

# Bitdefender<sup>®</sup> MOBILE SECURITY



**ANVÄNDARMANUAL**





## Bitdefender Mobile Security Användarmanual

Publication date 09-09-2019

Copyright© 2019 Bitdefender

### Juridisk notering

**Alla rättigheter förbehållna.** Ingen del av denna bok får reproduceras eller överföras i någon form eller på något sätt, elektroniskt eller mekaniskt, inklusive fotokopiering, inspelning eller på annan informationslagring eller något informationshämtningssystem, utan skriftligt tillstånd från en behörig företrädare för Bitdefender. Införande av korta citat i recensioner är möjligt endast med angivande av den citerade källan. Innehållet kan inte ändras på något sätt.

**Varning och friskrivningsklausul.** Denna produkt och dess dokumentation skyddas av upphovsrätt. Informationen i detta dokument tillhandahålls på "befintligt skick" utan garanti. Trots att alla försiktighetsåtgärder har tagits i utarbetandet av detta dokument kommer författarna inte ha något ansvar till någon person eller enhet med hänsyn till eventuell förlust eller skada som orsakats eller påstås ha orsakats direkt eller indirekt av informationen i detta arbete.

Denna bok innehåller länkar till tredje parts webbsidor som inte är under Bitdefenders kontroll, därför är inte Bitdefender ansvarig för innehållet av en länkad webbsida. Om du öppnar en tredje parts webbsida som listas i detta dokument, gör du så på egen risk. Bitdefender tillhandahåller endast dessa länkar som en förmån och integration av länkarna innebär inte att Bitdefender stöder eller accepterar något ansvar för innehållet av tredje parts webbsidor.

**Varumärken.** Varumärkets namn kan visas i denna bok. Alla registrerade och oregistrerade varumärken i detta dokument är respektive ägares enskilda egendom och är respektfullt erkända.



## Innehållsförteckning

1. Skyddsfunktioner .....	1
2. Komma igång .....	2
3. Skanner för skadlig kod .....	7
4. Web Protection .....	10
5. VPN .....	12
6. Anti-Theft-funktioner .....	15
7. Kontointegritet .....	19
8. App Lock .....	21
9. Rapporter .....	26
10. WearON .....	27
11. Om .....	28
12. Bitdefender Central .....	29
13. Vanliga frågor .....	35
14. Få hjälp .....	41



## 1. SKYDDSFUNKTIONER

Bitdefender Mobile Security skyddar din Android-enhet med följande funktioner:

- Skanner för skadlig kod
- Web Protection
- VPN
- Anti-Theft, inklusive:
  - Fjarrplats
  - Fjärråsning av enhet
  - Fjärrradering 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.



## 2. 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:



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. 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 kunna erbjuda 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. 7).

## **Web Protection**

Säkerställer en säker surfupplevelse genom att varna dig om möjliga skadliga webbsidor. Mer information finns på "[Web Protection](#)" (p. 10).

## **VPN**

Krypterar internetkommunikation, hjälper dig att bibehålla din integritet oavsett vilket nätverk du är ansluten till. Mer information finns på "[VPN](#)" (p. 12).

## **Anti-Theft**

Gör att du kan aktivera och inaktivera antistöldfunktionerna och konfigurera antistöldinställningarna. Mer information finns på "[Anti-Theft-funktioner](#)" (p. 15).

## **Kontointegritet**

Kontrollerar om dataintrång har inträffat i de onlinekonton du använder. Mer information finns på "[Kontointegritet](#)" (p. 19).





## **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. 21).

## **Rapporter**

För en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden i samband med enhetens aktivitet. Mer information finns på "[Rapporter](#)" (p. 26).

## **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. 27).



## 3. 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 avinstallationssskärm.

### ● 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**.

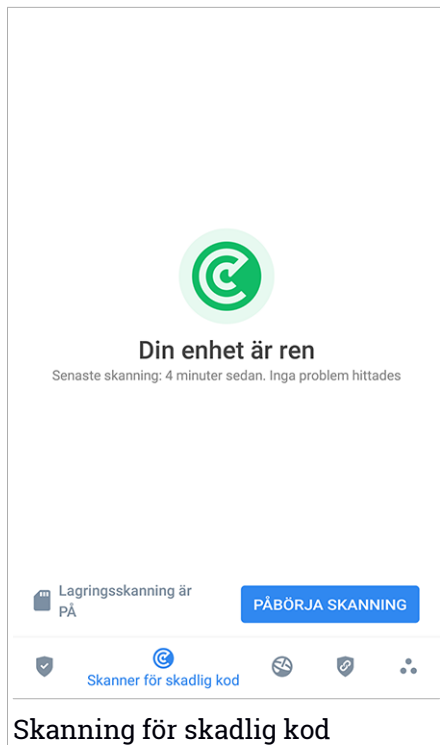


### Notera

Ytterligare behörigheter krävs på Android 6 för funktionen Skanner för skadlig kod. 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.



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 Virus-skanner.

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





## 4. WEB PROTECTION

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 webbplatsen tillfälligt och en varning visas.

Du kan välja att ignorera varningen och fortsätta till webbplatsen 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

	<b>Chrome</b> Installerad	<a href="#">ÖPPNA</a>
	<b>Dolphin</b>	
	<b>Firefox</b>	

---

   **Webbskydd**  

---

### Web Protection



## 5. 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

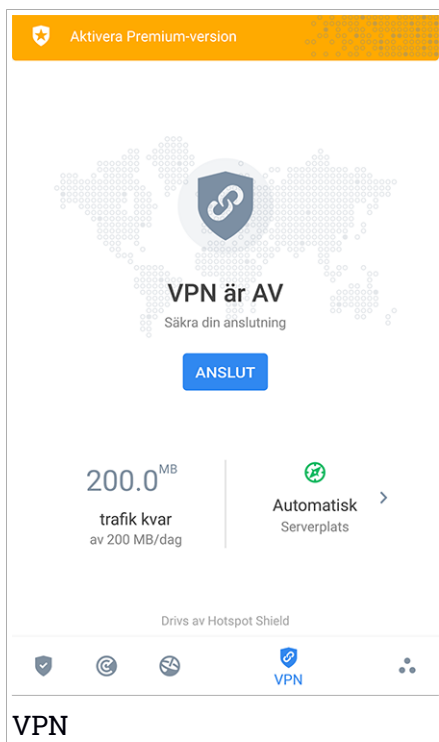


det trycker du och håller ned Bitdefender-ikonen på din startskärm eller App-låda och väljer sedan ikonen .

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. 14).




## 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 200 MB trafiksaldo per enhet för att säkra din anslutning varje gång du behöver det och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en server när du vill, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst genom att trycka på **AKTIVERA PREMIUM** som finns i kontrollpanelen eller **Aktivera Premium-version** i VPN-fönstret.

Bitdefender Premium VPN-prenumerationen är fristående från Bitdefender Mobile Security-prenumerationen, vilket innebär att du kan använda den under hela dess tillgänglighet, oavsett status på din säkerhetsprenumeration. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Mobile 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.



## 6. 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 antistöldfunktionen. 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. På enheter som har stöd för fingeravtrycksautentisering kan en fingeravtrycksverifiering 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 fingeravtrycksbekräftelsen du ställer för att skydda enheten anges fel tre gånger i rad, tas ett foto med framkameran. 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 fotot på 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 webbstyruingskommandon 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.



## 7. 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 validera 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 **Kointegritet** 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**. För att göra det:

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.



## 8. 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.





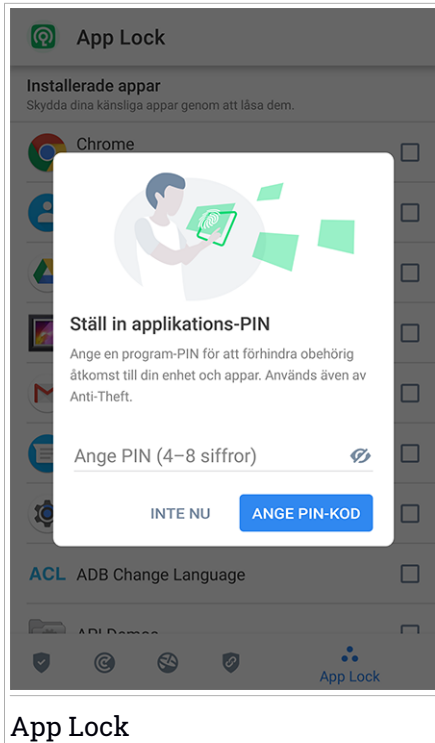
## 7. Välj de appar du vill skydda.

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.



## Låsläge



Första gången du lägger til en app till App Lock visas skärmen App Lock-läge. Härifrån kan du välja när funktionen App Lock ska skydda de appar 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 av 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 foton som togs.

Endast de två senaste foton 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.




## 9. 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**.



## 10. 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.



## 11. 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.



## 12. 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.
- **iOS** 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 webbplatsformen.


## 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** och 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.
- **Antistöld.** 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. 15).

## 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 prenumerationsskort.

## 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. 2).

## 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 prenumerationsskort.
4. Tryck **FÖRNYA** för att fortsätta.

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



## 13. VANLIGA FRÅGOR

### **Varför kräver Bitdefender Mobile Security en Internet-anslutning?**



Appen måste kommunicera med Bitdefender-serverar 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-serverar 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, siffror och symboler (@, !, %, #, mm.).
- Se till att den information du skickar går över säkra anslutningar. Webbplatstillägget online måste vara HTTPS:// och inte HTTP://.

## När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du öppnar, hämtar eller laddar upp innehåll på Internet. För att vara säker på att du är trygg när du surfar på nätet 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 designad för att skydda dina personuppgifter, dölja din IP-adress när du är ansluten på osäkra trådlösa nätverk och öppna 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 designa för att ge dig en lätt upplevelse när du surfar på nätet, men din Internet-anslutning eller serveravståndet du ansluter till kan orsaka att det går långsammare. I det fallet, om det inte är nödvändigt att du ansluter från din plats till en avlägsen server (t.ex. från USA till Kina), rekommenderar vi att tillåter Bitdefender VPN att automatiskt ansluta dig till den närmaste servern eller hitta en server närmare 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 fjärrlåsnings och enhetsradering skulle inte kunna ta bort dina 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.



## 14. FÅ HJÄLP

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.

### 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 in Bitdefender Support Center, som felkorrigeringsrapporter, workaroundsbeskrivningar eller informationsartiklar som tillägg till produkthjälpfiler.

Bitdefendera supportcenter är alltid tillgängligt på <https://www.bitdefender.com/support/>.

### Bitdefender Supportforum

Bitdefender Supportforum tillhandahåller Bitdefender användare med ett enkelt sätt att få hjälp samt att hjälpa andra.



Om din Bitdefenderprodukt inte fungerar som den ska, om den inte kan ta bort särskilda hot från din enhet eller om du har frågor om hur den fungerar, posta 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 Bitdefender-användare.

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 & Hemmakontorsskydd** för att öppna avsnittet som är avsett för konsumentprodukter.

## HOTforSecurity Portal

HOTforSecurity-portalen är en rik källa till säkerhetsinformation. Här kan du lära dig om olika hot din dator utsätts för när den är ansluten till Internet (skadlig kod, nätfiske, spam, cyberbrottslingar). En användbar ordlista hjälper dig att förstå datorsäkerhetstermer som du inte är bekant med.

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://hotforsecurity.bitdefender.com/>.