Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8.1 och Windows Server 2012 R2

På den här sidan

Din information

Dina val

Användning av informationen

Kontakta oss

Senast uppdaterad: april 2014

Dessa utvalda avsnitt ur den fullständiga sekretesspolicyn för Windows 8.1 och Windows Server 2012 R2 (”sekretesspolicyn för Windows”) beskriver överskådligt vissa datainsamlings- och användningsmetoder i anslutning till Windows 8.1 och Windows Server 2012 R2 (”Windows”). De fokuserar på onlinefunktioner och är inte avsedda att vara en fullständig beskrivning. De gäller inte för andra webbplatser, produkter eller tjänster från Microsoft, varken online eller offline.

Sekretesspolicyn innehåller följande avsnitt:

- **Huvudpunkter** (den här sidan)
- Policy, som är den fullständiga sekretesspolicyn för Windows 8.1, innehåller länkar till sekretesspolicyn för funktioner i Windows som har en egen, fristående policy
- Tillägg för funktioner, som beskriver funktionerna som påverkar sekretessen i Windows 8.1 och Windows Server 2012 R2
- Tillägg för appar, som beskriver apparna som påverkar

sekretessen i Windows 8.1

- Tillägg för server, som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012 R2

Mer information om hur du skyddar datorn, din personliga information och din familj på webben finns i Microsofts säkerhetscenter.

Din information

- Vissa Windows-funktioner kan be om ditt tillstånd att få samla in eller använda information från din dator, inklusive personlig information. Windows använder den här informationen på det sätt som beskrivs i den fullständiga Windows 8.1-sekretesspolicynsamt i Tillägg för funktioner, Tillägg för appar och Tillägg för server.

- Vissa funktioner i Windows kan, efter ditt medgivande, dela personlig information på Internet.

- Om du väljer att registrera programvaran kan du bli ombedd att tillhandahålla personlig information.

- Windows måste aktiveras. Detta är ett sätt att minska risken för förfalskad programvara och att säkerställa att våra kunder får den programvarukvalitet som de förväntar sig. Aktiveringsfunktionen skickar en del information om din dator till Microsoft.

- Om du väljer att logga in i Windows med ett Microsoft-konto synkroniserar Windows dina inställningar på dina enheter och loggar in dig automatiskt i vissa appar och på vissa webbplatser. Du behöver inte logga in med ett Microsoft-konto i Windows för att komma åt e-posttjänster eller sociala tjänster från andra leverantörer, men om leverantören tillhandahåller en app via Store behöver du logga in i Store med ett Microsoft-konto om du vill installera appen. Om du skapar ett Microsoft-konto ombeds du att uppge en del personliga uppgifter, till exempel geografisk region och födelsedatum.

- Ytterligare information

Överst på sidan

Dina val

- Du kan styra hur Windows-funktionerna överför information på Internet på flera olika sätt. Information om hur du använder dessa funktioner finns i Tillägg för funktioner, Tillägg för appar och Tillägg för server.
- För att förbättra din upplevelse är vissa funktioner som använder Internet aktiverade som standard.
- Ytterligare information

Överst på sidan

Användning av informationen

- Vi använder informationen som samlats in för att aktivera funktionerna som du använder eller tillhandahålla tjänsterna som du efterfrågar. Vi använder den även för att förbättra våra produkter och tjänster. Ibland ger vi andra företag tillgång till information för att tillhandahålla våra tjänster. Enbart företag som av affärsskäl behöver använda informationen har tillgång till dem. Dessa företag måste bevara informationens konfidentiella natur och de får inte använda den i några andra syften.
- Ytterligare information

Överst på sidan

Kontakta oss

Mer information om vår sekretesspraxis finns i den fullständiga sekretesspolicyn för Windows 8.1. Eller så kan du skriva till oss via vårt webbformulär.

Överst på sidan

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8.1 och Windows Server 2012 R2

På den här sidan

Insamling och användning av din information
Insamling och användning av information om din dator
Säkerhet för din information
Ändringar i denna sekretesspolicy
Mer information

Senast uppdaterad: april 2014

Den här policyn gäller Windows 8.1 och Windows Server 2012 R2 (”Windows”). Vissa Windows-komponenter har egna sekretesspolicyer, som också visas på den här sidan. Sekretesspolicyer för programvara och tjänster med anknytning till Windows och för tidigare versioner visas också där.

Information om specifika funktioner finns i Tillägg för funktioner, Tillägg för apparsamt i Tillägg för server. Information om Windows Embedded Industry Pro och Windows Embedded Industry Enterprise finns i den här policyn.

Denna policy fokuserar på funktioner som kommunicerar med Internet och är inte avsedd att vara en fullständig lista.

Insamling och användning av din information

Den personliga information som Microsoft samlar in från dig används av oss och våra kontrollerade dotterbolag och koncernbolag för att aktivera de funktioner som du använder samt för att tillhandahålla de tjänster eller utföra de transaktioner som du har begärt eller godkänt.

Informationen kan också användas för att analysera och förbättra Microsofts produkter och tjänster.

Förutom vad som anges i denna policy kommer inte personlig information som du tillhandahåller att överföras till tredje part utan ditt medgivande. Då och då anlitar vi andra företag för att tillhandahålla begränsade tjänster för vår räkning, t.ex. för att utföra statistiska analyser av våra tjänster. Dessa företag får endast tillgång till de personliga uppgifter som de behöver för att leverera tjänsten och de tillåts inte använda informationen i något annat syfte.

Microsoft kan komma åt eller lämna ut information om dig, inklusive innehållet i dina kommunikationer, i syfte att: (a) följa lagen eller svara på lagliga förfrågningar eller juridiska processer; (b) skydda Microsofts eller våra kunders rättigheter och egendom, inklusive efterlevnad av våra avtal eller principer som reglerar hur du får använda programvaran, eller (c) handla i god tro att åtkomst eller utlämnande är nödvändigt för att skydda den personliga säkerheten hos Microsofts anställda, kunder eller allmänheten.

Information som har samlats in av eller skickats till Microsoft via Windows 8.1 kan lagras och bearbetas i USA eller något annat land som Microsoft eller dess koncernbolag eller tjänstleverantörer bedriver verksamhet i. Microsoft följer de riktlinjer om intrång i privatlivet (safe harbor framework) som har fastställts av USA:s handelsdepartement när det gäller insamling, användning och bevarande av information från Europeiska unionen, Europeiska ekonomiska samarbetsområdet och Schweiz.

Överst på sidan

Insamling och användning av information om din dator

När du använder programvara med Internetaktiverade funktioner skickas information om datorn ("standardinformation om datorn") till de webbplatser som du besöker och de onlinetjänster som du använder. Standarddatorinformation omfattar normalt sådan information som din IP-adress, operativsystemversion, webbläsarversion och nationella inställningar och språkinställningar. I vissa fall kan den även omfatta ett maskinvaru-ID som anger enhetens tillverkare, enhetens namn och version. Om en viss funktion eller

tjänst skickar information till Microsoft skickas även standardinformation om datorn.

I den detaljerade informationen om varje Windows-funktion i Tillägg för funktioner, Tillägg för appar och Tillägg för server, samt de funktioner som anges på den här sidan, beskrivs vilken ytterligare information som samlas in och hur den används.

Administratörer kan använda en grupprincip för att ändra flera av inställningarna för funktionerna som beskrivs här. Mer information finns i detta white paper för administratörer.

Överst på sidan

Säkerhet för din information

Vi på Microsoft värnar om att skydda din personliga information. Vi använder flera olika säkerhetstekniker och säkerhetsrutiner för att skydda din information från obehörig åtkomst, användning eller visning. Vi lagrar t.ex. all information du lämnar på datorsystem med begränsad åtkomst och som finns i väl övervakade lokaler. När vi skickar mycket konfidentiell information (till exempel kreditkortsnummer eller lösenord) över Internet, skyddar vi den genom att kryptera den, t.ex. med SSL-protokoll (Secure Socket Layer).

Överst på sidan

Ändringar i denna sekretesspolicy

Vi uppdaterar denna sekretesspolicy från tid till annan för att återspegla ändringar i våra produkter, tjänster och kundfeedback. När detta sker ändrar vi datumet på raden "Senast uppdaterad" längst upp i sekretesspolicyn. Om viktiga ändringar görs i den här säkerhetspolicyn eller i hur Microsoft använder dina personliga uppgifter kommer vi att informera dig om detta genom att antingen publicera ett meddelande om ändringarna innan de genomförs eller genom att skicka ett meddelande direkt till dig. Vi rekommenderar att du läser igenom denna policy regelbundet för att hålla dig informerad om hur Microsoft skyddar din information.

Överst på sidan

Mer information

Microsoft välkomnar kommentarer om den här sekretesspolicyn. Om du har frågor om policyn eller om du anser att vi inte har följt den är du välkommen att kontakta oss via vårt webbformulär.

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

Överst på sidan

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8.1 och Windows Server 2012 R2

På den här sidan

Aktivering

Active Directory Rights Management Services (AD RMS) Client

Annonserings-ID

Granskning

Biometri

BitLocker-diskkryptering

Kontakter

Enhetsidentifiering och konfiguration

Enhetskryptering

DirectAccess

Hjälpmedelscenter

Senast uppdaterad: april 2014

Observera att den här sidan är ett tillägg till sekretesspolicyn för Windows 8.1 och Windows Server 2012 R2 (”sekretesspolicyn för Windows”), som innehåller följande avsnitt:

- Huvudpunkter
- Policy, som är den fullständiga sekretesspolicyn för Windows 8.1, innehåller länkar till sekretesspolicyn för Windows-funktioner som har en egen, fristående policy
- **Tillägg för funktioner** (den här sidan), som beskriver funktionerna som påverkar sekretessen i Windows 8.1 och Windows Server 2012 R2
- Tillägg för appar, som beskriver apparna som påverkar sekretessen i Windows 8.1
- Tillägg för server, som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012 R2

Om du vill ha information om hur vi samlar in och använder data i

Loggboken

Family Safety

Fax

Anpassa handskrift – automatisk inlärning

Hemgrupp

Input Method Editor (IME)

Internetanslutningsdelning

Internetutskrift

Språkinställningar

Positioneringstjänster

Hantera dina autentiseringsuppgifter

Namn och profilbild

Network Awareness

Aviseringar, låsskärmsappar och paneluppdateringar

Beställ foton

Förhämtning och förstart

Assistenten för programkompatibilitet

Egenskaper

Närhet

Fjärråtkomstanslutningar

RemoteApp- och fjärrskrivbordsanslutningar

Anslutning till

anslutning till en viss funktion eller tjänst i Windows läser du den fullständiga sekretesspolicyn och eventuella tillägg eller fristående policyinformation.

Aktivering

Funktionens uppgift

Aktiveringsfunktionen minskar risken för förfalskad programvara, vilket hjälper till att säkerställa att Microsofts kunder får den programvarukvalitet de förväntar sig. När programvaran är aktiverad, associeras en specifik produktnyckel med den dator (eller maskinvara) som programmet är installerat på. Associationen hindrar att produktnyckeln används för att aktivera samma kopia av programvaran på flera datorer. En del ändringar av datorns maskin- eller programvara kan kräva att du aktiverar om Windows. Aktiveringsfunktionen kan upptäcka och inaktivera aktiveringskryphål (programvara som kringgår eller förbigår Microsofts programvaruaktivering). Om det finns ett aktiveringskryphål kan det bero på att en program- eller maskinvaruleverantör har modifierat äkta Microsoft-programvara för att ta fram förfalskade kopior av programvaran. Aktiveringskryphål kan störa systemets normala drift.

Insamlad, bearbetad eller överförd information

Under aktiveringen skickas följande information till Microsoft:

- Microsoft-produktkoden (en femsiffrig kod som identifierar den Windows-produkt som du aktiverar).
- Ett kanal-ID eller en platskod som identifierar hur Windows-produkten ursprungligen erhölls. Ett kanal-ID eller en platskod identifierar till exempel om produkten ursprungligen köptes från en återförsäljare, införskaffades som en utvärderingsversion, införskaffades genom ett volymlicensprogram eller förinstallerades av en datortillverkare.
- Installationsdatumet och om installationen lyckades.
- Information som används för att bekräfta att Windows-

fjärrskrivbord

Logga in med ett Microsoft-konto

OneDrive-lagring i molnet

Inställningar för synkronisering

Teredo-teknik

TPM-tjänster (Trusted Platform Module)

Uppdatera rotcertifikat

Uppdateringstjänster

Virtuella privata nätverk

Windows Customer Experience Improvement Program (CEIP)

Windows Defender

Windows Felrapportering

Windows Filassociation

Hjälp om Windows

Fjärrhjälp

Windows Search

Installation av Windows

Windows Share

Windows SmartScreen

Windows Taligenkänning

Windows Store

Windows Time service

Windows Felsökning

produktnyckeln inte har ändrats.

- Datorns märke och modell.
- Versionsinformation för operativsystem och programvara.
- Nationella inställningar och språkinställningar.
- En unikt nummer som kallas GUID (global unik identifierare) som tilldelas datorn.
- Produktnyckel (hashkodad) och produkt-ID.
- BIOS-namn, versionsnummer och senaste ändringsdatum.
- Hårddiskvolymens serienummer (hashkodat).
- Resultatet av aktiveringskontrollen. Detta omfattar felkoder och information om eventuella aktiveringskryphål och relaterad skadlig eller ej auktoriserad programvara som har hittats eller inaktiverats:
  - ID:t för aktiveringskryphålet.
  - Aktiveringskryphålets aktuella status, t.ex. rensad eller i karantän.
  - Datortillverkarens ID.
  - Filnamn och hash för aktiveringskryphålet, samt hash för relaterade programvarukomponenter som kan tyda på att det finns ett aktiveringskryphål.
- Namn och hash för innehållet i datorns startinstruktionsfil. Om din Windows-licens är prenumerationsbaserad skickas också information om hur prenumerationen fungerar. Standardinformation om datorn skickas också.
- Om du har ett volymlicensierad exemplar av Windows som använder en aktiveringsserver kan serverns IP-adress skickas till Microsoft.

Användning av informationen

Microsoft använder informationen för att bekräfta att du har ett

licensierat exemplar av programvaran. Microsoft använder inte informationen för att kontakta enskilda konsumenter. Licensserverinformationen används för att kontrollera att licensservrarna följer tillämpliga licensavtal.

Val och kontroll

Aktivering är obligatoriskt och sker automatiskt när du installerar Windows. Om du inte har en giltig licens för programvaran kan du inte aktivera Windows.

Överst på sidan

Active Directory Rights Management Services (AD RMS) Client

Funktionens uppgift

Active Directory Rights Management Services (AD RMS) Client är en informationsskyddsteknik som fungerar med appar som har stöd för AD RMS och skyddar digital information mot obehörig användning. Ägare till digital information kan ange exakt hur mottagare ska få använda informationen i en fil, till exempel vem som kan öppna, ändra skriva ut eller utföra andra åtgärder med filen. Om du ska kunna skapa eller visa en fil med begränsad behörighet måste din dator köra en app med stöd för AD RMS och ha tillgång till en AD RMS-server.

Insamlad, bearbetad eller överförd information

AD RMS använder din e-postadress för att identifiera dig på en AD RMS-server. Det betyder att din e-postadress lagras på servern, och på din dator i licenser och identitetscertifikat som skapas av servern. Identitetscertifikat och licenser överförs till och från AD RMS-servrar när du försöker öppna, skriva ut eller utföra andra åtgärder i ett rättighetsskyddat dokument. Om din dator är ansluten till ett företagsnätverk brukar AD RMS-servern hanteras av företaget. Om du använder Windows Live AD RMS-tjänster hanteras servern av Microsoft. Information som skickas till Microsofts AD RMS-servrar krypteras för att skydda din integritet.

Användning av informationen

Med licensen kan du komma åt skyddade filer.

Identitetscertifikaten används för att identifiera dig på en AD RMS-server och gör att du kan skydda filer och komma åt skyddade filer.

Val och kontroll

Funktionerna i AD RMS måste vara aktiverade i en app med stöd för AD RMS. De är inte aktiverade som standard. Du kan välja att inte aktivera eller använda dem. Men om du inte aktiverar dem, kommer du inte att kunna komma åt skyddade filer.

Överst på sidan

Annonserings-ID

Funktionens uppgift

För att de ska kunna tillhandahålla mer relevanta annonser får apparna tillgång till ett unikt ID för varje användare på en enhet. Du kan återställa eller inaktivera åtkomsten till detta ID när du vill.

Insamlad, bearbetad eller överförd information

Om du tillåter att appar använder annonserings-ID:t får alla appar som begär ID:t tillgång till det. Appar kan lagra eller skicka denna information.

Användning av informationen

Ditt annonserings-ID används av apputvecklare och annonseringsnätverk för att leverera mer relevanta annonser baserat på vilka appar du använder och hur du använder dem. Det kan också användas av apputvecklare för att förbättra tjänstkvaliteten genom att de kan kontrollera annonsernas frekvens och effektivitet samt upptäcka bedrägerier och säkerhetsproblem.

Om du tillåter att appar använder annonserings-ID:t omfattas varje apps användning av ID:t av den appen sekretesspraxis.

Val och kontroll

Om du väljer standardinställningarna när du konfigurerar Windows kommer Windows att tillåta att appar använder ditt annonserings-ID. Om du väljer att anpassa inställningarna kan du hantera

åtkomsten till ditt annonserings-ID genom att välja **Låt appar använda mitt annonserings-ID för upplevelser i alla appar** under **Dela information med Microsoft och andra tjänster**. Efter installationen av Windows kan du ändra inställningen i **Sekretess** i Datorinställningar. Om du inaktiverar den här inställningen skickas inte annonserings-ID:t till appar som begär det. Om du väljer att aktivera inställningen igen genereras ett nytt ID.

Överst på sidan

Granskning

Med granskningsfunktionen kan en administratör konfigurera Windows att spara uppgifter om aktiviteter i operativsystemet i en säkerhetslogg som kan nås från Loggboken och andra appar. Med den här loggen kan administratören upptäcka obehörig åtkomst till datorn eller resurser på den. Med den här loggen kan administratörerna till exempel felsöka problem och ta reda på om någon har loggat in på datorn, skapat ett nytt användarkonto, ändrat en säkerhetsprincip eller öppnat ett dokument.

Insamlad, bearbetad eller överförd information

Administratörerna bestämmer vilka uppgifter som samlas in, hur länge de sparas och huruvida de skickas till någon annan. Informationen kan inbegripa personuppgifter, t.ex. användarnamn eller filnamn. Kontakta administratören om du vill ha mer information. Ingen information skickas till Microsoft.

Användning av informationen

Administratörerna bestämmer även hur granskningsinformationen används. I allmänhet används säkerhetsloggen av granskare och administratörer för att spåra aktiviteter på datorn eller för att identifiera obehörig åtkomst till datorn eller resurser på den.

Val och kontroll

Administratörerna bestämmer om den här funktionen är aktiverad och hur användarna meddelas. Andra användare kan inte se säkerhetsloggen om inte administratören ger dem tillgång till den.

Du kan konfigurera granskning på datorn genom att öppna Lokal säkerhetsprincip i Administrationsverktyg.

Överst på sidan

Biometri

Funktionens uppgift

Om datorn har en fingeravtryckläsare kan du använda ditt fingeravtryck för att logga in i Windows och för att identifiera dig i appar som stöder funktionen.

Insamlad, bearbetad eller överförd information

När du registrerar ett nytt fingeravtryck lagras avläsningarna av fingeravtrycket lokalt på datorn. Ingen information skickas till Microsoft. När du använder fingeravtryck för att identifiera dig i en app jämför Windows fingeravtrycket med de sparade fingeravtrycken på datorn och meddelar appen om det avlästa fingeravtrycket matchar ett fingeravtryck som associeras med ditt konto. Windows lämnar inte ut data om det avlästa fingeravtrycket till appen.

Användning av informationen

Windows använder fingeravtrycksinformationen som du väljer att spara på datorn för att logga in dig i Windows med ditt fingeravtryck.

Val och kontroll

Du kan lägga till och ta bort fingeravtryck i **Inloggningsalternativ** i **Konton** i Datorinställningar.

Överst på sidan

BitLocker-diskkryptering

Funktionens uppgift

BitLocker-diskkryptering skyddar dina data genom att kryptera dem så att obehöriga användare inte får åtkomst till dem. När BitLocker är aktiverat på en enhet som stöds krypterar Windows

informationen på enheten.

Insamlad, bearbetad eller överförd information

Om BitLocker är aktiverat med programvarukryptering krypteras och dekrypteras informationen av kryptografiska nycklar i minnet när den läses från eller skrivs till den skyddade enheten. Om BitLocker är aktiverat med maskinvarukryptering sköter enheten krypteringen och dekrypteringen av alla data.

Under installationen av BitLocker kan du välja att skriva ut en återställningsnyckel eller spara den på en plats i nätverket. Om du konfigurerar BitLocker på en fast enhet kan du även spara återställningsnyckeln på ett USB-flashminne.

Om datorn inte tillhör en domän kan du säkerhetskopiera BitLocker-återställningsnyckeln, återställningsnyckelns ID och datorns namn till MicrosoftOneDrive. Information skickas krypterad via SSL för att skydda din integritet.

Du kan konfigurera BitLocker att kryptera data med ett certifikat som lagras på ett smartkort. När du skyddar en dataenhet med ett smartkort, lagras smartkortets offentliga nyckel och unika identifierare okrypterade på enheten. Den här informationen kan användas för att hitta certifikat som användes för att generera smartkortets krypteringscertifikat.

Om datorn har säkerhetsmaskinvara med minst version 1.2 av TPM (Trusted Platform Module) använder BitLocker TPM för att skydda data på enheten där Windows är installerat med hjälp av maskinvara. Mer information finns i avsnittet om Trusted Platform Module (TPM) Services. På datorer med TPM kan du även skapa en PIN-kod och på så sätt skydda krypterade data ännu bättre. BitLocker sparar den här TPM-baserade PIN-koden i hashat och krypterat format på enheten.

Informationen som samlas in av BitLocker skickas inte till Microsoft såvida du inte väljer att säkerhetskopiera återställningsnyckeln till OneDrive.

Användning av informationen

Kryptografiska nycklar och globalt unika identifierare (GUID) lagras

i datorns minne för användning i samband med BitLocker-åtgärder. Återställningsinformationen i BitLocker gör att du kan komma åt dina skyddade data om maskinvaran går sönder eller om något annat problem uppstår. Med den här återställningsinformationen kan BitLocker skilja mellan obehöriga och behöriga användare.

Microsoft använder inte dina enskilda återställningsnycklar för något ändamål. När återställningsnycklar skickas till OneDrive kan Microsoft använda samlade uppgifter om dem för att analysera trender och förbättra sina produkter och tjänster.

Val och kontroll

BitLocker är inaktiverat som standard. På en flyttbar enhet kan vilken användare som helst inaktivera eller aktivera BitLocker när de vill genom att öppna BitLocker-diskkryptering på Kontrollpanelen. En administratör kan aktivera eller inaktivera BitLocker för alla enheter.

Du kan visa och hantera återställningsnycklarna som lagras i ditt OneDrive-konto.

Överst på sidan

Kontakter

Funktionens uppgift

Om du använder appen Kontakter eller en app från tredje part som stöds för att hantera dina kontakter kan du välja att dela vissa kontakter med andra appar på din dator, visa kontaktinformation på ett kontaktkort eller dela viss kontaktinformation med andra appar på datorn för att utföra en åtgärd, till exempel att ringa ett samtal eller kartlägga en adress.

Insamlad, bearbetad, lagrad och överförd information

När en app begär kontaktinformation gör Windows det möjligt att välja vissa kontakter som ska delas med appen. Kontakterna kan komma från appen Kontakter eller en kontaktinformationsapp från tredje part som stöds. Windows delar inte hela din kontaktlista med den begärande appen.

Om en app har åtkomst till viss information om någon av dina

kontakter, till exempel ett telefonnummer eller en e-postadress, kan Windows visa ett kontaktkort med den ytterligare informationen för den kontakten från kontaktinformationsappen. Windows delar inte den ytterligare kontaktinformationen med appen som visar kontaktkortet.

Om du trycker eller klickar på ett kommando, till exempel **Samtal**, **E-post**eller **Karta** , på kontaktkortet öppnar Windows lämplig app för att utföra den åtgärden och tillhandahåller den kontaktinformation som krävs för att slutföra åtgärden, till exempel telefonnumret som ska ringas.

Användning av informationen

Windows använder kontaktinformationen från appen Kontakter för att dela vissa kontakter som du väljer, visa kontaktkort, öppna appar och dela kontaktinformation för att utföra åtgärder som anges på kontaktkorten, samt för att visa dina kontakter i Windows Search. Appen Kontakter använder information om dina kontakter på det sätt som beskrivs i Sekretesspolicy för kommunikationsappar.

Om du delar kontaktinformation med en app från tredje part kommer användning av informationen regleras av den tredje partens sekretesspraxis. Om du delar kontaktinformation med en Microsoft-app förklaras appens sekretesspraxis i appens sekretesspolicy.

Val och kontroll

Windows visar och delar kontaktinformation endast när du väljer att dela vissa kontakter med en app, visa ett kontaktkort eller väljer en åtgärd från kontaktkortet.

Överst på sidan

Enhetsidentifiering och konfiguration

Windows innehåller flera funktioner som hjälper dig att identifiera och konfigurera enheter på datorn, t.ex. funktioner för enhetsinstallation, installation av mobila bredbandsenheter, nätverksidentifiering och koppling av trådlösa enheter.

Enhetsinstallation

Funktionens uppgift

När en ny enhet installeras på datorn kan Windows automatiskt söka efter, ladda ned och installera enhetens drivrutin. Windows kan också ladda ned information om enheten, t.ex. beskrivning, bild och tillverkarens logotyp. En del enheter, t.ex. vissa skrivare, webbkameror, mobila bredbandsenheter och bärbara enheter som synkroniseras med Windows, har en app som optimerar enhetens funktionalitet och användarupplevelse. Om enhetstillverkaren tillhandahåller en app för enheten kan Windows automatiskt ladda ned och installera appen från Windows Store om du är inloggad där.

Insamlad, bearbetad eller överförd information

När Windows söker efter drivrutiner kontaktas tjänsten Windows Update för att den ska leta reda på och ladda ned enhetsdrivrutiner, om det inte redan finns en lämplig drivrutin på datorn. Mer information om informationen som samlas in av Windows Update och hur den används finns i sekretesspolicyn för uppdateringstjänsterna.

För att kunna hämta information om din enhet och avgöra om det finns en app för enheten skickar Windows data om enheten till Microsoft, bland annat enhets-ID (exempelvis maskinvaru-ID eller modell-ID för den enhet som du använder), dina nationella inställningar och språkinställningar samt datumet då enhetsinformationen senast uppdaterades. Om det finns en enhetsapp laddar Windows ned och installerar den automatiskt från Windows Store. Appen är tillgänglig på ditt Windows Store-konto i listan med appar som du äger.

Användning av informationen

Den information som skickas till Microsoft används för att fastställa och ladda ned lämplig enhetsdrivrutin, enhetsinformation och enhetsapp. Microsoft använder inte informationen som skickas för att identifiera eller kontakta dig.

Val och kontroll

Om du väljer standardinställningar medan du konfigurerar

Windows aktiverar du automatiskt nedladdning och installation av enhetsdrivrutiner, enhetsinformation och enhetsappar. Om du väljer att anpassa inställningar kan du kontrollera automatiskt nedladdning och installation av enhetsdrivrutiner, appar och information genom att markera **Hämta enhetsdrivrutiner, appar och information om nya enheter automatiskt** under **Skydda och uppdatera datorn**. Efter installationen av Windows kan du ändra dessa inställningar på Kontrollpanelen genom att välja Ändra installationsinställningarna för enheten och sedan **Nej, jag väljer själv vad som ska göras**.

Du kan när som helst avinstallera en enhetsapp utan att avinstallera enheten, även om du kanske behöver appen för att kunna använda vissa av enhetens funktioner. Du kan installera om en enhetsapp efter det att du har avinstallerat den genom att gå till listan med appar som du äger i Windows Store.

Installation av en mobil bredbandsenhet

Funktionens uppgift

Om datorn är utrustad med maskinvara för mobilt bredband från en mobiloperatör kan Windows automatiskt ladda ned och installera en app som hjälper dig att hantera ditt konto och ditt avtal med mobiloperatören som du erhöll maskinvaran från. Ytterligare information om enheten laddas också ned för att visa den mobila bredbandsanslutningen i nätverkslistan.

Insamlad, bearbetad eller överförd information

För att avgöra vilken enhetsinformation och enhetsapp som ska laddas ned skickar Windows en del av maskinvaruidentifierarna från maskinvaran för det mobila bredbandet. Dessa maskinvaru-ID:n hjälper oss att identifiera din mobiloperatör. För att skydda din integritet skickas inte de fullständiga identifierarna till Microsoft.

Om din mobiloperatör har registrerat en app hos Microsoft laddar Windows ned appen från Windows Store och installerar den. När du öppnar appen efter att den har installerats har den åtkomst till maskinvaran för det mobila bredbandet, inklusive till unika maskinvaru-ID:n som mobiloperatören kan använda för att identifiera ditt konto.

Användning av informationen

Microsoft använder den del av identifieraren från maskinvaran för det mobila bredbandet som Windows skickar för att ta reda på vilken operatörs app som ska installeras på datorn. När appen har installerats kan den använda det mobila bredbandets maskinvaru-ID:n. En mobiloperatörs app skulle till exempel kunna använda dessa identifierare för att hämta information om kontot och avtalet på nätet. Appens användning av dessa uppgifter regleras av mobiloperatörens sekretesspolicy.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows kommer Windows automatiskt att söka efter och ladda ned appar från mobiloperatören. Du kan aktivera eller inaktivera den här funktionen på Kontrollpanelen. Mer information finns i avsnittet Installera enhet ovan.

Du kan när du vill avinstallera en mobiloperatörs app utan att avinstallera maskinvaran för det mobila bredbandet.

Nätverksidentifiering

Funktionens uppgift

När du ansluter datorn till ett litet privat nätverk, som du kanske har hemma, kan Windows automatiskt identifiera andra datorer och delade enheter i nätverket och göra datorn synlig för de andra datorerna i nätverket. Om det finns delade enheter kan Windows ansluta till och installera dem automatiskt. Exempel på delade enheter är skrivare och utökningsenheter för medier, men inte personliga enheter som kameror och mobiltelefoner

Insamlad, bearbetad eller överförd information

När du aktiverar delning och anslutning till enheter kan information om din dator, t.ex. datorns namn och nätverksadress, sändas ut i det lokala nätverket så att andra datorer kan hitta och ansluta till den.

Viss information om nätverket samlas in och skickas till Microsoft för att ta reda på om enheterna som är anslutna till nätverket ska installeras automatiskt. Informationen gäller antalet enheter i

nätverket, nätverkstypen (t.ex. ett privat nätverk) och nätverksenheternas typer och modellnamn. Ingen personlig information samlas in, t.ex. nätverksnamnet eller lösenordet

Beroende på inställningarna för enhetsinstallation kan Windows skicka viss information till Microsoft och installera enhetsprogramvara på datorn när delade enheter installeras. Mer information finns i avsnittet Installera enhet.

Användning av informationen

Informationen som skickas till Microsoft om nätverket används för att ta reda på vilka nätverksenheter som ska installeras automatiskt. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer att aktivera delning och ansluta till enheter när du ansluter till ett nätverk, aktiveras nätverksidentifiering för det nätverket. Du kan ändra den här inställningen för det aktuella nätverket genom att klicka på nätverkstypen som anges under nätverkets namn i Nätverks- och delningscenter.

Du kan välja om du över huvud taget vill aktivera nätverksidentifiering och huruvida nätverksanslutna enheter ska konfigureras automatiskt genom att välja **Ändra avancerade delningsinställningar** i Nätverks- och delningscenter.

Koppling av trådlösa enheter

Funktionens uppgift

I Windows kan du para ihop datorn med trådlösa enheter som använder Bluetooth eller Wi-Fi Direct. Wi-Fi Direct är en trådlös teknik som ger enheterna möjlighet att kommunicera direkt med varandra utan att behöva ansluta till ett Wi-Fi-nätverk.

Insamlad, bearbetad eller överförd information

Om du markerar **Tillåt att Bluetooth-enheter upptäcker den här datorn** i Bluetooth-inställningar skickar Windows ut datorns namn via Bluetooth så att enheter som stöder Bluetooth kan hitta och identifiera datorn.

Om du markerar **Lägg till en enhet** i Enheter i Datorinställningar skickar Windows ut datorns namn via Wi-Fi så att enheter som stöder Wi-Fi Direct kan hitta och identifiera den. När du stänger **Lägg till en enhet**slutar Windows att skicka datorns namn via Wi-Fi.

Beroende på inställningarna för enhetsinstallation kan Windows skicka viss information till Microsoft och installera enhetsprogramvara på datorn när Windows paras ihop med trådlösa enheter. Mer information finns i avsnittet Installera enhet ovan.

Användning av informationen

Windows skickar ut datorns namn så att andra enheter kan identifiera och ansluta till datorn. Datorns namn skickas inte till Microsoft.

Val och kontroll

Om du vill välja huruvida Windows ska skicka ut datorns namn via Bluetooth kan du trycka och hålla ned eller högerklicka på datorn i Enheter och skrivare på Kontrollpanelen, välja **Bluetooth-inställningar**och sedan välja **Tillåt att Bluetooth-enheter upptäcker den här datorn**. Om du inte vill att Windows ska skicka ut datorns namn via Wi-Fi när du lägger till enheter kan du temporärt inaktivera Wi-Fi i Trådlöst i Datorinställningar innan du lägger till en enhet.

Överst på sidan

Enhetskryptering

Funktionens uppgift

Enhetskryptering hjälper till att skydda dina data genom att kryptera dem med BitLocker-diskkrypteringsteknik, vilken kan förhindra offlineangrepp från program. När du aktiverar enhetskryptering krypterar Windows data på den enhet som Windows är installerat på.

Insamlad, bearbetad eller överförd information

När du använder programvarukryptering krypteras och dekrypteras

informationen av kryptografiska nycklar i minnet medan den läses från eller skrivs till den skyddade enheten. När du använder maskinvarukryptering utföras datakrypteringen och datadekrypteringen av enheten.

Windows använder TPM (Trusted Platform Module) på datorn för att lagra och hantera de kryptografiska nycklarna som används för att kryptera enheten. När enhetskryptering är aktiverat krypterar Windows automatiskt den enhet som Windows är installerat på och genererar en återställningsnyckel. Återställningsnyckeln hjälper dig att komma åt dina skyddade data om maskinvaran går sönder eller om något annat problem uppstår.

BitLocker-återställningsnyckeln för datorn säkerhetskopieras automatiskt online i MicrosoftOneDrive-kontot för varje administratörskonto som är kopplat till ett Microsoft-konto. Datorns namn och en identifierare för återställningsnyckeln säkerhetskopieras också i samma OneDrive-konto. Information skickas krypterad via SSL för att skydda din integritet.

Användning av informationen

Kryptografiska nycklar och globalt unika identifierare (GUID) lagras i datorns minne för användning i samband med BitLocker-åtgärder. Återställningsinformation kan användas för att komma åt skyddade data i händelse av vissa maskinvaruproblem eller andra fel och gör att BitLocker kan skilja mellan behöriga och obehöriga användare.

Microsoft säkerhetskopierar din återställningsinformation i ditt OneDrive-konto så att du kan komma åt den online. Vi använder inte återställningsinformation och lagrar den inte någon annanstans än i OneDrive-kontot. Vi använder kanske insamlade data om återställningsnycklar till att analysera trender och förbättra våra produkter och tjänster. Vi kan till exempel använda informationen för att avgöra i vilken omfattning Enhetskryptering är aktiverat på datorer.

Val och kontroll

Om du väljer att använda ett Microsoft-konto när du konfigurerar datorn, och om datorn stöder det, aktiveras enhetskryptering och din återställningsnyckel säkerhetskopieras i ditt OneDrive-konto.

Om du väljer att använda ett lokalt konto när du konfigurerar datorn är enhetskryptering inaktiverat.

Om du senare kopplar ett Microsoft-konto till ett administratörskonto på din dator:

- Om enhetskryptering inte redan är aktiverat i Windows aktiveras funktionen automatiskt och återställningsinformationen säkerhetskopieras till användarens OneDrive-konto.
- Om enhetskryptering redan är aktiverat säkerhetskopieras datorns återställningsinformation till användarens OneDrive-konto.

Du kan visa och hantera återställningsnycklarna som lagras i ditt OneDrive-konto här.

Överst på sidan

DirectAccess

Funktionens uppgift

Med DirectAccess kan din dator ansluta till nätverket på arbetsplatsen utan att du behöver göra något när datorn är ansluten till Internet, oavsett var du befinner dig.

Insamlad, bearbetad eller överförd information

Varje gång du startar datorn försöker DirectAccess ansluta till nätverket på din arbetsplats, oavsett om du är där eller inte. När du är ansluten laddar datorn ned principerna för arbetsplatsen och du kan då komma åt konfigurerade resurser i nätverket på arbetsplatsen. Administratören kanske använder DirectAccess-anslutningar för att hantera och övervaka din dator på distans, däribland de webbplatser du besöker även om du inte är på jobbet.

DirectAccess skickar ingen information till Microsoft.

Användning av informationen

Ditt företags policy avgör hur information som administratören på

arbetsplatsen samlar in används.

Val och kontroll

DirectAccess måste konfigureras av administratören på arbetsplatsen med Grupprincip. Administratören kan tillåta dig att tillfälligt inaktivera vissa element i DirectAccess, men det är bara administratören på arbetsplatsen som kan hindra Windows från att försöka ansluta till arbetsplatsen för hanteringsändamål. Om du eller administratören på arbetsplatsen tar bort din dator från arbetsplatsens domän, kan DirectAccess inte längre ansluta.

Överst på sidan

Hjälpmedelscenter

Funktionens uppgift

I Hjälpmedelscenter kan du aktivera hjälpmedelsalternativ och hjälpmedelsinställningar som gör det lättare att använda datorn.

Insamlad, bearbetad eller överförd information

Om du använder den här funktionen uppmanas du att välja lämpliga påståenden.

Exempel på påståenden:

- Det är svårt att se bilder och text på TV.
- Ljusförhållandena gör det svårt att se bilder på skärmen.
- Jag använder inte tangentbord.
- Jag är blind.
- Jag är döv.
- Jag har ett talfel.

Informationen sparas i ett icke-läsbart format och lagras lokalt på datorn.

Användning av informationen

Du får ett antal rekommendationer om konfigurationer med

ledning av vilka påståenden du valde. Informationen skickas inte till Microsoft och är inte tillgänglig för någon annan användare än du själv och administratörerna på datorn.

Val och kontroll

Du kan välja vilka påståenden som du vill markera genom att gå till Hjälpmedel på Kontrollpanelen. Du kan när som helst ändra dina val. Du kan även välja vilka av rekommendationerna som du vill använda på datorn.

Överst på sidan

Loggboken

Funktionens uppgift

Datoranvändare – huvudsakligen administratörer – kan se och hantera händelseloggar i Loggboken. Händelseloggar innehåller information om maskinvaru-, program- och säkerhetshändelser på datorn. Du kan även få information om händelser i händelseloggarna från Microsoft genom att klicka på Onlinehjälp för händelseloggen.

Insamlad, bearbetad eller överförd information

Händelseloggar innehåller information om händelser som har genererats av alla användare och appar på datorn. Som standard kan alla användare se poster i händelseloggen, men administratörerna kan välja att begränsa tillgången till händelseloggarna. Du kan komma åt datorns händelseloggar genom att öppna Loggboken. Information om hur du öppnar Loggboken finns i Windows Hjälp och support.

Om du använder Onlinehjälp för händelseloggen för att söka efter mer information om en viss händelse skickas informationen om händelsen till Microsoft.

Användning av informationen

När du använder Onlinehjälp för händelseloggen för att söka efter information om en händelse, används händelseinformationen som skickas från datorn för att leta efter och ge dig mer information om händelsen. För Microsoft-relaterade händelser skickas

händelseinformationen till Microsoft. Microsoft använder inte den här informationen för att identifiera, kontakta eller skicka reklam till dig. För händelser som hör till andra leverantörers appar skickas informationen till den plats som utgivaren eller tillverkaren har angett. Om du skickar information om händelser till externa utgivare eller tillverkare är bruket av informationen underställt den tredje partens sekretesspolicy.

Val och kontroll

Administratörer kan välja att begränsa tillgången till loggarna i Loggboken. Användare med fullständig åtkomst till loggarna i Händelseloggen kan tömma dem. Om du inte tidigare har godkänt att händelseinformation skickas automatiskt, ombeds du att bekräfta att informationen som visas får skickas via Internet när du klickar på Onlinehjälp för händelseloggen. Ingen händelseinformation skickas via Internet om du inte ger ditt tillstånd till det. Administratörer kan använda Grupprincip för att välja eller ändra webbplatsen dit händelseinformationen skickas.

Överst på sidan

Family Safety

Funktionens uppgift

Family Safety hjälper föräldrar att skydda sina barn när de använder en dator. Föräldrar kan styra vilka appar, spel och webbplatser som barnen kan använda. Föräldrar kan även ange tidsgränser och få regelbundna aktivitetsrapporter via e-post. Föräldrar kan hantera begränsningar och visa aktivitetsrapporter lokalt på datorn eller online på webbplatsen för Microsoft Family Safety.

Insamlad, bearbetad eller överförd information

Family Safety-inställningarna och Family Safety-rapporterna över barnens aktivitet lagras på datorn. Aktivitetsrapporter kan innehålla information om hur lång tid barnen använt datorn, hur lång tid de använt enskilda appar och spel samt vilka webbplatser de besökt (även försök att visa blockerade webbplatser). Administratörer på datorn kan ändra inställningarna och visa aktivitetsrapporten.

Om onlinehantering aktiveras för ett barnkonto kan föräldrarna visa barnets aktivitetsrapport och ändra inställningarna för barnet på webbplatsen för Microsoft Family Safety. En förälder kan tillåta andra personer att visa aktivitetsrapporter och ändra inställningar genom att lägga till dem som föräldrar på webbplatsen för Microsoft Family Safety. Om föräldern som konfigurerar Family Safety är inloggad i Windows med ett Microsoft-konto aktiveras onlinehantering automatiskt.

När Family Safety konfigureras för ett barnkonto och onlinehantering är aktiverat, skickas veckorapporter om barnets aktivitet automatiskt till föräldern via e-post.

Användning av informationen

Windows och webbplatsen för Microsoft Family Safety använder informationen som samlas in för att tillhandahålla Family Safety-funktionen. Microsoft kan analysera informationen i aktivitetsloggar i samlat format för att kontrollera informationens kvalitet, men använder inte den här informationen för att identifiera, kontakta eller skicka reklam till enskilda användare.

Val och kontroll

Family Safety-funktionen är inaktiverad som standard. Du kommer åt Family Safety genom att öppna Family Safety på Kontrollpanelen. Endast administratörer kan aktivera Family Safety och endast användare utan administrativ behörighet kan övervakas eller begränsas. Barn kan se sina inställningar, men kan inte ändra dem. Om Family Safety är aktiverat får barnet ett meddelande om att Family Safety övervakar barnets konto varje gång han eller hon loggar in i Windows. Om du anger att ett konto är ett barnkonto när du skapar kontot, kan du välja att aktivera Family Safety för kontot.

Om administratören som skapar ett barns konto är inloggad i Windows med ett Microsoft-konto aktiveras onlinehantering automatiskt och rapporter om barnets aktivitet skickas varje vecka. Föräldrakonton kan läggas till eller tas bort på webbplatsen för Microsoft Family Safety. Alla som har lagts till som en förälder på webbplatsen kan visa ett barns aktivitetsrapport och ändra barnets

Family Safety-inställningar, även om föräldern inte är en administratör på den dator som barnet använder.

Vi rekommenderar att endast föräldrar är administratörer på datorn och att barn inte beviljas administrativ behörighet. Observera att användningen av den här funktionen för att övervaka andra användare (t.ex. vuxna) kan strida mot gällande lagstiftning.

Överst på sidan

Fax

Funktionens uppgift

Med faxfunktionen kan du skapa och spara faxförsättsblad och skicka eller ta emot fax med din dator och ett externt eller inbyggt faxmodem eller en faxserver.

Insamlad, bearbetad eller överförd information

Informationen som samlas in är de personuppgifter som anges på faxets försättsblad samt de identifierare som finns i branschens standardfaxprotokoll, t.ex. TSID (Transmitting Subscriber ID) och CSID (Call Subscriber ID). Som standard använder Windows "Fax" som värde för alla identifierare.

Användning av informationen

Informationen som anges i dialogrutan vid avsändning visas på faxets försättsblad. Identifierare som TSID och CSID kan innehålla godtycklig text och brukar användas av den mottagande faxen eller datorn för att identifiera avsändaren. Ingen information skickas till Microsoft.

Val och kontroll

Faxåtkomsten bestäms av dina kontobehörigheter på datorn. Om inte en faxadministratör ändrar åtkomstinställningarna, kan alla användare skicka och ta emot fax. Som standard kan alla användare visa dokumenten som de skickar och alla fax som tas emot på datorn. Administratörer kan se alla faxade dokument, skickade som mottagna, och kan ange faxinställningar, däribland vilka som har behörighet att visa eller hantera fax, samt TSID- och CSID-värdena.

Överst på sidan

Anpassa handskrift – automatisk inlärning

Funktionens uppgift

Automatisk inlärning är ett verktyg i Anpassa handskrift som är tillgänglig på pekdatorer eller datorer med en Tablet PC-penna. Den här funktionen samlar in data om vilka ord du använder och hur du skriver dem. Detta hjälper programmet för handskriftsigenkänning att förbättra tolkningen av din handstil och de ord du använder, och förbättrar även autokorrigerings- och textförslagen för språk utan någon IME (input method editor).

Insamlad, bearbetad eller överförd information

Informationen som samlas in av funktionen för automatisk inlärning lagras i varje användares användarprofil på datorn. Informationen lagras i ett särskilt format som inte kan läsas med en textvisningsapp (t.ex. Anteckningar eller WordPad) och är bara tillgänglig för andra användare om de är administratörer på din dator.

Den insamlade informationen innehåller bland annat följande:

- Text från meddelanden som du skriver och kalenderuppgifter som du skapar i e-postappar (t.ex. Office Outlook eller Windows Live E-post), inklusive meddelanden som du redan har skickat.
- Pennanteckningar som du skriver i Inmatningspanelen.
- Text som känns igen från pennanteckningar som du skriver i Inmatningspanelen eller som du skriver med ett pektangentbord.
- Alternativa tecken som du väljer när du rättar den igenkända texten.

Användning av informationen

Informationen som samlas in används för att förbättra igenkänningen av handstilen genom att en version av

igenkänningsprogrammet skapas som är anpassad till din handstil och ditt vokabulär. Detta används även för automatisk korrigering och textförslag när du skriver på ett pektangentbord.

Textexemplen används för att skapa en utökad ordlista. Pennanteckningsexemplen används för att förbättra handskriftsigenkänningen för varje datoranvändare. Ingen information skickas till Microsoft.

Val och kontroll

Automatisk inlärning är aktiverat som standard. Du kan när som helst aktivera eller inaktivera automatisk inlärning genom att öppna **Avancerade inställningar** i **Språk** på Kontrollpanelen. När du inaktiverar automatisk inlärning tas alla data som har samlats in och sparats med automatisk inlärning bort.

Överst på sidan

Hemgrupp

Funktionens uppgift

I Windows kan du enkelt koppla samman datorer i hemnätverket så att du kan dela bilder, musik, video, dokument och enheter. Datorerna kan även strömma media till enheter i hemnätverket, t.ex. en media extender-enhet. Dessa datorer och enheter bildar din hemgrupp. Du kan skydda hemgruppen med ett lösenord och du kan välja vad du vill dela.

Insamlad, bearbetad eller överförd information

Du kan komma åt dina filer, t.ex. bilder, videor, musik och dokument, från vilken dator som helst i hemgruppen. När du ansluter till en hemgrupp delas kontoinformation (t.ex. e-postadress, visningsnamn och bild) för alla Microsoft-konton på datorn med andra i hemgruppen så att delning kan aktiveras med dessa användare.

Användning av informationen

Informationen som samlas in gör det möjligt för datorerna i hemgruppen att ta reda på vilka de ska dela innehåll med och hur

det ska presenteras. Ingen information skickas till Microsoft.

Val och kontroll

Du kan lägga till och ta bort datorer från hemgruppen och bestämma vad som ska delas med de övriga medlemmarna av hemgruppen. Du kan skapa en hemgrupp och hantera gruppens inställningar genom att gå till **Hemgrupp** under **Nätverk** i Datorinställningar.

Överst på sidan

Input Method Editor (IME)

Microsofts IME:er (Input Method Editors) används med östasiatiska språk för att omvandla tecken som skrivs på tangentbordet till ideogram. I det här avsnittet beskrivs flera funktioner, t.ex. automatisk justering och förutsägelse, rapporter om IME-konverteringsfel och registrering av IME-ord.

Molnbaserade IME-kandidater

Funktionens uppgift

När du använder Microsoft Pinyin IME för att ange förenklade kinesiska tecken kan IME använda en onlinetjänst för att leta efter kandidatideogram för en inmatning som inte finns i en lokal ordlista på datorn.

Insamlad, bearbetad eller överförd information

Medan du skriver förenklade kinesiska tecken med Microsoft Pinyin IME ger IME förslag på ideogram som du kanske vill använda. Om IME inte kan hitta ett bra förslag i din lokala ordlista skickar den tangentbordsinmatningen till Microsoft för att se om det finns bättre kandidatideogram för den inmatningen. Om det finns det visas de i listan över kandidater, och om de blir valda läggs de till i den lokala ordlistan. En slumpmässigt framtagen unik identifierare skickas också med för att vi ska kunna analysera hur den här funktionen används. Identifieraren associeras inte till ditt Microsoft-konto, och används inte för att identifiera, kontakta eller skicka reklam till dig.

Användning av informationen

Microsoft använder den insamlade informationen för att leta upp ideogram i molnet och för att förbättra sina produkter och tjänster. Vi använder den inte för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Molnbaserade IME-kandidater är inaktiverade som standard för Microsoft Pinyin IME för förenklad kinesiska. Öppna Datorinställningar, klicka på **Tid och språk**, **Region och språk**, välj ditt språk och klicka sedan på **Alternativ**.

Automatisk justering och förutsägelse

Funktionens uppgift

Beroende på vilken IME du använder, och dina inställningar, kan dess funktioner för automatisk justering och textförslag spara ord eller ordsekvenser för att förbättra urvalet av de ideogram som visas.

Insamlad, bearbetad eller överförd information

Funktioner för automatisk justering (inlärning) och textförslag sparar ett ord eller en ordsekvens och hur ofta du använder dem. Information för automatisk justering (med undantag av följer av siffror/symboltecken) lagras i filer för varje datoranvändare.

Användning av informationen

Data om automatisk inlärning och textförslag används av IME:n på datorn för att förbättra urvalet av de ideogram som visas när du använder IME:n. Om du väljer att skickas dessa data till Microsoft används de för att förbättra IME:n och relaterade produkter och tjänster.

Val och kontroll

Funktionerna för automatisk inlärning och textförslag är på som standard i de IME:er som stöder dem. De data som samlas in skickas inte automatiskt till Microsoft. Du kan välja om du vill samla in och skicka dessa data i Språk på Kontrollpanelen.

Rapporter om IME-konverteringsfel

Funktionens uppgift

Om fel uppstår då ideogram visas eller då inmatningar från tangentbordet konverteras kan denna funktion samla in information om felen som kan hjälpa Microsoft att förbättra sina produkter och tjänster.

Insamlad, bearbetad eller överförd information

Rapporterna om IME-konverteringsfel innehåller information om IME-konverteringsfel, t.ex. vad du skrev, det första konverterings- eller förutsägelseresultatet, den sträng du valde i stället, information om den IME du använde och information om hur du använde den. Om du råkar använda IME:n för japanska kan du dessutom välja att ta med information om automatisk inlärning i konverteringsfelrapporterna.

Användning av informationen

Microsoft använder informationen för att förbättra sina produkter och tjänster. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Efter att ett visst antal konverteringsfel har lagrats frågar rapportverktyget för felaktiga konverteringar om du vill skicka en konverteringsfelrapport. Du kan även välja att skicka en konverteringsfelrapport när som helst från rapportverktyget för felaktiga konverteringar. Du kan visa informationen i varje rapport innan du väljer att skicka den. Du kan även välja att skicka konverteringsfelrapporterna automatiskt i IME-inställningar.

Registrering av IME-ord

Funktionens uppgift

Beroende på vilken IME du använder, kanske du kan använda ordregistrering för att rapportera ord som inte stöds (ord som kanske inte konverteras korrekt till ideogram vid inmatning från tangentbordet).

Insamlad, bearbetad eller överförd information

Registreringsrapporter kan innehålla den information som du vill lägga till i dialogrutan Lägg till ord om de ord som rapporteras

samt versionsnumret för en IME. Dessa rapporter kan innehålla personlig information exempelvis om du lägger till personnamn med hjälp av ordregistrering. Du får tillfälle att granska informationen som skickas i rapporterna innan du väljer att skicka dem.

Användning av informationen

Microsoft använder informationen för att förbättra sina produkter och tjänster. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Varje gång du skapar en ordregistreringsrapport får du en fråga om du vill skicka den till Microsoft. Du kan visa informationen i rapporten innan du väljer att skicka den.

Överst på sidan

Internetanslutningsdelning

Funktionens uppgift

Med Internetanslutningsdelning kan du dela det mobila bredbandets Internetanslutning med andra enheter via Wi-Fi. Du kan också fjärrstarta Internetanslutningsdelning på den mobila bredbandsenheten från datorn om du är inloggad på båda med samma Microsoft-konto.

Insamlad, bearbetad eller överförd information

Första gången du delar din Internetanslutning genererar och sparar Windows automatiskt ett nätverksnamn och lösenord. Du kan ändra dessa när du vill.

Om datorn stöder det och om du har lagt till datorn till ditt Microsoft-konto som en betrodd enhet synkroniserar Windows nätverksnamnet och lösenordet med ditt Microsoft-konto. Windows synkroniserar också övrig information så att du kan fjärrstarta Internetanslutningsdelning från dina andra betrodda enheter. Den här informationen omfattar Bluetooth-radions maskinvaruadress och ett slumptal som används för att skydda anslutningen.

Användning av informationen

Den här informationen används för att konfigurera Internetanslutningsdelning. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du loggar in på en enhet som stöder Internetanslutningsdelning med ditt Microsoft-konto, och om du lägger till enheten som en betrodd enhet, synkroniseras informationen som krävs för att fjärrstarta Internetanslutningsdelning med OneDrive. Du kan stoppa synkroniseringen av informationen genom att välja att inte synkronisera lösenord. Mer information finns i avsnittet Inställningar för synkronisering på den här sidan.

Överst på sidan

Internetutskrift

Funktionens uppgift

Med Internetutskrift kan du skriva ut via Internet.

Insamlad, bearbetad eller överförd information

När du skriver ut med den här funktionen måste du först ansluta och autentisera dig för en utskriftsserver på Internet. Informationen som du måste ge till utskriftsservern beror på vilken säkerhetsnivå som utskriftsservern stöder (du kan t.ex. behöva ange ett användarnamn och ett lösenord). När du är ansluten visas en lista med kompatibla skrivare. Om din dator saknar en skrivardrivrutin för den valda skrivaren, kan du välja att ladda ned en drivrutin från utskriftsservern. Eftersom utskriftsjobben inte krypteras kan andra se innehållet som skickas.

Användning av informationen

Informationen som samlas in gör att du kan skriva ut på fjärrskrivare. Om du väljer att använda en utskriftsserver som Microsoft är värd för, använder vi inte den information som du uppger för att identifiera, kontakta eller skicka reklam till dig. Om du skickar information till en extern leverantörs utskriftsserver

regleras användningen av informationen av leverantörens sekretesspolicy.

Val och kontroll

Du kan aktivera eller inaktivera Internetutskrifter genom att öppna **Program och funktioner** på Kontrollpanelen och sedan välja **Aktivera eller inaktivera Windows-funktioner**.

Överst på sidan

Språkinställningar

Vad den här funktionen åstadkommer

Du kan lägga till de språk du föredrar att använda i språklistan i Windows 8.1. Appar och webbplatser visas på det första tillgängliga språket i listan.

Insamlad, bearbetad eller överförd information

När du besöker webbplatser och installerar appar på din dator, skickas listan med föredragna språk till webbplatserna du besöker och är tillgänglig för apparna du använder, så att de kan visa innehåll på de språk du föredrar.

Användning av informationen

Listan med prioriterade språk används av Microsofts webbplatser och appar för att tillhandahålla innehåll på det språk som du föredrar. Microsoft använder inte någon språkinformation för att identifiera eller kontakta dig. Språkinformation som skickas eller används av externa webbplatser och appar är underställda den externa webbplatsens eller apputgivarens sekretesspolicy.

Val och kontroll

Din lista med de språk du föredrar är tillgänglig för de appar du installerar och de webbplatser du besöker. Du kan lägga till och ta bort språk från den här listan i Språkinställningar på Kontrollpanelen. Om det inte finns några språk i listan skickas det språk som du väljer på fliken Format i Nationella inställningar på Kontrollpanelen till de webbplatser du besöker.

Överst på sidan

Positioneringstjänster

Med positioneringstjänsterna i Windows kan du bestämma vilka appar, webbplatser och Windows-funktioner som ska ha tillåtelse att fastställa datorns position. Windows-positioneringstjänsterna består av två komponenter. Windows-platsprovider ansluter till en Microsoft-onlinetjänst för att fastställa din position. Windows-positioneringsplattformen fastställer datorns position med hjälp av maskinvara, t.ex. en GPS-sensor, eller programvara som Windows-platsprovider.

Windows-positioneringsplattform

Funktionens uppgift

Om du väljer att aktivera Windows-positioneringsplattformen kan appar som du installerar från Windows Store, liksom vissa Windows-funktioner, be om tillstånd att fastställa datorns position. Om du tillåter att en app använder din position kan Windows-positioneringsplattformen, förutom att uppge din position när du använder appen, meddela appen när din dator finns i eller utanför bestämda geografiska områden som definieras av appen. Exempelvis skulle du kunna ställa in en påminnelse i en app som påminner dig om att handla när du åker från jobbet. Beroende på systemkonfigurationen kan Windows-positioneringsplattformen fastställa datorns position med hjälp av maskinvara, t.ex. en GPS-sensor, eller med programvara som Windows-platsprovider.

Windows-positioneringsplattformen hindrar inte appar från att fastställa datorns position på andra sätt. Du kan exempelvis installera enheter (t.ex. en GPS-mottagare) som kan skicka platsinformation direkt till en app och förbigå positioneringsplattformen. Oavsett vilka inställningar du gör för Windows-positioneringsplattformen kan onlinetjänster använda datorns IP-adress för att fastställa datorns ungefärliga position, normalt den stad som datorn finns i.

Insamlad, bearbetad eller överförd information

Själva Windows-positioneringsplattformen överför ingen

information från din dator, men enskilda platsproviders (t.ex. Windows-platsprovider) kan överföra information när Windows-positioneringsplattformen ber dem att fastställa datorns position. Appar, webbplatser och funktioner som har tillåtelse att använda positioneringsplattformen för att fastställa datorns position kan också överföra eller lagra den här typen av information. Om en app definierar geografiska gränser som ska övervakas, lagras dessa gränser i krypterad form på datorn. Informationen som lagras om dessa gränser omfattar ett namn, en plats samt huruvida datorn fanns i eller utanför det avgränsade området den senaste gången datorns position kontrollerades. Appar som definierar geografiska gränser kan överföra eller lagra den här informationen

Användning av informationen

Om du aktiverar Windows-positioneringsplattformen kan behöriga appar, webbplatser och Windows-funktioner komma åt datorns position och använda den för att tillhandahålla personligt innehåll. Om du använder en app eller platsprovider från en tredje part regleras appens eller platsproviderns användning av datorns position av den tredje partens sekretesspolicy. Innan du laddar ned en app från Windows Store kan du se i appbeskrivningen om appen är platsberoende.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows aktiveras Windows-positioneringsplattformen. Om du väljer att anpassa inställningarna kan du hantera Windows-positioneringsplattformen genom att markera Låt Windows och appar begära min position från Windows-positioneringsplattformen under Dela information med Microsoft och andra tjänster. Första gången en Store-app ber att få fastställa datorns position blir du tillfrågad om du vill tillåta detta. Du kan visa och ändra inställningen för varje Store-app i Behörigheter i appens inställningar.

Om du har en skrivbordsapp som använder Windows-positioneringsplattformen bör den be om din tillåtelse att använda datorns position. När appen får åtkomst till datorns plats visas en

ikon i meddelandefältet som meddelar dig att datorns position har hämtats. Användarna kan hantera sina egna platsinställningar för appar under **Sekretess** i Datorinställningar. Administratörer kan också stänga av positioneringsplattformen för alla användare under **Platsinställningar** på Kontrollpanelen. En administratör på datorn kan förhindra att appar meddelas när geografiska gränser som definieras av appar korsas genom att inaktivera Windows platsramverkstjänst på Kontrollpanelen.

Windows-platsprovider

Funktionens uppgift

Windows-platsprovidern ansluter till Microsofts platstjänst online, som hjälper till att fastställa din dators ungefärliga plats baserat på Wi-Fi-nätverk nära datorn och datorns IP-adress.

Insamlad, bearbetad eller överförd information

När en app, som du har godkänt för att ta emot din plats, frågar efter din plats kommer Windows-positioneringsplattformen att anmoda alla installerade platsproviders (inklusive Windows-platsprovidern) att fastställa datorns aktuella plats. Windows-platsprovidern kommer först att kontrollera om den har en lista med Wi-Fi-åtkomstpunkter sparad från en tidigare begäran av en platsberoende app. Om det inte redan finns någon lista med närliggande Wi-Fi-åtkomstpunkter, eller om listan är inaktuell, skickar providern information om Wi-Fi-åtkomstpunkter i närheten och GPS-information (om sådan finns) till Microsofts platstjänst. Tjänsten skickar tillbaka datorns ungefärliga plats till providern, som skickar platsen till Windows-positioneringsplattformen som i sin tur lämnar platsen till den app som begärde datorns plats. Windows-platsprovider kan även uppdatera listan med sparade Wi-Fi-åtkomstpunkter. Windows-platsprovider underhåller listan så att den kan fastställa datorns ungefärliga position utan att ansluta till Internet varje gång. Listan med åtkomstpunkter är krypterad när den lagras på disken så att apparna inte kan komma åt den direkt.

Informationen om närliggande Wi-Fi-åtkomstpunkter innehåller BSSID (Wi-Fi-åtkomstpunktens MAC-adress) och signalstyrka. GPS-informationen innehåller den observerade latituden, longituden, riktningen, farten och höjden. För att skydda din integritet skickar

inte Windows-platsprovider någon information som kan identifiera din dator unikt, utöver den standarddatorinformation om datorn som skickas i samband med alla anslutningar till Internet. För att skydda Wi-Fi-nätverkets ägares integritet skickar Windows inte information om SSID (namn på Wi-Fi-åtkomstpunkter) eller dolda Wi-Fi-nätverk. Av sekretess- och säkerhetsskäl skickas information om Wi-Fi-nätverk krypterad via SSL.

Om du väljer att hjälpa till med att förbättra Microsofts platstjänst efter att en app har begärt din dators plats, kan Windows åter skicka information om Wi-Fi-åtkomstpunkter till Microsoft när en app har begärt din dators plats. Om du är använder en Internetanslutning med fast pris, begränsar Windows det antal gånger per dag som det skickar informationen för att begränsa användningen av din Internetanslutning.

Användning av informationen

Informationen används av Windows-platsprovider för att lämna datorns ungefärliga position till Windows-positioneringsplattformen när en behörig app begär den.

Om du väljer att hjälpa till att förbättra Microsofts positioneringstjänster används informationen om Wi-Fi och GPS som skickas till Microsoft för att förbättra Microsofts positioneringstjänster, vilket i sin tur bidrar till att förbättra positioneringstjänsterna som används av dina appar. Microsoft lagrar inga data som samlas in från den här tjänsten som kan användas för att identifiera, kontakta, skicka reklam till dig eller för att spåra eller skapa historik över datorns position.

Val och kontroll

Windows-platsprovider används bara om en behörig app har begärt din dators position. Mer information om hur du kontrollerar om appar kan begära din plats finns i avsnittet Windows-positioneringsplattformen. Om du ger appar tillstånd att begära datorns position raderas och ersätts regelbundet den cachade listan med närliggande Wi-Fi-åtkomstpunkter som krypteras och lagras av Windows-platsprovider.

Om du väljer standardinställningarna när du installerar Windows

väljer du att hjälpa till att förbättra Microsofts positioneringstjänster. Om du väljer att anpassa inställningarna kan du välja om du vill hjälpa till att förbättra Microsofts positioneringstjänster genom att markera **Skicka viss positioneringsinformation till Microsoft när appar med positioneringsfunktioner används** under **Hjälp till att förbättra Microsofts produkter och tjänster**. Efter installationen av Windows kan du ändra den här inställningen i Positioneringsinställningar på Kontrollpanelen. Om du väljer att inte hjälpa till att förbättra tjänsterna kan du fortfarande använda Windows-platsprovider för att fastställa datorns ungefärliga position.

Du kan aktivera och inaktivera Windows-platsprovider genom att öppna **Aktivera eller inaktivera Windows-funktioner** på Kontrollpanelen. Om du inaktiverar Windows-platsprovidern kan du fortfarande använda andra platsproviders (till exempel GPS) tillsammans med Windows-positioneringsplattformen.

Överst på sidan

Hantera dina autentiseringsuppgifter

Funktionens uppgift

I Windows kan du koppla Windows Store-appar till konton som du använder för webbplatser. Om du tidigare har sparat ett lösenord för en webbplats i Internet Explorer kan Windows använda det sparade lösenordet när du kopplar en app till webbplatsen.

Insamlad, bearbetad eller överförd information

När en app ber om autentiseringsuppgifter för att logga in på en webbplats kan du välja att spara autentiseringsuppgifterna. Om du redan har loggat in på webbplatsen i Internet Explorer och har valt att spara dina autentiseringsuppgifter fyller Windows automatiskt i de sparade autentiseringsuppgifterna. Autentiseringsuppgifterna lagras i krypterad form på datorn. Mer information om hur dessa och andra autentiseringsuppgifter kan synkroniseras med OneDrive finns i avsnittet Inställningar för synkronisering på den här sidan.

Användning av informationen

Windows använder bara de sparade autentiseringsuppgifterna för att logga in dig på de webbplatser som du har valt. Om du sparar autentiseringsuppgifter när du kopplar en app till en webbplats används inte de sparade autentiseringsuppgifterna i Internet Explorer eller i andra appar.

Val och kontroll

Du kan hantera sparade autentiseringsuppgifter i Autentiseringshanteraren på Kontrollpanelen. Mer information om hur dessa och andra autentiseringsuppgifter kan synkroniseras med OneDrive finns i avsnittet Inställningar för synkronisering på den här sidan.

Överst på sidan

Namn och profilbild

Funktionens uppgift

Appar kan begära ditt namn och din profilbild från Windows för att kunna tillhandahålla anpassat innehåll. Ditt namn och din profilbild visas under **Ditt konto** i **Konton** i Datorinställningar. Om du loggar in i Windows med ett Microsoft-konto använder Windows namnet och profilbilden som är kopplade till det kontot. Om du inte har valt någon bild för ditt konto blir din profilbild en standardbild från Windows.

Insamlad, bearbetad eller överförd information

Om du tillåter att appar får åtkomst till ditt namn och din profilbild lämnar Windows den informationen till alla appar som begär den. Appar kan lagra eller skicka denna information.

Om du loggar in i Windows med ett domänkonto och väljer att tillåta att appar använder ditt namn och din profilbild får appar som kan använda dina Windows-uppgifter åtkomst till en del av din övriga domänkontoinformation. Denna information omfattar bland annat ditt huvudnamn som användare (t.ex. jack@contoso.com) och DNS-domännamn (t.ex. corp.contoso.com\jack).

Om du loggar in i Windows med ett Microsoft-konto eller om du loggar in i Windows med ett domänkonto som är kopplat till ett

Microsoft-konto kan Windows automatiskt synkronisera profilbilden på din dator med din profilbild för Microsoft.

Användning av informationen

Om du använder en app från tredje part kommer användning av ditt namn och din profilbild regleras av den tredje partens sekretesspraxis. Om du använder en Microsoft-app förklaras appens sekretesspraxis i sekretesspolicyn för appen.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows tillåter Windows appen att komma åt ditt namn och din profilbild. Om du väljer att anpassa inställningarna kan du kontrollera åtkomsten till ditt namn och din profilbild genom att markera **Låt appar använda mitt namn och min profilbild** under **Dela information med Microsoft och andra tjänster**. Efter installationen av Windows kan du ändra den här inställningen i **Sekretess** i Datorinställningar. Du kan ändra din profilbild i **Konton** i Datorinställningar. Du kan även välja att tillåta att vissa appar ändrar din profilbild.

Överst på sidan

Network Awareness

Funktionens uppgift

Om du har ett abonnemang för nätverksåtkomst (t.ex. via en mobil bredbandsanslutning) lämnar den här funktionen information om abonnemanget till appar och funktioner i Windows på datorn. Funktioner och appar i Windows kan optimera sitt beteende med hjälp av den här informationen. Om du exempelvis har ett abonnemang med rörlig kostnad för datatrafik väntar Windows Update med att leverera uppdateringar med lägre prioritet till din dator tills du är ansluten till ett annat slags nätverk. Den här funktionen ger även information om nätverksanslutningen, t.ex. signalstyrkan och huruvida datorn är ansluten till Internet.

Insamlad, bearbetad eller överförd information

Den här funktionen samlar in information om anslutningar till

Internet och i intranätet, t.ex. datorns DNS-suffix (Domain Name Service), nätverksnamnet och gatewayadressen till de nätverk som datorn ansluter till. Den här funktionen erhåller även information om abonnemang, t.ex. hur stora datamängder som återstår.

Nätverksanslutningsprofiler kan innehålla en historik över alla besökta nätverk och datumet och tiden för den senaste anslutningen. Den här funktionen kan försöka ansluta till en av Microsofts servrar för att kontrollera om du är ansluten till Internet. Den enda information som skickas till Microsoft i samband med nätverksanslutningskontroller är standardinformation om datorn.

Användning av informationen

Om data skickas till Microsoft används de endast i syfte att uppge nätverksanslutningens status. Nätverksanslutningens status görs tillgänglig för appar och funktioner på datorn som begär information om nätverksanslutningen. Om du använder ett externt företags app regleras användningen av informationen som samlas in av det företagets sekretesspolicy.

Val och kontroll

Network Awareness är aktiverat som standard. En administratör kan inaktivera funktionen med alternativen under Tjänster i Administrationsverktyg på Kontrollpanelen. Vi rekommenderar inte att funktionen inaktiveras eftersom det förhindrar att vissa funktioner i Windows fungerar korrekt.

Överst på sidan

Aviseringar, låsskärmsappar och paneluppdateringar

Windows Store-appar kan automatiskt ta emot innehåll och visa meddelanden på flera sätt. De kan till exempel hämta meddelanden som visas en liten stund i skärmens ena hörn eller på appaneler om panelerna har fästs på Startskärmen. Du kan också ta emot den här typen av meddelanden på låsskärmen om du vill. Låsskärmen kan också visa detaljerad eller översiktlig status för vissa appar. Apputgivare kan skicka innehåll till Windows Store-appar via Windows Push Notification Service som körs på Microsoft-servrar. Apparna kan också ladda ned information direkt

från tredjepartsservrar.

Aviseringar

Funktionens uppgift

Windows Store-appar kan leverera information i realtid eller periodvis. Dessa meddelanden visas en kort stund i hörnet av skärmen.

Insamlad, bearbetad eller överförd information

Appar kan visa text, bilder eller både text och bilder i meddelanden. Innehållet i meddelanden kan levereras lokalt av appen (t.ex. ett larm från en klockapp). Meddelanden kan också skickas från en apps onlinetjänst via Windows Push Notification Service (t.ex. en uppdatering i ett socialt nätverk). Bilder som visas i meddelanden kan laddas ned direkt från en server som angetts av apputgivaren. När detta görs skickas standardinformation om datorn till servern i fråga.

Användning av informationen

Microsoft använder bara meddelandeinformation för att leverera meddelanden från dina appar till dig. Ett meddelande kan lagras tillfälligt av Windows Push Notification Service innan det levereras till datorn. Om ett meddelande inte kan överföras direkt, lagras det bara i några minuter innan det tas bort.

Val och kontroll

Du kan inaktivera meddelanden för alla eller enskilda appar i **Aviseringar** under **Sök och appar** i Datorinställningar. Om du inaktiverar meddelanden för en app eller om du avinstallerar den, kan apputgivaren fortfarande skicka uppdateringar till Windows Push Notification Service, men meddelandena visas inte på datorn.

Låsskärmsappar

Funktionens uppgift

Vissa Windows Store-appar kan visa status och meddelanden på skärmen när datorn är låst. Låsskärmsappar kan också utföra åtgärder när datorn är låst, t.ex. synkronisera e-post i bakgrunden eller låta dig svara på inkommande telefonsamtal. Du kan också använda datorns kamera direkt från låsskärmen.

Insamlad, bearbetad eller överförd information

Låsskärmsappar kan ta emot statusuppdateringar från apputgivaren via Windows Push Notification Service eller direkt från apputgivarens (eller en annan tredje parts) servrar. Låsskärmsappar kan också skicka eller bearbeta annan information som inte är knuten till meddelanden och uppdateringar.

Användning av informationen

Windows använder status- och meddelandeinformationen från låsskärmsapparna för att uppdatera låsskärmen.

Val och kontroll

När du har installerat Windows definieras apparna E-post, Kalender och Skype automatiskt som låsskärmsappar. Du kan lägga till och ta bort dessa eller andra appar från låsskärmen och inaktivera användningen av kameran i **Låsskärm** under **Dator och enheter** i Datorinställningar. Du kan också välja en app som visar detaljerad status (t.ex. information om nästa avtalade tid i din kalender) på låsskärmen.

Du kan välja om låsskärmsappar ska kunna visa meddelanden på låsskärmen i **Aviseringar** under **Sök och appar** i Datorinställningar.

Paneluppdateringar

Funktionens uppgift

Windows Store-appar kan leverera information i realtid eller periodvis till dig. De visas som uppdateringar av apparnas paneler på Startskärmen.

Insamlad, bearbetad eller överförd information

Store-appar som har fästs på Startskärmen kan uppdatera sina paneler med text och/eller bilder. Innehållet på en apps panel kan levereras lokalt av appen, laddas ned regelbundet från en server som angetts av apputgivaren eller skickas från en apps onlinetjänst via Windows Push Notification Service. Om panelinnehåll laddas ned direkt från en server som angetts av apputgivaren skickas standardinformation om datorn till servern i fråga.

Användning av informationen

Microsoft använder bara panelinformationen för att leverera paneluppdateringar från dina appar till dig. Informationen kan lagras tillfälligt av Windows Push Notification Service innan den överförs till datorn. Om paneluppdateringen inte kan överföras direkt, lagras den bara i ett par dagar innan den tas bort.

Val och kontroll

När en app har börjat ta emot paneluppdateringar kan du inaktivera dem genom att markera appens panel på Startskärmen och välja **Stäng av levande panel** i appens tillgängliga kommandon. Om du tar bort en apps panel från Startskärmen visas inte appens paneluppdateringar. Om du avinstallerar en app kan apputgivaren fortfarande skicka uppdateringar till Windows Push Notification Service, men de visas inte på datorn.

Om du vill rensa uppdateringarna som visas på panelerna på Startskärmen sveper du från höger sida av Startskärmen eller pekar i det övre högra hörnet, trycker eller klickar på **Inställningar**och trycker eller klickar sedan på **Paneler**. Tryck eller klicka på **Rensa** under **Rensa personlig information i mina paneler**. Paneluppdateringar som levereras efter att du har rensat de aktuella uppdateringarna fortsätter att visas.

Överst på sidan

Beställ foton

Funktionens uppgift

Med Beställ foton kan du skicka digitala bilder som lagras på datorn eller en nätverksenhet till en utskriftstjänst på nätet som du väljer själv. Beroende på tjänsten kan du kanske skriva ut dina bilder och få dem levererade per post eller hämta bilderna i någon butik.

Insamlad, bearbetad eller överförd information

Om du vill beställa utskrifter av bilderna skickas de digitala bilderna via Internet till den tjänst som du har valt. Filsökvägen till de digitala bilderna som du väljer (som kan innehålla ditt

användarnamn) kan skickas till tjänsten så att den kan visa och överföra dem. Digitala bildfiler kan innehålla data om bilden som lagrades i filen av kameran, t.ex. datumet och tiden då bilden togs eller platsen där den togs, om kameran är utrustad med en GPS. Filerna kan även innehålla personlig information (t.ex. bildtexter) som kan ha kopplats till filen genom att du har använt ett program för behandling av digitala bilder och Utforskaren. Mer information finns i avsnittet Egenskaper nedan.

När du har valt en utskriftstjänst i Beställ foton tas du till tjänstens webbplats i fönstret Beställ foton. Information som du anger på utskriftstjänstens webbplats överförs till tjänsten.

Användning av informationen

Informationen som lagras i de digitala bildfilerna av kameran kan användas av utskriftstjänsten vid framställningen av bilderna, t.ex. för att justera bildens färger eller skärpa innan den skrivs ut. Information som lagras av program för digital bildhantering kan användas av utskriftstjänsten för att skriva ut bildtexten på fram- eller baksidan av fotot. Utskriftstjänsternas bruk av dessa uppgifter och annan information som du tillhandahåller, t.ex. uppgifter som du anger på webbplatsen, är underställt företagets sekretesspolicy.

Val och kontroll

Du kan använda Beställ foton för att välja vilka foton du vill skicka och vilken utskriftstjänst du vill anlita. Vissa bildbehandlingsprogram kan hjälpa dig med att ta bort lagrad personlig information innan bilderna skickas för utskrift. Du kan kanske även redigera filens egenskaper och ta bort lagrad personlig information.

Överst på sidan

Förhämtning och förstart

Funktionens uppgift

Windows håller reda på när och hur ofta appar och Windows-funktioner används och vilka systemfiler som då läses in för att dessa appar och funktioner ska kunna startas snabbare.

Insamlad, bearbetad eller överförd information

När du använder en app eller en Windows-funktion sparar Windows viss information på datorn om systemfilerna som används och om när och hur ofta appen eller funktionen används.

Användning av informationen

Windows använder informationen om app- och funktionsanvändning för att appar och funktioner ska kunna startas snabbare. I vissa fall kan det hända att appar startas automatiskt i väntetillstånd.

Val och kontroll

Appar som startas och pausas automatiskt visas i aktivitetshanteraren och kan avslutas. Medan dessa appar är pausade kan de inte använda webbkameran eller mikrofonen förrän du startar dem, även om du tidigare har aktiverar den funktionen.

Överst på sidan

Assistenten för programkompatibilitet

Funktionens uppgift

Om ett problem med kompatibiliteten upptäcks för en skrivbordsapp som du försöker köra hjälper Assistenten för programkompatibilitet dig att lösa det.

Insamlad, bearbetad eller överförd information

Om ett problem med kompatibiliteten upptäcks för en app som du försöker köra skapas en rapport med information om appens namn, version, de nödvändiga kompatibilitetsinställningarna och vad du har gjort med appen hittills. Problem med inkompatibla appar rapporteras till Microsoft via Windows Felrapportering eller Windows Customer Experience Improvement Program (CEIP).

Användning av informationen

Felrapporterna används för att ge svar om problem som du rapporterar om dina appar. Svaren innehåller (eventuellt) länkar till apputgivarens webbplats så att du kan läsa mer om möjliga

lösningar. Felrapporter som skapas när appar kraschar används för att avgöra vilken inställning som ska justeras då du stöter på kompatibilitetsproblem med appar som du kör i den här versionen av Windows. Informationen som rapporteras via CEIP används för att identifiera kompatibilitetsproblem med appar.

Microsoft använder inte informationen som samlas in av den här funktionen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

För problem som rapporteras via Windows Felrapportering skapas en felrapport bara när du väljer att kontrollera om det finns en lösning på nätet. Om du inte tidigare har gått med på att rapportera problem automatiskt så att du kan se om det finns någon lösning, får du en fråga om du vill skicka felrapporten. Mer information finns i avsnittet Windows Felrapportering.

Vissa problem rapporteras automatiskt via Windows CEIP om du har aktiverat alternativet. Mer information finns i avsnittet om Windows Customer Experience Improvement Program nedan.

Överst på sidan

Egenskaper

Funktionens uppgift

Egenskaper är filinformation som du kan använda för att snabbt söka efter och ordna dina filer. Vissa egenskaper hör till själva filen (t.ex. dess storlek) medan andra kan vara specifika för en app eller en enhet (t.ex. kamerainställningarna när du tog ett foto eller platsinformationen som sparades av kameran med fotot).

Insamlad, bearbetad eller överförd information

Vilken typ av information som lagras beror på filens typ och apparna som använder den. Exempel på egenskaper är filnamnet, ändringsdatumet, filstorleken, författaren, sökord och kommentarer. Egenskaperna lagras i filen och flyttas med den om den flyttas eller kopieras till en annan plats, t.ex. en filresurs, eller om den skickas som en e-postbilaga.

Användning av informationen

Egenskaper kan hjälpa dig att söka efter och ordna filerna snabbare. De kan även användas av appar för att utföra appspecifika uppgifter. Ingen information skickas till Microsoft.

Val och kontroll

Du kan redigera eller ta bort vissa egenskaper för en fil genom att välja filen i Utforskaren och klicka på **Egenskaper**. Vissa filspecifika egenskaper, t.ex. ändringsdatumet, filstorleken, filnamnet och vissa appspecifika egenskaper, går inte att ta bort på det här viset. Appspecifika egenskaper går bara att ändra eller ta bort om appen som genererade filen stöder dessa funktioner.

Överst på sidan

Närhet

Närhetstjänster

Funktionens uppgift

Om din dator är utrustad med NFC-maskinvara (Near-Field Communication) kan du knacka den mot en annan enhet eller ett tillbehör med NFC-maskinvara för att dela länkar, filer och annan information. Det finns två olika typer av närhetsanslutningar: Knackat och klart samt Knacka och håll. Med Knackat och klart kan du skapa en kort- eller långvarig anslutning mellan enheter via Wi-Fi, Wi-Fi Direct eller Bluetooth. Med Knacka och håll är anslutningen bara aktiv under den tid som enheterna befinner sig nära varandra.

Insamlad, bearbetad eller överförd information

När du knackar två enheter med närhetsstöd mot varandra, utbyter de information för att upprätta en anslutning mellan sig. Beroende på hur enheterna är konfigurerade kan dessa data omfatta Bluetooth-kopplingsinformation och Wi-Fi-nätverksadresser samt datorns namn.

När en anslutning har upprättats kan annan information utbytas mellan enheterna, beroende på den specifika närhetsfunktionen eller appen som du använder. Windows kan skicka filer, länkar och

annan information mellan enheter via en närhetsanslutning. Appar som använder närhetsfunktionen kan skicka och ta emot all information de har tillgång till. Informationen kan skickas via din nätverks- eller Internetanslutning eller direkt via en trådlös anslutning mellan enheterna.

Användning av informationen

Nätverks- och datorinformation som byts ut via en närhetsanslutning används för att upprätta en nätverksanslutning samt för att identifiera enheterna som ansluter till varandra. Data som överförs via en närhetsanslutning som har upprättats i en app kan användas på valfritt sätt av den appen. Ingen information skickas till Microsoft.

Val och kontroll

Närhetstjänsterna är aktiverade som standard. En administratör kan inaktivera funktionen genom att använda alternativen i Enheter och skrivare på Kontrollpanelen.

Knacka och skicka

Funktionens uppgift

Med Knacka och skicka i Windows är det enkelt att dela vald information med en vän som står bredvid dig eller med någon annan av dina enheter, t.ex. en mobiltelefon. Om du exempelvis har öppnat en webbläsare kan du starta Knacka och skicka från rutan Enheter. Nästa enhet som du knackar på får en länk till webbsidan som visas. Detta fungerar även med alla appar som stöder informationsdelning, t.ex. bilder, text eller filer.

Insamlad, bearbetad eller överförd information

Knacka och skicka använder den information som du delar och informationen som beskrivs i avsnittet om närhetstjänster ovan.

Användning av informationen

Informationen används bara för att upprätta anslutningen mellan de två enheterna. Den delade informationen lagras inte av Knacka och skicka. Ingen information skickas till Microsoft.

Val och kontroll

Om närhetstjänsten är aktiverad är även Knacka och skicka aktiverat. Mer information finns i avsnittet om närhetstjänster.

Överst på sidan

Fjärråtkomstanslutningar

Funktionens uppgift

Med fjärråtkomstanslutningar kan du ansluta till privata nätverk via en VPN-anslutning (virtuellt privat nätverk) och Fjärråtkomsttjänsten (RAS). RAS är en komponent som ansluter en datorklient (vanligtvis din dator) till en värddator (som även kallas fjärråtkomstservern) med hjälp av standardprotokoll i branschen. VPN-teknik ger användare möjlighet att ansluta till ett privat nätverk, t.ex. ett företagsnätverk, via Internet.

Med fjärråtkomstkomponenten Fjärranslutning kan du ansluta till Internet med ett modem eller bredbandsteknik, t.ex. ett kabelmodem eller en DSL-anslutning (digital subscriber line). Fjärranslutning innehåller uppringningskomponenter som RAS-klient, Anslutningshanteraren och RAS-telefon, samt uppringningsprogram som används i kommandotolken, t.ex. rasdial.

Insamlad, bearbetad eller överförd information

Uppringningskomponenterna samlar in information från datorn, t.ex. ditt användarnamn, ditt lösenord och ditt domännamn. Informationen skickas till systemet som du försöker ansluta till. För att skydda dig och din dator krypteras säkerhetsrelaterad information, till exempel ditt användarnamn och ditt lösenord, och lagras på din dator.

Användning av informationen

Uppringningsinformation används för att ansluta din dator till Internet. En fjärråtkomstserver kan behålla information om användarnamnet och IP-adressen av redovisnings- och regelefterlevnadsskäl, men ingen information skickas till Microsoft.

Val och kontroll

I uppringningskomponenter som inte används i kommandotolken

kan du spara ditt lösenord genom att välja **Spara det här användarnamnet och lösenordet**. Du kan när som helst avmarkera alternativet och därmed ta bort det sparade lösenordet från uppringningsprogrammet. Eftersom det här alternativet är inaktiverat som standard kan du bli uppmanad att ange ditt lösenord för att ansluta till Internet eller till ett nätverk. I uppringningsprogram som anropas i kommandotolken, t.ex. rasdial, finns det ingen möjlighet att spara lösenordet.

Överst på sidan

RemoteApp- och fjärrskrivbordsanslutningar

Funktionens uppgift

Med RemoteApp- och fjärrskrivbordsanslutningar kan du komma åt appar och skrivbord på fjärrdatorer som har gjorts tillgängliga online för fjärråtkomst.

Insamlad, bearbetad eller överförd information

När du aktiverar en anslutning laddas konfigurationsfiler ned till din dator från den URL som du anger. Dessa konfigurationsfiler länkar till appar och skrivbord på fjärrdatorerna så att du kan köra dem på din dator. Datorn kontrollerar automatiskt om det har kommit uppdateringar till dessa konfigurationsfiler och laddar ned dem med regelbundna mellanrum. Apparna körs på fjärrdatorerna, och informationen som du anger i apparna överförs via nätverket till fjärrdatorerna som du har valt att ansluta till.

Om Microsoft är värd för datorn eller appen som du ansluter till kan ytterligare information om din anslutning skickas till Microsoft för supportändamål.

Användning av informationen

Uppdateringar av konfigurationsfilerna kan innehålla inställningsändringar som bland annat ger tillgång till nya appar, men de nya apparna körs bara om du väljer att göra det. Den här funktionen skickar även information till fjärrdatorerna där fjärrapparna körs. Fjärrapparnas användning av dessa data regleras av appleverantörernas och fjärrdatoradministratörernas

sekretesspolicy. Ingen information skickas till Microsoft såvida inte Microsoft är värd för fjärranslutningen.

Val och kontroll

Du kan välja om du vill använda RemoteApp- och fjärrskrivbordsanslutningar eller inte. Du kan lägga till och ta bort RemoteApp- och fjärrskrivbordsanslutningar genom att öppna RemoteApp- och fjärrskrivbordsanslutningar på Kontrollpanelen. Du kan lägga till en ny anslutning genom att klicka på **RemoteApp och fjärrskrivbord**och ange en anslutnings-URL i dialogrutan. Du kan även ange din e-postadress för att hämta anslutnings-URL:en. Du kan ta bort en anslutning och dess anslutningsfiler genom att klicka på **Ta bort** i dialogrutan med anslutningsbeskrivningar. Om du kopplar ifrån en anslutning utan att stänga alla öppna appar förblir de öppna på fjärrdatorn. RemoteApp- och fjärrskrivbordsanslutningar visas inte i listan Lägg till eller ta bort program på Kontrollpanelen.

Överst på sidan

Anslutning till fjärrskrivbord

Funktionens uppgift

Anslutning till fjärrskrivbord är ett sätt för dig att upprätta en fjärranslutning till en värddator där Fjärrskrivbordstjänster körs.

Insamlad, bearbetad eller överförd information

Inställningarna för Anslutning till fjärrskrivbord sparas i appens lagring eller i en RDP-fil (Remote Desktop Protocol) på din dator. Dessa inställningar omfattar namnet på din domän och konfigurationsinställningar för anslutningen, t.ex. fjärrdatorns namn, användarnamnet, visningsinformation, lokal enhetsinformation, ljudinformation, urklipp, anslutningsinställningar, namn på fjärrappar och en sessionsikon eller miniatyrbild.

Autentiseringsuppgifter för dessa anslutningar och Fjärrskrivbordsgateway samt en lista över betrodda namn på fjärrskrivbordsgatewayservrar lagras lokalt på datorn. En lista lagras i registret. Listan lagras permanent om den inte tas bort av

en administratör. Ingen information skickas till Microsoft såvida inte Microsoft är värd för fjärranslutningen.

Användning av informationen

Med informationen som samlas in av Anslutning till fjärrskrivbord kan du ansluta till värddatorer som kör Fjärrskrivbordstjänster med de inställningar du föredrar. Information om ditt användarnamn, ditt lösenord och din domän samlas in så att du kan spara anslutningsinställningarna och dubbelklicka på RDP-filen eller klicka på en favorit för att öppna en anslutning utan att behöva ange uppgifterna igen.

Val och kontroll

Du kan välja om du vill använda Anslutning till fjärrskrivbord. Om du gör det innehåller RDP-filerna och Anslutning till fjärrskrivbord-favoriterna den information som krävs för att ansluta till en fjärrdator, däribland de alternativ och inställningar som konfigurerades när anslutningen sparades automatiskt. Du kan ändra RDP-filerna och favoriterna. Det gäller även filer för att ansluta till samma dator med olika inställningar. Om du vill ändra de sparade inloggningsuppgifterna öppnar du Autentiseringshanteraren i Användarkonton på Kontrollpanelen.

Överst på sidan

Logga in med ett Microsoft-konto

Funktionens uppgift

Ett Microsoft-konto (kallades tidigare Windows Live ID) är en e-postadress och ett lösenord som du kan använda för att logga in i appar, på webbplatser och på tjänster från Microsoft och utvalda Microsoft-partner. Du kan registrera dig för ett Microsoft-konto i Windows eller på de webbplatser från Microsoft som kräver att du loggar in med ett Microsoft-konto.

Du kan logga in i Windows med ett Microsoft-konto eller, i produkter som stöder det, välja att koppla ditt lokala konto eller domänkonto till ett Microsoft-konto. Om du gör det kan Windows ge dina datorer samma utseende och känsla genom att

automatiskt synkronisera inställningar och information i Windows och Microsoft-appar. Om du besöker en webbplats där du använder ett Microsoft-konto för att logga in, loggas du även in på den webbplatsen automatiskt av Windows.

Insamlad, bearbetad eller överförd information

Om du anger en e-postadress som ska användas som ett Microsoft-konto när du konfigurerar datorn eller i **Konton** i Datorinställningar, skickar Windows e-postadressen till Microsoft för att avgöra om det redan finns ett Microsoft-konto som är kopplat till den e-postadressen. Om du redan använder den e-postadressen som ett Microsoft-konto kan du använda adressen och lösenordet för Microsoft-kontot för att logga in i Windows. Om du inte redan har tillräckligt med säkerhetsinformation för Microsoft-kontot kan det hända att vi först ber dig att lämna ytterligare säkerhetsinformation, t.ex. ett mobiltelefonnummer som vi kan använda för att verifiera att kontot är ditt. Om du inte har ett Microsoft-konto kan du skapa ett med valfri e-postadress.

När du loggar in med ett Microsoft-konto skickar Windows också generell datorinformation till Microsoft, bland annat information om din datortillverkare, modellnamn och -version.

Varje gång du loggar in i Windows med ett Microsoft-konto när datorn är ansluten till Internet, verifierar Windows din e-postadress och ditt lösenord mot Microsofts servrar. Följande gäller när du är inloggad i Windows med ditt Microsoft-konto eller med ett domänkonto som är kopplat till ditt Microsoft-konto:

- Vissa inställningar i Windows synkroniseras mellan de datorer som du loggar in på med Microsoft-kontot. Mer information om vilka inställningar som synkroniseras och hur du styr dem finns i avsnittet Inställningar för synkronisering på den här sidan.

- Microsoft-appar som använder ett Microsoft-konto för autentisering (t.ex. E-post, Kalender, Kontakter, Microsoft Office och andra appar) kan börja ladda ned din information automatiskt (appen E-post laddar exempelvis automatiskt ned meddelanden som skickas till din Outlook.com- eller Hotmail.com-adress om du har en sådan). Webbläsare kan

logga in dig automatiskt på webbplatser som du loggar in på med ditt Microsoft-konto (om du till exempel går till Bing.com kan du loggas in automatiskt utan att behöva ange lösenordet för ditt Microsoft-konto).

Windows ber om din tillåtelse innan appar från tredje part får använda profilinformation eller andra personliga uppgifter som är kopplade till ditt Microsoft-konto. Om du loggar in i Windows med ett domänkonto som är kopplat till ett Microsoft-konto synkroniseras inställningarna och den information du väljer med ditt domänkonto, och du loggas automatiskt in på appar och webbplatser enligt beskrivningen ovan. Eftersom domänadministratörer kan komma åt all information på din dator, kan de också komma åt alla inställningar och all information som du har valt att synkronisera med andra datorer via ditt Microsoft-konto. Det kan gälla inställningar som namn, profilbild och webbläsarhistorik. Mer information om vilka inställningar som synkroniseras och hur du styr dem finns i avsnittet Inställningar för synkronisering på den här sidan.

Användning av informationen

När du skapar ett nytt Microsoft-konto i Windows använder vi informationen som du anger för att skapa och skydda kontot. Säkerhetsinformationen som du anger (t.ex. telefonnummer och alternativ e-postadress) används endast om du inte kan logga in på ditt konto. När du är inloggad på Windows med ett Microsoft-konto använder Windows informationen i ditt Microsoft-konto för att automatiskt logga in dig på appar och webbplatser. Mer information om hur ett Microsoft-konto påverkar din integritet finns i sekretesspolicyn för Microsoft-konton. Information om hur enskilda Microsoft-appar använder information som är kopplad till ditt Microsoft-konto finns i sekretesspolicyn för respektive app. Du hittar sekretesspolicyn för en Microsoft-app i appens inställningar eller i dialogrutan Om.

Generell enhetsinformation kan användas för att anpassa viss kommunikation, till exempel e-post som hjälper dig att komma igång med din enhet.

Val och kontroll

När du loggar in i Windows med ett Microsoft-konto synkroniseras vissa inställningar automatiskt. Information om hur du ändrar vilka Windows-inställningar som synkroniseras eller hur du slutar synkronisera finns i avsnittet Inställningar för synkronisering på den här sidan. Mer information om vilka data som samlas in av Microsoft-appar som använder ett Microsoft-konto för autentisering finns i sekretesspolicyn för respektive app.

I produkter som stöder det kan du skapa ett lokalt konto eller Microsoft-konto när du vill i **Konton** i Datorinställningar. Om du loggar in i Windows med ett domänkonto kan du koppla eller koppla från ditt Microsoft-konto när du vill i **Konton** i Datorinställningar.

När du använder InPrivate-surfning i Internet Explorer loggas du inte in automatiskt på webbplatser som använder Microsoft-konton.

Överst på sidan

OneDrive-lagring i molnet

Funktionens uppgift

När du loggar in med ett Microsoft-konto på en enhet kan du välja att spara en del innehåll och vissa inställningar automatiskt på Microsoft-servrar så att du har en säkerhetskopia om något händer med enheten.

Insamlad, bearbetad eller överförd information

Om du under installationen väljer att använda OneDrive för molnlagring skickar Windows automatiskt innehåll till Microsofts servrar, inklusive följande:

- Foton och videoklipp på enheten som sparats i mappen **Kamerabilder** .
- Inställningar som är specifika för enheten och som inte delas mellan dina enheter.
- Beskrivande information om din enhet, t.ex. enhetens namn och typ.

Du kan även välja att spara innehåll på Microsofts servrar och appar kan välja att använda Microsofts servrar som standardlagringsplats för dina filer.

Användning av informationen

Windows använder det här innehållet för att tillhandahålla molnlagringstjänsten. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer Använd OneDrive när du konfigurerar datorn kommer Windows att spara det innehåll som beskrivs i det här avsnittet på OneDrive. Du kan ändra de här inställningarna när du vill i avsnittet OneDrive i Datorinställningar.

Överst på sidan

Inställningar för synkronisering

Funktionens uppgift

När du loggar in i Windows med ett Microsoft-konto synkroniserar Windows en del av dina inställningar och information med Microsofts servrar för att göra det enklare att få personliga upplevelser på flera datorer. När du har loggat in på en eller flera datorer med ett Microsoft-konto, och när du för första gången loggar in på en annan dator med samma Microsoft-konto, laddar Windows ned och använder inställningarna och informationen som du valde att synkronisera från dina andra datorer. Inställningar som du väljer att synkronisera uppdateras automatiskt på Microsofts servrar och dina andra datorer när du använder dem.

Insamlad, bearbetad eller överförd information

Om du väljer att logga in i Windows med ett Microsoft-konto synkroniserar Windows en del inställningar med Microsoft servrar. Dessa inställningar omfattar:

- Startskärmens layout
- Appar som du har installerat från Windows Store

- Språkinställningar
- Hjälpmedelsinställningar
- Personligt anpassade inställningar som profilbild, låsskärmsbild, bakgrund och musinställningar
- Inställningar för Windows Store-appar
- Ordlistor för stavningskontroll, IME-ordlistor och personliga ordlistor
- Webbläsarhistorik, favoriter och webbplatser som är öppna
- Sparade lösenord för appar, webbplatser och nätverk
- Adresser för delade nätverksskrivare som du har anslutit till

Alla synkroniserade inställningar krypteras med SSL för att skydda din integritet. En del av inställningarna synkroniseras inte på datorn förrän du lägger till datorn i ditt Microsoft-konto som en betrodd dator.

Om du loggar in på Windows med ett domänkonto som är kopplat till ett Microsoft-konto synkroniseras inställningar och information till ditt domänkonto. Lösenord som du sparar när du är inloggad i Windows med ett domänkonto som är kopplat till ett Microsoft-konto synkroniseras aldrig. Eftersom domänadministratörer kan komma åt all information på din dator, kan de också komma åt alla inställningar och all information som du har valt att synkronisera med andra datorer via ditt Microsoft-konto.

Användning av informationen

Windows använder dessa inställningar och den här informationen för att tillhandahålla synkroniseringstjänsten. Microsoft använder inte de inställningar och den information som du har synkroniserat för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

När du loggar in i Windows med ett Microsoft-konto synkroniseras dina inställningar som standard. Du kan välja att synkronisera dina inställningar och styra vad som synkroniseras genom att gå till

Inställningar för synkronisering under OneDrive i Datorinställningar. Om du loggar in i Windows med ett domänkonto och du väljer att koppla det till ett Microsoft-konto tillfrågas du om vilka inställningar du vill synkronisera innan Microsoft-kontot kopplas.

Överst på sidan

Teredo-teknik

Funktionens uppgift

Teredo-teknik (Teredo) gör att datorer och nätverk kan kommunicera med flera nätverksprotokoll.

Insamlad, bearbetad eller överförd information

Varje gång du startar datorn, försöker Teredo hitta en öppen IPv6-tjänst (Internet Protocol version 6) på Internet. Detta sker automatiskt när datorn är ansluten till ett offentligt eller privat nätverk, men det sker inte i hanterade nätverk som företagsdomäner. Om du använder en app som kräver Teredo för att kunna använda IPv6-anslutningar, eller om du konfigurerar en brandvägg så att IPv6-anslutningar alltid är aktiverade, kommer Teredo att kontakta Microsoft Teredo-tjänsten via Internet med jämna mellanrum. Den enda information som skickas till Microsoft är standardinformation om datorn och namnet på den tjänst som efterfrågas (t.ex. teredo.ipv6.microsoft.com).

Användning av informationen

Informationen som skickas från din dator av Teredo används för att ta reda på om datorn är ansluten till Internet och om den kan hitta en öppen IPv6-tjänst. När tjänsten har hittats skickas information för att upprätthålla en anslutning till IPv6-tjänsten.

Val och kontroll

Med kommandotolksverktyget netsh kan du ändra frågan som tjänsten skickar via Internet så att andra servrar än Microsofts kontaktas i stället, eller så kan du stänga av den. Detaljerade anvisningar finns i avsnittet Internet Protocol Version 6, Teredo och relaterade tekniker i den här tekniska rapporten.

Överst på sidan

TPM-tjänster (Trusted Platform Module)

Funktionens uppgift

TPM (Trusted Platform Module) är säkerhetsmaskinvara som är inbyggd i vissa datorer. Om den finns och är allokerad kan datorn dra nytta av avancerade säkerhetsfunktioner. Några Windows-funktioner som utnyttjar TPM är diskkryptering, virtuellt smartkort, säker start, Windows Defender och TPM-baserade certifikatarkiv.

Insamlad, bearbetad eller överförd information

Som standard blir Windows ägare till TPM och lagrar den fullständiga auktoriseringsinformationen om TPM-ägaren så att den bara är tillgänglig för administratörer av Windows. Begränsade auktoriseringsvärden skapas för att utföra vanliga administrativa åtgärder och vanliga användaråtgärder och hanteras av Windows.

Med TPM-hanteringskonsolen kan du allokera TPM interaktivt och spara auktoriseringsvärdet för TPM-ägaren på externa medier, t.ex. ett USB-flashminne, efter det att TPM har allokerats. En sparad fil innehåller auktoriseringsinformationen om TPM-ägaren för TPM. Filen innehåller även datornamnet, operativsystemversionen, information om den skapande användaren och skapelsedatumet så att du känner igen filen.

I en domänmiljö kan domänadministratören bestämma att det fullständiga TPM-ägarlösenordet ska lagras i Active Directory under ett TPM-objekt när TPM allokeras.

Varje TPM har en unik kryptografisk bekräftelsenyckel som den använder för att visa att den är äkta. Bekräftelsenyckeln kan skapas och lagras i TPM av datortillverkaren, men på äldre datorer kanske Windows behöver initiera genereringen av nyckeln i TPM. Den privata delen av bekräftelsenyckeln är i säkert förvar i TPM, och när den har skapas brukar den inte gå att återställa. Ett bekräftelsenyckelcertifikat sparas i TPM på de flesta datorer med Windows. Bekräftelsenyckelcertifikatet visar att bekräftelsenyckeln finns i en maskinvaru-TPM. Certifikatet används av fjärrverifierare för att bekräfta att en TPM följer TPM-specifikationerna.

Bekräftelsenyckelcertifikatet brukar signeras av TPM-tillverkaren eller plattformtillverkaren.

Användning av informationen

När TPM har initierats kan appar använda den för att skapa och skydda ytterligare unika kryptografiska nycklar. Exempelvis använder diskkryptering TPM för att skydda nyckeln som krypterar enheten.

Om du väljer att spara TPM-ägarens lösenord i en fil ger informationen om datorn och användaren som sparas i filen dig möjlighet att identifiera motsvarande dator och TPM. TPM-bekräftelsenyckeln används av Windows under initieringen av TPM för att kryptera auktoriseringsvärdet för TPM-ägaren innan det skickas till TPM. Windows skickar inte kryptografiska nycklar till mottagare utanför datorn. Windows har ett gränssnitt för externa appar som skyddar mot skadlig kod. De kan använda bekräftelsenyckeln för vissa TPM-scenarier, t.ex. uppmätt start med attestering. För program som skyddar mot skadlig kod är bekräftelsenyckeln och nyckelns certifikat även användbara för att bekräfta startmätningar och tillhandahålls av en TPM från en viss tillverkare. Som standard är det bara administratörer och appar med administrativ behörighet som kan använda TPM-bekräftelsenyckeln.

Val och kontroll

Användare eller administratörer väljer själva att använda TPM genom att aktivera en funktion i Windows eller köra en app som använder TPM.

Du kan välja att rensa TPM och återställa den till fabriksinställningarna. När TPM rensas tas ägarinformationen bort, och med undantag av bekräftelsenyckeln samtliga TPM-baserade nycklar eller kryptografisk information som appar kan ha skapat när TPM användes.

Överst på sidan

Uppdatera rotcertifikat

Funktionens uppgift

Certifikat används huvudsakligen för att verifiera en persons eller enhets identitet, för att autentisera en tjänst eller för att kryptera filer. Betrodda rotcertifikatutfärdare är de organisationer som utfärdar certifikat. Uppdatera rotcertifikat kontaktar tjänsten Windows Update på nätet för att se om Microsoft har lagt till en certifikatutfärdare i listan med betrodda utfärdare, men bara då en app erhåller ett certifikat som har utfärdats av en certifikatutfärdare som inte är direkt betrodd (ett certifikat som inte lagras i en lista med betrodda certifikat på din dator). Om certifikatutfärdaren har lagts till i Microsofts lista med betrodda utfärdare, läggs dess certifikat till automatiskt i listan med betrodda certifikat på din dator.

Insamlad, bearbetad eller överförd information

Uppdatera rotcertifikat skickar en begäran till tjänsten Windows Update på nätet och ber om den aktuella listan med rotcertifikatutfärdare i Microsoft Root Certificate Program. Om det obetrodda certifikatet finns med i listan hämtar Uppdatera rotcertifikat det från Windows Update och sparar det i arkivet med betrodda certifikat på datorn. Informationen som överförs är bland annat rotcertifikatens namn och kryptografiska hashvärden.

Användning av informationen

Microsoft använder informationen för att uppdatera listan med betrodda certifikat på datorn. Microsoft använder inte den här informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Uppdatera rotcertifikat är aktiverat som standard. Administratörer kan konfigurera Grupprincip för att inaktivera Uppdatera rotcertifikat på en dator.

Överst på sidan

Uppdateringstjänster

Funktionens uppgift

I uppdateringstjänsterna för Windows ingår Windows Update och Microsoft Update:

- **Windows Update** är en tjänst som levererar programuppdateringar för Windows-programvara och annan stödprogramvara, t.ex. drivrutiner från enhetstillverkare.

- **Microsoft Update** är en tjänst som levererar programuppdateringar för Windows-programvara, samt för annan programvara från Microsoft, t.ex. Microsoft Office.

Insamlad, bearbetad eller överförd information

Uppdateringstjänsterna samlar in information från din dator som gör att Microsoft kan driva och förbättra tjänsterna, till exempel.:

- Microsoft-programvaran och andra stödprogram (till exempel drivrutiner och inbyggda program från enhetstillverkare) som är installerade på datorn som uppdateringstjänsterna har tillgängliga uppdateringar för. Det hjälper oss att avgöra vilka uppdateringar som är lämpliga för dig.

- Dina konfigurationsinställningar för Windows Update och/eller Microsoft Update, t.ex. om du vill att uppdateringar ska laddas ned eller installeras automatiskt.

- Vad som lyckas, vad som misslyckas och de fel du stöter på när du ansluter till och använder uppdateringstjänsterna.

- Plug and Play-ID-nummer för maskinvaruenheter – en kod som tilldelas av enhetstillverkaren och som identifierar enheten (t.ex. en viss tangentbordstyp).

- En globalt unik identifierare (GUID) – ett genererat slumptal som inte innehåller någon personlig information. GUID-värden används för att identifiera enskilda datorer utan att identifiera användaren.

- Namnet på BIOS, dess versionsnummer, leverantör och ändringsdatum – information om de nödvändiga programvarurutiner som testar maskinvaran, startar operativsystemet på datorn och överför data mellan maskinvaruenheterna som är anslutna till datorn.

- Tillverkare, modell, plattformsroll, och SKU-nummer – information om den dator som används för att aktivera diagnostikundersökningar vid installation av drivrutiner.

Du kan använda uppdateringstjänsterna genom att gå till Windows Update på Kontrollpanelen och kontrollera om det finns uppdateringar eller ändra dina inställningar så att Windows automatiskt kan installera uppdateringar när de blir tillgängliga (rekommenderas). I funktionen Windows Update kan du välja om du ska anmäla dig till Microsoft Update eller inte.

Om du väljer att hämta viktiga programuppdateringar för datorn kan verktyget Borttagning av skadlig programvara (MSRT) medfölja dessa uppdateringar. Verktyget Borttagning av skadlig programvara genomsöker datorn efter ofta förekommande skadlig programvara (malware) och gör det lättare att ta bort identifierade hot som kan smitta datorn. Om programvaran körs tar den bort skadliga program som finns publicerade på webbplatsen Microsoft Support. Under en genomsökning efter skadliga program skickas en rapport till Microsoft med specifik information om de skadliga program och fel som upptäcks samt annan information om din dator. Mer information finns i Windows sekretesspolicy för verktyget Borttagning av skadlig programvara .

Användning av informationen

Den information som skickas till Microsoft används till att driva och underhålla uppdateringstjänsterna. Den används också till att generera insamlingsstatistik som hjälper oss att analysera trender och förbättra våra produkter, inklusive uppdateringstjänsterna.

För att generera insamlingsstatistik används GUID-värdet som har samlats in av uppdateringstjänsterna för att spåra och registrera antalet enskilda datorer som använder uppdateringstjänsterna och huruvida nedladdningen och installationen av specifika uppdateringar lyckas eller misslyckas. Uppdateringstjänsterna registrerar GUID-värdet för den dator som försöker ladda ned och installera, ID:t för det objekt som begärdes, om uppdateringar var tillgängliga och standarddatorinformation.

MSRT-Informationen som beskrivs ovan används till att förbättra

våra produkter mot skadliga program och andra säkerhetsprodukter och tjänster. Ingen information i rapporterna om skadliga program används för att identifiera eller kontakta dig.

Uppdateringar som krävs

Om du aktiverar uppdateringstjänsterna måste en del programvarukomponenter i systemet som utgör eller är direkt relaterade till uppdateringstjänsterna då och då uppdateras. Dessa uppdateringar måste utföras innan tjänsten kan kontrollera, ladda ned eller installera andra uppdateringar. Dessa nödvändiga uppdateringar åtgärdar fel, levererar pågående förbättringar och upprätthåller kompatibiliteten med de Microsoft-servrar som stöder tjänsten.

Om uppdateringstjänsterna är inaktiverade, får du inte dessa uppdateringar.

Programuppdateringar som krävs för att installera eller uppdatera Windows Store-appar laddas ned och installeras automatiskt. Dessa uppdateringar krävs för att appar ska fungera korrekt.

Cookies och token

En token används ungefär som en cookie. Den lagrar information i en liten fil som placeras av uppdateringstjänsternas server på din hårddisk, och den används när din dator ansluter till servern för att upprätthålla en giltig anslutning. Den lagras bara på din dator – inte på servern. En cookie eller token innehåller information (t.ex. tidpunkten för den senaste genomsökningen) som gör att de senaste uppdateringarna hittas. Den innehåller information för styrning av vilket innehåll som ska laddas ned till datorn, när så ska ske samt ett GUID-värde för att identifiera datorn för servern.

Innehållet i en cookie eller token krypteras av servern (förutom förfallotiden). Den här cookien eller token är inte en webbläsarcookie och kan därför inte hanteras via webbläsarens inställningar. Du kan inte ta bort cookien eller token, men den används inte om du inte använder uppdateringstjänsterna.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows

aktiveras Windows Update och konfigureras så att uppdateringar installeras automatiskt.

Om du aktiverar uppdateringstjänsterna, oavsett vilken inställning du har valt, kommer nödvändiga uppdateringar för en del komponenter att laddas ned och installeras automatiskt utan föregående meddelande till dig. Om du föredrar att inte få nödvändiga uppdateringar inaktiverar du uppdateringstjänsterna.

Du kan också välja att kontrollera om det finns, eller automatiskt installera, viktiga och rekommenderade uppdateringar för din dator eller enbart viktiga uppdateringar. Valfria uppdateringar installeras aldrig automatiskt. Efter installationen av Windows kan du ändra inställningarna för Windows Update på Kontrollpanelen eller i Datorinställningar.

Om du har valt att söka efter och installera viktiga uppdateringar och verktyget Borttagning av skadliga program medföljer uppdateringarna för datorn kan du inaktivera programmets rapporteringsfunktion.

Överst på sidan

Virtuella privata nätverk

Funktionens uppgift

Ett virtuellt privat nätverk (VPN) låter dig ansluta till ett privat nätverk, t.ex. ett företagsnätverk, över Internet. En VPN-anslutning kan upprättas med VPN-klienten i Windows eller via en VPN-app från en tredje part.

Insamlad, bearbetad eller överförd information

När du ansluter till ett virtuellt privat nätverk skickas de autentiseringsuppgifter som du anger i VPN-klienten till fjärrnätverket. Du kan kanske lagra dessa autentiseringsuppgifter på datorn. När du har anslutit dirigeras en del eller all nätverksaktivitet genom fjärrnätverket (beroende på VPN-konfiguration). Administratörer kan konfigurera vissa appar att alltid dirigera sin trafik genom VPN-nätverket och att ansluta automatiskt till det privata virtuella nätverket när de startar. Ingen information skickas till Microsoft.

VPN-programvara från tredje part kan samla in ytterligare information. Insamlingen och användningen av den här informationen regleras av den tredje partens sekretesspolicy.

Användning av informationen

VPN-klienter använder de autentiseringsuppgifter som du anger för att autentisera mot fjärrnätverket och för att dirigera nätverkstrafik till och från fjärrnätverket. Om en VPN-klient från tredje part samlar in ytterligare information regleras användningen av den informationen av den tredje partens sekretesspolicy.

Val och kontroll

Du kan lägga till och ta bort en VPN-anslutning, och visa statusen för befintliga anslutningar, i **Nätverk** i Datorinställningar. När en VPN-anslutning har skapats kan du manuellt upprätta eller koppla från anslutningen genom att välja nätverket i listan i Inställningar.

Överst på sidan

Windows Customer Experience Improvement Program (CEIP)

Funktionens uppgift

Windows Customer Experience Improvement Program (CEIP) kan samla in information om hur du använder appar, datorer, anslutna tjänster och Windows. Det kan också samla in information om prestanda och tillförlitlighetsproblem som kan uppstå. Om du väljer att delta i Windows CEIP kommer Windows att skicka denna information till Microsoft och regelbundet ladda ned en fil för att samla in mer relevant information om hur du använder Windows och appar. CEIP-rapporterna skickas till Microsoft för att förbättra de funktioner som kunderna använder mest och för att skapa lösningar på vanliga problem.

Insamlad, bearbetad eller överförd information

CEIP-rapporter kan innehålla information som:

- Konfigurationsinformation, bland annat antalet processorer på datorn, antalet nätverksanslutningar som används, skärmupplösning för bildskärmsenheter och vilken Windows-

version som körs på datorn.

- Information om prestanda och tillförlitlighet, bland annat hur snabbt en app svarar när du klickar på en knapp, hur många problem du har haft med en app eller enhet och hur snabbt information skickas eller tas emot via en nätverksanslutning.

- Information om appanvändning, t.ex. information om de funktioner som du använder oftast, t.ex. hur ofta du öppnar appar, hur ofta du använder Windows Hjälp och support, vilka tjänster du använder för att logga in i appar och hur många mappar du normalt skapar på skrivbordet.

CEIP-rapporter kan också innehålla information om händelser (händelseloggdata) på din dator från upp till sju dagar innan du bestämde dig för att börja delta i CEIP. De flesta användare väljer att delta i CEIP i samband med installationen av Windows och Microsoft använder den här informationen för att analysera och förbättra installationen av Windows.

Information skickas till Microsoft när du är ansluten till Internet. CEIP-rapporter innehåller från början inte kontaktinformation, t.ex. ditt namn, din adress eller ditt telefonnummer, men en del rapporter kan oavsiktligt innehålla enskilda identifierare, t.ex. ett serienummer för en enhet som är ansluten till din dator. Microsoft filtrerar informationen i CEIP-rapporterna för att försöka få bort eventuella enskilda identifierare som de kan innehålla. Om enskilda identifierare tas emot använder Microsoft dem inte för att identifiera eller kontakta dig.

CEIP genererar ett slumptal, en så kallad global unik identifierare (GUID), som skickas till Microsoft med varje CEIP-rapport. GUID-värdet gör att vi kan fastställa vilken information som skickas från en viss dator. Vissa CEIP-rapporter kan också innehålla GUID-värden som kommer från ditt Microsoft-konto.

CEIP kan också regelbundet ladda ned en fil för att samla in mer relevant information om det sätt på vilket du använder Windows och appar. Windows använder den här filen för att samla in ytterligare information som Microsoft kan använda för att skapa lösningar på vanliga problem och för att bättre förstå

användningsmönster i Windows och appar.

Användning av informationen

Microsoft använder CEIP-informationen för att förbättra sina egna produkter och tjänster, liksom tredjepartsprogram och maskinvara som har utformats för användning med dessa produkter och tjänster. Vi kan också dela insamlad CEIP-information med Microsofts partner så att de kan förbättra sina produkter och tjänster, men den informationen får inte användas för att identifiera, kontakta eller skicka reklam till dig.

Vi använder GUID för att fastställa hur omfattande den feedback vi får är och hur den ska prioriteras. GUID-värdet gör det exempelvis möjligt för Microsoft att skilja en kund som upplevt ett problem hundra gånger från hundra kunder som har upplevt samma problem en gång var. Microsoft använder inte den information som samlats in av CEIP för att identifiera eller kontakta dig.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows aktiveras Windows CEIP: Windows och Microsoft-appar från Windows Store kan skicka CEIP-rapporter för alla användare på datorn. Om du väljer att anpassa inställningarna kan du hantera CEIP genom att välja **Skicka information till Microsoft om hur jag använder min dator, som en del i Programmet för kvalitetsförbättring** under **Hjälp till att förbättra Microsofts produkter och tjänster**. Efter installationen av Windows kan administratörer ändra den här inställningen i **Åtgärdscenter** på Kontrollpanelen.

Mer information finns i vanliga frågor och svar om CEIP.

Överst på sidan

Windows Defender

Windows Defender söker efter skadlig programvara och annan oönskad programvara på datorn. Funktionerna Microsoft Active Protection Service och Historik ingår.

Microsoft Active Protection Service

Om du använder Windows Defender kan Microsoft Active Protection Service (MAPS) bättre skydda datorn genom att automatiskt ladda ned nya signaturer för ny skadlig programvara som har identifierats och genom att övervaka datorns säkerhetsstatus. MAPS skickar information om skadlig programvara och annan oönskad programvara till Microsoft och kan även skicka filer som kan innehålla skadlig kod. Om MAPS upptäcker att datorn har smittats med vissa typer av skadlig programvara kan MAPS kontakta dig automatiskt via ditt Microsoft-konto för att hjälpa till att lösa problemet.

Insamlad, bearbetad eller överförd information

MAPS-rapporterna innehåller information om potentiellt skadliga filer, t.ex. filnamn, kryptografisk hash, programutgivare, storlek och datumstämplar. MAPS kan också samla in fullständiga URL:er som anger filernas ursprung, samt de IP-adresser som de potentiellt skadliga filerna ansluter till. Dessa URL-adresser kan ibland innehålla personlig information, t.ex. sökvillkor och data som du har angett i formulär. Rapporterna kan också innehålla de åtgärder som du vidtog när Windows Defender meddelade dig att eventuellt oönskad programvara hade upptäckts. MAPS tar med den här informationen för att hjälpa Microsoft att mäta hur effektivt Windows Defender kan upptäcka och ta bort skadlig kod och annan oönskad programvara, samt för att försöka identifiera nya skadliga program.

Rapporter skickas automatiskt till Microsoft när

- Windows Defender upptäcker programvara som inte har riskanalyserats än
- Windows Defender upptäcker ändringar på datorn som har utförts av programvara som inte har riskanalyserats än
- Windows Defender vidtar åtgärder mot skadliga program när sådana upptäcks (som en del av programmets automatiska reparationsfunktion)
- Windows Defender kör en schemalagd genomsökning och vidtar åtgärder på programvara som upptäcks baserat på dina inställningar

- Windows Defender söker igenom ActiveX-kontroller i Internet Explorer.

Om du väljer att gå med i MAPS när du installerar Windows får du ett grundläggande medlemskap. Rapporter från basmedlemmar innehåller den information som beskrivs i det här avsnittet. Rapporter från avancerade medlemskap är mer omfattande och kan ibland innehålla personlig information från t.ex. filsökvägar och ofullständiga minnesdumpar. De här rapporterna tillsammans med rapporterna från andra Windows Defender-användare som deltar i MAPS hjälper våra anställda att snabbare upptäcka nya hot. Definitioner för skadlig kod skapas sedan och de uppdaterade definitionerna görs tillgängliga för alla användare genom Windows Update.

Om du går med i MAPS kan Windows Defender skicka särskilda filer eller webbinnehåll från din dator som Microsoft bedömer som potentiellt oönskad programvara. Exempelrapporten används för ytterligare analys. Om det är troligt att en fil innehåller personlig information tillfrågas du innan den skickas. Om Windows Update inte har kunnat hämta uppdaterade signaturer för Windows Defender under en viss tid, försöker Windows Defender använda MAPS för att ladda ned signaturer från en annan nedladdningsplats.

All information som skickas till MAPS krypteras via SSL för att skydda din integritet.

För att kunna identifiera och åtgärda vissa typer av hot som kan smitta datorn skickar Windows Defender regelbundet information till MAPS om datorns säkerhetstillstånd. Den här informationen omfattar information om datorns säkerhetsinställningar och loggfiler som beskriver drivrutinerna och annan programvara som läses in när datorn startar. Ett tal som identifierar datorn unikt skickas också.

Användning av informationen

Rapporter som skickas till MAPS används för att förbättra Microsofts programvara och tjänster. Rapporterna kan också användas för statistik-, testnings- eller analyssyften och för att

generera definitioner. MAPS samlar inte avsiktligen in personlig information. I den utsträckning MAPS oavsiktligt kan samla in personlig information, använder inte Microsoft den för att identifiera, kontakta eller skicka reklam till dig.

Informationen om datorns säkerhetstillstånd som samlas in av MAPS används för att avgöra om vissa typer av skadlig programvara har smittat datorn. I det här fallet använder Microsoft kontaktinformationen i ditt Microsoft-konto för att kontakta dig med information om problemet och hur du kan lösa det.

Val och kontroll

Om du väljer standardinställningarna när du konfigurerar Windows aktiveras MAPS. Om du väljer att anpassa inställningarna kan du hantera MAPS genom att välja **Få bättre skydd mot skadlig kod genom att skicka information och filer till Microsoft Active Protection Service när Windows Defender är aktiverat** under **Dela information med Microsoft och andra tjänster**. Efter installationen av Windows kan du ändra ditt MAPS-medlemskap eller MAPS-inställningarna, och även inaktivera MAPS, på **Inställningar** -menyn i Windows Defender.

Om du får Borttagning av skadlig programvara via Windows Update kan verktyget skicka liknande information till MAPS även om Windows Defender är inaktiverat. Mer information finns i verktyget Borttagning av skadlig programvara i Windows .

Historikfunktionen

Funktionens uppgift

Historikfunktionen ger tillgång till en lista med alla appar på datorn som Windows Defender identifierar och de åtgärder som vidtogs när apparna identifierades.

Du kan också visa en lista med appar som Windows Defender inte övervakar när de körs på datorn (så kallade tillåtna objekt). Dessutom kan du visa en lista med appar som Windows Defender hindrar från att köra tills du väljer att ta bort dem eller tillåter dem att köra igen (så kallade objekt i karantän).

Insamlad, bearbetad eller överförd information

Listan med program som Windows Defender identifierar, de åtgärder som du och andra användare vidtar samt åtgärderna som Windows Defender vidtar lagras automatiskt på datorn. Alla användare kan granska historiken i Windows Defender och se skadlig kod och annan oönskad programvara som har försökt installera sig eller köras på datorn, eller som någon annan användare har tillåtit att köras. Om du exempelvis hör talas om ett nytt skadligt program kan du titta i historiken och se om Windows Defender har hindrat det från att infektera datorn. Ingen information skickas till Microsoft.

Val och kontroll

Historiklistor kan tas bort av en administratör.

Överst på sidan

Windows Felrapportering

Funktionens uppgift

Windows Felrapportering hjälper Microsoft och Microsofts partner att upptäcka problem i och tillhandahålla lösningar för den programvara som du använder. Det finns inte lösningar på alla problem, men om det finns en lösning får du steg-för-steg-instruktioner för hur du löser problemet du rapporterat eller också får du uppdateringar att installera. För att förhindra problem och göra programvaran mer pålitlig ingår en del lösningar också i Service Pack och framtida programversioner.

Insamlad, bearbetad eller överförd information

Många programvaruprodukter har utformats för att fungera med Windows Felrapportering. Om ett problem uppstår i någon av dessa produkter kan du bli tillfrågad om du vill rapportera det.

Windows Felrapportering samlar in information som kan användas för att diagnostisera och lösa problem. Exempel på den här informationen är var i program- eller maskinvaran som problemet uppstod, problemets typ eller allvarlighetsgrad, filer som kan innehålla mer information om problemet, grundläggande information om program- och maskinvara eller möjliga problem med programvarans prestanda och kompatibilitet. Om du använder

Windows som värd för virtuella datorer kan felrapporter som skickas till Microsoft innehålla information om virtuella datorer.

Windows Felrapportering samlar också in information om appar, drivrutiner och enheter för att hjälpa Microsoft att förstå och förbättra kompatibiliteten mellan appar och enheter. Informationen om en app kan innehålla namnen på appens körbara filer. Information om enheter och drivrutiner kan vara namnet på enheterna som du har installerat i datorn samt de körbara filer som är kopplade till enheternas drivrutiner. Information om företaget som publicerat en app eller drivrutin kan samlas in.

Om du väljer att aktivera automatisk rapportering när du konfigurerar Windows skickar rapporteringstjänsten automatiskt grundläggande information om var problemen uppstår. I vissa fall skickar rapporteringstjänsten automatiskt ytterligare information för att diagnostisera problemet, t.ex. en partiell ögonblicksbild av datorns minne. En del felrapporter kan oavsiktligt innehålla personlig information. En rapport som innehåller en ögonblicksbild av datorminnet kan exempelvis innehålla ditt namn, en del av ett dokument som du arbetar med eller data som du nyligen har skickat till en webbplats.

För att diagnostisera vissa typer av problem kan Windows Felrapportering skapa en rapport som innehåller ytterligare information, t.ex. loggfiler. Innan en rapport som innehåller den här extra informationen skickas tillfrågas du om du vill skicka rapporten, även om du har aktiverat automatisk rapportering.

När du har skickat en rapport kan du bli ombedd att ange mer information om problemet som har uppstått. Om du väljer att ange ditt telefonnummer eller din e-postadress blir din felrapport personligt identifierbar. Microsoft kan kontakta dig och be om ytterligare information för att lösa problemet som du rapporterat.

Windows Felrapportering genererar ett slumptal, en så kallad global unik identifierare (GUID), som skickas till Microsoft med varje rapport. GUID-värdet gör att vi kan fastställa vilken information som skickas från en viss dator. GUID innehåller inte någon personlig information.

Information skickas krypterad via SSL för att skydda din integritet.

Användning av informationen

Microsoft använder information om fel och problem som har rapporterats av Windows-användare för att förbättra Microsofts produkter och tjänster samt program- och maskinvara som är avsedd att användas tillsammans med dessa produkter och tjänster. Vi använder GUID-värdet för att bestämma hur omfattande den feedback vi får är och hur den ska prioriteras. GUID-värdet gör det exempelvis möjligt för Microsoft att skilja en kund som upplevt ett problem hundra gånger från hundra kunder som har upplevt samma problem en gång var.

Microsofts anställda, leverantörer, underleverantörer och partner kan få åtkomst till relevanta delar av den insamlade informationen, men har endast rätt att använda informationen för att reparera eller förbättra Microsofts produkter och tjänster eller programvara och maskinvara som utformats för att användas med Microsofts produkter och tjänster. Om en felrapport innehåller personlig information, använder inte Microsoft den för att identifiera, kontakta eller skicka reklam till dig. Om du däremot väljer att ange kontaktinformation enligt beskrivningen ovan kan vi använda denna information för att kontakta dig.

Val och kontroll

Om du väljer standardinställningarna när du konfigurerar Windows skickar Windows Felrapportering automatiskt grundläggande rapporter och söker efter lösningar på problem online. Om du väljer att anpassa inställningarna kan du hantera Windows Felrapportering genom att välja **Sök online efter lösningar på problem med hjälp av Windows Felrapportering** under **Sök efter lösningar på problem online**. Efter installationen av Windows kan du ändra inställningen i Åtgärdscenter på Kontrollpanelen.

Mer information finns i sekretesspolicyn för Microsofts felrapporteringstjänst.

Överst på sidan

Windows Filassociation

Funktionens uppgift

Windows Filassociation hjälper användarna att koppla filtyper till särskilda appar. Om du försöker öppna en filtyp och ingen app är associerad till den frågar Windows om du vill använda Windows Filassociation för att söka efter en app för filen, vilket även innebär att Windows Store genomsöks efter en kompatibel app. Appar som brukar associeras med filnamnstillägget visas.

Insamlad, bearbetad eller överförd information

Om du väljer att använda Windows Filassociation skickas filnamnstillägget (t.ex. docx eller pdf) och datorns visningsspråk till Microsoft. Resten av filnamnet skickas inte till Microsoft. När en filassociation till en viss app skapas skickas en unik identifierare för appen för att identifiera varje filtyps standardapp.

Användning av informationen

När du skickar in ett filnamnstillägg returnerar tjänsten en lista med de appar som Microsoft vet kan öppna filer med det tillägget. Såvida du inte väljer att ladda ned och installera en app, ändras inga associationer för filtypen.

Val och kontroll

När du försöker öppna en filtyp utan en associerad app kan du välja att använda Windows Filassociation om du vill. Ingen information om filassociationer skickas till Microsoft om du inte bestämmer dig för att använda tjänsten.

Överst på sidan

Hjälp om Windows

Windows Hjälp och support online

Funktionens uppgift

Om Windows Hjälp och support online har aktiverats får du tillgång till den senaste hjälpen och supporten när du är ansluten till Internet.

Insamlad, bearbetad eller överförd information

När du använder Windows Hjälp och support online skickas dina hjälpfrågor och förfrågningar om hjälpinnehåll till Microsoft när du klickar på en länk. Windows skickar en del information om datorns konfiguration för att hitta det mest relevanta hjälpinnehållet. Windows Hjälp och support online använder också standardwebbteknik som cookies.

Användning av informationen

Microsoft använder informationen för att returnera hjälpavsnitt som svar på dina sökfrågor, för att returnera de mest relevanta resultaten, för att utveckla nytt innehåll samt för att förbättra befintligt innehåll. Vi använder informationen om datorns konfiguration för att visa lämpligt hjälpinnehåll för den konfigurationen. Vi använder cookies och annan webbteknik för att göra det lättare att navigera i hjälpinnehållet och för att bättre förstå hur användarna använder Windows-onlinehjälpen.

Val och kontroll

Hjälp och support online är aktiverat som standard. Om du vill ändra den här inställningen trycker eller klickar du på ikonen **Inställningar** längst upp i fönstret Hjälp och support och markerar eller avmarkerar **Få hjälp online**. Om du vill rensa cookies som använts av Windows-hjälpen öppnar du Internetalternativ på Kontrollpanelen, klickar eller trycker på knappen **Ta bort** under **Webbhistorik**, markerar **Cookies och webbplatsdata**och klickar eller trycker på **Ta bort**. Om du väljer att blockera alla cookies (under Sekretess i Internetalternativ) sparas inga cookies av Windows-hjälpen.

Programmet för förbättring av hjälpfunktionen

Funktionens uppgift

Programmet för förbättring av hjälpfunktionen (HEIP) hjälper Microsoft att identifiera trender i hur våra kunder använder Windows Hjälp och support online så att vi kan förbättra sökresultaten och innehållets relevans.

Insamlad, bearbetad eller överförd information

HEIP skickar information till Microsoft om vilken Windows-version

som körs på din dator och om hur du använder Windows Hjälp och support, inklusive frågor som du anger när du söker i Windows Hjälp och support samt omdömen eller feedback om de hjälpavsnitt som returneras till dig. När du söker efter, bläddrar i eller lämnar omdömen och feedback om hjälpavsnitt skickas informationen till Microsoft.

HEIP genererar ett slumptal, en så kallad global unik identifierare (GUID), som skickas till Microsoft med varje HEIP-rapport. GUID-värdet gör att vi kan fastställa vilken information som skickas från en viss dator. GUID innehåller inte någon personlig information. GUID-värdet är fristående från de GUID-värden som används av Windows Felrapportering och Windows CEIP.

Användning av informationen

Insamlade data används för att identifiera trender och användningsmönster så att Microsoft kan förbättra innehållets kvalitet och relevans. Vi använder GUID för att bestämma hur omfattande problemen vi får är och hur de ska prioriteras. Till exempel gör GUID-värdet att Microsoft kan skilja en kund som upplevt ett problem hundra gånger från hundra kunder som har upplevt samma problem en gång.

Programmet för förbättring av hjälpfunktionen samlar inte avsiktligt in någon information som kan användas för att identifiera dig. Om du skriver sådan information i rutorna för sökning och feedback skickas informationen, men Microsoft använder den inte för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows går du automatiskt med i programmet för förbättring av hjälpfunktionen (Help Experience Improvement Program). Om du väljer att anpassa inställningarna kan du hantera inställningarna för programmet för förbättring av hjälpfunktionen genom att markera **Skicka information till Microsoft om hur jag använder hjälpen, som en del i programmet för förbättring av hjälpfunktionen** under **Hjälp till att förbättra Microsofts produkter och tjänster**. Efter installationen av Windows kan du ändra inställningen i Windows Hjälp och support.

Överst på sidan

Fjärrhjälp

Funktionens uppgift

Du kan använda Fjärrhjälp om du vill bjuda in någon att ansluta till datorn och hjälpa dig med ett datorproblem även om personen inte är i närheten. När anslutningen är gjord kan den andra personen se vad som händer på din dator. Om du tillåter det kan personen använda sin mus och sitt tangentbord för att styra din dator och visa hur du åtgärdar ett problem.

Insamlad, bearbetad eller överförd information

Fjärrhjälp skapar en krypterad anslutning mellan de två datorerna via Internet eller det lokala nätverket. När någon ansluter till din dator med hjälp av Fjärrhjälp får den personen tillgång till skrivbordet, alla öppna dokument och all personlig information som visas. Om du dessutom tillåter att den andra personen fjärrstyr din dator med sin mus eller sitt tangentbord kan han eller hon t.ex. ta bort filer och ändra inställningar. När anslutningen är upprättad utbyter Fjärrhjälp kontaktuppgifter, däribland användarnamnet, datorns namn och kontobilden. Alla fjärrhjälpsanslutningar dokumenteras i en sessionsloggfil.

Användning av informationen

Informationen används för att upprätta en krypterad anslutning och för att ge den andra personen tillgång till skrivbordet. Ingen information skickas till Microsoft.

Val och kontroll

Innan du låter någon ansluta till datorn stänger du alla öppna program och dokument som du inte vill visa för den som hjälper dig. Tryck på Esc om du vill avsluta sessionen för att du anar oråd med vad personen ser eller gör på datorn. Du kan inaktivera sessionsloggning och utbytet av kontaktuppgifter genom att avmarkera dessa alternativ i inställningarna för Fjärrhjälp.

Överst på sidan

Windows Search

Funktionens uppgift

Med Windows Search kan du söka på enheten och Internet från samma plats. För att kunna returnera bättre sökresultat kan Windows Search använda Bing och Windows-positioneringsplattformen. Observera att det finns andra separata sökfunktioner från Microsoft på enheten, till exempel sökning i Windows Store, Internet Explorer och andra Microsoft-produkter.

Insamlad, bearbetad eller överförd information

Om du väljer att få sökresultat från webben skickar Windows det du skriver i Windows Search till Microsoft. För att förbättra sökresultatet skickar Windows Search även information till Microsoft om hur du använder funktionen. Windows Search skickar också ett ID för att kunna returnera personligt anpassade sökresultat baserat på hur du använder Bing och andra produkter och tjänster från Microsoft. Om du loggar in i Windows med ett Microsoft-konto kopplas ID:t till ditt Microsoft-konto. Du kan välja att inte få personligt anpassade resultat i Windows Search. Om du gör det skickas inte ID:t.

Om du tillåter att Windows Search använder din plats skickas din fysiska position, som fastställs av Windows-positioneringsplattformen, till Microsoft som en del av varje sökförfrågan. Vi kan också försöka hämta din ungefärliga fysiska position baserat på din IP-adress.

När du använder Windows Search för att söka i en app lämnas dina sökord till appen.

Användning av informationen

Om du väljer att använda Windows Search för att hämta sökresultat från webben använder vi det sökord som du anger, din sökhistorik på den lokala datorn och på webben, information som associeras med ditt Microsoft-konto samt enhetens position för att returnera relevanta sökförslag, personligt anpassade sökresultat och personliga upplevelser i andra produkter och tjänster från Microsoft. Mer information om hur dina data används finns i

sekretesspolicyn för Bing.

Om du använder Windows Search för att söka i en app från tredje part omfattas användningen av den insamlade informationen av den tredje partens sekretesspolicy. Om du söker i en app från Microsoft förklaras appens sekretesspraxis i tillhörande sekretesspolicy.

Val och kontroll

Om du väljer standardinställningarna när du konfigurerar Windows tillåter du att Windows Search hämtar sökförslag och webbresultat samt att Microsoft använder data från Windows Search (även din plats) för att anpassa Windows Search och andra Microsoft-upplevelser. Om du väljer att anpassa inställningarna kan du välja om du vill ändra dessa inställningar för Windows Search. Efter installationen av Windows kan du ändra de här inställningarna i **Sök** i Datorinställningar.

Du kan rensa din lokala sökhistorik och viss sökhistorik i Bing som används för att anpassa din Windows Search-upplevelse i **Sök** i **Sök och appar** i Datorinställningar. När din sökhistorik rensas instrueras Microsoft att inte använda tidigare insamlad sökhistorik för att anpassa sökförslag eller sortera sökresultat. Det innebär inte att reklaminformation eller annan anpassningsinformation rensas (inklusive information som kommer från din sökhistorik) eller att information som används av Microsoft i samlat format för att förbättra sökresultat och andra Microsoft-upplevelser tas bort. Den informationen sparas och förblir anonym, enligt sekretesspolicyn för Bing. Du kan hantera Microsoft-reklam och annan anpassningsinformation online.

Överst på sidan

Installation av Windows

I det här avsnittet beskrivs funktioner som är tillgängliga som en del av installationsprocessen för Windows.

Dynamisk uppdatering

Funktionens uppgift

Med Dynamisk uppdatering kan Windows köra en engångskontroll mot Windows Update för att hämta de senaste uppdateringarna till din dator när Windows installeras. Om Dynamisk uppdatering hittar några uppdateringar så laddas de ned och installeras automatiskt, så att din dator är fullständigt uppdaterad första gången du loggar in på eller använder den.

Insamlad, bearbetad eller överförd information

För att kunna installera kompatibla drivrutiner skickar Dynamisk uppdatering information om din dators maskinvara till Microsoft. Dynamisk uppdatering kan ladda ned följande uppdateringar till din dator:

- **Installationsuppdateringar.** Viktiga programuppdateringar för installationsfiler som säkerställer en lyckad installation.
- **Uppdateringar av medföljande drivrutiner.** Viktiga drivrutinsuppdateringar för den Windows-version som du installerar.

Dessutom, om du installerar Windows från Windows Store kommer Dynamisk uppdatering att ladda ned och installera de senaste uppdateringarna av Windows samt vissa drivrutiner till maskinvara som din dator behöver.

Användning av informationen

Dynamisk uppdatering skickar information om datorns maskinvara till Microsoft så att lämpliga drivrutiner för ditt system kan identifieras.

Val och kontroll

Om du installerar Windows från Windows Store laddar installationsprogrammet ned uppdateringar och installerar dessa automatiskt. Om du installerar Windows från fysiska media tillfrågas du om du vill ansluta till Internet och installera uppdateringar.

Installationsförbättringsprogram

Funktionens uppgift

Funktionen skickar en enda rapport till Microsoft, och den innehåller grundläggande information om din dator och om hur du har installerat Windows. Microsoft använder informationen för att förbättra installationen och för att ta fram lösningar på vanliga installationsproblem.

Insamlad, bearbetad eller överförd information

Rapporten innehåller vanligen information om din installation, t.ex. installationsdatum, den tid varje installationsfas tog att slutföra, om installationen var en uppgradering eller en ny installation av produkten, versionsinformation, operativsystemets språk, medietyp, datorkonfiguration och status för lyckad eller felaktig installation tillsammans med eventuella felkoder.

Om du väljer att delta i installationsförbättringsprogrammet skickas rapporten till Microsoft när du ansluter till Internet. Installationsförbättringsprogrammet genererar ett slumptal, en så kallad global unik identifierare (GUID), som skickas till Microsoft tillsammans med rapporten. GUID-värdet gör att vi kan fastställa vilken information som skickas från en viss dator. GUID-värdet innehåller ingen personlig information och används inte för att identifiera dig.

Användning av informationen

Microsoft och våra partner använder rapporten för att förbättra våra produkter och tjänster. Vi använder GUID för att korrelera informationen med data som har samlats in av CEIP i Windows (Customer Experience Improvement Program), ett program som du kan välja att delta i när du använder Windows.

Val och kontroll

Du kan välja att delta i programmet när du installerar Windows genom att markera **Jag vill hjälpa till att förbättra Windows-installationen** .

Mer information finns i avsnittet Windows CEIP.

Kompatibilitetskontroll för installationer

Funktionens uppgift

När du installerar Windows kontrollerar installationsprogrammet

om den dator du har nu kan uppgraderas till Windows 8.1 och visar kompatibilitetsinformation om dina program och enheter.

Insamlad, bearbetad eller överförd information

När vi undersöker kompatibiliteten samlar vi in viss information om hur uppgraderingen kan komma att fungera, till exempel datorns maskinvarufunktioner, vilka enheter som är anslutna till datorn och vilka program som har installerats på datorn. Ibland kan programutgivarens information innehålla information som utgivarens namn eller e-postadress.

Användning av informationen

Vi använder den insamlade informationen för att avgöra vilka drivrutiner som passar din dator samt för att kontrollera om din dator, dina program och dina enheter är kompatibla med Windows 8.1. Vi kan också använda den för att förbättra våra produkter och tjänster. Vi använder inte den här informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du installerar Windows från Windows Store eller från fysiska media inuti en befintlig Windows-installation kommer den information som beskrivs i det här avsnittet att skickas till Microsoft. Om du startar datorn från fysiska installationsmedia för att installera Windows kommer installationsprogrammet inte att leta efter kompabilitetsinformation online.

Överst på sidan

Windows Share

Funktionens uppgift

Med Windows Share kan du dela innehåll mellan Windows Store-appar som stöder delning. Du kan även dela innehåll med dina vänner.

Insamlad, bearbetad eller överförd information

När du delar något överför källappen innehållet till målappen först när du har valt målet i rutan Dela. Om källappen inte har

implementerat delning har du möjlighet att dela en bild av det som visas på skärmen. Målappar och personer som du delar innehåll med ofta visas i en lista i rutan Dela så att du når dem lättare. Ingen information skickas till Microsoft.

Användning av informationen

Informationen som lagras om hur ofta du delar med målappar och de personer som du ofta delar innehåll med används för att sortera listan i rutan Dela i frekvensordning. Om du delar information med ett externt företags app regleras användningen av informationen som samlas in av företagets sekretesspolicy. Om du delar från en Microsoft-app förklaras appens sekretesspraxis i tillhörande sekretesspolicy.

Val och kontroll

Som standard lagrar Windows information om hur du använder Windows Share. Du kan välja att sluta lagra den här informationen eller ta bort alla lagrade mål i **Dela** under **Sök och appar** i Datorinställningar.

Överst på sidan

Windows SmartScreen

Funktionens uppgift

Windows SmartScreen skyddar datorn genom att söka efter skadlig programvara och potentiellt skadligt innehåll i nedladdade filer och webbinnehåll. En varning visas i Windows innan en okänd eller potentiellt osäker fil som du har laddat ned öppnas. Om SmartScreen upptäcker potentiellt osäkert webbinnehåll i en app visas en varning i Windows i stället för innehållet.

Insamlad, bearbetad eller överförd information

Om du väljer att använda Windows SmartScreen för att kontrollera filer som har laddats ned skickar Windows information till SmartScreen-onlinetjänsten. Informationen kan innehålla ett filnamn, en filidentifierare (ett ”hashvärde”) och digital certifikatinformation samt standardinformation om datorn och Windows SmartScreen-filtrets versionsnummer. Den information

som du skickar till Microsoft krypteras via SSL för att skydda din integritet.

Om du väljer att använda Windows SmartScreen för att blockera potentiellt osäkert innehåll i appar skickar Windows information till SmartScreen-onlinetjänsten, inklusive de adresser och typer av innehåll som vissa Windows Store-appar kommer åt när du använder dem. Onlinetjänsten meddelar sedan din dator om innehållet har rapporterats som osäkert eller misstänkt till Microsoft. Rapporter som skickas till Microsoft innehåller information som appens namn eller identifierare och de fullständiga adresserna för webbinnehåll som appen ansluter till.

Den information du skickar till Microsoft krypteras för att skydda din integritet. Information som kan associeras med en webbsida som en app använder, t.ex. sökvillkor, kan ingå i adressen som skickas till Microsoft. Om du till exempel söker efter ett ord i en ordboksapp kan ordet som du söker efter skickas till Microsoft som en del av den fullständiga adressen som appen använder. Microsoft filtrerar dessa adresser för att försöka avlägsna personlig information när detta är möjligt.

Windows genererar ett tal, en så kallad global unik identifierare (GUID), som skickas till Microsoft med varje rapport. GUID-värdet gör att vi kan fastställa vilken information som skickas från en viss dator. GUID innehåller inte någon personlig information.

Användning av informationen

Microsoft använder den information som beskrivs ovan för att varna dig om potentiellt osäkra nedladdade filer och innehåll i appar. Om SmartScreen exempelvis identifierar ett potentiellt hot i en app som stöder SmartScreen visar Windows en varning i stället för innehållet. Vi använder också informationen för att förbättra SmartScreen och andra produkter och tjänster. Microsoft använder inte informationen för skicka reklam till dig.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows aktiveras Windows SmartScreen. Om du väljer att anpassa inställningarna kan du hantera Windows SmartScreen genom att

välja **Använd SmartScreen-onlinetjänsterna för att skydda datorn mot skadligt innehåll på webbplatser som läses in av Windows Store-appar och Internet Explorer samt mot skadliga nedladdningar** under **Skydda datorn och din integritet**. Efter installationen av Windows kan du ändra inställningen i Åtgärdscenter på Kontrollpanelen. Information om SmartScreen-filtret i Internet Explorer finns i avsnittet om SmartScreen-filtret i sekretesspolicyn för Internet Explorer.

Överst på sidan

Windows Taligenkänning

Funktionens uppgift

Windows Taligenkänning tillhandahåller taligenkänning i Windows och i alla appar som väljer att använda funktionen. Precisionen i Windows Taligenkänning ökar genom att funktionen lär sig hur du använder språket, t.ex. ljud och ord som du ofta använder.

Insamlad, bearbetad eller överförd information

Windows Taligenkänning lagrar en lista med ord och deras uttal på datorn. Ord och uttal läggs till i listan med hjälp av ordlistan och genom att Windows Taligenkänning används för att diktera och korrigera ord.

Om funktionen för dokumentgranskning i Windows Taligenkänning är aktiverad samlas text från Microsoft Office Word-dokument (med filnamnstilläggen .doc eller .docx) och e-postmeddelanden (från andra e-postmappar än Borttaget och Skräppost) på datorn och på alla anslutna filresurser som har tagits med i sökindexplatserna i Windows in och lagras i fragment med ett, två eller tre ord. Fragment med ett ord omfattar enbart ord som du har lagt till i anpassade ordlistor och fragment med två eller tre ord omfattar bara ord som finns i standardordlistor.

All information som samlas in lagras i din standardprofil för tal på datorn. Talprofiler lagras för varje användare, och användarna kan inte komma åt andra användares profiler på datorn. Administratörer kan emellertid komma åt alla profiler på datorn. Profilinformationen skickas inte till Microsoft såvida du inte väljer

att skicka den när du tillfrågas i Windows Taligenkänning. Du kan granska uppgifterna innan de skickas. Om du väljer att skicka informationen skickas även de data om akustisk anpassning som användes för att anpassa dina ljudegenskaper.

I samband med taligenkänningssessioner tillfrågas du av Windows Taligenkänning om du vill skicka din talprofil till Microsoft. Du kan granska informationen innan den skickas. Uppgifterna kan gälla inspelningar av din röst då du genomförde sessionen och annan information från din talprofil.

Användning av informationen

Windows Taligenkänning använder ord från din talprofil för att omvandla tal till text. Microsoft använder informationen i din personliga talprofil för att förbättra sina produkter och tjänster. Vi använder inte den här informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Du kan välja om du vill köra Windows Taligenkänning eller inte. Om du kör Windows Taligenkänning granskas dokumenten som standard. Du kan ändra inställningarna för granskning av dokument den första gången du kör Windows Taligenkänning. Du kan ändra inställningarna för dokumentgranskning eller ta bort personliga talprofiler (och det mesta av uppgifterna om dokumentgranskning) genom att öppna Taligenkänning på Kontrollpanelen och klicka på **Avancerade talalternativ**. Du kan även använda alternativet Ändra befintliga ord i ordlistan och ta bort ord som du har lagt till i talprofilen. Även om du tar bort din talprofil tas inte de ord som har lagts till i den via ordlistan bort.

Du kan bestämma på vilka platser ordfragment samlas in genom att ändra vilka platser som tas med i sökindexet i Windows. Öppna Indexeringsalternativ på Kontrollpanelen om du vill visa eller ändra vilka platser som tas med i sökindexet i Windows.

I slutet av varje träningssession får du frågan om du vill skicka träningsuppgifter och annan profilinformation till Microsoft. Du kan även skicka information när Windows Taligenkänning startas genom att högerklicka på **Mikrofon**och sedan klicka på **Hjälp till**

att förbättra taligenkänning. I bägge fallen kan du granska alla datafiler innan de skickas och kan välja att inte skicka dem.

Överst på sidan

Windows Store

Med Windows Store kan du söka efter, hantera och installera appar på datorn. Avsnitten nedan beskriver hur funktionerna i Store – och apparna som du hämtar via Store – skulle kunna påverka din integritet och vad du kan göra för att kontrollera detta.

Store-appar och tjänsten

Funktionens uppgift

I Store kan du hitta och installera appar på datorn. Programmet håller även reda på vilka Store-appar som du har installerat, så att du kan hämta uppdateringar till dem och installera dem på fler än en dator.

Insamlad, bearbetad eller överförd information

För att kunna söka efter och installera appar måste du logga in i Store med ett Microsoft-konto. På så sätt får Store tillgång till informationen i din Microsoft-kontoprofil, t.ex. ditt namn, din e-postadress och din profilbild. Store samlar in och kopplar följande ytterligare information till ditt Store-konto:

- Betalningar till Store. Information om vad du har köpt, hur mycket och hur du betalade när du köpte appar eller något i appar med ditt Store-konto.

- Appar som du har installerat. Listan med appar som du har installerat från Store, licenspolicyn för varje app (permanent licens eller en tidsbegränsad provversion) och en lista med alla köp som du har gjort med ditt Store-konto i varje app. Utöver att lagra denna information på Internet i ditt Store-konto lagrar Store licensinformation på din dator för varje app som du installerar. Denna information visar att du äger licensen.

- Datorer som du har installerat appar på. Märket, modellen och datornamnet på varje dator som du installerar appar på

jämte ett nummer som identifierar datorn unikt. Numret genereras utifrån datorns maskinvarukonfiguration och innehåller inte någon information om dig.

- Omdömen, recensioner och problemrapporter. När du har installerat en app kan du skriva en recension eller ange ett omdöme i Store. Ditt Microsoft-konto kopplas till dessa omdömen. Om du skriver en recension publiceras namnet och bilden från ditt Microsoft-konto med recensionen.

- Store-inställningar. Inställningar som du väljer för att visa appar i Store, t.ex. om du bara vill visa appar som är tillgängliga på ditt modersmål.

Du kan välja att lagra dina betalningsuppgifter, t.ex. ditt kreditkortsnummer, i ditt Store-konto. Av säkerhetsskäl skickas den här informationen via SSL, och alla utom de sista fyra siffrorna i ditt kreditkortsnummer lagras krypterade.

Store samlar in viss information om ditt exemplar av Windows för att ta reda på om produkten såldes av en återförsäljare, är en utvärderingsversion, är föremål för ett volymlicensprogram eller förinstallerades av datortillverkaren. Första gången du ansluter till Store skickas en lista över alla appar som är förinstallerade på datorn till Store, som sedan associerar licenser för dessa appar med ditt Store-konto.

När du besöker och använder appar från Store samlar Microsoft in viss information som används för att identifiera och förstå användningsmönster och trender, på liknande sätt som många webbplatser analyserar sina besökares webbanvändning.

Användning av informationen

Microsoft använder dina kontaktuppgifter för att skicka dig de e-postmeddelanden som krävs för att tillhandahålla Stores tjänster, t.ex. kvitton för appar som du köper. Dina betalningsuppgifter används så att du kan betala för det du köper; om du väljer att lagra den här informationen slipper du ange den varje gång. Microsoft använder informationen om dina köp för att driva Store och för att ge kundsupport.

Store håller reda på alla appar som du har installerat. Du kan använda Store för att hantera listan med enheter som du har installerat appar på, och kundtjänsten kan även hjälpa dig att hantera dessa uppgifter. När du installerar en app visas den i köphistoriken i Store, även om du väljer att avinstallera den. Den här listan används även för att begränsa hur många datorer du kan installera appar på, enligt beskrivningen i användningsvillkoren för Windows Store. När du recenserar en app publiceras namnet och profilbilden som hör till ditt Windows-konto intill recensionen i Store. Om du rapporterar ett problem med en app får representanter för Store tillgång till den för bedömning och åtgärd. De kan använda ditt namn och den e-postadress som hör till Store-kontot för att kontakta dig när de granskar rapporten, om det skulle visa sig vara nödvändigt.

När det finns tillgängliga uppdateringar för appar som du har installerat visas ett meddelande i Store, och antalet tillgängliga uppdateringar visas på Stores panel. Du kan då se listan med tillgängliga uppdateringar och välja vilka du vill installera. Uppdaterade appar kan använda andra funktioner i Windows än de tidigare versionerna, vilket kan ge apparna tillgång till andra resurser på datorn. Du kan se de ändrade listorna med funktioner på sidan Appbeskrivning. Det finns en länk dit från sidan med de tillgängliga uppdateringarna.

Store använder informationen som samlas in om ditt exemplar av Windows för att ta reda på hur Windows installerades på din dator (t.ex. om datortillverkaren gjorde det). Store använder den här informationen för att ge dig tillgång till appar som tillverkaren vill erbjuda sina kunder. Den används även för att ge information till Microsoft (och i vissa fall i samlat format till tillverkaren) om användningsmönster för Windows.

Microsoft använder vissa data om appköp och användning i samlat format för att ta reda på hur kunderna använder Store (t.ex. hur användarna hittar de appar de installerar). Microsoft kan lämna ut vissa delar av denna samlade statistik till apputvecklare. Microsoft lämnar aldrig ut någon personlig information om dig till apputvecklare. Vi använder de surfnings- och användningsdata som Store samlar in för att skaffa oss en bättre bild av hur

kunderna använder Store och för att förbättra funktionerna och tjänsterna.

Val och kontroll

Om du väljer att använda Store skickas informationen som beskrivs i det här avsnittet till Microsoft i enlighet med vad som anges ovan.

Om du vill ta bort en recension som du har publicerat för en app går du till appbeskrivningen i Store, redigerar recensionen och tar bort all text.

Automatiska appuppdateringar

Funktionens uppgift

Den här funktionen söker efter, laddar ned och installerar uppdateringar för Windows Store-appar så att du alltid har de senaste versionerna. Exempel på appuppdateringar är säkerhetsuppdateringar, prestandauppdateringar, nya funktioner och nytt innehåll. Uppdaterade appar kan använda andra funktioner i Windows än de tidigare versionerna, vilket kan ge apparna tillgång till andra resurser på datorn. Information om funktionsändringar finns på sidan med appens produktbeskrivning Windows Store.

Insamlad, bearbetad eller överförd information

För att Store ska kunna tillhandahålla automatiska uppdateringar skickas följande information till Microsoft:

- En lista med samtliga appar som har installerats från Store av alla användare av datorn
- Licensinformationen för respektive app
- Vad som lyckas, vad som misslyckas och de fel du stöter på när du uppdaterar appar från Store
- En globalt unik identifierare (GUID) – ett genererat slumptal som inte innehåller någon personlig information
- Namn, revisionsnummer och revisionsdatum för BIOS
- Grundläggande information om datorn, t.ex. tillverkare, modell och den Windows-utgåva som du använder

Användning av informationen

Den här informationen används för att tillhandahålla uppdateringstjänsten. Den används också för att generera statistik som hjälper oss att analysera trender och förbättra våra produkter och tjänster. Informationen används inte för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows söker Windows Store efter, laddar ned och installerar appuppdateringar automatiskt, även om du är utloggad från Windows Store. Om du inaktiverar automatiska appuppdateringar kan du välja om du vill installera appuppdateringar när du loggar in i Windows Store.

Så här inaktiverar du automatiska appuppdateringar:

1. Öppna Windows Store.
2. Svep från högra kanten av skärmen och tryck på **Inställningar**.

   Om du använder en mus pekar du i det nedre högra hörnet av skärmen och klickar på **Inställningar**.
3. Tryck eller klicka på **Appuppdateringar**.
4. Tryck eller klicka på **Uppdatera mina appar automatiskt** om du vill inaktivera automatiska appuppdateringar.

Information om vad den senaste versionen av appen kan göra och information om när en app senast uppdaterades finns på sidan med appens produktbeskrivning i Windows Store.

Store-appars behörighet

Funktionens uppgift

Många appar som du installerar från Windows Store är utformade för att utnyttja särskilda maskinvaru- och programfunktioner på datorn. Exempelvis kan en fotoapp behöva använda din webbkamera, och en restaurangguide kan behöva veta var du

befinner dig för att kunna ge rekommendationer om restauranger i närheten.

Insamlad, bearbetad eller överförd information

Här är en lista med funktioner som appar måste tala om att de använder:

- Din Internetanslutning. Tillåter apparna att ansluta till Internet.
- Inkommande anslutningar via en brandvägg. Tillåter appen att skicka information till eller från din dator via en brandvägg.
- Ett hem- eller arbetsplatsnätverk. Tillåter appen att skicka information mellan din dator och andra datorer i samma nätverk
- Dina bilder, dina videor, din musik eller dina dokumentbibliotek. Tillåter appen att komma åt, ändra eller ta bort filer i dina bibliotek. Detta omfattar åtkomst till alla övriga data som är inbäddade i dessa filer, t.ex. platsinformation i foton.
- Flyttbart lagringsmedium. Tillåter appen att komma åt, lägga till, ändra eller ta bort filer på en extern hårddisk, ett USB-flashminne eller en bärbar enhet.
- Dina autentiseringsuppgifter för Windows. Tillåter att appen använder dina inloggningsuppgifter för att autentisera sig och ge tillgång till ett företags intranät.
- Certifikat som lagras på datorn eller ett smartkort. Tillåter appen att använda certifikat för att ansluta säkert till organisationer som banker, myndigheter eller din arbetsgivare.
- Datorns textmeddelandefunktion. Tillåter appen att skicka och ta emot textmeddelanden.
- Din webbkamera och mikrofon. Tillåter appen att ta bilder och spela in ljud och video.

- Din plats. Tillåter appen att ta reda på ungefär var du befinner dig med hjälp av en GPS eller nätverksinformation.
- Datorn funktion för kommunikation på nära håll. Tillåter appen att ansluta till andra enheter i närheten som samma app körs på.
- Dina bärbara enheter. Tillåter appen att kommunicera med enheter som din mobiltelefon, digitalkamera eller bärbara musikspelare.
- Din information på en bärbar enhet. Tillåter appen att komma åt, lägga till, ändra eller ta bort kontakter, kalendrar, uppgifter, anteckningar, statusar eller ringsignaler på din bärbara enhet.
- Ditt mobila bredbandskonto. Tillåter appen att hantera ditt mobila bredbandskonto.

Funktionerna som en app använder listas på appens beskrivningssida. Om du installerar en app tillåter Windows att appen använder dessa funktioner, förutom för plats, textmeddelanden, webbkamera och mikrofon, som betraktas som särskilt känsliga. Första gången en app begär åtkomst till någon av dessa känsliga funktioner tillfrågas du om du vill tillåta att appen använder den. Du kan när som helst ändra dig angående detta.

Förutom ovanstående tillstånd tillfrågas du också om en app begär information från en enhet som lagrar information om dig eller ditt beteende. Om du till exempel ansluter till en fitnessenhet som spårar din plats tillfrågas du om du vill lämna ut din position.

Användning av informationen

Apparnas användning av dessa funktioner regleras av utvecklarens sekretesspolicy. Om en app använder någon av de känsliga funktioner som beskrivs ovan finns det en länk till apputgivarens sekretesspolicy på appbeskrivningssidan i Store.

Val och kontroll

Du kan se vilka funktioner en app behöver i Store innan du installerar den. Windows frågar om du vill tillåta eller neka åtkomst

till de mest känsliga av dessa funktioner – din plats, textmeddelanden, webbkameran och mikrofonen – den första gången varje app använder dem.

När du läser en apps beskrivning i Windows Store ser du en förkortad lista med de funktioner som appen använder längst ned i den vänstra kolumnen. Den fullständiga listan finns på sidan Detaljer i appbeskrivningen. När du har installerat en app kan du se den fullständiga listan med de funktioner den använder när som helst och bestämma tillgången till de särskilt känsliga funktionerna. Det gör du genom att öppna appen, öppna **Inställningar**och sedan välja **Behörigheter**.

Anpassad Store-sökning och apprekommendationer

Funktionens uppgift

När du bläddrar bland eller söker efter appar i Windows Store visar Microsoft rekommendationer och sökresultat för att hjälpa dig att hitta relevanta appar.

Insamlad, bearbetad eller överförd information

För att förbättra sökresultaten skickar Windows Store information till Microsoft om hur du använder Windows Store, t.ex. vad du söker efter och vilket sökresultat du väljer. Windows Store skickar också en identifierare som associeras med ditt Microsoft-konto för att kunna returnera personligt anpassade sökresultat baserat på hur du använder Bing och andra produkter och tjänster från Microsoft. Du kan välja att inte få personligt anpassade resultat. Om du gör det skickas inte identifieraren.

Användning av informationen

Store använder identifieraren som associeras med ditt Microsoft-konto för att kunna erbjuda personligt anpassade sökresultat och rekommendationer baserat på hur du använder Store och andra produkter och tjänster från Microsoft, till exempel Bing och Windows Phone Store. Detta omfattar information som vilka appar du har köpt, profilinformation som du har uppgett i ditt Microsoft-konto och dina omdömen samt recensioner av appar. Den här informationen kan också användas för att anpassa andra produkter

och tjänster från Microsoft.

Val och kontroll

När du är inloggad i Windows med ett Microsoft-konto är personligt anpassade resultat och rekommendationer i Windows Store aktiverat som standard. Du kan välja att inte få personligt anpassade resultat och rekommendationer från Store under **Inställningar** i Store-inställningarna.

Hjälp till att göra Windows Store ännu bättre genom att skicka URL:er till webbinnehåll som appar använder

Funktionens uppgift

Vissa appar från Store liknar webbplatser och kan utsätta din dator för program som kan vara osäkra, t.ex. skadlig programvara. Om du väljer att aktivera den här funktionen samlar den in information om webbinnehållet som används av dessa appar och hjälper på så vis Microsoft att identifiera potentiellt osäkert beteende. Microsoft kan till exempel använda den här informationen för att ta bort en app från Store.

Insamlad, bearbetad eller överförd information

Om du väljer att skicka information om webbinnehållet som används av dina appar samlar Microsoft in information om URL:erna och typerna av innehåll som dessa appar använder. Det hjälper oss att identifiera vilka av apparna som tar emot innehåll från skadliga eller osäkra webbplatser. Rapporter som skickas till Microsoft innehåller information som appens namn eller identifierare, de fullständiga webbadresserna som apparna ansluter till och fullständiga webbadresser som anger platsen för eventuell JavaScript-kod som appen använder. Windows genererar ett tal, en så kallad global unik identifierare (GUID), som skickas till Microsoft med varje rapport. GUID-värdet gör att vi kan fastställa vilken information som skickas från en viss dator. GUID-värdet innehåller ingen personlig information och används inte för att identifiera dig.

Den information du skickar till Microsoft krypteras för att skydda din integritet. Information som kan associeras med en webbsida som apparna använder kan ingå, t.ex. sökvillkor och data som du

har angett i apparna. Om du till exempel slår upp ett ord i en ordboksapp kan informationen som skickas till Microsoft innehålla det ord som du sökte efter som en del av den fullständiga adressen som appen använde. Microsoft filtrerar dessa adresser för att försöka avlägsna personlig information när detta är möjligt.

Användning av informationen

Microsoft granskar regelbundet den information som du skickar för att upptäcka appar som kan använda osäkert webbinnehåll, t.ex. skadliga webbadresser eller skript. Vi skulle kunna använda informationen till att vidta åtgärder mot t.ex. appar som kan vara skadliga. Adresser till webbinnehåll kan oavsiktligt innehålla personlig information, men den används inte för att identifiera, kontakta eller skicka reklam till dig. Vi använder GUID-värdet för att bestämma hur omfattande den feedback vi får är och hur den ska prioriteras. GUID-värdet gör exempelvis att Microsoft kan skilja mellan potentiellt osäkert beteende som inträffar hundra gånger på en enskild dator och samma beteende som inträffar en enda gång vardera på hundra datorer.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows skickar Windows information om webbinnehåll som används av de Store-appar på din dator som har byggts med JavaScript. Om du väljer att anpassa inställningarna kan du hantera den här inställningen genom att välja **Använd SmartScreen-onlinetjänsterna för att skydda datorn mot skadligt innehåll på webbplatser som läses in av Windows Store-appar och Internet Explorer samt mot skadliga nedladdningar** under **Hjälp till att förbättra Microsofts produkter och tjänster**. Efter installationen kan du ändra inställningen i **Sekretess** i Datorinställningar.

Överst på sidan

Windows Time service

Funktionens uppgift

Windows Time Service synkroniserar automatiskt datorns klocka

mot en tidsserver i ett nätverk.

Insamlad, bearbetad eller överförd information

Tjänsten ansluter till en tidsserver via Internet eller i ett lokalt nätverk med NTP-standardprotokollet (Network Time Protocol). Som standard synkroniserar den här tjänsten med time.windows.com en gång i veckan. Ingen information annat än normal information om datorn skickas till tidsservern.

Användning av informationen

Informationen används av Windows Time Service för att synkronisera datorns tid.

Val och kontroll

Windows Time Service är aktiverad som standard. Du kan inaktivera den här funktionen i **Datum och tid** i Datorinställningar. Om du stänger av Windows Time Service har det ingen direkt effekt på appar eller andra tjänster, men utan en tillförlitlig tidskälla kan datorns klocka visa en annan tid än andra datorer i nätverket eller på Internet. Appar och tjänster som är beroende av att klockan går rätt kanske kraschar eller slutar fungera korrekt om klockan skiljer sig mycket mellan datorer i nätverket.

Överst på sidan

Windows Felsökning

Funktionens uppgift

Med Windows Felsökning kan du diagnostisera och åtgärda vanliga problem på datorn.

Insamlad, bearbetad eller överförd information

När du har kört ett felsökningspaket sparas resultatet på datorn. Dessa resultat kan innehålla personlig information, t.ex. ditt användarnamn eller namnet på en tjänst. Windows Felsökning kan hjälpa dig med att söka efter lösningar i Hjälp om Windows och i Windows-grupper på Internet. Sökord som förknippas med problemet skickas till Microsoft i ett försök att hitta en lösning. Om

din skrivare exempelvis inte fungerar korrekt och du vill ha hjälp skickas orden "skrivare", "skriva ut" och "utskrift" till Microsoft.

Användning av informationen

Microsoft använder informationen som samlas in av Windows Felsökning för att åtgärda problem som användarna stöter på.

Val och kontroll

Om du vill ta bort felsökningsresultat går du till Felsökning på Kontrollpanelen. Klicka på **Visa historik**, välj ett resultat och klicka på **Ta bort**.

Överst på sidan

Arbetsmappar

Funktionens uppgift

Arbetsmappar är mappar på datorn som synkroniseras automatiskt med din arbetsplats filserver.

Insamlad, bearbetad, lagrad eller överförd information

När du sparar en fil i en arbetsmapp synkroniseras filen automatiskt med en filserver som hanteras av din arbetsplats. Filer som sparas i din arbetsmapp från andra datorer synkroniseras med din dator.

Användning av informationen

Windows skickar och tar emot filerna i dina arbetsmappar för att synkronisera mapparna. Användningen av informationen som finns lagrad på din arbetsplats servrar omfattas av din arbetsplats sekretesspolicy.

Val och kontroll

Du kan hantera datorns anslutning till arbetsmappar i **Arbetsplats** i Datorinställningar.

Överst på sidan

Arbetsplats

Med den här funktionen kan du ansluta din enhet till Windows Intune (kräver en separat prenumeration från Microsoft) eller en annan enhetshanteringstjänst från en tredje part. Om du väljer att tillåta att företagsadministratören hanterar din dator med den här funktionen kan han eller hon utföra åtgärder som att tillämpa säkerhetsprinciper på datorn, installera appar, visa konfigurationsinställningar och annan information på datorn samt utföra andra hanteringsuppgifter. Läs företagets sekretesspolicy eller kontakta systemadministratören om du vill ha mer information om hur den här funktionen används på ditt företag.

Insamlad, bearbetad eller överförd information

När du konfigurerar och använder Arbetsplats kommunicerar din dator med företagets enhetshanteringstjänst, som Microsoft kan vara värd för. De autentiseringsuppgifter som du anger för att ansluta till arbetsplatsen skickas till tjänsten.

Användning av informationen

Informationen som skickas till enhetshanteringstjänsten används för att upprätta en anslutning mellan tjänsten och datorn och för att låta dig installera en självbetjäningsapp från Windows Store. Läs företagets sekretesspolicy eller kontakta systemadministratören om du vill ha mer information om självbetjäningsappen.

Val och kontroll

Om Arbetsplats används på ditt företag kan du upprätta eller koppla från anslutningen i Arbetsplats i Datorinställningar, under **Nätverk**. När du har anslutit din dator till tjänsten kan du visa information om anslutningen eller koppla från när du vill.

Överst på sidan

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8.1 och Windows Server 2012 R2

Observera att den här sidan är ett tillägg till sekretesspolicyn för Windows 8.1 och Windows Server 2012 R2 (”sekretesspolicyn för Windows”), som innehåller följande avsnitt:

- Huvudpunkter
- Policy, som är den fullständiga sekretesspolicyn för Windows 8.1, innehåller länkar till sekretesspolicyn för Windows-funktioner som har en egen fristående policy
- Tillägg för funktioner, som beskriver funktionerna som påverkar sekretessen i Windows 8.1 och Windows Server 2012 R2
- **Tillägg för appar** (den här sidan), som beskriver de appar som påverkar sekretessen i Windows 8.1 och innehåller länkar till de sekretesspolicyer som gäller för varje app
- Tillägg för server, som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012 R2

Om du vill ha information om hur vi samlar in och använder data i anslutning till en viss funktion eller tjänst i Windows läser du den fullständiga sekretesspolicyn och eventuella tillägg eller fristående

policyinformation.

Om du valde att delta i Programmet för kvalitetsförbättring (CEIP) när du konfigurerade datorn samlas information in om hur du använder varje app och om appens prestanda och tillförlitlighet. Microsoft använder CEIP-information för att förbättra sina produkter och tjänster. Informationen används inte för att identifiera, kontakta eller skicka reklam till dig. Du kan inaktivera CEIP i Datorinställningar. Mer information finns i sekretesspolicyn för CEIP.

Följande är länkar till sekretesspolicyerna för varje app:

Alarm

Kalkylatorn

Kalender

Kamera

Ekonomi

Mat

Spel

Hälsa

Hjälp och tips

E-post

Kartor

Musik

Nyheter

Kontakter

Läsare

Läslista

Skanna

Skype

Ljudinspelaren

Sport

Resor

Video

Väder

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8.1 och Windows Server 2012 R2

På den här sidan

Loggning av användaråtkomst

Serverhanteraren

Active Directory Federation Services

IPAM (IP Address Management)

Enhetlig fjärråtkomst

Fjärrskrivbordstjänster

Windows Customer Experience Improvement Program (CEIP) och Windows Felrapportering (WER).

Software Inventory

Den här sidan är ett tillägg till sekretesspolicyn för Windows 8.1 och Windows Server 2012 R2 (”sekretesspolicyn för Windows”). Sekretesspolicyn innehåller följande avsnitt:

- Huvudpunkter
- Policy, som är den fullständiga sekretesspolicyn för Windows 8.1, innehåller länkar till sekretesspolicyn för funktioner i Windows som har en egen, fristående policy
- Tillägg för funktioner, som beskriver funktionerna som påverkar sekretessen i Windows 8.1 och Windows Server 2012 R2
- Tillägg för appar, som beskriver apparna som påverkar sekretessen i Windows 8.1
- **Tillägg för server** (det här sidan), som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012 R2

Om du vill ha information om hur vi samlar in och använder data i anslutning till en viss funktion eller tjänst i Windows läser du den fullständiga sekretesspolicyn för Windows och relevanta tillägg. Du bör också läsa detta white paper för administratörer.

Mer information om hur funktionerna i Windows Server 2012 R2 Essentials påverkar sekretessen finns i sekretesspolicyn för Windows Server 2012 R2 Essentials och Windows Server Essentials Experience.

Loggning av användaråtkomst

Funktionens uppgift

Loggning av användaråtkomst samlar in och sammanställer poster med klientförfrågningar om serverroller (både begäranden om användare och enheter) och installerade produkter (om de är registrerade för loggning av användaråtkomst) på den lokala servern. Dessa data, i form av IP-adresser, användarnamn och i vissa fall värdnamn och/eller identiteter för virtuella datorer, lagras i lokala Extensible Storage Engine-databaser (ESE) och kan endast kommas åt av administratörer. Loggning av användaråtkomst har en WMIv2-provider och tillhörande Windows PowerShell-cmdlets som används för att hämta data om användaråtkomst som är avsedd för hantering av berättigande av klientåtkomstlicenser för offlinekunder, där faktiska poster med unika klientförfrågningar är avgörande.

Insamlad, bearbetad eller överförd information

IP-adresser, användarnamn och i vissa fall värdnamn (om DNS-rollen är installerad) samt identiteter för virtuella datorer (om Hyper-V-rollen är installerad) samlas in lokalt på servern när loggning av användaråtkomst är aktiverat. Inga insamlade data skickas till Microsoft.

Användning av informationen

Data från loggningen av användaråtkomst görs tillgängliga för administratörer via lokala ESE-databaser, WMI-providern och Windows PowerShell-cmdlets. Windows använder inte dessa data utanför själva funktionen för loggning av användaråtkomst.

Val och kontroll

Loggning av användaråtkomst är aktiverat som standard. Tjänsten kan stoppas och startas medan servern körs. Om du vill inaktivera loggning av användaråtkomst permanent öppnar du Windows PowerShell,

skriver Disable-UAL och startar om servern. En administratör kan ta bort alla historiska data som samlats in genom att först stoppa tjänsten, inaktivera loggning av användaråtkomst och sedan ta bort alla filer i mappen %SystemRoot%\System32\LogFiles\SUM\.

Överst på sidan

Serverhanteraren

Funktionens uppgift

Serverhanteraren är ett hanteringsverktyg som gör att en administratör kan övervaka en eller flera servrar och visa allmän eller rollspecifik status för att utföra hanteringsaktiviteter och komma åt andra serverhanteringsverktyg.

Insamlad, bearbetad eller överförd information

Serverhanteraren samlar in följande typer av information från en server som administratören hanterar:

- **Allmän serverinformation:** NetBios-namn och fullständigt domännamn, kontouppgifter som angetts i funktionen Hantera som, IPv4-adress, IPv6-adress, hanterbarhetsstatus, beskrivning, version av operativsystem, senaste uppdatering, processorer, minne, klusternamn, klusterobjekttyp, aktiveringsstatus, SKU, operativsystemets arkitektur, tillverkare, CEIP-konfiguration och konfiguration av Windows Felrapportering.
- **Händelser:** ID, allvarlighetsgrad, källa, logg, datum och tidpunkt för varje händelse från Windows och andra loggar som administratören väljer.
- **Alla tjänster:** namn, status och starttyp.
- **Serverrollinformation:** Best Practice Analyzer-resultat (BPA) för roller som är installerade på servern.
- **Prestandainformation:** exempel relaterade till prestandaräknare och meddelanden för processoranvändning och ledigt minne.

Användning av informationen

Informationen lagras i Serverhanteraren och skickas inte till Microsoft. Den visas i Serverhanteraren för att hjälpa administratörer att övervaka system.

Val och kontroll

En administratör kan välja att samla in data från en server, förutom den lokala servern, genom att lägga till eller ta bort servern i Serverhanteraren. En administratör kan uttryckligen tillhandahålla autentiseringsuppgifter för en fjärrserver. Serverhanteraren ber administratören om tillåtelse att lagra autentiseringsuppgifterna lokalt i Serverhanteraren och administratören kan när som helst ta bort dessa uppgifter.

Överst på sidan

Active Directory Federation Services

Funktionens uppgift

Active Directory Federation Services (AD FS) är en företagsklar federation och lösning med en enda inloggning för lokala eller andra nätverksbaserade appar. Administratörer kan använda AD FS för att ge användarna möjlighet att samarbeta mellan organisationer och att enkelt komma åt appar lokalt eller i nätverk utan att säkerheten äventyras. AD FS använder en säkerhetstokentjänst som använder Active Directory Domain Services (AD DS) för att autentisera användare och utfärda säkerhetstoken till dem med olika protokoll. Denna token signeras digitalt och innehåller anspråk om användaren som kommer från AD DS, LDAP-protokoll (Lightweight Directory Access Protocol), SQL Server eller ett anpassat arkiv eller en kombination av dessa.

Insamlad, bearbetad eller överförd information

En användares autentiseringsuppgifter samlas in när användaren autentiseras med AD FS. Autentiseringsuppgifterna skickas direkt till Active Directory Domain Services för autentisering och AD FS sparar dem inte lokalt. Användarens attribut i Active Directory Domain Services kan användas för att generera utgående anspråk, beroende på vilka anspråksregler en AD FS-administratör har konfigurerat. Utgående anspråk kommer att skickas till tillförlitliga partner som en

AD FS-administratör har upprättat en tillförlitlig relation med. Ingen information skickas till Microsoft.

Användning av informationen

Microsoft kommer inte att komma åt den här informationen. Informationen är endast avsedd att användas av kunden.

Val och kontroll

Använd AD FS om du vill att AD FS ska samla in eller skicka data till tillförlitliga partner.

Överst på sidan

IPAM (IP Address Management)

Funktionens uppgift

Med IPAM (IP Address Management) kan serveradministratörer spåra IP-adressen, värdnamnet och klientidentifierare (t.ex. MAC-adressen i IPv4 och DUID i IPv6) för datorer eller enheter i ett nätverk med användarens inloggningsuppgifter.

Insamlad, bearbetad eller överförd information

IPAM-servern samlar in granskningsloggar och händelser från DHCP-servrar, domänkontrollanter och nätverksprincipservrar. Sedan sparas IP-adressen, värdnamnet, klientidentifieraren och användarnamnet för den inloggade användaren lokalt. En serveradministratör kan söka i de insamlade loggarna baserat på IP-adress, klientidentifierare, värdnamn och användarnamn med IPAM-konsolen. Ingen del av informationen skickas till Microsoft.

Användning av informationen

Microsoft kommer inte åt den här informationen. Informationen är endast avsedd att användas av kunden.

Val och kontroll

IPAM installeras inte som standard och måste installeras av serveradministratören. När IPAM är installerad aktiveras granskningen av IP-adressen automatiskt. Om du vill inaktivera granskning av IP-adresser på en server där IPAM är installerad startar du

Schemaläggaren på IPAM-servern, bläddrar till Granskningsaktivitet under Microsoft\Windows\IPAM och inaktiverar sedan aktiviteten.

Överst på sidan

Enhetlig fjärråtkomst

Funktionens uppgift

Med enhetlig fjärråtkomst kan fjärranvändare ansluta till ett privat nätverk, t.ex. ett företagsnätverk, via Internet. Vid enhetlig fjärråtkomst används DirectAccess för att ge fjärrklientdatorer som kör Windows 8 en oavbruten och öppen anslutning till företagsnätverk. Den tillhandahåller även RAS-funktionen (Remote Access Service), som är traditionella VPN-tjänster, bland annat anslutning mellan webbplatser eller andra nätverk.

Insamlad, bearbetad eller överförd information

Vid användaröverväkning med enhetlig fjärråtkomst lagrar DirectAccess-servern fjärranvändarnas uppgifter när de ansluter till det privata nätverket. Detta omfattar information som värdnamnet för fjärranvändaren, användarnamnet för Active Directory och fjärrklientens offentliga IP-adress (om klienten finns bakom NAT (Network Address Translation) är det den offentliga IP-adressen). Dessa data kan även lagras i Windows Internal Database (WID)/RADIUS-servrar med administratörens medgivande. Endast en DirectAccess-administratör (en domänanvändare med ett lokalt administratörskonto) som kommer åt en server kan komma åt och visa informationen.

Användning av informationen

Den här informationen kommer att användas av administratören för att felsöka anslutningen samt i gransknings- eller regelefterlevnadssyfte. Ingen information skickas till Microsoft.

Val och kontroll

Fjärrklientövervakning aktiveras som standard och kan inte inaktiveras. Övervakningsdata lagras endast i WID/RADIUS-servrar om en administratör har konfigurerat redovisningen för att använda något av dessa alternativ. Om en administratör inte har konfigurerat

redovisningen lagras ingen del av informationen. En administratör kan även konfigurera redovisningen på en fjärråtkomstserver så att användarnamn och IP-adress inte sparas.

Överst på sidan

Fjärrskrivbordstjänster

Funktionens uppgift

Fjärrskrivbordstjänster är en plattform som hjälper företag att implementera en central skrivbordsstrategi, hantera datorer och appar samt förbättra flexibiliteten och regelefterlevnaden samtidigt som datasäkerheten förbättras.

Insamlad, bearbetad eller överförd information

Vid användaröverväkning med fjärrskrivbordstjänster lagrar värdservern för fjärrskrivbordssessioner information om fjärranvändare som ansluter till fjärrskrivbordstjänster. Detta omfattar information som värdnamnet för fjärranvändaren, användarnamnet för Active Directory och fjärrklientens offentliga IP-adress (om klienten finns bakom NAT (Network Address Translation) är det den offentliga IP-adressen). Dessa data lagras automatiskt i Windows Internal Database (WID)/SQL-servrar när användarna ansluter. Ingen information skickas till Microsoft. Endast en domänanvändare som har ett lokalt administratörskonto kan komma åt och visa informationen.

Användning av informationen

Den här informationen kommer att användas av administratören för att felsöka anslutningen samt i internt gransknings- eller regelefterlevnadssyfte. Ingen information skickas till Microsoft.

Val och kontroll

Klientövervakning är aktiverat som standard och kan inte inaktiveras. Övervakningsinformationen lagras på WID/SQL-servern.

Överst på sidan

Windows Customer Experience Improvement Program (CEIP) och Windows Felrapportering (WER).

Funktionens uppgift

Mer information om dessa funktioner finns på fliken Tillägg för funktioner och i detta white paper för administratörer.

Insamlad, bearbetad eller överförd information

Om du vill läsa mer om specifik information som samlas in, bearbetas och överförs via dess funktioner kan du läsa om CEIP och WER på fliken Tillägg för funktioner .

Användning av informationen

Om du vill läsa mer om hur vi använder information som samlas in via dess funktioner kan du läsa om CEIP och WER på fliken Tillägg för funktioner .

Val och kontroll

CEIP är inaktiverat som standard och WER är som standard inställt på att fråga innan felrapporter skickas till Microsoft. Du kan aktivera eller inaktivera CEIP i Serverhanteraren och på Kontrollpanelen samt genom att använda kommandoradsmetoder. WER kan endast styras via kommandoradsmetoder.

Om du vill aktivera eller inaktivera CEIP via Kontrollpanelen klickar du på **System och underhåll**och sedan på **Problemrapporter och -lösningar**. Under **Se även**, **Inställningar för Programmet för kvalitetsförbättring** för att aktivera eller inaktivera CEIP.

Kontroller i Serverhanteraren

Lokal server

- Aktivera CEIP
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken Customer Experience Improvement Program och välj **Ja, jag vill delta i Customer Experience Improvement Program** i dialogrutan och klicka sedan på **OK**.

- Inaktivera CEIP
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken Customer Experience Improvement Program och välj **Nej, jag vill inte delta** i dialogrutan och klicka sedan på **OK**.

- Aktivera WER

Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken för Windows Felrapportering och markera kryssrutan **Ja, skicka sammanfattningsrapporter automatiskt**. Klicka sedan på **OK**.

- Inaktivera WER
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken för Windows Felrapportering och markera kryssrutan **Jag vill inte delta. Fråga mig inte igen.**. Klicka sedan på **OK**.

Flera datorer

- Aktivera CEIP
  Öppna Serverhanteraren och välj **Alla servrar**. I serverrutan markerar du alla servrar (Ctrl+A), högerklickar och väljer **Konfigurera Windows Automatisk feedback** . Välj **Ja, jag vill delta (rekommenderas)**på fliken Customer Experience Improvement Program. Använd den här inställningen på alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

- Inaktivera CEIP
  Öppna Serverhanteraren och välj Alla servrar. I serverrutan markerar du alla servrar (Ctrl+A), högerklickar och väljer **Konfigurera Windows Automatisk feedback** . Välj **Nej, jag vill inte delta**på fliken Customer Experience Improvement Program. Använd den här inställningen på alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

- Aktivera WER
  Öppna Serverhanteraren och välj **Alla servrar**. I serverrutan markerar du alla servrar (Ctrl+A), högerklickar och väljer **Konfigurera Windows Automatisk feedback** . Välj **Ja, skicka sammanfattningsrapporter automatiskt (rekommenderas)**på fliken Customer Experience Improvement Program. Använd den här inställningen på alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

- Inaktivera WER

Öppna Serverhanteraren och välj **Alla servrar**. I serverrutan markerar du alla servrar (Ctrl+A), högerklickar och väljer **Konfigurera Windows Automatisk feedback** . Välj **Nej, jag vill inte delta**på fliken Customer Experience Improvement Program. Använd den här inställningen på alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

Överst på sidan

Software Inventory Logging

Funktionens uppgift

I funktionen Software Inventory Logging (SIL) finns en ny uppsättning WMI-klasser och Powershell-cmdlets som gör det enklare att inventera Windows Server-versionen, programvaran som finns installerad i Windows Server och egenskaperna för den server som programvaran körs på. En administratör kan ange att SIL ska samla in data varje timme från WMI-providern och vidarebefordra dessa data via nätverket till en aggregeringsserver, om en sådan har angetts med cmdleten Set-SilLogging -TargerUri.

Insamlad, bearbetad eller överförd information

En administratör kan ange att data ska överföras till en aggregeringsserver via nätverket. Som standard utförs ingen insamling, bearbetning eller överföring. Dessa data innefattar:

- Namnet och versionen för det Windows Server-operativsystem som är installerat.
- En lista över namn, versioner och utgivare för alla program som installerats på server samt programmets installationsdatum.
- Serversystemets fullständiga domännamn.
- Antal, typ och tillverkare för processorer, logiska processorer och kärnor som installerats på eller tilldelats till serversystemet.

Data samlas in och bearbetas men överförs inte som standard, även om insamling varje timme har aktiverats och en målaggregator har angetts av administratören:

- Med klassen MsftSil_UalAccess och cmdleten Get-SilUalAccess bearbetas det totala antalet unika användare och enheter för varje roll eller produkt som registrerats med funktionen Loggning av användaråtkomst två dagar före frågan. Det är endast antalet som bearbetas. Ingen information om användaren eller enheten returneras eller överförs. SIL måste bearbeta information om användare och enheter från UAL-klasser för att kunna beräkna antalet. Endast en administratör på den lokala datorn har åtkomst till dessa data. SIL ändrar inte åtkomsten som behövs för UAL-API:erna.

Inga insamlade data skickas till Microsoft.

Användning av informationen

SIL WMI-providers samlar in data från andra API:er som redan finns i systemet. Data kan överföras till en server för ytterligare aggregering via nätverket om en administratör har angett det. Som standard utförs ingen insamling, bearbetning eller överföring. Med klassen MsftSil_UalAccess och cmdleten Get-SilUalAccess bearbetas det totala antalet unika användare och enheter för varje roll eller produkt som registrerats med funktionen Loggning av användaråtkomst två dagar före frågan, men ingen information returneras som kan identifiera användaren eller enheten. Även om WMI-klassen och cmdleten finns i systemet ingår de inte i den SIL-datanyttolast som samlas in och vidarebefordras till en aggregator varje timme (om detta har konfigurerats av systemadministratören).

Val och kontroll

Den här aktiviteten är inaktiverad som standard. Som standard är alla SIL-API:er tillgängliga för frågor för administratörer i det lokala systemet. SIL-aktiviteten som utförs varje timme kan startas och stoppas medan servern körs med hjälp av cmdletarna Start-SilLogging och Stop-SilLogging. Med cmdleten Set-SilLogging kan serveradministratörer ange datum och tid då aktiviteten ska starta (standardinställningen är 03:00 lokal systemtid), URI för målaggregeringsservern och tumavtryck för certifikatet som behövs för att säkerställa en säker dataöverföring.

Alla SIL-konfigurationsinställningar (även start och stopp av

aktiviteten) kan ändras i registret, men inställningarna bör endast ändras om systemet är en virtuell dator och innan systemet startas för första gången.

Överst på sidan