

Norton™ AntiVirus Plus

Norton™ 360

Norton™ 360 met LifeLock™

Norton™ 360 for Gamers

Gebruikershandleiding



# Gebruikershandleiding voor Norton™ 360 met LifeLock™

De software die in deze handleiding wordt beschreven, wordt geleverd met een licentieovereenkomst en mag alleen worden gebruikt in overeenstemming met de voorwaarden in deze overeenkomst.

Copyright © 2021 NortonLifeLock Inc. Alle rechten voorbehouden.

Het product dat in dit document wordt beschreven, wordt gedistribueerd onder licenties waarmee het gebruik, het kopiëren, het distribueren en het decompileren/toepassen van reverse-engineering ervan wordt beperkt. Geen enkel deel van dit document mag worden gereproduceerd in enige vorm op enige wijze zonder voorafgaande schriftelijke toestemming van NortonLifeLock Inc en haar eventuele licentiegevers.

DE DOCUMENTATIE WORDT GELEVERD "ZOALS DEZE IS" EN ALLE EXPLICIETE OF IMPLICIETE VOORWAARDEN, REPRESENTATIES EN GARANTIES, WAARONDER IMPLICIETE GARANTIES VAN VERKOOPBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL OF NIET-SCHENDING WORDEN AFGEWEEZEN, TENZIJ DERGELIJKE DISCLAIMERS NIET WETTELIJK ZIJN TOEGESTAAN. NORTONLIFELock INC. IS NIET AANSPRAKELIJK VOOR INCIDENTELE OF GEVOLGSCHADE IN VERBAND MET DE VERSTREKKING, PRESTATIES OF HET GEBRUIK VAN DEZE DOCUMENTATIE. DE INFORMATIE IN DEZE DOCUMENTATIE KAN ZONDER VOORAFGAANDE KENNISGEVING WORDEN GEWIJZIGD.

De Gelicentieerde Software en Documentatie worden beschouwd als commerciële computersoftware zoals gedefinieerd in FAR 12.212 en zijn onderhevig aan beperkte rechten zoals gedefinieerd in FAR Sectie 52.227-19 'Commercial Computer Software - Restricted Rights' en DFARS 227.7202, e.v. 'Commercial Computer Software and Commercial Computer Software Documentation,' al naar gelang van toepassing, en eventuele verdere voorschriften, ongeacht of die door NortonLifeLock zijn geleverd op locatie of als hosted services. Het gebruiken, wijzigen, uitgeven van een reproductie, uitvoeren, weergeven of openbaar maken van de Gelicentieerde Software en Documentatie door de Amerikaanse regering zal uitsluitend gebeuren in overeenstemming met de voorwaarden van deze Overeenkomst.

NortonLifeLock Inc.  
60 East Rio Salado Parkway,  
Suite 1000,  
Tempe, AZ 85281

<https://www.nortonlifelock.com>

# Inhoudsopgave

Hoofdstuk 1	Welkom bij Norton LifeLock .....	6
	Systeemvereisten voor Norton 360 .....	6
	Uw NortonLifeLock-account openen .....	8
Hoofdstuk 2	Uw beveiliging instellen .....	9
	Apparaatbeveiliging configureren .....	9
	Norton Password Manager instellen .....	10
	Cloudback-up instellen .....	16
	LifeLock Identity Theft Protection configureren .....	17
	Toezicht op het dark web wordt mogelijk gemaakt door LifeLock** .....	18
	Uw Veilige VPN instellen .....	19
	Ouderlijk toezicht instellen .....	20
	Bescherm uw bankgegevens met Norton Safe Web .....	24
Hoofdstuk 3	Uw apparaatbeveiliging beheren .....	25
	Wat te doen als uw apparaat gevaar loopt .....	25
	LiveUpdate uitvoeren .....	26
	Beveiligingsrisico voor apparaten die Norton detecteert weergeven of verhelpen .....	27
	Risico's of bedreigingen in quarantaine verwerken .....	28
	Norton gebruiken om de prestaties van de computer te optimaliseren en te verbeteren .....	30
	Norton-scans uitvoeren om uw pc op bedreigingen te controleren .....	34
	Uw eigen aangepaste Norton-scans maken .....	37
	Norton-scans plannen .....	38
	Realtimebedreigingen weergeven die door Norton SONAR zijn gedetecteerd .....	39
	Bestanden en mappen uitsluiten van de scans Norton Auto-Protect, SONAR en Downloadinformatie .....	40
	Bestanden met handtekening voor laag risico van Norton-scans uitsluiten .....	41
	Automatische taken in- of uitschakelen .....	42
	Aangepaste taken uitvoeren .....	43

Beveiligings- en prestatiescans plannen .....	43
Gegevensbescherming configureren om schadelijke processen te blokkeren die uw pc beïnvloeden .....	45
Norton instellen om scripts die door phishing-pogingen kunnen worden misbruikt te verwijderen .....	47
Meer informatie over Scriptbeheer van Norton .....	50
Bescherm uw apparaat tegen misbruik, hackers en zero-day aanvallen. ....	53
Norton Firewall in- of uitschakelen .....	54
Programmaregels aanpassen om toegangsinstellingen voor programma's te wijzigen .....	55
De volgorde van firewallregels wijzigen .....	56
Een verkeersregel tijdelijk uitschakelen .....	57
Internettoegang toestaan voor een geblokkeerd programma .....	57
Melding van firewallblokkering uitschakelen .....	59
Meer informatie over de lijst met uitsluitingen voor Inbraakpreventie .....	59
Browserbeveiliging inschakelen .....	60
Stel Norton Firewall in om waarschuwingen over blokkering van een aanval in of uit te schakelen .....	61
AutoBlock in- of uitschakelen .....	62
De blokkering opheffen van computers die door Norton AutoBlock zijn geblokkeerd .....	63
Een apparaat toevoegen aan Apparaatvertrouwen .....	63
Downloadinformatie in- of uitschakelen .....	65
Filteren van spam in- of uitschakelen .....	65
Internetgebruik definiëren voor Norton .....	66
Beperken van netwerkgebruik in- of uitschakelen .....	67
Norton instellen om toezicht te houden op toepassingen en schadelijke websites te blokkeren op uw computer .....	68
Aan de slag met Norton Cloudback-up .....	70
Bestanden en mappen toevoegen aan of uitsluiten van uw back-upsets .....	71
De standaard bestandstypen of bestandsextensies die Norton in back-ups opneemt, weergeven of wijzigen .....	72
Foto's, muziek of andere belangrijke bestanden herstellen uit Norton-back-upsets .....	73
Back-upset en -bestanden verwijderen uit Cloudback-up .....	74
De instellingen van uw Norton-product aanpassen .....	75
Instellingen voor Realtimebeveiliging aanpassen .....	76
Meer informatie over de instellingen voor Scans en risico's .....	78
Meer informatie over de instellingen van Inbraakpreventie en browserbeveiliging .....	80

	Norton zo instellen dat u uw beschermde apparaten op afstand kunt beheren .....	81
	Instellingen voor Norton-apparaatbeveiliging beschermen tegen onbevoegde toegang .....	82
	Een sneltoets instellen om in Norton-apparaatbeveiliging te zoeken naar informatie .....	82
	Uw computer optimaliseren voor gamen met Game Optimizer .....	83
	Meer informatie over Game Optimizer .....	85
	Handmatig games aan de lijst Geoptimaliseerde games toevoegen .....	86
Hoofdstuk 4	Extra oplossingen vinden .....	88
	Apparaatbeveiliging op Windows verwijderen .....	88
	Disclaimers .....	88

# Welkom bij Norton LifeLock

Dit hoofdstuk bevat de volgende onderwerpen:

- [Systeemvereisten voor Norton 360](#)
- [Uw NortonLifeLock-account openen](#)

## Systeemvereisten voor Norton 360

### Alleen licenties voor Norton-apparaatbeveiliging

- Norton™ AntiVirus Plus dekt één pc of Mac

### Licenties voor Apparaatbeveiliging en Norton Secure VPN

Ondersteunt apparaten die draaien op Windows, Mac, Android en iOS

- Norton™ 360 Standard dekt één apparaat
- Norton™ 360 Deluxe dekt maximaal 5 apparaten
- Norton™ 360 Premium dekt maximaal 10 apparaten
- Norton™ 360 met LifeLock Select dekt maximaal 5 apparaten
- Norton™ 360 met LifeLock Advantage dekt maximaal 10 apparaten
- Norton™ 360 met LifeLock Ultimate Plus dekt een onbeperkt aantal apparaten (beperkingen zijn van toepassing\*)
- Norton™ 360 for Gamers dekt tot 3 apparaten

---

**Opmerking:** Niet alle aanbiedingen voor NortonLifeLock-bescherming die hierboven worden vermeld, zijn in alle regio's of voor alle partners beschikbaar.

---

## Apparaatbeveiliging

---

**Opmerking:** Niet alle functies zijn beschikbaar op alle platforms.

---

---

**Opmerking:** Ouderlijk toezicht, Cloudback-up en SafeCam worden momenteel niet ondersteund op Mac OS.

---

### Windows™-besturingssystemen

- ◆ ■ Microsoft Windows® 10 (alle versies)
  - Microsoft Windows® 10 in S-modus (32-bits, 64-bits of ARM32) versie 1803 en hoger
  - Microsoft Windows® 8/8.1 (alle versies)  
Sommige beschermingsfuncties zijn niet beschikbaar in browsers in het startscherm van Windows 8.
  - Microsoft Windows® 7 (32-bits en 64-bits) met Service Pack 1 (SP 1) of later

---

**Opmerking:** Norton AntiVirus Plus wordt niet ondersteund op Windows 10 in S-modus.

---

### Mac®-besturingssystemen

- ◆ Mac OS X 10.10.x of later voor een Norton-product met versie 8.0 of later.

---

**Opmerking:** Ouderlijk toezicht van Norton Family en Cloudback-up worden momenteel niet ondersteund op Mac OS.

---

### Android™-besturingssystemen

- ◆ Android 6.0 of hoger  
Google Play moet zijn geïnstalleerd.  
Automatisch scannen van apps op Google Play wordt ondersteund op Android 4.1 of later, met uitzondering van Samsung-apparaten. Samsung-apparaten met Android 4.2 of later worden ondersteund. Voor eerdere versies van Android moet de functie Delen van Google Play gebruiken om apps op Google Play te scannen.

### iOS-besturingssystemen

- ◆ iPhones of iPads met de huidige en laatste twee versies van Apple iOS

## Systeemvereisten voor Norton™ Secure VPN

Beschikbaar voor Windows™-pc's, Macs®, iOS- en Android™-apparaten:

Norton Secure VPN is compatibel met pc's, Macs, Android-smartphones en tablets, iPads en iPhones. Norton Secure VPN kan op het opgegeven aantal apparaten worden gebruikt - met onbeperkt gebruik tijdens de abonnementsperiode.

#### Windows™-besturingssystemen

- ◆ ■ Microsoft Windows® 10 (alle versies behalve Windows 10 S)
- Microsoft Windows® 8/8.1 (alle versies)
- Microsoft Windows® 7 (32-bits en 64-bits) met Service Pack 1 (SP 1) of later  
150 MB beschikbare schijfruimte.

#### Mac®-besturingssystemen

- ◆ Huidige en vorige twee versies van Mac OS.  
300 MB beschikbare schijfruimte.

#### Android™-besturingssystemen

- ◆ Android 6.0 of hoger  
Google Play moet zijn geïnstalleerd.

#### iOS-besturingssystemen

- ◆ iPhones of iPads met de huidige en laatste twee versies van Apple iOS

## Uw NortonLifeLock-account openen

Via uw NortonLifeLock-account kunt u uw abonnementsgegevens beheren, uw productsleutel vinden, abonnementsverlenging inschakelen of toegang krijgen tot andere services.

#### Uw account openen

- 1 Ga naar [my.Norton.com](https://my.Norton.com) en klik op **Aanmelden**.
- 2 Voer uw gebruikersnaam/e-mailadres en wachtwoord in en klik vervolgens op **Aanmelden**.
- 3 Bent u uw wachtwoord vergeten, klik dan op **Wachtwoord vergeten?** en geef uw e-mailadres op.

Als u een bericht ziet waarin staat dat uw account tijdelijk is geblokkeerd vanwege te veel mislukte aanmeldingspogingen, raden we u aan één uur te wachten en het dan nogmaals te proberen.



# Uw beveiliging instellen

Dit hoofdstuk bevat de volgende onderwerpen:

- [Apparaatbeveiliging configureren](#)
- [Norton Password Manager instellen](#)
- [Cloudback-up instellen](#)
- [LifeLock Identity Theft Protection configureren](#)
- [Uw Veilige VPN instellen](#)
- [Ouderlijk toezicht instellen](#)
- [Bescherm uw bankgegevens met Norton Safe Web](#)

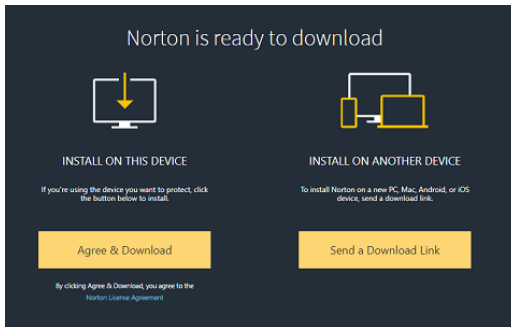
## Apparaatbeveiliging configureren

U moet Apparaatbeveiliging van Norton installeren om uw apparaat te beschermen. U kunt Apparaatbeveiliging installeren op Windows-desktops en -laptops, Mac-computers en mobiele apparaten met Android en iOS.

### Apparaatbeveiliging downloaden en installeren

- 1 Open uw browser op elke computer, laptop en smartphone en typ het volgende adres:  
<https://norton.com/setup>
- 2 Meld u aan bij uw NortonLifeLock-account.

3 Klik in het venster **Norton instellen op Akkoord en downloaden**



- 4 Klik op de sectie die de pijl op het scherm aanwijst en volg de instructies op het scherm. Uw service wordt automatisch gedownload, geïnstalleerd en geactiveerd.

---

**Opmerking:** Als u een foutmelding ziet wanneer u uw service downloadt, of als uw download niet wordt voltooid, kunt u de download opnieuw starten.

---

## Norton Password Manager instellen

Nadat u Apparaatbeveiliging heeft geïnstalleerd, wordt u gevraagd browserextensies toe te voegen. U moet de extensies aan de Internet Explorer-, Firefox- en Chrome-browsers toevoegen om ervoor te zorgen dat de functies werken.

U moet de Norton-browserextensies inschakelen voor toegang tot alle browserspecifieke functies. De Norton-browserextensies omvatten:

Norton Safe Web

Een beveiligde zoekervaring waarmee u veilig op internet kunt surfen, zoeken en winkelen. Het analyseert de websites die u bezoekt en detecteert of er virussen, spyware, malware of andere bedreigingen op staan.

Norton Safe Search

Een beveiligde zoekmachine die Ask.com en Yahoo! gebruikt om zoekresultaten te genereren. Norton Safe Search rangschikt de zoekresultaten op basis van de beveiligingsstatus van de site en de Norton-beoordeling.

Norton-startpagina	Een website die gebruik maakt van de functie Norton Safe Search om uw zoekervaring op internet te verbeteren. U ziet de beveiligingsstatus van de website en de Norton-beoordeling voor het gegenereerde zoekresultaat.
Norton Password Manager	Een veilige locatie waar u al uw vertrouwelijke gegevens kunt opslaan, zoals aanmeldingen, persoonlijke gegevens en financiële informatie. U kunt deze informatie gebruiken wanneer u zich aanmeldt bij websites, automatisch online formulieren invult en online betaalt.

## Internet Explorer

### De Norton-browserextensie toevoegen in Internet Explorer

- 1 Nadat u Norton de eerste keer heeft geïnstalleerd, wordt de pagina **Browserbeveiliging** automatisch in een nieuw venster geopend wanneer u Internet Explorer start.
- 2 Klik op de pagina **Browserbeveiliging** op de optie **Inschakelen** van de **Norton Security-werkbalk**.
- 3 In de pop-up van de extensies klikt u op **Extensie toevoegen**.
- 4 Nadat u de Norton Security-werkbalk heeft ingeschakeld, kunt u de extensies van Norton Safe Search, Norton-startpagina en Norton Password Manager voor uw browser inschakelen.  
  
Gebruik de optie **Klik om toe te voegen** en volg de instructies op het scherm om deze functies in te schakelen.
- 5 Als u deze extensies niet heeft geïnstalleerd, wordt de melding **Internet Explorer-beveiligingswaarschuwing** weergegeven wanneer u Internet Explorer na een week start.  
  
Klik op **Nu installeren** en volg de instructies op het scherm om de extensies te installeren.

---

**Opmerking:** Als u de Norton-extensie op een later tijdstip wilt activeren, klikt u op **Melding later herhalen**. Als u wilt dat de melding niet meer wordt weergegeven, klikt u op **Niet meer vragen**.

---

## Google Chrome

### De Norton-browserextensies toevoegen in Google Chrome

---

**Opmerking:** U moet de nieuwste versie van Norton 360 hebben om de browserextensies van Google Chrome te installeren. Als u de nieuwste versie niet heeft, moet u LiveUpdate uitvoeren in uw Norton-product. We bieden de volgende extensies voor de Google Chrome-browser:

---

- Norton Safe Web
- Norton Password Manager
- Norton Safe Search
- Norton-startpagina

Volg de onderstaande instructies om de browserextensies voor Chrome te installeren.

- 1 Nadat u Apparaatbeveiliging voor het eerst heeft geïnstalleerd, wordt de pagina **Browserbeveiliging** automatisch in een nieuw venster geopend wanneer u Google Chrome start.  
  
U kunt de pagina **Browserbeveiliging** ook openen door onder **Internetbeveiliging** op de optie **Nu instellen** te klikken.
- 2 Klik op de pagina **Browserbeveiliging** op de optie **Klik om toe te voegen** van **Norton Safe Web**.
- 3 In de pop-up van de extensies klikt u op **Extensie toevoegen**.
- 4 Nadat u Norton Safe Web heeft ingeschakeld, kunt u de extensies Norton Safe Search, Norton-startpagina en Norton Password Manager voor uw browser inschakelen. Gebruik de optie **Klik om toe te voegen** en volg de instructies op het scherm om deze extensies in te schakelen.  
  
Klik op **Alle Norton-extensies gratis toevoegen** en volg de instructies op het scherm om alle Norton-extensies in Google Chrome in te schakelen.
  - Als u de Norton Safe Web-extensie niet heeft geïnstalleerd, wordt de waarschuwing **Chrome-bescherming verwijderd** weergegeven wanneer u Google Chrome na een week start.

- Als u deze extensies niet heeft geïnstalleerd, wordt de melding **Google Chrome-beveiligingswaarschuwing** weergegeven wanneer u Google Chrome na een week start.
- 5 Klik op **Nu installeren** en volg de instructies op het scherm om de extensies te installeren.

---

**Opmerking:** Als u de Norton-extensie op een later tijdstip wilt activeren, klikt u op **Melding later herhalen**. Klik op **Niet meer vragen** als u wilt dat de melding niet meer wordt weergegeven.

---

## Mozilla Firefox

### De browserfuncties van Norton toevoegen in Mozilla Firefox

---

**Opmerking:** U moet de nieuwste versie van Norton 360 hebben om de webgebaseerde, zelfstandige browserextensies van Mozilla Firefox te installeren. Als u de nieuwste versie niet heeft, moet u LiveUpdate uitvoeren in uw Norton-product. We bieden de volgende extensies voor de Firefox-browser:

---

- Norton Safe Web
- Norton Safe Search
- Norton-startpagina
- Norton Password Manager

Volg de onderstaande instructies om de browserextensies voor Firefox te installeren of upgraden.

- 1 Nadat u Apparaatbeveiliging voor het eerst heeft geïnstalleerd, wordt de pagina **Browserbeveiliging** automatisch in een nieuw venster/tabblad geopend wanneer u Mozilla Firefox start.

Als u een upgrade heeft uitgevoerd voor Apparaatbeveiliging van Norton, klikt u in het waarschuwingsvenster **Browserbeveiliging** op **OK** om de extensiepagina weer te geven.

---

**Opmerking:** U kunt de pagina **Browserbeveiliging** ook openen door onder **Internetbeveiliging** op de optie **Nu instellen** te klikken.

---

- 2 Klik op de pagina **Browserbeveiliging** op de optie **Inschakelen** van **Norton Safe Web**.
- 3 In de pop-up van de extensies klikt u op **Toestaan**.

Nadat u Norton Safe Web heeft ingeschakeld, kunt u de functies van Norton Safe Search, Norton-startpagina en Norton Password Manager voor uw browser inschakelen. Gebruik de optie **Inschakelen** en volg de instructies op het scherm om deze functies te activeren.

Klik op **Alle Norton-extensies gratis toevoegen** en volg de instructies op het scherm om alle Norton-extensies in Firefox in te schakelen.

Als u deze extensies niet heeft geïnstalleerd, wordt de melding **Firefox-beveiligingswaarschuwing** weergegeven wanneer u Firefox na een week start. Als u de Norton-extensie op een later tijdstip wilt activeren, klikt u op **Melding later herhalen**. Als u wilt dat de melding niet meer wordt weergegeven, klikt u op **Niet meer vragen**. Als u de optie **Melding later herhalen** kiest, wordt na een week een beveiligingswaarschuwing in Firefox weergegeven. Klik in de melding op de optie **Nu installeren** en volg de instructies op het scherm om de extensies te installeren.

## Microsoft Edge

### De Norton-browserextensie toevoegen in Microsoft Edge

---

**Opmerking:** Norton Password Manager is een onafhankelijke extensie waarvoor geen Norton-product in de Microsoft Edge-browser hoeft te zijn geïnstalleerd. De extensie is alleen compatibel met computers waarop Windows 10-makersupdate en latere versies worden uitgevoerd.

---

- 1 Start de Microsoft Edge-browser.
- 2 Klik in de rechterbovenhoek op de knop **Meer** en selecteer **Extensies**.
- 3 Klik in het venster **Extensies** op **Extensies downloaden uit de Store**.
- 4 Typ in het venster **Store** het woord **Norton** in het zoekvakje en klik op **Norton Password Manager** in de resultaten.

- 5 Klik op **Installeren**.  
Klik op **Starten** wanneer de extensie is geïnstalleerd.
- 6 Klik in het pop-upvenster **U heeft een nieuwe extensie** op **Inschakelen**.
- 7 Als u het Norton Password Manager-pictogram wilt weergeven op de adresbalk, klikt u op de knop **Meer** in de rechterbovenhoek van de browser, en vervolgens op **Extensies**.
- 8 In het venster **Extensie** selecteert u **Norton Password Manager**.
- 9 In het venster **Norton Password Manager** zet u de schuifregelaar onder **Knop weergeven naast de adresbalk** op **Aan**.

## Browserextensies voor Microsoft Edge gebaseerd op Chromium

Microsoft heeft een nieuwe versie van Microsoft Edge uitgebracht gebaseerd op het Chromium-opensourceproject. Norton biedt de volgende browserextensies voor deze nieuwe browserversie in de Microsoft Edge Store.

- Norton Password Manager: biedt u de tools die u nodig heeft om uw wachtwoorden, creditcardgegevens en andere gevoelige online gegevens veiliger te genereren, op te slaan en te beheren
- Norton Safe Web: biedt bescherming tegen online bedreigingen terwijl u over het web surft.

De extensies zijn voor zowel Windows- als Mac-platforms beschikbaar.

### Norton-browserextensie toevoegen in Microsoft Edge

- 1 Start de Microsoft Edge-browser.
- 2 Start de [Norton Safe Web-extensie](#) vanaf de pagina Microsoft Edge Addons.

---

**Opmerking:** Klik op het instellingenpictogram > **Extensies** om te controleren of de extensie Norton Password Manager al is geïnstalleerd. Op de pagina **Extensies** verschuift u de Norton Safe Web-schuifregelaar om de extensie in te schakelen.

---

- 3 Klik op **Kopen** op de Addons-pagina voor Norton Safe Web.
- 4 Klik op **Extensie toevoegen** in de pop-up **Norton Safe Web toevoegen aan Microsoft Edge** om de extensie Norton Safe Web te installeren.

### De browserextensie Norton Password Manager toevoegen in Microsoft Edge

- 1 Start de Microsoft Edge-browser.
- 2 Start de [Norton Password Manager-extensie](#) vanaf de pagina Microsoft Edge Addons.

---

**Opmerking:** Klik op het instellingenpictogram > **Extensies** om te controleren of de extensie Norton Password Manager al is geïnstalleerd. Op de pagina **Extensies** verschuift u de Norton Password Manager-schuifregelaar om de extensie in te schakelen.

---

- 3 Klik op **Kopen** op de Addons-pagina voor Norton Password Manager.
- 4 Klik op **Extensie toevoegen** in de melding **Norton Password Manager toevoegen aan Microsoft Edge** om de extensie Norton Password Manager-extensie te installeren.

## Cloudback-up instellen

Cloudback-up werkt preventief om gegevensverlies door ransomware, malware of ernstige hardwareproblemen met uw pc te voorkomen. Uw abonnement geeft u recht op een bepaalde hoeveelheid opslagruimte in Norton Cloudback-up. De hoeveelheid gratis cloudopslag hangt af van het abonnement dat u heeft aangeschaft.

---

**Opmerking:** De functie Norton Cloudback-up is alleen beschikbaar op Windows.

---

Voordat u uw eerste back-up uitvoert, moet u Cloudback-up activeren.

---

**Opmerking:** Als u Cloudback-up wilt gebruiken, moet u de optie **Beperken van netwerkgebruik** in het venster **Firewallinstellingen** instellen op **Geen limiet**.

---

### Cloudback-up activeren

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Cloudback-up** op **Instellen**.
- 3 Klik in het venster dat verschijnt op **Back-up activeren**.
- 4 Voer het e-mailadres en wachtwoord van uw NortonLifeLock-account in en klik op **Aanmelden** wanneer u gevraagd wordt zich aan te melden.
- 5 Klik op **Gereed**.



# LifeLock Identity Theft Protection configureren

Nu LifeLock en Norton hun krachten in één bedrijf hebben gebundeld, kunnen we u nu helpen uw identiteit te beschermen.

U kunt de volgende persoonlijke gegevens aan LifeLock toevoegen voor toezicht:

- Rijbewijs
- Burgerservicenummer, geboortedatum, meisjesnaam van moeder
- 5 verzekerings-id's
- 5 adressen
- 5 telefoonnummers
- 10 bankrekeningen
- 10 creditcards\*

U kunt aanvullende informatie toevoegen voor toezicht, zoals telefoonnummers, e-mailadressen of accounts.

Het LifeLock Identity Alert System waarschuwt u wanneer uw identiteit door iemand anders wordt gebruikt. Dit kunnen bijvoorbeeld mensen zijn die proberen op uw naam een telefooncontract of een autolening af te sluiten.

---

**Opmerking:** LifeLock Identity Theft Protection biedt geen bescherming voor bedrijven. Onze technologie en service zijn ontworpen om individuen te beschermen die burgerservicenummers en andere persoonlijk identificeerbare informatie hebben die bedrijven niet hebben.

\*U kunt bekende creditcards, zoals Visa, MasterCard, American Express en Discover toevoegen. Helaas worden andere kaarten, zoals winkelkaarten of cadeaukaarten, op dit moment niet ondersteund.

Niemand kan identiteitsdiefstal of cybercriminaliteit volledig voorkomen.

LifeLock houdt geen toezicht op alle transacties bij alle bedrijven.

---

## LifeLock Identity Theft Protection configureren

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Identiteitsbescherming** op **Instellen**.
- 3 Klik op de pagina **LifeLock-ledenaanmelding** op de optie **Aanmelden met Norton**.
- 4 Voer uw accountgegevens in en meld u aan.
- 5 Volg de instructies op het scherm.

### LifeLock voor Norton 360 installeren op Android

- 1 Start de **Play Store** -app op uw Android-apparaat en zoek **LifeLock Identity Theft Protection**.
- 2 Zodra u de app-pagina in de Play Store heeft gevonden, tikt u op **Installeren** en vervolgens op **Accepteren**.
- 3 Open de app nadat deze is geïnstalleerd en meld u aan met uw accountgegevens.

### LifeLock voor Norton 360 installeren op iOS

- 1 Open de **App Store** -app op uw iOS-apparaat en zoek **LifeLock Identity Theft Protection**.
- 2 Zodra u de app-pagina in de App Store heeft gevonden, tikt u op **Download** en vervolgens op **Installeer**.
- 3 Open de app nadat deze is geïnstalleerd en meld u aan met uw accountgegevens.

## Toezicht op het dark web wordt mogelijk gemaakt door LifeLock\*\*

### Wat is toezicht op het dark web?

We houden toezicht op het gebruik van uw persoonlijke gegevens\*\* op moeilijk te vinden sites en forums op het dark web. Wanneer we uw informatie op het dark web vinden, stellen we u hiervan op de hoogte.

### Waarom is dit belangrijk?

Identiteitsdieven kunnen uw persoonlijke informatie verkopen op moeilijk te vinden sites en forums op het Dark Web.

### Wat moet ik doen?

Staat er informatie over uzelf in het bericht, raadpleeg dan de onderstaande stappen.

- **Betaalpas/creditcard gecompromitteerd** : als de rekening is gesloten, hoeft u niets te doen. Als het account actief is, neemt u contact op met uw creditcard-/betaalkaartbedrijf en vraagt u een nieuwe kaart aan. Houd uw afschriften goed in de gaten.
- **E-mail gecompromitteerd** : wijzig uw huidige e-mailwachtwoord. Heeft u accounts met hetzelfde wachtwoord, wijzig die dan ook. Houden de problemen aan, dan is het misschien verstandig een nieuw e-mailaccount te openen. Het helpt de beveiliging van uw accounts wanneer u uw wachtwoorden elke 30 dagen wijzigt.
- **Burgerservicenummer gecompromitteerd** : het is raadzaam fraudemeldingen in te stellen bij een van de drie kredietbureaus om uw identiteit verder te beschermen.
- **Naam/adres/telefoonnummer gecompromitteerd** : gelukkig zijn in dit geval geen mogelijk gevoeligere gegevens zoals uw burgerservicenummer gedeeld. Omdat sommige van uw

persoonlijke gegevens echter openbaar zijn gemaakt, raden we u aan om uw kredietrapport nauwlettend in de gaten te houden.

We blijven in de gaten houden of uw persoonlijke gegevens\*\* op het dark web staan. Als we uw gegevens vinden, sturen we een nieuwe e-mail.

---

**Opmerking:** Niemand kan identiteitsdiefstal volledig voorkomen.

Bij Toezicht op het dark web in Norton 360-abonnementen wordt alleen toezicht gehouden op uw e-mailadres. Meld u aan bij de portal om te controleren of u extra informatie kunt toevoegen voor toezicht.

---

## Uw Veilige VPN instellen

Openbare wifi is overal: vliegvelden, koffiezaken, winkelcentra en hotels. Gratis 'hotspots' zijn zo wijdverspreid en handig dat mensen er vaak verbinding mee maken zonder erover na te denken. Maar e-mails lezen, uw banksaldo checken en andere activiteiten waarvoor u zich moet aanmelden, zijn riskant wanneer u openbare wifi gebruikt. Als u openbare wifi gebruikt, kunnen anderen uw online activiteiten volgen. Cybercriminelen kunnen persoonlijke gegevens stelen zoals uw gebruikersnamen, wachtwoorden, locatiegegevens, chats, e-mails of rekeningnummers.

Met Secure VPN kunt u de verbinding beveiligen wanneer u een openbare draadloze verbinding gebruikt. Er wordt een VPN (Virtual Private Network) gemaakt dat uw gevoelige gegevens versleutelt.

Secure VPN beschermt als volgt de gegevens die u via openbare wifi verstuurt en ontvangt:

- Uw verbinding wordt beschermd met versleuteling van bankkwaliteit zodat u openbare wifihotspots veilig kunt gebruiken.
- U kunt anoniem internetten zodat uw online privacy geen gevaar loopt.
- U kunt overal werken met uw favoriete apps en inhoud, alsof u thuis bent.
- Uw gegevens worden versleuteld op een privénetwerk waar uw activiteiten niet worden gevolgd of opgeslagen.
- U kunt rekenen op de uitstekende klantondersteuning van Norton LifeLock, een leider in online consumentenbeveiliging.

---

**Opmerking:** De functie Secure VPN is niet met alle abonnementen beschikbaar.

---

Volg de onderstaande instructies om Secure VPN te configureren.

### Secure VPN configureren

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Veilige VPN** op **Instellen**.
- 3 Klik op de webpagina die verschijnt op **Aanmelden**.
- 4 Voer uw accountgegevens in en meld u aan.
- 5 Als u wordt gevraagd om de toepassing te downloaden, klikt u op **Downloaden**.
- 6 Volg de instructies op het scherm.

Doe hier mee aan de discussie met andere desktopgebruikers: [Norton Community](#).

## Ouderlijk toezicht instellen

U kunt Ouderlijk toezicht nu instellen zodat uw kinderen veiliger kunnen internetten. Het is gemakkelijk en er zijn maar drie stappen.

Ouderlijk toezicht biedt alles wat u nodig heeft om de online activiteiten van uw gezin te beschermen tegen gevaren op het internet en ongeschikte content. Het helpt u er zelfs voor te zorgen dat uw kinderen geen vertrouwelijke gegevens doorgeven via internet.

### Aanmelden bij uw NortonLifeLock-account

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** naast **Ouderlijk toezicht** op **Instellen**.
- 3 Als u wordt gevraagd om u aan te melden, voert u uw accountgegevens in en meldt u zich aan.
- 4 Klik op de pagina die verschijnt op het tabblad **Family**.
- 5 Lees de **Servicevoorwaarden** en klik op **Akkoord en doorgaan** om uw gezin te configureren.
- 6 Volg de instructies op het scherm.

### Een kind toevoegen aan uw account

Op ieder kind dat u toevoegt, past Ouderlijk toezicht de vooraf gedefinieerde huisregels toe die zijn gebaseerd op de leeftijd van het kind. U kunt de huisregels op elk moment aanpassen zodat deze beter aansluiten op de volwassenheid van ieder kind.

---

**Opmerking:** U kunt tot 15 kinderen aan uw account toevoegen. U kunt een kind op elk moment aan uw Norton Family-account toevoegen of hieruit verwijderen.

---

- 1 Typ de naam van uw kind in het vak **Naam van kind**.

---

**Opmerking:** De naam mag geen speciale tekens bevatten zoals &, # of \$.

---

- 2 Selecteer het geboortjaar van uw kind.  
Huisregels worden op basis van de leeftijd van het kind toegepast.
- 3 U kunt **een avatar selecteren** of **een foto uploaden** om een profielafbeelding voor uw kind in te stellen.

---

**Opmerking:** Nadat u de configuratie voor uw eerste kind heeft voltooid, kunt u meer kinderen toevoegen aan uw account.

---

- 4 Klik op **Volgende**.

## Norton Family installeren op het apparaat van uw kind

Installeer Norton Family op elk apparaat dat uw kind gebruikt. Als u niet op het apparaat van uw kind zit, klikt u op **Nee** om een downloadlink te verzenden in een e-mail. Open deze e-mail op het apparaat waarop u Norton Family wilt installeren.

### Norton Family installeren op Windows

- 1 Klik onder **Gebruikt uw kind dit apparaat?** op **Ja** en vervolgens op **Volgende**.
- 2 Klik op het gedownloadte installatiebestand of voer dit uit.
- 3 Norton-downloadbeheer installeert Norton Family automatisch op het apparaat.
- 4 Lees de licentieovereenkomst en klik op **Akkoord en installeren**.  
Het apparaat wordt automatisch aan uw account gekoppeld.
- 5 Klik op **Doorgaan**.
- 6 Klik in het venster Accounts bewerken op **Bewerken** naast het kind aan wie u dit apparaat wilt toewijzen.
- 7 Klik op **meldt zich aan als** en kies het account dat het kind gebruikt om zich op dit apparaat aan te melden. Als uw kind meerdere gebruikersaccounts heeft, moet u het kind voor al die gebruikersaccounts selecteren.
- 8 Klik op **Opslaan > OK**.

### De Norton Family-app installeren op Android

- 1 Tik in het venster **Norton Family installeren** op **Ja** en vervolgens op **Doorgaan**.
- 2 Tik op **Norton Family-app downloaden**.

- 3 Voltooi de handeling met **Play Store** als u hierom wordt gevraagd.
- 4 Tik op **Installeren** en volg de instructies op het scherm.
- 5 Open de Norton Family-app voor ouderlijk toezicht.
- 6 Lees de **Norton-licentieovereenkomst** en tik op **Accepteren en doorgaan Aan de slag**.
- 7 Klik op **Aanmelden** en voer uw accountgegevens in.
- 8 Tik op **Kind** om de modus Kind te activeren en tik vervolgens op **Doorgaan**.  
In de modus Kind kunt u een kind toevoegen en huisregels toewijzen aan dit apparaat.
- 9 Tik op **Een kind toevoegen** en voer in het venster **PROFIEL** de gegevens van uw kind in om een kind toe te voegen.  
Kies een avatar voor het profiel van uw kind door op de avatarafbeelding te tikken. U kunt een afbeelding uit uw galerie kiezen of direct een foto nemen voor het profiel van uw kind.
- 10 Tik op **Doorgaan** en vervolgens op **Opslaan**.  
Norton Family heeft standaardhuisregels ingesteld op basis van het geboortjaar van uw kind. U kunt op **Huisregels** tikken om de regels te zien die aan uw kind zijn toegewezen.
- 11 Selecteer het kind aan wie u dit apparaat wilt toewijzen, geef een handige naam op om dit apparaat te identificeren, en tik vervolgens op **Gereed**.
- 12 Als u daarom gevraagd wordt, schakelt u de opties **App-gebruik** en **Toegankelijkheid** in.
- 13 In de melding die wordt weergegeven, tikt u op **Activeren** om Norton Family als de apparaatbeheerder in te stellen.

#### De Norton Family-app installeren op iOS

- 1 Tik in het venster **Norton Family installeren** op **Ja** en vervolgens op **Doorgaan**.
- 2 Tik op **Norton Family-app downloaden**.
- 3 Tik om **Norton Family** te installeren.
- 4 Tik op **Openen**.
- 5 Tik op **OK** om Norton Family toe te staan meldingen te sturen.
- 6 Lees de **Norton-licentieovereenkomst** en het **Privacybeleid**. Tik vervolgens op **Accepteren en doorgaan**.
- 7 Meld u aan met uw accountgegevens.

- 8 Voer in het venster **Kind toevoegen** de gegevens van uw kind in. Tik vervolgens op **Toevoegen**.

Tik op **Een nieuw kind toevoegen**, voer in het venster **Kind toevoegen** de gegevens van uw kind in en tik op **Toevoegen** om nog een kind toe te voegen.

Kies een avatar voor het profiel van uw kind door op de avataraafbeelding te tikken. U kunt een afbeelding uit uw galerie kiezen of direct een foto nemen voor het profiel van uw kind.
- 9 Selecteer het kind aan wie u dit apparaat wilt toewijzen. Geef ook een naam op waarmee u dit apparaat gemakkelijk kunt identificeren.
- 10 Tik op **Toewijzen**.
- 11 Tik op **Installeren** en volg de instructies op het scherm om een profiel te installeren.

Profielinstallatie is vereist om Direct vergrendelen en andere functies in te schakelen op het apparaat van uw kind.
- 12 Volg de instructies op het scherm om beperkingen in te stellen.

## Norton Family installeren op het apparaat van een ouder

Nadat u de configuratie heeft voltooid, downloadt en installeert u de volgende mobiele app op uw apparaat:

- Android-apparaat: installeer de app **Norton Family voor ouderlijk toezicht**.
- iOS-apparaat: installeer de app **Norton Family voor ouders**

### De Norton Family-app voor ouderlijk toezicht op Android downloaden en installeren

- 1 Open de Play Store-app en zoek naar **Norton Family voor ouderlijk toezicht**.
- 2 Selecteer de **Norton Family-app voor ouderlijk toezicht** en tik vervolgens op **Installeren**.
- 3 Open de app nadat deze is geïnstalleerd.
- 4 Lees de **Norton-licentieovereenkomst** en andere beleidsdocumenten. Tik vervolgens op **Doorgaan**.
- 5 Meld u aan met uw accountgegevens.
- 6 Tik op **Apparaat van ouder**. Als u het apparaat met uw kind deelt, moet u naar de modus **Kind** overschakelen voordat u het apparaat aan uw kind geeft.

### De Norton Family-app voor ouders installeren op iOS

- 1 Open de App Store-app en zoek naar **Norton Family voor ouders**.
- 2 Selecteer **Norton Family voor ouders** en tik vervolgens op **Installeer**.
- 3 Open de app nadat deze is geïnstalleerd.

- 4 Lees de **Norton-licentieovereenkomst** en andere beleidsdocumenten. Tik vervolgens op **Doorgaan**.
- 5 Meld u aan met uw accountgegevens.

## Bespreek alles met uw gezin

Communicatie is de sleutel tot de online veiligheid van uw gezin. Hiertoe kunt u een gesprek voeren met uw kind waarin u het belang van verantwoordelijk internetgebruik uitlegt.

# Bescherm uw bankgegevens met Norton Safe Web

Bescherming tijdens het bankieren in Norton Safe Web biedt verhoogde beveiliging wanneer u transacties uitvoert via bankwebsites. Wanneer u een bankwebsite bezoekt met de browsers Google Chrome, Mozilla Firefox of Microsoft Edge, ontvangt u een melding om de Norton Safe Web-extensie te installeren of in te schakelen. Klik op **Installeren** of **Inschakelen** in de melding en volg de instructies op het scherm om de Norton Safe Web-extensie te installeren of in te schakelen.

U kunt de waarschuwing melding voor bescherming tijdens het bankieren uitschakelen door in de melding te klikken op **Niet meer weergeven** of door naar het venster **Instellingen** te gaan.

## Meldingen voor bescherming tijdens bankieren in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Onder het tabblad **Inbraak- en browserbeveiliging**, in de rij **Meldingen voor bescherming tijdens bankieren**, zet u de **Aan / Uit**-schakelaar op **Uit** of **Aan**.
- 5 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.



# Uw apparaatbeveiliging beheren

Dit hoofdstuk bevat de volgende onderwerpen:

- [Wat te doen als uw apparaat gevaar loopt](#)
- [Norton gebruiken om de prestaties van de computer te optimaliseren en te verbeteren](#)
- [Norton-scans uitvoeren om uw pc op bedreigingen te controleren](#)
- [Bescherm uw apparaat tegen misbruik, hackers en zero-day aanvallen.](#)
- [Norton instellen om toezicht te houden op toepassingen en schadelijke websites te blokkeren op uw computer](#)
- [Aan de slag met Norton Cloudback-up](#)
- [De instellingen van uw Norton-product aanpassen](#)
- [Uw computer optimaliseren voor gamen met Game Optimizer](#)

## Wat te doen als uw apparaat gevaar loopt

In het hoofdvenster van Norton geeft de kleur van de tegels Beveiliging, Internetbeveiliging, Back-up en Prestaties de status van elke categorie als volgt aan:

- **Groen** : u bent beschermd.
- **Oranje** : uw computer vereist aandacht.
- **Rood** : uw computer loopt gevaar.

---

**Opmerking:** De back-upcategorie is alleen beschikbaar bij de abonnementen Deluxe, Premium en Norton 360.

---

Norton verhelpt automatisch alle problemen die uw beveiliging of de systeemprestaties verminderen en geeft de status 'Beveiligd' weer in het hoofdvenster. Norton geeft kwesties die uw aandacht vereisen weer als **Kwetsbaar** of **Aandacht vereist**.

#### Reageren op de aanduidingen Aandacht vereist of Kwetsbaar

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik op de rode of oranje tegel die **Kwetsbaar** of **Aandacht vereist** aangeeft in het hoofdvenster van Norton.

- 3 Klik op **Nu verhelpen** en volg de aanwijzingen op het scherm.

Als u nog steeds problemen ondervindt, klikt u op **Help > Ondersteuning** om het diagnostische hulpprogramma uit te voeren.

U kunt ook de [Norton Rescue Tools](#) gebruiken als u denkt dat uw computer ernstig is geïnfecteerd.

## LiveUpdate uitvoeren

NortonLifeLock raadt aan om LiveUpdate regelmatig uit te voeren in de volgende gevallen:

- Als u de optie **Automatische LiveUpdate** heeft uitgeschakeld
- Als uw computer al geruime tijd niet met internet is verbonden

---

**Opmerking:** Voor LiveUpdate heeft u een geldig abonnement en een internetverbinding nodig.

---

#### LiveUpdate handmatig uitvoeren

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** en klik vervolgens op **LiveUpdate** in het hoofdvenster van het Norton-product.

- 3 Klik op **OK** in het venster **Norton LiveUpdate** wanneer de LiveUpdate is voltooid.

## Beveiligingsrisico voor apparaten die Norton detecteert weergeven of verhelpen

Wanneer Norton een beveiligingsrisico detecteert, wordt deze automatisch verwijderd, tenzij uw invoer vereist is om te bepalen hoe u de dreiging wilt oplossen. Als u informatie moet invoeren, geeft Norton de waarschuwing **Bedreigingen gedetecteerd of Beveiligingsrisico** weer met suggesties voor wat u kunt doen.

### Risico's bekijken die automatisch zijn opgelost tijdens een scan

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 In het venster **Beveiligingsgeschiedenis** selecteert u **Opgeloste beveiligingsrisico's** in de vervolgkeuzelijst **Weergeven**.
- 4 Selecteer een risico in de lijst en bekijk vervolgens in het deelvenster **Details** de actie die is ondernomen.

### Gedetecteerde beveiligingsrisico's verhelpen die tijdens een scan zijn gedetecteerd

In sommige gevallen wordt een risico niet automatisch opgelost door Norton, maar ziet u een aanbevolen actie die u kunt uitvoeren om het risico te verhelpen.

### Gedetecteerde beveiligingsrisico's verhelpen die tijdens een scan zijn gedetecteerd

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 In het venster **Beveiligingsgeschiedenis** selecteert u **Onopgeloste beveiligingsrisico's** in de vervolgkeuzelijst **Weergeven**.
- 4 Selecteer een risico in de lijst als er onopgeloste risico's worden weergegeven.
- 5 Volg de **Aanbevolen actie** in het deelvenster **Details**.

---

**Opmerking:** In sommige gevallen moet u uw computer opnieuw starten, nadat Norton een beveiligingsrisico heeft verwijderd. Als Norton u vraagt de computer opnieuw op te starten, slaat u eventuele geopende bestanden op en start u de computer opnieuw op.

---

---

**Opmerking:** Voer Norton Power Eraser als u het vermoeden heeft dat uw systeem is geïnfecteerd. Norton Power Eraser is een krachtig verwijderingsprogramma voor malware waarmee u de beveiligingsrisico's kunt elimineren die moeilijk te verwijderen zijn. Voor meer informatie: Zie "[Norton-scans uitvoeren om uw pc op bedreigingen te controleren](#)" op pagina 34.

---

## Risico's of bedreigingen in quarantaine verwerken

Items die in quarantaine worden geplaatst worden van de rest van uw computer geïsoleerd, zodat ze zich niet kunnen verspreiden en de computer niet kunnen infecteren. Als u van een item vermoedt dat het is geïnfecteerd, maar niet door Norton als een risico is geïdentificeerd, kunt u het handmatig in quarantaine plaatsen. U kunt een item uit de quarantaine terugzetten als u denkt dat het een laag risico heeft. Norton herstelt het item dat u terugzet niet. Norton kan de teruggezette items echter wel desinfecteren tijdens de daaropvolgende scans.

### Een item uit de quarantaine terugzetten

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de vervolgkeuzelijst **Weergeven** de categorie **Quarantaine**.
- 4 Selecteer een item dat u wilt beheren.
- 5 Klik in het deelvenster **Details** op **Opties**.

Gebruik de link **Meer opties** om meer details over het item te bekijken voordat u een actie voor het item selecteert. Via de link wordt het venster **Bestandsinformatie** geopend dat meer informatie over het risico bevat.

- 6 Kies een van de volgende opties in het venster **Bedreiging gedetecteerd** :
  - **Herstellen** : hiermee worden de bestanden teruggezet naar de oorspronkelijke locatie op uw computer. Deze optie is alleen beschikbaar voor items die handmatig in quarantaine zijn geplaatst.
  - **Dit bestand herstellen en uitsluiten** : hiermee wordt het item zonder reparatie teruggeplaatst op de oorspronkelijke locatie en wordt uitgesloten van detectie in latere scans. Deze optie is beschikbaar voor gedetecteerde bedreigingen die wel en geen virussen zijn.

- **Uit geschiedenis verwijderen** : hiermee kunt u het geselecteerde item uit het logbestand van de **Beveiligingsgeschiedenis** verwijderen.
- 7 Als u ervoor kiest het terug te zetten, klikt u in het venster **Uit quarantaine herstellen** op **Ja**.
  - 8 Selecteer in het dialoogvenster **Zoeken naar map** de map of het station waarnaar u het bestand wilt herstellen, en klik dan op **OK**.

## Een bestand herstellen dat onterecht als beveiligingsrisico is aangemerkt

Beveiligingsrisico's worden standaard door Norton van uw computer verwijderd en in quarantaine geplaatst. Als een bestand onterecht is verwijderd, kunt u het vanuit de quarantaine terugplaatsen op de oorspronkelijke locatie en het uitsluiten van latere scans.

### Een bestand uit quarantaine herstellen

---

**Opmerking:** Sluit een programma alleen uit van Norton-productscans als u zeker weet dat het programma veilig is. Als een programma bijvoorbeeld afhankelijk is van een ander programma dat een beveiligingsrisico vormt, kunt u besluiten dat programma toch op uw computer te laten staan.

---

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het Norton-hoofdvenster op **Beveiliging**. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** onder het vervolgkeuzemenu **Weergeven** de optie **Quarantaine**.
- 4 Selecteer het bestand dat u wilt herstellen.
- 5 Klik in het deelvenster **Details** op **Opties**.
- 6 Klik op **Dit bestand herstellen en uitsluiten** in het venster **Bedreiging gedetecteerd**.
- 7 In het venster **Uit quarantaine herstellen** klikt u op **Ja**.
- 8 Selecteer in het dialoogvenster **Zoeken naar map** de map of het station waarnaar u het bestand wilt herstellen, en klik dan op **OK**.

## Een item naar Norton verzenden voor analyse

Wanneer u bestanden opgeeft waarvan u denkt dat deze een beveiligingsrisico vormen, draagt u bij aan de doeltreffendheid van uw Norton-product. Norton Security Response analyseert het bestand, bepaalt of het een risico vormt en voegt het toe aan latere beveiligingsdefinities.

---

**Opmerking:** Persoonlijke identificatiegegevens worden nooit in inzendingen opgenomen.

---

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de vervolgkeuzelijst **Weergeven** de categorie **Quarantaine**.
- 4 Selecteer een item dat u wilt beheren.
- 5 Klik in het deelvenster **Details** op **Opties**.  
Gebruik de link **Meer opties** om meer details over het item te bekijken voordat u een actie voor het item selecteert. Via de link wordt het venster **Bestandsinformatie** geopend dat meer informatie over het risico bevat.
- 6 Klik in het venster **Bedreiging gedetecteerd** op **Verzenden naar NortonLifeLock**.
- 7 Klik op **OK** in het dialoogvenster dat verschijnt.

#### Een item handmatig in quarantaine plaatsen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de vervolgkeuzelijst **Weergeven** de categorie **Quarantaine**.
- 4 Klik op **In quarantaine plaatsen**.
- 5 Voeg in het venster **Handmatige quarantaine** het bestand toe dat u in quarantaine wilt plaatsen en voer een beschrijving in ter referentie.

---

**Opmerking:** Als u een bestand dat aan actieve processen is gekoppeld in quarantaine plaatst, worden de processen beëindigd. Sluit dus alle geopende bestanden en actieve processen voordat u een bestand in quarantaine plaatst.

---

## Norton gebruiken om de prestaties van de computer te optimaliseren en te verbeteren

We weten hoe frustrerend het is wanneer uw computer langzamer wordt en het een eeuwigheid duurt om eenvoudige taken uit te voeren. Sommige gebruikers zijn van mening dat de prestaties van hun computer verslechteren na installatie van Norton. Maar feit is dat Norton gestroomlijnd is om een bescherming van wereldklasse te bieden zonder in te boeten op prestaties.

U kunt uw computer ook sneller maken met de tools van Norton voor prestatiebeheer en optimalisatie zodat u dagelijkse taken sneller kunt uitvoeren.

## De opstarttijd van computer versnellen

Vele toepassingen zijn zo ingesteld dat ze worden gestart wanneer u uw computer start. Er worden programma's gestart die u zelden of nooit gebruikt, of waarvan u niet eens wist dat u ze had. En hoe meer programma's worden gestart, hoe langer alles duurt. Met **Opstartbeheer van Norton** kunt u opstartprogramma's uitschakelen of vertragen zodat u sneller aan de slag kunt gaan.

### Opstartitems uitschakelen of vertragen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het Norton-hoofdvenster. Klik vervolgens op **Opstartbeheer**.
- 3 Doe het volgende in het venster **Opstartbeheer** :
  - Hef in de kolom **Aan/Uit** de selectie op van de programma's die u niet gebruikt zodat deze niet worden gestart wanneer u uw computer start.
  - Selecteer in de kolom **Opstartvertraging** de programma's die pas moeten worden geladen nadat het opstarten is voltooid.
- 4 Klik op **Toepassen** en vervolgens op **Sluiten**.

## De laadtijd voor programma's en bestanden verbeteren

Met het hulpprogramma **Schijf optimaliseren** worden bestandsfragmenten die mettertijd over uw computer verspreid zijn geraakt, weer bij elkaar gezet. Het verbetert de prestaties van de computer, zodat u efficiënter werkt.

### Schijf optimaliseren uitvoeren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Schijf optimaliseren**.
- 3 Klik op **Sluiten** wanneer het proces is voltooid.

## Tijdelijke bestanden en mappen verwijderen die de computer vertragen

Telkens wanneer u internet of bestanden downloadt, worden tijdelijke bestanden op uw computer opgeslagen. U hoeft ze niet te bewaren. Toch bouwt u in de loop van de tijd een hele verzameling op wat de prestaties van uw computer kan aantasten. Met het hulpprogramma Bestandsopruiming kunt u onnodige bestanden verwijderen om uw computer sneller te maken.

### Tijdelijke bestanden en mappen verwijderen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Bestandsopruiming**.
- 3 Klik op **Sluiten** wanneer het proces is voltooid.

### Het opstartvolume optimaliseren

Wanneer u het opstartvolume optimaliseert, worden bestandsfragmenten in aansluitende of aangrenzende clusters herschikt, waardoor de bruikbare vrije ruimte wordt gemaximaliseerd. Wanneer de stationskop van de vaste schijf alle bestandsgegevens op één locatie vindt, kan het bestand sneller in het geheugen worden gelezen.

#### Het opstartvolume optimaliseren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Grafieken**.
- 3 Klik boven aan de beveiligingsstatusgrafiek in het venster **Grafieken** op **Optimaliseren**.

### Prestaties verbeteren wanneer ik game of films kijk

Is het u wel eens gebeurd dat uw beveiligingssoftware midden in een game of film werd gestart zodat het scherm op het meest ongelegen moment bevroor? U kunt instellen dat **Schermvullende detectie** bepaalt wanneer er een programma actief is dat niet mag worden onderbroken. De achtergrondtaken die u beschermen, gaan dan pas van start wanneer u klaar bent met de app.

#### Zorg dat Schermvullende detectie is ingeschakeld.

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Zet onder **Instellingen voor Stille modus** in de rij **Schermvullende detectie** de schakelaar op **Aan**.
- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

### Onderbrekingen stoppen wanneer ik mijn favoriete apps gebruik

Als u van mening bent dat Norton uw favoriete programma's langzamer maakt, kunt u de **Stille modus** instellen zodat Norton niet wordt uitgevoerd wanneer u de programma's gebruikt. De



achtergrondtaken die u beschermen, gaan dan pas van start wanneer u klaar bent met de programma's.

### Mijn favoriete programma's in Stille modus uitvoeren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Klik op **Configureren** in de rij **Gebruikergedefinieerde programma's** onder **Instellingen voor Stille modus**.
- 5 Klik in het venster **Programma's met stille modus** op **Toevoegen**.
- 6 Ga naar uw programma in het dialoogvenster **Programma toevoegen**.
- 7 Selecteer het bestand en klik op **Openen**. Klik vervolgens op **OK**.

### Programma's weergeven die veel systeembronnen gebruiken en mijn computer trager maken

Met Norton houdt u toezicht op uw computer en kunt u instellen dat een waarschuwing verschijnt wanneer een programma of proces een ongewone hoeveelheid bronnen gebruikt. U kunt deze programma's afsluiten om prestaties te verbeteren wanneer u ze niet gebruikt.

### Processen identificeren die veel systeembronnen gebruiken

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Prestaties** in het hoofdvenster van Norton. Klik vervolgens op **Grafieken**.
- 3 Klik in het venster **Grafieken** in het linkerdeelvenster op **Gebruik**.
- 4 Voer een van de volgende handelingen uit:
  - Klik op de tab **CPU** als u de CPU-grafiek wilt weergeven.

- Klik op de tab **Geheugen** als u de geheugengrafiek wilt weergeven.
- 5 Klik op een willekeurige plaats op de grafiek om een lijst met resource-belastende processen weer te geven.
- Klik op de naam van een proces als u aanvullende informatie over dat proces wilt zien in het venster **Bestandsinformatie**.

## Norton-scans uitvoeren om uw pc op bedreigingen te controleren

Virusdefinities worden automatisch bijgewerkt en uw pc wordt regelmatig op een reeks bedreigingen gescand. Als u offline bent geweest of vermoedt dat u een virus heeft, kunt u handmatig het volgende uitvoeren:

- **Snelle scan** om gebieden van uw computer te analyseren die het meest kwetsbaar zijn voor bedreigingen.
- **Volledige systeemsan** om uw hele systeem te analyseren, inclusief minder kwetsbare toepassingen, bestanden en actieve processen die tijdens een snelle scan niet worden gecontroleerd.
- **Aangepaste scan** om afzonderlijke bestanden, mappen of stations te analyseren als u vermoedt dat ze gevaar lopen.

---

**Opmerking:** Nadat u Norton heeft geïnstalleerd, kan de eerste scan een uur of langer duren om uw volledige systeem te analyseren.

---

### Een Snelle scan, Volledige systeemsan of Handmatige scan uitvoeren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 In het venster **Scans** naast **Scans en taken** selecteert u een van de volgende:
  - **Snelle scan > Start**
  - **Volledige systeemsan > Start**

- **Aangepaste scan > Start.** Klik vervolgens op **Uitvoeren** naast **Scan van station**, **Scan van map** of **Scan van bestand** om naar de onderdelen te gaan die u wilt scannen.

#### 4 Klik in het venster **Resultatenoverzicht** op **Voltooien**.

Als items aandacht vereisen, kunt u de risico's beoordelen in het venster **Bedreigingen gedetecteerd**.

## Volledige systeemsan

Met een volledige systeemsan wordt een uitvoerige scan uitgevoerd van de computer om virussen en andere beveiligingsbedreigingen te verwijderen. Hierbij worden alle opstartrecords, bestanden en actieve processen gecontroleerd waartoe de gebruiker toegang heeft. Hiermee wordt uw computer grondig en langduriger onderzocht.

---

**Opmerking:** Wanneer een volledige systeemsan wordt uitgevoerd door iemand met beheerdersrechten, worden er meer bestanden gescand dan wanneer de scan zonder beheerdersrechten wordt uitgevoerd.

---

### Een volledige systeemsan uitvoeren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Volledige systeemsan**.
- 4 Klik op **Start**.

## Aangepaste scan

U wilt misschien zo nu en dan een bepaald bestand, verwisselbare stations, een vaste schijf, of alle mappen of bestanden op uw computer scannen. Wanneer u bijvoorbeeld met verwisselbare media werkt en vermoedt dat een virus aanwezig is, kunt u die specifieke schijf scannen. Heeft u in een e-mailbericht een gecomprimeerd bestand ontvangen en vermoedt u dat het een virus bevat, dan kunt u dat specifieke element scannen.

### Afzonderlijke elementen scannen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**.
- 4 Klik op **Start**.

- 5 In het venster **Scans** voert u een van de volgende handelingen uit:
  - Als u specifieke stations wilt scannen, klikt u op **Uitvoeren** naast **Scan van station**, vervolgens selecteert u de stations die u wilt scannen en tot slot klikt u op **Scannen**.
  - Als u specifieke mappen wilt scannen, klikt u op **Uitvoeren** naast **Scan van map**, vervolgens selecteert u de mappen die u wilt scannen en tot slot klikt u op **Scannen**.
  - Als u specifieke bestanden wilt scannen, klikt u op **Uitvoeren** naast **Scan van bestand**, vervolgens selecteert u de bestanden die u wilt scannen en tot slot klikt u op **Toevoegen**. U kunt ook de **Ctrl** -toets ingedrukt houden om meerdere bestanden te selecteren die u wilt scannen.
- 6 Klik in het venster **Resultatenoverzicht** op **Voltooien**.  
 Als items aandacht vereisen, kunt u deze beoordelen en de aanbevolen actie ondernemen.

## Norton Power Eraser-scan

Norton Power Eraser is een krachtig verwijderingsprogramma voor malware waarmee u beveiligingsrisico's kunt opruimen die moeilijk te verwijderen zijn. Norton Power Eraser maakt gebruik van agressievere technieken dan het normale scanproces. Daardoor bestaat er soms het risico dat Norton Power Eraser een betrouwbaar programma voor verwijdering markeert. Controleer scanresultaten zorgvuldig voordat u bestanden met Norton Power Eraser verwijdert.

### Norton Power Eraser downloaden en een scan uitvoeren (op Windows 10/8/7)

- 1 Download [Norton Power Eraser](#).
- 2 Druk op de toetsen **Ctrl + J** om het venster **Downloads** in uw browser te openen en dubbelklik op het bestand **NPE.exe**.  
 Wanneer het venster Gebruikersaccountbeheer wordt weergegeven, klikt u op **Ja** of **Doorgaan**.
- 3 Lees de licentieovereenkomst en klik vervolgens op **Ik ga akkoord**.  
 Als u de licentieovereenkomst al heeft geaccepteerd, wordt u niet opnieuw gevraagd dit te doen.  
 Norton Power Eraser controleert of de nieuwe versie beschikbaar is en downloadt deze automatisch.
- 4 Selecteer in het venster Norton Power Eraser de optie **Volledige systeemscan** en klik op **Nu uitvoeren**.
- 5 Als u de rootkit-scan wilt opnemen, klikt u op **Instellingen** en schakelt u onder **Scan-en logboekinstellingen** de optie **Rootkit-scan opnemen (computer moet opnieuw worden opgestart)** en klik op **Toepassen**.
- 6 Wanneer u wordt gevraagd de computer opnieuw te starten, klikt u op **Opnieuw opstarten**.  
 Wacht tot de scan is voltooid. Volg de instructies op het scherm.

### Norton Power Eraser downloaden en een scan uitvoeren (op Windows XP/Vista)

- 1 Download [Norton Power Eraser](#).
- 2 Druk op de toetsen **Ctrl + J** om het venster **Downloads** in uw browser te openen en dubbelklik op het bestand **NPE.exe**.  
Wanneer het venster Gebruikersaccountbeheer wordt weergegeven, klikt u op **Ja** of **Doorgaan**.
- 3 Lees de licentieovereenkomst en klik op **Accepteren**.  
Norton Power Eraser controleert of de nieuwe versie beschikbaar is en als dit zo is, wordt u gevraagd deze te downloaden.
- 4 Klik in het venster **Norton Power Eraser** op het pictogram **Scannen op risico's**.
- 5 Norton Power Eraser voert standaard een rootkitscan uit waarna het systeem opnieuw moet worden opgestart. Wanneer u wordt gevraagd de computer opnieuw te starten, klikt u op **Opnieuw opstarten**.  
Als u geen rootkit-scan wilt opnemen, gaat u naar **Instellingen** en schakelt u de optie **Rootkit-scan opnemen (computer moet opnieuw worden opgestart)** uit.
- 6 Wacht tot de scan is voltooid. Volg de instructies op het scherm.

## Uw eigen aangepaste Norton-scans maken

Hoewel de standaard automatische scaninstellingen van Norton voor de meeste gebruikers goed werken, is het mogelijk dat sommige gebruikers opties willen aanpassen om specifieke schijven, mappen of bestanden volgens een door hen gekozen schema te scannen.

### Een aangepaste scan maken

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**. Klik vervolgens op **Start**.
- 4 Klik in het venster **Scans** op **Scan maken**.
- 5 Voer in het venster **Nieuwe scan** naast **Scannaam** een naam in voor uw aangepaste scan en geef de instellingen als volgt op:
  - Klik op het tabblad **Scanitems** op **Stations toevoegen**, **Mappen toevoegen** of **Bestanden toevoegen** om naar de onderdelen te gaan die u in de scan wilt opnemen.
  - Selecteer op het tabblad **Scan plannen** onder **Wanneer moet de scan worden uitgevoerd?** een interval en selecteer vervolgens de timingopties.

Selecteer een optie onder **De scan uitvoeren**. Voor de meeste gebruikers is het het beste om alle vakjes aangevinkt te houden. Dit zorgt ervoor dat scans alleen worden uitgevoerd wanneer u uw computer niet gebruikt of wanneer u geen batterijvoeding gebruikt, en het voorkomt dat uw computer tijdens een scan naar de slaapstand overschakelt.

- Verplaatst op het tabblad **Scanopties** de schakelaars om het gedrag aan te passen voor gecomprimeerde bestanden of bedreigingen met een laag risico tijdens de scan.

6 Klik op **Opslaan**.

## Een aangepaste scan van Norton bewerken of verwijderen

U kunt een aangepaste scan die u heeft gemaakt, bewerken om de naam te wijzigen, bestanden toe te voegen of te verwijderen of het schema aanpassen. U kunt de scan verwijderen als u deze niet meer nodig heeft.

### Een aangepaste scan bewerken of verwijderen

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.

3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**. Klik vervolgens op **Start**.

4 Voer in het venster **Scans**, in de kolom **Scan bewerken**, naast de aangepaste scan die u wilt wijzigen een van de volgende taken uit:

- Klik op het bewerkingpictogram en verschuif de schakelaars in het venster **Scan bewerken** om de scanopties in of uit te schakelen. De standaardinstellingen werken goed voor de meeste gebruikers. Klik op **Standaardwaarden gebruiken** om aangepaste instellingen te verwijderen.
- Klik op het prullenbakpictogram en dan op **Ja** om te bevestigen dat u de scan wilt verwijderen.

5 Klik op **Opslaan**.

## Norton-scans plannen

Norton detecteert wanneer u niet achter uw computer zit en voert automatisch scans uit om te zorgen dat uw systeem regelmatig op bedreigingen wordt gecontroleerd. U kunt ook uw eigen Snelle scan, Volledige systeemscan of Aangepaste scan plannen om op door u gewenste tijdstippen te worden uitgevoerd.

### Een Snelle scan, Volledige systeemsan of Handmatige scan van Norton plannen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste scan**.
- 4 Klik op **Start**.
- 5 Klik in het venster **Scans**, in de kolom **Scan bewerken**, op het bewerkingsspictogram naast Snelle scan, Volledige systeemsan of een Aangepaste scan die u eerder heeft gemaakt.
- 6 In het venster **Scan bewerken** op het tabblad **Scanplanning** doet u het volgende:
  - Selecteer onder **Wanneer moet de scan worden uitgevoerd?** een interval en selecteer vervolgens de timingopties.
  - Selecteer een optie onder **De scan uitvoeren**. Voor de meeste gebruikers is het het beste om alle vakjes aangevinkt te houden. Dit zorgt ervoor dat scans alleen worden uitgevoerd wanneer u uw computer niet gebruikt of wanneer u geen batterijvoeding gebruikt, en het voorkomt dat uw computer tijdens een scan naar de slaapstand overschakelt.
- 7 Klik op **Volgende**.
- 8 Klik op het venster **Scanopties** op **Opslaan**.

## Realtimebedreigingen weergeven die door Norton SONAR zijn gedetecteerd

SONAR biedt realtimebescherming tegen bedreigingen en detecteert proactief onbekende beveiligingsrisico's. SONAR identificeert nieuwe bedreigingen op basis van het gedrag van toepassingen. Dit gaat sneller dan de traditionele bedreigingsdetectie op basis van handtekeningen. Het beveiligt u al tegen schadelijke code voordat virusdefinities via LiveUpdate beschikbaar zijn.

---

**Opmerking:** SONAR-beveiliging moet altijd ingeschakeld zijn. Wanneer Auto-Protect is uitgeschakeld, is SONAR-beveiliging ook niet actief en is uw computer niet beschermd tegen nieuwe bedreigingen.

---

### Risico's weergeven die zijn gedetecteerd door SONAR

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 In het venster **Beveiligingsgeschiedenis** selecteert u **SONAR-activiteit** in de vervolgkeuzelijst.
- 4 Selecteer een risico in de lijst als er risico's worden weergegeven.
- 5 Volg de **Aanbevolen actie** in het deelvenster **Details**.  
Binnen deze categorie worden ook alle activiteiten vermeld die de configuratie of instellingen van uw computer aanpassen. De optie **Meer informatie** voor deze categorie biedt details over de resources die van invloed zijn op de activiteit.

### Zorg dat SONAR-beveiliging is ingeschakeld

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Zet op het tabblad **Automatische bescherming** onder **Realtimebeveiliging** de schakelaar **SONAR-beveiliging** op **Aan**.
- 5 Klik op **Toepassen**.
- 6 Klik in het venster **Instellingen** op **Sluiten**.

## Bestanden en mappen uitsluiten van de scans Norton Auto-Protect, SONAR en Downloadinformatie

U kunt Norton configureren om bepaalde programma's van de Auto-Protect- en SONAR-scans uit te sluiten. U kunt de vensters **Scanuitsluitingen** en **Realtime-uitsluitingen** gebruiken om virussen en andere beveiligingsbedreigingen met een hoog risico van scans uit te sluiten. Wanneer u een bestand of map aan de lijst met uitsluitingen toevoegt, negeert Norton het bestand of de map wanneer op beveiligingsrisico's wordt gescand.

Selecteer een map en download het bestand in de geselecteerde map om het bestand uit te sluiten van Downloadinformatie. Wanneer u bijvoorbeeld een onveilig uitvoerbaar bestand in deze map downloadt, laat Norton u het bestand downloaden en wordt het niet van uw computer verwijderd. U moet een nieuwe map maken speciaal voor uitsluitingen van Downloadinformatie.



---

**Opmerking:** Wanneer u een bestand van Norton-scans uitsluit, wordt het beveiligingsniveau van uw computer verlaagd. Doe dit alleen als u hier een specifieke reden voor heeft. Sluit items alleen uit als u zeker weet dat ze niet zijn geïnfecteerd.

---

### Beveiligingsbedreigingen met een hoog risico van scans uitsluiten

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik op de tab **Scans en risico's** in het venster **AntiVirus**.
- 5 Voer onder **Uitsluitingen/Lage risico's** een van de volgende handelingen uit:
  - Klik in de rij **Items uitsluiten van scans** op **Configureren**.
  - Klik in de rij **Items die van Auto-Protect-, Scriptbeheer-, SONAR- en downloadinformatiedetectie moeten worden uitgesloten** op **Instellen**.
- 6 Klik in het weergegeven venster op **Mappen toevoegen** of **Bestanden toevoegen**.  
U kunt uitsluitingen toewijzen aan lokale stations, mappen, groepen bestanden, afzonderlijke bestanden en netwerkstations. Het uitsluiten van bestanden op een netwerk wordt echter niet ondersteund door Norton. Als u een netwerkstation aan de lijst met uitsluitingen toevoegt, moet u ervoor zorgen dat het station met uw computer is verbonden.
- 7 Klik op het bladerpictogram in het dialoogvenster **Item toevoegen**.
- 8 Selecteer het item dat u van de scan wilt uitsluiten, in het dialoogvenster dat verschijnt.  
U kunt ook opgeven of submappen moeten worden opgenomen wanneer u mappen toevoegt.
- 9 Klik op **OK**.
- 10 Klik op **OK** in het dialoogvenster **Item toevoegen**.
- 11 Klik in het opgeroepen venster op **Toepassen** en vervolgens op **OK**.

## Bestanden met handtekening voor laag risico van Norton-scans uitsluiten

Via de Uitsluitingen van handtekeningen kunt u specifieke bekende beveiligingsrisico's selecteren om deze uit te sluiten van Norton-scans. Als bijvoorbeeld een legitieme app, zoals een gratis game, afhankelijk is van een ander programma, zoals adware, om te functioneren zou u kunnen besluiten om de adware te behouden, zelfs als deze u blootstelt aan risico's. Ook kunt u aangeven dat waarschuwen niet meer nodig is bij toekomstige scans.

---

**Opmerking:** Uitsluitingen verlagen uw bescherming. Gebruik ze alleen als u ze specifiek nodig heeft en volledig begrijpt wat de risico's zijn wanneer u bekende bedreigingen uitsluit van Norton-scans.

---

#### Een handtekening voor laag risico toevoegen aan Uitsluitingen van handtekeningen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik op het tabblad **Scans en risico's** in het venster met instellingen voor **AntiVirus**.
- 5 Klik op **Configureren** in de rij **Handtekeningen die van alle detecties worden uitgesloten** onder **Uitsluitingen/Lage risico's**.
- 6 Klik op **Toevoegen** in het venster **Uitgesloten handtekeningen**.
- 7 Klik in het venster **Beveiligingsrisico's** op een beveiligingsrisico dat u wilt uitsluiten, en klik op **Toevoegen**.
- 8 Klik in het venster **Uitgesloten handtekeningen** op **Toepassen** en vervolgens op **OK**.

## Automatische taken in- of uitschakelen

Uw Norton-product voert automatische taken uit om uw pc zo onopvallend mogelijk te beveiligen. Deze automatische taken omvatten het scannen op virussen, controleren van uw internetverbinding, downloaden van beveiligingsupdates en andere belangrijke taken. Deze activiteiten worden op de achtergrond uitgevoerd wanneer uw computer is ingeschakeld.

Als een item uw aandacht vereist, wordt een bericht weergegeven met informatie over de huidige status of om u te vragen iets te doen. Als u geen berichten ziet, is uw computer beveiligd.

U kunt uw Norton-product altijd openen om de status van uw computer te bekijken of beveiligingsdetails weer te geven.

Wanneer een achtergrondactiviteit in voortgang is, wordt een bericht weergegeven in het meldingsgebied uiterst rechts op de taakbalk. De resultaten van de recentste activiteiten worden weergegeven wanneer u het hoofdvenster van Norton de volgende keer opent.

#### Automatische taken in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.

- 3 Klik in het venster **Instellingen** op **Instellingen van Taakplanner**.
- 4 Voer de volgende handelingen uit op het tabblad **Automatische taken** van het venster **Taakplanner** :
  - Selecteer de functie die u automatisch wilt laten uitvoeren.  
Schakel het selectievakje **Taken** in om alle functies aan te vinken.
  - Hef de selectie op van de functie die u niet automatisch wilt laten uitvoeren.  
Schakel het selectievakje **Taken** uit om alle functies uit te schakelen.
- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

## Aangepaste taken uitvoeren

Norton controleert uw systeem automatisch en kiest de beste instellingen om uw systeem beveiligd te houden. U kunt echter ook een aantal specifieke taken uitvoeren. U kunt de specifieke taken die u wilt uitvoeren, selecteren aan de hand van de opties in het venster **Aangepaste taken**.

U kunt voor eenmalige scans zelf een combinatie van taken kiezen. U kunt LiveUpdate uitvoeren, een back-up maken van uw gegevens, uw browsergeschiedenis wissen, schijfruimte vrijmaken door ongewenste (schijf)bestanden op te ruimen en uw schijven optimaliseren.

### Aangepaste taken uitvoeren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het hoofdvenster van Norton. Klik vervolgens op **Scans**.
- 3 Klik in het venster **Scans** onder **Scans en taken** op **Aangepaste taak**. Klik vervolgens op **Start**.
- 4 Selecteer in het venster **Aangepaste taken** de taken die u wilt uitvoeren.  
Selecteer de optie **Taken** om alle taken te selecteren.
- 5 Klik op **Start**.

## Beveiligings- en prestatiescans plannen

Via de instellingen van Taakplanner kunt u uw systeem automatisch op beveiligings- en prestatieproblemen laten controleren door Norton. Norton

De volgende opties zijn beschikbaar voor het plannen van beveiligings- en prestatiescans:

**Automatisch (Aanbevolen)**

Met deze optie wordt uw pc op beveiligings- en prestatieproblemen gecontroleerd wanneer de pc niet actief is.

Deze optie biedt maximale beveiliging.

**Wekelijks**

Met deze optie wordt uw pc een of meer keer per week gecontroleerd op beveiligings- en prestatieproblemen.

U kunt de dagen van de week en het tijdstip van de dag selecteren waarop de scan moet worden uitgevoerd.

**Maandelijks**

Met deze optie wordt uw pc een keer per maand gecontroleerd op beveiligings- en prestatieproblemen.

U kunt de dag van de maand en het tijdstip van de dag selecteren waarop de scan moet worden uitgevoerd.

**Handmatige planning**

Met deze optie wordt geen geplande beveiligings- of prestatiescan van uw pc uitgevoerd.

Als u deze optie kiest, moet u regelmatig handmatige beveiligings- en prestatiescans van uw pc uitvoeren om de beveiliging in stand te houden.

Uw computer presteert optimaal als u belangrijke bewerkingen laat uitvoeren op momenten waarop uw computer niet actief is. Wanneer u de scans wekelijks of maandelijks plant en de optie **Alleen uitvoeren tijdens inactiviteit** selecteert, wordt uw computer door Norton gescand wanneer deze niet actief is. NortonLifeLock raadt aan om de optie **Alleen uitvoeren tijdens inactiviteit** te selecteren om computerprestaties te optimaliseren.

**Beveiligings- en prestatiescans plannen**

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.

- 3 Klik in het venster **Instellingen** op **Instellingen van Taakplanner**.

- 4 Selecteer een optie op het tabblad **Planning** onder **Plannen**.

Wanneer u de optie **Wekelijks** of **Maandelijks** selecteert, moet u het tijdstip en de datum selecteren waarop de automatische taken moeten worden uitgevoerd. U kunt ook opgeven dat de automatische taken alleen mogen worden uitgevoerd wanneer de pc niet actief is.

- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

## Gegevensbescherming configureren om schadelijke processen te blokkeren die uw pc beïnvloeden

Gegevensbescherming beschermt uw pc tegen schadelijke processen die uw pc destabiliseren, uw gegevens beschadigen en/of stelen, en hun schadelijke aard aan andere goede processen doorgeven. Het maakt gebruik van Norton-reputatietechnologie om een proces als veilig, schadelijk of onbekend te identificeren. Afhankelijk van uw situatie kunt u meer mappen en/of extensies toevoegen, en processen uitsluiten van scans en bescherming.

---

**Waarschuwing:** Als u deze functie uitschakelt, wordt uw pc minder beveiligd. We raden u dus aan om deze functie altijd ingeschakeld te houden. Als u deze functie echter wilt uitschakelen, doe het dan slechts tijdelijk en zorg dat de functie ook weer wordt ingeschakeld.

---

### Gegevensbescherming in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan** of **Uit**.
- 5 Voer een van de volgende handelingen uit in de rij **Meldingen weergeven** :
  - Zet de schakelaar op **Aan** om een melding te krijgen telkens wanneer Gegevensbescherming een bedreiging blokkeert.
  - Zet de schakelaar op **Uit** om meldingen te onderdrukken. U kunt de details van de geblokkeerde bedreigingen echter bekijken in het venster **Beveiligingsgeschiedenis**. U opent het venster **Beveiligingsgeschiedenis** door in het hoofdvenster van Norton te dubbelklikken op **Beveiliging** en dan op **Geschiedenis > Gegevensbescherming**.
- 6 Klik op **Toepassen**.
- 7 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de functie Gegevensbescherming moet worden uitgeschakeld en klikt u op **OK**.

### Een map voor Gegevensbescherming toevoegen of bewerken

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.

5 Ga als volgt te werk om een map toe te voegen of te bewerken:

- Klik naast **Beveiligde mappen** op **Configureren**.
- Voer de volgende stappen uit in het venster **Beveiligde mappen** :
  - Klik op **Toevoegen** om een nieuw item toe te voegen.
  - Als u een bestaand item wilt toevoegen, kiest u het item en klikt u op **Bewerken** om het te wijzigen.

---

**Opmerking:** Vooraf ingestelde mappen kunnen niet worden bewerkt.

---

- Blader in het venster **Item toevoegen** of **Item bewerken** en selecteer de map.
- Klik op het selectievakje om de submappen ook op te nemen.
- Klik op **OK**.

6 Klik op **Toepassen** en vervolgens op **OK**.

**Een extensie toevoegen voor Gegevensbescherming**

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.

3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.

4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.

5 Ga als volgt te werk om een extensie toe te voegen:

- Klik naast **Beschermde bestandstypen** op **Configureren**.
- Klik in het venster **Beschermde bestandstypen** op **Toevoegen**.
- In het venster **Item toevoegen** typt u de extensie die u wilt beschermen. Als u bijvoorbeeld uitvoerbare bestanden wilt beschermen, typt u .exe in het vak. Alle bestanden met een .exe-extensie op de pc zijn beschermd.
- Klik op **OK**.

6 Klik op **Toepassen** en vervolgens op **OK**.

**Een map of extensie uit Gegevensbescherming verwijderen**

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.

- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.
- 5 Klik naast **Beschermde mappen** of **Beschermde bestandstypen** op **Configureren**.
- 6 In het venster **Beschermde mappen** of **Beschermde bestandstypen** kiest u het item dat u wilt verwijderen.

---

**Opmerking:** U kunt geen vooraf ingestelde map of extensie verwijderen.

---

- 7 Klik op **Verwijderen**.
- 8 Klik op **Toepassen** en vervolgens op **OK**.

Een proces toevoegen aan of verwijderen van de uitsluitingslijst van Gegevensbescherming

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen > Antivirus**.
- 3 Klik in het venster **Antivirus** op het tabblad **Gegevensbescherming**.
- 4 Zet in de rij **Gegevensbescherming** de **Aan/Uit** -schakelaar op **Aan**.
- 5 Klik in de rij **Uitgesloten processen** op **Configureren** en voer de volgende stappen uit:
  - Als u een proces wilt toevoegen voor uitsluiting van Gegevensbescherming, klikt u op **Toevoegen** en kiest u vervolgens het proces.
  - Als u een proces wilt verwijderen van uitsluiting van Gegevensbescherming, klikt u op het proces en vervolgens op **Verwijderen**.
- 6 Klik op **Toepassen** en vervolgens op **OK**.

## Norton instellen om scripts die door phishing-pogingen kunnen worden misbruikt te verwijderen

Scriptbeheer helpt u te beschermen tegen malware die u downloadt of als bijlage ontvangt in phishingmails. De functie verwijdert standaard niet-gemeenschappelijke scripts uit bestanden en schoont de bestanden op\*\*. U kunt de originele bestanden echter nog met het script herstellen. Ook kunt u instellen hoe Norton documenten met ingesloten scripts moet afhandelen.

---

**Opmerking:** \*\*Deze functie wordt voor de browsers Chrome, Edge en Internet Explorer alleen ondersteund op Windows 10 RS2 en later.

---

Daarnaast voorkomt Norton dat programma's met ingesloten scripts worden uitgevoerd wanneer de toepassing niet-gemeenschappelijk gedrag detecteert bij de ingesloten scripts. U kunt echter instellen hoe Norton programma's met ingesloten scripts moet afhandelen.

Scripts worden gebruikt om documenten dynamisch en interactief te maken. Hoewel het primaire doel van scripts is de documentervaring te verbeteren, kunnen cybercriminelen deze gebruiken om stiekem malware op uw computer te zetten. Scripts zijn over het algemeen niet belangrijk voor het functioneren van een document en worden door veel softwareprogramma's standaard uitgeschakeld.

U kunt instellen dat Norton specifieke bestanden van Scriptbeheer uitsluit als u zeker weet dat deze geen schadelijke inhoud bevatten. Zie voor meer informatie Zie "[Bestanden en mappen uitsluiten van de scans Norton Auto-Protect, SONAR en Downloadinformatie](#)" op pagina 40.. U kunt de originele bestanden herstellen door de opgeschoonde bestanden te vervangen. Sluit alleen bestanden uit als u zeker weet dat ze geen schadelijke inhoud bevatten.

Scriptbeheer identificeert mogelijke bedreigingen op basis van het gedrag van bestanden. Als Norton mogelijk gevaarlijke activiteiten detecteert wanneer u een document of programma met een ingesloten script opent, voorkomt de toepassing dat het script wordt uitgevoerd. U kunt instellen hoe Norton de scripts moet afhandelen wanneer u documenten of programma's met ingesloten scripts opent.

## Het originele bestand herstellen

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** de optie **Weergeven** in de keuzelijst. Selecteer vervolgens **Scriptbeheer**.
- 4 Selecteer in de weergave **Scriptbeheer** het item dat u wilt herstellen.
- 5 Klik in het rechterdeelvenster onder **Details** op **Herstellen**.
- 6 Klik in het venster **Scriptbeheer herstellen** op **Ja**.
- 7 Selecteer **Ja** in de prompt die verschijnt.
- 8 Klik in het venster **Beveiligingsgeschiedenis** op **Sluiten**.

## Scriptbeheer in- of uitschakelen

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.



- 4 Klik in het venster **Antivirus** op het tabblad **Scriptbeheer**.
- 5 In de rij **Scripts verwijderen bij het downloaden van documenten** zet u de schakelaar **Aan/Uit** op **Aan** of **Uit**. Klik vervolgens op **Toepassen**.  
Als u deze uitschakelt, doet u het volgende:
  - Selecteer in het venster **Beveiligingsverzoek** in de keuzelijst **Selecteer de duur** hoelang u de optie wilt uitschakelen en klik op **OK**.
- 6 In de rij **Scripts blokkeren wanneer documenten worden geopend** zet u de schakelaar **Aan/Uit** op **Aan** of **Uit**. Klik vervolgens op **Toepassen**.  
Als u deze uitschakelt, doet u het volgende:
  - Selecteer in het venster **Beveiligingsverzoek** in de keuzelijst **Selecteer de duur** hoelang u de optie wilt uitschakelen en klik op **OK**.
- 7 Klik in het venster **Instellingen** op **Sluiten**.

## Alle items van Scriptbeheer permanent verwijderen

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** de optie **Weergeven** in de keuzelijst. Selecteer vervolgens **Scriptbeheer**.
- 4 Klik in de weergave **Scriptbeheer** op **Items wissen**.
- 5 Klik in het venster **Items wissen** op **Ja**.
- 6 Klik in het bevestigingsvenster op **Ja**.
- 7 Klik in het venster **Beveiligingsgeschiedenis** op **Sluiten**.

## Instellen hoe Norton documenten en programma's met ingesloten scripts moet afhandelen

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik in het venster **Antivirus** op het tabblad **Scriptbeheer**.
- 5 Klik onder **Scripts blokkeren wanneer documenten worden geopend** in de rij **Microsoft Office** op **Configureren**.

- 6 Selecteer in het venster **Voorkeuren voor Microsoft Office** onder **Acties** de actie die Norton voor elke toepassing moet uitvoeren.  
U kunt kiezen uit:
  - **Blokkeren**
  - **Toestaan**
  - **Mij vragen**U kunt voor elke toepassing een andere actie kiezen.
- 7 Klik op **OK** in het bevestigingsvenster dat verschijnt.
- 8 Klik op **Toepassen** in het venster **Voorkeuren voor Microsoft Office** en klik vervolgens op **OK**.
- 9 Selecteer in de rij **Adobe-document** de actie die Norton voor PDF-documenten moet uitvoeren.
- 10 Selecteer in de rij **Scripts met niet-gemeenschappelijk gedrag blokkeren** de actie die Norton moet uitvoeren voor programma's met ingesloten scripts.  
U kunt kiezen uit:
  - **Blokkeren**
  - **Toestaan**
  - **Mij vragen**
- 11 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

## Meer informatie over Scriptbeheer van Norton

Scripts worden gebruikt om documenten dynamisch en interactief te maken. Ze kunnen ook functionaliteit toevoegen door bepaalde taken te automatiseren. Scripts zijn bijvoorbeeld ActiveX-besturingselementen, invoegtoepassingen, gegevensverbindingen, macro's, gekoppelde OLE-bestanden (Object Linking and Embedding) en kleurthemabestanden.

Scriptbeheer helpt u te beschermen tegen malware die u downloadt of als bijlage in phishingmails ontvangt.

De functie verwijdert standaard onveilige scripts uit bestanden en schoont de bestanden op. U kunt de originele bestanden echter nog met het script herstellen. Ook kunt u instellen hoe Norton documenten met ingesloten scripts moet afhandelen.

De volgende secties helpen u bij het configureren van de Scriptcontrole-instellingen.

## Het originele bestand herstellen met ingesloten scripts

U kunt de originele bestanden herstellen door de opgeschoonde bestanden te vervangen. Herstel de originele bestanden alleen wanneer u zeker weet dat ze geen schadelijke inhoud bevatten.

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het Norton-hoofdvenster. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** de optie **Weergeven** in de keuzelijst. Selecteer vervolgens **Scriptbeheer**.
- 4 Selecteer in de weergave **Scriptbeheer** het actieve contentitem dat u wilt herstellen.
- 5 Klik in het rechterdeelvenster onder **Details** op **Herstellen**.
- 6 Klik in het venster **Scriptbeheer herstellen** op **Ja**.
- 7 Selecteer **Ja** in de prompt die verschijnt.
- 8 Klik in het venster **Beveiligingsgeschiedenis** op **Sluiten**.

## Instellen hoe Norton documenten en programma's met ingesloten scripts moet afhandelen

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik in het venster **Antivirus** op het tabblad **Scriptbeheer**.
- 5 Klik onder **Scripts blokkeren wanneer documenten worden geopend** in de rij **Microsoft Office** op **Configureren**.
- 6 Selecteer in het venster **Voorkeuren voor Microsoft Office** onder **Acties** de actie die Norton voor elke toepassing moet uitvoeren.

U kunt kiezen uit:

- **Blokkeren**
- **Toestaan**
- **Mij vragen**

U kunt voor elke toepassing een andere actie kiezen.

- 7 Klik op **OK** in het bevestigingsvenster dat verschijnt.

- 8 Klik op **Toepassen** in het venster **Voorkeuren voor Microsoft Office** en klik vervolgens op **OK**.
- 9 Selecteer in de rij **Adobe-document** de actie die Norton voor PDF-documenten moet uitvoeren.
- 10 Selecteer in de rij **Scripts met niet-gemeenschappelijk gedrag blokkeren** de actie die Norton moet uitvoeren voor programma's met ingesloten scripts.  
U kunt kiezen uit:
  - **Blokkeren**
  - **Toestaan**
  - **Mij vragen**
- 11 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

## Scriptbeheer uitschakelen

---

**Opmerking:** Door Scriptbeheer uit te schakelen heeft u minder bescherming. Doe dit alleen wanneer het nodig is voor een specifiek doeleinde. Scriptbeheer biedt een extra beveiligingslaag door scripts te verwijderen en documenten op te schonen. NortonLifeLock raadt aan om Scriptbeheer altijd ingeschakeld te laten, omdat het een extra beveiligingslaag biedt.

---

- 1 Start Norton.  
Als u het venster **Mijn Norton** ziet, klikt u in de rij **Apparaatbeveiliging** op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik in het venster **Antivirus** op het tabblad **Scriptbeheer**.
- 5 In de rij **Scripts verwijderen bij het downloaden van documenten** zet u de schakelaar **Aan/Uit** op **Uit**.
- 6 In de rij **Scripts blokkeren wanneer documenten worden geopend** zet u de schakelaar **Aan/Uit** op **Uit**.
- 7 Klik in het venster **Instellingen** op **Toepassen**.

- 8 Selecteer in het venster **Beveiligingsverzoek** in de keuzelijst **Selecteer de duur** hoelang u de functie wilt uitschakelen en klik vervolgens op **OK**.
- 9 Klik in het venster **Instellingen** op **Sluiten**.

## Bescherm uw apparaat tegen misbruik, hackers en zero-day aanvallen.

Een zero-day-exploit is een techniek die een hacker gebruikt om van kwetsbaarheden in een programma te profiteren en schadelijke acties op uw computer uit te voeren. Behalve dat deze exploits uw computer vertragen of programma's laten vastlopen, kunnen deze exploits uw persoonlijke gegevens en vertrouwelijke informatie blootstellen aan hackers.

De functie Misbruikpreventie in uw Norton-product beschermt toepassingen en bestanden die kwetsbaar zijn voor misbruikpogingen. Misbruikpreventie van Norton is standaard ingeschakeld en blokkeert aanvallen op kwetsbare programma's door die programma's te sluiten. Norton stuurt de melding Aanval geblokkeerd wanneer een programma wordt afgesloten en geeft links naar informatie over de aanval.

### Misbruikpreventie in- of uitschakelen

---

**Opmerking:** Wanneer **Misbruikpreventie** is uitgeschakeld, is uw computer kwetsbaar voor zero-day-exploits en andere vormen van misbruik.

---

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster Instellingen op **Misbruikpreventie**.
- 4 In de rij Misbruikpreventie zet u de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Klik in het venster Instellingen op **Toepassen** en klik vervolgens op **Sluiten**.

### Technieken voor misbruikpreventie

Norton gebruikt proactieve technieken voor misbruikpreventie om uw computer te beschermen tegen de nieuwste zero-day-aanvallen. U kunt technieken afzonderlijk in- of uitschakelen via het venster **Instellingen**. Standaard zijn alle technieken ingeschakeld.

---

**Opmerking:** Norton raadt aan om alle afzonderlijke technieken voor misbruikpreventie ingeschakeld te houden om u te beschermen tegen de meest uiteenlopende exploits.

---

Technieken voor misbruikpreventie omvatten:

- **Bescherming van Java-processen**  
Voorkomt dat hackers op afstand schadelijke code gebruiken via Java-processen en staat alleen de uitvoering van vertrouwde Java-processen toe.
- **Structured Exception Handler Overwrite-bescherming**  
Beschermt tegen exploits voor het afhandelen van gestructureerde uitzonderingen, die een toepassing in gevaar brengen door de pointer van een uitzonderingshandler te overschrijven met een door een aanvaller beheerd adres.
- **Stack Pivot-detectie**  
Blokkeert exploitaanvallen waarbij de stackpointer wordt veranderd door een geheugen van de aanvaller om een ROP-aanvalscode (Return Oriented Programming) uit te voeren.
- **Handhaving van preventie van gegevensuitvoering**  
Blokkeert aanvallers tegen het uitvoeren van schadelijke code vanuit het stack- of heap-geheugen van uw computer.
- **Handhaving van Memory Layout Randomization**  
Dwingt dynamisch geladen toepassings-DLL's of modules af om altijd op willekeurige locaties te worden geladen ter bescherming tegen aanvallers.
- **Heap Spray-bescherming**  
Beschermt vaak aangevallen geheugenlocaties waarbij exploits of aanvallers hun shellcode toewijzen met behulp van heap-spray-aanvalstechnieken.
- **Verbetering van Memory Layout Randomization**  
Verbeterd het ASLR-gedrag (Address Space Layout Randomization) van het besturingssysteem bij het toewijzen van kritieke geheugenlocaties van de toepassing. Hierdoor zijn die geheugenlocaties minder voorspelbaar voor aanvallers.
- **Null Page-bescherming**  
Wijst de null-geheugenlocatie van tevoren toe, wat helpt bij het voorkomen van aanvallen op null-pointer-dereference-kwetsbaarheden.
- **Remote DLL Injection-detectie**  
Voorkomt dat hackers op afstand schadelijke uitvoerbare code invoegen via externe netwerken zoals openbare IP-adressen of domeinen.
- De technieken **Stack-uitvoerpreventie**, **Detectie van verdachte API-aanroepen** en **Heap Payload-detectie** beschermen uw computer tegen ROP-aanvallen (Return-Orienting Programming) die niet worden tegengehouden door de misbruikbeperkingstechnieken Address Space Layout Randomization en Preventie van gegevensuitvoering.

## Norton Firewall in- of uitschakelen

De Slimme firewall controleert de communicatie tussen uw computer en de andere computers op internet. Daarnaast beveiligt de firewall uw computer tegen veelvoorkomende

beveiligingsproblemen. Wanneer de Slimme firewall is uitgeschakeld, is uw computer niet tegen internetbedreigingen en beveiligingsrisico's beveiligd.

Als u Slimme firewall wilt uitschakelen, doet u dit alleen voor een bepaalde duur, waarna de firewall automatisch weer wordt ingeschakeld.

#### Norton Firewall in- of uitschakelen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Zet in de rij **Slimme firewall** op het tabblad **Algemene instellingen** de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Klik op **Toepassen**.
- 6 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de firewallfunctie moet worden uitgeschakeld en klikt u op **OK**.

#### Norton Firewall uitschakelen of inschakelen vanuit het Windows-meldingsgebied

- 1 Rechtsklik op het Norton-pictogram in het meldingsgebied op de taakbalk, en klik vervolgens op **Slimme firewall uitschakelen** of **Slimme firewall inschakelen**.
- 2 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de firewallfunctie moet worden uitgeschakeld en klikt u op **OK**.

## Programmaregels aanpassen om toegangsinstellingen voor programma's te wijzigen

Nadat u Norton een tijdje heeft gebruikt, moet u de toegangsinstellingen voor bepaalde programma's misschien aanpassen.

#### Programmaregels aanpassen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Programmabeheer** selecteert u in de kolom **Programma** het programma dat u wilt wijzigen.

- 5 In de vervolgkeuzelijst naast het programma dat u wilt wijzigen, selecteert u het gewenste toegangsniveau voor dit programma. U kunt kiezen uit:

<b>Toestaan</b>	Alle toegangspogingen van dit programma worden toegestaan.
<b>Blokkeren</b>	Alle toegangspogingen van dit programma worden geblokkeerd.
<b>Aangepast</b>	Maak de regels waarmee wordt bepaald hoe dit programma toegang tot internet krijgt.

- 6 Klik op **Toepassen**.

## De volgorde van firewallregels wijzigen

Elke lijst met firewallregels wordt van boven naar beneden verwerkt. U kunt bepalen hoe deze regels worden verwerkt door de volgorde te wijzigen.

---

**Opmerking:** Wijzig de volgorde van de algemene verkeersregels niet, tenzij u een ervaren gebruiker bent. Wanneer u de volgorde van standaard verkeersregels wijzigt, kan dit de firewallfunctionaliteit beïnvloeden en de beveiliging van uw computer verminderen.

---

### De volgorde van verkeersregels wijzigen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Selecteer op het tabblad **Verkeersregels** de regel die u wilt verplaatsen.
- 5 Voer een van de volgende handelingen uit:
  - Als u deze regel een positie vóór de regel erboven wilt verplaatsen, klikt u op **Omhoog**.
  - Als u deze regel een positie na de regel eronder wilt verplaatsen, klikt u op **Omlaag**.
- 6 Wanneer u de gewenste regels heeft verplaatst, klikt u op **Toepassen**.

### De volgorde van programmaregels wijzigen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.



- 4 Selecteer op het tabblad **Programmabeheer** het programma dat de regel bevat die u wilt verplaatsen.
- 5 Klik op **Wijzigen**.
- 6 Selecteer in het venster **Regels** de regel die u wilt verplaatsen.
- 7 Voer een van de volgende handelingen uit:
  - Als u deze regel een positie vóór de regel erboven wilt verplaatsen, klikt u op **Omhoog**.
  - Als u deze regel een positie na de regel eronder wilt verplaatsen, klikt u op **Omlaag**.
- 8 Wanneer u de gewenste regels heeft verplaatst, klikt u op **OK**.
- 9 Klik op **Toepassen** in het venster **Firewall**.

## Een verkeersregel tijdelijk uitschakelen

U kunt een verkeersregel tijdelijk uitschakelen als u iemand specifieke toegang tot een computer of programma wilt verlenen. Vergeet niet deze regel weer in te schakelen wanneer u klaar bent met het programma of de computer waarvoor u deze wijziging moest doorvoeren.

---

**Opmerking:** Enkele standaard firewallregels in die lijst kunnen niet worden uitgeschakeld. U kunt de instellingen van deze regels alleen bekijken via de optie **Weergeven**.

---

### Een verkeersregel tijdelijk uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Verkeersregels** heft u de selectie op van de regel die u wilt uitschakelen.
- 5 Klik op **Toepassen**.

## Internettoegang toestaan voor een geblokkeerd programma

Standaard blokkeert de Slimme firewall de toegang tot internet voor bepaalde programma's. Dit kunnen soms bepaalde programma's zijn voor streaming media, netwerkgames of aangepaste zakelijke toepassingen die door uw werkgever worden geleverd. Als u zeker weet dat de internetactiviteiten van het programma geen beveiligingsrisico vormen, kunt u de blokkering van internettoegang voor het programma uitschakelen.

### Internettoegang toestaan voor een geblokkeerd programma

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Programmabeheer** selecteert u het programma waarvoor u internettoegang wilt toestaan.
- 5 Klik op **Toestaan** in de vervolgkeuzelijst **Toegang** voor de programma-ingang.
- 6 Klik op **Toepassen**.

Instellingen voor internettoegang worden standaard automatisch voor webprogramma's geconfigureerd door Norton Firewall. Dit gebeurt wanneer deze voor het eerst worden uitgevoerd. Wanneer een programma voor het eerst verbinding met internet probeert te maken, maakt Automatisch programmabeheer hier regels voor.

Met Norton kunt u echter de instellingen voor internettoegang handmatig configureren voor uw programma's.

### Instellingen voor internettoegang configureren voor uw programma's

#### Automatisch programmabeheer uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Klik in het venster **Firewall** op **Automatisch programmabeheer**.
- 5 In de rij **Automatisch programmabeheer** zet u de **Aan/Uit** -schakelaar op **Uit**.
- 6 Klik in het bevestigingsvenster op **Ja**.
- 7 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

### Instellingen voor internettoegang configureren voor een programma

- 1 Open uw programma.  
Wanneer het programma verbinding probeert te maken met internet, geeft Norton u een firewallwaarschuwing.
- 2 Selecteer in het venster **Firewallwaarschuwing** een actie uit de keuzelijst **Opties**.  
U kunt internettoegang toestaan, blokkeren of handmatig een programmaregel maken.
- 3 Klik op **OK**.

## Melding van firewallblokkering uitschakelen

Wanneer Automatisch programmabeheer ingeschakeld is, voorkomt Slimme firewall automatisch dat kwaadaardige toepassingen of toepassingen met een negatieve reputatie verbinding maken met internet of communiceren met andere computers in uw netwerk.

Norton stelt u op de hoogte wanneer Slimme firewall voorkomt dat een toepassing verbinding met het netwerk maakt. U kunt deze optie uitschakelen via **Geavanceerd programmabeheer** als u de melding niet wilt zien.

### Melding van firewallblokkering uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Zet op het tabblad **Geavanceerd programmabeheer** de schakelaar **Melding firewallblokkering weergeven** op **Uit**.

## Meer informatie over de lijst met uitsluitingen voor Inbraakpreventie

Als u zeker weet dat een apparaat in uw netwerk veilig is, kunt u het vertrouwensniveau voor het apparaat op Volledig vertrouwd instellen. U kunt het vertrouwensniveau van een apparaat configureren met behulp van Apparaatvertrouwen onder **Netwerkinstellingen**. U kunt deze vertrouwde apparaten van de inbraakpreventiescan uitsluiten. Wanneer u volledig vertrouwde apparaten van de inbraakpreventiescan uitsluit, wordt de scantijd korter en de netwerksnelheid van uw computer verbeterd. Wanneer u een volledig vertrouwd apparaat uitsluit, wordt informatie die van dat apparaat wordt ontvangen, niet gescand. Volledig vertrouwde apparaten die van de inbraakpreventiescan zijn uitgesloten, worden aan de lijst met uitsluitingen voor Inbraakpreventie toegevoegd.

Merkt u dat een van de apparaten die u van de inbraakpreventiescan heeft uitgesloten, is geïnfecteerd, dan kunt u de opgeslagen lijst met uitsluitingen leegmaken. Wanneer u dit doet,

verwijdert uw Norton-product alle door de inbraakpreventiescan uitgesloten apparaten van deze lijst.

U kunt de opgeslagen lijst met uitsluitingen in de volgende omstandigheden leegmaken:

- Een van de apparaten die u van inbraakpreventiescans heeft uitgesloten, is geïnfecteerd.
- Een van de apparaten die u van inbraakpreventiescans heeft uitgesloten, probeert de computer te infecteren.
- Uw thuisnetwerk is geïnfecteerd.

#### Alle apparaten uit de lijst met uitgesloten items voor Inbraakpreventie verwijderen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Leegmaken** in de rij **Lijst met uitsluitingen** onder **Inbraakpreventie**.
- 6 Klik in het bevestigingsvenster op **Ja**.
- 7 Klik in het venster **Instellingen** op **Sluiten**.

## Browserbeveiliging inschakelen

Schadelijke websites detecteren en misbruiken zwakke punten in browsers om malware te downloaden. Wanneer u Browserbeveiliging inschakelt, blokkeert Norton malware voordat deze kan aanvallen. Het beschermt uw gevoelige gegevens en voorkomt dat aanvallers toegang kunnen krijgen tot uw computer.

Browserbeveiliging is standaard ingeschakeld. Houd Browserbeveiliging ingeschakeld om bescherming tegen schadelijke websites te waarborgen.

---

**Opmerking:** De functie Browserbeveiliging is beschikbaar voor de browsers Google Chrome, Microsoft Internet Explorer, Mozilla Firefox en Microsoft Edge.

---

### Hoe kan ik Browserbeveiliging inschakelen?

De functie Browserbeveiliging is standaard ingeschakeld om uw browser tegen schadelijke websites te beschermen. Wanneer u de functie echter had uitgeschakeld, kunt u deze weer inschakelen.

### Browserbeveiliging inschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster Instellingen op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 In de rij Browserbeveiliging zet u de **Aan/Uit** -schakelaar op **Aan**.
- 6 Klik op **Toepassen**.
- 7 Klik in het venster **Instellingen** op **Sluiten**.

## Stel Norton Firewall in om waarschuwingen over blokkering van een aanval in of uit te schakelen

U kunt kiezen of u een waarschuwing wilt ontvangen wanneer Inbraakpreventie van Norton een verdachte aanval blokkeert.

Als u ervoor heeft gekozen geen waarschuwingen te ontvangen, kunt u nog steeds in uw beveiligingsgeschiedenis bekijken welke aanvallen Norton heeft geblokkeerd.

### Waarschuwingen voor Inbraakpreventie in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Onder **Inbraakpreventie**, in de rij **Meldingen**, zet u de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 6 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

### Afzonderlijke waarschuwingen voor Inbraakpreventie in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.

- 5 Klik op **Configureren** in de rij **Handtekeningen voor inbraakbeveiliging** onder **Inbraakpreventie**.
- 6 Schakel in het venster **Handtekeningen voor inbraak** de optie **Waarschuwen** in of uit voor de individuele handtekening.
- 7 Klik op **OK**.
- 8 Klik in het venster **Handtekeningen voor inbraak** op **Toepassen** en klik vervolgens op **OK**.
- 9 Klik in het venster **Instellingen** op **Sluiten**.

## AutoBlock in- of uitschakelen

Norton AutoBlock stopt al het verkeer tussen een apparaat in uw netwerk en elke andere computer die probeert dat apparaat te misbruiken. Aangezien dit verkeer omvat dat mogelijk niet schadelijk is, stopt AutoBlock de verbinding slechts voor beperkte tijd nadat een bedreiging is gedetecteerd. Hier kunt u opgeven hoelang uw Norton-product de verbindingen van aanvallende computers moet blokkeren. Standaard wordt al het verkeer tussen uw computer en de aanvallende computer 30 minuten geblokkeerd.

Als u toegang wilt krijgen tot een of meer computers die door AutoBlock worden geblokkeerd, kunt u AutoBlock uitschakelen.

### AutoBlock in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Beveiliging tegen inbreuk met AutoBlock** onder **Inbraakpreventie**.
- 6 In het venster **Beveiliging tegen inbreuk met AutoBlock** voert u onder **AutoBlock** een van de volgende handelingen uit:
  - Klik op **Uit** om Beveiliging tegen inbreuk met AutoBlock uit te schakelen.
  - Klik op **Aan (aanbevolen)** om Beveiliging tegen inbreuk met AutoBlock in te schakelen. Selecteer vervolgens in de vervolgkeuzelijst **AutoBlock aanvallende computers voor** hoelang automatische blokkering ingeschakeld moet blijven.
- 7 Klik in het venster **Beveiliging tegen inbreuk met AutoBlock** op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

## De blokkering opheffen van computers die door Norton AutoBlock zijn geblokkeerd

Als Norton Firewall netwerkverkeer stopt op een computer waarvan u weet dat deze veilig is, kunt u de verbindingen met de computer herstellen door deze te verwijderen uit de AutoBlock-lijst in de Norton Firewall-instellingen.

### De blokkering opheffen van computers die door AutoBlock zijn geblokkeerd

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Beveiliging tegen inbreuk met AutoBlock** onder **Inbraakpreventie**.
- 6 Selecteer het IP-adres van de computer in het venster **Beveiliging tegen inbreuk met AutoBlock** onder **Computers die momenteel door AutoBlock worden geblokkeerd**.
- 7 Selecteer onder de kolom **Actie** de optie **Blokkering opheffen** in de vervolgkeuzelijst.
- 8 Klik in het venster **Beveiliging tegen inbreuk met AutoBlock** op **OK**.
- 9 Klik in het venster **Instellingen** op **Sluiten**.

## Een apparaat toevoegen aan Apparaatvertrouwen

U kunt handmatig een apparaat aan Apparaatvertrouwen toevoegen. U kunt een apparaat toevoegen door het volgende op te geven:

- De naam of beschrijving van het apparaat
- Het IP-adres of fysieke adres van het apparaat

---

**Opmerking:** Als u een apparaat vertrouwt dat zich niet in uw netwerk bevindt, kunt u uw computer aan potentiële beveiligingsrisico's blootstellen.

---

### Een apparaat toevoegen aan Apparaatvertrouwen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.

- 4 Op het tabblad **Algemene instellingen** in de rij **Apparaatvertrouwen** klikt u op **Configureren**.
- 5 Klik in het venster **Apparaatvertrouwen** op **Toevoegen**.
- 6 Typ in het vak **Naam** van het venster **Apparaat toevoegen** de naam van het apparaat dat u aan uw netwerk wilt toevoegen.  
De apparaatnaam mag niet meer dan 15 tekens bevatten.
- 7 Typ in het tekstvak **IP-adres of fysiek adres** het IP-adres of fysieke adres van het apparaat dat u aan Apparaatvertrouwen wilt toevoegen.

U kunt de volgende indelingen gebruiken in het tekstvak **IP-adres of fysiek adres** :

IPv4-adres	172.16.0.0
IPv6-adres	fe80::12ac:fe44:192a:14cc
Fysiek adres	11-22-c3-5a-fe-a4
Herleidbare host	ftp.myfiles.com

Het adres wordt pas geverifieerd wanneer het apparaat fysiek op het netwerk wordt gevonden.

- 8 Selecteer een optie in de vervolgkeuzelijst **Vertrouwensniveau**. U kunt kiezen uit:

**Volledig vertrouwd**

Hiermee wordt een apparaat aan de lijst Volledig vertrouwd toegevoegd.

Apparaten met dit vertrouwensniveau worden alleen op bekende aanvallen en infecties gecontroleerd. Selecteer deze instelling alleen wanneer u zeker weet dat het apparaat helemaal veilig is.

**Beperkt**

Hiermee wordt een apparaat aan de lijst Beperkt toegevoegd.

Beperkte apparaten hebben geen toegang tot uw computer.

- 9 Zet een vinkje bij **Uitsluiten van Inbraakpreventie-scans** als u het apparaat wilt uitsluiten van Inbraakpreventie-scans.
- 10 Klik op **Apparaat toevoegen**.



## Downloadinformatie in- of uitschakelen

Downloadinformatie beschermt uw computer tegen onveilige bestanden die u op uw computer kunt uitvoeren nadat u deze heeft gedownload met een ondersteunde browser. De optie **Downloadinformatie** is standaard ingeschakeld. In dit geval verschaft Downloadinformatie informatie over het reputatieniveau van alle uitvoerbare bestanden die u downloadt. De door Downloadinformatie verstrekte reputatiedetails geven aan of het gedownloade bestand veilig kan worden geïnstalleerd.

Het kan voorkomen dat u Downloadinformatie moet uitschakelen. U wilt een onveilig bestand misschien downloaden. In dat geval moet u Downloadinformatie uitschakelen, zodat u het bestand kunt downloaden zonder dat het door uw Norton-product van uw computer wordt verwijderd.

U kunt de optie **Downloadinformatie** gebruiken om Downloadinformatie in of uit te schakelen.

### Downloadinformatie in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 In de rij **Downloadinformatie** zet u de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 6 Klik op **Toepassen**.
- 7 Indien u daarom wordt gevraagd, geeft u op na hoeveel tijd de functie Downloadinformatie moet worden uitgeschakeld en klikt u op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

## Filteren van spam in- of uitschakelen

Met het toenemende gebruik van e-mail ontvangen veel gebruikers grote hoeveelheden ongewenste en ongevraagde commerciële e-mailberichten, ook wel spam genoemd. Spam maakt het niet alleen moeilijk legitieme e-mailberichten te identificeren, sommige spamberichten bevatten bovendien stuitende teksten en afbeeldingen.

U kunt filteren op spam om deze spammails in de hand te houden. Spambeveiliging blijft standaard actief. Mocht u deze beveiliging willen uitschakelen, dan kunt u dit vanuit het programma zelf doen.

---

**Opmerking:** Wanneer u Norton AntiSpam uitschakelt, verhoogt u de kans op ongewenste e-mailberichten.

---

### Filteren van spam in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiSpam**.
- 4 Zet op het tabblad **Filter** in de rij **AntiSpam** de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Als u filteren van spam wilt uitschakelen, doet u het volgende:
  - Selecteer in het venster **Beveiligingsverzoek** in de vervolgkeuzelijst **Selecteer de duur** hoelang u filteren van spam wilt uitschakelen.
- 6 Klik op **Toepassen**.
- 7 Klik op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

## Internetgebruik definiëren voor Norton

Met **Beperken van netwerkgebruik** kunt u bepalen hoeveel bandbreedte Norton gebruikt. Beperken van netwerkgebruik is standaard ingeschakeld en ingesteld op Automatisch. In Windows 7 of eerder is de standaardinstelling **Geen limiet**. Als u een trage internetverbinding heeft, kunt u de bandbreedte die Norton gebruikt, verlagen. U kunt ook het communicatiebeleid instellen voor alle netwerkverbindingen die door uw computer worden gebruikt, door de instellingen van Beperken van netwerkgebruik te wijzigen.

### Internetgebruik definiëren voor Norton

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.
- 4 Op het tabblad **Algemene instellingen** in de rij **Beperken van netwerkgebruik** klikt u op **Configureren**. Als de optie **Configureren** is uitgeschakeld, zet u de schakelaar **Aan/Uit** op **Aan**.
- 5 Klik in het venster met instellingen voor **Beperken van netwerkgebruik** onder de kolom **Beleid** op de vervolgkeuzelijst naast de netwerkverbinding waarvoor u een beleid wilt instellen.
- 6 Selecteer een van de volgende opties:
  - **Auto** Met behulp van deze optie kan Norton het beleid voor het observeren van kosten van Windows gebruiken om alle updates van virusdefinities en producten te ontvangen.

---

**Opmerking:** De optie Automatisch is alleen beschikbaar in Windows 8 of later.

---

- **Geen limiet** Hiermee kan uw Norton-product de netwerkbandbreedte gebruiken die nodig is om alle product- en virusdefinitie-updates te ontvangen. Als u Windows 7 of eerder gebruikt, is het standaardbeleid ingesteld op **Geen limiet**.
  - **Beperkt** Hiermee krijgt Norton alleen toegang tot internet om essentiële productupdates en virusdefinities te ontvangen. Als u een beperkte internetverbinding heeft, kunt u de optie **Beperkt** selecteren om te zorgen dat u tegen de belangrijkste beveiligingsbedreigingen wordt beschermd.
  - **Geen verkeer** Hiermee kunt u voorkomen dat door Norton verbinding met internet wordt gemaakt. Als u dit beleid kiest, kan Norton geen essentiële virusdefinities en programma-updates ontvangen, wat tot potentiële internetgevaren en virusaanvallen kan leiden.
- 7 Klik op **Toepassen** en vervolgens op **OK**.
  - 8 Klik in het venster **Instellingen** op **Sluiten**.

## Beperken van netwerkgebruik in- of uitschakelen

U kunt beleidsregels instellen om het internetgebruik van Norton te beperken. Als u het internetgebruik van uw Norton-product niet wilt beperken, kunt u **Beperken van netwerkgebruik** uitschakelen.

Als u vindt dat Norton te veel netwerkbandbreedte gebruikt, kunt u **Beperken van netwerkgebruik** inschakelen. Vervolgens kunt u beleidsregels instellen om het internetgebruik van Norton te beperken. Norton maakt verbinding met internet op basis van het beleid dat u instelt in het venster **Beperken van netwerkgebruik**. **Beperken van netwerkgebruik** is standaard ingeschakeld.

### Beperken van netwerkgebruik in- of uitschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall**.  
Klik op **Netwerk** als u Norton AntiVirus heeft.
- 4 Zet op het tabblad **Algemene instellingen** in de rij **Beperken van netwerkgebruik** de **Aan/Uit** -schakelaar op **Uit** of **Aan**.
- 5 Klik in het venster **Instellingen** op **Toepassen** en klik vervolgens op **Sluiten**.

# Norton instellen om toezicht te houden op toepassingen en schadelijke websites te blokkeren op uw computer

Enkele schadelijke websites kunnen proberen ongeautoriseerde toegang te krijgen tot uw apparaatgegevens wanneer u freeware- of sharewaretoepassingen installeert en opent. Schadelijke websites detecteren en exploiteren kwetsbaarheden om malware te downloaden, zoals malware voor **crypto mining**, waarmee uw apparaatgegevens aan cybercriminelen kunnen worden onthuld.

Als **Toezicht op app-URL's** is ingeschakeld, controleert Norton alle toepassingen die op uw computer zijn geïnstalleerd en worden schadelijke websites geblokkeerd zodat ze geen toegang krijgen tot uw computer. Norton waarschuwt u wanneer een schadelijke website wordt geblokkeerd en u kunt de informatie over de aanval in het venster Beveiligingsgeschiedenis bekijken.

---

**Opmerking:** Browsertoepassingen worden niet door **Toezicht op app-URL's** gecontroleerd. U moet Norton-browserextensies toevoegen om uw browsertoepassing tegen schadelijke websites te beschermen.

---

## Toezicht op app-URL's inschakelen om schadelijke websites te blokkeren

**Toezicht op app-URL's** is standaard ingeschakeld. Houd Toezicht op app-URL's ingeschakeld om bescherming tegen schadelijke websites te waarborgen.

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster Instellingen op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Onder **Inbraakpreventie**, in de rij **Toezicht op app-URL's**, zet u de Aan/Uit-schakelaar op Aan.

## Een URL of domein uitsluiten van toezicht

Inbraakpreventie maakt gebruik van een uitgebreide lijst met aanvalshandtekeningen om schadelijke websites te detecteren en blokkeren. In sommige gevallen kunnen goedaardige websites als verdacht worden geïdentificeerd, omdat ze een vergelijkbare aanvalshandtekening hebben. Als u meldingen over een mogelijke aanval ontvangt en weet dat de websites of

domeinen die deze meldingen activeren veilig zijn, dan kunt u de handtekening van toezicht uitsluiten.

### Meldingen voor een URL of domein uitschakelen

- 1 Klik in de waarschuwing melding op **Details weergeven**.
- 2 Klik op **Blokkering van URL opheffen** in het venster **Beveiligingsgeschiedenis - Geavanceerde details**.

### Een URL of domein uitsluiten met uw Norton

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Firewall** of **Netwerk**.
- 4 Klik op het tabblad **Inbraak- en browserbeveiliging**.
- 5 Klik op **Configureren** in de rij **Uitsluitingen van Toezicht op app-URL's** onder **Inbraakpreventie**.
- 6 Klik op de knop **Toevoegen** en voer de URL of de domeinnaam in die u van toezicht wilt uitsluiten.
- 7 Als u een URL of domein wilt bewerken of verwijderen, doet u het volgende:
  - Selecteer een URL of domein in de lijst en klik op de knop **Bewerken**. Wijzig de URL of de domeinnaam.
  - Selecteer de URL die of het domein dat u wilt verwijderen en klik op de knop **Verwijderen**.

## Informatie over de geblokkeerde URL weergeven

### Informatie in de waarschuwing melding weergeven

- 1 Klik in de waarschuwing melding op **Details weergeven**.
- 2 In het venster **Beveiligingsgeschiedenis - Geavanceerde details** kunt u meer informatie bekijken over de geblokkeerde URL.

### Informatie weergeven met behulp van het venster Beveiligingsgeschiedenis

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Beveiliging** in het hoofdvenster van het Norton-product. Klik vervolgens op **Geschiedenis**.
- 3 Selecteer in het venster **Beveiligingsgeschiedenis** in de keuzelijst **Weergeven** de optie **Inbraakpreventie**.

- 4 Klik op een rij om de details voor dat item te bekijken.
- 5 Dubbelklik op een rij of klik op **Meer opties** om de Geavanceerde details van beveiligingsgeschiedenis te openen. Hier vindt u meer informatie over de activiteit en kunt u indien nodig actie ondernemen.

## Aan de slag met Norton Cloudback-up

Met Cloudback-up slaat u belangrijke bestanden en documenten op als preventieve maatregel tegen gegevensverlies als gevolg van een defecte vaste schijf, gestolen apparaten en zelfs ransomware.

---

**Opmerking:** Norton Cloudback-up is alleen beschikbaar op Windows.

---

Voordat u Norton Cloudback-up uitvoert, maakt u een back-upset waarmee u opgeeft van welke bestanden u een back-up wilt maken. U kunt ook opgeven waar en wanneer de back-up van de bestanden moet worden gemaakt. U kunt een back-up van uw bestanden naar de cloud maken via Norton Cloudback-up, of naar uw eigen externe stations.

---

**Opmerking:** De eerste keer dat u een back-up uitvoert, kan het even duren voordat alle bestanden op uw computer door Norton zijn gecontroleerd en gekopieerd. Dit proces kan nog langer duren als u een trage internetverbinding heeft.

Norton maakt geen automatische back-up van uw bestanden wanneer de back-upbestemming een lokale back-up is. Voor het maken van een back-up naar lokale opslagapparaten moet u zelf actie ondernemen.

---

### Een back-upset maken

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Back-upsets**.
- 3 Klik in het venster **Back-upinstellingen** op **Nieuwe set maken**.
- 4 In het venster dat verschijnt, typt u een naam voor uw back-upset. Klik vervolgens op **OK**.
- 5 Schakel op het tabblad **Wat** onder **Bestandstypen** een of meer bestandscategorieën waarvan u een back-up wilt maken in of uit.
- 6 Selecteer op het tabblad **Waar** in de kolom **Doel Veilige cloudopslag**.  
Wanneer u cloudback-up niet heeft geactiveerd, klik dan op de link **Gratis activeren** en volg de instructies.

- 7 Kies in de lijst **Schema** op het tabblad **Wanneer** het back-upschema dat het beste aan uw behoeften voldoet.
- 8 Klik op **Instellingen opslaan**.

#### Norton Cloudback-up uitvoeren

---

**Opmerking:** Norton kan u vragen uw accountgegevens voor authenticatie in te voeren wanneer u voor het eerst een back-up maakt.

---

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van het Norton-product. Klik vervolgens op **Back-up uitvoeren**.
- 3 Volg de instructies op het scherm in het venster **Back-up uitvoeren**.
- 4 Klik op **Sluiten**.

---

**Opmerking:** Als de back-up niet kan worden voltooid, biedt Norton mogelijke oorzaken zoals onvoldoende opslagcapaciteit of snelheidsbeperkingen. Controleer steeds of u met het internet bent verbonden wanneer u een back-up uitvoert, en dat opslagapparaten verbonden en ingeschakeld zijn.

---

## Bestanden en mappen toevoegen aan of uitsluiten van uw back-upsets

Met Norton kunt u in uw back-upsets back-ups zetten van verschillende bestandstypen, zoals foto-, muziek- of videobestanden. U kunt bestanden of mappen opgeven die bestandstypen bevatten die normaal gesproken in uw back-upsets worden opgenomen en deze uitsluiten van back-ups.

U kunt ook bestandsextensies toevoegen of verwijderen die normaal deel uitmaken van de standaardbestandstypen. Voor meer informatie: Zie "[De standaard bestandstypen of bestandsextensies die Norton in back-ups opneemt, weergeven of wijzigen](#)" op pagina 72.

#### Bestanden en mappen toevoegen aan of uitsluiten van uw back-upset

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Back-upsets**.

- 3 Selecteer de back-upset die u wilt configureren in het venster **Back-upinstellingen** in de vervolgkeuzelijst **Back-upset**.
- 4 Klik in het tabblad **Wat** op **Bestanden en mappen toevoegen of uitsluiten**.
- 5 Voer in het venster dat verschijnt de volgende handelingen uit:
  - Om een bestand aan de back-upset toe te voegen, klikt u op **Bestand opnemen** en gaat u naar het bestand dat u wilt toevoegen.
  - Om een map aan de back-upset toe te voegen, klikt u op **Map opnemen** en gaat u naar de map die u wilt toevoegen.
  - Om een bestand uit de back-upset te verwijderen, klikt u op **Bestand uitsluiten** en gaat u naar het bestand dat u wilt verwijderen.
  - Om een map uit de back-upset te verwijderen, klikt u op **Map uitsluiten** en gaat u naar de map die u wilt verwijderen.
- 6 Klik in het venster **Back-upinstellingen** op **Instellingen opslaan**.

---

**Opmerking:** U kunt ook met de rechtermuisknop op een bestand of map klikken en **Norton Security > Aan back-up toevoegen/Van back-up uitsluiten** selecteren in het snelmenu.

De opties **Aan back-up toevoegen** en **Van back-up uitsluiten** verschijnen alleen in het snelmenu, nadat u uw back-up heeft geconfigureerd en wanneer de vensters **Back-upinstellingen** en **Bestanden herstellen** zijn gesloten.

---

## De standaard bestandstypen of bestandsextensies die Norton in back-ups opneemt, weergeven of wijzigen

Norton Backup zoekt standaard naar bestanden die horen bij bepaalde bestandstypen, zoals afbeeldingen, muziek of video, voordat een back-up wordt uitgevoerd. De standaard bestandstypen zorgen ervoor dat gegevens die de meeste gebruikers belangrijk vinden, automatisch in een back-up worden opgenomen wanneer ze een back-upset hebben gemaakt en een back-up uitvoeren. U kunt de standaardinstellingen voor de bestandstypen of extensies in elk bestandstype, wijzigen als bepaalde gegevens wel of niet in back-ups wilt opnemen.

### Standaard bestandstypen of bestandsextensies voor back-ups weergeven of wijzigen

- 1 Start Norton.
  - Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Back-upsets**.
- 3 Selecteer de back-upset die u wilt configureren in het venster **Back-upinstellingen** in de vervolgkeuzelijst **Back-upset**.



- 4 Ga naar het tabblad **Wat** en vink **Bestandstype bewerken** aan om de extensies in bestandstypen voor afbeeldingen, muziek, video en andere bestandstypen te wijzigen.
- 5 Klik onder **Bestandstypen** op **Configureren** naast een bestandstype.
- 6 Voer de volgende handelingen uit in het venster dat wordt weergegeven en klik op **Opslaan**.
  - Selecteer de bestandsextensie in de lijst en klik op **Verwijderen** om een bestandsextensie te verwijderen.
  - Klik op **Nieuwe toevoegen** om extra extensies aan de lijst toe te voegen.
- 7 Klik in het venster **Back-upinstellingen** op **Instellingen opslaan**.

## Foto's, muziek of andere belangrijke bestanden herstellen uit Norton-back-upsets

U kunt uw Norton Back-upgegevens gemakkelijk herstellen als u het slachtoffer wordt van ransomware of andere malware, of als u met onherstelbare hardwareproblemen te maken krijgt. U kunt volledige back-upsets of specifieke bestanden in een back-upset herstellen. U kunt ook bepalen waar de back-upbestanden moeten worden hersteld.

---

**Opmerking:** Herstel wordt uitgevoerd volgens de geconfigureerde back-upset. Als u naar een nieuw apparaat herstelt, kunt u niet verwachten dat Norton uw bestanden herstelt volgens de gewenste mapstructuur van uw oude apparaat.

---

### Norton-back-upbestanden of volledige back-upsets herstellen

- 1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Bestanden herstellen**.
- 3 In het venster **Bestanden herstellen** klikt u onder **Herstellen vanaf** op **Alles weergeven**.

Klik op een back-upset en klik vervolgens op **OK**.
- 4 In het venster **Bestanden herstellen** onder **Bestanden** klikt u op **Naar bestanden en mappen bladeren**.

Selecteer de bestanden die u wilt herstellen en klik op **OK**.

- 5 In het venster **Bestanden herstellen** klikt u onder **Herstellen naar op Oorspronkelijke locatie**.

Klik op **Wijzigen** en volg de instructies als u niet naar de oorspronkelijke locatie wilt herstellen.

- 6 Klik op **Bestanden herstellen** en vervolgens op **Sluiten**.

#### Bestanden downloaden van Cloudback-up

- 1 Ga naar <https://my.Norton.com>.
- 2 Klik op **Aanmelden**.
- 3 Voer het e-mailadres en wachtwoord voor uw NortonLifeLock-account in en klik op **Aanmelden**.
- 4 Klik op de pagina **Mijn Norton** en op de tegel **Cloudback-up** op **Back-upsets weergeven**.
- 5 Selecteer de back-upset met het bestand dat u wilt downloaden.
- 6 Navigeer naar het bestand dat u wilt downloaden.  
  
Als u weet wat de bestandsnaam is, kunt u de zoekfunctie gebruiken om het bestand te zoeken.  
  
Gebruik de optie **Filter** om foto's en documenten uit te filteren.
- 7 Beweeg de muisaanwijzer over de bestandsnaam en klik op **Downloaden**.

## Back-upset en -bestanden verwijderen uit Cloudback-up

U kunt een back-upset verwijderen als u deze niet meer nodig heeft. Wanneer slechts één back-upset beschikbaar is, kunt u deze niet verwijderen. U kunt echter een nieuwe back-upset maken voordat u de oude back-upset verwijdert.

---

**Opmerking:** Het kan voorkomen dat u vanwege een onderbreking van de back-endservice of serveronderhoud uw back-upgegevens niet kunt verwijderen. Wacht in dat geval enige tijd voordat u ze opnieuw probeert te verwijderen. Kijk op de pagina [Servicestatus van Norton](#) om te zien of er een serviceonderbreking is.

---

Wanneer een back-upset wordt verwijderd, worden de back-updetails van de bestanden in de verwijderde back-upset ook gewijzigd. Zo worden de pictogramoverlays en het tabblad **Back-up** in de bestandseigenschappen van het bestand niet langer weergegeven.

Het is vooral nuttig een back-upset te verwijderen, als u ruimte vrij wilt maken in uw Veilige cloudopslag.

---

**Opmerking:** Als u een back-upset uit uw cloudback-up wilt verwijderen, moet u de optie **Beperken van netwerkgebruik** in het venster **Firewallinstellingen** instellen op **Geen limiet**.

Voor meer informatie: Zie "[Internetgebruik definiëren voor Norton](#)" op pagina 66.

---

### Een back-upset verwijderen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Dubbelklik op **Back-up** in het hoofdvenster van Norton. Klik vervolgens op **Back-upsets**.
- 3 Selecteer de back-upset die u wilt verwijderen in het venster **Back-upinstellingen** in de vervolgkeuzelijst **Back-upset**.
- 4 Klik op **Verwijderen**.
- 5 Voer in het venster **Back-upset verwijderen** een van de volgende opties uit:
  - Selecteer **Back-upset verwijderen** om de huidige back-upset te verwijderen.
  - Selecteer **Back-upset en -bestanden verwijderen** om de huidige back-upset en de bestanden waarvan al een back-up is gemaakt te verwijderen.
- 6 Klik op **Ja**.

### Back-upset uit uw account verwijderen

- 1 Meld u aan bij uw [account](#).
- 2 Klik op de pagina **Mijn Norton** op **Cloudback-up**.  
De bestaande back-upsets die in gebruik zijn, worden weergegeven.
- 3 Als u een back-upset wilt verwijderen, klikt u op het prullenbakpictogram van de back-upset die u wilt verwijderen.
- 4 Klik in het bevestigingsvenster **Back-upset verwijderen** op **Verwijderen**.  
Klik op **Annuleren** om de back-uppagina weer te geven zonder de back-upset te verwijderen.

## De instellingen van uw Norton-product aanpassen

In het venster **Instellingen** kunt u de volgende services voor **Snelle besturingselementen** in- of uitschakelen:

- **Stille modus**
- **Back-up**
- **Overlays van back-upstatus**

- **Automatische LiveUpdate**
- **Slimme firewall**
- **Norton Tamper Protection**

Het is raadzaam alle services behalve Stille modus ingeschakeld te laten.

#### **Snelle besturingselementen in- of uitschakelen**

1 Start Norton.

Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.

2 Klik in het hoofdvenster van Norton op **Instellingen**.

3 Onder **Snelle besturingselementen** in het venster **Instellingen** kunt u het volgende doen:

- Als u een service wilt inschakelen, schakelt u het bijbehorende selectievakje in.
- Als u een service wilt uitschakelen, schakelt u het bijbehorende selectievakje uit.  
Als een waarschuwing of bericht verschijnt, selecteert u de duur in het vervolgkeuzemenu en klikt u vervolgens op **OK**.

## **Instellingen voor Realtimebeveiliging aanpassen**

Realtimebeveiliging detecteert onbekende beveiligingsrisico's op uw computer en laat u bepalen welke actie moet worden ondernomen wanneer u een risico vindt.

---

**Opmerking:** Voor de meeste gebruikers worden standaardinstellingen aanbevolen. Als u een functie tijdelijk wilt uitschakelen, moet u hem zo snel mogelijk weer inschakelen. Als u wilt dat items met een laag risico automatisch worden verwijderd, configureert u de Geavanceerde modus van SONAR. Auto-Protect controleert op virussen en andere beveiligingsrisico's telkens wanneer u programma's op uw computer uitvoert. Zorg dat Auto-Protect altijd ingeschakeld is.

---

### **Auto-Protect instellen om verwisselbare media te scannen**

Hiermee wordt op opstartvirussen gecontroleerd wanneer u verwisselbare media activeert. Zijn de verwisselbare media eenmaal gescand op opstartvirussen, dan worden ze pas weer gescand wanneer ze opnieuw worden geplaatst of geformatteerd. Als u vermoedt dat een verwisselbaar medium door een opstartvirus is geïnfecteerd, moet u verifiëren dat Auto-Protect is ingeschakeld om het verwisselbare medium opnieuw te scannen. U plaatst vervolgens het verwisselbare medium en opent het via Deze computer om het opnieuw te laten scannen door Auto-Protect. U kunt de verwisselbare media ook handmatig scannen om te verifiëren dat ze niet zijn geïnfecteerd.

### Instellingen voor Automatische bescherming aanpassen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Zet onder **Scan van verwisselbare media** de schuifregelaar op **Aan**.

### SONAR instellen om bedreigingen automatisch te verwijderen

SONAR biedt realtimebeveiliging tegen bedreigingen en detecteert proactief onbekende beveiligingsrisico's op uw computer. SONAR identificeert nieuwe bedreigingen op basis van het gedrag van toepassingen. U kunt opgeven hoe SONAR een bedreiging verwijdert via de instellingen van de Geavanceerde modus van SONAR.

#### SONAR instellen om bedreigingen automatisch te verwijderen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Zet onder **Risico's automatisch verwijderen** de schuifregelaar op **Altijd**.
- 5 Zet onder **Risico's verwijderen als ik weg ben** de schuifregelaar op **Altijd**.
- 6 Klik op **Toepassen**.

### Auto-Protect instellen om bekende goede bestanden uit te sluiten van Norton-scans

Als u vindt dat een legitieme toepassing ten onrechte als een beveiligingsrisico is aangemerkt door Norton, kunt u het bestand uitsluiten van Norton-scans.

#### Bestanden van Norton-scans uitsluiten

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van Norton op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **AntiVirus**.
- 4 Klik op de tab **Scans en risico's** in het instellingenvenster voor AntiVirus.
- 5 Voer onder **Uitsluitingen/Lage risico's** een van de volgende handelingen uit:
  - Klik in de rij **Items uitsluiten van scans** op **Configureren**.

- Klik in de rij **Items die van Auto-Protect-, SONAR- en downloadinformatiedetectie moeten worden uitgesloten op Configureren**.
- 6 Klik in het weergegeven venster op **Mappen toevoegen** of **Bestanden toevoegen**.
  - 7 Klik op het bladerpictogram in het dialoogvenster **Item toevoegen**. In het dialoogvenster dat wordt geopend, selecteert u het item dat u van de scan wilt uitsluiten.
  - 8 Klik op **OK**.

## Meer informatie over de instellingen voor Scans en risico's

Via de instellingen voor **Scans en risico's** kunt u de scans aanpassen die door Norton op uw computer worden uitgevoerd. U kunt een scan configureren aan de hand van de digitale handtekening en het vertrouwensniveau van de bestanden op uw computer. U kunt opgeven wat moet worden gedaan tijdens het scannen van e-mailberichten.

U kunt de volgende instellingen voor **Scans en risico's** gebruiken:

### Computerscans

U kunt verschillende typen scans uitvoeren om virusinfecties op uw computer te detecteren en voorkomen. Dit zijn Snelle scan, Volledige systeemscan en Aangepaste scan. U kunt de verschillende opties van **Computerscans** gebruiken om de scans te verbeteren die door Norton op uw computer worden uitgevoerd. U kunt ook aangeven dat u gecomprimeerde bestanden wilt scannen.

Via de opties voor **Computerscans** kunt u ook instellen dat scans rootkits, andere onzichtbare items, tracking-cookies en onbekende beveiligingsbedreigingen scannen. U kunt kiezen uit:

- **Scan van gecomprimeerde bestanden**  
Met deze optie scant en herstelt u de bestanden in gecomprimeerde bestanden. Wanneer u deze functie inschakelt, worden virussen en andere beveiligingsrisico's in de bestanden in de gecomprimeerde bestanden gescand en gedetecteerd, en worden de gecomprimeerde bestanden verwijderd.
- **Scan van rootkits en onzichtbare items**  
Hiermee kunt u op rootkits en andere beveiligingsrisico's scannen die misschien op uw computer zijn verborgen.
- **Scan van netwerkstations**  
Hiermee worden de netwerkstations gescand die op uw computer zijn aangesloten. Norton voert een **Scan van netwerkstations** uit tijdens een **Volledige systeemscan** en **Aangepaste scan**. De optie **Scan van netwerkstations** is standaard ingeschakeld. Als u de optie uitschakelt, worden netwerkstations niet gescand.
- **Heuristische beveiliging**  
Hiermee wordt uw computer gescand om deze tegen onbekende beveiligingsbedreigingen te beschermen.

Norton maakt gebruik van heuristische technologie om verdachte eigenschappen van een bestand te controleren zodat het als geïnfecteerd kan worden gecategoriseerd. De technologie vergelijkt de eigenschappen van een bestand met die van een bekend geïnfecteerd bestand. Als voldoende verdachte eigenschappen worden gevonden, identificeert Norton het bestand als geïnfecteerd met een bedreiging.

- **Scan van trackingcookies**

Hiermee kunt u op kleine bestanden scannen die door programma's op uw computer kunnen worden geplaatst om uw computeractiviteiten te volgen.

- **Volledige systeemscaan**

Met een volledige systeemscaan wordt de volledige computer uitgebreid gescand op virussen, spyware en andere beveiligingskwetsbaarheden. Met de optie **Configureren** kunt u de volledige systeemscaan plannen.

## Beveiligde poorten

Met de instellingen voor deze optie kunt u de POP3- en SMTP-poorten van uw e-mailprogramma beveiligen.

U kunt deze optie gebruiken om uw POP3- en SMTP-e-mailpoorten handmatig te configureren voor e-mailbeveiliging. Als de SMTP- en POP3-poortnummers die u van uw internetaanbieder heeft ontvangen voor uw e-mailprogramma afwijken van de standaard SMTP- en POP3-poortnummers, moet u Norton configureren om de poorten te beveiligen.

## Antivirusscan voor e-mails

Antivirusscan voor e-mails beveiligt u tegen de bedreigingen die via e-mailbijlagen worden verzonden of ontvangen.

Met de opties van Antivirusscan voor e-mails kunt u bepalen wat Norton moet doen tijdens het scannen van e-mailberichten. Norton scant automatisch de e-mailberichten die u verzendt of ontvangt aan de hand van de opties die u kiest.

## Uitsluitingen/Lage risico's

Met uitsluitingsopties geeft u de items zoals mappen, bestanden en stations op die u van Norton-scans uitsluit. Scanhandtekeningen en items met laag risico zijn enkele items die u van scans kunt uitsluiten.

Met behulp van uitsluitingsopties kunt u ook kiezen welke risicocategorieën Norton moet detecteren. U kunt kiezen uit:

- **Lage risico's**

Hiermee kunt u de items met een laag risico beheren die op uw computer zijn gevonden. U kunt instellen hoe Norton op items met een laag risico moet reageren.

- **Items uitsluiten van scans**

Hiermee bepaalt u welke schijven, mappen of bestanden moeten worden uitgesloten van risicoscans.

U kunt nieuwe uitsluitingsitems toevoegen of de toegevoegde items bewerken in de lijst met uitgesloten items. U kunt items ook uit de lijst met uitgesloten items verwijderen.

- **Items die van Auto-Protect-, SONAR- en downloadinformatiedetectie moeten worden uitgesloten**

Hiermee bepaalt u welke schijven, mappen of bestanden moeten worden uitgesloten van Auto-Protect-scans en SONAR-scans.

U kunt nieuwe items die moeten worden uitgesloten, toevoegen of de items die u al heeft uitgesloten, aanpassen. U kunt items ook uit de lijst met uitgesloten items verwijderen.

- **Handtekeningen die van alle detecties worden uitgesloten**

Via Uitsluitingen van handtekeningen kunt u bekende risico's op naam selecteren en een risiconaan uit de lijst met uitgesloten items verwijderen.

U kunt ook de risicogevolgen bekijken op basis van de impact op prestaties, privacy, verwijdering en onzichtbaarheid.

- **Bestands-id's wissen die van scans worden uitgesloten**

Hiermee kunt u de reputatiegegevens van bestanden die van scans zijn uitgesloten, verwijderen.

U kunt de optie **Alles wissen** gebruiken om de reputatiegegevens van de bestanden die van scans zijn uitgesloten, te wissen.

---

**Opmerking:** Uitsluitingen verlagen uw beveiligingsniveau. Gebruik ze alleen als u ze specifiek nodig heeft.

---

## Meer informatie over de instellingen van Inbraakpreventie en browserbeveiliging

Inbraakpreventie scant alle netwerkcommunicatie van en naar uw computer en vergelijkt deze informatie met een verzameling aanvalshandtekeningen. Dit zijn gegevens aan de hand waarvan aanvalspogingen kunnen worden geïdentificeerd van aanvallers die bekende zwaktes in programma's of besturingssystemen uitbuiten. Inbraakpreventie beveiligt uw computer tegen de meeste internetaanvallen.

Als de informatie overeenkomt met een aanvalshandtekening, wordt het pakket automatisch door Inbraakpreventie verwijderd en wordt de verbinding verbroken met de computer waarvan de gegevens afkomstig zijn. Op die manier is uw computer volledig beveiligd.

Inbraakpreventie maakt gebruik van een uitgebreide lijst met aanvalshandtekeningen om verdachte netwerkactiviteiten te detecteren en te blokkeren. Het Norton-product voert LiveUpdate automatisch uit zodat uw lijst met aanvalshandtekeningen actueel blijft. Als u Automatische LiveUpdate niet gebruikt, dient u LiveUpdate eenmaal per week uit te voeren.



Het Norton-product biedt ook de functie Browserbeveiliging om uw browser tegen schadelijke programma's te beschermen.

---

**Opmerking:** De functie Browserbeveiliging is beschikbaar voor de browsers Google Chrome, Microsoft Internet Explorer, Mozilla Firefox en Microsoft Edge.

---

Internet wordt steeds intensiever gebruikt, waardoor uw webbrowswer kwetsbaarder wordt voor aanvallen door kwaadaardige websites. Deze websites detecteren de zwakke plek in uw webbrowswer en maken hier misbruik van door zonder uw toestemming of medeweten malwareprogramma's op uw systeem te downloaden. Deze malwareprogramma's worden ook wel 'drive-by downloads' genoemd. Het Norton-product beveiligt uw browser tegen 'drive-by downloads' van schadelijke websites.

De instellingen voor **Inbraak- en browserbeveiliging** bevatten ook de optie **Downloadinformatie** om uw computer te beveiligen tegen onveilige bestanden die u downloadt. Downloadinformatie verschaft informatie over het reputatieniveau van alle uitvoerbare bestanden die u downloadt via de webbrowswer. Downloadinformatie biedt alleen ondersteuning voor downloads via het HTTP-protocol, Internet Explorer 6.0 of later, Edge 40.15063 of later, Chrome 10.0 of later en Firefox 3.6 of later. De door Downloadinformatie verstrekte reputatiedetails geven aan of het gedownloade bestand veilig kan worden geïnstalleerd. Aan de hand van deze details kunt u bepalen of u het uitvoerbare bestand wilt installeren.

## Norton zo instellen dat u uw beschermde apparaten op afstand kunt beheren

**Extern beheer** van Norton verzendt de status van uw apparaat en andere informatie naar de Norton Studio-app voor Windows. U kunt deze app gebruiken om op afstand uw Norton-producten te bekijken, te beheren of te verkennen en een aantal beschermingsproblemen met uw apparaat op te lossen. Extern beheer is standaard uitgeschakeld.

### Extern beheer inschakelen

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 In de rij **Extern beheer** zet u de schakelaar op **Aan**.
- 5 Klik op **Toepassen** en vervolgens op **Sluiten**.

## Instellingen voor Norton-apparaatbeveiliging beschermen tegen onbevoegde toegang

U kunt onbevoegde wijzigingen van uw instellingen voor Norton-apparaatbeveiliging voorkomen door **Wachtwoordbeveiliging voor instellingen** en **Norton Tamper Protection** in te schakelen.

- Met **Wachtwoordbeveiliging voor instellingen** kunt u een wachtwoord instellen om de apparaatbeveiligingsinstellingen te kunnen bekijken of wijzigen.
- **Norton Tamper Protection** controleert op wijzigingen in uw instellingen door onbekende of verdachte apps.

**Wachtwoordbeveiliging voor instellingen en Norton Tamper Protection aan- of uitschakelen**

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Onder **Productbeveiliging** :
  - Zet de schakelaar in de rij **Wachtwoordbeveiliging voor instellingen** op **In** of **Uit**.
  - Zet de schakelaar in de rij **Norton Tamper Protection** op **In** of **Uit**.  
Indien u daarom wordt gevraagd, geeft u op hoelang de functie uit moet staan en klikt u op **OK**.
- 5 Klik op **Toepassen**.
- 6 Als u het venster **Wachtwoord instellen** ziet, typt u een wachtwoord en bevestigt u het. U moet een wachtwoord instellen telkens wanneer u deze functie in- en uitschakelt.
- 7 Klik op **OK**.
- 8 Klik in het venster **Instellingen** op **Sluiten**.

### Een verloren of vergeten wachtwoord voor Wachtwoord-beveiliging voor Norton-instellingen opnieuw instellen

U moet uw Norton opnieuw installeren om toegang te krijgen tot de instellingen en een nieuw wachtwoord in te stellen.

## Een sneltoets instellen om in Norton-apparaatbeveiliging te zoeken naar informatie

Wanneer u zoekt met behulp van het zoekpictogram in de app Norton Apparaatbeveiliging, kunt u online informatie vinden over Norton-functies en ondersteuning, evenals algemene

onderwerpen. U kunt de standaard sneltoets **Ctrl + F** gebruiken om sneller te zoeken of een sneltoets instellen.

#### Een sneltoets voor zoeken configureren

- 1 Start Norton.  
Wanneer u naast **Apparaatbeveiliging** het venster **Mijn Norton** ziet, klikt u op **Openen**.
- 2 Klik in het hoofdvenster van het Norton-product op **Instellingen**.
- 3 Klik in het venster **Instellingen** op **Beheerinstellingen**.
- 4 Zet in de rij **Sneltoets voor Zoeken** de schakelaar op **Aan**.
- 5 Klik op de pijl en kies de toets waaraan u Zoeken in product wilt toewijzen.
- 6 Voer een van de volgende handelingen uit:
  - Als de sneltoets alleen moet werken wanneer uw Norton-product is geselecteerd, moet u de **selectie ongedaan maken** van de optie **Algemeen**.
  - Moet de sneltoets ook werken wanneer uw Norton-product **niet** is geselecteerd, dan moet u de optie **Algemeen selecteren**.
- 7 Klik op **Toepassen** en vervolgens op **Sluiten**.

## Uw computer optimaliseren voor gamen met Game Optimizer

Game Optimizer<sup>1</sup> is gepatenteerde technologie voor pc's met een multi-core-CPU. Het zorgt voor een meeslepende spelervaring door onderbrekingen in de prestaties te verminderen, terwijl de beveiliging van uw computer toch behouden blijft. Door niet-essentiële apps te isoleren op een enkele CPU-kern, kan de rest van de CPU's worden toegewezen aan games.

---

**Opmerking:** De processor van uw computer moet minimaal vier kernen hebben om Game Optimizer te laten werken.

---

Game Optimizer helpt uw game-ervaring te verbeteren door het volgende te doen:

- Optimaliseert CPU-prestaties voor vloeiender gamen
- Isoleert niet-essentiële apps op een enkele CPU-kern zodat de rest van de CPU's kan worden toegewezen aan games.
- Detecteert games automatisch<sup>2</sup>
- Biedt u de mogelijkheid games toe te voegen of games te selecteren die u niet wilt optimaliseren

- Verhoogt frames per seconde (FPS) en vermindert latentie
- Elimineert de noodzaak om antivirusbescherming uit te schakelen door de CPU te gebruiken voor optimale gamingprestaties
- Door CPU-kernen aan de game te wijden, vermindert het willekeurige CPU-pieken die het gamen kunnen vertragen

Zie Zie [“Meer informatie over Game Optimizer”](#) op pagina 85. voor meer informatie.

---

**Opmerking:** Alle essentiële Norton-beschermingsfuncties die worden gebruikt om uw computer tegen virussen en andere beveiligingsbedreigingen te beschermen, worden op de achtergrond uitgevoerd zonder uw gamingervaring aan te tasten.

---

### Norton configureren voor een optimale gamingervaring

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** in het middelste venster op het pictogram met het bliksemschichtje.
- 3 Klik op het **Gamingdashboard** op **Optimalisatie beheren**.
- 4 Configureer in het venster **Game Optimizer** de volgende instellingen:
  - **Resourcegebruik voor gebruikersprocessen beperken** : schakel deze optie in om CPU-gebruik voor alle door de gebruiker geïnitieerde processen te beperken.
  - **Resourcegebruik voor systeemp processen beperken** : schakel deze optie in om CPU-gebruik voor alle door het besturingssysteem geïnitieerde processen te beperken.
  - **Energieschema autom. op max. prestaties instellen** : schakel deze optie in om over te schakelen naar de instelling voor energiebeheerschema voor hoge prestaties in Windows. Game Optimizer maakt een aangepaste instelling voor het Windows-energiebeheerschema om gamingprestaties te maximaliseren. Dit energiebeheerschema is alleen beschikbaar wanneer de gamingsessie in voortgang is. Nadat de gamingsessie is beëindigd, wordt het energiebeheerschema standaard teruggezet op de oorspronkelijke instelling.  
Norton raadt u aan deze optie ingeschakeld te laten voor een betere gamingervaring.
  - **Geoptimaliseerde games** : geeft de games weer die door Game Optimizer worden geoptimaliseerd.

### Game Optimizer uitschakelen

Game Optimizer is standaard ingeschakeld. U kunt Game Optimizer uitschakelen als u wilt dat Norton uw gamingervaring verbetert. Norton raadt u aan deze functie ingeschakeld te laten voor een betere gamingervaring.

### Game Optimizer in- of uitschakelen

- 1 Start Norton.
- 2 Verschuif in het venster **Mijn Norton** in het linkerdeelvenster de regelaar **Game Optimizer** om de functie in of uit te schakelen.

### Game Optimizer in- of uitschakelen via het meldingsgebied

- ◆ Klik met de rechtermuisknop op het Norton-pictogram in het meldingsgebied op de Windows-taakbalk en voer een van de volgende handelingen uit:
  - Klik op **Game Optimizer uitschakelen** om dit uit te schakelen.
  - Klik op **Game Optimizer inschakelen** om dit in te schakelen.

<sup>1</sup>Game Optimizer is alleen beschikbaar in Windows (behalve Windows 10 in S-modus, Windows met ARM-processor) met vier of meer kernprocessors.

<sup>2</sup>Detecteert automatisch games met hoog CPU-gebruik op basis van de modus Herkenning volledig scherm, evenals het gebruik van een game-launcher<sup>3</sup>, als de gebruiker een game handmatig toevoegt of als een game eerder is gedetecteerd.

<sup>3</sup>Game-launchers die we momenteel controleren (vanaf april 2021) zijn: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

## Meer informatie over Game Optimizer

Game Optimizer<sup>1</sup> is gepatenteerde technologie voor pc's met een multi-core-CPU. Het zorgt voor een meeslepende spelervaring door onderbrekingen in de prestaties te verminderen, terwijl de beveiliging van uw computer toch behouden blijft. Door niet-essentiële toepassingen te isoleren op een enkele CPU-kern, kan de rest van de CPU's worden toegewezen aan games.

Game Optimizer helpt uw game-ervaring te verbeteren door het volgende te doen:

- Optimaliseert CPU-prestaties voor vloeiender gamen
- Isoleert niet-essentiële apps op een enkele CPU-kern zodat de rest van de CPU's kan worden toegewezen aan games.
- Detecteert games automatisch<sup>2</sup>
- Biedt u de mogelijkheid games toe te voegen of games te selecteren die u niet wilt optimaliseren
- Verhoogt frames per seconde (FPS) en vermindert latentie
- Elimineert de noodzaak om antivirusbescherming uit te schakelen door de CPU te gebruiken voor optimale gamingprestaties
- Door CPU-kernen aan de game te wijden, vermindert het willekeurige CPU-pieken die het gamen kunnen vertragen

De minimale achtergrondactiviteiten zorgen ook voor betere prestaties van uw computer, wat ideaal is voor gamen. Nadat u uw gamingssessie heeft beëindigd, hervat Norton 360 for Gamers alle opgeschorte activiteiten om deze op de achtergrond uit te voeren.

---

**Opmerking:** De processor van uw computer moet minimaal vier kernen hebben om Game Optimizer te laten werken.

---

Game Optimizer start de optimalisatie wanneer u een gamingapp start en blijft actief tot u de game afsluit. De optimalisatie wordt gepauzeerd als u de modus Volledig scherm verlaat wanneer de gamingssessie actief is. Als u bijvoorbeeld op **Alt + Tab** drukt om naar een ander actief programma te gaan, sluit het de game-optimalisatie af en worden de beperkingen verwijderd. Wanneer u echter weer gaat gamen, wordt de game-optimalisatie voortgezet en krijgen beperkte programma's geen toegang tot CPU-gebruik.

---

**Opmerking:** Alle essentiële Norton-beschermingsfuncties die worden gebruikt om uw computer tegen virussen en andere beveiligingsbedreigingen te beschermen, worden op de achtergrond uitgevoerd zonder uw gamingervaring aan te tasten.

---

U kunt de status van Game Optimizer in het meldingsgebied van de taakbalk verifiëren. Op het Norton-productpictogram in het meldingsgebied verschijnt een groen bliksemschichtje wanneer Game Optimizer is ingeschakeld. Wanneer u Game Optimizer uitschakelt, verandert de kleur in grijs.

Het Gamingdashboard toont de status van Game Optimizer, de optimalisatiestatus van recent gespeelde games en toegang tot de Game Optimizer-instellingen. U kunt de schakelaar gebruiken om optimalisatie voor recent gespeelde games in of uit te schakelen.

---

**Opmerking:** De functie Game Optimizer is alleen beschikbaar in Norton 360 for Gamers.

---

<sup>1</sup>Game Optimizer is alleen beschikbaar in Windows (behalve Windows 10 in S-modus, Windows met ARM-processor) met vier of meer kernprocessors.

<sup>2</sup>Detecteert automatisch games met hoog CPU-gebruik op basis van de modus Herkenning volledig scherm, evenals het gebruik van een game-launcher<sup>3</sup>, als de gebruiker een game handmatig toevoegt of als een game eerder is gedetecteerd.

<sup>3</sup>Game-launchers die we momenteel controleren (vanaf april 2021) zijn: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

## Handmatig games aan de lijst Geoptimaliseerde games toevoegen

Game Optimizer<sup>1</sup> is gepatenteerde technologie voor pc's met een multi-core-CPU. Het zorgt voor een meeslepende spelervaring door onderbrekingen in de prestaties te verminderen,

terwijl de beveiliging van uw computer toch behouden blijft. Door niet-essentiële apps te isoleren op een enkele CPU-kern, kan de rest van de CPU's worden toegewezen aan games. Bovendien wordt er toezicht gehouden op de interne lijst met bekende games om gamingapps te detecteren.<sup>1,2</sup> Als Norton een specifieke game echter niet automatisch heeft gedetecteerd, kunt u de game handmatig toevoegen aan de lijst **Geoptimaliseerde games**.

U kunt games ook uit de lijst **Geoptimaliseerde games** verwijderen, als u de prestaties voor die games niet door Norton 360 for Gamers wilt laten verbeteren.

---

**Opmerking:** Wanneer u een specifieke game uit de lijst **Geoptimaliseerde games** verwijdert, wordt de game niet langer geoptimaliseerd en kan dit van invloed zijn op uw gamingervaring met die game.

---

#### Een game aan de lijst **Geoptimaliseerde games** toevoegen

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** in het middelste venster op het pictogram met het bliksemschichtje.
- 3 Klik op het **Gamingdashboard** op **Optimalisatie beheren**.
- 4 Klik in het venster **Game Optimizer** naast **Geoptimaliseerde games** op **Toevoegen**.
- 5 Ga naar het gamingprogramma dat Norton moet optimaliseren en selecteer het.

#### Een game uit de lijst **Geoptimaliseerde games** verwijderen

- 1 Start Norton.
- 2 Klik in het venster **Mijn Norton** in het middelste venster op het pictogram met het bliksemschichtje.
- 3 Klik op het **Gamingdashboard** op **Optimalisatie beheren**.
- 4 Zet in het venster **Game Optimizer** onder **Geoptimaliseerde games** de schakelaar naast het gamingprogramma dat u wilt verwijderen uit.

<sup>1</sup>Game Optimizer is alleen beschikbaar in Windows (behalve Windows 10 in S-modus, Windows met ARM-processor) met vier of meer kernprocessors.

<sup>2</sup>Detecteert automatisch games met hoog CPU-gebruik op basis van de modus Herkenning volledig scherm, evenals het gebruik van een game-launcher<sup>3</sup>, als de gebruiker een game handmatig toevoegt of als een game eerder is gedetecteerd.

<sup>3</sup>Game-launchers die we momenteel controleren (vanaf april 2021) zijn: Bethesda, Blizzard, Epic, ID, Origin, Rockstar, Steam, Uplay.

# Extra oplossingen vinden

Dit hoofdstuk bevat de volgende onderwerpen:

- [Apparaatbeveiliging op Windows verwijderen](#)
- [Disclaimers](#)

## Apparaatbeveiliging op Windows verwijderen

Voer onderstaande instructies uit om uw app Apparaatbeveiliging van uw computer te verwijderen.

### Apparaatbeveiliging van Windows verwijderen

- 1 Druk op de toetsen **Windows + R** om het dialoogvenster **Uitvoeren** te openen.
- 2 Typ `appwiz.cpl` en druk op **Enter**.
- 3 Selecteer in de lijst met momenteel geïnstalleerde programma's uw Norton-product en klik vervolgens op **Verwijderen/wijzigen**.
- 4 Volg de instructies op het scherm.

Apparaatbeveiliging wordt pas volledig verwijderd wanneer u de computer opnieuw opstart.

## Disclaimers

Copyright © 2021 NortonLifeLock Inc. Alle rechten voorbehouden. NortonLifeLock, het NortonLifeLock-logo, het keurmerkviñkje, Norton, LifeLock en het LockMan-logo zijn handelsmerken of gedeponeerde handelsmerken van NortonLifeLock Inc. of haar dochterondernemingen in de Verenigde Staten en andere landen. Firefox is een handelsmerk van de Mozilla Foundation. Google Chrome en Android zijn handelsmerken van Google, LLC. Mac, iPhone en iPad zijn handelsmerken van Apple Inc. Microsoft en het Windows-logo zijn handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen. De Android Robot wordt gereproduceerd of aangepast op basis van werk gemaakt en gedeeld door Google, en wordt gebruikt volgens de voorwaarden die zijn beschreven in de Creative Commons 3.0 Attribution License. Andere namen kunnen handelsmerken zijn van de respectieve eigenaars.