

Bitdefender® ENTERPRISE

SMALL OFFICE SECURITY

Ghid de pornire rapidă
pentru Parteneri >>

Small Office Security

Ghid de pornire rapidă pentru Parteneri

Publicat 2015.01.05

Copyright© 2015 Bitdefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al Bitdefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

Avertisment și declinarea responsabilității. Acest produs și documentația aferentă sunt protejate de legea drepturilor de autor. Informațiile incluse în acest document sunt furnizate „ca atare”, fără nicio garanție. Deși s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuți responsabili față de nici o persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest document conține linkuri către siteuri web aparținând unor terți, care nu se află sub controlul Bitdefender; prin urmare, Bitdefendernu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților al căror link este furnizat în acest document vă aparține în totalitate. Bitdefender furnizează aceste linkuri exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că Bitdefender susține sau își asumă responsabilitatea pentru conținutul siteurilor către care duc acestea.

Mărci înregistrate. Acest document poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora și sunt redată ca atare.

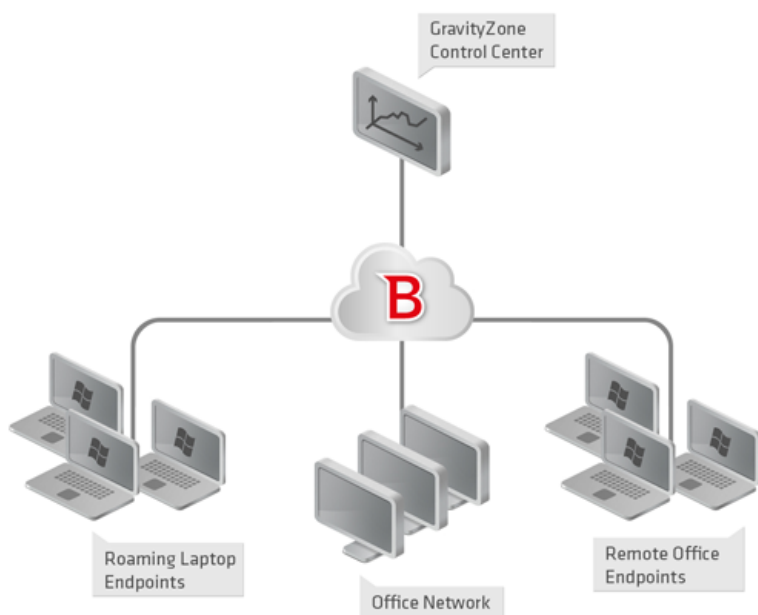


Cuprins

1. Despre Small Office Security	1
2. Introducere	3
2.1. Conectarea la Control Center	3
2.2. Control Center dintr-o privire	4
2.2.1. Vedere de ansamblu asupra Control Center	4
2.2.2. Date tabelare	5
2.2.3. Bare de instrumente pentru acțiuni	6
2.2.4. Meniul contextual	7
2.3. Administrarea contului dumneavoastră	7
2.4. Administrarea companiei dumneavoastră	8
2.5. Schimbarea parolei de conectare	10
3. Administrare conturi	12
3.1. Administrarea conturilor de companie	12
3.1.1. Crearea companiilor partener	13
3.1.2. Crearea companiilor client	15
3.2. Administrarea conturilor de utilizator	17
3.2.1. Rolurile contului de utilizator	17
3.2.2. Drepturile de utilizare	19
3.2.3. Crearea de conturi de utilizator	19
4. Administrarea serviciului pentru clienții dumneavoastră	21
4.1. Instalare și setare	21
4.1.1. Pregătirea pentru instalare	21
4.1.2. Instalarea serviciului pe calculatoare	22
4.1.3. Organizare calculatoare (opțional)	31
4.1.4. Crearea și configurarea unei politici de securitate	32
4.2. Monitorizarea stării de securitate	36
4.3. Scanarea calculatoarelor administrate	37
5. Obținere ajutor	39
A. Cerințe	40
A.1. Cerințe Security for Endpoints	40
A.1.1. Sisteme de operare suportate	40
A.1.2. Cerințe hardware	41
A.1.3. Browsere compatibile	41
A.1.4. Porturile de comunicare Small Office Security	42
A.2. Cum funcționează opțiunea de descoperire a rețelei	42
A.2.1. Mai multe despre serviciul Microsoft Computer Browser	43
A.2.2. Cerințe pentru aplicația de descoperire a rețelei	44

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

Security for Endpoints poate fi configurat și administrat utilizând Control Center, o interfață web găzduită de Bitdefender.

Control Center servește și ca și consolă de administrare pentru partenerii Bitdefender care comercializează serviciul. Le permite acestora să creeze și să administreze conturi pentru clienții lor și, opțional, să administreze serviciul pentru clienții utilizatori finali.

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**.

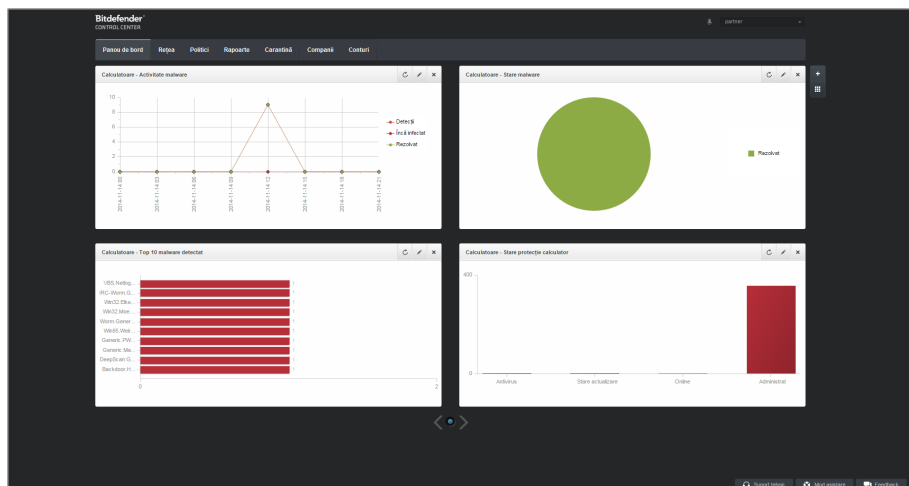


Notă

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

Partenerii 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

Vizualizați companiile și rețelele dumneavoastră, instalați protecția, aplicați politicile de administrare a setărilor 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 calculatoarele și companiile administrate.

Carantină

Administrați de la distanță fișierele aflate în carantină.

Companii

Creați și administrați conturile de companie (companiile partener și companiile client).

Conturi

Creați și administrați conturi de utilizator pentru companiile de tip partener și client cărora le furnizați servicii.

În acest meniu puteți găsi, de asemenea, pagina **Activitate utilizator**, care permite accesarea jurnalului de activitate al utilizatorului.



Notă

Pentru partenerii fără drepturi de administrare a rețelei, sunt disponibile în meniu doar opțiunile de setări generale și de monitorizare.

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:

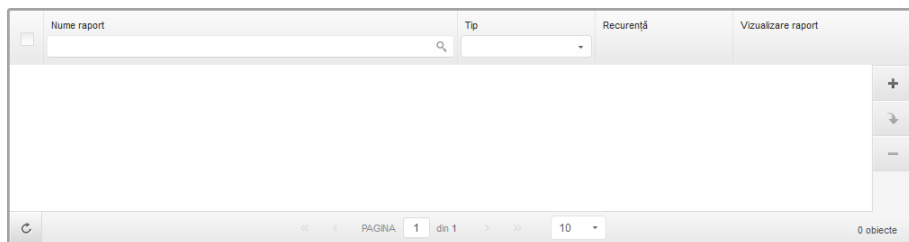
- **Contul meu.** Faceți clic pe această opțiune pentru a administra detaliile și preferințele contului dumneavoastră de utilizator.
- **Compania mea.** Faceți clic pe această opțiune pentru a administra detaliile și preferințele contului dumneavoastră de companie.
- **Integrări.** Faceți clic pe această opțiune pentru a administra integrarea Small Office Security cu alte platforme de administrare.
- **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:

- **Support 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 căutării 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.

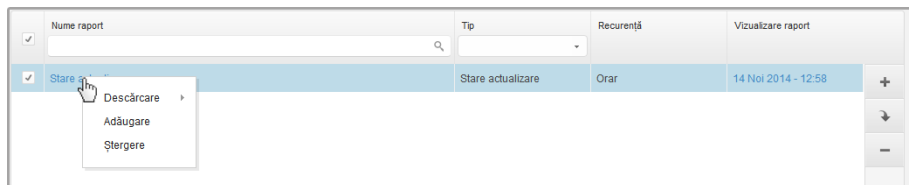
- Descărcare rapoarte generate de un raport programat.
- Ștergerea unui raport programat.



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.

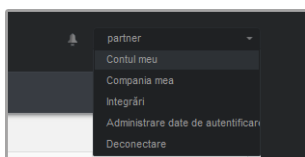


Pagina de Rapoarte - Meniul contextual

2.3. Administrarea contului dumneavoastră

Pentru a verifica sau modifica detaliile și setările contului dumneavoastră:

1. Îndreptați cursorul către numele de utilizator 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

Pentru a verifica sau modifica detaliile companiei și setările licenței:

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

Date companie

Nume companie:

Adresă:

ID:

Telefon:

Logo: Logo-ul trebuie să aibă dimensiunea de 200x30 px și trebuie să fie în format png sau jpg

Permiteți altor companii să administreze securitatea acestei companii

Licență

Cheie de licență:

Expiră la: 06 Oct 2018
Utilizat: 19
Disponibil pentru instalare: 313
Rezervat: 20
Total: 333

Bitdefender Partner [Schimbare](#)

Nume companie:

ID:

Adresă:

Telefon:

[Asociere companie cu MyBitdefender \(opțional\)](#)

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 totalul de utilizări aferente unei licențe lunare (excluzând utilizările folosite și rezervate).
 - **Rezervat**: numărul total de utilizări rezervate pentru alte companii din totalul aferent licenței dvs. lunare.
 - **Total**: numărul total de utilizări disponibile pe cheia dvs. de licență.
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.

Se recomandă să procedați după cum urmează:

- 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 utilizator 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. Administrare conturi

În calitate de partener al Bitdefender, va trebui să creați și să administrați conturi în Control Center pentru companiile de tip partener și client cărora le furnizați servicii. Suplimentar, veți administra licențele pentru acest serviciu ale companiilor de tip utilizator-final.

Mai întâi trebuie să creați conturi pentru companiile dvs. de tip partener sau client. Pentru fiecare companie administrată puteți crea un singur cont. Apoi, trebuie să creați conturile de utilizator asociate companiilor corespunzătoare. Pentru fiecare dintre companiile dumneavoastră puteți oricât de multe conturi de utilizator doriți.

- [Administrarea conturilor de companie](#)
- [Administrarea conturilor de utilizator](#)

3.1. Administrarea conturilor de companie

Puteți crea și administra conturile de companie din pagina **Companii**.

	Nume	Tip	Administrat	Utilizare licență	Valabilitate licență	
<input type="checkbox"/>	Client A	Client	Da	Utilizat: 0, Total: 9	niciodată	+
<input type="checkbox"/>	Comp CW	Client	Da	Utilizat: 0, Total: nelimitat	28 Dec 2014	☑
<input type="checkbox"/>	Partner 1	Partener	Da	Utilizat: 0, Total: 333	niciodată	☑
<input type="checkbox"/>	Partner 2	Partener	Da	Utilizat: 0, Total: nelimitat	02 Ian 2015	☑
<input type="checkbox"/>	Comp Y	Client	Da	Utilizat: 0, Total: nelimitat	28 Dec 2014	-

PAGINA 1 din 1 10 5 obiecte

Pagina Companii

Puteți crea două tipuri de conturi de companie:

1. **Companiile partener**, destinate companiilor care vând Small Office Security către alte companii (utilizatori finali, distribuitori sau reselleri ai serviciului).

Companiile partener pot oferi servicii cu valoare adăugată cu ajutorul Small Office Security, prin care pot administra direct rețelele de calculatoare ale clienților.

De asemenea, companiile partener pot folosi Small Office Security pentru a-și proteja rețelele, cu condiția ca acestea să aibă activat dreptul de **Administrare rețele** și o cheie de licență valabilă atribuită contului lor de companie.

O companie partener trebuie să fie conectată la cel puțin un cont de utilizator de tip partener.

2. **Companiile client**, destinate companiilor care utilizează serviciul Security for Endpoints pentru a își proteja rețelele de calculatoare. Aceste companii își pot instala, configura, administra și monitoriza propria protecție.

O companie client trebuie să fie conectată la cel puțin un cont de utilizator de tip administrator de companie.

3.1.1. Crearea companiilor partener

Pentru a crea o companie partener:

1. Mergeți la pagina **Companii**.
2. Faceți clic pe butonul **+ Adăugare** din dreapta tabelului. Este afișată fereastra **Companie nouă**.
3. La secțiunea **Detalii companie nouă**, completați detaliile companiei.
 - **Nume**. Introduceți denumirea companiei partener. Numele companiei trebuie să fie unic.
 - **Adrese**. Puteți adăuga adresa companiei partener.
 - **Telefon**. Puteți adăuga numărul de telefon al companiei partener.
 - **Logo**. Puteți adăuga sigla companiei partener. Toate rapoartele și notificările prin e-mail emise de această companie vor include sigla.
 - Faceți clic pe **Schimbare** pentru a selecta sigla din calculatorul dumneavoastră.
 - Faceți clic pe **Implicit** pentru a șterge imaginea și a reseta la imaginea furnizată de Bitdefender.
 - Selectați **Partener** la tipul companiei.
 - Utilizați opțiunea **Administrare rețele** pentru a configura dreptul companiei partener de administrare a securității rețelelor clienților săi.
 - Atunci când această opțiune este activă, compania partener va avea drept de vizualizare și control asupra rețelelor companiilor subordonate.
 - Atunci când această opțiune este inactivă, compania partener poate crea alte companii și poate gestiona licențele pentru servicii, fără a avea acces la rețelele acestora. Această configurație este potrivită pentru companiile partener care operează exclusiv ca reselleri de servicii.
 - În mod implicit, fiecare companie nou creată poate fi administrată de toate companiile mamă. Puteți bloca accesul companiilor mamă la rețeaua companiei noi dezactivând opțiunea **Permite altor companii să administreze securitatea acestei companii**.

Compania nu va fi vizibilă pentru ceilalți parteneri din rețeaua dumneavoastră și nu veți mai putea modifica sau administra subscripțiile pentru această companie.



Important

Odată dezactivată, această opțiune nu mai poate fi restabilită.

4. Sub **Licență**, puteți configura subscripția unei companii partener care utilizează și Small Office Security pentru administrarea propriei rețele.

- Există trei opțiuni pentru licențierea unei companii aferente contului dumneavoastră:
 - **Evaluare**. Această opțiune alocă noii companii o cheie de licență de testare generată automat.
 - **Licență**, pentru o subscripție plătită. În acest caz, introduceți cheia de licență corespunzătoare tipului de subscripție a clientului.

Faceți clic pe butonul **Verificare** și așteptați până când Control Center extrage informațiile despre cheia de licență introdusă.



Notă

Atunci când efectuați licențierea unei companii partener, trebuie activată opțiunea **Administrare rețele**.



Avertisment

Debifarea opțiunii **Administrare rețele** în timpul modificării unei companii deja create va șterge, totodată, și cheia de licență asociată și toate calculatoarele protejate din baza de date.

- **Abonament lunar**, pentru a partaja o cheie de licență cu utilizare lunară de către mai multe companii subordonate contului dumneavoastră. Această opțiune este disponibilă numai dacă una dintre companiile mamă are o cheie de licență pentru utilizare lunară.

În acest caz, toate companiile subordonate companiei mamă licențiate cu cheia de licență cu utilizare lunară vor împărți același număr de utilizări ale licenței.

De asemenea, puteți limita numărul de utilizări alocate companiei dintr-o cheie de licență lunară partajată, selectând opțiunea **Rezervare utilizări**. În acest caz, specificați numărul de utilizări pe care îl doriți în câmpul corespunzător. Companiei i se va permite să licențieze doar numărul de utilizări specificate.

5. Puteți furniza datele de autentificare ale contului **My Bitdefender** al partenerului, dacă acestea sunt disponibile.
6. Opțional, puteți continua cu crearea unui cont de utilizator pentru partener derulând în jos fereastra de configurare. Introduceți detaliile contului în secțiunea **Adăugare cont**

nou. Ulterior, puteți vizualiza și administra contul de utilizator al partenerului din pagina **Conturi**.



Notă

De asemenea, puteți crea mai târziu conturile de utilizator corespunzătoare. Cu toate acestea, dacă opțiunea **Permite altor companii să administreze securitatea acestei companii** este dezactivată, acest pas este obligatoriu.

7. Faceți clic pe **Salvare** pentru a crea contul de companie. Noul cont va apărea în lista de companii.

În cazul în care ați configurat și contul de utilizator asociat noii companii, se va transmite un e-mail automat cu detaliile de autentificare la adresa de e-mail furnizată.

Odată ce contul a fost creat, partenerul dumneavoastră poate începe să contruiască și să își administreze rețeaua de clienți Small Office Security.

3.1.2. Crearea companiilor client

Pentru a crea o companie client:

1. Mergeți la pagina **Companii**.
2. Faceți clic pe butonul **+ Adăugare** din dreapta tabelului. Este afișată fereastra **Companie nouă**.
3. La secțiunea **Detalii companie nouă**, completați detaliile companiei.
 - **Nume.** Introduceți denumirea companiei client. Numele companiei trebuie să fie unic.
 - **Adrese.** Puteți adăuga adresa companiei client.
 - **Telefon.** Puteți adăuga numărul de telefon al companiei client.
 - **Logo.** Puteți adăuga sigla companiei client. Toate rapoartele și notificările prin e-mail emise de această companie vor include sigla.
 - Faceți clic pe **Schimbare** pentru a selecta sigla din calculatorul dumneavoastră.
 - Faceți clic pe **Implicit** pentru a șterge imaginea (resetare la setările implicite).
 - Selectați **Client** la tipul companiei.
 - În mod implicit, fiecare companie nou creată poate fi administrată de toate companiile mamă. Puteți bloca accesul companiilor mamă la rețeaua companiei noi dezactivând opțiunea **Permite altor companii să administreze securitatea acestei companii**. Compania nu va fi vizibilă pentru ceilalți parteneri din rețeaua dumneavoastră și nu veți mai putea modifica sau administra subscripțiile pentru această companie.



Important

Odată dezactivată, această opțiune nu mai poate fi restabilită.

4. Sub **Licență**, puteți configura setările aferente subscripției clientului.

- Există trei opțiuni pentru licențierea unei companii aferente contului dumneavoastră:
 - **Evaluare**. Această opțiune alocă noii companii o cheie de licență de testare generată automat.
 - **Licență**, pentru o subscripție plătită. În acest caz, introduceți **Cheia de licență** corespunzătoare tipului de subscripție a clientului.

Faceți clic pe butonul **Verificare** și așteptați până când Control Center extrage informațiile despre cheia de licență introdusă.

- **Abonament lunar**, pentru a partaja o cheie de licență cu utilizare lunară de către mai multe companii subordonate contului dumneavoastră. Această opțiune este disponibilă numai dacă una dintre companiile mamă are o cheie de licență pentru utilizare lunară.

În acest caz, toate companiile subordonate companiei mamă licențiate cu cheia de licență cu utilizare lunară vor împărtăși același număr de utilizări ale licenței.

De asemenea, puteți limita numărul de utilizări alocate companiei dintr-o cheie de licență lunară partajată, selectând opțiunea **Rezervare utilizări**. În acest caz, specificați numărul de utilizări pe care îl doriți în câmpul corespunzător. Companiei i se va permite să licențieze doar numărul de utilizări specificate.

5. Puteți furniza datele de autentificare ale contului **My Bitdefender** al clientului, dacă acestea sunt disponibile.
6. Opțional, puteți continua cu crearea unui cont de utilizator pentru administratorul de companie derulând în jos fereastra de configurare. Introduceți detaliile contului în secțiunea **Adăugare cont nou**. Ulterior, puteți vizualiza și administra contul de utilizator al clientului din pagina **Conturi**.



Notă

De asemenea, puteți crea mai târziu conturile de utilizator corespunzătoare. Cu toate acestea, dacă opțiunea **Permite altor companii să administreze securitatea acestei companii** este dezactivată, acest pas este obligatoriu.

7. Faceți clic pe **Salvare** pentru a crea contul de companie. Noul cont va apărea în lista de companii.

În cazul în care ați configurat și contul de utilizator asociat noii companii, se va transmite un e-mail automat cu detaliile de autentificare la adresa de e-mail furnizată.

Odată ce contul a fost creat, clientul dumneavoastră poate începe să utilizeze serviciul. În funcție de relația dumneavoastră de afaceri, acest serviciu poate fi administrat de către client sau de compania dumneavoastră.

3.2. Administrarea conturilor de utilizator

Small Office Security folosește un ecosistem integrat de distribuție și instalare în care diferite tipuri de conturi de utilizator sunt asociate într-o structură ierarhică din fiecare companie. Fiecare cont are vizibilitate asupra sub-conturilor. Din motive de responsabilitate, acțiunile utilizatorilor sunt documentate în jurnalele de activitate, atât pentru conturile principale, cât și pentru cele secundare.

Pentru a permite angajaților companiilor din contul dumneavoastră să acceseze Small Office Security, trebuie să creați conturi de utilizator asociate companiilor lor. Fiecare cont de companie trebuie să fie asociat cel puțin unui singur cont de utilizator cu drepturi de administrare corespunzătoare. Pentru fiecare rol de cont de utilizator, puteți personaliza accesul la caracteristicile Small Office Security sau la anumite componente ale rețelei din care face parte.

Puteți crea și gestiona conturile de utilizator pe pagina **Conturi**.

	Nume complet	E-mail	Rol	Companie
<input type="checkbox"/>				Partner 1
<input type="checkbox"/>	Partner 1	partner1@bd.com	Partener	Partner 1
<input type="checkbox"/>	Comp Admin 1	compadmin1@bd.com	Administrator companie	Partner 1
<input type="checkbox"/>	Reporter 1	reporter1@bd.com	Raportor	Partner 1
<input type="checkbox"/>	Net Admin 1	netadmin1@bd.com	Administrator rețea	Partner 1

Pagina Conturi

3.2.1. Rolurile contului de utilizator

La crearea unui cont de utilizator, puteți alege unul dintre rolurile predefinite sau puteți crea un rol personalizat. În calitate de partener, puteți crea următoarele roluri ale conturilor de utilizator:

1. **Partener** - Adecvat pentru distribuitorii și resellerii Small Office Security. Utilizatorii cu conturi de partener pot crea și administra alte companii. La extinderea lanțului de distribuție, aceștia creează conturi de companie subordonate. La vânzarea direct către utilizatorii finali, aceștia creează conturi de companie pentru clienți. Utilizatorii de tip partener pot administra licențele companiilor subordonate și pot gestiona, de asemenea, conturile de utilizator asociate acestor calculatoare. Deoarece partenerii pot acționa ca furnizori de servicii de securitate, aceștia au drepturi de administrare asupra setărilor de

securitate pentru conturile de client subordonate. Conturile de utilizator de tip partener pot administra, de asemenea, securitatea companiei proprii.

2. **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.
3. Conturile de **Administrator de rețea** sunt conturi interne cu privilegii administrative asupra întregii instalări Small Office Security de la nivelul companiei sau asupra unui anumit grup de calculatoare. Administratorii de rețea sunt responsabili pentru gestionarea activă a setărilor de securitate Small Office Security.
4. **Raportor** - Conturile de raportor sunt conturi interne numai pentru consultare. Acestea permit doar accesul la rapoarte și la jurnalele de activitate ale utilizatorilor. Astfel de conturi pot fi alocate personalului cu responsabilități de monitorizare sau altor angajați care trebuie să fie ținuti la curent cu starea de securitate.
5. **Custom** - conturi de utilizator predefinite includ o anumită combinație de drepturi de utilizatorilor. 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 privind drepturile utilizatorilor, vă rugăm să consultați „[Drepturile de utilizare](#)” (p. 19).

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

3.2.2. Drepturile de utilizare

- **Administrare companii.** La extinderea lanțului de distribuție, utilizatorii de tip partener creează conturi de companie subordonate. La vânzarea direct către utilizatorii finali, aceștia creează conturi de companie pentru clienți. De asemenea, utilizatorii de tip partener pot edita, suspenda sau șterge companiile din contul lor. Acest privilegiu este specific conturilor de tip partener.
- **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.

Administratorii din cadrul companiilor partener pot avea drepturi de administrare asupra securității rețelelor companiilor client.

- **Administrare rapoarte.** Creați, modificați, ștergeți rapoarte și administrați panoul de bord.

3.2.3. 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. Conectați-vă la Control Center.
2. Mergeți la pagina **Conturi**.
3. Faceți clic pe butonul **+ Adăugare** din dreapta tabelului. Este afișată o fereastră de configurare.
4. La secțiunea **Detalii**, completați detaliile de utilizator.
 - **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.
- **Companie.** Selectați compania de care aparține noul cont de utilizator.

5. 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 „[Rolurile contului de utilizator](#)” (p. 17)
 - **Drepturi.** Fiecare rol de utilizator predefinit are o anumită configurație a [drepturilor](#). Cu toate acestea, puteți selecta doar drepturile de care aveți nevoie. În acest caz, rolul utilizatorului se modifică în **Personalizat**.

De exemplu, un utilizator cu rol de partener care acționează exclusiv în calitate de distribuitor de servicii nu trebuie să administreze rețelele. La crearea acestui tip de cont de utilizator, puteți dezactiva dreptul de administrare a rețelelor și rolul de utilizator devine unul de **Partener** personalizat.
6. **Selectare ținte.** Derulați în jos în fereastra de configurare pentru a afișa secțiunea aferentă țăintelor. Selectați grupurile de rețea la care va avea acces utilizatorul. Puteți restricționa accesul utilizatorilor la anumite zone din rețea.
7. 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**.

4. Administrarea serviciului pentru clienții dumneavoastră

Pe lângă conturile clienților și administrarea abonamentelor, conturile pentru parteneri permit de asemenea setarea și administrarea serviciului pentru clienții utilizatori finali. Astfel, partenerii Bitdefender pot furniza clienților servicii cu valoare adăugată, administrate integral.

În cele ce urmează, veți afla elementele de bază pentru instalarea și administrarea serviciului pentru clienții utilizatori finali dintr-un cont de partener.

4.1. Instalare și setare

Instalarea și setarea se fac cu ușurință. Aceștia sunt principalii pași:

1. [Pasul 1 - Pregătirea pentru instalare.](#)
2. [Pasul 2 - Instalarea serviciului pe calculatoare.](#)
3. [Pasul 3 - Organizarea calculatoarelor în grupuri \(opțional\).](#)
4. [Pasul 4 - Crearea și configurarea unei politici de securitate.](#)

Pentru primii doi pași, veți avea nevoie de asistență din partea clientului dumneavoastră, cum ar fi accesul local și este posibil să fie solicitate informații de autentificare pe calculator pentru a îi realiza. Ceilalți doi pași sunt executați din Control Center. Asigurați-vă că dumneavoastră și clientul conveniți asupra setărilor de securitate care vor fi aplicate pe calculatoare.

4.1.1. 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.

4.1.2. Instalarea serviciului pe calculatoare

Security for Endpoints a fost creat pentru stații de lucru, laptop-uri și servere ce funcționează cu Microsoft® 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.

Există două metode de instalare:

- **Instalare locală.** Descărcați pachetele de instalare din Control Center pe calculatoarele individuale și apoi executați local instalarea Endpoint Security. O alta opțiune este să descărcați pachetul, să îl salvați într-un spațiu partajat în rețea și să trimiteți utilizatorilor

din companie invitații prin e-mail cu link-ul pachetului, rugându-i să descarce și să instaleze protecția pe propriile calculatoare. Instalarea locală este ghidată de un asistent de instalare.

- **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. Apoi, protecția Security for Endpoints poate fi instalată de la distanță de pe consolă pe alte calculatoare din rețea. Instalarea la distanță este efectuată în fundal, fără ca utilizatorul să știe despre acest lucru.

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. 23).

Instalare locală

Instalarea locală necesită descărcarea din Control Center și executarea pachetului de instalare pe fiecare calculator țintă. Puteți crea diferite pachete de instalare conform cerințelor specifice ale fiecărui calculator (de exemplu, calea de instalare sau limba interfeței utilizatorului).

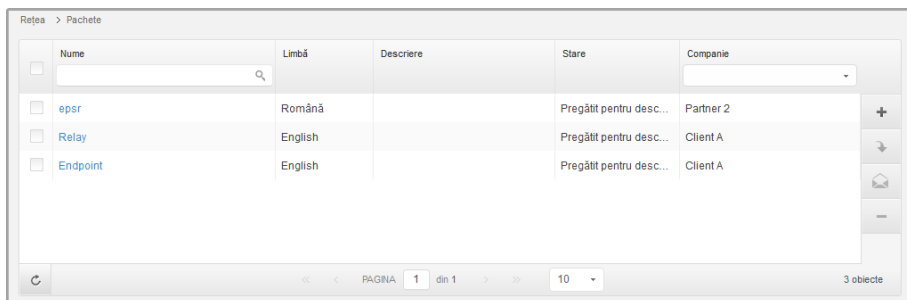
Crearea pachetelor de instalare Endpoint Security

Puteți crea pachete de instalare pentru propria companie sau pentru fiecare companie din cadrul contului dumneavoastră. Un pachet de instalare este valabil numai pentru compania pentru care a fost creat. Un pachet de instalare asociat unei anumite companii nu poate fi utilizat pe calculatoare care aparțin unei alte companii în Control Center.

Fiecare pachet de instalare va fi vizibil în Control Center numai pentru partenerul care a creat pachetul și pentru conturile de utilizator subordonate companiei asociate pachetului de instalare.

Pentru a crea un pachet de instalare Endpoint Security:

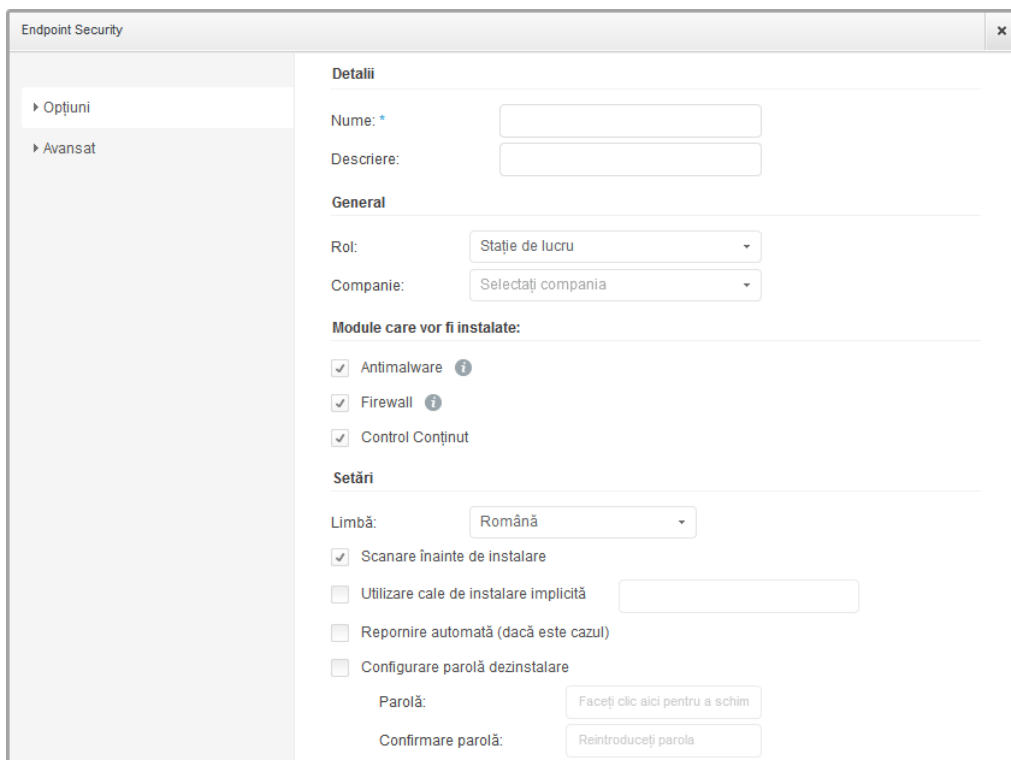
1. Conectați-vă și autentificați-vă la Control Center folosind propriul cont.
2. Mergeți la pagina **Rețea > Pachete**.



Nume	Limbă	Descriere	Stare	Companie
epsr	Română		Pregătit pentru desc...	Partner 2
Relay	English		Pregătit pentru desc...	Client A
Endpoint	English		Pregătit pentru desc...	Client A

Pagina pachete

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



Endpoint Security

Opțiuni

Avansat

Detalii

Nume: *

Descriere:

General

Rol: Stație de lucru

Companie: Selectați compania

Module care vor fi instalate:

Antimalware

Firewall

Control Conținut

Setări

Limbă: Română

Scanare înainte de instalare

Utilizare cale de instalare implicită

Repornire automată (dacă este cazul)

Configurare parolă dezinstalare

Parolă: Faceti clic aici pentru a schim

Confirmare parolă: Reintroduceți parola

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 ștergă 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 ale companiei țintă.

Descărcarea și Instalarea Endpoint Security

1. Conectați-vă la <https://gravityzone.bitdefender.com/> folosind contul de la 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. Rețineți că sunt disponibile două versiuni pentru Windows: una pentru sisteme pe 32 de biți, cealaltă pentru sisteme pe 64 de biți. Asigurați-vă că folosiți versiunea corectă pentru calculatorul pe care instalați.
5. Salvați fișierul în calculator.
6. Rulați pachetul de instalare.



Notă

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

7. 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.

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.

Pentru facilitarea instalării, Security for Endpoints include un mecanism de identificare automată a rețelei care permite detectarea calculatoarelor din aceeași rețea. Calculatoarele detectate sunt afișate ca și **calculatoare neadministrare** din pagina **Rețea**.

Pentru a permite identificarea rețelei și instalarea de la distanță, trebuie să aveți Endpoint Security instalat deja pe cel puțin un calculator din rețea. Acest calculator va fi utilizat pentru a scana rețeaua și a instala Endpoint Security pe calculatoarele neprotejate. Este posibil să dureze câteva minute până când restul calculatoarelor devin vizibile în Control Center.

Cerințe pentru instalarea de la distanță

Pentru ca descoperirea rețelei să funcționeze, trebuie îndeplinite o serie de cerințe. Pentru a afla mai multe, consultați „Cum funcționează opțiunea de descoperire a rețelei” (p. 42).

Pentru ca instalarea de la distanță să funcționeze:

- 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.

Rularea operațiilor de instalare Endpoint Security de la distanță


Pentru a rula o sarcină de instalare de la distanță:

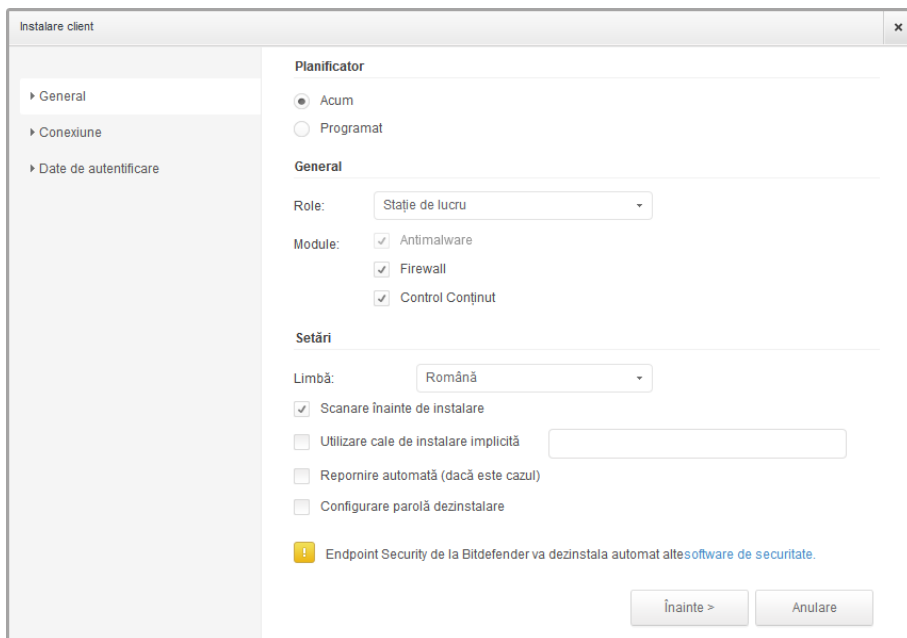
1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați grupul dorit din rețea din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.



Notă

Opțional, puteți aplica filtre pentru a afișa exclusiv calculatoarele neadministrare. 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.

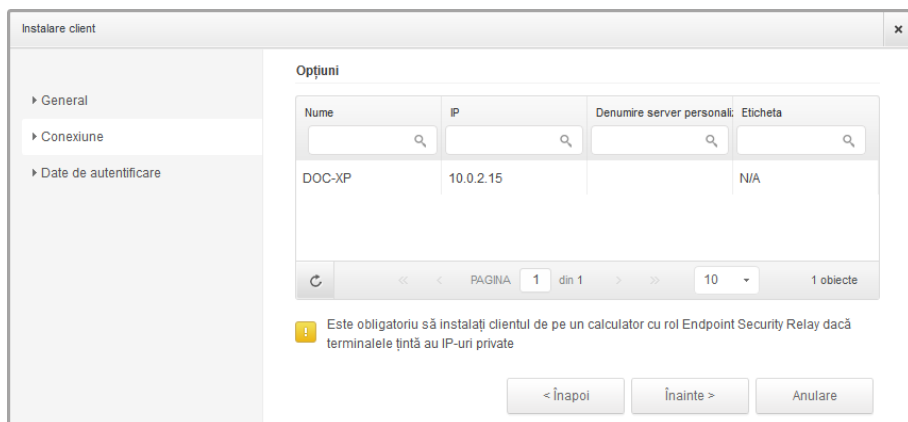


Notă

De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi deinstalarea 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.

<input type="checkbox"/>	Utilizator	Parolă	Descriere	Acțiune
				+
<input type="checkbox"/>	admin	*****		

Utilizatorul trebuie să fie în formatul DOMENIUUTILIZATOR, unde DOMENIU este numele NetBios al domeniului.

Pentru a adăuga datele SO necesare:

- 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**.

4.1.3. Organizare calculatoare (opțional)

Rețelele companiei sunt afișate în fereastra din stânga a paginii **Rețea**. Există un grup de bază implicit pentru fiecare dintre companiile dumneavoastră. Toate calculatoarele protejate sau detectate sunt plasate în mod automat în acest grup.

Dacă administrați un număr mai mare de calculatoare (zeci sau mai multe), va trebui probabil să le organizați în grupuri. Organizarea calculatoarelor în grupuri vă ajută să le administrați mai eficient. Beneficiul major este acela că puteți utiliza politicile de grup pentru a încheple diferite cerințe de securitate.

Puteți organiza calculatoarele prin crearea de grupuri sub grupul de bază și mutarea calculatoarelor în grupul adecvat.

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, Management, etc.).
- Necesitățile de securitate (desktopuri, laptopuri, servere etc.).
- Locația (sediul central, birouri locale, personal la distanță, birouri de acasă etc.).



Notă

- Grupurile create pot 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 dintr-un grup și din toate sub-grupurile acestuia, faceți clic pe meniul de filtre din partea superioară a tabelului și selectați **Tip > Calculatoare** și **Adâncime > Toate articolele recursiv**.

Pentru a organiza rețeaua unui client în grupuri:

1. Mergeți la pagina **Rețea**.
2. În panoul din partea stângă, la **Companii**, selectați compania clientului pe care doriți să o administrați.



Notă

Pentru companiile partenere din contul dumneavoastră care au drept de administrare a rețelelor, selectați grupul **Rețele**.

3. Faceți clic pe butonul + **Adăugare grup** din partea de sus a ferestrei din stânga.
4. Introduceți o denumire sugestivă pentru grup și faceți clic pe **OK**. Noul grup este afișat sub compania respectivă.
5. Urmați pașii anteriori pentru a crea grupuri suplimentare.
6. Mutați calculatoarele din grupul de bază în grupul potrivit:
 - a. Selectați căsuțele corespunzătoare calculatoarelor pe care doriți să le mutați.
 - b. Glisați și fixați selecția dumneavoastră în grupul dorit din panoul lateral stânga.

4.1.4. Crearea și configurarea unei politici de securitate

4.1.4. Crearea și configurarea unei politici de securitate

Odată instalată, protecția Security for Endpoints poate fi configurată și administrată din Control Center utilizând politicile de securitate. O politică specifică setările de securitate care vor fi aplicate pe calculatoarele țintă.

Imediat după instalare, politica implicită este alocată calculatoarelor, această politică fiind preconfigurată cu setările recomandate de protecție. Pentru a verifica setările implicite de protecție, mergeți la pagina **Politici** și faceți clic pe denumirea politicii implicite. Puteți modifica setările de protecție la nevoie și puteți de asemenea configura funcțiile suplimentare de protecție, prin crearea și alocarea de politici personalizate.



Notă

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. De exemplu, puteți configura diferite politici pentru stațiile de lucru de la birou, laptopuri și servere. O altă metodă este de a crea politici separate pentru fiecare dintre rețelele dumneavoastră.

Iată ce trebuie să știți despre politici:

- Politicile sunt create pe pagina **Politici** și alocate unor stații de lucru din pagina **Rețea**.
- Stațiile de lucru nu pot avea mai multe politici active simultan.
- Politicile sunt expediate către calculatoarele țintă imediat după crearea sau modificarea acestora. Setările ar trebui aplicate pe stațiile de lucru în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un calculator este offline, setările vor fi aplicate imediat ce calculatorul 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 suprascrive prin aplicarea unei alte politici obiectelor țintă.
- Calculatoarele asociate unui cont de companie pot fi administrate prin intermediul politicilor de către administratorul companiei și de către partenerul care a creat contul. Politicile create din contul de partener nu pot fi editate din contul de companie.

Pentru a crea o politică nouă:

1. Mergeți la pagina **Politici**.
2. Faceți clic pe butonul **+ Adăugare** din dreapta tabelului. Această comandă generează o politică nouă pornind de la modelul politicii implicite.
3. Introduceți un nume sugestiv pentru politică. Când alegeți o denumire, luați în considerare scopul și ținta politicii.
4. Apoi, configurați setările politicii. Setările implicite de securitate sunt recomandate pentru majoritatea situațiilor.
5. Faceți clic pe **Salvare**. Noua politică este enumerată în tabelul **Politici**.

După ce ați definit politicile necesare în secțiunea **Politici**, le puteți alocă 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:

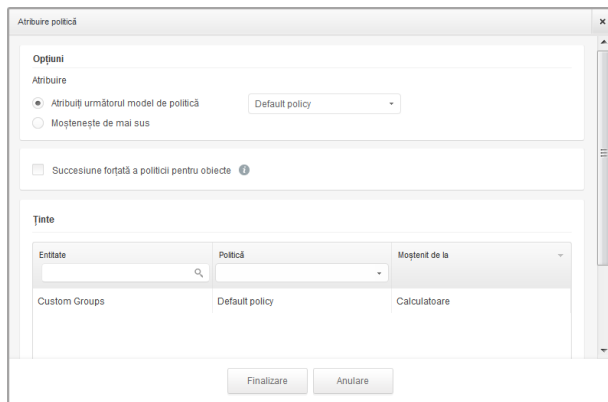
1. Mergeți la pagina **Rețea**.
2. Selectați caseta de bifare a obiectului de rețea dorit. Puteți selecta unul sau mai multe obiecte numai de la același nivel.
3. Faceți clic pe butonul **Atribuire politică** din partea dreaptă a tabelului.



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 atribuiriile 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 **Moștenește de mai sus** pentru a aloca obiectelor de rețea selectate politica grupului părinte.
- **Sucesiune 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 **Sucesiune 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.

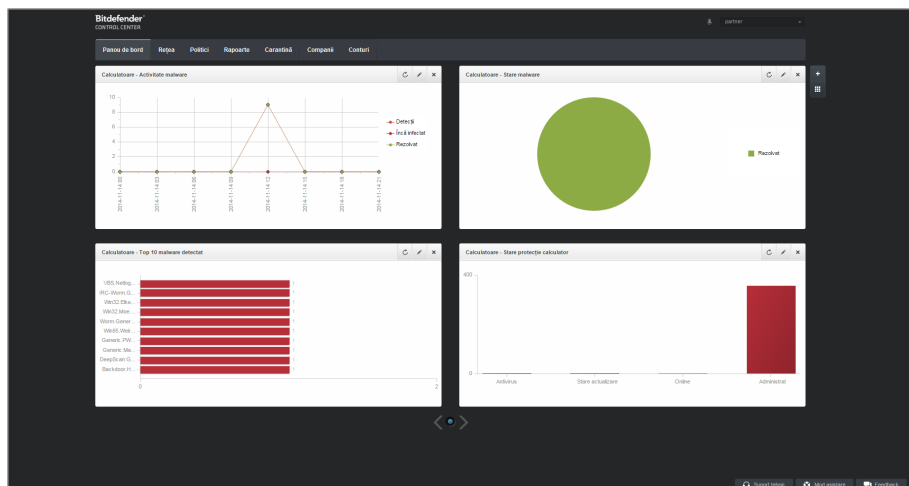
Politicile expediate către obiectele țintă ale rețelei imediat după realocare sau după modificarea setărilor politicii. Setările trebuie aplicate pe obiectele din rețea în mai puțin de un minut (cu condiția ca acestea să fie online). Dacă un obiect din rețea nu este online, setările vor fi aplicate imediat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

4.2. Monitorizarea stării de securitate

Instrumentul principal de monitorizare Security for Endpoints este panoul de bord al Control Center, un afișaj care poate fi personalizat și care oferă o privire rapidă de ansamblu asupra securității rețelei dumneavoastră.



Panoul de bord



Verificați regulat pagina **Dashboard** pentru a vedea informații în timp real cu privire la starea de securitate a rețelei.

Portlet-urile panoului de control afișează 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.

Aceasta este ceea ce trebuie să știți despre administrarea panoului de bord:

- Control Center este livrat cu mai multe portlet-uri predefinite pentru panoul de bord. De asemenea, puteți adăuga mai multe portlet-uri folosind butonul **+** **Adăugare portlet** din partea dreaptă a panoului de bord.
- Fiecare portlet al panoului de control include un raport detaliat în fundal, accesibil cu un singur clic pe grafic.
- Informațiile afișate de portlet-uri se referă numai la obiectele de rețea din contul dumneavoastră. Puteți personaliza informațiile afișate de un portlet (tip, interval de raportare, obiective) făcând clic pe pictograma **↕** **Modificare portlet** din bara de titlu a acestuia.

De exemplu, puteți configura portlet-urile pentru a afișa informațiile despre o anumită companie din rețea.


- 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.
- Faceți clic pe intrările de legendă din grafic, atunci când sunt disponibile, pentru a ascunde sau a afișa variabila corespunzătoare pe grafic.
- Puteți rearanja portlet-urile din panoul de bord conform nevoilor dumneavoastră făcând clic pe butonul  **Rearanjare portlet-uri** din partea dreaptă a panoului de bord. După aceasta puteți trage și glisa portlet-urile în poziția dorită.
- 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.

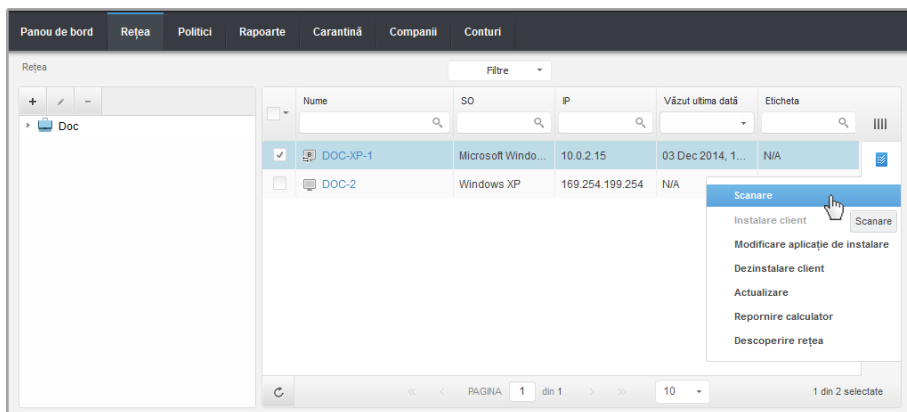
4.3. Scanarea calculatoarelor administrate

Există trei modalități de scanare a calculatoarelor protejate prin Endpoint Security:

- Utilizatorul autentificat pe calculator poate începe o scanare din interfața pentru utilizator Endpoint Security.
- Puteți crea sarcini de scanare programată utilizând politica.
- Rulați o scanare imediată din consolă.

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 rețea din fereastra din stânga. Toate calculatoarele din grupul selectat sunt afișate în tabelul din fereastra din dreapta.
3. Selectați entitățile pe care doriți să le scanați. Puteți selecta numai anumite calculatoare administrate sau un grup întreg.
4. Faceți clic pe butonul  **Sarcini** din dreapta tabelului și selectați **Scanare**. Va apărea o fereastră de configurare.



Sarcină de scanare calculatoare

5. În fila **General**, selectați tipul scanării din meniul **Tip**:

- **Scanare rapidă** verifică dacă există malware care rulează în sistem, fără a întreprinde nicio acțiune. 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 virusii, 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.

6. Faceți clic pe **Salvare** pentru a crea sarcina de scanare. Va apărea un mesaj de confirmare.



Notă

După ce a fost creată, sarcina de scanare va începe să ruleze imediat pe calculatoarele online.

Dacă un calculator este offline, va fi scanat imediat ce revine online.

7. Puteți vizualiza și administra sarcini pe pagina **Network > Tasks**.

5. Obținere ajutor

Pentru a găsi resurse suplimentare de ajutor sau pentru a obține ajutor de la Bitdefender:

- Faceți clic pe butonul **Support tehnic** din colțul dreapta jos al Control Center.
- Mergeți la [Centrul nostru de asistență online](#).

Pentru a deschide un tichet de suport prin e-mail, folosiți [acest formular online](#).

A. Cerințe

A.1. Cerințe Security for Endpoints

A.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

A.1.2. Cerințe hardware

- Procesor compatibil Intel® Pentium

Sisteme de operare pentru stații de lucru

- 1 GHz sau superior pentru Microsoft Windows XP SP3, Windows XP SP2 64 biți și Windows 7 Enterprise (32 și 64 biți)
- Viteze de 2 GHz sau mai mari pentru Microsoft Windows Vista SP1 sau mai recent (32 și 64 biți), Microsoft Windows 7 (32 și 64 biți), Microsoft Windows 7 SP1 (32 și 64 biți), 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

- **Spațiu HDD:**

- 1.5 GB spațiu liber pe hard-disk



Notă

Pentru entități cu rol Endpoint Security Relay este nevoie de un spațiu disponibil pe disc de cel puțin 6 GB, întrucât acestea vor stoca toate actualizările și pachetele de instalare.

A.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+

A.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](#).

A.2. 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.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFVS
```

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 neadministrare**. 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.

A.2.1. 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.

A.2.2. Cerințe pentru aplicația de descoperire a rețelei

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) trebuie să ruleze serviciul Computer Browser. Controlerul principal al 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.