ANVÄNDARMANUAL

Bitdefender CONSUMER SOLUTIONS

Ultimate Small Business Security

Bitdefender Ultimate Small Business Security

Användarmanual

Publication date 05/31/2024

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Bitdefender Ultimate Small Business Security är ett prenumerationspaket för flera abonnemang som är skräddarsytt för att möta cybersäkerhetsbehoven hos små företag. Med en omfattande funktionsuppsättning, dedikerad onboarding och intuitiva hanteringsverktyg kan småföretagare skydda sina digitala tillgångar utan IT- eller cybersäkerhetsexpertis.

Planen erbjuder omfattande skydd speciellt utformat för små företag, inklusive:

- **Enhetsskydd för flera plattformar:** Skydda alla dina enheter, från datorer till mobiltelefoner och servrar.
- **Enkel hantering:** Upprätthåll säkerheten för ditt team och affärsverksamhet utan ansträngning.
- **Skydd för affärstillgångar och rykte:** Säkerställ högsta skyddsnivå för ditt företag genom att förhindra samband med bedrägliga aktiviteter.
- **Strömlinjeformad installation:** Introduktionsprocessen förenklar installationen för icke-tekniska användare, vilket säkerställer en smidig och säker konfiguration.

Hur man använder den här guiden

Den här guiden är organiserad kring de fyra produkterna som ingår i Bitdefender Total Security:

- Total säkerhet för PC (sida 9)
  Lär dig hur du använder produkten på dina Windows-baserade datorer och bärbara datorer.
- Antivirus för Mac (sida 143)
  Lär dig hur du använder produkten på dina Mac-datorer.
- Mobil säkerhet för Android (sida 175)
  Lär dig hur du använder produkten på dina Android-baserade smartphones och surfplattor.
- Mobil säkerhet för iOS (sida 207)

Lär dig hur du använder produkten på dina iOS-baserade smartphones och surfplattor.

- VPN (sida 221)
  Lär dig hur du döljer din onlineidentitet med hjälp av Bitdefender VPN på någon av dina enheter.
- Lösenordshanteraren (sida 242)
  Håll reda på och lagra alla dina lösenord och referenser på ett säkert sätt med Password Manager.
- Digital identitetsskydd (sida 266)
  Lär dig hur du korrekt hanterar skyddet av din digitala identitet.
- Få hjälp (sida 273)
  Ta reda på var du kan söka hjälp om något oväntat dyker upp.

Konventioner som används i denna guide

Typografiska konventioner

Flera textstilar används i den här guiden för att förbättra läsbarheten. Deras aspekt och betydelse presenteras i tabellen nedan.

Utseende	Beskrivning
sample syntax	Syntaxexempel skrivs ut med monospaced tecken.
https://www.bitdefender.com	URL-länken pekar på någon extern plats, på http- eller ftp-servrar.
documentation@bitdefender.com	E-postadresser infogas i texten för kontaktinformation.
Om den här guiden (sida 1)	Detta är en intern länk till någon plats i dokumentet.
filename	Filer och kataloger skrivs ut med monospaced font.
alternativ	Alla produktalternativ skrivs ut med hjälp av **djärv** tecken.
nyckelord	Viktiga sökord eller fraser markeras med hjälp av **djärv** tecken.

Förmaningar

Förmaningarna är anteckningar i texten, grafiskt markerade, som uppmärksammar dig på ytterligare information relaterad till det aktuella stycket.

Notera

Anteckningen är bara en kort observation. Även om du kan utelämna det, kan anteckningarna ge värdefull information, som specifik funktion eller en länk till något relaterat ämne.

Viktig

Detta kräver din uppmärksamhet och rekommenderas inte att hoppa över det. Vanligtvis ger den icke-kritisk men betydande information.

Varning

Detta är viktig information som du bör behandla med ökad försiktighet. Inget dåligt kommer att hända om du följer anvisningarna. Du bör läsa och förstå den, för den beskriver något extremt riskabelt.

Begäran om kommentarer

Vi inbjuder dig att hjälpa oss att förbättra boken. Vi har testat och verifierat all information efter bästa förmåga. Skriv för att berätta för oss om eventuella brister du hittar i den här boken eller hur du tror att den kan förbättras, för att hjälpa oss att förse dig med bästa möjliga dokumentation.

Meddela oss genom att skicka ett mejl till documentation@bitdefender.com. Skriv alla dina dokumentationsrelaterade e-postmeddelanden på engelska så att vi kan behandla dem effektivt.

1. KONFIGURERA DIN PRENUMERATION

Processen för att komma igång med din **Bitdefender Ultimate Small Business Security**-prenumeration är särskilt skräddarsydd för att vara snabb och enkel, utan behov av IT- eller cybersäkerhetsexpertis. Du behöver:

1. **{Aktivera Bitdefender Ultimate Small Business Security:**
   Du kan göra det genom att följa instruktionerna i bekräftelsemeddelandet som du fick när du köpte produkten.
2. **{Konfigurera ditt företagskonto:**
   Vid aktivering blir du ombedd att ange ditt företagsnamn. Det är endast i identifieringssyfte och det visas på olika ställen i gränssnittet. Observera att du kan använda vilket namn du vill, eftersom det inte krävs någon validering för detta.
3. **Välj din roll i organisationen:**
   - **Företagsägare:** Om du är företagsägaren och sköter inköp och installation väljer du det här alternativet.
   - **Säkerhetsadministratör:** Välj det här alternativet om du är ansvarig för säkerhetsadministrationen inom företaget.

     Obs!
     Säkerhetsadministratören har liknande behörigheter som företagsägaren, med undantag för inköpsmöjligheter.

4. **Bjud in teammedlemmar att skapa konton:**
   När du är klar med att välja ditt namn och din roll ser du en översikt över din Bitdefender-prenumeration. Härifrån kan du välja att dela planen med andra teammedlemmar eller fortsätta med din egen installation genom att följa de installationsförfaranden som är lämpliga för den enhet som du vill installera Bitdefender på, var och en beskrivs i motsvarande kapitel i detta dokument.

     Viktigt
     Vi rekommenderar att du börjar med att bjuda in dina anställda innan du går in på installationsförfarandet.

5. **Välj roller för teammedlemmar:**

Välj rollerna för de anställda som du bjuder in att delta i företagets säkerhetsplan. Du kan bjuda in dem som:

- **Säkerhetsadministratör:** Den här rollen innebär att hantera medlemmar, enheter och säkerhetsoperationer och är avsedd för de anställda som har en viss nivå av förståelse för IT och som har till uppgift att hantera och övervaka cybersäkerhetsaspekterna i ditt företag.
- **Medarbetare:** Medarbetare har begränsad insyn och begränsade hanteringsmöjligheter. De behöver ett Bitdefender Central-konto för att skydda sina egna enheter, medan de med rollen **Säkerhetsadministratör** kan övervaka deras skydd och hantera sina enheter på distans.

6. **Skicka e-postinbjudningar till teammedlemmar:**
   Ange e-postadresserna till de medarbetare som du vill dela Bitdefender-planen med. Flera inbjudningar kan skickas samtidigt.

   Obs!
   Inbjudna medlemmar, oavsett roll, får en inbjudan via e-post. De måste klicka på knappen **Aktivera i Bitdefender Central** och acceptera inbjudan med hjälp av samma e-postadress som de blev inbjudna med.

7. **Lägg till känslig affärsinformation som ska övervakas:**
   Som sista steg i processen måste du nu konfigurera övervakning av exponeringen av affärstillgångar.

   Obs!
   Business Assets Exposure är en tjänst som endast är tillgänglig för administratörsroller. (**Säkerhetsadministratör** och **Företagsägare**)

   Den här funktionen kontrollerar om data exponeras på företagsnivå för att skydda företagets rykte och förhindra eventuella riktade attacker.

   - Från den vänstra menyn på ditt Bitdefender Central-konto navigerar du till avsnittet **Business Activity**.
   - Klicka på knappen **Gå till inställning** i panelen **Business Assets Exposure**.
   - Lägg till den begärda företagsinformationen:

- Företagets e-postadress
- Företagets kreditkort
- Konton för sociala medier

- När du har vidtagit alla föreslagna åtgärder klickar du på knappen **Markera som utförd** för att bekräfta resultatet och följa dina framsteg.

När du är klar med dessa steg kan du börja konfigurera **Bitdefender Ultimate Small Business Security** för dig själv:

- Installera på Windows-enheter: Installation (sida 9)
- Installera på macOS-enheter: Installerar Bitdefender Antivirus for Mac (sida 144)
- Installera på Android-mobilenheter: Installera Bitdefender Mobile Security (sida 175)
- Installera på iOS-mobilenheter: Installera Bitdefender Mobile Security för iOS (sida 208)
- Installera Bitdefender VPN på dina enheter: Installerar Bitdefender Password Manager (sida 223)
- Ställ in Password Manager: Installation (sida 244)
- Konfigurera Digital Identity Protection: Konfigurera digitalt identitetsskydd (sida 267)

När denna process har slutförts är aktiveringen och installationen av **Bitdefender Ultimate Small Business Security** för ditt företag klar.

2. EXPONERING AV FÖRETAGSTILLGÅNGAR

Business Assets Exposure är en Bitdefender Ultimate Small Business Security-tjänst som hanteras av administratörer (företagsägare och säkerhetsadministratör) och som ger insyn i exponeringen av viktig företagsinformation vid dataintrång. Business Assets Exposure övervakar 3 komponenter för att upptäcka dataintrång:

- Företagets e-postadress
- Företagets kreditkort
- Konton för sociala medier

Varför det är viktigt att övervaka exponeringen av affärstillgångar:

- **Skydd av anseende:** Förhindrar skador på företagets rykte genom att snabbt åtgärda överträdelser.
- **Medarbetarsäkerhet:** Skyddar medarbetare från nätfiske och andra sociala attacker genom att övervaka och hantera deras exponerade data.
- **Förebyggande av riktade attacker:** Begränsar risken för riktade attacker genom att säkerställa att känslig information förblir säker.

När du har ställt in din **Business Assets Exposure**-information som en del av **Konfigurera din prenumeration (sida 4)** -processen, kan du **granska resultat och agera på rekommendationer:**

Systemet informerar dig om eventuella intrång som rör dessa övervakade tillgångar, däribland de tjänster som utsatts för intrång och de typer av information som exponerats (t.ex. e-postadresser, användarnamn, lösenord, geografiska platser). Specifika detaljer visas inte, endast kategorierna av exponerade data.

Tillämpa säkerhetsrekommendationerna för varje övervakad komponent (företagse-post, företagskreditkort, konton i sociala medier). Föreslagna åtgärder kan omfatta:

- Be medarbetarna att övervaka sin företagse-post med Bitdefender Digital Identity Protection.
- Byte av lösenord på webbplatser som utsatts för intrång och råd till anställda att använda Bitdefender Password Manager.

- Säkerställa att medarbetarna installerar Bitdefenders säkerhetslösningar på alla enheter för att förhindra cyberattacker.
- Att rekommendera medarbetare att använda Scam Copilot för att få råd om potentiella bedrägerier och metoder för att förebygga bedrägerier.
- Övervaka transaktioner och ändra kreditkortet med hjälp av bankutgivaren.
- Aktivera tvåfaktorsautentisering på plattformar för sociala medier som utsatts för intrång för att förhindra obehöriga inloggningar.

> **Obs!**
> När du har vidtagit de föreslagna åtgärderna måste du klicka på knappen **Markera som utförd** för att bekräfta slutförandet och spåra dina förlopp.

Genom att följa dessa steg kan administratörer enkelt övervaka och skydda sitt företag mot risker för dataexponering med hjälp av tjänsten **Business Assets Exposure**.

3. TOTAL SÄKERHET FÖR PC

3.1. Installation

3.1.1. Förbereder för installation

Innan du installerar Bitdefender Ultimate Small Business Security, slutför dessa förberedelser för att säkerställa att installationen går smidigt:

- Se till att enheten där du planerar att installera Bitdefender uppfyller systemkraven. Om enheten inte uppfyller alla systemkrav kommer Bitdefender inte att installeras eller, om den är installerad, kommer den inte att fungera korrekt och det kommer att orsaka systemavbrott och instabilitet. För en fullständig lista över systemkrav, se Systemkrav (sida 9).
- Logga in på enheten med ett administratörskonto.
- Ta bort annan liknande programvara från enheten. Om någon upptäcks under Bitdefender-installationsprocessen kommer du att meddelas om att avinstallera den. Att köra två säkerhetsprogram samtidigt kan påverka deras funktion och orsaka stora problem med systemet. Windows Defender kommer att inaktiveras under installationen.
- Inaktivera eller ta bort eventuella brandväggsprogram som kan köras på enheten. Att köra två brandväggsprogram samtidigt kan påverka deras funktion och orsaka stora problem med systemet. Windows-brandväggen kommer att inaktiveras under installationen.
- Det rekommenderas att din enhet är ansluten till internet under installationen, även från en CD/DVD. Om nyare versioner av appfilerna som ingår i installationspaketet är tillgängliga kan Bitdefender ladda ner och installera dem.

3.1.2. Systemkrav

Du kan installera Bitdefender Ultimate Small Business Security endast på enheter som kör följande operativsystem:

- Windows 7 med Service Pack 1
- Windows 8.1

- Windows 10
- 2,5 GB ledigt ledigt hårddiskutrymme (minst 800 MB på systemenheten)
- 2 GB minne (RAM)

Du kan också installera och köra Bitdefender Ultimate Small Business Security på följande:

- Windows Server 2016 (med skrivbordserfarenhet):
  - Standard/RTM
  - Essentials
  - Datacenter
- Windows Server 2019 (med skrivbordsupplevelse):
  - Standard/RTM
  - Grundläggande
  - Datacenter
- Windows Server 2022 (med skrivbordserfarenhet):
  - Standard/RTM
  - Datacenter

> **Viktig**
> Systemprestandan kan påverkas på enheter som har gamla generationens processorer.

Notera

För att ta reda på vilket Windows-operativsystem din enhet körs och hårdvaruinformation:

- I **Windows 7**, Högerklicka **Min dator** på skrivbordet och välj sedan **Egenskaper** från menyn.
- I **Windows 8**, från startskärmen i Windows, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt på startskärmen) och sedan högerklicka på dess ikon. I **Windows 8.1**, lokalisera **Denna PC**.
  Välj **Egenskaper** i bottenmenyn. Titta i **Systemet** område för att hitta information om din systemtyp.
- I **Windows 10**, typ **Systemet** i sökrutan från aktivitetsfältet och klicka på dess ikon. Titta i **Systemet** område för att hitta information om din systemtyp.

3.1.3. Programvarukrav

För att kunna använda Bitdefender och alla dess funktioner måste din enhet uppfylla följande programvarukrav:

- Microsoft Edge 40 och högre
- Internet Explorer 10 och senare
- Mozilla Firefox 51 och senare
- Google Chrome 34 och senare
- Microsoft Outlook 2007/2010/2013/2016
- Mozilla Thunderbird 14 och högre

3.1.4. Installera din Bitdefender-produkt

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet som laddats ner på din enhet från Bitdefender Central.

Om ditt köp omfattar mer än en enhet, upprepa installationsprocessen och aktivera din produkt med samma konto på varje enhet. Kontot du behöver använda är det som innehåller din aktiva Bitdefender-prenumeration.

Installera från Bitdefender Central

Från Bitdefender Central kan du ladda ner installationssatsen som motsvarar den köpta prenumerationen. När installationsprocessen är klar, Bitdefender Ultimate Small Business Security är aktiverad.

Att ladda ned Bitdefender Ultimate Small Business Security från Bitdefender Central:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
3. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Spara installationsfilen.
   - **Skydda andra enheter**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Klick **SKICKA NEDLADDNINGSLÄNK**.
     c. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**.
     Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
     d. På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.
4. Vänta tills nedladdningen är klar och kör sedan installationsprogrammet.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om ditt system inte uppfyller systemkraven för att installera Bitdefender kommer du att informeras om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender upptäcks kommer du att uppmanas att ta bort den från ditt system. Följ anvisningarna för att ta bort programvaran från ditt system, så att du undviker problem som uppstår senare. Du kan behöva starta om enheten för att slutföra borttagningen av upptäckta säkerhetslösningar.

Installationspaketet för Bitdefender Total Security uppdateras ständigt.

> **Notera**
> Att ladda ner installationsfilerna kan ta lång tid, särskilt över långsammare internetanslutningar.

När installationen är validerad visas installationsguiden. Följ stegen för att installera Bitdefender Ultimate Small Business Security.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren som du får använda Bitdefender Ultimate Small Business Security.

Om du inte godkänner dessa villkor, stäng fönstret. Installationsprocessen kommer att överges och du kommer att avsluta installationen.

Två ytterligare uppgifter kan utföras i detta steg:

- Behåll **Skicka produktrapporter** alternativet aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information om hur du använder produkten till Bitdefender-servrarna. Denna information är viktig för att förbättra produkten och kan hjälpa oss att ge en bättre upplevelse i framtiden. Observera att dessa rapporter inte innehåller några konfidentiella uppgifter, såsom ditt namn eller IP-adress, och att de inte kommer att användas för kommersiella ändamål.
- Välj det språk du vill installera produkten på.

Klick **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills installationen är klar. Detaljerad information om framstegen visas.

Steg 3 - Installationen slutförd

Din Bitdefender-produkt har installerats.

En sammanfattning av installationen visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av systemet krävas.

Steg 4 - Enhetsanalys

Du kommer nu att bli tillfrågad om du vill utföra en analys av din enhet för att säkerställa att den är säker. Under detta steg kommer Bitdefender att skanna kritiska systemområden. Klick **Starta enhetsanalys** att initiera det.

Du kan dölja skanningsgränssnittet genom att klicka på **Kör Scan i bakgrunden**. Därefter väljer du om du vill bli informerad när skanningen är klar eller inte.

Klicka på när skanningen är klar **Öppna Bitdefender-gränssnittet**.

> **Notera**
> Alternativt, om du inte vill utföra skanningen kan du helt enkelt klicka på **Hoppa**.

Steg 5 - Kom igång

I den **Komma igång** fönster kan du se detaljer om din aktiva prenumeration.

Klick **AVSLUTA** för att komma åt Bitdefender Ultimate Small Business Security gränssnitt.

Installera från installationsskivan

För att installera Bitdefender från installationsskivan, sätt in skivan i den optiska enheten.

En installationsskärm bör visas inom några ögonblick. Följ instruktionerna för att starta installationen.

Om installationsskärmen inte visas, använd Windows Explorer för att bläddra till skivans rotkatalog och dubbelklicka på filen *autorun.exe*.

Om din internethastighet är långsam, eller om ditt system inte är anslutet till internet, klicka på **Installera från CD/DVD** knapp. I det här fallet kommer Bitdefender-produkten som är tillgänglig på skivan att installeras och en nyare version kommer att laddas ner från Bitdefender-servrarna via produktuppdatering.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om ditt system inte uppfyller systemkraven för att installera Bitdefender kommer du att informeras om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender upptäcks kommer du att uppmanas att ta bort den från ditt system. Följ anvisningarna för att ta bort programvaran från ditt system, så att du undviker problem som uppstår senare. Du kan behöva starta om enheten för att slutföra borttagningen av upptäckta säkerhetslösningar.

Installationspaketet för Bitdefender Total Security uppdateras ständigt.

> **Notera**
> Att ladda ner installationsfilerna kan ta lång tid, särskilt över långsammare internetanslutningar.

När installationen är validerad visas installationsguiden. Följ stegen för att installera Bitdefender Ultimate Small Business Security.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren som du får använda Bitdefender Ultimate Small Business Security.

Om du inte godkänner dessa villkor, stäng fönstret. Installationsprocessen kommer att överges och du kommer att avsluta installationen.

Två ytterligare uppgifter kan utföras i detta steg:

- Behåll **Skicka produktrapporter** alternativet aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information

om hur du använder produkten till Bitdefender-servrarna. Denna information är viktig för att förbättra produkten och kan hjälpa oss att ge en bättre upplevelse i framtiden. Observera att dessa rapporter inte innehåller några konfidentiella uppgifter, såsom ditt namn eller IP-adress, och att de inte kommer att användas för kommersiella ändamål.

- Välj det språk du vill installera produkten på.

Klick **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills installationen är klar. Detaljerad information om framstegen visas.

Steg 3 - Installationen slutförd

En sammanfattning av installationen visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av systemet krävas.

Steg 4 - Enhetsanalys

Du kommer nu att bli tillfrågad om du vill utföra en analys av din enhet för att säkerställa att den är säker. Under detta steg kommer Bitdefender att skanna kritiska systemområden. Klick **Starta enhetsanalys** att initiera det.

Du kan dölja skanningsgränssnittet genom att klicka på **Kör Scan i bakgrunden**. Därefter väljer du om du vill bli informerad när skanningen är klar eller inte.

Klicka på när skanningen är klar **Fortsätt med Skapa konto**.

Notera

Alternativt, om du inte vill utföra skanningen kan du helt enkelt klicka på **Hoppa**.

Steg 5 - Bitdefender-konto

När du har slutfört den första installationen, visas Bitdefender-kontofönstret. Ett Bitdefender-konto krävs för att aktivera produkten

och använda dess onlinefunktioner. För mer information, se Bitdefender Central.

Fortsätt enligt din situation.

- **Jag vill skapa ett Bitdefender-konto**

  1. Skriv in den information som krävs i motsvarande fält. De uppgifter du lämnar här kommer att förbli konfidentiella. Lösenordet måste vara minst 8 tecken långt, innehålla minst en siffra eller symbol och innehålla gemener och versaler.
  2. Innan du går vidare måste du godkänna användarvillkoren. Gå till användarvillkoren och läs dem noggrant eftersom de innehåller villkoren under vilka du får använda Bitdefender.
     Dessutom kan du komma åt och läsa sekretesspolicyn.
  3. Klick **SKAPA KONTO**.

     > **Notera**
     > När kontot har skapats kan du använda den angivna e-postadressen och lösenordet för att logga in på ditt konto på https://central.bitdefender.com, eller i Bitdefender Central-appen förutsatt att den är installerad på en av dina Android- eller iOS-enheter. För att installera Bitdefender Central-appen på Android måste du komma åt Google Play, söka i Bitdefender Central och sedan trycka på motsvarande installationsalternativ. För att installera Bitdefender Central-appen på iOS måste du gå till App Store, söka i Bitdefender Central och sedan trycka på motsvarande installationsalternativ.

- **Jag har redan ett Bitdefender-konto**

  1. Klick **Logga in**.
  2. Skriv in e-postadressen i motsvarande fält och klicka sedan **NÄSTA**.
  3. Skriv ditt lösenord och klicka sedan **LOGGA IN**.
     Om du har glömt lösenordet för ditt konto eller bara vill återställa det du redan har ställt in:
     a. Klick **Glömt ditt lösenord?**.
     b. Skriv din e-postadress och klicka sedan **NÄSTA**.

c. Kontrollera ditt e-postkonto, skriv in säkerhetskoden du har fått och klicka sedan **NÄSTA**.
Alternativt kan du klicka **ändra lösenord** i e-postmeddelandet som vi skickade till dig.

d. Skriv det nya lösenordet du vill ställa in och skriv det sedan igen. Klick **SPARA**.

> **Notera**
> Om du redan har ett MyBitdefender-konto kan du använda det för att logga in på ditt Bitdefender-konto. Om du har glömt ditt lösenord måste du först gå till https://my.bitdefender.com för att återställa den. Använd sedan de uppdaterade användaruppgifterna för att logga in på ditt Bitdefender-konto.

- **Jag vill logga in med mitt Microsoft-, Facebook- eller Google-konto**
Så här loggar du in med ditt Microsoft-, Facebook- eller Google-konto:

1. Välj den tjänst du vill använda. Du kommer att omdirigeras till inloggningssidan för den tjänsten.
2. Följ instruktionerna från den valda tjänsten för att länka ditt konto till Bitdefender.

> **Notera**
> Bitdefender får inte tillgång till någon konfidentiell information som lösenordet för kontot du använder för att logga in eller personlig information om dina vänner och kontakter.

Steg 6 - Aktivera din produkt

> **Notera**
> Det här steget visas om du har valt att skapa ett nytt Bitdefender-konto under föregående steg, eller om du loggade in med ett konto med en utgången prenumeration.

En aktiv internetanslutning krävs för att slutföra aktiveringen av din produkt.

Fortsätt enligt din situation:

- Jag har en aktiveringskod
I så fall aktiverar du produkten genom att följa dessa steg:

1. Skriv in aktiveringskoden i fältet Jag har en aktiveringskod och klicka sedan **FORTSÄTTA**.

   Notera
   Du kan hitta din aktiveringskod:
   - på CD/DVD-etiketten.
   - på produktregistreringskortet.
   - i e-postmeddelandet om köp online.

2. **Jag vill utvärdera Bitdefender**
   I det här fallet kan du använda produkten under en 30-dagarsperiod. För att börja provperioden, välj **Jag har ingen prenumeration, jag vill prova produkten gratis**, och klicka sedan **FORTSÄTTA**.

Steg 7 - Kom igång

I den **Komma igång** fönster kan du se detaljer om din aktiva prenumeration.

Klick **AVSLUTA** för att komma åt Bitdefender Ultimate Small Business Security gränssnitt.

3.2. Hantera din säkerhet

3.2.1. Antivirusskydd

Bitdefender skyddar din enhet från alla typer av hot (skadlig programvara, trojaner, spionprogram, rootkits och så vidare). Skyddet Bitdefender erbjuder är indelat i två kategorier:

- Skanning vid åtkomst - förhindrar att nya hot kommer in i ditt system. Bitdefender kommer till exempel att skanna ett word-dokument efter kända hot när du öppnar det och ett e-postmeddelande när du får ett.
  Genomsökning vid åtkomst säkerställer realtidsskydd mot hot, vilket är en viktig komponent i alla datorsäkerhetsprogram.

  Viktig
  För att förhindra hot från att infektera din enhet, behåll **skanning vid åtkomst** aktiverad.

- Skanning på begäran - gör det möjligt att upptäcka och ta bort hotet som redan finns i systemet. Detta är den klassiska skanningen som initieras av användaren - du väljer vilken enhet, mapp eller fil Bitdefender ska skanna, och Bitdefender skannar den - på begäran.

Bitdefender skannar automatiskt alla flyttbara media som är anslutna till enheten för att se till att de kan nås på ett säkert sätt. För mer information, se Automatisk skanning av flyttbara media (sida 33).

Avancerade användare kan konfigurera skanningsundantag om de inte vill att specifika filer eller filtyper ska skannas. För mer information, se Konfigurerar skanningsundantag (sida 35).

När den upptäcker ett hot kommer Bitdefender automatiskt att försöka ta bort den skadliga koden från den infekterade filen och rekonstruera den ursprungliga filen. Denna operation kallas desinfektion. Filer som inte kan desinficeras flyttas till karantän för att innehålla infektionen. För mer information, se Hantera filer i karantän (sida 37).

Om din enhet har infekterats med hot, se Ta bort hot från ditt system (sida 136). För att hjälpa dig att rensa din enhet från hot som inte kan tas bort från Windows-operativsystemet, ger Bitdefender dig Räddningsmiljö (sida 137). Detta är en pålitlig miljö, speciellt utformad för att ta bort hot, som gör att du kan starta upp din enhet oberoende av Windows. När enheten körs i Rescue Environment är Windows-hoten inaktiva, vilket gör det enkelt att ta bort dem.

Skanning vid åtkomst (realtidsskydd)

Bitdefender tillhandahåller realtidsskydd mot ett brett utbud av hot genom att skanna alla tillgängliga filer och e-postmeddelanden.

Slå på eller av realtidsskydd

Så här slår du på eller av realtidsskydd mot hot:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönster, slå på eller av **Bitdefender Shield**.
4. Om du vill inaktivera realtidsskyddet visas ett varningsfönster. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktiverat. Du kan inaktivera realtidsskydd i 5, 15 eller 30 minuter, i en timme, permanent eller tills ett system

startar om. Realtidsskyddet aktiveras automatiskt när den valda tiden går ut.

Varning
Detta är en kritisk säkerhetsfråga. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat kommer du inte att skyddas mot hot.

Konfigurera avancerade inställningar för realtidsskydd

Avancerade användare kanske vill dra fördel av skanningsinställningarna som Bitdefender erbjuder. Du kan konfigurera realtidsskyddsinställningarna i detalj genom att skapa en anpassad skyddsnivå.

Så här konfigurerar du realtidsskyddets avancerade inställningar:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönstret kan du konfigurera skanningsinställningarna efter behov.

Information om skanningsalternativen

Du kan hitta den här informationen användbar:

- **Skanna endast applikationer.** Du kan ställa in Bitdefender för att endast skanna appar som är tillgängliga.
- **Skanna potentiellt oönskade applikationer.** Välj det här alternativet för att söka efter oönskade program. Ett potentiellt oönskat program (PUA) eller ett potentiellt oönskat program (PUP) är en programvara som vanligtvis levereras med gratisprogram och som visar popup-fönster eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem kommer att ändra hemsidan eller sökmotorn, andra kommer att köra flera processer i bakgrunden som saktar ner datorn eller kommer att visa många annonser. Dessa program kan installeras utan ditt samtycke (även kallat adware) eller kommer att ingå som standard i expressinstallationspaketet (reklamstöds).
- **Skanna skript.** Funktionen Skanna skript gör att Bitdefender kan skanna powershell-skript och kontorsdokument som kan innehålla skriptbaserad skadlig programvara.

- **Skanna nätverksresurser.** För att säkert få åtkomst till ett fjärrnätverk från din enhet rekommenderar vi att du håller alternativet Skanna nätverksresurser aktiverat.
- **Skanna processminne.** Söker efter skadlig aktivitet i minnet av pågående processer.
- **Skanna kommandoraden.** Genomsöker kommandoraden för nystartade program för att förhindra fillösa attacker.
- **Skanna arkiv.** Att skanna inuti arkiv är en långsam och resurskrävande process, som därför inte rekommenderas för realtidsskydd. Arkiv som innehåller infekterade filer är inte ett omedelbart hot mot säkerheten för ditt system. Hotet kan bara påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att ha realtidsskydd aktiverat.

  Om du bestämmer dig för att använda det här alternativet, aktivera det och dra sedan skjutreglaget längs skalan för att utesluta arkiv som är större än ett givet värde i MB (megabyte) från skanning.
- **Skanna startsektorer.** Du kan ställa in Bitdefender att skanna startsektorerna på din hårddisk. Denna sektor av hårddisken innehåller den nödvändiga datorkoden för att starta uppstartsprocessen. När ett hot infekterar startsektorn kan enheten bli otillgänglig och du kanske inte kan starta ditt system och komma åt dina data.
- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och modifierade filer kan du avsevärt förbättra systemets övergripande reaktionsförmåga med en minimal kompromiss i säkerhet.
- **Skanna keyloggers.** Välj det här alternativet för att skanna ditt system efter keylogger-appar. Keyloggers registrerar vad du skriver på ditt tangentbord och skickar rapporter över internet till en illvillig person (hacker). Hackaren kan ta reda på känslig information från de stulna uppgifterna, såsom bankkontonummer och lösenord, och använda den för att få personliga fördelar.
- **Tidig startskanning.** Välj **Tidig startskanning** alternativet att skanna ditt system vid uppstart så snart alla dess kritiska tjänster är laddade. Uppdraget med den här funktionen är att förbättra upptäckten av hot vid systemstart och uppstartstiden för ditt system.

Åtgärder vidtagna för upptäckta hot

Du kan konfigurera de åtgärder som vidtas av realtidsskyddet genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönstret, scrolla ner i fönstret tills du ser **Hotåtgärder** alternativ.
4. Konfigurera skanningsinställningarna efter behov.

Följande åtgärder kan vidtas av realtidsskyddet i Bitdefender:

Vidta lämpliga åtgärder

Bitdefender kommer att vidta de rekommenderade åtgärderna beroende på typen av upptäckt fil:

- **Infekterade filer.** Filer som upptäckts som infekterade matchar en del av hotinformation som finns i Bitdefender Hot Information Database. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och rekonstruera den ursprungliga filen. Denna operation kallas desinfektion.

  Filer som inte kan desinficeras flyttas till karantän för att innehålla infektionen. Filer i karantän kan inte köras eller öppnas; därför försvinner risken att bli smittad. För mer information, se Hantera filer i karantän (sida 37).

  > **Viktig**
  > För särskilda typer av hot är desinficering inte möjlig eftersom den upptäckta filen är helt skadlig. I sådana fall tas den infekterade filen bort från disken.

- **Misstänkta filer.** Filer upptäcks som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen desinfektionsrutin finns tillgänglig. De kommer att flyttas till karantän för att förhindra en potentiell infektion.
- **Arkiv som innehåller infekterade filer.**
  - Arkiv som bara innehåller infekterade filer raderas automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer kommer Bitdefender att försöka ta bort de infekterade filerna förutsatt

att det kan rekonstruera arkivet med de rena filerna. Om arkivrekonstruktion inte är möjlig kommer du att informeras om att inga åtgärder kan vidtas för att undvika att förlora rena filer.

Flytta till karantän

Flyttar upptäckta filer till karantän. Filer i karantän kan inte köras eller öppnas; därför försvinner risken att bli smittad. För mer information, se Hantera filer i karantän (sida 37).

Neka åtkomst

Om en infekterad fil upptäcks kommer åtkomsten till denna att nekas.

Återställer standardinställningarna

Standardinställningarna för realtidsskydd säkerställer ett bra skydd mot hot, med mindre inverkan på systemets prestanda.

Så här återställer du standardinställningarna för realtidsskydd:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Avancerad** fönstret, scrolla ner i fönstret tills du ser **Återställ avancerade inställningar** alternativ. Välj det här alternativet för att återställa antivirusinställningarna till standardinställningarna.

Skanning på begäran

Huvudsyftet för Bitdefender är att hålla din enhet ren från hot. Detta görs genom att hålla nya hot borta från din enhet och genom att skanna dina e-postmeddelanden och alla nya filer som laddats ner eller kopierats till ditt system.

Det finns en risk att ett hot redan finns i ditt system, innan du ens installerat Bitdefender. Det är därför det är en mycket bra idé att skanna din enhet efter invånande hot efter att du har installerat Bitdefender. Och det är definitivt en bra idé att ofta skanna din enhet efter hot.

Skanning på begäran baseras på skanningsuppgifter. Skanningsuppgifter anger skanningsalternativen och de objekt som ska skannas. Du kan skanna enheten när du vill genom att köra standarduppgifterna eller dina egna skanningsuppgifter (användardefinierade uppgifter). Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen, konfigurera och kör en anpassad skanning.

Skanna en fil eller mapp efter hot

Du bör skanna filer och mappar när du misstänker att de kan vara infekterade. Högerklicka på filen eller mappen du vill skannas, peka på **Bitdefender** och välj **Skanna med Bitdefender**. De Antivirus Scan guide visas och guidar dig genom skanningsprocessen. I slutet av skanningen kommer du att bli ombedd att välja vilka åtgärder som ska vidtas på de upptäckta filerna, om några.

Kör en snabbskanning

Snabbskanning använder genomsökning i molnet för att upptäcka hot som körs i ditt system. Att köra en snabbsökning tar vanligtvis mindre än en minut och använder en bråkdel av de systemresurser som behövs för en vanlig antivirusskanning.

Så här kör du en snabbskanning:

1. Klicka på Skydd på navigeringsmenyn i Bitdefender-gränssnittet.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** windows klickar du på **Kör Scan** knappen bredvid **Snabbskanning**.
4. Följ Antivirus Scan guide för att slutföra skanningen. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer. Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

Kör en systemsökning

System Scan-uppgiften skannar hela enheten efter alla typer av hot som äventyrar dess säkerhet, såsom skadlig programvara, spionprogram, adware, rootkits och andra.

> **Notera**
> Därför att **Genomsökning av systemet** utför en grundlig genomsökning av hela systemet, kan genomsökningen ta ett tag. Därför rekommenderas det att köra den här uppgiften när du inte använder din enhet.

Innan du kör en systemsökning rekommenderas följande:

- Se till att Bitdefender är uppdaterad med sin databas med hotinformation. Genom att skanna din enhet med en föråldrad

hotinformationsdatabas kan det hindra Bitdefender från att upptäcka nya hot som hittats sedan den senaste uppdateringen. För mer information, se Håller Bitdefender uppdaterad.

- ❍ Stäng av alla öppna program.

Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen, konfigurera och kör en anpassad skanning. För mer information, se Konfigurera en anpassad skanning (sida 26).

Så här kör du en systemsökning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** windows klickar du på **Kör Scan** knappen bredvid **Genomsökning av systemet**.
4. Första gången du kör en systemsökning introduceras du i funktionen. Klick **Okej, förstår** att fortsätta.
5. Följ Antivirus Scan guide för att slutföra skanningen. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer. Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

Konfigurera en anpassad skanning

I den **Hantera skanningar** fönster kan du ställa in Bitdefender för att köra skanningar närhelst du anser att din enhet behöver en kontroll för potentiella hot. Du kan välja att schemalägga en Genomsökning av systemet eller a Snabbskanning, eller så kan du skapa en anpassad skanning när det passar dig.

Så här konfigurerar du en ny anpassad skanning i detalj:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** windows, klicka **+Skapa skanning**.
4. I den **Arbetsnamn** fältet, skriv ett namn för skanningen, välj sedan de platser du vill ska skannas och klicka sedan **Nästa**.
5. Konfigurera dessa allmänna alternativ:

- **Skanna endast applikationer.** Du kan ställa in Bitdefender för att endast skanna appar som är tillgängliga.
- **Skanningsuppgiftsprioritet.** Du kan välja vilken inverkan en skanningsprocess ska ha på systemets prestanda.
  - Auto - Prioriteten för skanningsprocessen beror på systemaktiviteten. För att säkerställa att skanningsprocessen inte kommer att påverka systemaktiviteten kommer Bitdefender att bestämma om skanningsprocessen ska köras med hög eller låg prioritet.
  - Hög - Prioriteten för skanningsprocessen kommer att vara hög. Genom att välja det här alternativet låter du andra program köras långsammare och minskar tiden som krävs för att skanningsprocessen ska slutföras.
  - Låg - Prioriteten för skanningsprocessen kommer att vara låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka den tid som krävs för att skanningsprocessen ska slutföras.
- **Åtgärder efter skanning.** Välj vilken åtgärd Bitdefender ska vidta om inga hot hittas:
  - Visa sammanfattningsfönster
  - Stäng av enheten
  - Stäng skanningsfönstret

6. Om du vill konfigurera skanningsalternativen i detalj, klicka på **Visa avancerade alternativ**. Du kan hitta information om de listade skanningarna i slutet av det här avsnittet.
   Klick **Nästa**.
7. Du kan aktivera **Schemalägg skanningsuppgift** om du vill, och välj sedan när den anpassade skanningen du skapade ska starta.
   - Vid systemstart
   - Dagligen
   - En gång i månaden
   - Varje vecka

Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.

8. Klick **Spara** för att spara inställningarna och stänga konfigurationsfönstret.
   Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot kommer att hittas under skanningsprocessen kommer du att uppmanas att välja vilka åtgärder som ska vidtas på de upptäckta filerna.

Information om skanningsalternativen

Du kan hitta den här informationen användbar:

- Om du inte är bekant med några av termerna, kontrollera dem i ordlista. Du kan också hitta användbar information genom att söka på internet.
- **Skanna potentiellt oönskade applikationer.** Välj det här alternativet för att söka efter oönskade program. Ett potentiellt oönskat program (PUA) eller ett potentiellt oönskat program (PUP) är en programvara som vanligtvis levereras med gratisprogram och som visar popup-fönster eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem kommer att ändra hemsidan eller sökmotorn, andra kommer att köra flera processer i bakgrunden som saktar ner datorn eller kommer att visa många annonser. Dessa program kan installeras utan ditt samtycke (även kallat adware) eller kommer att ingå som standard i expressinstallationspaketet (reklamstöds).
- **Skanna arkiv.** Arkiv som innehåller infekterade filer är inte ett omedelbart hot mot säkerheten för ditt system. Hotet kan bara påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att ha realtidsskydd aktiverat. Det rekommenderas dock att använda det här alternativet för att upptäcka och ta bort alla potentiella hot, även om det inte är ett omedelbart hot.
  Dra skjutreglaget längs skalan för att utesluta arkiv som är större än ett givet värde i MB (megabyte) från skanning.

  Notera
  Genom att skanna arkiverade filer ökar den totala skanningstiden och kräver mer systemresurser.

- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och modifierade filer kan du avsevärt förbättra systemets övergripande reaktionsförmåga med en minimal kompromiss i säkerhet.
- **Skanna startsektorer.** Du kan ställa in Bitdefender att skanna startsektorerna på din hårddisk. Denna sektor av hårddisken innehåller den nödvändiga datorkoden för att starta uppstartsprocessen. När ett hot infekterar startsektorn kan enheten bli otillgänglig och du kanske inte kan starta ditt system och komma åt dina data.
- **Skanna minne.** Välj det här alternativet för att skanna program som körs i systemets minne.
- **Skanna registret.** Välj det här alternativet för att skanna registernycklar. Windows-registret är en databas som lagrar konfigurationsinställningar och alternativ för Windows-operativsystemets komponenter, såväl som för installerade appar.
- **Skanna cookies.** Välj det här alternativet för att skanna cookies som lagras av webbläsare på din enhet.
- **Skanna keyloggers.** Välj det här alternativet för att skanna ditt system efter keylogger-appar. Keyloggers registrerar vad du skriver på ditt tangentbord och skickar rapporter över internet till en illvillig person (hacker). Hackaren kan ta reda på känslig information från den stulna informationen, såsom bankkontonummer och lösenord, och använda den för att få personliga fördelar.

Antivirus Scan Wizard

När du initierar en genomsökning på begäran (till exempel högerklicka på en mapp, peka på Bitdefender och välj **Skanna med Bitdefender**), kommer Bitdefender Antivirus Scan-guiden att visas. Följ guiden för att slutföra skanningsprocessen.

Notera

Om skanningsguiden inte visas kan skanningen vara konfigurerad att köras tyst i bakgrunden. Leta efter skanningsförloppsikonen i systemfältet. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsförloppet.

Steg 1 - Utför skanning

Bitdefender kommer att börja skanna de valda objekten. Du kan se realtidsinformation om skanningsstatus och statistik (inklusive förfluten tid, en uppskattning av återstående tid och antalet upptäckta hot).

Vänta på att Bitdefender ska slutföra skanningen. Skanningsprocessen kan ta ett tag, beroende på hur komplex skanningen är.

Stoppa eller pausa skanningen. Du kan sluta skanna när du vill genom att klicka **SLUTA**. Du kommer direkt till det sista steget i guiden. För att tillfälligt stoppa skanningsprocessen klickar du bara **PAUS**. Du måste klicka **ÅTERUPPTA** för att återuppta skanningen.

Lösenordsskyddade arkiv. När ett lösenordsskyddat arkiv upptäcks, beroende på skanningsinställningarna, kan du bli ombedd att ange lösenordet. Lösenordsskyddade arkiv kan inte skannas om du inte anger lösenordet. Följande alternativ är tillgängliga:

- **Lösenord.** Om du vill att Bitdefender ska skanna arkivet, välj det här alternativet och skriv lösenordet. Om du inte känner till lösenordet, välj ett av de andra alternativen.
- **Be inte om ett lösenord och hoppa över det här objektet från genomsökningen.** Välj det här alternativet för att hoppa över att skanna det här arkivet.
- **Hoppa över alla lösenordsskyddade objekt utan att skanna dem.** Välj det här alternativet om du inte vill bry dig om lösenordsskyddade arkiv. Bitdefender kommer inte att kunna skanna dem, men en post kommer att sparas i skanningsloggen.

Välj önskat alternativ och klicka **OK** för att fortsätta skanna.

Steg 2 - Välj åtgärder

I slutet av skanningen kommer du att bli ombedd att välja vilka åtgärder som ska vidtas på de upptäckta filerna, om några.

> **Notera**
> När du kör en snabbsökning eller en systemgenomsökning, kommer Bitdefender automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer under skanningen. Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

De infekterade objekten visas i grupper, baserat på de hot de är infekterade med. Klicka på länken som motsvarar ett hot för att ta reda på mer information om de infekterade objekten.

Du kan välja en övergripande åtgärd som ska vidtas för alla frågor eller så kan du välja separata åtgärder för varje grupp av frågor. Ett eller flera av följande alternativ kan visas på menyn:

Vidta lämpliga åtgärder

Bitdefender kommer att vidta de rekommenderade åtgärderna beroende på typen av upptäckt fil:

- **Infekterade filer.** Filer som upptäckts som infekterade matchar en del av hotinformation som finns i Bitdefender Hot Information Database. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och rekonstruera den ursprungliga filen. Denna operation kallas desinfektion.

  Filer som inte kan desinficeras flyttas till karantän för att innehålla infektionen. Filer i karantän kan inte köras eller öppnas; därför försvinner risken att bli smittad. För mer information, se Hantera filer i karantän (sida 37).

  > **Viktig**
  > För särskilda typer av hot är desinficering inte möjlig eftersom den upptäckta filen är helt skadlig. I sådana fall tas den infekterade filen bort från disken.

- **Misstänkta filer.** Filer upptäcks som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen desinfektionsrutin finns tillgänglig. De kommer att flyttas till karantän för att förhindra en potentiell infektion.

- **Arkiv som innehåller infekterade filer.**
  - Arkiv som bara innehåller infekterade filer raderas automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer kommer Bitdefender att försöka ta bort de infekterade filerna förutsatt att det kan rekonstruera arkivet med de rena filerna. Om arkivrekonstruktion inte är möjlig kommer du att informeras om att inga åtgärder kan vidtas för att undvika att förlora rena filer.

Radera

Tar bort upptäckta filer från disken.

Om infekterade filer lagras i ett arkiv tillsammans med rena filer, kommer Bitdefender att försöka ta bort de infekterade filerna och rekonstruera arkivet med de rena filerna. Om arkivrekonstruktion inte är möjlig kommer du att informeras om att inga åtgärder kan vidtas för att undvika att förlora rena filer.

Gör inga åtgärder

Inga åtgärder kommer att vidtas på de upptäckta filerna. När skanningen är klar kan du öppna skanningsloggen för att visa information om dessa filer.

Klick **Fortsätta** för att tillämpa de angivna åtgärderna.

Steg 3 - Sammanfattning

När Bitdefender har åtgärdat problemen, visas skanningsresultaten i ett nytt fönster. Om du vill ha omfattande information om skanningsprocessen, klicka **VISA LOGG** för att se skanningsloggen.

Viktig

I de flesta fall desinficerar Bitdefender framgångsrikt de infekterade filerna som den upptäcker eller isolerar infektionen. Det finns dock problem som inte kan lösas automatiskt. Om det behövs, starta om systemet för att slutföra rengöringsprocessen. För mer information och instruktioner om hur man tar bort ett hot manuellt, se Ta bort hot från ditt system (sida 136).

Kontrollerar skanningsloggar

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen i antivirusfönstret. Skanningsloggen innehåller detaljerad information om den loggade skanningsprocessen, såsom skanningsalternativ, skanningsmålet, hoten som hittats och de åtgärder som vidtagits mot dessa hot.

Du kan öppna skanningsloggen direkt från skanningsguiden, när skanningen är klar, genom att klicka **VISA LOGG**.

Så här kontrollerar du en skanningslogg eller någon upptäckt infektion vid ett senare tillfälle:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.

2. I den **Allt** fliken väljer du meddelandet om den senaste skanningen. Det är här du kan hitta alla hotskanningshändelser, inklusive hot som upptäcks av skanning vid åtkomst, användarinitierade genomsökningar och statusändringar för automatiska genomsökningar.
3. I aviseringslistan kan du kontrollera vilka skanningar som har utförts nyligen. Klicka på ett meddelande för att se detaljer om det.
4. Klicka på för att öppna skanningsloggen **Visa logg**.

Automatisk skanning av flyttbara media

Bitdefender upptäcker automatiskt när du ansluter en flyttbar lagringsenhet till din enhet och skannar den i bakgrunden när alternativet Autoskanning är aktiverat. Detta rekommenderas för att förhindra hot från att infektera din enhet.

Upptäckta enheter faller inom en av dessa kategorier:

- CD/DVD
- Flash-enheter, såsom flash-pennor och externa hårddiskar
- mappade (fjärr) nätverksenheter

Du kan konfigurera automatisk skanning separat för varje kategori av lagringsenheter. Automatisk genomsökning av mappade nätverksenheter är avstängd som standard.

Hur fungerar det?

När den upptäcker en flyttbar lagringsenhet börjar Bitdefender skanna den efter hot (förutsatt att automatisk genomsökning är aktiverad för den typen av enhet). Du kommer att få ett meddelande via ett popup-fönster om att en ny enhet har upptäckts och att den skannas.

En Bitdefender-skanning ikonen visas i systemfältet. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsförloppet.

När skanningen är klar visas fönstret för skanningsresultat för att informera dig om du säkert kan komma åt filer på det flyttbara mediet.

I de flesta fall tar Bitdefender automatiskt bort upptäckta hot eller isolerar infekterade filer i karantän. Om det finns olösta hot efter genomsökningen kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

> **Notera**
> Tänk på att inga åtgärder kan vidtas på infekterade eller misstänkta filer som upptäcks på CD-/DVD-skivor. På samma sätt kan inga åtgärder vidtas på infekterade eller misstänkta filer som upptäcks på mappade nätverksenheter om du inte har rätt behörighet.

Denna information kan vara användbar för dig:

- Var försiktig när du använder en hotinfekterad CD/DVD, eftersom hotet inte kan tas bort från skivan (mediet är skrivskyddat). Se till att realtidsskydd är aktiverat för att förhindra att hot sprids till ditt system. Det är bäst att kopiera all värdefull data från skivan till ditt system och sedan kassera skivan.
- I vissa fall kanske Bitdefender inte kan ta bort hot från specifika filer på grund av juridiska eller tekniska begränsningar. Ett sådant exempel är filer som arkiveras med en proprietär teknologi (detta beror på att arkivet inte kan återskapas korrekt).
  För att ta reda på hur man hanterar hot, se Ta bort hot från ditt system (sida 136).

Hantera skanning av flyttbara media

Så här hanterar du automatisk genomsökning av flyttbara media:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Välj **inställningar** fönster.

Skanningsalternativen är förkonfigurerade för bästa detekteringsresultat. Om infekterade filer upptäcks kommer Bitdefender att försöka desinficera dem (ta bort den skadliga koden) eller flytta dem till karantän. Om båda åtgärderna misslyckas låter guiden Antivirussökning dig ange andra åtgärder som ska vidtas på infekterade filer. Skanningsalternativen är standard och du kan inte ändra dem.

För bästa skydd rekommenderas det att låta valt den **Automatisk skanning** alternativ för alla typer av flyttbara lagringsenheter.

Skanna värdfil

Hosts-filen kommer som standard med din operativsysteminstallation och används för att mappa värdnamn till IP-adresser varje gång du går in på en ny webbsida, ansluter till en FTP eller till andra internetservrar.

Det är en vanlig textfil och skadliga program kan ändra den. Avancerade användare vet hur man använder det för att blockera irriterande annonser, banners, cookies från tredje part eller kapare.

Så här konfigurerar du fil för skanningsvärd:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Avancerad** flik.
3. Slå på eller av **Skanna värdfil**.

Konfigurerar skanningsundantag

Bitdefender tillåter att man undantar specifika filer, mappar eller filtillägg från genomsökning. Den här funktionen är avsedd att undvika störningar i ditt arbete och den kan också bidra till att förbättra systemets prestanda. Undantag ska användas av användare som har avancerad datorkunskap eller på annat sätt följer rekommendationerna från en Bitdefender-representant.

Du kan konfigurera undantag så att de endast gäller för skanning vid åtkomst eller på begäran, eller för båda. Objekten undantagna från skanning vid åtkomst kommer inte att skannas, oavsett om de nås av dig eller en app.

> **Notera**
> Undantag kommer INTE att gälla för kontextuell skanning. Kontextgenomsökning är en typ av skanning på begäran: du högerklickar på filen eller mappen du vill skanna och väljer **Skanna med Bitdefender**.

Undantag filer och mappar från skanning

För att undanta specifika filer och mappar från skanning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Ange sökvägen till den mapp som du vill utom genom att skanna i motsvarande fält.

Alternativt kan du navigera till mappen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.

6. Slå på strömbrytaren bredvid skyddsfunktionen som inte ska skanna mappen. Det finns tre alternativ:
   - Antivirus
   - Hotförebyggande online
   - Avancerat hotförsvar
7. Klick **Spara** för att spara ändringarna och stänga fönstret.

Undantag filtillägg från skanning

När du undantar ett filtillägg från genomsökning, kommer Bitdefender inte längre att skanna filer med det tillägget, oavsett var de befinner sig på din enhet. Undantaget gäller även filer på flyttbara media, såsom CD-skivor, DVD-skivor, USB-lagringsenheter eller nätverksenheter.

> **Viktig**
> Var försiktig när du undantar tillägg från genomsökning eftersom sådana undantag kan göra din enhet sårbar för hot.

För att undanta filtillägg från skanning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Skriv de tillägg som du vill ska undantas från att skanna med en punkt före dem, separera dem med semikolon (;).
   txt;avi;jpg
6. Slå på strömbrytaren bredvid skyddsfunktionen som inte ska skanna tillägget.
7. Klick **Spara**.

Hantera skanningsundantag

Om de konfigurerade skanningsundantagen inte längre behövs, rekommenderas att du tar bort dem eller inaktiverar skanningsundantag.

Så här hanterar du skanningsundantag:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**. En lista med alla dina undantag kommer att visas.
4. För att ta bort eller redigera skanningsundantag, klicka på en av de tillgängliga knapparna. Fortsätt enligt följande:
   - För att ta bort en post från listan, klicka på knappen bredvid.
   - För att redigera en post från tabellen, klicka på **Redigera** knappen bredvid. Ett nytt fönster visas där du kan ändra tillägget eller sökvägen som ska undantas och säkerhetsfunktionen du vill att de ska undantas från, efter behov. Gör nödvändiga ändringar och klicka sedan **ÄNDRA**.

Hantera filer i karantän

Bitdefender isolerar de hotinfekterade filerna som den inte kan desinficera och de misstänkta filerna i ett säkert område som heter karantän. När ett hot är i karantän kan det inte göra någon skada eftersom det inte kan verkställas eller läsas.

Dessutom skannar Bitdefender filerna i karantän varje gång hotinformationsdatabasen uppdateras. Rensade filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Så här kontrollerar och hanterar du filer i karantän:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Gå till **inställningar** fönster.
   Här kan du se namnet på filerna i karantän, deras ursprungliga plats och namnet på de upptäckta hoten.
4. Filer i karantän hanteras automatiskt av Bitdefender enligt standardkarantäninställningarna.
   Även om det inte rekommenderas, kan du justera karantäninställningarna enligt dina preferenser genom att klicka **Visa inställningar**.
   Klicka på omkopplarna för att slå på eller av:

Skanna om karantänen efter uppdatering av hotinformation
Behåll det här alternativet aktiverat för att automatiskt skanna filer i karantän efter att varje databas med hotinformation har uppdaterats. Rensade filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Ta bort innehåll som är äldre än 30 dagar
Filer i karantän som är äldre än 30 dagar raderas automatiskt.

Skapa undantag för återställda filer
Filerna du återställer från karantän flyttas tillbaka till sin ursprungliga plats utan att repareras och undantas automatiskt från framtida skanningar.

5. Om du vill ta bort en fil i karantän markerar du den och klickar på **Radera** knapp. Om du vill återställa en fil i karantän till sin ursprungliga plats, välj den och klicka **Återställ**.

3.2.2. Avancerat hotförsvar

Bitdefender Advanced Threat Defense är en innovativ proaktiv detekteringsteknik som använder avancerade heuristiska metoder för att upptäcka ransomware och andra nya potentiella hot i realtid.

Advanced Threat Defense övervakar kontinuerligt apparna som körs på enheten och letar efter hotliknande åtgärder. Var och en av dessa åtgärder poängsätts och en totalpoäng beräknas för varje process.

Som en säkerhetsåtgärd kommer du att meddelas varje gång hot och potentiellt skadliga processer upptäcks och blockeras.

Slå på eller av Advanced Threat Defense

Så här aktiverar eller inaktiverar du Advanced Threat Defense:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. Gå till **inställningar** fönstret och klicka på knappen bredvid **Bitdefender Advanced Threat Defense**.

> **Notera**
> För att hålla ditt system skyddat från ransomware och andra hot rekommenderar vi att du inaktiverar Advanced Threat Defense under så kort tid som möjligt.

Kontrollerar upptäckta skadliga attacker

Närhelst hot eller potentiellt skadliga processer upptäcks kommer Bitdefender att blockera dem för att förhindra att din enhet infekteras av ransomware eller annan skadlig programvara. Du kan när som helst kontrollera listan över upptäckta skadliga attacker genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. Gå till **Hotförsvar** fönster.
   De attacker som upptäckts under de senaste 90 dagarna visas. För att hitta information om typen av en upptäckt ransomware, sökvägen till den skadliga processen, eller om desinfektionen har lyckats, klicka helt enkelt på den.

Lägga till processer till undantag

Du kan konfigurera undantagsregler för betrodda appar så att Advanced Threat Defense inte blockerar dem om de utför hotliknande åtgärder.

Så här börjar du lägga till processer till undantagslistan för avancerade hotförsvar:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Ange sökvägen till den mapp som du vill utom genom att skanna i motsvarande fält.
   Alternativt kan du navigera till den körbara filen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.
6. Slå på strömbrytaren bredvid **Avancerat hotförsvar**.
7. Klick **Spara**.

Utnyttjar upptäckt

Ett sätt som hackare använder för att bryta mot system är att dra fördel av särskilda buggar eller sårbarheter som finns i datorprogram (appar eller

plugins) och hårdvara. För att se till att din enhet håller sig borta från sådana attacker, som normalt sprids väldigt snabbt, använder Bitdefender den senaste anti-exploateringstekniken.

Aktivera eller inaktivera exploateringsdetektering

Så här aktiverar eller inaktiverar du upptäckt av utnyttjande:

- Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
- I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
- Gå till **inställningar** fönstret och klicka på knappen bredvid **Exploateringsdetektering** för att slå på eller av funktionen.

> **Notera**
> Alternativet Detektering av utnyttjande är aktiverat som standard.

3.2.3. Hotförebyggande online

Bitdefender Online Threat Prevention säkerställer en säker surfupplevelse genom att varna dig om potentiella skadliga webbsidor.

Bitdefender tillhandahåller hotförebyggande online i realtid för:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Så här konfigurerar du inställningar för onlinehotprevention:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ONLINE FÖREBYGGANDE AV HOT** rutan, klicka **inställningar**.

I den **Nätskydd** sektioner, klicka på reglagen för att slå på eller av:

- Förebyggande av webbattacker blockerar hot som kommer från internet, inklusive drive-by-nedladdningar.

- Search Advisor, en komponent som betygsätter resultaten av dina sökmotorfrågor och länkarna som publiceras på sociala nätverkswebbplatser genom att placera en ikon bredvid varje resultat:

  Du bör inte besöka denna webbsida.

  Den här webbsidan kan innehålla farligt innehåll. Var försiktig om du bestämmer dig för att besöka den.

  Detta är en säker sida att besöka.

  Search Advisor betygsätter sökresultaten från följande webbsökmotorer:

  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor betygsätter länkarna som publiceras på följande sociala nätverkstjänster online:

  - Facebook
  - Twitter

- Krypterad webbskanning.
  Mer sofistikerade attacker kan använda säker webbtrafik för att vilseleda sina offer. Därför rekommenderar vi att du håller alternativet Krypterad webbskanning aktiverat.
- Bedrägeriskydd.
- Nätfiskeskydd.

Scrolla ner så kommer du till **Förebyggande av nätverkshot** sektion. Här har du **Förebyggande av nätverkshot** alternativ. För att hålla din enhet borta från attacker från komplexa skadliga program (som ransomware) genom utnyttjande av sårbarheter, låt det här alternativet vara aktiverat.

Du kan skapa en lista över webbplatser, domäner och IP-adresser som inte kommer att skannas av Bitdefender-motorerna för anti-hot, antinätfiske och antibedrägeri. Listan bör endast innehålla webbplatser, domäner och IP-adresser som du helt litar på.

För att konfigurera och hantera webbplatser, domäner och IP-adresser med hjälp av funktionen Online Threat Prevention som tillhandahålls av Bitdefender:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ONLINE FÖREBYGGANDE AV HOT** rutan, klicka **inställningar**.
3. Klick **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Skriv i motsvarande fält namnet på webbplatsen, namnet på domänen eller IP-adressen du vill lägga till i undantag.
6. Klicka på knappen bredvid **Hotförebyggande online**.
7. För att ta bort en post från listan, klicka på knappen bredvid. Klick **Spara** för att spara ändringarna och stänga fönstret.

Bitdefender-varningar i webbläsaren

När du försöker besöka en webbplats som klassificeras som osäker, blockeras webbplatsen och en varningssida visas i din webbläsare.

Sidan innehåller information som webbadressen och det upptäckta hotet.

Du måste bestämma dig för vad du ska göra härnäst. Följande alternativ är tillgängliga:

- Navigera bort från webbplatsen genom att klicka **TA MIG TILLBAKA TILL SÄKERHET**.
- Fortsätt till webbplatsen, trots varningen, genom att klicka **Jag förstår riskerna, ta mig dit ändå**.
- Om du är säker på att den upptäckta webbplatsen är säker klickar du på **SKICKA IN** för att lägga till det till undantag. Vi rekommenderar att du bara lägger till webbplatser som du litar på till fullo.

3.2.4. E-postskydd

Din e-post är en viktig del av ditt digitala liv, och med tanke på dess många tillämpningar i verkliga livet har det blivit en föredragen attackvektor för dåliga aktörer och en av de primära cybersäkerhetsproblemen för den dagliga användaren.

E-postskydd är en säkerhetsfunktion som låter dig skanna och identifiera potentiellt farligt innehåll i e-postmeddelanden som tas emot i din inkorg. Den här funktionen är ett paket med en mängd olika tekniker som samlas under samma skyddsmodul, som anti-phishing, antimalware, antispam, anti-bedrägeri och anti-scam programvara.

Genom att skapa en direkt anslutning mellan Bitdefender och din e-postleverantör tillåter du antiviruset att skanna dina e-postmeddelanden direkt och eliminera de begränsningar som uppstår genom att använda olika enheter eller e-postklienter.

> **Notera**
> Du kan skydda upp till 5 olika e-postkonton.

Konfigurerar ditt konto

Denna funktion är sömlöst integrerad i användargränssnittet. Så här börjar du använda e-postskydd:

1. Under **Skydd**, klick **Öppen** i **E-postskydd** kort.
2. Välj din e-postleverantör för det e-postkonto du vill skydda.

> **Notera**
> E-postskydd är för närvarande tillgängligt för Google-konton, Outlook-konton och snart även tillgängligt för Yahoo Mail.

3. Klicka på **Logga in** knapp.
   Operationen fortsätter sedan i din webbläsare.
4. Ange din e-postadress och klicka på **Nästa** knapp
5. För att fortsätta, ange ditt lösenord och klicka på **Nästa** knapp.
6. Kontrollera de begärda behörigheterna på skärmen och låt Bitdefender skydda ditt e-postkonto.

Ditt e-postkonto är nu skyddat och alla dina nya inkommande e-postmeddelanden kommer att skannas mot hot.

> **Notera**
> Varje skannat e-postmeddelande kommer att markeras med en etikett för att indikera dess säkerhetsnivåer.

instrumentbräda

Instrumentpanelen visar dina skyddade e-postmeddelanden där du hittar:

- konfigurationsdatum (datumet då kontot konfigurerades för e-postskydd)

- status (aktiv eller inaktiv)
- antal filtrerade e-postmeddelanden under de senaste 30 dagarna. Här kommer du att se ett diagram som visar antalet säkra e-postmeddelanden och farliga e-postmeddelanden som tagits emot.

För att lägga till flera e-postkonton Klicka på **Lägg till ett annat konto** och gå igenom konfigurationsprocessen ovan för var och en av dem.

För att pausa skanning eller ta bort ett konto från den här funktionen klicka på de tre prickarna bredvid kontot i fråga och klicka på **Hantera konto**.

3.2.5. Anti Spam

Spam är en term som används för att beskriva oönskad e-post. Spam är ett växande problem, både för individer och för organisationer. Det är inte vackert, du vill inte att dina barn ska se det, det kan få dig avskedad (för att du slösar bort för mycket tid eller för att ta emot porr på din kontorspost) och du kan inte hindra folk från att skicka det. Det näst bästa med det är uppenbarligen att sluta ta emot det. Tyvärr finns skräppost i ett brett utbud av former och storlekar, och det finns mycket av det.

Bitdefender Antispam använder anmärkningsvärda tekniska innovationer och branschstandardiserade antispamfilter för att rensa bort spam innan den når användarens inkorg. För mer information, se Antispam-insikter (sida 45).

Bitdefender Antispam-skydd är endast tillgängligt för e-postklienter som är konfigurerade att ta emot e-postmeddelanden via POP3-protokollet. POP3 är ett av de mest använda protokollen för att ladda ner e-postmeddelanden från en e-postserver.

> **Notera**
> Bitdefender tillhandahåller inte antispam-skydd för e-postkonton som du kommer åt via en webbaserad e-posttjänst.

Skräppostmeddelandena som upptäckts av Bitdefender är markerade med [spam] prefix i ämnesraden. Bitdefender flyttar automatiskt skräppostmeddelanden till en specifik mapp, enligt följande:

- I Microsoft Outlook flyttas skräppostmeddelanden till en **Spam** mapp, som finns i **Raderade föremål** mapp. De **Spam** mappen skapas när ett e-postmeddelande märks som skräppost.

- I Mozilla Thunderbird flyttas skräppostmeddelanden till en **Spam** mapp, som finns i **Skräp** mapp. De **Spam** mappen skapas när ett e-postmeddelande märks som skräppost.

Om du använder andra e-postklienter måste du skapa en regel för att flytta e-postmeddelanden markerade som [spam] av Bitdefender till en anpassad karantänmapp. Om de borttagna objekten eller papperskorgen tas bort, kommer skräppostmappen också att tas bort. En ny skräppostmapp kommer dock att skapas så fort ett e-postmeddelande märks som skräppost.

Antispam-insikter

Antispam-funktionen har följande funktioner och inställningar:

Antispam-filter

Bitdefender Antispam Engine innehåller molnskydd och andra flera olika filter som säkerställer att din inkorg är fri från SPAM, som Vänner lista, Lista över spammare och Teckenuppsättningsfilter.

Vänlista / Spammare lista

De flesta människor kommunicerar regelbundet med en grupp människor eller till och med får meddelanden från företag eller organisationer inom samma domän. Genom att använda **vänner eller spammare lista**, kan du enkelt klassificera vilka personer du vill få e-post från (vänner) oavsett vad meddelandet innehåller, eller vilka personer du aldrig vill höra från igen (spammare).

> **Notera**
> Vi rekommenderar att du lägger till dina vänners namn och e-postadresser i **Vänner lista**. Bitdefender blockerar inte meddelanden från de på listan; Att lägga till vänner bidrar därför till att se till att legitima meddelanden når fram.

Teckenuppsättningsfilter

Många skräppostmeddelanden är skrivna med kyrilliska och/eller asiatiska teckenuppsättningar. Teckenuppsättningsfiltret upptäcker den här typen av meddelanden och taggar dem som SPAM.

Antispam operation

Bitdefender Antispam Engine använder alla antispamfilter kombinerade för att avgöra om ett visst e-postmeddelande ska komma in i din **Inkorg** eller inte.

Varje e-postmeddelande som kommer från internet kontrolleras först med Vänner lista/Lista över spammare filtrera. Om avsändarens adress finns i Vänner lista mejlet flyttas direkt till ditt **Inkorg**.

Annars, den Lista över spammare filter tar över e-postmeddelandet för att verifiera om avsändarens adress finns på listan. Om en matchning görs kommer e-postmeddelandet att taggas som SPAM och flyttas till **Spam** mapp.

Annars, den Teckenuppsättningsfilter kommer att kontrollera om e-postmeddelandet är skrivet med kyrilliska eller asiatiska tecken. Om så är fallet kommer e-postmeddelandet att taggas som SPAM och flyttas till **Spam** mapp.

> **Notera**
> Om e-postmeddelandet är taggat som SEXUELLT EXPLICITAT i ämnesraden kommer Bitdefender att betrakta det som SPAM.

E-postklienter och protokoll som stöds

Antispam-skydd tillhandahålls för alla POP3/SMTP-e-postklienter. Bitdefender Antispam-verktygsfältet är dock endast integrerat i:

- Microsoft Outlook 2007/2010/2013/2016/2019
- Mozilla Thunderbird 14 och högre versioner

Slå på eller av antispamskyddet

Antispam-skydd är aktiverat som standard.

Så här slår du på eller av antispam-funktionen:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTI SPAM** rutan, slå på eller av strömbrytaren.

Använda antispam-verktygsfältet i ditt e-postklientfönster

I den övre delen av ditt e-postklientfönster kan du se verktygsfältet Antispam. Antispam-verktygsfältet hjälper dig att hantera antispamskydd

direkt från din e-postklient. Du kan enkelt korrigera Bitdefender om det markerat ett legitimt meddelande som SPAM.

> **Viktig**
> Bitdefender integreras i de mest använda e-postklienterna genom ett lättanvänt verktygsfält för skräppost. För en komplett lista över e-postklienter som stöds, se E-postklienter och protokoll som stöds (sida 46).

Varje knapp från Bitdefender verktygsfält kommer att förklaras nedan:

inställningar - öppnar ett fönster där du kan konfigurera antispamfiltren och verktygsfältsinställningarna.

Är skräppost - indikerar att det valda e-postmeddelandet är skräppost. E-postmeddelandet kommer omedelbart att flyttas till **Spam** mapp. Om antispam-molntjänsterna är aktiverade skickas meddelandet till Bitdefender Cloud för vidare analys.

Ej spam - indikerar att det valda e-postmeddelandet inte är skräppost och att Bitdefender inte borde ha taggat det. E-postmeddelandet kommer att flyttas från **Spam** mapp till **Inkorg** katalog. Om antispam-molntjänsterna är aktiverade skickas meddelandet till Bitdefender Cloud för vidare analys.

> **Viktig**
> De **Ej spam** knappen blir aktiv när du väljer ett meddelande markerat som SPAM av Bitdefender (normalt finns dessa meddelanden i **Spam** mapp).

Lägg till spammer - lägger till avsändaren av det valda e-postmeddelandet till listan över spammare. Du kan behöva klicka **OK** att erkänna. De e-postmeddelanden som tas emot från adresser i listan med spammare markeras automatiskt som [spam].

Lägg till vän - lägger till avsändaren av det valda e-postmeddelandet i vänlistan. Du kan behöva klicka **OK** att erkänna. Du kommer alltid att få e-postmeddelanden från den här adressen oavsett vad de innehåller.

Spammare - öppnar **Lista över spammare** som innehåller alla e-postadresser som du inte vill ta emot meddelanden från, oavsett innehåll. För mer information, se Konfigurera listan över spammare (sida 50).

Vänner - öppnar **Vänner lista** som innehåller alla e-postadresser som du alltid vill ta emot e-postmeddelanden från, oavsett innehåll. För mer information, se Konfigurera vänlistan (sida 49).

Indikerar detekteringsfel

Om du använder en e-postklient som stöds kan du enkelt korrigera antispamfiltret (genom att ange vilka e-postmeddelanden som inte ska ha markerats som [spam]). Att göra det hjälper till att förbättra effektiviteten hos antispamfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till skräppostmappen dit skräppostmeddelanden flyttas.
3. Välj det legitima meddelandet felaktigt markerat som [spam] av Bitdefender.
4. Klick de **Lägg till vän** knappen på Bitdefender antispam-verktygsfältet för att lägga till avsändaren i vänlistan. Du kan behöva klicka **OK** att erkänna. Du kommer alltid att få e-postmeddelanden från den här adressen oavsett vad de innehåller.
5. Klicka på **Ej spam** knappen på Bitdefender antispam-verktygsfältet (normalt placerad i den övre delen av e-postklientfönstret). E-postmeddelandet kommer att flyttas till mappen Inkorg.

Indikerar oupptäckta skräppostmeddelanden

Om du använder en e-postklient som stöds kan du enkelt ange vilka e-postmeddelanden som ska ha upptäckts som skräppost. Att göra det hjälper till att förbättra effektiviteten hos antispamfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen Inkorg.
3. Välj de oupptäckta skräppostmeddelandena.
4. Klicka på **Är skräppost** knappen på Bitdefender antispam-verktygsfältet (normalt placerad i den övre delen av e-postklientfönstret). De markeras omedelbart som [spam] och flyttade till skräppostmappen.

Konfigurera verktygsfältsinställningar

För att konfigurera inställningarna för antispam-verktygsfältet för din e-postklient, klicka på **inställningar** knappen i verktygsfältet och sedan **Verktygsfältsinställningar** flik.

Här har du följande alternativ:

- **Markera skräppostmeddelanden som "Läst"** - markerar skräppostmeddelandena som lästa automatiskt för att inte störa när de kommer.
- Du kan välja om du vill visa bekräftelsefönster eller inte när du klickar på **Lägg till spammer** och **Lägg till vän** knappar på antispam-verktygsfältet.
  Bekräftelsefönster kan förhindra att e-postavsändare av misstag läggs till i listan med vänner/spammare.

Konfigurera vänlistan

De **Vänner lista** är en lista över alla e-postadresser som du alltid vill ta emot meddelanden från, oavsett innehåll. Meddelanden från dina vänner märks inte som spam, även om innehållet liknar spam.

> **Notera**
> Alla e-postmeddelanden som kommer från en adress som finns i **Vänner lista**, kommer automatiskt att levereras till din inkorg utan ytterligare bearbetning.

Så här konfigurerar och hanterar du vänlistan:

- Om du använder Microsoft Outlook eller Thunderbird, klicka på Vänner-knappen på Bitdefender verktygsfält för antispam.
- Alternativt:
  1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **ANTI SPAM** rutan, klicka **inställningar**.
  3. Få tillgång till **Hantera vänner** fönster.

För att lägga till en e-postadress, välj **E-postadress** anger du adressen och klickar sedan **LÄGG TILL**. Syntax: namn@domän.com.

För att lägga till alla e-postadresser från en specifik domän, välj **Domän namn** anger du domännamnet och klickar sedan **LÄGG TILL**. Syntax:

- @domain.com och domain.com - alla mottagna e-postmeddelanden från domain.com kommer att nå din **Inkorg** oavsett deras innehåll;
- domän - alla mottagna e-postmeddelanden från domänen (oavsett domänsuffix) kommer att märkas som SPAM;
- com - alla mottagna e-postmeddelanden med domänsuffixet com kommer att taggas som SPAM;

Det rekommenderas att undvika att lägga till hela domäner, men detta kan vara användbart i vissa situationer. Du kan till exempel lägga till e-postdomänen för företaget du arbetar för, eller för dina betrodda partners.

För att ta bort ett objekt från listan, klicka på motsvarande knappen bredvid. För att ta bort alla poster från listan, klicka **Tydlig lista**.

Du kan spara vänlistan till en fil så att du kan använda den på en annan enhet eller efter att du har installerat om produkten. För att spara vänlistan, klicka på knappen Spara och spara den på önskad plats. Filen kommer att ha en .bwl förlängning.

För att ladda en tidigare sparad vänlista, klicka **Ladda** och öppna motsvarande .bwl fil. För att återställa innehållet i den befintliga listan när du laddar en tidigare sparad lista, markera rutan bredvid **Skriv över aktuell lista**.

Konfigurera listan över spammare

De **Lista över spammare** är en lista över alla e-postadresser som du inte vill ta emot meddelanden från, oavsett innehåll. Alla e-postmeddelanden som tas emot från en adress som finns i **Lista över spammare** kommer automatiskt att markeras som SPAM, utan ytterligare bearbetning.

Så här konfigurerar och hanterar du listan med spammare:

- Om du använder Microsoft Outlook eller Thunderbird klickar du på **Spammare** knappen på Bitdefender verktygsfält för antispam integrerad i din e-postklient.
- Alternativt:
  1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **ANTI SPAM** rutan, klicka **inställningar**.
  3. Få tillgång till **Hantera spammare** fönster.

För att lägga till en e-postadress, välj **E-postadress** anger du adressen och klickar sedan **LÄGG TILL**. Syntax: namn@domän.com.

För att lägga till alla e-postadresser från en specifik domän, välj **Domän namn** anger du domännamnet och klickar sedan **LÄGG TILL**. Syntax:

- @domain.com och domain.com - alla mottagna e-postmeddelanden från domain.com kommer att nå din **Inkorg** oavsett deras innehåll;
- domän - alla mottagna e-postmeddelanden från domänen (oavsett domänsuffix) kommer att märkas som SPAM;
- com - alla mottagna e-postmeddelanden med domänsuffixet com kommer att taggas som SPAM.

Det rekommenderas att undvika att lägga till hela domäner, men detta kan vara användbart i vissa situationer.

> **Varning**
> Lägg inte till domäner med legitima webbaserade e-posttjänster (som Yahoo, Gmail, Hotmail eller andra) till listan över spammare. Annars kommer e-postmeddelanden som tas emot från alla registrerade användare av en sådan tjänst att upptäckas som skräppost. Om man till exempel lägger till yahoo.com till listan med spammare, alla e-postmeddelanden som kommer från yahoo.com adresser kommer att markeras som [spam].

För att ta bort ett objekt från listan, klicka på motsvarande knappen bredvid. För att ta bort alla poster från listan, klicka **Tydlig lista**.

Du kan spara listan med spammare i en fil så att du kan använda den på en annan enhet eller efter att du har installerat om produkten. För att spara listan med spammare, klicka på **Spara** knappen och spara den på önskad plats. Filen kommer att ha en *.bwl* förlängning.

Klicka på för att ladda en tidigare sparad lista med spammare **LADDA** och öppna motsvarande .bwl fil. För att återställa innehållet i den befintliga listan när du laddar en tidigare sparad lista, välj Skriv över aktuell lista.

Konfigurera de lokala antispamfiltren

Som beskrivs i Antispam-insikter (sida 45), Bitdefender använder en kombination av olika antispamfilter för att identifiera spam. Antispamfiltren är förkonfigurerade för effektivt skydd.

Viktig

Beroende på om du får legitima e-postmeddelanden skrivna med asiatiska eller kyrilliska tecken eller inte, inaktivera eller aktivera inställningen som automatiskt blockerar sådana e-postmeddelanden. Motsvarande inställning är inaktiverad i de lokaliserade versionerna av programmet som använder sådana teckenuppsättningar (till exempel i den ryska eller kinesiska versionen).

Så här konfigurerar du de lokala antispamfiltren:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTI SPAM** rutan, klicka **inställningar**.
3. Gå till **inställningar** fönstret och klicka på motsvarande slå på eller av-knappar.

Om du använder Microsoft Outlook eller Thunderbird kan du konfigurera de lokala antispamfiltren direkt från din e-postklient. Klicka på **inställningar** knappen på Bitdefender antispam-verktygsfältet (normalt placerad i den övre delen av e-postklientfönstret), och sedan **Antispamfilter** flik.

Konfigurera molninställningarna

Molndetekteringen använder Bitdefender Cloud-tjänsterna för att ge dig ett effektivt och alltid uppdaterat antispamskydd.

Molnskyddet fungerar så länge du håller Bitdefender Antispam aktiverat.

Exempel på legitima e-postmeddelanden eller skräppostmeddelanden kan skickas till Bitdefender Cloud när du indikerar upptäcktsfel eller oupptäckt skräppost. Detta hjälper till att förbättra Bitdefender antispam-detektering.

Konfigurera e-postexemplet till Bitdefender Cloud genom att välja önskade alternativ genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTI SPAM** rutan, klicka **inställningar**.
3. Gå till **inställningar** fönstret och klicka på motsvarande slå på eller av-knappar.

Om du använder Microsoft Outlook eller Thunderbird kan du konfigurera molndetekteringen direkt från din e-postklient. Klicka på **inställningar**

knappen på Bitdefender antispam-verktygsfältet (normalt placerad i den övre delen av e-postklientfönstret), och sedan **Molninställningar** flik.

3.2.6. Brandvägg

> **Obs!**
> Brandväggsmodulen i Bitdefender Ultimate Small Business Security är avstängd som standard. Du måste aktivera den manuellt.
>
> Om **Windows Defender Firewall** aktiveras under denna procedur uppmanas du att inaktivera den först.

Brandväggen skyddar din enhet från inkommande och utgående obehöriga anslutningsförsök, både i lokala nätverk och på internet. Det är ungefär som en portvakt - den håller reda på anslutningsförsök och bestämmer vilka som ska tillåtas och vilka som ska blockeras.

Bitdefenders brandvägg använder en uppsättning regler för att filtrera data som överförs till och från ditt system.

Under normala förhållanden skapar Bitdefender automatiskt en regel när en app försöker komma åt internet. Du kan också manuellt lägga till eller redigera regler för appar.

Som en säkerhetsåtgärd får du ett meddelande varje gång en potentiellt skadlig app blockeras från att komma åt internet.

Bitdefender tilldelar automatiskt en nätverkstyp till varje nätverksanslutning som detekteras. Beroende på nätverkstyp ställs brandväggsskyddet in på lämplig nivå för varje anslutning.

Mer information om brandväggsinställningarna för varje nätverkstyp och hur du kan redigera nätverksinställningarna finns i Hantera anslutningsinställningar (sida 56).

Aktivera eller inaktivera av brandväggsskydd

Så här aktiverar eller inaktiverar du brandväggsskydd:

1. Klicka på **Skydd** i navigeringsmenyn på Bitdefender-gränssnittet.
2. Aktivera eller inaktivera knappen i fönstret **BRANDVÄGG**.

> **Varning**
> Att stänga av brandväggen bör endast vara en tillfällig åtgärd, eftersom det utsätter enheten för obehöriga anslutningar. Aktivera brandväggen igen så snart som möjligt.

Hantera appregler

Så här visar och hanterar du brandväggsreglerna som styr appars åtkomst till nätverksresurser och internet:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
3. Gå till **Applikationsåtkomst** fönster.

Du kan se de senaste programmen (processerna) som har passerat genom Bitdefender Firewall och internetnätverket du är ansluten till. För att se reglerna som skapats för en specifik app, klicka bara på den och klicka sedan på **Se ansökningsregler** länk. De **Regler** fönstret öppnas.

För varje regel visas följande information:

- **NÄTVERK** - processen och nätverksadaptertyperna (hem/kontor, offentligt eller alla) som regeln gäller. Regler skapas automatiskt för att filtrera nätverks- eller internetåtkomst via valfri adapter. Som standard gäller reglerna för alla nätverk. Du kan skapa regler manuellt eller redigera befintliga regler för att filtrera en apps nätverk eller internetåtkomst via en specifik adapter (till exempel en trådlös nätverksadapter).
- **PROTOKOLL** - IP-protokollet som regeln gäller. Som standard gäller reglerna för alla protokoll.
- **TRAFIK** - regeln gäller i båda riktningarna, ingående och utgående.
- **HAMNAR** - PORT-protokollet som regeln gäller. Som standard gäller reglerna för alla portar.
- **IP** - Internetprotokollet (IP) som regeln gäller. Som standard gäller reglerna för alla IP-adresser.
- **TILLGÅNG** - om appen tillåts eller nekas åtkomst till nätverket eller internet under de angivna omständigheterna.

För att redigera eller ta bort reglerna för den valda appen, klicka på ··· ikon.

- **Redigera regel** - öppnar ett fönster där du kan redigera den aktuella regeln.
- **Ta bort regel** - du kan välja att ta bort den aktuella uppsättningen regler för den valda appen.

Lägger till appregler

Så här lägger du till en appregel:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
3. I den **Regler** fönster, klicka **Lägg till regel**.

Här kan du tillämpa följande ändringar:

- **Tillämpa denna regel på alla ansökningar.** Aktivera den här omkopplaren för att tillämpa den skapade regeln på alla appar.
- **Programväg.** Klick **BLÄDDRA** och välj appen som regeln gäller.
- **Lov.** Välj en av de tillgängliga behörigheterna:

Lov	Beskrivning
Tillåta	Den angivna appen kommer att tillåtas nätverks-/internetåtkomst under de angivna omständigheterna.
Förneka	Den angivna appen kommer att nekas nätverks-/internetåtkomst under de angivna omständigheterna.

- **Nätverkstyp**. Välj vilken typ av nätverk regeln gäller. Du kan ändra typ genom att öppna **Nätverkstyp** rullgardinsmenyn och välja en av de tillgängliga typerna från listan.

Nätverkstyp	Beskrivning
Vilket nätverk som helst	Tillåt all trafik mellan din enhet och andra enheter oavsett nätverkstyp.
Hemmakontor	Tillåt all trafik mellan din enhet och olika i det lokala nätverket.
offentlig	All trafik filtreras.

- **Protokoll.** Välj i menyn vilket IP-protokoll regeln gäller.
  - Om du vill att regeln ska gälla för alla protokoll, välj **Några**.
  - Om du vill att regeln ska gälla för TCP, välj **TCP**.
  - Om du vill att regeln ska gälla för UDP väljer du **UDP**.
  - Om du vill att regeln ska gälla för ICMP, välj **ICMP**.
  - Om du vill att regeln ska gälla för IGMP, välj **IGMP**.
  - Om du vill att regeln ska gälla för GRE, välj **GRE**.

- Om du vill att regeln ska gälla för ett specifikt protokoll, skriv in numret som tilldelats protokollet du vill filtrera i det tomma redigeringsfältet.

> **Notera**
> IP-protokollnummer tilldelas av Internet Assigned Numbers Authority (IANA). Du hittar den fullständiga listan över tilldelade IP-protokollnummer på http://www.iana.org/assignments/protocol-numbers.

- **Riktning.** Välj i menyn vilken trafikriktning regeln gäller.

Riktning	Beskrivning
Utgående	Regeln gäller endast för den utgående trafiken.
Inkommande	Regeln gäller endast för den inkommande trafiken.
Både	Regeln gäller i båda riktningarna.

Klicka på **Avancerade inställningar** knappen i den nedre delen av fönstret för att anpassa följande inställningar:

- **Anpassad lokal adress.** Ange den lokala IP-adressen och porten som regeln gäller.
- **Anpassad fjärradress.** Ange fjärr-IP-adressen och porten som regeln gäller.

För att ta bort den aktuella uppsättningen regler och återställa standardreglerna, klicka **Återställ regler** i **Regler** fönster.

Hantera anslutningsinställningar

Oavsett om du ansluter till internet med en Wi-Fi- eller Ethernet-adapter kan du konfigurera vilka inställningar som ska tillämpas för en säker navigering. Alternativen du kan välja mellan är:

- **Dynamisk** – nätverkstypen kommer att ställas in automatiskt baserat på profilen för det anslutna nätverket, Home/Office eller Public. När detta händer kommer endast brandväggsregler för den specifika nätverkstypen eller de som är definierade att gälla för alla nätverkstyper att gälla.
- **Hemmakontor** – nätverkstypen kommer alltid att vara Hemma / Kontor, utan hänsyn till profilen för det anslutna nätverket. När detta

händer kommer endast brandväggsregler för hem/kontor eller de som är definierade att gälla för alla nätverkstyper att gälla.

- **offentlig** - Nätverkstypen kommer alltid att vara offentlig, utan hänsyn till profilen för det anslutna nätverket. När detta händer kommer endast brandväggsregler för offentliga eller de som är definierade att gälla för alla nätverkstyper att gälla.

Så här konfigurerar du dina nätverkskort:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
3. Välj **Nätverksadaptrar** fönster.
4. Välj de inställningar du vill använda när du ansluter till följande adaptrar:
   - Wi-Fi
   - Ethernet

Konfigurera avancerade inställningar

Så här konfigurerar du avancerade brandväggsinställningar:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
3. Välj **inställningar** fönster.

Följande funktioner kan konfigureras:

- **Skydd mot portskanning** - upptäcker och blockerar försök att ta reda på vilka portar som är öppna.
  Portskanningar används ofta av hackare för att ta reda på vilka portar som är öppna på din enhet. De kan sedan bryta sig in i din enhet om de hittar en mindre säker eller sårbar port.
- **Varningsläge** - varningar visas varje gång en app försöker ansluta till internet. Välj **Tillåta** eller **Blockera**. När varningsläget är aktiverat, visas Profiler funktionen stängs av automatiskt. Varningsläge kan användas samtidigt med **Batteriläge**.
- **Tillåt åtkomst till domännätverk** - tillåta eller neka åtkomst till resurser och resurser som definierats av dina domänkontrollanter.

- **Smygläge** - om du kan upptäckas av andra enheter. Klicka på **Redigera stealth-inställningar** för att välja när din enhet ska eller inte ska vara synlig för andra enheter.
- **Standardprogrambeteende** - Tillåt Bitdefender att tillämpa automatiska inställningar på appen utan definierade regler. Klick **Redigera standardregler** för att välja om automatiska inställningar ska tillämpas eller inte.
  - Automatiskt – appåtkomst tillåts eller nekas baserat på den automatiska brandväggen och användarreglerna.
  - Tillåt – appar som inte har definierat någon brandväggsregel kommer att tillåtas automatiskt.
  - Blockera – appar som inte har någon brandväggsregel definierad kommer att blockeras automatiskt.

3.2.7. Sårbarhet

Ett viktigt steg för att skydda din enhet mot skadliga åtgärder och appar är att hålla operativsystemet och de appar du regelbundet använder uppdaterade. Dessutom, för att förhindra obehörig fysisk åtkomst till din enhet, måste starka lösenord (lösenord som inte är lätta att gissa) konfigureras för varje Windows-användarkonto och även för de Wi-Fi-nätverk du ansluter till.

Bitdefender tillhandahåller två enkla sätt att fixa sårbarheterna i ditt system:

- Du kan skanna ditt system efter sårbarheter och åtgärda dem steg för steg med hjälp av **Sårbarhetsskanning** alternativ.
- Med hjälp av automatisk sårbarhetsövervakning kan du kontrollera och åtgärda upptäckta sårbarheter i Aviseringar fönster.

Du bör kontrollera och fixa systemsårbarheter varannan eller varannan vecka.

Skanna ditt system efter sårbarheter

För att upptäcka systemsårbarheter kräver Bitdefender en aktiv internetanslutning.

För att skanna ditt system efter sårbarheter:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. I den **Sårbarhetsskanning** flikklicka **Starta skanning**, vänta sedan på att Bitdefender ska kontrollera ditt system för sårbarheter. De upptäckta sårbarheterna är grupperade i tre kategorier:

   - **OPERATIV SYSTEM**
     - **Säkerhet för operativsystem**
       Ändrade systeminställningar som kan äventyra din enhet och data, som att inte visa varningar när körda filer utför ändringar på ditt system utan din tillåtelse eller när MTP-enheter som telefoner eller kameror ansluter och utför olika operationer utan din vetskap.
     - **Kritiska Windows-uppdateringar**
       En lista över viktiga Windows-uppdateringar som inte är installerade på din dator visas. En omstart av systemet kan krävas för att tillåta Bitdefender att slutföra installationen. Observera att det kan ta ett tag att installera uppdateringarna.
     - **Svaga Windows-konton**
       Du kan se listan över Windows-användarkonton som konfigurerats på din enhet och skyddsnivån deras lösenord ger. Du kan välja mellan att be användaren att byta lösenord vid nästa inloggning eller att byta lösenord själv direkt. För att ställa in ett nytt lösenord för ditt system, välj **Ändra lösenordet nu**.
       För att skapa ett starkt lösenord rekommenderar vi att du använder en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).
   - **ANSÖKNINGAR**
     - **Webbläsarsäkerhet**
       Ändra enhetens inställningar som tillåter körning av filer och program som laddas ner via Internet Explorer utan integritetsvalidering, vilket kan leda till att din enhet äventyras.
     - **Appuppdateringar**
       För att se information om appen som behöver uppdateras, klicka på dess namn i listan.

Om en app inte är uppdaterad klickar du **Ladda ner ny version** för att ladda ner den senaste versionen.

- **NÄTVERK**
  - **Nätverk och referenser**
    Ändrade systeminställningar som att automatiskt ansluta till öppna hotspot-nätverk utan din vetskap eller att inte upprätthålla kryptering på den utgående säkra kanaltrafiken.
  - **Wi-Fi-nätverk och routrar**
    För att ta reda på mer om det trådlösa nätverket och routern du är ansluten till, klicka på dess namn i listan. Om det rekommenderas att ställa in ett starkare lösenord för ditt hemnätverk, se till att du följer våra instruktioner, så att du kan hålla dig uppkopplad utan att oroa dig för din integritet.
    När andra rekommendationer finns tillgängliga, följ instruktionerna för att se till att ditt hemnätverk skyddas från hackarnas nyfikna ögon.

Använder automatisk sårbarhetsövervakning

Bitdefender skannar ditt system efter sårbarheter regelbundet, i bakgrunden, och håller register över upptäckta problem i Aviseringar fönster.

Så här kontrollerar och åtgärdar du de upptäckta problemen:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken väljer du meddelandet om sårbarhetsgenomsökningen.
3. Du kan se detaljerad information om de upptäckta systemets sårbarheter. Beroende på problemet, fortsätt enligt följande för att åtgärda en specifik sårbarhet:
   - Om Windows-uppdateringar är tillgängliga klickar du på **Installera**.
   - Om automatisk Windows-uppdatering är inaktiverad klickar du på **Gör det möjligt**.

- Om en app är föråldrad klickar du på **Uppdatera nu** för att hitta en länk till leverantörens webbsida där du kan installera den senaste versionen av den appen.
- Om ett Windows-användarkonto har ett svagt lösenord, klicka **ändra lösenord** för att tvinga användaren att ändra lösenordet vid nästa inloggning eller ändra lösenordet själv. För ett starkt lösenord, använd en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).
- Om Windows Autorun-funktionen är aktiverad klickar du på **Fixera** för att inaktivera den.
- Om routern du har konfigurerat har angett ett svagt lösenord, klicka på **ändra lösenord** för att komma åt dess gränssnitt där du kan ställa in ett starkt.
- Om nätverket du är ansluten till har sårbarheter som kan utsätta ditt system för risk, klicka **Ändra Wi-Fi-inställningar**.

Så här konfigurerar du inställningarna för sårbarhetsövervakning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.

   Viktig
   För att automatiskt bli meddelad om system- eller appsårbarheter, behåll **Sårbarhet** alternativet aktiverat.

3. Gå till **inställningar** flik.
4. Välj de systemsårbarheter som du vill ska kontrolleras regelbundet genom att använda motsvarande växlar.
   Windows-uppdateringar
   Kontrollera om ditt Windows-operativsystem har de senaste kritiska säkerhetsuppdateringarna från Microsoft.
   Appuppdateringar
   Kontrollera om appar som är installerade på ditt system är uppdaterade. Föråldrade appar kan utnyttjas av skadlig programvara, vilket gör din dator sårbar för attacker utifrån.
   Användarlösenord
   Kontrollera om lösenorden för Windows-konton och routrar som är konfigurerade på systemet är lätta att gissa eller inte. Att ställa in

lösenord som är svåra att gissa (starka lösenord) gör det mycket svårt för hackare att bryta sig in i ditt system. Ett starkt lösenord inkluderar stora och små bokstäver, siffror och specialtecken (som #, $ eller @).

Autospela

Kontrollera statusen för Windows Autorun-funktionen. Den här funktionen gör att appar kan startas automatiskt från CD-skivor, DVD-skivor, USB-enheter eller andra externa enheter.

Vissa typer av hot använder Autorun för att spridas automatiskt från flyttbara media till datorn. Det är därför det rekommenderas att inaktivera denna Windows-funktion.

Wi-Fi säkerhetsrådgivare

Kontrollera om det trådlösa hemnätverket du är ansluten till är säkert eller inte, och om det har sårbarheter. Kontrollera också om lösenordet för din hemrouter är tillräckligt starkt och hur du kan göra det säkrare.

De flesta oskyddade trådlösa nätverk är inte säkra, vilket gör att hackarnas nyfikna ögon har tillgång till dina privata aktiviteter.

Notera

Om du stänger av övervakning av en specifik sårbarhet kommer relaterade problem inte längre att registreras i meddelandefönstret.

Wi-Fi säkerhetsrådgivare

När du är på språng, arbetar på ett kafé eller väntar på flygplatsen kan det vara den snabbaste lösningen att ansluta till ett allmänt trådlöst nätverk för att göra betalningar, kolla e-post eller konton i sociala nätverk. Men nyfikna ögon som försöker kapa din personliga data kan vara där och se hur informationen läcker genom nätverket.

Personuppgifter avser lösenorden och användarnamnen du använder för att få tillgång till dina onlinekonton, såsom e-post, bankkonton, konton i sociala medier, men även de meddelanden du skickar.

Vanligtvis är det mer sannolikt att offentliga trådlösa nätverk är osäkra eftersom de inte kräver lösenord vid inloggning, och om de gör det kan lösenordet göras tillgängligt för alla som vill ansluta. Dessutom kan de vara skadliga nätverk eller nätverk som representerar ett mål för cyberbrottslingar.

Bitdefender Wi-Fi Security Advisor ger information om:

- Hemma Wi-Fi-nätverk

- Office Wi-Fi-nätverk
- Offentliga Wi-Fi-nätverk

Slå på eller av aviseringar från Wi-Fi Security Advisor

Så här slår du på eller av Wi-Fi Security Advisor-meddelanden:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **inställningar** fönstret och slå på eller av **Wi-Fi säkerhetsrådgivare** alternativ.

Konfigurera Wi-Fi-hemnätverk

Så här börjar du konfigurera ditt hemnätverk:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **Wi-Fi säkerhetsrådgivare** fönstret och klicka **Hemma Wi-Fi**.
4. I den **Hemma Wi-Fi** fliken, klicka **VÄLJ HEM WI-FI**.
   En lista med de trådlösa nätverk som du anslutit till hittills visas.
5. Peka på ditt hemnätverk och klicka sedan **VÄLJ**.

Om ett hemnätverk anses osäkert eller osäkert visas konfigurationsrekommendationer för att förbättra dess säkerhet.

För att ta bort det trådlösa nätverket du har ställt in som ett hemnätverk, klicka på **AVLÄGSNA** knapp.

För att lägga till ett nytt trådlöst nätverk som hem, klicka **Välj nytt hem wi-fi**.

Konfigurera Office Wi-Fi-nätverk

Så här börjar du konfigurera ditt kontorsnätverk:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.
3. Gå till **Wi-Fi säkerhetsrådgivare** fönster, klicka **Office Wi-Fi**.
4. I den **Office Wi-Fi** fliken, klicka **VÄLJ KONTOR WI-FI**.

En lista med de trådlösa nätverk som du anslutit till hittills visas.

5. Peka på ditt kontorsnätverk och klicka sedan **VÄLJ**.

Om ett kontorsnätverk anses osäkert eller osäkert visas konfigurationsrekommendationer för att förbättra dess säkerhet.

För att ta bort det trådlösa nätverket du har ställt in som kontorsnätverk, klicka på **AVLÄGSNA**.

För att lägga till ett nytt trådlöst nätverk som kontor, klicka **Välj nytt kontorswi-fi**.

Offentligt Wi-Fi

När den är ansluten till ett osäkert eller osäkert trådlöst nätverk är den offentliga Wi-Fi-profilen aktiverad. När du kör i den här profilen, Bitdefender Ultimate Small Business Security är inställd på att automatiskt utföra följande programinställningar:

- Advanced Threat Defense är aktiverat
- Bitdefender-brandväggen är påslagen och följande inställningar tillämpas på din trådlösa adapter:
  - Stealth-läge - PÅ
  - Nätverkstyp - Offentlig
- Följande inställningar från Online Threat Prevention är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägerier
  - Skydd mot nätfiske
- En knapp som öppnar Bitdefender Safepay™ är tillgänglig. I det här fallet är hotspot-skyddet för osäkra nätverk aktiverat som standard.

Kontrollera information om Wi-Fi-nätverk

Så här kontrollerar du information om de trådlösa nätverk du vanligtvis ansluter till:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SÅRBARHET** rutan, klicka **Öppen**.

3. Gå till **Wi-Fi säkerhetsrådgivare** fönster.
4. Beroende på vilken information du behöver, välj en av de tre flikarna, **Hemma Wi-Fi**, **Office Wi-Fi** eller **Offentligt Wi-Fi**.
5. Klick **Visa detaljer** bredvid nätverket du vill hitta mer information om.

Det finns tre typer av trådlösa nätverk som filtreras efter deras betydelse, varje typ indikeras av en specifik ikon:

Wi-Fi är osäkert - indikerar att säkerhetsnivån för nätverket är låg. Detta innebär att det finns en hög risk att använda den, och det rekommenderas inte att göra betalningar eller kontrollera bankkonton utan ett extra skydd. I sådana situationer rekommenderar vi att du använder Bitdefender Safepay™ med Hotspot-skydd för osäkra nätverk aktiverat.

Wi-Fi är osäkert - indikerar att säkerhetsnivån för nätverket är måttlig. Detta innebär att den kan ha sårbarheter och det rekommenderas inte att göra betalningar eller kontrollera bankkonton utan ett extra skydd. I sådana situationer rekommenderar vi att du använder Bitdefender Safepay™ med Hotspot-skydd för osäkra nätverk aktiverat.

Wi-Fi är säkert - indikerar att nätverket du använder är säkert. I det här fallet kan du använda känsliga uppgifter för att göra onlineoperationer.

Genom att klicka på **Visa detaljer** länk i området för varje nätverk, visas följande detaljer:

- **Säkrad** - här kan du se om det valda nätverket är skyddat eller inte. Okrypterade nätverk kan lämna data du använder exponerad.
- **Krypteringstyp** - här kan du se vilken krypteringstyp som används av det valda nätverket. Vissa krypteringstyper kanske inte är säkra. Därför rekommenderar vi starkt att du kontrollerar information om den visade krypteringstypen för att vara säker på att du är skyddad när du surfar på webben.
- **Kanal/frekvens** - här kan du se kanalfrekvensen som används av det valda nätverket.
- **Lösenordsstyrka** - här kan du se hur starkt lösenordet är. Observera att de nätverk som har angett svaga lösenord är ett mål för cyberbrottslingar.

- **Typ av inloggning** - här kan du se om det valda nätverket är skyddat med ett lösenord eller inte. Det rekommenderas starkt att endast ansluta till nätverk som har ställt in starka lösenord.
- **Autentiseringstyp** - här kan du se vilken autentiseringstyp som används av det valda nätverket.

3.2.8. Video- och ljudskydd

Fler och fler hot är utformade för att komma åt inbyggda webbkameror och mikrofoner. För att förhindra obehörig åtkomst till din webbkamera och för att informera dig om vilka opålitliga appar som kommer åt din enhets mikrofon och när, Bitdefender Video & Ljud har inkluderat:

- Webbkamera skydd
- Mikrofonmonitor

Webbkamera skydd

Att hackare kan ta över din webbkamera för att spionera på dig är ingen nyhet längre, och lösningar för att skydda den, som att återkalla appens privilegier, inaktivera enhetens inbyggda kamera eller att täcka över den är inte särskilt praktiska. För att förhindra ytterligare försök att få tillgång till din integritet övervakar Bitdefender Webcam Protection permanent de appar som försöker få åtkomst till din kamera och blockerar de som inte är listade som betrodda.

Som en säkerhetsåtgärd kommer du att meddelas varje gång en opålitlig app försöker få åtkomst till din kamera.

Slå på eller av webbkameraskydd

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå nu till **inställningar** fönstret och slå på eller av motsvarande strömbrytare.

Konfigurera webbkameraskydd

Du kan konfigurera vilka regler som ska tillämpas när en app ska försöka få åtkomst till din kamera genom att följa dessa steg:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.

2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå till **inställningar** flik.

Följande alternativ är tillgängliga:

Regler för applikationsblock

- **Blockera all åtkomst till webbkameran** - ingen app kommer att tillåtas få åtkomst till din webbkamera.
- **Blockera webbläsares åtkomst till webbkameran** - Ingen webbläsare förutom Internet Explorer och Microsoft Edge kommer att tillåtas att få åtkomst till din webbkamera. På grund av proceduren för Windows Store-appar som körs i en enda process, kan Internet Explorer och Microsoft Edge inte upptäckas av Bitdefender som webbläsare och är därför undantagna från denna inställning.
- **Ställ in applikationsbehörigheter baserat på gemenskapsval** - om majoriteten av Bitdefender-användare anser att en populär app är ofarlig, kommer dess åtkomst till webbkameran automatiskt att ställas in på Tillåt. Om en populär app anses vara farlig av många, kommer dess åtkomst automatiskt att ställas in på Blockerad.

Aviseringar

- **Meddela när tillåtna appar ansluter till webbkameran** - du kommer att meddelas varje gång en tillåten app kommer åt din webbkamera.

Lägga till appar i webbkameraskyddslistan

Appar som försöker ansluta till din webbkamera upptäcks automatiskt och beroende på deras beteende och gruppens val tillåts eller nekas deras åtkomst. Du kan dock manuellt börja konfigurera på egen hand vilken åtgärd som ska vidtas genom att följa dessa steg:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå till **Webbkamera skydd** fönster.
4. Klick **Lägg till applikation** fönster.
5. Klicka på önskad länk:

- **Från Windows Store** - en lista med de upptäckta Windows Store-apparna visas. Slå på reglagen bredvid de appar du vill lägga till i listan.
- **Från dina appar** - gå till .exe-filen du vill lägga till i listan och klicka sedan **OK**.

För att se vad Bitdefender-användarna har valt att göra med den valda appen, klicka på ikon.

Apparna som kommer att begära åtkomst till din kamera tillsammans med tidpunkten för senaste aktivitet visas i det här fönstret.

Du kommer att meddelas varje gång en av de tillåtna apparna blockeras av Bitdefender-användarna.

För att stoppa åtkomsten av en tillagd app till din webbkamera, klicka på ikon.

Ikonen vänder sig till , vilket betyder att den valda appen inte har tillgång till din webbkamera.

Mikrofonmonitor

Rogue appar kan komma åt din inbyggda mikrofon tyst eller i bakgrunden utan ditt medgivande. För att göra dig medveten om potentiella skadliga utnyttjande kommer Bitdefender Microphone Monitor att meddela dig om sådana händelser. På så sätt kommer ingen app att kunna få tillgång till din mikrofon utan att du är ansvarig.

Slå på eller av mikrofonmonitor

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Välj **inställningar** fönster.
4. I den **inställningar** fönster, slå på eller av **Mikrofonmonitor** växla.

Konfigurera aviseringar för mikrofonmonitor

Följ dessa steg för att konfigurera vilka aviseringar som ska visas när appar försöker få åtkomst till din mikrofon:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.

2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå till **inställningar** fönster.

Aviseringar

- **Meddela när ett program försöker komma åt mikrofonen**
- **Meddela när webbläsare kommer åt mikrofonen**
- **Meddela när opålitliga appar kommer åt mikrofonen**
- **Visa meddelande baserat på Bitdefender-användares val**

Lägger till appar till listan över mikrofonmonitorer

Appar som försöker ansluta till din mikrofon kommer automatiskt att upptäckas och läggas till i aviseringslistan. Du kan dock manuellt konfigurera på egen hand om ett meddelande ska visas eller inte genom att följa dessa steg:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå till **Ljudskydd** fönster.
4. Klick **Lägg till applikation** fönster.
5. Klicka på önskad länk:
   - **Från Windows Store** - en lista med de upptäckta Windows Store-apparna visas. Slå på reglagen bredvid de appar du vill lägga till i listan.
   - **Från dina appar** - gå till .exe-filen du vill lägga till i listan och klicka sedan **OK**.

För att se vad Bitdefender-användarna har valt att göra med den valda appen, klicka på ikon.

Apparna som kommer att begära åtkomst till din mikrofon tillsammans med tidpunkten för senaste aktivitet visas i det här fönstret.

För att sluta ta emot aviseringar om aktiviteten för en tillagd app, klicka på ikon.

Ikonen vänder sig till , vilket betyder att inget Bitdefender-meddelande kommer att visas när den valda appen försöker komma åt din mikrofon.

3.2.9. Ransomware-sanering

Bitdefender Ransomware Remediation säkerhetskopierar dina filer såsom dokument, bilder, videor eller musik för att se till att de är skyddade från att skadas eller förloras i händelse av ransomware-kryptering. Varje gång en ransomware-attack upptäcks kommer Bitdefender att blockera alla processer som är involverade i attacken och starta åtgärdsprocessen. På så sätt kommer du att kunna återställa innehållet i hela dina filer utan att betala för någon begärd lösen.

Slå på eller av Ransomware Remediation

Så här slår du på eller av Ransomware Remediation:

1. 1. Klicka **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **RANSOMWARE ÅTGÄRD** rutan, slå på eller av strömbrytaren.

> **Notera**
> För att säkerställa att dina filer är skyddade mot ransomware rekommenderar vi att du håller Ransomware Remediation aktiverat.

Slå på eller av automatisk återställning

Automatisk återställning ser till att dina filer automatiskt återställs i händelse av ransomware-kryptering.

Så här aktiverar eller inaktiverar du automatisk återställning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **RANSOMWARE ÅTGÄRD** rutan, klicka **Hantera**.
3. Slå på eller av i fönstret Inställningar **Automatisk återställning** växla.

Visa filer som har återställts automatiskt

När **Automatisk återställning** alternativet är aktiverat, kommer Bitdefender automatiskt att återställa filer som krypterades av ett ransomware. Härigenom kan du njuta av en bekymmersfri upplevelse och veta att dina filer är säkra.

Så här visar du filer som har återställts automatiskt:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken, välj aviseringen om det senast åtgärdade ransomware-beteendet och klicka sedan **Återställda filer**.

Listan med de återställda filerna visas. Här kan du också se platsen där dina filer har återställts.

Återställa krypterade filer manuellt

Om du måste återställa filer som krypterades av ett ransomware manuellt, följ dessa steg:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken, välj meddelandet om det senaste ransomware-beteendet som upptäckts och klicka sedan **Krypterade filer**.
3. Listan med de krypterade filerna visas.
   Klick **Återställ filer** att fortsätta.
4. Om hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de dekrypterade filerna ska sparas. Klick **Återställ plats**, och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.
   Klick **Avsluta** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas om de blir krypterade:

.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.db;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.htm;.html;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.mid;.midi;.mkv;.mp3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;.ogg;.pdf;.pkg;.php;.pl;.png;.pps;.ppt;.pptx;.ps;.psd;.py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.tex;.tif;.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.wav;.wks;.wma;.wpl;.wps;.wpd;.wsf;.z;.zip;

Lägga till applikationer till undantag

Du kan konfigurera undantagsregler för betrodda appar så att Ransowmare Remediation-funktionen inte blockerar dem om de utför ransomware-liknande åtgärder.

Så här lägger du till appar till undantagslistan för Ransomware Remediation:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **RANSOMWARE ÅTGÄRD** rutan, klicka **Hantera**.
3. Gå till **Undantag** fönstret och klicka **+Lägg till ett undantag**.

3.2.10. Cryptomining Protection

Vad är Cryptomining Protection?

Med hjälp av kryptominering kan angripare dra ekonomisk nytta utan att bära de tillhörande kostnaderna och juridiska konsekvenserna.

Bitdefenders Cryptomining Protection-funktion försvarar Windows-datorer mot det växande hotet från obehöriga kryptominingaktiviteter, en skadlig praxis som utnyttjar en användares resurser och el för att generera intäkter för angripare.

> **Notera**
> Kryptomineringsskydd förlitar sig på:
>
> - Bitdefender Shield
> - Förebyggande av webbattacker
>
> För att Cryptomining Protection ska kunna köras måste båda dessa två funktioner också vara aktiverade.

Aktiverar kryptomineringsskydd

Cryptomining Protection-funktionen finns på fliken Skydd.

För att aktivera det, växla helt enkelt motsvarande strömbrytare.

> **Notera**
> Cryptomining Protection är inaktiverat som standard, vilket säkerställer att användarna har kontroll över dess aktivering.

Driftsätt

När den har aktiverats fungerar Cryptomining Protection-funktionen i två distinkta tillstånd, var och en skräddarsydd efter användarens preferenser:

1. **Blockera alla Cryptomining-aktiviteter.** (blockerar automatiskt alla kryptominingaktiviteter och vidtar nödvändiga åtgärder för att förhindra ytterligare obehöriga försök)
   Det här läget är idealiskt för användare som inte har för avsikt att delta i kryptominingaktiviteter.
2. **Upptäck Cryptomining-aktiviteter.** (avger varningar närhelst en kryptominingaktivitet upptäcks och kräver användarinmatning för att bestämma lämplig åtgärd)

Det här läget är lämpligt för användare som är aktivt involverade i sina egna kryptominingaktiviteter men vill övervaka och kontrollera eventuella obehöriga försök.

Hantera undantag

Undantag kan anges för applikationer, med den extra möjligheten att definiera specifika kommandorader. Undantag kan dock också fastställas utan att man behöver tillhandahålla sådana detaljerade parametrar, vilket ger en balans mellan anpassning och enkelhet.

Så här lägger du till ett undantag:

1. Klick**Skydd**på menyn till vänster i Bitdefender-gränssnittet.
2. I den**Kryptomineringsskydd**rutan, klicka**inställningar**.
3. Klicka på**Hantera undantag**alternativ.
4. Klicka sedan på**Lägg till ett undantag**knapp.
5. Ett nytt fönster öppnas. Du kan manuellt utesluta applikationer, URL:er och IP-adresser.
6. Klicka slutligen**Spara**. Den nya regeln läggs till i undantagslistan för Cryptomining Protection.

> **Notera**
> För att ta bort ett undantag klickar du bara på papperskorgen bredvid.

3.2.11. Antispårare

Många webbplatser du besöker använder spårare för att samla in information om ditt beteende, antingen för att dela den med tredjepartsföretag eller för att visa annonser som är mer relevanta för dig. Härmed tjänar webbplatsägare pengar för att kunna ge dig innehåll gratis eller fortsätta att fungera. Förutom att samla in information kan spårare sakta ner din surfupplevelse eller slösa bort din bandbredd.

Med Bitdefender Anti-tracker-tillägget aktiverat i din webbläsare undviker du att bli spårad så att dina data förblir privata medan du surfar online och du påskyndar den tid som webbplatser behöver laddas.

Bitdefender-tillägget är kompatibelt med följande webbläsare:

- Internet Explorer

- Google Chrome
- Mozilla Firefox

De spårare vi upptäcker är grupperade i följande kategorier:

- **Reklam** - används för att analysera webbplatstrafik, användarbeteende eller besökarnas trafikmönster.
- **Kundinteraktion** - används för att mäta användarinteraktion med olika inmatningsformer som chatt eller support.
- **Grundläggande** - används för att övervaka viktiga webbsidors funktioner.
- **Webbplatsanalys** - används för att samla in data om webbsidaanvändning.
- **Sociala media** - används för att övervaka social publik, aktivitet och användarengagemang med olika sociala medieplattformar.

Anti-tracker gränssnitt

När Bitdefender Anti-tracker-tillägget är aktiverat, visas bredvid sökfältet i din webbläsare. Varje gång du besöker en webbplats kan en räknare märkas på ikonen som hänvisar till de upptäckta och blockerade spårarna. För att se mer information om de blockerade spårarna, klicka på ikonen för att öppna gränssnittet. Förutom antalet blockerade spårare kan du se hur lång tid det tar för sidan att ladda och kategorierna som de upptäckta spårarna tillhör. För att se listan över webbplatser som spårar, klicka på önskad kategori.

För att inaktivera Bitdefender från att blockera spårare på webbplatsen du för närvarande besöker, klicka **Pausa skyddet på denna webbplats**. Den här inställningen gäller bara så länge du har webbplatsen öppen och kommer att återställas till det ursprungliga tillståndet när du stänger webbplatsen.

För att tillåta spårare från en specifik kategori att övervaka din aktivitet, klicka på önskad aktivitet och klicka sedan på motsvarande knapp. Om du ändrar dig, klicka på samma knapp en gång till.

Stänger av Bitdefender Anti-tracker

Så här stänger du av Bitdefender Anti-tracker:

- Från din webbläsare:
  1. Öppna din webbläsare.
  2. Klicka på ikonen bredvid adressfältet i din webbläsare.
  3. Klicka på ikonen i det övre högra hörnet.
  4. Använd motsvarande strömbrytare för att stänga av. Bitdefender-ikonen blir grå.
- Från Bitdefender-gränssnittet:
  1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **ANTI-TRACKER** rutan, klicka **inställningar**.
  3. Bredvid webbläsaren som du vill inaktivera tillägget för, stäng av motsvarande strömbrytare.

Tillåter att en webbplats spåras

Om du vill bli spårad när du besöker en viss webbplats kan du lägga till dess adress till undantag enligt följande:

1. Öppna din webbläsare.
2. Klicka på ikonen bredvid sökfältet.
3. Klicka på ikonen i det övre högra hörnet.
4. Om du är på webbplatsen du vill lägga till undantag klickar du på **Lägg till aktuell webbplats till listan**.
   Om du vill lägga till en annan webbplats anger du dess adress i motsvarande fält och klickar sedan .

3.2.12. Safepay-säkerhet för onlinetransaktioner

Datorn blir snabbt det främsta verktyget för shopping och bank. Att betala räkningar, överföra pengar, köpa i stort sett allt du kan tänka dig har aldrig varit snabbare eller enklare.

Det handlar om att skicka personlig information, konto- och kreditkortsdata, lösenord och andra typer av privat information över internet, med andra ord exakt den typ av informationsflöde som cyberbrottslingar är mycket intresserade av att utnyttja. Hackare är

obevekliga i sina ansträngningar att stjäla denna information, så du kan aldrig vara för försiktig med att säkra onlinetransaktioner.

Bitdefender Safepay™ är först och främst en skyddad webbläsare, en förseglad miljö som är utformad för att hålla din onlinebank, e-shopping och alla andra typer av onlinetransaktioner privata och säkra.

Bitdefender Safepay™ erbjuder följande funktioner:

- Det blockerar åtkomst till ditt skrivbord och alla försök att ta ögonblicksbilder av din skärm.
- Den levereras med ett virtuellt tangentbord som, när det används, gör det omöjligt för hackare att läsa dina tangenttryckningar.
- Det är helt oberoende av dina andra webbläsare.
- Den kommer med inbyggt hotspot-skydd som kan användas när din enhet är ansluten till osäkra Wi-fi-nätverk.
- Den stöder bokmärken och låter dig navigera mellan dina favoritbanker/shoppingsajter.
- Det är inte begränsat till bank och e-shopping. Alla webbplatser kan öppnas i Bitdefender Safepay™.

Använder Bitdefender Safepay™

Som standard upptäcker Bitdefender när du navigerar till en bankwebbplats eller onlinebutik i valfri webbläsare på din enhet och uppmanar dig att starta den i Bitdefender Safepay™.

För att komma åt huvudgränssnittet för Bitdefender Safepay™, använd en av följande metoder:

- Från Bitdefender-gränssnitt:
  1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **SAFEPAY** rutan, klicka **inställningar**.
  3. I den **Safepay** fönster, klicka **Starta Safepay**.
- Från Windows:
  - I **Windows 7**:
    1. Klick **Start** och gå till **Alla program**.
    2. Klick **Bitdefender**.

3. Klick **Bitdefender Safepay™**.

- I **Windows 8** och **Windows 8.1**:
  Leta upp Bitdefender Safepay™ från startskärmen i Windows (du kan till exempel börja skriva "Bitdefender Safepay™" direkt på startskärmen) och klicka sedan på ikonen.
- I **Windows 10** och **Windows 11**:
  Skriv "Bitdefender Safepay™" i sökrutan från aktivitetsfältet och klicka på dess ikon.

Om du är van vid webbläsare har du inga problem med att använda Bitdefender Safepay™ - det ser ut och beter sig som en vanlig webbläsare:

- ange webbadresser du vill gå till i adressfältet.
- lägg till flikar för att besöka flera webbplatser i Bitdefender Safepay™-fönstret genom att klicka ⊞ .
- navigera fram och tillbaka och uppdatera sidor med hjälp av ← → ↻ respektive.
- komma åt Bitdefender Safepay™ inställningar genom att klicka och välja **inställningar**.
- hantera din bokmärken genom att klicka ☆ bredvid adressfältet.
- öppna det virtuella tangentbordet genom att klicka ⌨ .
- öka eller minska webbläsarens storlek genom att trycka samtidigt **Ctrl** och den **+/-** knapparna på det numeriska tangentbordet.
- visa information om din Bitdefender-produkt genom att klicka ⋯ och välja **Handla om**.
- skriv ut viktig information genom att klicka ⋯ och välja **Skriva ut**.

> **Notera**
> För att växla mellan Bitdefender Safepay™ och Windows skrivbord, tryck på **Alt+Tab** eller klicka på **Växla till skrivbordet** alternativet på den övre vänstra sidan av fönstret.

Konfigurera inställningar

Klick ⋯ och välj **inställningar** för att konfigurera Bitdefender Safepay™:

Tillämpa Bitdefender Safepay-regler för tillgängliga domäner

Webbplatserna du har lagt till Bokmärken med **Öppna automatiskt i Safepay** alternativet aktiverat visas här. Om du vill sluta automatiskt öppna en webbplats från listan med Bitdefender Safepay™, klicka på × bredvid den önskade posten från **Avlägsna** kolumn.

Blockera popup-fönster

Du kan välja att blockera popup-fönster genom att klicka på motsvarande knapp.

Du kan också skapa en lista över webbplatser att tillåta popup-fönster från. Listan bör endast innehålla webbplatser som du litar på till fullo.

För att lägga till en webbplats i listan, ange dess adress i motsvarande fält och klicka **LÄGG TILL DOMÄN**.

För att ta bort en webbplats från listan, välj X som motsvarar önskad post.

Hantera plugins

Du kan välja om du vill aktivera eller inaktivera specifika plugins i Bitdefender Safepay™.

Hantera certifikat

Du kan importera certifikat från ditt system till ett certifikatlager.

Klick **IMPORTERA** och följ guiden för att använda certifikaten i Bitdefender Safepay™.

Använd virtuellt tangentbord

Det virtuella tangentbordet visas automatiskt när ett lösenordsfält väljs.

Använd motsvarande omkopplare för att aktivera eller inaktivera funktionen.

Utskriftsbekräftelse

Aktivera det här alternativet om du vill ge din bekräftelse innan utskriftsprocessen startar.

Hantera bokmärken

Om du inaktiverade den automatiska upptäckten av vissa eller alla webbplatser, eller Bitdefender helt enkelt inte upptäcker vissa webbplatser, kan du lägga till bokmärken till Bitdefender Safepay™ så att du enkelt kan starta favoritwebbplatser i framtiden.

Följ dessa steg för att lägga till en URL till Bitdefender Safepay™-bokmärken:

1. Klick ⋯ och välj **Bokmärken** för att öppna sidan Bokmärken.

   > **Notera**
   > Bokmärkessidan öppnas som standard när du startar Bitdefender Safepay™.

2. Klicka på **+** för att lägga till ett nytt bokmärke.
3. Skriv in webbadressen och titeln på bokmärket och klicka sedan **SKAPA**. Kolla **Öppna automatiskt i Safepay** alternativet om du vill att den bokmärkta sidan ska öppnas med Bitdefender Safepay™ varje gång du kommer åt den. URL:en läggs också till i listan Domäner på inställningssidan.

Stänger av Safepay-aviseringar

När en banksajt upptäcks ställs Bitdefender-produkten in för att meddela dig via ett popup-fönster.

Så här stänger du av Safepay-aviseringarna:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SAFEPAY** rutan, klicka **inställningar**.
3. I den **inställningar** fönster, stäng av strömbrytaren bredvid **Safepay-aviseringar**.

3.2.13. Stöldskydd

Stöld av bärbara datorer är ett stort problem som påverkar både individer och organisationer. Till och med mer än att förlora själva hårdvaran, kan data som förloras med den orsaka betydande skada, både ekonomiskt och känslomässigt.

Ändå är det få som vidtar de rätta åtgärderna för att säkra sina viktiga personliga, affärsmässiga och finansiella uppgifter i händelse av stöld eller förlust.

Bitdefender Anti-Theft hjälper dig att vara bättre förberedd för en sådan händelse genom att tillåta dig att fjärrlokalisera eller låsa din bärbara dator och till och med radera all data från den, om du någonsin skulle skiljas från din bärbara dator mot din vilja.

För att använda stöldskyddsfunktionerna måste följande förutsättningar vara uppfyllda:

- Kommandona kan endast skickas från Bitdefender-kontot.
- Den bärbara datorn måste vara ansluten till internet för att ta emot kommandon.

Stöldskyddsfunktioner fungerar på följande sätt:

Lokalisera

Visa enhetens plats på Google Maps.

Platsens noggrannhet beror på hur Bitdefender kan bestämma den. Platsen bestäms inom tiotals meter om Wi-Fi är aktiverat på din bärbara dator och det finns trådlösa nätverk inom dess räckvidd.

Om den bärbara datorn är ansluten till ett trådbundet LAN utan någon tillgänglig Wi-Fi-baserad plats kommer platsen att bestämmas baserat på IP-adressen, som är betydligt mindre exakt.

Varna

Skicka en fjärrvarning på enheten.

Funktionen är endast tillgänglig på mobila enheter.

Låsa

Lås din bärbara dator och ange en 4-siffrig PIN-kod för att låsa upp den. När du skickar **Låsa** kommandot startar systemet om och inloggning till Windows är endast möjligt efter att du har angett PIN-koden du har angett.

Om du vill att Bitdefender ska ta bilder av den som försöker få tillgång till din bärbara dator, markera motsvarande kryssruta. De tagna bilderna är tagna med den främre kameran och visas tillsammans med tidsstämpeln i Anti-Theft-instrumentpanelen. Endast de två senaste bilderna kommer att sparas.

Denna åtgärd är endast tillgänglig för bärbara datorer som har en främre kamera.

Torka

Ta bort all data från ditt system. När du skickar **Torka** kommandot, startar den bärbara datorn om och data på alla hårddiskpartitioner raderas.

Visa IP

Visar den senaste IP-adressen för den valda enheten. Klick **VISA IP** för att göra det synligt.

Stöldskydd aktiveras efter installationen och kan endast nås via ditt Bitdefender-konto från vilken enhet som helst som är ansluten till internet, var som helst.

Använda stöldskyddsfunktioner

För att komma åt stöldskyddsfunktionerna, använd en av följande möjligheter:

- Från Bitdefender huvudgränssnitt:
  1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. Klick **GÅ TILL CENTRAL**.
     Du omdirigeras till Bitdefender Central-sidan. Se till att du är inloggad med dina referenser.
  3. I Bitdefender Central-fönstret som öppnas, klicka på önskat enhetskort och välj sedan **Anti-stöld**.

- På alla enheter med internetåtkomst:
  1. Öppna en webbläsare och gå till: https://central.bitdefender.com.
  2. Logga in på ditt Bitdefender-konto med din e-postadress och ditt lösenord.
  3. Välj **Mina enheter** panel.
  4. Klicka på önskat enhetskort och välj sedan **Anti-stöld**.
  5. Välj den funktion du vill använda:
     Lokalisera - visa enhetens plats på Google Maps.
     Visa IP - visa den senaste IP-adressen för din enhet.
     Varna - skicka en varning på enheten.
     Låsa - lås din bärbara dator och ställ in en PIN-kod för att låsa upp den.
     Torka - radera all data från din bärbara dator.

     Viktig
     När du har torkat en enhet upphör alla stöldskyddsfunktioner att fungera.

3.3. Verktyg

3.3.1. Profiler

Dagliga jobbaktiviteter, titta på film eller spela spel kan göra att systemet blir långsammare, särskilt om de körs samtidigt med Windows uppdateringsprocesser och underhållsuppgifter. Med Bitdefender kan du nu välja och använda din föredragna profil, vilket gör systemjusteringar lämpade för att öka prestandan för specifika installerade appar.

Bitdefender tillhandahåller följande profiler:

- Arbetsprofil
- Filmprofil
- Spelprofil
- Offentlig Wi-Fi-profil
- Batterilägesprofil

Om du bestämmer dig för att inte använda **Profiler**, en standardprofil som kallas **Standard** är aktiverat och det ger ingen optimering till ditt system.

Beroende på din aktivitet tillämpas följande produktinställningar när jobb-, film- eller spelprofiler är aktiverade:

- Alla Bitdefender-varningar och popup-fönster är inaktiverade.
- Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Antispam-funktionen är aktiverad.
- Sökrådgivare är ur funktion.
- Aviseringar om specialerbjudanden är inaktiverade.

Beroende på din aktivitet tillämpas följande systeminställningar när jobb-, film- eller spelprofiler är aktiverade:

- Windows Automatiska uppdateringar skjuts upp.
- Windows-varningar och popup-fönster är inaktiverade.
- Onödiga bakgrundsprogram stängs av.
- Visuella effekter justeras för bästa prestanda.

- Underhållsuppgifter skjuts upp.
- Inställningarna för energischemat justeras.

När du kör i den offentliga Wi-Fi-profilen, Bitdefender Ultimate Small Business Security är inställd på att automatiskt utföra följande programinställningar:

- Advanced Threat Defense är aktiverat
- Bitdefender-brandväggen är påslagen och följande inställningar tillämpas på din trådlösa adapter:
  - Stealth-läge - PÅ
  - Nätverkstyp - Offentlig
- Följande inställningar från Online Threat Prevention är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägerier
  - Skydd mot nätfiske

Arbetsprofil

Att köra flera uppgifter på jobbet, som att skicka e-post, ha en videokommunikation med dina avlägsna kollegor eller arbeta med designappar kan påverka din systemprestanda. Arbetsprofilen har utformats för att hjälpa dig att förbättra din arbetseffektivitet genom att stänga av några av dina bakgrundstjänster och underhållsuppgifter.

Konfigurerar arbetsprofil

Så här konfigurerar du de åtgärder som ska vidtas i arbetsprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** knappen från området Arbetsprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på jobbappar
   - Optimera produktinställningar för arbetsprofilen

- ❍ Skjut upp bakgrundsprogram och underhållsuppgifter
- ❍ Skjut upp Windows automatiska uppdateringar

5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till appar manuellt i listan med arbetsprofiler

Om Bitdefender inte automatiskt går in i arbetsprofilen när du startar en viss jobbapp, kan du lägga till appen manuellt i **Lista över arbetsansökningar**.

Så här lägger du till appar manuellt till listan över appar för arbete i arbetsprofil:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** knappen från området Arbetsprofil.
4. I den **Arbetsprofilinställningar** fönster, klicka **Applikationslista**.
5. Klick **LÄGG TILL**.
   Ett nytt fönster visas. Bläddra till appens körbara fil, välj den och klicka **OK** för att lägga till den i listan.

Filmprofil

Att visa videoinnehåll av hög kvalitet, t.ex. högupplösta filmer, kräver betydande systemresurser. Movie Profile justerar system- och produktinställningar så att du kan njuta av en oavbruten och sömlös filmupplevelse.

Konfigurera filmprofil

Så här konfigurerar du de åtgärder som ska vidtas i filmprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** från filmprofilområdet.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - ❍ Öka prestandan på videospelare

- Optimera produktinställningar för filmprofil
- Skjut upp bakgrundsprogram och underhållsuppgifter
- Skjut upp Windows automatiska uppdateringar
- Justera energischemainställningar för filmer

5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till videospelare manuellt till filmprofillistan

Om Bitdefender inte automatiskt går in i filmprofilen när du startar en viss videospelarapp, kan du lägga till appen manuellt i **Filmapplikationslista**.

Så här lägger du till videospelare manuellt i filmprogramlistan i filmprofil:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **KONFIGURERA** från filmprofilområdet.
4. I den **Filmprofilinställningar** fönster, klicka **Spelarlista**.
5. Klick **LÄGG TILL**.
   Ett nytt fönster visas. Bläddra till appens körbara fil, välj den och klicka **OK** för att lägga till den i listan.

Spelprofil

Att njuta av en oavbruten spelupplevelse handlar om att minska systembelastningen och minska nedgångarna. Genom att använda beteendeheuristik tillsammans med en lista över kända spel kan Bitdefender automatiskt upptäcka pågående spel och optimera dina systemresurser så att du kan njuta av din spelpaus.

Konfigurera spelprofil

Så här konfigurerar du de åtgärder som ska vidtas i spelprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **Konfigurera** från spelprofilområdet.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:

- Öka prestanda på spel
- Optimera produktinställningar för spelprofilen
- Skjut upp bakgrundsprogram och underhållsuppgifter
- Skjut upp Windows automatiska uppdateringar
- Justera energischemainställningar för spel

5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Lägger till spel manuellt i spellistan

Om Bitdefender inte automatiskt går in i spelprofilen när du startar ett visst spel eller en viss app, kan du lägga till appen manuellt i **Lista över spelapplikationer**.

Så här lägger du till spel manuellt i spelapplikationslistan i spelprofil:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **Konfigurera** från spelprofilområdet.
4. I den **Spelprofilinställningar** fönster, klicka **Spellista**.
5. Klick **LÄGG TILL**.
   Ett nytt fönster visas. Bläddra till spelets körbara fil, välj den och klicka **OK** för att lägga till den i listan.

Offentlig Wi-Fi-profil

Att skicka e-postmeddelanden, skriva känsliga uppgifter eller handla online medan du är ansluten till osäkra trådlösa nätverk kan utsätta dina personuppgifter för risker. Public Wi-Fi Profile justerar produktinställningar för att ge dig möjlighet att göra betalningar online och använda känslig information i en skyddad miljö.

Konfigurerar offentlig Wi-Fi-profil

Så här konfigurerar du Bitdefender att tillämpa produktinställningar när du är ansluten till ett osäkert trådlöst nätverk:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.

3. Klicka på **KONFIGURERA** knappen från området Public Wi-Fi Profile.
4. Låt **Justerar produktinställningar för att öka skyddet när du är ansluten till ett osäkert offentligt Wi-Fi-nätverk** kryssrutan aktiverad.
5. Klick **Spara**.

Batterilägesprofil

Batterilägesprofilen är speciellt utformad för användare av bärbara datorer och surfplattor. Syftet är att minimera både systemets och Bitdefender-effekten på strömförbrukningen när batteriladdningsnivån är lägre än standarden eller den du väljer.

Konfigurera batterilägesprofil

Så här konfigurerar du batterilägesprofilen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Klicka på **Konfigurera** knappen från området Batterilägesprofil.
4. Välj de systemjusteringar som ska tillämpas genom att markera följande alternativ:
   - Optimera produktinställningar för batteriläge.
   - Skjut upp bakgrundsprogram och underhållsuppgifter.
   - Skjut upp Windows automatiska uppdateringar.
   - Justera energischemainställningar för batteriläge.
   - Inaktivera externa enheter och nätverksportar.
5. Klick **SPARA** för att spara ändringarna och stänga fönstret.

Skriv ett giltigt värde i rutan eller välj ett med upp- och nedpiltangenterna för att ange när systemet ska börja arbeta i batteriläge. Som standard aktiveras läget när batteriladdningsnivån sjunker under 30 %.

Följande produktinställningar tillämpas när Bitdefender arbetar i batterilägesprofilen:

- Bitdefender Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.

Bitdefender upptäcker när din bärbara dator har bytt till batteridrift och baserat på batteriladdningsnivån går den automatiskt in i batteriläge. På samma sätt lämnar Bitdefender automatiskt batteriläget när den upptäcker att den bärbara datorn inte längre körs på batteri.

Realtidsoptimering

Bitdefender Realtidsoptimering är ett plugin som förbättrar din systemprestanda tyst, i bakgrunden, och ser till att du inte blir avbruten medan du är i ett profilläge. Beroende på CPU-belastningen övervakar plugin alla processer, med fokus på de som tar upp en högre belastning, för att anpassa dem efter dina behov.

Så här aktiverar eller inaktiverar du realtidsoptimering:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Profiler** fliken, klicka **inställningar**.
3. Rulla nedåt tills du ser alternativet Realtidsoptimering och använd sedan motsvarande knapp för att slå på eller av det.

3.3.2. OneClick Optimizer

Problem som hårddiskfel, överblivna registerfiler och webbläsarhistorik kan sakta ner ditt arbete, vilket kan bli tjatigt för dig. Alla dessa kan nu fixas med ett enda klick på en knapp.

OneClick Optimizer låter dig identifiera och ta bort värdelösa filer genom att köra flera rengöringsuppgifter samtidigt.

Så här startar du OneClick Optimizer-processen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Klicka på **Optimera** knapp.
   a. **Analyserar**
   Vänta tills Bitdefender slutför sökningen efter systemproblem.
   - Diskrensning - identifierar onödiga filer och mappar.
   - Registry Cleanup - identifierar ogiltiga eller inaktuella referenser i Windows-registret.
   - Privacy Cleanup - identifierar tillfälliga internetfiler och cookies, webbläsarcache och historik.

Antalet hittade problem visas. Klicka på länken Visa detaljer för att granska dem innan du fortsätter med rengöringsprocessen. Klicka på Optimera för att fortsätta.

b. **Optimerande**
Vänta på att Bitdefender har slutfört optimeringen av ditt system.

c. **frågor**
Det är här du kan se operationsresultatet.
Om du vill ha omfattande information om optimeringsprocessen, klicka på **Se detaljerad rapport** knapp.

3.3.3. Dataskydd

Raderar filer permanent

När du tar bort en fil kan den inte längre nås på vanliga sätt. Filen fortsätter dock att lagras på hårddisken tills den skrivs över när nya filer kopieras.

Bitdefender File Shredder hjälper dig att permanent radera data genom att fysiskt ta bort den från din hårddisk.

Du kan snabbt strimla filer eller mappar från din enhet med Windows sammanhangsberoende meny genom att följa dessa steg:

1. Högerklicka på filen eller mappen som du vill ta bort permanent.
2. Välj **Bitdefender > Filförstörare** i snabbmenyn som visas.
3. Klick **Ta bort permanent**och bekräfta sedan att du vill fortsätta med processen.
Vänta tills Bitdefender har avslutat fragmenteringen av filerna.
4. Resultaten visas. Klick **Avsluta** för att avsluta guiden.

Alternativt kan du strimla filer från Bitdefender-gränssnittet, enligt följande:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Dataskydd** rutan, klicka **Pappers strimlare**.
3. Följ guiden File Shredder:
   a. Klicka på **Lägg till mappar** för att lägga till de filer eller mappar som du vill ska tas bort permanent.

Alternativt kan du dra dessa filer eller mappar till det här fönstret.

b. Klick **ta bort permanent**och bekräfta sedan att du vill fortsätta med processen.
Vänta tills Bitdefender har avslutat fragmenteringen av filerna.

c. **Resultatsammanfattning**
Resultaten visas. Klick **Avsluta** för att avsluta guiden.

3.4. Hur

3.4.1. Installation

Hur installerar jag Bitdefender på en andra enhet?

Om prenumerationen du har köpt omfattar mer än en enhet kan du använda ditt Bitdefender-konto för att aktivera en andra dator.

Så här installerar du Bitdefender på en andra enhet:

1. Klick **Installera på en annan enhet** i det nedre vänstra hörnet av Bitdefender-gränssnitt.
Ett nytt fönster visas på skärmen.
2. Klick **DELA NEDLADDNINGSLÄNK**.
3. Följ instruktionerna på skärmen för att installera Bitdefender.

Den nya enheten som du har installerat Bitdefender-produkten på kommer att visas i Bitdefender Central-instrumentpanelen.

Hur kan jag installera om Bitdefender?

Typiska situationer när du skulle behöva installera om Bitdefender inkluderar följande:

- du har installerat om operativsystemet.
- du vill åtgärda problem som kan ha orsakat nedgångar och krascher.
- din Bitdefender-produkt startar inte eller fungerar inte korrekt.

I händelse av att en av de nämnda situationerna är ditt fall, följ dessa steg:

- I **Windows 7**:
  1. Klick **Start** och gå till **Alla program**.

2. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
3. Klick **INSTALLERA OM** i fönstret som visas.
4. Du måste starta om enheten för att slutföra processen.

- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera** ett program eller **Program och funktioner**.
  3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  4. Klick **INSTALLERA OM** i fönstret som visas.
  5. Du måste starta om enheten för att slutföra processen.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, Klicka sedan **inställningar**.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar och funktioner**.
  3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **INSTALLERA OM**.
  6. Du måste starta om enheten för att slutföra processen.

> **Notera**
> Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

Var kan jag ladda ner min Bitdefender-produkt från?

Du kan installera Bitdefender från installationsskivan, eller använda webbinstallationsprogrammet som du kan ladda ner på din enhet från Bitdefender Central-plattformen.

> **Notera**
> Innan du kör satsen, rekommenderas det att ta bort alla säkerhetslösningar som är installerade på ditt system. När du använder mer än en säkerhetslösning på samma enhet blir systemet instabilt.

För att installera Bitdefender från Bitdefender Central:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
3. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
   - **Skydda andra enheter**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     Klick **SKICKA NEDLADDNINGSLÄNK**. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
     På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.
4. Kör Bitdefender-produkten du har laddat ner.

Hur använder jag min Bitdefender-prenumeration efter en Windows-uppgradering?

Denna situation uppstår när du uppgraderar ditt operativsystem och du vill fortsätta använda ditt Bitdefender-abonnemang.

Om du använder en tidigare Bitdefender-version kan du uppgradera, kostnadsfritt, till den senaste Bitdefender, enligt följande:

- Från en tidigare version av Bitdefender Antivirus till den senaste tillgängliga Bitdefender Antivirus.

- Från en tidigare version av Bitdefender Internet Security till den senaste tillgängliga Bitdefender Internet Security.
- Från en tidigare version av Bitdefender Total Security till den senaste tillgängliga Bitdefender Total Security.

Det finns två fall som kan dyka upp:

- Du har uppgraderat operativsystemet med Windows Update och du märker att Bitdefender inte längre fungerar.
  I det här fallet måste du installera om produkten genom att följa dessa steg:
  - I **Windows 7**:
    1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
    2. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
    3. Klick **INSTALLERA OM** i fönstret som visas.
    4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
       Öppna gränssnittet för din nya installerade Bitdefender-produkt för att få tillgång till dess funktioner.
  - I **Windows 8** och **Windows 8.1**:
    1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
    2. Klick **Avinstallera ett program** eller **Program och funktioner**.
    3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
    4. Klick **INSTALLERA OM** i fönstret som visas.
    5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
       Öppna gränssnittet för din nya installerade Bitdefender-produkt för att få tillgång till dess funktioner.
  - I **Windows 10** och **Windows 11**:

1. Klick **Start**, Klicka sedan **inställningar**.
2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar**.
3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
4. Klick **Avinstallera** igen för att bekräfta ditt val.
5. Klick **INSTALLERA OM** i fönstret som visas.
6. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
   Öppna gränssnittet för din nya installerade Bitdefender-produkt för att få tillgång till dess funktioner.

> **Notera**
> Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

- Du ändrade ditt system och du vill fortsätta använda Bitdefender-skyddet. Därför måste du installera om produkten med den senaste versionen.
  För att lösa denna situation:

  1. Ladda ner installationsfilen:
     a. Tillgång Bitdefender Central.
     b. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
     c. Välj ett av de två tillgängliga alternativen:
        - **Skydda den här enheten**
          Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
        - **Skydda en annan enhet**
          Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
          Klick **SKICKA NEDLADDNINGSLÄNK**. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast

är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.

På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.

2. Kör Bitdefender-produkten du har laddat ner.

För mer information om Bitdefender installationsprocessen, se Installera din Bitdefender-produkt (sida 11).

Hur kan jag uppgradera till den senaste Bitdefender-versionen?

Från och med nu är uppgraderingen till den senaste versionen möjlig utan att följa den manuella proceduren för avinstallation och ominstallation. Mer exakt, den nya produkten inklusive nya funktioner och större produktförbättringar levereras via produktuppdatering och om du redan har ett aktivt Bitdefender-abonnemang aktiveras produkten automatiskt.

Om du använder 2020-versionen kan du uppgradera till den senaste versionen genom att följa dessa steg:

1. Klick **STARTA OM NU** i meddelandet du får med uppgraderingsinformationen. Om du missar det, gå till Aviseringar peka på den senaste uppdateringen och klicka sedan på **STARTA OM NU** knapp. Vänta tills enheten startar om.

   De **Vad är nytt** fönster med information om de förbättrade och nya funktionerna visas.

2. Klicka på **Läs mer** länkar som ska omdirigeras till vår dedikerade sida med mer information och användbara artiklar.

3. Stäng **Vad är nytt** fönster för att komma åt gränssnittet för den nya installerade versionen.

Användare som vill uppgradera gratis från Bitdefender 2016 eller en lägre version till den senaste Bitdefender-versionen måste ta bort sin nuvarande version från kontrollpanelen och sedan ladda ner den senaste installationsfilen från Bitdefender-webbplatsen på följande adress: https://www.bitdefender.com/Downloads/. Aktiveringen är endast möjlig med ett giltigt abonnemang

3.4.2. Bitdefender Central

Hur loggar jag in på Bitdefender-kontot med ett annat konto?

Du har skapat ett nytt Bitdefender-konto och du vill använda det från och med nu.

För att lyckas logga in med ett annat Bitdefender-konto:

1. Klicka på ditt kontonamn i den övre delen av Bitdefender-gränssnitt.
2. Klick **Byt konto** i det övre högra hörnet av skärmen för att ändra kontot som är kopplat till enheten.
3. Skriv in e-postadressen i motsvarande fält och klicka sedan **NÄSTA**.
4. Skriv ditt lösenord och klicka sedan **LOGGA IN**.

> **Notera**
> Bitdefender-produkten från din enhet ändras automatiskt enligt prenumerationen som är kopplad till det nya Bitdefender-kontot. Om det inte finns något tillgängligt abonnemang kopplat till det nya Bitdefender-kontot, eller om du vill överföra det från det tidigare kontot, kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Hur stänger jag av Bitdefender Central hjälpmeddelanden?

För att hjälpa dig förstå vad varje alternativ i Bitdefender Central är användbart för, visas hjälpmeddelanden i instrumentpanelen.

Om du vill sluta se den här typen av meddelanden:

1. Tillgång Bitdefender Central.
2. Klicka på ikonen i den övre högra sidan av skärmen.
3. Klick **Mitt konto** i bildmenyn.
4. Klick **inställningar** i bildmenyn.
5. Inaktivera Turn **på/av hjälpmeddelanden** alternativ.

Jag har glömt lösenordet som jag angav för mitt Bitdefender-konto. Hur återställer jag den?

Det finns två möjligheter att ställa in ett nytt lösenord för ditt Bitdefender-konto:

- Från Bitdefender-gränssnitt:
  1. Klick **Mitt konto** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. Klick **Byt konto** i det övre högra hörnet av skärmen.
     Ett nytt fönster visas.
  3. Skriv din e-postadress och klicka **NÄSTA**.
     Ett nytt fönster visas.
  4. Klick **Glömt ditt lösenord?**.
  5. Klick **NÄSTA**.
  6. Kontrollera ditt e-postkonto, skriv in säkerhetskoden du har fått och klicka sedan **NÄSTA**.
     Alternativt kan du klicka **ändra lösenord** i e-postmeddelandet som vi skickade till dig.
  7. Skriv det nya lösenordet du vill ställa in och skriv det sedan igen. Klick **SPARA**.

- Från din webbläsare:
  1. Gå till: https://central.bitdefender.com.
  2. Klick **LOGGA IN**.
  3. Skriv din e-postadress och klicka sedan **NÄSTA**.
  4. Klick **Glömt ditt lösenord?**.
  5. Klick **NÄSTA**.
  6. Kontrollera ditt e-postkonto och följ instruktionerna för att ställa in ett nytt lösenord för ditt Bitdefender-konto.

För att komma åt ditt Bitdefender-konto från och med nu, skriv in din e-postadress och det nya lösenordet du just har angett.

Hur kan jag hantera inloggningssessionerna som är kopplade till mitt Bitdefender-konto?

I ditt Bitdefender-konto har du möjlighet att se de senaste inaktiva och aktiva inloggningssessionerna som körs på enheter som är kopplade till ditt konto. Dessutom kan du logga ut på distans genom att följa dessa steg:

1. Tillgång Bitdefender Central.
2. Klicka på ikonen i den övre högra sidan av skärmen.
3. Klick **Sessioner** i bildmenyn.
4. I den **Aktiva Sessioner** område, välj **LOGGA UT** alternativet bredvid den enhet du vill avsluta inloggningssessionen.

3.4.3. Skanna med Bitdefender

Hur skannar jag en fil eller en mapp?

Det enklaste sättet att skanna en fil eller mapp är att högerklicka på objektet du vill skanna, peka på Bitdefender och välja **Skanna med Bitdefender** från menyn.

För att slutföra skanningen, följ guiden Antivirus Scan. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer.

Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem.

Typiska situationer när du använder den här skanningsmetoden inkluderar följande:

- Du misstänker att en specifik fil eller mapp är infekterad.
- När du laddar ner filer från internet som du tror kan vara farliga.
- Skanna en nätverksresurs innan du kopierar filer till din enhet.

Hur skannar jag mitt system

För att utföra en fullständig genomsökning av systemet:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klicka på **Kör Scan** knappen bredvid **Genomsökning av systemet**.
4. Följ systemsökningsguiden för att slutföra skanningen. Bitdefender kommer automatiskt att vidta de rekommenderade åtgärderna på upptäckta filer.
   Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem. För mer information, se.

Hur schemalägger jag en skanning?

Du kan ställa in din Bitdefender-produkt så att den börjar skanna viktiga systemplatser när du inte är på framsidan av enheten.

Så här schemalägger du en skanning:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klick ··· bredvid skanningstypen som du vill schemalägga, System Scan eller Quick Scan, i den nedre delen av gränssnittet, välj sedan **Redigera**.
   Alternativt kan du skapa en skanningstyp som passar dina behov genom att klicka **+Skapa Scan** bredvid **Hantera skanningar**.
4. Anpassa skanningen efter dina behov och klicka sedan **Nästa**.
5. Markera rutan bredvid **Välj när du vill schemalägga denna uppgift**.
   Välj ett av motsvarande alternativ för att ställa in ett schema:
   - ❍ Vid systemstart
   - ❍ Dagligen
   - ❍ Varje vecka
   - ❍ En gång i månaden

   Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.

Om du väljer att skapa en ny anpassad skanning, **Skanningsuppgift** fönstret visas. Härifrån kan du välja de platser du vill ska skannas.

Hur skapar jag en anpassad skanningsuppgift?

Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen, konfigurera och kör en anpassad skanningsuppgift.

Gör så här för att skapa en anpassad skanningsuppgift:

1. I den **ANTIVIRUS** rutan, klicka **Öppen**.
2. Klick **+Skapa Scan** bredvid **Hantera skanningar**.

3. I uppgiftsnamnsfältet anger du ett namn för skanningen, väljer de platser du vill ska skannas och klickar sedan på **NÄSTA**.
4. Konfigurera dessa allmänna alternativ:
   - **Skanna endast applikationer**. Du kan ställa in Bitdefender för att endast skanna appar som är tillgängliga.
   - **Skanningsuppgiftsprioritet**. Du kan välja vilken inverkan en skanningsprocess ska ha på systemets prestanda.
     - Auto - Prioriteten för skanningsprocessen beror på systemaktiviteten. För att säkerställa att skanningsprocessen inte kommer att påverka systemaktiviteten kommer Bitdefender att bestämma om skanningsprocessen ska köras med hög eller låg prioritet.
     - Hög - Prioriteten för skanningsprocessen kommer att vara hög. Genom att välja det här alternativet låter du andra program köras långsammare och minskar tiden som krävs för att skanningsprocessen ska slutföras.
     - Låg - Prioriteten för skanningsprocessen kommer att vara låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka den tid som krävs för att skanningsprocessen ska slutföras.
   - **Åtgärder efter skanning**. Välj vilken åtgärd Bitdefender ska vidta om inga hot hittas:
     - Visa sammanfattningsfönster
     - Stäng av enheten
     - Stäng skanningsfönstret
5. Om du vill konfigurera skanningsalternativen i detalj, klicka på **Visa avancerade alternativ**.
   Klick **Nästa**.
6. Du kan aktivera **Schemalägg skanningsuppgift** alternativet, om du vill, välj sedan när den anpassade skanningen du skapade ska starta.
   - Vid systemstart
   - Dagligen

- En gång i månaden
- Varje vecka

Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.

7. Klick **Spara** för att spara inställningarna och stänga konfigurationsfönstret.
   Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot kommer att hittas under skanningsprocessen kommer du att uppmanas att välja vilka åtgärder som ska vidtas på de upptäckta filerna.

Om du vill kan du snabbt köra en tidigare anpassad skanning igen genom att klicka på motsvarande post i den tillgängliga listan.

Hur undantar jag en mapp från att skannas?

Bitdefender tillåter att man undantar specifika filer, mappar eller filtillägg från genomsökning.

Undantag ska användas av användare med avancerad datorkunskap och endast i följande situationer:

- Du har en stor mapp på ditt system där du förvarar filmer och musik.
- Du har ett stort arkiv på ditt system där du förvarar olika data.
- Du har en mapp där du installerar olika typer av mjukvara och appar för teständamål. Genom att skanna mappen kan du förlora en del av data.

Så här lägger du till en mapp i listan med undantag:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klicka på **inställningar** flik.
4. Klicka på **Hantera undantag**.
5. Klick **+Lägg till ett undantag**.
6. Ange sökvägen till den mapp som du vill utom genom att skanna i motsvarande fält.

Alternativt kan du navigera till mappen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.

7. Slå på strömbrytaren bredvid skyddsfunktionen som inte ska skanna mappen. Det finns tre alternativ:
   - Antivirus
   - Hotförebyggande online
   - Avancerat hotförsvar
8. Klick **Spara** för att spara ändringarna och stänga fönstret.

Vad ska man göra när Bitdefender upptäckte en ren fil som infekterad?

Det kan finnas fall då Bitdefender av misstag flaggar en legitim fil som ett hot (en falsk positiv). För att rätta till detta fel, lägg till filen i området Bitdefender Exceptions:

1. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
   Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktiverat. Du kan inaktivera realtidsskydd i 5, 15 eller 30 minuter, i en timme, permanent eller tills ett system startar om.
2. Visa dolda objekt i Windows. För att ta reda på hur du gör detta, se Hur visar jag dolda objekt i Windows? (sida 114).
3. Återställ filen från karantänområdet:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. Gå till **inställningar** windows och klicka **Hantera karantän**.
   d. Välj filen och klicka sedan **Återställ**.

4. Lägg till filen i listan med undantag. För att ta reda på hur du gör detta, se Hur undantar jag en mapp från att skannas? (sida 101).
5. Slå på Bitdefender antivirusskydd i realtid.
6. Kontakta våra supportrepresentanter så att vi kan ta bort upptäckten av hotinformationsuppdateringen. För att ta reda på hur du gör detta, se Ber om hjälp (sida 273).

Hur kontrollerar jag vilka hot Bitdefender upptäckte?

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen.

Skanningsloggen innehåller detaljerad information om den loggade skanningsprocessen, såsom skanningsalternativ, skanningsmålet, hoten som hittats och de åtgärder som vidtagits mot dessa hot.

Du kan öppna skanningsloggen direkt från skanningsguiden, när skanningen är klar, genom att klicka **VISA LOGG**.

Så här kontrollerar du en skanningslogg eller någon upptäckt infektion vid ett senare tillfälle:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken väljer du meddelandet om den senaste skanningen.
   Det är här du kan hitta alla hotskanningshändelser, inklusive hot som upptäcks av skanning vid åtkomst, användarinitierade genomsökningar och statusändringar för automatiska genomsökningar.
3. I aviseringslistan kan du kontrollera vilka skanningar som har utförts nyligen. Klicka på ett meddelande för att se detaljer om det.
4. För att öppna en skanningslogg, klicka **Visa logg**.

3.4.4. Privat skydd

Hur ser jag till att min onlinetransaktion är säker?

För att se till att din onlineverksamhet förblir privat kan du använda webbläsaren som tillhandahålls av Bitdefender för att skydda dina transaktioner och appar för hembanker.

Bitdefender Safepay™ är en säker webbläsare utformad för att skydda din kreditkortsinformation, kontonummer eller andra känsliga uppgifter du kan ange när du kommer åt olika onlineplatser.

Så här håller du din onlineaktivitet säker och privat:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **SAFEPAY** rutan, klicka **inställningar**.
3. I den **Safepay** fönster, klicka **Starta Safepay**.
4. Klicka på knappen för att komma åt **Virtuellt tangentbord**.
   Använd **Virtuellt tangentbord** när du skriver känslig information som dina lösenord.

Vad kan jag göra om min enhet har blivit stulen?

Stöld av mobila enheter, oavsett om det är en smartphone, en surfplatta eller en bärbar dator, är en av huvudproblemen idag som påverkar individer och organisationer över hela världen.

Bitdefender Anti-Theft låter dig inte bara lokalisera och låsa den stulna enheten, utan också torka all data för att säkerställa att den inte kommer att användas av tjuven.

Så här kommer du åt stöldskyddsfunktionerna från ditt konto:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Klicka på önskat enhetskort och välj sedan **Anti-stöld**.
4. Välj den funktion du vill använda:
   - **LOKALISERA** - visa enhetens plats på Google Maps.
     Visa IP - visar den senaste IP-adressen för den valda enheten.
   - **Varna** - skicka en varning på enheten.
   - **Låsa** - lås din enhet och ställ in en numerisk PIN-kod för att låsa upp den. Alternativt, aktivera motsvarande alternativ för att låta Bitdefender ta ögonblicksbilder av personen som försöker komma åt din enhet.
   - **Torka** - radera all data från din enhet.

Viktig
När du har torkat en enhet upphör alla stöldskyddsfunktioner att fungera.

Hur tar jag bort en fil permanent med Bitdefender?

Om du vill ta bort en fil permanent från ditt system måste du radera data fysiskt från din hårddisk.

Bitdefender File Shredder hjälper dig att snabbt strimla filer eller mappar från din enhet med hjälp av Windows sammanhangsberoende meny genom att följa dessa steg:

1. Högerklicka på filen eller mappen du vill ta bort permanent, peka på Bitdefender och välj **Pappers strimlare**.
2. Klick **ta bort permanent**och bekräfta sedan att du vill fortsätta med processen.
   Vänta tills Bitdefender har avslutat fragmenteringen av filerna.
3. Resultaten visas. Klick **AVSLUTA** för att avsluta guiden.

Hur skyddar jag min webbkamera från att bli hackad?

Du kan ställa in din Bitdefender-produkt för att tillåta eller neka åtkomst av installerade appar till din webbkamera genom att följa dessa steg:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **VIDEO & LJUDSKYDD** rutan, klicka **inställningar**.
3. Gå till **Webbkamera skydd** fönstret och du kommer att se listan med appar som har begärt åtkomst till din kamera.
4. Peka på appen du vill tillåta eller förbjuda åtkomst och klicka sedan på knappen som representeras av en videokamera, som ligger bredvid den.
   För att se vad de andra Bitdefender-användarna har valt att göra med den valda appen, klicka på ikon. Du kommer att meddelas varje gång en av de listade apparna blockeras av Bitdefender-användarna.

För att manuellt lägga till appar till den här listan, klicka på **Lägg till applikation** och välj ett av de två alternativen.

- Från Windows Store

- Från dina appar

Hur kan jag manuellt återställa krypterade filer när återställningsprocessen misslyckas?

Om krypterade filer inte kan återställas automatiskt kan du återställa dem manuellt genom att följa dessa steg:

1. Klick **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **Allt** fliken, välj meddelandet om det senaste ransomware-beteendet som upptäckts och klicka sedan **Krypterade filer**.
3. Listan med de krypterade filerna visas.
   Klick **Återställ filer** att fortsätta.
4. Om hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de dekrypterade filerna ska sparas. Klick **Återställ plats**, och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.
   Klick **Avsluta** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas om de blir krypterade:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .fladdermus; .bin; .bmp; .c; .cda; .cgi; .kla ss; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h26 4; .h; .flv; .htm; .html;.ico; .burk; .java; .jpeg; .jpg;.js; .jsp; .nyckel; .m4v; .m db; .mitten; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .o gg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; . sav; .sql; .sh; .svg; .snabb; .swf; .tjära; .tex; .tif; .tiff; .Text; .xlr; .xls; .xlsx; .x ml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .blixtlås;

3.4.5. Optimeringsverktyg

Hur förbättrar jag min systemprestanda?

Systemets prestanda beror inte bara på hårdvarukonfigurationen, såsom CPU-belastning, minnesanvändning och hårddiskutrymme. Den är också direkt ansluten till din mjukvarukonfiguration och till din datahantering.

Det här är de viktigaste åtgärderna du kan vidta med Bitdefender för att förbättra ditt systems hastighet och prestanda:

❍ Optimera systemets prestanda med ett enda klick (sida 107)
❍ Skanna ditt system med jämna mellanrum (sida 107)

Optimera systemets prestanda med ett enda klick

Alternativet OneClick Optimizer sparar värdefull tid när du vill ha ett snabbt sätt att förbättra systemets prestanda genom att snabbt skanna, upptäcka och rensa värdelösa filer.

Så här startar du OneClick Optimizer-processen:

1. Klick **Verktyg** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Klicka på **Optimera** knapp.
3. Låt Bitdefender söka efter filer som kan raderas och klicka sedan på **Optimera** knappen för att avsluta processen.

Skanna ditt system med jämna mellanrum

Din systemhastighet och dess allmänna beteende kan också påverkas av hot.

Se till att skanna ditt system med jämna mellanrum, minst en gång i veckan.

Det rekommenderas att använda System Scan eftersom den söker efter alla typer av hot som äventyrar säkerheten för ditt system och den skannar även inuti arkiv.

Så här startar du systemsökningen:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klick **Kör Scan** bredvid **Genomsökning av systemet**.
4. Följ stegen i guiden.

3.4.6. Användbar information

Hur testar jag min säkerhetslösning?

För att säkerställa att din Bitdefender-produkt fungerar korrekt rekommenderar vi att du använder Eicar-testet.

Eicar-testet låter dig kontrollera din säkerhetslösning med hjälp av en säker fil utvecklad för detta ändamål.

Så här testar du din säkerhetslösning:

1. Ladda ner testet från den officiella webbsidan för EICAR-organisationen http://www.eicar.org/.
2. Klicka på **Anti-Malware testfil** flik.
3. Klick **Ladda ner** i menyn till vänster.
4. Från **Nedladdningsområde med standardprotokollet http** Klicka på **eicar.com** testfil.
5. Du kommer att informeras om att sidan du försöker komma åt innehåller EICAR-testfilen (inte ett hot).
   Om du klickar **Jag förstår riskerna, ta mig dit ändå**, kommer nedladdningen av testet att börja och en Bitdefender-popup kommer att informera dig om att ett hot upptäcktes.
   Klick **Fler detaljer** för att få mer information om denna åtgärd.

Om du inte får någon Bitdefender-varning rekommenderar vi att du kontaktar Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Hur tar jag bort Bitdefender?

Om du vill ta bort din Bitdefender Ultimate Small Business Security:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  3. Klick **AVLÄGSNA** i fönstret som visas.
  4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera ett program** eller **Program och funktioner**.

3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
4. Klick **AVLÄGSNA** i fönstret som visas.
5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar**.
  3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **AVLÄGSNA** i fönstret som visas.
  6. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

> **Notera**
> Denna ominstallation kommer att ta bort de anpassade inställningarna permanent.

Hur tar jag bort Bitdefender VPN?

Proceduren för att ta bort Bitdefender VPN liknar den du använder för att ta bort andra program från din enhet:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender VPN** och välj **Avinstallera**.
     Vänta tills avinstallationsprocessen är klar.

- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.

2. Klick **Avinstallera** ett program eller **Program och funktioner**.
3. Hitta **Bitdefender VPN** och välj **Avinstallera**.
   Vänta tills avinstallationsprocessen är klar.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender VPN** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
     Vänta tills avinstallationsprocessen är klar.

Hur tar jag bort Bitdefender Anti-tracker-tillägget?

Beroende på vilken webbläsare du använder, följ dessa steg för att avinstallera Bitdefender Anti-tracker-tillägget:

- Internet Explorer
  1. Klick bredvid sökfältet och välj sedan Hantera tillägg. En lista med installerade tillägg visas.
  2. Klicka på Bitdefender Anti-tracker.
  3. Klick **Inaktivera** längst ner till höger.

- Google Chrome
  1. Klick bredvid sökfältet.
  2. Välj **Fler verktyg**, och då **Tillägg**.
     En lista med installerade tillägg visas.
  3. Klick **Avlägsna** i Bitdefender Anti-tracker-kortet.
  4. Klick **Avlägsna** i popup-fönstret som visas.

- Mozilla Firefox
  1. Klick bredvid sökfältet.
  2. Välj **Tillägg**, och då **Tillägg**.
     En lista med installerade tillägg visas.

3. Klick ··· och välj sedan **Avlägsna**.

Hur stänger jag av enheten automatiskt efter att skanningen är över?

Bitdefender erbjuder flera skanningsuppgifter som du kan använda för att se till att ditt system inte är infekterat med hot. Att skanna hela enheten kan ta längre tid att slutföra beroende på systemets hård- och mjukvarukonfiguration.

Av denna anledning låter Bitdefender dig konfigurera din produkt för att stänga av ditt system så snart genomsökningen är över.

Tänk på det här exemplet: du har avslutat ditt arbete och du vill gå och lägga dig. Du skulle vilja ha hela ditt system kontrollerat för hot av Bitdefender.

Så här stänger du av enheten när Quick Scan eller System Scan är över:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. I den **Skanningar** fönster, klicka ··· bredvid Quick Scan eller System Scan och välj **Redigera**.
4. Anpassa skanningen efter dina behov och klicka **Nästa**.
5. Markera rutan bredvid **Välj när du vill schemalägga denna uppgift**, och välj sedan när uppgiften ska starta.
   Om du väljer Dagligen, Månadsvis eller Veckovis, dra skjutreglaget längs skalan för att ställa in önskad tidsperiod när den schemalagda skanningen ska starta.
6. Klick **Spara**.

Så här stänger du av enheten när en anpassad skanning är över:

1. Klick ··· bredvid den anpassade skanningen du skapade.
2. Klick **Nästa** och klicka sedan **Nästa** igen.
3. fan rutan bredvid **Välj när du vill schemalägga denna uppgift**, och välj sedan när uppgiften ska starta.
4. Klick **Spara**.

Om inga hot hittas kommer enheten att stängas av.

Om det finns kvar olösta hot kommer du att uppmanas att välja vilka åtgärder som ska vidtas mot dem. För mer information, se Antivirus Scan Wizard (sida 29).

Hur konfigurerar jag Bitdefender för att använda en proxy-internetanslutning?

Om din enhet ansluter till internet via en proxyserver måste du konfigurera Bitdefender med proxyinställningarna. Normalt upptäcker och importerar Bitdefender automatiskt proxyinställningarna från ditt system.

> **Viktig**
> Internetanslutningar i hemmet använder normalt inte en proxyserver. Som en tumregel, kontrollera och konfigurera proxyanslutningsinställningarna för ditt Bitdefender-program när uppdateringar inte fungerar. Om Bitdefender kan uppdatera är den korrekt konfigurerad för att ansluta till internet.

Så här hanterar du proxyinställningarna:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.
2. Välj **Avancerad** flik.
3. Sätta på **Proxyserver**.
4. Klick **Byte av proxy**.
5. Det finns två alternativ för att ställa in proxyinställningarna:
   - **Importera proxyinställningar från standardwebbläsaren** - proxyinställningar för den aktuella användaren, extraherad från standardwebbläsaren. Om proxyservern kräver ett användarnamn och ett lösenord måste du ange dem i motsvarande fält.

     > **Notera**
     > Bitdefender kan importera proxyinställningar från de mest populära webbläsarna, inklusive de senaste versionerna av Microsoft Edge, Internet Explorer, Mozilla Firefox och Google Chrome.

   - **Anpassade proxyinställningar** - proxyinställningar som du kan konfigurera själv.
     Följande inställningar måste anges:
     - **Adress** - skriv in proxyserverns IP.

- **Hamn** - skriv in porten som Bitdefender använder för att ansluta till proxyservern.
- **Användarnamn** - skriv in ett användarnamn som känns igen av proxyn.
- **Lösenord** - skriv in det giltiga lösenordet för den tidigare angivna användaren.

6. Klick **OK** för att spara ändringarna och stänga fönstret.

Bitdefender kommer att använda de tillgängliga proxyinställningarna tills den lyckas ansluta till internet.

Använder jag en 32-bitars eller en 64-bitarsversion av Windows?

Så här tar du reda på om du har ett 32-bitars eller ett 64-bitars operativsystem:

- I **Windows 7**:
  1. Klick **Start**.
  2. Lokalisera **Dator** på **Start** meny.
  3. Högerklicka **Dator** och välj **Egenskaper**.
  4. Titta under **Systemet** för att kontrollera informationen om ditt system.
- I **Windows 8**:
  1. Från startskärmen i Windows, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt på startskärmen) och sedan högerklicka på dess ikon.
  2. Välj **Egenskaper** i bottenmenyn.
  3. Titta i systemområdet för att se din systemtyp.
- I **Windows 10** och **Windows 11**:
  1. Skriv "System" i sökrutan från aktivitetsfältet och klicka på dess ikon.
  2. Titta i området System för att hitta information om din systemtyp.

Hur visar jag dolda objekt i Windows?

Dessa steg är användbara i de fall där du har att göra med en hotsituation och du behöver hitta och ta bort de infekterade filerna, som kan vara dolda.

Följ dessa steg för att visa dolda objekt i Windows:

1. Klick **Start**, gå till **Kontrollpanel**.
   I **Windows 8** och **Windows 8.1**: Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
2. Välj **Mappalternativ**.
3. Gå till **Se** flik.
4. Välj **Visa dolda filer och mappar**.
5. Klar **Dölj filnamnstillägg för kända filtyper**.
6. Klar **Dölj skyddade operativsystemfiler**.
7. Klick **Tillämpa**, Klicka sedan **OK**.

I **Windows 10** och **Windows 11**:

1. Skriv "Visa dolda filer och mappar" i sökrutan från aktivitetsfältet och klicka på dess ikon.
2. Välj **Visa dolda filer, mappar och enheter**.
3. Klar **Dölj filnamnstillägg för kända filtyper**.
4. Klar **Dölj skyddade operativsystemfiler**.
5. Klick **Tillämpa**, Klicka sedan **OK**.

Hur tar jag bort andra säkerhetslösningar?

Det främsta skälet till att använda en säkerhetslösning är att ge skydd och säkerhet för dina data. Men vad händer när du har mer än en säkerhetsprodukt på samma system?

När du använder mer än en säkerhetslösning på samma enhet blir systemet instabilt. De Bitdefender Ultimate Small Business Security installationsprogrammet upptäcker automatiskt andra säkerhetsprogram och erbjuder dig möjligheten att avinstallera dem.

Om du inte tog bort de andra säkerhetslösningarna under den första installationen:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Vänta några ögonblick tills listan med installerad programvara visas.
  3. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.
  4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera ett program** eller **Program och funktioner**.
  3. Vänta några ögonblick tills listan med installerad programvara visas.
  4. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Appar**.
  3. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

Om du misslyckas med att ta bort den andra säkerhetslösningen från ditt system, skaffa avinstallationsverktyget från leverantörens webbplats eller kontakta dem direkt för att ge dig riktlinjerna för avinstallation.

Hur startar jag om i felsäkert läge?

Säkert läge är ett diagnostiskt driftläge, som främst används för att felsöka problem som påverkar normal drift av Windows. Sådana problem

sträcker sig från motstridiga drivrutiner till hot som hindrar Windows från att starta normalt. I felsäkert läge fungerar bara ett fåtal appar och Windows laddar bara de grundläggande drivrutinerna och ett minimum av operativsystemkomponenter. Det är därför de flesta hot är inaktiva när du använder Windows i felsäkert läge och de kan enkelt tas bort.

Så här startar du Windows i felsäkert läge:

- I **Windows 7**:
  1. Starta om enheten.
  2. tryck på **F8** flera gånger innan Windows börjar komma åt startmenyn.
  3. Välj **Säkert läge** i startmenyn eller **Säkert läge med nätverk** om du vill ha tillgång till internet.
  4. Tryck **Stiga på** och vänta medan Windows laddas i felsäkert läge.
  5. Denna process avslutas med ett bekräftelsemeddelande. Klick **OK** att erkänna.
  6. Starta Windows normalt genom att helt enkelt starta om systemet.

- I **Windows 8**, **Windows 8.1**, **Windows 10** och **Windows 11**:
  1. Lansera **Systemkonfiguration** i Windows genom att samtidigt trycka på **Windows + R** tangenterna på ditt tangentbord.
  2. Skriva **msconfig** i **Öppen** dialogrutan och klicka sedan på **OK**.
  3. Välj **Känga** flik.
  4. I den **Startalternativ** område, välj **Säker stövel** kryssruta.
  5. Klick **Nätverk**, och då **OK**.
  6. Klick **OK** i **Systemkonfiguration** fönster som informerar dig om att systemet måste startas om för att kunna göra de ändringar du ställt in.
     Ditt system startar om i felsäkert läge med nätverk.

För att starta om i normalt läge, byt tillbaka inställningarna genom att starta igen **System operation** och rensa **Säker stövel** kryssruta. Klick **OK**, och då **Omstart**. Vänta tills de nya inställningarna tillämpas.

3.5. Felsökning

3.5.1. Löser vanliga problem

Det här kapitlet presenterar några problem du kan stöta på när du använder Bitdefender och ger dig möjliga lösningar på dessa problem. De flesta av dessa problem kan lösas genom lämplig konfiguration av produktinställningarna.

- Mitt system verkar vara långsamt (sida 117)
- Skanningen startar inte (sida 118)
- Jag kan inte längre använda en app (sida 121)
- Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker (sida 122)
- Hur man uppdaterar Bitdefender på en långsam internetanslutning (sida 126)
- Bitdefender-tjänsterna svarar inte (sida 127)
- Antispamfiltret fungerar inte korrekt (sida 128)
- Borttagning av Bitdefender misslyckades (sida 132)
- Mitt system startar inte upp efter installation av Bitdefender (sida 133)

Om du inte kan hitta ditt problem här, eller om de presenterade lösningarna inte löser det, kan du kontakta Bitdefender tekniska supportrepresentanter som presenteras i kapitel Ber om hjälp (sida 273).

Mitt system verkar vara långsamt

Vanligtvis, efter installation av en säkerhetsprogramvara, kan det förekomma en liten nedgång i systemet, vilket till en viss grad är normalt.

Om du märker en betydande avmattning kan det här problemet uppstå av följande anledningar:

- **Bitdefender är inte det enda säkerhetsprogrammet som är installerat på systemet**.
  Även om Bitdefender söker och tar bort säkerhetsprogrammen som hittas under installationen, rekommenderas det att ta bort alla andra säkerhetslösningar som du kan använda innan du installerar

Bitdefender. För mer information, se Hur tar jag bort andra säkerhetslösningar? (sida 114).

- **Systemkraven för att köra Bitdefender är inte uppfyllda.**
  Om din maskin inte uppfyller systemkraven kommer enheten att bli trög, särskilt när flera appar körs samtidigt. För mer information, se Systemkrav (sida 9).
- **Du har installerat appar som du inte använder.**
  Alla enheter har program eller appar som du inte använder. Och många oönskade program körs i bakgrunden och tar upp diskutrymme och minne. Om du inte använder ett program, avinstallera det. Detta gäller även för alla andra förinstallerade program eller testappar som du har glömt att ta bort.

  > **Viktig**
  > Om du misstänker att ett program eller en app är en viktig del av ditt operativsystem, ta inte bort det och kontakta Bitdefender kundtjänst för hjälp.

- **Ditt system kan vara infekterat.**
  Din systemhastighet och dess allmänna beteende kan också påverkas av hot. Spionprogram, skadlig programvara, trojaner och adware tar alla hårt på enhetens prestanda. Se till att skanna ditt system med jämna mellanrum, minst en gång i veckan. Det rekommenderas att använda Bitdefender System Scan eftersom den söker efter alla typer av hot som äventyrar säkerheten för ditt system.
  Så här startar du systemsökningen:

  1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
  2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
  3. I den **Skanningar** fönster, klicka **Kör Scan** bredvid **Genomsökning av systemet**.
  4. Följ stegen i guiden.

Skanningen startar inte

Den här typen av problem kan ha två huvudorsaker:

- **En tidigare Bitdefender-installation som inte togs bort helt eller en felaktig Bitdefender-installation.**

I det här fallet installerar du om Bitdefender:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  3. Klick **INSTALLERA OM** i fönstret som visas.
  4. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 8** och **Windows 8.1**:
  1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
  2. Klick **Avinstallera** ett program eller **Program och funktioner**.
  3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  4. Klick **INSTALLERA OM** i fönstret som visas.
  5. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, Klicka sedan **inställningar**.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **INSTALLERA OM** i fönstret som visas.
  6. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.

> **Notera**
> Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

- **Bitdefender är inte den enda säkerhetslösningen som är installerad på ditt system.**
  I detta fall:

  1. Ta bort den andra säkerhetslösningen. För mer information, se Hur tar jag bort andra säkerhetslösningar? (sida 114).
  2. Installera om Bitdefender:
     - I **Windows 7**:
       a. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
       b. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
       c. Klick **INSTALLERA OM** i fönstret som visas.
       d. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.
     - I **Windows 8** och **Windows 8.1**:
       a. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
       b. Klick **Avinstallera** ett program eller **Program och funktioner**.
       c. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
       d. Klick **INSTALLERA OM** i fönstret som visas.
       e. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.
     - I **Windows 10** och **Windows 11**:
       a. Klick **Start**, Klicka sedan **inställningar**.

b. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.

c. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.

d. Klick **Avinstallera** igen för att bekräfta ditt val.

e. Klick **INSTALLERA OM** i fönstret som visas

f. Vänta tills ominstallationsprocessen är klar och starta sedan om systemet.

> **Notera**
> Genom att följa denna ominstallationsprocedur sparas anpassade inställningar och är tillgängliga i den nya installerade produkten. Andra inställningar kan ändras tillbaka till standardkonfigurationen.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Jag kan inte längre använda en app

Det här problemet uppstår när du försöker använda ett program som fungerade normalt innan du installerade Bitdefender.

Efter installation av Bitdefender kan du stöta på en av dessa situationer:

- Du kan få ett meddelande från Bitdefender om att programmet försöker göra en modifiering av systemet.
- Du kan få ett felmeddelande från programmet du försöker använda.

Denna typ av situation uppstår när Advanced Threat Defense av misstag upptäcker vissa appar som skadliga.

Advanced Threat Defense är en Bitdefender-funktion som ständigt övervakar apparna som körs på ditt system och rapporterar dem med potentiellt skadligt beteende. Eftersom den här funktionen är baserad på ett heuristiskt system kan det finnas fall då legitima appar rapporteras av Advanced Threat Defense.

När denna situation inträffar kan du undanta respektive app från att övervakas av Advanced Threat Defense.

Så här lägger du till programmet i undantagslistan:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **AVANCERAD HOT FÖRSVAR** rutan, klicka **Öppen**.
3. I den **inställningar** fönster, klicka **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Ange sökvägen för den körbara filen du vill ha förutom skanning i motsvarande fält.
   Alternativt kan du navigera till den körbara filen genom att klicka på bläddringsknappen till höger i gränssnittet, markera den och klicka på **OK**.
6. Slå på strömbrytaren bredvid **Avancerat hotförsvar**.
7. Klick **Spara**.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker

Bitdefender erbjuder en säker webbupplevelse genom att filtrera all webbtrafik och blockera allt skadligt innehåll. Det är dock möjligt att Bitdefender betraktar en webbplats, en domän, en IP-adress eller onlineapp som är säkra som osäkra, vilket gör att Bitdefender HTTP-trafikskanning blockerar dem felaktigt.

Skulle samma sida, domän, IP-adress eller onlineapp blockeras upprepade gånger, kan de läggas till i undantagen så att de inte skannas av Bitdefender-motorerna, vilket säkerställer en smidig webbupplevelse.

För att lägga till en webbplats **Undantag**:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ONLINE FÖREBYGGANDE AV HOT** rutan, klicka **inställningar**.
3. Klick **Hantera undantag**.
4. Klick **+Lägg till ett undantag**.
5. Skriv i motsvarande fält namnet på webbplatsen, namnet på domänen eller IP-adressen du vill lägga till i undantag.

6. Klicka på knappen bredvid **Hotförebyggande online**.
7. Klick **Spara** för att spara ändringarna och stänga fönstret.

Endast webbplatser, domäner, IP-adresser och appar som du litar på bör läggas till i den här listan. Dessa kommer att undantas från genomsökning av följande motorer: hot, nätfiske och bedrägeri.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Jag kan inte ansluta till internet

Du kanske märker att ett program eller en webbläsare inte längre kan ansluta till internet eller komma åt nätverkstjänster efter installation av Bitdefender.

I det här fallet är den bästa lösningen att konfigurera Bitdefender för att automatiskt tillåta anslutningar till och från respektive programvaruapp:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
3. I den **Regler** fönster, klicka **Lägg till regel**.
4. Ett nytt fönster visas där du kan lägga till detaljerna. Se till att välja alla tillgängliga nätverkstyper och i **Lov** avsnitt välj **Tillåta**.

Stäng Bitdefender, öppna programvaruappen och försök igen att ansluta till internet.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Jag kan inte komma åt en enhet i mitt nätverk

Beroende på nätverket du är ansluten till kan Bitdefender-brandväggen blockera anslutningen mellan ditt system och en annan enhet (som en annan dator eller en skrivare). Som ett resultat kan du inte längre dela eller skriva ut filer.

I det här fallet är den bästa lösningen att konfigurera Bitdefender för att automatiskt tillåta anslutningar till och från respektive enhet, enligt följande:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.

2. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
3. I den **Regler** fönster, klicka **Lägg till regel**.
4. Slå på **Tillämpa denna regel på alla ansökningar** alternativ.
5. Klicka på **Avancerade inställningar** knapp.
6. I den **Anpassad fjärradress** rutan, skriv in IP-adressen för den dator eller skrivare du vill ha obegränsad åtkomst till.

Om du fortfarande inte kan ansluta till enheten, kanske problemet inte orsakas av Bitdefender.

Kontrollera om det finns andra potentiella orsaker, till exempel följande:

- Brandväggen på den andra enheten kan blockera fil- och skrivardelning med din PC.
  - Om Windows-brandväggen används kan den konfigureras för att tillåta fil- och skrivardelning enligt följande:
    - I **Windows 7**:
      1. Klick **Start**, gå till **Kontrollpanel** och välj **System och säkerhet**.
      2. Gå till **Windows brandvägg**, och klicka sedan **Tillåt ett program via Windows-brandväggen**.
      3. Välj **Fil- och skrivardelning** kryssruta.
    - I **Windows 8** och **Windows 8.1**:
      1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
      2. Klick **System och säkerhet**, gå till **Windows brandvägg** och välj **Tillåt en app via Windows-brandväggen**.
      3. Välj **Fil- och skrivardelning** kryssrutan och klicka sedan på **OK**.
    - I **Windows 10** och **Windows 11**:
      1. Skriv "Tillåt en app genom Windows-brandväggen" i sökrutan från aktivitetsfältet och klicka på dess ikon.
      2. Klick **Ändra inställningar**.

3. I den **Tillåtna appar och funktioner** lista välj **Fil- och skrivardelning** kryssrutan och klicka sedan på **OK**.

- Om ett annat brandväggsprogram används, se dess dokumentation eller hjälpfil.

- Allmänna villkor som kan förhindra användning eller anslutning till den delade skrivaren:
  - Du kan behöva logga in på ett Windows-administratörskonto för att komma åt den delade skrivaren.
  - Behörigheter är inställda för den delade skrivaren för att endast tillåta åtkomst till specifika enheter och användare. Om du delar din skrivare, kontrollera behörigheterna för skrivaren för att se om användaren på den andra enheten tillåts åtkomst till skrivaren. Om du försöker ansluta till en delad skrivare, kontrollera med användaren på den andra enheten om du har behörighet att ansluta till skrivaren.
  - Skrivaren som är ansluten till din enhet eller till den andra är inte delad.
  - Den delade skrivaren läggs inte till på enheten.

    Notera
    För att lära dig hur du hanterar skrivardelning (dela en skrivare, ställa in eller ta bort behörigheter för en skrivare, ansluta till en nätverksskrivare eller till en delad skrivare), gå till Windows Hjälp- och supportcenter (i Start-menyn klickar du på **Hjälp och support**).

- Åtkomst till en nätverksskrivare kan vara begränsad till endast specifika enheter eller användare. Du bör kontrollera med nätverksadministratören om du har behörighet att ansluta till den skrivaren.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Mitt internet är långsamt

Denna situation kan uppstå efter att du har installerat Bitdefender. Problemet kan orsakas av fel i Bitdefender-brandväggskonfigurationen.

Så här felsöker du den här situationen:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **BRANDVÄGGEN** stäng av strömbrytaren för att inaktivera funktionen.
3. Kontrollera om din internetanslutning förbättrades med Bitdefender-brandväggen inaktiverad.
   - ❍ Om du fortfarande har en långsam internetanslutning kanske problemet inte orsakas av Bitdefender. Du bör kontakta din Internetleverantör för att kontrollera om anslutningen fungerar på deras sida.
     Om du får en bekräftelse från din Internetleverantör att anslutningen fungerar på deras sida och problemet fortfarande kvarstår, kontakta Bitdefender enligt beskrivningen i avsnittet Ber om hjälp (sida 273).
   - ❍ Om internetanslutningen förbättrades efter att Bitdefender-brandväggen inaktiverats:
     a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
     b. I den **BRANDVÄGGEN** rutan, klicka **inställningar**.
     c. Gå till **Nätverksadaptrar** och ställ in din internetanslutning **Hemmakontor**.
     d. I den **inställningar** flik, stäng av **Skydd mot portskanning**.
     I den **Smygläge** område, klicka **Redigera stealth-inställningar**. Slå på Stealth Mode för nätverksadaptern du är ansluten till.
     e. Stäng Bitdefender, starta om systemet och kontrollera internetanslutningshastigheten.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Hur man uppdaterar Bitdefender på en långsam internetanslutning

Om du har en långsam internetanslutning (som uppringd), kan fel uppstå under uppdateringsprocessen.

För att hålla ditt system uppdaterat med den senaste Bitdefender hotinformationsdatabasen:

1. Klick **inställningar** på navigeringsmenyn på Bitdefender-gränssnitt.

2. Välj **Uppdatering** flik.
3. Stäng av **Tyst uppdatering** växla.
4. Nästa gång när en uppdatering blir tillgänglig kommer du att bli ombedd att välja vilken uppdatering du vill ladda ner. Välj endast **Uppdatering av signaturer**.
5. Bitdefender kommer endast att ladda ner och installera hotinformationsdatabasen.

Bitdefender-tjänsterna svarar inte

Den här artikeln hjälper dig att felsöka **Bitdefender Services svarar inte** fel. Du kan stöta på detta fel enligt följande:

- Bitdefender-ikonen i systemfältet är nedtonad och du informeras om att Bitdefender-tjänsterna inte svarar.
- Bitdefender-fönstret indikerar att Bitdefender-tjänsterna inte svarar.

Felet kan orsakas av något av följande tillstånd:

- tillfälliga kommunikationsfel mellan Bitdefender-tjänsterna.
- några av Bitdefender-tjänsterna stoppas.
- andra säkerhetslösningar som körs på din enhet samtidigt med Bitdefender.

För att felsöka det här felet, prova dessa lösningar:

1. Vänta en stund och se om något förändras. Felet kan vara tillfälligt.
2. Starta om enheten och vänta några ögonblick tills Bitdefender laddas. Öppna Bitdefender för att se om felet kvarstår. Att starta om enheten löser vanligtvis problemet.
3. Kontrollera om du har någon annan säkerhetslösning installerad eftersom de kan störa den normala driften av Bitdefender. Om så är fallet rekommenderar vi att du tar bort alla andra säkerhetslösningar och sedan installerar om Bitdefender.
   För mer information, se Hur tar jag bort andra säkerhetslösningar? (sida 114).

Om felet kvarstår, kontakta våra supportrepresentanter för hjälp enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Antispamfiltret fungerar inte korrekt

Den här artikeln hjälper dig att felsöka följande problem angående Bitdefender Antispam-filtreringsoperationen:

- Ett antal legitima e-postmeddelanden är markerade som [spam].
- Många skräppostmeddelanden markeras inte i enlighet med detta av antispamfiltret.
- Antispamfiltret upptäcker inget skräppostmeddelande.

Legitima meddelanden är markerade som [spam]

Legitima meddelanden är markerade som [spam] helt enkelt för att de ser ut som skräppost för Bitdefender antispamfiltret. Du kan normalt lösa det här problemet genom att konfigurera antispamfiltret på lämpligt sätt.

Bitdefender lägger automatiskt till mottagarna av dina e-postmeddelanden till en vänlista. De e-postmeddelanden som tas emot från kontakterna i vänlistan anses vara legitima. De verifieras inte av antispamfiltret och därför markeras de aldrig som [spam].

Den automatiska konfigurationen av vänlistan förhindrar inte upptäcktsfel som kan uppstå i dessa situationer:

- Du får mycket efterfrågad reklampost som ett resultat av att du prenumererar på olika webbplatser. I det här fallet är lösningen att lägga till e-postadresserna som du får sådana e-postmeddelanden från till vänlistan.
- En betydande del av din legitima e-post kommer från personer som du aldrig har skickat e-post till tidigare, som kunder, potentiella affärspartners och andra. I detta fall krävs andra lösningar.

Om du använder en av e-postklienterna Bitdefender integrerar i, indikera upptäcktsfel.

> **Notera**
> Bitdefender integreras i de mest använda e-postklienterna genom ett lättanvänt verktygsfält för skräppost. För en komplett lista över e-postklienter som stöds, se E-postklienter och protokoll som stöds (sida 46).

Lägg till kontakter i vänlistan

Om du använder en e-postklient som stöds kan du enkelt lägga till avsändare av legitima meddelanden till vänlistan. Följ dessa steg:

1. I din e-postklient väljer du ett e-postmeddelande från avsändaren som du vill lägga till i vänlistan.
2. Klicka på **Lägg till vän** knappen på Bitdefender antispam-verktygsfältet.
3. Du kan bli ombedd att bekräfta adresserna som lagts till i vänlistan. Välj **Visa inte det här meddelandet igen** och klicka **OK**.

Du kommer alltid att få e-postmeddelanden från den här adressen oavsett vad de innehåller.

Om du använder en annan e-postklient kan du lägga till kontakter till vänlistan från Bitdefender-gränssnittet. Följ dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTI SPAM** rutan, klicka **Hantera vänner**.
   Ett konfigurationsfönster visas.
3. Skriv den e-postadress du alltid vill ta emot e-postmeddelanden från och klicka sedan **LÄGG TILL**. Du kan lägga till så många e-postadresser du vill.
4. Klick **OK** för att spara ändringarna och stänga fönstret.

Ange detekteringsfel

Om du använder en e-postklient som stöds kan du enkelt korrigera antispamfiltret (genom att ange vilka e-postmeddelanden som inte ska ha markerats som *[spam]*). Att göra det hjälper till att förbättra effektiviteten hos antispamfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till skräppostmappen dit skräppostmeddelanden flyttas.
3. Välj det legitima meddelandet som är felaktigt markerat som *[spam]* av Bitdefender.
4. Klicka på **Lägg till vän** knappen på Bitdefender antispam-verktygsfältet för att lägga till avsändaren i vänlistan. Du kan behöva klicka **OK** att erkänna. Du kommer alltid att få e-postmeddelanden från den här adressen oavsett vad de innehåller.
5. Klicka på **Ej spam** knappen på Bitdefender antispam-verktygsfältet (normalt placerad i den övre delen av e-postklientfönstret). E-postmeddelandet kommer att flyttas till mappen Inkorg.

Många skräppostmeddelanden upptäcks inte

Om du får många skräppostmeddelanden som inte är markerade som [spam], måste du konfigurera Bitdefender antispamfiltret för att förbättra dess effektivitet.

Prova följande lösningar:

1. Om du använder en av e-postklienterna Bitdefender integrerar i, indikera oupptäckta skräppostmeddelanden.

   > **Notera**
   > Bitdefender integreras i de mest använda e-postklienterna genom ett lättanvänt verktygsfält för skräppost. För en komplett lista över e-postklienter som stöds, se E-postklienter och protokoll som stöds (sida 46).

2. Lägg till spammare till listan med spammare. De e-postmeddelanden som tas emot från adresser i listan med spammare markeras automatiskt som [spam].

Ange oupptäckta skräppostmeddelanden

Om du använder en e-postklient som stöds kan du enkelt ange vilka e-postmeddelanden som ska ha upptäckts som skräppost. Att göra det hjälper till att förbättra effektiviteten hos antispamfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen Inkorg.
3. Välj de oupptäckta skräppostmeddelandena.
4. Klicka på **Är skräppost** knappen på Bitdefender antispam-verktygsfältet (normalt placerad i den övre delen av e-postklientfönstret). De markeras omedelbart som [spam] och flyttas till skräppostmappen.

Lägg till spammare till listan över spammare

Om du använder en e-postklient som stöds kan du enkelt lägga till avsändare av skräppostmeddelandena till listan med skräppost. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till skräppostmappen dit skräppostmeddelanden flyttas.

3. Välj meddelanden markerade som *[spam]* av Bitdefender.
4. Klicka på **Lägg till spammer** knappen på Bitdefender antispam-verktygsfältet.
5. Du kan bli ombedd att bekräfta adresserna som lagts till i listan över spammare. Välj **Visa inte det här meddelandet igen** och klicka **OK**.

Om du använder en annan e-postklient kan du manuellt lägga till spammare till listan med spammare från Bitdefender-gränssnittet. Det är bekvämt att göra detta endast när du har fått flera skräppostmeddelanden från samma e-postadress. Följ dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTI SPAM** rutan, klicka **inställningar**.
3. Gå till **Hantera spammare** fönster.
4. Skriv in spammarens e-postadress och klicka sedan på **Lägg till**. Du kan lägga till så många e-postadresser du vill.
5. Klick **OK** för att spara ändringarna och stänga fönstret.

Antispamfiltret upptäcker inget skräppostmeddelande

Om inget skräppostmeddelande är markerat som [spam], kan det vara ett problem med Bitdefender Antispam-filtret. Innan du felsöker det här problemet, se till att det inte orsakas av något av följande tillstånd:

- Antispamskyddet kan vara avstängt. För att verifiera antispam-skyddsstatusen, klicka **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt. Titta i **Anti Spam** rutan för att kontrollera om funktionen är aktiverad.
  Om Antispam är avstängt är det detta som orsakar ditt problem. Klicka på motsvarande knapp för att aktivera ditt antispam-skydd.
- Bitdefender Antispam-skydd är endast tillgängligt för e-postklienter som är konfigurerade att ta emot e-postmeddelanden via POP3-protokollet. Detta betyder följande:
  - E-postmeddelanden som tas emot via webbaserade e-posttjänster (som Yahoo, Gmail, Hotmail eller andra) filtreras inte för skräppost av Bitdefender.
  - Om din e-postklient är konfigurerad att ta emot e-postmeddelanden med ett annat protokoll än POP3 (till exempel

IMAP4), kontrollerar inte Bitdefender Antispam-filtret dem för skräppost.

> **Notera**
> POP3 är ett av de mest använda protokollen för att ladda ner e-postmeddelanden från en e-postserver. Om du inte känner till protokollet som din e-postklient använder för att ladda ner e-postmeddelanden, fråga personen som konfigurerade din e-postklient.

- Bitdefender Ultimate Small Business Security skannar inte Lotus Notes POP3-trafik.

En möjlig lösning är att reparera eller installera om produkten. Du kanske vill kontakta Bitdefender för support istället, som beskrivs i avsnittet Ber om hjälp (sida 273).

Borttagning av Bitdefender misslyckades

Om du vill ta bort din Bitdefender-produkt och du märker att processen hänger ut eller systemet fryser, klicka på **Annullera** för att avbryta åtgärden. Om detta inte fungerar, starta om systemet.

När borttagningen misslyckas kan vissa Bitdefender-registernycklar och filer finnas kvar i ditt system. Sådana rester kan förhindra en ny installation av Bitdefender. De kan också påverka systemets prestanda och stabilitet.

För att helt ta bort Bitdefender från ditt system:

- I **Windows 7**:
  1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
  2. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  3. Klick **AVLÄGSNA** i fönstret som visas.
  4. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 8** och **Windows 8.1**:

1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
2. Klick **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
4. Klick **AVLÄGSNA** i fönstret som visas.
5. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, klicka sedan på Inställningar.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
  5. Klick **AVLÄGSNA** i fönstret som visas.
  6. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

Mitt system startar inte upp efter installation av Bitdefender

Om du precis har installerat Bitdefender och inte kan starta om ditt system i normalt läge längre kan det finnas olika orsaker till detta problem.

Antagligen orsakas detta av en tidigare Bitdefender-installation som inte togs bort ordentligt eller av en annan säkerhetslösning som fortfarande finns på systemet.

Så här kan du hantera varje situation:

- **Du hade Bitdefender tidigare och du tog inte bort den ordentligt.**
  För att lösa detta:
  1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 115).

2. Ta bort Bitdefender från ditt system:
   - I **Windows 7**:
     a. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
     b. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
     c. Klick **AVLÄGSNA** i fönstret som visas.
     d. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
     e. Starta om ditt system i normalt läge.
   - I **Windows 8** och **Windows 8.1**:
     a. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
     b. Klick **Avinstallera ett program** eller **Program och funktioner**.
     c. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
     d. Klick **AVLÄGSNA** i fönstret som visas.
     e. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
     f. Starta om ditt system i normalt läge.
   - I **Windows 10** och **Windows 11**:
     a. Klick **Start**, klicka sedan på Inställningar.
     b. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
     c. Hitta **Bitdefender Ultimate Small Business Security** och välj **Avinstallera**.
     d. Klick **Avinstallera** igen för att bekräfta ditt val.
     e. Klick **AVLÄGSNA** i fönstret som visas.

f. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

g. Starta om ditt system i normalt läge.

3. Installera om din Bitdefender-produkt.

- **Du hade en annan säkerhetslösning tidigare och du tog inte bort den ordentligt.**
  För att lösa detta:

  1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 115).
  2. Ta bort den andra säkerhetslösningen från ditt system:
     - I **Windows 7**:
       a. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
       b. Hitta namnet på programmet du vill ta bort och välj **Avlägsna**.
       c. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
     - I **Windows 8** och **Windows 8.1**:
       a. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
       b. Klick **Avinstallera ett program** eller **Program och funktioner**.
       c. Hitta namnet på programmet du vill ta bort och välj **Avlägsna**.
       d. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.
     - I **Windows 10** och **Windows 11**:
       a. Klick **Start**, klicka sedan på Inställningar.

b. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.

c. Hitta namnet på programmet du vill ta bort och välj **Avinstallera**.

d. Vänta tills avinstallationsprocessen är klar och starta sedan om systemet.

För att korrekt avinstallera den andra programvaran, gå till deras webbplats och kör deras avinstallationsverktyg eller kontakta dem direkt för att ge dig riktlinjerna för avinstallation.

3. Starta om ditt system i normalt läge och installera om Bitdefender.

Du har redan följt stegen ovan och situationen är inte löst.

För att lösa detta:

1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 115).
2. Använd alternativet Systemåterställning från Windows för att återställa enheten till ett tidigare datum innan du installerar Bitdefender-produkten.
3. Starta om systemet i normalt läge och kontakta våra supportrepresentanter för hjälp enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

3.5.2. Ta bort hot från ditt system

Hot kan påverka ditt system på många olika sätt och Bitdefender-metoden beror på typen av hotattack. Eftersom hot ändrar sitt beteende ofta är det svårt att skapa ett mönster för deras beteende och handlingar.

Det finns situationer när Bitdefender inte automatiskt kan ta bort hotinfektionen från ditt system. I sådana fall krävs ditt ingripande.

- Räddningsmiljö (sida 137)
- Vad ska jag göra när Bitdefender hittar hot på din enhet? (sida 138)
- Hur rensar jag ett hot i ett arkiv? (sida 139)
- Hur rensar jag ett hot i ett e-postarkiv? (sida 140)
- Vad ska jag göra om jag misstänker att en fil är farlig? (sida 141)

- Vilka är de lösenordsskyddade filerna i skanningsloggen? (sida 141)
- Vilka är de överhoppade objekten i skanningsloggen? (sida 142)
- Vilka är de överkomprimerade filerna i skanningsloggen? (sida 142)
- Varför tog Bitdefender automatiskt bort en infekterad fil? (sida 142)

Om du inte kan hitta ditt problem här, eller om de presenterade lösningarna inte löser det, kan du kontakta Bitdefender tekniska supportrepresentanter som presenteras i kapitel Ber om hjälp (sida 273).

Räddningsmiljö

Räddningsmiljö är en Bitdefender-funktion som låter dig skanna och desinficera alla befintliga hårddiskpartitioner i och utanför ditt operativsystem.

Bitdefender Rescue Environment är integrerad med Windows RE.

Starta ditt system i Rescue Environment

Du kan endast gå in i Rescue Environment från din Bitdefender-produkt, enligt följande:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
2. I den **ANTIVIRUS** rutan, klicka **Öppen**.
3. Klick **Öppen** bredvid **Räddningsmiljö**.
4. Klick **STARTA OM** i fönstret som visas.
   Bitdefender Rescue Environment laddas på några ögonblick.

Skanna ditt system i Rescue Environment

För att skanna ditt system Rescue Environment:

1. Gå in i Rescue Environment, som beskrivs i Starta ditt system i Rescue Environment (sida 137).
2. Bitdefender-skanningsprocessen startar automatiskt så snart systemet laddas i Rescue Environment.
3. Vänta tills skanningen är klar. Om något hot upptäcks, följ instruktionerna för att ta bort det.
4. För att avsluta Rescue Environment, klicka på knappen Stäng i fönstret med skanningsresultaten.

Vad ska jag göra när Bitdefender hittar hot på din enhet?

Du kan få reda på att det finns ett hot på din enhet på något av följande sätt:

- Du skannade din enhet och Bitdefender hittade infekterade föremål på den.
- En hotvarning informerar dig om att Bitdefender blockerade ett eller flera hot på din enhet.

I sådana situationer, uppdatera Bitdefender för att se till att du har den senaste hotinformationsdatabasen och kör en systemsökning för att analysera systemet.

Så snart systemgenomsökningen är över, välj önskad åtgärd för de infekterade föremålen (Desinficera, Ta bort, Flytta till karantän).

Varning
Om du misstänker att filen är en del av Windows-operativsystemet eller att den inte är en infekterad fil, följ inte dessa steg och kontakta Bitdefender kundtjänst så snart som möjligt.

Om den valda åtgärden inte kunde vidtas och skanningsloggen avslöjar en infektion som inte kunde raderas, måste du ta bort filen/filerna manuellt:

Den första metoden kan användas i normalt läge:

1. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
2. Visa dolda objekt i Windows. För att ta reda på hur du gör detta, se Hur visar jag dolda objekt i Windows? (sida 114).
3. Bläddra till platsen för den infekterade filen (kontrollera skanningsloggen) och ta bort den.
4. Slå på Bitdefender antivirusskydd i realtid.

Om den första metoden inte lyckades ta bort infektionen:

1. Starta om ditt system och gå in i felsäkert läge. För att ta reda på hur du gör detta, se Hur startar jag om i felsäkert läge? (sida 115).

2. Visa dolda objekt i Windows. För att ta reda på hur du gör detta, se Hur visar jag dolda objekt i Windows? (sida 114).
3. Bläddra till platsen för den infekterade filen (kontrollera skanningsloggen) och ta bort den.
4. Starta om ditt system och gå in i normalt läge.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Hur rensar jag ett hot i ett arkiv?

Ett arkiv är en fil eller en samling filer komprimerade under ett speciellt format för att minska det utrymme på disken som behövs för att lagra filerna.

Vissa av dessa format är öppna format, vilket ger Bitdefender möjlighet att skanna inuti dem och sedan vidta lämpliga åtgärder för att ta bort dem.

Andra arkivformat är delvis eller helt stängda, och Bitdefender kan bara upptäcka förekomsten av hot inuti dem, men kan inte vidta några andra åtgärder.

Om Bitdefender meddelar dig att ett hot har upptäckts i ett arkiv och ingen åtgärd är tillgänglig, betyder det att det inte är möjligt att ta bort hotet på grund av begränsningar i arkivets behörighetsinställningar.

Så här kan du rensa ett hot som lagras i ett arkiv:

1. Identifiera arkivet som innehåller hotet genom att utföra en systemsökning av systemet.
2. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
3. Gå till platsen för arkivet och dekomprimera det med en arkiveringsapp, som WinZip.
4. Identifiera den infekterade filen och ta bort den.
5. Ta bort det ursprungliga arkivet för att se till att infektionen är helt borttagen.

6. Komprimera om filerna i ett nytt arkiv med en arkiveringsapp, som WinZip.
7. Slå på Bitdefender-antivirusskyddet i realtid och kör en systemsökning för att säkerställa att det inte finns någon annan infektion på systemet.

> **Notera**
> Det är viktigt att notera att ett hot som lagras i ett arkiv inte är ett omedelbart hot mot ditt system, eftersom hotet måste dekomprimeras och exekveras för att infektera ditt system.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Hur rensar jag ett hot i ett e-postarkiv?

Bitdefender kan också identifiera hot i e-postdatabaser och e-postarkiv lagrade på disk.

Ibland är det nödvändigt att identifiera det infekterade meddelandet med hjälp av informationen i skanningsrapporten och radera det manuellt.

Så här kan du rensa ett hot som lagras i ett e-postarkiv:

1. Skanna e-postdatabasen med Bitdefender.
2. Stäng av Bitdefender antivirusskydd i realtid:
   a. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnitt.
   b. I den **ANTIVIRUS** rutan, klicka **Öppen**.
   c. I den **Avancerad** fönster, stäng av **Bitdefender Shield**.
3. Öppna skanningsrapporten och använd identifieringsinformationen (Ämne, Från, Till) för de infekterade meddelandena för att hitta dem i e-postklienten.
4. Ta bort de infekterade meddelandena. De flesta e-postklienter flyttar också det raderade meddelandet till en återställningsmapp, från vilken det kan återställas. Du bör se till att meddelandet också raderas från denna återställningsmapp.
5. Komprimera mappen som lagrar det infekterade meddelandet.
   - I Microsoft Outlook 2007: Klicka på Datafilhantering på Arkiv-menyn. Välj de personliga mappfiler (.pst) som du tänker komprimera och klicka på Inställningar. Klicka på Komprimera nu.

- I Microsoft Outlook 2010/2013/2016: På Arkiv-menyn, klicka på Info och sedan Kontoinställningar (Lägg till och ta bort konton eller ändra befintliga anslutningsinställningar). Klicka sedan på Datafil, välj de personliga mappfilerna (.pst) som du tänker komprimera och klicka på Inställningar. Klicka på Komprimera nu.

6. Slå på Bitdefender antivirusskydd i realtid.

Om denna information inte var till hjälp kan du kontakta Bitdefender för support enligt beskrivningen i avsnittet Ber om hjälp (sida 273).

Vad ska jag göra om jag misstänker att en fil är farlig?

Du kan misstänka att en fil från ditt system är farlig, även om din Bitdefender-produkt inte upptäckte den.

För att se till att ditt system är skyddat:

1. Kör a **Genomsökning av systemet** med Bitdefender. För att ta reda på hur du gör detta, se Hur skannar jag mitt system (sida 98).
2. Om skanningsresultatet verkar vara rent, men du fortfarande har tvivel och vill vara säker på filen, kontakta våra supportrepresentanter så att vi kan hjälpa dig.
   För att ta reda på hur du gör detta, se Ber om hjälp (sida 273).

Vilka är de lösenordsskyddade filerna i skanningsloggen?

Detta är bara ett meddelande som indikerar att Bitdefender har upptäckt att dessa filer antingen är skyddade med ett lösenord eller av någon form av kryptering.

Vanligast är de lösenordsskyddade objekten:

- Filer som tillhör en annan säkerhetslösning.
- Filer som tillhör operativsystemet.

För att faktiskt skanna innehållet måste dessa filer antingen extraheras eller på annat sätt dekrypteras.

Skulle innehållet extraheras, skulle Bitdefenders realtidsskanner automatiskt skanna dem för att hålla din enhet skyddad. Om du vill skanna dessa filer med Bitdefender måste du kontakta produkttillverkaren för att ge dig mer information om dessa filer.

Vår rekommendation till dig är att ignorera dessa filer eftersom de inte är ett hot mot ditt system.

Vilka är de överhoppade objekten i skanningsloggen?

Alla filer som visas som överhoppade i skanningsrapporten är rena.

För ökad prestanda skannar inte Bitdefender filer som inte har ändrats sedan den senaste skanningen.

Vilka är de överkomprimerade filerna i skanningsloggen?

De överkomprimerade objekten är element som inte kunde extraheras av skanningsmotorn eller element för vilka dekrypteringstiden skulle ha tagit för lång tid och gjort systemet instabilt.

Överkomprimerad betyder att Bitdefender hoppade över skanningen i det arkivet eftersom uppackning av det visade sig ta för många systemresurser. Innehållet skannas vid realtidsåtkomst om det behövs.

Varför tog Bitdefender automatiskt bort en infekterad fil?

Om en infekterad fil upptäcks kommer Bitdefender automatiskt att försöka desinficera den. Om desinfektionen misslyckas flyttas filen till karantän för att innehålla infektionen.

För särskilda typer av hot är desinficering inte möjlig eftersom den upptäckta filen är helt skadlig. I sådana fall tas den infekterade filen bort från disken.

Detta är vanligtvis fallet med installationsfiler som laddas ner från opålitliga webbplatser. Om du hamnar i en sådan situation, ladda ner installationsfilen från tillverkarens webbplats eller annan pålitlig webbplats.

4. ANTIVIRUS FÖR MAC

4.1. Vad är Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac är en kraftfull antivirusskanner som kan upptäcka och ta bort alla typer av skadlig programvara ("hot"), inklusive:

- ransomware
- adware
- virus
- spionprogram
- Trojaner
- keyloggers
- maskar

Den här appen upptäcker och tar bort inte bara Mac-hot, utan även Windows-hot, vilket förhindrar dig från att av misstag skicka infekterade filer till din familj, vänner och kollegor med hjälp av datorer.

4.2. Installation och borttagning

Det här kapitlet innehåller följande ämnen:

- Systemkrav (sida 143)
- Installerar Bitdefender Antivirus for Mac (sida 144)
- Ta bort Bitdefender Antivirus för Mac (sida 148)

4.2.1. Systemkrav

Du kan installera Bitdefender Antivirus for Mac på Macintosh-datorer som kör OS X Yosemite (10.10) eller nyare versioner.

Din Mac måste också ha minst 1 GB tillgängligt hårddiskutrymme.

En internetanslutning krävs för att registrera och uppdatera Bitdefender Antivirus for Mac.

Notera
Bitdefender Anti-tracker och Bitdefender VPN kan endast installeras på system som kör macOS 10.12 eller nyare versioner.

> **Så här tar du reda på din macOS-version och hårdvaruinformation om din Mac**
>
> Klicka på Apple-ikonen i det övre vänstra hörnet av skärmen och välj Om **Denna Mac**. I fönstret som visas kan du se versionen av ditt operativsystem och annan användbar information. Klick **Systemrapport** för detaljerad hårdvaruinformation.

4.2.2. Installerar Bitdefender Antivirus for Mac

De Bitdefender Antivirus for Mac appen kan installeras från ditt Bitdefender-konto enligt följande:

1. Logga in som administratör.
2. Gå till: https://central.bitdefender.com.
3. Logga in på ditt Bitdefender-konto med din e-postadress och ditt lösenord.
4. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.
5. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Spara installationsfilen.
   - **Skydda andra enheter**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
     b. Klick **SKICKA NEDLADDNINGSLÄNK**.
     c. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**.
     Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.

d. På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.

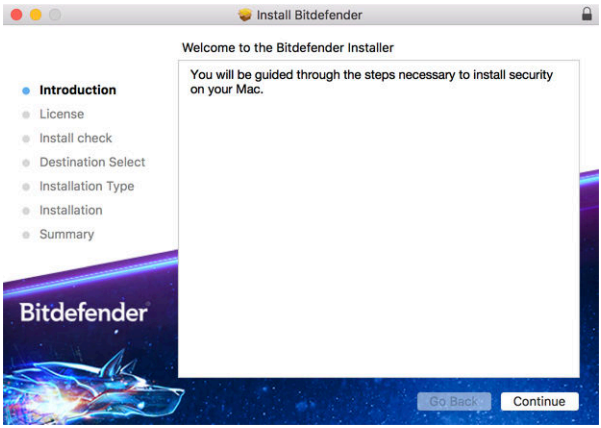
6. Kör Bitdefender-produkten du har laddat ner.
7. Slutför installationsstegen.

Installationsprocess

Att installera Bitdefender Antivirus for Mac:

1. Klicka på den nedladdade filen. Detta kommer att starta installationsprogrammet, som guidar dig genom installationsprocessen.
2. Följ installationsguiden.

Steg 1 - Välkomstfönster



Klick **Fortsätta**.

Steg 2 - Läs prenumerationsavtalet

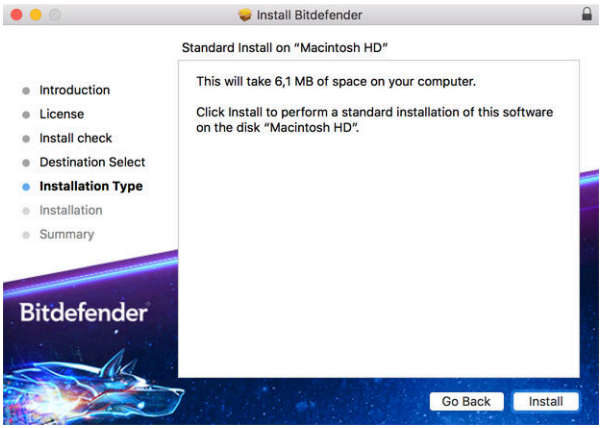
Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren under vilka du får använda Bitdefender Antivirus för Mac.

Från det här fönstret kan du också välja vilket språk du vill installera produkten på.

Klick **Fortsätta**, och klicka sedan **Hålla med**.

> **Viktig**
> Om du inte godkänner dessa villkor, klicka **Fortsätta**, och klicka sedan **Instämmer inte alls** för att avbryta installationen och avsluta installationsprogrammet.

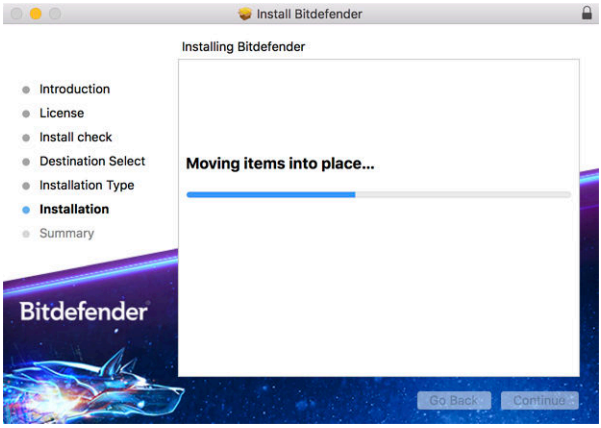
Steg 3 - Starta installationen



Bitdefender Antivirus för Mac kommer att installeras i Macintosh HD/Library/Bitdefender. Installationssökvägen kan inte ändras.

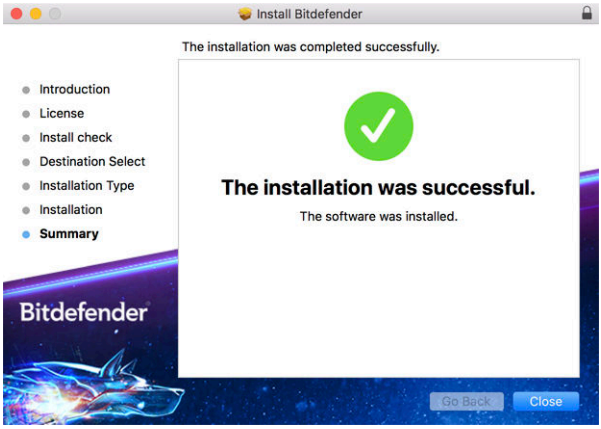
Klick **Installera** för att starta installationen.

Steg 4 - Installera Bitdefender Antivirus för Mac



Vänta tills installationen är klar och klicka sedan **Fortsätta**.

Steg 5 - Avsluta



Klick **Stänga** för att stänga installationsfönstret.

Installationsprocessen är nu klar.

Viktig

- Om du installerar Bitdefender Antivirus för Mac på macOS High Sierra 10.13.0 eller en nyare version, **Systemtillägg blockerat** meddelande visas. Det här meddelandet informerar dig om att tilläggen signerade av Bitdefender har blockerats och måste aktiveras manuellt. Klicka på OK för att fortsätta. I Bitdefender Antivirus för Mac-fönstret som visas klickar du på **Säkerhet och integritet** länk. Klick **Tillåta** i den nedre delen av fönstret, eller välj Bitdefender SRL från listan och klicka sedan **OK**.
- Om du installerar Bitdefender Antivirus för Mac på macOS Mojave 10.14 eller en nyare version kommer ett nytt fönster att visas som informerar dig om att du måste **Ge Bitdefender full diskåtkomst** och **Tillåt Bitdefender att ladda**. Följ instruktionerna på skärmen för att konfigurera produkten korrekt.

4.2.3. Ta bort Bitdefender Antivirus för Mac

Eftersom det är en komplex app kan Bitdefender Antivirus för Mac inte tas bort på vanligt sätt genom att dra appikonen från *Ansökningar* mappen till papperskorgen.

För att ta bort Bitdefender Antivirus för Mac, följ dessa steg:

1. Öppna a **Upphittare** fönstret och gå sedan till *Ansökningar* mapp.
2. Öppna Bitdefender-mappen i Applications, och dubbelklicka sedan **BitdefenderUninstaller**.
3. Välj önskat avinstallationsalternativ.

   Notera
   Om du försöker ta bort bara Bitdefender VPN-appen väljer du **Avinstallera VPN** endast.

4. Klick **Avinstallera** och vänta på att processen ska slutföras.
5. Klick **Stänga** att avsluta.

   Viktig
   Om det finns ett fel kan du kontakta Bitdefender kundtjänst enligt beskrivningen i Ber om hjälp (sida 273).

4.3. Komma igång

Det här kapitlet innehåller följande ämnen:

- Öppna Bitdefender Antivirus för Mac (sida 149)
- Appens huvudfönster (sida 150)
- App Dock-ikon (sida 151)
- Navigeringsmeny (sida 151)
- Mörkt läge (sida 152)

4.3.1. Öppna Bitdefender Antivirus för Mac

Du har flera sätt att öppna Bitdefender Antivirus för Mac.

- Klicka på Bitdefender Antivirus för Mac-ikonen i startfältet.
- Klicka på ikonen i menyraden och välj **Öppna Antivirus-gränssnittet**.
- Öppna ett Finder-fönster, gå till Applications och dubbelklicka på ikonen **Bitdefender Antivirus för Mac**.

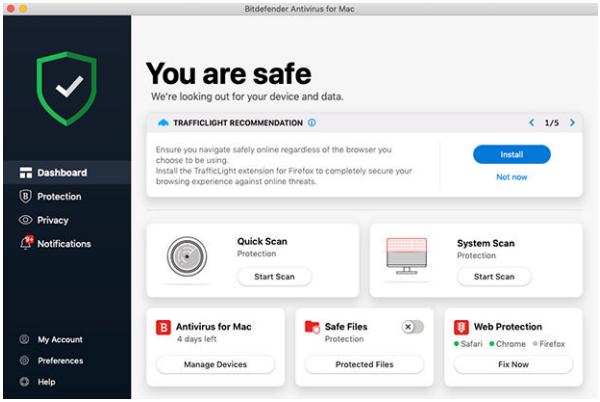
Viktig

Första gången du öppnar Bitdefender Antivirus för Mac på macOS Mojave 10.14 eller en nyare version visas en skyddsrekommendation. Den här rekommendationen visas eftersom vi behöver behörighet för att skanna hela ditt system efter hot. För att ge oss behörigheter måste du vara inloggad som administratör och följa dessa steg:

1. Klicka på **Systeminställningar** länk.
2. Klicka på ikonen och skriv sedan in dina administratörsuppgifter.
3. Ett nytt fönster öppnas. Dra **BDLDaemon** filen till listan över tillåtna appar.

4.3.2. Appens huvudfönster

Bitdefender Antivirus för Mac möter behoven hos både datornybörjare och mycket tekniska personer. Dess grafiska användargränssnitt är utformat för att passa varje kategori av användare.



För att gå igenom Bitdefender-gränssnittet visas en introduktionsguide som innehåller information om hur man interagerar med produkten och hur man konfigurerar den på den övre vänstra sidan. Välj den räta vinkeln för att fortsätta guidas, eller **Skippa rundtur** för att stänga guiden.

Statusfältet överst i fönstret informerar dig om systemets säkerhetsstatus med hjälp av explicita meddelanden och suggestiva färger. Om Bitdefender Antivirus för Mac inte har några varningar är statusfältet grönt. När ett säkerhetsproblem har upptäckts ändrar statusfältet sin färg

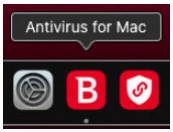
till rött. För detaljerad information om problem och hur du åtgärdar dem, se Åtgärda problem (sida 164).

För att erbjuda dig en effektiv operation och ökat skydd samtidigt som du utför olika aktiviteter, **Bitdefender autopilot** kommer att fungera som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, antingen arbetar du eller gör onlinebetalningar Bitdefender Autopilot kommer med kontextuella rekommendationer baserat på din enhetsanvändning och behov. Detta hjälper dig att upptäcka och dra nytta av fördelarna med funktionerna som ingår i Bitdefender Antivirus för Mac-appen.

Från navigeringsmenyn på vänster sida kan du komma åt Bitdefender-sektionerna för detaljerad konfiguration och avancerade administrativa uppgifter (**Skydd** och **Integritet** flikar), aviseringar, din Bitdefender-konto och den Inställningar område. Du kan också kontakta oss (**Hjälp** fliken) för support om du har frågor eller något oväntat dyker upp.

4.3.3. App Dock-ikon

Bitdefender Antivirus för Mac-ikonen kan ses i Dock så snart du öppnar appen. Ikonen i Dock ger dig ett enkelt sätt att skanna filer och mappar efter hot. Dra och släpp filen eller mappen över Dock-ikonen så startar skanningen omedelbart.



4.3.4. Navigeringsmeny

På vänster sida på Bitdefender-gränssnittet finns navigeringsmenyn, som gör att du snabbt kan komma åt Bitdefender-funktionerna du behöver för att hantera din produkt. Flikarna som är tillgängliga i det här området är:

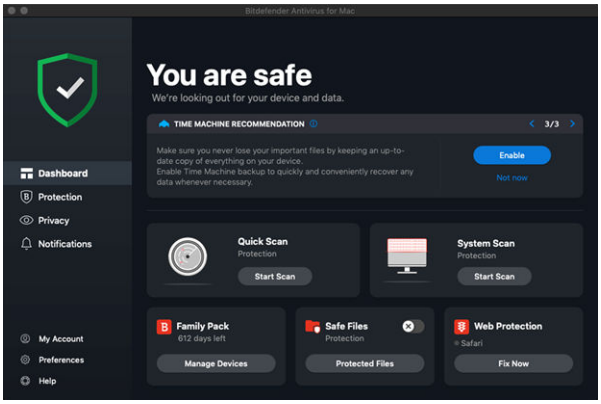
- **instrumentbräda**. Härifrån kan du snabbt fixa säkerhetsproblem, visa rekommendationer enligt dina systembehov och användningsmönster, utföra snabba åtgärder och gå till ditt Bitdefender-konto för att hantera de enheter du har lagt till i ditt Bitdefender-abonnemang.
- **Skydd**. Härifrån kan du starta antivirusgenomsökningar, lägga till filer i undantagslistan, skydda filer och appar från ransomware-

attacker, säkra dina Time Machine-säkerhetskopior och konfigurera skydd när du surfar på internet.

- **Integritet**. Härifrån kan du öppna Bitdefender VPN-appen och installera Anti-tracker-tillägget i din webbläsare.
- **Aviseringar**. Härifrån kan du se detaljer om de åtgärder som vidtagits på skannade filer.
- **Mitt konto**. Härifrån kan du se Bitdefender-kontot och prenumerationen som din enhet skyddas av, samt byta konto om det behövs.
- **Inställningar**. Härifrån kan du konfigurera Bitdefender-inställningarna.
- **Hjälp**. Härifrån, närhelst du behöver hjälp med att lösa en situation med din Bitdefender-produkt, kan du kontakta avdelningen för teknisk support. Du kan också skicka oss din feedback för att hjälpa oss att förbättra produkten.

4.3.5. Mörkt läge

För att ge dina ögon skydd mot bländning och ljus när du arbetar på natten eller i ett ljusfritt tillstånd, stöder Bitdefender Antivirus för Mac Dark Mode för Mojave 10.14 och senare. Färgerna på gränssnittet har optimerats så att du kan använda din Mac utan att anstränga ögonen. Bitdefender Antivirus för Mac-gränssnittet justerar sig själv beroende på enhetens utseendeinställningar.



4.4. Skydda mot skadlig programvara

Det här kapitlet innehåller följande ämnen:

- Bästa metoder (sida 153)
- Skanna din Mac (sida 154)
- Scan Wizard (sida 155)
- Karantän (sida 156)
- Bitdefender Shield (realtidsskydd) (sida 157)
- Scan Undantag (sida 158)
- Nätskydd (sida 159)
- Antispårare (sida 160)
- Säkra filer (sida 162)
- Time Machine-skydd (sida 164)
- Åtgärda problem (sida 164)
- Aviseringar (sida 166)
- Uppdateringar (sida 166)

4.4.1. Bästa metoder

För att hålla ditt system skyddat mot hot och för att förhindra oavsiktlig infektion av andra system, följ dessa bästa metoder:

- Ha kvar **Bitdefender Shield** aktiverat för att tillåta att systemfiler automatiskt skannas av Bitdefender Antivirus för Mac.
- Håll din Bitdefender Antivirus för Mac-produkt uppdaterad med den senaste hotinformationen och produktuppdateringarna.
- Kontrollera och åtgärda problemen som rapporterats av Bitdefender Antivirus för Mac regelbundet. För detaljerad information, se Åtgärda problem (sida 164).
- Kontrollera den detaljerade loggen över händelser som rör Bitdefender Antivirus för Mac-aktiviteten på din dator. Närhelst något som är relevant för säkerheten för ditt system eller data inträffar läggs ett nytt meddelande till i Bitdefender-meddelandeområdet. För mer information, gå till Aviseringar (sida 166).
- Du bör också följa dessa bästa metoder:
  - Ta för vana att skanna filer som du laddar ner från ett externt lagringsminne (som ett USB-minne eller en CD), särskilt när du inte känner till källan.
  - Om du har en DMG-fil, montera den och skanna sedan dess innehåll (filerna i den monterade volymen/bilden).

  Det enklaste sättet att skanna en fil, en mapp eller en volym är att dra och släppa den över Bitdefender Antivirus för Mac-fönstret eller Dock-ikonen.

Ingen annan konfiguration eller åtgärd krävs. Men om du vill kan du justera appinställningarna och inställningarna för att bättre passa dina behov. För mer information, se Konfigurera inställningar (sida 168).

4.4.2. Skanna din Mac

Förutom **Bitdefender Shield** funktion, som övervakar de installerade apparna regelbundet, letar efter hotliknande åtgärder och förhindrar nya hot från att komma in i ditt system. Du kan skanna din Mac eller specifika filer när du vill.

Det enklaste sättet att skanna en fil, en mapp eller en volym är att dra och släppa den över Bitdefender Antivirus för Mac-fönstret eller Dock-ikonen. Skanningsguiden visas och guidar dig genom skanningsprocessen.

Du kan också starta en skanning enligt följande:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Antivirus** flik.
3. Klicka på en av de tre skanningsknapparna för att starta den önskade skanningen.
   - **Snabbskanning** - söker efter hot på de mest sårbara platserna på ditt system (till exempel mapparna som innehåller dokument, nedladdningar, e-postnedladdningar och temporära filer för varje användare).
   - **Genomsökning av systemet** - utför en omfattande kontroll av hot från hela systemet. Alla anslutna fästen skannas också.

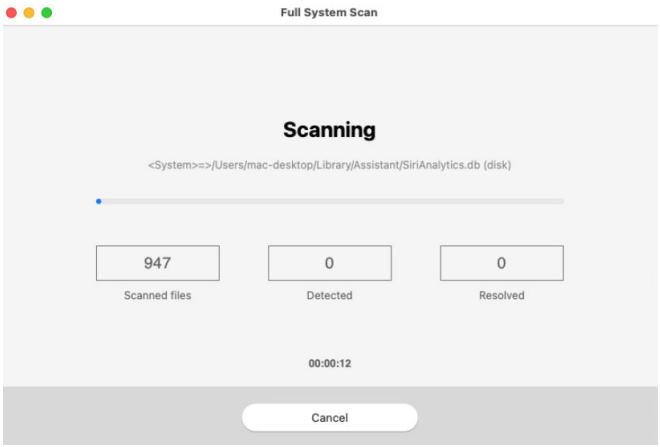
     > **Notera**
     > Beroende på storleken på din hårddisk kan det ta en stund att skanna hela systemet (upp till en timme eller till och med mer). För förbättrad prestanda rekommenderas att du inte kör den här uppgiften medan du utför andra resurskrävande uppgifter (som videoredigering).
     >
     > Om du föredrar det kan du välja att inte skanna specifika monterade volymer genom att lägga till dem i Undantag lista från skyddsfönstret.

   - **Anpassad skanning** - hjälper dig att kontrollera specifika filer, mappar eller volymer för hot.

Du kan också starta ett system eller en snabbsökning från Dashboard.

4.4.3. Scan Wizard

När du initierar en skanning visas skanningsguiden för Bitdefender Antivirus för Mac.



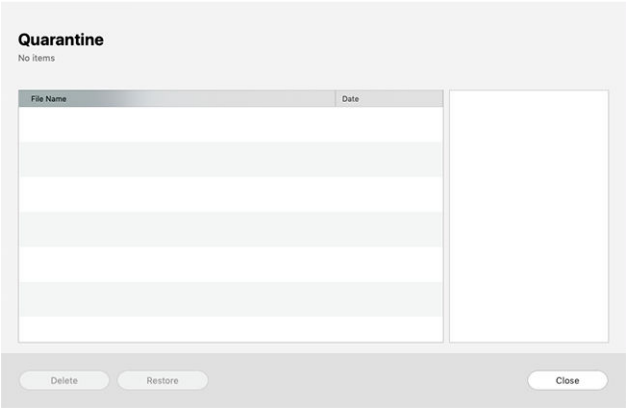
Realtidsinformation om upptäckta och lösta hot visas under varje skanning.

Vänta tills Bitdefender Antivirus för Mac ska avslutas.

> **Notera**
> Skanningsprocessen kan ta ett tag, beroende på hur komplex skanningen är.

4.4.4. Karantän

Bitdefender Antivirus för Mac gör det möjligt att isolera de infekterade eller misstänkta filerna i ett säkert område, kallat karantän. När ett hot är i karantän kan det inte göra någon skada eftersom det inte kan verkställas eller läsas.



Avsnittet Karantän visar alla filer som för närvarande är isolerade i karantänmappen.

För att ta bort en fil från karantänen, välj den och klicka **Radera**. Om du vill återställa en fil i karantän till sin ursprungliga plats, välj den och klicka **Återställ**.

Så här visar du en lista med alla objekt som lagts till i karantänen:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Klick **Öppen** i **Karantän** rutan.

4.4.5. Bitdefender Shield (realtidsskydd)

Bitdefender ger realtidsskydd mot ett brett utbud av hot genom att skanna alla installerade appar, deras uppdaterade versioner och nya och modifierade filer.

Så här inaktiverar du realtidsskyddet:

1. Klick **Inställningar** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Stäng av **Bitdefender Shield** i **Skydd** fönster.

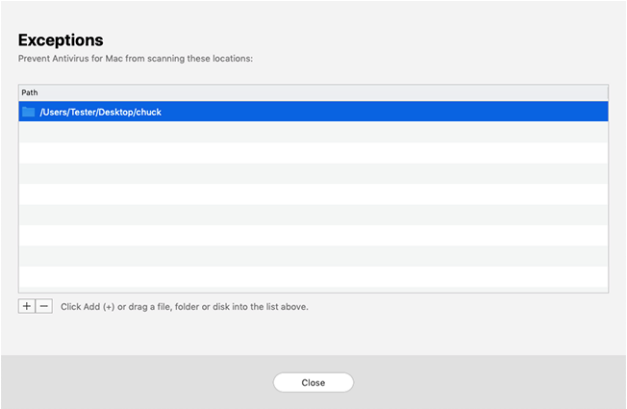
Varning

Detta är en kritisk säkerhetsfråga. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat kommer du inte att skyddas mot hot.

4.4.6. Scan Undantag

Om du vill kan du ställa in Bitdefender Antivirus för Mac att inte skanna specifika filer, mappar eller ens en hel volym. Du kanske till exempel vill utesluta från skanning:

- Filer som av misstag identifieras som infekterade (kända som falska positiva)
- Filer som orsakar skanningsfel
- Säkerhetskopieringsvolymer



Undantagslistan innehåller de sökvägar som har undantagits från skanning.

För att komma åt undantagslistan:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Klick **Öppen** i **Undantag** rutan.

Det finns två sätt att ställa in ett skanningsundantag:

- Dra och släpp en fil, mapp eller volym över undantagslistan.
- Klicka på knappen märkt med plustecknet (+), som finns under undantagslistan. Välj sedan den fil, mapp eller volym som ska undantas från skanning.

För att ta bort ett skanningsundantag, välj det från listan och klicka på knappen märkt med minustecknet (-), som finns under undantagslistan.

4.4.7. Nätskydd

Bitdefender Antivirus för Mac använder TrafficLight-tilläggen för att helt säkra din webbupplevelse. TrafficLight-tilläggen fångar upp, bearbetar och filtrerar all webbtrafik och blockerar skadligt innehåll.

Tilläggen fungerar och integreras med följande webbläsare: Mozilla Firefox, Google Chrome och Safari.

Aktiverar TrafficLight-tillägg

Så här aktiverar du TrafficLight-tilläggen:

1. Klick **Fixa nu** i **Nätskydd** kort på instrumentpanelen.
2. De **Nätskydd** fönstret öppnas.
   Den upptäckta webbläsaren som du har installerat på ditt system visas. Klicka på för att installera TrafficLight-tillägget i din webbläsare **Skaffa förlängning**.
3. Du omdirigeras till:
   https://bitdefender.com/solutions/trafficlight.html
4. Välj **Gratis nedladdning**.
5. Följ stegen för att installera TrafficLight-tillägget som motsvarar din webbläsare.

Hantera tilläggsinställningar

En rad funktioner finns tillgängliga för att skydda dig från alla typer av hot du kan stöta på när du surfar på webben. För att komma åt dem, klicka på TrafficLight-ikonen bredvid din webbläsares inställningar och klicka sedan på ⚙ **inställningar** knapp:

- **Bitdefender TrafficLight-inställningar**
  - Webbskydd – hindrar dig från att komma åt webbplatser som används för skadlig programvara, nätfiske och bedrägerisattacker.
  - Search Advisor - ger förvarning för riskfyllda webbplatser i dina sökresultat.
- **Undantag**
  Om du är på webbplatsen du vill lägga till undantag klickar du på **Lägg till aktuell webbplats till listan**.

Om du vill lägga till en annan webbplats anger du dess adress i motsvarande fält och klickar sedan ⊕.
Ingen varning kommer att visas om hot förekommer på de undantagna sidorna. Det är därför endast webbplatser du litar på bör läggas till i den här listan.

Sidbetyg och varningar

Beroende på hur TrafficLight klassificerar webbsidan du för närvarande visar, visas en av följande ikoner i dess område:

Det här är en säker sida att besöka. Du kan fortsätta ditt arbete.

Den här webbsidan kan innehålla farligt innehåll. Var försiktig om du bestämmer dig för att besöka den.

Du bör lämna webbsidan omedelbart eftersom den innehåller skadlig programvara eller andra hot.

I Safari är bakgrunden för TrafficLight-ikonerna svart.

4.4.8. Antispårare

Många webbplatser du besöker använder spårare för att samla in information om ditt beteende, antingen för att dela den med tredjepartsföretag eller för att visa annonser som är mer relevanta för dig. Härmed tjänar webbplatsägare pengar för att kunna ge dig innehåll gratis eller fortsätta att fungera. Förutom att samla in information kan spårare sakta ner din surfupplevelse eller slösa bort din bandbredd.

Med Bitdefender Anti-tracker-tillägget aktiverat i din webbläsare undviker du att bli spårad så att dina data förblir privata medan du surfar online och du påskyndar den tid som webbplatser behöver laddas.

Bitdefender-tillägget är kompatibelt med följande webbläsare:

- Google Chrome
- Mozilla Firefox
- Safari

De spårare vi upptäcker är grupperade i följande kategorier:

- **Reklam** - används för att analysera webbplatstrafik, användarbeteende eller besökarnas trafikmönster.

- **Kundinteraktion** - används för att mäta användarinteraktion med olika inmatningsformer som chatt eller support.
- **Grundläggande** - används för att övervaka viktiga webbsidors funktioner.
- **Webbplatsanalys** - används för att samla in data om webbsidaanvändning.
- **Sociala media** - används för att övervaka social publik, aktivitet och användarengagemang med olika sociala medieplattformar.

Aktiverar Bitdefender Anti-tracker

Så här aktiverar du Bitdefender Anti-tracker-tillägget i din webbläsare:

1. Klick **Integritet** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Antispårare** flik.
3. Klick **Aktivera tillägg** bredvid webbläsaren som du vill aktivera tillägget för.

Anti-tracker gränssnitt

När Bitdefender Anti-tracker-tillägget är aktiverat, visas bredvid sökfältet i din webbläsare. Varje gång du besöker en webbplats kan en räknare märkas på ikonen som hänvisar till de upptäckta och blockerade spårarna. För att se mer information om de blockerade spårarna, klicka på ikonen för att öppna gränssnittet. Förutom antalet blockerade spårare kan du se hur lång tid det tar för sidan att ladda och kategorierna som de upptäckta spårarna tillhör. För att se listan över webbplatser som spårar, klicka på önskad kategori.

För att inaktivera Bitdefender från att blockera spårare på webbplatsen du för närvarande besöker, klicka **Pausa skyddet på denna webbplats**. Den här inställningen gäller bara så länge du har webbplatsen öppen och kommer att återställas till det ursprungliga tillståndet när du stänger webbplatsen.

För att tillåta spårare från en specifik kategori att övervaka din aktivitet, klicka på önskad aktivitet och klicka sedan på motsvarande knapp. Om du ändrar dig, klicka på samma knapp en gång till.

Stänger av Bitdefender Anti-tracker

Så här stänger du av Bitdefender Anti-tracker från din webbläsare:

1. Öppna din webbläsare.
2. Klicka på ikonen bredvid adressfältet i din webbläsare.
3. Klicka på ikonen i det övre högra hörnet.
4. Använd motsvarande strömbrytare för att stänga av.
   Bitdefender-ikonen blir grå.

Tillåter att en webbplats spåras

Om du vill bli spårad när du besöker en viss webbplats kan du lägga till dess adress till undantag enligt följande:

1. Öppna din webbläsare.
2. Klicka på ikonen bredvid sökfältet.
3. Klicka på ikonen i det övre högra hörnet.
4. Om du är på webbplatsen du vill lägga till undantag klickar du på **Lägg till aktuell webbplats till listan**.
   Om du vill lägga till en annan webbplats anger du dess adress i motsvarande fält och klickar sedan .

4.4.9. Säkra filer

Ransomware är en skadlig programvara som attackerar sårbara system genom att låsa dem, och ber om pengar för att låta användaren ta tillbaka kontrollen över sitt system. Denna skadliga programvara agerar intelligent genom att visa falska meddelanden för att få användaren i panik, och uppmanar honom att fortsätta med den begärda betalningen.

Genom att använda den senaste tekniken säkerställer Bitdefender systemets integritet genom att skydda kritiska systemområden mot ransomware-attacker utan att påverka systemet. Men du kanske också vill skydda dina personliga filer som dokument, foton eller filmer från att nås av opålitliga appar. Med Bitdefender Safe Files kan du placera personliga filer till ett skydd och konfigurera på egen hand vilka appar som ska tillåtas göra ändringar i de skyddade filerna och vilka som inte ska göra det.

Så här lägger du till filer i den skyddade miljön:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.

2. Välj **Anti-Ransomware** flik.
3. Klick **Skyddade filer** i området Säkra filer.
4. Klicka på knappen märkt med plustecknet (+), som finns under listan med skyddade filer. Välj sedan filen, mappen eller volymen som ska skyddas ifall ransomware-attacker försöker komma åt dem.

För att undvika att systemet går långsammare rekommenderar vi att du lägger till maximalt 30 mappar eller sparar flera filer i en enda mapp.

Som standard är mapparna Bilder, Dokument, Skrivbord och Nedladdningar skyddade mot hotattacker.

> **Notera**
> Anpassade mappar kan endast skyddas för nuvarande användare. Externa enheter, system- och appfiler kan inte läggas till i skyddsmiljön.

Du kommer att informeras varje gång en okänd app med ett ovanligt beteende försöker ändra filerna du lagt till. Klick **Tillåta** eller **Blockera** för att lägga till den i Hantera applikationer lista.

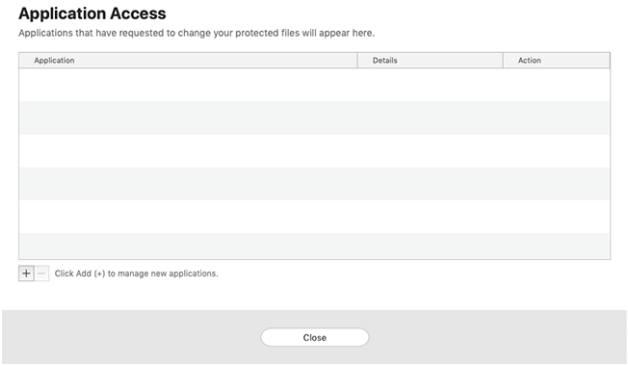
Tillgång till applikationer

De appar som försöker ändra eller ta bort skyddade filer kan flaggas som potentiellt osäkra och läggas till i listan med blockerade appar. Om en sådan app är blockerad och du är säker på att dess beteende är normalt kan du tillåta det genom att följa dessa steg:

1. Klick **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Anti-Ransomware** flik.
3. Klick **Applikationsåtkomst** i området Säkra filer.
4. Ändra statusen till Tillåt bredvid den blockerade appen.

Appar som är inställda på Tillåt kan också ställas in på Blockerade.

Använd dra och släpp-metoden eller klicka på plustecknet (+) för att lägga till fler appar i listan.



4.4.10. Time Machine-skydd

Bitdefender Time Machine Protection fungerar som ett extra lager av säkerhet för din säkerhetskopieringsenhet, inklusive alla filer du har bestämt dig för att lagra i den, genom att blockera åtkomsten för någon extern källa. Om filer från din Time Machine-enhet kommer att krypteras med ransomware, kommer du att kunna återställa dem utan att betala för den begärda lösen.

Om du behöver återställa objekt från en Time Machine-säkerhetskopia, kolla Apples supportsida för instruktioner.

Slå på eller av Time Machine Protection

Så här slår du på eller av inaktiverar Time Machine Protection:

1. Klick **Skydd** på navigeringsmenyn på **Bitdefender-gränssnitt**.
2. Välj **Anti-Ransomware** flik.
3. Aktivera eller inaktivera **Time Machine-skydd** växla.

4.4.11. Åtgärda problem

Bitdefender Antivirus för Mac upptäcker och informerar dig automatiskt om en rad problem som kan påverka säkerheten för ditt system och dina data. På så sätt kan du åtgärda säkerhetsrisker enkelt och i rätt tid.

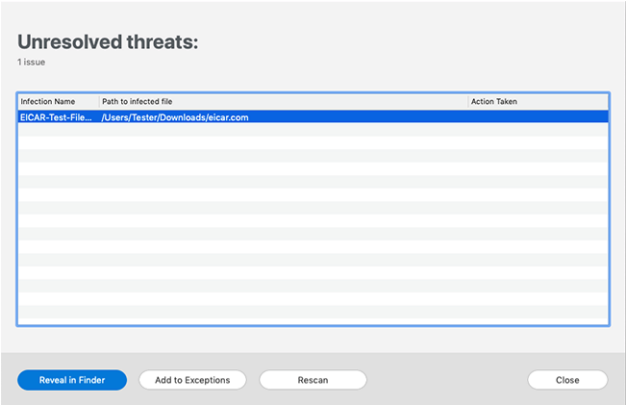
Att åtgärda problemen som indikeras av Bitdefender Antivirus för Mac är ett snabbt och enkelt sätt att säkerställa optimalt skydd av ditt system och dina data.

Upptäckta problem inkluderar:

- Den nya hotinformationsuppdateringen laddades inte ner från våra servrar.
- Hot har upptäckts på ditt system och produkten kan inte desinficera dem automatiskt.
- Realtidsskyddet är inaktiverat.

Så här kontrollerar och åtgärdar du upptäckta problem:

1. Om Bitdefender inte har några varningar är statusfältet grönt. När ett säkerhetsproblem har upptäckts ändrar statusfältet sin färg till rött.
2. Se beskrivningen för mer information.
3. När ett problem upptäcks klickar du på motsvarande knapp för att vidta åtgärder.



Listan över olösta hot uppdateras efter varje systemgenomsökning oavsett om genomsökningen görs automatiskt i bakgrunden eller initieras av dig.

Du kan välja att vidta följande åtgärder för olösta hot:

- Radera manuellt. Vidta den här åtgärden för att ta bort infektionerna manuellt.
- Lägg till i undantag. Den här åtgärden är inte tillgänglig för hot som finns i arkiv.

4.4.12. Aviseringar

Bitdefender håller en detaljerad logg över händelser som rör dess aktivitet på din dator. Närhelst något som är relevant för säkerheten för ditt system eller data inträffar läggs ett nytt meddelande till i Bitdefender-meddelandeområdet, på liknande sätt som ett nytt e-postmeddelande som visas i din inkorg.

Meddelanden är ett viktigt verktyg för att övervaka och hantera ditt Bitdefender-skydd. Du kan till exempel enkelt kontrollera om uppdateringen genomfördes framgångsrikt, om hot eller sårbarheter hittades på din dator, etc. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som Bitdefender vidtar.

Klicka på för att komma åt meddelandeloggen **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnittet. Varje gång en kritisk händelse inträffar kan en räknare märkas på ikon.

Beroende på typ och svårighetsgrad grupperas meddelanden i:

- **Kritisk** händelser indikerar kritiska problem. Du bör kontrollera dem omedelbart.
- **Varning** händelser indikerar icke-kritiska frågor. Du bör kontrollera och fixa dem när du har tid.
- **Information** händelser indikerar framgångsrika operationer.

Klicka på varje flik för att hitta mer information om de genererade händelserna. Korta detaljer visas med ett enda klick på varje händelsetitel, nämligen: en kort beskrivning, åtgärden Bitdefender vidtog när den hände och datum och tid när den inträffade. Alternativ kan tillhandahållas för att vidta ytterligare åtgärder vid behov.

För att hjälpa dig att enkelt hantera loggade händelser, ger meddelandefönstret alternativ för att ta bort eller markera som lästa alla händelser i det avsnittet.

4.4.13. Uppdateringar

Nya hot hittas och identifieras varje dag. Det är därför det är mycket viktigt att hålla Bitdefender Antivirus för Mac uppdaterad med de senaste hotinformationsuppdateringarna.

Hotinformationsuppdateringarna utförs i farten, vilket innebär att filerna som ska uppdateras ersätts successivt. På detta sätt kommer

uppdateringen inte att påverka produktens funktion och samtidigt kommer alla sårbarheter att undantas.

- Om Bitdefender Antivirus för Mac är uppdaterad kan det upptäcka de senaste hoten som upptäckts och rensa de infekterade filerna.
- Om Bitdefender Antivirus för Mac inte är uppdaterad kommer det inte att kunna upptäcka och ta bort de senaste hoten som upptäckts av Bitdefender Labs.

Begär en uppdatering

Du kan begära en uppdatering manuellt när du vill.

En aktiv internetanslutning krävs för att söka efter tillgängliga uppdateringar och ladda ner dem.

Så här begär du en uppdatering manuellt:

1. Klicka på **Handlingar** knappen i menyraden.
2. Välja **Uppdatera databas för hotinformation**.

Alternativt kan du begära en uppdatering manuellt genom att trycka på CMD + U.

Du kan se uppdateringsförloppet och nedladdade filer.

Få uppdateringar via en proxyserver

Bitdefender Antivirus för Mac kan endast uppdateras via proxyservrar som inte kräver autentisering. Du behöver inte konfigurera några programinställningar.

Om du ansluter till internet via en proxyserver som kräver autentisering måste du byta till en direkt internetanslutning regelbundet för att få uppdateringar av hotinformation.

Uppgradera till en ny version

Ibland lanserar vi produktuppdateringar för att lägga till nya funktioner och förbättringar eller åtgärda produktproblem. Dessa uppdateringar kan kräva en omstart av systemet för att initiera installationen av nya filer. Som standard, om en uppdatering kräver omstart av datorn, fortsätter Bitdefender Antivirus för Mac att arbeta med de tidigare filerna tills du startar om systemet. I det här fallet kommer uppdateringsprocessen inte att störa användarens arbete.

När en produktuppdatering är klar kommer ett popup-fönster att informera dig om att starta om systemet. Om du missar det här meddelandet kan du antingen klicka **Starta om för att uppgradera** från menyraden eller starta om systemet manuellt.

Hitta information om Bitdefender Antivirus för Mac

För att hitta information om Bitdefender Antivirus för Mac-versionen som du har installerat, gå till **Handla om** fönster. I samma fönster kan du komma åt och se prenumerationsavtalet, sekretesspolicyn och licenser för öppen källkod.

För att komma åt Om-fönstret:

1. Öppna Bitdefender Antivirus för Mac.
2. Klicka på Bitdefender Antivirus för Mac i menyraden och välj **Om Antivirus för Mac**.

4.5. Konfigurera inställningar

Det här kapitlet innehåller följande ämnen:

- Åtkomst till inställningar (sida 168)
- Skyddsinställningar (sida 168)
- Avancerade inställningar (sida 169)
- Specialerbjudanden (sida 170)

4.5.1. Åtkomst till inställningar

Så här öppnar du fönstret Bitdefender Antivirus för Mac-inställningar:

- Gör något av följande:
  - Klick **Inställningar** på navigeringsmenyn på Bitdefender-gränssnittet.
  - Klicka på Bitdefender Antivirus för Mac i menyraden och välj **Inställningar**.

4.5.2. Skyddsinställningar

Fönstret med skyddsinställningar låter dig konfigurera den övergripande skanningsmetoden. Du kan konfigurera de åtgärder som vidtas på

de upptäckta infekterade och misstänkta filerna och andra allmänna inställningar.

- **Bitdefender Shield.** Bitdefender Shield ger realtidsskydd mot ett brett utbud av hot genom att skanna alla installerade appar, deras uppdaterade versioner och nya och modifierade filer. Vi rekommenderar inte att du inaktiverar Bitdefender Shield, men om du måste, gör det så kort tid som möjligt. Om Bitdefender Shield är inaktiverat kommer du inte att skyddas mot hot.
- **Skanna endast nya och ändrade filer.** Markera den här kryssrutan för att ställa in Bitdefender Antivirus för Mac att endast skanna filer som inte har skannats tidigare eller som har ändrats sedan den senaste genomsökningen.
  Du kan välja att inte använda den här inställningen för anpassad och dra och släpp skanning genom att avmarkera motsvarande kryssruta.
- **Skanna inte innehåll i säkerhetskopior.** Markera den här kryssrutan för att utesluta säkerhetskopior från genomsökning. Om de infekterade filerna återställs vid ett senare tillfälle kommer Bitdefender Antivirus för Mac automatiskt att upptäcka dem och vidta lämpliga åtgärder.

4.5.3. Avancerade inställningar

Du kan välja en övergripande åtgärd som ska vidtas för alla problem och misstänkta föremål som hittas under en skanningsprocess.

Åtgärd för infekterade föremål

- **Försök att desinficera eller flytta till karantän** - Om infekterade filer upptäcks kommer Bitdefender att försöka desinficera dem (ta bort den skadliga koden) eller flytta dem till karantän.
- **Gör inga åtgärder** - Inga åtgärder kommer att vidtas på de upptäckta filerna.

Åtgärd för misstänkta föremål

- **Flytta filer till karantän** - Om misstänkta filer upptäcks kommer Bitdefender att flytta dem till karantän.
- **Gör inga åtgärder** - Inga åtgärder kommer att vidtas på de upptäckta filerna.

4.5.4. Specialerbjudanden

När kampanjerbjudanden är tillgängliga är Bitdefender-produkten inställd för att meddela dig via ett popup-fönster. Detta ger dig möjlighet att dra nytta av förmånliga priser och hålla dina enheter skyddade under en längre tid.

Så här aktiverar eller inaktiverar du aviseringar om specialerbjudanden:

1. Klick **Inställningar** på navigeringsmenyn på Bitdefender-gränssnittet.
2. Välj **Övrig** flik.
3. Slå på eller av **Mina erbjudanden** växla.

> **Notera**
> De **Mina erbjudanden** alternativet är aktiverat som standard.

4.6. Vanliga frågor

Hur kan jag prova Bitdefender Antivirus för Mac innan jag ansöker om en prenumeration?

Du är en ny kund hos Bitdefender och skulle vilja prova vår produkt innan du köper den. Provperioden är 30 dagar och du kan fortsätta använda den installerade produkten endast om du köper ett Bitdefender-abonnemang. För att prova Bitdefender Antivirus för Mac måste du:

1. Skapa ett Bitdefender-konto genom att följa dessa steg:
   a. Gå till: https://central.bitdefender.com.
   b. Skriv in den information som krävs i motsvarande fält. De uppgifter du lämnar här kommer att förbli konfidentiella.
   c. Innan du går vidare måste du godkänna användarvillkoren. Gå till användarvillkoren och läs dem noggrant eftersom de innehåller villkoren under vilka du får använda Bitdefender.
      Dessutom kan du komma åt och läsa sekretesspolicyn.
   d. Klick **SKAPA KONTO**.
2. Ladda ner Bitdefender Antivirus för Mac enligt följande:
   a. Välj **Mina enheter** panelen och klicka sedan på **INSTALLATIONSSKYDD**.

b. Välj ett av de två tillgängliga alternativen:

- **Skydda den här enheten**
  i. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
  ii. Spara installationsfilen.

- **Skydda andra enheter**
  i. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan, klicka på motsvarande knapp.
  ii. Klick **SKICKA NEDLADDNINGSLÄNK**.
  iii. Skriv en e-postadress i motsvarande fält och klicka **SKICKA EPOST**.
  Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
  iv. På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och klicka sedan på motsvarande nedladdningsknapp.

c. Kör Bitdefender-produkten du har laddat ner.

Jag har en aktiveringskod. Hur lägger jag till dess giltighet till mitt abonnemang?

Om du har köpt en aktiveringskod från en av våra återförsäljare eller fått den i present, kan du lägga till dess tillgänglighet till ditt Bitdefender-abonnemang.

För att aktivera ett abonnemang med en aktiveringskod, följ dessa steg:

1. Tillgång Bitdefender Central.
2. Välj **mina prenumerationer** panel.
3. Klicka på **AKTIVERINGSKOD** knappen och skriv sedan koden i motsvarande fält.
4. Klick **AKTIVERA** att fortsätta.

Tillägget är nu synligt i ditt Bitdefender-konto och i din Bitdefender Antivirus för Mac-installerade produkt, i den nedre högra delen av skärmen.

Skanningsloggen indikerar att det fortfarande finns olösta objekt. Hur tar jag bort dem?

De olösta objekten i skanningsloggen kan vara:

- arkiv med begränsad åtkomst (xar, rar, etc.)
  Lösning: Använd **Avslöja i Finder** alternativet för att hitta filen och radera den manuellt. Se till att tömma papperskorgen.
- postlådor med begränsad åtkomst (Thunderbird, etc.)
  Lösning: Använd appen för att ta bort posten som innehåller den infekterade filen.
- Innehåll i säkerhetskopior
  Lösning: Aktivera **Skanna inte innehåll i säkerhetskopior** alternativ i Skyddsinställningar eller **Lägg till i undantag** de upptäckta filerna.
  Om de infekterade filerna återställs vid ett senare tillfälle kommer Bitdefender Antivirus för Mac automatiskt att upptäcka dem och vidta lämpliga åtgärder.

> **Notera**
> Filer med begränsad åtkomst betyder att filer som Bitdefender Antivirus för Mac bara kan öppna, men inte ändra dem.

Var kan jag se information om produktaktiviteten?

Bitdefender håller en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden relaterade till dess aktivitet. För att komma åt denna information, klicka **Aviseringar** på navigeringsmenyn på Bitdefender-gränssnittet.

Kan jag uppdatera Bitdefender Antivirus för Mac via en proxyserver?

Bitdefender Antivirus för Mac kan endast uppdateras via proxyservrar som inte kräver autentisering. Du behöver inte konfigurera några programinställningar.

Om du ansluter till internet via en proxyserver som kräver autentisering måste du byta till en direkt internetanslutning regelbundet för att få uppdateringar av hotinformation.

Hur tar jag bort Bitdefender Antivirus för Mac?

Följ dessa steg för att ta bort Bitdefender Antivirus för Mac:

1. Öppna a **Upphittare** fönstret och gå sedan till mappen Applications.

2. Öppna mappen Bitdefender och dubbelklicka sedan på BitdefenderUninstaller.
3. Klick **Avinstallera** och vänta på att processen ska slutföras.
4. Klick **Stänga** att avsluta.

> **Viktig**
> Om det finns ett fel kan du kontakta Bitdefender kundtjänst enligt beskrivningen i Ber om hjälp (sida 273).

Hur tar jag bort TrafficLight-tilläggen från min webbläsare?

- Följ dessa steg för att ta bort TrafficLight-tilläggen från Mozilla Firefox:
  1. Gå till **Verktyg** och välj **Tillägg**.
  2. Välj **Tillägg** i den vänstra kolumnen.
  3. Välj tillägget och klicka **Avlägsna**.
  4. Starta om webbläsaren för att borttagningsprocessen ska slutföras.
- Följ dessa steg för att ta bort TrafficLight-tilläggen från Google Chrome:
  1. Klicka på uppe till höger **Mer** ⋮ .
  2. Gå till **Fler verktyg** och välj **Tillägg**.
  3. Klicka på **Avlägsna** 🗑 ikonen bredvid tillägget du vill ta bort.
  4. Klick **Avlägsna** för att bekräfta borttagningsprocessen.
- För att ta bort Bitdefender TrafficLight från Safari, följ dessa steg:
  1. Gå till **Inställningar** eller tryck **Kommando-Komma(,)**.
  2. Välj **Tillägg**.
     En lista med installerade tillägg visas.
  3. Välj Bitdefender TrafficLight-tillägget och klicka sedan **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta borttagningsprocessen.

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du använder, laddar ner eller laddar upp innehåll på internet. För att se till att du är säker när du surfar på webben rekommenderar vi att du använder Bitdefender VPN när du:

- vill ansluta till offentliga trådlösa nätverk
- vill komma åt innehåll som normalt är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, kreditkortsinformation, etc.)
- vill dölja din IP-adress

Kommer Bitdefender VPN att ha en negativ inverkan på batteritiden för min enhet?

Bitdefender VPN är utformad för att skydda dina personliga data, dölja din IP-adress när du är ansluten till osäkra trådlösa nätverk och komma åt begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning av din enhet rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort när du är offline.

Varför stöter jag på internetnedgångar när jag är ansluten till Bitdefender VPN?

Bitdefender VPN är designad för att erbjuda dig en lätt upplevelse när du surfar på webben; din internetanslutning eller serveravståndet du ansluter till kan dock orsaka nedgången. I det här fallet, om det inte är ett måste att ansluta från din plats till en fjärransluten server (t.ex. från USA till Kina), rekommenderar vi att du tillåter Bitdefender VPN att automatiskt ansluta dig till närmaste server, eller hitta en server närmare din nuvarande plats.

5. MOBIL SÄKERHET FÖR ANDROID

5.1. Vad är Bitdefender Mobile Security

Onlineaktiviteter som att betala räkningar, göra semesterbokningar eller köpa varor och tjänster är bekväma och problemfria. Men eftersom många aktiviteter har utvecklats på internet, kommer dessa med höga risker och, om säkerhetsdetaljer ignoreras, kan personuppgifter hackas. Och vad är viktigare än att skydda data som lagras på onlinekonton och på den personliga smartphonen?

Bitdefender Mobile Security låter dig:

- Få det bästa skyddet för din Android-smarttelefon och surfplatta med minimal påverkan på batteritiden
- Skydda dig själv från att falla offer för länkbaserade mobilbedrägerier
- Ha tillgång till vårt säkra VPN för en snabb, anonym och säker upplevelse när du surfar på webben
- Hitta, lås och torka din Android-enhet på distans i händelse av förlust eller stöld
- Kontrollera om ditt e-postkonto har varit inblandat i databrott eller dataläckor

5.2. Komma igång

5.2.1. Enhetskrav

Bitdefender Mobile Security fungerar på alla enheter som kör Android 5.0 eller senare versioner av operativsystemet. En aktiv internetanslutning krävs för genomsökning av hot i molnet.

5.2.2. Installera Bitdefender Mobile Security

- **Från Bitdefender Central**
  - På Android
    1. Gå till: https://central.bitdefender.com.
    2. Logga in på ditt Bitdefender-konto.

3. Välj **Mina enheter** panel.
4. Knacka **INSTALLATIONSSKYDD**och tryck sedan på **Skydda den här enheten**.
5. Välj enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
6. Du omdirigeras till **Google Play** app. På Google Play-skärmen trycker du på installationsalternativet.

- På Windows, macOS och iOS
  1. Gå till: https://central.bitdefender.com.
  2. Logga in på ditt Bitdefender-konto.
  3. Välj **Mina enheter** panel.
  4. Tryck **INSTALLATIONSSKYDD**, och tryck sedan på **Skydda andra enheter**.
  5. Välj enhetens ägare. Om enheten tillhör någon annan, tryck på motsvarande knapp.
  6. Tryck **SKICKA NEDLADDNINGSLÄNK**.
  7. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
  8. På enheten du vill installera Bitdefender kontrollera e-postkontot som du skrev in och tryck sedan på motsvarande nedladdningsknapp.

- **Från Google Play**
  Sök efter Bitdefender Mobile Security för att hitta och installera appen. Alternativt, skanna QR-koden:

  Innan du går igenom valideringsstegen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren under vilka du får använda Bitdefender Mobile Security.

Knacka **FORTSÄTTA** för att gå vidare till nästa fönster.

5.2.3. Logga in på ditt Bitdefender-konto

För att använda Bitdefender Mobile Security måste du länka din enhet till ett Bitdefender-, Facebook-, Google-, Microsoft- eller Apple-konto genom att logga in på kontot från appen. Första gången du öppnar appen blir du ombedd att logga in på ett konto.

Om du installerade Bitdefender Mobile Security från ditt Bitdefender-konto kommer appen att försöka logga in på det kontot automatiskt.

Så här länkar du din enhet till ett Bitdefender-konto:

1. Ange e-postadressen och lösenordet för ditt Bitdefender-konto i motsvarande fält. Om du inte har ett Bitdefender-konto och vill skapa ett, välj motsvarande länk.
2. Knacka **LOGGA IN**.

För att logga in med ett Facebook-, Google- eller Microsoft-konto trycker du på tjänsten du vill använda i området ELLER LOGGA MED. Du omdirigeras till inloggningssidan för den valda tjänsten. Följ instruktionerna för att länka ditt konto till Bitdefender Mobile Security.

> **Notera**
> Bitdefender får inte tillgång till någon konfidentiell information som lösenordet för kontot du använder för att logga in eller personlig information om dina vänner och kontakter.

5.2.4. Konfigurera skydd

När du har loggat in på appen visas fönstret Konfigurera skydd. För att säkra din enhet rekommenderar vi att du går igenom dessa steg:

- **Prenumerationsstatus**. För att skyddas av Bitdefender Mobile Security måste du aktivera din produkt med ett abonnemang, som anger hur länge du får använda produkten. Så snart den löper ut slutar appen att utföra sina funktioner och skydda din enhet.
  Om du har en aktiveringskod trycker du på I **HAR EN KOD**och tryck sedan på **AKTIVERA**.
  Om du har loggat in med ett nytt Bitdefender-konto och inte har någon aktiveringskod kan du använda produkten i 14 dagar utan kostnad.
- **Nätskydd**. Om din enhet kräver tillgänglighet för att aktivera webbskydd trycker du på **AKTIVERA**. Du omdirigeras till

tillgänglighetsmenyn. Tryck på Bitdefender Mobile Security och slå sedan på motsvarande switch.

- **Skanner för skadlig programvara**. Kör en engångsskanning för att se till att din enhet är fri från hot. För att starta skanningsprocessen, tryck på **SKANNA NU**.
  Så snart skanningsprocessen börjar visas instrumentpanelen. Här kan du se säkerhetsstatusen för din enhet.

5.2.5. instrumentbräda

Tryck på Bitdefender Mobile Security-ikonen i enhetens applåda för att öppna appgränssnittet.

Instrumentpanelen ger information om din enhets säkerhetsstatus och genom Autopilot hjälper du dig att förbättra enhetens säkerhet genom att ge dig rekommendationer om funktioner.

Statuskortet högst upp i fönstret informerar dig om enhetens säkerhetsstatus med hjälp av explicita meddelanden och suggestiva färger. Om Bitdefender Mobile Security inte har några varningar är statuskortet grönt. När ett säkerhetsproblem har upptäckts ändras statuskortets färg till rött.

För att erbjuda dig en effektiv operation och ökat skydd samtidigt som du utför olika aktiviteter, **Bitdefender autopilot** kommer att fungera som din personliga säkerhetsrådgivare. Beroende på aktiviteten du utför kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov. Detta hjälper dig att upptäcka och dra nytta av fördelarna med funktionerna som ingår i Bitdefender Mobile Security-appen.

Närhelst det pågår en process eller en funktion kräver din input, visas ett kort med mer information och möjliga åtgärder i instrumentpanelen.

Du kan komma åt Bitdefender Mobile Security-funktionerna och enkelt navigera från det nedre navigeringsfältet:

Skanner för skadlig programvara

Gör att du kan starta en genomsökning på begäran och aktivera skanningslagring. För mer information, se Skanner för skadlig programvara (sida 180).

Nätskydd

Säkerställer en säker surfupplevelse genom att varna dig om potentiella skadliga webbsidor. För mer information, se Nätskydd (sida 182).

VPN

Krypterar internetkommunikation, vilket hjälper dig att behålla din integritet oavsett vilket nätverk du är ansluten till. För mer information, se VPN (sida 184).

Scam Alert

Håller dig säker genom att varna dig om skadliga länkar som kommer via SMS, meddelandeprogram och alla typer av meddelanden. För mer information, se Scam Alert (sida 186).

Anti-stöld

Låter dig aktivera eller inaktivera stöldskyddsfunktionerna och konfigurera stöldskyddsinställningar. För mer information, se Stöldskyddsfunktioner (sida 189).

Kontosekretess

Kontrollerar om något dataintrång har inträffat i dina onlinekonton. För mer information, se Kontosekretess (sida 193).

Applås

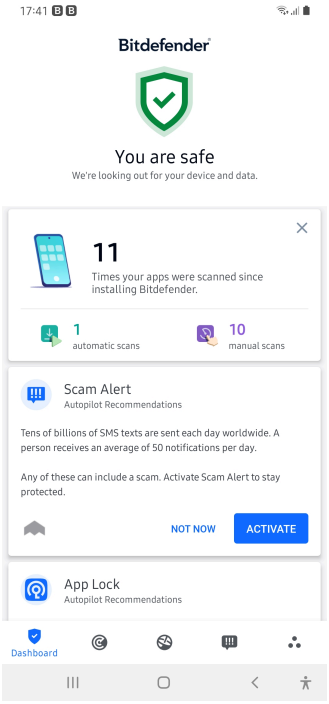
Låter dig skydda dina installerade appar genom att ställa in en PIN-kod. För mer information, se Applås (sida 195).

Rapporter

Håller en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden relaterade till din enhets aktivitet. För mer information, se Rapporter (sida 199).

Bära PÅ

Kommunicerar med din smartklocka för att hjälpa dig hitta din telefon ifall du tappar bort eller glömmer var du lämnade den. För mer information, se Bära PÅ (sida 200).



5.3. Skanner för skadlig programvara

Bitdefender skyddar din enhet och data mot skadliga appar med hjälp av skanning på installation och skanning på begäran.

Malware Scanner-gränssnittet ger en lista över alla typer av hot Bitdefender letar efter, tillsammans med deras definitioner. Klicka bara på ett hot för att se dess definition.

> **Notera**
> Se till att din mobila enhet är ansluten till internet. Om din enhet inte är ansluten till internet kommer skanningsprocessen inte att starta.

- **Skanning på installation**
  När du installerar en app skannar Bitdefender Mobile Security den automatiskt med hjälp av in-the-cloud-teknik. Samma skanningsprocess startar varje gång de installerade apparna uppdateras.

Om appen visar sig vara skadlig visas en varning som uppmanar dig att avinstallera den. Knacka **Avinstallera** för att gå till appens avinstallationsskärm.

- **Skanning på begäran**
  Närhelst du vill försäkra dig om att apparna som är installerade på din enhet är säkra att använda kan du initiera en genomsökning på begäran.
  Så här startar du en genomsökning på begäran:

  1. Knacka **Skanner för skadlig programvara** på det nedre navigeringsfältet.
  2. Knacka **STARTA SKANNING**.

  > **Notera**
  > Ytterligare behörigheter krävs på Android 6 för skannerfunktionen för skadlig programvara. Efter knackning **STARTA SKANNING**, Välj **Tillåta** för följande:
  >
  > - Tillåta **Antivirus** ringa och hantera telefonsamtal?
  > - Tillåta **Antivirus** för att komma åt foton, media och filer på din enhet?

  Skanningsförloppet visas och du kan stoppa processen när som helst.

Som standard kommer Bitdefender Mobile Security att skanna din enhets interna lagring, inklusive eventuellt monterat SD-kort. På så sätt kan alla farliga appar som kan finnas på kortet upptäckas innan de kan orsaka skada.

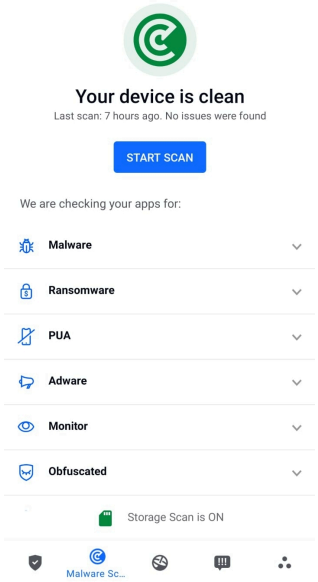
Så här inaktiverar du inställningen Scan Storage:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Inaktivera **Skanna lagring** i området Malware Scanner.

Om några skadliga appar upptäcks kommer information om dem att visas och du kan ta bort dem genom att trycka på **AVINSTALLERA**.

Malware Scanner-kortet visar statusen för din enhet. När din enhet är säker är kortet grönt. När enheten kräver en skanning, eller det finns någon åtgärd som kräver din input, blir kortet rött.

Om din Android-version är 7.1 eller senare kan du komma åt en genväg till Malware Scanner så att du kan köra skanningar snabbare utan att öppna Bitdefender Mobile Security-gränssnittet. För att göra detta, tryck och håll Bitdefender-ikonen på din hemskärm eller applåda och välj sedan ikon.



5.3.1. Appavvikelsedetektering

Bitdefender App Anomaly Detection är en ny teknik integrerad i Bitdefender Malware Scanner för att tillhandahålla ett extra skyddslager genom att kontinuerligt övervaka och upptäcka alla skadliga beteenden och varna användaren om misstänkta aktiviteter identifieras.

Bitdefender App Anomaly Detection skyddar användare även när de omedvetet har installerat en farlig app som körs vilande under en period eller en till synes pålitlig app som bryter dess funktionalitet och blir oseriös.

5.4. Nätskydd

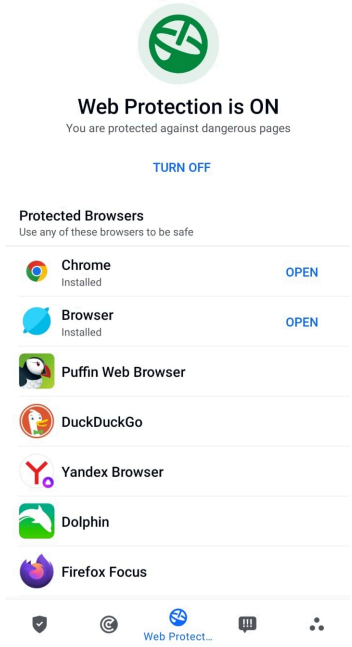
Webbskydd kontrollerar med Bitdefender molntjänster webbsidor som du kommer åt med standardwebbläsaren Android, Google Chrome,

Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser och Dolphin.

Notera

Ytterligare behörigheter krävs på Android 6 för webbskyddsfunktionen.

Tillåt behörighet att registrera dig som tillgänglighetstjänst och tryck på **SÄTTA PÅ** när det efterfrågas. Knacka **Antivirus** och aktivera omkopplaren, bekräfta sedan att du godkänner åtkomsten till din enhets behörighet.



Varje gång du går in på en bankwebbplats är Bitdefender Web Protection inställt på att meddela dig att du ska använda Bitdefender VPN. Meddelandet visas i statusfältet. Vi rekommenderar att du använder Bitdefender VPN medan du är inloggad på ditt bankkonto så att dina data kan förbli säkra från potentiella säkerhetsintrång.

Så här inaktiverar du webbskyddsmeddelandet:

1. Knacka **Mer** på det nedre navigeringsfältet.

2. Knacka **inställningar**.
3. Stäng av motsvarande strömbrytare i området Webbskydd.

5.5. VPN

Med Bitdefender VPN kan du hålla din data privat varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personlig data eller försök att göra din enhets IP-adress tillgänglig för hackare undvikas.

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter för att säkra din anslutning, kryptera data med bankklassad kryptering och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet nästan omöjlig att identifieras genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via VPN, kan du komma åt innehåll som normalt är begränsat i specifika områden.

> **Notera**
> Vissa länder utövar internetcensur och därför har användningen av VPN på deras territorium förbjudits enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen för första gången. Genom att fortsätta använda appen bekräftar du att du är medveten om tillämpliga landsbestämmelser och de risker som du kan utsättas för.

Det finns två sätt att slå på eller stänga av Bitdefender VPN:

- Knacka **ANSLUTA** i VPN-kortet från Dashboard.
  Status för Bitdefender VPN visas.
- Knacka **VPN** på det nedre navigeringsfältet och tryck sedan på **ANSLUTA**.
  Knacka **ANSLUTA** varje gång du vill vara skyddad medan du är ansluten till osäkra trådlösa nätverk.
  Knacka **KOPPLA IFRÅN** när du vill inaktivera anslutningen.

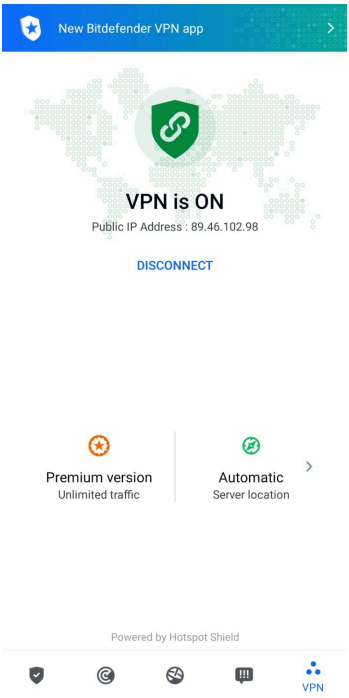
> **Notera**
> Första gången du slår på VPN ombeds du att tillåta Bitdefender att konfigurera en VPN-anslutning som övervakar nätverkstrafik. Knacka **OK** att fortsätta.

Om din Android-version är 7.1 eller senare kan du komma åt en genväg till Bitdefender VPN utan att öppna Bitdefender Mobile Security-gränssnittet.

För att göra detta, tryck och håll Bitdefender-ikonen på din hemskärm eller applåda och välj sedan ikon.

För att spara batteri, rekommenderar vi att du stänger av VPN-funktionen när du inte behöver den.

Om du har ett premiumabonnemang och vill ansluta till en server som du vill, tryck på Serverplats i VPN-funktionen och välj sedan den plats du vill ha. Mer information om VPN-prenumerationer finns i



5.5.1. VPN-inställningar

För en avancerad konfiguration av ditt VPN:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.

I VPN-området kan du konfigurera följande alternativ:

- Snabb VPN-åtkomst – ett meddelande visas i statusfältet på din enhet så att du snabbt kan slå på VPN.
- Öppna Wi-Fi-varning - varje gång du ansluter till ett öppet Wi-Fi-nätverk meddelas du i statusfältet på din enhet om att använda VPN.

5.5.2. Prenumerationer

Bitdefender VPN erbjuder gratis en daglig trafikkvot på 200 MB per enhet för att säkra din anslutning varje gång du behöver, och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad tillgång till innehåll över hela världen genom att välja en serverplats efter din vilja, uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-version när som helst genom att trycka på **Aktivera Premium** i VPN-fönstret.

Bitdefender Premium VPN-prenumeration är oberoende av Bitdefender Mobile Security-prenumerationen, vilket innebär att du kommer att kunna använda den under hela dess tillgänglighet, oavsett tillståndet för ditt säkerhetsabonnemang. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Mobile Security fortfarande är aktiv, kommer du att återgå till den kostnadsfria planen.

Bitdefender VPN är en plattformsoberoende produkt, tillgänglig i Bitdefender-produkter som är kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kommer du att kunna använda ditt abonnemang på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

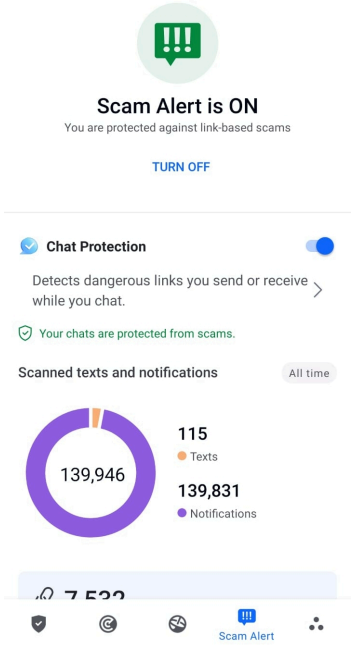
> **Notera**
> Bitdefender VPN fungerar också som en fristående applikation på alla operativsystem som stöds, nämligen Windows, macOS, Android och iOS.

5.6. Scam Alert

Scam Alert-funktionen tar förebyggande åtgärder i förgrunden och hanterar potentiellt farliga situationer innan de ens har en chans att bli ett problem, inklusive hot mot skadlig programvara. Scam Alert övervakar alla inkommande SMS-meddelanden och Android-aviseringar i realtid.

När en farlig länk kommer i ett meddelande på din telefon kommer en varning att dyka upp på din skärm. Bitdefender kommer att erbjuda två alternativ. Det första alternativet är att avvisa informationen. Det andra alternativet är att **VISA DETALJER**. Detta ger dig mer information om händelsen, samt viktiga råd, såsom:

- Öppna eller vidarebefordra inte den upptäckta länken.
- För sms, radera meddelandet om möjligt.
- Blockera avsändaren om de inte är en betrodd kontakt.
- Avinstallera appen som skickar farliga länkar i aviseringar.



Notera

På grund av Android-operativsystemets begränsningar kan Bitdefender inte radera textmeddelanden, vidta några direkta åtgärder relaterade till SMS-meddelanden eller någon annan källa till skadliga meddelanden. Om du ignorerar Scam Alert-varningen och försöker öppna den farliga länken, kommer Bitdefenders webbskyddsfunktion automatiskt att fånga den, vilket förhindrar din enhet från att bli infekterad.

5.6.1. Aktiverar Scam Alert

För att aktivera Scam Alert måste du ge Bitdefender Mobile Security-appen åtkomst till SMS-meddelanden och meddelandesystemet:

1. Öppna Bitdefender Mobile Security-appen installerad på din Android-telefon eller surfplatta.
2. På Bitdefender-appens huvudskärm, tryck på **Scam Alert** alternativet i det nedre navigeringsfältet och tryck sedan på **SÄTTA PÅ**.
3. Tryck på **TILLÅTA** knapp.
4. I listan Notification Access, växla Bitdefender Security till **PÅ** placera.
5. Bekräfta åtgärden genom att trycka på **TILLÅTA**.
6. Återgå till skärmen Scam Alert och tryck **TILLÅTA** för att ge Bitdefender möjligheten att skanna inkommande SMS-meddelanden.

5.6.2. Chattskydd i realtid

Chattmeddelanden är vårt bekvämaste sätt att hålla kontakten, men de är också ett enkelt sätt för farliga länkar att nå dig.

Med chattskyddsfunktionen aktiverad utökas Scam Alert-modulen från att skydda dina texter och aviseringar till att skydda dina chattar även mot länkbaserade attacker, genom att upptäcka farliga länkar som du antingen skickar eller tar emot medan du chattar.

Så här aktiverar du chattskydd:

1. Öppna Bitdefender Mobile Security-appen installerad på din Android-telefon eller surfplatta.
2. På Bitdefender-appens huvudskärm, tryck på **Scam Alert** alternativet i det nedre navigeringsfältet.
3. Du kommer att mötas av chattskyddsfunktionen överst på fliken Scam Alert. Växla dess motsvarande omkopplare till **PÅ** placera.

Notera

För närvarande är Chat Protection kompatibelt med följande applikationer:

- WhatsApp
- Facebook Messenger
- Telegram
- Disharmoni

5.7. Scam Copilot

Den här funktionen är i huvudsak en AI-driven chatbot som utbildats av Bitdefender för att upptäcka olika bedrägerier, phishing-försök, kampanjer med felaktig information och falska webbplatser.

Så här aktiverar du Scam Copilot:

1. Öppna appen Bitdefender Mobile Security. I kontrollpanelen visas ett kort som gäller Scam Copilot. Tryck på **Aktivera**.
2. Aktivera åtkomst till Bitdefender Mobile Security genom att trycka på knappen **TURN ON**.
3. **{Tillåt** aviseringsbehörighet.

Scam Copilot är nu korrekt konfigurerad på din enhet.

Du kan komma åt den dedikerade fliken Scam Copilot. Här hittar du:

- **Scam Detection Chatbot:** Be chatbotten att granska alla meddelanden som du tycker är misstänkta.
- **Prevention Assistant:** Hjälper dig att lära dig mer om bedrägerier för att bli skicklig på att upptäcka dem.
- **Automatisk bedrägeridetektering** status och kontrollpanel.
- **SMS-filtrering**: Få dina farliga meddelanden filtrerade direkt i din meddelandeapp.

5.8. Stöldskyddsfunktioner

Bitdefender kan hjälpa dig att hitta din enhet och förhindra att dina personuppgifter hamnar i fel händer.

Allt du behöver göra är att aktivera Stöldskydd från enheten och, när det behövs, komma åt **Bitdefender Central** från vilken webbläsare som helst, var som helst.

> **Notera**
> Stöldskyddsgränssnittet innehåller också en länk till vår Bitdefender Central-app på Google Play Butik. Du kan använda den här länken för att ladda ner appen, om du inte redan har gjort det.

Bitdefender Mobile Security erbjuder följande stöldskyddsfunktioner:

Fjärrlokalisera

Visa enhetens aktuella plats på Google Maps. Platsen uppdateras var 5:e sekund, så att du kan spåra den om den är på resande fot.

Platsens noggrannhet beror på hur Bitdefender kan bestämma den:

- Om GPS är aktiverat på enheten kan dess plats fastställas inom ett par meter så länge den är inom GPS-satelliternas räckvidd (dvs. inte inne i en byggnad).
- Om enheten är inomhus kan dess plats bestämmas inom tiotals meter om Wi-Fi är aktiverat och det finns trådlösa nätverk tillgängliga inom dess räckvidd.
- I annat fall kommer platsen att bestämmas med hjälp av endast information från mobilnätet, som kan erbjuda en noggrannhet som inte är bättre än flera hundra meter.

Fjärrlås

Lås enhetens skärm och ange en numerisk PIN-kod för att låsa upp den.

Fjärrtorka

Ta bort all personlig data från din främmande enhet.

Skicka varning till enheten (Scream)

Skicka ett meddelande på distans som ska visas på enhetens skärm, eller utlösa ett högt ljud som spelas upp på enhetens högtalare.

Om du tappar bort din enhet kan du låta den som hittar den veta hur de kan returnera den till dig genom att visa ett meddelande på enhetens skärm.

Om du har tappat bort din enhet och det finns en chans att den inte är långt ifrån dig (till exempel någonstans i huset eller på kontoret), vilket

bättre sätt att hitta den än att få den att spela ett högt ljud? Ljudet spelas även om enheten är i tyst läge.

5.8.1. Aktivera stöldskydd

För att aktivera stöldskyddsfunktioner, slutför du helt enkelt konfigurationsprocessen från stöldskyddskortet som finns tillgängligt i instrumentpanelen.

Alternativt kan du aktivera Stöldskydd genom att följa dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Anti-stöld**.
3. Knacka **SÄTTA PÅ**.
4. Följande procedur kommer att börja hjälpa dig att aktivera den här funktionen:

   > **Notera**
   > Ytterligare behörigheter krävs på Android 6 för stöldskyddsfunktionen.
   >
   > För att aktivera det, följ dessa steg:
   >
   > a. Knacka **Aktivera stöldskydd**, tryck sedan på **SÄTTA PÅ**.
   >
   > b. Tillåt behörigheter för **Antivirus** för att komma åt enhetens plats.

   a. **Ge administratörsrättigheter**
   Dessa privilegier är väsentliga för driften av Anti-Theft och måste därför beviljas för att fortsätta.

   b. **Ställ in program-PIN**
   För att förhindra obehörig åtkomst till din enhet måste en PIN-kod ställas in. Varje gång ett försök görs att komma åt din enhet måste PIN-koden anges först. Alternativt, på enheter som stöder fingeravtrycksautentisering, kan en fingeravtrycksbekräftelse användas istället för den konfigurerade PIN-koden.
   Samma PIN-kod används av App Lock för att skydda dina installerade appar.

   c. **Aktivera Snap Photo**

Varje gång någon försöker låsa upp din enhet utan framgång medan Snap Photo är på, kommer Bitdefender att ta ett foto av honom.

Mer exakt, varje gång PIN-koden, lösenordet eller fingeravtrycksbekräftelsen du ställt in för att skydda din enhet skrivs in fel tre gånger i rad, tas ett foto med den främre kameran. Fotot sparas tillsammans med tidsstämpeln och anledningen och kan ses när du öppnar Bitdefender Mobile Security och kommer åt fönstret Stöldskydd.

Alternativt kan du se det tagna fotot i ditt Bitdefender-konto:

i. Gå till: https://central.bitdefender.com.

ii. Logga in på ditt konto.

iii. Välj **Mina enheter** panel.

iv. Välj din Android-enhet och sedan **Anti-stöld** flik.

v. Knacka ⋮ bredvid **Kontrollera dina ögonblicksbilder** för att se de senaste bilderna som togs.
Endast de två senaste fotona sparas.

När stöldskyddsfunktionen är aktiverad kan du aktivera eller inaktivera webbkontrollkommandon individuellt från stöldskyddsfönstret genom att trycka på motsvarande alternativ.

5.8.2. Använda stöldskyddsfunktioner från Bitdefender Central

> **Notera**
> Alla stöldskyddsfunktioner kräver **Bakgrundsdata** alternativet för att aktiveras i enhetens inställningar för dataanvändning.

För att komma åt stöldskyddsfunktionerna från ditt Bitdefender-konto:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. I den **MINA ENHETER** fönstret, välj önskat enhetskort genom att trycka på motsvarande **Visa detaljer** knapp.
4. Välj **Anti-stöld** flik.

5. Tryck på knappen som motsvarar den funktion du vill använda:
   Lokalisera - visa enhetens plats på Google Maps.
   VISA IP - visar den senaste IP-adressen för den valda enheten.
   Varna - skriv ett meddelande som ska visas på enhetens skärm och/eller få din enhet att spela ett ljudlarm.
   Låsa - lås din enhet och ställ in en PIN-kod för att låsa upp den.
   Torka - radera all data från din enhet.

   > **Viktig**
   > När du har torkat en enhet upphör alla stöldskyddsfunktioner att fungera.

5.8.3. Stöldskyddsinställningar

Om du vill aktivera eller inaktivera fjärrkommandona:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Anti-stöld**.
3. Aktivera eller inaktivera önskade alternativ.

5.9. Kontosekretess

Bitdefender-kontosekretess upptäcker om något dataintrång har inträffat på de konton du använder för att göra onlinebetalningar, handla eller logga in på olika appar eller webbplatser. De data som kan lagras på ett konto kan vara lösenord, kreditkortsinformation eller bankkontoinformation, och om den inte är ordentligt säkrad kan identitetsstöld eller intrång i integriteten förekomma.

Sekretessstatusen för ett konto visas direkt efter validering.

Automatiska omkontroller är inställda på att köras i bakgrunden, men manuella skanningar kan också köras dagligen.

Meddelanden kommer att visas varje gång nya intrång som inkluderar något av de validerade e-postkontona upptäcks.

Så här börjar du hålla personlig information säker:

1. Knacka **Mer** på det nedre navigeringsfältet.

2. Knacka **Kontosekretess**.
3. Knacka **KOMMA IGÅNG**.
4. E-postadressen som används för att skapa ditt Bitdefender-konto visas och läggs automatiskt till i listan över övervakade konton.
5. För att lägga till ett annat konto, tryck på **LÄGG TILL KONTO** i fönstret Kontosekretess och skriv sedan in e-postadressen.
   Knacka **LÄGG TILL** att fortsätta.
   Bitdefender måste validera detta konto innan privat information visas. Därför skickas ett e-postmeddelande med en valideringskod till den angivna e-postadressen.
   Kontrollera din inkorg och skriv sedan den mottagna koden i **Kontosekretess** område av din app. Om du inte hittar valideringse-postmeddelandet i mappen Inkorg, kontrollera skräppostmappen.
   Sekretessstatusen för det validerade kontot visas.

Om intrång upptäcks på något av dina konton rekommenderar vi att du ändrar lösenordet så snart som möjligt. För att skapa ett starkt och säkert lösenord, ta hänsyn till dessa tips:

- Gör den minst åtta tecken lång.
- Inkludera gemener och versaler.
- Lägg till minst en siffra eller symbol, som #, @, % eller !.

När du väl har säkrat ett konto som var en del av ett integritetsintrång kan du bekräfta ändringarna genom att markera de identifierade brotten som Lösta. Att göra detta:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Kontosekretess**.
3. Tryck på kontot du just säkrade.
4. Tryck på intrånget du säkrade kontot för.
5. Knacka **LÖST** för att bekräfta att kontot är säkert.

När alla upptäckta överträdelser är markerade som **Löst**, kommer kontot inte längre att visas som intrång, åtminstone tills ett nytt intrång upptäcks.

Så här slutar du att meddelas varje gång automatiska skanningar görs:

1. Knacka **Mer** på det nedre navigeringsfältet.

2. Knacka **inställningar**.
3. Stäng av motsvarande strömbrytare i området Kontosekretess.

5.10. Applås

Installerade appar som e-post, foton eller meddelanden kan innehålla personuppgifter som du vill förbli privata genom att selektivt begränsa åtkomsten till dem.

Applås hjälper dig att blockera oönskad åtkomst till appar genom att ställa in en säkerhets-PIN-åtkomstkod. PIN-koden du anger måste vara minst 4 siffror lång, men inte mer än 8, och krävs varje gång du vill komma åt de valda begränsade apparna.

Biometrisk autentisering (som fingeravtrycksbekräftelse eller ansiktsigenkänning) kan användas istället för den konfigurerade PIN-koden.

5.10.1. Aktiverar applås

För att begränsa åtkomsten till utvalda appar, konfigurera App Lock från kortet som visas i instrumentpanelen efter aktivering av Anti-Theft.

Alternativt kan du aktivera App Lock genom att följa dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Applås**.
3. Knacka **SÄTTA PÅ**.
4. Tillåt åtkomst till användningsdata för Bitdefender Security.
5. Tillåta **rita över andra appar**.
6. Gå tillbaka till appen, konfigurera åtkomstkoden och tryck sedan på **STÄLL IN PIN**.

> **Notera**
> Det här steget är endast tillgängligt om du inte tidigare har konfigurerat PIN-koden i Anti-Theft.

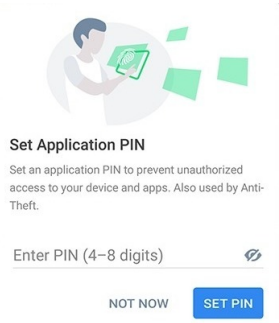
7. Aktivera alternativet Snap Photo för att fånga alla inkräktare som försöker komma åt dina privata data.

> **Notera**
> Ytterligare behörigheter krävs på Android 6 för Snap Photo-funktionen. Tillåt för att aktivera det **Antivirus** att ta bilder och spela in video.

8. Välj de appar du vill skydda.

Om du använder fel PIN-kod eller fingeravtryck fem gånger i rad, aktiveras en 30 sekunders timeout-session. På så sätt kommer alla försök att bryta sig in i de skyddade apparna att blockeras.

> **Notera**
> Samma PIN-kod används av Anti-Theft för att hjälpa dig att hitta din enhet.



5.10.2. Låsläge

Första gången du lägger till en app i App Lock visas skärmen för App Lock Mode. Härifrån kan du välja när applåsfunktionen ska skydda apparna som är installerade på din enhet.

Du kan välja mellan ett av följande alternativ:

- **Kräv upplåsning varje gång** - varje gång de låsta apparna öppnas måste PIN-koden eller fingeravtrycket som du har ställt in användas.
- **Håll olåst tills skärmen stängs av** - åtkomsten till dina appar kommer att vara giltig tills skärmen stängs av.
- **Lås efter 30 sekunder** - du kan avsluta och komma åt dina olåsta appar igen inom 30 sekunder.

Om du vill ändra den valda inställningen:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Knacka **Kräv upplåsning varje gång** i applåsområdet.
4. Välj önskat alternativ.

5.10.3. Applåsinställningar

För en avancerad konfiguration av App Lock:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.

I området för applås kan du konfigurera följande alternativ:

- **Känsligt appförslag** - få ett låsmeddelande varje gång du installerar en känslig app.
- **Kräv upplåsning varje gång** - välj ett av de tillgängliga lås- och upplåsningsalternativen.
- **Smart upplåsning** - håll appar olåsta medan du är ansluten till betrodda Wi-Fi-nätverk.
- **Slumpmässigt tangentbord** - förhindra PIN-läsning genom att slumpvisa nummerpositioner.

5.10.4. Snap Photo

Med Bitdefender Snap Photo kan du fånga dina vänner eller släktingar på hopp. På så sätt kan du utbilda deras nyfikna ögon att inte titta igenom dina personliga filer eller apparna du använder.

Funktionen fungerar enkelt: varje gång PIN-koden eller fingeravtrycksbekräftelsen du ställt in för att skydda dina appar matas in fel tre gånger i rad, tas ett foto med den främre kameran. Fotot sparas tillsammans med tidsstämpeln och anledningen, och kan ses när du öppnar Bitdefender Mobile Security och kommer åt funktionen App Lock.

> **Notera**
> Den här funktionen är endast tillgänglig för telefoner som har en främre kamera.

Så här konfigurerar du Snap Photo-funktionen för App Lock:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Aktivera motsvarande omkopplare i området Snap Photo.

Bilderna som togs när felaktig PIN-kod anges visas i App Lock-fönstret och kan visas i helskärmsläge.

Alternativt kan de ses i ditt Bitdefender-konto:

1. Gå till: https://central.bitdefender.com.
2. Logga in på ditt konto.
3. Välj **Min enhet** panel.
4. Välj din Android-enhet och sedan **Anti-stöld** flik.
5. Knacka bredvid **Kontrollera dina ögonblicksbilder** för att se de senaste bilderna som togs.

Endast de två senaste fotona sparas.

Så här slutar du ladda upp tagna foton på ditt Bitdefender-konto:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Inaktivera **Ladda upp foton** i området Snap Photo.

5.10.5. Smart upplåsning

En enkel metod för att sluta bli ombedd av App Lock-funktionen att ange PIN-koden eller fingeravtrycksbekräftelsen för de skyddade apparna varje gång du kommer åt dem är att aktivera Smart Unlock.

Med Smart Unlock kan du ställa in som betrodda Wi-Fi-nätverk du vanligtvis ansluter till, och när du är ansluten till dem kommer blockeringsinställningarna för applås att inaktiveras för de skyddade apparna.

Så här konfigurerar du Smart Unlock-funktionen:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Applås**.
3. Tryck på knapp.

4. Tryck på knappen bredvid **Smart upplåsning**, om funktionen ännu inte är aktiverad.
   Verifiera med ditt fingeravtryck eller din PIN-kod.
   Första gången du aktiverar funktionen måste du aktivera platsbehörigheten. Tryck på **TILLÅTA** knappen och tryck sedan på **TILLÅTA** igen.
5. Knacka **LÄGG TILL** för att ställa in den Wi-Fi-anslutning du använder som betrodd.

När du ändrar dig, inaktivera funktionen och de Wi-Fi-nätverk som du har angett som betrodda kommer att behandlas som opålitliga.

5.11. Rapporter

Rapportfunktionen för en detaljerad logg över händelser som rör skanningsaktiviteten på din enhet.

När något som är relevant för din enhets säkerhet händer läggs ett nytt meddelande till i rapporterna.

Så här kommer du till avsnittet Rapporter:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Rapporter**.

Följande flikar är tillgängliga i fönstret Rapporter:

- **VECKORAPPORTER** - här har du tillgång till säkerhetsstatus och utförda uppgifter från innevarande och föregående vecka. Den aktuella veckans rapport genereras varje söndag och du kommer att få ett meddelande om att den blir tillgänglig.
  Varje vecka kommer ett nytt tips att visas i det här avsnittet, så se till att du tittar in regelbundet för att få ut det bästa av appen.
  Så här slutar du ta emot aviseringar varje gång en rapport genereras:

  1. Knacka **Mer** på det nedre navigeringsfältet.
  2. Knacka **inställningar**.
  3. Inaktivera **Ny rapportavisering** växla i området Rapporter.

- **AKTIVITETS LOGG** - här kan du kontrollera detaljerad information om aktiviteten för din Bitdefender Mobile Security-app sedan den installerades på din Android-enhet.

Så här tar du bort den tillgängliga aktivitetsloggen:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Knacka **Rensa aktivitetsloggoch** tryck sedan på **KLAR**.

5.12. Bära PÅ

Med Bitdefender WearON kan du enkelt hitta din smartphone oavsett om du lämnade den på kontoret i ett konferensrum eller under en kudde i soffan. Enheten kan hittas även om det tysta läget är aktiverat.

Håll den här funktionen aktiverad för att se till att du alltid har din smartphone till hands.

Notera
Funktionen fungerar med Android 4.3 och Android Wear.

5.12.1. Aktiverar WearON

För att använda WearON behöver du bara ansluta din smartklocka till Bitdefender Mobile Security-appen och aktivera funktionen med följande röstkommando:

Start:<Var är min telefon>

Bitdefender WearON har två kommandon:

1. **Telefonvarning**
   Med funktionen Telefonvarning kan du snabbt hitta din smartphone när du går för långt bort från den.
   Om du har din smartklocka med dig känner den automatiskt av appen på din telefon och vibrerar när du går för långt från telefonen, mer exakt när Bluetooth-anslutningen tappas.
   För att aktivera den här funktionen, öppna Bitdefender Mobile Security, tryck på **Globala inställningar** i menyn och välj motsvarande omkopplare under WearON-sektionen.
2. **Skrika**

Att hitta din telefon har aldrig varit enklare. När du glömmer var du lämnade telefonen trycker du på kommandot Scream på klockan för att få telefonen att skrika.

5.13. Handla om

För att hitta information om Bitdefender Mobile Security-versionen som du har installerat, för att komma åt och läsa prenumerationsavtalet och integritetspolicyn, och se Open-source-licenserna:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Tryck på önskat alternativ i området Om.

5.14. Vanliga frågor

Varför kräver Bitdefender Mobile Security en internetanslutning?

Appen måste kommunicera med Bitdefender-servrar för att fastställa säkerhetsstatusen för apparna som den skannar och för webbsidorna du besöker, och även för att ta emot kommandon från ditt Bitdefender-konto när du använder stöldskyddsfunktionerna.

Vad behöver Bitdefender Mobile Security varje behörighet för?

- Internetåtkomst -> används för molnkommunikation.
- Läs telefonstatus och identitet -> används för att upptäcka om enheten är ansluten till internet och för att extrahera viss enhetsinformation som behövs för att skapa ett unikt ID när du kommunicerar med Bitdefender-molnet.
- Läs och skriv webbläsarbokmärken -> Webbskyddsmodulen tar bort skadliga webbplatser från din webbhistorik.
- Läs loggdata -> Bitdefender Mobile Security upptäcker spår av hotaktiviteter från Android-loggarna.
- Plats -> krävs för fjärrplats.
- Kamera -> krävs för Snap-foto.
- Lagring -> används för att tillåta skannern för skadlig programvara att kontrollera SD-kortet.

Hur kan jag sluta skicka information till Bitdefender om misstänkta appar?

Som standard skickar Bitdefender Mobile Security rapporter till Bitdefender-servrar om de misstänkta appar som du installerar. Denna information är viktig för att förbättra hotupptäckten och kan hjälpa oss att erbjuda dig en bättre upplevelse i framtiden. Om du vill sluta skicka information om misstänkta appar till oss:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Stäng av **Detektering i molnet** i området Malware Scanner.

Var kan jag se detaljer om appens aktivitet?

Bitdefender Mobile Security för en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden relaterade till dess aktivitet. För att komma åt se om appens aktivitet:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Rapporter**.
   I fönstret VECKRAPPORTER kan du komma åt rapporterna som genereras varje vecka och i fönstret AKTIVITETSLOGG kan du se information om aktiviteten i din Bitdefender-app.

Jag glömde PIN-koden som jag ställde in för att skydda min app. Vad gör jag?

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och tryck sedan på i det övre högra hörnet av skärmen.
4. Välj **inställningar**.
5. Hämta PIN-koden från **Applikations-PIN** fält.

Hur kan jag ändra PIN-koden jag ställer in för applås och stöldskydd?

Om du vill ändra PIN-koden du ställer in för applås och stöldskydd:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.

3. Tryck på Säkerhet **PINKOD** i stöldskyddsområdet.
4. Skriv in den aktuella PIN-koden.
5. Skriv in den nya PIN-koden du vill ställa in.

Hur kan jag stänga av applåsfunktionen?

Det finns inget avstängningsalternativ för applåsfunktionen, men du kan enkelt inaktivera den genom att avmarkera kryssrutorna bredvid de valda apparna efter att ha validerat PIN-koden eller fingeravtrycket du har angett.

Hur kan jag ställa in ett annat trådlöst nätverk som tillförlitligt?

Först måste du ansluta din enhet till det trådlösa nätverk du vill ställa in som betrodd. Följ sedan dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Applås**.
3. Knacka i det övre högra hörnet.
4. Knacka **LÄGG TILL** bredvid nätverket du vill ställa in som tillförlitligt.

Hur kan jag sluta se tagna bilder tagna på mina enheter?

Så här slutar du göra synliga foton som tagits på dina enheter:

1. Tillgång Bitdefender Central.
2. Knacka i den övre högra sidan av skärmen.
3. Knacka **inställningar** i bildmenyn.
4. Inaktivera **Visa/visa inte snapbilder tagna på dina enheter** alternativ.

Hur kan jag hålla min onlineshopping säker?

Online shopping kommer med höga risker när vissa detaljer ignoreras. För att inte bli offer för bedrägeri rekommenderar vi följande:

- Håll din säkerhetsapp uppdaterad.
- Skicka onlinebetalningar endast med köparskydd.
- Använd ett VPN när du ansluter till internet från offentliga och osäkra trådlösa nätverk.

- Var uppmärksam på lösenorden du har tilldelat dina onlinekonton. De måste vara starka inklusive stora och små bokstäver, siffror och symboler (@, !, %, #, etc.).
- Se till att informationen du skickar är över säkra anslutningar. Webbplatstillägget online måste vara HTTPS:// och inte HTTP://.

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du använder, laddar ner eller laddar upp innehåll på internet. För att se till att du är säker när du surfar på webben rekommenderar vi att du använder Bitdefender VPN när du:

- vill ansluta till offentliga trådlösa nätverk
- vill komma åt innehåll som normalt är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, kreditkortsinformation, etc.)
- vill dölja din IP-adress

Kommer Bitdefender VPN att ha en negativ inverkan på batteritiden för min enhet?

Bitdefender VPN är utformad för att skydda dina personliga data, dölja din IP-adress när du är ansluten till osäkra trådlösa nätverk och komma åt begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning av din enhet rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort när du är offline.

Varför stöter jag på internetnedgångar när jag är ansluten till Bitdefender VPN?

Bitdefender VPN är designad för att erbjuda dig en lätt upplevelse när du surfar på webben; din internetanslutning eller serveravståndet du ansluter till kan dock orsaka nedgången. I det här fallet, om det inte är ett måste att ansluta från din plats till en fjärransluten server (t.ex. från USA till Kina), rekommenderar vi att du tillåter Bitdefender VPN att automatiskt ansluta dig till närmaste server, eller hitta en server närmare din nuvarande plats.

Kan jag ändra Bitdefender-kontot som är länkat till min enhet?

Ja, du kan enkelt ändra Bitdefender-kontot som är länkat till din enhet genom att följa dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Tryck på din e-postadress.
3. Knacka **Logga ut från ditt konto**. Om en PIN-kod har ställts in, uppmanas du att ange den.
4. Bekräfta ditt val.
5. Skriv in e-postadressen och lösenordet för ditt konto i motsvarande fält och tryck sedan på **LOGGA IN**.

Hur kommer Bitdefender Mobile Security att påverka min enhets prestanda och batteriautonomi?

Vi håller effekten väldigt låg. Appen körs bara när det är nödvändigt – efter att du installerat en app, när du surfar i appens gränssnitt eller när du vill ha en säkerhetskontroll. Bitdefender Mobile Security körs inte i bakgrunden när du ringer dina kompisar, skriver ett meddelande eller spelar ett spel.

Vad är enhetsadministratör?

Enhetsadministratör är en Android-funktion som ger Bitdefender Mobile Security de behörigheter som behövs för att utföra vissa uppgifter på distans. Utan dessa privilegier skulle fjärrlås inte fungera och enhetsrensning skulle inte kunna ta bort dina data helt. Om du vill ta bort appen, se till att återkalla dessa privilegier innan du försöker avinstallera från **Inställningar > Säkerhet > Välj enhetsadministratörer**.

Så här fixar du felet "Inget Google Token" som visas när du loggar in på Bitdefender Mobile Security.

Det här felet uppstår när enheten inte är kopplad till ett Google-konto, eller när enheten är kopplad till ett konto men ett tillfälligt problem hindrar den från att ansluta till Google. Prova någon av följande lösningar:

- Gå till Android-inställningar > Applikationer > Hantera applikationer > Bitdefender Mobile Security och tryck på **Radera data**. Försök sedan logga in igen.
- Se till att din enhet är kopplad till ett Google-konto.
  För att kontrollera detta, gå till Inställningar > Konton och synkronisering och se om ett Google-konto är listat under **Hantera konton**. Lägg till ditt konto om ett inte finns med i listan, starta om din enhet och försök sedan logga in på Bitdefender Mobile Security.

- Starta om enheten och försök sedan logga in igen.

På vilka språk är Bitdefender Mobile Security tillgängligt?

Bitdefender Mobile Security är för närvarande tillgängligt på följande språk:

- brasiliansk
- tjeckiska
- holländska
- engelsk
- franska
- tysk
- grekisk
- ungerska
- italienska
- japanska
- koreanska
- putsa
- portugisiska
- rumänska
- ryska
- spanska
- svenska
- Thai
- turkiska
- vietnamesiska

Andra språk kommer att läggas till i framtida utgåvor. För att ändra språket för Bitdefender Mobile Security-gränssnittet, gå till din enhets **Språk & tangentbord** inställningar och ställ in enheten på det språk du vill använda.

6. MOBIL SÄKERHET FÖR IOS

6.1. Vad är Bitdefender Mobile Security för iOS

Onlineaktiviteter som att betala räkningar, göra semesterbokningar eller köpa varor och tjänster är bekväma och problemfria. Men eftersom många aktiviteter har utvecklats på internet, kommer dessa med höga risker och, om säkerhetsdetaljer ignoreras, kan personuppgifter hackas. Och vad är viktigare än att skydda data som lagras på onlinekonton och på den personliga smartphonen?

Bitdefender Mobile Security för iOS låter dig:

- Få det mest kraftfulla skyddet mot hot med minsta möjliga påverkan på batteriet
- Skydda dina personuppgifter: lösenord, adress, social och ekonomisk information
- Kontrollera enkelt telefonens säkerhet för att upptäcka och åtgärda felkonfigurationer som kan avslöja den
- Undvik oavsiktlig dataexponering och missbruk för alla installerade appar
- Skanna din enhet för att uppnå optimala säkerhets- och sekretessinställningar
- Få användningsinsikter om din onlineaktivitet och historik över förhindrade incidenter
- Kontrollera dina onlinekonton mot dataintrång eller dataläckor
- Kryptera internettrafik med det medföljande VPN

Bitdefender Mobile Security för iOS levereras gratis och kräver aktivering med en Bitdefender-konto. Vissa viktiga funktioner i Bitdefender, såsom vår "Web Protection"-modul, kräver dock en betald prenumeration för att vara tillgängliga för våra användare.

6.2. Komma igång

6.2.1. Enhetskrav

Bitdefender Mobile Security för iOS fungerar på alla enheter som kör iOS 12 eller senare versioner av operativsystemet och behöver en

aktiv internetanslutning för att aktiveras och för att upptäcka om något dataläckage har inträffat i dina onlinekonton.

6.2.2. Installera Bitdefender Mobile Security för iOS

- **Från Bitdefender Central**
  - På iOS
    1. Tillgång Bitdefender Central.
    2. Välj **Mina enheter** panel.
    3. Knacka **INSTALLATIONSSKYDD**och tryck sedan på **Skydda den här enheten**.
    4. Välj enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    5. Du omdirigeras till **App Store** app. På App Store-skärmen trycker du på installationsalternativet.
  - På Windows, macOS, Android
    1. Tillgång Bitdefender Central.
    2. Välj **Mina enheter** panel.
    3. Tryck **INSTALLATIONSSKYDD**, och tryck sedan på **Skydda andra enheter**.
    4. Välj enhetens ägare. Om enheten tillhör någon annan, tryck på motsvarande knapp.
    5. Tryck **SKICKA NEDLADDNINGSLÄNK**.
    6. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.
    7. På enheten du vill installera Bitdefender kontrollera e-postkontot som du skrev in och tryck sedan på motsvarande nedladdningsknapp.
- **Från App Store**

Sök efter Bitdefender Mobile Security för iOS för att hitta och installera appen.

Ett introduktionsfönster med information om produktens funktioner visas första gången du öppnar appen. Tryck på Kom igång för att fortsätta till nästa fönster.

Innan du går igenom valideringsstegen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren under vilka du får använda Bitdefender Mobile Security för iOS.

Knacka **Fortsätta** för att gå vidare till nästa fönster.

6.2.3. Logga in på ditt Bitdefender-konto

För att använda Bitdefender Mobile Security för iOS måste du länka din enhet till ett Bitdefender-, Facebook-, Google-, Apple- eller Microsoft-konto genom att logga in på kontot från appen. Första gången du öppnar appen uppmanas du att logga in på ett konto.

Så här länkar du din enhet till ett Bitdefender-konto:

1. Skriv in e-postadressen för ditt Bitdefender-konto i motsvarande fält och tryck sedan på **NÄSTA**. Om du inte har ett Bitdefender-konto och vill skapa ett, välj motsvarande länk och följ sedan instruktionerna på skärmen tills kontot är aktiverat.
   För att logga in med ett Facebook-, Google-, Apple- eller Microsoft-konto, tryck på tjänsten du vill använda från **Eller logga in** med område. Du omdirigeras till inloggningssidan för den valda tjänsten. Följ instruktionerna för att länka ditt konto till Bitdefender Mobile Security för iOS.

   > **Notera**
   > Bitdefender får inte tillgång till någon konfidentiell information som lösenordet för kontot du använder för att logga in eller personlig information om dina vänner och kontakter.

2. Skriv ditt lösenord och tryck sedan på **LOGGA IN**.

Härifrån kan du också komma åt Bitdefender sekretesspolicy.

6.2.4. instrumentbräda

Tryck på Bitdefender Mobile Security för iOS-ikonen i enhetens applåda för att öppna applikationsgränssnittet.

Första gången du öppnar appen uppmanas du att tillåta Bitdefender att skicka meddelanden till dig. Knacka **Tillåta** att hålla sig informerad varje gång Bitdefender måste kommunicera dig något som är relevant för din app. För att hantera Bitdefender-aviseringar, gå till Inställningar > Meddelanden > Mobilsäkerhet.

För att få tillgång till avsnittet du behöver, tryck på motsvarande ikon längst ned på skärmen.

Nätskydd

Var säker medan du surfar på webben och när mindre säkra appar försöker komma åt opålitliga domäner. För mer information, se Nätskydd (sida 214).

VPN

Behåll din integritet oavsett vilket nätverk du är ansluten till genom att hålla din internetkommunikation krypterad. För mer information, se VPN (sida 216).

Kontosekretess

Ta reda på om dina e-postkonton har läckt eller inte. För mer information, se Kontosekretess (sida 219).

För att se ytterligare alternativ, tryck på ••• ikonen på din enhet när du är på programmets startskärm. Följande alternativ visas:

- **Återställa köp** - härifrån kan du återställa de tidigare prenumerationer du har köpt via ditt iTunes-konto.
- **inställningar** - härifrån har du tillgång till:
  - **VPN-inställningar**
    - **Avtal** - du kan läsa villkoren under vilka du använder Bitdefender VPN-tjänsten. Om du trycker på **Jag håller inte med längre**, kommer du inte att kunna använda Bitdefender VPN åtminstone förrän du trycker **Jag håller med**.
    - **Öppna Wi-Fi-varning** - du kan aktivera eller inaktivera produktaviseringen som visas varje gång du ansluter till ett osäkrat Wi-Fi-nätverk.

Syftet med detta meddelande är att hjälpa dig att hålla dina data privata och säkra genom att använda Bitdefender VPN.

- **Webbskyddsinställningar**
  - **Avtal** - du kan läsa villkoren under vilka du använder tjänsten Bitdefender Web Protection. Om du trycker på **Jag håller inte med längre**, kommer du inte att kunna använda Bitdefender VPN åtminstone förrän du trycker **Jag håller med**.
  - **Aktivera webbskyddsmeddelande** - Meddelar dig att webbskydd kan aktiveras efter avslutad VPN-session.
- **Produktrapporter**

- **Respons** - härifrån kan du starta standarde-postklienten för att skicka oss din feedback om appen.
- **App info** - härifrån har du tillgång till information om den installerade versionen och till prenumerationsavtal, integritetspolicy och överensstämmelse med öppen källkod.

6.3. Skanna

Bitdefender Mobile Security för iOS låter dig skanna din enhet efter eventuella säkerhetsbrister och potentiella hot på din enhet. Att köra skanningen kommer att söka efter:

- **OS-version:** Kontrollerar din iOS-version för de senaste uppdateringarna.
- **Lösenord/biometri:** Kontrollera säkerhetsnivån när det gäller åtkomst till din enhet.
- **Nätskydd:** Kontrollerar webbskyddsmodulens tillstånd
- **Kontosekretess:** Kontrollerar om det finns övervakade konton som anges i modulen Kontosekretess.
- **Skanna Wi-Fi:** Söker efter säkerhetsstatus för det för närvarande anslutna nätverket.

Skyddsstatusen bestäms efter att du kört en manuell skanning.

Efter att ha kört den första skanningen kommer du att mötas av Bitdefenders Autopilotrekommendationer. Det här är din personliga säkerhetsrådgivare som ger kontextuella rekommendationer baserat på

din enhetsanvändning och behov. På så sätt kan du dra nytta av allt som din app har att erbjuda.

> **Notera**
> När du först går in i appen blir du ombedd att köra en skanning.

6.4. Scam Alert

Scam Alert-funktionen som är tillgänglig i Bitdefender Mobile Security för iOS skyddar proaktivt Apple-användare från nätfiske. Scam Alert för iOS inkluderar två lager av skydd som övervakar bedrägerier som levereras via SMS/MMS-meddelanden och kalenderinbjudningar:

- **Textmeddelandefilter (SMS, MMS)**
  Den här funktionen identifierar och filtrerar oönskade SMS- och MMS-meddelanden.
  Ett skadligt SMS/MMS (Short Message Service/Multimedia Messaging Service) hänvisar till en typ av meddelande som skickas till mobila enheter med skadlig avsikt. Dessa meddelanden är utformade för att utnyttja sårbarheter, lura mottagare eller orsaka skada på målets enhet, personliga information eller säkerhet.
- **Calendar Invite Link Scanner**
  Den här funktionen upptäcker skräppostkalendrar och händelser som innehåller farliga länkar. Kalenderviruset är en typ av spam som påverkar kalenderappen på din iPhone, vilket kan vara irriterande och potentiellt farligt:
  - Du får oönskade kalenderinbjudningar eller händelseaviseringar när du av misstag accepterar en falsk kalenderinbjudan som skickas till din e-postadress av hackare eller spammare.
  - När du klickar på länken i inbjudan prenumererar du omedvetet på avsändarens kalender, vilket gör att de kan skicka fler spamhändelser till dig.
  - Spamhändelserna kan innehålla länkar eller bilagor som kan leda dig till nätfiskesidor eller andra cyberhot om du öppnar dem.

6.4.1. Hur man ställer in Scam Alert

För att aktivera Scam Alert måste du ge Bitdefender Mobile Security-appen åtkomst till kalenderaviseringar och SMS-meddelanden:

Så här aktiverar du SMS-filtrering:

För att Bitdefender ska börja filtrera meddelanden måste du manuellt aktivera alternativet Filtrera okända avsändare i inställningarna för appen Meddelanden:

1. Öppna **inställningar** app på din iPhone eller iPad.
2. Rulla ned och välj **Meddelanden** i listan.
3. Tryck på **Okänd & Spam** sektion.
4. Växla **Filtrera okända avsändare** till på-läget.
5. Välj **Mobil säkerhet** i avsnittet SMS-filtrering och välj sedan **Gör det möjligt**.

Bitdefender kommer nu att kunna filtrera skräpmeddelanden på din iPhone/iPad.

> **Notera**
> På grund av iOS-begränsningar kan Bitdefender SMS-filtrering endast användas för SMS- och MMS-meddelanden som kommer från personer som du inte har sparat i dina kontakter. Det betyder att det inte kommer att filtrera meddelanden från personer som redan finns i din kontaktlista eller iMessage-meddelanden från någon.

Så här aktiverar du kalenderskanning:

1. Öppna **Bitdefender Mobile Security** app installerad på din iPhone eller iPad.
2. Gå till **Scam Alert** alternativet i det nedre navigeringsfältet och tryck på **Ställ in nu**.
3. Knacka **Fortsätta** och tryck sedan på **Gör det möjligt**.
4. Välja **OK** för att ge Bitdefender åtkomst till din kalender. En kalenderskanning påbörjas omedelbart.

6.5. Scam Copilot

Den här funktionen är i huvudsak en AI-driven chatbot som utbildats av Bitdefender för att upptäcka olika bedrägerier, phishing-försök, kampanjer med felaktig information och falska webbplatser.

Så här aktiverar du Scam Copilot:

1. Öppna appen Bitdefender Mobile Security. I kontrollpanelen visas ett kort som gäller Scam Copilot. Tryck på **Aktivera**.
2. Du måste aktivera SMS-filtrering enligt anvisningarna nedan:
   a. Öppna **Inställningar** på din enhet.
   b. Välj **Meddelanden** från listan.
   c. Välj **Okänd och Spam**.
   d. Växla till ON **Filtrera okända avsändare**.
   e. Välj **Mobilsäkerhet** i SMS-filtrering.
3. När du är klar trycker du på **Fortsätt**.
4. Aktivera kalenderskanning. Ett popup-fönster visas på skärmen strax efter att du har tryckt på knappen **Aktivera**. Tryck på **Tillåt fullständig åtkomst**.

Scam Copilot är nu korrekt konfigurerad på din enhet.

Du kan komma åt den dedikerade fliken Scam Copilot. Här hittar du:

- **Scam Detection Chatbot:** Be chatbotten att granska alla meddelanden som du tycker är misstänkta.
- **Prevention Assistant:** Hjälper dig att lära dig mer om bedrägerier för att bli skicklig på att upptäcka dem.
- **Automatisk bedrägeridetektering** status och kontrollpanel.
- **SMS-filtrering**: Få dina farliga meddelanden filtrerade direkt i din meddelandeapp.

6.6. Nätskydd

Bitdefender Web Protection säkerställer en säker surfupplevelse genom att varna dig om potentiella skadliga webbsidor och när mindre säkra installerade appar försöker få åtkomst till opålitliga domäner.

När en URL pekar på en känd nätfiske eller bedräglig webbplats, eller till skadligt innehåll som spionprogram eller virus, blockeras webbsidan och en varning visas. Samma sak händer när installerade appar försöker komma åt skadliga domäner.

Viktig
Om du befinner dig i ett område där användningen av en VPN-tjänst är begränsad enligt lag, kommer funktionaliteten för webbskydd inte att vara tillgänglig.

Så här aktiverar du webbskydd:

1. Tryck på ikonen längst ned på skärmen.
2. Knacka **Jag håller med**.
3. Aktivera webbskyddsbrytaren.

Notera
Första gången du aktiverar webbskydd kan du bli ombedd att tillåta Bitdefender att ställa in VPN-konfigurationer som övervakar nätverkstrafik. Knacka **Tillåta**, att fortsätta. Om en autentiseringsmetod (fingeravtryck eller PIN-kod) har ställts in för att skydda din smartphone måste du använda den. För att kunna upptäcka åtkomst till opålitliga domäner arbetar Web Protection tillsammans med VPN-tjänsterna.

Viktig
Webbskyddsfunktionen och VPN kan inte fungera samtidigt. Närhelst en av dem är aktiverad, kommer den andra (om den är aktiv vid den tidpunkten) att inaktiveras.

6.6.1. Bitdefender-varningar

När du försöker besöka en webbplats som klassificeras som osäker blockeras webbplatsen. För att göra dig medveten om händelsen meddelas du av Bitdefender i meddelandecentret och i din webbläsare. Varningssidan innehåller information som webbadressen och det upptäckta hotet. Du måste bestämma dig för vad du ska göra härnäst.

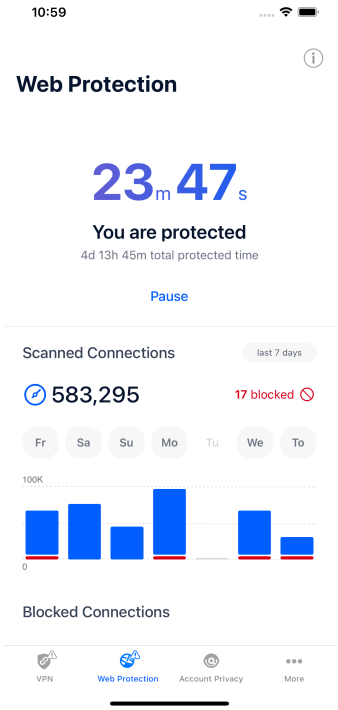
Du får också ett meddelande i meddelandecentret när en mindre säker app försöker få åtkomst till opålitliga domäner. Tryck på det visade meddelandet för att omdirigeras till fönstret där du kan bestämma vad du ska göra härnäst.

Följande alternativ är tillgängliga för båda fallen:

- Navigera bort från webbplatsen genom att trycka på **TA MIG TILLBAKA TILL SÄKERHET**.

- Fortsätt till webbplatsen, trots varningen, genom att trycka på det visade meddelandet och sedan **Jag vill komma åt sidan**.

Bekräfta ditt val.



6.7. VPN

Med Bitdefender VPN kan du hålla din data privat varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personlig data eller försök att göra din enhets IP-adress tillgänglig för hackare undvikas.

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter för att säkra din anslutning, kryptera data med kryptering av militär kvalitet och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet omöjlig att identifieras av din internetleverantör, genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via Bitdefender

Password Manager, kan du komma åt innehåll som normalt är begränsat i specifika områden.

> **Notera**
> Vissa länder utövar internetcensur och därför har användningen av VPN på deras territorium förbjudits enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen för första gången. Genom att fortsätta använda appen bekräftar du att du är medveten om tillämpliga landsbestämmelser och de risker som du kan utsättas för.

Så här aktiverar du Bitdefender VPN:

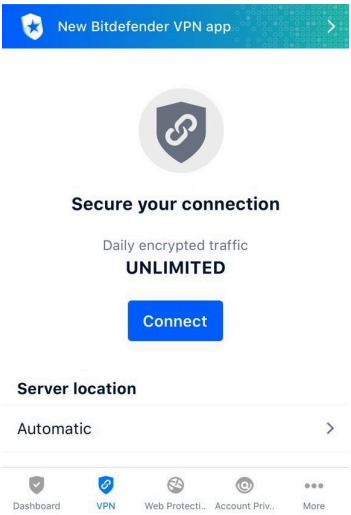
1. Tryck på ikonen längst ned på skärmen.
2. Knacka **Ansluta** varje gång du vill vara skyddad medan du är ansluten till osäkra trådlösa nätverk.
   Knacka **Koppla ifrån** när du vill inaktivera anslutningen.

> **Notera**
> Första gången du slår på VPN uppmanas du att tillåta Bitdefender att ställa in VPN-konfigurationer som övervakar nätverkstrafik. Knacka **Tillåta**, att fortsätta. Om en autentiseringsmetod (fingeravtryck eller PIN-kod) har ställts in för att skydda din smartphone måste du använda den.

De VPN ikonen visas i statusfältet när VPN är aktivt.

För att spara batteri, rekommenderar vi att du stänger av VPN när du inte behöver det.

Om du har ett premiumabonnemang och vill ansluta till en server som du vill, tryck på Automatisk i VPN-gränssnittet och välj sedan den plats du vill ha. Mer information om VPN-prenumerationer finns i Prenumerationer (sida 218).



6.7.1. Prenumerationer

Bitdefender VPN erbjuder gratis en daglig trafikkvot på 200 MB per enhet för att säkra din anslutning varje gång du behöver, och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad tillgång till innehåll över hela världen genom att välja en serverplats efter din vilja, uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-version när som helst genom att trycka på **Aktivera Premium VPN** knappen tillgänglig i VPN-fönstret. Det finns två typer av prenumerationer att välja mellan: års- och månadsabonnemang.

Bitdefender Premium VPN-prenumeration är oberoende av Bitdefender Mobile Security för iOS gratisabonnemang, vilket innebär att du kommer att kunna använda den under hela dess tillgänglighet. Om Bitdefender Premium VPN-prenumeration går ut, kommer du automatiskt att återgå till gratisplanen.

Bitdefender VPN är en plattformsoberoende produkt, tillgänglig i Bitdefender-produkter som är kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kommer du att kunna använda ditt abonnemang på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

Notera
Bitdefender VPN fungerar också som en fristående applikation på alla operativsystem som stöds, nämligen Windows, macOS, Android och iOS.

6.8. Kontosekretess

Bitdefender Account Privacy upptäcker om något dataläckage har inträffat på de konton du använder för att göra onlinebetalningar, handla eller logga in på olika appar eller webbplatser. De data som kan lagras på ett konto kan vara lösenord, kreditkortsinformation eller bankkontoinformation, och om den inte är ordentligt säkrad kan identitetsstöld eller intrång i integriteten förekomma.

Sekretessstatusen för ett konto visas direkt efter validering.

För att kontrollera om något av kontona har läckt, tryck på **Sök efter läckor**.

Så här börjar du hålla personlig information säker:

1. Tryck på ikonen längst ned på skärmen.
2. Knacka **Lägg till konto**.
3. Skriv din e-postadress i motsvarande fält och tryck sedan på **Nästa**.
   Bitdefender måste validera detta konto innan privat information visas. Därför skickas ett e-postmeddelande med en valideringskod till den angivna e-postadressen.
4. Kontrollera din inkorg och skriv sedan den mottagna koden i **Kontosekretess** område av din app. Om du inte kan hitta valideringse-postmeddelandet i mappen Inkorg, kontrollera även skräppostmappen.
   Sekretessstatusen för det validerade kontot visas.

Om läckor upptäcks på något av dina konton rekommenderar vi att du ändrar lösenordet så snart som möjligt. För att skapa ett starkt och säkert lösenord, ta hänsyn till dessa tips:

- Gör den minst åtta tecken lång.
- Inkludera gemener och versaler.
- Lägg till minst en siffra eller symbol, som #, @, % eller !.

När du väl har säkrat ett konto som var en del av ett integritetsintrång kan du bekräfta ändringarna genom att markera de identifierade läckorna som **Löst**. Att göra detta:

1. Knacka ··· bredvid intrånget du löste.
2. Knacka **Markera som löst**.

När alla upptäckta läckor är markerade som Lösta kommer kontot inte längre att visas som läckt, åtminstone tills ett nytt läckage upptäcks.

6.9. Vanliga frågor

Hur skyddar Bitdefender Mobile Security för iOS mig mot virus och cyberhot?

Bitdefender Mobile Security för iOS ger absolut skydd mot alla cyberhot och är speciellt utformad för att skydda din känsliga data från nyfikna ögon.

Du får en mängd avancerade säkerhets- och sekretessfunktioner för din iPhone och iPad – plus många bonusfunktioner, inklusive VPN och webbskydd.

Bitdefender Mobile Security för iOS reagerar omedelbart på virus och skadlig programvara utan att kompromissa med ditt systems prestanda.

Vilken typ av enheter och operativsystem täcker Bitdefender Mobile Security för iOS?

Bitdefender Mobile Security för iOS kommer att skydda dina smartphones och surfplattor som kör iOS mot alla cyberhot.

Varför behöver jag Bitdefender Mobile Security för iOS på Apple OS?

En del av dina mest personliga uppgifter lagras på din iPhone eller iPad – och du måste veta att den alltid är säker. Bitdefender Mobile Security för iOS ger absolut skydd mot cyberhot och tar hand om din integritet online och privat information utan att störa dina dagliga aktiviteter.

Får jag ett VPN med min Bitdefender Mobile Security för iOS-prenumeration?

Bitdefender Mobile Security för iOS kommer med en grundläggande version av Bitdefender VPN som inkluderar en generös mängd trafik (200 MB/dag, totalt 6GB/månad) gratis.

7. VPN

7.1. Vad är Bitdefender Password Manager

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter för att säkra din anslutning, kryptera data med militärklassad kryptering och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet omöjlig att identifieras av din internetleverantör, genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via Bitdefender VPN, kan du komma åt innehåll som normalt är begränsat i specifika områden.

> **Notera**
> Vissa länder utövar internetcensur och därför har användningen av VPN på deras territorium förbjudits enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender Password Manager funktion för första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om tillämpliga landsbestämmelser och de risker som du kan utsättas för.

7.1.1. Krypteringsprotokoll

Standarduppsättningarna för chiffersvit som är aktiverade i Hydra-klienten och servern finns nedan. Alla andra chiffersviter är inaktiverade.

Hydra Client ciphersuites:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Notera

Serversidans uppsättning är mycket mer restriktiv och både Hydra-klienten och servern kommer att avvisa ett läge som skiljer sig från GCM som använder AES. Hydra-servern upprätthåller serversidans prioritet för starkare chiffersviter och kommer att avvisa TLS-handskakning om en svagare svit efterfrågas av en klient. Denna lista är också konfigurerbar i runtime på serversidan.

7.2. Installation

7.2.1. Förbereder för installation

Innan du installerar Bitdefender Password Manager, slutför dessa förberedelser för att säkerställa att installationen går smidigt:

- Se till att enheten där du planerar att installera Bitdefender uppfyller systemkraven. Om enheten inte uppfyller alla systemkrav, Bitdefender kommer inte att installeras eller, om det är installerat, kommer det inte att fungera korrekt och det kommer att orsaka systemavbrott och instabilitet.
  För en fullständig lista över alla systemkrav, se Systemkrav (sida 222)
- Logga in på enheten med ett administratörskonto.
- Det rekommenderas att din enhet är ansluten till internet under installationen, även från en CD/DVD. Om nyare versioner av appfilerna som ingår i installationspaketet är tillgängliga, Bitdefender kan ladda ner och installera dem.

7.2.2. Systemkrav

- **För Windows-användare**
  - **Operativ system:**Windows 7 med Service Pack 1, Windows 8, Windows 8.1 Windows 10 och Windows 11
  - **Minne (RAM):**1 GB
  - **Tillgängligt ledigt hårddiskutrymme:**500 MB ledigt utrymme
  - **Net Framework:**min version 4.5.2

Viktig
Systemprestandan kan påverkas på enheter som har gamla generationens processorer.

- **För macOS-användare**
  - **Operativ system:**macOS Sierra (10.12) eller senare
  - **Tillgängligt ledigt hårddiskutrymme:**100MB ledigt utrymme
- **För Android-användare**
  - **Operativ system:**Android 5.0 eller senare
  - **Lagring:**100 MB
  - En aktiv Internetanslutning
- **För iOS-användare**
  - **Operativ system:**iOS 12 eller senare
  - **Lagring på iPhone:**50 MB
  - **Lagring på iPad:**100 MB
  - En aktiv Internetanslutning

7.2.3. Installerar Bitdefender Password Manager

För att påbörja installationen, följ instruktionerna som motsvarar det operativsystem du använder:

- **För Windows-användare**
  1. För att påbörja installationen av Bitdefender Password Manager på en Windows-dator, börja helt enkelt med att ladda ner installationssatsen från https://www.bitdefender.com/solutions/vpn/download eller från e-postmeddelandet mottaget efter ett köp.
  2. Dubbelklicka på det nedladdade installationsprogrammet för att köra det.
  3. Välj Ja om det visas med dialogrutan Användarkontokontroll.
  4. Vänta tills nedladdningen är klar.

5. Välj produktspråk med hjälp av rullgardinsmenyn på installationsprogrammet.
6. Markera rutan "Jag bekräftar att jag har läst och jag godkänner prenumerationsavtalet och sekretesspolicyn", klicka sedan på **STARTA INSTALLATIONEN**.
7. Vänta tills installationen är klar.
8. **LOGGA IN** med ditt Bitdefender Central-konto. Om du inte har ett centralt konto, registrera dig för ett genom att klicka på knappen **SKAPA KONTO**.
9. Välja **Jag har en aktiveringskod** om du har köpt en Premium VPN-prenumeration.
   Annars kan du välja **STARTA TESTPERIOD** att testa produkten gratis i 7 dagar innan du förbinder dig att betala för den.
10. Skriv in koden som du fått via e-post och klicka sedan på **AKTIVERA PREMIUM** knapp.
11. Efter en kort väntan, Bitdefender Password Manager är installerat och redo att användas på din dator.

❍ **För macOS-användare**

1. För att påbörja installationen av Bitdefender Password Manager på macOS, börja helt enkelt med att ladda ner installationssatsen från https://www.bitdefender.com/solutions/vpn/download eller från e-postmeddelandet mottaget efter ett köp.
2. Installationsprogrammet kommer att sparas på Mac. I mappen Nedladdningar dubbelklickar du på paketfilen.
3. Följ instruktionerna på skärmen. Välja **Fortsätta**.
4. Du kommer att guidas genom de steg som krävs för att installera Bitdefender Password Manager på din Mac. Klicka två gånger **Fortsätta** knapp.
5. Klick **Hålla med**, efter att du har läst och godkänt villkoren i programvarulicensavtalet.
6. Klick **Installera**.
7. Ange ett användarnamn och lösenord för administratören och klicka sedan **Installera programvara**.

8. Du kommer att meddelas att ett systemtillägg undertecknats av Bitdefender har blockerats. Detta är inte ett fel, bara en säkerhetskontroll. Klick **Öppna Säkerhetsinställningar**.
9. Klicka på låsikonen för att låsa upp den.
   Ange ett administratörsnamn och lösenord och tryck sedan på **Låsa upp**.
10. Klick **Tillåta** för att ladda BitdefenderBitdefenders systemtillägg. Stäng sedan fönstret Säkerhet och sekretess och installationsprogrammet.
11. Gå sedan till sköldikonen i menyraden **Logga in** med ditt Bitdefender Central-konto. Om du inte har ett centralt konto, vänligen registrera dig för ett.
12. Välj jag har en **Aktiveringskod** om du har köpt en Premium VPN-prenumeration.
    Annars kan du välja **STARTA TESTPERIOD** att testa produkten gratis i 7 dagar innan du förbinder dig att betala för den.
13. Skriv in koden som du fått via e-post och klicka sedan på **Aktivera kod** knapp.
14. Efter en kort väntan, Bitdefender Password Manager är installerat och redo att användas på din Mac.

❍ **För Android-användare**

1. Att installera Bitdefender Password Manager på Android öppnar du först **Google Play Butik** app på din smartphone eller surfplatta.
2. Söka efter Bitdefender Password Manager och välj den här appen.
3. Tryck på **Installera** och vänta tills nedladdningen är klar.
4. Knacka **Öppen** för att köra appen.
5. Markera rutan "Jag godkänner prenumerationsavtalet och sekretesspolicyn" och tryck sedan på **Fortsätta**.
6. **Logga in** med ditt Bitdefender Central-konto. Om du inte har ett centralt konto, registrera dig för ett genom att trycka på **Skapa konto**.
7. Välja **Jag har en aktiveringskod** om du har köpt en Premium VPN-prenumeration.

Annars kan du välja Starta 7 dagars provperiod för att testa produkten gratis i 7 dagar innan du åtar dig att betala för den.

8. Skriv in koden som du fått via e-post och tryck sedan på **Aktivera kod**.

- **För iOS-användare**

1. Att installera Bitdefender Password Manager på iOS, öppnas först **App Store** på din iPhone eller iPad.
2. Söka efter Bitdefender Password Manager och välj den här appen.
3. Tryck på **Skaffa sig** och vänta tills nedladdningen är klar.
4. Knacka **Öppen** för att köra appen.
5. Markera rutan **Jag godkänner prenumerationsavtalet och sekretesspolicyn**, tryck sedan på **Fortsätta**.
6. **Logga in** med ditt Bitdefender Central-konto. Om du inte har ett konto, registrera dig för ett genom att trycka på **Skapa konto**.
7. Knacka **Tillåta** om du vill ta emot Bitdefender Password Manager meddelanden.
8. Välja **Jag har en aktiveringskod** om du har köpt en Premium VPN-prenumeration.
   Annars kan du välja Starta 7 dagars provperiod för att testa produkten gratis i 7 dagar innan du åtar dig att betala för den.
9. Skriv in koden som du fått via e-post och tryck sedan på **Aktivera kod**.

7.3. Använder Bitdefender VPN

7.3.1. Öppnar Bitdefender VPN

- **För Windows**

  För att komma åt**huvudgränssnittet för Bitdefender VPN**, använd någon av följande metoder:

  - **Från systemfältet**

    Högerklicka på den röda sköldikonen i systemfältet och välj sedan **Show** i menyn.

- **Från Bitdefender-gränssnittet**
  Om en Bitdefender-säkerhetsprodukt som Bitdefender Total Security eller Bitdefender Antivirus Plus etc. redan är installerad på din Windows-dator, kan du öppna Bitdefender VPN därifrån:

  1. Klick **Integritet** på vänster sidofält i Bitdefender-gränssnittet.
  2. Klick **Öppna VPN** på VPN-rutan.

- **Från ditt skrivbord**
  Dubbelklicka på Bitdefender VPN-genvägen på ditt skrivbord.

- **För macOS**

  Du kan öppna Bitdefender VPN-appen genom att klicka på ikonen från menyraden längst upp till höger på skärmen.
  Om Bitdefender-skölden inte kan hittas i menyraden, använd din Mac Launchpad eller Finder för att ta tillbaka den:

  - **Från Launchpad**

    1. Tryck**F4**på ditt tangentbord för att öppna Launchpad på din Mac.
    2. Bläddra igenom sidorna med installerade appar tills du hittar Bitdefender VPN-appen. Alternativt kan du skriva**Bitdefender VPN**i Launchpad för att börja filtrera dina resultat.
    3. När du ser Bitdefender VPN-appen klickar du på dess ikon för att fästa den i menyraden.

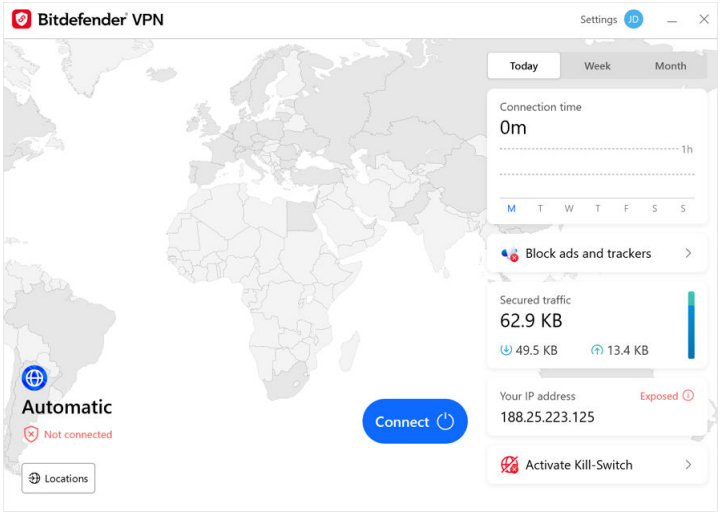
  - **Från Finder**

    1. Klicka på**Upphittare**längst ner till vänster i Dock (Finder är ikonen som ser ut som en blå fyrkant med en smiley).
    2. Klicka sedan**Gå**längst upp till vänster på skärmen, i menyraden.
    3. Välj**Ansökningar**från menyn för att öppna mappen Program på din Mac.
    4. Öppna mappen Applications**Bitdefender**mapp och dubbelklicka sedan på**Bitdefender VPN**app.

> **Notera**
> För att komma åt Bitdefender VPN på dina Android- eller iOS-mobilenheter, öppna helt enkelt Bitdefender VPN-applikationen efter att du har installerat den.

7.3.2. Hur man ansluter till Bitdefender Password Manager

VPN-gränssnittet visar status för appen: ansluten eller frånkopplad. Serverplatsen för användare med gratisversionen ställs automatiskt in av Bitdefender till den mest lämpliga servern, medan premiumanvändare har möjlighet att ändra serverplatsen de vill ansluta till genom att välja den från listan med virtuell plats. För att ansluta eller koppla från, klicka helt enkelt på strömknappen från VPN-gränssnittet.



- **För Windows:** Ikonen i systemfältet visar en grön bock när VPN är ansluten och en svart markering när VPN är frånkopplat. När du är ansluten till en manuellt vald plats visas IP-adressen på huvudgränssnittet.
- **För macOS:** Menyradens ikon visar svart när VPN är anslutet, och vit när VPN är frånkopplat. Klicka på den cirkulära knappen i mitten av gränssnittet och vänta tills anslutningen upprättas.
- **För Android och iOS:** För att ansluta till Bitdefender VPN för Android, iOS och iPadOS:

- **I Bitdefender VPN-appen:** För att ansluta eller koppla från, tryck bara på strömknappen på VPN-gränssnittet. Status för Bitdefender VPN visas.
- **I Bitdefender Mobile Security-appen:**
  1. Få tillgång till VPN-ikon i det nedre navigeringsfältet i Bitdefender Mobile Security.
  2. Knacka**ANSLUTA**varje gång du vill vara skyddad medan du är ansluten till osäkra trådlösa nätverk. Knacka**KOPPLA IFRÅN**närhelst du vill inaktivera VPN-anslutningen.

7.3.3. Hur man ansluter till en annan server

Med en Premium-prenumeration, Bitdefender Password Manager låter dig ansluta till någon av våra servrar runt om i världen, när som helst. För att göra detta måste du:

1. Öppna Bitdefender Password Manager app.
2. Tryck på **Virtuell plats** knappen i den nedre delen av gränssnittet.
3. Välj vilket land du vill.
4. Klicka på **Anslut till [valfritt land]** knappen i den nedre delen av gränssnittet.

- Ikonen i systemfältet visar en grön bock när VPN är anslutet.
- Den virtuella serverns IP-adress visas på startskärmen när den är ansluten till Bitdefender VPN.
- En sammanfattning av din anslutningstid, mängden säker trafik och de senaste 5 platserna du anslutit till visas också på huvudinstrumentpanelen.

7.4. Bitdefender Password Manager Inställningar och funktioner

7.4.1. Åtkomst till inställningar

För att komma åt Bitdefender Password Manager inställningar måste du följa stegen som beskrivs nedan:

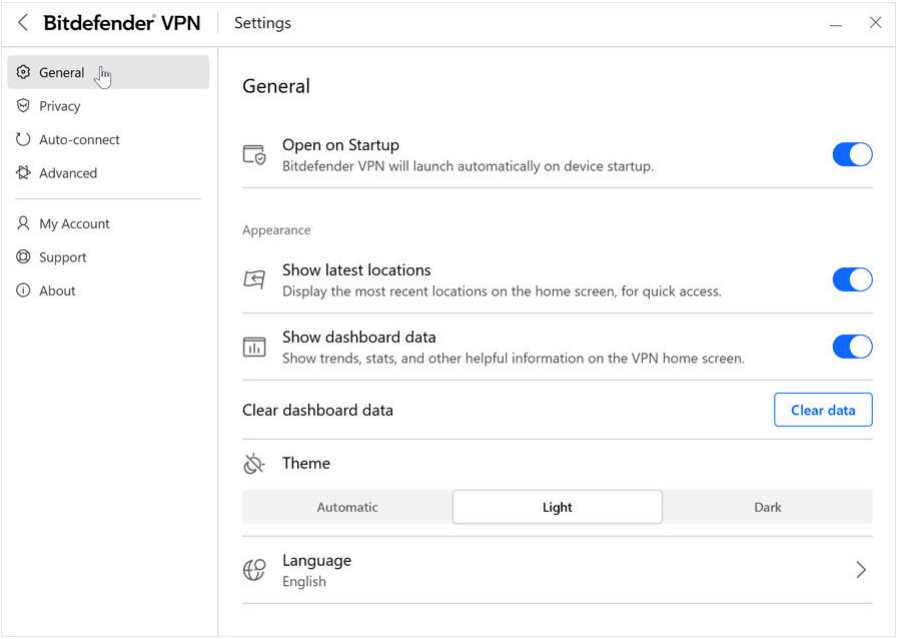
- **På Windows**
  1. Öppna Bitdefender Password Manager app på din enhet genom att dubbelklicka på dess ikon i systemfältet eller genom att högerklicka på den och välja Visa.
  2. Klicka på **inställningar** knappen (representerad av ett kugghjul) på vänster sida av gränssnittet.
- **På macOS**
  1. Öppna Bitdefender Password Manager app på din macOS-enhet genom att klicka på dess ikon i menyraden.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender Password Manager gränssnittet och välj Inställningar.
- **På Android**
  1. Öppna Bitdefender Password Manager app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender Password Manager gränssnitt.
- **På iOS**
  1. Öppna Bitdefender Password Manager app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender Password Manager gränssnitt.

7.4.2. Allmän

Här kan du ändra följande:

- **Öppna vid start**– Bitdefender VPN startar automatiskt vid start av enheten.
- **Visa senaste platserna**– Visa de senaste platserna på startskärmen för snabb åtkomst.
- **Visa instrumentpanelsdata** – Visa trender, statistik och annan användbar information på VPN-startskärmen.
- **Rensa instrumentpanelsdata**– Alla dina instrumentpaneldata kommer att raderas och alla räknare återställs.
- **Tema**– Ljus/mörkt tema

- **Språk**– Ändra språket för Bitdefender VPN.
- **Aviseringar**– Hantera dina aviseringsinställningar.
- **Hjälp till att förbättra Bitdefender VPN**– Skicka in anonyma produktrapporter för att hjälpa oss att förbättra din upplevelse.
- **Återställ alla inställningar**– Återställ VPN till dess ursprungliga inställningar utan att installera om det.



7.4.3. Funktioner

Integritet

Internet Kill-Switch

Kill-Switch är en ny funktion implementerad i Bitdefender Password Manager. När den är aktiverad stänger den här funktionen tillfälligt av all internettrafik om VPN-anslutningen av misstag avbryts. Så snart du är online igen kommer VPN-anslutningen att återupprättas.

För att aktivera Kill-Switch, följ stegen nedan:

- **På Windows**
  1. Öppna Bitdefender Password Manager app på din enhet genom att dubbelklicka på dess ikon i systemet försök eller genom att högerklicka på den och välja **Show**.
  2. Klicka på **inställningar** knappen (representerad av ett kugghjul) på vänster sida av gränssnittet.
  3. Välj **Avancerad**.
  4. Aktivera **Internet Kill-Switch** alternativ.

- **På Android**
  1. Öppna Bitdefender Password Manager app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender Password Manager gränssnitt.
  3. Under **inställningar**, aktivera **Kill-Switch** alternativ.

- **På iOS**
  1. Öppna Bitdefender Password Manager app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender Password Manager gränssnitt.
  3. Under **inställningar**, aktivera **Kill-Switch** alternativ.

> **Notera**
> Den här funktionen är även tillgänglig för macOS-enheter med operativsystem 10.15.4 eller senare versioner.

Annonsblockerare och Anti-tracker

Dessa funktioner är utformade för att hjälpa dig att hålla dig privat och njuta av webben utan irriterande annonser eller företag som tittar in på dig. De hjälper till att blockera annonser och stoppa onlinespårare.

Annonsblockerare

De **Annonsblockerare** används för att blockera annonser, popup-fönster, högljudda videoannonser eller annonsbanner medan du surfar. Detta hjälper webbplatser att laddas snabbare och vara renare, samt säkrare att interagera med.

Så här aktiverar du annonsblockeraren:

1. Leta upp **Annonsblockerare och Antitracker** inslag i **inställningar**.
2. Växla omkopplaren till **PÅ** placera.

Antispårare

De **Antispårare** används för att blockera spårare som angetts av annonsörer för att följa och profilera dig online. Vissa webbplatser kan inte fungera när spårare blockeras, men att lägga till webbadressen till vitlistan kan fixa detta.

Så här aktiverar du Anti-tracker:

1. Leta upp **Annonsblockerare och Antitracker** inslag i **inställningar**.
2. Växla omkopplaren till **PÅ** placera.

Vitlista

Vissa webbplatser kanske inte laddas korrekt om du blockerar deras spårningskod och annonser. Att lägga till webbadresserna för dessa specifika domäner till vitlistan kan lösa det här problemet, men kom ihåg att när du surfar på dessa webbplatser kommer du att se annonser och deras spårningskod kommer att vara aktiv.

Lägg till webbplatser som du vill tillåta att visa annonser och använda spårare genom att:

1. Leta upp **Annonsblockerare och Antitracker** inslag i **inställningar**.
2. Klicka på **Hantera** länk. Gå sedan till avsnittet Vitlista i fönstret och klicka på motsvarande **Hantera** länk.
3. Klicka på **Lägg till webbplats** och infoga önskad URL.

Autoanslut

När du är på språng, arbetar på ett kafé eller väntar på flygplatsen kan det vara den snabbaste lösningen att ansluta till ett allmänt trådlöst nätverk för att göra betalningar, kolla e-post eller konton i sociala nätverk. Men nyfikna ögon som försöker kapa din personliga data kan vara där och se hur informationen läcker genom nätverket.

För att skydda dig mot farorna med osäkra eller okrypterade offentliga trådlösa hotspots, Bitdefender Password Manager inkluderar en autoconnect-funktion. Detta innebär att Bitdefender Password

Manager kan aktiveras automatiskt i vissa situationer, beroende på dina preferenser och vilket operativsystem du kör.

- På **Windows** funktionen för automatisk anslutning kan aktiveras för följande situationer:
  - **Börja:** Anslut VPN vid start av Windows.
  - **Osäkert Wi-Fi:** Använd VPN när du ansluter till offentliga eller osäkra Wi-Fi-nätverk.
  - **Peer-to-peer-appar:** Anslut till VPN när du startar en peer-to-peer fildelningsapp.
  - **Appar och domäner:** Använd alltid VPN för vissa appar och webbplatser.

    Notera

    1. Klicka på**Hantera**länk.
    2. Bläddra till platsen för appen som du vill använda VPN för, välj appnamnet och klicka sedan**Lägg till**.
  - **Webbplatskategorier:** Anslut till VPN när du besöker specifika webbplatskategorier. Bitdefender VPN kan ansluta automatiskt för följande webbplatskategorier:
    - Finansiell
    - Onlinebetalningar
    - Hälsa
    - Fildelning
    - Online dejting
    - Vuxet innehåll

    Notera

    För varje kategori kan du välja en annan server för VPN att ansluta till.
- På **Mac OS** funktionen för automatisk anslutning kan aktiveras för följande situationer:
  - **Börja:** Anslut VPN vid start av macOS.

- **Osäkert Wi-Fi:** Använd VPN när du ansluter till offentliga eller osäkra Wi-Fi-nätverk.
- **Peer-to-peer-appar:** Anslut till VPN när du startar en peer-to-peer fildelningsapp.
- **Applikationer:** Anslut alltid VPN för vissa appar.

- På **Android** och **iOS** Bitdefender Password Manager kan ställas in för att ansluta automatiskt endast när du är på ett osäkrat eller offentligt Wi-Fi.

Avancerad

Delad tunnling

Virtual Private Network (VPN) delad tunneling låter dig dirigera en del av din applikations- eller enhetstrafik genom ett krypterat VPN, medan andra applikationer eller enheter har direktåtkomst till internet. Detta är särskilt användbart om du vill dra nytta av tjänster som fungerar bäst när din plats är känd samtidigt som du har säker åtkomst till potentiellt känslig kommunikation och data.

Genom att aktivera **Delad tunnling** funktionen kommer utvalda appar och webbplatser att kringgå VPN och komma åt Internet direkt.

Så här hanterar du applikationer och webbplatser som kringgår VPN:

1. Klicka på**Hantera**länk när funktionen är aktiverad.
2. Klicka på **Lägg till** knapp.
3. Bläddra till platsen för appen i fråga eller skriv in webbadressen till den önskade webbplatsen och klicka sedan**Lägg till**.

> **Notera**
> Genom att lägga till en webbplats kommer hela domänen inklusive alla underdomäner att kringgås.

> **Viktig**
> På **Mac OS** enheter är funktionen Split tunneling endast tillgänglig för webbplatser.

App Traffic Optimizer

Bitdefender Password ManagerApp Traffic Optimizer låter dig prioritera trafik till de viktigaste apparna på din enhet utan att utsätta din anslutning för integritetsrisker. VPN:er omdirigerar internettrafik genom en säker tunnel samtidigt som de använder robusta krypteringsalgoritmer för att skydda den.

Denna kombination av tekniker kan dock ha vissa nackdelar, främst när det gäller anslutningens hastighet. Flera faktorer kan utlösa nedgångar i anslutningen, den vanligaste är avståndet till servern du ansluter till, nätverksstockning och hög bandbreddsanvändning. Om du någonsin känt det ibland Bitdefender Password Manager lägger en onödig börda på din anslutning och avmattningar ständigt kommer i vägen för dig, kan det finnas ett bättre svar än att koppla bort.

Hur fungerar App Traffic Optimizer?

Vissa appar och tjänster som streamingplattformar, torrentklienter och spel kräver mer bandbredd. Att ständigt använda dem kan påverka din internetanslutningshastighet. Att dirigera din trafik genom en VPN-tunnel utsätter redan din anslutning för en relativ avmattning. Att lägga ytterligare påfrestningar på din anslutning kan allvarligt försämra din onlineupplevelse.

Bitdefender Password Managers App Traffic Optimizer-funktion kan hjälpa dig att ta itu med långsamma VPN-anslutningar genom att prioritera den till den app du väljer. Funktionen låter dig bestämma vilka appar som ska ta emot huvuddelen av din trafik och allokerar sedan resurserna därefter. Om du till exempel är i ett möte och märker att kvaliteten på ditt samtal är undermålig, låter App Traffic Optimizer dig prioritera trafik till videokonferensappen för förbättrade resultat.

Vanligtvis skulle VPN-användare tillgripa att stänga alla störande processer på sin enhet eller till och med inaktivera sin VPN-anslutning för att få snabbare internethastighet. App Traffic Optimizer låter dig njuta av oavbrutet integritetsskydd utan att kompromissa med din anslutningshastighet.

Använder App Traffic Optimizer

För närvarande är funktionen endast tillgänglig på Windows-enheter och låter dig prioritera trafik till upp till 3 applikationer.

Följ dessa steg för att aktivera och konfigurera det med minimal ansträngning:

1. Starta Bitdefender VPN programmet på din Windows-dator.
2. Klicka på knappen på sidofältet för att komma åt VPN-inställningarna.
3. Gå till**Allmän**fliken och aktivera**App Traffic Optimizer**funktion. Färgen på omkopplaren kommer att ändras från grå till blå.

Så här hanterar du de applikationer som prioriteras av den här funktionen:

1. Klicka på**Hantera**länk.
2. Bläddra till platsen för appen som du vill optimera trafiken för, välj appnamnet och klicka sedan**Lägg till**. Appen kommer att visas i **Prioriterat** sektion.

> **Notera**
> Alternativt, om du nyligen har öppnat programmet du vill prioritera, tryck på +-knappen i fönstret App Traffic Optimizer.

3. Koppla från och återanslut till Bitdefender VPN efter att ha lagt till eller tagit bort appar från listan.

För att ta bort en app från App Traffic Optimizer, klicka helt enkelt på ikonen bredvid appens namn.

> **Notera**
> App Traffic Optimizer är inte tillgänglig på macOS.

Protokoll

Här kan du välja vilken typ av protokoll du vill använda för dataöverföring. Följande alternativ är tillgängliga:

- **Automatisk** - Bitdefender VPN kommer att välja det optimala protokollet för din specifika enhet och nätverk.
- **Hydra Catapult** - Snabbt och säkert, perfekt för streaming och spel.
- **OpenVPN UDP** - Optimerad för höga hastigheter. Detta protokoll är dock inte lika tillförlitligt när det gäller dataförlust som andra protokoll i listan.

- **OpenVPN TCP** - Designad för tillförlitlighet. Säkerställer att din data levereras helt, men den är inte lika snabb som OpenVPN UDP.
- **Trådskydd** - Nyare protokoll som ger stark säkerhet och hög prestanda.

Dubbelhopp

Med den här funktionen kan du hantera servrarna för att skicka och dubbelkryptera din internettrafik. Din data kommer att passera genom två VPN-servrar istället för en, vilket gör det svårare att spåra din internetaktivitet.

Notera
Du kan bara lägga till totalt 5 dubbelhoppplatser. Du kan dock ta bort de anpassade dubbelhoppen i din lista och skapa andra när som helst.

Viktig
Att använda servrar på olika kontinenter i samma dubbelhopp kan sänka din anslutningshastighet.

7.5. Avinstallerar Bitdefender Password Manager

Proceduren för att ta bort Bitdefender Password Manager liknar den du använder för att ta bort andra program från din dator:

- **Avinstallerar Bitdefender Password Manager från Windows-enheter**
  - I **Windows 7**:
    1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
    2. Hitta **Bitdefender Password Manager** och välj **Avinstallera**. Vänta tills avinstallationsprocessen är klar.
  - I **Windows 8** och **Windows 8.1**:
    1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
    2. Klick **Avinstallera ett program** eller **Program och funktioner**.
    3. Hitta **Bitdefender Password Manager** och välj **Avinstallera**.

Vänta tills avinstallationsprocessen är klar.

- I **Windows 10** och **Windows 11**:
  1. Klick **Start**, Klicka sedan **inställningar**.
  2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
  3. Hitta **Bitdefender Password Manager** och välj **Avinstallera**.
  4. Klick **Avinstallera** igen för att bekräfta ditt val.
     Vänta tills avinstallationsprocessen är klar.

- **Avinstallerar från macOS-enheter**
  1. Klicka på **Gå** i menyraden och välj **Ansökningar**.
  2. Dubbelklicka på **Bitdefender** mapp.
  3. Springa **BitdefenderUninstaller**.
  4. I det nya fönstret markerar du rutan bredvid **Bitdefender Password Manager**, klicka sedan på **Avinstallera**.
  5. Skriv ett giltigt administratörskontonamn och ett lösenord och klicka sedan **OK**.
  6. Slutligen kommer du att få besked om det Bitdefender Password Manager har avinstallerats. Klick **Stänga**.

- **Avinstallerar från Android-enheter**
  1. Öppna **Play Butik** app.
  2. Söka efter **Bitdefender Password Manager**.
  3. I den Bitdefender Password Manager appbutikssida, välj **Avinstallera**.
  4. Bekräfta genom att trycka på **OK**.

- **Avinstallerar från iOS-enheter**
  1. Håll fingret på Bitdefender Password Manager app.
  2. Välj **Ta bort appen**.
  3. Knacka **Radera**.

7.6. Vanliga frågor

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du använder, laddar ner eller laddar upp innehåll på Internet. För att du ska vara säker när du surfar på webben rekommenderar vi att du använder VPN när du:

- vill ansluta till offentliga trådlösa nätverk
- vill komma åt innehåll som normalt är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, e-postadresser, kreditkortsinformation, etc.)
- vill dölja din IP-adress

Kan jag välja en stad med Bitdefender VPN?

Ja. För närvarande kan Bitdefender VPN för Windows, macOS, Android och iOS användas för att välja en specifik stad. Här är listan över tillgängliga städer:

- **USA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Kanada:** Montreal, Toronto, Vancouver
- **STORBRITANNIEN:** London, Manchester

Kan Bitdefender VPN installeras som en fristående app?

VPN-appen installeras automatiskt tillsammans med din Bitdefender-säkerhetslösning. Den kan också installeras som en fristående app från produktsidan, från Google Play Store och App Store.

Kommer Bitdefender att dela min IP-adress och personliga data som delas med tredje part?

Nej, med Bitdefender VPN är din integritet 100 % säker. Ingen (reklambyråer, internetleverantörer, försäkringsbolag, etc.) kommer att ha tillgång till dina onlineloggar.

Vilken krypteringsalgoritm använder den?

Bitdefender VPN använder Hydra-protokollet på alla plattformar, 256-bitars AES-kryptering eller den högsta tillgängliga cypher som stöds av

både klient och server, med Perfect Forward Secrecy. Detta innebär att krypteringsnycklar genereras för varje ny VPN-session och raderas från minnet när sessionen är över.

Kan jag få tillgång till GEO-IP-begränsat innehåll?

Med Premium VPN har du tillgång till ett omfattande nätverk av virtuella platser över hela världen.

Kommer det att ha en negativ inverkan på batteritiden för min enhet?

Bitdefender VPN är utformad för att skydda dina personliga data, dölja din IP-adress när du är ansluten till osäkra trådlösa nätverk och komma åt begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning av din enhet rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort när du är offline.

Varför saktar VPN ner min internetanslutning?

Bitdefender VPN är designad för att erbjuda en lätt upplevelse när du surfar på webben. Beroende på avståndet mellan din faktiska plats och serverplatsen du väljer att ansluta till, förväntas en viss hastighetsstraff, men det är nästan alltid tillräckligt litet för att det går obemärkt förbi under normal onlineaktivitet. Dessutom förlitar vi oss på en av de snabbaste VPN-infrastrukturerna i världen. Om det inte är ett måste att ansluta från din plats till en fjärransluten server (t.ex. från USA till Frankrike), rekommenderar vi att du tillåter VPN att automatiskt ansluta dig till närmaste server eller hitta en server närmare din nuvarande plats.

8. LÖSENORDSHANTERAREN

8.1. Vad är Bitdefender Password Manager

Bitdefender Password Manager är en multiplattformstjänst utformad för att hjälpa användare att lagra och organisera alla sina onlinelösenord. Den är byggd med de starkaste kända kryptografiska algoritmerna för högsta nivå av säkerhet och digital säkerhet. Det fungerar som en webbläsartillägg och mobilappslösning för identitets- och lösenordshantering, banktjänster och all annan typ av känslig information över enheter.

Bitdefender Password Manager kan automatiskt spara, autofyll, automatiskt generera och hantera dina lösenord för alla webbplatser och onlinetjänster med hjälp av ett enda huvudlösenord, vilket gör din övergripande digitala identitet mycket lättare att hantera.

8.1.1. Säkerhet och hur det fungerar

Bakom Bitdefender Password Manager Programvaran står för några av de senaste kryptografiska algoritmerna som garanterar den högsta datasäkerheten användare kan hoppas på, såsom AES-256-CCM, SH512, BCRYPT, HTTPS och WSS-protokoll för dataöverföring. All data inblandad är alltid krypterad och dekrypterad lokalt. Detta gör det så att endast kontoinnehavaren ensam kan ha tillgång till den information som finns lagrad på kontot, samt till huvudlösenordet som används för att komma åt och därefter använda uppgifterna i fråga.

8.2. Komma igång

8.2.1. Systemkrav

Du kan använda den senaste versionen av Bitdefender Password Manager endast på enheter som kör följande operativsystem:

- **För PC-användare:**
  - Windows 7 med Service Pack 1
  - Windows 8
  - Windows 8.1

- Windows 10
- Windows 11

- **För macOS-användare:**
  - macOS 10.14 (Mojave) och senare macOS-operativsystem

> **Notera**
> Observera att systemprestanda kan påverkas på enheter som har gamla generationens processorer.

- **För iOS-användare:**
  - iOS 11.0 eller senare iOS operativsystem

- **För Android-användare:**
  - Android 5.1 och senare Android-operativsystem

> **Notera**
> - Funktionen för upplåsning av fingeravtryck stöds på **Android 6.0** och senare.
> - Autofyll-funktionen stöds på **Android 8.0** och senare, kompatibel med iPhone, iPad och iPod touch.

Programvarukrav

För att kunna använda Bitdefender Password Manager och alla dess funktioner måste dina Windows- eller macOS-enheter uppfylla följande programvarukrav:

- **Microsoft Edge** (baserat på Chromium 80 och senare)
- **Mozilla Firefox** (version 65 eller senare)
- **Google Chrome** (version 72 eller senare)
- **Safari** (version 12 eller senare)

> **Notera**
> Programvarukraven gäller inte för Android och iOS.

Varning

Underlåtenhet att uppfylla systemkraven som presenteras ovan kommer att resultera i antingen oförmåga att installera Bitdefender Password Manager eller fel på produkten.

8.2.2. Installation

Det här kapitlet kommer att vägleda dig om hur du installerar Bitdefender Password Manager till både webbläsarna på din Windows-dator och macOS, såväl som på dina mobila Android- eller iOS-enheter.

Viktig

Innan installationen, se till att du har en giltig Password Manager-prenumeration i din Bitdefender Central konto så att det här webbläsartillägget kan hämta sin giltighet från ditt konto.

Aktiva prenumerationer listas i **mina prenumerationer** avsnitt inom Bitdefender Central.

Installerar på Windows- och macOS-enheter

Till skillnad från de flesta stationära applikationer och mjukvara som måste installeras och konfigureras på dessa enheter, kommer Bitdefender Password Manager som ett webbläsartillägg - även kallat ett tillägg - som snabbt kan läggas till och aktiveras i din föredragna webbläsare.

De webbläsare som för närvarande stöds för produkten är följande: **Google Chrome**e, **Mozilla Firefox**, **Microsoft Edge**, och **Safari**.

1. Gå till https://central.bitdefender.com/ och logga in på ditt konto.
   Om du inte redan har ett konto, klicka på **SKAPA KONTO**, skriv sedan ditt fullständiga namn, en e-postadress och ett lösenord.
2. Välj **Mina enheter** på skärmens vänstra sidofält.
3. I den **Mina enheter** fortsätt genom att klicka på **+ Lägg till enhet**.
4. Denna åtgärd kommer att uppmana ett nytt fönster att dyka upp. Välja **Lösenordshanteraren** i urvalsskärmen.
5. Välja **Denna apparat**.
   Om du vill installera på en annan enhet väljer du Andra enheter. Du kan sedan e-posta en nedladdningslänk till respektive enhet eller direkt kopiera URL:en för installationen.

6. Välj sedan i vilken webbläsare du vill installera tillägget Password Manager.
7. Varje motsvarande knapp omdirigerar dig till webbläsarens Extensions Store. Därifrån följer du bara instruktionerna på skärmen som visas nedan:

   Microsoft Edge

   - Klicka på **Skaffa sig** knapp
   - Klick **Lägg till tillägg** i prompten som visas på skärmen

   Google Chrome

   - Klicka på **Lägg till i Chrome** knapp
   - Klicka på i bekräftelserutan **Lägg till tillägg**

   Mozilla Firefox

   - Klicka på **Lägg till i Firefox** knapp
   - Klicka på **Installera** knappen i det övre högra hörnet av skärmen

   Safari

   - Klicka på **Skaffa sig** knappen och klicka sedan **Installera**
   - Öppna Safari och välj **Inställningar** i den översta menyraden
   - I fönstret Inställningar klickar du på **Tillägg** flik
   - Markera kryssrutan bredvid Password Manager för att aktivera det

När du har följt dessa steg, ställ in ett starkt huvudlösenord och tryck sedan på **Spara huvudlösenord** knappen efter att du läst och godkänner **Villkor**.

Viktig

Observera att du kommer att kräva detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender Password Manager. Detta är i huvudsak nyckeln som gör att ägaren kan använda denna produkt.

Varning

När du skapar huvudlösenordet får du ett **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren i händelse av att du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.

❍ Du kan trycka på **Stänga** när det är klart.

Installerar på Android-enheter

Den enklaste metoden för att installera Bitdefender Password Manager för Android-telefoner och surfplattor är att ladda ner applikationen direkt från Google Play.

Installation av Bitdefender Password Manager-appen kan också göras via din Bitdefender Central konto:

1. Logga in på ditt Bitdefender Central-konto på din Android-mobilenhet genom att gå till https://login.bitdefender.com/central/login.
2. Välj **Mina enheter** på skärmens vänstra sidofält.
3. I den **Mina enheter** fortsätt genom att klicka på **+ Lägg till enhet**.
4. Denna åtgärd kommer att uppmana ett nytt fönster att dyka upp. Välja **Lösenordshanteraren** i urvalsskärmen.
5. Välja **Denna apparat**.
   Om du vill installera på en annan enhet, välj **Andra enheter**. Du kan sedan e-posta en nedladdningslänk till respektive enhet eller direkt kopiera URL:en för installationen.
6. Du kommer att omdirigeras till Google Play. Knacka **Installera** för att ladda ner Bitdefender Password Manager på Android.
7. När nedladdningen är klar öppnar du Lösenordshanteraren program.
8. Om du inte är inloggad automatiskt på ditt konto, logga in med ditt användarnamn och lösenord.

När du har följt dessa steg, ställ in ett starkt huvudlösenord och tryck sedan på **Spara huvudlösenord** knappen efter att du läst och godkänner **Villkor**.

> **Viktig**
> Observera att du kommer att kräva detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender Password Manager. Detta är i huvudsak nyckeln som gör att ägaren kan använda denna produkt.

> **Varning**
> När du skapar huvudlösenordet får du ett **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren i händelse av att du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.
>
> ❍ Du kan trycka på **Stänga** när det är klart.

9. Skapa en **4-siffrig PIN-kod**, så om du byter till en annan app och sedan återgår till lösenordshanteraren behöver du inte ange huvudlösenordet som du ställt in tidigare. Om tillgängligt kan du även aktivera ansiktsigenkänning eller fingeravtrycksautentisering.
10. Knacka på **Aktivera Autofyll** för att konfigurera Android autofyll-inställningar.

> **Notera**
> Om du hoppar över det här steget kan du aktivera och anpassa Androids autofyllfunktioner vid ett senare tillfälle genom att följa instruktionerna på Intelligent autofyll (sida 257).

11. Du kommer att mötas av en lista med appar som kan fylla i lösenord automatiskt.
    Välj **Lösenordshanteraren** och sedan kommer enheten att uppmana dig att bekräfta att du litar på den här appen.
    Knacka **OK**.
12. Ange PIN-koden du konfigurerade i **steg 9** för att bekräfta denna åtgärd.

Installationen på din Android-enhet är nu klar.

Installerar på iOS-enheter

Den enklaste metoden för att installera Bitdefender Password Manager för iOS- och iPadOS-enheter är att ladda ner programmet från Apple App Store.

Download on the App Store

Installation av Bitdefender Password Manager-appen kan också göras via din Bitdefender Central konto:

1. Logga in på ditt Bitdefender Central-konto på din iPhone eller iPad genom att gå till https://login.bitdefender.com/central/login.
2. Välj **Mina enheter** på skärmens vänstra sidofält.
3. I den **Mina enheter** fortsätt genom att klicka på **+ Lägg till enhet**.
4. Denna åtgärd kommer att uppmana ett nytt fönster att dyka upp. Välja **Lösenordshanteraren** i urvalsskärmen.
5. Välja **Denna apparat**.
   Om du vill installera på en annan enhet, välj **Andra enheter**. Du kan sedan e-posta en nedladdningslänk till respektive enhet eller direkt kopiera URL:en för installationen.
6. Du kommer att omdirigeras till **App Store**. Tryck på molnikonen med en pil som pekar nedåt för att ladda ner Bitdefender Password Manager för iOS.
7. När applikationen är installerad, öppna den och markera den lilla rutan på skärmen. Välj **Fortsätta** efter att du läst och håller med **Prenumerationsavtal**.
8. Om du inte är inloggad automatiskt på ditt konto, logga in med ditt användarnamn och lösenord.
   När du har följt dessa steg, ställ in ett starkt huvudlösenord och tryck sedan på **Spara huvudlösenord** knappen efter att du läst och godkänner **Villkor**.

> **Viktig**
> Observera att du kommer att kräva detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender Password Manager. Detta är i huvudsak nyckeln som gör att ägaren kan använda denna produkt.

Varning

När du skapar huvudlösenordet får du ett **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren i händelse av att du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.

- Du kan trycka på **Stänga** när det är klart.

9. Skapa en **4-siffrig PIN-kod**, så om du byter till en annan app och sedan återgår till lösenordshanteraren behöver du inte ange huvudlösenordet som du ställt in tidigare. Om tillgängligt kan du även aktivera ansiktsigenkänning eller fingeravtrycksautentisering.

Installationen på din iOS / iPadOS-enhet är nu klar!

8.2.3. Delad plan

Bitdefender Password Manager delad plan gör det möjligt för flera användare att komma åt och använda samma abonnemang. Det ger en centraliserad metod för åtkomst till programvara, administration och support.

- Den person som ansvarar för den delade prenumerationsplanen, känd som Plan Manager, kan dela tjänsten mellan medlemmarna.
- Varje medlem får sin egen unika **Bitdefender Central** konto kopplat till deras e-postadress och tillgång till tjänsten Bitdefender Password Manager.

Dela Bitdefender Password Manager med flera användare

Bjuder in medlemmar

För att lägga till en eller flera användare till den delade prenumerationen måste planhanteraren följa dessa steg:

1. Logga in på ditt Bitdefender Central-konto påhttps://central.bitdefender.com/
2. Gå till **mina prenumerationer** menyn till vänster på sidan.
3. Välja **Bjud in medlem** i **Bitdefender Password Manager** panel.

4. Ange e-postadressen för varje person som du vill dela din prenumeration med och klicka sedan på **Skicka**. Max 3 medlemmar kan läggas till samtidigt.
5. Installationsinstruktioner skickas direkt till de nya medlemmarna. Klicka på **Stänga** för att stänga bekräftelsefönstret.

> **Notera**
> Medlemmar har 24 timmar på sig att acceptera din inbjudan när den har mailats till dem.
>
> - Inbjudna medlemmar kommer att visas med statusen "Inbjudna".
> - Du kommer att se dem som "aktiva" medlemmar efter att de accepterat inbjudan. Du meddelas också via e-post om varje accepterad inbjudan.

Ta bort medlemmar

Bitdefender Password Manager Shared Plan-åtkomst går förlorad för medlemmar som tas bort. När planansvarig bestämmer sig för att ta bort en prenumerationsmedlem får medlemmen ett e-postmeddelande. Under de följande 30 dagarna byts ex-medlemmen till en 30-dagars Bitdefender Password Manager **testversion** med full kapacitet. Tjänsten kommer då att stängas av.

Planhanteraren kan eliminera användare från den delade planen på följande sätt:

1. Logga in på ditt Bitdefender Central-konto påhttps://central.bitdefender.com/
2. Gå till **mina prenumerationer** menyn till vänster på sidan.
3. I den **Bitdefender Password Manager delad plan** panel klicka på **Hantera**, sedan Välj **Redigera medlemmar** i menyn.
4. Klicka på **Avlägsna** knappen för att ta bort en medlem från den delade planen.
5. Välja **Ja**, ta bort medlem och klicka sedan på **Slutför redigeringen** knappen för att ändringarna ska träda i kraft.

Notera
När en medlem tas bort från den delade planen ändras deras status till **Väntar på borttagning** tills de är helt eliminerade.

Accepterar en inbjudan

Du kommer att få ett e-postmeddelande när någon bjuder in dig att bli prenumerationsmedlem för Bitdefender Password Manager Shared Plan. Du har 24 timmar på dig att acceptera en inbjudan när den väl har skickats till dig.

För att acceptera inbjudan och få tillgång till lösenordshanterarens funktioner måste användaren följa dessa steg:

1. Öppna e-postmeddelandet du fick med titeln **[Börja använda ditt Bitdefender-abonnemang som medlem]** och klicka på **AKTIVERA I CENTRAL** knapp.
2. Bitdefender Central-sidan öppnas sedan i din webbläsare.
   - Om du redan har ett Bitdefender-användarkonto kopplat till e-postmeddelandet dit inbjudan skickades ,**logga in** för att göra anspråk på din delade prenumeration.
   - Om du inte har ett Bitdefender-användarkonto, klicka på **Skapa en** och registrera dig med samma e-postmeddelande som inbjudan skickades för att göra anspråk på din delade prenumeration.
     - Ange ditt fullständiga namn
     - Skriv in din mailadress
     - Ange ditt lösenord
     - Klicka på **Skapa konto** knappen och du kommer att signeras.
3. När du har loggat in klickar du på **Komma igång** på välkomstskärmen som informerar dig om att din Bitdefender Password Manager-prenumeration nu är aktiv.
4. Följ stegen på skärmen som också beskrivs i Installation (sida 244).

Notera

Planhanterarens e-post visas i ditt Bitdefender Central-konto högst upp på menyn Lösenordshanteraren och på prenumerationskortet, under Mina prenumerationer.

Om du behöver hjälp med den delade planen, vänligen kontakta dem.

8.3. Importera och exportera dina lösenord

Bitdefender Password Manager är byggd på ett sådant sätt att det effektivt underlättar kommunikation och dataöverföring med externa källor, plattformar och mjukvaruverktyg. Detta är den centrala anledningen till att det mycket vanliga behovet av att importera eller exportera lösenord till eller ut ur Bitdefender Password Manager kan tillfredsställas med lätthet.

8.3.1. Kompatibilitet

Bitdefender Password Manager kan sömlöst överföra data från följande lista med applikationer:

- **1 Lösenord**
- **Bitwarden**
- **Bitdefender Password Manager**
- **Hejdå**
- **Chrome webbläsare**
- **Claro**
- **Dashlane**
- **Edge webbläsare**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox webbläsare**
- **Gestor de contraseñas – Claro**

- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeepPass 2.x**
- **LastPass**
- **Panda Dome lösenord**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SITTA**
- **F-Secure**
- **Telnor**

> **Notera**
> Om namnet på webbläsaren eller lösenordshanteraren som du försöker överföra datafiler från inte nämns i listan ovan kan du följa vår onlineguide om hur användare kan redigera en CSV-fil från lösenordshanterare som inte stöds så att du kan importera din information till **Bitdefender Password Manager**: https://www.bitdefender.com/consumer/support/answer/2472/

Denna överföring av data mellan Bitdefender Password Manager och annan programvara för kontohantering kan göras genom följande dataformat:

CSV, **JSON**, **XML**, **Text**, **1pif** och **FSK**.

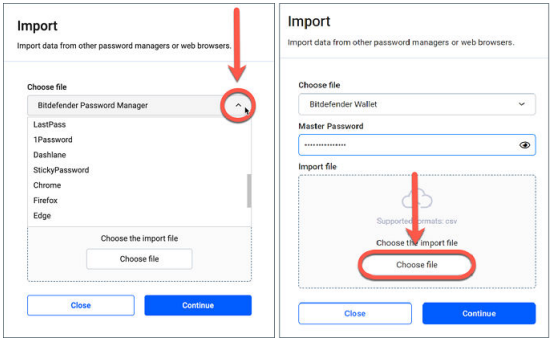
8.3.2. Importerar till lösenordshanteraren

Bitdefender Password Manager låter dig enkelt importera lösenord från andra lösenordshanterare och webbläsare. Om du för närvarande funderar på att byta till Bitdefender Password Manager från en annan lösenordshanteringstjänst, har du med största sannolikhet lagrat en stor mängd referenser som användarnamn, lösenord och annan inloggningsinformation som krävs för alla dina konton.

Nu när du har valt Bitdefender Password Manager kommer du att leta efter att importera den sparade informationen till den.

Så här importerar du din lagrade information från andra appar och webbläsare till Bitdefender Password Manager, **oavsett operativsystem** där du har valt att installera denna produkt:

1. Klicka på ikonen Lösenordshanteraren i din webbläsare (på Windows eller macOS) eller starta applikationen Lösenordshanteraren (på Android eller iOS). Om du uppmanas anger du din Huvudlösenord.
2. Öppna lösenordshanteraren menyn för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Scrolla ner till **Data** avsnittet och klicka på **Importera data** alternativ.
4. Använd rullgardinsmenyn för att välja namnet på lösenordshanterarens app eller webbläsare som du vill importera dina konton från. Mata in din Huvudlösenord i motsvarande fält och klicka sedan på **Välj FIL**.



5. Bläddra igenom dina mappar för att hitta platsen där du har sparat filen som innehåller dina användarnamn och lösenord, exporterat från din andra lösenordshanterare eller webbläsare och tryck sedan på **Fortsätta**.

När de har importerats kommer dina lösenord att vara tillgängliga på alla enheter där Bitdefender Password Manager-applikationen eller webbläsartillägget är installerat.

8.3.3. Exporterar från Password Manager

Bitdefender Password Manager låter dig enkelt exportera dina sparade lösenord (inklusive kontoinloggningsuppgifter, säkra anteckningar etc.) till en CSV-fil (kommaseparerade värden) eller en krypterad fil om du någonsin vill byta till en annan lösenordshanterartjänst, så att din avgång från Bitdefender Password Manager inte kommer att vara en svår process.

> **Viktig**
> En CSV-fil är **inte** krypterad och innehåller användarnamn och lösenord i vanlig textformat, vilket innebär att din privata information kan läsas av alla som har tillgång till din enhet. Vi rekommenderar därför att du följer instruktionerna nedan på en betrodd enhet.

Så här kan du exportera dina data från Bitdefender Password Manager:

1. Klicka på ikonen Lösenordshanteraren i din webbläsare (på Windows eller macOS) eller starta applikationen Lösenordshanteraren (på Android eller iOS). Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Scrolla ner till **Data** avsnitt och klicka på **Exportera data** alternativ.
4. Nu bör du få följande två alternativ:
   - **CSV**
   - **Lösenordsskyddade filer**

   Välj önskat alternativ, ange sedan ditt huvudlösenord och klicka på **Exportera data** knapp.

   > **Notera**
   > Om du väljer alternativet för lösenordsskyddad fil kommer du att bli ombedd att kryptera data som innehåller kontolistan med ett lösenord, så på detta sätt skulle bara du kunna komma åt den om det behövs.

5. Din webbläsare/app kommer att fortsätta genom att spara en fil med namnet Bitdefender Password Manager_exported_data_current-date till ditt system i standardmappen för nedladdning. Den innehåller alla dina data lagrade i Bitdefender Password Manager.

Efter att ha exporterat din data kan du ladda upp den till den lösenordshanterare du väljer.

8.4. Funktioner och funktioner

Det här kapitlet tar dig igenom alla funktioner och funktioner i Bitdefender Password Manager, förklarar deras användbarhet och hur du använder dem mest effektivt.

8.4.1. Lösenordshantering

Lösenordsgenerator

Den gyllene regeln när det gäller onlinesäkerhet är att alltid använda unika slumpmässiga lösenfraser för varje tjänst som kräver kontoskapande. Lösenordsåteranvändning på flera plattformar är den främsta orsaken bakom identitetsstöld och förluster i samband med fientlig kontoövertagande.

Den här funktionen hjälper användare att skapa säkra, komplexa och unika lösenord för varje nytt konto de skapar var som helst online. Detta eliminerar behovet för användare att komma på starka lösenord på egen hand eller vara noga med att inte återanvända samma lösenord för flera konton.

De **Lösenordsgenerator** kan nås via fliken överst i lösenordshanterarens gränssnitt.

Generatorn kan ställas in för att returnera lösenord **mellan 4 och 32 tecken**.

Du kan också ange vilka typer av tecken som ska eller inte ska finnas i det slumpmässigt genererade lösenordet genom att markera eller avmarkera motsvarande kryssrutor. **(gemener, versaler, siffror, special)**

Genom att trycka på knappen till höger om det visade lösenordet kommer generatorn att ändra det föreslagna lösenordet.

För att använda det visade lösenordet, tryck **Använd lösenord**, åtgärd som sparar teckensträngen till ditt urklipp.

> **Notera**
> Dina tidigare genererade lösenord kommer att lagras tillfälligt i lösenordshistoriken, som kan nås via **Lösenordshistorik** knapp.

Lösenordsfångning

Med den här funktionen i Lösenordshanteraren kommer du att bli ombedd att lagra alla dina nya lösenord direkt efter att du har skapat dem. Lösenordshanteraren kommer att uppmana användare att lagra sina nyskapade lösenord, så att de kan läggas till i den ultrasäkra miljön som tillhandahålls av Bitdefender direkt.

Intelligent autofyll

Bitdefender Password Manager kan ställas in på ett sådant sätt att den kan autofylla dina inloggningsuppgifter och viktigast av allt lösenord. Proprietära algoritmer kan upptäcka och förfylla inloggningsuppgifter på tidigare besökta webbplatser, vilket sparar användarnas tid varje gång de loggar in på en tjänst.

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.

   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.

2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Klicka på **Enhetsinställningar**.
4. Här kommer du att märka en knapp som visar antingen **Inaktivera automatisk fyllning** eller **Aktivera automatisk fyllning**. Den här inställningen styr drifttillståndet för den intelligenta autofyllfunktionen.

Säkerhetsrapport

Säkerhetsrapporten är ett verktyg som genererar rapporter baserade på ett antal funktioner som är avsedda att stärka din digitala säkerhet. Det kommer att meddela dig om ett lösenord kräver din omedelbara uppmärksamhet genom att bestämma dess säkerhetsnivå. Det kommer att upptäcka lösenordsdubbletter och uppmana dig att ändra dem i enlighet med detta, vilket undviker farorna med att återvinna samma lösenord för flera konton.

Rapporten kommer att koncentrera sig på att ge dig information om din övergripande lösenordshygien: detta avser dubbletter av lösenord, svaga eller på annat sätt läckta lösenord eller e-postadresser.

Detta görs genom att jämföra listan med krypterade hash från Troys webbsida lokalt på din enhet för att kontrollera om den innehåller motsvarande hash för dina lösenord. Om en matchning hittas kommer du att meddelas för att uppmuntra dig att följaktligen ändra dina lösenord och andra inloggningsuppgifter.

För att komma åt **Säkerhetsrapport**, gå in i lösenordshanterarens gränssnitt och välj motsvarande knappen i den övre raden.

Synkronisera mellan andra plattformar

Genom att spara dina lösenord en gång i Bitdefender Password Manager kan du lagra och säkert komma åt dem på alla dina Windows-, Mac-, Android- eller iOS-enheter från Chrome, Safari, Firefox och Edge eller inuti mobilappar.

> **Notera**
> Bitdefender är också utrustad med en **offlineläge** för att komma åt dina lösenord, i händelse av att du inte råkar ha tillgång till internet. Detta gör dina lösenord tillgängliga när som helst och var som helst.

Ta bort en post

För att radera sparade lösenord tryck först på redigera-ikonen bredvid posten du vill ta bort, som finns i **konton** flik. Scrolla ner och välj sedan **Radera**. När du tillfrågas om du är säker på att du vill ta bort kontot väljer du **Avlägsna**.

8.4.2. Kontohantering

Autentisering

Autentiseringen i Bitdefender Password Manager görs genom **STIFT** ställs in i installationsprocessen av produkten. (Observera att **Auto lås** funktionen låser lösenordshanteraren eller loggar ut efter en period av inaktivitet på webbläsarnivå eller stängning av mobilappen)

Dessutom kan det också göras genom att använda biometri, om tillgängligt, som t.ex **Fingeravtryck** eller **Ansiktsupplåsning**.

Till **aktivera eller inaktivera** biometribaserad autentisering:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.

På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
Om du uppmanas anger du din Huvudlösenord.

2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
3. Klicka på **Enhetsinställningar**.
4. Här kommer du att märka en knapp som visar antingen **Inaktivera biometri** eller **Aktivera biometri**. Den här inställningen styr driftsstatusen för den biometribaserade autentiseringsfunktionen.

Återställ huvudlösenord

> **Viktig**
> De **Ändra huvudlösenord** funktionen är inte tillgänglig på mobila enheter. Det enda sättet du kan ändra eller återställa ditt huvudlösenord är via webbläsartillägget Bitdefender Password Manager på en Windows-dator eller en macOS-enhet.

Så här ändrar du din Huvudlösenord som en försiktighetsåtgärd och skapa en ny i Bitdefender Password Manager:

1. När du har installerat webbläsartillägget klickar du på **Lösenordshanteraren** ikonen i webbläsarens verktygsfält.
2. Ange ditt nuvarande huvudlösenord för att låsa upp valvet.

> **Viktig**
> Om du inte kommer ihåg det aktuella huvudlösenordet, klicka på **jag har glömt mitt lösenord** alternativet på samma skärm. Gå in i **24-siffrig återställningsnyckel** tillhandahålls under den initiala Bitdefender Password Manager-inställningen och skriv sedan ett nytt huvudlösenord. **Om du glömmer eller tar bort** både Huvudlösenord och den **återställningsnyckel**, som en sista utväg, **kontakta en Bitdefender-representant för att hjälpa dig att återställa ditt konto**. Återställa ditt konto kommer radera alla dina data och lösenord sparas i Bitdefender Password Manager.

3. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **inställningar** menyalternativ.
4. Klicka på **Mitt konto** knappen i **konto** sektion.

5. Ett fönster med information om din Password Manager-prenumeration kommer att visas.
   Klicka på **Ändra huvudlösenord** knapp.
6. Du omdirigeras till ett nytt fönster där du kan välja ett nytt huvudlösenord. Ange ditt nuvarande huvudlösenord och skriv sedan ett nytt huvudlösenord. Det nya huvudlösenordet måste innehålla minst 8 tecken, minst en liten bokstav, en stor bokstav och en siffra.
7. tryck på **Förändra** knappen när du är klar.
8. Vänta några ögonblick tills Bitdefender återställer det gamla huvudlösenordet.
   Lämna inte din webbläsare!
9. Därefter får du en ny **24-siffrig återställningsnyckel**. Anteckna återställningsnyckeln på en säker plats och **tappa den inte**. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Lösenordshanteraren om du glömmer huvudlösenordet.
   Tryck **Stänga** när du är klar.
10. Du kommer att loggas ut från Bitdefender Password Manager.
    För att låsa upp valvet, använd det nya huvudlösenordet du just angett.

8.4.3. Andra funktioner

Identitetshantering

Den här funktionen tillåter användare att lagra flera identiteter och låter Password Manager automatiskt fylla i detaljer i webbformulär innan de gör ett köp på ett snabbt, enkelt och säkert sätt.

Som allt annat i lösenordshanteraren är all känslig data som finns i dessa lagrade identiteter krypterad och endast tillgänglig för användarens enhet.

Så här lägger du till en identitet i lösenordshanteraren:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Identiteter** menyalternativ.

3. Tryck på **Lägg till identitet** knappen längst ner.
4. Fyll i de uppgifter du vill lagra och tryck sedan på **Spara**.

Kreditkortshantering

Den här funktionen låter dig spara och fylla i kreditkortsuppgifter för enklare, snabbare och säkrare shopping.

Så här lägger du till ett kreditkort i lösenordshanteraren:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Kreditkort** menyalternativ.
3. Tryck på **Lägg till identitet** knappen längst ner.
4. Fyll i de uppgifter du vill lagra och tryck sedan på **Spara**.

Säkra mig

Secure Me-funktionen låter dig logga ut på distans eller ta bort webbhistorik på din dator, surfplatta eller mobilenhet. Om du delar en enhet med andra rekommenderar vi starkt att du aktiverar den här funktionen.

Så här hittar du och aktiverar den här funktionen:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.
   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.
2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Säkra mig** menyalternativ.
3. Tryck på **Säkra alla sessioner** knapp.
   Om du bara vill säkra en viss enhet, leta efter den i listan över enheter där lösenordshanteraren är installerad eller aktiverad i en specifik webbläsare.

Anteckningar

Secure Notes är en funktion som fungerar precis som en hemlig anteckningsbok där du kan lagra känslig data, sortera den och använda färgkodning för att bättre visualisera den. Det håller inte bara informationen snygg, utan du håller den också säker och säker.

Så här hittar du och aktiverar den här funktionen:

1. På Windows eller macOS klickar du på **Lösenordshanteraren** ikonen i din webbläsare.

   På Android eller iOS, starta **Lösenordshanteraren** Ansökan.
   Om du uppmanas anger du din Huvudlösenord.

2. Öppna menyn Lösenordshanteraren för att expandera sidofältet till vänster och klicka på **Anteckningar** menyalternativ.

3. Tryck på **Lägg till anteckning** knapp.
   När du har skrivit ner den information du vill förvara trycker du på **Spara**.

8.5. Vanliga frågor

Några vanliga frågor om Bitdefender Password Manager tenderar att återkomma. Vi har svaren! Här kan du lära dig mer om ditt Bitdefender-konto, import av lösenord, datasäkerhetsprotokoll och andra ämnen som är viktiga för våra kunder.

Allmänna frågor om Bitdefender Password Manager

Hur stoppar jag lösenordshanterarens popup-fönster i min Bitdefender-säkerhetslösning?

Lösenordshanterarens meddelande som visas av Bitdefender Total Security, Internet Security och Antivirus Plus i augusti 2022 kan avvisas genom att klicka på knappen "x". Fönstret "Hantera dina lösenord med Bitdefender Password Manager" kommer att dyka upp igen slumpmässigt ett par gånger innan det försvinner för alltid. Du kan välja bort detta reklammeddelande genom att växla**Rekommendationsmeddelanden**till avstängd position i Bitdefender-inställningarna.

Vad händer när Bitdefender Password Manager löper ut?

När din Password Manager-prenumeration löper ut och inte längre är aktiv har du högst 90 dagar på dig att exportera dina lösenord. Dina lösenord

kommer att säkerhetskopieras i ytterligare 30 dagar. Under dessa 90 dagar kommer du bara att kunna exportera dina data. Du kan inte fortsätta använda lösenordshanteraren. Autofyll-funktionen slutar fungera, liksom möjligheten att generera lösenord.

I slutet av den 90-dagars respitperioden har du 30 extra dagar på dig att kontakta Bitdefender-supporten och begära att återställa dina lösenord till livedatabasen. Du kommer då att kunna exportera dina lösenord från Bitdefender Password Manager.

Dina data kommer endast att lagras i livedatabasen till slutet av dagen då de återställdes på begäran. Vid midnatt raderas databasen – och om du ännu inte har överskridit den extra 30-dagarsperioden kan lösenord återställas från backup. Rådatabasdata från säkerhetskopian kan tillhandahållas på begäran till användaren, men databasen är krypterad och informationen kan inte nås.

Vad är ett huvudlösenord och varför måste jag komma ihåg det?

Huvudlösenordet är nyckeln som låser upp dörren till alla lösenord som är lagrade i ditt Bitdefender Password Manager-konto. Huvudlösenordet måste vara minst 8 tecken långt. Så skapa ett starkt huvudlösenord, memorera det och dela det aldrig med någon. För att skapa ett starkt huvudlösenord rekommenderar vi att du använder en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).

Hur kan jag hindra Bitdefender från att fråga efter mitt huvudlösenord varje gång jag öppnar webbläsaren?

Om du låser din enhet utan att stänga din webbläsare, låses inte Password Manager och du kan komma åt din data när du kommer tillbaka. Som en säkerhetsåtgärd, varje gång du öppnar webbläsaren måste du logga in med ditt Bitdefender Central-konto och sedan ange ditt huvudlösenord.

- För att stoppa den centrala inloggningsprompten, gå till Inställningar och markera "Inaktivera inloggningsfliken vid start".
- För att stoppa uppmaningen av huvudlösenordet, markera rutan "Kom ihåg mig" på skärmen Lås upp ditt valv.

Varför sparar du inte mitt huvudlösenord, och vad händer om jag glömmer det?

Anledningen till att vi inte lagrar ditt huvudlösenord på våra servrar är så att bara du kan komma åt ditt konto. Det är det säkraste sättet. Om Bitdefender Password Manager inte känner igen ditt huvudlösenord, se

till att du skriver det korrekt och att Caps Lock-tangenten inte är aktiv på tangentbordet.

Om du glömmer huvudlösenordet kan du alltid använda återställningsnyckeln för att låsa upp lösenordshanteraren. Under registreringsprocessen tillhandahåller Bitdefender Password Manager en **återställningsnyckel** som kan användas för att återfå åtkomst till kontot utan att förlora din data.

Om du glömmer eller tappar bort både huvudlösenordet och återställningsnyckeln, som en sista utväg, kontakta en Bitdefender-representant för att återställa ditt konto.

> **Viktig**
> Att återställa ditt konto kommer att radera alla dina data och lösenord som sparats i Bitdefender Password Manager.

Kan flera användare dela en Bitdefender Password Manager-prenumeration?

För närvarande är möjligheten att ha flera användare på samma Password Manager-prenumeration inte tillgänglig men vi arbetar på att aktivera den här funktionen inom en snar framtid.

Vad är offlineläge och hur fungerar det?

Offlineläge aktiveras automatiskt när Internetanslutningen sjunker när du använder Bitdefender Password Manager. Om du redan är inloggad och har angett ditt huvudlösenord, låter offlineläget dig komma åt dina lösenord när en internetanslutning är utom räckhåll.

Hur avinstallerar jag Bitdefender Password Manager?

För att avinstallera Bitdefender Password Manager:

- På Windows och macOS:
  Ta bort tillägget Password Manager från din webbläsare. Högerklicka på Bitdefender-ikonen och välj "Ta bort".
- På Android:
  Knacka och håll appen Password Manager och dra den till toppen av skärmen där det står "Avinstallera".
- På iOS och iPadOS:

Tryck och håll appen Lösenordshanteraren tills alla appar på skärmen börjar vicka, tryck sedan på X:et uppe till vänster om Bitdefender-ikonen.

Sekretess- och säkerhetsfrågor om Bitdefender Password Manager

Kan Bitdefender-anställda se mina lösenord?

Absolut inte. Din integritet är vår högsta prioritet. Detta är huvudorsaken till att vi inte lagrar ditt huvudlösenord på våra dataservrar: så att ingen har tillgång till ditt konto, inte ens företagets anställda. Varje lösenord och konto är mycket krypterade med den starkaste datasäkerhetsalgoritmen, och koden vi ser ser helt enkelt ut som en slumpmässig sträng av siffror och bokstäver som blandas ihop.

Vad skulle hända om lösenordshanterarens servrar hackades?

Varje lösenord krypteras lokalt på din enhet innan det kommer någonstans i närheten av våra servrar, så om hackare skulle bryta sig in i vårt system skulle de bara få sidor med slumpmässiga bokstäver och siffror utan din nyckel för att dekryptera dem. Det betyder att du och dina kontouppgifter alltid är säkra hos oss.

9. DIGITAL IDENTITETSSKYDD

9.1. Vad är Bitdefender Digital Identity Protection

Online integritet och säkerhet är några av huvudfokusen för internetanvändare nuförtiden. Och det finns några mycket goda skäl till det. Med större dataintrång som inträffar oftare än inte är det absolut nödvändigt att se till att din personligt identifierbara information (PII) är säker och säker.

Men vad kan klassas som personligt identifierbar information? Traditionellt sett betraktades känslig information som fullständigt namn, personnummer, körkort, postadress eller kreditkortsinformation som PII. Så småningom inkluderades också mindre känslig information, som postnummer, IP-adresser eller inloggnings-ID. Med tiden kan ditt digitala fotavtryck, det vill säga de data du lämnar efter dig som ett resultat av att du surfar på internet, komma att inkludera några av dessa.

Bitdefender Digital Identity Protection representerar den privata vägen till online-frihet, vilket gör att du kan återta kontrollen över ditt digitala liv. Och det kräver bara ditt namn, mest använda e-postadress och ditt telefonnummer. Baserat på dessa söker den på både Surface Web och Dark Web efter personlig information som har exponerats offentligt.

Bitdefender Digital Identity Protection erbjuder följande:

- **Övervaknings- och detekteringstjänster:** den övervakar mer än 100 personligt identifierbar information som SSN, kreditkort eller hemadress, och visar all data som hittas om ditt fotavtryck online.

  > **Notera**
  > Bitdefender lagrar eller behandlar inte personligt identifierbar information. Endast hänvisningar till potentiella dataintrång sparas, utan att inkludera känsliga uppgifter.

- **Realtidsvarningar:** Du får meddelanden om dataintrång och exponerad data i Dark Web, personlig information i Surface Web och potentiella imitationer av dig på sociala medier.

- **Lösningar:** Vår tjänst föreslår tydliga åtgärder som krävs för att lösa problem och ger påminnelser om ett problem inte är helt löst. Den kan

också ge instruktioner om hur du tar bort de personliga annonserna, exporterar din data eller stänger av spårningen.

9.2. Komma igång

9.2.1. Aktivera digitalt identitetsskydd

Aktivera Bitdefender Digital Identity Protection-prenumerationen efter att din beställning har lagts och betalats.

1. Öppna bekräftelsen via e-postmeddelandet som du fick kort efter att du har slutfört din beställning och klicka på**KOMMA IGÅNG**.
2. Du kommer att omdirigeras tillhttps://central.bitdefender.com.
   Logga in med ditt Bitdefender Central-konto. Om du inte har ett konto, välj att skapa ett.
3. Efter att ha loggat in kommer prenumerationen automatiskt att kopplas till ditt centrala konto och kommer att utlösa introduktionsprocessen.

Alternativt:

- komma åt**mina prenumerationer**panel från Central, som finns till vänster i fönstret, och klicka**+ Aktivera med kod**.
- skriv in den 10-siffriga nyckeln som finns i ditt bekräftelsemail och tryck**AKTIVERA**.
- om du uppmanas, välj hur du vill använda koden och klicka sedan på**AKTIVERA**.

9.2.2. Konfigurera digitalt identitetsskydd

1. Gå till https://central.bitdefender.com/ och logga in på ditt konto.
   Om du inte redan har ett konto, klicka på **SKAPA KONTO**, skriv sedan ditt fullständiga namn, en e-postadress och ett lösenord.
2. Välj panelen Digital Identity Protection.
   En välkomstskärm visas.
3. Klick **BÖRJA**.
4. Du kommer nu att få information om vilken information du behöver lämna. Dina uppgifter kommer alltid att vara krypterade och säkra.
   Klick **NÄSTA**.

5. Skriv ditt förnamn, mellannamn (om något) och efternamn i motsvarande rutor och klicka sedan **NÄSTA**.
6. Skriv din e-postadress och klicka sedan **NÄSTA**.
   Se till att det är en giltig e-postadress som du kan komma åt.
7. En säkerhetskod skickas till den adress du angett.
   Öppna din e-post, kopiera koden och klistra in den i motsvarande fält.
   Efter det klickar du **KOLLA UPP**.
8. Välj ditt land och ange ditt telefonnummer och klicka sedan **NÄSTA**.
9. Du bör få en säkerhetskod kort efter det.
   Ange koden och välj sedan **KOLLA UPP**.
10 När den första kontrollen har utförts, klicka **AVSLUTA**.

.

> **Notera**
> Du kommer att informeras om några intrång, personligt identifierbar information eller potentiella försök till identitetsstöld upptäcks under denna första kontroll.

Bitdefender Digital Identity Protection är nu konfigurerat.

9.2.3. Granska ditt digitala fotavtryck, dataintrång och möjliga identitetsstölder

Efter att du har slutfört konfigurationen utför Bitdefender Digital Identity Protection en onlinekontroll för att upptäcka potentiella personifieringar, dataintrång och personligt identifierbar information på den öppna webben. Vi rekommenderar att du granskar all information som ingår i **DIGITALT FOTSPÅR**, **DATABROTT** och **KONTROLL FÖR IMPERSONATION** flikar.

- Granska ditt digitala fotavtryck (sida 270)
- Granska dataintrång (sida 271)
- Granska möjliga personifieringar (sida 271)

9.2.4. Förbättra din kontroll

Vi använder data som du tillhandahåller för att övervaka Surface Web och Dark Web för att upptäcka all aktivitet som kan påverka din integritet eller ditt personliga varumärkesrykte.

Om du vill lägga till en annan e-postadress eller ett annat telefonnummer, klicka ⊕, klicka sedan på **LÄGG TILL E-POSTADRESS** eller **LÄGG TILL TELEFONNUMMER** och följ instruktionerna.

9.3. instrumentbräda

Dashboarden samlar information som ingår i **DIGITALT FOTSPÅR**, **DATABROTT** och **KONTROLL FÖR IMPERSONATION** sektioner.

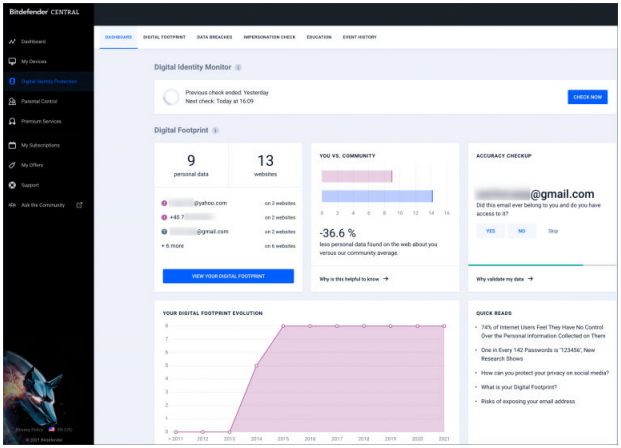
Den innehåller följande:

- Din exponerade data och deras webbkällor
- Den genomsnittliga mängden exponerad data för hela samhället
- Din digitala fotavtrycksutveckling
- Sekretessrelaterat innehåll
- Dataintrång
- Det genomsnittliga antalet dataintrång inom gemenskapen

9.3.1. Digital Identity Monitor

Bitdefenders system använder endast korrekt information och letar efter nya personliga data som exponeras på den öppna webben och den mörka webben och genomsöker alla stora sociala medieplattformar efter tecken på ett försök till identitetsstöld.

Klicka på **KOLLA NU** för att utföra en onlineskanning.



9.4. Digitalt fotavtryck

Din personligt identifierbara information och deras källor visas här. Det är upp till dig att utvärdera om det är ett hot att ha informationen offentlig på webben.

Vår AI-drivna monitor förlitar sig mycket på korrekt data för att upptäcka nya hot, så vänligen berätta för oss om informationen är korrekt eller felaktig.

När du har bekräftat att en bit information är din lägger vi till den i vårt övervakningssystem och förbättrar chanserna att upptäcka andra i framtiden.

9.4.1. Granska ditt digitala fotavtryck

Så här granskar du ditt digitala fotavtryck:

1. Gå till **DIGITALT FOTSPÅR** flik.
2. Information som ännu inte har verifierats visas tillsammans med texten **Kontrollera** på höger sida. Klick **Kontrollera**, välj sedan Ja eller Nej, beroende på fallet.

> **Notera**
> Varje bekräftad information läggs till vår övervakningsalgoritm, vilket förbättrar resultaten som visas av våra tjänster. Information som avvisas kommer inte längre att visas. Den kommer dock fortfarande att finnas tillgänglig på webben.

9.5. Dataintrång

Intrång uppstår när hackare lyckas kringgå ett företags säkerhetsåtgärder och få din personliga information, för att sälja den på den mörka webben. Vanligtvis riktar sig cyberbrottslingar till inloggningsdata, personligt identifierbar information (PII), medicinska journaler och bankrelaterade detaljer.

Alla organisationer eller tjänster kan falla offer för ett dataintrång, men de med en stor konsumentbas gör mer attraktiva mål. Överträdelser inkluderar vanligtvis namn, e-postadresser, användarnamn, lösenord, postadresser, telefonnummer, personnummer (SSN) och kreditkortsuppgifter (nummer, utgångsdatum, CVV).

9.5.1. Granska dataintrång

Så här granskar du dina dataintrång:

1. Gå till **DATABROTT** flik.
2. Under vissa poster hittar du en lista över åtgärder som krävs för att säkra ditt konto. När du har utfört en åtgärd klickar du på rutan bredvid den för att bekräfta.
   Om du inte är säker på hur du utför en uppgift kan du alltid klicka på länken som ingår i uppgiftsbeskrivningen och du omdirigeras till en sida där du hittar alla nödvändiga steg.
   Alla överträdelser kan inte hanteras på detta sätt. Några av dem, som t.ex **Samling #1**, innehåller inte steg. Istället kommer du att omdirigeras till artiklar tillgängliga online där du kan hitta mer hjälp.

> **Notera**
> Bitdefender lagrar eller behandlar inte personligt identifierbar information. Endast hänvisningar till potentiella dataintrång sparas, utan att inkludera känsliga uppgifter.

9.6. Imitationskontroll

Brottslingar som kallas "pretexters" använder konsten att efterlikna sig på många sätt och spelar rollen som en pålitlig individ för att lura sina offer och få tillgång till känslig information. Användningen av "förevändning" definieras som att framställa sig själv som någon annan för att manipulera en mottagare till att tillhandahålla känslig information som lösenord, kreditkortsnummer eller annan konfidentiell information.

Bitdefender Digital Identity Protection övervakar 25 sociala medieplattformar och meddelar dig omedelbart om den hittar en profil som kan vara ett försök till identitetsstöld.

9.6.1. Granska möjliga personifieringar

De **KONTROLL FÖR IMPERSONATION** fliken är där alla möjliga försök kommer att visas. För varje upptäckt kan du välja en av tre möjligheter:

- Det är ett imitationsförsök
- Det är din egen profil
- Det är en annan profil

Beroende på valet kommer Bitdefender Digital Identity Protection att rekommendera specifika steg för att hantera problemet. Varje gång du slutför ett steg kan du markera det som **Gjort**.

9.7. Utbildning

Fliken Utbildning fungerar som en kunskapsbas där användaren kan hitta mer information om hur man skyddar sin digitala identitet.

Artiklar listade här kan sorteras i flera kategorier:

- Brott
- Exponeringar
- Imitationskontroll

För att komma åt den fullständiga versionen av en artikel, klicka på motsvarande **Läs mer** länk.

9.8. Händelsehistorik

Händelsehistoriksektionen är det sätt på vilket vi ständigt kommunicerar med våra användare. Den representerar en kronologiskt ordnad lista över händelser angående skyddet av din digitala identitet.

Förutom nyupptäckta hot (om några) kan du återvända till den här sidan för värdefulla råd om hur du ska uppträda korrekt online, för att öka chanserna att inte hantera sekretessfrågor.

I avsnittet Händelsehistorik kan du hitta följande information:

- Åtgärder utförda
- Serviceuppdateringar
- Dataintrång

10. FÅ HJÄLP

10.1. Ber om hjälp

Bitdefender ger sina kunder en oöverträffad nivå av snabb och exakt support. Om du upplever några problem eller om du har några frågor om din Bitdefender-produkt, kan du använda flera onlineresurser för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefender Customer Care-teamet. Våra supportrepresentanter kommer att svara på dina frågor i tid och ge dig den hjälp du behöver.

10.2. Onlineresurser

Flera onlineresurser finns tillgängliga för att hjälpa dig att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefender Support Center:
  https://www.bitdefender.se/consumer/support/
- Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Du kan också använda din favoritsökmotor för att ta reda på mer information om datorsäkerhet, Bitdefender-produkterna och företaget.

10.2.1. Bitdefender Support Center

Bitdefender Support Center är ett onlineförråd med information om Bitdefender-produkterna. Den lagrar, i ett lättillgängligt format, rapporter om resultaten av den pågående tekniska supporten och buggfixningsaktiviteterna för Bitdefender-support- och utvecklingsteamen, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefender Support Center är öppet för allmänheten och fritt sökbart. Den omfattande informationen den innehåller är ytterligare ett sätt att förse Bitdefender-kunder med den tekniska kunskap och insikt de behöver. Alla giltiga förfrågningar om information eller buggrapporter

som kommer från Bitdefender-klienter hittar så småningom vägen till Bitdefender Support Center, som bugfixrapporter, fuskblad för lösningar eller informationsartiklar för att komplettera produkthjälpfiler.

Bitdefender Support Center är tillgängligt när som helst på följande adress: https://www.bitdefender.se/consumer/support/.

10.2.2. Bitdefender Expert Community

Expertgemenskapen är en miljö där Bitdefender-användare, entusiaster och fans kan engagera sig, utbyta idéer, stödja varandra och dela sina kunskaper och lösningar. Det är också en plats för idéer och ger värdefull feedback till våra utvecklingsteam. Community-medlemmarna är erfarna Bitdefender-användare som gärna hjälper andra kamrater på sin egen tid. Med deras enorma bidrag och genuina frivilliga insatser har vi skapat en kunskapsbas där användare kan hitta svar och vägledning, men med den mänskliga touchen.

Här hittar du meningsfulla konversationer med personer som använder Bitdefender på sina enheter. Gemenskapen erbjuder en sann kontakt med våra medlemmar och gör din röst hörd. Det är en plats där du uppmuntras att delta i vetskapen om att din åsikt och din input respekteras och omhuldas. Som en uppskattad leverantör strävar vi efter att erbjuda en oöverträffad nivå av snabb, exakt support och vi vill föra våra användare närmare oss. Vi har utformat vår community med detta syfte i åtanke.

Du hittar vår webbsida för expertgemenskapen här:

https://community.bitdefender.com/en/

10.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia har all information du behöver om de senaste cyberhoten. Det här är platsen där Bitdefender-experter delar med sig av tips och tricks om hur man kan hålla sig skyddad från hackare, dataintrång, identitetsstöld och sociala identitetsförsök.

Bitdefender Cyberpedias webbsida finns här:

https://www.bitdefender.com/cyberpedia/.

10.3. Kontaktinformation

Effektiv kommunikation är nyckeln till ett framgångsrikt företag. Sedan 2001 har BITDEFENDER etablerat ett obestridligt rykte genom att ständigt

sträva efter bättre kommunikation för att överträffa våra kunders och partners förväntningar. Om du har några frågor, tveka inte att kontakta oss direkt via vår Bitdefender Support Center (sida 273).

https://www.bitdefender.se/consumer/support/

10.3.1. Lokala distributörer

Bitdefender lokala distributörer är redo att svara på alla förfrågningar om deras verksamhetsområden, både i kommersiella och allmänna frågor.

Så här hittar du en Bitdefender-distributör i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din stad med hjälp av motsvarande alternativ.

ORDLISTA

Aktiveringskod

Det är en unik nyckel som kan köpas från återförsäljare och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av en giltig prenumeration för en viss tidsperiod och antal enheter och kan också användas för att förlänga en prenumeration med villkoret att genereras för samma produkt eller tjänst.

ActiveX

ActiveX är en modell för att skriva program så att andra program och operativsystemet kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och beter sig som datorprogram, snarare än statiska sidor. Med ActiveX kan användare ställa eller svara på frågor, använda tryckknappar och interagera på andra sätt med webbsidan. ActiveX-kontroller skrivs ofta med Visual Basic. Active X är anmärkningsvärt för en fullständig brist på säkerhetskontroller; datorsäkerhetsexperter avråder från att använda det över internet.

Avancerat ihållande hot

Advanced persistent hot (APT) utnyttjar sårbarheter i system för att stjäla viktig information för att leverera den till källan. Stora grupper som organisationer, företag eller regeringar är föremål för detta hot. Målet med ett avancerat ihållande hot är att förbli oupptäckt under lång tid och kunna övervaka och samla in viktig information utan att skada de riktade maskinerna. Metoden som används för att injicera hotet i nätverket är genom en PDF-fil eller ett Office-dokument som ser ofarliga ut så att alla användare kan köra filerna.

Reklamprogram

Adware kombineras ofta med en värdapp som tillhandahålls utan kostnad så länge som användaren accepterar adware. Eftersom adware-appar vanligtvis installeras efter att användaren har godkänt ett licensavtal som anger syftet med appen, begås inget brott. Men popup-annonser kan bli irriterande och i vissa fall försämra systemets prestanda. Dessutom kan informationen som vissa av dessa appar samlar in orsaka integritetsproblem för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En disk, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera filer i ett komprimerat format.

Bakdörr

Ett hål i säkerheten i ett system som medvetet lämnats på plats av designers eller underhållare. Motivationen för sådana hål är inte alltid olycksbådande; vissa operativsystem, till exempel, kommer ur lådan med privilegierade konton avsedda att användas av fältservicetekniker eller säljarens underhållsprogrammerare.

Boot sektor

En sektor i början av varje disk som identifierar diskens arkitektur (sektorstorlek, klusterstorlek, och så vidare). För startdiskar innehåller bootsektorn även ett program som laddar operativsystemet.

Boot virus

Ett hot som infekterar startsektorn på en fast eller diskett. Ett försök att starta från en diskett som är infekterad med ett bootsektorvirus gör att hotet blir aktivt i minnet. Varje gång du startar ditt system från den tidpunkten kommer du att ha hotet aktivt i minnet.

Botnet

Termen "botnät" är sammansatt av orden "robot" och "nätverk". Botnät är internetanslutna enheter som är infekterade med hot och kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogram, ransomware och andra typer av hot. Deras mål är att infektera så många uppkopplade enheter som möjligt, såsom datorer, servrar, mobila eller IoT-enheter som tillhör stora företag eller industrier.

Webbläsare

Förkortning för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare inkluderar Microsoft Internet Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare, vilket innebär att de kan visa grafik såväl som text. Dessutom kan de flesta moderna webbläsare presentera multimediainformation, inklusive ljud och video, även om de kräver plugin-program för vissa format.

Brute Force Attack

Lösenordsgissningsattack används för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast med det enklast att gissa lösenordet.

Kommandorad

I ett kommandoradsgränssnitt skriver användaren kommandon i utrymmet som tillhandahålls direkt på skärmen med hjälp av kommandospråk.

Småkakor

Inom internetbranschen beskrivs cookies som små filer som innehåller information om enskilda datorer som kan analyseras och användas av annonsörer för att spåra dina intressen och smaker online. I det här området utvecklas fortfarande cookieteknologi och avsikten är att rikta annonser direkt till det du har sagt att dina intressen är. Det är ett tveeggat svärd för många människor eftersom det å ena sidan är effektivt och relevant eftersom du bara ser annonser om det du är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" vart du går och vad du klickar på. Det är förståeligt nog att det finns en debatt om integritet och många känner sig kränkta av uppfattningen att de ses som ett "SKU-nummer" (ni vet, streckkoden på baksidan av paketen som skannas vid utcheckningslinjen) . Även om denna synpunkt kan vara extrem, är den i vissa fall korrekt.

Cybermobbning

När kamrater eller främlingar begår kränkande handlingar mot barn med avsikt för att fysiskt skada dem. För att skada känslomässigt skickar angriparna elaka meddelanden eller föga smickrande bilder, vilket gör att deras offer isolerar sig från andra eller känner sig frustrerade.

Ordbok Attack

Lösenordsgissningsattacker används för att bryta sig in i ett datorsystem genom att ange en kombination av vanliga ord för att generera potentiella lösenord. Samma metod används för att gissa dekrypteringsnycklar för krypterade meddelanden eller dokument. Ordboksattacker lyckas eftersom många människor är benägna att välja korta och enstaka ordlösenord som är lätta att gissa.

Diskenhet

Det är en maskin som läser data från och skriver data till en disk. En hårddisk läser och skriver hårddiskar. En diskettenhet får åtkomst till disketter. Diskenheter kan antingen vara interna (inrymd i en dator) eller externa (inrymd i en separat låda som ansluts till datorn).

Ladda ner

Att kopiera data (vanligtvis en hel fil) från en huvudkälla till en kringutrustning. Termen används ofta för att beskriva processen att kopiera en fil från en onlinetjänst till sin egen dator. Nedladdning kan också syfta på att kopiera en fil från en nätverksfilserver till en dator i nätverket.

E-post

E-post. En tjänst som skickar meddelanden på datorer via lokala eller globala nätverk.

evenemang

En åtgärd eller händelse som upptäckts av ett program. Händelser kan vara användaråtgärder, som att klicka på en musknapp eller trycka på en tangent, eller systemhändelser, som att minnet blir slut.

Utnyttjar

Ett sätt att dra nytta av olika buggar eller sårbarheter som finns i en dator (mjukvara eller hårdvara). Således kan hackare få kontroll över datorer eller nätverk.

Falskt positivt

Uppstår när en skanner identifierar en fil som infekterad när den faktiskt inte är det.

Filnamnstillägg

Den del av ett filnamn, efter den sista punkten, som anger vilken typ av data som lagras i filen. Många operativsystem använder filnamnstillägg, t.ex. Unix, VMS och MS-DOS. De är vanligtvis från en till tre bokstäver (vissa tråkiga gamla operativsystem stöder inte mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Heuristisk

En regelbaserad metod för att identifiera nya hot. Denna metod för skanning är inte beroende av specifik databas med hotinformation. Fördelen med den heuristiska skanningen är att den inte luras av en ny

variant av ett befintligt hot. Det kan dock ibland rapportera misstänkt kod i vanliga program, vilket genererar den så kallade "falska positiva".

Honungsburk

Ett lockdatorsystem som lockar hackare att studera hur de agerar och identifiera de kätterska metoder de använder för att samla in systeminformation. Företag och företag är mer intresserade av att implementera och använda honeypots för att förbättra sin övergripande säkerhet.

IP

Internet Protocol - Ett routbart protokoll i TCP/IP-protokollsviten som ansvarar för IP-adressering, routing och fragmentering och återmontering av IP-paket.

Java applet

Ett Java-program som är designat för att endast köras på en webbsida. För att använda en applet på en webbsida skulle du ange namnet på appleten och storleken (längd och bredd, i pixlar) som appleten kan använda. När webbsidan nås laddar webbläsaren ner appleten från en server och kör den på användarens dator (klienten). Applets skiljer sig från appar genom att de styrs av ett strikt säkerhetsprotokoll.

Till exempel, även om appletar körs på klienten, kan de inte läsa eller skriva data på klientens dator. Dessutom är appletar ytterligare begränsade så att de bara kan läsa och skriva data från samma domän som de betjänas från.

Keylogger

En keylogger är en app som loggar allt du skriver. Keyloggers är inte skadliga till sin natur. De kan användas för legitima ändamål, som att övervaka anställda eller barnaktivitet. De används dock i allt högre grad av cyberbrottslingar i skadliga syften (till exempel för att samla in privata uppgifter, såsom inloggningsuppgifter och personnummer).

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, stöder kraftfulla makrospråk. Dessa appar låter dig bädda in ett makro i ett dokument och få makrot att köras varje gång dokumentet öppnas.

E-postklient

En e-postklient är en app som gör att du kan skicka och ta emot e-post.

Minne

Interna lagringsutrymmen i datorn. Termen minne identifierar datalagring som kommer i form av chips, och ordet lagring används för minne som finns på band eller diskar. Varje dator kommer med en viss mängd fysiskt minne, vanligtvis kallat huvudminne eller RAM.

Icke-heuristisk

Denna metod för skanning bygger på specifik databas med hotinformation. Fördelen med den icke-heuristiska skanningen är att den inte luras av vad som kan tyckas vara ett hot och inte genererar falsklarm.

Rovdjur online

Individer som försöker locka minderåriga eller tonåringar till konversationer med avsikt att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den idealiska platsen där utsatta barn lätt kan jagas och förföras till att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Packade program

En fil i ett komprimeringsformat. Många operativsystem och appar innehåller kommandon som gör att du kan packa en fil så att den tar mindre minne. Anta till exempel att du har en textfil som innehåller tio på varandra följande mellanslagstecken. Normalt skulle detta kräva tio byte lagring.

Ett program som packar filer skulle dock ersätta mellanslagstecken med ett speciellt mellanslagsserietecken följt av antalet mellanslag som ersätts. I detta fall skulle de tio utrymmena endast kräva två byte. Detta är bara en packningsteknik - det finns många fler.

Väg

Den exakta vägbeskrivningen till en fil på en dator. Dessa riktningar beskrivs vanligtvis med hjälp av det hierarkiska arkiveringssystemet uppifrån och ner.

Rutten mellan två valfria punkter, till exempel kommunikationskanalen mellan två datorer.

Nätfiske

Handlingen att skicka ett e-postmeddelande till en användare som falskeligen påstår sig vara ett etablerat legitimt företag i ett

försök att lura användaren till att överlämna privat information som kommer att användas för identitetsstöld. E-postmeddelandet uppmanar användaren att besöka en webbplats där de ombeds att uppdatera personlig information, såsom lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och inrättad endast för att stjäla användarens information.

Foton

Photon är en innovativ, icke-påträngande Bitdefender-teknik, designad för att minimera prestandapåverkan från din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den användningsmönster som hjälper till att optimera uppstarts- och skanningsprocesser.

Polymorft virus

Ett hot som ändrar form för varje fil som den infekterar. Eftersom de inte har något konsekvent binärt mönster är sådana hot svåra att identifiera.

Hamn

Ett gränssnitt på en dator som du kan ansluta en enhet till. Persondatorer har olika typer av portar. Internt finns det flera portar för att ansluta diskenheter, bildskärmar och tangentbord. Externt har persondatorer portar för anslutning av modem, skrivare, möss och annan kringutrustning.

I TCP/IP- och UDP-nätverk, en slutpunkt till en logisk anslutning. Portnumret identifierar vilken typ av port det är. Till exempel används port 80 för HTTP-trafik.

Ransomware

Ransomware är ett skadligt program som försöker tjäna pengar på användare genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall, är bara några varianter som jagar användarnas personliga system.

Infektionen kan spridas genom att komma åt skräppostmeddelanden, ladda ner e-postbilagor eller installera appar, utan att låta användaren veta vad som händer på hans system. Dagliga användare och företag riktas mot ransomware-hackare.

Rapportfil

En fil som listar åtgärder som har inträffat. Bitdefender har en rapportfil som visar sökvägen som skannats, mapparna, antalet skannade arkiv och filer, hur många infekterade och misstänkta filer som hittades.

Rootkit

Ett rootkit är en uppsättning mjukvaruverktyg som ger åtkomst till ett system på administratörsnivå. Termen användes först för UNIX-operativsystemen och den hänvisade till omkompilerade verktyg som gav inkräktare administrativa rättigheter, så att de kunde dölja sin närvaro så att de inte syns av systemadministratörerna.

Den huvudsakliga rollen för rootkits är att dölja processer, filer, inloggningar och loggar. De kan också fånga upp data från terminaler, nätverksanslutningar eller kringutrustning, om de innehåller lämplig programvara.

Rootkits är inte skadliga till sin natur. Till exempel döljer system och till och med vissa appar viktiga filer med rootkits. Men de används mest för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. I kombination med hot utgör rootkits ett stort hot mot integriteten och säkerheten i ett system. De kan övervaka trafik, skapa bakdörrar i systemet, ändra filer och loggar och undvika upptäckt.

Manus

En annan term för makro- eller batchfil, ett skript är en lista med kommandon som kan köras utan användarinteraktion.

Spam

Elektronisk skräppost eller skräpnyhetsgrupper. Allmänt känd som all oönskad e-post.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens internetanslutning utan hans eller hennes vetskap, vanligtvis i reklamsyfte. Spionprogram är vanligtvis paketerade som en dold komponent av gratisprogram eller shareware-program som kan laddas ner från internet; Det bör dock noteras att majoriteten av shareware och freeware-appar inte kommer med spionprogram. När det väl har installerats övervakar spionprogrammet användaraktivitet på internet och överför informationen i bakgrunden till någon annan. Spionprogram kan också samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med ett trojansk hästhot är det faktum att användare omedvetet installerar produkten när de installerar något annat. Ett vanligt sätt att bli offer för spionprogram är att ladda ner vissa peer-to-peer filbytesprodukter som är tillgängliga idag.

Bortsett från frågorna om etik och integritet stjäl spionprogram från användaren genom att använda datorns minnesresurser och även genom att äta bandbredd då det skickar information tillbaka till spionprogrammets hembas via användarens internetanslutning. Eftersom spionprogram använder minne och systemresurser kan apparna som körs i bakgrunden leda till systemkrascher eller allmän systeminstabilitet.

Startobjekt

Alla filer som placeras i den här mappen öppnas när datorn startar. Till exempel kan en startskärm, en ljudfil som ska spelas upp när datorn startar, en påminnelseskalender eller appar vara startobjekt. Normalt placeras ett alias för en fil i den här mappen istället för själva filen.

Prenumeration

Köpeavtal som ger användaren rätt att använda en viss produkt eller tjänst på ett visst antal enheter och under en viss tid. Ett utgånget abonnemang kan förnyas automatiskt med den information som användaren lämnade vid första köpet.

Systemfältet

Systemfältet, som introducerades med Windows 95, finns i aktivitetsfältet i Windows (vanligtvis längst ner bredvid klockan) och innehåller miniatyrikoner för enkel åtkomst till systemfunktioner som fax, skrivare, modem, volym med mera. Dubbelklicka eller högerklicka på en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Transmission Control Protocol/Internet Protocol - En uppsättning nätverksprotokoll som ofta används på internet som tillhandahåller kommunikation över sammankopplade nätverk av datorer med olika hårdvaruarkitekturer och olika operativsystem. TCP/IP innehåller standarder för hur datorer kommunicerar och konventioner för att ansluta nätverk och dirigera trafik.

Hot

Ett program eller kod som läses in på din dator utan din vetskap och som körs mot din vilja. De flesta hot kan också replikera sig själva. Alla

datorhot är konstgjorda. Ett enkelt hot som kan kopiera sig själv om och om igen är relativt lätt att producera. Även ett så enkelt hot är farligt eftersom det snabbt kommer att använda allt tillgängligt minne och få systemet att stanna. En ännu farligare typ av hot är en som kan överföra sig själv över nätverk och kringgå säkerhetssystem.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att upptäcka och eliminera hotet.

Trojan

Ett destruktivt program som maskerar sig som en godartad app. Till skillnad från skadliga program och maskar replikerar trojaner inte sig själva men de kan vara lika destruktiva. En av de mest lömska typerna av trojanska hästhot är ett program som påstår sig befria din dator från hot men istället introducerar hot på din dator.

Termen kommer från en berättelse i Homeros Iliaden, där grekerna ger en gigantisk trähäst till sina fiender, trojanerna, skenbart som ett fredsoffer. Men efter att trojanerna släpat hästen innanför sina stadsmurar, smyger grekiska soldater ut ur hästens ihåliga mage och öppnar stadsportarna, så att deras landsmän kan strömma in och fånga Troja.

Uppdatering

En ny version av en mjuk- eller hårdvaruprodukt utformad för att ersätta en äldre version av samma produkt. Dessutom kontrollerar installationsrutinerna för uppdateringar ofta att en äldre version redan är installerad på din dator; Om inte kan du inte installera uppdateringen.

Bitdefender har sin egen uppdateringsfunktion som låter dig söka manuellt efter uppdateringar, eller låta den uppdatera produkten automatiskt.

Virtuellt privat nätverk (VPN)

Är en teknik som aktiverar en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka data och svårt för snokare att få tag på dem. Ett bevis på säkerheten är autentiseringen, som endast kan göras med ett användarnamn och lösenord.

Mask

Ett program som sprider sig över ett nätverk och reproducerar sig själv allt eftersom. Den kan inte koppla sig till andra program.