Bitdefender
SMALL OFFICE SECURITY

ANVÄNDARMANUAL

Android Windows Mac iOS

Bitdefender Small Office Security
Användarmanual

Publication date 07-10-2019

Juridisk notering

Bitdefender

Innehållsförteckning

Introduktion till Bitdefender Small Office Security

Bitdefender Small Office Security-prenumerationen vänder sig till små företag som kör mellan 5 och 20 Windows-, macOS-, Android- och iOS-baserade enheter och vill öka säkerheten, förhindra dataförlust eller förhindra att hackare eller skadlig kod exploaterar säkerhetsbrister i nätverket.

Hanteringen av alla anslutna enheter kan göras från Bitdefender Central-plattformen förutsatt att administratören är inloggad med de inloggningsuppgifter som användes för att aktivera den köpta prenumerationen. För att komma till Bitdefender Central på Windows och macOS, gå till https://central.bitdefender.com och installera önskad app på iOS och Android, som kan laddas ned från butiksappen associerad med varje plattform.

För att förhindra användare från att göra ändringar inom funktionerna och inställningarna som kan påverka nätverkets säkerhet, kan administratören ange ett lösenord från Bitdefender-kontot. Det här alternativet är tillgängligt för Bitdefender Total Security-produkten som kan installeras på Windows-baserade enheter.

Aktivitetsområdet i Bitdefender Central ger dig en allmän översikt över de anslutna enheterna och deras skyddsstatus. Ifall hot identifieras kan administratören köra en skanning på alla påverkade enheterna samtidigt.

Om du redan hare ett Bitdefender-konto med en aktiv prenumeration för en annan produkt eller paket, måste du ändå skapa ett nytt konto med en annan e-postadress för att aktivera prenumerationen på Bitdefender Small Office Security. En prenumeration kan aktiveras under installationsprocessen för en av produkterna som ingår i paketet, eller från Bitdefender Central såsom beskrivs i *"Aktivera prenumeration"* (p. 30). Tillsammans med aktiveringsprocessen börjar giltigheten för prenumerationen räknas ned.

Den här guiden är ordnad runt de fyra produkter som ingår i Bitdefender Small Office Security:

- "Total Security for PC" (p. 1)

  Lär dig hur du använder produkten på dina Windows-baserade stationära och bärbara datorer.

- "Antivirus for Mac" (p. 183)

  Lär dig hur du använder produkten på din Mac.

- "Mobile Security for iOS" (p. 225)

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

- "Mobile Security for Android" (p. 248)

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

- "Kontakta oss" (p. 289)

  Ta reda på var du ska leta efter hjälp om något oväntat inträffar.

TOTAL SECURITY FOR PC

1. INSTALLATION

1.1. Förbereder för installation

Innan du installerar Bitdefender Total Security, fullför dessa förberedelser för att försäkra att installationen ska gå smidigt:

- Försäkra dig om att datorn som du har tänkt installera Bitdefender på, uppfyller de lägsta systemkraven. Om datorn inte uppfyller alla minsta systemkrav kommer inte Bitdefender att installeras, eller om den installeras kommer den inte att fungera som den ska och orsaka avmattning samt instabilitet på systemet. För en komplett lista över systemkrav, se "*Systemkrav*" (p. 2).
- Logga in på datorn genom att använda ett administratörskonto.
- Ta bort alla andra liknande program från datorn. Om något upptäcks under Bitdefender-installationsprocessen blir du meddelad om att avinstallera det. Att köra två säkerhetsprogram samtidigt kan påverka deras aktivitet samt orsaka stora problem med systemet. Windows Defender inaktiveras under installationen.
- Inaktivera eller ta bort alla brandväggsprogram som kanske körs på datorn. Att köra två brandväggssprogram samtidigt kan påverka deras aktivitet samt orsaka stora problem med systemet. Windows-brandväggen inaktiveras under installationen.
- Vi rekommenderar att din dator är ansluten till Internet under installationen, även vid installation från en CD/DVD. Om nyare versioner av de app-filer som ingår i installationspaketet är tillgängliga kan Bitdefender hämta och installera dem.

1.2. Systemkrav

Du kan endast installera Bitdefender Total Security på datorer som använder följande operativsystem:

- Windows 7 med Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Innan installation, försäkra dig om att din dator möter minimisystemkraven.

Notera

Du hittar det Windows-operativsystem din dator kör och maskinvaruinformation:

- I **Windows 7** högerklickar du på **Min dator** på skrivbordet och väljer sedan **Egenskaper** från menyn.
- I **Windows 8**, från Windows Start-skärm, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt i startskärmen) och högerklicka sedan på dess ikon. I **Windows 8.1** letar du upp **Den här datorn**.

  Välj**Egenskaper** i menyn längst ned. Titta i **System**-området för att hitta information om din systemtyp.
- I **Windows 10**, skriver du **System** i sökrutan från aktivitetsfältet och klickar på ikonen. Titta i **System**-området för att hitta information om din systemtyp.

1.2.1. Minsta systemkrav

- 2 GB ledigt hårddiskutrymme tillgängligt
- Dual Core 1.6 GHz processor
- 1 GB minne (RAM)

1.2.2. Rekommenderade systemkrav

- 2,5 GB tillgängligt hårddiskutrymme (minst 800 MB på systemenheten)
- Intel CORE Duo (2 GHz) eller motsvarande processor
- 2 GB minne (RAM)

1.2.3. Programvarukrav

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

- Microsoft Edge 40 och senare
- 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 senare

1.3. Installera din Bitdefender-produkt

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet hämtat till din dator från Bitdefender Central.

Om ditt köp omfattar mer än en dator upprepar du installationsprocessen och aktiverar produkten med samma konto på varje dator. Det konto du måste använda är det som innehåller din Bitdefender aktiva prenumeration.

1.3.1. Installera från Bitdefender Central

Från Bitdefender Central kan du hämta installationspaketet som motsvarar den köpta prenumerationen. När installationsprocessen är klar är Bitdefender Total Security aktiverad.

Hämta Bitdefender Total Security från Bitdefender Central:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:
   - **Skydda den här enheten**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.
     b. Spara installationsfilen.
   - **Skydda andra enheter**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.
     b. Klicka på **SKICKA NEDLADDNINGSLÄNK**.
     c. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**.

        Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.
     d. Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.
4. Vänta tills nedladdningen är slutfört och kör sedan installationsprogrammet.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om systemet inte uppfyller de minsta kraven för att installera Bitdefender informeras du om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender hittas, uppmanas du att ta bort den från systemet. Följ anvisningarna för att ta bort programvaran från systemet och därmed undvika problem som inträffar senare. Du kanske måste starta om datorn för att slutföra borttagningen av de hittade säkerhetslösningarna.

Bitdefender Total Security-installationspaketet uppdateras fortlöpande.

Notera
Hämtning av installationsfilerna kan ta lång tid, särskilt över långsamma Internet-anslutningar.

När installationen är validerad visas konfigurationsguiden. Följ stegen för att installera Bitdefender Total Security.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Total Security.

Om du inte accepterar dessa villkor stänger du fönstret. Installationsprocessenn kommer att överges och du kommer att lämna installationen.

Två ytterligare uppgifter kan utföras vid det här steget:

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

Klicka på **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills det är slutfört. Detaljerad information om förloppet visas.

Viktiga områden i systemet skannas för hot, de senaste versionerna av app-filerna hämtas och installeras och Bitdefender-tjänsterna startas. Det här steget kan ta några minuter. Klicka **HOPPA ÖVER SKANNING** om du vill skanna systemet senare. Mer information om hur du kör en systemskanning finns i *"Kör en systemskanning"* (p. 71).

Steg 3 - Installation slutförd

Din Bitdefender har installerats.

En sammanfattning av install processen kommer att visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av datorn behövas. Klicka på **BÖRJA ANVÄNDA Bitdefender** för att fortsätta.

Steg 4 - Kom igång

I fönstret **Kom igång** kan du se information om din aktiva prenumeration.

Klicka på **AVSLUTA** för att komma till Bitdefender Total Security-gränssnittet.

2. KOMMA IGÅNG

2.1. Grunderna

När du väl installerat Bitdefender Total Security är din dator skyddad mot alla typer av hot (som skadlig kod, ransomware, exploateringar, botnets och trojaner) och Internet hot (som hackare, nätfiske och skräppost).

Appen använder Photon-teknik för att förbättra hastigheten och prestanda för hotskanningsprocessen. Det fungerar genom att lära sig användningsmönstren för dina systemappar för att veta vad och när det ska skanna och minimerar därmed påverkan på din systemprestanda.

Att ansluta till offentliga nätverk som tillhör flygplatser, köpcenter, kaféer eller hotell utan skydd kan vara farligt för din enhet och dina data. Huvudsakligen för att bedragare kan se din aktivitet och hitta det rätta ögonblicket för att stjäla personlig information, men också för att alla kan se din IP-adress och därmed göra din maskin till ett offer för framtida cyberattacker. För att undvika sådana olyckliga situationer ska du installera och använda appen *"VPN"* (p. 131).

Du kan hålla reda på dina lösenord och onlinekonton genom att lagra dem med *"Lösenordshanteringsskydd för dina inloggningsuppgifter"* (p. 122) i en plånbok. Med ett enda huvudlösenord kan du skydda din integritet från inkräktare som kan försöka komma åt dina pengar.

"Webbkameraskydd" (p. 110)håller ej betrodda appar borta från att nå din videokamera, för att undvika hackningsförsök. Baserat på Bitdefender-användarnas val är åtkomst till webbkameran från populära appar tillåten eller blockerad.

För att skydda dig från eventuella snokar och spioner när din enhet är ansluten till ett osäkert trådlöst nätverk, analyserar Bitdefender dess säkerhetsnivå och när det behövs, ger rekommendationer för att öka säkerheten för dina onlineaktiviteter. Se *"Wi-Fi Security Advisor"* (p. 106) för anvisningar om hur du håller dina personuppgifter säkra.

Dina personliga filer lagrade lokalt som dokument, foton eller filmer och även de som är lagrade i molnet kan hållas långt bort från dagens farligaste hot, nämligen ransomware. Se *"Safe Files"* (p. 113) för information om hur du placerar personliga filer i ett skydd.

Filer som krypterats av ransomware kan nu återställas utan att behöva betala pengar för en begärd lösensumma. Se *"Avhjälpning av ransomware"* (p. 116) för information om hur du återställer krypterade filer.

När du arbetar, spelar spel eller tittar på film kan Bitdefender ge dig en kontinuerlig användarupplevelse genom att fördröja uppgifter, eliminera avbrott och justera systemets visuella effekter. Du kan utnyttja allt detta genom att aktivera och konfigurera *"Profiler"* (p. 146).

Bitdefender fattar de mest säkerhetsrelaterade besluten åt dig och visar sällan popup-meddelanden. Detaljer om åtgärder som vidtas och information om programdrift finns i fönstret Meddelanden. Mer information finns på *"Aviseringar"* (p. 9).

Då och då bör du öppna Bitdefender och lösa eventuella existerande problem. Du kan behöva konfigurera särskilda Bitdefenderkomponenter eller ta till förebyggande åtgärder för att skydda din dator och din information.

För att använda onlinefunktionerna i Bitdefender Total Security och hantera dina prenumerationer och enheter öppnar du ditt Bitdefender-konto. Mer information finns på *"Bitdefender Central"* (p. 25).

I avsnitt *"Hur"* (p. 40) hittar du alla steg för steg-anvisningar om hur du utför vanliga uppgifter. Om du upplever problem med Bitdefender kan du läsa avsnittet *"Lösa vanliga problem"* (p. 154) för möjliga lösningar till de vanligaste problemen.

2.1.1. Öppna Bitdefender-fönstret

Följ stegen nedan för att komma till huvudgränssnittet i Bitdefender Total Security:

- I **Windows 7**:
  1. Klicka på **Start** och gå till **Alla program**.
  2. Klicka på **Bitdefender**.
  3. Klicka på **Bitdefender Total Security** eller, snabbare, dubbelklicka på Bitdefender -ikonen i systemfältet.
- I **Windows 8 och Windows 8.1**:

  Leta upp Bitdefender från Windows Start-skärm (du kan till exempel börja skriva "Bitdefender" direkt på Start-skärmen) och därefter klicka på ikonen.

Alternativy kan du öppna skrivbordsappen och sedan dubbelklicka på Bitdefender -ikonen i systemfältet.

- I **Windows 10**:

  Skriv "Bitdefender" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon. Alternativt dubbelklickar du på Bitdefender -ikonen i systemfältet.

Mer information om Bitdefender-fönstret och ikonen i systemfältet finns i *"Bitdefender-gränssnitt"* (p. 13).

2.1.2. Aviseringar

Bitdefender för endetaljerad logg över händelser som rör dess aktivitet på din dator. Varje gång något som är relevant för säkerheten för system eller data inträffar, läggs ett nytt meddelande till i området Bitdefender-meddelanden, på ett liknande sätt som när ett nytt e-postmeddelande visas i inkorgen.

Meddelanden är ett viktigt verktyg för att övervaka och hantera ditt Bitdefender-skydd. Exempelvis kan du enkelt kontrollera om uppdateringen utfördes med framgång, om hot eller säkerhetsrisker hittades på din dator osv. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som vidtagits av Bitdefender.

Öppna meddelandeloggen genom att klicka på **Meddelanden** på navigeringsmenyn på Bitdefender-gränssnittet. Varje gång en kritisk händelse inträffar kan du se en räknare på -ikonen.

Beroende på typ och allvarlighetsgrad grupperas meddelanden i:

- **Kritiska** händelser indikerar kritiska problem. Du bör kontrollera dem omedelbart.
- **Varnings**-händelser anger problem som inte är kritiska. Du bör kontrollera dem och åtgärda dem när du har tid.
- **Informations**-händelser indikerar lyckade åtgärder.

Klicka på varje flik för att hitta mer information om de genererade händelserna. Kort information visas med ett klicka på varje händelserubrik, nämligen: en kort beskrivning, åtgärden Bitdefender vidtog för den när den inträffade samt datum och tid när den inträffade. Alternativ kan finnas för att vidta ytterligare åtgärder om det behövs.

För att det ska vara enklare att hantera loggade händelser har meddelandefönstret alternativ för att ta bort alla händelser i det avsnittet eller markera dem som lästa.

2.1.3. Profiler

Vissa datoraktiviteter, som onlinespel eller videopresentationer, kräver ökad systemresponsivitet, hög prestanda och inga avbrott. När din bärbara dator körs på batterikraft är det bäst att onödiga åtgärder, som kräver ytterligare kraft, skjuts upp tills datorn återigen är ansluten till elnätet.

Bitdefender-profiler tilldelar mer systemresurser till de appar som körs genom att tillfälligt ändra skyddsinställningar och justera systemkonfiguration. Följdriktligen minimeras systeminverkan på din aktivitet.

För att anpassa sig till olika aktiviteter levereras Bitdefender med följande profiler:

Arbetsprofil
: Optimerar din arbetseffektivitet genom att identifiera och justera produkt- och systeminställningarna.

Filmprofil
: Förbättrar visuella effekter och eliminerar avbrott när du tittar på film.

Spelprofil
: Förbättrar visuella effekter och eliminerar avbrott när du spelar spel.

Publik Wi-Fi-profil
: Tillämpar produktinställningar för att dra nytta av fullständigt skydd vid anslutning till ett osäkert trådlöst nätverk.

Batterilägesprofil
: Tillämpar produktinställningar och håller ned bakgrundsaktivitet för att spara batteritid.

Konfigurera automatisk aktivering av profiler

För en lättanvänd upplevelse kan du konfigurera Bitdefender att hantera din arbetsprofil. I det här fallet upptäcker Bitdefender automatiskt den aktivitet du utför och tillämpar optimeringsinställningar för system och produkt.

För att tillåta Bitdefender att aktivera profiler:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.

2. Gå till fliken **Profiler**.
3. Använd motsvarande omkopplare för att slå på **Aktivera profiler automatiskt**.

Om du inte vill att profilerna ska aktiveras automatiskt slår du av omkopplaren.

Slå på motsvarande omkopplare för att aktivera en profil manuellt. Endast en profil i taget kan aktiveras manuellt.

Mer information om profiler finns i "*Profiler*" (p. 146).

2.1.4. Lösenordskyddade Bitdefender-inställningar

Om du inte är den enda personen med administrativa rättigheter som använder den här datorn, rekommenderas det att du skyddar dina Bitdefenderinställningar med ett lösenord.

Konfigurera lösenordsskydd för Bitdefender-inställningarna:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** aktiverar du **Lösenordsskydd**.
3. Skriv lösenordet i de två fälten och klicka därefter på **OK**. Lösenordet måste innehålla minst 8 tecken

När du har ställt in ett lösenord måste den som försöker ändra Bitdefender-inställningarna först ange lösenordet.

Viktigt

Kom ihåg ditt lösenord eller förvara det på en säker plats. Om du glömmer bort lösenordet måste du ominstallera programmet eller kontakta Bitdefender för support.

För att ta bort lösenordsskydd:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** inaktiverar du **Lösenordsskydd**.
3. Skriv lösenordet och klicka sedan på **OK**.

Notera

Ändra lösenordet för din produkt genom att klicka på **Ändra lösenord**. Skriv ditt aktuella lösenord och klicka sedan på **OK**. I det nya fönster som visas

skriver du det nya lösenord du vill använda från och med nu för att begränsa åtkomsten till dina Bitdefender-inställningar.

2.1.5. Produktrapporter

Produktrapporter innehåller information om hur du använder den Bitdefender-produkt du har installerat. Den här informationen är viktig för att förbättra produkten och kan hjälpa oss att ge dig en bättre upplevelse i framtiden.

Observera att dessa rapporter inte innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.

Om du under installationsprocessen har valt att skicka sådana rapporter till Bitdefender-servrarna och nu vill stoppa processen:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till **Avancerat** fliken.
3. Stäng av **Produktrapporter**.

2.1.6. Meddelanden om särskilda erbjudanden

När kampanjerbjudanden är tillgängliga ställs Bitdefender-produkten in på att meddela dig via ett popup-fönster. Det här ger dig möjlighet att dra nytta ab fördelaktiga priser och hålla dina enheter skyddade under en längre tidsperiod.

För att slå av eller på meddelanden om specialerbjudanden:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Slå av eller på motsvarande omkopplare i fönstret **Allmänt**.

Alternativet för specialerbjudanden och produktmeddelanden är aktiverad som standard.

2.1.7. Skanningstjänst mot skadlig kod

Bitdefender integreras med Microsoft Antimalware Scan Interface (AMSI), ett sätt att hjälpa dig fortsätta vara skyddad från dynamisk skriptbaserad skadlig kod och icke-traditionella cyberattacker. AMSI är en generisk gränssnittsstandard som låter program och tjänster integreras med Bitdefender-produkter.

Stänga av eller slå på integration med Antimalware Scan Interface:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Slå av eller på motsvarande omkopplare i fönstret **Allmänt**.

Alternativet för integrering med Antimalware Scan Interface är aktiverat som standard och är endast tillgängligt i Windows 10.

2.2. Bitdefender-gränssnitt

Bitdefender Total Security uppfyller behoven lika mycket för nybörjare på datorer som för väldigt tekniska människor. Dess grafiska användargränssnitt är utformat för att passa alla sorters människor.

För att gå igenom Bitdefender-gränssnittet finns en introduktionsguide som innehåller information om hur du interagerar med produkten och hur du konfigurerar den på den övre vänstra sidan. Välj rätt höger vinkelparentes för att fortsätta guidas eller **Hoppa över rundtur** för att stänga guiden.

Bitdefenders systemfältsikon är tillgänglig när som helst, oavsett om du vill öppna huvudfönstret, köra en produktuppdatering eller visa information om den installerade versionen.

I huvudfönstret finns information om din säkerhetsstatus. Baserat på din enhetsanvändning och behov visar Autopilot här olika typer av rekommendationer som hjälper dig att förbättra din enhetssäkerhet och prestanda. Dessutom kan du lägga till snabbåtgärder som du använder ofta, så att du har dem till hands när du behöver dem.

Från navigeringsmenyn till vänster kan du öppna ditt Bitdefender-konto, inställningarna, meddelanden och Bitdefender-avsnitten för detaljerad konfiguration och avancerade administrativa uppgifter. Du kan även kontakta oss för support om du har frågor eller något oväntat inträffar.

Om du vill hålla ett konstant öga på viktig säkerhetsinformation och ha snabb åtkomst till viktiga inställningar lägger du till säkerhetswidgeten på skrivbordet.

2.2.1. Systemfältsikon

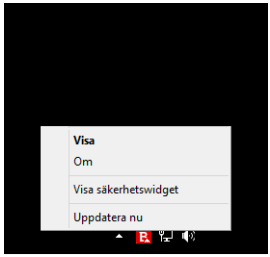
För att snabbare hantera hela produkten kan du använda Bitdefender-ikonen  i systemfältet.

Notera

Bitdefender-ikonen kanske inte är synlig hela tiden. För att ikonen ska visas permanent:

- I **Windows 7, Windows 8 och Windows 8.1**:
  1. Klicka på pilen i det nedre högra hörnet på skärmen.
  2. Klicka på **Anpassa...** för att öppna fönstret Meddelandeområdesikoner.
  3. Välj alternativet **Visa ikoner och meddelanden** för **Bitdefender-agent**-ikonen.
- I **Windows 10**:
  1. Högerklicka aktivitetsfältet och välj **Egenskaper**.
  2. Klicka på **Anpassa** i fönstret Aktivitetsfält.
  3. Klicka på länken **Välj vilka ikoner som ska visas i aktivitetsfältet** i fönstret **Meddelanden och åtgärder**.
  4. Aktivera omkopplaren bredvid **Bitdefender-agenten**.

Om du dubbelklickar den här ikonen kommer Bitdefender att öppnas. Genom att högerklicka ikonen kommer en kontextmeny att snabbt låta dig hantera Bitdefenderprodukten.



Ikon

- **Visa** - öppnar huvudfönstret i Bitdefender.
- **Om** - öppnar ett fönster där du kan se information om Bitdefender, var du kan få hjälp om något oväntat inträffar, var du hittar och visar prenumerationsavtalet, tredjepartskomponenter och sekretesspolicy.
- **Dölj/Visa säkerhetswidget** - aktiverar/inaktiverar Säkerhetswidget.
- **Uppdatera nu** - startar en omedelbar uppdatering. Du kan följa upp uppdateringsstatusen i uppdateringspanelen i Bitdefenders huvudfönster.

Bitdefender systemfältsikon informerar dig när problem påverkar din dator eller om hur produkten fungerar, genom att visa en speciell symbol, enligt följande:

Det finns inga problem som påverkar ditt systems säkerhet.

Kritiska problem påverkar ditt systems säkerhet. De kräver din omedelbara uppmärksamhet och måste lösas så snart som möjligt.

Om Bitdefender inte fungerar visas systemfältsikonen mot en grå bakgrund: . Det här händer oftast när prenumerationen går ut. Det kan även hända när Bitdefender tjänsterna inte svarar eller när andra fel påverkar Bitdefender normala aktivitet.

2.2.2. Navigeringsmeny

På den vänstra sidan i Bitdefender-gränssnittet finns navigeringsmenyn, som gör det möjligt för dig att snabbt komma till Bitdefender-funktionerna och verktygen du behöver för att hantera din produkt. Flikarna som finns i det området är:

- **Kontrollpanel**. Härifrån kan du snabbt åtgärda säkerhetsproblem, visa rekommendationer enligt dina systembehov och användningsmönster, utföra snabbåtgärder och installera Bitdefender på andra enheter.
- **Skydd**. Härifrån kan du starta och konfigurera antivirusskanningar, öppna brandväggsinställningar, skydda filer och appar från ransomwareattacker, återställa data ifall de krypteras av ransomware och konfigurera skydd medan du surfar på Internet.
- **Sekretess**. Härifrån kan du skapa lösenordshanterare för dina onlinekonton, skydda åtkomsten till din webbkamera från oönskade ögon, göra onlinebetalningar i en säker miljö, öppna VPN-appen och skydda dina barn genom att visa och begränsa deras onlineaktivitet.
- **Verktyg**. Härifrån kan du förbättra systemets hastighet och konfigurera antistöldfunktionen för dina enheter.
- **Meddelanden**. Härifrån har du åtkomst till de genererade meddelandena.
- **Mitt konto**. Härifrån kan du komma åt ditt Bitdefender-konto för att verifiera dina prenumerationer och utföra säkerhetsåtgärder på de enheter du hanterar. Information om Bitdefender-konto och pågående prenumeration finns också.
- **Inställningar**. Härifrån har du åtkomst till allmänna inställningar.

- **Support**. Härifrån kan du, när du behöver hjälp med att lösa ett problem med Bitdefender Total Security, kontakta Bitdefenders tekniska supportavdelning.

2.2.3. Kontrollpanel

I kontrollpanelsfönstret kan du utföra vanliga åtgärder, snabbt lösa säkerhetsproblem, visa information om produktfunktion och öppna panelerna varifrån du kan konfigurera produktinställningarna.

Allt är bara några klick borta.

Fönstret är indelat i tre huvudområden:

Säkerhetsstatusområde
: Härifrån kan du kontrollera datorns säkerhetsstatus.

Auto Pilot
: Härifrån kan du kontrollera Autopilot-rekommendationerna för att säkerställa korrekt funktionalitet i systemet.

Snabbåtgärder
: Härifrån kan du köra olika jobb för att hålla systemet skyddat och att det körs i optimal hastighet. Du kan även installera Bitdefender på andra enheter förutsatt att din prenumeration har tillgängliga platser.

Säkerhetsstatusområde

Bitdefender använder system för spårning av problem för att upptäcka och informera dig om problem som kan påverka din dators säkerhet och information. Upptäckta problem omfattar viktiga skyddsinställningar som är avstängda och andra förhållanden som kan innebära en säkerhetsrisk.

Varje gång problem påverkar säkerheten för din dator ändras statusen som visas på den övre sidan av Bitdefender-gränssnittet till röd. Den visade statusen anger hur problemen påverkar ditt system. Dessutom ändras systemfältsikonen till och om du för muspekaren över ikonen kommer en popup att bekräfta att det finns olösta problem.

Eftersom de upptäckta problemen kan förhindra Bitdefender från att skydda dig mot hot eller utgöra en stor säkerhetsrisk, rekommenderar vi att du är uppmärksam och löser dem så snabbt som möjligt. Klicka på knappen bredvid det upptäckta problemet för att lösa det.

Auto Pilot

För att ge dig en effektiv drift och ökat skydd när du utför olika aktiviteter, fungerar Bitdefender Autopilot som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, om du antingen arbetar, utför onlinebetalningar, ser på film eller spelar spel, kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov. De föreslagna rekommendationerna kan också handla om åtgärder du behöver utföra för att din produkt ska fungera fullt ut.

För att börja använda en föreslagen funktion eller göra förbättringar av din produkt, klickar du på motsvarande knapp.

Stänga av Autopilot-meddelanden

För att du ska uppmärksamma Autopilot-rekommendationerna är Bitdefender-produkten inställd på att meddela dig via ett popupfönster.

Stänga av Autopilot-meddelanden:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** stänger du av **Rekommendationsmeddelanden**.

Snabbåtgärder

Med snabbåtgärder kan du snabbt starta uppgifter som du anser vara viktiga för att hålla ditt system skyddat och köra i optimal hastighet.

Som standard kommer Bitdefender med några snabbåtgärder som kan ersättas med dem du använder mest. Byta ut en snabbåtgärd:

1. Klicka på + -ikonen i det övre högra hörnet på det kort du vill ta bort.
2. Peka på den uppgift du vill lägga till i huvudgränssnittet och klicka sedan på **LÄGG TILL**.

De uppgifter du kan lägga till i huvudgränssnittet är:

- **Snabbsökning**. Kör en snabbskanning för att direkt upptäcka möjliga hot som kan finns på din dator.
- **Systemskanning**. Kör en systemskanning för att se till att din dator är ren från hot.
- **Vulnerability Scan**. Skanna din dator för säkerhetsrisker för att se till att alla installerade appar, tillsammans med operativsystemet, är uppdaterade och fungerar som de ska.

- **Kontrollera Wi-Fi-säkerhet**. Öppna Wi-Fi Security Advisor för att kontrollera om det trådlösa hemnätverk du är ansluten till är säkert eller inte och om det har säkerhetsrisker.
- **Plånböcker**. Visa och hantera dina plånböcker.
- **Öppna SafePay**. Öppna Bitdefender Safepay™ för att skydda dina känsliga data medan du utför onlinetransaktioner.
- **Öppna VPN**. Öppna Bitdefender VPN för att lägga till ett extra lager skydd när du är ansluten till Internet.
- **Filförstöraren**. Starta verktyget File Shredder för att ta bort spår efter känsliga data från din dator.
- **Filvalv**. Skapa valv där du lagrar dina konfidentiella och känsliga dokument.
- **Öppna OneClick Optimizer**. Frigör diskutrymmer, åtgärda registerfel och skydda din integritet genom att ta bort filer som kanske inte längre behövs med en enda knapptryckning.
- **Öppna startoptimerare**. Minska systemstarttid genom att undanta onödiga appar från att köras vid start.
- **Rensa min enhet**. Gör plats för nya data genom att radera onödiga filer.

Börja skydda ytterligare enheter med Bitdefender:

1. Klicka på **Installera på en annan enhet**.

   Du omdirigeras till Bitdefender-kontosidan. Se till att du är inloggad med dina inloggningsuppgifter.

2. Klicka på **SKICKA HÄMTNINGSLÄNK** i det fönster som visas.

3. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

   Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och tryck på motsvarande hämtningsknapp.

Beroende på ditt val installeras följande Bitdefender-produkter:

- Bitdefender på Windows-baserade enheter.
- Bitdefender Antivirus for Mac på macOS-baserade enheter.
- Bitdefender Mobile Security på Android-baserade enheter.
- Bitdefender Mobile Security på iOS-baserade enheter.

2.2.4. Bitdefender-avsnitten

Bitdefender-produkten kommer med tre avsnitt indelade i användbara funktioner som hjälper dig att hålla dig skyddad medan du arbetar, surfar på nätet eller gör onlinebetalningar, förbättrar hastigheten för systemet och mycket mer.

När du vill komma åt funktionerna för ett specifikt avsnitt eller börja konfigurera din produkt använder du följande ikoner som finns på navigeringsmenyn på Bitdefender-gränssnittet:

- Skydd
- Sekretess
- Verktyg

Skydd

I avsnittet Skydd kan du konfigurera dina avancerade säkerhetsinställningar, hantera vänner och spammare, visa och redigera nätverksanslutningsinställningar, konfigurera funktionerna Safe Files och Online Threat Prevention, kontrollera och åtgärda systemsäkerhetsrisker för de trådlösa nätverk du ansluter till.

De funktioner du kan hantera i avsnittet Skydd är:

VIRUSSKYDD

Antivirusskydd är grunden i din säkerhet. Bitdefender skyddar dig i realtid och på begäran mot alla typer av hot, som skadlig kod, trojaner, spionprogramvara, adware, mm.

Från antivirusfunktionen kan du enkelt komma åt följande skanningsåtgärder:

- Snabbsökning
- Systemskanning
- Hantera skanningar
- Räddningsläge (räddningsmiljö i Windows 10)

Mer information om skanningsjobb och hur du konfigurerar antivirusskydd finns i *"Antivirusskydd"* (p. 65).

FÖREBYGGANDE AV ONLINEHOT

Med förebyggande av onlinehot kan du skydda dig mot nätfiskeattacker, bedrägeriförsök och läckage av privat information, när du surfar på nätet.

Mr information om hur du konfigurerar Bitdefender för att skydda din nätaktivitet finns i "*Förebygga onlinehot*" (p. 86).

BRANDVÄGG

Brandväggen skyddar dig när du är ansluten till nätverk och Internet genom att filtrera alla anslutningsförsök.

Mer information om brandväggskonfiguration finns i "*Brandvägg*" (p. 97).

ADVANCED THREAT DEFENSE

Avancerat hotförsvar skyddar aktivt ditt system mot hot som ransomware, spyware och trojaner genom att analysera beteende hos alla installerade appar. Misstänkta processer identifieras och blockeras, om det behövs.

;er information om hur du skyddar systemet mot hot finns i "*Avancerat hotskydd*" (p. 84).

ANTISPAM

Bitdefenders skräppostfunktioner säkerställer att din inkorg är fri från oväntade e-postmeddelanden genom att filtrera POP3-e-postrafik.

Mer information om skräppostskydd finns i "*Antispam*" (p. 88).

SÄKERHETSRISK

Funktionen Säkerhetsrisk hjälper dig att hålla det operativsystem och de appar du använder regelbundet uppdaterade och att identifiera de trådlösa nätverk du ansluter till.

Klicka på **Säkerhetsriskskanning** i funktionen Säkerhetsrisk för att börja identifiera viktiga Windows-uppdateringar, appuppdateringar, svaga lösenord som hör till Windows-konton och trådlösa nätverk som int är säkra.

Klicka på **Wi-Fi security** för att visa listan över de trådlösa nätverk du ansluter till, tillsammans med vår ryktesutvärdering för var och ett av dem och de åtgärder du kan vidta för att skydda dig mot eventuella spioner.

Mer information om hur du konfigurerar säkerhetsriskskydd finns i "*Säkerhetsrisk*" (p. 102).

SÄKRA FILER

Funktionen Säkra filer ser till att dina personliga filer är skyddade från ransomwareattacker.

Mer information om hur du konfigurerar Säkra filer för att skydda dina personliga filer från ransomware attacker finns i *"Safe Files"* (p. 113).

AVHJÄLPNING AV RANSOMWARE

Funktionen Avhjälpning av ransomware hjälper dig att återställa filer ifall de krypteras av ransomware.

Mer information om hur du återställer krypterade filer finns i *"Avhjälpning av ransomware"* (p. 116).

Sekretess

I sekretessavsnittet kan du öppna Bitdefender VPN-appen, kryptera dina privata data, skydda dina onlinetransaktioner, håll din webbkamera och surfupplevelse säker och skydda dina barn genom att visa och begränsa deras onlineaktivitet.

De funktioner du kan hantera i avsnittet Sekretess är:

VPN

VPN säkrar din onlineaktivitet och döljer din IP-adress varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, köpcenter, kaféer eller hotell. Dessutom kan du komma åt innehåll som i normala fall är begränsat i vissa områden.

Mer information om den här funktionen finns i *"VPN"* (p. 131).

FILKRYPTERING

Skapa krypterade, lösenordsskyddade logiska enheter (eller valv) på din dator där du säkert kan förvara privat och känslig information.

Mer information om hur du skapar krypterade, lösenordsskyddade logiska enheter (eller valv) på din dator finns i *"Filkryptering"* (p. 118).

VIDEO- OCH LJUDSKYDD

Video- och ljudskydd ser till att din webbkamera är utom fara genom att blockera åtkomst för obetrodda appar och meddelar dig när apparna försöker få tillgång till din mikrofon.

Mer information om hur du håller din webbkamera skyddad från oönskad åtkomst och hur du ställer in Bitdefender för att meddela dig om din mikrofonaktivitet finns i *"Video- och ljudskydd"* (p. 109).

PASSWORD MANAGER

Bitdefender lösenordshanterare hjälper dig att hålla reda på dina lösenord, skyddar din integritet och ger en säker surfupplevelse.

Mer information om hur du konfigurerar lösenordshanteraren finns i *"Lösenordshanteringsskydd för dina inloggningsuppgifter"* (p. 122).

SAFEPAY

Webbläsaren Bitdefender Safepay™ hjälper dig att se till att dina bankärenden online, e-shopping och andra typer av onlinetransaktioner är privata och säkra.

Mer information om Bitdefender Safepay™ finns i *"Safepay-säkerhet för onlinetranslationer"* (p. 133).

DATASKYDD

Med funktionen Dataskydd kan du ta bort filer permanent.
Klicka på **Filförstöraren** i panelen Dataskydd för att starta en guide där du kan helt eliminera filer från ditt system.

Mer information om hur du konfigurerar dataskydd finns i *"Dataskydd"* (p. 138).

Verktyg

I avsnittet Verktyg kan du förbättra systemet hastighet och hantera dina enheter.

Optimeringsverktyg

Bitdefender Total Security erbjuder inte bara säkerhet, den hjälper dig också att se till att datorns prestanda är på topp.

Tillgängliga optimeringsverktyg är:
- OneClick Optimizer
- Startup Optimizer
- Diskrensning

Mer information om prestandaoptimeringsverktygen finns i *"Verktyg"* (p. 143).

Anti-Theft

Bitdefender Antistöld skyddar din dator och dina data mot stöld eller förlust. Om det sker kan du fjärrlokalisera eller låsa din dator. Du kan också radera alla data som finns i ditt system.

Bitdefender Antistöld erbjuder följande funktioner:
- Hitta via fjärrstyrning
- Lås via fjärrstyrning
- Fjärradera

- Fjärrvarning

Mer information om hur du håller datorn borta från fel händer finns i *"Enhetsantistöld"* (p. 139).

2.2.5. Security widget

Säkerhetswidget är det snabba och säkra sättet att övervaka och styra Bitdefender Total Security. Om du lägger till den här lilla och ej störande widgeten på skrivbordet kan du se kritisk information och utföra viktiga åtgärder hela tiden.

- öppna huvudfönstret i Bitdefender.
- övervaka skanningsaktivitet i realtid.
- övervaka säkerhetsstatus för ditt system och fixa befintliga problem.
- visa när en uppdatering pågår.
- via meddelanden och få åtkomst till de senaste händelserna som rapporterats av Bitdefender.
- skanna filer eller mappar genom att dra och släppa ett eller flera objekt över widgeten.

Security widget

Den allmänna säkerhetsstatusen för din dator visas **i mitten** av widgeten. Statusen anges av färgen och formen för ikonen som visas i det här området.


Kritiska problem påverkar säkerheten i ditt system.

De kräver din omedelbara uppmärksamhet och måste lösas så snart som möjligt. Klicka på statusikonen för att börja åtgärda de rapporterade problemen.


Icke-kritiska problem påverkar säkerheten i ditt system. Du bör kontrollera dem och åtgärda dem när du har tid. Klicka på statusikonen för att börja åtgärda de rapporterade problemen.

 Ditt system är skyddat.

 När en på begäran-åtgärd utförs visas den här animerade ikonen.

När problem rapporteras klickar du på statusikonen för att starta guiden Åtgärda problem.

Den lägre sidan av widgeten visar räknaren för olästa händelser (antalet utestående händelser som rapporterats av Bitdefender, om det finns några). Klicka på händelseräknaren, till exempel 1 för en oläst händelse, för att öppna meddelandefönstret. Mer information finns på *"Aviseringar"* (p. 9).

Skanna filer och mappar

Du kan använda säkerhetswidgeten för att snabbt skanna filer och mappar. Dra en fil eller mapp som du vill ska skannas och släpp den över **säkerhetswidgeten**.

Guiden för antivirusskanning kommer att visas och leda dig genom skanningsprocessen. Skanningsalternativen är förkonfigurerade för bästa upptäcktsresultat och kan inte ändras. Om smittade filer hittas försöker Bitdefender desinfektera dem (ta bort den skadliga koden). Om desinfektering misslyckas, kommer guiden för Antivirus-skanning att låta dig välja andra åtgärder att ta till mot infekterade filer.

Dölj/visa säkerhetswidget

När du inte längre vill se widgeten klickar du på ⊗.

Använd en av följande metoder för att återställa säkerhetswidgeten:

- Från systemfältet:
  1. Högerklicka på Bitdefender-ikonen i systemfältsikonen.
  2. Klicka på **Visa säkerhetswidget** i kontextmenyn som visas.
- Från Bitdefenders gränssnitt:
  1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I fönstret **Allmänt** slår du på **Säkerhetswidget**.

Bitdefenders säkerhetswidget är inaktiverad som standard.

2.2.6. Ändra produktspråk

Bitdefender-gränssnittet är tillgängligt på flera språk och kan ändras genom att följa dessa steg:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** klickar du på **Ändra språk**.
3. Välj önskat språk i listan och klicka därefter på **SPARA**.
4. Vänta en stund tills de nya inställningarna tillämpas.

2.3. Bitdefender Central

Bitdefender Central är en plattform vart du har tillgång till produktens alla onlinefunktioner och tjänster och kan fjärransluta viktiga uppgifter på enheterna Bitdefender är installerat på. Du kan logga in på ditt Bitdefender-konto från vilken dator som helst som är ansluten till Internet genom att gå till https://central.bitdefender.com, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

Så här installerar du Bitdefender Central-appen på dina enheter:

- **På Android** - sök Bitdefender Central på Google Play och hämta och installera appen. Följ stegen för att slutföra installationen.
- **På Android** - sök Bitdefender Central på App Store och hämta och installera appen. Följ stegen för att slutföra installationen.

När du är inloggad kan du börja göra följande:

- Hämta och installera Bitdefender på Windows, macOS, iOS och Android. De produkter som är tillgängliga för hämtning är:
  - Bitdefender Total Security
  - Bitdefender Antivirus för Mac
  - Bitdefender Mobile Security för Android
  - Bitdefender Mobile Security för iOS
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter till nätverket och hantera dem var du än är.
- Skydda nätverksenheterna och deras data mot stöld eller förlust med Antistöld.

2.3.1. Öppna Bitdefender Central

Det finns flera sätt att öppna Bitdefender Central:

- Från Bitdefenders huvudgränssnitt:
  1. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. Klicka på **Gå till Bitdefender Central**.
  3. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.
- Från din webbläsare:
  1. Öppna en webbläsare på en enhet med Internet-åtkomst.
  2. Gå till: https://central.bitdefender.com.
  3. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.
- Från din Android- eller iOS-baserade enhet:

  Öppna Bitdefender Central-appen som du har installerat.

Notera
I det här materialet har du alternativ och instruktioner tillgängliga på webbplattformen.

2.3.2. Tvåfaktorautentisering

2-faktorautentiseringsmetoden ger ett extra säkerhetslager till ditt Bitdefender-konto, genom att kräva en autentiseringskod förutom dina inloggningsuppgifter. På det här sättet förhindrar du kontokapning och håller vissa typer av cyberattacker borta, som keyloggers, råstyrke- eller ordlisteattacker.

Aktivera tvåfaktorautentisering

Genom att aktivera tvåfaktorautentisering gör du ditt Bitdefender-konto mycket säkrare. Din identitet verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera status för din prenumeration eller köra uppgifter via fjärrstyrning på dina enheter.

Aktivera tvåfaktorautentisering:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.

3. Klicka på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Klicka på **Tvåfaktorautentisering**.
6. Klicka på **KOM IGÅNG**.

   Välj en av följande metoder:

   - **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in till ditt Bitdefender-konto.

     Om du vill använda en autentiseringsapp, men inte är säker på vad du ska välja, finns det en lista över de autentiseringsappar vi rekommenderar.

     a. Klicka på **ANVÄND AUTENTISERINGSAPP** för att börja.

     b. Logga in på en Android- eller iOS-baserad enhet genom att använda enheten för att skanna QR-koden.

        För att logga in på en bärbar eller stationär dator kan du manuellt lägga till den visade koden.

        Klicka på **FORTSÄTT**.

     c. Infoga koden som appen gav eller den som visas i föregående steg och klicka sedan på **AKTIVERA**.

   - **E-post** - varje gång du loggar in på ditt Bitdefender-konto skickas en verifieringskod till din e-postinkorg. Kontrollera ditt e-postkonto och skriv sedan in den kod du har fått.

     a. Klicka på **ANVÄND E-POST** för att starta.

     b. Kontrollera ditt e-postkonto och skriv in den angivna koden.

        Observera att du har fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.

     c. Klicka på **AKTIVERA**.

     d. Du får tio aktiveringskoder. Du kan antingen kopiera, ladda ned eller skriva ut listan ifall du tappar bort din e-postadress eller inte kan logga in. Varje kod kan bara användas en gång.

     e. Klicka på **KLAR**.

Ifall du vill sluta använda tvåfaktorautentisering:

1. Klicka på **STÄNG AV TVÅFAKTORAUTENTISERING**.
2. Kontrollera din app eller ditt e-postkonto och skriv in koden du har fått.

   Ifall du har valt att få autentiseringskoden via e-post har du fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.
3. Bekräfta ditt val.

Lägga till betrodda enheter

För att se till att bara du kan komma åt ditt Bitdefender-konto kan vi kräva en säkerhetskod först. Om du vill hoppa över det här steget varje gång du ansluter från samma enhet, rekommenderar vi att du utser den till en betrodd enhet.

Lägga till enheter som betrodda enheter:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.
3. Klicka på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Klicka på **Betrodda enheter**.
6. Listan över de enheter som Bitdefender är installerad på visas. Klicka på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och att din prenumeration är giltig.

2.3.3. Mina prenumerationer

Ett Bitdefender-konto som har en Bitdefender Small Office Security-prenumeration kan inte ha bifogat en annan Bitdefender-prenumeration förutom den för Bitdefender Premium VPN. Ägaren av kontot är den som kan hantera nätverket, förnya prenumerationen och uppgradera till premiumversionen av Bitdefender VPN.

Kontrollera tillgängliga prenumerationer

Kontrollera dina tillgängliga prenumerationer:

1. Öppna Bitdefender Central.

2. Välj panelen **Mina prenumerationer**.

Här har du information om de prenumerationer du äger och antal enheter som använder var och en av dem.

Du kan lägga till en ny enhet till en prenumeration eller förnya den genom att välja ett prenumerationskort.

Lägg till ny enhet

Om din prenumeration omfattar mer än en enhet kan du lägga till en ny enhet och installera din Bitdefender Total Security på den, enligt följande:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:
   - **Skydda den här enheten**

     Välj det här alternativet och spara installationsfilen.
   - **Skydda andra enheter**

     Välj det här alternativet och klicka därefter på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

     Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.
4. Vänta tills nedladdningen är slutfört och kör sedan installationsprogrammet.

Förnya prenumeration

Om du inte valde bort att automatiskt förnya din Bitdefender-prenumeration, kan du manuellt förnya den genom att följa de här stegen:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina prenumerationer**.
3. Välj önskat prenumerationskort.
4. Klicka på **FÖRNYA** för att fortsätta.

En webbsida öppnas i din webbläsare där du kan förnya din Bitdefender-prenumeration.

Aktivera prenumeration

En prenumeration kan aktiveras under installationsprocessen genom att använda ditt Bitdefender-konto. Tillsammans med aktiveringsprocessen börjar giltigheten räknas ned.

Om du har köpt en aktiveringskod från någon av våra återförsäljare eller om du fått den som present, kan du lägga till dess tillgänglighet till en befintlig Bitdefender-prenumeration som är tillgänglig på kontot, förutsatt att de är för samma produkt.

Aktivera en prenumeration med en aktiveringskod:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina prenumerationer**.
3. Klicka på knappen **AKTIVERINGSKOD** och skriv sedan in koden i motsvarande fält.
4. Klicka på **AKTIVERA** för att fortsätta.

Prenumerationen är nu aktiv. Gå till panelen **Mina enheter** och välj **INSTALLERA SKYDD** för att installera produkten på en av dina enheter.

2.3.4. Mina enheter

I området **Mina enheter** i Bitdefender Central har du möjlighet att installera, hantera och vidta fjärråtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till Internet. Enhetskorten visar enhetsnamn, skyddsstatus och om det finns säkerhetsrisker som påverkar enheternas skydd.

Visa en lista över dina enheter sorterad efter deras status eller användare genom att klicka på rullgardinspilen i det övre högra hörnet på skärmen.

För att enkelt identifiera dina enheter kan du anpassa enhetsnamnet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.

4. Välj **Inställningar**.
5. Skriv in ett nytt namn i fältet **Enhetsnamn**, klicka därefter på **SPARA**.

Du kan skapa och tilldela en ägare för varje enhet för bättre hantering:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Profil**.
5. Klicka på **Lägg till ägare** och fyll i motsvarande fält. Anpassa profilen genom att lägga till ett foto och välj ett födelsedatum.
6. Klicka på **LÄGG TILL** för att spara profilen.
7. Välj önskad ägare från listan **Enhetsägare** och klicka på **TILLDELA**.

Fjärruppdatera Bitdefender på en Windows-enhet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

Klicka på önskat enhetskort för fler fjärråtgärder och information angående din Bitdefender-produkt på en specifik enhet.

När du klickar på ett enhetskort är följande flikar tillgängliga:

- **Kontrollpanel**. I det här fönstret kan du visa information om den valda enheten, kontrollera dess skyddsstatus, status för Bitdefender VPN och hur många hot som har blockerats de senaste sju dagarna. Skyddsstatus kan vara grönt när det inte finns några problem som påverkar enheten, gult när enheten behöver åtgärdas från din sida eller rött när enheten är utsatt för risk. När det finns problem som påverkar enheten klickar du på rullgardinsmenyn i det övre statusområdet för att se mer information. Härifrån kan du manuellt åtgärda problem som påverkar dina enheters säkerhet.

- **Skydd**. Från det här fönstret kan du fjärrstyra en snabb- eller systemskanning på dina enheter. Klicka på knappen **SKANNA** för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och det finns en rapport från den senaste skanningen med den viktigaste informationen.Mer information om de här två skanningsprocesserna finns i *"Kör en systemskanning"* (p. 71) och *"Köra en snabbskanning"* (p. 71).
- **Optimerare**. Här kan du via fjärrstyrning förbättra en enhets prestanda genom att snabbt skanna, upptäcka och rensa onödiga filer. Klicka på **STARTA** och välj sedan de områden du vill optimera. Klicka på **STARTA** igen för att påbörja optimeringsprocessen. Klicka på **Mer information** för att komma åt en detaljerad rapport om de problem som åtgärdats.

  Dessutom kan du förbättra enhetens uppstart genom att identifiera de appar som har hög systemresursförbrukning. Klicka på **MER INFORMATION** och välj sedan vad du vill göra med de hittade apparna. Mer information om de här funktionerna finns i *"Optimerar din systemhastighet med ett enda klick"* (p. 143) och *"Optimera din PC:s starttid"* (p. 144).
- **Anti-Theft**. Ifall du förlägger din enhet, den blir stulen eller försvinner kan du hitta den och utföra fjärrstyrda åtgärder med Antistöld-funktionen. Klicka på **HITTA** för att ta reda på enhetens position. Senaste kända position visas, tillsammans med datum och tid. Mer information om den här funktionen finns i *"Enhetsantistöld"* (p. 139).
- **Säkerhetsrisk**. Klicka på knappen **SKANNA** på fliken Säkerhetsrisk för att kontrollera en enhet för eventuella säkerhetsrisker som saknade Windows-uppdateringar, utdaterade appar eller svaga lösenord. Säkerhetsrisker kan inte åtgärdas via fjärrstyrning. Om en säkerhetsrisk hittas måste du köra en ny skanning på enheten och sedan vidta rekommenderade åtgärder. Klicka på **Mer information** för att komma åt en detaljerad rapport om de problem som hittas. Mer information om den här funktionen finns i *"Säkerhetsrisk"* (p. 102).

2.3.5. Lösenordskyddade Bitdefender-inställningar

Om du är administratör för Bitdefender Small Office Security-prenumertionen, kan du ange ett lösenord för att förhindra medlemmar i ditt team från att göra ändringar i produkten.

Konfigurera lösenordsskydd för Bitdefender Total Security-inställningarna:

- Öppna Bitdefender Central.

- Klicka på ikonen uppe till höger på skärmen.
- Klicka på **Administratörskonto** i listmenyn.
- Aktivera motsvarande omkopplare.
- Skriv in lösenordet i motsvarande fält och klicka därefter på **ANGE ADMINISTRATÖRSLÖSENORD**.

När du har ställt in ett lösenord måste den som försöker ändra Bitdefender-inställningarna först ange lösenordet.

2.3.6. Aktivitet

När du öppnar fönstret **AKTIVITET** är följande kort tillgängliga:

- **Mina enheter**. Här kan du visa antal anslutna enheter tillsammans med deras skyddsstatus. Åtgärda problem via fjärrstyrning på de upptäckta enheterna, klicka på **Åtgärda problem** och klicka sedan på **SKANNA OCH ÅTGÄRDA ENHETER**.

  Information om upptäckta hot kan inte hämtas från iOS-baserade enheter.

- **Blockerade hot**. Här kan du visa en graf som visar allmän statistik, däribland information om de hot som blockerats under de senaste 24 timmarna och sju dagarna. Den visade informationen hämtas beroende på det skadliga beteende som upptäckts på öppnade filer, appar och URL:er.
- **Toppanvändare med blockerade hot**. Här kan du visa en topp med de enheter där flest hot hittats.

2.3.7. Aviseringar

För att du ska vara informerad om vad som händer på de enheter som är kopplade till ditt konto finns -ikonen till hands. När du klickar på den har du en översiktsbild som består av information om aktiviteten för de Bitdefender-produkter som är installerade på dina enheter.

2.4. Se till att Bitdefender är uppdaterad

Nya hot hittas och identifieras varje dag. Det här är orsaken till varför det är mycket viktig att se till att Bitdefender är uppdaterad med den senaste hotinformationsdatabasen.

Om du är ansluten till Internet via bredband eller DSL, tar Bitdefender hand om detta själv. Som standard söker det efter updateringar när du slår på din dator samt varje **timme** efter det. Om en uppdatering upptäcks kommer den automatiskt att hämtas och installeras på din dator.

Uppdateringsprocessen utförs i farten, vilket betyder att filerna som ska uppdateras ersätts efter hand. På så sätt kommer inte uppdateringsprocessen att påverka produktaktiviteten och samtidigt kommer alla säkerhetsrisker att exkluderas.

Viktigt
För att vara skyddad mot de senaste hoten ska du se till att Automatisk uppdatering är aktiverat.

I vissa särskilda situationer krävs ingripande från dig för att hålla ditt Bitdefender-skydd uppdaterat:

- Om din dator ansluts till Internet via en proxyserver måste du konfigurera proxyinställningarna såsom beskrivs i *"Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?"* (p. 59).
- Om du är ansluten till Internet via en uppringningsanslutning rekommenderas du att regelbundet uppdatera Bitdefender på användarbegäran. Mer information finns på *"Utför en uppdatering"* (p. 34).

2.4.1. Kontrollerar om Bitdefender är uppdaterad

Kontrollera tidpunkten för den senaste uppdateringen av din Bitdefender:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste uppdateringen.

Du kan ta reda på när uppdateringar startades och information om dem (om de lyckades eller inte, om det krävs en omstart för att slutföra installationen). Om så krävs startar du om systemet så snabbt som möjligt.

2.4.2. Utför en uppdatering

För att göra uppdateringar krävs en Internet-anslutning.

Starta en uppdatering genom att högerklicka på Bitdefender B-ikonen i systemfältet och sedan välja **Uppdatera nu**.

Uppdateringsfunktionen ansluter till Bitdefender-uppdateringsserver och kontrollerar om det finns uppdateringar. Om en uppdatering upptäcks kommer du antingen att ombes att bekräfta uppdateringen, eller så utförs uppdateringen automatiskt, beroende påuppdateringsinställningarna.

Viktigt
Det kan vara nödvändigt att starta om datorn när du har slutfört uppdateringen. Vi rekommenderar att göra det så snart som möjligt.

Du kan också fjärrstyra uppdateringar på dina enheter, förutsatt att de är påslagna och anslutna till Internet.

Fjärruppdatera Bitdefender på en Windows-enhet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

2.4.3. Slå på eller av automatisk uppdatering

Slå på eller av automatisk uppdatering:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Uppdatera**.
3. Slå av eller på motsvarande omkopplare.
4. Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att automatiskt uppdatering ska vara inaktiv. Du kan inaktivera den automatiska uppdateringen i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart.

Varning
Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar automatisk uppdatering under så kort tid som möjligt. Om Bitdefender inte uppdateras regelbundet kan det inte skydda dig mot de senaste hoten.

2.4.4. Automatiska uppdateringsinställningar

Uppdateringarna kan utföras från det lokala nätverket, över Internet, direkt eller via en proxyserver. Som standard kommer Bitdefender att söka efter uppdateringar över Internet varje timme, och installera tillgängliga uppdateringar utan att meddela dig.

Standardinställningarna för uppdatering är anpassade efter de flesta användare och i normala fall behöver du inte ändra dem.

Justera uppdateringsinställningarna:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Uppdatera** och justera inställningarna enligt dina önskemål.

Uppdateringsfrekvens

Bitdefender är konfigurerad att kontrollera efter uppdateringar varje timme. Ändra uppdateringsfrekvensen genom att dra reglaget längs skalan för att ange önskad tidsperiod när uppdateringen ska ske.

Uppdatera bearbetninsgregler

Varje gång en uppdatering är tillgänglig hämtar Bitdefender uppdateringen automatiskt och implementerar den utan att visa meddelanden. Stäng av alternativet **Tyst uppdatering** om du vill bli meddelad varje gång en ny uppdatering är tillgänglig.

Vissa uppdateringar kräver en omstart för att slutföra installationen.

Som standard fortsätter Bitdefender arbeta med de gamla filerna tills användaren frivilligt startar om datorn, om en uppdatering kräver en omstart. Det är för att förhindra Bitdefender-uppdateringsprocessen från att störa användarens arbete.

Om du vill ha ett meddelande när en uppdatering kräver en omstart slår du på **Omstartsmeddelande**.

2.4.5. Kontinuerliga uppdateringar

För att se till att du använder den senaste versionen kontrollerar Bitdefender automatiskt för produktuppdateringar. Dessa uppdateringar kan medföra nya funktioner och förbättringar, lösa produktproblem eller automatiskt uppgradera dig till en ny version. När den nya Bitdefender-versionen kommer

via en uppdatering sparas anpassade inställningar och avinstallations- och ominstallationsproceduren hoppas över.

Dessa uppdateringar kräver en systemomstart för att installationen av nya filer ska starta. När en produktuppdatering är slutförd talar ett popup-fönster om att du ska starta om systemet. Om du missar det här meddelandet kan du antingen klicka på **STARTA OM NU** i fönstret Meddelanden där den senaste uppdateringen nämns eller starta om systemet manuellt.

Notera
Uppdateringarna omfattar nya funktioner och förbättringar som endast levereras till användare som har Bitdefender 2018 installerat.

2.5. Smart voice assistance

If you use the Amazon Alexa smart-speaker or the Google Assistant app, you can initiate voice commands to run a set of tasks or check information on the devices that have Bitdefender installed. Thus, you can perform scanning and optimization tasks, pause the internet on the connected devices, check the status of your current subscription, or check your children's locations or online activities. To view the complete list of the voice commands that you can initiate, refer to *"Voice commands to interact with Bitdefender"* (p. 38).

2.5.1. Setting voice commands

The Bitdefender voice commands can be configured for:

- **Google Home app on**
  - Android 5.0 and up
  - iOS 10.0 and up
  - Chromebooks
- **Amazon Alexa app on**
  - Echo
  - Echo Dot
  - Echo Show
  - Echo Spot
  - Fire TV Cube

Setting up Amazon Alexa voice commands for Bitdefender

To set up the Bitdefender voice commands on Amazon Alexa:

1. Open the Amazon Alexa app.
2. Tap the **Menu** icon, and then go to **Skills**.
3. Search for Bitdefender.
4. Tap **Bitdefender** and then tap **ENABLE**.
5. You are prompted to sign in to your Bitdefender account.

   Type your username and your password, and then tap **SIGN IN**.

As soon as the synchronization of Bitdefender with your Amazon Alexa is done, you are introduced into the voice commands you can use to initiate tasks or check information about the devices that have Bitdefender installed.

Whenever you need the assistant to give you the list of all available voice commands or skills, say **HELP ME**.

Setting up Google Home voice commands for Bitdefender

To set up the voice commands on Google Home:

1. Open the Google Home app.
2. Tap Menu in the top left corner of the Home screen, and then tap **Explore**.
3. Search for Bitdefender.
4. Tap **Bitdefender**, and then tap **Link**.
5. You are prompted to sign in to your Bitdefender account.

   Type your username and your password, and then tap **SIGN IN**.

As soon as the synchronization of Bitdefender with Google Home is done, you are introduced into the voice commands you can use to initiate tasks or check information about the devices that have Bitdefender installed.

Whenever you need the assistant to give you the list of all available voice commands or skills, say **HELP ME**.

2.5.2. Voice commands to interact with Bitdefender

To open the Bitdefender voice commands:

- On Amazon Alexa: **Alexa, open Bitdefender**

- On Google Home: **OK, Google, talk with Bitdefender**

To launch the Bitdefender voice commands:

- On Amazon Alexa: **Alexa, ask Bitdefender**
- On Google Home: **OK, Google, ask Bitdefender**

The questions and tasks you can initiate once the Bitdefender assistant is open, are:

How is my activity today?

What is my subscription status?

Optimize my devices. (This command will launch OneClick Optimizer on the connected Windows-based devices).

Run a quick scan on my [device type]. (As device type you can say laptop, computer, phone or tablet).

3. HUR

3.1. Installation

3.1.1. Hur installerar jag Bitdefender på en andra dator?

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

Installera Bitdefender på en andra dator:

1. Klicka på **Installera på annan enhet** i det nedre vänstra hörnet av Bitdefender-gränssnittet.

   Du omdirigeras till Bitdefender-kontosidan. Se till att du är inloggad med dina inloggningsuppgifter.

2. Klicka på **SKICKA HÄMTNINGSLÄNK** i det fönster som visas.

3. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

   Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och tryck på motsvarande hämtningsknapp.

4. Kör den Bitdefender-produkt du har hämtat.

Den nya enhet på vilken du har installerat Bitdefender-produkten visas i Bitdefender Central-kontrollpanelen.

3.1.2. Hur installerar jag om Bitdefender?

Typiska situationer när du skulle behöva installera om Bitdefender kan vara följande:

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

Om något av de nämnda situationerna är ditt fall följer du de här stegen:

- I **Windows 7**:

1. Klicka på **Start** och gå till **Alla program**.
2. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
3. Klicka på **INSTALLERA OM** i det fönster som visas.
4. Du måste starta om datorn för att slutföra processen.

- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
  4. Klicka på **INSTALLERA OM** i det fönster som visas.
  5. Du måste starta om datorn för att slutföra processen.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Appar och funktioner**.
  3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
  5. Klicka på **INSTALLERA OM**.
  6. Du måste starta om datorn för att slutföra processen.

> **Notera**
> Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

3.1.3. Hur ändrar jag språk på min Bitdefender-produkt?

Bitdefender-gränssnittet är tillgängligt på flera språk och kan ändras genom att följa dessa steg:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I fönstret **Allmänt** klickar du på **Ändra språk**.

3. Välj önskat språk i listan och klicka därefter på **SPARA**.
4. Vänta en stund tills de nya inställningarna tillämpas.

3.1.4. Hur uppgraderar jag till den senaste Bitdefender-versionen?

Från och med nu går det att uppgradera till den nyaste versionen utan att följa proceduren med manuell avinstallation och ominstallation. Mer exakt så levereras den nya produkten inklusive nya funktioner och stora produktförbättringar via produktuppdatering och om du redan har en aktiv Bitdefender-prenumeration aktiveras produkten automatiskt.

Om du använde 2018-versionen kan du uppgradera till den senaste versionen genom att följa de här stegen:

1. Klicka på **STARTA OM NU** i det meddelande du får med uppgraderingsinformationen. Om du missade det öppnar du fönstret Meddelanden, pekar på den senaste uppdateringen och klickar därefter på knappen **STARTA OM NU**. Vänta tills datorn startar om.

   Fönstret **Nyheter** med information om de förbättrade och nya funktionerna visas.
2. Klicka på länkarna **Läs mer** för att dirigeras om till vår särskilda sida med mer information och användbara artiklar.
3. Stäng fönstret **Nyheter** för att gå till gränssnittet för den installerade versionen.

Användare som vill uppgradera kostnadsfritt från Bitdefender 2016 eller en tidigare version till den senaste versionen av Bitdefender måste ta bort den aktuella versionen från Kontrollpanelen och därefter hämta den senaste installationsfilen från Bitdefenders webbplats på följande adress: https://www.bitdefender.com/Downloads/. Aktiveringen är endast möjlig med en giltig prenumeration.

3.2. Bitdefender Central

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

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

Logga in med ett annat Bitdefender-konto:

1. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **Växla konto** i det övre högra hörnet av skärmen för att ändra kontot som är länkat till datorn.
3. Skriv e-postadressen i motsvarande fält och klicka sedan på **NÄSTA**.
4. Skriv lösenordet och klicka sedan på **LOGGA IN**.

Notera
Bitdefender-produkten från din enhet ändras automatiskt enligt prenumerationen som är kopplad till det nya Bitdefender-konto.
Om det inte finns någon tillgänglig prenumeration kopplad till det nya Bitdefender-kontot eller om du vill överföra den från det tidigare kontot, kontaktar du Bitdefender för support sosom beskrivs i avsnitt *"Be om hjälp"* (p. 290).

3.2.2. Hur stänger jag av Bitdefender Central-hjälpmeddelanden?

För att hjälpa dig förstå vad varje alternativ i Bitdefender Central används för visas hjälpmeddelanden på kontrollpanelen.

Om du inte längre vill se den här typen av meddelanden:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.
3. Klicka på **Mitt konto** i reglagemenyn.
4. Klicka på **Inställningar** i reglagemenyn.
5. Inaktivera alternativet **Slå på/av hjälpmeddelanden**.

3.2.3. Jag har glömt det lösenord jag ställde in för mitt Bitdefender-konto. Hur återställer jag det?

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

- Från Bitdefender-gränssnittet:
  1. Klicka på **Mitt konto** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. Klicka på **Byt konto** i det övre högra hörnet av skärmen.

     Ett nytt fönster visas.

3. Klicka på **Glömt lösenord?**.
4. Kontrollera e-postkontot, skriv in säkerhetskoden du fått och klicka på **NÄSTA**.

   Alternativt kan du klicka på **Byt lösenord** i det e-postmeddelande vi skickat till dig.
5. Skriv in det lösenord du vill ställa in och skriv det sedan en gång till. Klicka på **SPARA**.

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

För att öppna ditt Bitdefender-konto från och med nu skriver du din e-postadress och det nya lösenordet du precis har ställt in.

3.2.4. Hur hanterar jag inloggningssessionerna kopplade till mitt Bitdefender-konto?

I ditt Bitdefender-konto har du möjlighet att visa de senaste inaktiva och aktiva inloggningssessionerna som körs på enheter som är kopplade till ditt konto. Dessutom kan du logga ut via fjärrstyrning genom att följa de här stegen:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.
3. Klicka på **Mitt konto** i reglagemenyn.
4. Klicka på **Sessionshantering** i reglagemenyn.
5. I området **Aktiva sessioner** väljer du alternativet **LOGGA UT** bredvid den enhet du vill ska slutföra inloggningssessionen.

3.3. Skanna med Bitdefender

3.3.1. Hur skannar jag en fil eller en mapp?

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

Följ Antivirus-guiden för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer.

Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

Typiska situationer när du skulle använda denna skanningsmetod innefattar följande:

- Du misstänker att en specifik fil eller mapp är infekterad.
- När du hämtar filer från Internet som du tror kan vara skadliga.
- Skanna nätverksresurser innan du kopierar filer till din dator.

3.3.2. Hur skannar jag mitt system?

Utföra en fullständig skanning av systemet:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
3. Följ guiden för Systemskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer.

   Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem. Mer information finns på *"Guiden för Antivirusskanning"* (p. 75).

3.3.3. Hur schemalägger jag en skanning?

Du kan ställa in Bitdefender-produkten att börja skanna viktiga systemplatser när du inte sitter vid datorn.

Schemalägga en skanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.

3. Klicka på bredvid den skanningstyp du vill schemalägga, Systemskanning eller Snabbskanning.

   Alternativt kan du skapa en skanningstyp som passar dina behov genom att klicka på **Skapa ett nytt skanningsjobb**.

4. Aktivera alternativet **Schemalägg skanningsjobb**.

   Välj ett av motsvarande alternativ för att ställa in ett schema:

   - Vid systemstart
   - Dagligen
   - Veckovis
   - Månadsvis

   Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.

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

3.3.4. Hur skapar jag ett anpassat skanningsjobb?

Om du vill skanna specifika platser på din dator eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb.

Gör enligt följande för att skapa ett anpassat skanningsjobb:

1. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
2. Klicka på **Skapa ett nytt skanningsjobb**.
3. I fältet **Jobbnamn** skriver du ett namn för skanningen, därefter klickar du på de platser du vill ska skannas och sedan på **NÄSTA**.
4. Konfigurera dessa allmänna alternativ:

   - **Skanna endast program**. Du kan konfigurera Bitdefender till att skanna endast öppnade appar.
   - **Prioritet för skanningsjobb**. Du kan välja vilken inverkan en skanningsprocess ska ha på din systemprestanda.
     - Auto - Prioritet för skanningsprocessen beror på systemaktiviteten. För att se till att skanningsprocessen inte påverkar systemaktiviteten

bestämmer Bitdefender om skanningsprocessen ska köras med hög eller låg prioritet.

- Hög - Skanningsprocessens prioritet är hög. Genom att välja det här alternativet kommer du att tillåta andra program att köras långsammare och minska tiden som behövs för att skanningsprocessen ska slutföras.
- Låg - Skanningsprocessens prioritet är låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka tiden som behövs för att skanningsprocessen ska slutföras.

- **Efterskanningsåtgärder**. Välj vilken åtgärd Bitdefender ska utföra om inga hot upptäcks:
  - Visa sammanfattningsfönster
  - Stäng ned dator
  - Stäng skanningsfönster

5. Om du vill konfigurera skanningsalternativen i detalj klickar du på **Visa avancerade alternativ**.

   Klicka **NÄSTA**.

6. Aktivera **Schemalägg skanningsjobb** och välj sedan när den anpassade skanning du skapade ska starta.
   - Vid systemstart
   - Dagligen
   - Månadsvis
   - Veckovis

   Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.

7. Klicka på **SPARA** för att spara inställningarna och stänga konfigurationsfönstret.

   Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot hittas under skanningsprocessen ombes du att välja åtgärder som ska vidtas för de hittade filerna.

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

3.3.5. Hur undantar jag en mapp från att skannas?

Bitdefender tillåter undantag av specifika filer, mappar eller filändelsen från skanning.

Undantag ska användas av användare som har 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 programvara och appar i testsyften. Skanning av mappen kan innebära att du förlorar vissa data.

Lägg till en mapp i undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Klicka på fliken **Undantag**.
4. Klicka på menyn **Lista över filer och mappar undantagna från skanning** och sedan på **Lägg till**.
5. Klicka på **BLÄDDRA**, välj den mapp du vill ska undantas från skanning och välj sedan den typ av skanning den ska undantas ifrån.
6. Klicka på **Lägg till** för att spara ändringarna och stänga fönstret.

3.3.6. Vad ska man göra när Bitdefender visar att en ren fil är infekterad?

Det finns tillfällen då Bitdefender av misstag flaggar en legitim fil som ett hot (en falsk positiv). För att rätta till det här felet lägger du till filen till området för Bitdefender-undantag:

1. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.

      Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktivt. Du kan

inaktivera realtidsskyddet i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart.

2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?"* (p. 61) hur du gör det.
3. Återskapa filen från karantänområdet:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Karantän**.
   c. Välj filen och klicka sedan på **ÅTERSTÄLL**.
4. Lägg till filen till undantagslistan. Se i *"Hur undantar jag en mapp från att skannas?"* (p. 48) hur du gör det.
5. Slå på Bitdefender realtids-antivirusskydd.
6. Kontakta våra supportmedarbetare så att vi kan ta bort upptäckten av hotinformationsuppdateringen. Se i *"Be om hjälp"* (p. 290) hur du gör det.

3.3.7. 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 de loggade skanningsprocesserna, som skanningsalternativ, skanningsmål, vilka hot som hittats samt vilka åtgärder som vidtagits på dessa hot.

Du kan öppna skanningsloggen direkt från guiden för skanning när skanningen slutförts, genom att klicka **VISA LOGG**.

Kontrollera en skanningslogg eller en upptäckt infektion vid ett senare tillfälle:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste skanningen.

   Här hittar du alla hotskanningshändelser, inklusive hot upptäckta av pågående skanning, användarinitierade skanningar och statusändringar för automatiska skanningar.
3. I meddelandelistan kan du kontrollera vilka skanningar som har utförts på senaste tiden. Klicka på ett meddelande för att visa information om det.
4. Öppna en skanningslogg genom att klicka på **Visa logg**.

3.4. Integritetsskydd

3.4.1. Hur vet jag att min onlinetransaktion är säker?

För att vara säker på att det du gör online förblir privat kan du använda webbläsaren som finns i Bitdefender för att skydda dina transaktioner och bankappar.

Bitdefender Safepay™ är en säker webbläsare designad för att skydda din kreditkortsinformation, kontonummer eller annan känslig information du kan ange på olika platser online.

För att se till att din onlineaktivitet är säker och privat:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **Safepay**-panelen klickar du på **Öppna Safepay**.
3. Klicka på knappen  för att öppna det **virtuella tangentbordet**.

   Använd det **virtuella tangentbordet** när du skriver känslig information som lösenord.

3.4.2. Vad kan jag göra om min enhet blir stulen?

Stöld av mobilenhet, oavsett om det är en smartphone, en surfplatta eller en bärbar dator, är ett av huvudproblemen idag som påverkar enskilda personer och organisationer över hela världen.

Med Bitdefender Anti-Theft kan du inte bara lokalisera och låsa den stulna enheten, utan även radera alla data för att säkerställa att de inte används av tjuven.

Så här kommer du åt Anti-Theft-funktionerna från ditt -konto:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och välj sedan **Antistöld**.
4. Välj den funktion du vill använda:
   - **LOKALISERA** - visa din enhets plats på Google Maps.
   -  **Varning** - skicka en varning på enheten.

- **Lås** - lås din dator och ställ in en numerisk PIN-kod för att låsa upp den. Alternativt, aktivera motsvarande alternativ för att tillåta att Bitdefender tar bilder av den person som försöker öppna din enhet.
- **Radera** - ta bort alla data från din dator.

  Viktigt
  När du har raderat en enhet slutar alla Anti-Theft-funktionerna att fungera.

- **Visa IP** - visar den senaste IP-adressen för den valda enheten.

3.4.3. Hur använder jag filvalv?

Bitdefender Filvalvet möjliggör för dig att skapa krypterade och lösenordsskyddade enheter (eller valv) på din dator där du kan förvara privat och känslig information. Fysiskt är valvet en fil som finns lagrad med filändelsen .bvd på den lokala hårddisken.

När du skapar ett filvalv finns det två saker som är viktiga: storleken och lösenordet. Standardstorleken på 100 MB ska räcka för dina privata dokument, Excel-filer och andra liknande data. Dock kan det behövas mer utrymme för filmer och andra stora filer.

För att säkert lagra dina hemliga eller känsliga filer och mappar i Bitdefenders filvalv:

- **Skapa ett filvalv och ställ in ett starkt lösenord för det.**

  För att skapa ett valv högerklickar du på ett tomt område på skrivbordet eller i en mapp på din dator, pekar på **Bitdefender** > **Bitdefender Filvalv** och välj **Skapa filvalv**.

  Ett nytt fönster visas. Fortsätt enligt följande:

  1. Klicka **Bläddra**, välj plats för valvet och spara valvfilen under valt namn.
  2. Välj en enhetsbokstav från menyn. När du öppnar valvet kommer en virtuell hårddisk märkt med den valda bokstaven att visas under **Min dator**.
  3. Skriv in valvets lösenord i fälten **Lösenord** och **Bekräfta**.
  4. Om du vill ändra standardstorleken (100 MB) för valvet använder du upp- och nedpilarna från stegningsrutan **Valvstorlek**.

5. Klicka på **Skapa**.

> **Notera**
> När du öppnar valvet visas en virtuell disk i **Min dator**. Enheten är märkt med enhetsbokstaven som är tilldelad valvet.

- **Lägg till de filer eller mappar, du vill hålla säkra, till valvet.**

  För att kunna lägga till en fil till ett valv måste du först öppna valvet.

  1. Bläddra till valvfilen .bvd.
  2. Högerklicka valvfilen, peka på Bitdefender Filvalv och välj **Öppna**.
  3. I det fönster som visas anger du lösenordet, väljer en enhetsbokstav att tilldela till valvet och klickar på **OK**.

  Du kan nu utföra aktiviteter på den enhet som motsvarar det önskade filvalvet, genom att använda Windows Explorer, precis som du skulle ha gjort med en vanlig enhet. För att lägga till en fil till ett öppet valv kan du även högerklicka filen, peka på Bitdefenders filvalv och välja **Lägg till i filvalv**.

- **Håll alltid valvet låst.**

  Öppna endast valv när du behöver tillgång till eller ska hantera dess innehåll. För att låsa ett valv, högerklicka på motsvarande virtuella hårddisk i **Min dator**, peka på **Bitdefender Filvalv** och välj **Lås**.

- **Försäkra dig om att du raderar .bvd valvfilen.**

  Att radera filen raderar även valvets innehåll.

Mer information om hur man arbetar med filvalv finns i *"Filkryptering"* (p. 118).

3.4.4. Hur tar jag bort en fil permanent med Bitdefender?

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

Bitdefender File Shredder hjälper dig att snabbt strimla filer eller mappar från datorn med kontextmenyn i Windows genom att följa de här stegen:

1. Högerklicka på filen eller mappen som du vill ta bot permanent, peka på Bitdefender och välj **File Shredder**.
2. Klicka på **TA BORT PERMANENT** och bekräfta sedan att du vill fortsätta med processen.

Vänta medan Bitdefender slutför filborttagning.

3. Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.

3.4.5. Hur skyddar jag min webbkamera från att hackas?

Du kan ställa in din Bitdefender-produkt att tillåta eller neka åtkomst för installerade appar till webbkameran genom att följa de här stegen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Webbkameraåtkomst**.

   Listan med appar som har begärt åtkomst till din kamera visas.
3. Peka på den app du vill tillåta eller spärra åtkomst för och klicka på motsvarande omkopplare.

   För att visa vad andra Bitdefender-användare har valt att göra med den valda appen klickar du på -ikonen. Du meddelas varje gång en av de listade apparna blockeras av Bitdefender-användare.

Om du vill lägga till nya appar manuellt i listan klickar du på länken **Lägg till nytt program i listan**.

3.4.6. Hur kan jag manuellt återställa krypterade filer när återställningsprocessen misslyckas?

ifall krypterade filer inte kan återställas automatiskt kan du manuellt återställa dem genom att följa de här stegen:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** markerar du information avseende det senast upptäckta ransomwarebeteendet som upptäckts och klickar sedan på **Krypterade filer**.
3. Listan med krypterade filer visas.

   Klicka på **ÅTERSTÄLL FILER** för att fortsätta.
4. Ifall hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de avkrypterade filerna ska sparas. Klicka på **ÅTERSTÄLL PLATS** och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.

   Klicka på **SLUTFÖR** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas ifall 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;

3.5. Optimeringsverktyg

3.5.1. Hur förbättrar jag min systemprestanda?

Systemets prestanda beror inte bara på hårdvarukonfigurationen, som CPU-belastning, minnesanvändning och hårddiskutrymme. Den är också direkt kopplad till din programkonfiguration och din datahantering.

Detta är huvudåtgärderna du kan ta med Bitdefender för att förbättra ditt systems hastighet och prestanda:

- *"Optimera din systemprestanda med ett enda klick"* (p. 54)
- *"Skanna ditt system regelbundet"* (p. 54)

Optimera din systemprestanda med ett enda klick

OneClick Optimizer-alternativet sparar värdefull tid när du snabbt vill förbättra din systemprestanda genom att skanna, upptäcka och rensa bort oanvändbara filer.

Starta OneClick Optimizer-processen:

1. Klicka på **Verktyg** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **OPTIMERA MIN ENHET**.
3. Låt Bitdefender söka efter filer som går att ta bort, klicka sedan på knappen **OPTIMERA** för att slutföra processen.

Mer information om hur du kan förbättra hastigheten i din dator med ett enda klicka finns i *"Optimerar din systemhastighet med ett enda klick"* (p. 143),

Skanna ditt system regelbundet

Systemets hastighet och allmänna beteende kan också påverkas av hot.

Se till att du skannar systemet regelbundet, minst en gång i veckan.

Du rekommenderas att använda systemskanningen eftersom den skannar efter alla typer av hot som äventyrar säkerheten i ditt system och den skannar även inuti arkiv.

Starta systemskanningen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
3. Följ guidestegen.

3.5.2. Hur kan jag förbättra mitt systems uppstartstid?

Onödiga appar som gör uppstartstiden långsammare när du öppnar din PC kan inaktiveras eller fördröjas från att öppnas med Startup Optimizer och därmed spara värdefull tid.

Använda Startup Optimizer:

1. Klicka på **Verktyg** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **OPTIMERA ENHETSSTART**.
3. Välj de appar du vill fördröja vid systemstart.

Mer information om hur du optimerar din PC:s starttid finns i *"Optimera din PC:s starttid"* (p. 144).

3.6. Användbar information

3.6.1. Hur testar jag min säkerhetslösning?

För att vara säker på att din Bitdefender-produkt körs som den ska rekommenderar vi att du använder Eicar-testet.

Med Eicar-testet kan du kontrollera din säkerhetslösning med en säker fil utvecklad för detta ändamål.

Testa din säkerhetslösning:

1. Hämta testet från den officiella hemsidan för EICAR-organisationen http://www.eicar.org/.
2. Klicka på fliken **Antimalware-testfil**.
3. Klicka på **Hämta** i menyn på vänster sida.

4. Från **Hämtningsområde som använder standardprotokollet http** klickar du på testfilen **eicar.com**.
5. Du informeras om att den sida du försöker öppna innehåller EICAR-Test-File (inte ett hot).

   Om du klickar på **Jag förstår riskerna, ta mig dit iallafall**, startar hämtningen testet och en Bitdefender-popup informerar dig om att ett hot upptäcktes.

   Klicka på **Mer information** för att hitta mer information om den här åtgärden.

Om du inte får någon Bitdefender-avisering rekommenderar vi att du kontaktar Bitdefender för support såsom beskrivs i avsnitt *"Be om hjälp"* (p. 290).

3.6.2. Hur tar jag bort Bitdefender?

Om du vill ta bort Bitdefender Total Security:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
  3. Klicka på **TA BORT** i det fönster som visas.
  4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
  4. Klicka på **TA BORT** i det fönster som visas.
  5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Appar**.

3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **TA BORT** i det fönster som visas.
6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

Notera
Den här ominstallationsproceduren tar bort de anpassade inställningarna permanent.

3.6.3. Hur tar jag bort Bitdefender VPN?

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

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Hitta **Bitdefender VPN** och välj **Avinstall**.

     Vänta tills avinstallationsprocessen är slutförd.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender VPN** och välj **Avinstall**.

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

     Vänta tills avinstallationsprocessen är slutförd.

3.6.4. Hur tar jag bort tillägget Bitdefender Anti-tracker?

Beroende på vilken webbläsare du använder följer du de här stegen för att avinstallera tillägget Bitdefender Anti-tracker:

- Internet Explorer

  1. Klicka på  bredvid sökfältet och välj sedan Hantera tillägg.

     En lista med installerade tillägg visas.
  2. Klicka på Bitdefender Anti-tracker.
  3. Klicka på **Inaktivera** längst ned till höger.

- Google Chrome

  1. Klicka på bredvid sökfältet.
  2. Välj **Fler verktyg** och därefter **Tillägg**.

     En lista med installerade tillägg visas.
  3. Klicka på **Ta bort** i kortet Bitdefender Anti-tracker.
  4. Klicka på **Ta bort** i den popup-ruta som visas.

- Mozilla Firefox

  1. Klicka på  bredvid sökfältet.
  2. Välj **Tillägg** och därefter **Utökningar**.

     En lista med installerade tillägg visas.
  3. Klicka på **Ta bort** i kortet Bitdefender Anti-tracker.

3.6.5. Hur stänger jag automatiskt ned datorn när skanningen är klar?

Bitdefender erbjuder flera skanningsjobb som du kan använda för att vara säker på att systemet inte är infekterat av hot. Att skanna hela datorn kan ta längre tid att slutföra beroende på systemet hårdvaru- och programvarukonfiguration.

Av det skälet tillåter Bitdefender att du konfigurerar din produkt så att den stänger systemet så fort skanningen är klar.

Fundera på det här exemplet: du har avslutat dit arbete vid datorn och vill gå och lägga dig. Du vill att Bitdefender ska kontrollera hela ditt system.

Stänga ned datorn när Snabbskanning eller Systemskanning är klart:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
3. Klicka på bredvid Snabbskanning eller Systemskanning.
4. Från listan **Efterskanningsåtgärder** väljer du **Stäng ned dator** och klickar därefter på **NÄSTA**.
5. Aktivera **Schemalägg skanningsjobb** och välj sedan när jobbet ska starta.

   Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.

Stänga ned datorn när en anpassad skanning är klar:

1. Klicka på bredvid den anpassade skanning som du skapat.
2. I fönstret **Skanningsjobb** klickar du på **NÄSTA**.
3. Från listan **Efterskanningsåtgärder** väljer du **Stäng ned dator**.
4. Klicka på **NÄSTA** och därefter på **SPARA**.

Om inga hot hittas stängs datorn ned.

Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem. Mer information finns på *"Guiden för Antivirusskanning"* (p. 75).

3.6.6. Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?

Om din dator ansluts till Internet via en proxyserver måste du konfigurera Bitdefender med proxyinställningarna. Normalt upptäcker och importerar Bitdefender automatiskt proxyinställningarna från ditt system.

> **Viktigt**
> Internet-anslutningar från hemmet använder vanligtvis inte en proxyserver. Som en tumregel ska du kontrollera och konfigurera proxyinställningarna för Bitdefender-programmet när uppdateringarna inte fungerar. Om Bitdefender kan uppdatera är den korrekt konfigurerad för att ansluta till Internet.

Hantera proxyinställningar:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till **Avancerat** fliken.
3. Aktivera **Proxy-server**.
4. Klicka på **Proxy-ändring**.
5. Det finns två alternativ för att ange proxyinställningarna:
   - **Importera proxyinställningar från standardwebbläsare** - proxyinställningar för aktuell användare, extraherade från standardwebbläsaren. Om proxyservern kräver ett användarnamn och lösenord måste du skriva in dem i motsvarande fält.

     Notera
     Bitdefender kan importera proxy-inställningar från de mest populära webbläsarna, däribland de senaste versionerna av Microsoft Edge, Internet Explorer, Mozilla Firefox och Google Chrome.

   - **Anpassade proxy-inställningar** - proxy-inställningar som du kan konfigurera själv. Följande inställningar måste specificeras:
     - **Adress** - skriv in proxyserverns IP.
     - **Port** - skriv in vilken port som Bitdefender använder för att ansluta till proxyservern.
     - **Användarnamn** - skriv in ett användarnamn som känns igen av proxy.
     - **Lösenord** - skriv in det giltiga lösenordet för den tidigare valde användaren.
6. Klicka **OK** för att spara ändringarna och stänga fönstret.

Bitdefender använder tillgängliga proxy-inställningar tills den kan ansluta till Internet.

3.6.7. Använder jag en 32-bitars eller en 64-bitars version av Windows?

Ta reda på om du har ett 32-bitars eller ett 64-bitars operativsystem:

- I **Windows 7**:
  1. Klicka **Starta**.
  2. Lokalisera **Dator** i **Start** menyn.
  3. Högerklicka **Dator** och välj **Egenskaper**.

4. Se under **System** för att kontrollera informationen om ditt system.

- I **Windows 8**:

  1. Från Windows Start-skärm, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt i startskärmen) och högerklicka sedan på dess ikon.

     I **Windows 8.1** letar du upp **Den här datorn**.

  2. Välj**Egenskaper** i menyn längst ned.
  3. Titta i området System för att se din systemtyp.

- I **Windows 10**:

  1. Skriv "System" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon.
  2. Titta i System-området för att hitta information om din systemtyp.

3.6.8. Hur visar jag dolda objekt i Windows?

Dessa steg är användbara i de fall där du arbetar med en situation med hot och behöver hitta och radera den infekterade filen, som kan vara dold.

Följ dessa steg för att visa dolda objekt i Windows:

1. Klicka på **Start** och gå sedan till **Kontrollpanelen**.

   I **Windows 8 och Windows 8.1**: Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

2. Välj **Mappalternativ**.
3. Gå till fliken **Visa**
4. Välj **Visa dolda filer och mappar**.
5. Avmarkera **Dölj tillägg för kända filtyper**.
6. Rensa **Dölj skyddade operativsystemfiler**.
7. Klicka på **Verkställ** och sedan på **OK**.

I **Windows 10**:

1. Skriv "Visa dolda filer och mappar" i sökrutan från aktivitetsfältet och klicka på ikonen.
2. Välj **Visa dolda filer, mappar och enheter**.

3. Avmarkera **Dölj tillägg för kända filtyper**.
4. Rensa **Dölj skyddade operativsystemfiler**.
5. Klicka på **Verkställ** och sedan på **OK**.

3.6.9. Hur tar jag bort andra säkerhetslösningar?

Den huvudsakliga orsaken för att använda en säkerhetslösning är för att tillhandahålla skydd och säkerhet för dina data. Men vad händer om man har fler än en säkerhetsprodukt på samma system?

När du använder fler än en säkerhetslösning på samma dator blir systemet instabilt. Bitdefender Total Security installeraren upptäcker automatiskt andra säkerhetsprogram och ger dig möjlighet att avinstallera dessa.

Om du inte tog bort de andra säkerhetslösningarna under installationen:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Vänta ett ögonblick tills dess listan med installerade program visas.
  3. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
  4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Vänta ett ögonblick tills dess listan med installerade program visas.
  4. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
  5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.
  2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Appar**.
  3. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
  4. Klicka på **Avinstallera** igen för att bekräfta ditt val.

5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

Om du misslyckas med att ta bort den andra säkerhetslösningen från ditt system, hämta avinstalleringsverktyget från försäljarens webbsida eller kontakta dem direkt för att få riktlinjer för avinstallering.

3.6.10. Hur startar jag om i Felsäkert läge?

Felsäkert läge ät ett diagnosticerande driftläge som vanligtvis används för att söka efter problem som påverkar den vanliga driften av Windows. Den typen av problem sträcker sig från konflikter mellan enheter, till hot som förhindrar att Windows startas normalt. I felsäkert läge fungerar endast ett fåtal appar och Windows laddar bara de grundläggande drivrutinerna samt ett minimum av operativsystemets komponenter. Det är därför de flesta hot är inaktiva och enkelt kan tas bort när du kör Windows i felsäkert läge.

För att starta Windows i felsäkert läge:

- I **Windows 7**:
  1. Starta om datorn.
  2. Tryck tangenten **F8** flera gånger innan Windows startar för att nå boot-menyn.
  3. Välj **Felsäkert läge** i boot-menyn eller **Felsäkert läge med nätverk** om du vill ha Internet-åtkomst.
  4. Tryck **Enter** och vänta tills Windows laddas i Felsäkert läge.
  5. Den här processen avslutas med ett bekräftelsemeddelande. Klicka på **OK** för att bekräfta.
  6. För att starta Windows normalt, bara starta om systemet.
- I **Windows 8, Windows 8.1 och Windows 10**:
  1. Starta **Systemkonfiguration** i Windows genom att samtidigt trycka på knapparna **Windows + R** på tangentbordet.
  2. Skriv **msconfig** i dialogrutan **Öppna**, klicka därefter **OK**.
  3. Välj fliken **Boot**.
  4. I området **Startalternativ** markerar du kryssrutan **Säker start**.
  5. Klicka på **Nätverk** och därefter **OK**.

6. Klicka **OK** i fönstret **Systemkonfiguration** som informerar dig om att systemet måste startas om för att kunna göra de ändringar du har ställt in.

   Ditt system startar om i felsäkert läge med nätverksanslutning.

För att starta om i normalläge ställer du tillbaka inställningarna genom att starta **Systemdrift** igen och avmarkera kryssrutan **Säker start**. Klicka på **OK** och sedan på **Starta om**. Vänta tills de nya inställningarna tillämpas.

4. HANTERA DIN SÄKERHET

4.1. Antivirusskydd

Bitdefender skyddar din dator från alla typer av hot (skadlig kod, trojaner, spionprogram, spökprogram osv). Skyddet som Bitdefender erbjuder delas in i två kategorier:

- Skanning vid åtkomst - förhindrar nya hot från att komma in i systemet. Bitdefender kan till exempel skanna ett Word-dokument efter kända hot när du öppnar det och ett e-postmeddelande när du får det.

  Skanning vid åtkomst säkerställer realtidsskydd mot hot och är en viktig komponent i alla datorsäkerhetsprogram.

  Viktigt
  Förhindra hot från att infektera din dator genom att ha **skanning vid åtkomst** aktiverat.

- På begäran-skanning - tillåter upptäckt och borttagning av hot som redan finns i systemet. Detta är en klassisk skanning som startats av användaren - du bestämmer vilken enhet, mapp eller fil som Bitdefender ska skanna, och Bitdefender skannar den på begäran.

Bitdefender skannar automatiskt alla borttagbara medier som är anslutna till datorn för att se till att den går att använda säkert. Mer information finns på *"Automatisk skanning av borttagbara medier"* (p. 79).

Avancerade användare kan konfigurera undantag från skanning om de inte vill att särskilda filer eller filtyper ska skannas. Mer information finns på *"Konfigurera skanningsundantag"* (p. 81).

När det upptäcker ett hot kommer Bitdefender automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering. Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Mer information finns på *"Hantera filer i karantän"* (p. 83).

Om din dator har infekterats med virus finns mer information i *"Ta bort hot från ditt system"* (p. 174). För att hjälpa dig rensa datorn från hot som inte kan tas bort inifrån Windows-operativsystemet, tillhandahåller Bitdefender *"Bitdefender Räddningsläge (räddningsmiljö i Windows 10)"* (p. 174). Det här en

betrodd miljö, särskilt utvecklad för att ta bort hot, silket gör det möjligt för dig att starta din dator oberoende av Windows. När datorn körs i räddningsläger (räddningsmiljö i Windows 10) är Windows-hot inaktiva, vilket gör det enkelt att ta bort dem.

4.1.1. Skanning vid åtkomst (realtidsskydd)

Bitdefender ger realtidsskydd mot flera olika hot genom att skanna alla öppnade filer och e-postmeddelanden.

Stänga av eller slå på realtidsskydd

Stänga av eller slå på realtidsskydd mot hot:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** stänger du av eller slår på **Bitdefender Shield**.
4. Om du vill inaktivera realtidsskydd visas ett varningsfönster. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktivt. Du kan inaktivera realtidsskyddet i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart. Realtidsskyddet slås automatiskt på när den valda tiden löper ut.

Varning
Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat är du inte skyddad mot hot.

Konfigurerar avancerade inställningar för realtidsskydd

Avancerade användare kan vilja dra fördel av de skanningsinställningar som Bitdefender erbjuder. Du kan konfigurera inställningarna för realtidsskyddet detaljerat genom att skapa en anpassad skyddsnivå.

Konfigurera avancerade inställningar för realtidsskydd:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** klickar du på rullgardinsmenyn **Visa avancerade inställningar**.

Ett panelfönster visas.

4. Bläddra upp och ned i fönstret för att konfigurera de skanningsinställningarna efter behov.

Information om skanningsalternativ

Du kan finna denna information användbar:

- **Skanna endast program.** Du kan konfigurera Bitdefender till att skanna endast öppnade appar.
- **Skanna potentiellt oönskade program.** Välj det här alternativet för att skanna efter oönskade program. En eventuellt oönskad applikation (PUA) eller eventuellt oönskat program (PUP) är en programvara som oftast ingår i freewareprogram och som visar popup-rutor eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem ändrar hemsidan eller sökmotorn, andra kär flera processer i bakgrunden som gör datorn långsammare eller visar många annonser. De här programmen kan installeras utan ditt samtycke (kallas även adware) eller ingår som standard i expressinstallationspaketet (annonsstöd).
- **Skanna nätverksresurser.** För att säkert komma åt ett fjärrnätverk från datorn rekommenderar vi att du har alternativet Skanna nätverksdelningar aktiverat.
- **Skanna arkiv.** Att skanna inne i arkiv är en långsam och resursintensiv process och rekommenderas därför inte för realtidsskydd. Arkiv som innehåller infekterade filer är inte ett direkt hot mot ditt systems säkerhet. Hotet kan endast påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att realtidsskyddet är aktiverat.

  Om du bestämmer dig för att använda det här alternativet aktiverar du det och drar sedan reglaget längs skalan för att exkludera skanning av arkiv som är längre än ett givet värde i MB (megabytes).
- **Skanna e-post.** För att förhindra att hot hämtas till din dator, skannar Bitdefender automatiskt inkommande och utgående e-postmeddelanden.

  Även om det inte rekommenderas kan du inaktivera hotskanning för att öka systemprestandan. Om du inaktiverar de motsvarande skanningsalternativen kommer de e-postmeddelanden och filer som tas emot inte att skannas och tillåter därmed att infekterade filer sparas på din dator. Det här är inte ett stort hot eftersom realtidsskyddet kommer

att blockera hotet när de infekterade filerna används (Öppnas, flyttas,kopieras eller körs).

- **Skanna bootsektorer.** Du kan konfigurera Bitdefender att skanna startsektorerna på hårddisken. Den här sektorn på hårddisken innehåller den datorkod som behövs för att starta bootprocessen. När ett hot infekterar startsektorn kan enheten bli oåtkomlig och du kanske inte kan starta systemet och komma åt dina data.
- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och ändrade filer, kan du kraftigt förbättra systemets responsivitet med en minimal förlust av säkerhet.
- **Skanna efter tangentloggning.** Välj det här alternativet för att skanna systemet efter keyloggerappar. Keyloggers spelar in det du skriver på tangetbordet och skickar rapporter över Internet till en person med ont uppsåt (hackare). Hackaren kan utvinna känslig information, såsom bankkontonummer och lösenord ur den stulna uppgifterna, och använda detta för att skaffa sig personliga fördelar.
- **Skanna vid systemstart.** Välj alternativet **Tidig startskanning** för att skanna systemet vid start så fort alla kritiska tjänster har laddats. Syftet med den här funktionen är att förbättra hotupptäckt vid systemstart och starttid för systemet.

Åtgärder som vidtas vid upptäckta hot

Du kan konfigurera de åtgärder som vidtas av realtidsskyddet genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** klickar du på rullgardinsmenyn **Visa avancerade inställningar**.

   Ett panelfönster visas.
4. Bläddra nedåt i fönstret till du ser alternativet **Hotåtgärder**.
5. Konfigurera skanningsinställningarna efter behov.

Följande åtgärder kan vidtas av realtidsskyddet i Bitdefender:

Vidta rätt åtgärder

Bitdefender vidtar rekommenderade åtgärder beroende på typ av upptäckt fil:

- **Smittade filer.** Filer som upptäcks som infekterade matchar en del av den hotinformation som hittas i Bitdefenders hotinformationsdatabas. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering.

  Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på *"Hantera filer i karantän"* (p. 83).

  > **Viktigt**
  > För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

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

  Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en hotinformationsuppdatering för att tillåta borttagning av hotet.

- **Arkiv som innehåller infekterade filer.**
  - Arkiv som endast innehåller infekterade filer tas bort automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer försöker Bitdefender att ta bort de infekterade filerna förutsatt att det går att rekonstruera arkivet med rena filer. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Flytta till karantän

Flyttar upptäckta filer till karantän. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på *"Hantera filer i karantän"* (p. 83).

Neka åtkomst
Om en infekterad fil hittas nekas åtkomst till den.

Återställa standardinställningarna

Standardinställningarna för realtidsskyddet försäkrar ett bra skydd mot hot, med liten påverkan på systemets prestanda.

För att återställa standardinställningarna för realtidsskyddet:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. I fönstret **Shield** klickar du på rullgardinsmenyn **Visa avancerade inställningar**.

   Ett panelfönster visas.
4. Bläddra nedåt i fönstret till du ser alternativet **Återställ inställningar**. Välj det här alternativet för att återställa antivirusinställningarna till standard.

4.1.2. Skanning på begäran

Huvudmålet för Bitdefender är att hålla din dator ren från hot. Detta görs genom att hålla nya hot borta från din dator och genom att skanna dina e-postmeddelanden och alla nya filer som hämtas eller kopieras till ditt system.

Det finns en risk för att ett hot redan finns i systemet innan du ens installerar Bitdefender. Därför är det en god idé att skanna din dator för befintliga hot efter att du installerat Bitdefender. Och det är definitivt en bra idé att regelbundet skanna datorn för hot.

På begäran-skanning baseras på skanningsuppgifter. Skanningsuppgifter specificerar skanningsalternativen och de objekt som ska skannas. Du kan när du vill skanna datorn genom att köra standarduppgifterna för dina egna skanningsuppgifter (användardefinierade uppgifter). Om du vill skanna specifika platser på din dator eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb.

Skanna en fil eller mapp för hot

Du borde alltid skanna filer och mappar när du misstänker att de kan vara infekterade. Högerklicka på de filer eller mappar du vill skanna, peka på **Bitdefender** och välj **Skanna med Bitdefender**. Guiden för antivirusskanning

kommer att visas och leda dig genom skanningsprocessen. I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.

Köra en snabbskanning

Snabbskanning använder skanning i "molnet" för att upptäcka hot som körs på ditt system. Att köra en snabbskanning tar vanligtvis under en minut och använder en bråkdel av de systemresurser som krävs vid en vanlig antivirusskanning.

Köra en snabbskanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Snabbskanning**.
3. Följ guiden för Antivirusskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

Kör en systemskanning

Systemskanningen skannar hela datorn efter alla typer av hot som är riskabla för säkerheten, som skadlig kod, spionprogramvara, adware, rootkits och annat.

> **Notera**
> Eftersom **Systemskanning** utför en noggrann skanning av hela systemet kan skanningen ta en stund. Därför rekommenderas du att köra det här jobbet när du inte använder din dator.

Innan du kör en skanning rekommenderas följande:

- Se till att Bitdefender är uppdaterad med sin hotinformationsdatabas. Om du skannar datorn med en utdaterad hotinformationsdatabas kan Bitdefender förhindras från att upptäcka nya hot som hittats sedan den senaste uppdateringen. Mer information finns på *"Se till att Bitdefender är uppdaterad"* (p. 33).
- Stäng ned alla öppna program.

Om du vill skanna specifika platser på din dator eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb. Mer information finns på *"Konfigurera en anpassad skanning"* (p. 72).

Köra en systemskanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
3. Första gången du kör en systemskanning presenteras du för funktionen. Klicka **JAG FATTAR** för att fortsätta.
4. Följ guiden för Antivirusskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

Konfigurera en anpassad skanning

I fönstret **Hantera skanningar** kan du ställa in Bitdefender på att köra skanningar när du anser att din dator behöver kontrolleras för eventuella hot. Du kan välja att schemalägga en Systemskanning eller en Snabbskanning, eller så kan du skapa en anpassad skanning när det passar dig.

När du öppnar fönstret är följande ikoner tillgängliga:

Det schemalagda skanningsjobbet är avstängt.

Det schemalagda skanningsjobbet är på.

Konfigurationen i detalj kan göras härifrån.

Ta bort den valda skanningen. Det här alternativet är bara tillgängligt för nya anpassade skanningar.

Konfigurera en ny anpassad skanning i detalj:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS** fliken, klicka på **Hantera skanningar**.
3. Klicka på **Skapa ett nytt skanningsjobb**.
4. I fältet **Jobbnamn** skriver du ett namn för skanningen, därefter klickar du på de platser du vill ska skannas och sedan på **NÄSTA**.
5. Konfigurera dessa allmänna alternativ:

- **Skanna endast program**. Du kan konfigurera Bitdefender till att skanna endast öppnade appar.
- **Prioritet för skanningsjobb**. Du kan välja vilken inverkan en skanningsprocess ska ha på din systemprestanda.
  - Auto - Prioritet för skanningsprocessen beror på systemaktiviteten. För att se till att skanningsprocessen inte påverkar systemaktiviteten bestämmer Bitdefender om skanningsprocessen ska köras med hög eller låg prioritet.
  - Hög - Skanningsprocessens prioritet är hög. Genom att välja det här alternativet kommer du att tillåta andra program att köras långsammare och minska tiden som behövs för att skanningsprocessen ska slutföras.
  - Låg - Skanningsprocessens prioritet är låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka tiden som behövs för att skanningsprocessen ska slutföras.
- **Efterskanningsåtgärder**. Välj vilken åtgärd Bitdefender ska utföra om inga hot upptäcks:
  - Visa sammanfattningsfönster
  - Stäng ned dator
  - Stäng skanningsfönster

6. Om du vill konfigurera skanningsalternativen i detalj klickar du på **Visa avancerade alternativ**. Du kan hitta information om de listade skanningarna i slutet av det här avsnittet.

   Klicka **NÄSTA**.

7. Aktivera **Schemalägg skanningsjobb** och välj sedan när den anpassade skanning du skapade ska starta.
   - Vid systemstart
   - Dagligen
   - Månadsvis
   - Veckovis

   Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.

8. Klicka på **SPARA** för att spara inställningarna och stänga konfigurationsfönstret.

   Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot hittas under skanningsprocessen ombes du att välja åtgärder som ska vidtas för de hittade filerna.

Information om skanningsalternativ

Du kan finna denna information användbar:

- Om du inte är bekant med några av dessa termer, kontrollera dem i ordlistan. Du kan också hitta användbar information genom att söka på Internet.
- **Skanna potentiellt oönskade program.** Välj det här alternativet för att skanna efter oönskade program. En eventuellt oönskad applikation (PUA) eller eventuellt oönskat program (PUP) är en programvara som oftast ingår i freewareprogram och som visar popup-rutor eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem ändrar hemsidan eller sökmotorn, andra kär flera processer i bakgrunden som gör datorn långsammare eller visar många annonser. De här programmen kan installeras utan ditt samtycke (kallas även adware) eller ingår som standard i expressinstallationspaketet (annonsstöd).
- **Skanna arkiv.** Arkiv som innehåller infekterade filer är inte ett direkt hot mot ditt systems säkerhet. Hotet kan endast påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att realtidsskyddet är aktiverat. Det rekommenderas dock att använda det här alternativet för att upptäcka och ta bort alla potentiella hot, även om det inte är ett direkt hot.

  Dra reglaget längs skalan för att exkludera arkiv som är längre än ett givet värde i MB (megabytes) från skanning.

  > **Notera**
  > Skanning av arkiverade filer ökar den totala skanningstiden och kräver högre systemresurser.

- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och ändrade filer, kan du kraftigt förbättra systemets responsivitet med en minimal förlust av säkerhet.

- **Skanna bootsektorer.** Du kan konfigurera Bitdefender att skanna startsektorerna på hårddisken. Den här sektorn på hårddisken innehåller den datorkod som behövs för att starta bootprocessen. När ett hot infekterar startsektorn kan enheten bli oåtkomlig och du kanske inte kan starta systemet och komma åt dina data.
- **Skanna minne.** Välj det här alternativet för att skanna program som körs i systemets minne.
- **Skanna register.** Välj det här alternativet för att skanna registernycklar. Windows Registry är en databas som lagrar konfigurationsinställningar och alternativ för systemkomponenter i Windows operativsystem, samt för installerade appar.
- **Skanna cookies.** Välj det här alternativet för att skanna de cookies som din webbläsare har lagrat på datorn.
- **Skanna efter tangentloggning.** Välj det här alternativet för att skanna systemet efter keyloggerappar. Keyloggers spelar in det du skriver på tangetbordet och skickar rapporter över Internet till en person med ont uppsåt (hackare). Hackaren kan utvinna känslig information, såsom bankkontonummer och lösenord ur den stulna uppgifterna, och använda detta för att skaffa sig personliga fördelar.

Guiden för Antivirusskanning

När du än inleder en på begäranskanning (till exempel högerklickar på en mapp, pekar på Bitdefender och väljer **Skanna med Bitdefender**), kommer Bitdefenders guide för antivirusskanning att visas. Följ guiden för att slutföra skanningsprocessen.

Notera

Om guiden för skanning inte visas kan skanningen vara konfigurerad att köras tyst i bakgrunden. Sök efter ikonen för skanningsframgång i systemfältet. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsframgången.

Steg 1 - Utför skanning

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

Vänta medan Bitdefender slutför skanningen. Skanningsprocessen kan ta en stund beroende på hur komplicerad den är.

Stoppar eller pausar skanningen. Du kan stoppa skanningen när du vill genom att klicka på **STOPP**. Du kommer att gå direkt till att se guidens sista steg. För att tillfälligt stoppa skanningsprocessen klickar du bara på **Pause**. Du måste klicka på **FORTSÄTT** för att återuppta skanningen.

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

- **Lösenord.** Om du vill att Bitdefender ska skanna arkivet, välj detta alternativ och skriv in lösenordet. Om du inte kan lösenordet, välj ett av de andra alternativen.
- **Fråga inte efter lösenordet och hoppa över denna post för skanning.** Välj det här alternativet för att hoppa över skanning av det här arkivet.
- **Hoppa över alla lösenordsskyddade poster utan att skanna dem.** Välj detta alternativ om du ej vill störas om lösenordsskyddade arkiv. Bitdefender kommer inte att kunna skanna dem, men ett register kommer att finnas i skanningsloggen.

Välj önskat alternativ och klicka på **OK** för att fortsätta skanningen.

Steg 2 - Välj åtgärder

I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.

Notera

När du kör en snabbskanning eller en systemskanning vidtar Bitdefender automatiskt rekommenderade åtgärder på upptäckta filer under skanningen. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

De infekterade objekten visas i grupper baserade på vilken typ av hot de är infekterade med. Klicka länken som motsvarar ett hot för att få mer information om de infekterade objekten.

Du kan välja en omfattande åtgärd som ska tas på alla problem, eller så kan du välja separata åtgärder för varje problemgrupp. Ett eller flera av följande alternativ kan visas i menyn:

Vidta rätt åtgärder

Bitdefender vidtar rekommenderade åtgärder beroende på typ av upptäckt fil:

- **Smittade filer.** Filer som upptäcks som infekterade matchar en del av den hotinformation som hittas i Bitdefenders hotinformationsdatabas. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering.

  Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på *"Hantera filer i karantän"* (p. 83).

  > **Viktigt**
  > För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

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

  Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en informationsuppdatering för att tillåta borttagning av hotet.

- **Arkiv som innehåller infekterade filer.**
  - Arkiv som endast innehåller infekterade filer tas bort automatiskt.
  - Om ett arkiv innehåller både infekterade och rena filer försöker Bitdefender att ta bort de infekterade filerna förutsatt att det går att rekonstruera arkivet med rena filer. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Radera

Tar bort upptäckta filer från enheten.

Om infekterade filer lagras i ett arkiv tillsammans med rena filer försöker Bitdefender ta bort de infekterade filerna och bygga om arkivet med de rena filerna. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Vidta ingen åtgärd.
Ingen åtgärd kommer att tas på de upptäckta filerna. När skanningen är slutförd kan du öppna skanningsloggen för att se information om dessa filer.

Klicka **Fortsätt** för att tillämpa den valda åtgärden.

Steg 3 - Sammanfattning

När Bitdefender är färdig med att lösa problemen kommer skanningsresultaten att visas i ett nytt fönster. Om du vill få omfattande information om skanningsprocessen, klicka **VISA LOGG** för att visa skanningsloggen.

> **!** **Viktigt**
>
> I de flesta fall lyckas Bitdefender desinficera de infekterade filer den upptäcker, annars isolerar den infektionen. Dock finns det problem som inte kan lösas automatiskt. Om det krävs startar du om systemet för att slutföra rensningsprocessen. Mer information och instruktioner om hur du tar bort ett hot manuellt finns i *"Ta bort hot från ditt system"* (p. 174).

Kontrollera skanningsloggar

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen i fönstret Antivirus. Skanningsloggen innehåller detaljerad information om de loggade skanningsprocesserna, som skanningsalternativ, skanningsmål, vilka hot som hittats samt vilka åtgärder som vidtagits på dessa hot.

Du kan öppna skanningsloggen direkt från guiden för skanning när skanningen slutförts, genom att klicka **VISA LOGG**.

Kontrollera en skanningslogg eller en upptäckt infektion vid ett senare tillfälle:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste skanningen.

Här hittar du alla hotskanningshändelser, inklusive hot upptäckta av pågående skanning, användarinitierade skanningar och statusändringar för automatiska skanningar.

3. I meddelandelistan kan du kontrollera vilka skanningar som har utförts på senaste tiden. Klicka på ett meddelande för att visa information om det.
4. Öppna skanningsloggen genom att klicka på **Visa logg**.

4.1.3. Automatisk skanning av borttagbara medier

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

Upptäckta enheter placeras i en av dessa kategorier:

- CDs/DVDs
- Flash-enheter, som flash-stickor och externa hårddiskar
- kartlagda (fjärr) nätverksenheter

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

Hur fungerar det?

När Bitdefender upptäcker en borttagbar lagringsenhet börjar den skanna efter hot (förutsatt att automatisk skanning är aktiverat för den typen av enhet). Du meddelas via ett popup-fönster att en ny enhet har upptäckts och att den skannas.

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

När skanningen är klar visas skanningsresultatfönstret för att informera dig om du säkert kan öppna filer på det borttagbara mediet.

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

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

Den här informationen kan vara användbar för dig:

- Var försiktig när du använder en hotinfekterad CD/DVD, eftersom hotet inte kan tas bort från disken (mediet är skrivskyddat). Se till att realtidsskydd är aktiverat för att förhindra hot från att spridas till ditt system. Det är bästa praxis att kopiera alla värdefulla data från skivan till ditt system och sedan kasta bort skivan.
- I vissa fall kan inte Bitdefender ta bort hot från specifika filer på grund av juridiska eller tekniska begränsningar. Ett sådant exempel är filer som arkiverats med en egen teknik (det är för att arkivet inte kan rekonstrueras korrekt).

  Information om hur du hanterar hot finns i "*Ta bort hot från ditt system*" (p. 174).

Hantera skanning av borttagbara medier

Hantera automatisk skanning av borttagbara medier:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Diskar och enheter**.

Skanningsalternativen är förkonfigurerade för bästa upptäcktsresultat. Om smittade filer hittas försöker Bitdefender desinfektera dem (ta bort den skadliga koden) eller flytta dem till karantän. Om båda åtgärderna misslyckas, kommer guiden för Antivirus-skanning att låta dig välja andra åtgärder att ta till mot infekterade filer. Skanningsalternativen är standard och du kan inte ändra dem.

För bästa skydd rekommenderar vi att alternativet **Autoskanning** är markerat för alla typer av borttagbara lagringsenheter.

4.1.4. Skanna värdens fil

Värdens filer kommer som standard med installationen av operativsystemet och används för att mappa värdnamn till IP-adresser varje gång du öppnar

en ny webbsida, ansluter till en FTP eller till andra Internet-servrar. Det är vanlig textfil och skadliga program kan ändra den. Avancerade användare vet hur de ska använda den för att blockera irriterande annonser, banners, tredjepartscookies eller kapare.

Konfigurera skanning av värdfil:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till **Avancerat** fliken.
3. Aktivera eller inaktivera **Skanna värdfil**.

4.1.5. Konfigurera skanningsundantag

Bitdefender tillåter undantag av specifika filer, mappar eller filändelsen från skanning. Den här funktionen är avsedd för att undvika att du störs i ditt arbete och den kan också bidra till att förbättra systemprestanda. Undantag ska användas av användare som har avancerad datorkunskap eller som annars följer rekommendationerna från en Bitdefender-medarbetare.

Du kan konfigurera undantag att gälla endast för vid åtkomst- eller på begäran-skanning, eller för båda. De objekt som exkluderas från en på begäran-skanning kommer inte att skannas även om de öppnas av dig eller ett program.

Notera

Undantag kommer INTE att tillämpas på kontextskanning. Innehållsskanning är en typ av på begäran-skanning: du högerklickar filen eller mappen du vill söka igenom och väljer **Skanna med Bitdefender**.

Undanta filer och mappar från skanning

Undanta specifika filer och mappar från skanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Undantag**.
4. Klicka på rullgardinsmenyn **Lista över filer och mappar undantagna från skanning**. I det fönster som visas kan du hantera de filer och mappar som är undantagna från skanning.
5. Lägg till undantag genom att följa dessa steg:

a. Klicka **Lägg till**.

b. Klicka **BLÄDDRA**, välj den fil eller mapp som du vill ska undantas från skanningen och klicka sen på **LÄGG TILL**. Alternativt kan du skriva (eller kopiera och klistra in) sökvägen till filen eller mappen i redigeringsfältet.

c. Som standard undantas den valda filen eller mappen från både vid åtkomst- och på begäran-skanning. För att ändra när undantaget ska tillämpas väljer du ett av de andra alternativen.

d. Klicka **Lägg till**.

Undanta filtillägg från skanning

När du undantar ett filtillägg från skanning, skannar Bitdefender inte längre filer med det tillägget, oavsett var de finns på din dator. Undantaget gäller även filer på borttagbara medier, som CD-skivor, DVD-skivor, USB-lagringsenheter eller nätverksenheter.

Viktigt
Var försiktig när du undantar filtillägg från skanning eftersom sådana undantag kan göra datorn mer sårbar för hot.

Undanta filtillägg från skanning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Undantag**.
4. Klicka på rullgardinsmenyn **Lista med tillägg undantagna från skanning**. I det fönster som visas kan du hantera filtillägg som är undantagna från skanning.
5. Lägg till undantag genom att följa dessa steg:
   a. Klicka **Lägg till**.
   b. Skriv in de filtillägg som du vill ska undantas från skanning, separerade med semikolon (;). Här är ett exempel:

      txt;avi;jpg

   c. Som standard är alla filer med de specificerade tilläggen undantagna från både vid åtkomst- och på begäran-skanning. För att ändra när undantaget ska tillämpas väljer du ett av de andra alternativen.

d. Klicka på **LÄGG TILL**.

Hantera skanningsundantag

Om de inställda undantagen från skanning inte längre behövs rekommenderar vi att du raderar dem eller inaktiverar skanningsundantag.

Hantera skanningsundantag:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
3. Välj fliken **Undantag**.
4. Använd alternativen i rullgardinsmenyn **Lista över filer och mappar undantagna från skanning** för att hantera skanningsundantag.
5. Ta bort eller redigera skanningsundantag genom att klicka på en a de tillgängliga länkarna. Fortsätt enligt följande:
   - Ta bort en post från listan genom att markera den och klicka på **Ta bort**.
   - Redigera en post från tabellen genom att dubbelklicka på den (eller markera den och klicka på **Redigera**). Ett nytt fönster visas där du kan ändra det tillägg eller den sökväg som ska undantas och den typ av skanning du vill att de ska undantas från, efter behov. Gör de nödvändiga ändringarna och klicka sedan på **ÄNDRA**.

4.1.6. Hantera filer i karantän

Bitdefender isolerar de hotinfekterade filerna den inte kan desinfektera och de misstänkta filerna i ett säkert område som kallas karantän. När ett hot är satt i karantän kan det inte göra någon skada eftersom det inte kan köras eller läsas.

Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en informationsuppdatering för att tillåta borttagning av hotet.

Dessutom skannar Bitdefender filerna som är satta i karantän varje gång hotinformationsdatabasen uppdateras. Rengjorda filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Kontrollera och hantera filer i karantän:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.

2. I **ANTIVIRUS**-panelen klickar du på **Karantän**.

   Här kan du visa namnet på filerna i karantän, deras ursprungliga plats och namnet på de upptäckta hoten.

3. Filer satta i karantän hanteras automatiskt av Bitdefender enligt standardinställningarna för karantän.

   Även om det inte rekommenderas kan du justera karantäninställningarna enligt dina önskemål genom att klicka på **Visa inställningar**.

   Klicka på reglagen för att aktivera eller inaktivera:

   Skanna om karantän efter uppdatering av information
   Behåll detta alternativ aktiverat för att automatiskt skanna filer i karantän varje gång hotinformationsdatabas uppdateras. Rengjorda filer flyttas automatiskt tillbaka till sin ursprungliga plats.

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

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

4. Ta bort en fil i karantän genom att markera den och klicka på knappen **TA BORT**. Om du vill återställa en fil från karantän till sin ursprungliga plats, välj den och klicka **ÅTERSTÄLL**.

4.2. Avancerat hotskydd

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

Advanced Threat Defense övervakar kontinuerligt de appar som körs på datorn på jakt efter hotlika aktiviteter. Alla dessa åtgärder poängsätts och en total poäng räknas ut för varje process.

Som en säkerhetsåtgärd meddelas du varje gång hot och eventuellt skadliga processer upptäcks och blockeras.

4.2.1. Aktivera eller inaktivera Advanced Threat Defense

Aktivera eller inaktivera Advanced Threat Defense:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** aktiverar eller inaktiverar du omkopplaren.

> **Notera**
> För att systemet ska vara skyddat mot ransomware och andra hot rekommenderar vi att du inaktiverar Advanced Threat Defense under så kort tid som möjligt.

4.2.2. Kontrollera upptäckta skadliga attacker

Varje gång hot eller potentiellt skadliga processer upptäcks blockerar Bitdefender dem för att förhindra att datorn infekteras av ransomware eller annan skadlig kod. Du kan när som helst kontrollera listan med upptäckta skadliga attacker genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Hotförsvar**.
3. Första gången du öppnar Webbkameraskydd presenteras du för funktionen. Klicka **JAG FATTAR** för att fortsätta.

   De attacker som upptäckts under de senaste 90 dagarna visas. För att visa information om typen av upptäckt ransomware, sökvägen till den skadliga processen eller om desinfektionen har lyckats, klickar du bara på det.

4.2.3. Lägga till processer till undantag

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

Börja lägga till processer till undantagslistan för Advanced Threat Defense:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Inställningar**.
3. I området **Undantag** klickar du på **Lägg till program till undantag**.
4. Hitta och välj den app du vill ska undantas och klicka sedan på **OK**.

   Om du vill ta bort en post från listan klickar du på alternativet **Ta bort** bredvid den.

4.2.4. Upptäckt av exploateringar

Ett sätt som hackare använder för att bryta sig in i system är att utnyttja särskilda buggar eller sårbarheter som finns i datorprogramvara (appar eller plugin-program) och hårdvara. För att säkerställa att din dator hålls borta från sådana attacker, som normalt sprider sig mycket fort, använder Bitdefender de senaste antiexploateringsteknikerna.

Aktivera eller inaktivera exploateringsupptäckt

Aktivera eller inaktivera exploateringsupptäckt:

- Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
- I panelen **ADVANCED THREAT DEFENSE** klickar du på **Inställningar**.
- Klicka på motsvarande omkopplare för att slå på eller av.

Notera
Alternativet Exploateringsupptäckt aktiveras som standard.

4.3. Förebygga onlinehot

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

Bitdefender tillhandahåller förebyggande av onlinehot för:

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

Konfigurera inställningar för förebyggande av onlinehot:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Inställningar**.

I fönstret **Webbskydd** klickar du på reglagen för att aktivera eller inaktivera:

- Förebyggande av webbattack blockerar hot som kommer från Internet, däribland drive-by-nedladdningar.

- Search Advisor, en komponent som rankar resultat från dina sökmotorfrågor och de länkar som publicerats på sociala nätverk genom att placera en ikon bredvid varje resultat:

  Du bör inte besöka den här webbsidan.

  Den här webbsidan kan innehålla farligt innehåll. Iaktta försiktighet om du besöker den.

  Det här är en säker sida att besöka.

  Search Advisor rankar resultaten från följande sökmotorer:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor rankar länkar som publicerats på följande sociala nätverkstjänster:
  - Facebook
  - Twitter

- Krypterad webbskanning.

  Mer sofistikerade attacker kan använda säker webbtrafik för att missleda sina offer. Därför rekommenderar vi att du har alternativet Krypterad webbskanning aktiverat.

- Skydd mot bedrägeri.

- Skydd mot nätfiske.

I fönstret **Förebyggande av nätverkshot** finns alternativet **Förebyggande av näthot**. För att hålla datorn borta från attacker från komplexa skadeprogram (som ransomware) via exploatering av säkerhetsbrister ska du ha det här alternativet aktiverat.

Du kan skapa en lista över webbplatser, domäner och IP-adresser som inte skannas av antihot-, antinätfiske- och antibedrägerimotorerna i Bitdefender. Listan ska endast innehålla webbplatser, domäner och IP-adresser som du litar helt på.

Konfigurera och hantera webbplatser, domäner och IP-adresser via funktionen Online Threat Prevention från Bitdefender:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.

2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Undantag**.
3. Skriv namnet på webbplatsen, domänen eller IP-adresse du vill lägga till i undantagen i motsvarande fält och klicka på **LÄGG TILL**.

   Ta bort en post från listan genom att markera den och klicka på **Ta bort**.

   Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

4.3.1. Bitdefender-varningar i webbläsaren

Varje gång du försöker besöka en webbplats som är klassad som osäker blockeras webbplatsen och en varningssida visas i webbläsaren.

Den här sidan innehåller information som webbplats-URL och upptäckta hot.

Du måste bestämma vad som ska göras härnäst. Följande alternativ är tillgängliga:

- Navigera bort från webbplatsen genom att klicka på **TA MIG TILLBAKA TILL SÄKERHETEN**.
- Fortsätt till webbplatsen, trots varningen, genom att klicka på **Jag förstår risken, ta mig dit ändå**.
- Om du är säker på att den hittade webbplatsen är säker klickar du på **SKICKA** för att lägga till den i undantagen. Vi rekommenderar att du bara lägger till webbplatser du verkligen litar på.

4.4. Antispam

Skräppost är en term som används för att beskriva oönskad e-post. Skräppost är ett växande problem både för privatpersoner och företag.Det är inte vackert, du skulle inte vilja att dina barn såg det, det kan få dig sparkad (för att ödsla tid på att ta emot porr till din arbets e-post) och du kan inte hindra människor från att sända den. Det näst bästa efter det är självklar att sluta få den. Olyckligtvis kommer skräppost i många olika former och storlekar, och det finns mycket av den. Olyckligtvis kommer skräppost i många olika former och storlekar, och det finns mycket av den.

Bitdefender skydd mot skräppost använder sig av häpnadsväckande tekniska innovationer och branschstandardiserade skräppostfilter för att sålla bort skräppost innan det når användarens inkorg. Mer information finns på "*Skräppostinsikter*" (p. 89).

Bitdefenders skräppostskydd är endast tillgängligt för e-postklienter som konfigurerats att ta emot e-postmeddelanden via POP3-protokollet. POP3

är ett av de mest använda protokollen för hämtning av e-postmeddelanden från en e-postserver.

Notera
Bitdefender tillhandahåller inte skräppostskydd för e-postkonton du når via en webbaserad e-posttjänst.

De skräppost-meddelanden som upptäcks av Bitdefender märks med prefixet [spam] i ämnesraden. Bitdefender flyttar automatiskt skräppostmeddelanden till en vald mapp enligt följande:

- I Microsoft Outlook flyttas skräppost-meddelanden till en **Skräppost** mapp som finns i mappen **Raderade poster**. **Skräppost**-mappen skapas så fort ett e-postmeddelande markeras som skräppost.
- I Mozilla Thunderbird flyttas skräppost-meddelanden till en **Skräppost** mapp som finns i mappen **Papperskorgen**. **Skräppost**-mappen skapas så fort ett e-postmeddelande markeras som skräppost.

Om du använder andra e-postklienter måste du skapa en regel för att flytta de e-postmeddelanden som är markerade som [spam] av Bitdefender till en anpassad karantänmapp. Om mapparna Borttagna objekt eller Papperskorg raderas, raderas mappen Skräppost också. En ny skräppostmapp skapas dock så fort ett e-postmeddelande markeras som skräppost.

4.4.1. Skräppostinsikter

Skräppostfilter

Bitdefenders skräppostmotor införlivar molnskydd och andra flera olika filter som ser till att din inkorg är fri från skräppost, som Lista över vänner, Lista över spammare och Teckenuppsättningsfilter.

Lista över vänner/lista över spammare

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

Notera
Vi rekommenderar att du lägger till dina vänners namn och e-postadresser till **vänlistan**. Bitdefender blockerar inte meddelanden från de som finns på den listan; därför hjälper att lägga till vänner dig med att se till att legitima meddelanden kommer fram.

Charset-filter

Många skräppostmeddelanden är skrivna med Kyrillisk och / eller Asiatisk teckenuppsättning. Teckenuppsättningsfiltret upptäcker den här sortens meddelanden och märker dem som SKRÄPPOST.

Skräppost-aktivitet

Bitdefenders motor för skydd mot skräppost använder sig av alla skräppostfilter tillsammans för att avgöra om ett visst e-postmeddelande bör hamna i din **Inkorg** eller ej.

Varje e-postmeddelande som kommer från Internet kontrolleras först mot filtret Vänlista/Spammarlista. Om avsändarens adress hittas i vänlistan flyttas meddelandet direkt till din **Inkorg**.

Annars tar filtret Spammarlista över e-postmeddelandet för att verifiera om avsändarens adress är med på listan. Om en matchning görs taggas e-postmeddelandet som SKRÄPPOST och flyttas till mappen **Skräppost**.

Annars kontrollerar Charset-filter om e-postmeddelandet är skrivet i kyrilliska eller asiatiska tecken. Om det är så taggas e-postmeddelandet som SKRÄPPOST och flyttas till mappen **Skräppost**.

Notera
Om e-postmeddelandet är märkt som SEXUALLY EXPLICIT i ämnesraden kommer Bitdefender att betrakta det som SKRÄPPOST.

E-postklienter och protokoll som stöds

Skräppostskyddet finns tillgängligt för alla POP3/SMTP e-postklienter. Bitdefenders verktygsfält mot skräppost är dock endast integrerat i:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 och senare

4.4.2. Slå på eller av skräppostskydd

Skräppostskydd är aktiverat som standard.

Slå på eller av skräppostfunktionen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTISPAM**-panelen slår du av eller på reglaget.

4.4.3. Använda verktygsfältet mot skräppost i din e-postklients fönster

I den övre delen på din e-postklient kan du se verktygsfältet för skydd mot skräppost. Verktygsfältet för skräppost hjälper dig att hantera skydd mot skräppost direkt från din e-postklient. Du kan enkelt rätta till Bitdefender om ett legitimt/ brev markerats som SKRÄPPOST.

Viktigt

Bitdefender integreras in i de vanligaste e-postklienterna genom ett enkelt använt verktygsfält för skydd mot skräppost. En komplett lista över e-postklienter som stöds finns i *"E-postklienter och protokoll som stöds"* (p. 90).

Varje knapp i verktygsfältet för Bitdefender beskrivs nedan:

Inställningar - öppnar ett fönster där du kan konfigurera skräppostfilter och verktygsinställningar.

Är skräppost - anger att det valda e-postmeddelandet är skräppost. E-postmeddelandet flyttas direkt till mappen **Skräppost**. Om molntjänster för skräppost är aktiverat skickas meddelandet till Bitdefender Cloud för vidare analys.

Inte skräppost - anger att det valda e-postmeddelandet inte är skräppost och Bitdefender skulle inte ha taggat det. E-postmeddelandet kommer att flyttas från mappen **Skräppost** till katalogen **Inkorg**. Om molntjänster för skräppost är aktiverat skickas meddelandet till Bitdefender Cloud för vidare analys.

Viktigt

Knappen **Inte skräppost** aktiveras när du markerar ett meddelande som Bitdefender märkt som Skräppost (vanligtvis finns dessa i mappen **Skräppost**).

Lägg till spammare - lägger till det valda e-postmeddelandets avsändare till listan över spammare. Du kan behöva klicka **OK** för att bekräfta.

E-postmeddelanden från adresser i listan över spammare märks automatiskt som [spam].

Lägg till vän - lägger till det valda e-postmeddelandets avsändare till listan över vänner. Du kan behöva klicka **OK** för att bekräfta. Du kommer alltid att få e-postmeddelanden från denna adress oavsett innehåll.

Spammare - Öppnar **Listan över spammare** som innehåller alla e-postadresser från vilka du inte vill ta emot meddelanden oavsett innehåll. Mer information finns på *"Konfigurera listan över spammare"* (p. 94).

Vänner - Öppnar **Listan över vänner** som innehåller alla e-postadresser från vilka du alltid vill ta emot e-postmeddelanden oavsett innehåll. Mer information finns på *"Konfigurera Listan över vänner"* (p. 93).

Anger upptäcktsfel

Om du använder en e-postklient som stöds kan du enkelt korrigera skräppostfiltret (genom att indikera vilka e-postmeddelanden som ska markeras som [spam]). Att göra så hjälper till att förbättra effektiviteten för skräppostfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen skräppost som skräppost-meddelanden flyttas till.
3. Välj det legitima meddelandet som felaktigt märkts som [spam] av Bitdefender.
4. Klicka på knappen **Lägg till vän** i Bitdefenders verktygsfält för skydd mot skräppost för att lägga till avsändaren i Listan över vänner. Du kan behöva klicka **OK** för att bekräfta. Du kommer alltid att få e-postmeddelanden från denna adress oavsett innehåll.
5. Klicka knappen **Inte skräppost** i Bitdefenders verktygsfält mot skräppost (finns normalt i övre delen av e-postklientens fönster). E-postadressen flyttas till mappen Inkorg.

Visar oupptäckta skräppostmeddelanden

Om du använder en e-postklient som stöds kan du enkelt markera vilka e-postmeddelanden som skulle markerats som skräppost. Att göra så hjälper till att förbättra effektiviteten för skräppostfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen Inkorg.

3. Välj meddelande (skräppost) som ej upptäckts.
4. Klicka knappen **Är skräppost** i Bitdefenders verktygsfält mot skräppost (finns normalt i övre delen av e-postklientens fönster). De märks direkt som [spam] och flyttas till mappen för skräppost.

Konfigurera verktygsfältinställningar

Konfigurera inställningarna för skräppostverktygsfältet för din e-postklient genom att klicka på **Inställningar** på verktygsfältet och sedan på fliken **Verktygsfältsinställningar**.

Här har du följande alternativ:

- **Markera skräppostmeddelanden som "Läst"** - markera skräppostmeddelanden som lästa automatiskt, så att de inte är störande när de kommer.
- Du kan välja om vill visa bekräftelsefönster eller inte när du klickar på knapparna **Lägg till spammare** och **Lägg till vän** på verktygsfältet för skräppost.

  Bekräftelsefönster kan förhindra att du av misstag lägger till e-postavsändare på vänner-/spammarelistan.

4.4.4. Konfigurera Listan över vänner

Lista över vänner är en lista över alla e-postadresser som du alltid vill få meddelanden från, oavsett dess innehåll. Meddelanden från dina vänner märks inte som skräppost även om deras innehåll påminner om skräppost.

Notera
All e-post som anländer från en e-postadress som finns i **Listan för vänner** kommer att levereras till Inkorgen automatiskt utan vidare bearbetning.

För att konfigurera och hantera listan över vänner:

- Om du använder Microsoft Outlook eller Thunderbird klickar du på **Vänner** på Bitdefenders verktygsfält för skräppost.
- Alternativt:
  1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **SKRÄPPOST**-panelen klickar du på **Hantera vänner**.

För att lägga till en e-postadress väljer du alternativet **E-postadress**, skriver in adressen och klickar på **LÄGG TILL**. Syntax: name@domain.com.

För att lägga till alla e-postadresser från en vald domän, väljer du alternativet **Domännamn**, skriver in domännamnet och klickar på **LÄGG TILL**. Syntax:

- @domain.comoch domain.com - alla mottagna e-postmeddelanden från domain.com kommer att nå din **Inkorg** oavsett innehåll;
- domän - all mottagen e-post som har domännamnet domän (oavsett domänsuffix) kommer att märkas som SKRÄPPOST.
- com - all mottagen e-post som har domännamnet com kommer att märkas som SKRÄPPOST;

Det är rekommenderat att försöka 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 jobbar på eller för dina betrodda vänner.

Ta bort ett objekt från listan genom att klicka på motsvarande **Ta bort**-länk. Ta bort alla poster från listan genom att klicka på **RENSA LISTA**.

Du kan spara Listan över vänner på en fil, så att du kan använda den på en annan dator eller efter att du har återinstallerat produkten. För att spara listan med vänner, klicka på **Spara**-knappen och spara den på önskad plats. Filen kommer att ha en .bwl ändelse.

För att hämta en lista över spammare som sparats tidigare, klicka på **Hämta** knappen och öppna motsvarande .bwl fil. Återställ innehållet för den befintliga listan när du laddar en tidigare sparad lista genom att välja **Skriv över aktuell lista**.

Klicka **OK** för att spara ändringarna och stänga fönstret.

4.4.5. Konfigurera listan över spammare

Lista över spammare är en lista över alla e-postadresser som du inte vill få meddelanden från, oavsett dess innehåll. Alla e-postmeddelanden som mottas från en adress som finns i **Lista över spammare** kommer automatiskt att märkas som SKRÄPPOST, utan vidare bearbetning.

För att konfigurera och hantera listan över spammare:

- Om du använder Microsoft Outlook eller Thunderbird klickar du på knappen **Spammare** i Bitdefender-verktygsfältet mot skräppost som finns integrerat i din e-postklient.
- Alternativt:
  1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **SKRÄPPOST** fliken, klicka på **Hantera spammare**.

För att lägga till en e-postadress väljer du alternativet **E-postadress**, skriver in adressen och klickar på **LÄGG TILL**. Syntax: name@domain.com.

För att lägga till alla e-postadresser från en vald domän, väljer du alternativet **Domännamn**, skriver in domännamnet och klickar på **LÄGG TILL**. Syntax:

- @domain.comoch domain.com - alla mottagna e-postmeddelanden från domain.com kommer att nå din **Inkorg** oavsett innehåll;
- domän - all mottagen e-post som har domännamnet domän (oavsett domänsuffix) kommer att märkas som SKRÄPPOST.
- com - all mottagen e-post som har domännamnet com kommer att märkas som SKRÄPPOST.

Det är rekommenderat att försöka undvika att lägga till hela domäner men detta kan vara användbart i vissa situationer.

Varning

Lägg inte till domäner för legitima webbaserade e-posttjänster (som Yahoo, Gmail, Hotmail eller andra) till spammarlistan. Annars ses de e-postmeddelanden som tas emot från en oregistrerad användare av sådan tjänst som skräppost. Om du till exempel lägger till yahoo.com i Listan över spammare, kommer alla e-postmeddelanden från yahoo.com adresser att märkas som [spam].

Ta bort ett objekt från listan genom att klicka på motsvarande **Ta bort**-länk. Ta bort alla poster från listan genom att klicka på **RENSA LISTA**.

Du kan spara Skräppost-listan på en fil, så att du kan använda den på en annan dator eller efter att du har återinstallerat produkten. För att spara listan för spammare, klicka på **Spara**-knappen och spara den på önskad plats. Filen kommer att ha en .bwl ändelse.

För att hämta en lista över spammare som sparats tidigare, klicka på **Hämta** knappen och öppna motsvarande .bwl fil. Återställ innehållet för den befintliga listan när du laddar en tidigare sparad lista genom att välja **Skriv över aktuell lista**.

Klicka **OK** för att spara ändringarna och stänga fönstret.

4.4.6. Konfigurera lokala skräppostfilter

I *"Skräppostinsikter"* (p. 89), Bitdefender beskrivs hur det använder en kombination av filter för att identifiera skräppost. Skräppost-filtren är förinställda för effektivt skydd.

Viktigt

Beroende på om du får legitima e-postmeddelanden som är skrivna med asiatiska eller kyrilliska tecken eller inte, inaktiverar eller aktiverar du inställningen som automatiskt blockerar sådana e-postmeddelanden. Den motsvarande inställningen är inaktiverad i lokala versioner av programmet som innehåller sådana teckenuppsättningar (till exempel i den Ryska eller Kinesiska versionen).

Konfigurera lokala skräppostfilter:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **SKRÄPPOST**-panelen klickar du på **Inställningar**.
3. Klicka på motsvarande omkopplare för att slå på eller av.

Om du använder Microsoft Outlook eller Thunderbird kan du konfigurera lokala skräppostfilter direkt från e-postklienten. Klicka på **Inställningar** på Bitdefender-verktygsfältet för skräppost (finns normalt i den övre delen av e-postklientfönstret) och sedan på fliken **Skräppostfilter**.

4.4.7. Konfigurera molninställningarna.

Molnupptäckten använder Bitdefender Cloud-tjänsterna för att ge dig effektivt och alltid uppdaterat skydd mot skräppost.

Molnskyddet fungerar så länge som du har Bitdefender Antispam aktiverat.

Exempel på legitima eller skräppostmeddelanden kan skickas till Bitdefender Cloud när du anger upptäcktsfel eller oupptäckta skräppostmeddelanden. Det hjälper till att förbättra Bitdefenders skydd mot skräppost.

Konfigurera inskickat e-postexempel till Bitdefender Cloud genom att välja önskade alternativ genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **SKRÄPPOST**-panelen klickar du på **Inställningar**.
3. Klicka på motsvarande omkopplare för att slå på eller av.

Om du använder Microsoft Outlook eller Thunderbird kan du konfigurera molnupptäckt direkt från e-postklienten. Klicka på **Inställningar** på Bitdefender-verktygsfältet för skräppost (finns normalt i den övre delen av e-postklientfönstret) och sedan på fliken **Molninställningar**.

4.5. Brandvägg

Brandväggen skyddar din dator från ingående och utgående obehöriga anslutningsförsök, både på lokala nätverk och på Internet. Det är ungefär som en vakt vid grinden - det 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 omständigheter skapar Bitdefender automatiskt en regel varje gång en app försöker komma åt Internet. Du kan också manuellt lägga till eller redigera regler för appar.

Som en säkerhetsåtgärd meddelas du varje gång en potentiellt skadlig app blockeras från att komma åt Internet.

Bitdefender tilldelar automatiskt en nätverkstyp till varje nätverksanslutning den upptäcker. Beroende på nätverkstyp är brandväggstypen inställd på lämplig nivå för varje anslutning.

Mer information om brandväggsinställningarna för varje nätverkstyp och hur du redigerar nätverksinställningarna finns i *"Hantera anslutningsinställningar"* (p. 100).

4.5.1. Aktivera eller inaktivera brandväggsskydd

Aktivera eller inaktivera brandväggsskydd:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** aktiverar eller inaktiverar du omkopplaren.

Varning

Eftersom din dator exponeras för obehöriga anslutningar, ska en avstängning av brandväggen endast vara en tillfällig åtgärd. Slå på brandväggen igen så fort som möjligt.

4.5.2. Hantera appregler

Visa och hantera brandväggsregler som styr appars åtkomst till nätverksresurser och Internet:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** klickar du på **Programåtkomst**.

3. Första gången du använder brandväggen får du en presentation av funktionen. Klicka **JAG FATTAR** för att fortsätta.

Du kan se de senaste 15 programmen (processerna) som har passerat igenom Bitdefenders brandvägg och det Internet-nätverk du är ansluten till. För att se vilka reglers som skapats för en specifik app klickar du bara på den och klickar därefter på länken **Visa programregler**. Fönstret **Regler** öppnas.

För varje regel visas följande information:

- **NÄTVERK** - processen och nätverksadaptertyperna (Hem/Kontor, Publik eller Alla) som regeln gäller för. Regler skapas automatiskt för att filtrera nätverks- eller Internet-åtkomst via en adapter. Som standard gäller reglerna för alla nätverk. Du kan manuellt skapa eller ändra befintliga regler för att filtrera en apps nätverks- eller Internetåtkomst genom en specifik adapter (till exempel, en trådlöst nätverksadapter).
- **PROTOKOLL** - det IP-protokoll regeln gäller för. Som standard gäller reglerna för alla protokoll.
- **TRAFIK** - regeln gäller i båda riktningarna, ingående och utgående.
- **PORTAR** - det PORT-protokoll regeln gäller för. Som standard gäller reglerna för alla portar.
- **IP** - det Internet-protokoll (IP) regeln gäller för. Som standard gäller reglerna för alla IP-adresser.
- **ÅTKOMST** - huruvida appen tillåts eller nekas tillgång till nätverk eller Internet under de angivna omständigheterna.

För att redigera eller ta bort reglerna för den valda appen klickar du på  -ikonen.

- **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.

Lägga till appregler

Lägga till en appregel:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** klickar du på **Inställningar**.

3. I fönstret **Regler** klickar du på **Lägg till regel**.

I fönstret **Inställningar** kan du tillämpa följande ändringar:

- **Använd den här regeln för alla program.** Aktivera den här omkopplaren för att tillämpa den skapade regeln för alla appar.
- **Programsökväg.** Klicka **BLÄDDRA** och välj den app som regeln tillämpas på.
- **Tillstånd.** Välj en av de tillgängliga behörigheterna:

Tillstånd	Beskrivning
Tillåt allt	Den angivna appen tillåts nätverks-/Internet-åtkomst under angivna omständigheterna.
Förneka	Den angivna appen nekas nätverks-/Internet-åtkomst under angivna omständigheterna.

- **Nätverkstyp.** Välj vilken typ av nätverk som regeln gäller för. Du kan ändra typ genom att öppna rullgardinsmenyn **Nätverkstyp** och välj en av följande typer från listan.

Nätverkstyp	Beskrivning
Något nätverk	Tillåt all trafik mellan din dator och andra datorer oavsett nätverkstyp.
Hem/Kontor	Tillåt all trafik mellan din dator och datorer i det lokala nätverket.
Publik	All datatrafik filtreras.

- **Protokoll.** Välj från menyn det IP-protokoll som regeln gäller.
  - Om du vill att regeln ska gälla för alla protokoll, välj **Alla**.
  - Om du vill att regeln ska gälla för TCP, välj **TCP**.
  - Om du vill att regeln ska gälla för UDP, välj **UDP**.
  - Om du vill att regeln ska gälla för ICMP, väljer du **ICMP**.
  - Om du vill att regeln ska gälla för IGMP, väljer du **IGMP**.

- Om du vill att regeln ska gälla för ett specifikt protokoll, skriver du det numret som är tilldelat det protokollet du vill filtrera i det tomma redigeringsfältet.

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

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

Riktning	Beskrivning
Utgående	Regeln tillämpas endast på utgående trafik.
Inkommande	Regeln tillämpas endast på inkommande trafik.
Båda	Regeln gäller för båda riktningarna.

I fönstret **Avancerat** kan du anpassa följande inställningar:

- **Anpassa lokal adress.** Specificera den lokala IP-adress och port som regeln tillämpas på.
- **Anpassa fjärradress.** Specificera den fjärr-IP-adress och port som regeln tillämpas på.

Ta bort den aktuella regeluppsättningen och återställ standardreglerna, klickar du på **Återställ regler** i fönstret **Regler**.

4.5.3. Hantera anslutningsinställningar

Oavsett om du ansluter till Internet via Wi-Fi eller Ethernet-adapter, kan du konfigurera vilka inställningar som ska gälla för en säker navigering. De alternativ du kan välja från är:

- **Dynamisk** – nätverkstypen anges automatiskt baserat på profilen för det anslutna nätverket, Hem/Kontor eller Publik. När detta sker gäller endast brandväggsregler för den specifika nätverkstypen eller de som definieras för alla nätverkstyper.
- **Hem/Kontor** – nätverkstypen är alltid Hem/Kontor, oavsett profilen för det anslutna nätverket. När detta sker gäller endast brandväggsregler för Hem/Kontor eller de som definieras för alla nätverkstyper.

- **Publik** - nätverkstypen kommer alltid att vara Publik, oavsett profilen för det anslutna nätverket. När detta sker gäller endast brandväggsregler för Publik eller de som definieras för alla nätverkstyper.

Konfigurera dina nätverksadaptrar:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** klickar du på **Inställningar**.
3. Välj fliken **Nätverksadaptrar**.
4. Välj de inställningar du vill använda när du ansluter till följande adaptrar:
   - Wi-Fi
   - Ethernet

4.5.4. Konfigurera avancerade inställningar

Konfigurera avancerade brandväggsinställningar:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** klickar du på **Inställningar**.
3. Välj fliken **Inställningar**.

Följande funktioner kan konfigureras:

- **Portskanningsskydd** - upptäcker och blockerar försök att ta reda på vilka portar som är öppna.

  Hackare använder sig ofta av portskanningar för att få reda på vilka av din dators portar som är öppna. De kan då bryta sig in i din dator om de hittar en mindre säker eller sårbar port.

- **Varningsläge** - varningar visas varje gång en app försöker ansluta till Internet. Välj **Tillåt** eller **Blockera**. När Varningsläge är aktiverat stängs funktionen Profiler av automatiskt. Aviseringsläge kan användas samtidigt som **Batteriläge**.

- **Tillåt åtkomst till domännätverk** - tillåt eller neka åtkomst till resurser och delningar definierade av dina domänkontroller.

- **Smygläge** - Huruvida du kan upptäckas av andra datorer eller ej. Klicka på **Redigera stöldinställningar** för att välja när din enhet ska kunna ses eller inte av andra datorer.

- **Standardprogrambeteende** - tillåt Bitdefender att använda automatiska inställningar på appen utan definierade regler. Klicka på **Redigera standardregler** för att välja om automatiska inställningar ska tillämpas eller inte.
  - Automatiskt - appåtkomst tillåts eller nekas baserat på den automatiska brandväggen och användarregler.
  - Tillåt - appar som inte har någon brandväggsregel definierad tillåts automatiskt.
  - Blockera - appar som inte har någon brandväggsregel definierad blockeras automatiskt.

4.6. Säkerhetsrisk

Ett viktig steg för att skydda din dator mot skadliga aktiviteter och program är att se till att operativsystemet och de appar du regelbundet använder är uppdaterade. Dessutom måste starka lösenord (lösenord som inte enkelt kan gissas) konfigureras för varje Windows-användarkonto och för de Wi-Fi-nätverk du ansluter till, för att förhindra obehörig fysisk åtkomst till din dator.

Bitdefender kontrollerar automatiskt ditt system efter sårbarheter och varnar dig om dem. Den skannar efter följande:

- utdaterade appar på datorn.
- saknade Windowsuppdateringar
- svaga lösenord till Windows användarkonton.
- osäkra trådlösa nätverk och routrar.

Bitdefender har två enkla sätt att åtgärda säkerhetsbristerna i ditt system:

- Du kan skanna systemet efter säkerhetsbrister och åtgärda dem steg för steg genom att använda alternativet **Sårbarhetsskanning**.
- Med automatisk sårbarhetsövervakning kan du kontrollera och åtgärda upptäckta säkerhetsbrister i fönstret Meddelanden.

Du bör kontrollera och åtgärda systemsäkerhetsbrister varje eller varannan vecka.

4.6.1. Skanna systemet för säkerhetsrisker

För att hitta systemsårbarheter kräver Bitdefender en aktiv Internet-anslutning.

Skanna systemet för säkerhetsrisker:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSRISK** klickar du på **Sårbarhetsskanning**.
3. Första gången du öppnar Sårbarhetsskanning presenteras du för funktionen. Klicka på **STARTA SKANNING** för att fortsätta och vänta sedan på att Bitdefender ska kontrollera systemet för säkerhetsrisker.

   - **Kritiska Windows-uppdateringar**

     En lista över kritiska Windows-uppdateringar som inte är installerade på datorn visas. En systemomstart kan krävas för att Bitdefender ska avsluta installationen.

     Observera att det kan ta en stund att installera uppdateringarna.

   - **Programuppdateringar**

     Klicka på namnet i listan för att se information om den app som måste uppdateras.

     Om en app inte är uppdaterad klickar du på **HÄMTA NY VERSION** för att hämta den senaste versionen.

   - **Svaga Windows-konton**

     Du kan se den ändrade listan över Windows-användarkonton på din dator, och skyddsnivån deras lösenord håller.

     Du kan välja mellan att be användaren ändra lösenordet vid nästa inloggning eller ändra lösenordet själv direkt.

     Ange ett nytt lösenord för systemet genom att välja **Byt lösenord nu**.

     För att skapa ett starkt lösenord rekommenderar vi att du använder en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).

   - **Wi-Fi-nätverk och routrar**

     Klicka på namnet i listan för att läsa mer om det trådlösa nätverk och den router du är ansluten till. Om det rekommendera att du ställer in ett starkare lösenord för ditt hemmanätverk ska du se till att följa våra

anvisningar, så att du kan fortsätta vara ansluten utan att oroa dig om din integritet.

När andra rekommendationer är tillgängliga följer du angivna instruktioner för att se till att hemnätverket förblir säkert för hackares nyfikna ögon.

4.6.2. Använda automatisk sårbarhetsövervakning

Bitdefender skannar regelbundet systemet efter sårbarheter, i bakgrunden, och håller reda på upptäckta problem i fönstret Meddelanden.

Kontrollera och åtgärda upptäckta problem:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** väljer du meddelandet som avser den senaste sårbarhetsskanningen.
3. Du kan se detaljerad information avseende de upptäckta säkerhetsbristerna i systemet. Beroende på händelse, för att åtgärda ett specifikt säkerhetsproblem fortsätt enligt följande:
   - Om det finns tillgängliga Windows-uppdateringar klickar du på **Installera**.
   - Om automatisk Windows-uppdatering är inaktiverat klickar du på **Aktivera**.
   - Om en app är utdaterad klickar du på **Uppdatera nu** för att hitta en länk till leverantörens hemsida varifrån du kan installera den senaste versionen av appen.
   - Om ett Windows-användarkonto har ett svagt lösenord klickar du på **Byt lösenord** för att tvinga användaren att byta lösenord vid nästa inloggning eller så kan du ändra lösenordet själv. För ett starkt lösenord, använd en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).
   - Om Windows-funktionen Autorun är aktiverad klickar du **Åtgärda** för att inaktivera den.
   - Om den router du har konfigurerat har angett ett svagt lösenord klickar du på **Ändra lösenord** för att komma till dess gränssnitt varifrån du kan ange ett starkt.
   - Om det nätverk du är ansluten till har säkerhetsbrister som kan försätta systemet i risk klickar du på **Ändra Wi-Fi-lösenord**.

Konfigurera inställningar för säkerhetsbristövervakning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Inställningar**.

> **Viktigt**
> För att regelbundet meddelas om system- eller appsäkerhetsbrister ska du har alternativet **Säkerhetsbrist** aktiverat.

3. Välj de systemsäkerhetsbrister du regelbundet vill ska kontrolleras genom att använda motsvarande omkopplare.

   Windowsuppdateringar
   Kontrollera om operativsystemet Windows har de senaste kritiska säkerhetsuppdateringarna från Microsoft.

   Programuppdateringar
   Kontrollera om appar installerade på ditt system är uppdaterade. Utdaterade appar kan exploateras av skadlig programvara, vilket gör din PC sårbar för utomstående attacker.

   Användarlösenord
   Kontrollera om lösenorden för de Windows-konton och routrar som är konfigurerade på systemet är enkla att gissa eller inte. Att konfigurera lösenord som svåra att gissa (starka lösenord) gär det mycket svårt för hackare att bryta sig in i systemet. Ett starkt lösenord innehåller en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).

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

   Vissa typer av hot använder Autorun för att spridas automatiskt från borttagbara medier till datorn. Därför rekommenderar vi att du inaktiverar den här Windows-funktionen.

   Wi-Fi Security Advisor
   Kontrollera om det trådlösa hemnätverk du är ansluten till är säkert eller inte, eller om det har säkerhetsbrister. Kontrollera också om lösenordet för din hemrouter är tillräckligt starkt och hur du kan göra det säkrare.

De flesta oskyddade nätverk är inte säkra och tillåter därmed att en hackare får tillgång till dina privata aktiviteter.

Notera
Om du stänger av övervakning av en specifik säkerhetsbrist kommer tillhörande problem inte längre att registreras i meddelandefönstret.

4.6.3. Wi-Fi Security Advisor

När du är på språng, arbetar på kafé eller väntar på flygplatsen, kan den snabbaste lösningen vara att ansluta till ett publikt trådlöst nätverk för att göra betalningar, kolla e-post eller sociala nätverkskonton. Men det kan finnas någon som försöker kapa dina personuppgifter där och som ser hur informationen läcker genom nätverket.

Personuppgifter innebär lösenord och användarnamn du använder för att få åtkomst till dina onlinekonton, som e-post, bankkonton, sociala mediekonton, men även de meddelanden du skickar.

Oftast är det mer troligt att publika trådlösa nätverk är osäkra, eftersom de inte kräver lösenord vid inloggning, och om de gör det, kan det lösenordet göras tillgängligt för alla som vill ansluta. Dessutom kan de vara skadliga nätverk, som utgör en måltavla för kriminella.

För att skydda dig mot farorna med osäkra eller okrypterade publika trådlösa surfzoner, analyserar Bitdefender Wi-Fi Security Advisor hur säkert ett trådlöst nätverk är, och om det behövs, rekommenderar dig att använda Bitdefender VPN.

Bitdefender Wi-Fi Security Advisor ger dig följande information om:

- Trådlösa hemnätverk
- Trådlösa kontorsnätverk
- Trådlösa publika nätverk

Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor

Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Inställningar**.

3. I fönstret **Inställningar** kan du aktivera eller inaktivera alternativet **Säkerhetsrådgivare**.

Konfigurera trådlöst hemnätverk

För att börja konfigurera ditt hemnätverk:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Wi-Fi-säkerhet**.
3. På fliken **Hem-Wi-Fi** klickar du på knappen **VÄLJ HEM-WI-FI**.

   En lista med de trådlösa nätverk du anslutit till hittills visas.
4. Peka på ditt hemnätverk och klicka därefter på **VÄLJ**.

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

Ta bort det trådlösa nätverk du har angett som hemnätverk genom att klicka på knappen **TA BORT**.

Lägg till ett nytt trådlöst nätverk som hemma genom att klicka på **Välj nytt hem-Wi-Fi**.

Konfigurera trådlöst kontorsnätverk

För att börja konfigurera ditt kontorsnätverk:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Wi-Fi-säkerhet**.
3. På fliken **Kontors-Wi-Fi** klickar du på knappen **VÄLJ KONTORS-WI-FI**.

   En lista med de trådlösa nätverk du anslutit till hittills visas.
4. Peka på ditt kontorsnätverk och klicka därefter på **VÄLJ**.

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

Ta bort det trådlösa nätverk du har angett som kontorsnätverk genom att klicka på **TA BORT**.

Lägg till ett nytt trådlöst nätverk som kontor genom att klicka på **Välj nytt kontors-Wi-Fi**.

Offentlig Wi-Fi

Medan du är ansluten till ett osäkert trådlöst nätverk är profilen Publikt Wi-Fi aktiverad. När den körs i den här profilen är Bitdefender Total Security inställd på att automatiskt uppnå följande programinställningar:

- Advanced Threat Defense är aktiverat
- Bitdefenders brandvägg är aktiverad och följande inställningar används för din trådlösa adapter:
  - Stöldläge - PÅ
  - Nätverkstyp - Publik
- Följande inställningar från Förebyggande av onlinehot är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägeri
  - Skydd mot nätfiske
- En knapp som öppnar Bitdefender Safepay™ är tillgänglig. I det här fallet är hotspot-skydd för osäkra nätverk aktiverat som standard.

Kontrollera information om Wi-Fi-nätverk

Kontrollera information om de trådlösa nätverk du oftast ansluter till:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SÄKERHETSBRIST** klickar du på **Wi-Fi-säkerhet**.
3. Beroende på vilken information du behöver väljer du en av de tre flikarna, **Hem-Wi-Fi**, **Kontots-Wi-Fi** eller **Publikt Wi-Fi**.
4. Klicka på **Visa information** bredvid det nätverk du vill hitta mer information om.

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

Wi-Fi är osäkert - anger att säkerhetsnivån för nätverket är låg. Det innebär att det är en stor risk att använda det och vi rekommenderar inte att göra betalningar eller kontrollera bankkonton utan extra skydd. I sådana situationer rekommenderar vi att du har Bitdefender Safepay™ med hotspotskydd för osäkra nätverk aktiverat.

Wi-Fi är osäkert - anger att säkerhetsnivån för nätverket är måttlig. Det innebär att det kan finnas säkerhetsbrister och vi rekommenderar inte att göra betalningar eller kontrollera bankkonton utan extra skydd. I sådana situationer rekommenderar vi att du har Bitdefender Safepay™ med hotspotskydd för osäkra nätverk aktiverat.
Wi-Fi är säkert - anger att det nätverk du använder är säkert. I det här fallet kan du använda känslig information för onlineåtgärder.

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

- **Säkert** - här kan du se om det valda nätverket är säkert eller inte. Okrypterade nätverk kan exponera den information du använder.
- **Krypteringstyp** - här kan du visa den krypteringstyp som används av valt nätverk. Vissa krypteringstyper kanske inte är säkra. Därför rekommenderar vi att du kontrollerar informationen om den visade krypteringstypen för att vara säker på att du är skyddad när du surfar på nätet.
- **Kanal/Frekvens** - här kan du visa den kanalfrekvens som används av det valda nätverket.
- **Lösenordsstyrka** - här kan du visa hur starkt lösenordet är. Observera att de nätverk som har svaga lösenord utgör en måltavla för cyberbrottslingar.
- **Typ av inloggning** - här kan du visa om valt nätverk är skyddat av ett lösenord eller inte. Vi rekommenderar att du endast ansluter till nätverk som har konfigurerat starka lösenord.
- **Autentiseringstyp** - här kan du visa den autentiseringstyp som används av valt nätverk.

4.7. Video- och ljudskydd

Fler och fler hot designas för att komma åt inbyggda webbkameror och mikrofoner. För att förhindra obehörig åtkomst till din webbkamera och för att informera dig om vilka obetrodda appar som kommer åt din enhets mikrofon och när, har Bitdefender Video- och ljud inkluderat:

- Webbkameraskydd
- Mikrofonövervakning

4.7.1. Webbkameraskydd

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 appars behörigheter, inaktivera enhetens inbyggda kamera eller att täcka över den är inte så praktiskt. För att förhindra ytterligare försök att komma åt din integritet övervakar Bitdefender Webcam Protection permanent de appar som försöker få åtkomst til kameran och blockerar dem som inte listade som betrodda.

Som en säkerhetsåtgärd vill du bli meddelad varje gång en ej betrodd app försöker få åtkomst till din kamera.

Aktivera eller inaktivera webbkameraskydd

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Inställningar**.
3. Slå av eller på motsvarande omkopplare i fönstret **Webbkamera**.

Konfigurera webbkameraskydd

Du kan konfigurera vilka regler som ska tillämpas när en app försöker få tillgång till din kamera genom att följa de här stegen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Inställningar**.
3. Välj fliken **Webbcam**.

Följande alternativ är tillgängliga:

Regler för programblockering

- **Blockera all åtkomst till webbkameran** - ingen app tillåts få åtkomst till webbkameran.
- **Blockera webbläsarnas åtkomst till webbkameran** - ingen webbläsare förutom Internet Explorer och Microsoft Edge får åtkomst till webbkameran. På grund av Windows Stores procedur att köra i en process kan Internet Explorer och Microsoft Edge inte upptäckas av Bitdefender som webbläsare och är därför undantagna från den här inställningen.
- **Konfigurera behörigheter baserat på gemensamma val** - om majoriteten av Bitdefender-användarna anser att en populär app är ofarlig, så sätts

dess åtkomst till webbkameran automatiskt till Tillåt. Om en populär app anses vara farlig av många, kommer dess åtkomst automatiskt att anges till Blockerad.

Du informeras varje gång någon av dina installerade appar listas som blockerad av majoriteten av Bitdefender-användarna.

Aviseringar

- **Meddela när tillåtna program ansluter till webbkameran** - du meddelas varje gång en tillåten app öppnar webbkameran.

Lägga till appar till listan Webbkameraskydd

Appar som försöker ansluta till din webbkamera hittas automatiskt och beroende på deras beteende och communityns val, tillåts eller nekas åtkomst. Du kan dock manuellt börja konfigurera på egen hand vilken åtgärd som ska vidtas genom att följa de här stegen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Webbkameraåtkomst**.
3. Första gången du öppnar Webbkameraskydd presenteras du för funktionen.
4. Klicka på önskad länk:
   - **Välj Windows Store-appar att lägga till i behörighetslistan** - en lista med upptäckta Windows Store-appar visas. Slå på omkopplarna bredvid de appar du vill lägga till i listan.
   - **Börja lägga till program till webbkamerans åtkomstlista** - gå till den .exe-fil du vill lägga till i listan och klicka sedan på **OK**.

     För att lägga till ytterligare appar klickar du på länken **Lägg till nytt program i listan**.

För att visa vad Bitdefender-användarna har valt att göra med den valda appen klickar du på -ikonen.

Apparna som begär åtkomst till din kamera tillsammans med den senaste aktiviteten visas i det här fönstret.

Du meddelas varje gång en av de tillåtna apparna blockeras av Bitdefender-användare.

Stoppa åtkomst till webbkameran för en tillagd app genom att klicka på ikonen  . Ikonen växlar till  , vilket innebär att den valda appen inte har åtkomst till webbkameran.

4.7.2. Mikrofonskärm

Falska appar kan komma åt din inbyggda mikrofon i tysthet eller i bakgrunden med ditt samtycke. För att göra dig medveten om eventuella skadliga exploateringar meddelar Bitdefender-mikrofonövervakare dig om sådana händelser. På så sätt får ingen app åtkomst till mikrofonen utan att du bestämmer det.

Slå på eller av mikrofonövervakning

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Inställningar**.
3. Välj fliken **Mikrofon**.
4. Slå av eller på motsvarande omkopplare i fönstret **Mikrofon**.

Konfigurera aviseringar för mikrofonövervakning

Konfigurera vilka aviseringar som ska visas när appar försöker få åtkomst till mikrofonen genom att följa de här stegen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Inställningar**.
3. Välj fliken **Mikrofon**.

Aviseringar

- **Meddela när ett program försöker komma åt mikrofonen**
- **Meddela när webbläsare kommer åt mikrofonen**
- **Meddela när obehöriga appar använder mikrofonen**
- **Visa meddelande baserat på Bitdefender-användarnas val**

Lägga till appar på mikrofonövervakningslistan

Appar som försöker ansluta till mikrofonen upptäcks automatiskt och läggs till i aviseringslistan. Du kan dock manuellt konfigurera på egen hand om en avisering ska visas eller inte genom att följa de här stegen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VIDEO- OCH LJUDSKYDD** klickar du på **Mikrofonövervakning**.
3. Första gången du öppnar Mikrofonövervakning presenteras du för funktionen.
4. Klicka på önskad länk:
   - **Välj Windows Store-appar att lägga till i listan** - en lista med upptäckta Windows Store-appar visas. Slå på omkopplarna bredvid de appar du vill lägga till i listan.
   - **Börja lägga till program till listan** - gå till den .exe-fil du vill lägga till i listan och klicka sedan på **OK**.

     För att lägga till ytterligare appar klickar du på länken **Lägg till nytt program i listan**.

För att visa vad Bitdefender-användarna har valt att göra med den valda appen klickar du på -ikonen.

Apparna som begär åtkomst till din mikrofon tillsammans med den senaste aktiviteten visas i det här fönstret.

För att sluta ta emot aviseringar avseende aktivitet för en tillagd app klickar du på ikonen . Ikonen blir , vilket innebär att ingen Bitdefender-avisering visas när vald app försöker nå din mikrofon.

4.8. Safe Files

Ransomware är skadlig programvara som attackerar sårbara system genom att låsa dem och be om pengar för att låta användaren få tillbaka kontroll över sitt system. Sådan här skadlig programvara agerar smart genom att visa falska meddelanden för att skrämma användaren och tvinga denne att gå vidare med betalningen.

Infektionen kan spridas via spam e-post, genom att ladda ned bilagor eller genom att besöka smittade webbplatser och installera skadliga program utan att låta användaren veta vad som händer på systemet.

Ransomware kan ha ett av följande beteenden för att förhindra användaren att komma åt sitt system:

- Krypterar känsliga och personliga filer utan möjligheten att dekryptera tills en lösen betalas av offret.
- Låser datorns skärm och visar ett meddelande som ber om pengar. I det här fallet är ingen fil krypterad, men användaren är tvungen att fortsätta med betalningen.
- Blockerar appar från att köras.

Med Bitdefender Safe Files kan du hålla personliga filer, som dokument, foton eller filmer skyddade från ransomwareattacker.

Notera
Advanced Threat Defense och Safe Files är två lager skydd som skyddar mot ransomware. Advanced Threat Defense är funktionen som stoppar ransomwareattacker när de spårar systemets kritiska områden, medan Safe Files ser till att ingen viktig fil på datorn krypteras.

4.8.1. Aktivera och inaktivera Safe Files

Aktivera och inaktivera funktionen Safe Files:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SAFE FILES** aktiverar eller inaktiverar du omkopplaren.

Varje gång en app försöker öppna en av de skyddade filerna visas en Bitdefender-popupruta. Du kan tillåta eller blockera åtkomst.

Notera
Funktionen Safe Files är som standard inte aktiverad.

4.8.2. Skydda personliga filer från ransomwareattacker

Om du vill placera personliga filer i ett skydd:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SAFE FILES** klickar du på **Skyddade mappar**.

3. Första gången du öppnar Skyddade mappar presenteras du för funktionen. Klicka på **SKYDDA FLER MAPPAR** för att fortsätta.
4. Välj den mapp du vill skydda och klicka sedan på **OK**.

   Klicka på länken **Skydda fler mappar** för att lägga till ytterligare mappar. Alternativt så drar du mappar till det här fönstret.

Som standard skyddas mapparna Bilder, Videor, Dokument och Musik mot hotattacker. Personlig information som lagras i onlinefiltjänster som Box, Dropbox, Google Drive och OneDrive omfattas också av skyddsmiljö, förutsatt att deras appar är installerade på systemet.

För att undvika att systemet blir långsammare rekommenderar vi att du lägger till som mest 30 mappar eller sparar flera filer i en mapp.

Notera
Anpassade mappar kan endast skyddas för aktuella användare. System- och appfiler kan inte läggas till som undantag.

4.8.3. Konfigurera appåtkomst

De appar som försöker ändra eller ta bort skyddade filer kan flaggas som potentiellt osäkra och läggas till i listan Blockerade appar. Om en sådan app blockeras och du är säker på att dess beteende är normalt, kan du tillåta den genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **SAFE FILES** klickar du på **Programåtkomst**.
3. Apparna som har begärt att ändra filer i dina skyddade mappar listades. Aktivera omkopplaren bredvid den app du vet är säker.

I samma fönster kan du inaktivera ransomwareskydd för specifika appar genom att inaktivera motsvarande omkopplare.

Om du vill lägga till nya appar i listan klickar du på länken **Lägg till nytt program i listan**.

4.8.4. Skydd vid start

Det är känt att många skadliga appar är konfigurerade att köras vid systemstart, något som allvarligt kan skada en maskin. Bitdefenders starttidsskydd skannar alla viktiga systemområden innan alla filer laddas, utan att systemet påverkas.

Inaktivera skydd vid start:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **SAFE FILES**-panelen klickar du på **Inställningar**.
3. Inaktivera **Skydd vid start**.

Notera
Appar som läggs till i undantag skannas och behandlas utifrån det.

4.9. Avhjälpning av ransomware

Bitdefender Ransomware Remediation säkerhetskopierar filer som dokument, bilder, videor eller musik för att se till att de skyddas från att skadas eller förloras i händelse av ransomwarekryptering. Varje gång en ransomwareattack upptäcks blockerar Bitdefender alla processer som är inblandade i attacken och startar avhjälpningsprocessen. På så sätt kan du återställa innehållet för alla dina filer utan att betala den begärda lösensumman.

4.9.1. Aktivera eller inaktivera ransomwareavhjälpning

Aktivera eller inaktivera ransomwareavhjälpning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** aktiverar eller inaktiverar du omkopplaren.

Notera
För att säkerställa att dina filer är skyddade mot ransomware rekommenderar vi att du har Avhjälpning av ransomware aktiverat.

4.9.2. Aktivera eller inaktivera automatisk återställning

Med Automatisk återställning kan du se till att dina filer återställs automatiskt i händelse av ransomwarekryptering.

Aktivera eller inaktivera automatisk återställning:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** klickar du på **Inställningar**.
3. Aktivera eller inaktivera omkopplaren **Automatisk återställning**.

4.9.3. Visa filer som har återställts automatiskt

När alternativet **Automatisk återställning** är aktiverat återställer Bitdefender automatiskt filer som krypterats av ransomware. På så sätt kan du ha en bekymmersfri datorupplevelse och veta att dina filer är säkra.

Visa filer som har återställts automatiskt:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** markerar du meddelandet avseende det senast upptäckta ransomwarebeteendet som avhjälpts och klickar sedan på **Återställda filer**.

   Listan med återställda filer visas. Här kan du även visa platsen dit dina filer har återställts.

4.9.4. Återställa krypterade filer manuellt

Ifall du manuellt måste återställa filer som krypterats av ransomware följer du de här stegen:

1. Klicka på **Meddelanden** på navigeringsmenyn i Bitdefender-gränssnittet.
2. På fliken **Alla** markerar du information avseende det senast upptäckta ransomwarebeteendet som upptäckts och klickar sedan på **Krypterade filer**.
3. Listan med krypterade filer visas.

   Klicka på **ÅTERSTÄLL FILER** för att fortsätta.
4. Ifall hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de avkrypterade filerna ska sparas. Klicka på **ÅTERSTÄLL PLATS** och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.

   Klicka på **SLUTFÖR** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas ifall 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;

4.9.5. Lägga till program till undantag

Du kan konfigurera undantagsregler för betrodda appar så att funktion Avhjälpning av ransomware inte blockerar dem om de utför ransomwareliknande åtgärder.

Lägga till appar till undantagslistan för avhjälpning av ransomware:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** klickar du på **Undantag**.
3. Om du vill lägga till appar i listan klickar du på **Lägg till ett nytt program i listan**.

4.10. Filkryptering

Bitdefender Filkryptering tillåter dig att skapa krypterade, lösenordsskyddade logiska enheter (eller valv) på din dator, där du säkert kan lagra dina hemliga och känsliga dokument. Informationen som lagras i valven kan endast nås av användare som kan lösenordet.

Detta lösenord tillåter dig att öppna, lagra data och stänga ett valv samtidigt som du upprätthåller dess säkerhet. När ett valv är öppet, kan du lägga till nya filer, få tillgång till nuvarande filer eller ändra dem.

Den verkliga placeringen för valvet är lokalt på hårddisken med filändelsen .bvd. Även om de fysiska filerna, som valven representerar, kan nås från andra operativsystem (som Linux), kan informationen som lagrats på dem inte läsas eftersom den är krypterad.

Filvalv kan hanteras från Bitdefender-fönstret eller genom att använda Windows kontextmeny och logisk enhet kopplad till valvet.

4.10.1. Hantera filvalv

Hantera din filvalv från Bitdefender:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Inställningar**.

   De befintliga filvalven visas i det här fönstret.

4.10.2. Skapa filvalv

Skapa ett nytt valv:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Skapa nytt filvalv**.
3. Ange namn och plats för filvalvet.
   - Skriv namnet på filvalvet i motsvarande fält.
   - Klicka **BLÄDDRA**, välj plats för valvet och spara valvfilen under valt namn.
4. Välj en enhetsbokstav från motsvarande meny. När du öppnar valvet kommer en virtuell hårddisk märkt med den valda bokstaven att visas under Min Dator.
5. Om du vill ändra standardstorleken (100 MB) för valvet använder du upp- och nedpilarna från stegningsrutan **Valvstorlek**.
6. Skriv in valvets önskade lösenord i fälten **Lösenord Bekräfta lösenord**. Lösenordet måste innehålla minst 8 tecken. Alla som försöker öppna valvet och komma åt dess filer måste ange lösenordet.
7. Klicka på **SKAPA**.

Bitdefender kommer direkt att informera dig om aktivitetens resultat. Om ett fel inträffat, använd felmeddelandet till att felsöka problemet.

Skapa ett valv snabbare genom att högerklicka på skrivbordet eller i en mapp på datorn, peka på **Bitdefender** > **Bitdefender Filvalv** och välj **Skapa filvalv**.

Notera
Det kan vara praktiskt att spara alla filvalv på samma plats. På det här sättet kan du hitta dem snabbare.

4.10.3. Importera ett filvalv

Importera ett filvalv som är lagrat lokalt:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Importera valv**.
3. Sök efter ditt valv och markera det (.bvd-filen).
4. Klicka **Öppna**.

4.10.4. Öppna filvalv

För att få tillgång till och jobba med filer som lagrats i ett valv måste du öppna valvet. När du öppnar valvet kommer en virtuell disk/enhet bli tillgänglig i Utforskaren/Den här datorn. Enheten är märkt med enhetsbokstaven som är tilldelad valvet.

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Inställningar**.
3. Välj det valv du vill öppna och klicka sedan på **LÅS UPP**.
4. Skriv lösenordet och klicka sedan på **OK**.
5. Klicka på **ÖPPNA** för att öppna valvet.

Bitdefender kommer direkt att informera dig om aktivitetens resultat. Om ett fel inträffat, använd felmeddelandet till att felsöka detta.

Öppna ett valv snabbare genom att leta upp .bvd-filen som representerar det valv du vill öppna. Högerklicka på filen, peka på **Bitdefender** > **Bitdefender Filvalv** och välj **Lås upp**. Skriv lösenordet och klicka sedan på **OK**.

4.10.5. Lägga till filer i valv

Du måste öppna valvet innen du kan lägga till filer eller kataloger i valvet.

Lägga till nya filer till dina valv:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Inställningar**.
3. Välj det valv du vill lägga till filer i och klicka på **LÅS UPP**.
4. Skriv lösenordet och klicka sedan på **OK**.
5. Klicka på **ÖPPNA** för att öppna valvet.
6. Lägg till filer eller mappar som du normalt gör i Windows (du kan till exempel kopiera och klistra in).

Lägg till filer och mappar snabbare i valvet genom att högerklicka på den fil eller mapp du vill kopiera till ett valv, peka på **Bitdefender** > **Bitdefender Filvalv** och välj **Lägg till i filvalv**.

- Om endast ett valv är öppet, kopieras filen eller mappen direkt till det valvet.

- Om flera valv är öppna kommer du att ombes att välja vilket valv föremålet ska kopieras till. Välj enhetsbokstav som motsvarar det önskade valvet och klicka **OK** för att kopiera objektet.

4.10.6. Låsa valv

När du arbetat färdigt i ett filvalv måste du låsa det för att skydda dina data. Genom att låsa valvet försvinner den motsvarande virtuella hårddisken från Min Dator. Följaktligen är tillgången till informationen i valvet helt blockerad.

Låsa ett valv:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Inställningar**.
3. Välj det valv du vill låsa och klicka sedan på **LÅS**.

Bitdefender kommer direkt att informera dig om aktivitetens resultat. Om ett fel inträffat, använd felmeddelandet till att felsöka problemet.

För att låsa ett valv snabbare klickar du på .bvd-filen som motsvarar valvet, pekar på **Bitdefender** > **Bitdefender File Vault** och väljer **Lås**.

4.10.7. Ta bort filer från valv

För att kunna ta bort filer och mappar från ett valv, måste valvet vara öppet. Ta bort filer eller mappar från ett valv:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Inställningar**.
3. Välj det valv du vill ta bort filer ifrån och klicka sedan på **LÅS UPP** ifall det är låst.
4. Klicka på **ÖPPNA**.

   Ta bort filer eller mappar på samma sätt som du normalt göt i Windows (till exempel, högerklicka en fil du vill radera och välj **Radera**).

4.10.8. Ändra valvlösenord

Lösenordet skyddar ett valvs innehåll från obehörig tillgång Endast användare som känner till lösenordet kan öppna valvet och få tillgång till de dokument och data som är lagrade inuti det.

Valvet måste låsas innan du kan ändra dess lösenord. Ändra lösenordet till ett valv:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FILKRYPTERING** klickar du på **Inställningar**.
3. Välj det valv som du vill ändra lösenord för och klicka därefter på **INSTÄLLNINGAR**.
4. Skriv in valvets nuvarande lösenord i fältet **Gammalt lösenord**.
5. Skriv in valvets nya lösenord i fälten **Nytt lösenord Bekräfta nytt lösenord**.

> **Notera**
> Lösenordet måste innehålla minst 8 tecken. För ett starkt lösenord, använd en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, $ eller @).

Bitdefender kommer direkt att informera dig om aktivitetens resultat. Om ett fel inträffat, använd felmeddelandet till att felsöka problemet.

Ändra lösenordet för ett valv snabbare genom att leta upp .bvd-filen som representerar valvet på datorn. Högerklicka filen, peka på **Bitdefender** > **Bitdefender Filvalv** och välj **Ändra lösenord till valvet**.

4.11. Lösenordshanteringsskydd för dina inloggningsuppgifter

Vi använder våra datorer för att shoppa online eller betala räkningar, för att ansluta till sociala media-plattformar eller logga in med snabbmeddelandeappar.

Men som alla vet är det inte alltid så lätt att komma ihåg lösenordet!

Och om vi inte är försiktiga när vi surfar online kan vår privata information, som e-postadress, snabbmeddelande-ID eller kreditkortsinformation komprometteras.

Att ha sina lösenord eller personuppgifter på ett papper eller i datorn kan vara farligt, eftersom de kan hittas och användas av andra personer som vill stjäla och använda den informationen. Och det är inte så lätt att komma ihåg alla lösenord du ställt in för dina onlinekonton eller för dina favoritwebbsidor.

Finns det därför något sätt för att vi ska vara säkra på att vi hittar våra lösenord när vi behöver dem? Och kan vi lita på att våra hemliga lösenord alltid är säkra?

lösenordshanterare hjälper dig att hålla reda på dina lösenord, skyddar din integritet och ger en säker surfupplevelse.

Genom att använda ett enda huvudlösenord för att komma åt dina inloggningsuppgifter gör Password Manager det enkelt för dig att ha dina lösenord säkra i en plånbok.

Password Manager är integrerat med Bitdefender Safepay™ för att erbjuda det bästa skyddet för dina onlineaktiviteter och ger en enhetlig lösning för de olika sätt på vilka din privata information kan komprometteras.

Password Manager skyddar följande privata information:

- Personlig information, som e-postadress eller telefonnummer
- Inloggningsuppgifter för webbplatserna
- Bankkontoinformation eller kreditkortsnummer
- Komma åt data till e-postkonton
- Lösenord till apparna
- Lösenord för Wi-Fi-nätverken

4.11.1. Skapa en ny plånboksdatabas

Bitdefender Wallet är platsen där du kan lagra din personliga information. För en enklare surfupplevelse måste du skapa en plånboksdatas så här:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **PASSWORD MANAGER** fliken, klicka på **Skapanyplånbok**.
3. Klicka på **Skapa ny**.
4. Skriv in den önskade informationen i de motsvarande fälten.
   - Plånboksetikett - skriv ett unikt namn för din plånboksdatabas.
   - Huvudlösenord - skriv ett lösenord för din plånbok.
   - Skriv lösenordet igen - skriv in det lösenord du angav igen.
   - Ledtråd - skriv en ledtråd för att komma ihåg lösenordet.
5. Klicka på **FORTSÄTT**.

6. I det här steget kan du välja att lagra din information i molnet. Om du väljer Ja lagras bankinformation lokalt på din enhet. Välj önskat alternativ och klicka på **FORTSÄTT**.
7. Välj den webbläsare du vill importera inloggningsuppgifter från.
8. Klicka på **SLUTFÖR**.

4.11.2. Importera en befintlig databas

Importera en plånbok lagrad lokalt:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **PASSWORD MANAGER** fliken, klicka på **Skapanyplånbok**.
3. Klicka på **FRÅN MÅL**.
4. Gå till den plats på enheten där du vill spara plånboksdatabasen och välj sedan ett namn för den.
5. Klicka **Öppna**.
6. Ge ett namn åt din plånbok och skriv in det lösenord du tilldelade när den skapades första gången.
7. Klicka på **IMPORTERA**.
8. Välj de program du vill att plånboken ska importera inloggningsuppgifter från och sedan knappen **SLUTFÖR**.

4.11.3. Exportera plånboksdatabasen

Exportera plånboksdatabasen:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Mina plånböcker**.
3. Klicka på ⋮ -ikonen i önskad plånbok och välj sedan **Exportera**.
4. Sök på platsen för din plånboksdatabas och välj den (.dtb-filen).
5. Klicka **Spara**.

Notera
Plånböckerna måste vara öppna för att **Exportera**-funktionen ska vara tillgänglig.

Om den plånbok du behöver exportera är låst klickar du på **AKTIVERA PLÅNBOK** och skriver därefter i det lösenord som tilldelades när den skapades första gången.

4.11.4. Synkronisera plånböckerna i molnet

Aktivera eller inaktivera plånbokssynkronisering i molnet:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Mina plånböcker**.
3. Klicka på ⋮ -ikonen i önskad plånbok och välj sedan **Inställningar**.
4. Välj det önskade alternativet i det fönster som visas och klicka sedan på **Spara**.

Notera
Plånböckerna måste vara öppna för att **Exportera**-funktionen ska vara tillgänglig.
Om den plånbok du behöver synkronisera är låst klickar du på **AKTIVERA PLÅNBOK** och skriver därefter i det lösenord som tilldelades när den skapades första gången.

4.11.5. Hantera dina plånboksinloggningsuppgifter

Hantera dina lösenord:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Mina plånböcker**.
3. Välj den önskade plånboksdatabasen och klicka sedan på **AKTIVERA PLÅNBOK**.
4. Skriv huvudlösenordet och klicka sedan på **OK**.

Ett nytt fönster visas. Välj önskad kategori från den övre delen i fönstret:

- Identitet
- Webbsidor
- Internetbank
- E-postmeddelanden
- Appar

- Wi-Fi-nätverk

Lägga till/redigera inloggningsuppgifter

- Lägg till ett nytt lösenord genom att välja önskad kategori överst, klicka på **+ Lägg till objekt**, infoga informationen i motsvarande fält och klicka på Spara.
- För att redigera en post i tabellen, välj den och klicka på **Redigera** knappen.
- Ta bort en post genom att markera den och klicka på **Ta bort** .

4.11.6. Aktivera eller inaktivera Password Manager-skyddet

Aktivera eller inaktivera Password Manager-skyddet:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** aktiverar eller inaktiverar du omkopplaren.

4.11.7. Hantera inställningarna för Password Manager

Konfigurera huvudlösenordet i detalj:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fliken **Säkerhetsinställningar**.

Följande alternativ är tillgängliga:

- **Fråga om mitt huvudlösenord när jag loggar in till min enhet** - du ombes att infoga ditt huvudlösenord när du öppnar enheten.
- **Fråga om mitt huvudlösenord när jag öppnar mina webbläsare och appar** - du ombes att infoga ditt huvudlösenord när du öppnar en webbläsare eller en app.
- **Fråga inte efter mitt huvudlösenord** - du kommer inte att tillfrågas om ditt huvudlösenord när du öppnar datorn, en webbläsare eller en app.
- **Lås automatiskt plånbok när jag lämnar min enhet utan uppsikt** - du uppmanas att infoga ditt huvudlösenord när du återgår till enheten efter 15 minuter.

Viktigt
Kom ihåg ditt huvudlösenord eller förvara det på en säker plats. Om du glömmer bort lösenordet måste du ominstallera programmet eller kontakta Bitdefender för support.

Förbättra din upplevelse

Välj de mappar eller appar där du vill integrera Password Manager:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fliken **Insticksprogram**.

   Markera en app för att använda Password Manager och förbättra din upplevelse:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Säker betalning

Konfigurera Automatisk ifyllnad

Funktionen Automatisk ifyllnad gör det enkelt att ansluta till dina favoritwebbsidor eller logga in med dina onlinekonton. Första gången du anger dina inloggningsuppgifter och personliga information i webbläsaren är de automatiskt säkrade i plånboken.

Konfigurera inställningarna för **Automatisk ifyllnad**:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fliken **Inställningar för Automatisk ifyllnad**.
4. Konfigurera följande alternativ:
   - **Konfigurera hur plånboken håller dina inloggningsuppgifter säkra**:
     - **Spara inloggningsuppgifter automatiskt i plånboken** - inloggningsuppgifter och annan identifierbar information som person- och kreditkortsuppgifter sparas automatiskt och uppdateras i plånboken.

- **Fråga mig varje gång** - du tillfrågas varje gång du om du vill lägga till dina uppgifter i plånboken.
- **Spara inte, jag uppdaterar informationen manuellt** - inloggningsuppgifterna kan endast läggas till manuellt i plånboken.

- **Fyll i inloggningsuppgifter automatiskt**:
  - **Fyll i inloggningsuppgifter automatiskt varje gång** - inloggningsuppgifterna infogas automatiskt i webbläsaren.
- **Fyll i formulär automatiskt**:
  - **Fråga efter mina ifyllningsalternativ när jag besöker en sida med formulär** - en popupruta med ifyllningsalternativen visas varje gång Bitdefender upptäcker att du vill utföra en onlinebetalning eller registrera dig.

Hantera Password Manager-information från webbläsaren

Du kan enkelt hantera Password Manager-information direkt från webbläsaren för att ha all viktig information till hands. Tillägget Bitdefender-plånbok stöds av följande webbläsare: Google Chrome, Internet Explorer och Mozilla Firefox, och är även integrerat med Safepay.

För att komma till Bitdefender-plånboken öppnar du webbläsaren, tillåter att tillägget installeras och klickar på -ikonen i verktygsfältet.

Tillägget Bitdefender-plånbok innehåller följande alternativ:

- Öppna plånbok - öppnar plånboken.
- Lås plånbok - låser plånboken.
- Webbsidor - öppnar en undermeny med alla webbplatsinloggningar sparade i plånboken. Klicka på **Lägg till webbsida** för att lägga till nya webbplatser i listan.
- Fyll i formulär - öppnar en undermeny som innehåller den information du lagt till för en särskild kategori. Härifrån kan du lägga till nya uppgifter i plånboken.
- Lösenordsgenerator - gör att du kan generera slumpmässiga lösenord du kan använda för befintliga konton. Klicka på **Visa avancerade inställningar** för att anpassa komplexiteten för lösenordet.
- Inställningar - öppnar inställlningsfönstret för lösenordshanteraren.

- Rapportera problem - rapportera alla problem du stöter på med Bitdefenders lösenordshanterare.

4.12. Anti-tracker

Många webbplatser du besöker använder spårningsverktyg 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. På så sätt tjänar webbplatsägare pengar för att kunna ge dig innehåll utan kostnad eller fortsätta vara verksamma. Förutom att samla in information kan spårningsverktyg göra din surfupplevelse långsammare eller slösa på bandbredd.

Med tillägget Bitdefender Anti-tracker aktiverat i webbläsaren undviker du att bli spårad så att dina data fortsätter att vara privata medan du surfar online och du ökar hastigheten som webbplatserna behöver för att läsas in.

Bitdefender-tillägget är kompatibelt med följande webbläsare:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

De spårningsverktyg vi hittar grupperas i följande kategorier:

- **Reklam** - används för att analysera webbsidestrafik, användarbeteende eller besökares trafikmönster.
- **Kundinteraktion** - används för att mäta användarinteraktion med olika inmatningsformulär som chatt eller support.
- **Viktigt** - används för att övervaka viktiga webbsidesfunktioner.
- **Sidanalys** - används för att samla in data avseende webbsidesanvändning.
- **Sociala medier** - används för att övervaka social målgrupp, aktivitet och användarengagemang med olika sociala medieplattformar.

4.12.1. Anti-tracker-gränssnitt

När tillägget Bitdefender Anti-tracker är aktiverad visas ikonen  bredvid sökfältet i webbläsaren. Varje gång du besöker en webbplats ses en räknare på ikonen, som hänvisar till upptäckta och blockerade spårningsverktyg. För att visa mer information om de blockerade spårningsverktygen klickar du

på ikonen för att öppna gränssnittet. Förutom antalet blockerade spårningsverktyg kan du visa den tid som krävs för att sidan ska ladda och kategorierna till vilka de upptäckta spårningsverktygen hör. Klicka på önskad kategori för att visa listan över webbplatser som spårar.

Inaktivera Bitdefender från att blockera spårningsverktyg på den webbplats du besöker genom att klicka på **Pausa skydd på den här webbplatsen**. Den här inställningen gäller endast så länge som du har webbplatsen öppen och återgår till den initiala tillståndet när du stänger webbplatsen.

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

4.12.2. Inaktivera Bitdefender Anti-tracker

Inaktivera Bitdefender Anti-tracker:

- Från din webbläsare:
  1. Öppna webbläsaren.
  2. Klicka på ikonen bredvid adressfältet i webbläsaren.
  3. Klicka på ikonen i det övre högra hörnet.
  4. Använd motsvarande omkopplare för att aktivera eller inaktivera.

     Bitdefender-ikonen blir grå.
- Från Bitdefenders gränssnitt:
  1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **ANTI-TRACKER**-panelen klickar du på **Inställningar**.
  3. Bredvid webbläsaren för vilken du vill inaktivera tillägget slår du av motsvarande omkopplare.

4.12.3. Tillåta att en webbplats spåras

Om du vill bli spårad medan du besöker en viss webbplats kan du lägga till dess adress till undantagen så här:

1. Öppna webbläsaren.
2. Klicka på ikonen bredvid sökfältet.

3. Klicka på ikonen i det övre högra hörnet.
4. Om du är på den webbplats du vill lägga till bland undantagen klickar du på **Lägg till aktuell webbplats i listan**.

   Om du vill lägga till en annan webbplats skriver du in adressen i motsvarande fält och klickar på .

4.13. VPN

VPN-appen kan installeras från din Bitdefender-produkt och användas varje gång du vill lägga till en extra skyddslag till din anslutning. VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter till för att säkra din anslutning, kryptera data med kryptering i bankklass och dölja din IP-adress oavsett var du är. Din trafik omdirigeras via en separat server och gör det därmed näst intill omöjligt att identifiera din enhet bland de myriader av andra enheter som använder våra tjänster. När du är ansluten till Internet via Bitdefender VPN, kan du dessutom ha åtkomst till innehåll som i normala fall är begränsat i vissa områden.

Notera
Vissa länder censurerar Internet och därför kan användning av VPN på deras territorier vara förbjudet enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om regelverken i det land du befinner dig i och de risker du kan utsättas för.

4.13.1. Installera VPN

VPN-appen kan installeras från ditt Bitdefender gränssnitt enligt följande:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **VPN** klickar du på **Installera VPN**.
3. I fönstret med beskrivningen av VPN-appen, läs **Prenumerationsavtalet** och klicka sedan på **INSTALLERA BITDEFENDER VPN**.

   Vänta flera ögonblick tills filerna hämtas och installeras.

   Om en annan VPN-app upptäcks rekommenderar vi att du avinstallerar den. Om du har flera VPN-lösningar installerade kan systemet bli långsammare eller få andra funktionalitetsproblem.

4. Klicka på **ÖPPNA BITDEFENDER VPN** för att avsluta installationsprocessen.

> **Notera**
> Bitdefender VPN kräver att .Net Framework 4.5.2 eller högre är installerat. Om du inte har det här paketet installerat visas ett meddelandefönster. Klicka på **Installera .Net Framework** för omdirigering till en sida där du kan hämta den senaste versionen av den här programvaran.

4.13.2. Öppna VPN

För att komma åt huvudgränssnittet för Bitdefender VPN använder du en av följande metoder:

- Från systemfältet
  1. Högerklicka på -ikonen i systemfältet och klicka sedan på **Visa**.
- Från Bitdefenders gränssnitt:
  1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **VPN**-panelen klickar du på **Öppna VPN**.

4.13.3. VPN-gränssnitt

VPN-gränssnittet visar status för appen, ansluten eller frånkopplad. Serverplatsen för användare med den fria versionen ställs automatiskt av Bitdefender till den lämpligaste servern, medan premium användare har möjlighet att ändra serverplatsen de vill ansluta till. Mer information om VPN-prenumerationer finns i "*Prenumerationer*" (p. 133).

Klicka bara på den status som visas längst upp på skärmen för att ansluta eller koppla ifrån, eller högerklicka på systemfältsikonen. Systemfält ikonen visar ett grönt kontrollmärke när VPN är ansluten och en röd markering när VPN är frånkopplad.

När du är ansluten visas den förflutna tiden och bandbreddsanvändningen under den nedre delen av gränssnittet.

För att få tillgång till fler alternativ går du till **Meny**-området genom att högerklicka på -ikonen på den övre vänstra sidan. Här har du följande alternativ:

- **Mitt Konto** - information om ditt Bitdefender-konto och VPN-prenumeration visas. Klicka på **Växla konto** om du vill logga in med ett annat konto.

- **Inställningar** – beroende på dina behov kan du anpassa produktens beteende:
  - ta emot meddelanden när VPN automatiskt ansluter eller kopplar ifrån
  - kör automatiskt VPN-appen när Windows startas
  - starta automatiskt VPN-appen när enheten ansluter till osäkra trådlösa nätverk
- **Uppgradera till Premium** - om du använder den fria versionen kan du uppgradera till premiumplanen härifrån.
- **Support** - du omdirigeras till vår supportcenterplattform varifrån du kan läsa en användbar artikel om hur du använder Bitdefender VPN.
- **Om** - information om den installerade versionen visas.

4.13.4. Prenumerationer

Bitdefender VPN erbjuder utan kostnad en daglig trafikkovot på 200 MB per enhet för att säkra anslutningen varje gång ditt team behöver det.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en serverplats enligt ditt teams önskemål, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst från panelen **Mina prenumerationer** som finns på ditt Bitdefender-konto.

Bitdefender Premium VPN-prenumerationen är oberoende av den prenumerationen på Bitdefender Small Office Security, vilket innebär att du kan använda den under hela dess tillgänglighet. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Small Office Security fortfarande är aktiv återgår du till gratisversionen.

Bitdefender VPN är en produkt över flera plattformar, tillgänglig i Bitdefender-produkter kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kan du använda din prenumeration på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

4.14. Safepay-säkerhet för onlinetranslationer

Datorn blir snabbt huvudverktyg för att shoppa och utföra bankärenden. Betala räkningar, överföra pengar, köpa i princip allt du kan föreställa dig har aldrig varit snabbare eller enklare.

Det innebär att skicka personlig information, konto- och kreditkortsuppgifter, lösenord och andra typer av privat information över Internet, med andra ord exakt den typ av informationsflöde som cyberbrottslingar är mycket intresserade av att komma över. Hackare är outtröttliga i sina ansträngningar att stjäla den här informationen, så du kan aldrig vara nog försiktig när det gäller säkra onlinetransaktioner.

Bitdefender Safepay™ är först och främst en skydda webbläsare, en förseglad miljö som är utvecklad för att hålla dina bankärende, e-handel och andra typer av onlinetransaktioner privata och säkra.

För bästa integritetsskydd har Bitdefender Password Manager integrerats i Bitdefender Safepay™ för att säkra dina inloggningsuppgifter varje gång du vill öppna privata onlineplatser. Mer information finns på *"Lösenordshanteringsskydd för dina inloggningsuppgifter"* (p. 122).

Bitdefender Safepay™ erbjuder följande funktioner:

- Det blockerar åtkomst till ditt skrivbord och alla försök att ta bilder av din skärm.
- Det skyddar dina hemliga lösenord när du surfar online med Password Manager.
- Den har ett virtuellt tangentbord som när det används, gör det omöjligt för hackare att avläsa tangenttryckningar.
- Den är helt oberoende av dina andra webbläsare.
- Den har inbyggt hotspotskydd som ska användas när datorn är ansluten till osäkra Wi-Fi-nätverk.
- Den har stöd för bokmärken och tillåter att du navigerar mellan dina favoritwebbplatser för bankärenden/shopping.
- Den är inte begränsad till bankärenden och e-handel. Alla webbplatser kan öppnas i Bitdefender Safepay™.

4.14.1. Använda Bitdefender Safepay™

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

För att komma åt huvudgränssnittet för Bitdefender Safepay™ använder du en av följande metoder:

- Från Bitdefender-gränssnittet:
  1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **Safepay**-panelen klickar du på **Öppna Safepay**.
- Från Windows:
  - I **Windows 7**:
    1. Klicka på **Start** och gå till **Alla program**.
    2. Klicka på **Bitdefender**.
    3. Klicka på **Bitdefender Safepay™**.
  - I **Windows 8 och Windows 8.1**:

    Leta upp Bitdefender Safepay™ från Windows Start-skärm (du kan till exempel börja skriva "Bitdefender Safepay™" direkt på Start-skärmen) och därefter klicka på ikonen.
  - I **Windows 10**:

    Skriv "Bitdefender Safepay™" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon.

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

- ange de webbadresser du vill gå till i adressfältet.
- lägg till flikar för att besöka flera webbplatser i Bitdefender Safepay™-fönstret genom att klicka på  .
- navigera tillbaka och framåt och uppdatera sidor med respektive. 
- öppna Bitdefender Safepay™-inställningar genom att klicka på och välja **Inställningar**.
- skydda dina lösenord med Password Manager genom att klicka på  .
- hantera dina bokmärken genom att klicka på  bredvid adressfältet.

- öppna det virtuella tangentbordet genom att klicka på .
- öka eller minska webbläsarens storlek genom att trycka samtidigt på **Ctrl**- och **+/-**-tangenterna på den numeriska knappsatsen.
- visa information om din Bitdefender-produkt genom att klicka på och välja **Om**.
- skriv ut viktig information genom att klicka på och välja **Skriv ut**.

Notera
För att växla mellan Bitdefender Safepay™ och Windows-skrivbordet trycker du på **Alt+Tab**-tangenterna eller klickar på alternativet **Växla till skrivbord** på den övre vänstra sidan av fönstret.

4.14.2. Konfigurera inställningar

Klicka på och välj **Inställningar** för att konfigurera Bitdefender Safepay™:

Domänlista
De webbplatser du lagt till i Bokmärken med alternativet **Öppna automatiskt i Safepay** aktiverat visas här. Om du vill sluta att automatiskt öppna en webbplats från listan med Bitdefender Safepay™, klickar du på × bredvid önskad post från kolumnen **Ta bort**.

Blockera popup-rutor
Du kan välja att blockera popup-rutor genom att klicka på motsvarande omkopplare.

Du kan också skapa en lista över webbplatser att tillåta popup-rutor från. Listan bör endast innehålla webbsidor du litar fullständigt på.

Lägg till en webbplats till listan, ange dess adress i motsvarande fält och klicka på **Lägg till domän**.

Ta bort en webbplats från listan genom att välja X för önskad post.

Hantera plugin-program
Du kan välja om du vill aktivera eller inaktivera specifika insticksprogram i Bitdefender Safepay™.

Hantera certifikat

Du kan importera certifikat från systemet till ett certifikatlager.

Klicka på **IMPORTERA CERTIFIKAT** och följ guiden för att använda certifikaten i Bitdefender Safepay™.

Automatiskt starta virtuellt tangentbord vid lösenordsfält

Det virtuella tangentbordet visas automatiskt när ett lösenordsfält väljs.

Använd motsvarande omkopplare för att aktivera eller inaktivera funktionen.

Be om bekräftelse innan utskrift

Aktivera det här alternativet om du vill bekräfta innan utskriftsprocessen startar.

4.14.3. Hantera bokmärken

Om du har inaktiverat den automatiska upptäckten av vissa eller alla webbplatser eller om Bitdefender helt enkelt inte hittar vissa webbplatser kan du lägga till bokmärken till Bitdefender Safepay™ så att du enkelt kan gå till favoritwebbplatser i framtiden.

Följ de här stegen för att lägga till en webbadress till Bitdefender Safepay™-bokmärken:

1. Klicka på ☆ -ikonen bredvid adressfältet för att öppna bokmärkessidan.

   Notera
   Sidan Bokmärken öppnas som standard när du startar Bitdefender Safepay™.

2. Klicka på **+**-knappen för att lägga till ett nytt bokmärke.
3. Skriv in webbadressen och titel på bokmärket och klicka på **SKAPA**. Markera alternativet **Öppna automatiskt i Safepay** om du vill att den bokmärkta sidan ska öppnas med Bitdefender Safepay™ varje gång du öppnar den. Webbadressen läggs också till i domänlistan på sidan Inställningar.

4.14.4. Inaktivera Safepay-meddelanden

När en bankwebbplats hittas är Bitdefender-produkten inställd på att meddela dig via en popup-ruta.

Inaktivera Safepay-meddelandena:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **Safepay**-panelen klickar du på **Inställningar**.
3. Inaktivera **Safepay-meddelanden**.

4.14.5. Använda VPN med Safepay

För att göra onlinebetalningar i en säker miljö när du är ansluten till osäkra nätverk kan Bitdefender-produkten ställas in för att automatiskt starta VPN-appen samtidigt med Safepay.

Börja använda VPN-appen tillsammans med Safepay:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **Safepay**-panelen klickar du på **Inställningar**.
3. Aktivera **Använd VPN med Safepay**.

4.15. Dataskydd

4.15.1. Radera filer permanent

När du raderar en fil kan den inte längre nås på normalt sätt. Filen är dock fortfarande lagrad på hårddisken tills den skrivs över, då du kopierar nya filer.

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

Du kan snabbt strimla filer eller mappar från datorn med Windows-kontextmenyn genom att följa de här stegen:

1. Högerklicka på den fil eller mapp du vill ta bort permanent.
2. Välj **Bitdefender** > **File Shredder** i kontextmenyn som visas.
3. Klicka på **TA BORT PERMANENT** och bekräfta sedan att du vill fortsätta med processen.

   Vänta medan Bitdefender slutför filborttagning.

4. Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.

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

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **DATASKYDD** klickar du på **File Shredder**.
3. Följ File Shredder-guiden:
   a. Klicka på knappen **LÄGG TILL MAPPAR** för att lägga till filer och mappar du vill ta bort permanent.

      Alternativt drar du dessa filer eller mappar till det här fönstret.

   b. Klicka på **TA BORT PERMANENT** och bekräfta sedan att du vill fortsätta med processen.

      Vänta medan Bitdefender slutför filborttagning.

   c. **Sammanfattning resultat**

      Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.

4.16. Enhetsantistöld

Stöld av bärbara datorer är ett stort problem som påverkar både enskilda personer och organisationer. Förutom att förlora själva hårdvaran kan dataförlusten medföra betydlig skada, både ekonomiskt och känslomässigt.

Ändå är det få personer som vidtar åtgärder för att säkra sina viktiga personliga, affärsmässiga och ekonomiska data i händelse av stöld eller förlust.

Bitdefender Anti-Theft hjälper dig att vara bättre förberedd för en sådan händelse genom att tillåta dig att via fjärrstyrning hitta eller låsa din bärbara dator och till och med radera alla data från den, om du blir av med datorn mot din vilja.

Följande förutsättningar måste uppfyllas för att använda Anti-Theft-funktionerna:

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

Anti-Theft-funktionerna fungerar på följande sätt:

Hitta
Visa din enhets plats på Google Maps.

Riktigheten för platsen beror på hur Bitdefender kan fastställa den. Platsen fastställs till inom tio meter om Wi-Fi är aktiverat på din bärbara dator och det finns trådlösa nätverk inom räckhåll.

Om den bärbara datorn är anslutet till ett trådbundet LAN utan Ei-Fi-baserad plats tillgänglig, fastställs platsen baserat på IP-adressen, som är betydligt mindre noggrann.

Varning
Skicka en fjärrvarning på enheten.

Funktionen är endast tillgänglig på mobilenheter.

Lås
Lås din bärbara dator och ställ in en 4-siffrig PIN-kod för att låsa upp den. När du skickar **Lås**-kommandot startar systemet om och det gr bara att logga tillbaka in i Windows när du har angett den PIN-kod du ställt in.

Om du vill att Bitdefender ska ta foton av den som försöker öppna din bärbara dator, markerar du motsvarande kryssruta. De knäppta bilderna tas med frontkameran och visas tillsammans med tidsstämpeln i antistöld-kontrollpanelen. Endast de två senaste fotona sparas.

Den här åtgärden är endast tillgänglig för bärbara datorer som har en frontkamera.

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

Visa IP
Visar den senaste IP-adressen för den valda enheten. Klicka på **VISA IP** för att göra den synlig.

Antistöld är aktiverat efter installationen och kan öppnas exklusivt genom ditt Bitdefender-konto från en enhet ansluten till Internet, var som helst ifrån.

Använda Antistöld-funktioner

Använd något av följande för att öppna Antistöld-funktionerna:

- Från Bitdefenders huvudgränssnitt:
  1. Klicka på **Verktyg** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. Klicka på **GÅ TILL CENTRAL**.

     Du omdirigeras till Bitdefender Central-sidan. Se till att du är inloggad med dina inloggningsuppgifter.
  3. I det Bitdefender Central-fönster som öppnas klickar du på önskat enhetskort och väljer sedan **Antistöld**.
- På en enhet med Internet-åtkomst:
  1. Öppna en webbläsare och gå till: https://central.bitdefender.com.
  2. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.
  3. Välj panelen **Mina enheter**.
  4. Klicka på önskat enhetskort och välj sedan **Antistöld**.
  5. Välj den funktion du vill använda:

     Visa IP - visa din enhets senaste IP-adress.
     Hitta - visa enhetens plats på Google Maps.
     Varning - skicka en varning på enheten.
     Lås - lås din bärbara dator och ställ in en PIN-kod för att låsa upp den.
     Radera - ta bort alla data från din bärbara dator.

     Viktigt
     När du har raderat en enhet slutar alla Anti-Theft-funktionerna att fungera.

4.17. USB Immunizer

Den inbyggda funktionen Autorun i Windows-operativsystem är ett mycket användbart verktyg som gör att datorer automatiskt kör en fil från de medier som är anslutna till den. Till exempel kan programvaruinstallationer startas automatiskt när en CD sätts in i den optiska enheten.

Tyvärr kan den här funktionen även användas av hot för att automatiskt starta och infiltrera din dator från skrivbara medier, som USB-flashenheter

och minneskort anslutna via kortläsare. Flera Autorun-baserade attacker har skapats de senaste åren.

Med USB Immunizer kan du förhindra att NTFS-, FAT32- eller FAT.formaterade flashenheter från att automatiskt exekvera hot. När en USB-enhet är immuniserad kan inte hot längre konfigurera den för att köra vissa appar när enheten är ansluten till en dator som kör Windows.

Immunisera en USB-enhet:

1. Anslut flashenheten till datorn.
2. Sök på datorn för att hitta den borttagbara lagringsenheten och högerklicka på dess ikon.
3. I kontextmenyn pekar du på **Bitdefender** och väljer **Immunisera den här enheten**.

> **Notera**
> Om enheten redan är immuniserad visas meddelandet **USB-enheten är skyddad mot autorun-baserade hot** istället för alternativet Immunisera.

För att förhindra datorn från att köra hot från ej immuniserade USB-enheter inaktiverar du funktionen för autokörning av medier. Mer information finns på *"Använda automatisk sårbarhetsövervakning"* (p. 104).

5. SYSTEMOPTIMERING

5.1. Verktyg

Bitdefender levereras med ett verktygsavsnitt som hjälper dig att upprätthålla systemets integritet. Underhållsverktyget som erbjuds är avgörande för förbättringen av ditt systems lyhördhet och för effektiv hantering av hårddiskutrymme.

Bitdefender tillhandahåller följande verktyg för optimering av din PC:

- OneClick Optimizer analyserar och förbättrar systemhastigheten genom att köra flera åtgärder med ett enda klicka på en knapp.
- Startup Optimizer sänker systemets uppstartstid genom att stoppa onödiga appar från att laddas när PC:n startar.
- Diskrensning identifierar de filer som kan vara huvudorsak till ditt låga diskutrymme och ger dig möjlighet att bestämma om du vill behålla dem eller inte.

5.1.1. Optimerar din systemhastighet med ett enda klick

Problem som hårddiskfel, överblivna registerfiler och webbläsarhistorik kan göra ditt datorarbete långsammare, vilket kan vara irriterande för dig. Allt detta kan nu åtgärdas med ett enda klick på en knapp.

Med OneClick Optimizer kan du identifiera och ta bort onödiga filer genom att köra flera rensningsåtgärder samtidigt.

Starta OneClick Optimizer-processen:

1. Klicka på **Verktyg** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **OPTIMERA MIN ENHET**.
   a. **Analysera**

      Vänta medan Bitdefender slutför sökandet efter systemproblem.

      - Diskrensning - identifierar onödiga filer och mappar.
      - Registerrensning identifierar och ogiltiga eller utdaterade referenser i Windows-registret.
      - Integritetsrensning - identifierar tillfälliga Internet-filer och cookies, webbläsarcache och historik.

Antal hittade problem visas. Klicka på länken **Visa detaljer** för att granska dem innan du fortsätter med rensningsprocessen. Klicka på **OPTIMERA** för att fortsätta.

b. **Optimera**

Vänta tills Bitdefender avslutas för att optimera ditt system.

c. **Problem**

Det är här du kan se aktivitetsresultat.

Om du vill ha omfattande information om optimeringsprocessen klickar du på knappen **VISA DETALJERAD RAPPORT**.

5.1.2. Optimera din PC:s starttid

Förlängd systemuppstart är ett verkligt problem på grund av appar som är inställda att köras utan att det behövs. Att vänta flera minuter på att systemet ska starta kan kosta värdefull tid och produktivitet.

Fönstret Uppstartsoptimerare visar vilka appar som körs under systemstart och låter dig hantera deras beteende i det här steget.

Starta Uppstartsoptimerarprocessen:

1. Klicka på **Verktyg** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **OPTIMERA ENHETSSTART**.

a. **Välj program**

Du kan se en lista över de appar som körs vid systemstart. Välj de du vill inaktivera eller fördröja vid start.

b. **Communityns val**

Se vad andra Bitdefender-företagsanvändare har beslutat att göra med den app du har valt.

c. **Uppstartstid för systemet**

Kontrollera reglaget längst upp i fönstret för att se hur lång tid som krävs för att både systemet och de valda apparna ska köras vid start.

En systemomstart krävs för att kunna hämta information om uppstartstid för system och appar.

d. **Uppstartsstatus**

- **Aktivera.** Välj det här alternativet när du vill att en app ska köras vid systemstart. Det här alternativet är aktiverat som standard.
- **Fördröj.** Välj det här alternativet för att fördröja att ett program körs vid systemstart. Det betyder att de valda apparna startar med en femminutersfördröjning när användarna har loggat in på systemet. Funktionen **Fördröj** är fördefinierad och kan inte konfigureras av användaren.
- **Inaktivera.** Välj det här alternativet för att inaktivera att ett program körs vid systemstart.

e. **Resultat**

Information som uppskattad systemstarttid efter fördröjning eller inaktivering av program visas.

En omstart av systemet kan krävas för att se all den här informationen.

Klicka **OK** för att spara ändringarna och stänga fönstret.

Notera
Om din prenumeration förfaller eller om du bestämmer dig för att avinstallera Bitdefender återställs de program som du schemalagt för att inte köras vid start till sina standardstartinställningar.

5.1.3. Optimera din disk

Onödiga filer och mappar som tar upp diskutrymme kan göra systemet långsamt. Därför rekommenderas du att förbättra systemhastigheten genom att rensa det med regelbundna intervall.

Bitdefender Disk Cleanup hjälper dig att optimera ditt diskutrymme på ett enkelt sätt genom att identifiera de filer som kan vara huvudorsak till ditt låga diskutrymme. Dessutom har du möjlighet att bestämma vad som ska göras med de identifierade filerna.

Börja rensa ditt system:

1. Klicka på **Verktyg** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Klicka på **RENSA MIN ENHET**.
3. Första gången du använder Diskrensning får du en presentation av funktionen. Klicka **JAG FATTAR** för att fortsätta.

   a. **Diskar och enheter**

Du kan se en lista över tillgängliga diskar. Förutom Windows-diskar skannas externa hårddiskar och USB-enheter och visas i listan. Klicka på **ANALYSERA ENHET** från diskområdet du vill rensa.

b. **Analyserar enhet**

Den valda enheten analyseras. Vänta medan Bitdefender slutför sökandet efter stora filer och mappar.

c. **Problem**

Här kan du visa åtgärdsresultaten. För att välja i vilken ordning resultatet ska visas använder du rullgardinsmenyn **SORTERA EFTER** som finns till vänster om fönstret. Du kan sortera resultatet efter storlek (från 10 MB till mer än 5 GB) eller efter typ (filerna sorteras i separata mappar efter sina tillägg).

Välj de filer du vill ta bort och klicka sedan på **BEKRÄFTA VAL** för att starta raderingsprocessen.

Skyddade och viktiga filer som ansvarar för driften av systemet identifieras också, men kan inte väljas eller tas bort.

Klicka på -ikonen för att få tillgång till de mappar som hör till de valda filerna.

d. **Bekräfta ditt val**

Listan med valda filer visas. Ta en titt och kontrollera igen om du verkligen inte behöver de här filerna längre, eftersom när du går vidare kan de inte återtas från papperskorgen. Bekräfta ditt val genom att klicka på **TA BORT**.

e. **Sammanfattning resultat**

Processens status visas, enligt följande:

Alla valda filer togs bort.
En eller fler av de valda filerna kunde inte tas bort **eller** ingen av de valda filerna kunde tas bort.

Klicka på **SLUTFÖR** för att stänga fönstret.

5.2. Profiler

Dagliga jobbaktiviteter, titta på film eller spela spel kan orsaka att systemet blir långsammare, särskilt om de körs samtidigt med

Windows-uppdateringsprocesser och underhållsåtgärder. Med Bitdefender kan du nu välja och tillämpa din föredragna profil, vilket gör att systemjusteringar anpassas för att öka prestandan för specifika installerade appar.

Bitdefender tillhandahåller följande profiler:

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

Om du bestämmer dig för att inte använda **Profiler**, aktiveras en standardprofil som heter **Standard** och den skapar ingen optimering för ditt system.

Enligt din aktivitet tillämpas följande produktinställningar när profilerna Arbete, Film eller Spel aktiveras:

- Alla Bitdefendervarningar och popups är inaktiverade.
- Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Skräppostfiltret är aktiverat.
- Säkhjälp inaktiveras.
- Meddelanden om specialerbjudanden inaktiveras.

Enligt din aktivitet tillämpas följande systeminställningar när profilerna Arbete, Film eller Spel aktiveras:

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

När den körs i profilen publik Wi-Fi är Bitdefender Total Security inställd på att automatiskt uppnå följande programinställningar:

- Advanced Threat Defense är aktiverat
- Bitdefenders brandvägg är aktiverad och följande inställningar används för din trådlösa adapter:
  - Stöldläge - PÅ
  - Nätverkstyp - Publik
- Följande inställningar från Förebyggande av onlinehot är aktiverade:
  - Krypterad webbskanning
  - Skydd mot bedrägeri
  - Skydd mot nätfiske

5.2.1. Arbetsprofil

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

Konfigurera Arbetsprofil

Konfigurera de åtgärder som ska vidtas när Arbetsprofil används:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Arbetsprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Ökar prestanda på arbetsappar
   - Optimera produktinställningar för arbetsprofil
   - Skjut upp bakgrundsprogram och underhållsuppgifter
   - Skjut upp Windows automatiska uppdateringar
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till appar manuellt till arbetsprofillistan

Om Bitdefender inte automatiskt laddar Jobbprofil när du startar en viss jobbapp, kan du manuellt lägga till appen till **listan Jobbappar**.

Lägga till appar i listan Jobbprogram i Jobbprofil manuellt:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Arbetsprofil.
4. I fönstret **Inställningar av jobbprofil** klickar du på **Programlista**.
5. Klicka på **LÄGG TILL**.

   Ett nytt fönster visas. Bläddra till appens exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

5.2.2. Filmprofil

Att visa högkvalitativt videoinnehåll, som HD-filmer, kräver mycket systemresurser. Filmprofil justerar system- och produktinställningar så att du kan njuta av en oavbruten och smidig filmupplevelse.

Konfigurera filmprofil

Konfigurera de åtgärder som ska vidtas när filmprofil används:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området filmprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på videospelare
   - Optimera produktinställningar för filmprofil
   - Skjut upp bakgrundsprogram och underhållsuppgifter
   - Skjut upp Windows automatiska uppdateringar
   - Justera energiplansinställningar för filmer
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till videospelare till listan Filmprofil manuellt

Om Bitdefender inte automatiskt laddar Filmprofil när du startar en viss videospelarapp, kan du manuellt lägga till appen till **listan Filmappar**.

Lägga till videospelare till listan Filmappar i Filmprofil manuellt:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området filmprofil.
4. I fönstret **Inställningar av filmprofil** klickar du på **Spelarlista**.
5. Klicka på **LÄGG TILL**.

   Ett nytt fönster visas. Bläddra till appens exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

5.2.3. Spelprofil

Att njuta av en oavbruten spelupplevelse handlar om att minska spelbelastningen och minska nedgångar. Genom att använda beteendemässig heuristik tillsammans med en lista med kända spel kan Bitdefender automatiskt upptäcka spel som körs och optimera dina systemresurser så att du kan njuta av din spelstund.

Konfigurera spelprofil

Konfigurera de åtgärder som ska vidtas när spelprofil används:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området spelprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
   - Öka prestanda på spel
   - Optimera produktinställningar för spelprofil
   - Skjut upp bakgrundsprogram och underhållsuppgifter
   - Skjut upp Windows automatiska uppdateringar
   - Justera energiplansinställningar för spel

5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till spel manuellt till spellistan

Om Bitdefender inte automatiskt laddar Spelprofil när du startar ett visst spel eller app, kan du manuellt lägga till appen till **listan Spelappar**.

Lägga till spel i listan Spelappar i Spelprofil manuellt:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området spelprofil.
4. I fönstret **Inställningar av spelprofil** klickar du på **Spellista**.
5. Klicka på **LÄGG TILL**.

   Ett nytt fönster visas. Bläddra till spelets exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

5.2.4. Publik Wi-Fi-profil

Att skicka e-post, skriv in känsliga personuppgifter eller shoppa online medan du är ansluten till osäkra trådlösa nätverk kan utsätta din personliga information för risk. Publik Wi-Fi-profil justerar produktinställningar för att ge dig möjlighet att göra betalningar online och använda känslig information i en skyddad miljö.

Konfigurera publik Wi-Fi-profil

För att konfigurera Bitdefender att använda produktinställningar när du är ansluten till ett osäkert trådlöst nätverk:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** från området Publik Wi-Fi-profil.
4. Låt kryssrutan **Justerar produktinställningar för att öka skyddet när du är ansluten till ett osäkert publikt Wi-Fi-nätverk** vara markerad.
5. Klicka **Spara**.

5.2.5. Batterilägesprofil

Batterilägesprofil är specialdesignad för användare av bärbar dator och surfplatta. Dess syfte är att minimera både system- och Bitdefender-inverkan på strömförbrukning när batteriladdningsnivån är lägre än standard eller den du valt.

Konfigurera Batterilägesprofil

Konfigurera batterilägesprofil:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Klicka på knappen **KONFIGURERA** 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 energiplansinställningar för batteriläge.
   - Inaktivera externa enheter och nätverksportar.
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Skriv in ett giltigt läge i listrutan eller välj ett med upp- och nedpilarna för att ange när systemet ska gå över till batteriläge. Som standard aktiveras läget när batteriladdningsnivån faller lägre än 30 %.

Följande produktinställningar tillämpas när Bitdefender drivs av batterilägesprofilen:

- Bitdefender Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Säkerhetswidget är avstängd.

Bitdefender upptäcker när din bärbara dator har växlat till batterikraft och utifrån batteriladdningsnivån går den automatiskt över till batteriläge. På samma sätt går Bitdefender automatiskt ur Batteriläge när det upptäcker att den bärbara datorn inte längre körs på batteri.

5.2.6. Realtidsoptimering

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

Aktivera eller inaktivera realtidsoptimering:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Gå till fliken **Profiler**.
3. Bläddra ned tills du ser alternativet Realtidsoptimering och använd sedan motsvarande omkopplare för att aktivera eller inaktivera.

6. FELSÖKNING

6.1. Lösa vanliga problem

Det här kapitlet presenterar några problem du kan stöta på när du använder Bitdefender och tillhandahåller dig med möjliga lösningar till dessa problem. De flesta av dessa problem kan lösas genom passande konfigurering av produktinställningarna.

- *"Mitt system verkar vara långsamt"* (p. 154)
- *"Skanningen startar inte"* (p. 155)
- *"Jag kan inte längre använda en app"* (p. 158)
- *"Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker."* (p. 159)
- *"Det här ska du göra om Bitdefender anger en säker app som ransomware"* (p. 159)
- *"Så här uppdaterar du Bitdefender på en långsam Internet-anslutning"* (p. 163)
- *"Tjänsterna för Bitdefender svarar inte"* (p. 164)
- *"Antispamfilter fungerar inte som det ska"* (p. 164)
- *"Funktionen Autofill i min plånbok fungerar inte"* (p. 169)
- *"Bitdefender-borttagning misslyckades"* (p. 170)
- *"Mitt system startar inte efter att ha installerat Bitdefender"* (p. 171)

Om du ej kan finna ditt problem här eller om den valda lösningen inte fungerar kan du kontakta Bitdefender representanter för teknisk support som visat i kapitlet *"Be om hjälp"* (p. 290).

6.1.1. Mitt system verkar vara långsamt

Vanligtvis när man installerat ett säkerhetsprogram, kan det förekomma en liten sänkning av systemhastigheten, detta är i viss grad normalt.

Om du märker en betydande försämring av hastigheten kan bero på något av följande:

- **Bitdefender är inte det enda installerade säkerhetsprogrammet på systemet.**

Även om Bitdefender söker och tar bort funna säkerhetsprogram under installationen, rekommenderas det att man tar bort alla andra säkerhetslösningar du använder innan du installerar Bitdefender. Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 62).

- **Minsta systemkrav för att köra Bitdefender är inte uppfyllda.**

  Om din maskin inte uppfyller de minsta systemkraven, kommer datorn att bli trög, särskilt när flera olika appar körs samtidigt. Mer information finns på *"Minsta systemkrav"* (p. 3).

- **Du har installerat appar du inte använder**.

  Alla datorer har program eller appar som inte används. Och många oönskade program körs i bakgrunden vilket tar upp diskutrymme och minne. Om du inte använder ett program, avinstallera det. Det gäller även för annan förinstallerad programvara eller utvärderingsappar du glömt att ta bort.

  > **Viktigt**
  > Om du misstänker att ett program eller en app är en viktig del av ditt operativsystem tar du inte bort det och kontaktar Bitdefenders kundtjänst för att få hjälp.

- **Ditt system kan vara infekterat**.

  Systemets hastighet och allmänna beteende kan också påverkas av hot. Spionprogramvara, skadlig kod, trojaner och adware belastar alla datorns prestanda. Se till att du skannar systemet regelbundet, minst en gång i veckan. Vi rekommenderar att du använder Bitdefender Systemskanning eftersom den skannar efter alla typer av hot som riskerar säkerheten för ditt system.

  Starta systemskanningen:

  1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
  2. I **ANTIVIRUS**-panelen klickar du på **Systemskanning**.
  3. Följ guidestegen.

6.1.2. Skanningen startar inte

Denna typ av problem kan ha två huvudsakliga orsaker:

- **En tidigare Bitdefenderinstallation som inte var helt borttagen eller en felaktig Bitdefenderinstallation**.

  I det här fallet installer du om Bitdefender:

  - I **Windows 7**:

    1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
    2. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
    3. Klicka på **INSTALLERA OM** i det fönster som visas.
    4. Vänta tills ominstallationen slutförts och starta sedan om ditt system.

  - I **Windows 8 och Windows 8.1**:

    1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
    2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
    3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
    4. Klicka på **INSTALLERA OM** i det fönster som visas.
    5. Vänta tills ominstallationen slutförts och starta sedan om ditt system.

  - I **Windows 10**:

    1. Klicka på **Start**, därefter på Inställningar.
    2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
    3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
    4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
    5. Klicka på **INSTALLERA OM** i det fönster som visas.
    6. Vänta tills ominstallationen slutförts och starta sedan om ditt system.

> **Notera**
> Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

- **Bitdefender är inte den enda installerade säkerhetslösningen på ditt system**.

  I det här fallet:

  1. Ta bort den andra säkerhetslösningen. Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 62).
  2. Installera om Bitdefender:
     - I **Windows 7**:
       a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
       b. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
       c. Klicka på **INSTALLERA OM** i det fönster som visas.
       d. Vänta tills ominstallationen slutförts och starta sedan om ditt system.
     - I **Windows 8 och Windows 8.1**:
       a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
       b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
       c. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
       d. Klicka på **INSTALLERA OM** i det fönster som visas.
       e. Vänta tills ominstallationen slutförts och starta sedan om ditt system.
     - I **Windows 10**:
       a. Klicka på **Start**, därefter på Inställningar.
       b. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
       c. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
       d. Klicka på **Avinstallera** igen för att bekräfta ditt val.
       e. Klicka på **INSTALLERA OM** i det fönster som visas.
       f. Vänta tills ominstallationen slutförts och starta sedan om ditt system.

> **Notera**
> Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.1.3. Jag kan inte längre använda en app

Detta problem inträffar när du försöker använda ett program som fungerade normalt innan du installerade Bitdefender.

När du har installerat Bitdefender kan du stöta på någon av följande situationer:

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

Detta inträffar när Advanced Threat Defense av misstag anger vissa appar som skadliga.

Advanced Threat Defense är en Bitdefender-funktion som hela tiden övervakar de program som körs på ditt system och rapporterar de med potentiellt skadligt beteende. Eftersom den här funktion baseras på ett heuristiskt system kan det finnas fall då legitima appar rapporteras av Advanced Threat Defense.

När den här situationen kan du undanta respektive app från att övervakas av Advanced Threat Defense.

Lägga till en app i undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Inställningar**.
3. I området **Undantag** klickar du på **Lägg till program till undantag**.
4. Hitta och välj den app du vill ska undantas och klicka sedan på **OK**.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

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

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

Om samma sida, domän, IP-adress eller app blockeras flera gånger kan de läggas till i undantagen så att de inte skannas av Bitdefender-motorerna, och därmed säkerställa en smidig surfupplevelse.

Lägga till en webbplats till **Undantag**:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Undantag**.
3. Ange adressen till den blockerade webbplatsen, namnet på domänen, IP-adressen eller onlineappen i motsvarande fält och klicka på **LÄGG TILL**.
4. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Endast webbsidor, domäner IP-adresser och appar du litar på helt ska läggas till i den här listan. Dessa undantas från skanning av följande motorer: hot, nätfiske och bedrägeri.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.1.5. Det här ska du göra om Bitdefender anger en säker app som ransomware

Ransomware är ett skadligt program som försöker tjäna pengar från användarna genom att låsa deras sårbara system. För att hålla systemet säkert för otursamma situationer ger Bitdefender ger dig möjlighet att trygga personliga filer.

När en app försöker ändra eller ta bort en av dina skyddade filer anses den vara osäker och Bitdefender blockerar dess funktionalitet.

Om en sådan app läggs till i listan över ej betrodda appar och du är säker på att den är säker att använda, gör du så här:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.

2. I panelen **SAFE FILES** klickar du på **Programåtkomst**.
3. Apparna som har begärt att ändra filer i dina skyddade mappar listades. Klicka på omkopplaren **Tillåt** bredvid den app du är säker på är säker.

6.1.6. Jag kan inte ansluta till Internet

Du kanske märker att ett program eller en webbläsare inte längre kan ansluta till Internet eller få tillgång till nätverkstjänster efter installation av Bitdefender.

I detta fall är den bästa lösningen att konfigurera Bitdefender att automatiskt tillåta anslutningar till och från respektive program.

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** klickar du på **Inställningar**.
3. I fönstret **Regler** klickar du på **Lägg till regel**.
4. Ett nytt fönster visas där du kan lägga till information. Se till att du väljer alla tillgängliga nätverkstyper och i avsnittet **Behörighet** väljer du **Tillåt**.

Stäng Bitdefender, öppna programmet och försök ansluta till Internet igen.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.1.7. Jag kommer inte åt en enhet på mitt nätverk

Beroende på det nätverk du är ansluten till kan Bitdefenders brandvägg 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 detta fall är den bästa lösningen att konfigurera Bitdefender att automatiskt tillåta anslutningar till och från respektive enhet, enligt följande:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** klickar du på **Inställningar**.
3. I fönstret **Regler** klickar du på **Lägg till regel**.
4. I fönstret **Inställningar** aktiverar du alternativet **Använd denna regel för alla program**.
5. Klicka på fliken **Avancerat**.

6. I rutan **Anpassa fjärradress** skriver du IP-adressen för den dator eller skrivare du vill ha obegränsad åtkomst till.

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

Kontrollera efter andra möjliga orsaker, som följande:

- Den andra datorns brandvägg kan komma att blockera delning av filer och skrivare, med din dator.
  - Om du använder Windows brandvägg kan den konfigureras till att tillåta delning av filer och skrivare enligt följande:
    - I **Windows 7**:
      1. Klicka **Start**, gå till **Kontrollpanel** och välj **System och säkerhet**.
      2. Gå till **Windows Firewall** och klicka sedan på **Tillåt ett program genom Windows Firewall**.
      3. Markera kryssrutan **Fil- och skrivardelning**.
    - I **Windows 8 och Windows 8.1**:
      1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
      2. Klicka på **System och säkerhet**, gå till **Windows Firewall** och välj **Tillåt en app genom Windows Firewall**.
      3. Markera kryssrutan **Fil- och skrivardelning** och klicka därefter på **OK**.
    - I **Windows 10**:
      1. Skriv "Tillåt en app genom Windows Firewall" i sökrutan från aktivitetsfältet och klicka på ikonen.
      2. Klicka **Ändra inställningar**.
      3. I listan **Tillåtna appar och funktioner** markerar du kryssrutan **Fil- och skrivardelning** och klickar därefter på **OK**.
  - Om en annan brandvägg används, se dess tillhörande dokumentation eller hjälpfil.
- Allmänna villkor som kan förhindra användning eller anslutning till den delade skrivaren:

- Du kan behöva logga in som administratör för åtkomst till delad skrivare.
- Behörigheten för den delade skrivaren är inställd för att endast tillåta åtkomst för valda datorer och användare. Om du delar din skrivare, kontrollera tillståndsinställningarna för skrivaren för att se om den andra datorns användare är tillåten tillgång till skrivaren. Om du försöker ansluta till en delad skrivare, kontrollera med den andra datorns användare om du har tillstånd att ansluta till skrivaren.
- Skrivaren som är ansluten till din eller den andra datorn är inte delad.
- Den delade skrivaren har inte lagts till den här datorn.

> **Notera**
> För att lära sig hur man hanterar delning av skrivare (dela en skrivare, ställa in eller ta bort tillstånd för en skrivare, ansluta till en nätverksskrivare eller en delad skrivare), gå till Windows hjälp och supportcenter (i startmenyn, klicka **Hjälp och Support**).

- Tillgång till ett nätverks skrivare kan vara begränsad till vissa datorer eller användare. Du bör alltid kontrollera med nätverksadministratorn om du har tillstånd att ansluta till den skrivaren.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.1.8. Mitt Internet är långsamt

Denna situation kan inträffa efter du installerat Bitdefender. Problemet kan vara orsakat av fel i Bitdefenders brandväggskonfiguration.

Felsök den här situationen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I panelen **BRANDVÄGG** stänger du av omkopplaren för att inaktivera funktionen.
3. Kontrollera om din Internet-anslutning förbättras med Bitdefenders brandvägg inaktiverad.
   - Om du fortfarande har en långsam Internet-anslutning kanske felet inte orsakas av Bitdefender. Du bör kontakta din Internet-tjänstleverantör och verifiera att anslutningen fungerar på deras sida.

Om du får bekräftelse från din Internetleverantör att anslutningen fungerar från deras håll och problemet fortfarande kvarstår, kontakta Bitdefender som beskrivet i sektion *"Be om hjälp"* (p. 290).

- Om internetanslutningen förbättrades efter att Bitdefender-brandväggen inaktiverades:
  a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
  b. I panelen **BRANDVÄGG** klickar du på **Inställningar**.
  c. Gå till fliken **Nätverksadapter** och ställ in din internetanslutning till **Hem/kontor**.
  d. På fliken **Inställningar** stänger du av **Portskanningsskydd**.

     I området **Tyst läge** klickar du på **Redigera stöldinställningar**. Slå på Tyst läge för den nätverksadapter du är ansluten till.
  e. Stäng Bitdefender, starta om systemet och kontrollera internetanslutningshastigheten.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.1.9. Så här uppdaterar du Bitdefender på en långsam Internet-anslutning

Om du har en långsam Internet-anslutning (som uppringd) kan fel inträffa under uppdateringsprocessen.

För att se till att systemet är uppdaterat med den senaste Bitdefender-hotinformationsdatabasen:

1. Klicka på **Inställningar** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Uppdatera**.
3. Inaktivera omkopplaren **Tyst uppdatering** switch.
4. Nästa gång en uppdatering är tillgänglig uppmanas du att välja vilken uppdatering du vill ladda ner. Välj endast **Uppdatering av signaturer**.
5. Bitdefender hämtar och installerar bara hotinformationsdatabasen.

6.1.10. Tjänsterna för Bitdefender svarar inte

Denna artikel hjälper dig att felsöka felet **Bitdefender Tjänster svarar inte**. Du kan få det här problemet på följande sätt:

- Bitdefender-ikonen i systemfältet är utgråad och du informeras om att Bitdefender-tjänsterna inte svarar.
- Bitdefenderfönstret visar att Bitdefenders tjänster inte svarar.

Felet kan vara orsakat av något av följande:

- temporära kommunikationsfel mellan Bitdefendertjänsterna.
- några av Bitdefender tjänster har stoppats
- andra säkerhetslösningar körs på din dator samtidigt som Bitdefender.

För att felsöka detta fel, testa dessa lösningar:

1. Vänta en stund och se om något förändras. Felet kan vara temporärt.
2. Starta om datorn och vänta ett tag tills Bitdefender har laddats. Öppna Bitdefender för att se om felet kvarstår. Omstart av datorn löser oftast problemet.
3. Kontrollera om du har en annan säkerhetslösning installerad då den i så fall kan störa Bitdefender normala aktivitet. Om så är fallet rekommenderar vi dig att ta bort alla andra säkerhetslösningar och sedan installera Bitdefender igen.

   Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 62).

Om felet kvarstår kontaktar du våra supportmedarbetare för hjälp, såsom beskrivs i avsnitt *"Be om hjälp"* (p. 290).

6.1.11. Antispamfilter fungerar inte som det ska

Denna artikel hjälper dig med att felsöka följande problem som rör Bitdefender Skräppost-filtrering:

- En del legitima e-postmeddelanden är märkta som [spam].
- Flera skräppost-meddelanden har inte markerats som skräppost av skräppostfiltret.
- Skräppostfiltret upptäcker inte några skräppost-meddelanden.

Legitima meddelanden märks som [spam]

Legitima meddelanden märks helt enkelt som [spam] för att Bitdefenders skräppostfilter tycker att de ser ut som skräppost. Normalt kan du lösa detta problem genom att anpassa inställningarna för Skräppostfiltret.

Bitdefender lägger automatiskt till mottagarna av dina e-postmeddelanden till Listan över vänner. E-postmeddelanden som tas emot från kontakterna i listan över vänner anses vara legitima. De verifieras inte av skräppost-filtret och märks alltså aldrig som [spam].

Automatisk konfigurering av Listan med vänner hindrar inte upptäckten av fel som kan inträffa i följande situationer:

- Du mottar mycket beställda e-postmeddelanden som ett resultat av att du prenumererar på olika webbsidor. I detta fall är lösningen att lägga till de e-postadresser som du mottar sådana meddelanden från till listan över vänner.
- En stor del av din legitima e-post kommer från människor du aldrig tidigare har haft kontakt med via e-post, såsom kunder, potentiella affärspartners och andra. I detta fall krävs andra lösningar.

  Om du använder en av e-postklienterna som Bitdefender integreras med, ange upptäcktsfel.

  Notera
  Bitdefender integreras in i de vanligaste e-postklienterna genom ett enkelt använt verktygsfält för skydd mot skräppost. En komplett lista över e-postklienter som stöds finns i *"E-postklienter och protokoll som stöds"* (p. 90).

Lägg till kontakter i listan över vänner

Om du använder en stödd e-postklient så kan du enkelt lägga till avsändare av legitima meddelanden till listan över vänner. Följ dessa steg:

1. I din e-postklient väljer du ett e-postmeddelande från den avsändare som du vill lägga till i listan över vänner.
2. Klicka knappen **Lägg till vän** i Bitdefenders verktygsfält för skydd mot skräppost.
3. Du kan bli ombedd att bekräfta de adresser som har lagts till i listan över vänner. Markera **Visa inte detta meddelande igen** och klicka på **OK**.

Du kommer alltid att få e-postmeddelanden från denna adress oavsett innehåll.

Om du använder en annan e-postklient kan du lägga till kontakter i Listan över vänner från Bitdefender gränssnitt. Följ dessa steg:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **SKRÄPPOST**-panelen klickar du på **Hantera vänner**.

   Ett konfigurationsfönster öppnas.
3. Skriv e-postadressen du alltid vill ta emot meddelanden från och klicka på **LÄGG TILL**. Du kan lägga till så många e-postadresser du vill.
4. Klicka **OK** för att spara ändringarna och stänga fönstret.

Anger upptäcktsfel

Om du använder en e-postklient som stöds kan du enkelt korrigera skräppostfiltret (genom att indikera vilka e-postmeddelanden som ska markeras som [spam]). Att göra så hjälper till att förbättra effektiviteten för skräppostfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen skräppost som skräppost-meddelanden flyttas till.
3. Välj det legitima meddelandet som felaktigt märkts som [spam] av Bitdefender.
4. Klicka på knappen **Lägg till vän** i Bitdefenders verktygsfält för skydd mot skräppost för att lägga till avsändaren i Listan över vänner. Du kan behöva klicka **OK** för att bekräfta. Du kommer alltid att få e-postmeddelanden från denna adress oavsett innehåll.
5. Klicka knappen **Inte skräppost** i Bitdefenders verktygsfält mot skräppost (finns normalt i övre delen av e-postklientens fönster). E-postadressen flyttas till mappen Inkorg.

Många skräppostmeddelanden upptäcks inte

Om du får många skräppostmeddelanden som ej märkts som [spam] måste du konfigurera Bitdefenders skräppostfilter för att höja dess effektivitet.

Prova följande lösningar:

1. Om du använder en av e-postklienterna som Bitdefender integreras med, ange ej upptäckta skräppostmeddelanden.

   Notera

   Bitdefender integreras in i de vanligaste e-postklienterna genom ett enkelt använt verktygsfält för skydd mot skräppost. En komplett lista över e-postklienter som stöds finns i *"E-postklienter och protokoll som stöds"* (p. 90).

2. Lägg till spammare i listan över spammare. E-postmeddelanden från adresser i listan över spammare märks automatiskt som [spam].

Visa oupptäckta Skräppost-meddelanden

Om du använder en e-postklient som stöds kan du enkelt markera vilka e-postmeddelanden som skulle markerats som skräppost. Att göra så hjälper till att förbättra effektiviteten för skräppostfiltret. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen Inkorg.
3. Välj meddelande (skräppost) som ej upptäckts.
4. Klicka knappen **Är skräppost** i Bitdefenders verktygsfält mot skräppost (finns normalt i övre delen av e-postklientens fönster). De märks direkt som [spam] och flyttas till mappen för skräppost.

Lägg till spammare i listan över spammare

Om du använder en stödd e-postklient så kan du enkelt lägga till skräppost-avsändares meddelanden till listan över spammare. Följ dessa steg:

1. Öppna din e-postklient.
2. Gå till mappen skräppost som skräppost-meddelanden flyttas till.
3. Välj de meddelanden som märkts som [spam] av Bitdefender.
4. Klicka knappen **Lägg till spammare** i Bitdefenders verktygsfält för skydd mot skräppost.
5. Du kan bli ombedd att bekräfta de adresser som har lagts till i listan över spammare. Markera **Visa inte detta meddelande igen** och klicka på **OK**.

Om du använder en annan e-postklient kan du manuellt lägga till spammare till Listan över spammare från Bitdefenders gränssnitt. Det är praktiskt att göra det endast när du har fått flera skräppostmeddelanden från samma e-postadress. Följ dessa steg:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **SKRÄPPOST** fliken, klicka på **Hantera spammare**.

   Ett konfigurationsfönster öppnas.
3. Skriv spammarens e-postadress och klicka sedan på **LÄGG TILL**. Du kan lägga till så många e-postadresser du vill.
4. Klicka **OK** för att spara ändringarna och stänga fönstret.

Skräppostfiltret upptäcker inte några skräppost-meddelanden

Om inga skräppostmeddelanden märks som [spam] kan det vara något fel på Bitdefenders skräppostfilter. Innan du felsöker detta problem, försäkra dig om att det inte orsakats av något av följande:

- Skräppostskyddet kan vara avstängt. För att verifiera status på skräppostskyddet klickar du på **Skydd** på navigeringsmenyn på Bitdefender-gränssnittet. Titta i panelen **Antispam** för att se om funktionen är aktiverad.

  Om Antispam är inaktiverat är det det som orsakar ditt problem. Klicka på motsvarande reglage för att aktivera ditt skräppostskydd.
- Bitdefenders skräppostskydd är endast tillgängligt för e-postklienter som konfigurerats att ta emot e-postmeddelanden via POP3-protokollet. Detta betyder följande:
  - E-postmeddelanden som mottagits via webb-baserade e-posttjänster (som Yahoo, Gmail, Hotmail eller annat) filtreras inte efter skräppost av Bitdefender.
  - Om din e-postklient konfigurerats till ett ta emot e-postmeddelanden genom att använda sig av något annat protokoll än POP3 (till exempel IMAP4), kommer inte Bitdefenders skräppostfilter att kontrollera dem för skräppost.

    Notera

    POP3 är ett av de mest använda protokollen för hämtning av e-postmeddelanden från en e-postserver. Om du inte vet vilket protokoll

som din e-postklient använder sig av för att hämta e-postmeddelanden, fråga den person som konfigurerade din e-postklient.

- Bitdefender Total Security skannar inte Lotus Notes POP3-trafik.

En möjlig lösning är att reparera eller installera om produkten. Du kan dock istället vilja kontakta Bitdefender för support som beskrivet i sektionen *"Be om hjälp"* (p. 290).

6.1.12. Funktionen Autofill i min plånbok fungerar inte

Du har sparat dina onlineuppgifter i din Bitdefender Password Manager och du märker att automatisk ifyllnad inte fungerar. Oftast dyker det här problemet upp när Bitdefender-plånbokstilläget inte är installerat i din webbläsare.

Följ de här stegen för att lösa den här situationen:

- I **Internet Explorer:**
  1. Öppna Internet Explorer.
  2. Klicka på Verktyg.
  3. Klicka på Hantera tillägg.
  4. Klicka på Verktygsfält och tillägg.
  5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.
- I **Mozilla Firefox:**
  1. Öppna Mozilla Firefox.
  2. Klicka på Verktyg.
  3. Klicka på Tilläggsprogram.
  4. Klicka på Tillägg.
  5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.
- I **Google Chrome:**
  1. Öppna Google Chrome.
  2. Gå till Meny-ikonen.
  3. Klicka på Fler verktyg.
  4. Klicka på Tillägg.
  5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.

Notera
Tillägget aktiveras när du startat om webbläsaren.

Kontrollera nu om funktionen för automatisk ifyllnad i plånboken fungerar för dina onlinekonton.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.1.13. Bitdefender-borttagning misslyckades

Om du vill ta bort din Bitdefender-produkt och märker att processen hänger sig eller systemet fryser, så klickar du på **Avbryt** för att avbryta åtgärden. Om det inte fungerar startar du om systemet.

När borttagning misslyckas kan vissa Bitdefender-registernycklar och filer vara kvar i systemet. Sådana rester kan förhindra en ny installation av Bitdefender. De kan även påverka systemets prestanda och stabilitet.

Gör så här för att helt ta bort Bitdefender från systemet:

- I **Windows 7**:
  1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
  2. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
  3. Klicka på **TA BORT** i det fönster som visas.
  4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 8 och Windows 8.1**:
  1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
  2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
  3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
  4. Klicka på **TA BORT** i det fönster som visas.
  5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- I **Windows 10**:
  1. Klicka på **Start**, därefter på Inställningar.

2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
3. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **TA BORT** i det fönster som visas.
6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

6.1.14. Mitt system startar inte efter att ha installerat Bitdefender

Om du precis har installerat Bitdefender och inte kan starta om systemet i normalt läge längre kan det finns flera olika orsaker till det här problemet.

Mest troligt är att det orsakas av en tidigare Bitdefender-installation, som inte togs bort korrekt eller av en annan säkerhetslösning som fortfarande finns kvar på systemet.

Så här kan du ta hand om varje situation:

- **Du hade Bitdefender tidigare och du tog inte bort det ordentligt.**

  För att lösa det:

  1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?" (p. 63)* hur du gör det.
  2. Ta bort Bitdefender från ditt system:
     - I **Windows 7**:
       a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
       b. Hitta **Bitdefender Total Security** och välj **Avinstallera**.
       c. Klicka på **TA BORT** i det fönster som visas.
       d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
       e. Starta om systemet i normalt läge.
     - I **Windows 8 och Windows 8.1**:

a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.

c. Hitta **Bitdefender Total Security** och välj **Avinstallera**.

d. Klicka på **TA BORT** i det fönster som visas.

e. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

f. Starta om systemet i normalt läge.

- I **Windows 10**:

a. Klicka på **Start**, därefter på Inställningar.

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

c. Hitta **Bitdefender Total Security** och välj **Avinstallera**.

d. Klicka på **Avinstallera** igen för att bekräfta ditt val.

e. Klicka på **TA BORT** i det fönster som visas.

f. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

g. Starta om systemet 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 det:

1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 63) hur du gör det.
2. Ta bort den andra säkerhetslösningen från systemet:

   - I **Windows 7**:

a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.

b. Hitta namnet på det program du vill ta bort och välj **Ta bort**.

c. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 8 och Windows 8.1**:

  a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

  b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.

  c. Hitta namnet på det program du vill ta bort och välj **Ta bort**.

  d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

- I **Windows 10**:

  a. Klicka på **Start**, därefter på Inställningar.

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

  c. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.

  d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

För att korrekt avinstallera den andra programvaran går du till deras webbplats och kör deras avinstallationsverktyg eller kontaktar dem direkt så att de kan ge dig riktlinjer för avinstallationen.

3. Starta om systemet i normalt läge och installera om Bitdefender.

Du har redan följt stegen ovan och situationen är inte löst.

För att lösa det:

1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 63) hur du gör det.
2. Använd alternativet Systemåterställning från Windows för att återställa datorn till ett tidigare datum innan du installerade Bitdefender-produkten.
3. Starta om systemet i normalt läge och kontakta vår support för hjälp såsom beskriv i avsnitt *"Be om hjälp"* (p. 290).

6.2. Ta bort hot från ditt system

Hot kan påverka ditt system på många olika sätt och Bitdefender tillvägagångssätt beror på typen av hotattack. Eftersom hota ofta ändrar sitt beteende är det svårt att bestämma ett mönster för deras beteenden och handlingar.

Det finns situationer när Bitdefender inte automatiskt kan ta bort hotinfektionen från ditt system. I sådana fall krävs en åtgärd av dig.

- *"Bitdefender Räddningsläge (räddningsmiljö i Windows 10)"* (p. 174)
- *"Vad ska du göra när Bitdefender hittar hot på din dator?"* (p. 177)
- *"Hur rensar jag bort ett hot i ett arkiv?"* (p. 179)
- *"Hur rensar jag ett e-postarkiv från hot?"* (p. 180)
- *"Vad gör jag om jag misstänker att en fil är farlig?"* (p. 181)
- *"Vad är de lösenordsskyddade filerna i skanningsloggen?"* (p. 181)
- *"Vad är de överhoppade posterna i skanningsloggen?"* (p. 182)
- *"Vad är de överkomprimerade filerna i skanningsloggen?"* (p. 182)
- *"Varför raderade Bitdefender en infekterad fil automatiskt?"* (p. 182)

Om du ej kan finna ditt problem här eller om den valda lösningen inte fungerar kan du kontakta Bitdefender representanter för teknisk support som visat i kapitlet *"Be om hjälp"* (p. 290).

6.2.1. Bitdefender Räddningsläge (räddningsmiljö i Windows 10)

Räddningsläge är en Bitdefender-funktion som gör att du kan skanna och desinfektera alla befintliga hårddiskpartitioner inuti och utanför operativsystemet.

När Bitdefender Total Security installeras på **Windows 7, Windows 8 och Windows 8.1** och Bitdefenders räddningslägesavbildning laddas ner, räddningsläget användas även om du inte längre kan starta i Windows.

I Windows 10 är Bitdefenders räddningsmiljö integrerad med Windows RE, vilket innebär att du inte behöver ladda ner någon räddningslägesavbildning på det här operativsystemet.

Hämtar Bitdefender Rescue Mode Image

För att kunna använda räddningsläget i **Windows 7, Windows 8 och Windows 8.1**, måste du först hämta dess avbildningsläget enligt följande:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Räddningsläge**.
3. Klicka på **Ja** i det bekräftelsefönster som visas för att starta om datorn.

   Vänta tills Bitdefender Rescue Mode Image-filen laddas ner från Bitdefender-servrarna. Så fort hämtningsprocessen är avslutad, startar datorn om.

   En meny visas som uppmanar dig att välja ett operativsystem. I det här steget kan du välja att starta ditt system i räddningsläge eller i normalt läge.

Notera
På grund av integrationen med Windows återställningsmiljö i **Windows 10**, finns det inget behov av att ladda ner någon räddningslägesavbildning på det här operativsystemet.

Starta ditt system i räddningsläget i Windows 7, Windows 8 och Windows 8.1

Du kan öppna räddningsläget på ett av två sätt:

Från Bitdefender-gränssnittet

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Räddningsläge**.
3. Klicka på **Ja** i det bekräftelsefönster som visas för att starta om datorn.
4. När datorn startat om visas en meny som uppmanar dig att välja ett operativsystem. Välj **Bitdefender Rescue Mode** för att starta i en Bitdefender-miljö varifrån du kan rensa din Windows-partition.
5. Vid uppmaning trycker du på **Enter** och väljer skärmupplösningen närmast den du normalt använder. Tryck sedan på **Enter** igen.

   Bitdefender Rescue Mode laddas på några minuter.

Starta din dator direkt i räddningsläge

Om Windows inte startar längre kan du starta datorn direkt i Bitdefenders räddningsläge genom att följa stegen nedan:

- I **Windows 7**:
  1. Tryck på **F8** tills skärmen **Avancerade startalternativ** visas.
  2. Använd piltangenterna för att välja Bitdefenders räddningsläge och tryck sedan på **Enter**.

     Bitdefenders räddningsläge laddas om några minuter.
- I **Windows 8 och Windows 8.1**:
  1. Tryck på **Shift**-tangenten tills skärmen **Avancerade startalternativ** visas.
  2. Välj alternativet **Använd ett annat operativsystem** och sedan Bitdefender Rescue Mode.

     Bitdefenders räddningsläge laddas om några minuter.

> **Notera**
> Det är möjligt att starta datorn i räddningsläge endast om räddningslägesavbildningen tidigare har har hämtats såsom beskrivs i "Hämtar Bitdefender Rescue Mode Image" (p. 175).

Starta systemet i räddningsmiljö i Windows 10

Du kan endast komma in i räddningsmiljön från din Bitdefender-produkt enligt följande:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. I **ANTIVIRUS**-panelen klickar du på **Räddningsläge**.
3. Klicka på **Starta om** i det fönster som visas.

   Bitdefender Rescue Environment laddas på några minuter.

Skanna systemet i räddningsläge (räddningsmiljö i Windows 10)

Skanna systemet i räddningsläge (räddningsmiljö):

- I **Windows 7, Windows 8 och Windows 8.1**:
  1. Öppna räddningsläget såsom beskrivs i "Starta ditt system i räddningsläget i Windows 7, Windows 8 och Windows 8.1" (p. 175).

2. Bitdefender-logotypen visas och säkerhetslösningsmotorerna börjar kopieras.
3. Ett välkomstfönster visas. Klicka på **Fortsätt**.
4. En uppdatering av hotinformationsdatabasen startas.
5. När uppdateringen är klar visas fönstret Bitdefender On-demand Antivirus Scanner.
6. Klicka på **Skanna nu**, välj skanningsmål i det fönster som visas och klicka därefter på **Öppna** för att börja skanna.

   Du rekommenderas att skanna hela Windows-partitionen.

   > **Notera**
   > När du arbetar i räddningsläget hanterar du partitionsnamn av Linux-typ. Diskpartitioner visas som sda1 motsvarar troligen (C:) som Windows-typpartition, sda2 motsvarar (D:) och så vidare.

7. Vänta tills skanningen är klar. Om ett hot upptäcks följer du instruktionerna för att ta bort det.
8. Avsluta räddningsläget genom att högerklicka på ett tomt område på skrivbordet, välj **Avsluta** i menyn som visas och välj sedan om du vill starta om eller stänga ned datorn.

- I **Windows 10**:

1. Öppna räddningsläget såsom beskrivs i "Starta systemet i räddningsmiljö i Windows 10" (p. 176).
2. Bitdefender-skanningsprocessen startar automatiskt så fort systemet laddas i räddningsmiljön.
3. Vänta tills skanningen är klar. Om ett hot upptäcks följer du instruktionerna för att ta bort det.
4. Avsluta räddningsmiljön genom att klicka på knappen **STÄNG** i fönstret med skanningsresultaten.

6.2.2. Vad ska du göra när Bitdefender hittar hot på din dator?

Du kan få reda på att det finns hot på din dator på något av följande sätt:

- Du skannade din dator och Bitdefender fann infekterade objekt på den.

- En hotvarning meddelar dig om att Bitdefender blockerat ett eller flera hot på din dator.

I dessa situationer uppdaterar du Bitdefender för att försäkra dig om att du har den senaste hotinformationsdatabasen och kör en systemskanning för att analysera systemet.

Så fort systemskanningen är avslutad, väljer du önskad åtgärd för de infekterade objekten (desinficera, radera, flytta till karantän).

Varning
Om du misstänker att en fil är en del av Windows operativsystem eller att det inte är en infekterad fil, följ inte dessa steg utan kontakta Bitdefender kundtjänst så snart som möjligt.

Om vald handling inte kunde utföras och att loggen för skanning visar att en smitta inte kunde tas bort, måste filen (-erna) tas bort manuellt.

Den första metoden kan användas i normalt läge:

1. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.
2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?"* (p. 61) hur du gör det.
3. Bläddra till den infekterade filens plats (sök igenom skanningsloggen) och radera den.
4. Slå på Bitdefender realtids-antivirusskydd.

Om den första metoden misslyckas med att ta bort infektionen:

1. Starta om ditt system och gå in i felsäkert läge. Se i *"Hur startar jag om i Felsäkert läge?"* (p. 63) hur du gör det.
2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?"* (p. 61) hur du gör det.
3. Bläddra till den infekterade filens plats (sök igenom skanningsloggen) och radera den.
4. Starta om ditt system och gå in i normalt läge.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.2.3. Hur rensar jag bort ett hot i ett arkiv?

En komprimerad fil innehåller en eller flera filer som packats ihop till ett speciellt format för att spara på diskutrymmet.

Vissa av dessa format är öppna format, och tillhandahåller såvida Bitdefender möjligheten att skanna dem på insidan för att sen vidta passande åtgärder för att ta bort dem.

Andra komprimerade format är delvis eller helt stängda och Bitdefender kan endast hitta hot inuti dem, men kan inte vidta andra åtgärder.

Om Bitdefender meddelar dig om att ett hot upptäckts inuti ett arkiv och att ingen åtgärd är tillgänglig, betyder detta att det inte är möjligt att ta bort hotet på grund av begränsningar av arkivets inställningar för behörigheter.

Så här kan du rensa bort ett hot som lagrats i ett arkiv:

1. Identifiera arkivet som innehåller hotet genom att utföra en Systemskanning av systemet.
2. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.
3. Gå till arkivets plats och dekomprimera det genom att använda en arkiveringsapp, som WinZip.
4. Identifiera den infekterade filen och radera den.
5. Radera det ursprungliga arkivet för att vara säker på att infektionen är fullständigt borttagen.
6. Komprimera filerna i ett nytt arkiv med hjälp av en arkiveringsapp, som WinZip.
7. Slå igång Bitdefenders realtidsskydd och kör en systemskanning för att försäkra dig om att det inte finns någon mer infektion på systemet.

Notera
Det är viktigt att notera, att ett hot som är lagrat i ett arkiv inte utgör ett omedelbart hot mot ditt system eftersom hotet måste expanderas och verkställas för att kunna infektera ditt system.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.2.4. Hur rensar jag ett e-postarkiv från hot?

Bitdefender kan också identifiera hot i e-postdatabaser och e-postarkiv lagrade på en disk.

Ibland är det nödvändigt att identifiera det infekterade meddelandet, genom att använda den information du fått i skanningsrapporten, och radera det manuellt.

Så här kan du rensa bort ett hot som lagrats i ett e-postarkiv:

1. Skanna e-postdatabasen med Bitdefender.
2. Slå av Bitdefenders realtidsskydd:
   a. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
   b. I **ANTIVIRUS**-panelen klickar du på **Inställningar**.
   c. I fönstret **Shield** stänger du av **Bitdefender Shield**.
3. Öppna skanningsrapporten och använd identifieringsinformationen (ämne, från, till) från de infekterade meddelandena för att hitta dem i din e-postklient.
4. Radera de infekterade meddelandena. De flesta e-postklienter flyttar även det raderade meddelandet till en återställningsmapp, från vilken meddelandet kan återställas. Du bör försäkra dig om att meddelandet även är raderat från denna återställningsmapp.
5. Komprimera mappen som innehåller det infekterade meddelandet.
   - I Microsoft Outlook 2007: I filmenyn, klicka datafilshantering. Välj de personliga mappar-filerna (.pst) du har tänkt komprimera och klicka sen på inställningar. Klicka på Packa nu.
   - I Microsoft Outlook 2010/2013/2016: På menyn Arkiv klickar du på Info och därefter på Kontoinställningar (Lägg till eller ta bort konton eller ändra befintliga anslutningsinställningar). Klicka sedan på Dataarkiv,

välj de personliga mappfiler (.pst) du avser att komprimera och klicka på Inställningar. Klicka på Packa nu.

6. Slå på Bitdefender realtids-antivirusskydd.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 290).

6.2.5. Vad gör jag 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 vara säker på att ditt system är skyddat:

1. Kör en **Systemskanning** med Bitdefender. Se i *"Hur skannar jag mitt system?"* (p. 45) hur du gör det.
2. Om skanningsresultatet visar sig vara rent, men du fortfarande är tveksam och vill vara säker på filen, kontaktar du vår support så att vi kan hjälpa dig.

   Se i *"Be om hjälp"* (p. 290) hur du gör det.

6.2.6. Vad är de lösenordsskyddade filerna i skanningsloggen?

Det här är bara ett meddelande som visar att Bitdefender har upptäckt att dessa filer antingen skyddas med ett lösenord eller någon form av kryptering.

De vanligaste lösenordsskyddade posterna är:

- Filer som tillhör en annan säkerhetslösning.
- Filer som hör till operativsystemet.

För att verkligen kunna skanna innehållet, skulle dessa filer behöva antingen extraheras eller på annat sätt avkrypteras.

Skulle dessa innehåll extraheras, skulle Bitdefenderns realtidsskanner automatiskt skanna dem för att hålla din dator skyddad. Om du vill skanna de filerna med Bitdefender måste du kontakta tillverkaren av produkten så att de kan ge dig fler detaljer om filerna.

Vår rekommendation till dig är att ignorera dessa filer då de ej utgör något hot mot ditt system.

6.2.7. Vad är de överhoppade posterna i skanningsloggen?

Alla filer som visas som överhoppade i skanningsrapporten är rena.

För bättre prestanda skannar inte Bitdefender filer som inte har ändrats sedan den senaste skanningen.

6.2.8. Vad är de överkomprimerade filerna i skanningsloggen?

De överkomprimerade posterna är delar som inte kunde extraheras av skanningsmotorn, eller delar som det skulle ta för lång tid att dekryptera vilket skulle göra systemet instabilt.

Överkomprimerad betyder att Bitdefender hoppade över skanning av det arkivet eftersom det skulle krävas för stora systemresurser för att packa upp det. Innehållet kommer att skannas i realtid vid behov.

6.2.9. Varför raderade Bitdefender en infekterad fil automatiskt?

Om en infekterad fil upptäcks, kommer Bitdefender automatiskt att försöka desinficera den. Om desinficering misslyckas flyttas filen till karantän för att innesluta infektionen.

För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

Detta är vanligtvis fallet med installationsfiler som hämtas från opålitliga webbsidor. Om du hamnar i en sådan situation, hämta installationsfilen från tillverkarens webbsida eller annan betrodd webbsida.

ANTIVIRUS FOR MAC

7. INSTALLERING OCH BORTTAGNING

Det här kapitlet omfattar följande ämnen:

7.1. Systemkrav

Du kan installera Bitdefender Antivirus for Mac Macintosh-datorer som kör OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra (10.12.6), MacOS High Sierra (10.13.6) eller macOS Mojave (10.14 eller senare).

Din Mac måste även ha minst 1 GB tillgängligt hårddiskutrymme.

Du måste ha en Internet-anslutning för att registrera och uppdatera Bitdefender Antivirus for Mac.

Så här tar du reda på macOS-version och hårdvaruinformation om din Mac

Klicka på Apple-ikonen överst till vänster på skärmen och välj **Om denna Mac**. I fönstret som visas kan du se din version av operativsystem och annan användbar information. Klicka på **Systemrapport** för detaljerad hårdvaruinformation.

7.2. Installerar Bitdefender Antivirus for Mac

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 till ditt Bitdefender-konto med e-postadress och lösenord.
4. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
5. Välj ett av två möjliga alternativ:
   - **Skydda den här enheten**
     a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.

b. Spara installationsfilen.

- **Skydda andra enheter**

  a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.

  b. Klicka på **SKICKA NEDLADDNINGSLÄNK**.

  c. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**.

  Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

  d. Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.

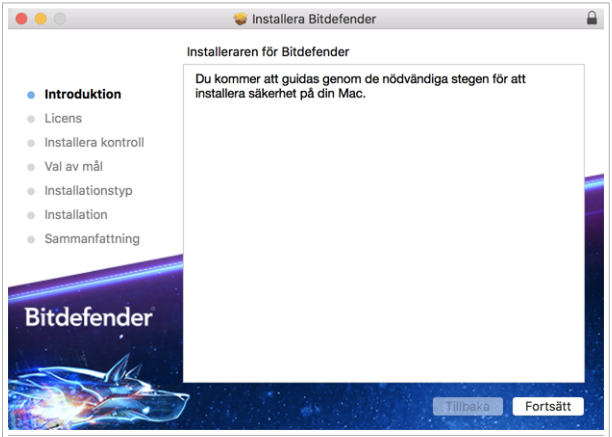
6. Kör den Bitdefender-produkt du har hämtat.
7. Slutför installationsstegen.

7.2.1. Installationsprocess

Installera Bitdefender Antivirus for Mac:

1. Klicka på den hämtade filen. Det startar installationsprogrammet, som guidar dig igenom installationsprocessen.
2. Följ installationsguiden.

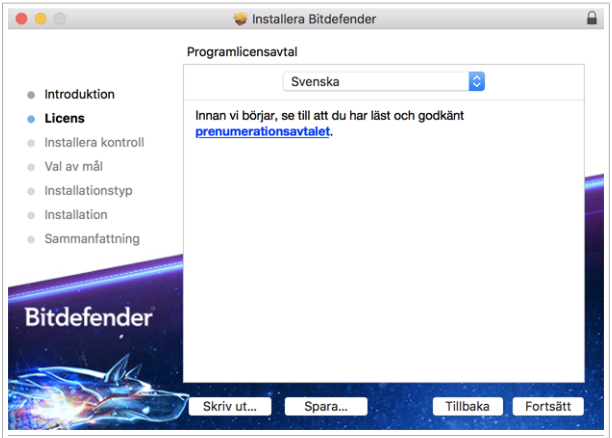
Steg 1 - Välkomstfönster



Välkomstfönster

Klicka på **Fortsätt**.

Steg 2 - Läs prenumerationsavtalet



Läs prenumerationsavtalet

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet

eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Antivirus for Mac.

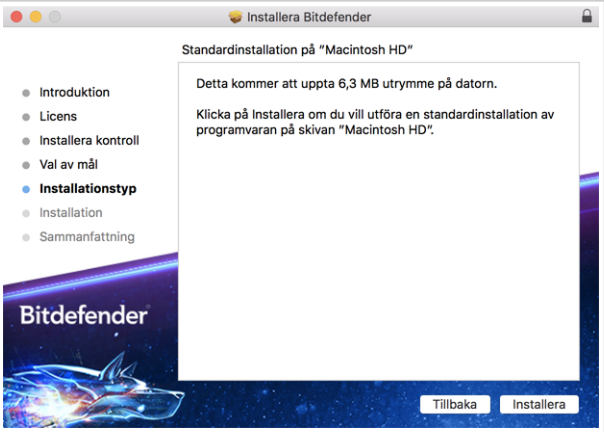
Från det här fönstret kan du även välja det språk du vill installera produkten på.

Klicka på **Fortsätt** och klicka sedan på **Godkänn**.

Viktigt

Om du inte godkänner villkoren klickar du på **Fortsätt** och därefter på **Godkänner inte** för att avbryta installationen och avsluta installationsprogrammet.

Steg 3 - Starta installationen

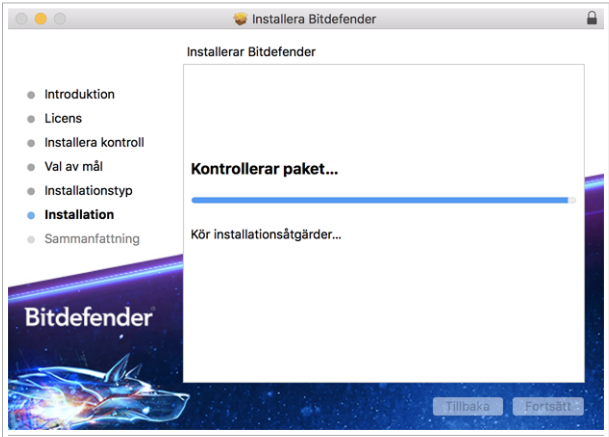


Starta installationen

Bitdefender Antivirus for Mac installeras i Macintosh HD/Library/Bitdefender. Installationssökvägen kan inte ändras. Installationssökvägen kan inte ändras.

Klicka på **Installera** för att starta installationen.

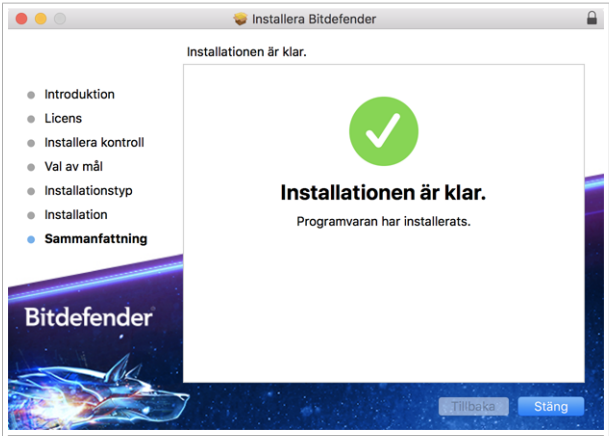
Steg 4 - Installera Bitdefender Antivirus for Mac



Installerar Bitdefender Antivirus for Mac

Vänta tills installationen är klar och klicka sedan på **Fortsätt**.

Steg 5 - Slutför



Avsluta

Klicka **Stäng** för att stänga installationsfönstret.

Installationsprocessen är nu slutförd.

Viktigt

- Om du installerar Bitdefender Antivirus for Mac på macOS High Sierra 10.13.0 eller en nyare version visas meddelandet **Systemtillägg blockerat**. Det här meddelandet informerar om att tillägg signerade av Bitdefender har blockerats och måste aktiveras manuellt. Klicka **OK** för att fortsätta. I Bitdefender Antivirus for Mac-fönstret som visas klickar du på länken **Säkerhet och sekretess**. Klicka på **Tillåt** i den nedre delen av fönstret eller välj Bitdefender SRL i listan och klicka sedan på **OK**.
- Om du installerar Bitdefender Antivirus for Mac på macOS Mojave 10.14 eller en nyare version, visas ett meddelande. Meddelandet informerar om att manuellt måste tillåta Bitdefender Antivirus for Mac att ladda sina filer på ditt system. För att fortsätta klickar du på länken **Säkerhet & Sekretess** och därefter på **OK**. Klicka på **Tillåt** bredvid Bitdefender SRL.

7.3. Tar bort Bitdefender Antivirus for Mac

Eftersom Bitdefender Antivirus for Mac är en komplex app kan den inte tas bort på vanligt sätt genom att dra appikonen från Program-mappen till papperskorgen.

Ta bort Bitdefender Antivirus for Mac genom att följa dessa steg:

1. Öppna ett **Sökar**-fönster och gå sedan till Program-mappen.
2. Öppna Bitdefender-mappen och dubbelklicka på BitdefenderUninstaller.
3. Klicka på **Avinstallera** och vänta tills processen slutförs.
4. Klicka på **Stäng** för att avsluta.

Viktigt

Om fel uppstår kan du kontakta Bitdefender kundtjänst enligt "Kontakta oss" (p. 289).

8. KOMMA IGÅNG

Det här kapitlet omfattar följande ämnen:

8.1. Om 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 inte bara och tar bort Mac-hot, tan även Windows-hot, och förhindrar därmed att du oavsiktligt skickar smittade filer till familj, vänner och kollegor som använder PC.

8.2. Öppnar Bitdefender Antivirus for Mac.

Du kan öppna Bitdefender Antivirus for Mac på flera sätt.

- Klicka på Bitdefender Antivirus for Mac-ikonen i Launchpad.
- Klicka på ikonen i menyfältet och välj **Öppna huvudfönster**.
- Öppna ett Sökarfönster, gå till Program och dubbelklicka på ikonen Bitdefender Antivirus for Mac.

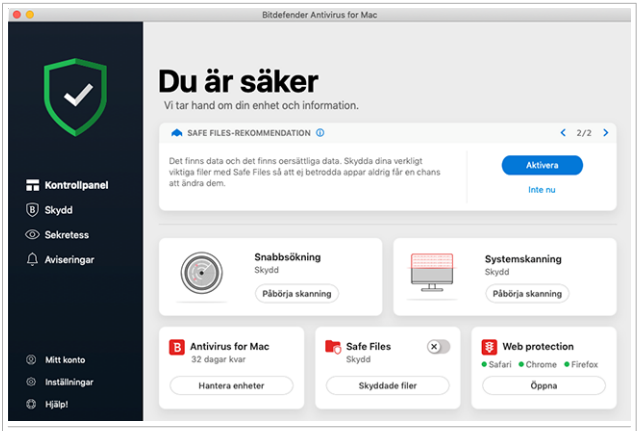
Viktigt

Första gången du öppnar Bitdefender Antivirus for Mac på macOS Mojave 10.14 eller en nyare version visas en skyddsrekommendation. Den här rekommendationen visas eftersom vi behöver behörighet att skanna hela ditt system för hot. För att ge oss behörighet måste du logga in som administratör och följa de här stegen:

1. Klicka på länken **Systemegenskaper**.
2. Klicka på -ikonen och skriv dina administratörsinloggningsuppgifter.
3. Ett nytt fönster öppnas. Dra filen **BDLDaemon** till listan med tillåtna appar.

8.3. Appens huvudfönster

Bitdefender Antivirus for Mac uppfyller behoven lika mycket för nybörjare på datorer som för väldigt tekniska människor. Dess grafiska användargränssnitt är utformat för att passa alla sorters människor.



Appens huvudfönster

För att gå igenom Bitdefender-gränssnittet finns en introduktionsguide som innehåller information om hur du interagerar med produkten och hur du konfigurerar den på den övre vänstra sidan. Välj rätt höger vinkelparentes för att fortsätta guidas eller **Hoppa över rundtur** för att stänga guiden.

Statusfältet längst upp i fönstret informerar om systemets säkrhetsstatus via explicita meddelanden och tydliga färger. Om Bitdefender Antivirus for Mac inte har några varningar är statusfältet grönt. När ett säkerhetsproblem

upptäcks byter statusfältet färg till röd. Detaljerad information om problem och hur du löser dem finns i *"Löser problem"* (p. 205).

För att ge dig en effektiv drift och ökat skydd när du utför olika aktiviteter, fungerar **Bitdefender Autopilot** som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, om du antingen arbetar, utför onlinebetalningar, kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov. Det hjälper dig att upptäcka och dra nytta av de funktioner som ingår i Bitdefender Antivirus for Mac-appen.

Från navigeringsmenyn till vänster kan du komma till Bitdefender-avsnitten för detaljerad konfiguration och avancerade administrativa uppgifter (flikarna **Skydd** och **Sekretess**), meddelanden, ditt Bitdefender-konto och området Inställningar. Du kan också kontakta oss (fliken **Hjälp**) för support i fall du har frågor eller om något oväntat inträffar.

8.4. App Dock-ikon

Du hittar Bitdefender Antivirus for Mac-ikonen i Dock så fort du öppnar appen. Ikonen i Dock ger dig ett enkelt sätt att skanna filer och mappar för hot. Bara dra och släpp filen eller mappen över Dock-ikonen så startar skanningen direkt.

Dock-ikon

8.5. Navigeringsmeny

På vänster sida på Bitdefender-gränssnittet finns navigeringsmenyn, vilket gör att du snabbt når de Bitdefender-funktioner du behöver för att hantera din produkt. Flikarna som finns i det området är:

- **Kontrollpanel**. Härifrån kan du snabbt lösa problem, visa rekommendationer efter dina systembehov och användningsmönster, utföra snabbåtgärder och gå till ditt Bitdefender-konto för att hantera de enheter du har lagt till i din Bitdefender-prenumeration.

- **Skydd**. Härifrån kan du starta antivirusskanningar, lägga till filer till undantagslistan, skydda filer och appar från ransomware-attacker, säkra dina Time Machine-backuper och konfigurera skydd medan du surfar på Internet.
- **Sekretess**. Härifrån kan du öppna Bitdefender VPN-appen och installera Anti-tracker-tillägget i din webbläsare.
- **Meddelanden**. Härifrån kan se information om de åtgärder som vidtas på skannade filer.
- **Mitt konto**. Härifrån kan du komma åt ditt Bitdefender-konto för att verifiera dina prenumerationer och utföra säkerhetsåtgärder på de enheter du hanterar. Information om Bitdefender-konto och pågående prenumeration finns också.
- **Inställningar**. Härifrån kan du konfigurera Bitdefender-inställningarna.
- **Hjälp!**. Härifrån kan du när du behöver hjälp med att lösa en situation med din Bitdefender-produkt kontakta avdelningen för teknisk support. Du kan också skicka oss feedback för att hjälpa oss att förbättra produkten.

8.6. Mörkt läge

För att skydda dina ögon mot bländning och ljus när du arbetar på natten eller i under mörka förhållanden stödjer Bitdefender Antivirus for Mac Mörkt läge för Mojave 190.14 och senare. Färgerna i gränssnittet har optimerats så att du kan använda din Mac utan att anstränga ögonen. Bitdefender Antivirus for Mac-gränssnittet justerar sig själv beroende på enhetens utseendeinställningar.

9. SKYDD MOT SKADLIGA PROGRAM

Det här kapitlet omfattar följande ämnen:

9.1. Bästa praxis

Följ denna bästa praxis för att skydda ditt system från hot och förhindra oavsiktlig smitta på andra system:

- Ha **Bitdefender Shield** aktiverad, så att systemfiler automatiskt skannas av Bitdefender Antivirus for Mac.
- Se till att din Bitdefender Antivirus for Mac-produkt är uppdaterad med den senaste hotinformationen och produktuppdateringarna.
- Kontrollera och åtgärda problem som rapporteras av Bitdefender Antivirus for Mac regelbundet. För detaljerad information, se *"Löser problem"* (p. 205).
- Kontrollera den detaljerade händelseloggen avseende Bitdefender Antivirus for Mac-aktivitet på din dator. Varje gång något som är relevant för säkerheten för ditt system eller dina data inträffar läggs ett nytt meddelande till i området Bitdefender-meddelanden. Mer information finns i *"Aviseringar"* (p. 206).

- Du bör även följa bästa praxis:
  - Gör en vana av att skanna filer du hämtar från ett externt lagringsminne (som en USB-sticka eller en CD), särskilt om du inte känner till källan.
  - Om du har em DMG-fil monterar du den och skannar dess innehåll (filerna inom 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 for Mac-fönstret eller Dock-ikonen.

Ingen annan konfiguration eller åtgärd behövs. Om du vill kan du dock justera appinställningarna och egenskaperna för att bättre passa dina behov. Mer information finns på *"Konfigurera egenskaper"* (p. 209).

9.2. Skanna din Mac

Förutom funktionen **Bitdefender Shield**, som regelbundet övervakar de installerade apparna och letar efter hotlika åtgärder och förhindrar nya hot från att komma in in systemet, kan du 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 for Mac-fönstret eller Dock-ikonen. Skanningsguiden kommer att visas och leda dig genom skanningsprocessen.

Du kan också starta en skanning så här:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Antivirus**.
3. Klicka på en av de tre skanningsknapparna för att starta önskad skanning.
   - **Snabbsökning** - kontrollerar de mest sårbara platserna i systemet för hot (till exempel mappar som innehåller dokument, nedladdningar, e-posthämtningar och tillfälliga filer för varje användare).
   - **Fullständig skanning** - utför en omfattande kontroll av hot för hela systemet. Alla anslutna tillbehör skannas också.

     Notera

     Beroende på din hårddiskstorlek kan en skanning av hela systemet ta en stund (upp till en timme eller ännu längre). För bättre prestanda rekommenderas du att inte köra den hör uppgiften medan du utför andra resursintensiva uppgifter (som videoredigering).

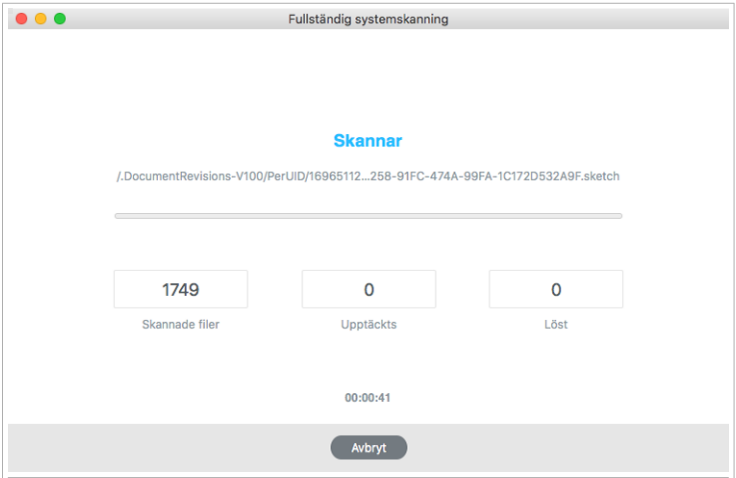
Om du föredrar det kan du välja att inte skanna specifika monterade volymer genom att lägga till dem till listan Undantag från fönstret Skydd.

- **Anpassad skanning** - hjälper dig att kontrollera specifika filer, mappar och volymer för hot.

Du kan även starta en system- eller snabbskanning från kontrollpanelen.

9.3. Guide för skanning

Varje gång du startar en skanning visas Bitdefender Antivirus for Mac-skanningsguiden.



Skanning pågår

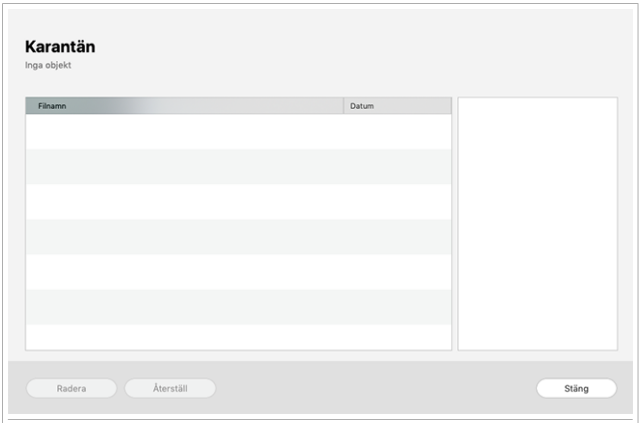
Realtidsinformation om upptäckta och lösta hot visas under varje skanning.

Vänta medan Bitdefender Antivirus for Mac slutför skanningen.

Notera
Skanningsprocessen kan ta en stund beroende på hur komplicerad den är.

9.4. Karantän

Bitdefender Antivirus for Mac låter dig isolera de infekterade eller misstänkta filerna i ett skyddat område, karantän. När ett hot är satt i karantän kan det inte göra någon skada eftersom det inte kan köras eller läsas.



Filer i karantän

Karantän-sektionen visar alla filer som just nu är isolerade i karantänmappen.

Ta bor en fil från karantän genom att markera den och klicka på **Ta bort**. Om du vill återställa en fil från karantän till sin ursprungliga plats, välj den och klicka **Återställ**.

För att visa en lista med alla objekt som lagts till i karantän:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Fönstret **Antivirus** öppnas.

   Klicka på **Öppna** i panelen **Karantän**.

9.5. Bitdefender Shield (realtidsskydd)

Bitdefender tillhandahåller realtidsskydd mot flera olika hot genom att skanna alla installerade appar, deras uppdaterade versioner och nya och modifierade filer.

Inaktivera realtidsskydd:

1. Klicka på **Egenskaper** på navigeringsmenyn i Bitdefender-gränssnittet.

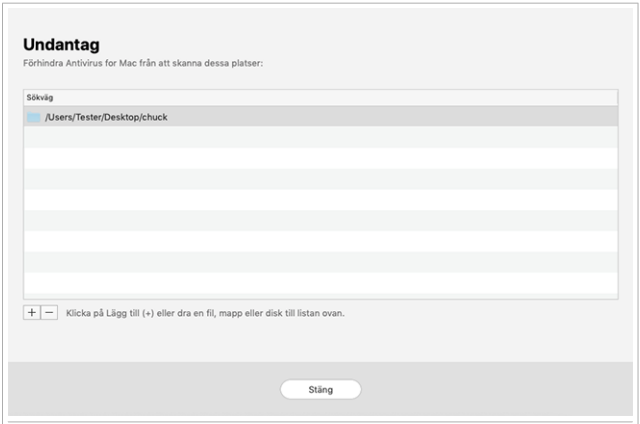
2. Inaktivera **Bitdefender Shield** i fönstret **Skydd**.

Varning
Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat är du inte skyddad mot hot.

9.6. Undantag från skanning

Om du vill kan du ställa in Bitdefender Antivirus for Mac att inte skanna vissa filer, mappar eller till och med en hel volym. Du kan till exempel vilja undanta från skanning:

- Filer som av misstag identifierats som smittade (kallas falska positiver)
- Filer som orsakar skanningsfel
- Säkerhetskopieringsvolymer



Undantag från skanning

Undantagslistan innehåller sökvägar som har exkluderats från skanning.

Öppna undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Fönstret **Antivirus** öppnas.

   Klicka på **Öppna** i panelen **Undantag**.

Det finns två sätt att ställa in ett skanningsundantag:

- Dra och släpp en fil, mapp eller volym över undantagslistan.
- Klicka på knappen med plustecken (+), som finns under undantagslistan. Välj sedan fil, mapp eller volym som ska undantas från skanning.

Ta bort ett skanningsundantag genom att markera det i listan och klicka på knappen med minustecken (-), som finns under undantagslistan.

9.7. Webbskydd

Bitdefender Antivirus for Mac använder TrafficLight-tilläggen för att helt säkra din surfupplevelse. TrafficLight-tilläggen, bryter, bearbetar och filtrerar all webbtrafik, för att blockera skadligt innehåll.

Tilläggen fungerar och integreras med följande webbläsare: Mozilla Firefox, Google Chrome och Safari.

Aktivera TrafficLight-tillägg

Aktivera TrafficLight-tillägg:

1. Klicka på **Fixa nu** i kortet **Webbskydd** på kontrollpanelen.
2. Fönstret **Webbskydd** öppnas.

   Den upptäckta webbläsaren du har installerat på ditt system visas. För att installera TrafficLight-tillägget i din webbläsare klickar du på **Hämta tillägg**.
3. Du omdirigeras till:

   https://bitdefender.com/solutions/trafficlight.html
4. Välj **Gratis nedladdning**.
5. Följ de här stegen för att installera det TrafficLight-tillägg som motsvarar din webbläsare.

Hantera tilläggsinställningar

En lång räcka av funktioner finns tillgängliga för att skydda dig från alla typer av hot som du kan stöta på när du surfar. För att nå dem klickar du på ikonen TrafficLight bredvid webbläsarens inställningar och klickar därefter på **Inställningar**:

- **Bitdefender TrafficLight - inställningar**

- Avancerat hotfilter - förhindrar att du öppnar webbsidor som används för skadlig kod, nätfiske och bedrägeriattacker.
- Spårningsupptäckt - upptäcker spårningskod på besökta webbsidor och informerar dig om detta.
- Sökresultatsanalys - ger avancerad varning för riskabla webbplatser inom dina sökresultat.

  Om alla inställningar är avaktiverade skannas ingen webbplats.

- **Vitlista**

  Webbplatser kan undantas från att skannas av Bitdefender-motorerna. I motsvarande fält skriver du namnet på den webbplats du vill lägga till i undantagslistan och klickar sedan på **LÄGG TILL**.

  Ingen varning visas om dessa hot finns på de undantagna sidorna. Därför ska du bara lägga till webbplatser du litar på helt och hållet till den här listan.

Sidklassning och varningar

Beroende på hur TrafficLight klassificerar den webbsida du visar, visas en av följande ikoner i området:

Det här är en säker sida att besöka. Du kan fortsätta arbeta.
Den här webbsidan kan innehålla farligt innehåll. Iaktta försiktighet om du besöker den.
Du bör lämna webbsidan omedelbart eftersom den innehåller skadlig kod och andra hot.

I Safari är bakgrunden för TrafficLight-ikonerna svart.

9.8. Anti-tracker

Många webbplatser du besöker använder spårningsverktyg 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. På så sätt tjänar webbplatsägare pengar för att kunna ge dig innehåll utan kostnad eller fortsätta vara verksamma. Förutom att samla in information kan spårningsverktyg göra din surfupplevelse långsammare eller slösa på bandbredd.

Med tillägget Bitdefender Anti-tracker aktiverat i webbläsaren undviker du att bli spårad så att dina data fortsätter att vara privata medan du surfar online och du ökar hastigheten som webbplatserna behöver för att läsas in.

Bitdefender-tillägget är kompatibelt med följande webbläsare:

- Google Chrome
- Mozilla Firefox
- Safari

De spårningsverktyg vi hittar grupperas i följande kategorier:

- **Reklam** - används för att analysera webbsidestrafik, användarbeteende eller besökares trafikmönster.
- **Kundinteraktion** - används för att mäta användarinteraktion med olika inmatningsformulär som chatt eller support.
- **Viktigt** - används för att övervaka viktiga webbsidesfunktioner.
- **Sidanalys** - används för att samla in data avseende webbsidesanvändning.
- **Sociala medier** - används för att övervaka social målgrupp, aktivitet och användarengagemang med olika sociala medieplattformar.

Aktivera Bitdefender Anti-tracker

Aktivera Bitdefender Anti-tracker-tillägget i din webbläsare:

1. Klicka på **Sekretess** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Anti-tracker**.
3. Klicka på **Aktivera tillägg** bredvid den webbläsare för vilken du vill aktivera tillägget.

9.8.1. Anti-tracker-gränssnitt

När tillägget Bitdefender Anti-tracker är aktiverad visas ikonen  bredvid sökfältet i webbläsaren. Varje gång du besöker en webbplats ses en räknare på ikonen, som hänvisar till upptäckta och blockerade spårningsverktyg. För att visa mer information om de blockerade spårningsverktygen klickar du på ikonen för att öppna gränssnittet. Förutom antalet blockerade spårningsverktyg kan du visa den tid som krävs för att sidan ska ladda och

kategorierna till vilka de upptäckta spårningsverktygen hör. Klicka på önskad kategori för att visa listan över webbplatser som spårar.

Inaktivera Bitdefender från att blockera spårningsverktyg på den webbplats du besöker genom att klicka på **Pausa skydd på den här webbplatsen**. Den här inställningen gäller endast så länge som du har webbplatsen öppen och återgår till den initiala tillståndet när du stänger webbplatsen.

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

9.8.2. Inaktivera Bitdefender Anti-tracker

Stänga av Bitdefender Anti-tracker från webbläsaren:

1. Öppna webbläsaren.
2. Klicka på ikonen bredvid adressfältet i webbläsaren.
3. Klicka på ikonen i det övre högra hörnet.
4. Använd motsvarande omkopplare för att aktivera eller inaktivera.

   Bitdefender-ikonen blir grå.

9.8.3. Tillåta att en webbplats spåras

Om du vill bli spårad medan du besöker en viss webbplats kan du lägga till dess adress till undantagen så här:

1. Öppna webbläsaren.
2. Klicka på ikonen bredvid sökfältet.
3. Klicka på ikonen i det övre högra hörnet.
4. Om du är på den webbplats du vill lägga till bland undantagen klickar du på **Lägg till aktuell webbplats i listan**.

   Om du vill lägga till en annan webbplats skriver du in adressen i motsvarande fält och klickar på .

9.9. Safe Files

Ransomware är skadlig programvara som attackerar sårbara system genom att låsa dem och be om pengar för att låta användaren få tillbaka kontroll över sitt system. Sådan här skadlig programvara agerar smart genom att visa falska meddelanden för att skrämma användaren och tvinga denne att gå vidare med betalningen.

Med hjälp av den senaste tekniken säkerställer Bitdefender systemintegritet genom att skydda viktiga systemområden mot ransomwareattacker utan att påverka systemet. Du kanske även vill skydda dina personliga filer, som dokument, foton eller filmer från att nås av obehöriga appar. Med Bitdefender Safe Files kan du placera personliga filer i ett skydd och på egen hand konfigurera vilka appar som ska tillåtas göra ändringar i de skyddade filerna och vilka som inte ska göra det.

För att i efterhand lägga till filer till den skyddade miljön:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Anti-Ransomware**.
3. Klicka på **Skyddade filer** i området Säkra filer.
4. Klicka på knappen med plustecken (+), som finns under listan med skyddade filer. Välj sedan fil, mapp eller volym som ska skyddas ifall ransomwareattacker försöker komma åt dem.

För att undvika att systemet blir långsammare rekommenderar vi att du lägger till som mest 30 mappar eller sparar flera filer i en mapp.

Som standard skyddas mapparna Bilder, Dokument, Skrivbord och Hämtade filer från hotattacker.

> **Notera**
> Anpassade mappar kan endast skyddas för aktuella användare. Externa enheter, system och appfiler kan inte läggas till i skyddsmiljön.

Du informeras varje gång en okänd app med ett ovanligt beteende försöker ändra de filer du lagt till. Klicka på **Tillåt** eller **Blockera** för att lägga till den i listan Hantera program list.

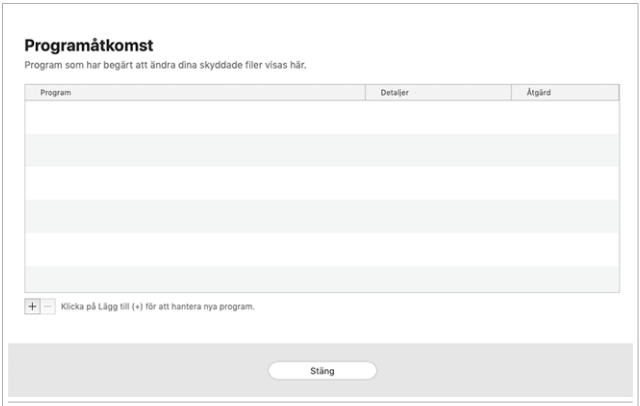
9.9.1. Hantera program

De appar som försöker ändra eller ta bort skyddade filer kan flaggas som potentiellt osäkra och läggas till i listan Blockerade appar. Om en sådan app blockeras och du är säker på att dess beteende är normalt, kan du tillåta den genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Anti-Ransomware**.
3. Klicka på **Programåtkomst** i området Säkra filer.
4. Ändra status till Tillåt bredvid den blockerade appen.

Appar som är angivna till Tillåt kan även anges till Blockerad.

Använd dra och släpp-metoden eller klicka på plustecknen (+) för att lägga till fler appar i listan.



Safe Files

9.10. Time Machine-skydd

Bitdefender Time Machine-skydd fungerar som ett ytterligare lager av säkerhet för din säkerhetskopieringsenhet, inklusive alla filer du lagrar i den, genom att blockera åtkomst från alla externa källor. Ifall filer från din Time Machine-enhet krypteras av ransomware, kan du återskapa dem utan att betala lösensumma.

Ifall du måste återställa objekt från en Time Machine-säkerhetskopia bör du kontrollera Apples supportsida för anvisningar.

Aktivera eller inaktivera Time Machine-skydd

Aktivera eller inaktivera Time Machine-skydd:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Välj fliken **Anti-Ransomware**.
3. Aktivera eller inaktivera reglaget **Time Machine-skydd**.

9.11. Löser problem

Bitdefender Antivirus for Mac upptäcker och informerar dig automatiskt om en serie problem som kan påverka säkerheten för ditt system och dina data. På så sätt kan du åtgärda säkerhetsrisker enkelt och snabbt.

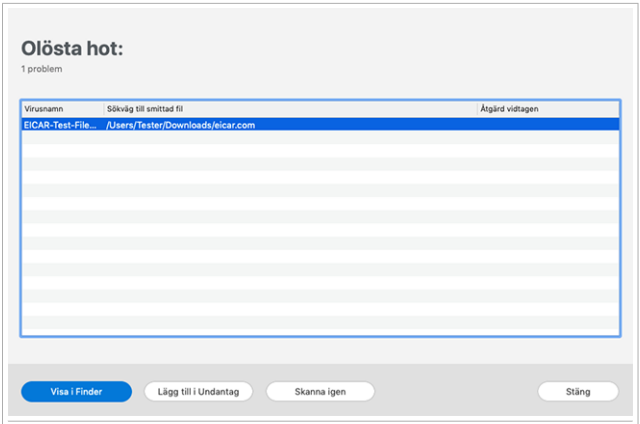
Att åtgärda problemen som indikeras av Bitdefender Antivirus for Mac är ett snabbt och enkelt sätt att säkerställa optimalt skydd för system och data.

Upptäckta problem omfattar:

- Den nya virusinformationsuppdateringen hämtades inte från våra servrar.
- Virus har upptäckts på ditt system och produkten kan inte desinfektera dem automatiskt.
- Realtidsskydd är inaktiverat.

Kontrollera och åtgärda upptäckta problem:

1. Om Bitdefender inte har några varningar är statusfältet grönt. När ett säkerhetsproblem upptäcks byter statusfältet färg till röd.
2. Kontrollera beskrivningen för mer information.
3. När ett problem upptäcks klickar du på motsvarande knapp för att vidta åtgärd.



Fönstret Ej åtgärdade hot

Listan med ej åtgärdade hot uppdateras efter varje systemskanning oavsett om skanningen sker automatiskt i bakgrunden eller startas av dig.

Du kan välja att vidta följande åtgärder för ej åtgärdade hot:

- Ta bort manuellt. Vidta den här åtgärden för att ta bort infektioner manuellt.
- Lägg till i Undantag. Den här åtgärden är inte tillgänglig för virus som hittas i arkiv.

9.12. Aviseringar

Bitdefender för endetaljerad logg över händelser som rör dess aktivitet på din dator. Varje gång något som är relevant för säkerheten för system eller data inträffar, läggs ett nytt meddelande till i området Bitdefender-meddelanden, på ett liknande sätt som när ett nytt e-postmeddelande visas i inkorgen.

Meddelanden är ett viktigt verktyg för att övervaka och hantera ditt Bitdefender-skydd. Exempelvis kan du enkelt kontrollera om uppdateringen utfördes med framgång, om hot eller säkerhetsrisker hittades på din dator osv. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som vidtagits av Bitdefender.

Öppna meddelandeloggen genom att klicka på **Meddelanden** på navigeringsmenyn på Bitdefender-gränssnittet. Varje gång en kritisk händelse inträffar kan du se en räknare på 2-ikonen.

Beroende på typ och allvarlighetsgrad grupperas meddelanden i:

- **Kritiska** händelser indikerar kritiska problem. Du bör kontrollera dem omedelbart.
- **Varnings**-händelser anger problem som inte är kritiska. Du bör kontrollera dem och åtgärda dem när du har tid.
- **Informations**-händelser indikerar lyckade åtgärder.

Klicka på varje flik för att hitta mer information om de genererade händelserna. Kort information visas med ett klicka på varje händelserubrik, nämligen: en kort beskrivning, åtgärden Bitdefender vidtog för den när den inträffade samt datum och tid när den inträffade. Alternativ kan finnas för att vidta ytterligare åtgärder om det behövs.

För att det ska vara enklare att hantera loggade händelser har meddelandefönstret alternativ för att ta bort alla händelser i det avsnittet eller markera dem som lästa.

9.13. Uppdateringar

Nya hot hittas och identifieras varje dag. Därför är det mycket viktigt att du ser till att Bitdefender Antivirus for Mac är uppdaterad med de senaste virusuppdateringarna.

Uppdateringarna av virusinformation utförs i farten, vilket betyder att filerna som ska uppdateras ersätts efter hand. På detta sätt kommer inte uppdateringen att påverka produktaktiviteten, och samtidigt, kommer alla sårbarheter att exkluderas.

- Om Bitdefender Antivirus for Mac är uppdaterad kan den hitta de senast upptäckta hoten och rensa bort smittade filer.
- Om Bitdefender Antivirus for Mac inte är uppdaterad kan den inte hitta och ta bort se senaste hoten som upptäckts av Bitdefenders labb.

9.13.1. Begär en uppdatering

Du kan begära en uppdatering manuellt när du vill.

En aktiv Internet-uppkoppling krävs för att kontrollera efter tillgängliga uppdateringar och hämta dem.

Begär en uppdatering manuellt:

1. Klicka på knappen **Åtgärder** i menyfältet.

2. Välj **Uppdatera hotinformationsdatabas**.

Alternativt kan du begära en uppdatering manuellt genom att trycka på CMD + U.

Du kan se uppdateringsförloppet och hämtade filer.

9.13.2. Hämta uppdateringar via en proxyserver

Bitdefender Antivirus for Mac kan endast uppdatera 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 växla till en direkt Internet-anslutning med jämna mellanrum för att få hotinformationsuppdateringar.

9.13.3. 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 systemomstart för att installationen av nya filer ska starta. Som standard fortsätter Bitdefender Antivirus for Mac att fungera med de föregående filerna tills du startar om systemet, om en uppdatering kräver en omstart. I det fallet stör inte uppdateringsprocessen användarens arbete.

När en produktuppdatering är slutförd talar ett popup-fönster om att du ska starta om systemet. Om du missar det meddelandet kan du antingen klicka på **Starta om för att uppgradera** från menyfältet eller starta om systemet manuellt.

9.13.4. Hitta information om Bitdefender Antivirus for Mac

Du hittar information om den version av Bitdefender Antivirus for Mac du har installerat i fönstret **Om**. I samma fönster kan du öppna och läsa prenumerationsavtalet, sekretesspolicyn och visa Open-source-licenser.

Öppna fönstret Om:

1. Öppna Bitdefender Antivirus for Mac.
2. Klicka på Bitdefender Antivirus for Mac i menyfältet och välj **Om Antivirus för Mac**.

10. KONFIGURERA EGENSKAPER

Det här kapitlet omfattar följande ämnen:

10.1. Öppna Egenskaper

Öppna fönstret Bitdefender Antivirus for Mac-egenskaper:

1. Gör något av följande:
   - Klicka på **Egenskaper** på navigeringsmenyn i Bitdefender-gränssnittet.
   - Klicka på Bitdefender Antivirus for Mac i menyfältet och välj **Egenskaper**.
   - Tryck Command-Komma (,).

10.2. Skyddsegenskaper

I fönstret för skyddsegenskaper kan du konfigurera det allmänna skanningssättet. Du kan konfigurera vilka åtgärder som ska vidtas för smittade och misstänkta filer som hittas och andra allmänna inställningar.

- **Bitdefender Shield.** Bitdefender Shield tillhandahåller realtidsskydd mot flera olika 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 det, gör det under så kort tid som möjligt. Om Bitdefender Shield inaktiveras är du inte skyddad mot hot.
- **Skanna endast nya och/eller ändrade filer.** Markera den här kryssrutan för att ställa in Bitdefender Antivirus for Mac till att endast skanna filer som inte skannats tidigare eller som har ändrats sedan den senaste skanningen.

  Du kan välja att inte tillämpa 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 exkludera säkerhetskopieringsfiler från skanning. Om de smittade filerna återställs vid ett senare tillfälle hittar Bitdefender Antivirus for Mac dem automatiskt och vidtar korrekt åtgärd.

10.3. Avancerade inställningar

Du kan välja en allmän åtgärd som ska vidtas för alla problem och misstänkta objekt som hittas under en skanningsprocess.

Åtgärd för smittade objekt

Försök att desinfektera eller flytta till karantän - Om infekterade filer upptäcks, försöker Bitdefender att desinfektera dem (ta bort skadlig kod) eller flytta dem till karantän.

Vidta ingen åtgärd - Ingen åtgärd kommer att tas på de upptäckta filerna.

Åtgärd för misstänkta objekt

Flytta filer till karantän - Om misstänkta filer upptäcks flyttar Bitdefender dem till karantän.

Vidta ingen åtgärd - Ingen åtgärd kommer att tas på de upptäckta filerna.

10.4. Specialerbjudanden

När kampanjerbjudanden är tillgängliga ställs Bitdefender-produkten in på att meddela dig via ett popup-fönster. Det här ger dig möjlighet att dra nytta ab fördelaktiga priser och hålla dina enheter skyddade under en längre tidsperiod.

För att slå av eller på meddelanden om specialerbjudanden:

1. Klicka på **Egenskaper** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Välj fliken **Övrigt**.
3. Aktivera eller inaktivera reglaget **Mina erbjudanden**.

Alternativet **Mina erbjudanden** är aktiverat som standard.

11. VPN

Det här kapitlet omfattar följande ämnen:

11.1. Om VPN

Med Bitdefender VPN kan du hålla dina data privata varje gång du ansluter till osäkra trådlösa nätverk på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personuppgifter eller försök att göra din enhets IP-adress åtkomlig för hackare undvikas.

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter till för att säkra din anslutning, kryptera data med kryptering i bankklass och dölja din IP-adress oavsett var du är. Din trafik omdirigeras via en separat server och gör det därmed näst intill omöjligt att identifiera din enhet bland de myriader av andra enheter som använder våra tjänster. När du är ansluten till Internet via Bitdefender VPN, kan du dessutom ha åtkomst till innehåll som i normala fall är begränsat i vissa områden.

Notera

Vissa länder censurerar Internet och därför kan användning av VPN på deras territorier vara förbjudet enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om regelverken i det land du befinner dig i och de risker du kan utsättas för.

11.2. Öppna VPN

Det finns tre sätt att öppna Bitdefender VPN-appen:

- Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.

  Klicka på **Öppna** i Bitdefender VPN-kortet.

- Klicka på -ikonen från menyfältet.

- Gå till mappen Program, öppna mappen Bitdefender och dubbelklicka sedan på Bitdefender VPN-ikonen.

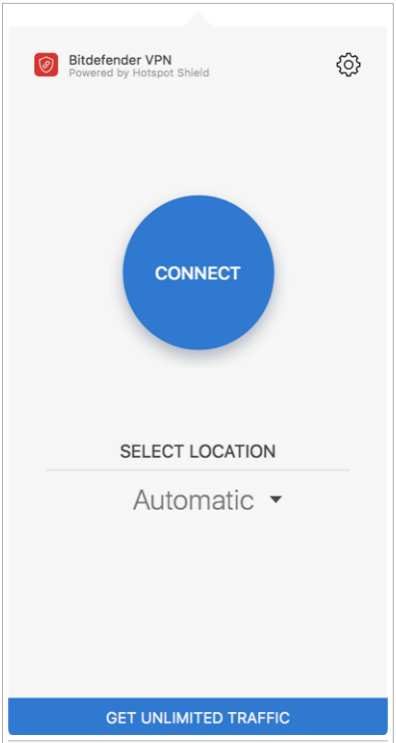
Första gången du öppnar appen uppmanas du att tillåta Bitdefender att lägga till konfigurationer. Genom att tillåta att Bitdefender lägger till konfigurationer samtycker du till att all nätverksaktivitet för enheten kan filtreras eller övervakas när du använder VPN-appen.

Notera
Bitdefender VPN-appen kan endast installeras på macOS Sierra (10.12.6), macOS High Sierra (10.13.6), eller macOS Mojave (10.14 eller senare).

11.3. Gränssnitt

VPN-gränssnittet visar status för appen, ansluten eller frånkopplad. Serverplatsen för användare med den fria versionen ställs automatiskt av Bitdefender till den lämpligaste servern, medan premium användare har möjlighet att ändra serverplatsen de vill ansluta till genom att välja den från **VÄLJ PLATS** listan. Mer information om VPN-prenumerationer finns på "*Prenumerationer*" (p. 214).

Klicka bara på statusen som visas överst på skärmen för att ansluta eller koppla ifrån. Menyrad ikonen är svart när VPN är ansluten och vit när VPN-enheten är frånkopplad.



VPN-gränssnitt

När du är ansluten visas den förflutna tiden under den nedre delen av gränssnittet. För att få åtkomst till fler funktioner klickar du på ikonen ⚙ upptill till höger:

- **Mitt Konto** - information om ditt Bitdefender-konto och VPN-prenumeration visas. Klicka på **Växla konto** om du vill logga in med ett annat konto.
- **Inställningar** - beroende på dina behov kan du anpassa produktens beteende:
  - ställ in VPN att köra vid systemstart
  - ta emot meddelanden när VPN automatiskt ansluter eller kopplar ifrån
- **Uppgradera till Premium** - om du använder gratisversionen av produkten kan du uppgradera till premiumplanen härifrån. Klicka på **UPPGRADERA**

NU för att omdirigeras till en webbsida varifrån du kan köpa en prenumeration.

- **Support** - du omdirigeras till vår supportcenterplattform varifrån du kan läsa en användbar artikel om hur du använder Bitdefender VPN.
- **Om** - information om den installerade versionen visas.
- **Avsluta** - lämna appen.

11.4. Prenumerationer

Bitdefender VPN erbjuder utan kostnad en daglig trafikkovot på 200 MB per enhet för att säkra anslutningen varje gång ditt team behöver det.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en serverplats enligt ditt teams önskemål, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst från panelen **Mina prenumerationer** som finns på ditt Bitdefender-konto.

Bitdefender Premium VPN-prenumerationen är oberoende av den prenumerationen på Bitdefender Small Office Security, vilket innebär att du kan använda den under hela dess tillgänglighet. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Small Office Security fortfarande är aktiv återgår du till gratisversionen.

Bitdefender VPN är en produkt över flera plattformar, tillgänglig i Bitdefender-produkter kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kan du använda din prenumeration på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

12. BITDEFENDER CENTRAL

Det här kapitlet omfattar följande ämnen:

12.1. Om Bitdefender Central

Bitdefender Central är en plattform vart du har tillgång till produktens alla onlinefunktioner och tjänster och kan fjärransluta viktiga uppgifter på enheterna Bitdefender är installerat på. Du kan logga in på ditt Bitdefender-konto från vilken dator eller mobil enhet som helst som är ansluten till Internet genom att gå till https://central.bitdefender.com, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

Så här installerar du Bitdefender Central-appen på dina enheter:

- **På Android** - sök Bitdefender Central på Google Play och hämta och installera appen. Följ stegen för att slutföra installationen.
- **På Android** - sök Bitdefender Central på App Store och hämta och installera appen. Följ stegen för att slutföra installationen.

När du är inloggad kan du börja göra följande:

- Hämta och installera Bitdefender på Windows, macOS, iOS och Android. De produkter som är tillgängliga för hämtning är:
  - Bitdefender Antivirus for Mac
  - Bitdefender Windows-produktlinjen
  - Bitdefender Mobile Security för Android
  - Bitdefender Mobile Security för iOS
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter till nätverket och hantera dem var du än är.

12.2. Öppna Bitdefender Central

Det finns flera sätt att öppna Bitdefender Central. Beroende på vilken uppgift du vill utföra kan du använda någon av följande möjligheter:

- Från Bitdefender Antivirus for Macs huvudgränssnitt:
  1. Klicka på länken **Gå till ditt konto** längst ned till höger på skärmen.
- Från din webbläsare:
  1. Öppna en webbläsare på en enhet med Internet-åtkomst.
  2. Gå till: https://central.bitdefender.com.
  3. Logga in till ditt -konto med e-postadress och lösenord.
- Från din Android- eller iOS-enhet:

  Öppna Bitdefender Central-appen som du har installerat.

Notera
I det här materialet har vi inkluderat de alternativ du hittar i webbgränssnittet.

12.3. Tvåfaktorautentisering

2-faktorautentiseringsmetoden ger ett extra säkerhetslager till ditt Bitdefender-konto, genom att kräva en autentiseringskod förutom dina inloggningsuppgifter. På det här sättet förhindrar du kontokapning och håller vissa typer av cyberattacker borta, som keyloggers, råstyrke- eller ordlisteattacker.

Aktivera tvåfaktorautentisering

Genom att aktivera tvåfaktorautentisering gör du ditt Bitdefender-konto mycket säkrare. Din identitet verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera status för din prenumeration eller köra uppgifter via fjärrstyrning på dina enheter.

Aktivera tvåfaktorautentisering:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.
3. Klicka på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Klicka på **KOM IGÅNG**.

   Välj en av följande metoder:

- **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in till ditt Bitdefender-konto.

  Om du vill använda en autentiseringsapp, men inte är säker på vad du ska välja, finns det en lista över de autentiseringsappar vi rekommenderar.

  a. Klicka på **ANVÄND AUTENTISERINGSAPP** för att börja.

  b. Logga in på en Android- eller iOS-baserad enhet genom att använda enheten för att skanna QR-koden.

  För att logga in på en bärbar eller stationär dator kan du manuellt lägga till den visade koden.

  Klicka på **FORTSÄTT**.

  c. Infoga koden som appen gav eller den som visas i föregående steg och klicka sedan på **AKTIVERA**.

- **E-post** - varje gång du loggar in på ditt Bitdefender-konto skickas en verifieringskod till din e-postinkorg. Kontrollera ditt e-postkonto och skriv in den angivna koden.

  a. Klicka på **ANVÄND E-POST** för att starta.

  b. Kontrollera ditt e-postkonto och skriv in den angivna koden.

  c. Klicka på **AKTIVERA**.

Ifall du vill sluta använda tvåfaktorautentisering:

1. Klicka på **STÄNG AV TVÅFAKTORAUTENTISERING**.
2. Kontrollera din app eller ditt e-postkonto och skriv in koden du har fått.
3. Bekräfta ditt val.

12.4. Lägga till betrodda enheter

För att se till att bara du kan komma åt ditt Bitdefender-konto kan vi kräva en säkerhetskod först. Om du vill hoppa över det här steget varje gång du ansluter från samma enhet, rekommenderar vi att du utser den till en betrodd enhet.

Lägga till enheter som betrodda enheter:

1. Öppna Bitdefender Central.
2. Klicka på ikonen uppe till höger på skärmen.

3. Klicka på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Klicka på **Betrodda enheter**.
6. Listan över de enheter som Bitdefender är installerad på visas. Klicka på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och att din prenumeration är giltig.

12.5. Mina prenumerationer

Bitdefender Central-plattformen ger dig möjlighet att enkelt hantera de prenumerationer du har för alla dina enheter.

12.5.1. Aktivera prenumeration

En prenumeration kan aktiveras under installationsprocessen genom att använda ditt Bitdefender-konto. Tillsammans med aktiveringsprocessen börjar prenumerationens giltighet att räknas ned.

Om du har köpt en aktiveringskod från en av våra återförsäljare eller om du fått en i present, kan du lägga till dess tillgänglighet till din Bitdefender-prenumeration.

Följ de här stegen för att aktivera en prenumeration med en aktiveringskod:

1. Öppna Bitdefender Central.
2. Klicka på ikonen ☰ som finns i det övre vänstra hörnet av fönstret och välj sedan panelen **Min prenumerationer**.
3. Klicka på knappen **AKTIVERINGSKOD** och skriv sedan in koden i motsvarande fält.
4. Klicka på **AKTIVERA** för att fortsätta.

Prenumerationen är nu aktiv.

För att börja installera produkten på dina enheter, se *"Installerar Bitdefender Antivirus for Mac"* (p. 184).

12.5.2. Köp prenumeration

Du kan köpa en prenumeration direkt från ditt Bitdefender-konto genom att följa de här stegen:

1. Öppna Bitdefender Central.
2. Klicka på ikonen ☰ som finns i det övre vänstra hörnet av fönstret och välj sedan panelen **Min prenumerationer**.
3. Klicka på länken **Köp nu**. Du omdirigeras till en webbsida varifrån du kan göra dina köp.

Så fort du avslutar processen visas tillgängligheten för prenumerationen i det nedre högra hörnet av produktens huvudgränssnitt.

12.6. Mina enheter

Området **Mina enheter** i ditt Bitdefender-konto ger dig möjlighet att installera, hantera och vidta fjärrstyrningsåtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till Internet. Enhetskorten visar enhetsnamn, skyddsstatus och om det finns säkerhetsrisker som påverkar enheternas skydd.

12.6.1. Anpassa din enhet

För att enkelt identifiera dina enheter kan du anpassa enhetsnamnet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.
4. Välj **Inställningar**.
5. Skriv in ett nytt namn i fältet **Enhetsnamn**, klicka därefter på **SPARA**.

Du kan skapa och tilldela en ägare för varje enhet för bättre hantering:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.
4. Välj **Profil**.

5. Klicka på **Lägg till ägare** och fyll i motsvarande fält. Anpassa profilen genom att lägga till ett foto, välj ett födelsedatum och lägg till en e-postadress och ett telefonnummer.
6. Klicka på **LÄGG TILL** för att spara profilen.
7. Välj önskad ägare från listan **Enhetsägare** och klicka på **TILLDELA**.

12.6.2. Fjärraktiviteter

Fjärruppdatera Bitdefender på en enhet:

1. Öppna Bitdefender Central.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på ⋮ -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

När du klickar på ett enhetskort är följande flikar tillgängliga:

- **Kontrollpanel**. I det här fönstret kan du visa information om den valda enheten, kontrollera dess skyddsstatus och hur många hot som har blockerats de senaste sju dagarna. Skyddsstatus kan vara grönt när det inte finns några problem som påverkar enheten, gult när enheten behöver åtgärdas från din sida eller rött när enheten är utsatt för risk. När det finns problem som påverkar enheten klickar du på rullgardinsmenyn i det övre statusområdet för att se mer information. Härifrån kan du manuellt åtgärda problem som påverkar dina enheters säkerhet.
- **Skydd**. Från det här fönstret kan du fjärrstyra en snabb- eller fullständig skanning på dina enheter. Klicka på knappen **SKANNA** för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och det finns en rapport från den senaste skanningen med den viktigaste informationen. Mer information om de här två skanningsprocesserna finns i *"Skanna din Mac"* (p. 195).

13. VANLIGA FRÅGOR

Hur kan jag testa Bitdefender Antivirus for Mac innan jag tar en prenumeration?

Du är en ny Bitdefender-kund och vill testa vår produkt innan du köper den. Utvärderingsperioden är 30 dagar och du kan fortsätta använda den installerade produkten endast om du köper en Bitdefender-prenumeration. För att testa Bitdefender Antivirus for Mac måste du:

1. Skapa ett Bitdefender-konto genom att följa dessa steg:
   a. Gå till: https://central.bitdefender.com.
   b. Skriv in den önskade informationen i de motsvarande fälten. De uppgifter du lämnar här kommer att hållas konfidentiella.
   c. Innan du går vidare måste du godkänna användningsvillkoren. Öppna användningsvillkoren och läs dem noggrant eftersom de innehåller de villkor under vilka du får använda Bitdefender.

      Dessutom kan du öppna och läsa sekretesspolicyn.
   d. Klicka på **SKAPA KONTO**.
2. Hämta Bitdefender Antivirus for Mac så här:
   a. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
   b. Välj ett av två möjliga alternativ:
      - **Skydda den här enheten**
        i. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.
        ii. Spara installationsfilen.
      - **Skydda andra enheter**
        i. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.
        ii. Klicka på **SKICKA NEDLADDNINGSLÄNK**.
        iii. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**.

Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

iv. Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.

c. Kör den Bitdefender-produkt du har hämtat.

Skanningsloggen anger att det fortfarande finns olösta objekt. Hur tar jag bort dem?

De olösta objekten i skanningsloggen kan vara:

- arkiv med begränsad åtkomst (xar, rar, m.fl.)

  Lösning: Använd alternativet **Visa i Sökaren** för att hitta filen och ta bort den manuellt. Se till att du tömmer Papperskorgen.

- inkorgar med begränsad åtkomst (Thunderbird, m.fl.)

  Lösning: Använd appen för att ta bort posten som innehåller den smittade filen.

- Innehåll i säkerhetskopior

  Lösning: Aktivera alternativet **Skanna inte innehåll i säkerhetskopior** i Skyddsegenskaper eller **Lägg till i undantag** de hittade filerna.

  Om de smittade filerna återställs vid ett senare tillfälle hittar Bitdefender Antivirus for Mac dem automatiskt och vidtar korrekt åtgärd.

> **Notera**
> File med begränsad åtkomst innebär filer som Bitdefender Antivirus for Mac bara kan öppna, men inte ändra.

Var hittar jag information om produktens aktivitet?

Bitdefender för en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden i samband med enhetens aktivitet. För att komma åt den här informationen klickar du på **Meddelanden** på navigeringsmenyn på Bitdefender-gränssnittet.

Kan jag uppdatera Bitdefender Antivirus for Mac genom en proxyserver?

Bitdefender Antivirus for Mac kan endast uppdatera 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 växla till en direkt Internet-anslutning med jämna mellanrum för att få hotinformationsuppdateringar.

Hur tar jag bort Bitdefender Antivirus for Mac?

Ta bort Bitdefender Antivirus for Mac genom att följa dessa steg:

1. Öppna ett **Sökar**-fönster och gå sedan till Program-mappen.
2. Öppna Bitdefender-mappen och dubbelklicka på BitdefenderUninstaller.
3. Klicka på **Avinstallera** och vänta tills processen slutförs.
4. Klicka på **Stäng** för att avsluta.

> **Viktigt**
> Om fel uppstår kan du kontakta Bitdefender kundtjänst enligt "Kontakta oss" (p. 289).

Hur tar jag bort TrafficLight-tilläggen från min webbläsare?

- Följ de här stegen för att ta bort TrafficLight-tilläggen från Mozilla Firefox:
  1. Gå till **Verktyg** och välj **Tillägg**.
  2. Välj **Tillägg** i den vänstra kolumnen.
  3. Markera tillägget och klicka på **Ta bort**.
  4. Starta om webbläsaren för att borttagningsprocessen ska slutföras.
- Följ de här stegen för att ta bort TrafficLight-tilläggen från Google Chrome:
  1. Längst upp till höger klickar du på **Mer** .
  2. Gå till **Fler verktyg** och välj **Tillägg**.
  3. Klicka på ikonen **Ta bort...** bredvid det tillägg du vill ta bort.
  4. Klicka på **ta bort** för att bekräfta borttagningsprocessen.

- Följ de här stegen för att ta bort Bitdefender TrafficLight från Safari:
  1. Gå till **Egenskaper** eller tryck **Command-Komma(,)**.
  2. Välj **Tillägg**.

     En lista med installerade tillägg visas.
  3. Välj tillägget Bitdefender TrafficLight och klicka sedan på **Avinstallera**.
  4. Klicka på **Avinstallera** en gång till för att bekräfta borttagningsprocessen.

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du öppnar, laddar ner eller laddar upp innehåll på Internet. För att du ska vara säker när du surfar på webben rekommenderar vi att du använder Bitdefender VPN när du:

- vill ansluta till publika trådlösa nätverk
- vill öppna innehåll som i normala fall är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, kreditkortsinformation, mm.)
- vill dölja din IP-adress

Kommer Bitdefender VPN att ha en negativ inverkan på min enhets batteritid?

Bitdefender VPN är utformat för att skydda dina personuppgifter, dölja din IP-adress när du är ansluten till oskyddade trådlösa nätverk och få tillgång till begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort det när du är offline.

Varför upplever jag att Internet blir långsammare när jag är ansluten till Bitdefender VPN?

Bitdefender VPN är utformad för att ge dig en lätt upplevelse när du surfar på webben. Men din internetanslutning eller avståndet av server du ansluter till kan orsaka avmattningen. Om det inte är ett måste att ansluta från din plats till en fjärrserverad 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 till dig.

MOBILE SECURITY FOR IOS

14. VAD ÄR BITDEFENDER MOBILE SECURITY FOR IOS

Onlineaktiviteter som att betala räkningar, boka semestrar eller köpa varor och tjänster är bekvämt och problemfritt. Men precis som många aktiviteter som utvecklats på Internet kan de medföra risker och om säkerhetsdetaljerna ignoreras, kan personlig information hackas. Och vad är viktigare än att skydda data som lagras på onlinekonton och på en personlig smartphone?

Med Bitdefender Mobile Security for iOS kan du:

- Skydda dina data när du använder osäkra trådlösa nätverk.
- Akta dig för potentiellt skadliga webbsidor och domäner när du är online.
- Kontrollera om något har läckt från de onlinekonton du använder varje dag.
- Hitta, lås och radera data från din enhet om den blir stulen eller försvinner.

Bitdefender Mobile Security for iOS levereras utan kostnad och kräver aktivering med ett Bitdefender-konto.

15. KOMMA IGÅNG

Enhetskrav

Bitdefender Mobile Security for iOS fungerar på alla enheter som kör iOS 11.2 och senare och behöver en aktiv internetanslutning för att aktiveras och upptäcka om något dataläckage har inträffat på dina onlinekonton.

Installerar Bitdefender Mobile Security for iOS

- **Från Bitdefender Central**
  - På iOS
    1. Öppna Bitdefender Central.
    2. Tryck på -ikonen i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
    3. Tryck på **INSTALLERA SKYDD** och därefter på **Skydda den här enheten**.
    4. Välj ägare av enheten. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    5. Du omdirigeras till appen **App Store**. På App Store-skärmen trycker du på installationsalternativet.
  - På Windows, macOS, Android
    1. Öppna Bitdefender Central.
    2. Tryck på -ikonen i det övre vänstra hörnet på skärmen och sedan på **Mina enheter**.
    3. Tryck på **INSTALLERA SKYDD** och därefter på **Skydda den här övriga enheter**.
    4. Välj ägare av enheten. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    5. Tryck på **SKICKA NEDLADDNINGSLÄNK**.
    6. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

7. Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och tryck på motsvarande hämtningsknapp.

- **Från App Store**

  Sök efter Bitdefender Mobile Security for iOS för att hitta och installera appen.

Ett introduktionsfönster som innehåller information om produktfunktionerna visas första gången du öppnar appen. Tryck på **Kom igång** för att fortsätta till nästa fönster.

Innan du går igenom valideringsstegen måste du samtycka till prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Mobile Security for iOS.

Tryck på **Fortsätt** för att gå vidare till nästa fönster.

Logga in till ditt Bitdefender-konto

För att använda Bitdefender Mobile Security for iOS måste du koppla din enhet till ett Bitdefender-, Facebook-, Google- eller Microsoft-konto genom att logga in på kontot från appen. Första gången du öppnar appen ombes du att logga in på ett konto.

Så här kopplar du din enhet till ett Bitdefender-konto:

1. Skriv e-postadressen till ditt Bitdefender-konto i motsvarande fält och tryck sedan på **NÄSTA**. Om du inte har något Bitdefender-konto och vill skapa ett väljer du motsvarande länk och följer sedan anvisningarna på skärmen tills kontot är aktiverat.

   För att logga in med ett Facebook-, Google- eller Microsoft-konto trycker du på den tjänst du vill använda från området **ELLER LOGGA IN MED**. Du omdirigeras till inloggningssidan för den valda tjänsten. Följ instruktionerna för att koppla kontot till Bitdefender Mobile Security for iOS.

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

2. Skriv ditt lösenord och tryck sedan på **LOGGA IN**.

Härifrån kan du även nå sekretesspolicyn för Bitdefender.

Kontrollpanel

Tryck på Bitdefender Mobile Security for iOS-ikonen i enhetens applåda för att öppna programgränssnittet.

Första gången du öppnar appen ombes du att tillåta att Bitdefender att skicka aviseringar. Tryck på **Tillåt** för att bli informerad varje gång Bitdefender måste kommunicera något som är relevant för din app. Hantera Bitdefender-aviseringar genom att gå till Inställningar > Aviseringar > Mobile Security.

För att få åtkomst till den information du behöver trycker du på motsvarande ikon längst ned på skärmen.

VPN
Upprätthåll din integritet oavsett vilket nätverk du är ansluten till genom att se till att din internetkommunikation är krypterad. Mer information finns på *"VPN"* (p. 231).

Webbskydd
Var säker medan du surfar på nätet och varje gång mindre säkra appar försöker komma åt osäkra domäner. Mer information finns på *"Webbskydd"* (p. 234).

Kontointegritet
Ta reda på om dina e-postkonton har läckts eller inte. Mer information finns på *"Kontointegritet"* (p. 237).

Anti-Theft
Hitta och lås din enhet för att förhindra att din personliga information hamnar i fel händer. Mer information finns på *"Anti-Theft"* (p. 239).

Se ytterligare alternativ genom att trycka på ••• -ikonen på din enhet från programmets startskärm. Följande alternativ visas:

- **Återföra köp** - härifrån kan du återföra den Premium VPN-prenumeration du har köpt via ditt iTunes-konto.
- **Inställningar** - härifrån har du åtkomst till VPN-inställningarna, enligt följande:

- **Avtal** - du kan läsa villkoren enligt vilka du använder Bitdefender VPN-tjänsten. Om du trycker på **Jag samtycker inte längre** kan du inte använda Bitdefender VPN förrän du trycker på **Jag samtycker**.
- **Öppen Wi-Fi-varning** - du kan aktivera eller inaktivera produktaviseringen som visas varje gång du ansluter till ett osäkert Wi-Fi-nätverk. Syftet med den här aviseringen är att hjälpa dig att se till att dina uppgifter är privata och säkra genom att använda Bitdefender VPN.

- **Feedback** - härifrån kan du starta standarde-postklienten för att skicka feedback till oss om appen.
- **Appinfo** - härifrån har du tillgång till information om den installerade versionen och till prenumerationsavtal, sekretesspolicy och öppen källkodslicenser.

16. VPN

Med Bitdefender VPN kan du hålla dina data privata varje gång du ansluter till osäkra trådlösa nätverk på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personuppgifter eller försök att göra din enhets IP-adress åtkomlig för hackare undvikas.

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter till för att säkra din anslutning, kryptera data med kryptering i bankklass och dölja din IP-adress oavsett var du är. Din trafik omdirigeras via en separat server och gör det därmed näst intill omöjligt att identifiera din enhet bland de myriader av andra enheter som använder våra tjänster. När du är ansluten till Internet via Bitdefender VPN, kan du dessutom ha åtkomst till innehåll som i normala fall är begränsat i vissa områden.

Notera
Kina, Irak, Förenade Arabemiraten, Turkiet, Vitryssland, Oman, Iran och Ryssland har Internet-censur och därför kan användning av VPN:er på deras territorier vara förbjudet i lag. Därför är Bitdefender VPN-funktionen inte tillgänglig i deras territorier.

Så här aktiverar du Bitdefender VPN:

1. Tryck på -ikonen längst ned på skärmen.
2. Tryck på **Anslut** varje gång du vill fortsätta vara skyddad när du ansluter till osäkra trådlösa nätverk.

   Tryck på **Koppla ifrån** när du vill inaktivera anslutningen.

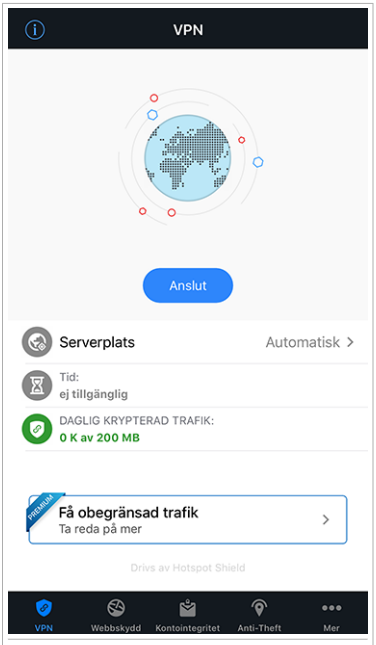
Notera
Första gången du aktiverar VPN ombes du att tillåta att Bitdefender konfigurerar VPN-konfigurationer som övervakar nätverkstrafiken. Tryck på **Allow** för att fortsätta. Om en autentiseringsmetod (fingeravtryck eller PIN-kod) har ställts in för att skydda din smartphone måste du använda den.

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 premium prenumeration och vill ansluta till en server på din vilja, tryck på **VÄLJ PLATS** i VPN-funktionen och välj sedan den önskade

platsen. Mer information om VPN-prenumerationer finns på *"Prenumerationer" (p. 232)*.



VPN

16.1. Prenumerationer

Bitdefender VPN erbjuder utan kostnad en daglig trafikkovot på 200 MB per enhet för att säkra anslutningen varje gång ditt team behöver det.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en serverplats enligt ditt teams önskemål, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst från panelen **Mina prenumerationer** som finns på ditt Bitdefender-konto.

Bitdefender Premium VPN-prenumerationen är oberoende av den prenumerationen på Bitdefender Small Office Security, vilket innebär att du kan använda den under hela dess tillgänglighet. Om Bitdefender Premium

VPN-prenumerationen går ut, men den för Bitdefender Small Office Security fortfarande är aktiv återgår du till gratisversionen.

Bitdefender VPN är en produkt över flera plattformar, tillgänglig i Bitdefender-produkter kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kan du använda din prenumeration på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

17. WEBBSKYDD

Bitdefender Web Protection ser till att du har en säker surfupplevelse genom att varna dig om potentiellt skadliga webbsidor och när mindre säkra installerade appar försöker komma åt osäkra domäner.

Cuando una URL apunta a un sitio web conocido de phishing o fraudulento o a contenidos maliciosos como spyware o virus, se bloquea la página web y se muestra una alerta. Samma sak händer när installerade appar försöker komma åt skadliga domäner.

Aktivera webbskydd:

1. Tryck på -ikonen längst ned på skärmen.
2. Tryck på **TESTA WEBBSKYDD**.
3. Välj en av de kostnadsfria utvärderingsperioderna och bekräfta sedan betalningsinformationen.
4. Aktivera webbskyddsomkopplaren.

Notera
Första gången du aktiverar webbskydd kan du ombes att tillåta att Bitdefender konfigurerar VPN-konfigurationer som övervakar nätverkstrafiken. Tryck på **Allow** för 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 osäkra domäner arbetar webbskyddet tillsammans med VPN-tjänsterna.

Viktigt
Om du befinner dig i ett område där användning av en VPN-tjänst är förbjuden enligt lag är inte funktionen för webbskydd tillgänglig.

17.1. Bitdefender-varningar

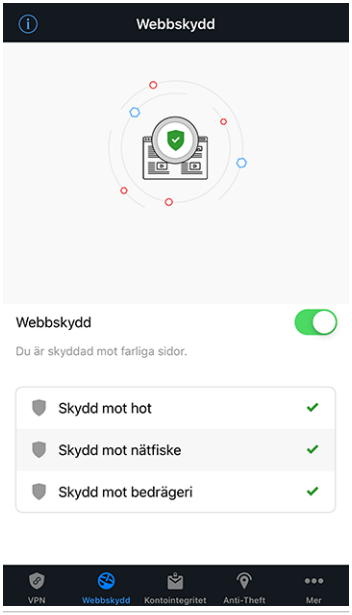
Varje gång du försöker besöka en webbplats som är klassad som osäker, blockeras webbsidan. För att göra det medveten om händelsen meddelas du av Bitdefender i meddelandecentret och i din webbläsare. Den här sidan innehåller information som webbplats-URL och upptäckta hot. Du måste bestämma vad som ska göras härnäst.

Du meddelas även i meddelandecentret varje gång en mindre säker app försöker komma åt osäkra domäner. Tryck på det visade meddelandet för att omdirigeras till fönstret där du kan bestämma vad du ska göra härnäst.

Följande alternativ är tillgängliga i båda fallen:

- Navigera bort från webbplatsen genom att trycka på **TA MIG TILLBAKA TILL SÄKERHETEN**.
- Fortsätt till webbplatsen, trots varningen, genom att trycka på det visade meddelandet och därefter på **Jag vill gå till sidan**.

  Bekräfta ditt val.



Webbskydd

17.2. Prenumerationer

Webbskydd är en prenumerationsbaserad funktion med möjlighet att utvärdera utan kostnad så att du kan bestämma dig för om den uppfyller dina krav. Det finns två typer av prenumerationer att välja mellan: per år och per månad.

Ifall prenumerationen på Bitdefender Web Protection förfaller får du inga varningar när skadligt innehåll öppnas.

Om du har köpt ett av Bitdefender-paketen, som Bitdefender Total Security, så har du obegränsad tillgång till webbskydd.

18. KONTOINTEGRITET

Bitdefender Account Privacy upptäcker om något dataläckage har inträffat på de konton du använder för att betala online, handla eller logga in på olika appar eller webbplatser. Data som kan lagras på ett konto kan vara lösenord, kreditkortsinformation eller bankkontoinformation och om det inte är tillräckligt säkert, kan identitetsstöld eller integritetsöverträdelse inträffa.

Det här kontots sekretesstatus visas direkt efter validering.

Kontrollera om några konton har läckts genom att trycka på **Skanna för läckor**.

För att börja hålla personlig information säker:

1. Tryck på -ikonen längst ned på skärmen.
2. Tryck på **Lägg till** i det övre högra hörnet på skärmen.
3. Skriv din e-postadress i motsvarande fält och tryck sedan **Nästa**.

   Bitdefender måste valideras det här kontot innan personlig information visas. Därför skickas ett e-postmeddelande med en valideringskod till den angivna e-postadressen.
4. Kontrollera din inkorg och skriv sedan den kod du fått i området **Kontointegritet** i din app. Om du inte hittar valideringsmeddelandet i inkorgen kan du titta i skräppostmappen också.

   Sekretesstatus på det validerade kontot visas.

Om läckor hittas på något av dina konton rekommenderar vi att du byter lösenord till dem så fort som möjligt. För att skapa ett starkt och säkert lösenord bör du beakta följande tips:

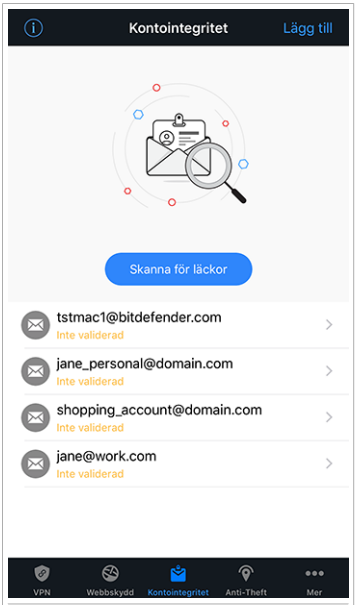
- Gör det minst åtta tecken långt.
- Inkludera gemener och versaler.
- Lägg till minst en siffra eller symbol, som #, @, % eller !.

När du har säkrat ett konto som ingått i ett integritetsintrång kan du bekräfta ändringarna genom att markera identifierade läckor som **Lösta**. Så här gör du:

1. Tryck på ··· bredvid det konto du precis säkrade.
2. Tryck på **Markera som löst**.

Kontot visas i listan **Lösta**.

När alla upptäckta läckor är markerade som **Lösta** visas inte kontot längre som läckt, inte förrän en ny läcka upptäcks.



Kontointegritet

19. ANTI-THEFT

Bitdefender kan hjälpa dig att lokalisera enheten och förhindra att personlig information hamnar i fel händer.

Allt du behöver göra är att aktivera Anti-Theft från enheten och vid behov, gå till **Bitdefender Central** från en webbläsare, var som helst.

Bitdefender Mobile Security for iOS har följande Anti-Theft-funktioner:

Hitta via fjärrstyrning
Visa enhetens aktuella plats på Maps.

Riktigheten för platsen beror på hur Bitdefender kan fastställa den:

- Om GPS:en är aktiverad på enheten kan dess plats preciseras inom några meter så länge som den är inom räckhåll för GPS-satelliter (dvs. inte inuti en byggnad).
- Om enheten är inomhus kan dess plats fastställas till inom ett tiotal meter om Wi-Fi är aktiverat och det finns trådlösa nätverk tillgängliga inom dess räckhåll.
- Annars fastställs platsen med bara informationen från mobilnätverket, som inte kan erbjuda mer noggrannhet än flera hundra meter.

Lås via fjärrstyrning
Lås enhetens skärm via fjärrstyrning.

Fjärradera
Ta bort all personlig information från din förlupna enhet.

Aktivera Anti-Theft

Så här aktiverar du Anti-Theft-funktioner:

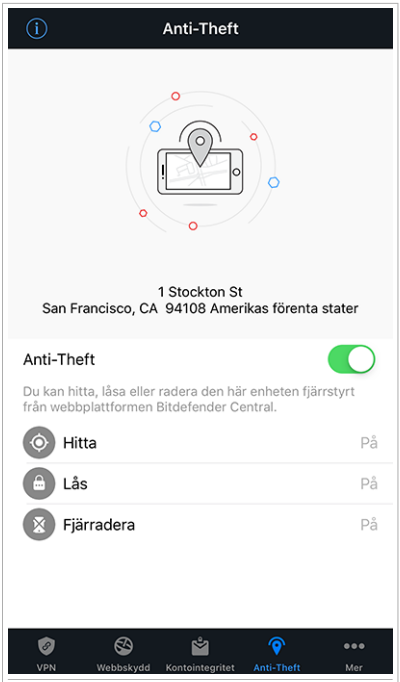
1. Tryck på -ikonen längst ned på skärmen.
2. Aktivera omkopplaren.
3. Ge åtkomst till enhetens plats så att Bitdefender kan hitta den ifall den stjäls eller tappas bort. Den här aviseringen visas bara när du aktiverar Bitdefender Anti-Theft första gången. Hantera Bitdefender-åtkomst genom att gå till Inställningar > Sekretess > Platstjänster > Mobile Security.

4. Första gången du aktiverar Anti-Theft-funktionen på din enhet måste du också installera en MDM-profil (Mobile Device Management). Fortsätt därför med dessa steg:
   a. Tryck på **Tillåt** för att omdirigeras till Inställningar.
   b. Tryck på **Installera** för att installera MDM-profilen (Mobile Device Management) som Bitdefender behöver för att fortsätta aktiveringsprocessen.

      Om en PIN-kod har ställts in för att skydda din smartphone måste du använda den.
   c. Läs informationen som hör till CA-rotcertifikatet och Mobile Device Management.
   d. Om du samtycker till villkoren trycker du på **Installera**.
   e. Tryck på **Lita på** i Remote Management-aviseringen och sedan på **Klar** för att stänga fönstret.

Notera

Om installationen av aktuell Bitdefender MDM-profil misslyckas kan en äldre MDM-profil redan vara installerad och måste tas bort. Därför går du till Inställningar > Allmänt > Enhetshantering > Bitdefender. Välj den upptäckta profilen och tryck sedan på **Ta bort hantering**. Om en PIN-kod har ställts in för att skydda din smartphone måste du använda den. Tryck igen på **Ta bort hantering** för att bekräfta ditt val. Försök att aktivera Anti-Theft igen. Om problemet kvarstår skickar du ett e-postmeddelande till vårt team på bdios@bitdefender.com.



Anti-Theft

Använda Anti-Theft-funktioner från Bitdefender Central (webbstyrning)

Så här kommer du åt Anti-Theft-funktionerna från ditt Bitdefender-konto:

1. Öppna Bitdefender Central.
2. Tryck på -ikonen i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
3. Tryck på önskat enhetskort och sedan på fliken **Anti-Theft**.
4. I det nedersta fältet i fönstret trycker du på ikonen för den funktion du vill använda:

   VISA IP - Visar den senaste IP-adressen för den valda enheten.
   HITTA - Visa enhetens plats på Maps.

   Lås - Lås enheten och ställ in en PIN-kod för att låsa upp den.

 **Radera** - Ta bort alla data från enheten.

Viktigt

När du har raderat en enhet slutar alla Anti-Theft-funktionerna att fungera.

20. BITDEFENDER CENTRAL

Bitdefender Central är webbplattformen där du öppnar produktens onlinefunktioner och tjänster och kan fjärrstyra viktiga åtgärder på de enheter där Bitdefender är installerad. Du kan logga in på ditt Bitdefender-konto från vilken dator eller mobil enhet som helst som är ansluten till Internet genom att gå till https://central.bitdefender.com, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

Så här installerar du Bitdefender Central-appen på dina enheter:

- **På Android** - sök Bitdefender Central på Google Play och hämta och installera appen. Följ stegen för att slutföra installationen.
- **På Android** - sök Bitdefender Central på App Store och hämta och installera appen. Följ stegen för att slutföra installationen.

När du är inloggad kan du börja göra följande:

- Hämta och installera Bitdefender på Windows, macOS, iOS och Android. De produkter som är tillgängliga för hämtning är:
  - Bitdefender Mobile Security för Android
  - Bitdefender Mobile Security för iOS
  - Bitdefender Antivirus för Mac
  - Bitdefender Windows-produktlinjen
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter till nätverket och hantera dem var du än är.
- Skydda nätverksenheterna och deras data mot stöld eller förlust med Antistöld.

Öppna ditt Bitdefender-konto

Det finns två sätt att öppna Bitdefender Central

- Från din webbläsare:
  1. Öppna en webbläsare på en enhet med Internet-åtkomst.
  2. Gå till: https://central.bitdefender.com.
  3. Logga in till ditt -konto med e-postadress och lösenord.

- Från din Android- eller iOS-enhet:

  Öppna Bitdefender Central-appen som du har installerat.

> **Notera**
> I det här materialet har du alternativ och instruktioner tillgängliga på webbplattformen.

Tvåfaktorautentisering

2-faktorautentiseringsmetoden ger ett extra säkerhetslager till ditt Bitdefender-konto, genom att kräva en autentiseringskod förutom dina inloggningsuppgifter. På det här sättet förhindrar du kontokapning och håller vissa typer av cyberattacker borta, som keyloggers, råstyrke- eller ordlisteattacker.

Aktivera tvåfaktorautentisering

Genom att aktivera tvåfaktorautentisering gör du ditt Bitdefender-konto mycket säkrare. Din identitet verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera status för din prenumeration eller köra uppgifter via fjärrstyrning på dina enheter.

Aktivera tvåfaktorautentisering:

1. Öppna Bitdefender Central.
2. Tryck på ikonen uppe till höger på skärmen.
3. Tryck på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Tryck på **Tvåfaktorautentisering**.
6. Tryck på **KOM IGÅNG**.

   Välj en av följande metoder:

   - **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in till ditt Bitdefender-konto.

     Om du vill använda en autentiseringsapp, men inte är säker på vad du ska välja, finns det en lista över de autentiseringsappar vi rekommenderar.

a. Tryck på **ANVÄND AUTENTISERINGSAPP** för att börja.

b. Logga in på en Android- eller iOS-baserad enhet genom att använda enheten för att skanna QR-koden.

För att logga in på en bärbar eller stationär dator kan du manuellt lägga till den visade koden.

Tryck på **FORTSÄTT**.

c. Infoga koden som appen gav eller den som visas i föregående steg och tryck sedan på **AKTIVERA**.

- **E-post** - varje gång du loggar in på ditt Bitdefender-konto skickas en verifieringskod till din e-postinkorg. Kontrollera ditt e-postkonto och skriv sedan in den kod du har fått.

a. Tryck på **ANVÄND E-POST** för att starta.

b. Kontrollera ditt e-postkonto och skriv in den angivna koden.

Observera att du har fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.

c. Tryck på **AKTIVERA**.

d. Du får tio aktiveringskoder. Du kan antingen kopiera, ladda ned eller skriva ut listan ifall du tappar bort din e-postadress eller inte kan logga in. Varje kod kan bara användas en gång.

e. Tryck på **KLAR**.

Ifall du vill sluta använda tvåfaktorautentisering:

1. Tryck på **STÄNG AV TVÅFAKTORAUTENTISERING**.
2. Kontrollera din app eller ditt e-postkonto och skriv in koden du har fått.

   Ifall du har valt att få autentiseringskoden via e-post har du fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.
3. Bekräfta ditt val.

Lägga till betrodda enheter

För att se till att bara du kan komma åt ditt Bitdefender-konto kan vi kräva en säkerhetskod först. Om du vill hoppa över det här steget varje gång du

ansluter från samma enhet, rekommenderar vi att du utser den till en betrodd enhet.

Lägga till enheter som betrodda enheter:

1. Öppna Bitdefender Central.
2. Tryck på ikonen uppe till höger på skärmen.
3. Tryck på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Tryck på **Betrodda enheter**.
6. Listan över de enheter som Bitdefender är installerad på visas. Tryck på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och att din prenumeration är giltig.

Mina enheter

Området **Mina enheter** i ditt Bitdefender-konto ger dig möjlighet att installera, hantera och vidta fjärrstyrningsåtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till Internet. Enhetskorten visar enhetsnamn, skyddsstatus och om det finns säkerhetsrisker som påverkar enheternas skydd.

Identifiera och hantera dina enheter enkelt genom att anpassa enhetsnamn och skapa eller tilldela en ägare till var och en av dem:

1. Tryck på -ikonen i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
2. Tryck på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen. Följande alternativ är tillgängliga:
   - **Inställningar** - Härifrån kan du ändra namnet på den valda enheten.
   - **Profil** - Härifrån kan en profil tilldelas till den valda enheten. Tryck på **Lägg till ägare**, fyll sedan i motsvarande fält, ange namn, e-postadress, telefonnummer, födelsedatum och lägg till och till en profilbild.
   - **Ta bort** - Härifrån kan en profil tillsammans med den tilldelade enheten tas bort från ditt Bitdefender-konto.

Logga in med ett annat Bitdefender-konto

Så här loggar du in med ett annat Bitdefender-konto:

1. Tryck på -ikonen längst ned på skärmen.
2. Tryck på **Logga ut**.
3. Skriv e-postadress och lösenord till Bitdefender-kontot i motsvarande fält.
4. Tryck på **LOGGA IN**.

MOBILE SECURITY FOR ANDROID

21. SKYDDSFUNKTIONER

Bitdefender Mobile Security skyddar din Android-enhet med följande funktioner:

- Skanner för skadlig kod
- Webbskydd
- VPN
- Anti-Theft, inklusive:
  - Fjärrplats
  - Fjärrlåsning av enhet
  - Fjärradering av enhet
  - Fjärrenhetsvarningar
- Kontointegritet
- App Lock
- Rapporter
- WearON

Du kan använda produktfunktionerna i 14 dagar, utan kostnad. När perioden är slut måste du köpa den fullständiga versionen för att skydda din mobilenhet.

22. KOMMA IGÅNG

Enhetskrav

Bitdefender Mobile Security fungerar ¨på alla enheter som kör Android 4.1 och uppåt. En aktiv Internet-anslutning krävs för hotskanning i molnet.

Installerar Bitdefender Mobile Security

- **Från Bitdefender Central**
  - På Android
    1. Gå till: https://central.bitdefender.com.
    2. Logga in på ditt Bitdefender-konto.
    3. Tryck på ☰ i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
    4. Tryck på **INSTALLERA SKYDD** och därefter på **Skydda den här enheten**.
    5. Välj ägare av enheten. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    6. Du omdirigeras till **Google Play**-appen. På Google Play-skärmen trycker du på installationsalternativet.
  - På Windows, macOS, iOS
    1. Gå till: https://central.bitdefender.com.
    2. Logga in på ditt Bitdefender-konto.
    3. Tryck på ☰ i det övre vänstra hörnet på skärmen och sedan på **Mina enheter**.
    4. Tryck på **INSTALLERA SKYDD** och därefter på **Skydda den här övriga enheter**.
    5. Välj ägare av enheten. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    6. Tryck på **SKICKA NEDLADDNINGSLÄNK**.
    7. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i

24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

8. Kontrollera e-postkontot på den enhet du vill installera Bitdefender på och tryck på motsvarande hämtningsknapp.

- **Från Google Play**

  Sök efter Bitdefender Mobile Security för att hitta och installera appen.

  Alternativt skannar du QR-koden:

QR-kod

Innan du går igenom valideringsstegen måste du samtycka till prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Mobile Security.

Tryck på **FORTSÄTT** för att gå vidare till nästa fönster.

Logga in till ditt Bitdefender-konto

För att använda Bitdefender Mobile Security måste du koppla din enhet till ett Bitdefender-, Facebook-, Google- eller Microsoft-konto genom att logga in på kontot från appen. Första gången du öppnar appen ombes du att logga in på ett konto.

Om du har installerat Bitdefender Mobile Security från ditt Bitdefender-konto kommer appen att automatiskt försöka logga in på det kontot.

Så här kopplar du din enhet till ett Bitdefender-konto:

1. Skriv e-postadress och lösenord till Bitdefender-kontot i motsvarande fält. Om du inte har något Bitdefender-konto och vill skapa ett väljer du motsvarande länk.

2. Tryck på **LOGGA IN**.

För att logga in med ett Facebook-, Google- eller Microsoft-konto trycker du på den tjänst du vill använda från området **ELLER LOGGA IN MED**. Du omdirigeras till inloggningssidan för den valda tjänsten. Följ instruktionerna för att koppla kontot till Bitdefender Mobile Security.

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

Konfigurera skydd

När du har loggat in i appen visas fönstret **Konfigurera skydd**. För att säkra din enhet rekommenderar vi att du går igenom dessa steg:

- **Prenumerationsstatus.** För att vara skyddad av Bitdefender Mobile Security måste du aktivera din produkt med en prenumeration, som anger hur länge du kan använda produkten. Så fort den går ut slutar appen att utföra sina funktioner och skydda din enhet.

  Om du har en aktiveringskod, tryck på **JAG HAR EN KOD** och därefter 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.

- **Webbskydd.** Om din enhet kräver Tillgänglighet för att aktivera Webbskydd trycker du på **AKTIVERA**. Du omdirigeras till menyn Tillgänglighet. Du omdirigeras till menyn Tillgänglighet. Tryck på Bitdefender Mobile Security och därefter på motsvarande omkopplare.

- **Skanner för skadlig kod.** Kör en engångsskanning för att säkerställa att din enhet är fri från virus. Starta skanningsprocessen genom att trycka på **SKANNA NU**.

  Så fort skanningsprocessen startar visas kontrollpanelen. Här kan du enhetens säkerhetsstatus.

Kontrollpanel

Tryck på Bitdefender Mobile Security-ikonen i enhetens applåda för att öppna appgränssnittet.

På Kontrollpanelen finns information om säkerhetsstatus för enheten och Autopilot hjälper dig att förbättra enhetens säkerhet genom att ge dig funktionsrekommendationer.

Statuskortet längst upp i fönstret informerar om enhetens säkerhetsstatus med explicita meddelanden och olika färger. Om Bitdefender Mobile Security inte har några varningar är statuskortet grönt. När ett säkerhetsproblem har upptäckts blir statuskortet rött.

För att ge dig en effektiv drift och ökat skydd när du utför olika aktiviteter, fungerar **Bitdefender Autopilot** som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du håller på med kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på enhetens användning och behov. Det hjälper dig att upptäcka och dra nytta av de funktioner som ingår i Bitdefender Mobile Security-appen.

Varje gång en process pågår eller en funktion kräver inmatning från dig, visas ett kort med mer information och möjliga åtgärder i kontrollpanelen.

Du kan öppna Bitdefender Mobile Security-funktionerna och enkelt navigera från navigationsfältet längst ned:

Skanner för skadlig kod
Du kan starta en skanning på begäran eller aktivera skanningslagring. Mer information finns på *"Skanner för skadlig kod"* (p. 255).

Webbskydd
Säkerställer en säker surfupplevelse genom att varna dig om möjliga skadliga webbsidor. Mer information finns på *"Webbskydd"* (p. 258).

VPN
Krypterar internetkommunikation, hjälper dig att bibehålla din integritet oavsett vilket nätverk du är ansluten till. Mer information finns på *"VPN"* (p. 260).

Anti-Theft
Gör att du kan aktivera och inaktivera antistöldfunktionerna och konfigurera antistöldinställningarna. Mer information finns på *"Anti-Theft-funktioner"* (p. 263).

Kontointegritet
Kontrollerar om dataintrång har inträffat i de onlinekonton du använder. Mer information finns på *"Kontointegritet"* (p. 267).

App Lock
Gör att du kan skydda dina installerade appar genom att ange en PIN-kod för åtkomst. Mer information finns på "*App Lock*" (p. 269).

Rapporter
För en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden i samband med enhetens aktivitet. Mer information finns på "*Rapporter*" (p. 274).

WearON
Kommunicerar med din smartwatch för att hjälpa dig hitta din telefon om du tappar bort den eller glömmer var du lämnade den. Mer information finns på "*WearON*" (p. 275).

23. SKANNER FÖR SKADLIG KOD

Bitdefender skyddar din enhet och din information mot skadliga appar via skanning vid installation och skanning på begäran.

Notera
Se till att mobilenheten är ansluten till Internet. Om enheten inte är ansluten till Internet startar inte skanningsprocessen.

- **Skanning vid installation**

  Varje gång du installerar en app skannar Bitdefender Mobile Security den automatiskt med hjälp av molnteknik. Samma skanningsprocess startar automatiskt varje gång de installerade apparna uppdateras.

  Om appen befinns vara skadlig visas en varning som uppmanar dig att avinstallera den. Tryck på **Avinstallera** för att gå till appens avinstallationsskärm.

- **Skanning på begäran**

  Varje gång du vill vara säker på att de appar som är installerade på din enhet är säkra att använda kan du starta en skanning på begäran.

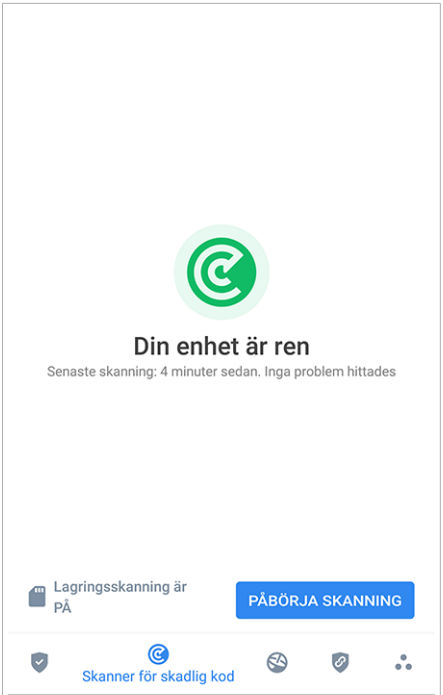
  Starta en skanning på begäran:

  1. Tryck på **Skanner för skadlig kod** på navigationsfältet längst ned.
  2. Tryck på **STARTA SKANNING**.

     Notera
     Ytterligare behörigheter krävs på Android 6 för funktionen Malware Scanner. När du har tryckt på knappen **STARTA SKANNING** väljer du **Tillåt** för följande:

     - Tillåt **Antivirus** att ringa och hantera telefonsamtal?
     - Tillåt **Antivirus** att komma åt foton, medier och filer på din enhet?

  Skanningsförloppet visas och du kan stoppa processen när som helst.



Skanning för skadlig kod

Som standard skannar Bitdefender Mobile Security enhetens interna lagring, däribland eventuella monterade SD-kort. På så sätt kan farliga appar som kan finnas på kortet upptäckas innan de kan göra någon skada.

Inaktivera inställningen för att skanna lagring:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Inaktivera **Skanna lagring** i området Virusskanner.

Om skadliga appar hittas visas information om dem och du kan ta bort dem genom att trycka på knappen **AVINSTALLERA**.

Kortet Skanner för skadlig kod visar enhetens status. När enheten är säker är kortet grönt. När enheten behöver skannas eller om någon åtgärd kräver inmatning från dig blir kortet rött.

Om din Android-version är 7.1 eller nyare har du en genväg till Malware Scanner så att du kan köra skanningar snabbare utan att öppna Bitdefender Mobile Securitys gränssnitt. För att göra det trycker du och håller ned Bitdefender-ikonen på din startskärm eller App-låda och väljer sedan ikonen  .

24. WEBBSKYDD

Webbskydd kontrollerar med Bitdefender-molntjänster de webbsidor du öppnar med Androids standardwebbläsare, Google Chrome, Firefox, Opera, Opera Mini och Dolphin. En fullständig lista med webbläsare som stöds finns i avsnittet Webbskydd.

Om en webbadress pekar på en känd nätfiske- eller falsk webbplats, eller mot skadligt innehåll som spyware eller virus, blockeras webbsidan tillfälligt och en varning visas.

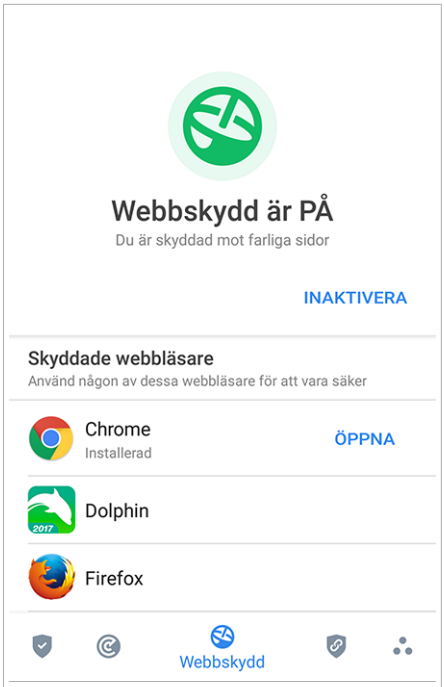
Du kan välja att ignorera varningen och fortsätta till webbsidan eller återgå till en säker sida.

Notera
Ytterligare behörigheter krävs på Android 6 för webbskyddsfunktionen. Ge behörighet att registrera som åtkomsttjänst och tryck på **SLÅ PÅ** vid förfrågan. Tryck på **Antivirus** och aktivera omkopplaren, bekräfta sedan att du godkänner åtkomsten till enhetens behörighet.

Varje gång du öppnar en bankwebbplats är Bitdefender Web Protection inställt på att meddela dig om att du ska använda Bitdefender VPN. Aviseringen visas i statusfältet. Vi rekommenderar att du använder Bitdefender VPN när du är inloggad på ditt bankkonto så att dina uppgifter är säkra från eventuella säkerhetsbrister.

Inaktivera Webbskyddsmeddelandet:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Inaktivera motsvarande reglage i området Webbskydd.


Webbskydd är PÅ
Du är skyddad mot farliga sidor
INAKTIVERA
Skyddade webbläsare
Använd någon av dessa webbläsare för att vara säker
Chrome
Installerad
ÖPPNA
Dolphin
Firefox
Webbskydd

Webbskydd

25. VPN

Med Bitdefender VPN kan du hålla dina data privata varje gång du ansluter till osäkra trådlösa nätverk på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personuppgifter eller försök att göra din enhets IP-adress åtkomlig för hackare undvikas.

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter till för att säkra din anslutning, kryptera data med kryptering i bankklass och dölja din IP-adress oavsett var du är. Din trafik omdirigeras via en separat server och gör det därmed näst intill omöjligt att identifiera din enhet bland de myriader av andra enheter som använder våra tjänster. När du är ansluten till Internet via Bitdefender VPN, kan du dessutom ha åtkomst till innehåll som i normala fall är begränsat i vissa områden.

Notera
Vissa länder censurerar Internet och därför kan användning av VPN på deras territorier vara förbjudet enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-funktionen första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om regelverken i det land du befinner dig i och de risker du kan utsättas för.

Det finns två sätt att slå på eller slå av Bitdefender VPN:

- Tryck **ANSLUT** i VPN-kortet från instrumentpanelen.

  Status för Bitdefender VPN visas.

- Tryck på **VPN** i navigeringsfältet längst ned och sedan på **ANSLUT**.

  Tryck på **ANSLUT** varje gång du vill fortsätta vara skyddad när du ansluter till osäkra trådlösa nätverk.

  Tryck på **KOPPLA IFRÅN** när du vill inaktivera anslutningen.

Notera
Första gången du slår på VPN ombes du att tillåta Bitdefender att konfigurera en VPN-anslutning som övervakar nätverkstrafiken. Tryck på **OK** för att fortsätta.

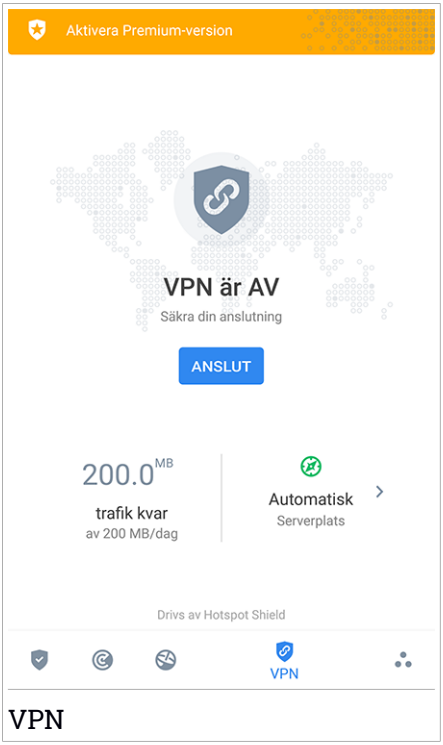
Om din Android-version är 7.1 eller nyare har du en genväg till Bitdefender VPN utan att öppna Bitdefender Mobile Securitys gränssnitt. För att göra

det trycker du och håller ned Bitdefender-ikonen på din startskärm eller App-låda och väljer sedan ikonen .

Ikonen visas i statusfältet när Bitdefender VPN är aktivt.

För att spara batteri rekommenderar vi att du stänger av VPN-funktionen när du inte behöver det.

Om du har en premiumprenumeration och vill välja vilken server du ansluter till trycker du på **Serverplats** i VPN-funktionen och väljer sedan den plats du valt. Mer information om VPN-prenumerationer finns på "Prenumerationer" (p. 262).



VPN

VPN-inställningar

För en avancerad konfiguration av ditt VPN:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.

I VPN-området kan du konfigurera följande alternativ:

- Snabb VPN-åtkomst - en avisering visas i statusfältet på din enhet så att du snabbt kan slå på VPN.
- Öppet Wi-Fi-nätverk - varje gång du ansluter till ett öppet Wi-Fi-nätverk meddelas du i enhetens statusfält om att använda VPN.

Prenumerationer

Bitdefender VPN erbjuder utan kostnad en daglig trafikkovot på 200 MB per enhet för att säkra anslutningen varje gång ditt team behöver det.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en serverplats enligt ditt teams önskemål, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst från panelen **Mina prenumerationer** som finns på ditt Bitdefender-konto.

Bitdefender Premium VPN-prenumerationen är oberoende av den prenumerationen på Bitdefender Small Office Security, vilket innebär att du kan använda den under hela dess tillgänglighet. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Small Office Security fortfarande är aktiv återgår du till gratisversionen.

Bitdefender VPN är en produkt över flera plattformar, tillgänglig i Bitdefender-produkter kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kan du använda din prenumeration på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

26. ANTI-THEFT-FUNKTIONER

Bitdefender kan hjälpa dig att lokalisera enheten och förhindra att personlig information hamnar i fel händer.

Allt du behöver göra är att aktivera Anti-Theft från enheten och vid behov, gå till **Bitdefender Central** från en webbläsare, var som helst.

Bitdefender Mobile Security har följande Anti-Theft-funktioner:

Hitta via fjärrstyrning

Visa enhetens aktuella plats på Google Maps. Platsen uppdateras var 5:e sekund, så du kan spåra den om den rör på sig.

Riktigheten för platsen beror på hur Bitdefender kan fastställa den:

- Om GPS:en är aktiverad på enheten kan dess plats preciseras inom några meter så länge som den är inom räckhåll för GPS-satelliter (dvs. inte inuti en byggnad).
- Om enheten är inomhus kan dess plats fastställas till inom ett tiotal meter om Wi-Fi är aktiverat och det finns trådlösa nätverk tillgängliga inom dess räckhåll.
- Annars fastställs platsen med bara informationen från mobilnätverket, som inte kan erbjuda mer noggrannhet än flera hundra meter.

Lås via fjärrstyrning

Lås enhetens skärm och ange en numerisk PIN-kod för att låsa upp den.

Fjärradera

Ta bort all personlig information från din förlupna enhet.

Skicka varning till enhet (skrik)

Skicka ett fjärrmeddelande som ska visas på enhetens skärm eller lös ut ett högt ljud som ska spelas upp på enhetens högtalare.

Om du förlorar enheten kan du låta den som hittar den returnera den till dig genom att visa ett meddelande på enhetens skärm.

Om du har förlagt din enhet och det finns en chans att den inte är så långt ifrån dig (till exempel någonstans i huset eller på kontoret), finns det då något bättre sätt att hitta den än att spela upp ett högt ljud? Ljudet spelas även om enheten är i tyst läge.

Aktivera Anti-Theft

För att aktivera antistöldfunktioner slutför du konfigurationsprocessen från antistöldkortet som finns i kontrollpanelen.

Alternativt kan du aktivera Anti-Theft genom att följa dessa steg:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Anti-Theft**.
3. Tryck på **SLÅ PÅ**.
4. Följande procedur startar för att hjälpa dig aktivera funktionen:

   Notera
   Ytterligare behörigheter krävs på Android 6 för funktionen Anti-Theft. Aktivera den genom att följa stegen nedan:

   a. Tryck på **Aktivera Anti-Theft**, tryck därefter på **SLÅ PÅ**.

   b. Tillåt behörigheter för **Antivirus** att komma åt den här enhetens plats.

   a. **Tilldela adminbehörigheter**

   Dessa behörigheter är nödvändiga för att antistöldmodulen ska fungera och måste därför tillåtas för att fortsätta.

   b. **Ställ in applikations-PIN**

   För att förhindra obehörig åtkomst till din enhet måste en PIN-kod anges. Varje gång ett försök att öppna din enhet görs måste en PIN-kod anges först. Alternativt, på enheter med stöd för 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 tar Bitdefender ett foto av personen när Snap Photo är aktiverat.

   Mer exakt: varje gång PIN-koden, lösenordet eller det fingeravtryck du angav för att skydda din enhet anges fel tre gånger i rad tas ett foto med frontkameran. Fotot sparas tillsammans med tidsstämpel och orsak och kan användas när du öppnar Bitdefender Mobile Security

och går till Antistöld-fönstret. Alternativt kan du visa det tagna foto i ditt Bitdefender-konto.

i. Gå till: https://central.bitdefender.com.

ii. Logga in på ditt konto.

iii. Tryck på ☰ i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.

iv. Välj din Android-enhet och sedan fliken **Antistöld**.

v. Tryck på ⋮ bredvid **Kontrollera dina bilder** för att visa de senaste fotona som togs.

Endast de två senaste fotona sparas.

När Antistöld-funktionen är aktiverad kan du aktivera eller inaktivera webbstyrningskommandon individuellt från Antistöld-funktionen genom att trycka på motsvarande alternativ.

Använda Anti-Theft-funktioner från Bitdefender Central

Notera
Alla Antistöld-funktioner kräver att alternativet **Bakgrundsdata** är aktiverat i enhetens inställningar för dataanvändning.

Så här kommer du åt Anti-Theft-funktionerna från ditt Bitdefender-konto:

1. Öppna Bitdefender Central.
2. Tryck på ☰ i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
3. I fönstret **MINA ENHETER** väljer du önskat enhetskort.
4. Välj fliken **Antistöld**.
5. I det nedersta fältet i fönstret trycker du på ikonen ··· icon och därefter på knappen för den funktion du vill använda:

   Hitta - visa enhetens plats på Google Maps.

   Varning - skriv ett meddelande för att visa enhetens skärm och/eller få din enhet att spela upp ett larm.

Lås - Lås enheten och ställ in en PIN-kod för att låsa upp den.

Radera - Ta bort alla data från enheten.

Viktigt
När du har raderat en enhet slutar alla Anti-Theft-funktionerna att fungera.

VISA IP - visar den senaste IP-adressen för den valda enheten.

Anti-Theft-inställningar

Om du vill aktivera eller inaktivera fjärrkommandon:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Anti-Theft**.
3. Aktivera eller inaktivera önskade alternativ.

27. KONTOINTEGRITET

Bitdefender Account Privacy upptäcker om något dataintrång har inträffat på de konton du använder för att betala online, handla eller logga in på olika appar eller webbplatser. Data som kan lagras på ett konto kan vara lösenord, kreditkortsinformation eller bankkontoinformation och om det inte är tillräckligt säkert, kan identitetsstöld eller integritetsöverträdelse inträffa.

Det här kontots sekretesstatus visas direkt efter validering.

Automatiska omkontroller är inställda på att köras i bakgrunden, men manuella skanningar kan också köras varje dag.

Meddelanden visas varje gång nya intrång som innehåller något av de validerade e-postkontona upptäcks.

För att börja hålla personlig information säker:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Kontosekretess**.
3. Tryck på **KOM IGÅNG**.
4. Det e-postkonto du använde för att skapa ditt Bitdefender-konto visas.

   Tryck på **LÄGG TILL** för att fortsätta.

   Bitdefender måste valideras det här kontot innan personlig information visas. Därför skickas ett e-postmeddelande med en valideringskod till den angivna e-postadressen.
5. Kontrollera din inkorg och skriv sedan den kod du fått i området **Kontointegritet** i din app. Om du inte hittar valideringsmeddelandet i inkorgen kan du titta i skräppostmappen också.

   Sekretesstatus på det validerade kontot visas.

   Lägg till andra konton genom att trycka på **LÄGG TILL KONTO** i fönstret Kontosekretess och följ sedan nödvändiga steg.

Om intrång hittas på något av dina konton rekommenderar vi att du byter lösenord till dem så fort som möjligt. För att skapa ett starkt och säkert lösenord bör du beakta följande tips:

- Gör det minst åtta tecken långt.
- Inkludera gemener och versaler.

- Lägg till minst en siffra eller symbol, som #, @, % eller !.

När du har säkrat ett konto som ingått i ett integritetsintrång kan du bekräfta ändringarna genom att markera identifierade intrång som **Lösta**. Så här gör du:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Kontosekretess**.
3. Tryck på det konto du precis säkrade.
4. Tryck på det intrång du säkrade kontot mot.
5. Tryck på **LÖST** för att verifiera att kontot är säkrat.

När alla upptäckta intrång är markerade som **Lösta** visas inte kontot längre som överträtt, inte förrän ett nytt intrång upptäcks.

Om du inte vill meddelas varje gång automatiska skanningar genomförs:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Inaktivera motsvarande reglage i området Kontosekretess.

28. APP LOCK

Installerade appar som e-post, foton eller meddelanden kan innehålla personliga data som du vill ska fortsätta vara privata genom att selektivt begränsa åtkomst till dem.

Med App Lock kan du blockera oönskad åtkomst till appar genom att ange en säkerhets-PIN-kod för åtkomst. PIN-koden måste vara minst 4 siffror, men inte mer än 8, och den måste anges varje gång du vill ha åtkomst till de valda begränsade apparna.

Alternativt, på enheter med stöd för fingeravtrycksautentisering, kan en fingeravtrycksbekräftelse användas istället för den konfigurerade PIN-koden.

Aktivera App Lock

Konfigurera App Lock från kortet som visas i kontrollpanelen när du har aktiverat Antistöld för att begränsa åtkomst till valda appar.

Alternativt kan du aktivera App Lock genom att följa dessa steg:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **App Lock**.
3. Tryck på **SLÅ PÅ**.
4. Tillåt åtkomst till användningsdata för Bitdefender.

   Notera
   Ytterligare behörigheter krävs på Android 6 för funktionen Snap Photo. Aktivera det genom att tillåta att **Antivirus** tar bilder och spelar in video.

5. Gå tillbaka till appen, konfigurera åtkomstkoden och tryck därefter på **ANGE PIN**.

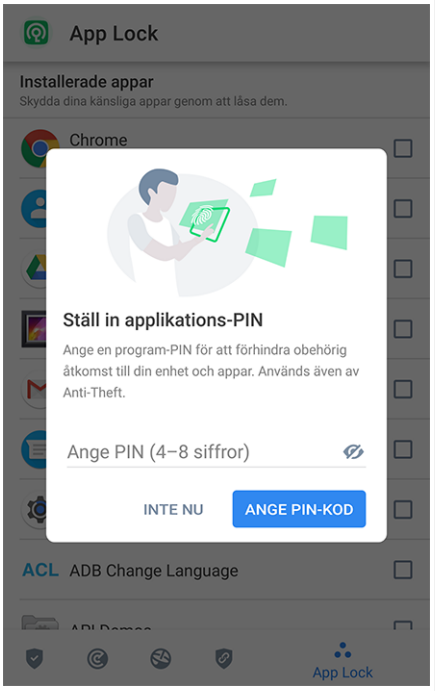
   Notera
   Det här steget är endast tillgängligt om du inte tidigare konfigurerade PIN-koden i Antistöld.

6. Gör det möjligt för alternativet Snap Photo att fånga en inkräktare som försöker komma åt dina privata data.

7. Välj de appar du vill skydda.

Om du använder fel PIN eller fingeravtryck fem gånger i rad aktiveras en 30 sekunders timeout. På så sätt blockeras alla försök att bryta sig in i de skyddade apparna.

Notera
Samma PIN-kod används av Antistöld för att hjälpa dig hitta din enhet.



App Lock

Låsläge

Första gången du lägger til en app till App Lock visas skärmen App Lock-läge. Härifrån kan du välja när app Lock-funktionen ska skydda apparna som är installerade på din enhet.

Du kan välja ett av följande alternativ:

- **Kräv upplåsning varje gång** - varje gång de låsta apparna öppnas måste den PIN-kod eller det fingeravtryck du ställt in användas.
- **Håll upplåst tills skärmen stängs av** - åtkomst till dina appar är giltig tills skärmen stängs av.
- **Lås efter 30 sekunder** - du kan avsluta och öppna dina olåsta appar igen inom 30 sekunder.

Om du vill ändra den valda inställningen:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Tryck på **Kräv upplåsning varje gång** i området App Lock.
4. Välj önskat alternativ.

App Lock-inställningar

För en avancerad konfiguration av App Lock:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.

I App Lock-området kan du konfigurera följande alternativ:

- **Känslig app-förslag** - ta emot en låsavisering varje gång du installerar en känslig app.
- **Kräv upplåsning varje gång** - välj ett ab de tillgängliga lås- och lås upp-alternativen.
- **Smart upplåsning** - håll appar olåsta medan du ansluter till betrodda Wi-Fi-nätverk.
- **Slumpmässig knappsats** - förhindra PIN-avläsning genom slumpvisa nummerpositioner.

Snap Photo

Med Bitdefender Snap Photo kan du fånga dina vänner och släktingar på bild. På så sätt kan du lära dem att inte titta igenom dina personliga filer eller appar du använder.

Funktionen är enkel: varje gång den PIN-kod eller det fingeravtryck du angav för att skydda dina appar anges fel tre gånger i rad tas ett foto med frontkameran. Fotot sparas tillsammans med tidsstämpel och orsak och kan ses när du öppnar Bitdefender Mobile Security och går till App Lock-funktionen.

Notera
Den här funktionen är endast tillgänglig för telefoner som har en frontkamera.

Konfigurera funktionen Ta foto för App Lock:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Aktivera motsvarande reglage i området Ta foto.

Foton som tas när felaktig PIN-kod anges visas i App Lock-fönstret och kan visas i helskärm.

Alternativt kan de visas i ditt Bitdefender-konto:

1. Gå till: https://central.bitdefender.com.
2. Logga in på ditt konto.
3. Tryck på i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
4. Välj din Android-enhet och sedan fliken **Antistöld**.
5. Tryck på bredvid **Kontrollera dina bilder** för att visa de senaste fotona som togs.

Endast de två senaste fotona sparas.

Sluta ladda upp tagna foton till ditt Bitdefender-konto:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Inaktivera **Ladda upp foton** i området Ta foto.

Smart upplåsning

En enkel metod för att inte bli tillfrågad av App Lock att ange PIN-kod eller fingeravtrycksbekräftelse för de oskyddade apparna är att aktivera Smart Unlock.

Med Smart Unlock kan du ange de Wi-Fi-nätverk du oftast ansluter till som betrodda och när du är ansluten till dem inaktiveras App Locks blockeringsinställningar för de skyddade apparna.

Konfigurera funktionen Smart Unlock:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **App Lock**.
3. Tryck **LÄGG TILL** för att ange den Wi-Fi-anslutning du för närvarande använder som betrodd.

Notera
Den här inställningen är endast tillgänglig om funktionen Smart Unlock är aktiverad.

När du ändrar dig kan du inaktivera funktionen och de Wi-Fi-nätverk du har angett som betrodda behandlas som ej betrodda.

29. RAPPORTER

Rapportfunktionen för en detaljerad logg över händelser som rör skanningsaktiviteten på din enhet.

Varje gång något som är relevant för enhetens säkerhet inträffar läggs ett nytt meddelande till i rapporterna.

Så här kommer du till rapportavsnittet:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Rapporter**.

Följande flikar är tillgängliga i fönstret Rapporter:

- **VECKORAPPORTER** - här har du tillgång till säkerhetsstatus och de uppgifter som utförts aktuell och föregående vecka. Aktuell veckas rapport genereras varje söndag och du får ett meddelande som informerar dig när det blir tillgängligt.

  Varje vecka visas ett nytt tips i det här avsnittet, så se till att du kommer tillbaka regelbundet för att få ut det bästa av appen.

  För att sluta få aviseringar varje gång en rapport genereras:

  1. Tryck på **Mer** längst ned i navigationsfältet.
  2. Tryck på **Inställningar**.
  3. Inaktivera reglaget **Ny rapportavisering** i området Rapporter.

- **AKTIVITETSLOGG** - här kan du kontrollera detaljerad information om aktiviteten i din Bitdefender Mobile Security-app sedan den installerade på din Android-enhet.

  Ta bort tillgänglig aktivitetslogg:

  1. Tryck på **Mer** längst ned i navigationsfältet.
  2. Tryck på **Inställningar**.
  3. Tryck på **Rensa aktivitetslogg** och därefter på **RENSA**.

30. WEARON

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 tyst läge är aktiverat.

Ha den här funktionen aktiverad för att vara säker på att du alltid har din smartphone till hands.

Notera
Funktionen fungerar med Android 4.3 och Android Wear.

Aktivera WearON

För att använda WearON behöver du bara ansluta din smartwatch till Bitdefender Mobile Security-appen och aktivera funktionen med följande röstkommando:

Start:<Where is my phone>

Bitdefender WearON har två kommandon:

1. **Phone Alert**

   Med funktionen Phone Alert kan du snabbt hitta din smartphone när du kommer för långt bort ifrån den.

   Om du har din smartwatch med dig upptäcker den automatiskt appen på din telefon och vibrerar nä du kommer för långt bort från telefonen, mer exakt när Bluetooth-anslutningen förloras.

   Aktivera den här funktionen genom att öppna Bitdefender Mobile Security, tryck på **Globala inställningar** i menyn och välj motsvarande reglage under WearON-avsnittet.

2. **Skrik**

   Det har aldrig varit enklare att hitta in telefon. När du glömmer var du har lagt telefonen trycker du på Scream-kommandot på klockan för att få din telefon att skrika.

31. OM

För att hitta information om den Bitdefender Mobile Security-version du har installerat, för att öppna och läsa prenumerationsavtalet och sekretesspolicyn och visa öppen källkodslicenser:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Tryck på önskat alternativ i området Om.

32. BITDEFENDER CENTRAL

Bitdefender Central är webbplattformen där du öppnar produktens onlinefunktioner och tjänster och kan fjärrstyra viktiga åtgärder på de enheter där Bitdefender är installerad. Du kan logga in på ditt Bitdefender-konto från vilken dator eller mobil enhet som helst som är ansluten till Internet genom att gå till https://central.bitdefender.com, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

Så här installerar du Bitdefender Central-appen på dina enheter:

- **På Android** - sök Bitdefender Central på Google Play och hämta och installera appen. Följ stegen för att slutföra installationen.
- **På Android** - sök Bitdefender Central på App Store och hämta och installera appen. Följ stegen för att slutföra installationen.

När du är inloggad kan du börja göra följande:

- Hämta och installera Bitdefender på Windows, macOS, iOS och Android. De produkter som är tillgängliga för hämtning är:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security för iOS
  - Bitdefender Antivirus för Mac
  - Bitdefender Windows-produktlinjen
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter till nätverket och hantera dem var du än är.
- Skydda nätverksenheterna och deras data mot stöld eller förlust med Antistöld.

Öppna ditt Bitdefender-konto

Det finns två sätt att öppna Bitdefender Central

- Från din webbläsare:
  1. Öppna en webbläsare på en enhet med Internet-åtkomst.
  2. Gå till: https://central.bitdefender.com.
  3. Logga in till ditt -konto med e-postadress och lösenord.

- Från din Android- eller iOS-enhet:

  Öppna Bitdefender Central-appen som du har installerat.

Notera
I det här materialet har du alternativ och instruktioner tillgängliga på webbplattformen.

Tvåfaktorautentisering

2-faktorautentiseringsmetoden ger ett extra säkerhetslager till ditt Bitdefender-konto, genom att kräva en autentiseringskod förutom dina inloggningsuppgifter. På det här sättet förhindrar du kontokapning och håller vissa typer av cyberattacker borta, som keyloggers, råstyrke- eller ordlisteattacker.

Aktivera tvåfaktorautentisering

Genom att aktivera tvåfaktorautentisering gör du ditt Bitdefender-konto mycket säkrare. Din identitet verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera status för din prenumeration eller köra uppgifter via fjärrstyrning på dina enheter.

Aktivera tvåfaktorautentisering:

1. Öppna Bitdefender Central.
2. Tryck på ikonen uppe till höger på skärmen.
3. Tryck på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Tryck på **Tvåfaktorautentisering**.
6. Tryck på **KOM IGÅNG**.

   Välj en av följande metoder:

   - **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in till ditt Bitdefender-konto.

     Om du vill använda en autentiseringsapp, men inte är säker på vad du ska välja, finns det en lista över de autentiseringsappar vi rekommenderar.

a. Tryck på **ANVÄND AUTENTISERINGSAPP** för att börja.

b. Logga in på en Android- eller iOS-baserad enhet genom att använda enheten för att skanna QR-koden.

För att logga in på en bärbar eller stationär dator kan du manuellt lägga till den visade koden.

Tryck på **FORTSÄTT**.

c. Infoga koden som appen gav eller den som visas i föregående steg och tryck sedan på **AKTIVERA**.

- **E-post** - varje gång du loggar in på ditt Bitdefender-konto skickas en verifieringskod till din e-postinkorg. Kontrollera ditt e-postkonto och skriv sedan in den kod du har fått.

a. Tryck på **ANVÄND E-POST** för att starta.

b. Kontrollera ditt e-postkonto och skriv in den angivna koden.

Observera att du har fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.

c. Tryck på **AKTIVERA**.

d. Du får tio aktiveringskoder. Du kan antingen kopiera, ladda ned eller skriva ut listan ifall du tappar bort din e-postadress eller inte kan logga in. Varje kod kan bara användas en gång.

e. Tryck på **KLAR**.

Ifall du vill sluta använda tvåfaktorautentisering:

1. Tryck på **STÄNG AV TVÅFAKTORAUTENTISERING**.
2. Kontrollera din app eller ditt e-postkonto och skriv in koden du har fått.

   Ifall du har valt att få autentiseringskoden via e-post har du fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.
3. Bekräfta ditt val.

Lägga till betrodda enheter

För att se till att bara du kan komma åt ditt Bitdefender-konto kan vi kräva en säkerhetskod först. Om du vill hoppa över det här steget varje gång du

ansluter från samma enhet, rekommenderar vi att du utser den till en betrodd enhet.

Lägga till enheter som betrodda enheter:

1. Öppna Bitdefender Central.
2. Tryck på ikonen uppe till höger på skärmen.
3. Tryck på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Tryck på **Betrodda enheter**.
6. Listan över de enheter som Bitdefender är installerad på visas. Tryck på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och att din prenumeration är giltig.

Mina enheter

Området **Mina enheter** i ditt Bitdefender-konto ger dig möjlighet att installera, hantera och vidta fjärrstyrningsåtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till Internet. Enhetskorten visar enhetsnamn, skyddsstatus och om det finns säkerhetsrisker som påverkar enheternas skydd.

För att enkelt identifiera dina enheter kan du anpassa enhetsnamnet:

1. Öppna Bitdefender Central.
2. Tryck på i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
3. Tryck på önskat enhetskort och sedan på i det övre högra hörnet på skärmen.
4. Välj **Inställningar**.
5. Skriv in ett nytt namn i fältet **Enhetsnamn** och välj därefter **SPARA**.

Du kan skapa och tilldela en ägare för varje enhet för bättre hantering:

1. Öppna Bitdefender Central.
2. Tryck på i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.

3. Tryck på önskat enhetskort och sedan på ⋮ i det övre högra hörnet på skärmen.
4. Välj **Profil**.
5. Tryck på **Lägg till ägare** oh fyll i motsvarande fält. Anpassa profilen genom att lägga till ett foto och välj ett födelsedatum.
6. Tryck på **LÄGG TILL** för att spara profilen.
7. Välj önskad ägare från listan **Enhetsägare** och tryck på **TILLDELA**.

Välj önskat enhetskort för fler fjärråtgärder och information angående din Bitdefender-produkt på en specifik enhet.

När du har valt ett enhetskort är följande flikar tillgängliga:

- **Kontrollpanel**. I det här fönstret kan du visa information om den valda enheten, kontrollera dess skyddsstatus, status för Bitdefender VPN och hur många hot som har blockerats de senaste sju dagarna. Skyddsstatus kan vara grönt när det inte finns några problem som påverkar enheten, gult när enheten behöver åtgärdas från din sida eller rött när enheten är utsatt för risk. När det finns problem som påverkar enheten trycker du på rullgardinsmenyn i det övre statusområdet för att se mer information. Härifrån kan du manuellt åtgärda problem som påverkar dina enheters säkerhet.
- **Skydd**. Från det här fönstret kan fjärrstyra en skanning på din enhet. Tryck på knappen **SKANNA** för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och det finns en rapport från den senaste skanningen med den viktigaste informationen.
- **Anti-Theft**. Ifall du förlägger din enhet kan du hitta den och utföra fjärrstyrda åtgärder med Antistöld-funktionen. Tryck på **HITTA** för att få reda var enheten är. Senaste kända position visas, tillsammans med datum och tid. Mer information om den här funktionen finns i *"Anti-Theft-funktioner"* (p. 263).

Mina prenumerationer

Bitdefender Central-plattformen ger dig möjlighet att enkelt hantera de prenumerationer du har för alla dina enheter.

Kontrollera tillgängliga prenumerationer

Kontrollera dina tillgängliga prenumerationer:

1. Öppna Bitdefender Central.
2. Tryck på ☰ i det övre vänstra hörnet på skärmen och välj sedan **Mina prenumerationer**.

Här har du information om de prenumerationer du äger och antal enheter som använder var och en av dem.

Du kan lägga till en ny enhet till en prenumeration eller förnya den genom att välja ett prenumerationskort.

Lägg till ny enhet

Om din prenumeration omfattar mer än en enhet kan du lägga till en ny enhet och installera din Bitdefender Mobile Security på den, såsom beskrivs i ”Installerar Bitdefender Mobile Security” (p. 250).

Förnya prenumeration

Om det har gått mindre än 30 dagar sedan din prenumeration och du valde bort att förnya automatiskt, kan du manuellt förnya genom att följa de här stegen:

1. Öppna Bitdefender Central.
2. Tryck på ☰ i det övre vänstra hörnet på skärmen och välj sedan **Mina prenumerationer**.
3. Välj önskat prenumerationskort.
4. Tryck **FÖRNYA** för att fortsätta.

En webbsida öppnas i din webbläsare där du kan förnya din Bitdefender-prenumeration.

33. VANLIGA FRÅGOR

Varför kräver Bitdefender Mobile Security en Internet-anslutning?

Appen måste kommunicera med Bitdefender-servrar för att fastställa säkerhetsstatus för apparna den skannar och för de webbplatser du besöker och även för att få kommandon från ditt Bitdefender-konto, nä du använder Antistöld-funktionerna.

Vad behöver Bitdefender Mobile Security varje behörighet för?

- Internet-åtkomst -> används för molnkommunikation.
- Läs telefonstatus och identitet -> används för att upptäcka om enheten är ansluten till Internet och för att hämta viss enhetsinformation som behövs för att skapa ett unikt ID vid kommunikation med Bitdefender-molnet.
- Webbläsarbokmärken, läs och skriv -> Webbskyddsmodulen tar bort skadliga webbplatser från din surfhistorik.
- Läs loggdata -> Bitdefender Mobile Security upptäcker spår av hotaktiviteter från Android-loggarna.
- Plats -> krävs för fjärrplats.
- Kamera -> krävs för Snap photo.
- Lagring -> används för att tillåta skannern för skadlig kod att kontrollera SD-kortet.

Hur kan jag sluta skicka information om misstänkta appar till Bitdefender?

Som standard skickar Bitdefender Mobile Security rapporter till Bitdefender-servrar om de misstänkta appar du installerar. Den här informationen är viktig för att förbättra hotupptäckt och kan hjälpa oss att erbjuda dig en bättre upplevelse i framtiden. Ifall du vill sluta skicka oss information om misstänkta appar:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Stäng av **Upptäckt i molnet** i området Skanner för skadlig kod.

Var hittar jag information om appens aktivitet?

Bitdefender Mobile Security för en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden i samband med dess aktivitet. För att öppna information om appens aktivitet:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Rapporter**.

   I fönstret VECKORAPPORT kan du öppna de rapporter som genereras varje vecka och i fönstret AKTIVITETSLOGG kan du visa information om aktiviteten för din Bitdefender-app.

Jag har glömt PIN-koden jag angav för att skydda min app. Vad gör jag?

1. Öppna Bitdefender Central.
2. Tryck på i det övre vänstra hörnet på skärmen och välj sedan **Mina enheter**.
3. Tryck på önskat enhetskort och sedan på i det övre högra hörnet på skärmen.
4. Välj **Inställningar**.
5. Hämta PIN-koden från fältet **Program-PIN**.

Hur kan jag ändra den PIN-kod jag ställer in för App Lock och Anti-Theft?

Om du vill ändra den PIN-kod du ställt in för App Lock och Anti-Theft?

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **Inställningar**.
3. Tryck på Säkerhet **PIN-KOD** i området Anti-Theft.
4. Skriv in aktuell PIN-kod.
5. Skriv in den nya PIN-kod du vill ställa in.

Hur stänger jag av funktionen App Lock?

Det går inte att stänga av App Lock-funktionen, men du kan enkelt inaktivera den genom att avmarkera kryssrutorna bredvid de valda apparna när du har validerat PIN-koden eller det fingeravtryck du ställt in.

Hur kan jag ange ett annat trådlöst nätverk som betrott?

Först måste du ansluta enheten till det trådlösa nätverk du vill ange som betrott. Följ sedan dessa steg:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Tryck på **App Lock**.
3. Tryck på i det övre högra hörnet.
4. Tryck på **LÄGG TILL** bredvid det nätverk du vill ange som betrott.

Hur kan jag slippa se foton som är tagna på mina enheter?

Slippa se de foton som är tagna på dina enheter:

1. Öppna Bitdefender Central.
2. Tryck på i det övre högra hörnet på skärmen.
3. Tryck på **Mitt konto** i reglagemenyn.
4. Välj fliken **Inställningar**.
5. Inaktivera **Visa/visa inte foton som tas på dina enheter**.

Hur kan jag se till att min onlineshopping säker?

Onlineshopping kan medföra stora risker om viss information ignoreras. Vi rekommenderar att du gör följande för att inte utsättas för bedrägeri:

- Ha din säkerhetsapp uppdaterad.
- Skicka endast onlinebetalningar med köparskydd.
- Använd en VPN när du ansluter till Internet från publika och osäkra trådlösa nätverk.
- Var uppmärksam på de lösenord du använder för dina onlinekonton. De måste vara starka och innehålla både gemener och versaler, siffor och symboler (@, !, %, #, mm.).
- Se till att den information du skickar går över säkra anslutningar. Webbplats tillägget online måste vara HTTPS:// och inte HTTP://.

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du öppnar, laddar ner eller laddar upp innehåll på Internet. För att du ska vara säker när du surfar på webben rekommenderar vi att du använder Bitdefender VPN när du:

- vill ansluta till publika trådlösa nätverk

- vill öppna innehåll som i normala fall är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, kreditkortsinformation, mm.)
- vill dölja din IP-adress

Kommer Bitdefender VPN att ha en negativ inverkan på min enhets batteritid?

Bitdefender VPN är utformat för att skydda dina personuppgifter, dölja din IP-adress när du är ansluten till oskyddade trådlösa nätverk och få tillgång till begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort det när du är offline.

Varför upplever jag att Internet blir långsammare när jag är ansluten till Bitdefender VPN?

Bitdefender VPN är utformad för att ge dig en lätt upplevelse när du surfar på webben. Men din internetanslutning eller avståndet av server du ansluter till kan orsaka avmattningen. Om det inte är ett måste att ansluta från din plats till en fjärrserverad 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 till dig.

Kan jag ändra det Bitdefender-konto som är kopplat till min enhet?

Ja, du byter enkelt det Bitdefender-konto som är kopplat till din enhet genom att göra följande:

1. Tryck på **Mer** längst ned i navigationsfältet.
2. Ange din e-postadress.
3. Tryck på **Logga ut från ditt konto**. Om en PIN-kod har angetts uppmanas du att skriva in den.
4. Bekräfta ditt val.
5. Skriv in e-postadressen och lösenord till ditt konto i motsvarande fält och tryck sedan på **LOGGA IN**.

Hur påverkar Bitdefender Mobile Security min enhets prestanda och batteri?

Vi håller påverkan mycket lågt. Appen körs bara när det behövs - när du har installerat en app, när du använder 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 fjärrstyrda uppgifter. Utan dessa behörigheter fungerar inte fjärrlåsning och enhetsradering skulle inte kunna ta bort dna data helt. Om du vill ta bort appen återkallar du dessa behörigheter innan du försöker avinstallera från **Inställningar > Säkerhet > Välj enhetsadministratörer**.

Så här löser du felet "Ingen Google Token" som visas när du loggar in i Bitdefender Mobile Security.

Det här felet inträffar när enheten inte är associerad med ett Google-konto eller om enheten är associerad med ett konto, men ett tillfälligt problem förhindrar att den ansluts till Google. Prova med en av följande lösningar:

- Gå till Android-inställningar > Appar > Hantera appar > Bitdefender Mobile Security och tryck på **Rensa data**. Försök sedan logga in igen.
- Se till att enheten är associerad med ett Google-konto.

  Kontrollera detta genom att gå till Inställningar > Konton & synkronisera och se om ett Google-konto är listat under **Hantera konton**. Lägg till ditt konto om inget är listat, starta om enheten och försök sedan logga in i Bitdefender Mobile Security.
- Starta om enheten och försök logga in igen.

På vilka språk är Bitdefender Mobile Security tillgängligt?

Bitdefender Mobile Security är för närvarande tillgängligt på följande språk:

- Brasilianska
- Tjeckiska
- Holländska
- Engelska
- Franska
- Tyska
- Grekiska
- Ungerska
- Italienska
- Japanska
- Koreanska

- Polska
- Portugisiska
- Rumänska
- Ryska
- Spanska
- Svenska
- Thai
- Turkiska
- Vietnamesiska

Andra språk läggs till i kommande versioner. För att byta språk i gränssnittet för Bitdefender Mobile Security går du till enhetens inställningar för **Språk & tangentbord** och anger enheten till det språk du vill använda.

KONTAKTA OSS

34. BE OM HJÄLP

Bitdefender erbjuder sina kunder en oöverträffad nivå av snabb och korrekt support. Om du upplever några problem med, eller om du har några frågor om din Bitdefender-produkt kan du använda flera resurser på nätet för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefenders kundtjänst. Våra supportmedarbetare besvarar dina frågor snabbt och ger dig den hjälp du behöver.

Avsnitt *"Lösa vanliga problem"* (p. 154) innehåller den nödvändiga informationen avseende de vanligaste problemen du kan stöta på när du använder den här produkten.

Om du inte hittar något svar på din fråga i medföljande resurser kan du ringa oss på **(+1)800 839 6823** eller skicka e-post till soho@bitdefender.com. Alternativt kan du kontakta oss direkt:

- "Kontakta oss direkt från Bitdefender Total Security" (p. 290)
- "Kontakta oss via vårt onlinesupportcenter" (p. 291)

Kontakta oss direkt från Bitdefender Total Security

Om du har en fungerande Internet-anslutning kan du kontakta Bitdefender för hjälp direkt från produktgränssnittet.

Följ dessa steg:

1. Klicka på **Support** på navigeringsmenyn i Bitdefender-gränssnittet.
2. Du har följande alternativ:
   - **ANVÄNDARGUIDE**

     Gå till vår databas och sök efter nödvändig information.
   - **SUPPORTCENTER**

     Gå till våra onlineartiklar och videohandledningar.
   - **KONTAKTA SUPPORT**

     Klicka på **KONTAKTA SUPPORT** för att starta Bitdefender-supportverktyget och kontakta kundtjänsten.

     a. Fyll i formuläret med nödvändig information:

        i. Välj vilken typ av problem du upplever.

ii. Skriv en beskrivning av det problem du stötte på.

iii. Klicka på **FÖRSÖK ATT ÅTERSKAPA DET HÄR PROBLEMET** ifall du stöter på ett produktproblem. Återskapa problemet och klicka därefter på **SLUTFÖR** i ramen ÅTERSKAPA PROBLEMET.

iv. Klicka på **BEKRÄFTA ÄRENDE**.

b. Fortsätt fylla i formuläret med nödvändig information.

i. Skriv ditt fullständiga namn.

ii. Ange din e-postadress.

iii. Markera avtalskryssrutan.

iv. Klicka **SKAPA FELSÖKNINGSPAKET**.

Vänta en stund medan Bitdefender samlar in produktrelaterad information. Denna information kommer att hjälpa våra tekniker att finna en lösning på ditt problem.

c. Klicka på **STÄNG** för att lämna guiden. Du kommer att bli kontaktad så fort som möjligt av en av våra medarbetare.

Kontakta oss via vårt onlinesupportcenter

Om du inte kommer åt nödvändig information via Bitdefender-produkten, gå till vårt onlinesupportcenter:

1. Gå till https://www.bitdefender.com/support/consumer.html.

   Bitdefender Support Center har flera artiklar som innehåller lösningar på Bitdefender-relaterade frågor.

2. Använd sökfältet längst upp i fönstret för att hitta artiklar som kan ge en lösning på ditt problem. För att söka skriver du bara in en term i sökfältet och klickar på **Sök**.

3. Läs de relevanta artiklarna och dokumenten, och prova de föreslagna lösningarna.

4. Om lösningen inte löser ditt problem går du till

   https://www.bitdefender.com/support/contact-us.htmloch kontaktar våra supportmedarbetare.

35. ONLINERESURSER

Flera på nätet-resurser finns tillgängliga för att hjälpa dig med att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefenders supportcenter:

  https://www.bitdefender.com/support/consumer.html

- Bitdefender Supportforum:

  https://forum.bitdefender.com

- Datorsäkerhetsportalen HOTforSecurity:

  https://www.hotforsecurity.com

Du kan även använda din favoritsökmotor för att hitta mer information om datorsäkerhet, Bitdefenderprodukter och företaget.

35.1. Bitdefenders supportcenter

Bitdefenders supportcenter är en databas med information om Bitdefenderprodukter på nätet. Den lagrar, i ett lättåtkomligt format, rapporter om resultaten för utgående teknisk support och felkorrigeringsåtgärder för Bitdefenders support- och utvecklingsteam, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefenders supportcenter är öppet för allmänheten och gratis att söka igenom. Den omfattande information den innehåller är ännu ett sätt att förse Bitdefenders kunder med den tekniska kunskap och insikt de behöver. Alla giltiga begäran om information eller buggrapporter som kommer från Bitdefender-klienter hittar till slut in i Bitdefenders supportcenter, som felkorrigeringsrapporter, workaroundbeskrivningar eller informationsartiklar som tillägg till produkthjälpfiler.

Bitdefendera supportcenter är alltid tillgängligt på

https://www.bitdefender.com/support/consumer.html.

35.2. Bitdefender Supportforum

Bitdefender Supportforum tillhandahåller Bitdefender användare med ett enkelt sätt att få hjälp samt att hjälpa andra.

Om din Bitdefender-produkt inte fungerar som den ska, om den inte kan ta bort specifika hot från din dator eller om du har frågor om hur den fungerar, postar du dina problem eller frågor i forumet.

Bitdefenders supporttekniker söker i forumet efter nya poster för att kunna hjälpa dig. Du kan även få svar eller en lösning från en mer van Bitdefenderanvändare.

Innan du skickar ditt problem eller din fråga, sök igenom forumet efter ett liknande eller relaterat ämne.

Bitdefenders supportforum är tillgängligt på https://forum.bitdefender.com, på 5 olika språk: Engelska, Tyska, Franska, Spanska och Rumänska. Klicka länken **Hemma & Hemma Kontor Skydd** för att öppna sektionen som är avsedd för konsumentprodukter.

35.3. HOTforSecurity Portal

HOTforSecurity är en rik källa till datorsäkerhetsinformation. Här kan du lära dig om olika hot din dator utsätts för när den är ansluten till Internet (skadlig kod, nätfiske, spam, cyberbrottslingar).

Nya artiklar postas regelbundet för att hålla dig uppdaterad med de senaste hot som upptäckts, de nuvarande säkerhetstrenderna och annan information om branschen för datorsäkerhet.

Webbsidan HOTforSecurity är https://www.hotforsecurity.com.

36. HJÄLPINFORMATION

Effektiv kommunikation är nyckeln till en framgångsrik affärsverksamhet. Sedan 2001 har BITDEFENDER etablerat ett obestridligt anseende genom att hela tiden sträva efter bättre kommunikation för att överträffa våra klienters och partners förväntningar. Om du har frågor, tveka inte att kontakta oss.

36.1. Webbadresser

Försäljningsavdelning: sales@bitdefender.com
Supportcenter:https://www.bitdefender.com/support/consumer.html
Dokumentation: documentation@bitdefender.com
Lokala återförsäljare:https://www.bitdefender.com/partners
Partnerprogram: partners@bitdefender.com
Mediarelationer: pr@bitdefender.com
Jobbmöjligheter: jobs@bitdefender.com
Virusinlagor: virus_submission@bitdefender.com
Skräppostinlagor: spam_submission@bitdefender.com
Rapportera missbruk: abuse@bitdefender.com
Webbsida:https://www.bitdefender.com

36.2. Lokala återförsäljare

Bitdefenders lokala återförsäljare är redo att svara på alla frågor rörande deras uppgiftsområde, både i kommersiella allmänna ärenden.

För att finna en återförsäljare av Bitdefender i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din ort genom att använda motsvarande alternativ.
3. Om du inte hittar någon Bitdefender-återförsäljare i ditt land får du gärna kontakta oss via e-post på sales@bitdefender.com. Skriv ditt e-postmeddelande på engelska så att vi kan hjälpa dig så snart som möjligt.

36.3. Bitdefender-kontor

Bitdefenders kontor är redo att svara på alla frågor rörande deras verksamhetsområde, både i kommersiella och allmänna ärenden. Deras respektive adresser och kontakter finns listade nedanför.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (office&sales): 1-954-776-6262
Försäljning: sales@bitdefender.com
Tekniskt stöd: https://www.bitdefender.com/support/consumer.html
Webb: https://www.bitdefender.com

UK och Irland

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-post: info@bitdefender.co.uk
Telefon: (+44) 2036 080 456
Försäljning: sales@bitdefender.co.uk
Tekniskt stöd: https://www.bitdefender.co.uk/support/
Webb: https://www.bitdefender.co.uk

Tyskland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Office: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Försäljning: vertrieb@bitdefender.de
Tekniskt stöd: https://www.bitdefender.de/support/consumer.html
Webb: https://www.bitdefender.de

Danmark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Office: +45 7020 2282
Tekniskt stöd: http://bitdefender-antivirus.dk/
Webb: http://bitdefender-antivirus.dk/

Spanien

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Försäljning: comercial@bitdefender.es
Tekniskt stöd: https://www.bitdefender.es/support/consumer.html
Webbsida: https://www.bitdefender.es

Rumänien

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax: +40 21 2641799
Försäljning Telefon: +40 21 2063470
Försäljnings-e-post: sales@bitdefender.ro
Tekniskt stöd: https://www.bitdefender.ro/support/consumer.html
Webbsida: https://www.bitdefender.ro

Förenade Arabemiraten

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Försäljning Telefon: 00971-4-4588935 / 00971-4-4589186
Försäljnings-e-post: mena-sales@bitdefender.com
Tekniskt stöd: https://www.bitdefender.com/support/consumer.html
Webbsida: https://www.bitdefender.com

Ordlista

Abonnemang

Köpeavtal som ger användaren behörighet att använda en viss produkt eller tjänst på ett visst antal enheter och för en viss tidsperiod. En utgången prenumeration kan automatiskt förnyas med den information som användaren uppger vid det första köpet.

ActiveX

ActiveX är ett sätt att skriva program på så att andra program kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och uppför sig som datorprogram mer än statiska sidor. med ActiveX kan användare ställa eller besvara frågor, använda knappar och interagera på andra sätt med webbsidan. ActiveX-kontroller är ofta skrivna i Visual Basic.

Active X är känt för total avsaknad av säkerhetskontroller; experter på datorsäkerhet avråder från att använda det på Internet.

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.

Annonsprogram

Annonsprogram kombineras ofta med ett värdprogram som är gratis så länge som användaren går med på att tillåta annonsprogrammet. Eftersom sådana program oftast installeras efter att användaren gått med på licensavtalet, har inget brott begåtts.

Popup-reklam kan dock bli ett irritationsmoment, och i vissa fall försämra systemets prestanda. Även den privata information som vissa av dessa program samlar in kan vara oroande för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En skiva, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera komprimerade filer.

Avancerat kvarstående hot

APT (Advanced persistent threat) exploaterar säkerhetsrisker i system för att stjäla viktig information att leverera till källan. Stora grupper som organisationer, företag eller myndigheter, är måltavlor för detta hot.

Målet med ett APT är att förbli oupptäckt under en lång tid för att kunna övervaka och samla in viktig information utan att skada målmaskinerna. Den metod som används är att injicera hotet i nätverket via en PDF-fil eller ett Office-dokument som ser ofarligt ut så att alla användare kan köra filerna.

Bakdörr

Ett hål i säkerhetssystemet som avsiktligen lämnats av de som utformat och underhåller systemet. Meningen med sådana hål är inte alltid ondskefull, till exempel, "come out of the box with privileged accounts" är menat för fälttekniker eller för försäljarens underhållsprogrammerare.

Boot virus

Ett hot som infekterar startsektorn på en fast eller flyttbar disk. Ett försök att starta från en diskett infekterad med ett startsektorvirus gör att viruset blir aktivt i minnet. Varje gång du startar ditt system från och med nu innebär att du har hotet aktivt i minnet.

Bootsektor

En sektor i början av varje enhet som identifierar enhetens arkitektur (sektorstorlek, klusterstorlek osv). För startenheter innehåller boot-sektorn även ett program laddar operativsystemet.

Botnet

Termen “botnet” är sammansatt av orden “robot” och “nätverk”. Botnets är Internet-anslutna enheter infekterade med hot och som kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogramvara, ransomware och andra typer av hot. Deras mål är att infektera sp många anslutna enheter som möjligt, som datorer, servrar, mobil- eller IoT-enheter som tillhör stora företag eller industrier.

E-post

Elektronisk post. En tjänst som sänder datormeddelanden via lokala eller globala nätverk.

E-postklient
En e-postklient är en app som låter dig sända och ta emot e-postmeddelanden.

Eponeringar
Ett sätt att utnyttja olika buggar eller sårbarheter som finns i en dator (programvara eller hårdvara). På så sätt kan hackar ta kontroll över datorer eller nätverk.

Falska positiva
Inträffar när en skanning identifierar en fil som ett hot när den i själva verket inte är det.

Filändelse
Den del av ett filnamn, som kommer efter sista punkten, som visar vilken typ av data som finns lagrad på filen.

Många operativsystem använder sig av filändelser,t.ex. Unix, VMS, och MS-DOS. De består oftast av en till tre bokstäver (vissa sorgliga gamla operativsystem har inte stöd för mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Hämta
För att kopiera data (vanligtvis en hel fil) från en huvudkälla till en fjärrenhet. Termen används ofta för att beskriva processen att kopiera en fil från en tjänst på nätet till sin egen dator. Hämta kan även hänvisa till att kopiera en fil från en nätverksfilserver till en dator på nätverket.

Händelser
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 få slut minnesutrymme.

Hårddisk
Det är en maskin som läser data från, och skriver data till en skiva.

En hårddisk skriver och läser hårddiskar.

En diskettenhet har tillgång till disketter.

Diskar kan antingen vara interna (inuti ett datorchassi) eller externa (inuti en mindre extern låda som ansluts till en dator).

Heuristiskt

En regelbaserad metod för att identifiera nya hot. Den här skanningsmetoden förlitar sig inte på en specifik hotinformationsdatabas. Fördelen med den heuristiska skanningen är att den inte luras av en ny variant av ett befintligt hot. Det kan dock hända att den ibland rapporterar misstänkta koder i vanliga program, genererar de så kallade "falsk positiv".

Honungsfälla

Ett lockbetessystem som konfigureras för att locka hackare för att studera hur de agerar och identifiera vilka metoder de använder för att samla in systeminformation. Företag och koncerner är mer intresserade av att implementera och använda honungsfällor för att förbättra sin allmänna säkerhetsstatus.

Hot

Ett program eller en kod som utan din vetskap laddas upp till din dator mot din vilja. De flesta virus kan även kopiera sig själva. Alla datorvirus är tillverkade av människor. Ett simpelt virus som kan kopiera sig själv om och om igen är relativt lätt att tillverka. Även ett sådant simpelt virus är farligt eftersom det snabbt kommmer att använda upp allt ledigt minnesutrymme och orsaka en systemkrasch. Ett ännu farligare typ av virus är ett virus som kan sända sig själv via nätverk och ta sig förbi säkerhetssystem.

Icke-heuristiskt

Den här skanningsmetoden förlitar sig på en specifik hotinformationsdatabas. Fördelen med icke-heuristisk skanning är att den inte låter sig luras av vad som kan se ut som ett hot och genererar inte falska alarm.

IP

Internetprotokoll - Ett routabelt protokoll i TCP/IP som ansvarar för IP-adressering, routing, och fragmenteringen och återmonteringen av IP-paket.

Java-applet

Ett Java-program som är konstruerat för att endast köras på en webbsida. För att använda en applet på en webbsida måste du ange namnet op appleten och storleken (längd och bredd, i pixlar) som appleten kan

använda. När webbsidan öppnas laddar webbläsaren ner appleten från en server och kör den på användarens maskin (klienten). Appletar skiljer sig från appar eftersom de styrs av ett strikt säkerhetsprotokoll.

Till exempel, fastän applets körs på klienten kan de inte läsa eller skriva data till klientens maskin. Dessutom är applets mer begränsade till att endast kunna läsa och skriva data från samma domän de kommer ifrån.

Kaka

I Internet-branschen beskrivs cookies som små filer som innehåller information om individuella datorer, som kan analyseras och användas av annonsörer för att följa vad du gör och dina intressen på nätet. Inom detta område utvecklas cookie-teknologin fortfarande, och målet är att kunna rikta annonser direkt mot vad su sagt att du är intresserad av. För många är det ett tveeggat svärd då det å ena sidan är effektivt och relevant eftersom man bara ser annonser om sådant man är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" dina aktviteter. Förståeligt nog så finns det en debatt om privatliv, och många människor känner sig kränkta av känslan att de behandlas som en EAN-kod (du vet streckkoden på baksidan av förpackningar som skannas i matbutiken). Även om detta sätt att se på saken kan vara extremt, så är det i vissa fall sant.

Keylogger

En keylogger är en app som loggar allt du skriver.

Keyloggers är inte skadliga till sin natur. De kan användas i legitima syften, som att övervaka anställdas eller barns aktivitet. De används dock mer och mer av cyberbrottslingar för skadliga syften (till exempel för att samla in privat information, som inloggningsuppgifter och personnummer).

Kommandorad

I ett kommandorads-gränssnitt skriver användaren kommandon i utrymmet som finns direkt på skärmen genom att använda kommandospråk.

Komprimerade program

En fil i komprimerat format. Många operativsystem och appar innehåller kommandon som gör att du kan komprimera en fil så att den tar upp mindre minne. Till exempel, säg att du har en textfil som innehåller tio

blanksteg på varandra. Detta skulle normalt kräva tio bytes lagringsutrymme.

Dock skulle ett program som komprimerar filer ersätta blankstegen med ett speciellt tecken för blanksteg följt av hur många blanksteg som ersätts. I detta fall kommer de tio stegen endast kräva två bytes utrymme. Detta är bara en komprimeringsmetod - det finns många fler.

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, har stöd för kraftfulla makrospråk.

Dessa appar tillåter dig att bädda in ett makro i ett dokument samt låter makrot köras varje gång dokumentet öppnas.

Mask

Ett program som sprider sig själv över ett nätverk och reproducerar sig självt efter hand. Det kan inte fästa sig till andra program.

Minne

Interna lagringsytor på datorn. Med termen minne menas lagring av information i kretsar, och ordet lagring används för minne som finns på band eller diskar. Till varje dator följer det en viss mängd fysiskt minne, vilket brukar kallas för internminne eller RAM-minne.

Onlineförövare

Personer som försöker locka minderåriga eller tonåringar till konversationer i syfte att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den perfekta platsen där sårbara barn kan sökas upp och lockas att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Onlinemobbning

När kollegor eller främlingar begår oegentliga handlingar mot barn i syfte att fysiskt skada. För att skada emotionellt skickas förövarna elaka meddelanden eller osmickrande foton, för att därmed isolera sina offer från andra eller få dem att känna sig frustrerade.

Ordlisteattack

Lösenordsgissningsattacker som används för att bryta sig in i ett datorsystem genom att ange em kombination av vanliga ord för att generera potentiella lösenord. Samma metod används för att gissa

avkrypteringsnycklar för krypterade meddelanden eller dokument. Ordlisteattacker lyckas eftersom många människor tenderar att använda korta lösenord och lösenord med ett ord som är enkla att gissa.

Phishing

Att skicka ett e-postmeddelanden till en användare och utge sig för att vara ett legitimt företag i ett försök att lura användaren att uppge privat information som kan användas för identitetsstöld. E-postmeddelandet skickar användaren till en webbsida där de ombes uppdatera personlig information, som lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och endast uppsatt för att stjäla användarens information.

Photon

Photon är en innovativ, ej störande Bitdefender-teknik, konstruerat för att minimera prestandainverkan för din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den ett användningsmönster som bidrar till att optimera start- och skanningsprocesser.

Polymorfa Virus

Ett virus som ändrar form med varje fil det smittar. Eftersom det inte har något konsekvent binärt mönster är sådana virus svåra att identifiera.

Port

En dators gränssnitt till vilket du kan ansluta en enhet. Hemdatorer har olika sorters portar. Internt finns flera portar för anslutning av diskenheter, skärmar och tangentbord. Externt finn portar för anslutning av modem, skrivare, möss och andra externa enheter.

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 från användarna genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall är några varianter som jagar personliga användarsystem.

Infektionen kan spridas genom att öppna skräppostmeddelanden, hämta e-postbilagor eller installera appar, utan att låta användaren vet vad som händer på deras system. Varje dag utsätts användare och företag för ransomwarehackare.

Rapportera fil
En fil som listar inträffade åtgärder. Bitdefender underhåller en rapportfil som listar den skannade sökvägen, de mappar, antal filer och arkiv som skannats, hur många infekterade och misstänkta filer som hittats.

Råstyrkeattack
Lösenordsgissningsattack använd för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast genom att börja med de som är lättast att gissa.

Script
En annan term för makro eller batch-fil, ett script är en lista med kommandon som kan utföras utan användarens medverkan.

Skräppost
Elektronisk skräppost eller skräp nyhetsgruppsinlägg. Generellt känt som oönskade e-postmeddelanden.

Sökväg
Exakt anvisning till en fil på en dator. Dessa anvisningar är vanligtvis beskrivna i ett hierarkiskt katalogsystem uppifrån och nedåt.

Vägen mellan två punkter, exempelvis vägen för kommunikation mellan två datorer.

Spionprogram
All programvara som i hemlighet samlar in användarinformation via användarens Internetuppkoppling utan hans eller hennes vetande, vanligen ur reklamsyfte. Spionprogram är vanligtvis paketerat som en dold komponent i gratisprogram eller delningsprogram som kan laddas ner från Internet; det bör dock noteras att majoriteten av gratisprogrammen och delningsprogrammen inte bär på spionprogram. När det väl installerats så övervakar spionprogrammet användarens aktiviteter på Internet och skickar i bakgrunden denna information till någon annan. Spionprogram kan även samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med Trojanska hästar är att användare ovetande installerar produkten när de installerar något annat. Ett vanligt sätt att falla offer för spionprogram är att hämta vissa pir till pir fildelningsprodukter som finns tillgängliga idag.

Förutom frågorna om etik och sekretess stjäl spionprogram från användaren genom att använda datorns minnesresurser och ta upp bandbredd när den sänder tillbaka information till sin hemmabas via användarens Internetanslutning. Eftersom spionprogram använder minnes- och systemresurser kan de program som körs i bakgrunden leda till systemkrasch eller generell systeminstabilitet.

Spökprogram

Ett rootkit är en uppsättning programvaruverktyg som erbjuder administratörsnivååtkomst till ett system. Termen användes från början av operativsystemet UNIX och refererade till ombyggnadsverktyg som gav inkräktare administrativa rättigheter och lät dem dölja sin närvaro för att inte upptäckas av systemadministratörerna.

Den huvudsakliga uppgiften för spökprogram är att gömma processer, filer, inloggningsuppgifter och loggar. De kan även snappa upp information från terminaler, nätverksanslutningar och externa enheter om de lyckas nästla sig in i "rätt" program.

Spökprogram är inte naturligt skadliga. Till exempel gömmer system och även vissa program kritiska filer genom att använda spökprogram. De används dock oftast för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. När de kombineras med hot utgör rootkits ett stort hot till systemets integritet och säkerhet. De kan övervaka trafik, skapa bakdörrar in i system, ändra filter och loggar för att undgå upptäckt.

Startposter

Alla filer som placeras i denna mapp kommer att öppnas när datorn startas. Till exempel, en startskärm, en ljudfil som ska spelas upp när datorn först startar, en påminnelsekalender eller appar kan vara uppstartsobjekt. Vanligen placeras ett alias för filen i mappen istället för den aktuella filen.

Systemfältet

Introducerat med Windows 95, finns systemfältet i Windows aktivitetsfält (vanligtvis längst ner vid klockan) och innehåller miniatyrikoner för enkel

tillgång till systemfunktioner såsom fax, skrivare, modem, volym och mer. Dubbelklicka eller högerklicka en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Överföringskontroll/Internetprotokoll - En uppsättning nätverksprotokoll som ofta används på Internet och erbjuder kommunikation över sammankopplade datornätverk med diverse maskinvaruarkitekturer och operativsystem. TCP/IP omfattar standard för hur datorer kommunicerar och konvent för anslutna nätverk och routing-trafik.

Trojansk

Ett destruktivt program som maskerar sig som ett godartat. Till skillnad från skadliga program och maskar kan inte trojaner kopiera sig själva, men de kan vara minst lika destruktiva. Ett av de mest försåtliga typerna av trojaner är ett program som gör anspråk på att rensa datorn från hot, men istället inför hot på datorn.

Termen kommer från en berättelse i Homeros Illiaden där Grekerna ger en enorm trähäst till sina fiender Trojanerna, skenbart en fredsgåva. Men när Trojanerna dragit hästen innanför murarna så smyger Grekiska soldater ut ur hästens mage och öppnar porten till staden så deras kamrater kan välla in och ta över Troja.

Uppdatera

En ny version av programvara eller maskinvara utformad för att ersätta äldre versioner av samma produkt. Dessutom kontrollerar ofta installations-rutinerna för uppdatering, din dator för att vara säker på att en äldre version redan finns installerad på din dator; om inte, kan du installera uppdateringen.

Bitdefender har sin egen uppdateringsmodul som låter dig manuellt kontrollera efter uppdateringar, eller automatiskt låter den uppdatera produkten.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att hitta och ta bort hotet.

Utforskaren

Kort för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare omfattar Microsoft Internet

Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare vilket betyder att de kan visa både grafik och text. Dessutom kan de flesta moderna webbläsare visa multimediainformation som inkluderar ljud och bild, även om det för vissa format krävs insticksprogram.

Virtual Private Network (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.