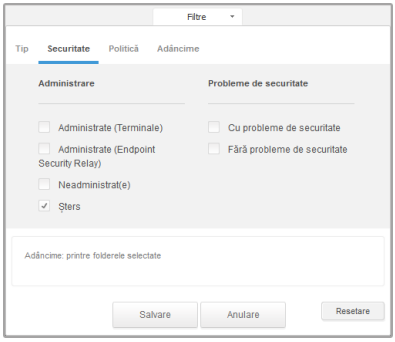
Pentru a exclude calculatoarele din inventarul rețelei:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați caseta de bifare corespunzătoare calculatorului pe care doriți să îl excludeți.
4. Faceți clic pe butonul − **Ștergere** din dreapta tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

> **Notă**
> Dacă ștergeți un calculator administrat, Endpoint Security va fi dezinstalat automat de pe acesta.

După ce ați șters calculatorul, nu îl mai puteți vizualiza în tabel. Calculatoarele șterse vor exista în continuare în baza de date Small Office Security, însă nu vor mai fi vizibile.

Este posibil ca o parte dintre calculatoarele șterse să necesite din nou administrare. În acest caz, trebuie să afișați calculatoarele șterse și să instalați Endpoint Security pe cele care vă interesează. Pentru afișarea calculatoarelor șterse, faceți clic pe meniul **Filtre** situat deasupra tabelului, mergeți la fila **Securitate**, bifați opțiunea **Șters** și apoi faceți clic pe **Salvare**.



Calculatoare - Filtrare după stații de lucru șterse

Notă
Dacă reinstalați protecția pe un calculator exclus, acesta va fi detectat ca fiind administrat și va fi reintrodus în tabel.

5.8.2. Ştergerea permanentă a calculatoarelor

Pentru a șterge permanent calculatoarele din inventarul rețelei:

1. Mergeți la pagina **Rețea**.
2. Selectați grupul dorit din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Filtrați conținutul tabelului după calculatoare **Șterse**.
4. Selectați caseta de bifare corespunzătoare calculatoarelor pe care doriți să le ștergeți.
5. Faceți clic pe butonul **Ștergere** din dreapta tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

   Calculatoarele corespunzătoare sunt șterse permanent din baza de date Small Office Security.

Avertisment
Calculatoarele șterse permanent din baza de date Small Office Security nu pot fi recuperate.

5.9. Pachetele de instalare

Componentele de protecție ale Small Office Security pot fi instalate pe obiectele de rețea țintă fie prin instalarea lor din Control Center, fie prin descărcarea pachetului de instalare necesar și executarea manuală a acestuia pe obiectele de rețea țintă.

Puteți gestiona pachetele de instalare de pe pagina **Rețea > Pachete**.

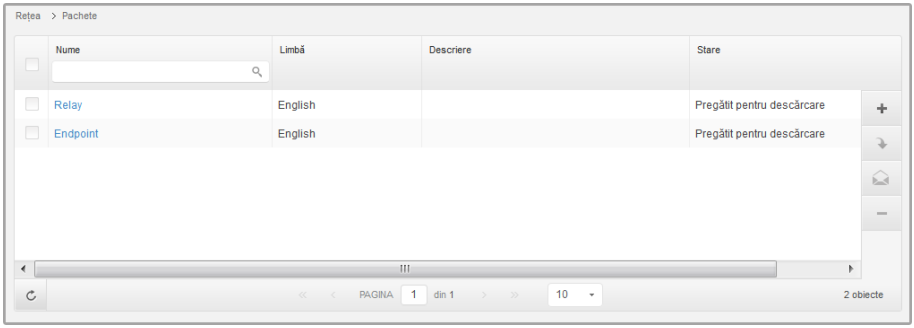
5.9.1. Generarea pachetelor de instalare

Este posibil să fie necesar să efectuați anumite adaptări ale pachetelor de instalare, pentru a corespunde mai bine necesităților de securitate.

Crearea pachetelor de instalare Endpoint Security

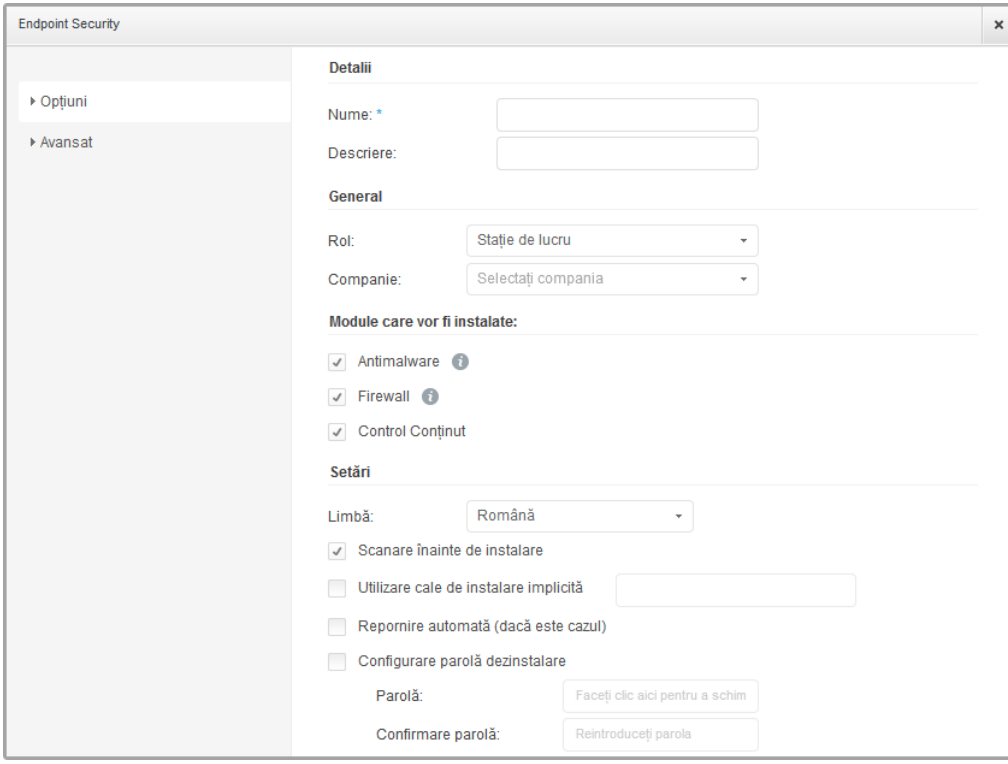
Pentru a crea un pachet de instalare Endpoint Security:

1. Conectați-vă și autentificați-vă la Control Center folosind propriul cont.
2. Mergeți la pagina **Rețea > Pachete**.



Pagina pachete

3. Faceți clic pe butonul + **Adăugare** din dreapta tabelului. Va apărea o fereastră de configurare.



Crearea pachetelor Endpoint Security - Opțiuni

4. Introduceți o denumire sugestivă și o descriere pentru pachetul de instalare pe care doriți să îl creați.
5. Selectați rolul calculatorului țintă:
   - **Stație de lucru**. Selectați această opțiune pentru a crea pachetul pentru un terminal obișnuit.
   - **Endpoint Security Relay**. Selectați această opțiune pentru a crea pachetul pentru un terminal cu rol Endpoint Security Relay. Endpoint Security Relay este un rol special care instalează un server de actualizări pe mașina țintă, alături de Endpoint Security, care poate fi utilizat pentru toți ceilalți clienți din rețea, diminuând gradul de utilizare a lățimii de bandă între mașinile client și Control Center.
6. Selectați compania unde se va utiliza pachetul de instalare.
7. Selectați modulele de protecție pe care doriți să le instalați.
8. Din câmpul **Limbă**, selectați limba dorită pentru interfața clientului.
9. Selectați **Scanare înainte de instalare** dacă doriți să vă asigurați că ați curățat calculatoarele, înainte de instalarea Endpoint Security pe acestea. Se va efectua o scanare rapidă prin cloud pe calculatoarele corespunzătoare, înainte de pornirea instalării.
10. Endpoint Security este instalat în directorul de configurare implicit pe calculatoarele selectate. Selectați **Utilizare cale de instalare implicită** dacă doriți să instalați Endpoint Security într-o altă locație. În acest caz, introduceți calea dorită în câmpul corespunzător. Folosiți convențiile Windows la introducerea căii (de exemplu, `D:\folder`). Dacă folderul specificat nu există, acesta va fi generat în timpul instalării.
11. Dacă doriți, puteți seta o parolă pentru a împiedica utilizatorii să șteargă protecția. Selectați **Configurare parolă dezinstalare** și introduceți parola dorită în câmpurile corespunzătoare.
12. Faceți clic pe **Înainte**.
13. În funcție de rolul pachetului de instalare (Endpoint sau Endpoint Security Relay), selectați entitatea la care se vor conecta periodic calculatoarele țintă, pentru actualizarea clientului:
    - **Bitdefender Cloud**, dacă doriți să actualizați clienții direct de pe internet.
    - **Endpoint Security Relay**, dacă doriți să conectați terminalele la un Endpoint Security Relay instalat în rețeaua dvs. Toate calculatoarele cu rolul de Endpoint Security Relay detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați Endpoint Security Relay dorit. Terminalele conectate vor comunica cu Control Center exclusiv prin Endpoint Security Relay specificat.

Important
Portul 7074 trebuie să fie deschis pentru ca instalarea prin Endpoint Security Relay să funcționeze.

14. Faceți clic pe **Salvare**.

Noul pachet de instalare va apărea în lista de pachete alte companiei țintă.

5.9.2. Descărcaţi pachetele de instalare

Pentru descărcarea pachetelor de instalare Endpoint Security:

1. Înregistrați-că în Control Center de pe calculatorul pe care doriți să instalați protecția.
2. Mergeți la pagina **Rețea > Pachete**.
3. Selectați pachetul de instalare Endpoint Security pe care doriți să îl descărcați.
4. Faceți clic pe butonul **Descărcare** din partea dreaptă a tabelului și selectați tipul de instalare pe care doriți să o utilizați. Există două tipuri de fișiere de instalare:
   - **Aplicație de descărcare**. Aplicația de descărcare descarcă mai întâi setul complet de instalare de pe serverele cloud ale Bitdefender și apoi demarează instalarea. Este de dimensiuni reduse și poate fi rulată atât pe sistemele de 32, cât și pe cele de 64 de biți (ceea ce ușurează distribuția). Dezavantajul este că necesită o conexiune activă la Internet.
   - **Kit complet**. Setul complet va fi utilizat pentru a instala protecția pe calculatoare cu o conexiune slabă sau chiar inexistentă la internet. Descărcați acest fișier pe un calculator conectat la Internet și apoi distribuiți-l pe alte calculatoare folosind un mediu de stocare extern sau un director partajat în rețea.

     Notă
     Versiuni cu kit complet disponibile:
     – **Windows OS:** sisteme pe 32 de biți și pe 64 de biți
     – **Mac OS X:** numai sisteme pe de biți
     Asigurați-vă că folosiți versiunea corectă pentru calculatorul pe care instalați.
5. Salvați fișierul în calculator.

5.9.3. Trimitere link-uri de descărcare pachete de instalare prin e-mail

Este posibil să trebuiască să informați rapid ceilalți utilizatori că pot descărca un pachet de instalare. În acest caz, urmați pașii de mai jos:

1. Mergeți la pagina **Rețea > Pachete**.
2. Selectați pachetul de instalare dorit.
3. Faceți clic pe butonul **Trimitere link-uri descărcare** din partea dreaptă a tabelului. Va apărea o fereastră de configurare.

4. Introduceți adresa de e-mail a fiecărui utilizator care urmează să primească link-ul de descărcare a pachetului de instalare. Apăsați `Enter` după fiecare adresă de e-mail.

   Asigurați-vă că fiecare adresă de e-mail introdusă este validă.

5. Dacă doriți să vizualizați link-urile de descărcare înainte de trimiterea acestora prin e-mail, faceți clic pe butonul **Vizualizare link-uri de instalare**.

6. Faceți clic pe **Trimitere**. Un e-mail care conține link-ul de instalare este trimis fiecărei adrese de e-mail specificate.

5.10. Vizualizarea şi administrarea sarcinilor

Pagina **Rețea > Sarcini** vă permite să vizualizați și să gestionați toate sarcinile generate.

După ce ați generat o sarcină pentru unul sau mai multe obiecte din rețea, o puteți vizualiza în tabelul sarcinilor.

Puteți efectua următoarele operațiuni de pe pagina **Rețea > Sarcini**:

- Verificarea stării sarcinii
- Vizualizarea rapoartelor sarcinii
- Re-executarea sarcinilor
- Ștergere sarcini

5.10.1. Verificarea stării sarcinii

De fiecare dată când creați o sarcină pentru unul sau mai multe obiecte din rețea, trebuie să verificați progresul acesteia și să fiți informat în cazul apariției erorilor.

Mergeți la pagina **Rețea > Sarcini** și verificați coloana **Stare** pentru fiecare sarcină dorită. Puteți verifica starea sarcinii principale și puteți, de asemenea, să obțineți informații detaliate referitoare la fiecare sub-sarcină.

Pagina Sarcini

- **Verificarea stării sarcinii principale**.

  Sarcina principală se referă la acțiunile lansate asupra obiectelor din rețea (cum ar fi instalarea clientului sau scanare) și include o serie de sub-sarcini, una pentru fiecare obiect din rețea selectat. De exemplu, o sarcină de instalare principală creată pentru opt

calculatoare include opt sub-sarcini. Numerele dintre paranteze reprezintă procentul de finalizare a sub-sarcinilor. De exemplu, (2/8) înseamnă că au fost finalizate două din opt sub-sarcini.

Starea principală a sarcinii poate fi:

– **În așteptare**, dacă nu a fost pornită niciuna dintre sub-sarcini.
– **În curs**, dacă toate sub-categoriile rulează. Starea sarcinii principale rămâne În curs până la finalizarea ultimei sub-sarcini.
– **Finalizat**, dacă toate sub-sarcinile au fost finalizate (cu sau fără succes). În cazul sub-sarcinilor finalizate cu succes, se afișează un simbol de avertizare.

- **Verificarea stării sub-sarcinilor**.

  Mergeți la sarcina dorită și faceți clic pe link-ul disponibil în coloana **Stare** pentru a deschide fereastra **Stare**. Puteți vizualiza o listă a obiectelor din rețea alocate sarcinii principale și starea sub-sarcinii aferente. Starea sub-sarcinii poate fi:

  – **În curs,** când sub-sarcina încă se execută.

  – **Finalizat**, dacă sub-sarcina a fost finalizată cu succes.

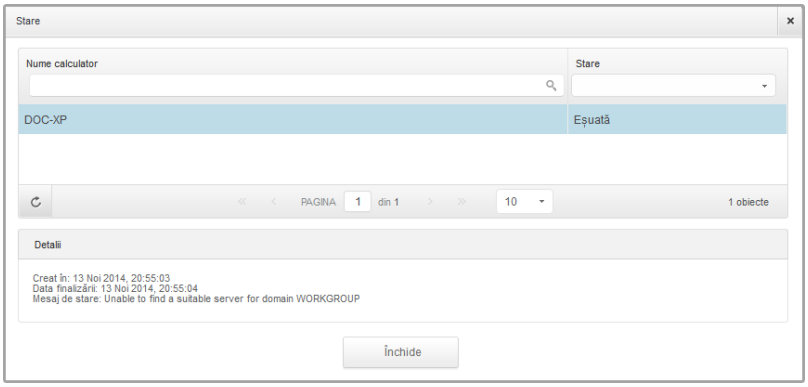
  – **În așteptare**, dacă sub-sarcina nu a început încă. Aceasta se poate întâmpla în următoarele situații:

    • Sub-sarcina este într-o coadă de așteptare.

    • Există probleme de conectivitate între Control Center și obiectul rețelei țintă.

  – **Eșuată**, dacă sub-sarcina nu a putut fi inițiată sau a fost întreruptă din cauza erorilor, cum ar fi datele de autentificare și spațiul redus de memorie.

  Pentru a vizualiza detaliile fiecărei sub-sarcini, selectați-o și bidați secțiunea **Detalii** din partea de jos a tabelului.



Detalii privind starea sarcinilor

Veți obține informații referitoare la:

- Data și ora începerii sarcinii.
- Data și ora la care s-a încheiat sarcina.
- Descrierea erorilor întâlnite.

5.10.2. Vizualizarea rapoartelor referitoare la sarcină

Din pagina **Rețea > Sarcini** puteți opta pentru vizualizarea rapoartelor cu privire la sarcinile de scanare rapidă.

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați caseta de bifare care corespunde sarcinilor de scanare care vă interesează.
3. Faceți clic pe butonul corespunzător din coloana **Rapoarte**. Așteptați până când se afișează raportul. Pentru mai multe informații, consultați capitolul „Utilizarea rapoartelor” (p. 121).

5.10.3. Re-executarea sarcinilor

Din diverse motive, este posibil ca sarcinile de instalare, dezinstalare sau actualizare a clientului să nu se finalizeze. Puteți alege să re-executați sarcinile nereușite în loc să creați unele noi, urmând acești pași:

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați căsuțele corespunzătoare sarcinilor nereușite.
3. Faceți clic pe butonul **Reluare sarcină** din dreapta tabelului. Sarcinile selectate vor fi repornite, iar starea sarcinilor se va modifica în **Reîncercare**.

Notă
Pentru sarcinile cu sub-sarcini multiple, opțiunea **Reluare sarcină** este disponibilă numai atunci când toate sub-sarcinile s-au finalizat și va executa doar sub-sarcinile nereușite.

5.10.4. Ştergerea unei sarcini

Pentru a preveni aglomerarea listei de sarcini, se recomandă să ștergeți sarcinile de care nu mai aveți nevoie.

1. Mergeți la pagina **Rețea > Sarcini**.
2. Selectați caseta de bifare care corespunde sarcinii pe care doriți să o ștergeți.
3. Faceți clic pe butonul **Ștergere** din dreapta tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

Avertisment
Ștergerea unei sarcini în curs va anula sarcina respectivă.

Dacă este ștearsă o sarcină în curs, orice sub-sarcini în așteptare vor fi anulate. În acest caz, sub-sarcinile finalizate nu pot fi anulate.

5.11. Administrare date de autentificare

Secțiunea de Administrare date de autentificare vă ajută să gestionați datele de autentificare necesare pentru autentificarea de la distanță pe diferite sisteme de operare din rețeaua dumneavoastră.

Pentru a deschide fereastra Administrare date de autentificare, îndreptați cursorul către numele de utilizator din colțul din dreapta sus al paginii și selectați **Administrare date de autentificare**.

5.11.1. Adăugarea datelor de autentificare în modulul de Administrare date de autentificare

Administrare date de autentificare

1. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont. În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

   Folosiți convențiile Windows la introducerea numelui unui cont de utilizator de domeniu, de exemplu, `utilizator@domeniu.com` sau `domeniu\utilizator`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`utilizator@domeniu.com` și `domeniu\utilizator`).

2. Faceți clic pe butonul + **Adăugare**. Noul set de date de autentificare este adăugat la tabel.

Notă
Dacă nu ați specificat datele de autentificare, vi se va solicita să le introduceți atunci când executați sarcinile de instalare. Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

5.11.2. Ştergerea datelor de autentificare din fereastra Administrare date de autentificare

Pentru a șterge datele de autentificare care nu mai sunt valabile din fereastra Administrare date de autentificare:

1. Îndreptați cursorul către rândul din tabel care include datele pe care doriți să le ștergeți.
2. Faceți clic pe butonul **Ștergere** din dreapta rândului corespunzător din tabel. Contul selectat va fi șters.

6. Politici de securitate

Odată instalată, protecția Bitdefender poate fi configurată și administrată din Control Center utilizând politicile de securitate. O politică specifică setările de securitate care vor fi aplicate pe calculatoare.

Imediat după instalare, politica implicită este alocată obiectelor din rețea, această politică fiind preconfigurată cu setările recomandate de protecție. Politica implicită nu poate fi modificată sau ștearsă. O puteți utiliza doar ca și model pentru crearea de politici noi.

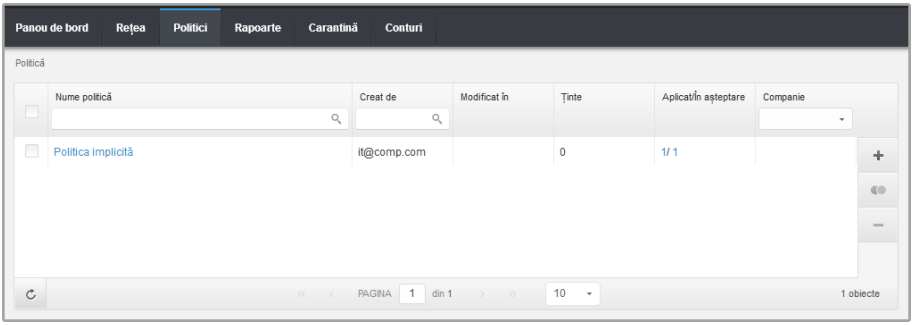
Puteți crea oricât de multe politici vă sunt necesare pe baza cerințelor de securitate.

Iată ce trebuie să știți despre politici:

- Politicile sunt create în pagina **Politici** și atribuite obiectelor de rețea din pagina **Rețea**.
- Obiectele de rețea nu pot avea mai multe politici active simultan.
- Politicile sunt expediate către obiectele țintă din rețea imediat după crearea sau modificarea acestora. Setările trebuie aplicate pe obiectele din rețea în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un obiect din rețea nu este online, setările vor fi aplicate imediat ce obiectul revine online.
- Politica se aplică exclusiv pentru modulele de protecție instalate. Vă rugăm rețineți că pentru sistemele de operare pentru servere este disponibilă numai protecția împotriva malware.
- Nu puteți edita politicile create de alți utilizatori (cu excepția cazului în care autorii politicilor permit acest lucru din setări), însă le puteți suprascrie prin aplicarea unei alte politici obiectelor țintă.

6.1. Administrarea politicilor

Politicile pot fi vizualizate și administrate pe pagina **Politici**.



Pagina Politici

Politicile existente sunt afișate în tabel. Pentru fiecare politică puteți vedea:

- Nume politică.
- Utilizatorul care a creat politica.
- Data și ora ultimei modificări a politicii.
- Numărul de destinatari către care a fost trimisă politica. Faceți clic pentru a afișa destinatarii corespunzători în inventarul de rețea.
- Numărul de obiective pentru care s-a aplicat/este în așteptare politica. Faceți clic pe numărul pe care doriți să îl afișați în inventarul de rețea al destinatarilor corespunzători.

Puteți sorta politicile existente și căuta anumite politici folosind criteriile disponibile.

6.1.1. Crearea politicilor

Puteți crea politici prin două metode: adăugarea unei politici noi sau duplicarea (clonarea) unei politici existente.

Pentru a crea o politică nouă:

1. Mergeți la pagina **Politici**.
2. Selectați metoda de creare a politicii:
   - **Adăugare politică nouă**.
     - Faceți clic pe butonul + **Adăugare** din dreapta tabelului. Această comandă generează o politică nouă pornind de la modelul politicii implicite.
   - **Clonarea unei politici existente**.

a. Selectați caseta de bifare a politicii pe care doriți să o duplicați.

b. Faceți clic pe butonul **Clonare politică** din dreapta tabelului.

3. Configurați setările politicii. Pentru informații detaliate, consultați capitolul „Politicile pentru calculator” (p. 74).
4. Faceți clic pe **Salvare** pentru a genera politica și a reveni la lista politicilor.

6.1.2. Modificarea setărilor politicii

Setările politicilor pot fi configurate inițial la crearea politicii. Acestea pot fi ulterior modificate după caz, în orice moment.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate modifica. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

Pentru a modifica setările unei politici existente:

1. Mergeți la pagina **Politici**.
2. Identificați politica dorită în listă și faceți clic pe denumirea acesteia pentru a o edita.
3. Configurați setările politicii după caz. Pentru informații detaliate, consultați capitolul „Politicile pentru calculator” (p. 74).
4. Faceți clic pe **Salvare**.

   Politicile expediate către obiectele țintă ale rețelei imediat după realocare sau după modificarea setărilor politicii. Setările trebuie aplicate pe obiectele din rețea în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un obiect din rețea nu este online, setările vor fi aplicate imediat ce obiectul revine online.

6.1.3. Redenumirea politicilor

Politicile trebuie să aibă denumiri sugestive, astfel încât dumneavoastră sau un alt administrator să le puteți identifica rapid.

Pentru a redenumi o politică:

1. Mergeți la pagina **Politici**.
2. Faceți clic pe denumirea politicii. Aceasta va deschide pagina politicii.
3. Introduceți o denumire pentru politică.
4. Faceți clic pe **Salvare**.

Notă
Denumirea politicii este unică. Trebuie să introduceți o denumire diferită pentru fiecare politică nouă.

6.1.4. Ştergerea politicilor

Dacă nu mai aveți nevoie de o politică, ștergeți-o. După ce ați șters o politică, obiectelor de rețea pentru care se aplica aceasta li se va aloca politica grupului mamă. Dacă nu se aplică nicio altă politică, în final, va fi activată cea implicită.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate șterge. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

Pentru a șterge o politică:

1. Mergeți la pagina **Politici**.
2. Selectați caseta de bifare corespunzătoare.
3. Faceți clic pe butonul **Ștergere** din dreapta tabelului. Vi se va solicita să confirmați alegerea făcând clic pe **Da**.

6.1.5. Alocarea politicilor unor obiecte din rețea

După ce ați definit politicile necesare în secțiunea **Politici**, le puteți aloca obiectelor din rețea din secțiunea **Rețea**.

Inițial, politica implicită este atribuită tuturor obiectelor din rețea.

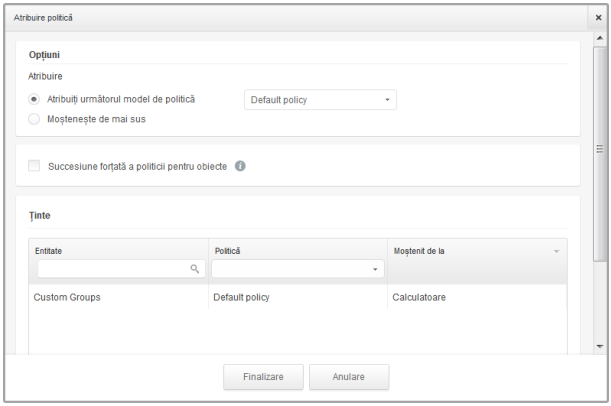
Notă
Puteți atribui numai politici create de dumneavoastră. Pentru a atribui o politică creată de alt utilizator, trebuie prima dată să o clonați în pagina **Politici**.

Pentru a atribui o politică:

1. Mergeți la pagina **Rețea**.
2. Selectați caseta de bifare a obiectului de rețea dorit. Puteți selecta unul sau mai multe obiecte numai de la același nivel.
3. Faceți click pe butonul **Atribuire politică** din partea dreaptă a tabelului.

Notă
Puteți, de asemenea, face clic dreapta pe un grup din arborele de rețea și selecta **Atribuire politică** din meniul contextual.

Este afișată fereastra **Atribuire politică**:



Setări atribuire politică

4. Configurați setările de atribuire a politicii pentru obiectele selectate:
   - Vizualizați atribuirile actuale ale politicii pentru obiectele selectate în tabelul din secțiunea **Ținte**.
   - **Atribuiți următorul model de politică**. Selectați această opțiune pentru a atribui obiectelor țintă o politică din meniul afișat în partea dreaptă. Numai politicile create din contul dumneavoastră de utilizator sunt disponibile în meniu.
   - **Moștenește de mai sus**. Selectați opțiunea **Moșteneste de mai sus** pentru a aloca obiectelor de rețea selectate politica grupului părinte.
   - **Succesiune forțată a politicii pentru obiecte**. În mod implicit, fiecare obiect din rețea preia politica grupului mamă. Dacă modificați politica grupului, toate elementele subordonate grupului vor fi afectate, cu excepția elementelor membre ale grupului pentru care ați alocat o altă politică în mod specific.

     Selectați opțiunea **Succesiune forțată a politicii pentru obiecte** pentru a aplica politica selectată unui grup, inclusiv elementelor subordonate ale grupului cărora le-a fost alocată o altă politică. În acest caz, tabelul de mai jos va afișa elementele membre selectate ale grupului care nu preiau politica grupului.
5. Faceți click pe **Terminare** pentru a salva și a aplica modificările.

Politicile expediate către obiectele țintă ale rețelei imediat după realocare sau după modificarea setărilor politicii. Setările trebuie aplicate pe obiectele din rețea în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un obiect din rețea nu este online, setările vor fi aplicate imediat ce acesta revine online.

Pentru a verifica dacă politica a fost alocată cu succes, mergeți pe pagina **Rețea** și faceți click pe numele obiectului pe care doriți să îl afișați în fereastra **Detalii**. Verificați secțiunea

Politică pentru a vizualiza starea politicii curente. Dacă este în starea de așteptare, politica nu a fost aplicată încă obiectului țintă.

6.2. Politicile pentru calculator

Setările politicilor pot fi configurate inițial la crearea politicii. Acestea pot fi ulterior modificate după caz, în orice moment.

Pentru a configura setările unei politici:

1. Mergeți la pagina **Politici**.
2. Faceți clic pe denumirea politicii. Aceasta va deschide pagina de setări ale politicii.
3. Configurați setările politicii după caz. Setările sunt organizate în următoarele categorii:
   - General
   - Antimalware
   - Firewall
   - Control Conținut

   Puteți selecta categoria de setări folosind meniul din partea stângă a paginii.
4. Faceți clic pe **Salvare** pentru a salva modificările și a le aplica la calculatoarele țintă. Pentru a părăsi pagina de politici fără a salva modificările, faceți clic pe **Anulare**.

Notă
Pentru a învăța modul de lucru cu politicile, consultați „Administrarea politicilor” (p. 70).

6.2.1. General

Setările generale vă ajută să administrați opțiunile de afișare ale interfeței cu utilizatorul, opțiunile de comunicare, să actualizați preferințele, protejarea cu parolă și alte setări ale Endpoint Security.

Setările sunt organizate în următoarele secțiuni:

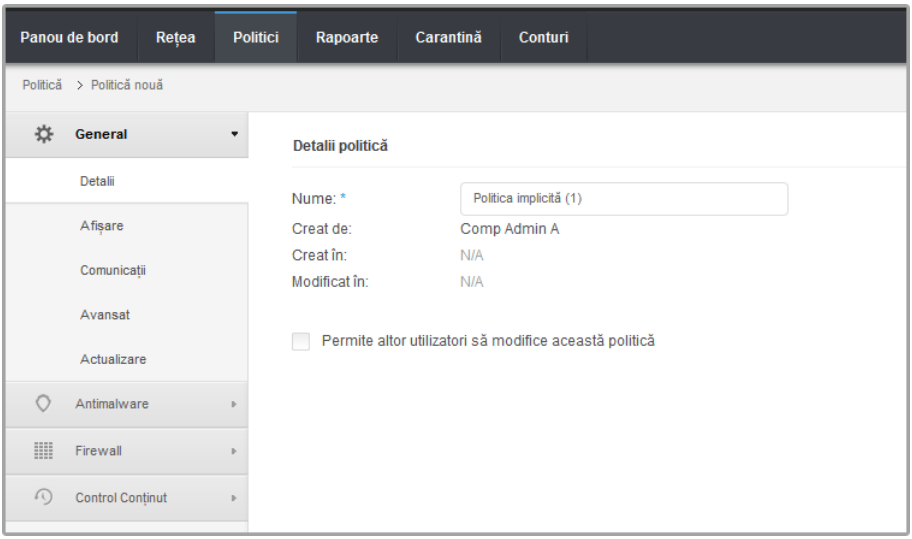
- Detalii
- Afișare
- Comunicații
- Avansat
- Actualizare

Detalii

Pagina Details prezintă detalii generale privind politica:

- Nume politică
- Utilizatorul care a creat politica

- Data și ora când a fost creată politica
- Data și ora când a fost modificată politica ultima dată



Politicile pentru calculator

Puteți redenumi politica introducând noul nume în câmpul corespunzător și făcând clic pe **Salvare**. Politicile trebuie să aibă denumiri sugestive, astfel încât dumneavoastră sau un alt administrator să le puteți identifica rapid.

Notă
În mod implicit, numai utilizatorul care a creat politica o poate modifica. Pentru a schimba această setare, deținătorul politicii trebuie să bifeze opțiunea **Permite altor utilizatori să modifice această politică** din pagina **Detalii** a politicii.

Afișare

În această secțiune puteți configura opțiunile de afișare a interfeței utilizator.

Politici pentru calculatoare - Setări de afișare

- **Activează Modul Silențios.** Utilizați caseta de selecție pentru a activa sau opri Modul Silențios. Modul Silențios este conceput pentru a vă ajuta să dezactivați cu ușurință interacțiunea cu utilizatorul în Endpoint Security. La activarea opțiunii Modul Silențios, sunt aduse următoarele modificări la configurația politicii:
  - Opțiunile **Afișare pictogramă în zona de notificare**, **Afișare notificări de tip pop-up** și **Afișare alerte de tip pop-up** din această secțiune vor fi dezactivate.
  - Dacă nivelul de protecție firewall a fost fixat pe **Set de reguli și întreabă** sau **Set de reguli, fișiere cunoscute și întreabă** acesta se va modifica în **Set de reguli, fișiere cunoscute și permite**. În caz contrar, setarea nivelului de protecție va rămâne neschimbată.
- **Afișare pictogramă în zona de notificare.** Selectați această opțiune pentru a afișa pictograma Bitdefender din zona de notificare (cunoscută și sub numele de bară de sistem). Pictograma informează utilizatorii cu privire la statutul de protecție prin schimbarea aspectul său și prin afișarea unei notificări de tip pop – up corespunzătoare. În plus, utilizatorii pot face clic dreapta pe acesta pentru a deschide rapid fereastra principală Endpoint Security sau fereastra **Despre**. Deschiderea fereastrei **Despre** inițiază automat o actualizare la cerere.
- **Afișare notificări de tip pop-up.** Selectați această opțiune pentru a informa utilizatorii cu privire la evenimentele importante de securitate, cum ar fi detectarea de programe periculoase și măsurile luate prin intermediul unor mici pop-up-uri de notificare. Ferestrele de tip pop-up dispar automat în câteva secunde, fără intervenția utilizatorului.
- **Afișare alerte de tip pop-up.** Spre deosebire de pop-up-urile de notificare, pop-up-urile de alertă atenționează utilizatori pentru acțiune. Dacă alegeți să nu se afișeze pop-up-urile de alertă, Endpoint Security întreprinde automat acțiunea recomandată. Pop-up-urile sunt generate în următoarele situații:
  - În cazul în care firewall-ul este setat pentru a solicita utilizatorului luarea de măsuri ori de câte ori aplicații necunoscute solicită acces la rețea sau Internet.

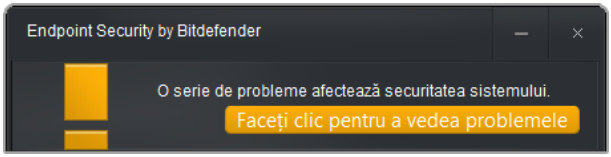
– În cazul în care este activat Active Virus Control/Sistem de Detectare a Intruziunilor, ori de câte ori este detectată o aplicație potențial periculoasă.

– Dacă scanarea dispozitivului este activată, ori de câte ori este conectat la computer un dispozitiv de stocare extern. Puteți configura această setare în secțiunea **Antimalware > Scanare la cerere**.

- **Alerte de stare.** Utilizatorii determină atunci când stația de lucru întâmpină probleme de configurare a securității sau alte riscuri de securitate în baza alertelor de stare. De exemplu, utilizatorii pot vedea când există o problemă cu protecția antimalware, cum ar fi: Modulul de scanare la accesare este dezactivat sau este necesară o scanare completă a sistemului.

  Utilizatorii sunt informați cu privire la stadiul lor de protecție în două moduri:

  – Prin zona de notificare a ferestrei principale, care afișează un mesaj de stare corespunzător și își schimbă culoarea în funcție de nivelul de severitate al problemelor de securitate. De asemenea, utilizatorii au posibilitatea de a vizualiza detaliile problemelor detectate făcând clic pe butonul disponibil.



Zona de notificare Endpoint Security

  – Prin pictograma Bitdefender din bara de sistem, care își modifică aspectul atunci când sunt detectate probleme.

  Endpoint Security folosește următoarea convenție de culori pentru zona de notificare:

  – Verde: Nu sunt detectate probleme.

  – Portocaliu: Stația de lucru prezintă probleme minore care îi afectează securitatea. Nu este necesar ca utilizatorii să-ți întrerupă lucrul pentru a soluționa aceste probleme.

  – Roșu: Stația de lucru prezintă probleme grave care necesită atenția imediată a utilizatorului.

  Pentru a configura alertele de stare, selectați nivelul de alertă care se potrivește cel mai bine nevoilor dumneavoastră (**Activare toate**, **Personalizat**, **Dezactivare toate**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

  Dacă doriți să personalizați alertele:

  1. Selectați nivelul **Personalizat**.
  2. Faceți clic pe link-ul **Setări** pentru a deschide fereastra de configurare.

3. Selectați aspectele de securitate care doriți să fie monitorizate. Opțiunile sunt descrise aici:
   - **General**. Alerta de stare este generată de fiecare dată când este necesară repornirea sistemului în timpul sau la finalizarea unei operațiuni de întreținere a produsului. Puteți alege să afișați alerta ca avertizare sau ca problemă gravă.
   - **Antimalware**. Alertele de stare sunt generate în următoarele situații:
     - Scanarea la accesare este activată, dar multe fișiere locale sunt excluse.
     - A trecut un anumit număr de zile de la data ultimei scanări complete a sistemului.

     Puteți selecta modul de afișare a alertelor și defini numărul de zile de la ultima scanare a sistemului.
   - **Firewall**. Această alertă de stare este generată atunci când modulul Firewall este dezactivat.
   - **Control Conținut**. Această alertă de stare este generată atunci când modulul Control conținut este dezactivat.
   - **Actualizare**. Alerta de stare este generată de fiecare dată când este necesară repornirea sistemului pentru finalizarea unei operațiuni de actualizare. Puteți selecta să afișați alerta ca avertizare sau ca problemă gravă.

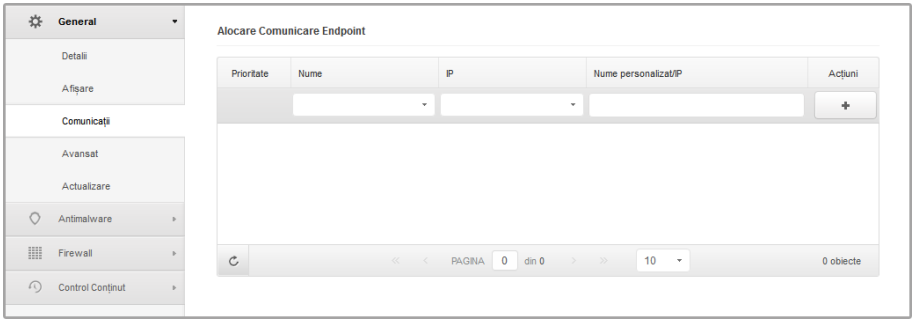
- **Informații privind asistența.** Puteți personaliza informațiile privind asistența tehnică și datele de contact disponibile în Endpoint Security completând câmpurile corespunzătoare. Utilizatorii pot accesa aceste informații din fereastra Endpoint Security făcând clic pe pictograma din colțul din dreapta jos sau, alternativ, prin clic dreapta pe pictograma Bitdefender din bara de sistem și selectând **Despre**).

Comunicaţii

Când în rețeaua țintă sunt disponibili mai mulți Endpoint Security Relay, puteți atribui calculatoarele selectate către unul sau mai mulți Endpoint Security Relay prin intermediul politicii.

Pentru a atribui un Endpoint Security Relay către calculatoarele țintă:

1. În tabelul **Alocare Comunicare Endpoint**, faceți clic pe câmpul **Nume**. Se afișează lista de Endpoint Security Relay detectați din rețeaua dumneavoastră.
2. Selectați o entitate.



Politici pentru calculatoare - Setări de comunicare

3. Faceți clic pe butonul **Adăugare** din dreapta tabelului.

   Endpoint Security Relay este adăugat în listă. Toate calculatoarele țintă vor comunica cu Control Center prin intermediul Endpoint Security Relay specificat.

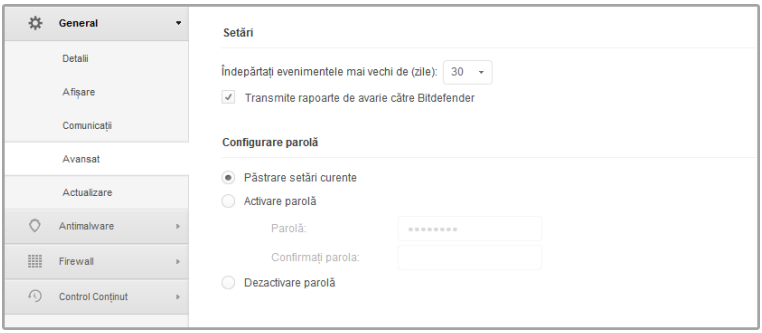
4. Urmați aceeași pași pentru a adăuga mai multe Endpoint Security Relay, dacă sunt disponibile.

5. Puteți configura prioritatea Endpoint Security Relay, folosind săgețile în sus și în jos disponibile în partea dreaptă a fiecărei entități. Comunicarea cu calculatoarele țintă va fi efectuată prin intermediul entității localizată în partea de sus a listei. În cazul în care nu se poate realiza comunicarea cu această entitate, va fi luată în considerare următoarea.

6. Pentru a șterge o entitate din listă, faceți clic pe butonul **Ștergere** din partea dreaptă a tabelului.

Avansat

În această secțiune puteți configura setările generale și parola de dezinstalare.



Politici pentru calculatoare - Setări avansate

- **Îndepărtați evenimentele mai vechi de (zile).** Endpoint Security păstrează un jurnal detaliat al evenimentelor referitoare la activitatea sa pe computer (inclusiv, de asemenea, activitățile calculatorului monitorizate de Content Control). În mod implicit, evenimentele sunt șterse din jurnal după 30 de zile. Dacă doriți să schimbați acest interval, alegeți o altă opțiune din meniu.
- **Transmiteți rapoarte de avarie la Bitdefender.** Selectați această opțiune astfel încât rapoartele să fie trimise la Laboratoarele Bitdefender pentru analiză în cazul în care Endpoint Security se blochează. Rapoartele vor ajuta inginerii noștri să își dea seama ce a cauzat problema și să prevină reapariția ei. Nu vor fi transmise informații cu caracter personal.
- **Configurare parolă.** Pentru a împiedica utilizatorii care beneficiază de drepturi de administrare să dezinstaleze protecția, trebuie să setați o parolă.

  Parola de dezinstalare poate fi configurată înainte de instalare prin personalizarea pachetului de instalare. Dacă ați făcut acest lucru, selectați **Păstrare setări curente** pentru a păstra parola curentă.

  Pentru a seta parola sau pentru a schimba parola curentă, selectați **Activare parolă** și introduceți parola dorită. Pentru a elimina protecția cu parolă, selectați **Dezactivare parolă**.

Actualizare

În această secțiune, puteți configura Endpoint Security și setările de actualizare a semnăturii virsului. Actualizările sunt foarte importante, întrucât permit combaterea celor mai noi amenințări.

Politici pentru calculatoare - Opțiuni de actualizare

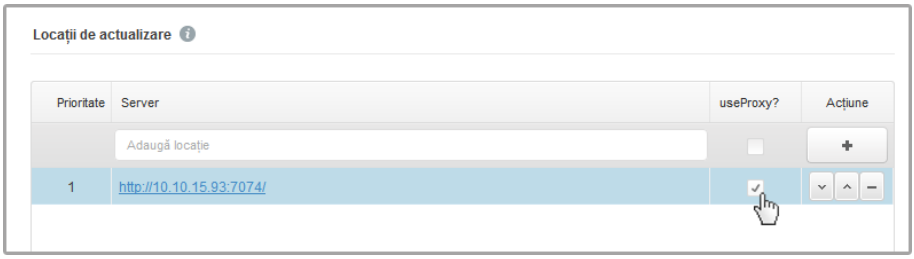
- **Actualizare produs.** Endpoint Security verifică, descarcă și instalează automat actualizările în fiecare oră (setare implicită). Actualizările automate sunt efectuate discret, în fundal.
  - **Recurență**. Pentru a modifica recurența de actualizare automată, selectați o altă opțiune din meniu și configurați-o conform necesităților dvs. în câmpurile ulterioare.
  - **Amânare repornire**. Unele actualizări necesită o repornire a sistemului pentru instalarea și funcționarea coresponzătoare. Selectând această opțiune, programul va continua să funcționeze folosind fișierele vechi până când computerul este repornit, fără a informa utilizatorul. În caz contrar, o notificare în interfața cu utilizatorul va solicita utilizatorului să repornească sistemul de fiecare dată când este necesară o actualizare.
  - Dacă alegeți să amânați repornirea, puteți seta un timp convenabil atunci când calculatoarele vor reporni în mod automat dacă este (încă) necesar. Acest lucru poate fi foarte util pentru servere. Selectați **Repornire după instalarea actualizărilor, dacă este cazul** și precizați când este convenabil să se facă repornirea (zilnic sau săptămânal într-o anumită zi, la un anumit moment al zilei).
- **Actualizare semnături.** Endpoint Security caută automat actualizări de semnătură în fiecare oră (setare implicită). Actualizările automate sunt efectuate discret, în fundal. Pentru a modifica recurența de actualizare automată, selectați o altă opțiune din meniu și configurați-o conform necesităților dvs. în câmpurile ulterioare.
- **Setări proxy.** Selectați această opțiune în cazul în care calculatoarele se conectează la Internet (sau la serverul de actualizări local) printr-un server proxy. Există trei opțiuni de configurare a setărilor proxy:
  - **Importare setări proxy din browser-ul implicit.** Endpoint Security poate importa setări proxy de la browserele cele mai des folosite, inclusiv cele mai noi versiuni pentru Internet Explorer, Mozilla Firefox și Opera.
  - **Detectare automată proxy de rețea.** Endpoint Security folosește protocolul Web Proxy Auto-Discovery (WPAD) inclus în Windows pentru a prelua în mod automat setările proxy dintr-un fișier Proxy Auto-Configuration (PAC) publicat pe rețeaua locală. În cazul în care nu este disponibil niciun fișier PAC, actualizările vor eșua.
  - **Utilizați setările proxy personalizate.** Dacă știți setările proxy, selectați această opțiune și apoi specificați-le:
    - **Server** - introduceți adresa IP a serverului proxy.
    - **Port** - introduceți portul folosit pentru conectarea la serverul proxy.
    - **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
    - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.

Notă

Modificarea opțiunii de configurare proxy va suprascrie setările proxy existente în Endpoint Security.

În plus, trebuie să selectați căsuța de selecție **Folosește Proxy** corespunzătoare locului de actualizare la care se aplică setările (Internet sau adresa locală a serverului de actualizări).

- **Locații de actualizare**. Pentru a evita supraîncărcarea traficului extern al rețelei, Endpoint Security este configurat pentru a se actualiza de la http://upgrade.bitdefender.com. De asemenea, puteți adăuga în listă și alte adrese de server local de actualizare și le puteți configura prioritatea cu ajutorul butoanelor sus și jos afișate când poziționați mouse-ul deasupra. Dacă prima locație de actualizare nu este disponibilă, se verifică următoarea și așa mai departe.



Politici pentru calculatoare - Locații de actualizare

Pentru a seta adresa de actualizare locală:

1. Introduceți adresa serverului local de actualizări în câmpul **Adăugare locație**. Utilizați una dintre aceste sintaxe:
   - `ip_server_actualizări:port`
   - `nume_server_actualizări:port`

   Portul implicit este 7074.
2. În cazul în care calculatoarele client se conectează la serverul local de actualizări, printr-un server proxy, selectați **Folosește Proxy**.
3. Faceți clic pe butonul **Adăugare** din dreapta tabelului.
4. Folosiți săgețile Sus / Jos din coloana **Acțiune** pentru a seta prima adresă de actualizare locală din listă. Plasați cursorul mouse-ului pe rândul corespunzător pentru ca săgețile să devină vizibile.

Pentru a șterge o locație din listă, deplasați cursorul peste aceasta și faceți clic pe butonul **Ștergere** corespunzător. Deși puteți elimina adresa implicită a locației de actualizare, acest lucru nu este recomandat.

6.2.2. Antimalware

Modulul Antimalware protejează sistemul contra tuturor tipurilor de malware (viruși, troieni, aplicații spion, rootkit-uri, adware și așa mai departe). Protecția se împarte în două categorii:

- Scanare la acces: previne pătrunderea în sistem a noilor amenințări de programe periculoase.
- Scanare la cerere: permite detectarea și îndepărtarea programelor periculoase care există deja în sistem.

Atunci când detectează un virus sau un alt cod periculos, Endpoint Security va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original. Această operațiune este denumită dezinfectare. Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a izola infecția. Atunci când sunt în carantină, virușii sunt inofensivi deoarece nu pot fi executați sau citiți.

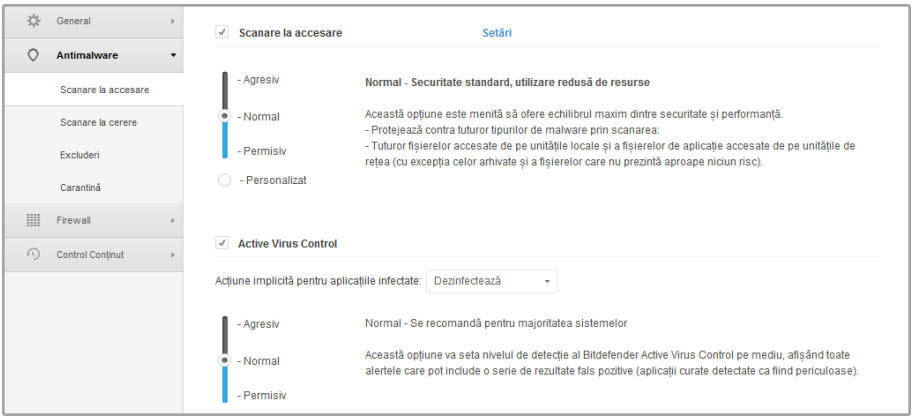
Utilizatorii avansați pot configura excepțiile de la scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate.

Setările sunt organizate în următoarele secțiuni:

- Scanare la accesare
- Scanare la cerere
- Excluderi
- Carantină

Scanare la accesare

În această secțiune puteți configura componentele protecției antimalware în timp real.



Politici pentru calculatoare - Setări la accesare

- Scanare la accesare
- Active Virus Control

Setări scanare la accesare

Scanarea la accesare previne pătrunderea în sistem a noilor amenințări malware prin scanarea fișierelor locale și din rețea atunci când acestea sunt accesate (deschise, mutate, copiat sau executate), a sectoarelor de boot și a eventualelor aplicații nedorite.

Pentru a configura scanarea la accesare:

1. Utilizați caseta de selecție pentru a porni sau opri scanarea la accesare. Dacă opriți scanarea la accesare, calculatoarele vor fi vulnerabile la malware.
2. Pentru o configurare rapidă, faceți clic pe nivelul de securitate care se potrivește cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.
3. Puteți configura setările de scanare în detaliu prin selectarea nivelului de protecție **Personalizat** și făcând clic pe link-ul **Setări**. Se va deschide fereastra de **Setări scanare la accesare**, care conține mai multe opțiuni organizate structurate în două file, **Setări generale** și **Setări avansate**. Opțiunile sunt descrise în continuare de la prima până la ultima secțiune:

   - **Scanare fișiere locale**. Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Preferințele de scanare pot fi configurate separat pentru fișiere locale (stocate pe computerul local) sau fișiere în rețea (stocate pe partajările în rețea). În cazul în care protecția antimalware este instalată pe toate computerele din rețea, puteți dezactiva scanarea fișierelor de rețea, pentru a permite un acces mai rapid la rețea.

     Puteți seta Endpoint Security să scaneze toate fișierele accesate (indiferent de extensia de fișier), numai fișierele aplicației sau extensii de fișiere specifice pe care le considerați periculoase. Scanarea tuturor fișierelor accesate asigură cea mai bună protecție, în timp ce scanarea exclusivă a aplicațiilor poate fi utilizată pentru asigurarea unei performanțe ridicate a sistemului.

     Notă

     Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Lista de tipuri de fișiere de aplicații ” (p. 149).

     Dacă doriți să fie scanate doar extensii specifice, alegeți **Extensii definite de utilizator** din meniu și apoi introduceți extensiile în câmpul de editare și apăsați `Enter` după fiecare extensie.

     Din motive ce țin de performanța sistemului, puteți exclude de la scanare și fișiere de dimensiuni mari. Selectați caseta de selecție **Dimensiune maximă (MB)** și specificați limita de mărime a fișierelor ce vor fi scanate. Folosiți această opțiune cu înțelepciune, deoarece programele periculoase poate afecta și fișiere mai mari.

- **Arhive** Selectați **Scanare în arhive** dacă doriți să activați scanarea la accesare a fișierelor arhivate. Scanarea în interiorul arhivelor este un proces lent și care necesită multe resurse, nefiind recomandată, prin urmare, pentru protecția în timp real. Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoasevă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția la accesare.

  Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:

  – **Dimensiunea maximă a arhivei (MB).** Puteți seta o limită maximă de dimensiune acceptată pentru arhive pentru a fi scanate la accesare. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

  – **Adâncimea maximă a arhivei (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.

- **Diverse.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.

  – **Scanare sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.

  – **Scanare numai de fișiere noi sau modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

  – **Scanare după keyloggers.** Aplicațiile keyloggers înregistrează ceea ce introduceți de pe tastatură și trimit raporte pe Internet către o persoană rău intenționată (hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.

  – **Scanare pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.

- **Acțiuni la scanare.** În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

  – **Acțiune implicită pentru fișierele infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date a Bitdefender. În mod

normal, Endpoint Security poate șterge codul malware din fișierul infestat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

În cazul în care este detectat un fișier infectat, Endpoint Security va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Important
Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

– **Acțiune implicită pentru fișierele suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice. Deoarece B-HAVE este o tehnologie euristică de analiză, Endpoint Security nu vă poate asigura dacă fișierul este într-adevăr virusat sau nu. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

  Atunci când este detectat un fișier suspect, utilizatorilor le se va refuza accesul la acel fișier, pentru a preveni o potențială infecție.

Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți defini două acțiuni pentru fiecare tip de fișier. Următoarele acțiuni sunt disponibile:

Interzice accesul
Interzice accesul la fișiere detectate.

Dezinfectează
Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Ștergere
Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Mută în carantină
Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

Setări Active Virus Control

Bitdefender Active Virus Control este o tehnologie inovatoare de detecție proactivă, care folosește metode euristice avansate pentru a detecta potențiale amenințări în timp real.

Modulul Active Virus Control monitorizează continuu aplicațiile care rulează pe calculatorul dumneavoastră, căutând acțiuni periculoase. Fiecare dintre aceste acțiuni are un anumit

punctaj iar punctajul global este calculat pentru fiecare proces. În cazul în care scorul total pentru un proces atinge un anumit prag, procesul este considerat a fi dăunător. Active Virus Control va încerca automat să dezinfecteze fișierul detectat. Dacă procedura de dezinfecție eșuează, Active Virus Control va șterge fișierul.

Notă
Înainte de a aplica acțiunea de dezinfectare, o copie a fișierului este trimisă în carantină, pentru ca dvs. să puteți recupera fișierul mai târziu, în cazul unui rezultat fals pozitiv. Acțiunea poate fi configurată folosind opțiunea **Copiere fișiere în carantină înaintea aplicării acțiunii de dezinfectare** din fila **Carantină** a setărilor politicii. Această opțiune este activată implicit în modelul politicii.

Notă
Pentru mai multe informații, vizitați site-ul nostru și consultați whitepaper privind Active Virus Control.

Pentru a configura Active Virus Control:

1. Utilizați caseta de selecție pentru a activa sau opri Active Virus Control. Dacă opriți Active Virus Control, computerele vor fi vulnerabile la programele periculoase necunoscute.
2. Acțiunea implicită pentru aplicațiile infectate detectate de Active Virus Control este dezinfectarea. Pentru a seta o altă acțiune implicită, folosiți meniul disponibil.
3. Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

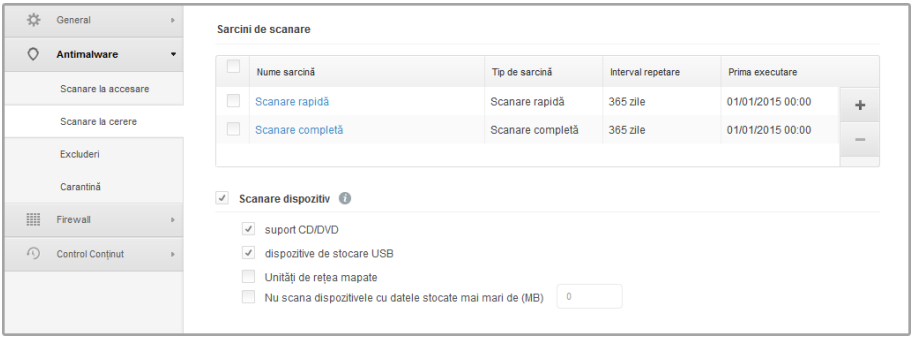
   Notă
   După ce setați un nivel de protecție superior, Active Virus Control va necesita mai puține semne de comportament tipic malware pentru a raporta un anumit proces. Acest lucru va contribui la raportarea unui număr mai mare de aplicații și, în același timp, la o probabilitate sporită de false pozitive (aplicații legitime detectate ca fiind nocive).

4. Trebuie să creați reguli de excludere pentru aplicațiile utilizate frecvent sau cunoscute pentru a preveni alarmele false (detectarea greșită de aplicații legitime). Accesați secțiunea Excluderi și configurați **regulile AVC/SD pentru excluderi de procese** pentru aplicațiile de încredere.

Politică pentru calculatoare - Opțiunea AVC/IDS de excludere a proceselor

Scanare la cerere

În această secțiune puteți configura sarcini de scanare antimalware, care vor rula în mod regulat pe calculatoarele țintă, în funcție de programul specificat de dvs.



Politici pentru calculatoare - Sarcini de scanare la cerere

Scanarea este efectuată discret, pe fundal. Utilizatorul este informat despre existența unui proces de scanare în curs printr-o singură pictogramă vizibilă în zona de notificare.

Deși nu este obligatoriu, este recomandat să programați rularea unei scanări complete de sistem o dată pe săptămână pe toate calculatoarele. Scanarea calculatoarelor în mod regulat este o măsură de securitate proactivă, care pot ajuta la detectarea și blocarea malware-ului care s-ar putea sustrage caracteristicilor de protecție în timp real.

În afară de scanările periodice, puteți configura și detectarea automată și scanarea mijloacelor externe de stocare.

Administrarea sarcinilor de scanare

Tabelul Scan Tasks vă informează cu privire la sarcinile de scanare existente, furnizând informații importante despre fiecare dintre ele:

- Numele și tipul sarcinii.
- Program pe baza căruia sarcina rulează regulat (recurență).
- Momentul când a fost rulată sarcina pentru prima dată.

Există două sarcini de scanare implicite de sistem pe care le puteți configura pentru a rula după cum este necesar:

- **Scanare rapidă** utilizează scanarea în cloud pentru a detecta malware-ul care rulează pe sistem. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.
- **Scanare completă** verifică întregul calculator pentru identificarea tuturor tipurilor de malware care îi amenință siguranța, cum ar fi virușii, aplicațiile spion, adware, rootkit-uri și altele.

Opțiunile de scanare pentru sarcinile de scanare implicite sunt preconfigurate și nu le puteți modifica.

Pe lângă sarcinile de scanare implicite (care nu pot fi șterse sau duplicate), aveți posibilitatea de a crea câte sarcini de scanare personalizate doriți. Sarcina de scanare personalizată vă permite să alegeți locațiile specifice care trebuie scanate și să configurați opțiunile de scanare.

Pentru a crea și a configura o nouă sarcină de scanare personalizată, faceți clic pe butonul + **Adăugare** din partea dreaptă a tabelului. Pentru a modifica setările unei sarcini de scanare existente, faceți clic pe numele sarcinii respective. Consultați următorul subiect pentru a afla modalitatea de configurare a setărilor sarcinii.

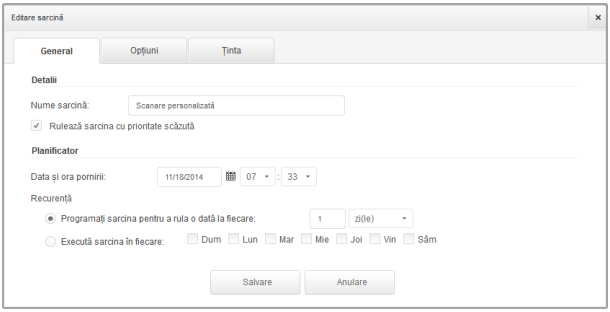
Pentru a elimina o sarcină din listă, selectați sarcina și faceți clic pe butonul − **Ștergere** din partea dreaptă a tabelului.

Configurarea sarcinilor de scanare

Setările sarcinii de scanare sunt organizate în trei file:

- **General**: se stabilește numele sarcinii și graficul de execuție.
- **Opțiuni**: se alege un profil de scanare pentru configurarea rapidă a setărilor de scanare și se definesc setările de scanare pentru o scanare personalizată.
- **Țintă**: se selectează fișierele și folderele care urmează a fi scanate.

Opțiunile sunt descrise în continuare de la prima până la ultima secțiune:



Politici pentru calculatoare - Configurarea setărilor generale ale sarcinilor de scanare la cerere

- **Detalii.** Alegeți un nume sugestiv pentru sarcină care să vă ajute la identificarea cu ușurință la ce se referă. Atunci când alegeți un nume, luați în considerare obiectivul sarcinii de scanare și, eventual, setările de scanare.
- **Planificator.** Folosiți opțiunile de planificare pentru a configura programul de scanare. Puteți seta ca scanarea să ruleze la fiecare câteva ore, zile sau săptămâni, începând cu o anumită dată și oră.

  Rețineți faptul că calculatoarele trebuie să fie pornite când este stabilită programarea. Scanarea programată nu va funcționa conform programului în cazul în care computerul este oprit, în hibernare sau în modul sleep, sau în cazul în care nu există niciun utilizator conectat. În astfel de situații, scanarea va fi amânată până data viitoare.

  Notă
  Scanare programată va rula la ora locală a punctului terminus. De exemplu, în cazul în care scanarea programată este setată să pornească la ora 18:00, ăi punctul terminus se află pe un fus orar diferit față de Control Center, scanarea va începe la ora 18:00 (ora punctului terminus).

- **Opțiuni de scanare.** Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

  În funcție de profilul selectat, opțiunile de scanare din secțiunea **Setări** sunt configurate automat. Cu toate acestea, dacă doriți, le puteți configura detaliat. În acest scop, selectați caseta de bifare **Personalizat** și mergeți la secțiunea **Setări**.

Sarcină de scanare calculatoare

- **Tipuri de fișiere.** Folosiți aceste opțiuni pentru a specifica tipurile de fișiere pe care doriți să le scanați. Puteți seta Endpoint Security să scaneze toate fișierele (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase. Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

  Notă

  Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Pentru mai multe informații, consultați capitolul „Lista de tipuri de fișiere de aplicații ” (p. 149).

  Dacă doriți să fie scanate doar extensii specifice, alegeți **Extensii definite de utilizator** din meniu și apoi introduceți extensiile în câmpul de editare și apăsați `Enter` după fiecare extensie.

- **Arhive.** Arhivele cu fișiere infestate nu sunt o amenințare directă pentru securitatea sistemului. Programele periculoase pot afecta sistemul numai dacă fișierul infestat este extras din arhivă și executat fără ca protecția în timp real să fie activată. Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

  Notă

  Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

  – **Scanare în arhive.** Selectați această opțiune dacă doriți să scanați fișierele arhivate, pentru identificarea de malware. Dacă decideți să utilizați această opțiune, puteți configura următoarele opțiuni de optimizare:

    - **Limitare dimensiune arhivă la (MB).** Puteți seta o dimensiune limită acceptată pentru arhivele care vor fi scanate. Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

- **Adâncime maximă arhivă (niveluri).** Selectați caseta de bifare corespunzătoare și alegeți adâncimea maximă a arhivei din meniu. Pentru performanțe superioare, alegeți cea mai mică valoare; pentru protecție maximă, alegeți cea mai mare valoare.

– **Scanare arhive de e-mail.** Selectați această opțiune dacă doriți să activați scanarea fișierelor atașate la mesajele e-mail și bazele de date e-mail, inclusiv format de fișiere de tipul .eml, .msg, .pst, .dbx, .mbx, .tbb și altele.

Notă
Scanarea arhivei e-mail necesită numeroase resurse și poate afecta performanțele sistemului.

- **Diverse.** Selectați casetele de bifare corespunzătoare pentru a activa opțiunile de scanare dorite.
  - **Scanare sectoare de boot.** Scanează sectoarele de boot ale sistemului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.
  - **Scanează regiștrii.** Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
  - **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.
  - **Scanare după keyloggers.** Selectați această opțiune pentru a scana software-urile de tip keylogger.
  - **Scanează memoria.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului.
  - **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe calculator.
  - **Scanează doar fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
  - **Scanare pentru aplicații potențial nedorite (PUA).** O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea

de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.

- **Acțiuni.** În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:
  - **Acțiune implicită pentru fișierele infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date a Bitdefender. În mod normal, Endpoint Security poate șterge codul malware din fișierul infestat și poate reconstitui fișierul inițial. Această operațiune este cunoscută sub denumirea de dezinfectare.

    În cazul în care este detectat un fișier infectat, Endpoint Security va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

    Important
    Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

  - **Acțiune implicită pentru fișierele suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice. Deoarece B-HAVE este o tehnologie euristică de analiză, Endpoint Security nu vă poate asigura dacă fișierul este într-adevăr virusat sau nu. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

    Sarcinile de scanare sunt configurate implicit să ignore fișierele suspecte. Ar putea fi util să modificați sarcina implicită, pentru a trece fișierele suspecte sub carantină. Fișierele sub carantină sunt transmise regulat spre analiză la Laboratoarele Bitdefender. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

  - **Acțiune implicită pentru rootkit-uri.** Rootkit-urile reprezintă aplicații specializate utilizate pentru ascunderea fișierelor de sistemul de operare. Deși nu sunt periculoase, rootkit-urile sunt adesea utilizate pentru ascunderea programelor periculoase sau pentru a disimula prezența unui intrus în sistem.

    Rootkit-urile și fișierele ascunse detectate sunt ignorate implicit.

  Deși nu este recomandat, puteți modifica acțiunile implicite. Puteți preciza o a doua acțiune de aplicat în cazul în care prim eșuează, precum și acțiuni diferite pentru fiecare categorie. Alegeți din meniurile corespunzătoare prima și a doua acțiune de aplicat pentru fiecare tip de fișier detectat. Următoarele acțiuni sunt disponibile:

  Nicio acțiune
  Nu se vor lua niciun fel de măsuri împotriva fișierelor detectate. Aceste fișiere vor fi doar afișate în jurnalul de scanare.

Dezinfectează
Elimină codul periculos din fișierele infectate. Se recomandă să mențineți întotdeauna această acțiune ca fiind prima aplicată asupra fișierelor infestate.

Ștergere
Ștergeți fișierele detectate de pe disc, fără nicio avertizare. Se recomandă să evitați această acțiune.

Mută în carantină
Mutați fișierele detectate din locația curentă, în folderul de carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Fișierele în carantină pot fi gestionate de pe pagina Carantină a consolei.

- **Țintă scanare.** Adăugați la listă de toate locațiile care doriți să fie scanate pe calculatoarele țintă.

  Pentru a adăuga un nou fișier sau un folder care să fie scanat:

  1. Selectați o locație predefinită din meniul derulant sau introduceți **Căi specifice** pe care doriți să le folosiți.
  2. Specificați calea către obiectul de scanat în câmpul de editare.
     - Dacă ați ales o locație predefinită, completați calea, după caz. De exemplu, pentru a scana integral folderul `Program Files`, este suficient să selectați locația predefinită corespunzătoare din meniul derulant. Pentru a scana un anumit folder din `Program Files`, trebuie să completați calea adăugând o bară oblică inversă (\) și denumirea folderului.
     - Dacă ați selectat **Căi specifice**, introduceți calea completă către obiectul de scanat. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.
  3. Faceți clic pe butonul + **Adăugare** corespunzător.

  Pentru a edita o locație existentă, faceți clic pe aceasta. Pentru a șterge o locație din listă, deplasați cursorul peste aceasta și faceți clic pe butonul − **Ștergere** corespunzător.

- **Excluderi.** Puteți utiliza excepțiile definite în secțiunea **Antimalware > Excluderi** a politicii curente au puteți defini excluderile personalizate pentru sarcina de scanare curentă. Pentru detalii referitoare la excepții, consultați „Excluderi” (p. 96).

Scanare dispozitiv

Puteți configura Endpoint Security pentru a detecta automat și scana dispozitivele de stocare externe atunci când acestea sunt conectate la calculator. Unitățile detectate fac parte din următoarele categorii:

- CD-uri/DVD-uri
- unități de stocare pe USB, cum ar fi memoriile flash sau hard discurile externe

- Unități de rețea mapate
- Dispozitive cu mai mult de o anumită sumă de date stocate.

Scanările dispozitivului încercă automat să dezinfecteze fișierele detectate ca fiind infectate sau să le mute în carantină dacă dezinfectarea nu este posibilă. Rețineți faptul că nu poate fi aplicată nici o acțiune fișierelor infectate detectate pe CD-uri/DVD-uri sau pe unități mapate de rețea care permit acces doar în citire.

Notă
În timpul scanării dispozitivului, utilizatorul poate accesa orice date de pe dispozitiv.

Dacă sunt activate pop-up-urile de alertă în secțiunea **General > Afișare**, utilizatorul este întrebat dacă să scaneze dispozitivul detectat în loc de a porniri scanarea automat.

Atunci când este pornită scanarea unui dispozitiv:

- O notificare de tip pop - up informează utilizatorul cu privire la scanarea dispozitiv, cu condiția ca notificările de tip pop-up să fie activate în secțiunea **General > Afișare**.
- O pictogramă de scanare apare în bara de sistem. Utilizatorul poate face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

După finalizarea scanării, utilizatorul trebuie să verifice amenințările detectate, dacă este cazul.

Selectați opțiunea **Scanare dispozitive** pentru a activa detectarea și scanarea automată a dispozitivelor de stocare. Pentru a configura scanarea dispozitivului individual pentru fiecare tip de dispozitiv, folosiți următoarele opțiuni:

- **suport CD/DVD**
- **dispozitive de stocare USB**
- **Unități de rețea mapate**
- **Nu scana dispozitivele cu datele stocate mai mari de (MB)**. Utilizați această opțiune pentru a evita automat scanarea unui dispozitiv detectat în cazul în care cantitatea de date stocate depășește dimensiunea specificată. Introduceți limita de dimensiune (în megabytes) în câmpul corespunzător. Zero semnifică neimpunerea nici unei restricții de dimensiuni.

Notă
Această opțiune se aplică exclusiv în cazul CD-urilor/DVD-urilor și a unităților de stocare USB.

Excluderi

În această secțiune puteți configura regulile de excludere scanare. Excluderile se pot aplica la scanarea la accesare sau la solicitarea de scanare, sau ambelor. Pe baza obiectului excluderii, există patru tipuri de excluderi:

Politici pentru calculatoare - Excluderi antimalware

- **Excluderi de fișiere:** doar fișierul specificat este exclus de la scanare.
- **Excluderi de foldere:** sunt excluse de la scanare toate fișierele din interiorul directorului specificat și toate subdirectoarele sale.
- **Excluderi de extensii:** - toate fișierele având extensia specificată sunt excluse de la scanare.
- **Excluderi de procese:** orice obiect accesat de către procesul exclus, este și el exclus de la scanare. Puteți configura și excepțiile de la proces pentru tehnologiile Active Virus Control șiSistem de Detectare a Intruziunilor.

Important

Excepțiile de la scanare vor fi utilizate în circumstanțe speciale sau conform recomandărilor Microsoft sau Bitdefender. Pentru o listă actualizată a excluderilor recomandate de Microsoft, vă rugăm consultați acest articol. Dacă aveți un fișier cu un test EICAR pe care îl folosiți periodic pentru a testa protecția antimalware, este recomandat să-l excludeți de la scanarea la acces.

Utilizați caseta de selecție **Activare excepții** pentru a activa sau dezactiva excepțiile.

Pentru a configura o regulă de excludere:

1. Selectați tipul de excludere din meniu.
2. În funcție de tipul de excludere, specificați obiectul care trebuie exclus, după cum urmează:
   - **Excluderi de extensii.** Specificați una sau mai multe extensii de fișiere care vor fi excluse de la scanare, separându-le cu punct și virgulă ";". Puteți introduce extensii,

cu sau fără punctul care le precede. De exemplu, introduceți `txt` pentru a exclude fișierele text.

Notă
Înainte de a exclude extensii, documentați-vă pentru a vedea care sunt vizate de obicei de programe periculoase și care nu.

- **Excluderi de fișiere, directoare și procese.** Specificați calea către obiectul exclus de pe calculatoarele țintă.
  a. Alegeți din meniu o locație prestabilită sau opțiunea **Căi specifice**.
  b. Dacă ați ales o locație predefinită, completați calea, după caz. De exemplu, pentru a exclude întregul director `Program Files`, este suficient să selectați locația corespunzătoare predefinită din meniu. Pentru a exclude un anumit director din `Program Files`, trebuie să completați calea prin adăugarea unei bare oblice inverse (\) și numele directorului. Pentru excluderi de proces, trebuie să adăugați și numele fișierului executabil al aplicației.
  c. Dacă ați ales **Căi specifice**, introduceți calea completă a obiectului care urmează a fi exclus. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.

3. Selectați tipurile de scanare la care se va aplica regula. Unele excluderi pot fi relevante doar pentru scanare la accesare, altele doar pentru scanarea la cerere, în timp ce altele pot fi recomandate pentru ambele. Excluderile de proces pot fi configurate pentru scanarea la accesare și pentru tehnologiile Active Virus Control șiSistem de Detectare a Intruziunilor.

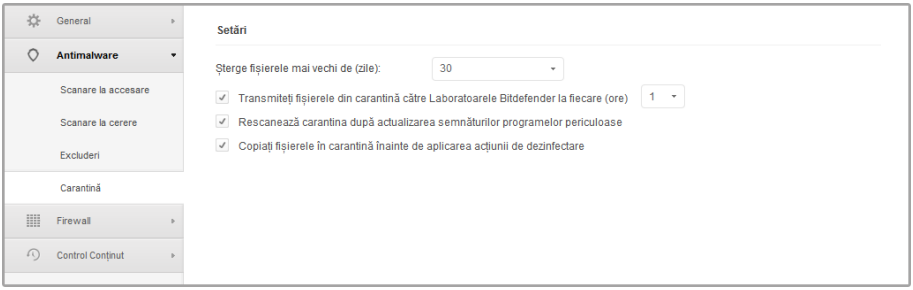
Notă
Vă rugăm să rețineți că excluderile de scanare la cerere nu se vor aplica scanării contextuale. Scanarea contextuală este inițiată făcând clic-dreapta pe un fișier sau director și selectând **Scanare cu Endpoint Security de la Bitdefender**.

4. Faceți clic pe butonul + **Adăugare**. Noua regulă va fi adăugată în listă.

Pentru a elimina o regulă din listă, faceți clic pe butonul − **Ștergere**.

Carantină

În această secțiune puteți configura setările de carantină.



Politici pentru calculatoare - Carantină

Puteți seta Endpoint Security să realizeze următoarele acțiuni în mod automat:

- **Șterge fișierele mai vechi de (zile).** Implicit, fișierele aflate în carantină de mai mult de 30 de zile sunt șterse automat. Dacă doriți să schimbați acest interval, alegeți o altă opțiune din meniu.
- **Transmiteți fișierele din carantină către Laboratoarele Bitdefender la fiecare (ore).** Păstrați această opțiune selectată pentru de a trimite automat fișierele din carantină la Laboratoarele Bitdefender. Puteți edita intervalul de timp când sunt trimise fișierele aflate în carantină (o oră în mod implicit). Fișierele mostră vor fi analizate de către cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

  În mod implicit, fișierele aflate în carantină sunt trimise automat la Laboratoarele Bitdefender din oră în oră. Dacă doriți să schimbați acest interval, alegeți o altă opțiune din meniu.
- **Rescanează carantina după actualizarea semnăturilor programelor periculoase.** Păstrați această opțiune selectată pentru a scana automat fișierele aflate în carantină după fiecare actualizare a semnăturilor de malware. Fișierele curățate sunt mutate automat în locația lor originală.
- **Copiază fișierele în carantină înainte de aplicarea acțiunii de dezinfectare.** Selectați această opțiune pentru a preveni pierderea de date în caz de pozitive false și copiați fiecare fișier detectat ca infectat în carantină înainte de a aplica acțiunea de dezinfectare. Ulterior puteți recupera fișiere legitime din pagina **Carantină**.

6.2.3. Firewall

Firewallul vă protejează calculatorul de tentativele de conectare neautorizate, atât la intrare, cât și la ieșire.

Funcționalitatea firewall-ului se bazează pe profile de rețea. Profilele se bazează pe niveluri de încredere, care trebuie definite pentru fiecare rețea.

De fiecare dată când se creează o nouă conexiune, Firewall-ul o detectează și compară informațiile adaptorului de conexiune cu informațiile de la profilele existente, aplicând profilul corect. Pentru informații detaliate cu privire la modul în care sunt aplicate profilele, consultați secțiunea setări de rețea.

Setările sunt organizate în următoarele secțiuni:

- General
- Setări
- Reguli

General

În această secțiune puteți activa sau dezactiva firewallul Bitdefender și puteți configura setările generale.

Politici pentru calculatoare - Setări generale firewall

- **Firewall.** Utilizați caseta de selecție pentru a activa sau opri Firewall. Dacă dezactivați protecția firewall, computerele vor fi vulnerabile la atacurile de rețea și de pe Internet.
- **Blocare scanare porturi.** Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculator. Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculator.
- **Permite Internet Connection Sharing (ICS).** Selectați această opțiune pentru a seta firewall-ul pentru a permite traficul Internet Connection Sharing.

> **Notă**
> Această opțiune nu activează automat ICS pe sistemul utilizatorului.

- **Monitorizare conexiuni Wi-Fi.** Endpoint Security poate informa utilizatorii conectați la o rețea Wi-Fi atunci când un nou computer devine membru al rețelei. Selectați această opțiune pentru a afișa astfel de notificări pe ecranul utilizatorului.

- **Nivel detaliere jurnal.** Endpoint Security păstrează un jurnal al evenimentelor referitoare la activitatea modulului Firewall (activare/dezactivare firewall, blocare trafic, modificare setări) sau generate de activitățile detectate de firewall (scanare porturi, blocare tentative de conectare sau trafic conform regulilor). Alegeți o opțiune din **Log verbosity level** tpentru a specifica câte informații va include registrul.
- **Sistem de detecție a intruziunilor.** Sistem de Detectare a Intruziunilor (SDI) monitorizează sistemul pentru activități suspecte (de exemplu, încercările neautorizate de a modifica fișierele Bitdefender, injecții DLL, încercări de utilizare keyloggere etc.).

  Pentru a configura sistemul de detectare a intruziunilor:

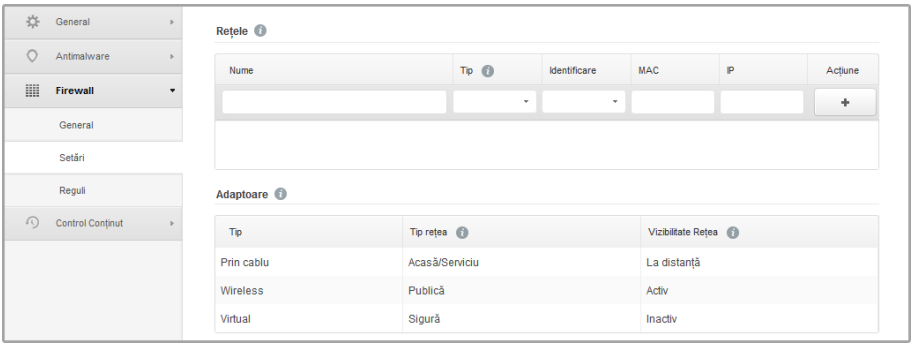
  1. Utilizați caseta de selectare pentru a activa sau opri sistemul de detecție a intruziunilor.
  2. Faceți clic pe nivelul de securitate care corespunde cel mai bine necesităților dumneavoastră (Agresiv, Normal sau Permisiv). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea.

  Pentru a preveni cazul în care o aplicație legitimă este detectată de Sistemul de detectare a intruziunilor, adăugați o **regulă AVC/IDS pentru excluderi de procese** pentru respectiva aplicație în secțiunea **Antimalware > Excluderi**.

Setări

Firewall-ul aplică în mod automat un profil bazat pe tipul de rețea. Puteți specifica profilurile generice care urmează să fie aplicate în funcție de tipul de adaptor și, de asemenea, puteți specifica profile individuale pentru rețelele companiei dvs. Setările sunt organizate în următoarele tabele:

- Rețele
- Adaptoare



Politici pentru calculatoare - Setări firewall

Setări de rețea

Pentru ca firewall-ul să funcționeze corect, administratorul trebuie să definească rețelele care vor fi gestionate în tabelul **Networks** table. Câmpurile din tabelul **Rețele** table sunt descrise după cum urmează:

- **Nume.** Un nume după care administratorul poate recunoaște rețeaua din listă.
- **Tip.** Selectați din meniu tipul de profil alocat rețelei.

  Endpoint Security aplică în mod automat una din cele patru profiluri firewall pentru fiecare conexiune de rețea detectată pentru a defini opțiunile de bază de filtrare a traficului. Profilurile firewall sunt:

  - Rețea **Sigură**. Dezactivează firewallul pentru adaptorul respectiv.
  - Rețea **Acasă/Serviciu**. Permite tot traficul către și de la calculatoarele din rețeaua locală.
  - Rețea **Publică**. Tot traficul este filtrat.
  - Rețea **Nesigură**. Blochează complet traficul de rețea și Internet prin adaptorul respectiv.
- **Identificare.** Selectați din meniu metoda prin care rețeaua va fi identificată prin Endpoint Security. Rețelele pot fi identificate prin trei metode: **DNS**, **Gateway** și **Rețea**.
- **MAC.** Utilizați acest câmp pentru a specifica adresa MAC a unui server DNS specific.

  Notă
  Acest câmp este obligatoriu dacă este selectată metoda de identificare DNS.

- **IP.** Utilizați acest câmp pentru a defini anumite adrese IP într-o rețea. Puteți folosi, de asemenea, o mască pentru a defini o întreagă sub-rețea.

După ce ați definit o rețea, faceți clic pe butonul **Adăugare** din partea dreaptă a tabelului pentru a o adăuga la listă.

Setările adaptoarelor

În cazul în care este detectată o rețea care nu este definită în tabelul **Rețele**, Endpoint Security detectează tipul de adaptor de rețea și aplică un profil corespunzător conexiunii. Câmpurile din tabelul **Adaptoare** sunt descrise după cum urmează:

- **Tip.** Afișează tipul de adaptoare de rețea. Endpoint Security poate detecta trei tipuri de adaptoare predefinite: **Prin cablu**, **Wireless** și **Virtual** (Virtual Private Network).
- **Tip rețea.** Descrie profilul de rețea alocat unui tip anume de adaptor. Tipurile de rețele sunt descrise în secțiunea setări de rețea. Dacă faceți clic pe câmpul tip de rețea puteți să schimbați setarea. Dacă selectați **Lasă Windows să decidă**, pentru orice nouă

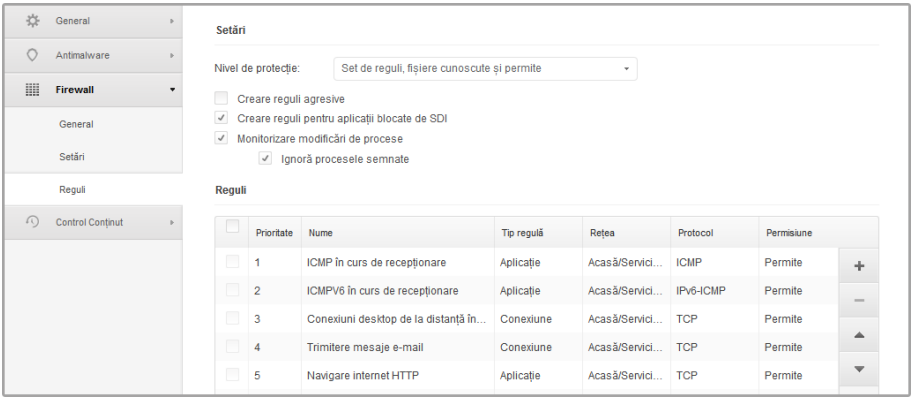
conexiune de rețea detectată după aplicarea politicii, Endpoint Security aplică un profil firewall bazat pe clasificarea rețelei în Windows, ignorând setările din tabelul **Adaptoare**.

În cazul în care detectarea bazată pe Windows Network Manager eșuează, se încearcă o detectare de bază. Se utilizează un profil generic în care tipul de rețea este considerat **Publică** iar setările ascunse sunt setate pe **Activ**. Dacă adresa IP a domeniului în care se găsește computerul se află într-una din rețelele asociate cu adaptorul, apoi nivelul de încredere este considerat **Acasă/Serviciu** și setările ascunse sunt setate pentru **La distanță**. În cazul în care calculatorul nu este într-un domeniu, această condiție nu se aplică.

- **Mod ascuns .** Ascunde calculatorul față de aplicații periculoase și de hackeri din rețea sau din Internet. Configurează Stealth Mode după cum este necesar pentru fiecare tip de adaptor selectând una dintre următoarele opțiuni:
  - **Activ.** Computerul nu poate fi detectat nici din rețeaua locală, nici de pe internet.
  - **Inactiv.** Oricine din rețeaua locală sau de pe Internet poate da ping și detecta calculatorul.
  - **La distanță.** Calculatorul nu poate fi detectat din Internet. Oricine din rețeaua locală poate da ping și detecta calculatorul.

Reguli

În această secțiune puteți configura accesul aplicației la rețea și regulile de trafic de date, puse în aplicare de către firewall. Rețineți că setările disponibile se aplică numai pentru **Acasă/Serviciu** și profilele de firewall de tip **Publică** .



Politici pentru calculatoare - Setări reguli firewall

Setări

Puteți configura următoarele setări:

- **Nivel de protecție.** Nivelul de protecție selectat definește logica de luare a deciziilor firewall folosită atunci când aplicațiile solicită acces la servicii de rețea și de Internet. Sunt disponibile următoarele opțiuni:

  Set de reguli și permite
  Se aplică regulile firewall existente și permite în mod automat toate celelalte încercări de conectare. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli și întreabă
  Se aplică regulile firewall existente și cere utilizatorului acțiune pentru toate celelalte încercări de conectare. Pe ecranul utilizatorului apare o fereastră de alertă cu informații detaliate despre încercarea de conectare necunoscută. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli și respinge
  Se aplică regulile firewall existente și se respinge în mod automat toate celelalte încercări de conectare. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli, fișiere cunoscute și permite
  Se aplică regulile firewall existente, se permite în mod automat tentativele de conexiune realizate de aplicații cunoscute și se solicit[utilizatorului acțiune pentru toate celelalte încercări de conectare necunoscute. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli, fișiere cunoscute și întreabă
  Se aplică regulile firewall existente, se permit în mod automat tentativele de conectare realizate de aplicații cunoscute și în mod automat se resping toate celelalte încercări de conectare necunoscute. Pe ecranul utilizatorului apare o fereastră de alertă cu informații detaliate despre încercarea de conectare necunoscută. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Set de reguli, fișiere cunoscute și respinge
  Se aplică regulile firewall existente, se permit în mod automat tentativele de conectare realizate de aplicații cunoscute și în mod automat se resping toate celelalte încercări de conectare necunoscute. Pentru fiecare nouă încercare de conectare, este creată o regulă și adăugată la setul de reguli.

  Notă
  Fișierle cunoscute, reprezintă o colecție mare de aplicații sigure, de încredere, care sunt compilate și întreținute în mod continuu de către Bitdefender.

- **Creare reguli agresive.** Fiind selectată această opțiune, firemwall-ul va crea reguli pentru fiecare proces diferit care deschide aplicația care necesită acces la rețea sau Internet.

- **Creare reguli pentru aplicații blocate de SDI.** Fiind selectată această opțiune, firewall-ul va crea automat o regulă **Interzice** de fiecare dată când Sistemul de detectare a intruziunilor blochează o aplicație.
- **Monitorizare modificări de procese.** Selectați această opțiune dacă doriți ca fiecare aplicație care încearcă să se conecteze la Internet să fie verificată dacă a fost modificată de la momentul adăugării regulii care controlează accesul ei la Internet. În cazul în care aplicația a fost modificată, va fi creată o nouă regulă în funcție de nivelul de protecție existent.

  Notă

  De obicei, aplicațiile sunt modificate de actualizări. Dar, există riscul ca acestea să fie modificate de aplicații periculoase, în scopul infectării calculatorului local și a altor stații din rețea.

  Aplicațiile semnate sunt presupuse a fi sigure și au un grad sporit de securitate. Puteți selecta **Ignoră procesele semnate** pentru a permite automat conectarea aplicațiilor semnate la Internet.

Reguli

Tabelul de reguli enumeră regulile firewall existente, furnizândinformații importante despre fiecare dintre ele:

- Numele regulii sau aplicația la care se referă.
- Protocolul căruia i se aplică regula.
- Acțiunea prevăzută de regulă (permite sau respinge accesul pachetelor).
- Acțiunile pe care le puteți întreprinde cu privire la regulă.
- Prioritatea regulii.

Notă

Acestea sunt regulile de firewall impuse în mod explicit de politică. Ca urmare a aplicării setărilor firewall pot fi configurate reguli suplimentare pe calculatoare.

O serie de reguli implicite de firewall vă ajută să permiteți sau să refuzați cu ușurință tipuri de trafic populare. Alegeți opțiunea dorită din meniul **Permisiune**.

ICMP / ICMPv6 în curs de recepționare
Permite sau respinge mesajele ICMP / ICMPv6. Mesajele ICMP sunt folosite adesea de hackeri pentru a lansa atacuri asupra rețelelor computerului. În mod implicit, acest tip de trafic nu este permis.

Conexiuni desktop de la distanță în curs de recepționare
Permite sau respinge accesul altor computere la conexiunile desktop de la distanță. În mod implicit, acest tip de trafic este permis.

Trimitere mesaje e-mail
Permite sau respinge trimiterea de mesaje e-mail prin SMTP. În mod implicit, acest tip de trafic este permis.

Navigare internet HTTP
Permite sau respinge navigare web HTTP. În mod implicit, acest tip de trafic este permis.

Imprimarea în altă rețea
Permite sau refuză accesul la imprimante într-o altă rețea locală. În mod implicit, acest tip de trafic nu este permis.

Trafic Windows Explorer pe HTTP / FTP
Permite sau respinge traficul HTTP sau FTP de la Windows Explorer. În mod implicit, acest tip de trafic nu este permis.

În afară de regulile implicite, puteți crea reguli de firewall suplimentare pentru alte aplicații instalate pe calculatoare. Însă această configurație este rezervată administratorilor cu abilități dezvoltate de networking.

Pentru a crea și a configura o nouă regulă, faceți clic pe butonul + **Adăugare** din partea dreaptă a tabelului. Pentru mai multe informații consultați următorul subiect.

Pentru a elimina o reguă din listă, faceți clic pe butonul corespunzător − **Ștergere** din partea dreaptă a tabelului.

Notă
Nu puteți șterge sau modifica regulile implicite de firewall.

Configurarea Regulilor personalizate

Puteți configura două tipuri de reguli firewall:

- **Reguli bazate pe aplicații.** Aceste reguli se aplică software-uilor specifice care se găsesc pe calculatoarele client.
- **Reguli bazate pe conexiune.** Aceste reguli se aplică la orice aplicație sau serviciu care utilizează o conexiune specifică.

Pentru a crea și configura o nouă regulă, faceți clic pe butonul + **Adăugare** din partea dreaptă a tabelului și selectați din meniu tipul de regulă dorit. Pentru a edita o regulă existentă, faceți clic pe numele regulii.

Pot fi configurate următoarele setări:

- **Nume regulă.** Introduceți numele cu care regula va fi introdusă în tabelul de reguli (de exemplu, numele aplicației la cere se aplică de regulă).
- **Calea către aplicație** (numai pentru regulile bazate pe aplicație). Trebuie să specificați calea către fișierul executabil al aplicației de pe calculatoarele țintă.

  - Alegeți din meniu o locație prestabilită și completați calea după cum este necesar. De exemplu, pentru o aplicație instalată în directorul `Program Files`, selectați `%ProgramFiles%` și completați calea prin adăugarea unei bare oblice inversă (\) și numele directorului aplicației.
  - Introduceți calea completă în câmpul editabil. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.

- **Linie de comandă** (numai pentru regulile bazate pe aplicații). Dacă doriți ca regula să fie aplicată doar atunci când aplicația specificată este deschisă cu o anumită comandă în linia de comandă Windows, introduceți respectiva comandă în câmpul corespunzător. În caz contrar, lăsați-l necompletat.
- **MD5-ul aplicației** (numai pentru regulile bazate pe aplicație). Dacă doriți ca regula să verifice integritatea datelor din fișierul aplicației bazat pe codul hash MD5, introduceți-l în câmpul editabil. Dacă nu este cazul, lăsați acest câmp necompletat.
- **Adresă locală.** Specificați adresa IP locală și portul local cărora li se aplică regula. Dacă aveți mai multe adaptoare de rețea, puteți debifa căsuța **Oricare** și introduce o anumită adresă IP. De asemenea, pentru a filtra conexiunile pe un anumit port sau o gamă de porturi, debifați caseta de selecție **Oricare** și introduceți portul dorit sau gama de porturi în câmpul corespunzător.
- **Adresă de la distanță.** Specificați adresa IP și portul la distanță cărora li se aplică regula. Pentru a filtra traficul către și de la un anumit calculator, debifați căsuța **Oricare** și introduceți adresa IP a acestuia.
- **Aplicați regula numai pentru calculatoare conectate direct.** Puteți filtra accesul bazat pe adresa Mac.
- **Protocol.** Selectați protocolul IP căruia i se aplică regula.
  - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
  - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
  - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.
  - Dacă doriți ca regula să se aplice unui anumit protocol, selectați protocolul din meniul **Altul**.

    Notă

    Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA). Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa http://www.iana.org/assignments/protocol-numbers.

- **Direcție.** Selectați direcția de trafic căreia i se aplică regula.

Direcție	Description
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

- **Versiune IP.** Selectați versiunea IP (IPv4, IPv6 sau ambele) căreia i se aplică regula.
- **Rețea.** Selectați tipul de rețea pentru care se aplică regula.
- **Permisiune.** Selectați una dintre permisiunile disponibile:

Permisiune	Description
Permite	Aplicației specificate îi va fi permis accesul la rețea / Internet în condițiile specificate.
Interzice	Aplicației specificate îi va fi refuzat accesul la rețea / Internet în condițiile specificate.

Faceți clic pe **Salvare** pentru a adăuga regula.

Pentru regulile create de dvs., folosiți săgețile din partea dreaptă a tabelului pentru a seta prioritatea fiecărei reguli. Regula cu prioritatea mai mare va fi mai aproape de partea de sus a listei.

6.2.4. Control Conținut

Folosiți modulul Content Control pentru a vă configura preferințele în ceea ce privește filtrarea conținutului și protecția datelor pentru activitatea utilizatorului, inclusiv navigarea pe internet, e-mail și aplicații software. Puteți restricționa sau permite accesul web și folosirea aplicației, configura scanarea traficului, regulile antiphishing și de protecție a datelor. Vă rugăm să rețineți că setările configurate pentru Control Conținut se aplică tuturor utilizatorilor care se autentifică pe calculatoarele țintă.

Setările sunt organizate în următoarele secțiuni:

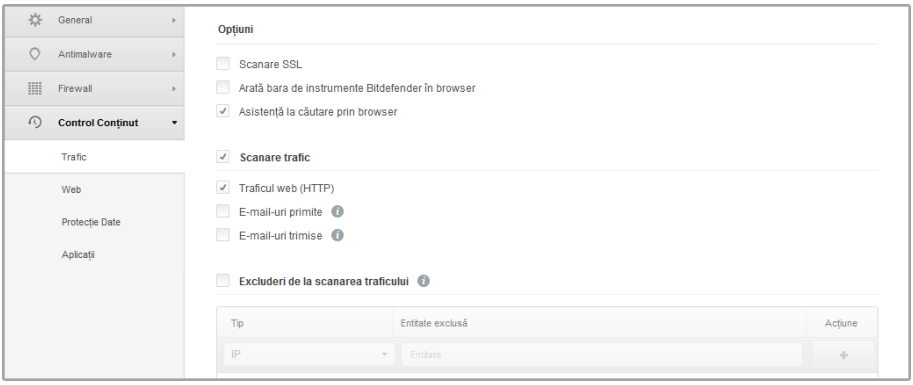
- Trafic
- Web
- Protecție Date
- Aplicații

Trafic

Configurați preferințele de securitate a traficului folosind setările din următoarele secțiuni:

- Opțiuni
- Scanare trafic

- Excluderi de la scanarea traficului



Politici pentru calculatoare - Control conținut - Trafic

Opţiuni

- **Scanează SSL**. Selectați această opțiune dacă doriți ca traficul web al Secure Sockets Layer (SSL) să fie verificat de modulele de protecție Endpoint Security.
- **Arată bara de instrumente Bitdefender în browser**. Bara de instrumente Bitdefender informează utilizatorii cu privire la rating-ul paginilor web pe care le vizualizează. Bara de instrumente Bitdefender nu este aceeași cu bara de instrumente obișnuită a browser-ului dumneavoastră. Singurul lucru pe care îl adaugă browser-ului dumneavoastră este un mic instrument care glisează în partea superioară a fiecărei pagini web. Făcând clic pe acest buton se deschide bara de instrumente.

  În funcție de cum este clasificată pagina web de către Bitdefender, va fi afișată, în partea stângă a barei de instrumente, una dintre următoarele clasificări:

  – Apare mesajul "Această pagină nu este sigură", pe un fond de culoare roșie.

  – Mesajul "Se recomandă prudență" apare pe un fundal portocaliu.

  – Mesajul "Această pagină este sigură" apare pe un fond verde.
- **Asistență la căutare prin browser.** Consilier pentru căutare clasifică rezultatele afișate în urma căutărilor efectuate prin intermediul Google, Bing și Yahoo! precum și link-urile de pe Facebook și Twitter, plasând o pictogramă în fața fiecărui rezultat: Pictograme utilizate și semnificația lor:

  Nu este recomandat să vizitați această pagină web.

  Această pagină web poate avea conținut periculos. Vizitați cu atenție această pagină.

  Această pagină este sigură.

Scanare trafic

E-mailuri primite și traficul web sunt scanate în timp real pentru a preveni descărcarea de malware pe calculator. E-mailurile trimise sunt scanate pentru a preveni infectarea altor calculatoare cu malware. Scanarea traficului web poate încetini puțin navigarea pe internet, însă aceasta va bloca programele malware provenite de pe internet, inclusiv descărcările ascunse.

Când un e-mail este găsit infectat, acesta este înlocuit automat cu un e-mail standard de informare a destinatarului cu privire la e-mailul infectat original. În cazul în care o pagină web conține sau distribuie malware, aceasta este blocată în mod automat. În schimb este afișată pagină de avertizare specială pentru informarea utilizatorului că pagina web solicitată este periculoasă.

Deși nu se recomandă, puteți dezactiva scanarea traficului e-mail și web pentru a îmbunătăți performanțele sistemului. Aceasta nu este o amenințare majoră atâta timp cât scanarea la accesarea fișierelor locale rămâne activată.

Excluderi de la scanarea traficului

Puteți alege să săriți peste scanarea antimalware pentru un anumit trafic în timp ce sunt activate opțiunile de scanare trafic.

Pentru a defini o excludere de scanare trafic:

1. Selectați tipul de excludere din meniu.
2. În funcție de tipul de excludere, definiți entitatea de trafic care să fie exclusă de la scanare, după cum urmează:
   - **IP**. Introduceți adresa IP pentru care nu doriți scanarea traficului de intrare și de ieșire.
   - **URL**. Exclude de la scanare adresele web menționate. Pentru a defini o excludere URL de scanare:
     - Introduceți URL-ul specific, precum `www.example.com/example.html`
     - Utilizați metacaractere pentru a defini modele adresei web:
       - Asterisc (*) este substitut pentru zero sau mai multe caractere.
       - Semn de întrebare (?) este substitut pentru exact un caracter. Puteți folosi mai multe semne de întrebare pentru a defini orice combinație a unui anumit număr de caractere. De exemplu, ??? înlocuiește orice combinație de exact trei caractere.

     În tabelul de mai jos, puteți găsi mai multe exemple de sintaxă pentru specificarea adreselor de web.

Sintaxă	Aplicabilitatea excepției
`www.example*`	Orice site web sau pagina de web care începe cu `www.example` (indiferent de extensia de domeniu).

Sintaxă	Aplicabilitatea excepției
	Excluderea nu se va aplica la subdomeniile site-ului specificat, cum ar fi `subdomain.example.com`.
`*example.com`	Orice site care se termină în `example.com`, ininclusiv pagini și subdomenii ale acestora.
`*Șir*`	Orice site web sau pagină web a cărei adresă conține șirul de caractere specificat.
`*.com`	Orice site care are extensia de domeniu `.com` inclusiv paginile și subdomeniile acestora. Utilizați această sintaxă pentru a exclude de la scanare toate domeniile de nivel superior.
`www.example?.com`	Orice adresa de web care începe cu `www.example?.com`, unde ? poate fi înlocuit cu orice caracter unic. Aceste site-uri pot include: `www.example1.com` sau `www.exampleA.com`.

- **Aplicație**. Exclude de la scanare procesul specificat sau aplicația specificată. Pentru a defini o excludere de scanare pentru o aplicație:
  - Introduceți întreaga cale către aplicație. De exemplu, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Utilizați variabile de mediu pentru a specifica calea aplicației. De exemplu: `%programfiles%\Internet Explorer\iexplore.exe`
  - Utilizați metacaractere pentru a specifica orice aplicații care se potrivesc unui anumit model de nume. De exemplu:
    - `c*.exe` vizează toate aplicațiile care încep cu "c" (chrome.exe).
    - `??????.exe` vizează toate aplicațiile care au șase caractere în nume (chrome.exe, safari.exe, etc.).
    - `[^c]*.exe` vizează toate aplicațiile cu excepția celor care încep cu "c".
    - `[^ci]*.exe` vizează toate aplicațiile cu excepția celor care încep cu "c" sau "i".

3. Faceți clic pe butonul **Adăugare** din dreapta tabelului.

Pentru a elimina o entitate din listă, faceți clic pe butonul corespunzător **Ștergere**.

Web

În această secțiune puteți configura preferințele de securitate pentru navigarea web.

Setările sunt organizate în următoarele secțiuni:

- Control Web
- Antiphishing

Control Web

Cu ajutorul opțiunii Control Web puteți permite sau bloca accesul utilizatorilor sau al aplicațiilor în anumite intervale de timp.

Paginile web blocate de Controlul Web nu sunt afișate în browser. În locul acestora se afișează o pagină web implicită, prin care utilizatorul este informat că pagina web solicitată a fost blocată de Controlul Web.

Politici pentru calculatoare - Control conținut - Web

Utilizați selectorul pentru a activa sau dezactiva opțiunea **Control Web**.

Dispuneți de trei opțiuni de configurare:

- Selectați **Permite** pentru a acorda întotdeauna acces web.
- Selectați **Blocare** pentru a bloca întotdeauna accesul web.
- Selectați **Programare** pentru a permite restricții de timp pentru accesul web la un program detaliat.

Indiferent dacă alegeți să permiteți sau să blocați accesul web, puteți defini excepții de la aceste acțiuni pentru toate categoriile de web sau doar pentru adresele de web specifice. Faceți clic pe **Setări** pentru a configura programul dvs. de acces web și excepțiile, după cum urmează:

Planificator

Pentru a restricționa accesul la Internet la anumite ore din zi, pe o bază săptămânală:

1. Selectați din grilă intervalele temporale în care accesul la internet doriți să fie blocat.

   Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp. Faceți clic din nou în celulă pentru a inversa selecția.

   Pentru a începe o nouă selecție, faceți clic pe **Permite tot** sau **Blochează tot**, în funcție de tipul de restricție pe care doriți să îl puneți în aplicare.

2. Faceți clic pe **Salvare**.

Notă
Endpoint Security va efectua actualizări în fiecare oră indiferent dacă accesul la internet este blocat.

Categorii

Filtrul de categorii web filtrează în mod dinamic accesul la site-uri web în funcție de conținutul acestora. Puteți utiliza Filtrul de categorii web pentru a defini excepții de la acțiunea de control web selectată (Permite sau Blochează) pentru categorii web întregi (cum ar fi jocuri, conținut matur sau Rețele Online).

Pentru a configura Filtrul de categorii web:

1. Selectați **Filtru Categorii Web**.
2. Pentru o configurație rapidă, faceți clic pe unul dintre profilurile predefinite(**Agresiv**, **Normal** sau **Permisiv**). Utilizați descrierea din partea dreaptă a scalei pentru a vă ghida alegerea. Puteți vizualiza acțiunile predefinite pentru categorii web disponibile făcând clic pe butonul **Categorii** localizat mai jos.
3. Dacă setările implicite nu sunt satisfăcătoare, puteți defini dun filtru personalizat.
   a. Selectați **Personalizat**.
   b. Faceți clic pe butonul **Categorii** pentru a extinde secțiunea corespunzătoare.
   c. Identificați categoria pe care o doriți în listă și alegeți acțiunea dorită din meniu.
4. Puteți alege să **Tratează Categoriile web ca excepții pentru Acces Internet** dacă doriți să ignorați setările de acces web existente și să aplicați numai Filtrul categoriilor web.
5. Faceți clic pe **Salvare**.

Notă

- Permisiunea **Permite** pentru categorii specifice de web este și ea luată în considerare în timpul intervalelor de timp când accesul la internet este blocat de Control Web.
- Permisiunile **Permite** funcționează numai atunci când accesul la internet este blocat de Control Web, în timp ce permisiunile **Blocare** funcționează numai atunci când accesul web este permis de Control Web.
- Puteți înlocui permisiunea de categorie pentru adrese web individuale, adăugându-le în lista de permisiuni opuse în **Control Web > Setări > Excluderi**. De exemplu, dacă o adresă web este blocată de Filtrul Categorii Web, adăugați o regulă web pentru adresa respectivă cu caracteristica de permisiune setată pe **Permite**.

Excluderi

De asemenea, puteți defini reguli web pentru a bloca în mod explicit sau permite anumite adrese de web, modificând setările Control Web existente. De exemplu, utilizatorii vor putea accesa o anumită pagină Web și atunci când navigarea pe web este blocată de Control Web.

Pentru a crea o regulă web:

1. Selectați **Utilizează excepțiile** pentru a permite excepții web.
2. Introduceți adresa pe care doriți să o permiteți sau blocați în câmpul **Adresă Web**.
3. Selectați **Permite** sau**Blochează** din meniul **Permisiune**.
4. Faceți click pe butonul **Adăugare** din partea dreaptă a tabelului pentru a adăuga adresa la lista de excepții.
5. Faceți clic pe **Salvare**.

Pentru a edita o regulă web:

1. Faceți clic pe adresa de web pe care doriți să o editați.
2. Modificați URL-ul existent.
3. Faceți clic pe **Salvare**.

Pentru a elimina o regulă web:

1. Mutați cursorul pe adresa de web pe care doriți să o eliminați.
2. Faceți clic pe butonul **Ștergere**.
3. Faceți clic pe **Salvare**.

Antiphishing

Protecția antiphishing blochează automat paginile web de phishing cunoscute pentru a împiedica utilizatorii să divulge accidental informații private sau confidențiale unor infractori online. În loc de pagina de web de phishing, în browser este afișată o pagină de avertizare specială de informare a utilizatorului că pagina web solicitată este periculoasă.

Selectați **Antiphishing** pentru a activa protecția antiphishing. Puteți optimiza în continuare Antiphishing prin configurarea următoarelor setări:

- **Protecție împotriva fraudelor**. Selectați această opțiune dacă doriți să extindeți protecția și la alte tipuri de escrocherii în afară de phishing. De exemplu, site-uri care reprezintă companii false, care nu solicită în mod direct informații private, dar în schimb încearcă să pozeze ca afaceri legitime și să obțină profit prin determinarea oamenilor să facă afaceri cu ei.
- **Protecție împotriva tentativelor de phishing**. Păstrați această opțiune selectată pentru a proteja utilizatorii împotriva tentativelor de phishing.

În cazul în care o pagină web legitimă este incorect detectat ca phishing și blocată, o puteți adăuga la lista albă pentru a permite utilizatorilor accesarea acesteia. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.

Pentru a gestiona excepțiile antiphishing:

1. Faceți click **Excluderi**.

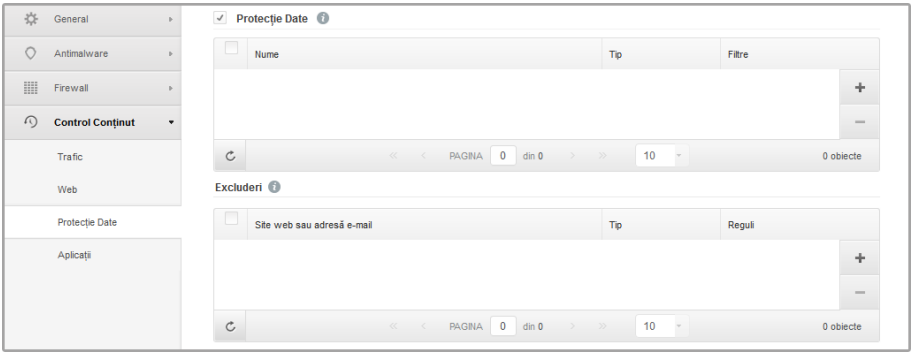
2. Introduceți adresa de web și faceți clic pe butonul + **Adăugare**.

   Pentru a șterge o excepție de pe listă, deplasați cursorul și faceți clic pe butonul − **Ștergere**.

3. Faceți clic pe **Salvare**.

Protecţie Date

Modulul Protecție Date împiedică divulgarea neautorizată a datelor sensibile pe baza regulilor definite de administrator.



Politici pentru calculatoare - Control conținut - Protecția datelor

Puteți crea reguli pentru a proteja orice informații personale sau confidențiale, cum ar fi:

- Informații cu caracter personal ale clientului
- Numele și detalii cheie privind produsele și tehnologiile în dezvoltare
- Informații de contact ale directorilor companiei

Informații protejate care ar putea include nume, numere de telefon, informații privind cardurile de credit și conturile bancare, adrese de e-mail și așa mai departe.

Pe baza regulilor de protecție a datelor pe care le creați, Endpoint Security scanează traficul web și de e-mail care părăsește calculatorul de șiruri de caractere specifice (de exemplu, un număr de card de credit). În cazul în care există o potrivire, pagina web respectivă sau mesajul de e-mail este blocat pentru a preveni transmiterea datelor protejate. Utilizatorul este imediat informat cu privire la măsurile luate de Endpoint Security printr-o pagină web sau e-mail de alertă.

Pentru a configura Protecția datelor:

1. Utilizați caseta de selecție pentru a activa protecția datelor.
2. Creați reguli de protecție a datelor pentru toate datele sensibile pe care doriți să le protejați. Pentru a crea o regulă:

a. Faceți clic pe butonul **Adăugare** din dreapta tabelului. Este afișată o fereastră de configurare.

b. Introduceți numele cu care regula va fi introdusă în tabelul de reguli. Alegeți un nume sugestiv, astfel încât dvs. sau alt administrator să poată identifica cu ușurință la ce se referă regula.

c. Introduceți datele pe care doriți să le protejați (de exemplu, numărul de telefon al unui director de companie sau numele intern al unui nou produs al companiei care este în lucru). Este aceptată orice combinație de cuvinte, numere sau șiruri de caractere formate din caractere alfanumerice și speciale (cum ar fi @, # sau $).

Asigurați-vă ca introduceți cel puțin cinci caractere pentru a evita blocarea greșită a unor mesaje și pagini web.

Important

Datele furnizate sunt stocate în formă criptată pe calculatoare protejate, dar se pot vizualiza în contul dvs. de Control Center. Pentru mai multă siguranță, nu introduceți toate datele pe care vreți să le protejați. În acest caz, trebuie să debifați opțiunea **Potrivire cuvinte întregi**.

d. Configurați opțiunile de scanare trafic după cum este cazul:

- **Scanare trafic web (HTTP)** - scanează traficul web (HTTP) și blochează la ieșire toate datele care corespund unei reguli.
- **Scanare trafic e-mail (SMTP)** - scanează traficul mail (SMTP) și blochează trimiterea mesajelor e-mail care corespund unei reguli.

Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

e. Faceți clic pe **Salvare**. Noua regulă va fi adăugată în listă.

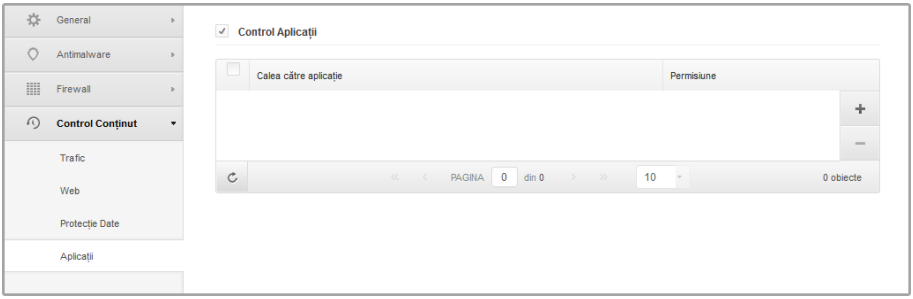
3. Configurați excepțiile de la regulile de protecție a datelor astfel încât utilizatorii să continue să poată trimite date protejate către site-uri autorizate și beneficiari. Excluderile se pot aplica la nivel global (la toate regulile) sau numai la anumite reguli. Pentru a adăuga o excludere:
   a. Faceți clic pe butonul **Adăugare** din dreapta tabelului. Este afișată o fereastră de configurare.
   b. Introduceți adresa de web sau de e-mail către care utilizatorii sunt autorizați să divulge date protejate.
   c. Selectați tipul de excludere (web sau adresa de e-mail).
   d. Din tabelul **Reguli**, selectați regulile de protecție a datelor la care ar trebui să se aplice această excludere.
   e. Faceți clic pe **Salvare**. Noua regulă de excludere va fi adăugată în listă.

Notă
În cazul în care un e-mail care conține date blocate este adresat mai multor destinatari, acesta va fi primit de cei pentru care au fost definite excluderi.

Pentru a elimina o regulă sau o excludere din listă, faceți clic pe butonul corespunzător − **Ștergere** din partea dreaptă a tabelului.

Aplicații

În această secțiune puteți configura opțiunea Control Aplicații. Funcția Control Aplicații vă ajută să blocați complet sau să restricționați accesul utilizatorilor la aplicațiile de pe calculatoarele lor. Astfel puteți bloca jocurile, fișierele video/audio și aplicațiile de mesagerie, precum și alte categorii de aplicații, inclusiv cele periculoase.



Politici pentru calculatoare - Control conținut - Aplicații

Pentru a configura Control aplicații:

1. Utilizați selectorul pentru a activa opțiunea Control aplicații.
2. Specificați aplicațiile la care doriți să restricționați accesul. Pentru a restricționa accesul la o aplicație:
   a. Faceți clic pe butonul + **Adăugare** din dreapta tabelului. Este afișată o fereastră de configurare.
   b. Trebuie să specificați calea către fișierul executabil al aplicației de pe calculatoarele țintă. Există două moduri de a face acest lucru:
      - Alegeți din meniu o locație prestabilită și completați calea după cum este necesar în câmpul de editare. De exemplu, pentru o aplicație instalată în directorul `Program Files`, selectați `%ProgramFiles%` și completați calea prin adăugarea unei bare oblice inversă (\) și numele directorului aplicației.
      - Introduceți calea completă în câmpul editabil. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.
   c. **Accesare Planificator**. Planificați accesul aplicațiilor în anumite intervale ale zilei, săptămânal:

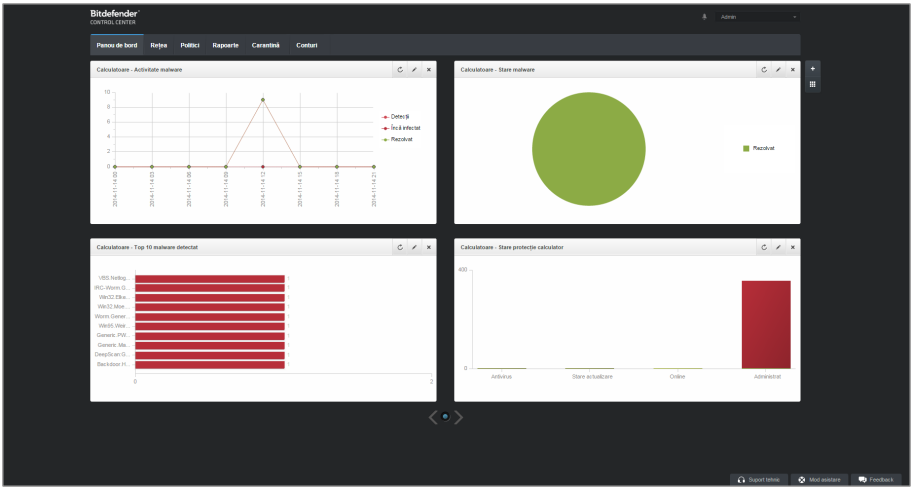
- Selectați din grilă intervalele de timp în care doriți să blocați accesul la aplicație. Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp. Faceți clic din nou în celulă pentru a inversa selecția.
- Pentru a începe o nouă selecție, faceți clic pe **Permite tot** sau **Blochează tot**, în funcție de tipul de restricție pe care doriți să îl puneți în aplicare.
- Faceți clic pe **Salvare**. Noua regulă va fi adăugată în listă.

Pentru a elimina o regulă din listă, faceți clic pe butonul corespunzător − **Ștergere** din partea dreaptă a tabelului. Pentru a edita o regulă existentă, faceți clic pe numele aplicației.

7. Panoul de monitorizare

Panoul de bord Control Center reprezintă un mod de afișare personalizabilă, ce oferă o vedere de ansamblu și rapidă asupra securității tuturor obiectelor protejate din rețea.

Portlet-urile panoului de bord afișează în timp real diferite informații referitoare la securitate, utilizând tabele ușor de citit, permițându-vă astfel să identificați rapid orice probleme care ar putea să vă solicite atenția.



Panoul de bord

Ce trebuie să știți despre portleturi:

- Control Center este livrat cu mai multe portlet-uri predefinite pentru panoul de bord.
- Fiecare portlet al panoului de control include un raport detaliat în fundal, accesibil cu un singur clic pe grafic.
- Există mai multe tipuri de portlet-uri care includ diverse informații despre protecția obiectelor de rețea, cum ar fi starea de actualizare, starea programelor periculoase, activitatea firewall etc. Pentru mai multe informații cu privire la tipurile de portleturi din panoul de bord, consultați „Tipuri de rapoarte disponibile ” (p. 121).
- Informațiile afișate de portlet-uri se referă numai la obiectele de rețea din contul dumneavoastră. Puteți personaliza ținta fiecărui portlet folosind comanda **Editare portlet**.

- Faceți clic pe intrările de legendă din grafic, atunci când sunt disponibile, pentru a ascunde sau a afișa variabila corespunzătoare pe grafic.
- Portlet-urile sunt afișate în grupuri de câte patru. Folosiți cursorul din partea de jos a paginii pentru a naviga între grupurile de portlet-uri.

Panoul este ușor de configurat, în funcție de preferințele individuale. Puteți edita setările portlet-ului, adăuga portlet-uri suplimentare, șterge sau rearanja portlet-uri existente.

7.1. Reîmprospătarea datelelor de portlet

Pentru a vă asigura că portletul afișează cele mai recente informații, faceți clic pe pictograma **Reîmprospătare** din bara de titlu a acestuia.

7.2. Editarea setărilor Portlet

Unele dintre portlet-uri oferă informații despre stare, în timp ce altele raportează evenimentele de securitate din ultima perioadă. Puteți verifica și configura perioada de raportare a unui portlet printr-un clic pe pictograma **Editare portlet** de pe bara cu denumirea sa.

7.3. Adăugarea unui portlet nou

Puteți adăuga portlet-uri suplimentare pentru a obține informațiile de care aveți nevoie.

Pentru a adăuga un nou portlet:

1. Mergeți la pagina **Panou de bord**.
2. Faceți clic pe butonul **Adăugare portlet** din partea dreaptă a panoului. Este afișată fereastra de configurare.
3. La secțiunea **Detalii**, configurați detaliile portlet:
   - Tip de raport cadru
   - Nume portlet sugestiv
   - Intervalul de actualizare

   Pentru mai multe informații cu privire la tipurile de rapoate disponibile, consultați „Tipuri de rapoarte disponibile ” (p. 121).
4. La secțiunea **Ținte**, selectați obiectele și grupurile de rețea pe care le doriți incluse.
5. Faceți clic pe **Salvare**.

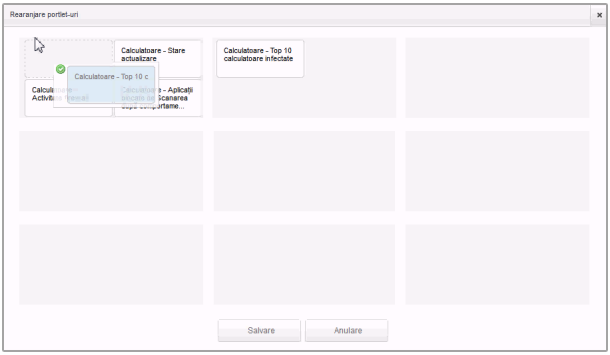
7.4. Ştergerea unui portlet

Puteți elimina cu ușurință orice portlet, făcând clic pe pictograma **Ștergere** de pe bara de titlu. După ce ați eliminat un portlet, nu îl mai puteți recupera. Cu toate acestea, puteți crea un alt portlet cu exact aceleași setări.

7.5. Rearanjarea portlet-urilor

Puteți rearanja portlet-urile panou pentru ca acestea să răspundă mai bine nevoilor dvs. Pentru a rearanja portlet-uri:

1. Mergeți la pagina **Panou de bord**.
2. Faceți clic pe butonul **Rearanjează portlet-urile** din partea dreaptă a panoului. Se afișează fereastra cu harta portlet-uri.
3. Glisați și fixați fiecare portlet în poziția dorită.
4. Faceți clic pe **Salvare**.



Rearanjați portlet-urile de pe panoul de bord

8. Utilizarea rapoartelor

Control Center vă permite să creați și să vizualizați rapoarte centralizate privind starea de securitate a obiectelor de rețea gestionate. Rapoartele pot fi utilizate în mai multe scopuri, cum ar fi:

- Monitorizarea și asigurarea conformității cu politicile de securitate ale organizației.
- Verificarea și evaluarea stării de securitate a rețelei.
- Identificarea problemelor referitoare la securitatea rețelei, a amenințărilor și vulnerabilităților.
- Monitorizarea incidentelor de securitate și a activității programelor periculoase.
- Oferirea informațiilor ușor de interpretat privind securitatea rețelei către managementul superior.

Sunt disponibile mai multe tipuri de rapoarte diferite, astfel încât să puteți obține cu ușurință informațiile de care aveți nevoie. Informațiile sunt prezentate sub forma unor tabele interactive ușor de consultat, care vă permit să verificați rapid starea de securitate a rețelei și să identificați problemele de securitate.

Rapoartele pot include date din întreaga rețea de obiecte de rețea administrate sau numai din anumite grupuri specifice. Astfel, consultând un singur raport, puteți afla:

- Date statistice referitoare la grupuri sau la toate obiecte de rețea administrate.
- Informații detaliate pentru fiecare obiect din rețea administrat.
- Lista calculatoarelor care îndeplinesc anumite criterii (de exemplu, cele care au protecția contra programelor periculoase dezactivată).

Toate rapoartele programate sunt disponibile în Control Center însă le puteți salva și pe calculator sau transmite prin e-mail.

Formatele disponibile includ Portable Document Format (PDF) și comma-separated values (CSV).

8.1. Tipuri de rapoarte disponibile

Aceasta este lista de tipuri de rapoarte disponibile pentru calculatoare:

Stare actualizare

Arată stadiul de actualizare a protecției Endpoint Security instalată pe calculatoarele selectate. Starea de actualizare se referă la versiunea de produs și versiunea de motoare (semnături).

Folosind filtrele disponibile, puteți afla cu ușurință ce clienți au efectuat sau nu au efectuat actualizările în ultimele 24 de ore.

Activitate malware

Vă oferă informații generale referitoare la programele periculoase detectate într-o anumită perioadă de timp, pe calculatoarele selectate. Puteți vedea:

- Număr de detectări (fișiere care au fost găsite infectate cu programe periculoase)
- Numărul de infecții rezolvate (fișiere care au fost dezinfectate sau mutate cu succes în carantină)
- Numărul de infecții nerezolvate (fișiere care se poate să nu fi fost dezinfectate, dar la care accesul a fost blocat; de exemplu, un fișier infectat memorat într-un format de arhivă proprietate)

Pentru fiecare amenințare detectată, făcând clic pe link-urile disponibile în coloanele cu rezultatele dezinfectării, puteți vizualiza lista calculatoarelor afectate și calea fișierelor De exemplu, dacă faceți clic pe numărul din coloana **Rezolvat(e)**, veți putea vizualiza fișierele și calculatoarele de pe care a fost eliminată amenințarea.

Stare malware

Vă ajută să aflați numărul și identitatea calculatoarelor selectate din rețea care au fost afectate de programele periculoase într-un anumit interval de timp și metoda de gestionare a amenințărilor.

Calculatoarele sunt grupate pe baza următoarelor criterii:

- Calculatoare pe care nu s-a detectat nimic (nu au fost detectate amenințări malware în perioada de timp specificată)
- Calculatoare cu programe periculoase soluționate (toate fișierele detectate au fost dezinfectate sau mutate cu succes în carantină)
- Calculatoare încă infectate cu malware (s-a blocat accesul la unele dintre fișierele detectate)

Pentru fiecare calculator, făcând clic pe link-urile disponibile în coloanele cu rezultatele dezinfectării, puteți vizualiza lista amenințărilor și calea către fișierele afectate.

Stare rețea

Vă oferă informații detaliate cu privire la starea generală de securitate a calculatoarelor selectate. Calculatoarele sunt grupate pe baza următoarelor criterii:

- Stadiul problemelor
- Stadiul managementului
- Stadiul infecției
- Stare protecție antimalware
- Starea actualizării produsului
- Stadiul acordării licențelor

- Stadiul de activitate a rețelei pentru fiecare calculator (online/offline). În cazul în care calculatorul este deconectat atunci când este generat raportul, veți vedea data și ora la care a fost văzut ultima oară online, prin Control Center.

Top 10 calculatoare infectate

Vă arată top 10 a celor mai infectate calculatoare după numărul total de detecții dintr-o anumită perioadă de timp din calculatoarele selectate.

Notă

Tabelul detaliilor afișează toate tipurile de programe periculoase detectate pe primele 10 calculatoare cele mai infectate.

Top 10 malware detectat

Vă indică primele 10 amenințări malware detectate într-o anumită perioadă de timp pe calculatoarele selectate.

Notă

Tabelul de detalii afișează toate calculatoarele care au fost infectate în funcție de primele 10 programe periculoase detectate.

Activitate firewall

Vă informează despre starea modulului Firewall din Endpoint Security. Puteți vedea numărul de încercări de trafic blocate și scanările de porturi blocate pe calculatoarele selectate.

Website-uri blocate

Vă informează despre activitatea modulului Control web din Endpoint Security. Puteți vedea numărul de site-uri blocate pe calculatoarele selectate.

Aplicații blocate

Vă informează despre activitatea modulului Control aplicații din Endpoint Security. Puteți vedea numărul de aplicații blocate pe calculatoarele selectate.

Activitate Antiphishing

Vă informează despre activitatea modulului Antiphishing din Endpoint Security. Puteți vedea numărul de site-uri blocate pe calculatoarele selectate.

Stadiul protecției calculatorului

Vă oferă diverse informații de stare privind calculatoarele selectate din rețea.

- Stare protecție antimalware
- Stadiu actualizare Endpoint Security
- Starea de activitate a rețelei (online/offline)
- Stadiul managementului

Puteți aplica filtre în funcție de aspectul de securitate și de stare pentru a identifica informațiile pe care le căutați.

Protecție Date

Vă informează despre activitatea modulului Protecție date din Endpoint Security. Puteți vedea numărul de emailuri și site-uri blocate pe calculatoarele selectate.

Aplicații blocate de scanarea după comportament

Vă informează despre aplicațiile blocate de AVC (Active Virus Control) / SDI(Sistem de detecție a intruziunilor). Puteți vizualiza numărul de aplicații blocate de AVC / SDI pentru fiecare calculator selectat. Faceți clic pe numărul de aplicații blocate pentru calculatorul care vă interesează pentru a vizualiza lista de aplicații blocate și informații asociate (numele aplicației, motivul blocării, numărul de tentative de blocare, precum și data și ora ultimei tentative de blocare).

Stare module Endpoint Security

Vă oferă o vedere de ansamblu asupra modulelor de protecție Endpoint Security pentru calculatoarele selectate. Puteți vizualiza ce module sunt active și care dintre acestea sunt dezactivate sau nu sunt instalate.

8.2. Crearea rapoartelor

Puteți crea două categorii de rapoarte:

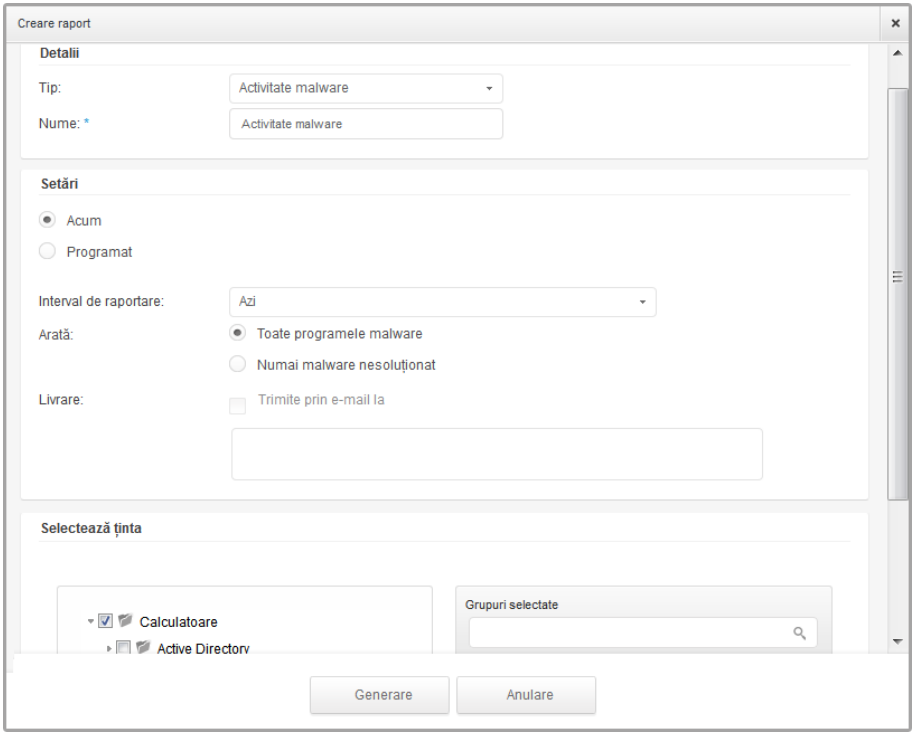
- **Rapoarte instant.** Rapoartele instant sunt afișate în mod automat după ce le generați.
- **Rapoarte programate.** Rapoartele programate pot fi configurate să ruleze la un moment dat și la o anumită dată, o listă a tuturor rapoartelor programate fiind afișată în pagina **Repoarte**.

Important

Rapoartele instant sunt șterse automat atunci când închideți pagina de raport. Rapoartele programate sunt salvate și afișate în pagina **Raporate**.

Pentru a crea un raport:

1. Mergeți la pagina **Rapoarte**.
2. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Este afișată o fereastră de configurare.



Opțiuni rapoarte calculator

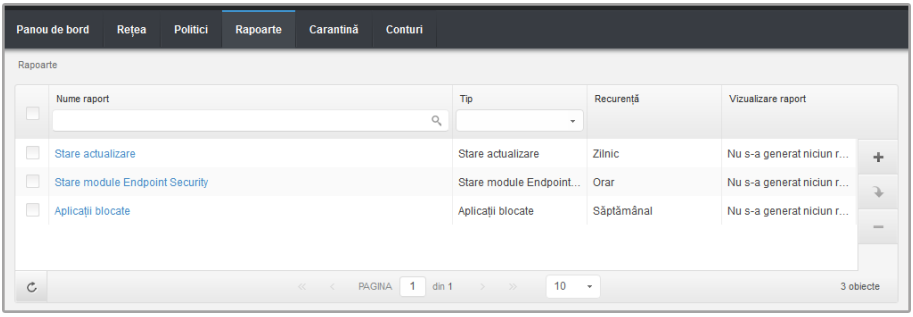
3. Selectați tipul dorit de raport din meniu. Pentru mai multe informații, consultați capitolul „Tipuri de rapoarte disponibile ” (p. 121).
4. Introduceți un nume sugestiv pentru raport. Atunci când alegeți un nume, luați în considerare tipul de raport și, eventual, opțiunile de raportare.
5. Configurați recurența raportului:
   - Selectați **Acum** pentru a crea un raport instant.
   - Selectați **Programat** pentru a configura generarea automată a raportului la intervalul dorit:
     - Orar, la intervalul specificat.
     - Zilnic. În acest caz, puteți să setați și ora de începere (oră și minute).
     - Săptămânal, în zilele specificate ale săptămânii și la ora de începere selectată (oră și minute).
     - Lunar, în fiecare zi specificată a lunii și la ora de începere specificată (oră și minute).

6. Pentru majoritatea tipurilor de rapoarte, trebuie să specificați intervalul temporar la care se referă datele pe care acestea le conțin. Raportul va afișa doar datele din perioada selectată.
7. Mai multe tipuri de rapoarte furnizează opțiuni de filtrare pentru a vă ajuta să identificați mai facil informațiile de care sunteți interesați. Utilizați opțiunile de filtrare din secțiunea **Arată** pentru a obține doar informațiile dorite.

   De exemplu, pentru un raport de **Stare actualizare**, puteți selecta să vizualizați doar lista calculatoarelor care au fost actualizate în perioada de timp selectată sau a celor care necesită repornire pentru finalizarea actualizării.
8. **Livrare**. Pentru a primi prin email un raport programat, selectați opțiunea corespunzătoare. Introduceți adresele e-mail dorite în câmpul de mai jos.
9. **Selectare țintă**. Parcurgeți în jos pentru a configura ținta raportului. Selectați grupul pe care doriți să ruleze raportul.
10. Faceți clic pe **Generare** pentru a crea un raport instant sau **Salvare** pentru a crea un raport programat.
    - Dacă ați ales să creați un raport instant, acesta va fi afișat imediat după ce faceți clic pe **Generare**. Intervalul necesar pentru crearea rapoartelor poate diferi în funcție de numărul de rapoarte administrate. Vă rugăm să așteptați pentru a se crea raportul solicitat.
    - Dacă ați ales să creați un raport programat, acesta va fi afișat în lista de la pagina **Rapoarte**. După crearea raportului, puteți vizualiza raportul făcând clic pe link-ul său corespunzător din coloana **Vizualizare raport** de pe pagina **Rapoarte**.

8.3. Vizualizarea şi gestionarea rapoartelor programate

Pentru a vizualiza și administra rapoarte programate, mergeți la pagina **Rapoarte**.



Pagina Rapoarte

Toate rapoartele programate sunt afișate într-un tabel. Puteți vizualiza rapoartele planificate generate și informații utile referitoare la acestea:

- Numele si tipul raportului.
- Când va fi generat raportul.

Notă
Rapoartele programate sunt disponibile doar pentru utilizatorul care le-a creat.

Pentru a sorta rapoartele pe baza unei anumite coloane, facți clic pe titlul coloanei. Faceți clic pe titlul coloanei din nou pentru a modifica ordinea sortării.

Detaliile raportului sunt afișate într-un tabel care constă din mai multe coloane furnizând informații diferite. Tabelul poate cuprinde mai multe pagini (numai 50 de înregistrări sunt afișate implicit pe pagină). Pentru a răsfoi printre paginile cu detalii, utilizați butoanele din partea inferioară a tabelului.

Pentru a găsi ușor ceea ce cauți, utilizați casetele de căutare sau opțiunile de filtrare de sub anteturile de coloană.

Pentru a sorta detaliile despre rapoarte pe baza unei anumite coloane, facți clic pe tilul coloanei. Faceți clic pe titlul coloanei din nou pentru a modifica ordinea sortării.

Pentru a goli o casetă de căutare, plasați cursorul peste ea și faceți clic pe pictograma **Ștergere** icon.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe pictograma **Reîmprospătare** din colțul din stânga - jos al tabelului.

8.3.1. Vizualizarea rapoartelor

Pentru a vizualiza un raport:

1. Mergeți la pagina **Rapoarte**.
2. Sortați rapoartele după nume, tip sau reapariție pentru a găsi cu ușurință raportul pe care îl căutați.
3. Faceți clic pe link-ul corespunzător în coloana **Vizualizare raport** pentru a afișa raportul.

Toate rapoartele cuprind o secțiune rezumat (jumătatea de sus a paginii de raport) și o secțiune de detalii (jumătatea inferioară a paginii de raport).

- Secțiunea rezumat vă oferă date statistice (diagrame și grafice) pentru toate obiectele sau grupurile de rețea țintă precum și informații generale despre raport, cum ar fi perioada de raportare (dacă este cazul), raportul țintă etc.
- Secțiunea de detalii furnizează informații detaliate pentru fiecare obiect din rețea administrat.

Notă

- Pentru a configura informațiile afișate de diagramă, faceți clic pe intrările de legendă pentru a afișa sau a ascunde datele selectate.
- Faceți clic pe zona grafică care vă interesează pentru a vizualiza detaliile aferente din tabelul situat sub grafic.

8.3.2. Editarea unui raport programat

Notă

Când editați un raport programat, toate actualizările vor fi aplicate începând cu următorul raport. Rapoartele generate anterior nu vor fi afectate de editare.

Pentru a modifica setările unui raport programat:

1. Mergeți la pagina **Rapoarte**.
2. Faceți clic pe numele raportului.
3. Modificați setările raportului după cum este necesar. Puteți modifica următoarele opțiuni:
   - **Nume raport.** Alegeți un nume sugestiv pentru raport care să vă ajute la identificarea cu ușurință la ce se referă. Atunci când alegeți un nume, luați în considerare tipul de raport și, eventual, opțiunile de raportare. Rapoartele generate de un raport programat sunt denumite după el.
   - **Recurența raportului (programul).** Puteți programa ca raportul să fie generat automat orar (după un anumit interval orar), zilnic (la o anumită oră de începere), săptămânal (într-o anumită zi a săptămânii și la o anumită oră de începere) sau lunar (într-o anumită zi a lunii și la o anumită oră de începere). În funcție de programul selectat, raportul va conține numai datele din ultima zi, săptămână sau respectiv lună.
   - **Setări.**
     - Puteți programa ca raportul să fie generat automat în fiecare oră (în baza unui anumit interval orar), zi (la o anumită oră de începere), săptămână (într-o anumită zi a săptămânii și la o anumită oră de începere) sau lunar (într-o anumită zi a lunii și la o anumită oră de începere). În funcție de programul selectat, raportul va conține numai datele din ultima zi, săptămână sau respectiv lună.
     - Raportul va include date din intervalul de timp selectat. Aveți posibilitatea să modificați intervalul începând cu următorul raport.
     - Cele mai multe tirapoarte asigură opțiuni de filtrare pentru a vă ajuta să identificați mai facil informațiile de care sunteți interesați. Când vizualizați raportul în consolă, vor fi disponibile toate informațiile, indiferent de opțiunile selectate. Însă dacă descărcați raportul sau îl trimiteți prin e-mail, în fișierul PDF vor fi incluse numai rezumatul raportului și informațiile selectate. Detalii cu privire la raport vor fi disponibile doar în format CSV.

– Puteți alege să primiți raportul prin e-mail.

- **Selectare țintă.** Opțiunea selectată indică tipul țintei curente a raportului (fie grupuri, fie obiecte individuale din rețea). Faceți clic pe link-ul corespunzător pentru a vizualiza raportul țintă curent. Pentru a-l schimba, selectați grupurile sau obiectele de rețea care urmează să fie incluse în raport.

4. Faceți clic pe **Salvare** pentru a aplica modificările.

8.3.3. Ştergerea unui raport programat

Atunci când nu mai aveți nevoie de un raport programat, cel mai bine este să-l ștergeți. Ștergerea unui raport programat va șterge toate rapoartele pe care le-a generat în mod automat la acel moment.

Pentru a șterge un raport programat.

1. Mergeți la pagina **Rapoarte**.
2. Selectați raportul pe care doriți să-l ștergeți.
3. Faceți clic pe butonul **– Ștergere** din dreapta tabelului.

8.4. Salvarea rapoartelor

În mod implicit, rapoartele programate sunt salvate automat în Control Center.

Dacă aveți nevoie ca rapoartele să fie disponibile mai mult timp, puteți să le salvați pe calculator. Rezumatul raportului va fi disponibil în format PDF, în timp ce detaliile raportului vor fi disponibile doar în format CSV.

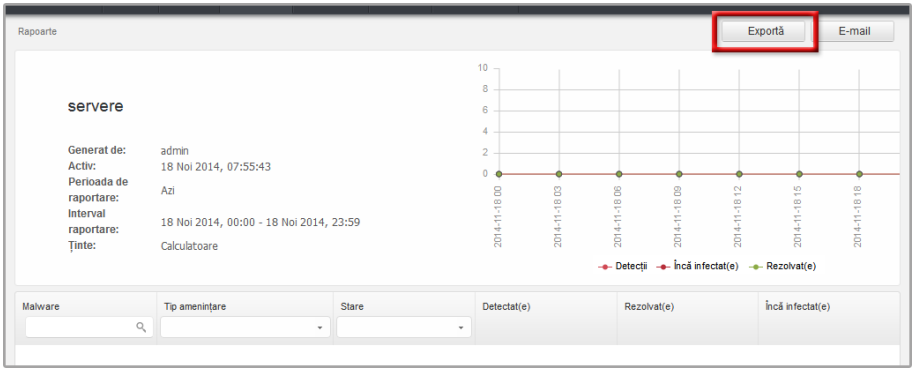
Aveți la dispoziție două modalități de salvare a rapoartelor:

- Export
- Descărcare

8.4.1. Exportarea rapoartelor

Pentru a exporta raportul în calculator:

1. Faceți clic pe butonul **Export** în colțul din dreapta sus al paginii raportului.



Opțiunea Rapoarte - Export

2. Selectați formatul dorit al raportului:
   - Format Document Portabil (PDF) sau
   - Fișier cu valori separate prin virgulă (CSV)
3. În funcție de setările browser-ului, fișierul poate fi descărcat în mod automat într-o locație de descărcare implicită sau va apărea o fereastră de descărcare unde trebuie să specificați directorul de destinație.

8.4.2. Descărcarea rapoartelor

O arhivă de raport conține atât rezumatul raportului cât și detaliile acestuia.

Pentru a descărca o arhivă de raport:

1. Mergeți la pagina **Rapoarte**.
2. Selectați raportul pe care doriți să-l salvați.
3. Faceți clic pe butonul **Descărcare** și selectați fie **Ultima instanță** tpentru a descărca ultima instanță generată a raportului sau **Arhiva completă** pentru a descărca o arhivă ce conține toate instanțele.

   În funcție de setările browser-ului, fișierul poate fi descărcat în mod automat într-o locație de descărcare implicită sau va apărea o fereastră de descărcare unde trebuie să specificați directorul de destinație.

8.5. Transmiterea prin e-mail a rapoartelor

Puteți trimite rapoarte prin e-mail, folosind următoarele opțiuni:

1. Pentru a trimite raportul pe care îl vizualizați, faceți clic pe butonul **Email** din colțul din dreapta - sus al paginii de raport. Raportul va fi trimis la adresa de e-mail asociată contului dumneavoastră.
2. Pentru a configura livrarea prin e-mail a rapoartelor programate dorite:
   a. Mergeți la pagina **Rapoarte**.
   b. Faceți clic pe numele raportului dorit.
   c. În **Opțiuni > Livrare**, selectați **Trimite prin e-mail la**.
   d. Introduceți adresa de e-mail dorită în câmpul de mai jos. Puteți adăuga oricâte adrese de e-mail doriți.
   e. Faceți clic pe **Salvare**.

Notă
în fișierul PDF trimis prin e-mail vor fi incluse numai rezumatul raportului și graficul. Detalii cu privire la raport vor fi disponibile în fișierul CSV.

8.6. Printarea rapoartelor

Control Center nu acceptă în prezent funcționalitatea de buton de imprimare. Pentru a imprima un raport, trebuie mai întâi să-l salvați pe calculator.

9. Carantină

În mod implicit, Endpoint Security izolează fișierele suspecte și fișierele infectate cu programe periculoase care nu pot fi dezinfectate într-o zonă sigură numită carantină. Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

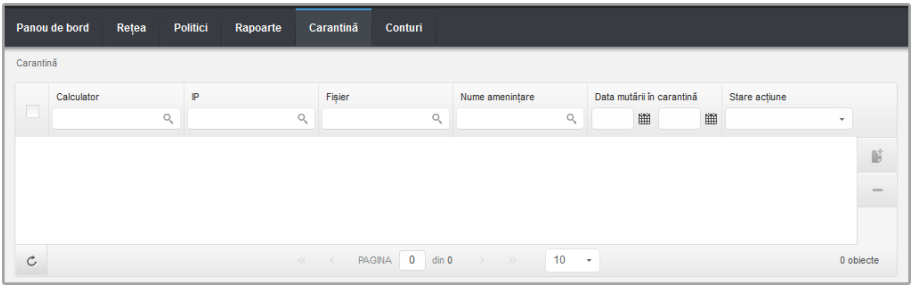
Security for Endpoints stochează fișierele din carantină pe fiecare calculator administrat. Folosind Control Center aveți opțiunea de a șterge sau de a restaura fișierele specifice aflate în carantină.

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

De asemenea, fișierele în carantină sunt scanate după fiecare actualizare a semnăturii programului periculos. Fișierele curățate sunt mutate automat în locația lor originală.

Control Center oferă informații detaliate cu privire la toate fișierele mutate în carantină pe obiectele de rețea administrate de pe contul tău.

Pentru a verifica și administra fișierele aflate în carantină, mergeți în pagina **Carantină**:



Pagina Carantină

Informațiile referitoare la fișierele în carantină sunt afișate în tabel. Vă sunt furnizate următoarele informații:

- Numele obiectului de rețea pe care a fost detectată amenințarea.
- IP-ul obiectului de rețea pe care a fost detectată amenințarea.
- Calea către fișierul infectat sau suspect pe obiectul de rețea pe care a fost detectat.
- Nume dat amenințării de programe periculoase de către cercetătorii de securitate ai Bitdefender.

- Moment în care fișierul a fost în carantină.
- Măsurile în așteptare solicitate de administrator pentru fișierul în carantină.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din colțul din stânga - jos al tabelului. Acest lucru poate fi necesar atunci când petreceți mai mult timp pe pagină.

9.1. Navigare şi căutare

În funcție de numărul de obiecte de rețea administrate și natura infecțiilor, numărul de fișiere aflate în carantină poate fi uneori mare. Tabelul poate cuprinde mai multe pagini (numai 50 de înregistrări sunt afișate implicit pe pagină).

Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului. Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă există prea multe intrări, puteți utiliza casetele de căutare din anteturile de coloană pentru a filtra datele afișate. De exemplu, puteți căuta o amenințare specifică detectată în rețea sau pentru un obiect din rețea specific. De asemenea puteți să faceți clic pe anteturile de coloană pentru a sorta datele în funcție de o anumită coloană.

9.2. Restabilirea fişierelor aflate în carantină

În anumite situații, este posibil să fie necesar să recuperați fișierele izolate în carantină, fie în locațiile inițiale, fie într-o locație alternativă. O astfel de situație este când doriți să recuperați fișiere importante stocate într-o arhivă infectată care a fost izolată în carantină.

Pentru a restaura unul sau mai multe fișiere aflate în carantină:

1. Mergeți la pagina **Carantină**.
2. Selectați casetele care corespund fișierelor din carantină pe care doriți să le restabiliți.
3. Faceți clic pe butonul **Restaurare** din dreapta tabelului.
4. Alegeți locația unde doriți să fie recuperate fișierele selectate (fie locația originală sau o locație anume de pe calculatorul țintă).

   Dacă alegeți să restaurați o locație personalizată, trebuie să introduceți calea în câmpul corespunzător. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă. Pentru mai multe informații, consultați capitolul „Utilizarea variabilelor de sistem” (p. 149).
5. Selectați **Adaugă automat excepția în politică** pentru a exclude fișierele care urmează să fie restaurate din scanările viitoare. Excluderea sde aplică tuturor politicilor care afectează fișierele selectate, cu excepția politicii implicite, care nu poate fi modificată.

6. Faceți clic pe **Salvare** pentru a solicita acțiunea de recuperare a fișierului. Puteți observa acțiunea în curs în coloana **Acțiune**.
7. Măsura necesară este trimisă către calculatoarele țintă imediat sau de îndată ce revin online. După ce un fișier este recuperat, datele corespunzătoare vor dispărea din tabelul de Carantină.

9.3. Ştergerea automată a fişierelor din carantină

Implicit, fișierele aflate în carantină de mai mult de 30 de zile sunt șterse automat. Această setare poate fi modificată prin editarea politicii atribuită la obiectele de rețea administrate.

Pentru a schimba intervalul automat de ștergere pentru fișierele aflate în carantină:

1. Mergeți la pagina **Politici**.
2. Găsi politica atribuită obiectelor de rețea pe care doriți să modificați setările și faceți clic pe numele său.
3. Mergeți la secțiunea **Antimalware > Carantină**.
4. Selectați perioada dorită de ștergere automată din meniu.
5. Faceți clic pe **Salvare** pentru a aplica modificările.

9.4. Ştergerea fişierelor aflate în carantină

Dacă doriți să ștergeți fișierele din carantină manual, mai întâi trebuie să vă asigurați că fișierele pe care alegeți să le ștergeți, nu sunt necesare. Utilizați aceste sfaturi atunci când ștergeți fișierele aflate în carantină:

- Un fișier poate fi de fapt program periculos în sine. Dacă cercetarea dumneavoastră va duce la o astfel de situație, puteți căuta în carantină pentru amenințarea specifică și ștergerea ei din carantină.
- Puteți șterge în condiții de siguranță:
  - Fișiere arhivă neimportante
  - Fișiere de setare neimportante

Pentru a șterge unul sau mai multe fișiere aflate în carantină:

1. Mergeți la pagina **Carantină**.
2. Verificați lista de fișiere în carantină și selectați căsuțele corespunzătoare pentru cele pe care doriți să le ștergeți.
3. Faceți clic pe butonul **Ștergere** din dreapta tabelului. Puteți observa starea în curs în coloana **Acțiune**.

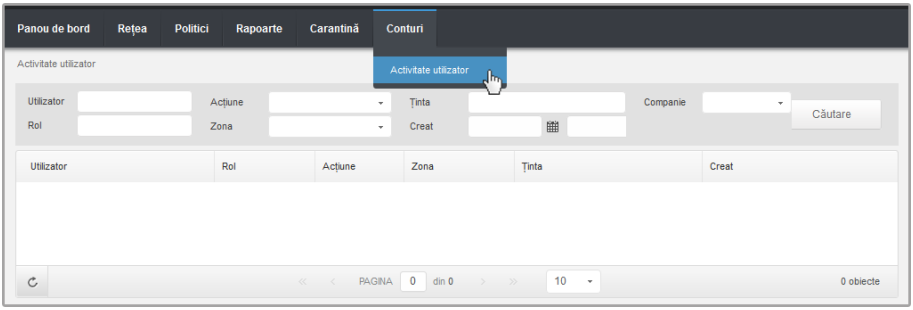
4. Măsura necesară este trimisă către obiectele de rețea țintă imediat sau de îndată ce revin online. După ce un fișier este șters, datele corespunzătoare vor dispărea din tabelul de Carantină.

10. Jurnalul activității utilizatorului

Control Center listează toate operațiunile și acțiunile întreprinse de către utilizatori. Lista de activități ale utilizatorului include următoarele evenimente, conform nivelului drepturilor administrative pe care le dețineți:

- Conectarea și deconectarea
- Crearea, editarea, redenumirea și ștergerea rapoartelor
- Adăugarea și eliminarea portlet-urilor din panoul de bord
- Crearea, editarea și ștergerea acreditărilor
- Crearea, modificarea, descărcarea și ștergerea pachetelor de rețea
- Crearea de sarcini de rețea
- Crearea, editarea, redenumirea și ștergerea conturilor de utilizator
- Ștergerea sau mutarea calculatoarelor între grupuri
- Crearea, mutarea, redenumirea și ștergerea grupurilor
- Ștergerea și restaurarea fișierelor aflate în carantină
- Crearea, editarea și ștergerea conturilor de utilizator
- Crearea, editarea, redenumirea, atribuirea și eliminarea politicilor

Pentru a examina înregistrările privind activitatea utilizatorului, mergeți la pagina **Conturi > Activitate utilizator**.



Pagina Activităților utilizatorului

Pentru a afișa evenimentele înregistrate care vă interesează, trebuie să definiți o căutare. Completați câmpurile disponibile cu criteriile de căutare și faceți clic pe butonul **Căutare**. Toate înregistrările care se potrivesc criteriilor dvs. vor fi afișate în tabel.

Coloanele din tabel vă oferă informații utile despre evenimentele din listă:

- Numele de utilizator al persanei care a efectuat acțiunea.

- Rolul utilizatorului.
- Acțiunea care a cauzat evenimentul.
- Tip de obiect de consolă afectat de acțiune.
- Obiect de consolă specific afectat de acțiune.
- Momentul în care a avut loc evenimentul.

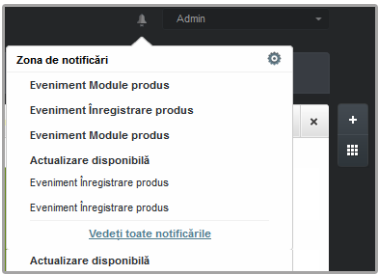
Pentru a sorta evenimentele pe baza unei anumite coloane, faceți clic pe titlul coloanei. Faceți clic pe titlul coloanei din nou pentru a inversa ordinea sortării.

Pentru a vizualiza informații detaliate despre un eveniment, selectați-l și verificați secțiunea de sub tabel.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din colțul din stânga - jos al tabelului.

11. Notificări

În funcție de evenimentele care ar putea apărea în întreaga rețea, Control Center va afișa diverse notificări pentru a vă informa cu privire la starea de securitate a mediului dumneavoastră. Notificările vor fi afișate în **Zona de notificări** situată în partea din dreapta sus a interfeței Control Center.



Zona de notificări

Atunci când în rețea este detectat un nou eveniment, zona de notificare va afișa o pictogramă roșie  care va indica numărul de evenimente detectate recent. Un clic pe pictogramă afișează lista de evenimente detectate.

11.1. Tipuri de notificări

Aceasta este lista tipurilor de notificări disponibile:

Epidemie de malware
Această notificare este trimisă utilizatorilor care au cel puțin 5 % din toate obiectele lor de rețea administrate infectate de aceeași program periculos.

Puteți configura pragul pentru epidemia de malware în fereastra **Setări notificări**. Pentru mai multe informații, consultați capitolul „Configurarea setărilor de notificare” (p. 141).

Licența expiră
Această notificare este trimisă cu 30, șapte și o zi înainte de expirarea licenței.

Limita de utilizare a licenței a fost atinsă
Această notificare este trimisă atunci când au fost utilizate toate licențele disponibile .

Limita de utilizare a licenței este pe cale de a fi atinsă
Această notificare este trimisă atunci când au fost folosite 90 % din licențele disponibile.

Actualizare disponibilă

Această notificare vă informează despre disponibilitatea unei noi actualizări Small Office Security.

Eveniment Antiphishing

Această notificare vă informează de fiecare dată când agentul stației de lucru blochează accesul la o pagină de web cunoscută pentru tentative de phishing. Această notificare vă oferă, de asemenea, detalii precum stația de lucru care a încercat să acceseze site-ul nesigur (nume și IP), agentul instalat sau URL-ul blocat.

Eveniment Firewall

Prin această notificare sunteți informat de fiecare dată când modulul firewall al unui agent instalat a blocat scanarea unui port sau accesul la rețea al unei aplicații, în conformitate cu politica aplicată.

Eveniment AVC/SDI

Această notificare se trimite de fiecare dată când o aplicație potențial periculoasă este detectată și blocată pe o stație de lucru din rețeaua dumneavoastră. De asemenea, veți găsi detalii despre tipul, numele și calea aplicației periculoase.

Eveniment Control utilizator

Această notificare se trimite de fiecare dată când activitatea unui utilizator, precum navigarea pe internet sau o aplicație software este blocată de clientul instalat pe stația de lucru în conformitate cu politica aplicată.

Eveniment privind protecția datelor

Această notificare se trimite de fiecare dată când traficul de date este blocat pe o stație de lucru conform regulilor de protecție a datelor.

Eveniment Module produs

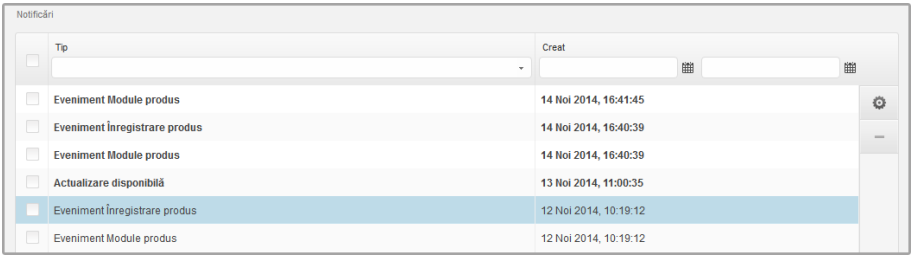
Această notificare se trimite de fiecare dată când un modul de securitate al unui agent instalat este dezactivat.

Eveniment Înregistrare produs

Această notificare vă informează atunci când starea de înregistrare a unui agent instalat în rețeaua dumneavoastră s-a modificat.

11.2. Vizualizarea notificărilor

Pentru a vizualiza notificările, faceți clic butonul **Zona de notificări** și apoi faceți clic pe **Vedeți toate notificările**. Este afișat un tabel care conține toate notificările.



Pagina Notificări

În funcție de numărul de notificări, tabelul se poate întinde pe mai multe pagini (implicit, sunt afișate doar 10 intrări pe pagină).

Pentru a trece de la o pagină la alta, folosiți butoanele de navigație din partea de jos a tabelului.

Pentru a modifica numărul de intrări afișate pe pagină, selectați o opțiune din meniul de lângă butoanele de navigație.

Dacă există prea multe intrări, puteți utiliza casetele de căutare din antetele de coloană sau meniul de filtrare din partea de sus a tabelului pentru a filtra datele afișate.

- Pentru a filtra notificări, selectați tipul de notificare pe care doriți să-l vizualizați din meniul **Tip**. Opțional, puteți selecta intervalul de timp în care a fost generată notificarea, pentru a reduce numărul de intrări în tabel, mai ales în cazul în care a fost generat un număr mare de notificări.
- Pentru a vedea detaliile de notificare, faceți clic pe numele notificării din tabel. Secțiunea **Detalii** este afișată în tabelul de mai jos, unde puteți vedea evenimentul care a generat notificarea.

11.3. Ştergerea notificărilor

Pentru a șterge notificări:

1. Faceți clic pe butonul **Zona de notificări** din partea dreaptă a barei de meniu și apoi faceți clic pe **Vedeți toate notificările**. Este afișat un tabel care conține toate notificările.
2. Selectați notificările pe care doriți să le eliminați.
3. Faceți clic pe butonul **Ștergere** din dreapta tabelului.

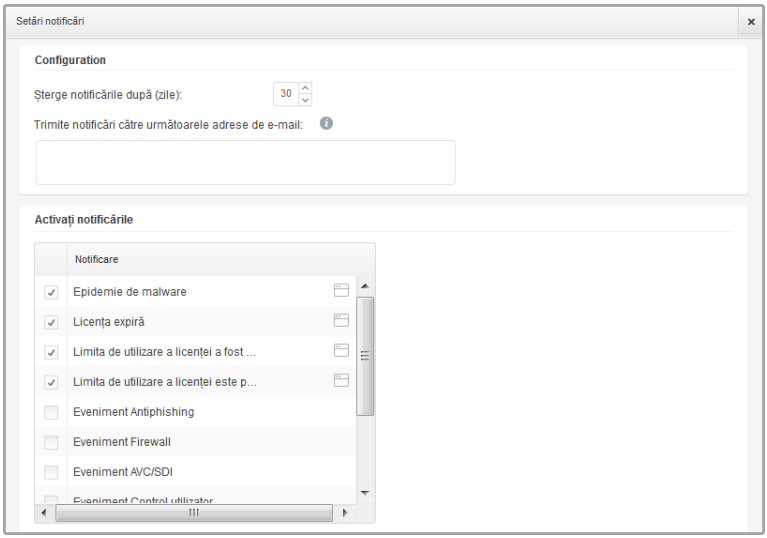
De asemenea, puteți configura notificările care vor fi șterse automat după un anumit număr de zile. Pentru mai multe informații, consultați capitolul „Configurarea setărilor de notificare” (p. 141).

11.4. Configurarea setărilor de notificare

Pentru fiecare utilizator se pot configura tipul de notificări care să fie transmise și adresele de e-mail la care sunt trimise.

Pentru configurarea setărilor de notificare:

1. Faceți clic pe butonul **Zona de notificări** din partea dreaptă a barei de meniu și apoi faceți clic pe **Vedeți toate notificările**. Este afișat un tabel care conține toate notificările.
2. Faceți clic pe butonul **Configurare** din dreapta tabelului. Este afișată fereastra **Setări notificări**.



Setări notificări

Notă

De asemenea, puteți accesa direct fereastra **Setări de notificare** folosind pictograma **Configurare** din colțul din dreapta - sus al ferestrei **Zona de notificare**.

3. În secțiunea **Configurare** puteți defini următoarele setări:
   - Puteți configura notificările care vor fi șterse automat după un anumit număr de zile. Introduceți numărul de zile dorit în câmpul **Șterge notificările după (zile)**.
   - Opțional, puteți alege să trimiteți notificări prin e-mail către adrese de e-mail specifice. Introduceți adresele e-mail în câmpul dedicat, apăsând `Enter` după fiecare adresă.

4. În secțiunea **Activare notificări** puteți selecta tipul de notificări pe care doriți să le primiți de la Small Office Security. De asemenea, puteți configura individual vizibilitatea și opțiunile de transmitere pentru fiecare tip de notificare.

   Selectați din listă tipul de notificare dorit. Pentru mai multe informații, consultați capitolul „Tipuri de notificări” (p. 138). După ce ați selectat un tip de notificare, puteți configura opțiunile specifice în partea din dreapta:

   - **Afișare în consolă** specifică faptul că acest tip de eveniment este afișat în Control Center, cu ajutorul pictogramei  **Zonă de notificări**.
   - **Transmitere prin e-mail** specifică faptul că acest tip de eveniment se transmite, de asemenea, către anumite adrese de e-mail. În acest caz, vi se solicită să introduceți adresele de e-mail în câmpul dedicat, apăsând `Enter` după fiecare adresă.

   Notă
   În mod implicit, notificarea de Epidemie de malware este transmisă utilizatorilor care au cel puțin 5% din obiectele de rețea administrate infectate cu același malware. Pentru a modifica valoarea pragului de pentru notificarea epidemiei de malware, selectați opțiunea **Utilizare prag personalizat** și apoi introduceți valoarea dorită în câmpul **Prag epidemie de malware**.

5. Faceți clic pe **Salvare**.

12. Obținere ajutor

Bitdefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confruntați cu o problemă sau dacă aveți orice întrebare cu privire la produsul Bitdefender dvs., mergeți la Centrul de asistență online. Acesta oferă mai multe resurse pe care le puteți folosi pentru a găsi rapid o soluție sau un răspuns. Sau, dacă preferați, puteți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

12.1. Centrul de asistență Bitdefender

Centrul de asistență Bitdefender disponibil la http://www.bitdefender.ro/support/business.html este locul unde veți găsi tot ajutorul de care aveți nevoie pentru produsul dumneavoastră Bitdefender.

Puteți utiliza mai multe resurse pentru a găsi rapid o soluție sau un răspuns:

- Articolele din Knowledge Base
- Forum asistență Bitdefender
- Documentație de produs

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

Articolele din Knowledge Base

Bitdefender Knowledge Base este o bază online de informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea virușilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Knowledge Base este deschisă pentru public și putând fi efectuate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide pentru informații sau rapoartele de eroare care vin din partea clienților Bitdefender ajung la Baza de date Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor, articole informaționale pentru a completa fișierele de ajutor ale produsului.

Bitdefender Knowledge Base pentru produsele business este disponibilă oricând la adresa http://www.bitdefender.ro/support/business.html.

Forum asistenţă Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții. Puteți posta orice probleme sau întrebări legate de produsul dumneavoastră Bitdefender.

Tehnicienii pentru suport tehnic ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator Bitdefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al Bitdefender este disponibil la http://forum.bitdefender.com, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română. Faceți clic pe link-ul **Protecție Bussiness** pentru a accesa secțiunea dedicată produselor business.

Documentaţie de produs

Documentația de produs este sursa cea mai completă de informații despre produs.

Puteți consulta și descărca cea mai recentă versiune a documentației pentru produsele business Bitdefender la Centrul de asistență > Documentație.

12.2. Solicitarea de asistenţă profesională

Ne puteți contacta pentru asistență prin intermediul Centrului de asistență online:

1. Mergeți la http://www.bitdefender.ro/support/contact-us.html.
2. Folosiți formularul de contact pentru a deschide un tichet de asistență prin e-mail sau accesați o altă opțiune de contact disponibilă.

12.3. Utilizarea Support Tool

Small Office Security Support Tool este conceput pentru a ajuta utilizatorii și pentru a sprijini tehnicienii în obținerea cu ușurință a informațiilor necesare pentru rezolvarea problemelor. Rulați Support Tool pe calculatoarele afectate și trimiteți arhiva rezultată cu informațiile de depanare la reprezentantul de asistență alBitdefender .

Pentru a utiliza Support Tool:

1. Descărcați Support Tool și distribuiți-l către calculatoarele afectate. Pentru a descărca Support Tool:
   a. Conectați-vă la Control Center utilizând contul dumneavoastră.
   b. Faceți clic pe link-ul **Suport tehnic** din colțul dreapta jos al consolei.

c. Link-uri de download sunt disponibile la secțiunea **Suport**. Sunt disponibile două versiuni: una pentru sisteme pe 32 de biți, cealaltă pentru sisteme pe 64 de biți. Asigurați-vă că utilizați versiunea corectă atunci când rulați Support Tool pe un calculator.

2. Rulați Support Tool local, pe fiecare dintre calculatoarele afectate.
   a. Selectați căsuța de acceptare și faceți clic pe **Înainte**.
   b. Completați formularul cu datele necesare:
      i. Introduceți adresa de e-mail.
      ii. Introduceți numele dumneavoastră.
      iii. Alegeți-vă țara din meniul corespunzător.
      iv. Introduceți o descriere a problemei întâmpinate.
      v. Opțional, puteți încerca să reproduceți problema înainte de a începe să colectați date. În acest caz, procedați după cum urmează:
         A. Activați opțiunea **Try to reproduce the issue before submitting**.
         B. Faceți clic pe **Înainte**.
         C. Selectați tipul de problemă pe care ați întâlnit-o.
         D. Faceți clic pe **Înainte**.
         E. Reproduceți problema pe calculator. Când ați terminat, reveniți la Support Tool și selectați opțiunea **I have reproduced the issue**.
   c. Faceți clic pe **Înainte**. Instrumentul de suport adună informații despre produs, informatii legate de alte aplicații instalate pe calculator și informații privind configurația software și hardware.
   d. Așteptați finalizarea procesului.
   e. Faceți clic pe **Finalizare** pentru a închide fereastra. O arhivă zip a fost creată pe desktop.

      Trimiteți arhiva zip împreună cu cererea dumneavoastră la reprezentantul de asistență Bitdefender folosind formularul de bonul de asistență e-mail disponibil pe pagina **Suport tehnic** a consolei.

12.4. Informaţii de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani Bitdefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

12.4.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Centrul de asistență:http://www.bitdefender.ro/support/business.html
Documentație: documentation@bitdefender.com
Distribuitori locali:http://www.bitdefender.ro/partners
Programe de Parteneriat: partners@bitdefender.com
Relații Media: pr@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Site web:http://www.bitdefender.ro

12.4.2. Filialele Bitdefender

Reprezentanțele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Statele Unite ale Americii

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (vânzări&suport tehnic): 1-954-776-6262
Vânzări: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrul de asistență: http://www.bitdefender.com/support/business.html

Franţa

PROFIL TECHNOLOGY
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
E-mail: supportpro@profiltechnology.com
Site web: http://www.bitdefender.fr
Centrul de asistență: http://www.bitdefender.fr/support/professionnel.html

Spania

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (birou&vânzări): (+34) 93 218 96 15
Telefon (suport tehnic): (+34) 93 502 69 10
Vânzări: comercial@bitdefender.es
Site web: http://www.bitdefender.es
Centrul de asistență: http://www.bitdefender.es/support/business.html

Germania

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Telefon (birou&vânzări): +49 (0)2301 91 84 222
Telefon (suport tehnic): +49 (0)2301 91 84 444
Vânzări: vertrieb@bitdefender.de
Site web: http://www.bitdefender.de
Centrul de asistență: http://www.bitdefender.de/support/business.html

Marea Britanie şi Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (vânzări&suport tehnic): +44 (0) 8451-305096
E-mail: info@bitdefender.co.uk
Vânzări: sales@bitdefender.co.uk
Site web: http://www.bitdefender.co.uk
Centrul de asistență: http://www.bitdefender.co.uk/support/business.html

România

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax: +40 21 2641799
Telefon (vânzări&suport tehnic): +40 21 2063470
Vânzări: sales@bitdefender.ro

Site web: http://www.bitdefender.ro
Centrul de asistență: http://www.bitdefender.ro/support/business.html

Emiratele Arabe Unite

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (vânzări&suport tehnic): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vânzări: sales@bitdefender.com
Web: http://www.bitdefender.com/world
Centrul de asistență: http://www.bitdefender.com/support/business.html

A. Anexe

A.1. Lista de tipuri de fişiere de aplicaţii

Motoarele de scanare antimalware incluse în soluțiile de securitate Bitdefender pot fi configurate să scaneze numai fișiere aplicație (sau program). Fișierele de program sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere.

Această categorie conține fișiere cu următoarele extensii:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu;
acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat;
bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek;
dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe;
ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd;
ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam;
maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt;
mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub;
puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr;
script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx;
tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm;
wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls;
xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

A.2. Utilizarea variabilelor de sistem

Unele dintre setările disponibile în consolă necesită specificarea calea pe calculatoarele țintă. Se recomandă să utilizați variabile de sistem (dacă este cazul) pentru a vă asigura că o cale este corectă pe toate calculatoarele țintă.

Mai jos este lista variabilelor de sistem predefinite:

`%ALLUSERSPROFILE%`
: Directorul profilului All Users. Cale obișnuită:

  `C:\Documents and Settings\All Users`

`%APPDATA%`
: Directorul Application Data a utilizatorului înregistrat. Cale obișnuită:

- Windows XP:

`C:\Documents and Settings\{username}\Application Data`

- Windows Vista/7:

  `C:\Users\{username}\AppData\Roaming`

`%HOMEPATH%`
Directoarele utilizatorului. Cale obișnuită:

- Windows XP:

  `\Documents and Settings\{username}`

- Windows Vista/7:

  `\Users\{username}`

`%LOCALAPPDATA%`
Fișiere temporare ale aplicațiilor. Cale obișnuită:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`
Directorul Program Files. O cale tipică este `C:\Program Files`.

`%PROGRAMFILES(X86)%`
Folderul Program Files pentru aplicații pe 32 de biți (pe sistemele pe 64 de biți). Cale obișnuită:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`
Directorul Common Files. Cale obișnuită:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`
Folderul Common Files pentru aplicații pe 32 de biți (pe sistemele pe 64 de biți). Cale obișnuită:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`
Directorul Windows sau SYSROOT. O cale tipică este `C:\Windows`.

Vocabular

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiaşi produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

Bitdefender dispune de modulul său propriu care realizează actualizarea automată sau manuală.

adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Backdoor

Reprezintă o breșă de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanța produsului din partea furnizorului.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în bara de sarcini Windows (de obicei în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele legate de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox și Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafice cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Cookie

În domeniul Internetului, cookie-urile reprezintă mici fișiere ce conțin informații despre fiecare calculator care pot fi analizate și folosite de către cei care publică reclame pentru a vă urmări interesele și preferințele online. În acest domeniu, tehnologia cookie-urilor este în curs de dezvoltare, iar intenția este de a afișa direct acele anunțuri care corespund intereselor dumneavoastră. Această facilitate are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizați doar acele anunțuri despre subiecte care vă interesează. Pe de altă parte, cookie-urile implică de fapt o "monitorizare" și "urmărire" a site-urilor vizitate și a link-urilor accesate. Astfel, în mod logic, părerile sunt împărțite în ceea ce privește confidențialitatea și mulți se simt jigniți de faptul că sunt văzuți ca un simplu "număr SKU" (este vorba de codul de bare de pe spatele ambalajelor care este scanat pe bandă la supermarket). Deși acest punct de vedere poate fi considerat extrem, în anumite cazuri el reprezintă chiar ceea ce se întâmplă în realitate.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei litere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "c" pentru fișierele sursă scrise în limbajul C, "ps" pentru fișiere PostScript sau "txt" pentru fișierele text oarecare.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. Bitdefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați.

Keyloggerele nu au o natură periculoasă. Pot fi folosite în scopuri legitime, cum ar fi monitorizarea activității angajaților sau a companiilor subordonate. Cu toate acestea, utilizarea lor de către infractorii cibernetici în scopuri negative este din ce în ce mai răspândită (de exemplu, pentru colectarea informațiilor cu caracter privat, cum ar fi acreditările de înregistrare și codurile numerice personale).

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Malware

Malware este termenul generic pentru software-ul care este proiectat pentru a face rău - o contracție a " malicious software Acesta nu este încă în uz universal, dar popularitatea sa ca un termen general pentru viruși, cai troieni, viermi, și coduri malware mobile este în creștere.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături de viruși cunoscuți. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului, și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Semnătură malware

Semnăturile malware sunt fragmente de coduri extrase din mostre reale de malware. Acestea sunt utilizate de către programele antivirus pentru a realiza o identificare după model și detectare a programelor malware. Semnăturile sunt utilizate și pentru a elimina codul malware din fișierele infectate.
Baza de date cu semnături malware a Bitdefender reprezintă o colecție de semnături malware actualizate în fiecare oră de către cercetătorii malware ai Bitdefender.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.