

Hvis du vil ha oppdatert informasjon om Microsofts databehandlingspraksis, kan du se [Microsofts personvernerklæring](#). Her kan du også finne ut mer om de nyeste verktøyene vi tilbyr for åpne og kontrollere data, og hvordan du kontakter oss hvis du har et spørsmål om personvern.

Personvernerklæring for Windows 8 og Windows Server 2012

Høydepunkt Erklæring Funksjonstillegg Servertillegg

På denne siden Sist oppdatert: **August 2012**

Dine opplysninger Disse hovedpunktene fra fullstendig [Personvernerklæring for Windows 8 og Windows Server 2012](#) ("Personvernerklæring for Windows") forklarer på et overordnet nivå noe av datainnsamlingen og brukspraksisen i Windows 8 og Windows Server 2012 ("Windows"). De fokuserer på funksjoner som kommuniserer med Internett, og de er ikke ment å være fullstendige beskrivelser. De gjelder ikke for andre av Microsofts tilkoblede eller frakoblede nettsteder, produkter eller tjenester.

Dine valg

Bruk av informasjon

Slik kontakter du oss

Denne personvernerklæringen har fire deler:

- Hovedpunkter (denne siden)
- Erklæring, som er den fullstendige personvernerklæringen for Windows som inneholder koblinger til Windows-funksjoner med egne frittstående erklæringer
- Funksjonstillegg, som beskriver funksjonene som har

innvirkning på personvernet i Windows 8 og Windows Server 2012

- [Servertillegg](#), som beskriver tilleggsfunksjonene som har innvirkning på personvernet i Windows Server 2012

Hvis du vil ha mer informasjon om hvordan du kan bidra til å beskytte den personlige datamaskinen din, dine personlige opplysninger og familien på Internett, kan du gå til vårt [Sikkerhetssenter](#).

Dine opplysninger

- Enkelte Windows-funksjoner ber deg kanskje om tillatelse til å samle inn eller bruke informasjon fra PC-en din, inkludert personlige opplysninger. Windows bruker denne informasjonen som beskrevet i fullstendig [Personvernerklæring for Windows](#), i [Funksjonstillegg](#) og [Servertillegg](#).
- Noen Windows-funksjoner kan, med din tillatelse, dele personlige opplysninger via Internett.
- Hvis du velger å registrere programvaren, blir du bedt om å oppgi personlige opplysninger.
- Windows krever aktivering for å redusere piratkopiering av programvare og bidra til å sikre at kundene våre får programvarekvaliteten de forventer. Aktivering sender informasjon om PC-en din til Microsoft.
- Du kan velge å logge på Windows med en [Microsoft-konto](#), som lar deg synkronisere Windows-innstillinger og automatisk logge på apper og nettsteder. Når du oppretter en Microsoft-konto, blir du bedt om å angi noen personlige opplysninger.
- [Tilleggsdetaljer](#)

[Toppen av siden](#)

Dine valg

- Windows inneholder en rekke metoder for å kontrollere

hvordan Windows-funksjoner overfører informasjon via Internett. Du finner mer informasjon om hvordan du styrer disse funksjonene i funksjonstillegget og servertillegget.

- Noen funksjoner som bruker Internett, er aktivert som standard for å bidra til å forbedre opplevelsen.
- [Tilleggsdetaljer](#)

[Toppen av siden](#)

Bruk av informasjon

- Vi bruker den innsamlede informasjonen til å aktivere funksjonene du bruker eller levere tjenestene du ber om. Vi bruke den også til å forbedre våre produkter og tjenester. For å bidra til å levere tjenestene våre gir vi av og til informasjon til andre firmaer som arbeider på våre vegne. Bare firmaer som trenger informasjonen i virksomheten får tilgang til den. Disse firmaene er forpliktet til å holde informasjonen konfidensiell og har ikke lov til å bruke den til andre formål.
- [Tilleggsdetaljer](#)

[Toppen av siden](#)

Slik kontakter du oss

Hvis du vil ha mer informasjon om vår personvernpraksis, kan du gå til fullstendig [Personvernerklæring for Windows](#). Du kan også skrive til oss ved hjelp av vår [nettskjema](#).

[Toppen av siden](#)

Hvis du vil ha oppdatert informasjon om Microsofts databehandlingspraksis, kan du se [Microsofts personvernerklæring](#). Her kan du også finne ut mer om de nyeste verktøyene vi tilbyr for åpne og kontrollere data, og hvordan du kontakter oss hvis du har et spørsmål om personvern.

Personvernerklæring for Windows 8 og Windows Server 2012

Høydepunkt **Erklæring** Funksjonstillegg Servertillegg

På denne siden

Innsamling og bruk av dine opplysninger

Innsamling og bruk av informasjon datamaskinen

Informasjonssikkerhet

Endringer i denne personvernerklæringen

Hvis du vil ha mer informasjon

Andre

personvernerklæringer

Internet Explorer

Denne erklæringen gjelder Windows 8 og Windows Server 2012 ("Windows"). Enkelte Windows-komponenter har sine egne personvernerklæringer, som er oppført til høyre på denne siden. Personvernerklæringer for programvare og tjenester som er relatert til Windows og for tidligere versjoner er også oppført der.

Hvis du vil ha informasjon om bestemte funksjoner, kan du se [Funksjonstillegg](#) og [Servertillegg](#).

Dette er en erklæring som fokuserer på funksjoner som kommuniserer med Internett, og er ikke ment å være en fullstendig liste.

Innsamling og bruk av dine opplysninger

De personlige opplysningene vi samler inn fra deg, brukes av Microsoft, dets kontrollerte datterselskaper og tilknyttede selskaper, for å aktivere funksjonene du bruker og tilby

Microsofts feilrapporteringstjeneste	tjenestene eller utføre transaksjonene du har bedt om eller godkjent. Informasjonen kan også brukes til å analysere og forbedre Microsoft-produkter og -tjenester.
Microsoft Online	
Microsoft Windows Verktøy for fjerning av skadelig programvare	Med unntak av det som nevnes i denne erklæringen, vil ikke personlige opplysninger som du oppgir, bli overført til tredjeparter uten ditt samtykke. Vi leier av og til andre firmaer til å utføre begrensede tjenester på våre vegne, for eksempel til å utføre statistisk analyse av våre tjenester. Til disse firmaene oppgir vi bare de personlige opplysningene de trenger for å levere tjenesten, og de har ikke lov til å bruke disse opplysningene til andre formål.
Oppdateringstjenester	
Windows Media Center	
Windows Media Player	
Windows 7	Microsoft kan få tilgang til eller fremlegge informasjon om deg, inkludert innholdet i din kommunikasjon, for å gjøre følgende: (a) overholde loven, eller svare på rettsgyldige forespørsler eller rettslige prosesser, (b) beskytte rettighetene eller eiendommen til Microsoft eller våre kunder, inkludert håndhevelse av våre avtaler eller retningslinjer som regulerer bruken av programvaren, eller (c) i god tro anta at slik tilgang til eller utlevering er nødvendig for å beskytte den personlige sikkerheten til Microsofts ansatte eller kunder eller allmennheten.

Informasjon som samles inn av eller sendes til Microsoft av Windows 8, kan oppbevares og behandles i USA eller andre land der Microsoft eller tilknyttede selskaper, datterselskaper eller tjenesteleverandører har kontorer. Microsoft retter seg etter rammebetingelsene fra næringsmyndighetene i USA om sikker plassering når det gjelder innsamling, bruk og eierskap av data fra Den europeiske union, Det europeiske økonomiske samarbeidsområdet og Sveits.

[Toppen av siden](#)

Innsamling og bruk av informasjon datamaskinen

Når du bruker programvare med Internett-aktiverte funksjoner, blir informasjon om datamaskinen din (" standard datamaskininformasjon") sendt til nettsteder du besøker, og tilkoblede tjenester du bruker. Standardinformasjon om

datamaskinen kan for eksempel være IP-adresse, operativsystemversjon, nettleserversjon, regionale innstillinger og språkinnstillinger. I enkelte tilfeller kan også standard datamaskininformasjon inkludere maskinvare-ID, som angir enhetsprodusenten, enhetsnavnet og versjonen. Hvis en bestemt funksjon eller tjeneste sender informasjon til Microsoft, vil standard datamaskininformasjon også bli sendt.

Personverndetaljene for hver Windows 8-funksjonen i [Funksjonstillegg](#) og [Servertillegg](#), i tillegg til funksjonene som er oppført på denne siden, beskriver hvilken tilleggsinformasjon som samles inn og hvordan den brukes.

Administratorer kan bruke gruppepolicy til å endre mange av innstillingene for funksjonene som beskrives nedenfor. Hvis du vil ha mer informasjon, kan du se [denne hvitboken for administratorer](#).

[Toppen av siden](#)

Informasjonssikkerhet

Microsoft er opptatt av å beskytte sikkerheten til informasjonen din. Vi bruker en rekke sikkerhetsteknologier og -prosedyrer for å beskytte opplysningene dine mot uautorisert tilgang, bruk eller utlevering. Vi oppbevarer for eksempel informasjonen du oppgir, i datasystemer med begrenset tilgang i kontrollerte anlegg. Når vi sender svært fortrolig informasjon (for eksempel kredittkortnummer eller passord) over Internett, beskytter vi den i tillegg ved hjelp av kryptering, for eksempel ved bruk av SSL-protokollen (Secure Socket Layer).

[Toppen av siden](#)

Endringer i denne personvernerklæringen

Vi vil av og til oppdatere denne personvernerklæringen slik at den viser endringer i våre produkter, tjenester og tilbakemelding fra kunder. Når vi foretar endringer, vil vi endre datoen for "sist oppdatert" øverst i denne erklæringen.

Hvis det er omfattende endringer i denne erklæringen eller i hvordan Microsoft vil bruke dine personlige opplysninger, vil du bli varslet enten ved at vi legger ut en notis om slike endringer før de implementeres, eller ved at vi varsler deg direkte. Vi oppfordrer deg til å gå gjennom denne erklæringen med jevne mellomrom for å bli informert om hvordan Microsoft beskytter informasjonen din.

[Toppen av siden](#)

Hvis du vil ha mer informasjon

Microsoft ønsker tilbakemeldinger fra deg angående denne personvernerklæringen. Hvis du har spørsmål angående denne erklæringen eller mener at vi ikke har overholdt den, kan du skrive til oss ved hjelp av vår [nettskjema](#).

Microsofts personvernerklæring
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

[Toppen av siden](#)

Hvis du vil ha oppdatert informasjon om Microsofts databehandlingspraksis, kan du se [Microsofts personvernerklæring](#). Her kan du også finne ut mer om de nyeste verktøyene vi tilbyr for åpne og kontrollere data, og hvordan du kontakter oss hvis du har et spørsmål om personvern.

Personvernerklæring for Windows 8 og Windows Server 2012

Høydepunkt Erklæring **Funksjonstillegg** Servertillegg

På denne siden Sist oppdatert: Oktober 2012

[Aktivering](#) Vær oppmerksom på at denne siden er et tillegg til [Windows 8 og Windows Server 2012](#) ("Personvernerklæring for Windows"), som består av fire deler:

[Active Directory RMS-klient \(Rights Management Services\)](#)

- [Hovedpunkter](#)

[Overvåking](#)

- Erklæring, som er [hele personvernerklæringen for Windows](#), og inneholder koblinger til personvernerklæringer for Windows-funksjoner med egne frittstående erklæringer

[BitLocker-stasjonskryptering](#)

[Søke etter og konfigurere enheter](#)

- Funksjonstillegg (dette dokumentet), som beskriver tilleggsfunksjonene som påvirker personvernet for Windows 8 og Windows Server 2012

[DirectAccess](#)

[Dynamisk oppdatering](#)

- [Servertillegg](#), som beskriver tilleggsfunksjonene som påvirker personvernet for Windows Server 2012

[Hjelpemiddelsenter](#)

[Hendelsesliste](#)

For å forstå datainnsamlingen og brukspraksisen som er relevant for en bestemt funksjon eller tjeneste i Windows, bør du lese hele

Tryggere for familien	personvernerklæringen og aktuelle tillegg eller frittstående erklæringer.
Faks	
Håndskrifttilpassing – automatisk læring	Aktivering
Hjemmegruppe	Hva denne funksjonen gjør
IME (Input Method Editor)	Aktivering reduserer falsk programvare, noe som er med på å sikre at Microsoft-kunder får forventet programvarekvalitet. Når programvaren er aktivert, blir en spesifikk produktnøkkel knyttet til PCen (eller maskinvaren) der programvaren er installert. Denne tilknytningen forhindrer at produktnøgkelen blir brukt til å aktivere den samme kopien av programvaren på flere PCer. Noen endringer i PC-komponenter eller programvaren kan gjøre at du må aktivere programvaren på nytt. Noen endringer i PC-maskinvaren eller -programvaren kan gjøre at du må aktivere Windows på nytt.
Program for installasjonsforbedring	Aktivering kan registrere og deaktivere aktiveringsutnyttelser (programvare som omgår eller hopper over programvareaktivering).
Internett-utskrift	Hvis en aktiveringsutnyttelse forekommer, kan det hende en programvare- eller maskinvareleverandør har redigert opprinnelig Microsoft-programvare for å opprette piratkopier av programvaren. Aktiveringsutnyttelser kan forstyrre den vanlige systemdriften.
Språkinnstillinger	
Posisjonstjenester	
Navn og kontobilde	
Nettverkssporing	
Varslinger, låseskjermapper og flisoppdateringer	
Bestill kopier	Informasjon som samles inn, behandles eller overføres
Program Compatibility Assistant	Ved aktivering sendes følgende informasjon til Microsoft:
Egenskaper	<ul style="list-style-type: none"> • Microsofts produktkode (en femsifret kode som identifiserer Windows-produktet du aktiverer).
Nærhet	<ul style="list-style-type: none"> • En kanal-ID eller områdekode som identifiserer hvordan Windows-produktet opprinnelig ble anskaffet. En kanal-ID eller områdekode identifiserer for eksempel om produktet opprinnelig ble kjøpt fra en forhandler, anskaffet som en evaluerversjon, var en del av et volumlisensprogram eller ble forhåndsinstallert av PC-produsenten.
Eksterne tilkoblinger	<ul style="list-style-type: none"> • Installasjonsdatoen, og om installasjonen var vellykket.
Tilkoblinger til RemoteApp og skrivebord	<ul style="list-style-type: none"> • Informasjon som bekrefter at produktnøgkelen for Windows ikke har blitt endret.
Tilkobling til eksternt skrivebord	
Logg på med en	

Microsoft-konto	<ul style="list-style-type: none"> • PC-type og -modell.
Synkronisere innstillinger	<ul style="list-style-type: none"> • Versjonsinformasjon for operativsystem og programvare.
Teredo-teknologi	<ul style="list-style-type: none"> • Område- og språkinnstillinger.
TPM-tjenester (Trusted Platform Module)	<ul style="list-style-type: none"> • Et unikt nummer kalt GUID (globalt unik identifikator) som er tilordnet til PCen din.
Oppdater rotsertifikater	<ul style="list-style-type: none"> • Produktnøkkel (hash-kodet) og produkt-ID.
Oppdateringstjenester	<ul style="list-style-type: none"> • BIOS-navn, revisjonsnummer og revisjonsdato.
Windows CEIP (Customer Experience Improvement Program)	<ul style="list-style-type: none"> • Serienummer (hash-kode) for harddiskvolum.
Windows Defender	<ul style="list-style-type: none"> • Resultatet av aktiveringskontrollen. Dette inkluderer feilkoder og følgende informasjon om aktiveringsutnyttelser og relatert skadelig eller uautorisert programvare som ble funnet eller deaktivert: <ul style="list-style-type: none"> • Aktiveringsutnyttelsens ID.
Windows-feilrapportering	<ul style="list-style-type: none"> • Aktiveringsutnyttelsens gjeldende tilstand, for eksempel Tømt eller I karantene.
Windows Filtilknytning	<ul style="list-style-type: none"> • PC-produsentens ID.
Windows Hjelp	<ul style="list-style-type: none"> • Aktiveringsutnyttelsens filnavn og hash-kode, og i tillegg en hash-kode for beslektede programvarekomponenter som kan angi tilstedeværelse av en aktiveringsutnyttelse.
Fjernhjelp	
Windows Søk	
Windows-ressurs	<ul style="list-style-type: none"> • Navnet på og hash-koden for innholdet på PCens oppstartsinstruksjonsfil. Hvis Windows-lisensen gjelder på abonnementsbasis, sendes også informasjon om hvordan abonnementet fungerer. Standardinformasjon om datamaskin sendes også, men PCens IP-adresse beholdes bare midlertidig.
Windows SmartScreen	
Windows Talegjenkjenning	
Windows Store	
Tjenesten Windows Time	
Windows Feilsøking	

Bruk av informasjon

Microsoft bruker informasjonen til å bekrefte at du har en lisensiert versjon av programvaren. Microsoft bruker ikke informasjonen til å kontakte enkeltkunder.

Valg og kontroll

Aktivering kreves og forekommer automatisk når du konfigurerer Windows. Hvis du ikke har en gyldig lisens for programvaren, kan du ikke aktivere Windows.

[Øverst på siden](#)

Active Directory RMS-klient (Rights Management Services)

Hva denne funksjonen gjør

AD RMS-klient (Active Directory Rights Management Services) er teknologi som brukes til å beskytte informasjon, og som fungerer med AD RMS-aktiverte apper for å bidra til å beskytte digital informasjon mot uautorisert bruk. Eiere av digital informasjon kan angi hvordan mottakere kan bruke informasjonen i en fil, for eksempel hvem som kan åpne, endre, skrive ut eller gjøre andre ting med filen. Hvis du vil opprette eller vise en fil med begrensede tillatelser, må du kjøre en AD RMS-aktivert app på PCen og ha tilgang til en AD RMS-server.

Informasjon som samles inn, behandles eller overføres

AD RMS bruker e-postadressen din til å identifisere deg for en AD RMS-server. Det fører til at e-postadressen din lagres på serveren, og i tillegg på PCen din i lisenser og ID-sertifikater som opprettes av serveren. ID-sertifikater og lisenser overføres til og fra AD RMS-servere når du forsøker å åpne, skrive ut eller utføre andre handlinger for et dokument som er beskyttet av rettighetsadministrasjon. Hvis PCen er koblet til et organisasjonsnettverk, betjenes AD RMS-serveren vanligvis av organisasjonen. Hvis du bruker Windows Live AD RMS-tjenester, betjenes serveren av Microsoft. Informasjonen som sendes til Microsoft AD RMS-servere, krypteres slik at personvernet ditt beskyttes.

Bruk av informasjon

Du kan bruke lisensen til å åpne beskyttede filer. ID-sertifikatene brukes til å identifisere deg for en AD RMS-server, og til å beskytte filer og åpne beskyttede filer.

Valg og kontroll

AD RMS-funksjoner må aktiveres via en app som har støtte for AD RMS. De er som standard ikke aktivert. Du kan velge ikke å aktivere eller bruke dem. Hvis du ikke aktiverer dem, kan du imidlertid ikke få tilgang til beskyttede filer.

[Øverst på siden](#)

Overvåking

Overvåking lar en administrator konfigurere Windows slik at aktiviteten i operativsystemet kan registreres i en sikkerhetslogg som kan åpnes i Hendelsesliste og andre apper. Denne loggen kan gjøre det enklere for en administrator å oppdage uautorisert tilgang til PCen eller ressurser på PCen. Den kan for eksempel være til hjelp når administratorer feilsøker problemer og finner ut om noen har logget på PCen, opprettet en ny brukerkonto, endret en sikkerhetspolicy eller åpnet et dokument.

Informasjon som samles inn, behandles eller overføres

Administratorer bestemmer hvilken informasjon som samles inn, hvor lenge den beholdes, og om den skal overføres til andre parter. Informasjonen kan omfatte personlige opplysninger, for eksempel brukernavn eller filnavn. Du kan kontakte administratoren hvis du vil ha mer informasjon. Det sendes ingen informasjon til Microsoft.

Bruk av informasjon

Administratorer kan også bestemme hvordan overvåkingsinformasjon skal brukes. Generelt brukes sikkerhetsloggen av revisorer og administratorer til å spore PC-aktivitet eller identifisere uautorisert tilgang til PCen eller ressurser på PCen.

Valg og kontroll

Administratorer bestemmer om denne funksjonen skal aktiveres, og hvordan brukere skal varsles. Andre brukere kan ikke vise sikkerhetsloggen med mindre administratoren gir dem tilgang til den. Du kan konfigurere overvåking på PCen ved å åpne Lokal sikkerhetspolicy i Administrative verktøy.

[Øverst på siden](#)

BitLocker-stasjonskryptering

Hva denne funksjonen gjør

BitLocker-stasjonskryptering beskytter dataene dine mot kryptering, noe som kan bidra til å hindre at en uautorisert bruker får tilgang til dataene. Når BitLocker aktiveres på en stasjon som støttes, krypterer Windows dataene på stasjonen.

Informasjon som samles inn, behandles eller overføres

Når BitLocker aktiveres ved hjelp av programvarekryptering, blir data hele tiden kryptert og dekryptert av kryptografiske nøkler i minnet mens dataene leses fra eller skrives til den beskyttede stasjonen. Når BitLocker aktiveres ved hjelp av maskinvarekryptering, utføres datakryptering og -dekryptering av stasjonen.

Når du konfigurerer BitLocker, kan du velge om du vil skrive ut en gjenopprettingsnøkkel eller lagre den på nettverket. Hvis du konfigurerer BitLocker på en ikke-flyttbar stasjon, kan du også lagre gjenopprettingsnøkkelen på en USB-flash-enhet.

Hvis PCen ikke er koblet til et domene, kan du sikkerhetskopiere BitLocker-gjenopprettingsnøkkelen, gjenopprettingsnøkkel-IDen og datamaskinnavnet til OneDrive. For å beskytte personvernet ditt blir informasjonen sendt kryptert via SSL.

Du kan konfigurere BitLocker til å kryptere data ved hjelp av et sertifikat som er lagret på et smartkort. Når du beskytter en datastasjon med et smartkort, lagres fellesnøkkelen og den unike identifikatoren for smartkortet ukryptert på stasjonen. Du kan bruke denne informasjonen til å finne sertifikatet som opprinnelig ble brukt til å generere smartkortets krypteringssertifikat.

Hvis PCen har sikkerhetsmaskinvare med minst versjon 1.2 av TPM (Trusted Platform Module), bruker BitLocker TPM til å gi maskinvareforbedret databeskyttelse for stasjonen der Windows er installert. Hvis du vil ha mer informasjon, kan du se delen om TPM-tjenester (Trusted Platform Module). På PCer med TPM kan du også konfigurere en PIN-kode for å bidra med et ekstra beskyttelseslag for de krypterte dataene. BitLocker lagrer denne TPM-baserte PIN-koden i hash-kodet og kryptert form på stasjonen.

Informasjon som samles inn av BitLocker, sendes ikke til Microsoft med mindre du velger å sikkerhetskopiere gjenopprettingsnøkkelen til OneDrive.

Bruk av informasjon

Kryptografiske nøkler og GUIDer (globalt unik identifikator) lagres i PC-minnet for å støtte BitLocker-operasjoner. Du kan bruke BitLocker-gjenopprettingsinformasjon til å få tilgang til de beskyttede dataene dine i tilfelle maskinvarefeil og andre problemer. Denne gjenopprettingsinformasjonen gjør at BitLocker kan skille mellom autoriserte og uautoriserte brukere.

Microsoft bruker ikke de enkelte gjenopprettingsnøklerne dine til noe formål. Når du sender gjenopprettingsnøkler til OneDrive, kan det hende at Microsoft bruker aggregerte data om dem til å analysere trender og forbedre sine produkter og tjenester.

Valg og kontroll

BitLocker er som standard deaktivert. På en flyttbar stasjon kan alle brukere aktivere eller deaktivere BitLocker når som helst ved å åpne BitLocker-stasjonskryptering i Kontrollpanel. En administrator kan aktivere eller deaktivere BitLocker for alle stasjoner.

Hvis du har valgt å sikkerhetskopiere gjenopprettingsnøkkelen til OneDrive, kan du få tilgang til eller slette denne nøkkelen [her](#).

[Øverst på siden](#)

Søke etter og konfigurere enheter

Windows har flere funksjoner som du kan bruke til å registrere og konfigurere enheter på PCen, inkludert enhetsinstallasjon, enhetsinstallasjon av mobilt bredbånd, nettverkssøk og trådløs enhetsforbindelse.

Enhetsinstallasjon

Hva denne funksjonen gjør

Når en ny enhet installeres på PCen, kan Windows automatisk søke etter, laste ned og installere enhetens driverprogramvare. Windows kan også laste ned informasjon om enheten, for eksempel en

beskrivelse, et bilde og en produsentlogo. Noen enheter, inkludert bestemte skrivere, webkameraer, mobile bredbåndsenheter og bærbare enheter som kan synkroniseres med Windows, har en app som gir bedre funksjonalitet og brukeropplevelse på enheten. Hvis enhetens produsent har inkludert en app for enheten, kan Windows automatisk laste ned og installere den appen fra Windows Store hvis du er logget på Store.

Informasjon som samles inn, behandles eller overføres

Når Windows søker etter drivere, sjekkes det først om en riktig driver allerede er tilgjengelig på PCen. Hvis ikke kontakter Windows Windows Update-tjenesten elektronisk for å søke etter og laste ned enhetsdrivere. Hvis du vil vite mer om hvilken informasjon som samles inn av Windows Update og hvordan den brukes, kan du se [personvernerklæringen for Oppdateringstjenester](#).

Hvis du vil hente informasjon om enheten og fastslå om en app er tilgjengelig for den, sender Windows data om enheten til Microsoft, inkludert enhets-IDen (for eksempel maskinvare-ID eller modell-ID for enheten du bruker), område og språk, og datoen da enhetsinformasjonen sist ble oppdatert. Hvis informasjon eller en enhetsapp er tilgjengelig, laster Windows ned og installerer den fra Windows Store. Appen blir tilgjengelig på Windows Store-kontoen i listen over apper du har lastet ned.

Bruk av informasjon

Informasjonen som ble sendt til Microsoft, brukes til å fastslå og laste ned riktig enhetsdriver, informasjon og app for enheten. Microsoft bruker ikke informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du automatisk nedlasting og installasjon av enhetsdrivere, informasjon og apper. Hvis du velger å tilpasse innstillinger, kan du kontrollere automatisk nedlasting og installasjon av enhetsdrivere, apper og informasjon ved å velge **Hente enhetsapper og informasjon for nye enheter automatisk** under Help protect and update your PC. Etter å ha konfigurert Windows, kan du endre

disse innstillingene i Kontrollpanel ved å velge Change device installation settings, og deretter velge **Nei, la meg velge hva jeg vil gjøre**.

Du kan avinstallere en enhetsapp når som helst uten å måtte avinstallere enheten, men du trenger kanskje appen for å bruke bestemte funksjoner på enheten. Du kan installere en enhetsapp på nytt etter at du har avinstallert den ved å gå til listen over apper du eier, i Windows Store.

Installere enheter for mobilt bredbånd

Hva denne funksjonen gjør

Hvis PCen har maskinvare for mobilt bredbånd, som enkelte mobiloperatører tilbyr, kan Windows automatisk laste ned og installere en app der du kan administrere kontoen og dataplanen hos mobiloperatøren som leverte PCens maskinvare for mobilt bredbånd. Ytterligere enhetsinformasjon lastes også ned for å bidra til å vise den mobile bredbåndstilkoblingen i nettverkslister.

Informasjon som samles inn, behandles eller overføres

Windows sender en del av maskinvare-IDene fra maskinvaren for mobilt bredbånd slik at vi kan identifisere mobiloperatøren din. Dermed kan vi fastslå hvilken enhetsinformasjon og app som skal lastes ned. Windows sender ikke de fullstendige maskinvare-IDene for mobilt bredbånd til Microsoft. På den måten beskyttes personvernet ditt.

Hvis mobiloperatøren har sendt en app til Microsoft, laster Windows den ned fra Windows Store og installerer den. Når du åpner appen etter at den er installert, har den tilgang til maskinvaren for mobilt bredbånd, inkludert unike maskinvare-IDer som mobiloperatøren kan bruke til å identifisere kontoen din.

Bruk av informasjon

Microsoft bruker delen av maskinvare-IDen for mobilt bredbånd som Windows sender, til å fastslå hvilken leverandørs app som skal installeres på datamaskinen. Når appen er installert, kan den bruke IDene for maskinvaren for mobilt bredbånd. En mobiloperatørs app kan for eksempel bruke de IDene til å slå opp konto- og planinformasjon på Internett. Appens bruk av denne informasjonen

er underlagt personvernpraksisene til mobiloperatøren din.

Valg og kontroll

Hvis du velger hurtiginstillinger mens du konfigurerer Windows for første gang, søker Windows etter og laster ned mobiloperatørapper automatisk. Du kan aktivere eller deaktivere denne funksjonen i Kontrollpanel. Hvis du vil ha mer informasjon, kan du se delen om enhetsinstallasjon ovenfor.

Du kan avinstallere en mobiloperatørs app når som helst uten å avinstallere maskinvaren for mobilt bredbånd.

Nettverkssøk

Hva denne funksjonen gjør

Når du kobler PCen til et lite privat nettverk som du kanskje har hjemme, kan Windows automatisk søke etter andre PCer og delte enheter på nettverket og gjøre PCen synlig for andre på nettverket. Når delte enheter er tilgjengelige, kan Windows automatisk koble til og installere dem. Eksempler på delte enheter er skrivere og Media Extender-enheter, men ikke personlige enheter som kameraer og mobiltelefoner.

Informasjon som samles inn, behandles eller overføres

Når du aktiverer deling og tilkobling til enheter, blir kanskje informasjon om PCen, for eksempel navn og nettverksadresse, sendt over det lokale nettverket slik at PCer kan finne og koble til den.

For å avgjøre om enheter som er koblet til nettverket, skal installeres automatisk, blir en del informasjon om nettverket samlet inn og sendt til Microsoft. Denne informasjonen omfatter antallet enheter på nettverket, nettverkstypen (for eksempel privat nettverk) og typene og modellnavnene på enhetene på nettverket. Ingen personlige opplysninger, for eksempel navn eller passord, samles inn.

Når Windows installerer delte enheter, kan det hende at Windows sender en del informasjon til Microsoft og installerer enhetsprogramvare på PCen. Dette avhenger av innstillingene for enhetsinstallasjon. Hvis du vil ha mer informasjon, kan du se delen om enhetsinstallasjon.

Bruk av informasjon

Informasjonen om nettverket som sendes til Microsoft, brukes til å avgjøre hvilke enheter på nettverket som skal installeres automatisk. Microsoft bruker ikke informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Hvis du velger å aktivere deling og koble til enheter når du slutter deg til et nettverk, aktiveres nettverkssøk for dette nettverket. Du kan endre denne innstillingen for det gjeldende nettverket ved å klikke nettverkstypen som er oppført under nettverksnavnet i Nettverks- og delingssenter.

Du kan velge om du vil aktivere nettverkssøk og automatisk konfigurasjon av nettverkstilkoblede enheter ved å velge **Endre innstillinger for avansert deling** i Nettverks- og delingssenter.

Kombinere trådløse enheter

Hva denne funksjonen gjør

Windows lar deg kombinere PCen med trådløse enheter som bruker Bluetooth eller Wi-Fi Direct. Wi-Fi Direct er en trådløs teknologi som gjør at enheter kan kommunisere direkte med hverandre uten å måtte koble til et Wi-Fi-nettverk.

Informasjon som samles inn, behandles eller overføres

Når du velger **Tillat Bluetooth-enheter å finne denne datamaskinen i Bluetooth-innstillinger**, sender Windows PCens navn via Bluetooth slik at Bluetooth-aktiverte enheter kan finne og identifisere PCen.

Når du velger **Legg til en enhet** under Enheter i PC-innstillinger, kringkaster Windows PCens navn via Wi-Fi, slik at Wi-Fi Direct-aktiverte enheter kan oppdage og identifisere den. Når du lukker **Legg til en enhet**, slutter Windows å kringkaste PCens navn via Wi-Fi.

Når Windows kombineres med trådløse enheter, kan det hende at Windows sender en del informasjon til Microsoft og installerer enhetsprogramvare på PCen. Dette avhenger av innstillingene for enhetsinstallasjon. Hvis du vil ha mer informasjon, kan du se delen

om enhetsinstallasjon ovenfor.

Bruk av informasjon

Windows kringkaster PCens navn for at andre enheter skal kunne identifisere og koble til PCen. PCens navn sendes ikke til Microsoft.

Valg og kontroll

Du kan endre om Windows skal kringkaste PCens navn ved hjelp av Bluetooth, ved å trykke og holde inne eller høyreklikke PCen i Enheter og skrivere i Kontrollpanel, velge **Bluetooth-innstillinger** og deretter velge **Tillat Bluetooth-enheter å finne denne datamaskinen**. Hvis du ikke vil at Windows skal kringkaste PCens navn via Wi-Fi mens du legger til enheter, kan du midlertidig deaktivere Wi-Fi i Trådløs i PC-innstillinger før du legger til en enhet.

[Øverst på siden](#)

DirectAccess

Hva denne funksjonen gjør

Ved hjelp av DirectAccess kan PCen koble til arbeidsstasjonen eksternt og trådløst når PCen er koblet til Internett, uavhengig av hvor du befinner deg.

Informasjon som samles inn, behandles eller overføres

Hver gang du starter PCen, prøver DirectAccess å koble til nettverket på arbeidsplassen, uansett om du er fysisk til stede på arbeidsplassen eller ikke. Når du er tilkoblet, laster PCen ned arbeidsplasspolicyen, og du har tilgang til konfigurerte ressurser på nettverket på arbeidsplassen. Administratoren på arbeidsplassen kan bruke DirectAccess-tilkobling til å administrere og overvåke PCen din eksternt, inkludert nettstedene du besøker når du ikke er fysisk til stede på arbeidsplassen.

DirectAccess sender ikke informasjon til Microsoft.

Bruk av informasjon

Selskapets policyer fastslår hvordan informasjonen som er samlet inn av administratoren på arbeidsplassen, blir brukt.

Valg og kontroll

Administratoren på arbeidsplassen må konfigurere DirectAccess ved å bruke Gruppetpolicy. Selv om administratoren kan tillate at du midlertidig deaktiverer enkelte elementer i DirectAccess, er det bare administratoren på arbeidsplassen som kan stoppe Windows fra å prøve å koble til arbeidsplassen for administrasjonsformål. Hvis du eller administratoren på arbeidsplassen fjerner PCen fra arbeidsplassdomenet, kan ikke DirectAccess lenger koble til.

[Øverst på siden](#)

Dynamisk oppdatering

Hva denne funksjonen gjør

Dynamisk oppdatering lar Windows utføre en engangssjekk i Windows Update for å hente de siste oppdateringene for PCen mens Windows installeres. Hvis det blir funnet oppdateringer, laster Dynamisk oppdatering dem automatisk ned, slik at PCen din er oppdatert første gang du logger på eller bruker den.

Informasjon som samles inn, behandles eller overføres

For å installere kompatible drivere, sender Dynamisk oppdatering informasjon til Microsoft om maskinvaren på PCen din. Dynamisk oppdatering kan blant annet laste ned følgende typer oppdateringer til PCen:

- **Installasjonsoppdateringer.** Viktige programvareoppdateringer for installasjonsfiler for å bidra til at installasjonen blir vellykket.
- **Oppdateringer av inkluderte drivere.** Viktige driveroppdateringer for versjonen av Windows du installerer.

Bruk av informasjon

Dynamisk oppdatering sender informasjon til Microsoft om maskinvaren på PCen for å kunne finne de riktige driverne for systemet. Hvis du vil ha mer informasjon om hvordan informasjonen som samles inn av Dynamisk oppdatering, brukes, kan du se [personvernerklæringen for Oppdateringstjenester](#).

Valg og kontroll

Når du begynner å installere Windows, blir du spurt om du vil koble til Internett for å installere oppdateringer.

[Øverst på siden](#)

Hjelpemiddelsenter

Hva denne funksjonen gjør

Ved hjelp av hjelpemiddelsentret kan du aktivere tilgjengelighetsalternativer og -innstillinger slik at det blir enklere å samhandle med PCen.

Informasjon som samles inn, behandles eller overføres

Hvis du bruker denne funksjonen, blir du bedt om å velge riktige innstillinger.

Disse innstillingene inkluderer:

- Bilder og tekst på TV som er vanskelige å se.
- Lysforhold som gjør det vanskelig å se bilder på skjermen.
- Jeg bruker ikke et tastatur.
- Jeg er blind.
- Jeg er døv.
- Jeg har en talehemmelse.

Denne informasjonen lagres i et uleselig format og lagres lokalt på PCen.

Bruk av informasjon

Du får et sett med konfigurasjonsanbefalinger basert på utsagnene du velger. Denne informasjonen sendes ikke til Microsoft og er ikke tilgjengelig for andre brukere, unntatt deg og administratorer på PCen.

Valg og kontroll

Du kan velge hvilke utsagn du vil bruke, ved å gå til Hjelpemiddel i

Kontrollpanel. Du kan når som helst endre valgene dine. Du kan også velge hvilke anbefalinger du vil konfigurere på PCen.

[Øverst på siden](#)

Hendelsesliste

Hva denne funksjonen gjør

PC-brukere, primært administratorer, kan bruke hendelseslisten til å vise og administrere hendelseslogger. Hendelseslogger inneholder informasjon om maskinvare-, programvare- og sikkerhetshendelser på PCen. Du kan også få informasjon fra Microsoft om hendelser i hendelseslogger ved å klikke Logghjelp på Internett.

Informasjon som samles inn, behandles eller overføres

Hendelseslogger inneholder hendelsesinformasjon som genereres av alle brukere og apper på PCen. Alle brukere kan som standard vise oppføringer i hendelseslogger. Administratorer kan imidlertid begrense tilgangen til hendelseslogger. Du får tilgang til hendelsesloggene for PCen ved å åpne Hendelsesliste. Hvis du vil vite hvordan du åpner Hendelsesliste, kan du se Windows Hjelp og støtte.

Hvis du bruker Logghjelp på Internett til å slå opp tilleggsinformasjon om en bestemt hendelse, sendes informasjon om hendelsen til Microsoft.

Bruk av informasjon

Når du bruker Logghjelp på Internett til å slå opp informasjon om en hendelse, brukes hendelsesdataene som sendes fra PCen din, til å finne og bruke tilleggsinformasjon om hendelsen. Når det gjelder Microsoft-hendelser, sendes hendelsesdetaljene til Microsoft.

Microsoft bruker ikke denne informasjonen til å identifisere, kontakte eller sende reklame til deg. Når det gjelder hendelser som er knyttet til tredjepartsapper, sendes informasjonen til stedet som er angitt av tredjepartsutgiveren eller -produsenten. Hvis du sender informasjon om hendelser til tredjepartsutgivere eller -produsenter, er bruk av informasjonen underlagt personvernpraksisen til hver enkelt tredjepart.

Valg og kontroll

Administratorer kan begrense tilgang til logger i Hendelsesliste. Brukere som har full tilgang til logger i hendelseslisten, kan tømme dem. Hvis ikke du tidligere har godtatt at hendelsesinformasjon sendes automatisk når du klikker Logghjelp på Internett, blir du bedt om å bekrefte at informasjonen kan sendes via Internett. Det sendes ingen hendelsesloginformasjon via Internett hvis du ikke samtykker i at den sendes. Administratorer kan bruke Gruppetpolicy til å velge eller endre nettstedet som hendelsesinformasjon sendes til.

[Øverst på siden](#)

Tryggere for familien

Hva denne funksjonen gjør

Tryggere for familien hjelper foreldre med å beskytte barna når de bruker en PC. Foreldre kan kontrollere hvilke apper, spill og nettsteder barna bruker. Foreldre kan også angi tidsbegrensninger og motta regelmessige aktivitetsrapporter via e-post. Foreldre kan definere begrensninger og vise aktivitetsrapporter lokalt på PCen, eller elektronisk ved hjelp av nettstedet for Microsoft Tryggere i familien.

Informasjon som samles inn, behandles eller overføres

Innstillinger for Tryggere for familien og rapporter for barns aktiviteter lagres på PCen. Aktivitetsrapporter kan inkludere informasjon om tidsbruk på datamaskinen, tidsbruk på apper og spill, og nettsteder som er besøkt (inkludert forsøk på å vise blokkerte nettsteder). Administratorer på PCen kan endre innstillinger og vise aktivitetsrapporten.

Hvis elektronisk administrasjon er aktivert for en barnekonto, kan foreldre vise barnets aktivitetsrapport og endre innstillinger på nettstedet Microsoft Tryggere for familien. En forelder kan tillate at andre personer viser aktivitetsrapporter og endrer innstillinger ved å legge til seg selv som foreldre på nettstedet for Microsoft Tryggere for familien. Hvis forelderens som konfigurerer Tryggere for familien, er logget på Windows med en Microsoft-konto, aktiveres elektronisk administrasjon automatisk.

Når Tryggere for familien er konfigurert for en barnekonto med elektronisk administrasjon aktivert, blir ukentlige rapporter med barnets aktivitet sendt automatisk via e-post til forelder.

Bruk av informasjon

Windows og nettstedet for Microsoft Tryggere i familien bruker den innsamlede informasjonen til bruk av funksjonen Tryggere for familien. Microsoft kan i enkelte tilfeller analysere aktivitetslogginformasjon av hensyn til datakvaliteten, men vi bruker ikke denne informasjonen til å identifisere, kontakte eller sende reklame til enkeltbrukere.

Valg og kontroll

Tryggere for familien er som standard deaktivert. Du får tilgang til Tryggere for familien i Kontrollpanel. Bare administratorer kan aktivere Tryggere for familien, og bare brukere uten administratorrettigheter kan overvåkes eller begrenses. Barn kan se sine innstillinger, men kan ikke endre dem. Hvis Tryggere for familien er aktivert, mottar barnet en varsling om at Tryggere for familien overvåker kontoen, hver gang barnet logger på Windows. Hvis du angir at kontoen er en barnekonto under kontoopprettingen, kan du velge å aktivere Tryggere for familien for den kontoen.

Hvis administratoren som konfigurerer en barnekonto, er logget på Windows med en Microsoft-konto, aktiveres elektronisk administrasjon automatisk, og rapporter om barnets aktivitet sendes ukentlig. Foreldrekontoer kan legges til eller fjernes på nettstedet for Microsoft Tryggere for familien. Brukere som er lagt til som en forelder på nettstedet, kan vise et barns aktivitetsrapport og endre barnets innstillinger for Tryggere for familien, selv om forelder ikke er administrator på PCen som barnet bruker.

Hvis Tryggere for familien skal brukes på riktig måte, bør bare foreldre være administratorer på sin egen PC, og barn bør ikke få administratorrettigheter. Vær oppmerksom på at bruk av denne funksjonen til å overvåke andre brukere (for eksempel voksne) kan være et brudd på gjeldende lov.

[Øverst på siden](#)

Faks

Hva denne funksjonen gjør

Faksfunksjonen gir deg også muligheten til å skrive og lagre faksforsider, og hvordan du sender og mottar fakser ved hjelp av PCen og et eksternt eller innebygd modem eller en fakserver.

Informasjon som samles inn, behandles eller overføres

Informasjon som samles inn, omfatter alle personlige opplysninger som er på en faksforside, samt identifikatorer i faksprotokoller som er bransjestandard, for eksempel sendeabonnementsidentifikator (TSID) og mottaksstasjonsidentifikator (CSID). Windows bruker som standard "Faks" som verdi for hver identifikator.

Bruk av informasjon

Informasjon du skriver inn i dialogboksen Avsender, vises på faksforsiden. Identifikatorer som TSID og CSID kan inneholde vilkårlig tekst og brukes vanligvis av den mottakende faksmaskinen eller PCen til å identifisere avsenderen. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Fakstilgang fastsettes av brukerkontorettingene på PCen. Hvis ikke en faksadministrator har endret tilgangsinstillingene, kan alle brukere sende og motta fakser. Alle brukere kan som standard vise dokumentene de sender, og alle fakser de mottar på PCen. Administratorer kan vise alle sendte og mottatte faksdokumenter og konfigurere faksinnstillinger, inkludert hvem som har tillatelse til å vise eller administrere fakser, og TSID- og CSID-verdiene.

[Øverst på siden](#)

Håndskrifttilpassing – automatisk læring

Hva denne funksjonen gjør

Automatisk læring er et tilpassingsverktøy for håndskriftgjenkjenning som er tilgjengelig på PCer med berøring eller tavlepen. Denne funksjonen samler inn data om ordene du bruker, og hvordan du skriver dem. Dette bidrar til at programvaren for

håndskriftgjenkjenning kan gjenkjenne og forbedre tolkningen av håndskriftstilen og vokabularet, og det forbedrer også automatisk korrigerings- og tekstforslagsfunksjonen for språk uten IMEer (Input Method Editors).

Informasjon som samles inn, behandles eller overføres

Informasjonen som samles inn av automatisk læring, lagres i brukerprofilen for hver bruker på PCen. Dataene lagres i rettighetsbeskyttet format som ikke kan leses med en tekstvisningsapp (for eksempel Notisblokk eller WordPad), og bare er tilgjengelig for andre brukere hvis de er administratorer på PCen din.

Den innsamlede informasjonen inkluderer:

- Tekst fra meldinger du skriver og kalenderoppføringer du oppretter ved hjelp av e-postapper (for eksempel Office Outlook eller Windows Live Mail), inkludert meldinger du allerede har sendt.
- Bokstaver du skriver i Inndatapanel.
- Gjenkjent tekst du skriver i Inndatapanel eller på skjermtastaturet.
- Alternative tegn du velger for å korrigere den gjenkjente teksten.

Bruk av informasjon

Den innsamlede informasjonen brukes til å forbedre håndskriftgjenkjenning ved å opprette en versjon av gjenkjenningsprogramvaren som er tilpasset din egen stil og ditt eget vokabular, og til å aktivere automatisk korrigerings- og tekstforslagsfunksjonen etter hvert som du skriver på skjermtastaturet.

Teksteksemplene brukes til å opprette en utvidet ordliste. Håndskrifteksemplene brukes til å bidra til å forbedre tegngjenkjenning for hver bruker på en PC. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Automatisk læring er aktivert som standard. Du kan når som helst aktivere eller deaktivere automatisk læring ved å gå til Avanserte innstillinger i Språk i Kontrollpanel. Når du deaktiverer automatisk læring, slettes alle data som er samlet inn og lagret ved hjelp av automatisk læring.

[Øverst på siden](#)

Hjemmegruppe

Hva denne funksjonen gjør

Ved hjelp av Windows kan du enkelt koble PCer i hjemmenettverket slik at du kan dele bilder, musikk, videoer, dokumenter og enheter. Den gir også PCer muligheten til å strøemme medier på enheter i hjemmenettverket, for eksempel en Media Extender-enhet. Disse PCene og enhetene er hjemmegruppen din. Du kan beskytte hjemmegruppen med et passord, og du kan velge hva du vil dele.

Informasjon som samles inn, behandles eller overføres

Du har tilgang til egne filer, for eksempel bilder, videoer, musikk og dokumenter, fra alle PCene i hjemmegruppen. Når du blir med i en hjemmegruppe, deles kontoinformasjon (inkludert e-postadresse, visningsnavn og bilde) for alle Microsoft-kontoer på PCen din, med andre i hjemmegruppen slik at deling med andre aktiveres.

Bruk av informasjon

Informasjonen som samles inn, gjør at PCene i hjemmegruppen kan finne ut hvem innholdet skal deles med, og hvordan det skal presenteres. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Du kan legge til eller fjerne PCer fra hjemmegruppen og bestemme hva som skal deles med andre medlemmer i hjemmegruppen. Du kan opprette en hjemmegruppe og administrere innstillingene for den ved å gå til Hjemmegruppe i PC-innstillinger.

[Øverst på siden](#)

IME (Input Method Editor)

Microsoft IMEer (Input Method Editors) brukes med østasiatiske språk til å konvertere tastaturinndata til ideogrammer. Denne delen omtaler flere funksjoner, inkludert automatisk justering og forutsigelse i IMEer, rapportering av IME-konverteringsfeil og IME-ordregistrering.

Automatisk justering og forutsigelse i IMEer **Hva denne funksjonen gjør**

Avhengig av IMEen og innstillingene du bruker, kan det hende at funksjonene for automatisk justering og tekstforslag i IME registrerer ord eller ordsekvenser for å forbedre valget av ideogrammene som vises.

Informasjon som samles inn, behandles eller overføres

Funksjonene for automatisk justering (selvlæring) og tekstforslag i IME registrerer et ord eller en sekvens med ord og hvor ofte du bruker dem. Informasjon om automatisk justering (unntatt tegnsekvenser med sifre/symboler) lagres i filer for hver bruker på en PC.

Bruk av informasjon

Data for automatisk læring og tekstforslag brukes av IMEen på PCen til å forbedre valg av ideogrammer som vises når du bruker IMEen. Hvis du velger å sende disse dataene til Microsoft, brukes de til å forbedre IMEen og relaterte produkter og tjenester.

Valg og kontroll

Med unntak av IMEen for forenklet kinesisk (der forutsigelsesfunksjonen er av som standard) er funksjonene for automatisk læring og tekstforslag aktivert som standard i IMEene som støtter dem. De innsamlede dataene sendes ikke automatisk til Microsoft. Du kan velge om du vil samle inn eller sende disse dataene, i Språk i Kontrollpanel.

Rapportering av IME-konverteringsfeil **Hva denne funksjonen gjør**

Hvis det forekommer feil under visning av ideogrammer eller under konvertering av tastaturinndata til ideogrammer, kan denne funksjonen samle inn informasjon om feilene, og denne

informasjonen kan bidra til at Microsoft kan forbedre sine produkter og tjenester.

Informasjon som samles inn, behandles eller overføres

Funksjonen for rapportering av IME-konverteringsfeil samler inn informasjon om IME-konverteringsfeil, for eksempel det du har skrevet inn, den første konverteringen og forutsigelsesresultatet, strengen du valgte i stedet, informasjon om IMEen du bruker, og informasjon om hvordan du bruker den. Hvis du bruker den japanske IMEen, kan du i tillegg inkludere informasjon om automatisk læring i konverteringsfeilrapporter.

Bruk av informasjon

Microsoft bruker informasjonen til å forbedre produktene og tjenestene sine. Microsoft bruker ikke informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Etter at et visst antall konverteringsfeil er lagret, får du spørsmål om du vil sende en konverteringsfeilrapport, i verktøyet for konverteringsfeilrapport. Du kan også når som helst sende en konverteringsfeilrapport fra verktøyet for IME-konverteringsfeilrapport. Du kan vise informasjonen i hver rapport før du eventuelt velger å sende den. Du kan også aktivere automatisk sending av konverteringsfeilrapporter i IME-innstillinger.

IME-ordregistrering

Hva denne funksjonen gjør

Du kan kanskje bruke ordregistrering til å rapportere ustøttede ord (ord som kanskje ikke konverteres riktig til ideogrammer fra tastaturinndata), men dette avhenger av IME-enheten du bruker.

Informasjon som samles inn, behandles eller overføres

Registreringsrapporter kan inneholde informasjonen du oppgir i dialogboksen Legg til ord om ordene som rapporteres, og programvare versjonsnummeret for en IME. Disse rapportene kan inneholde personlige opplysninger, for eksempel hvis du legger til personnavn ved å bruke ordregistrering. Du kan gå gjennom dataene som sendes med hver rapport, før du eventuelt velger å

sende den.

Bruk av informasjon

Microsoft bruker informasjonen til å forbedre produktene og tjenestene sine. Microsoft bruker ikke informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Hver gang du oppretter en ordregistreringsrapport, får du spørsmål om du vil sende denne rapporten til Microsoft. Du kan vise informasjonen i rapporten før du eventuelt velger å sende den.

[Øverst på siden](#)

Program for installasjonsforbedring

Hva denne funksjonen gjør

Denne funksjonen sender en enkelrapport til Microsoft, og rapporten inneholder grunnleggende informasjon om PCen din og hvordan du installerte Windows 8. Microsoft bruker denne informasjonen til å forbedre installasjonsopplevelsen og finne løsninger på vanlige installasjonsproblemer.

Informasjon som samles inn, behandles eller overføres

Rapporten inneholder generelt sett informasjon om installasjonsprosessen, for eksempel installasjonsdatoen, hvor lang tid det gikk før hver installasjonsfase ble fullført, om installasjonen var en oppgradering eller en ny installasjon av produktet, versjonsdetaljer, operativsystemspråk, medietype, PC-konfigurasjon, om installasjonen var vellykket eller mislykket, og i tillegg eventuelle feilkoder.

Hvis du velger å bli med i programmet for installasjonsforbedring, sendes rapporten til Microsoft når du er tilkoblet Internett. Programmet for installasjonsforbedring genererer et tilfeldig nummer kalt GUID (globalt unik identifikator) som sendes til Microsoft sammen med rapporten. GUIDen lar oss fastslå hvilke data som sendes fra en bestemt datamaskin over tid. GUIDen inneholder ingen personlige opplysninger og brukes ikke til å identifisere deg.

Bruk av informasjon

Microsoft og våre partnere bruker rapporten til å forbedre produktene og tjenestene sine. Vi bruker GUIDen til å opprettholde disse dataene med dataene som er innsamlet av Windows CEIP (Customer Experience Improvement Program), som er et program du kan velge å delta i når du bruker Windows 8

Valg og kontroll

Du kan velge å delta i dette programmet når du installerer Windows 8 ved å velge **Jeg vil hjelpe til med å gjøre installasjonen av Windows bedre** .

Hvis du vil ha mer informasjon, kan du se delen om Windows-programmet for forbedret kundeopplevelse.

[Øverst på siden](#)

Internett-utskrift

Hva denne funksjonen gjør

Internett-utskrift lar deg skrive ut via Internett.

Informasjon som samles inn, behandles eller overføres

Når du skriver ut ved å bruke denne funksjonen, må du først koble til og godkjenne deg selv på en Internett-utskriftsserver. Informasjonen du må sende inn til utskriftsserveren, varierer avhengig av sikkerhetsnivået som utskriftsserveren støtter (for eksempel kan du bli bedt om å oppgi et brukernavn og passord). Når du er koblet til, vises en liste over kompatible skrivere. Hvis PCen ikke har en skriverdriver for den valgte skriveren, kan du laste ned en driver fra utskriftsserveren. Utskriftsjobber krypteres ikke, og derfor er det mulig for andre å se innholdet som sendes.

Bruk av informasjon

Informasjonen som samles inn, gjør at du kan skrive ut ved å bruke eksterne skrivere. Hvis du velger å bruke en utskriftsserver som er driftet av Microsoft, bruker vi ikke informasjonen du oppgir, til å identifisere, kontakte eller sende reklame til deg. Hvis du sender informasjon til en tredjeparts utskriftsserver, er bruk av

informasjonen underlagt tredjepartens personvernpraksiser.

Valg og kontroll

Du kan aktivere eller deaktivere Internett-utskrift ved å åpne Programmer og funksjoner i Kontrollpanel, og deretter velger du **Slå Windows-funksjoner på eller av**.

[Øverst på siden](#)

Språkinnstillinger

Hva denne funksjonen gjør

Du kan legge til språkene du foretrekker å bruke, i språklisten i Windows 8. Apper og nettsteder vises på det første språket som er tilgjengelig i denne listen.

Informasjon som samles inn, behandles eller overføres

Når du besøker nettsteder og installerer apper på PCen, sendes listen over foretrukkede språk til nettstedene du besøker, og er tilgjengelig for appene du bruker, slik at de kan tilby innholdet på språkene du foretrekker.

Bruk av informasjon

Listen over foretrukkede språk brukes av Microsofts nettsteder og apper til å formidle innhold på de foretrukkede språkene. Microsoft bruker ikke språkinformasjon til å identifisere eller kontakte deg. Språkinformasjon som er sendt eller som brukes tredjepartsnettsteder og -apper, er underlagt personvernpraksisene for tredjepartsnettstedet eller -apputgiveren.

Valg og kontroll

Listen over foretrukkede språk er tilgjengelig for appene du installerer, og nettsteder du besøker. Du kan legge til eller fjerne språk fra denne listen i Språkinnstillinger i Kontrollpanel. Hvis du ikke har noen språk i denne listen, sendes språkene du velger i kategorien Formater i Område i Kontrollpanel, til nettstedene du besøker.

[Øverst på siden](#)

Posisjonstjenester

På PCer med Windows henviser "posisjonstjenester" til Windows-programvaren og Microsofts netjtjenester som brukes til å fastslå den omtrentlige fysiske posisjonen til PCen din, som oppgis til apper eller nettsteder du gir tilgang til denne informasjonen. Windows Location-plattform finner posisjonen med dedikert maskinvare, for eksempel en GPS-sensor i PCen, eller med programvare, for eksempel Windows Lokasjonstjeneste.

Windows Location-plattform

Hva denne funksjonen gjør

Hvis du velger å aktivere Windows Location-plattformen, kan apper du installerer fra Windows Store, be om tillatelse til å bruke PCens plassering. Avhengig av systemkonfigurasjonen, kan det hende plattformen kan fastslå PCens plassering ved hjelp av maskinvare, for eksempel en GPS-sensor eller programvare, for eksempel Windows Lokasjonstjeneste.

Plattformen hindrer ikke at apper får tilgang til PCens plassering på andre måter. Du kan for eksempel installere enheter (for eksempel en GPS-mottaker) som kan sende plasseringsinformasjon direkte til en app og dermed omgå plattformen. Uavhengig av innstillingene for Windows Location-plattform, kan elektroniske tjenester bruke PCens IP-adresse til å fastslå den omtrentlige plasseringen, som vanligvis er byen PCen din befinner seg i.

Informasjon som samles inn, behandles eller overføres

Selve Windows Location-plattformen overfører ingen informasjon fra PCen, men enkeltstående plasseringsleverandører (for eksempel Windows Lokasjonstjeneste) kan overføre informasjon når du bruker plasseringsfølsomme apper. Apper som er autorisert til å bruke plattformen til å fastslå plasseringen din, kan også overføre eller lagre den informasjonen.

Bruk av informasjon

Hvis du aktiverer Windows Location-plattformen, kan autoriserte apper få tilgang til plasseringen din og bruke den til å gi deg tilpasset innhold. Hvis du bruker en tredjepartsapp eller -

lokasjonstjeneste, vil dens bruk av PCens plassering være underlagt tredjepartens personvernpraksis. Før du laster ned en Windows Store-app, kan du se om appen er plasseringsfølsom i appbeskrivelsen.

Valg og kontroll

Hvis du velger hurtiginstillinger mens du konfigurerer Windows, aktiverer du Windows Location-plattformen. Hvis du velger å tilpasse innstillingene, kan du kontrollere Windows Location-plattformen ved å velge **Slå på Windows Location-plattform slik at apper kan spørre brukerne om deres plassering** under **Del informasjon med apper**. Første gang hver Store-app ber om PCens plassering, spør Windows om du vil tillate det eller ikke. Du kan kontrollere om apper kan spørre om plasseringen, under Personvern i PC-innstillinger, og du kan kontrollere om en enkeltstående Store-app kan bruke plasseringen din i Tillatelser i appens Innstillinger-perle.

Hvis du bruker en skrivebordsapp som bruker Windows Location-plattform, bør den be om din tillatelse til å bruke PCens plassering, og når den får tilgang til PCens plassering, vises det et ikon i varslingsområdet slik at du får beskjed om at PCens plassering er oppgitt. Hver bruker kan kontrollere sine egne plasseringsinnstillinger for alle apper under Personvern i PC-innstillinger. I tillegg kan administratorer velge å slå av Windows Location-plattformen for alle brukere under Plassering i Kontrollpanel.

Windows Lokasjonstjeneste

Hva denne funksjonen gjør

Windows Lokasjonstjeneste kobler til den elektroniske forekomsten av Microsoft Lokasjonstjeneste som fastslår PCens omtrentlige plassering basert på Wi-Fi-nettverk i nærheten av PCen eller PCens IP-adresse.

Informasjon som samles inn, behandles eller overføres

Når en app du har autorisert til å få oppgitt plasseringen din, spør om dette, spør Windows Location-plattformen alle installerte plasseringstjenester (inkludert Windows Lokasjonstjeneste) om å fastslå din gjeldende plassering. Windows Lokasjonstjeneste sjekker

først om det finnes en liste med Wi-Fi-tilgangspunkt fra en tidligere forespørsel fra en plasseringsfølsom app. Hvis det ikke allerede finnes en liste over Wi-Fi-tilgangspunkt i nærheten, eller hvis listen er utdatert, sender leverandøren informasjon om Wi-Fi-tilgangspunkt i nærheten og GPS-informasjon (hvis tilgjengelig) til Microsoft Lokasjonstjeneste. Tjenesten returnerer PCens omtrentlige plassering tilbake til Windows Lokasjonstjeneste, som sender plasseringen til Windows Location-plattformen, som på sin side sender den til appen som ba om plasseringen. Windows Lokasjonstjeneste kan også oppdatere sin lagrede liste over Wi-Fi-tilgangspunkt. Windows Lokasjonstjeneste administrerer denne listen slik at den kan fastslå PCens omtrentlige plassering uten å koble til Internett hver gang. Denne listen over tilgangspunkt krypteres når den lagres på en disk slik at apper ikke direkte får tilgang til den.

Informasjonen som ble sendt om Wi-Fi-tilgangspunkt i nærheten, inkluderer BSSID (MAC-adressen for Wi-Fi-tilgangspunktet) og signalstyrke. GPS-informasjonen omfatter observert breddegrad, lengdegrad, retning, hastighet og høyde. Windows Lokasjonstjeneste sender ikke informasjon for å identifisere PCen din utover standardinformasjonen for datamaskin, som sendes med alle tilkoblinger til Internett. På den måten beskyttes personvernet. Windows sender ikke SSIDer (navn på Wi-Fi-tilgangspunkt) eller skjulte Wi-Fi-nettverk. På den måten beskyttes personvernet for eiere av Wi-Fi-nettverk. Av hensyn til personvern og sikkerhet sendes informasjon om Wi-Fi-nettverk kryptert via SSL.

Bruk av informasjon

Informasjonen brukes av Windows Lokasjonstjeneste til å gi Windows Location-plattformen den omtrentlige plasseringen for PCen din når en autorisert app ber om den.

Hvis du velger å forbedre Microsoft Lokasjonstjeneste, blir Wi-Fi- og GPS-informasjon som er sendt til Microsoft, brukt til å forbedre Microsofts lokasjonstjenester, noe som forbedrer lokasjonstjenestene i appene dine. Microsoft lagrer ingen innsamlede data fra denne tjenesten som kan brukes til å identifisere, kontakte, sende reklame til deg eller spore eller opprette en logg over plasseringen til PCen din.

Valg og kontroll

Windows Lokasjonstjeneste brukes bare hvis en autorisert app har bedt om PCens plassering. Hvis du vil ha mer informasjon om hvordan du kontrollerer om apper kan be om PCens plassering, kan du se delen Windows Location-plattform. Hvis du autoriserer apper til å be om plasseringen til PCen din, blir den bufrede listen med Wi-Fi-tilgangspunkt i nærheten, som er kryptert og lagret av Windows Lokasjonstjeneste, slettet og erstattet regelmessig.

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, velger du å forbedre Microsoft Lokasjonstjeneste. Hvis du velger å tilpasse innstillinger, kan du kontrollere om du vil forbedre Microsoft Lokasjonstjeneste ved å velge **Hjelp med å forbedre Microsoft-tjenester ved å sende noen plasseringsdata når plasseringsfølsomme apper brukes** under **Send Microsoft-informasjon for å bidra til å gjøre Windows og apper bedre**.

Etter at du har konfigurert Windows, kan du endre denne innstillingen under Plasseringsinnstillinger i Kontrollpanel. Hvis du velger ikke å forbedre tjenesten, kan du likevel bruke Windows Lokasjonstjeneste til å fastslå PCens omtrentlige plassering.

Du kan aktivere og deaktivere Windows Lokasjonstjeneste ved å åpne **Slå Windows-funksjoner på eller av** i Kontrollpanel. Hvis du deaktiverer Windows Lokasjonstjeneste, kan du likevel bruke andre lokasjonstjenester (for eksempel GPS) med Windows Location-plattform.

[Øverst på siden](#)

Navn og kontobilde

Hva denne funksjonen gjør

Apper kan be om navnet og kontobildet ditt fra Windows for å gi deg tilpasset innhold. Navnet og kontobildet ditt vises under Din konto under Brukere i PC-innstillinger. Hvis du logger på Windows med en Microsoft-konto, bruker Windows navnet og kontobildet som er knyttet til den kontoen. Hvis du ikke har valgt et bilde for kontoen, blir kontobildet illustrert med et standardbilde fra Windows.

Informasjon som samles inn, behandles eller overføres

Hvis du tillater at apper får tilgang til navnet og kontobildet ditt, oppgir Windows den informasjonen til alle apper som ber om det. Apper kan lagre eller overføre denne informasjonen.

Hvis du logger på Windows med en domenekonto, og du velger å tillate at apper bruker navnet og kontobildet ditt, får apper som kan bruke Windows-legitimasjonen din, tillatelse til å bruke andre deler av informasjonen om domenekontoen din. Denne informasjonen inkluderer for eksempel brukerhovednavnet ditt (for eksempel jack@contoso.com) og DNS-domenenavnet ditt (for eksempel corp.contoso.com\jack).

Hvis du logger på Windows med en Microsoft-konto, eller hvis du logger på Windows med en domenekonto som er koblet til en Microsoft-konto, kan Windows automatisk synkronisere kontobildet ditt på PCen med kontobildet for Microsoft.

Bruk av informasjon

Hvis du bruker en tredjepartsapp, er praksisen for hvordan appen bruker navnet og kontobildet ditt underlagt tredjepartens personvernpraksis. Hvis du bruker en Microsoft-app, blir appens personvernpraksis forklart i denne personvernerklæringen.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, lar Windows apper få tilgang til navnet og kontobildet ditt. Hvis du velger å tilpasse innstillingene, kan du kontrollere tilgang til navnet og kontobildet ved å velge **La apper bruke navnet og kontobildet mitt** under **Del informasjon med apper**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under **Personvern** i PC-innstillinger. Du kan endre kontobildet under **Tilpass** i PC-innstillinger. Du kan også velge å tillate at bestemte apper kan endre kontobildet ditt.

[Øverst på siden](#)

Nettverkssporing

Hva denne funksjonen gjør

Hvis du har en abonnementsplan for nettverkstilgang (for eksempel

via en mobil bredbåndstilkobling), gir denne funksjonen informasjon om abonnementsplanen til apper og Windows-funksjoner på PCen din. Windows-funksjoner og apper kan bruke denne informasjonen til å optimalisere virkemåten. Hvis du for eksempel har et dataabonnement med forbruksmåling, venter Windows Update med å levere oppdateringer med lavere prioritet til PCen til du er koblet til en annen type nettverk. Denne funksjonen gir også informasjon om nettverkstilkoblingen, for eksempel signalstyrke og om PCen er koblet til Internett.

Informasjon som samles inn, behandles eller overføres

Denne funksjonen samler inn tilkoblingsinformasjon for Internett og intranett, for eksempel DNS-suffikset (Domain Name Service) for PCen, nettverksnavnet og gateway-adressen til nettverkene som PCen kobler til. Denne funksjonen mottar også abonnementsplaninformasjon, for eksempel gjenstående mengde data i planen.

Profiler for nettverkstilkobling kan omfatte en logg over alle besøkte nettverk samt dato og klokkeslett for siste tilkobling. Denne funksjonen kan prøve å koble til en Microsoft-server for å avgjøre om du er koblet til Internett. De eneste dataene som sendes til Microsoft under nettverkstilkoblingssjekker, er standard PC-informasjon.

Bruk av informasjon

Hvis det sendes data til Microsoft, brukes de bare til å gi statusen for nettverkstilkoblingen. Status for nettverkstilkobling gjøres tilgjengelig for apper og funksjoner på PCen som ber om informasjon om nettverkstilkobling. Hvis du bruker en tredjepartsapp, er bruk av innsamlet informasjon underlagt tredjepartens personvernpraksis.

Valg og kontroll

Nettverkssporing er aktivert som standard. En administrator kan deaktivere den ved å bruke alternativer for Tjenester i Administrative verktøy i Kontrollpanel. Det anbefales ikke at denne funksjonen deaktiveres, siden enkelte Windows-funksjoner dermed blir forhindret fra å fungere riktig.

[Øverst på siden](#)

Varslinger, låseskjermapper og flisoppdateringer

Windows Store-apper kan motta innhold og vise varslinger automatisk på flere måter. De kan for eksempel motta varslinger som vises et par sekunder i hjørnet på skjermen, eller på appfliser hvis de flisene er festet på startmenyen. Du kan også motta de varslingsene på låseskjermen hvis du ønsker det. Låseskjermen kan i tillegg vise detaljert eller kort status for bestemte apper. Apputgivere kan sende innhold til Windows Store-appene dine via Windows Push Notification-tjenesten som kjører på Microsoft-servere, eller appene kan laste ned informasjon direkte fra tredjepartsservere.

Varslinger

Hva denne funksjonen gjør

Windows Store-apper kan sende deg regelmessig informasjon eller sanntidsinformasjon som vises kort som varslinger i hjørne på skjermen.

Informasjon som samles inn, behandles eller overføres

Apper kan vise tekst, bilder eller begge deler i varslinger. Innholdet i varslinger kan formidles lokalt av appen (for eksempel en alarm fra en klokkeapp). Varslinger kan også sendes fra en apps elektroniske tjeneste via Windows Push Notification-tjenesten (for eksempel en oppdatering om sosialt nettverk). Bilder som vises i varslinger, kan være lastet ned fra en server som ble angitt av apputgiveren. Når det skjer, sendes standardinformasjon om datamaskin til den serveren.

Bruk av informasjon

Microsoft bruker bare varslingsinformasjon til å sende deg varslinger fra appene. Varslingen kan lagres midlertidig av Windows Push Notification-tjenesten før den leveres til PCen din. Hvis en varsling ikke kan leveres med en gang, lagres den bare i et par minutter før den slettes.

Valg og kontroll

Du kan slå av varslinger for alle apper eller for enkeltapper under **Varslinger** i PC-innstillinger. Hvis du slår av varslinger for en app

eller avinstallerer den, kan apputgiveren likevel sende oppdateringer til Windows Push Notification-tjenesten, men de varslingene vises ikke på PCen din.

Låseskjermapper

Hva denne funksjonen gjør

Noen apper kan vises status og varslinger på skjermen når PCen din er låst. Låseskjermapper kan også utføre oppgaver i bakgrunnen mens du ikke bruker dem, for eksempel synkronisering av e-post.

Informasjon som samles inn, behandles eller overføres

Låseskjermapper kan motta statusoppdateringer fra apputgiveren via Windows Push Notification-tjenesten, eller direkte fra apputgiverens (eller en annen tredjeparts) servere. Låseskjermapper kan også overføre eller behandle annen informasjon som ikke er relatert til varslinger og oppdateringer.

Bruk av informasjon

Windows bruker status- og varslingsinformasjonen fra låseskjermappene til å oppdatere låseskjermen.

Valg og kontroll

Etter at du har konfigurert Windows, angis Mail-, Kalender- og Meldinger-appene automatisk som låseskjermapper. Du kan legge til eller fjerne disse eller andre apper fra låseskjermen under Tilpass i PC-innstillinger. Du kan også velge at én app konsekvent viser detaljert status (for eksempel detaljer om den neste avtalen i kalenderen din) på låseskjermen.

Du kan kontrollere om låseskjermapper kan vise varsler på låseskjermen, under Varslinger i PC-innstillinger.

Flisoppdateringer

Hva denne funksjonen gjør

Windows Store-apper kan sende deg regelmessig informasjon eller sanntidsinformasjon som vises som oppdateringer for flisene for appene i Start.

Informasjon som samles inn, behandles eller overføres

Store-apper som er festet på startmenyen, kan oppdatere sine fliser med tekst, bilder eller begge deler. Innholdet som vises på en appflis, kan formidles lokalt av appen, lastes ned regelmessig fra en angitt server av apputgiveren, eller sendes fra en apps elektroniske tjeneste via Windows Push Notification-tjenesten. Hvis flisinnhold lastes ned fra en server som ble angitt av apputgiveren, sendes standardinformasjon om datamaskin til den serveren.

Bruk av informasjon

Microsoft bruker bare flisinformasjon til å levere flisoppdateringer fra appene dine til deg. Denne informasjonen kan lagres midlertidig av Windows Push Notification-tjenesten før den leveres til PCen din. Hvis en flisoppdatering ikke kan leveres med en gang, lagres den bare i noen dager før den slettes.

Valg og kontroll

Etter at en app har begynt å motta flisoppdateringer, kan du slå dem av ved å velge appflisen på startmenyen og velge **Deaktiver dynamisk flis** blant kommandoene som er tilgjengelige for appen. Hvis du løsner en appflis fra startmenyen, vises ikke flisoppdateringene. Hvis du avinstallerer en app, kan apputgiveren likevel sende oppdateringer til Windows Push Notification-tjenesten, men de vises ikke på PCen din.

Hvis du vil fjerne gjeldende oppdateringer som vises på flisene på startmenyen, sveiper du fra høyre side av startskjermen eller peker i øvre høyre hjørne på startmenyen, trykker eller klikker **Innstillinger** og trykker eller klikker deretter **Fliser**. Trykk eller klikk **Fjern** -knappen under **Fjern personlige opplysninger fra flisene mine**. Flisoppdateringer som leveres etter at du fjerner gjeldende oppdateringer, vises fortsatt.

[Øverst på siden](#)

Bestill kopier

Hva denne funksjonen gjør

Du kan bruke Bestill kopier til å sende digitale bilder som er lagret på PCen eller en nettverksstasjon, til en bildeutskriftstjeneste på Internett. Avhengig av tjenesten kan du få bildene skrevet ut og

deretter levert i posten, eller du kan hente dem i en lokal butikk.

Informasjon som samles inn, behandles eller overføres

Hvis du foretar en bestilling i en bildeutskriftstjeneste på Internett, sendes de digitale bildene via Internett til tjenesten du har valgt. Filbanen til de digitale bildene du velger (som kan inkludere brukernavnet ditt), kan sendes til tjenesten for å tillate at tjenesten viser og laster opp bildene. Digitale bildefiler kan inneholde data om bildet som ble lagret i filen av kameraet, for eksempel datoen og klokkeslettet da bildet ble tatt, eller stedet der bildet ble tatt, hvis kameraet har GPS-funksjoner. Filene kan også inneholde personlige opplysninger (for eksempel bildetekster) som kan ha blitt knyttet til filen gjennom bruk av apper for digital bildebehandling og Windows Utforsker. Hvis du vil ha mer informasjon, kan du se delen om egenskaper nedenfor.

Når du har valgt en bildeutskriftstjeneste på Internett fra Bestill kopier, kommer du til tjenestens nettsted i Bestill kopier-vinduet. Informasjonen du skriver inn på nettstedet for bildeutskriftstjenesten, overføres til tjenesten.

Bruk av informasjon

Informasjonen som lagres i digitale bildefiler av kameraet, kan kanskje bli brukt av bildeutskriftstjenesten på Internett under utskriften, for eksempel for å justere fargene eller skarpheten på bildet før det skrives ut. Informasjon som lagres av apper for digital bildebehandling, brukes kanskje av bildeutskriftstjenesten på Internett som bildetekster på for- eller baksiden av kopien. Bildeutskriftstjenestens bruk av denne informasjonen og annen informasjon du oppgir i tjenesten, for eksempel informasjon du skriver inn på nettstedene deres, er underlagt personvernpraksisen deres.

Valg og kontroll

Du kan bruke Bestill kopier til å velge hvilke bilder du vil sende, og hvilken tjeneste du vil bruke til å skrive ut bilder. Enkelte apper for bildebehandling kan kanskje gjøre det enklere å fjerne lagrede personlige opplysninger før du sender bildene til utskrift. Du kan kanskje også redigere filegenskapene for å fjerne lagrede personlige

opplysninger.

[Øverst på siden](#)

Program Compatibility Assistant

Hva denne funksjonen gjør

Hvis det oppstår et inkompatibilitetsproblem med en app du forsøker å kjøre, kan du bruke Program Compatibility Assistant til å løse problemet.

Informasjon som samles inn, behandles eller overføres

Hvis det oppstår et kompatibilitetsproblem med en app du prøver å kjøre, genereres en rapport med informasjon som appnavn, appversjon, nødvendige kompatibilitetsinnstillinger og handlingene dine i appen så langt. Problemer med inkompatible apper rapporteres til Microsoft via Windows-feilrapportering eller Windows CEIP (Customer Experience Improvement Program).

Bruk av informasjon

Feilrapporter brukes til å gi deg tilbakemelding på problemer du rapporterer for apper. Svar inneholder koblinger (når tilgjengelig) til apputgiverens nettsted slik at du kan finne ut mer om mulige løsninger. Feilrapporter som genereres på grunn av appfeil, brukes til å prøve å finne ut hvilke innstillinger som skal justeres når det oppstår kompatibilitetsproblemer for appene du kjører i denne versjonen av Windows. Informasjon som rapporteres gjennom programmet for forbedret kundeopplevelse, brukes til å identifisere problemer med appkompatibilitet.

Microsoft bruker ikke informasjon som er samlet inn ved hjelp av denne funksjonen, til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Når det gjelder problemer som er rapportert via Windows-feilrapportering, opprettes det en feilrapport bare når du velger alternativet for å sjekke Internett for en løsning. Hvis du ikke tidligere har samtykket i å rapportere problemer automatisk, slik at du kan se etter løsninger, får du spørsmål om du vil sende

feilrapporten. Hvis du vil ha mer informasjon, kan du se delen Windows-feilrapportering.

Noen problemer rapporteres automatisk via Windows CEIP hvis du har valgt å slå funksjonen på. Hvis du vil ha mer informasjon, kan du se delen Windows CEIP (Customer Experience Improvement Program).

[Øverst på siden](#)

Egenskaper

Hva denne funksjonen gjør

Egenskaper er filinformasjon du kan bruke til å søke etter og organisere filer raskt. Enkelte egenskaper er iboende i filen (for eksempel filstørrelsen), mens andre kan gjelde for en bestemt app eller enhet (for eksempel innstillingene i kameraet da du tok et bilde, eller posisjonsdataene som ble registrert for bildet av kameraet).

Informasjon som samles inn, behandles eller overføres

Typen informasjon som lagres, er avhengig av filtypen og appene som bruker den. Eksempler på egenskaper er filnavn, endringsdato, filstørrelse, forfatter, nøkkelord og kommentarer. Egenskaper lagres i filen, og de flyttes med filen hvis den flyttes eller kopieres til en annen plassering, for eksempel en delt filressurs, eller sendes som et e-postvedlegg.

Bruk av informasjon

Egenskaper gjør det enklere å søke etter og organisere filer raskere. De kan også brukes av apper til å utføre appspesifikke oppgaver. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Du kan redigere eller fjerne enkelte egenskaper for en fil ved å merke filen i Windows Utforsker og klikke Egenskaper. Enkelte iboende egenskaper, for eksempel endringsdato, filstørrelse, filnavn og noen appspesifikke egenskaper kan ikke fjernes på denne måten. Når det gjelder appspesifikke egenskaper, kan du redigere eller fjerne dem bare hvis appen du bruker til å generere filen, støtter

disse funksjonene.

[Øverst på siden](#)

Nærhet

Nærhetstjeneste for nærfelt

Hva denne funksjonen gjør

Hvis PCen har maskinvare for nærfeltkommunikasjon (NFC), kan du holde den inntil en annen enhet med NFC-maskinvare for å dele koblinger, filer og annen informasjon. Det finnes to typer nærhetstilkoblinger: Klappet og klart og Klappe sammen. Med Klappet og klart kan du opprette en kort- eller langvarig tilkobling mellom enheter over Wi-Fi, Wi-Fi Direct eller Bluetooth. Med Klappe sammen er tilkoblingen bare aktiv så lenge enhetene holdes inntil hverandre.

Informasjon som samles inn, behandles eller overføres

Når du holder nærhetsaktiverte enheter inntil hverandre, utveksler de informasjon for å opprette en tilkobling til hverandre. Disse dataene kan omfatte Bluetooth- og Wi-Fi-nettverksadresser og navnet på PCen din, avhengig av hvordan enhetene er konfigurert.

Etter at en tilkobling er opprettet, kan annen informasjon utveksles mellom enhetene, avhengig av den bestemte nærhetsfunksjonen eller appen du bruker. Windows kan sende filer, koblinger, og annen informasjon mellom enhetene ved hjelp av en nærhetstilkobling. Apper som bruker nærhet, kan sende og motta all informasjon de har tilgang til. Denne informasjonen kan sendes via nettverket eller Internett-tilkoblingen eller direkte gjennom en trådløs tilkobling fra enhet til enhet.

Bruk av informasjon

Nettverks- og PC-informasjon som utveksles via en nærhetstilkobling brukes til å opprette en nettverkstilkobling og å identifisere enhetene som kobler til hverandre. Data som opprinnelig kommer fra en app og overføres via en nærhetstilkobling, kan brukes av denne appen på en hvilken som helst måte. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Nærhetstjenesten for nærfelt er som standard aktivert. En administrator kan deaktivere den ved å bruke alternativer i Enheter og skrivere i Kontrollpanel.

Trykk og send

Hva denne funksjonen gjør

Trykk og send i Windows gjør det enkelt å dele valgt informasjon med en venn som står ved siden av deg, eller med en annen av enhetene dine, for eksempel en mobiltelefon. Når du for eksempel er i en nettleser, kan du starte Trykk og send i Enheter-ruten. Den neste enheten du berører, mottar en kobling til nettsiden som vises. Dette fungerer også med alle apper som støtter deling av informasjon, for eksempel bilder, tekst eller filer.

Informasjon som samles inn, behandles eller overføres

Trykk og Send bruker informasjonen du deler, og informasjonen som er beskrevet i delen Nærhetstjeneste for nærfelt ovenfor.

Bruk av informasjon

Denne informasjonen brukes bare til å opprette tilkoblingen mellom de to enhetene. Den delte informasjonen lagres ikke av Trykk og send. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Hvis Nærhetstjeneste for nærfelt er aktivert, er også Trykk og Send aktivert. Hvis du vil ha mer informasjon, kan du se delen Nærhetstjeneste for nærfelt.

[Øverst på siden](#)

Eksterne tilkoblinger

Hva denne funksjonen gjør

Med eksterne tilkoblinger kan du koble til private nettverk ved å bruke en VPN-tilkobling (virtuelt privat nettverk) og tjenesten Ekstern pålogging (RAS). RAS er en komponent som kobler en klient-PC (vanligvis PCen din) til en vert-PC (også kalt en RAS-

server) ved hjelp av protokoller som er bransjestandard. VPN-teknologier gjør at brukere kan koble til et privat nettverk, for eksempel et firmanettverk, via Internett.

En komponent for ekstern tilkobling, ekstern pålogging, gjør at du kan få tilgang til Internett ved å bruke et modem eller bredbåndsteknologi, for eksempel et kabelmodem eller en DSL (Digital Subscriber Line). Ekstern pålogging omfatter oppringingskomponenter, for eksempel RAS-klient, Tilkoblingsbehandling og RAS-telefon, samt oppringingsprogrammer med kommandolinje, for eksempel rasdial.

Informasjon som samles inn, behandles eller overføres

Oppringingskomponentene samler inn informasjon fra PCen din, for eksempel brukernavn, passord og domenenavn. Denne informasjonen sendes til systemet du prøver å koble til. For å bidra til å ivareta personvernet og beskytte PCen krypteres og lagres sikkerhetsrelatert informasjon, for eksempel brukernavn og passord, på PCen.

Bruk av informasjon

Oppringingsinformasjon brukes av PCen til å koble til Internett. En RAS-server beholder kanskje brukernavnet og IP-adressen for kontobehandlings- og samsvarsformål, men det sendes ingen informasjon til Microsoft.

Valg og kontroll

Når det gjelder oppringingsprogram uten kommandolinje, kan du lagre passordet ved å velge **Lagre dette brukernavnet og passordet**. Du kan når som helst oppheve dette alternativet hvis du vil slette tidligere lagrede passord fra oppringingsprogrammet. Siden dette alternativet er deaktivert som standard, må du kanskje oppgi passordet for å koble til Internett eller et nettverk. Når det gjelder oppringingsprogrammer med kommandolinje, for eksempel rasdial, finnes det ikke noe alternativ for lagring av passord.

[Øverst på siden](#)

Tilkoblinger til RemoteApp og skrivebord

Hva denne funksjonen gjør

Tilkoblinger til RemoteApp og skrivebord gir deg tilgang til apper og skrivebord på eksterne PCer som har blitt gjort tilgjengelig elektronisk for ekstern tilgang.

Informasjon som samles inn, behandles eller overføres

Når du aktiverer en tilkobling, lastes konfigurasjonsfiler ned til PCen fra den eksterne nettadressen du angir. Disse konfigurasjonsfilene kobler apper og skrivebord på eksterne PCer, slik at du kan kjøre dem fra PCen din. PCen ser etter og laster ned oppdateringer for disse konfigurasjonsfilene regelmessig og automatisk. Disse appene kjører på eksterne PCer, og informasjon du angir i appene, overføres over nettverket til den eksterne PCen du kobler til.

Bruk av informasjon

Oppdateringer til konfigurasjonsfiler inneholder kanskje innstillingsendringer, inkludert formidling av tilgang til nye apper. Nye apper kjører imidlertid bare hvis du velger å kjøre dem. Denne funksjonen sender også informasjon til de eksterne PCene som den eksterne appen kjører på. Bruk av disse dataene av de eksterne appene er underlagt personvernpolicyene til apputgiverne og administratorene av de eksterne PCene. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Du kan velge om du vil bruke Tilkoblinger til RemoteApp og skrivebord. Du kan legge til og fjerne tilkoblinger til RemoteApp og skrivebord ved å gå til Tilkoblinger til RemoteApp og skrivebord i Kontrollpanel. Du kan legge til en ny tilkobling ved å klikke

Konfigurer ny tilkobling med Tilkoblinger til RemoteApp og skrivebord og skrive inn en tilkoblingsnettadresse i dialogboksen.

Du kan også bruke e-postadressen til å hente tilkoblingsnettadressen. Du kan fjerne en tilkobling og tilkoblingsfilene for den ved å klikke **Fjern** i dialogboksen for tilkoblingsbeskrivelse. Hvis du kobler fra en tilkobling uten å lukke alle åpne apper, forblir disse appene åpne på den eksterne PCen. Tilkoblinger til RemoteApp og skrivebord vises ikke i listen Legg til eller fjern programmer i Kontrollpanel.

Tilkobling til eksternt skrivebord

Hva denne funksjonen gjør

Tilkobling til eksternt skrivebord formidler en metode for å opprette en ekstern tilkobling til en verts-PC som kjører Eksterne skrivebordstjenester.

Informasjon som samles inn, behandles eller overføres

Innstillinger for Tilkobling til eksternt skrivebord lagres i et applokalt lager eller i en RDP-fil (Remote Desktop Protocol) på PCen. Disse innstillingene omfatter navnet på domenet og konfigurasjonsinnstillinger for tilkobling, for eksempel navn på ekstern PC, brukernavn, visningsinformasjon, informasjon om lokal enhet, lydinformasjon, utklippstavle, tilkoblingsinnstillinger, navn på eksterne apper og ikon eller miniatyrbilde for økt.

Legitimasjon for disse tilkoblingene, legitimasjon for Eksterne skrivebordstjenester, og en liste over navn på klarerte gatewayservere for Eksternt skrivebord er lagret lokalt på PCen din. Denne listen lagres permanent med mindre den slettes av en administrator. Det sendes ingen informasjon til Microsoft.

Bruk av informasjon

Informasjon som samles inn av Tilkobling til eksternt skrivebord, lar deg koble til verts-PCer som kjører Tilkobling til eksternt skrivebord, med dine foretrukne innstillinger. Brukernavn, passord og domeneinformasjon samles inn for at du skal kunne lagre tilkoblingsinnstillingene, og slik at du kan dobbeltklikke en RDP-fil eller klikke en favoritt for å opprette en tilkobling uten å måtte angi denne informasjonen på nytt.

Valg og kontroll

Du kan velge om du vil bruke Tilkobling til eksternt skrivebord. Hvis du bruker denne funksjonen, inneholder RDP-filene og Tilkobling til eksternt skrivebord-favorittene informasjon som kreves for å koble til en ekstern PC, inkludert alternativene og innstillingene som ble konfigurert da tilkoblingen ble lagret automatisk. Du kan tilpasse

RDP-filer og favoritter, inkludert filer for tilkobling til samme PC med andre innstillinger. Hvis du vil endre lagret legitimasjon, åpner du Legitimasjonsbehandling i Brukerkontoer i Kontrollpanel.

[Øverst på siden](#)

Logg på med en Microsoft-konto

Hva denne funksjonen gjør

En Microsoft-konto (tidligere kalt Windows Live-ID) er en løsning med én e-postadresse og ett passord som du kan bruke når du registrerer informasjon for å logge på apper, nettsteder og tjenester fra Microsoft, og når du velger Microsoft-partnere. Du kan registrere deg for en Microsoft-konto i Windows eller på Microsoft-nettsteder som krever at du logger på med en Microsoft-konto.

Du kan velge å logge på Windows med en Microsoft-konto, eller velge å koble den lokale kontoen eller domenekontoen til en Microsoft-konto. Hvis du gjør dette, kan Windows bidra til at PCen ser og føles lik ut ved automatisk å synkronisere innstillinger og informasjon i Windows- og Microsoft-apper. Hvis du går til påloggingssiden for de nettstedene, blir du også automatisk logget på nettstedene som bruker Microsoft-kontoer til å logge på.

Informasjon som samles inn, behandles eller overføres

Når du oppgir en e-postadresse som skal brukes som en Microsoft-konto under mens du konfigurerer PCen, eller under Brukere i PC-innstillinger, sender Windows e-postadressen til Microsoft for å fastslå om det allerede finnes en Microsoft-konto som er knyttet til den e-postadressen. Hvis du allerede bruker den e-postadressen som en Microsoft-konto, kan du bruke e-postadressen og passordet for Microsoft-kontoen til å logge på Windows. Hvis du ikke allerede har nok sikkerhetsinformasjon for Microsoft-kontoen, ber vi deg kanskje først om ekstra sikkerhetsinformasjon, for eksempel et mobilnummer som vi kan bruke til å bekrefte at kontoen er din hvis du har problemer med å logge på kontoen. Hvis du ikke har en Microsoft-konto, kan du opprette en ved hjelp av en e-postadresse.

Hver gang du logger på Windows med en Microsoft-konto mens PCen er koblet til Internett, bekrefter Windows e-postadressen og

passordet med Microsofts servere. Når du er logget på Windows med Microsoft-kontoen din eller med en domenekonto som er koblet til Microsoft-kontoen din:

- Bestemte Windows-innstillinger blir synkronisert mellom PCen som du logger på med en Microsoft-konto. Hvis du vil ha mer informasjon om hvilke innstillinger som synkroniseres og hvordan du kontrollerer dem, kan du se delen Synkronisere innstillinger.
- Microsoft-apper som bruker en Microsoft-konto til godkjenning (for eksempel E-post, Kalender, Bilder, Personer, Meldinger, OneDrive, Microsoft Office og andre apper), kan automatisk begynne å laste ned informasjonen (e-post-appen laster for eksempel automatisk ned meldingene som sendes til Outlook.com- eller Hotmail.com-adressen hvis du har en).
- Nettlesere kan automatisk logge deg på nettsteder som du logger på med Microsoft-kontoen (hvis du for eksempel besøker OneDrive.com, kan du bli logget på automatisk uten at du må angi passordet for Microsoft-kontoen på nytt).

Windows ber deg om tillatelse før tredjepartsapper tillates å bruke profilinformasjon eller andre personlige opplysninger som er knyttet til Microsoft-kontoen din. Hvis du logger på Windows med en domenekonto som er koblet til en Microsoft-konto, blir innstillingene og informasjonen du velger, synkronisert med domenekontoen, og du blir automatisk logget på apper og nettsteder som beskrevet ovenfor. Domeneadministratorer kan få tilgang til all informasjon på PCen din, og derfor kan de også få tilgang til alle innstillinger og all informasjon du har valgt å synkronisere med andre PCer ved hjelp av Microsoft-kontoen. Dette kan inkludere innstillinger som navn, kontobilde og leserlogg. Hvis du vil ha mer informasjon om hvilke innstillinger som synkroniseres og hvordan du kontrollerer dem, kan du se delen Synkronisere innstillinger.

Bruk av informasjon

Når du oppretter en ny Microsoft-konto i Windows, bruker vi informasjonen du oppgir, til å opprette og beskytte kontoen. Sikkerhetsinformasjonen du oppgir (for eksempel telefonnummer

eller alternativ e-postadresse), brukes for eksempel bare hvis du ikke kan logge på kontoen. Når du er logget på Windows med en Microsoft-konto, bruker Windows informasjon om Microsoft-kontoen din til å logge deg på apper og nettsteder automatisk. Hvis du vil finne ut mer om hvordan personvernet blir påvirket av å bruke en Microsoft-konto, kan du lese [personvernerklæringen](#) som vises når du velger Registrer deg for en ny e-postadresse. Hvis du vil ha informasjon om hvordan enkeltstående Microsoft-apper bruker informasjon som er knyttet til Microsoft-kontoen, kan du se appenes personvernerklæringer. Du finner personvernerklæringen for en Microsoft-app i appens Innstillinger-perle eller i dialogboksen Om.

Valg og kontroll

Når du logger på Windows med en Microsoft-konto, synkroniseres noen innstillinger automatisk. Hvis du vil finne ut hvordan du endrer hvilke Windows-innstillinger som synkroniseres, eller hvordan du stopper synkronisering, kan du se delen Synkronisere innstillinger. Hvis du vil finne ut mer om dataene som samles inn av Microsoft-apper som bruker en Microsoft-konto til godkjenning, kan du lese personvernerklæringen for de ulike appene. Du finner personvernerklæringen for Windows Live-appene (E-post, Kalender, Bilder, Personer, Meldinger, OneDrive) på go.microsoft.com/fwlink/?LinkId=257483, og for Microsoft Office på go.microsoft.com/fwlink/?LinkId=257484. Du kan også finne personvernerklæringen for en app i appens Innstillinger-perle eller Om-dialogboks.

Du trenger ikke logge på Windows med en Microsoft-konto. Når du legger til en bruker på PCen mens du konfigurerer den, eller under **Brukere** i PC-innstillinger, kan du velge å bruke en lokal konto eller en Microsoft-konto. Du kan bytte til en lokal konto eller Microsoft-konto når som helst under **Brukere** i PC-innstillinger. Hvis du logger på Windows med en domenekonto, kan du koble til eller fra Microsoft-kontoen når som helst under **Brukere** i PC-innstillinger.

Når du bruker InPrivate-visning i Internet Explorer, blir du ikke automatisk logget på nettsteder som bruker Microsoft-kontoer.

[Øverst på siden](#)

Hva denne funksjonen gjør

Når du logger på Windows med en Microsoft-konto, synkroniserer Windows noen av innstillingene dine og informasjonen din med Microsoft-servere for å gjøre det enklere å ha tilpassede brukeropplevelser på tvers av flere PCer. Etter at du har logget på en PC med en Microsoft-konto, og når du logger på en annen PC med samme Microsoft-konto for første gang, laster Windows ned og bruker innstillingene og informasjonen du velger å synkronisere fra de andre PCene dine. Innstillinger du velger å synkronisere, oppdateres automatisk på Microsoft-servere og andre PCer når du bruker dem.

Informasjon som samles inn, behandles eller overføres

Hvis du velger å logge på Windows med en Microsoft-konto, synkroniserer Windows bestemte innstillinger med Microsoft-servere. Disse innstillingene omfatter følgende:

- Språkinnstillinger
- Innstillinger for hjelpemiddel
- Tilpassingsinnstillinger, for eksempel kontobildet, låseskjerm bildet, bakgrunnen og museinnstillingene
- Innstillinger for Windows Store-apper
- Stavekontroll og IME-ordbøker
- Nettleserlogg og -favoritter
- Lagrede passord for apper, nettsteder og nettverk

Alle synkroniserte innstillinger sendes kryptert via SSL for å beskytte personvernet ditt. Noen av disse innstillingene synkroniseres ikke på PCen før du legger til PCen på Microsoft-kontoen som en klarert PC.

Hvis du logger på Windows med en domenekonto som er koblet til en Microsoft-konto, blir innstillinger og informasjon du har valgt, synkronisert med domenekontoen. Passord som du lagrer mens du er logget på Windows med en domenekonto som er koblet til en Microsoft-konto, blir ikke synkronisert. Domeneadministratorer kan få tilgang til all informasjon på PCen din, og derfor kan de også få

tilgang til alle innstillinger og all informasjon, inkludert leserloggen, du har valgt å synkronisere med andre PCer ved hjelp av Microsoft-kontoen.

Bruk av informasjon

Windows 8 bruker disse innstillingene og den informasjonen til å formidle synkroniseringstjenesten. Microsoft bruker ikke dine synkroniserte innstillinger og din synkroniserte informasjon til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Når du logger på Windows med en Microsoft-konto, er synkronisering av innstillinger aktivert. Du kan velge å synkronisere innstillinger, og du kan kontrollere hva som er synkronisert ved å gå til **Synkronisere innstillinger** i PC-innstillinger. Hvis du logger på Windows med en domenekonto og du velger å koble den kontoen til en Microsoft-konto, spør Windows deg om hvilke innstillinger du vil synkronisere før du kobler til Microsoft-kontoen.

[Øverst på siden](#)

Teredo-teknologi

Hva denne funksjonen gjør

Teredo-teknologi (Teredo) tillater at PCer og nettverk kommuniserer via flere nettverksprotokoller.

Informasjon som samles inn, behandles eller overføres

Hver gang du starter PCen, prøver Teredo å finne en offentlig IPv6-tjeneste (Internet Protocol versjon 6) på Internett. Dette skjer automatisk når PCen kobler til et offentlig eller privat nettverk, men det skjer ikke på administrerte nettverk, for eksempel organisasjonsdomener. Hvis du bruker en app som krever Teredo for å bruke IPv6-tilkobling, eller hvis du konfigurerer brannmuren slik at IPv6-tilkobling alltid aktiveres, kontakter Teredo regelmessig Microsoft Teredo-tjenesten via Internett. Den eneste informasjonen som sendes til Microsoft, er standard PC-informasjon og navnet på den forespurte tjenesten (for eksempel teredo.ipv6.microsoft.com).

Bruk av informasjon

Informasjonen som sendes fra PCen av Teredo, brukes til å avgjøre om PCen er koblet til Internett, og om den kan finne en offentlig IPv6-tjeneste. Når tjenesten er funnet, sendes det informasjon for å opprettholde en tilkobling til IPv6-tjenesten.

Valg og kontroll

Du kan bruke kommandolinjeverktøyet netsh til å endre spørringen som tjenesten sender via Internett, hvis du vil bruke andre servere i stedet for Microsoft-servere, eller du kan deaktivere den. Hvis du vil ha detaljerte instruksjoner, kan du se delen Internet Protocol Version 6, Teredo, and Related Technologies i denne tekniske hvitboken.

[Øverst på siden](#)

TPM-tjenester (Trusted Platform Module)

Hva denne funksjonen gjør

TPM (Trusted Platform Module) er sikkerhetsmaskinvare som er bygget inn i noen PCer, som, hvis den finnes og er klargjort, gjør at PCen kan bruke avanserte sikkerhetsfunksjoner. Windows-funksjoner som bruker TPMen, omfatter BitLocker-stasjonskryptering, Virtuelt smartkort, Sikker oppstart, Windows Defender og TPM-basert sertifikatlager.

Informasjon som samles inn, behandles eller overføres

Windows overtar som standard TPMen og lagrer all autorisasjonsinformasjon for TPM-eier, slik at den bare er tilgjengelig for Windows-administratorer. Begrensede autorisasjonsverdier opprettes for å utføre typiske administrative handlinger og standard brukerhandling, og administreres av Windows.

Du kan bruke TPM-konsollen til å klargjøre TPMen interaktivt og lagre autorisasjonsverdien for TPM-eier på et eksternt medium, for eksempel en USB-flash-enhet etter at TPMen er klargjort. En lagret fil inneholder autorisasjonsinformasjonen for TPM-eier for TPMen. Filen inneholder også PC-navnet, operativsystemversjonen, opprettingsbrukeren og opprettingsdatoen for å gjøre det enklere å gjenkjenne filen.

I et domenenemiljø kan passordet for den fullstendige TPM-eieren konfigureres av domeneadministratoren til å lagre i Active Directory under et TPM-objekt når TPM klargjøres.

Hver TPM har en unik kryptografisk bekreftelsesnøkkel som den bruker til å angi sin ekthet. Bekreftelsesnøkkelen kan opprettes og lagres i TPMen av PC-produsenten. Når det gjelder eldre PCer, må kanskje Windows utløse generering av bekreftelsesnøkkelen i TPMen. Den private dele av bekreftelsesnøkkelen vises aldri utenfor TPMen, og når den er opprettet, kan den vanligvis ikke tilbakestilles. Et bekreftelsesnøkkelsertifikat lagres i TPM for de fleste Windows 8-datamaskiner. Bekreftelsesnøkkelsertifikatet angir at bekreftelsesnøkkelen finnes i en maskinvare-TPM. Sertifikatet kan brukes av eksterne verifikatorer til å bekrefte at TPMen er i samsvar med TPM-spesifikasjonene. Bekreftelsesnøkkelsertifikatet signeres vanligvis av TPM-produsenten eller plattformprodusenten.

Bruk av informasjon

Når TPMen er initialisert, kan apper bruke den til å opprette og bidra til å sikre ytterligere unike krypteringsnøkler. BitLocker-stasjonskryptering bruker for eksempel TPMen til å bidra til å beskytte nøkkelen som krypterer stasjonen.

Hvis du velger å lagre passordet for TPM-eier i en fil, gjør tilleggsinformasjonen om PCen og brukeren som lagres i denne filen, det enklere å identifisere den tilhørende PCen og TPMen. TPM-bekreftelsesnøkkelen brukes av Windows under TPM-initialisering til å kryptere autorisasjonsverdien for TPM-eier før den sendes til TPMen. Windows sender ingen krypteringsnøkler fra PCen din. Windows har et grensesnitt for tredjepartsapper, for eksempel programvare for beskyttelse mot skadelig programvare, slik at de kan bruke bekreftelsesnøkkelen i enkelte TPM-scenarier, for eksempel Measured Boot with Attestation. Når det gjelder programvare for beskyttelse mot skadelig programvare, er bekreftelsesnøkkelen og bekreftelsesnøkkelsertifikatet nyttig for å bekrefte at oppstartsmålinger kommer fra en TPM fra en bestemt produsent. Det er som standard bare administratorer eller apper med administrative rettigheter som kan bruke TPM-bekreftelsesnøkkelen.

Valg og kontroll

Brukere eller administratorer kan velge å bruke TPM ved å aktivere en Windows-funksjon eller kjøre en app som bruker TPM.

Du kan velge om du vil tømme TPMen og tilbake stille den til fabrikkinnstillingene. Hvis du tømmer TPMen, fjernes eierinformasjon og, med unntak av bekreftelsesnøkkelen, alle TPM-baserte nøkler eller all kryptografisk informasjon som apper kan ha opprettet da TPMen var i bruk.

[Øverst på siden](#)

Oppdater rotsertifikater

Hva denne funksjonen gjør

Sertifikater brukes hovedsakelig til å kontrollere identiteten til en person eller enhet, godkjenne en tjeneste eller kryptere filer. Klarerte rotsertifiseringsinstanser er organisasjonene som utsteder sertifikater. Oppdater rotsertifikater kontakter Windows Update-tjenesten på nettet for å se om Microsoft har lagt til en sertifiseringsinstans i listen over klarerte instanser, men bare når en app mottar et sertifikat som er utstedt av en sertifiseringsinstans som ikke er direkte klarert (et sertifikat som ikke er lagret i en liste over klarerte sertifikater på PCen din). Hvis sertifiseringsinstansen er lagt til i Microsoft-listen over klarerte instanser, blir sertifikatet automatisk lagt til i listen over klarerte sertifikater på PCen din.

Informasjon som samles inn, behandles eller overføres

Oppdater rotsertifikater sender en forespørsel til Windows Update-tjenesten på nettet der den ber om den gjeldende listen over rotsertifiseringsinstanser i Microsofts rotsertifikatprogram. Hvis det uklarerte sertifikatet er i listen, henter Oppdater rotsertifikat dette sertifikatet fra Windows Update og plasserer det i lageret for klarerte sertifikater på PCen din. Informasjonen som overføres, omfatter navnene på og de kryptografiske hash-kodene for rotsertifikater.

Hvis du vil ha mer informasjon om Windows Update og personvernet ditt, kan du lese [personvernerklæringen for Oppdateringstjenester](#).

Bruk av informasjon

Informasjonen brukes av Microsoft til å oppdatere listen over klarerte sertifikater på PCen. Microsoft bruker ikke denne informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Oppdater rotsertifikater er som standard aktivert. Administratorer kan konfigurere Gruppepolicy for å deaktivere Oppdater rotsertifikater på en PC.

[Øverst på siden](#)

Oppdateringstjenester

Hva denne funksjonen gjør

Oppdateringstjenester for Windows inkluderer Windows Update og Microsoft Update:

- **Windows Update** er en tjeneste som sender deg programvareoppdateringer for Windows-programvare og annen programvare som støttes, for eksempel drivere fra enhetsprodusenter.
- **Microsoft Update** er en tjeneste som sender deg programvareoppdateringer for Windows-programvare, og i tillegg annen Microsoft-programvare, for eksempel Microsoft Office.

Informasjon som samles inn, behandles eller overføres

Hvis du velger å få viktige programvareoppdateringer til PCen din, kan Windows Verktøy for fjerning av skadelig programvare (MSRT) være inkludert blant disse oppdateringene. MSRT sjekker om PCer er infisert av enkelte utbredte skadelige programmer ("skadelig programvare"), og fjerner alle infeksjoner den finner. Hvis programvaren kjører, fjerner den [skadelige programvare som står oppført](#) på nettstedet for Microsoft Kundestøtte. Under et søk etter skadelig programvare blir det sendt en rapport til Microsoft med spesifikk informasjon om oppdaget skadelig programvare, feil og annen informasjon om PCen din. Hvis du vil ha mer informasjon, kan du lese personvernerklæringen for [Windows Verktøy for fjerning av](#)

[skadelig programvare](#) .

Hvis du vil vite hvilken annen informasjon som samles inn av Oppdateringstjenester, kan du se [personvernerklæringen for Oppdateringstjenester](#).

Bruk av informasjon

Denne MSRT-informasjonen brukes til å forbedre våre programmer for beskyttelse mot skadelig programvare og andre sikkerhetsprodukter og -tjenester. Ingen informasjon i MSRT-rapportene vil bli brukt til å identifisere eller kontakte deg.

Hvis du vil vite hvordan Oppdateringstjenester bruker annen informasjon, kan du se [personvernerklæringen for Oppdateringstjenester](#).

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du Oppdateringstjenester og angir at Windows Update skal installere oppdateringer automatisk. Hvis du velger å tilpasse innstillingene, kan du kontrollere Oppdateringstjenester i **Windows Update** under **Beskytt og oppdater PCen**. Etter at Windows er installert, kan du endre innstillinger for Oppdateringstjenester i Kontrollpanel. Hvis du vil ha mer informasjon, kan du se personvernerklæringen for Oppdateringstjenester.

Hvis du har valgt å se etter og installere viktige oppdateringer og motta MSRT som en del av disse oppdateringene for PCen, kan du deaktivere programvarens rapporteringsfunksjonalitet ved å følge [disse instruksjonene](#) på Microsoft Kundestøtte.

[Øverst på siden](#)

Windows CEIP (Customer Experience Improvement Program)

Hva denne funksjonen gjør

Windows CEIP (Customer Experience Improvement Programs) kan samle inn informasjon om hvordan du bruker appene dine, PCene dine, tilkoblede enheter og Windows. Den kan også samle inn informasjon om ytelses- og pålitelighetsproblemer som kan forekomme. Hvis du velger å delta i Windows CEIP, sender Windows

disse dataene til Microsoft, og laster også regelmessig ned en fil for å samle inn mer relevant informasjon om hvordan du bruker Windows og apper. CEIP-rapporter sendes til Microsoft for å hjelpe med å forbedre funksjonene våre kunder bruker oftest, og for å finne løsninger på vanlige problemer.

Informasjon som samles inn, behandles eller overføres

CEIP-rapporter kan inkludere følgende informasjon:

- Konfigurasjonsinformasjon. inkludert informasjon om hvor mange prosessorer som befinner seg på PCen din, antallet nettverkstilkoblinger som er i bruk, skjermopløsninger for visningsenheter, og hvilken versjon av Windows som kjører.
- Ytelses- og pålitelighetsinformasjon, inkludert informasjon om hvor raskt en app svarer når du klikker en knapp, hvor mange problemer du støter på med en app eller enhet, og hvor raskt informasjon sendes eller mottas via en nettverkstilkobling.
- Informasjon om appbruk, inkludert informasjon om funksjonene du bruker oftest, for eksempel hvor ofte du åpner apper, hvor ofte du bruker Hjelp og støtte for Windows, hvilke tjenester du bruker til å logge på apper, og hvor mange mapper du vanligvis oppretter på skrivebordet.

CEIP-rapporter inneholder også informasjon om hendelser (hendelsesloggdata) på PCen fra opptil sju dager før du valgte å delta i CEIP. De fleste brukere velger å delta i CEIP innen noen dager etter å ha konfigurert Windows, og derfor bruker Microsoft denne informasjonen til å analysere og forbedre opplevelsen når du konfigurerer Windows.

Denne informasjonen sendes til Microsoft når du er tilkoblet Internett. CEIP rapporterer ikke kontaktinformasjon, for eksempel navn, adresse eller telefonnummer, med hensikt. Noen rapporter kan likevel utilsiktet inneholde personlige identifikatorer, for eksempel serienummer på en enhet som er koblet til PCen din. Microsoft filtrerer informasjonen i CEIP-rapporter for å prøve å fjerne eventuelle personlige identifikatorer de kan inneholde.

CEIP genererer et tilfeldig nummer kalt GUID (globalt unik

identifikator) som sendes til Microsoft sammen med hver CEIP-rapport. GUIDen lar oss fastslå hvilke data som sendes fra en bestemt datamaskin over tid. De forhåndsinstallerte Microsoft-appene som er lisensiert med Windows, kan opprette sine egne unike IDer for bruk med CEIP, og disse kan være basert på informasjon fra Microsoft-kontoen din.

CEIP laster også regelmessig ned en fil for å samle inn mer relevant informasjon om måten du bruker Windows og apper på. Denne filen hjelper Windows med å samle inn tilleggsinformasjon for å bidra til at Microsoft oppretter løsninger for vanlige problemer, samt forstår bruksmønstre for Windows og apper på en bedre måte.

Bruk av informasjon

Microsoft bruker CEIP-informasjon til å forbedre våre produkter og tjenester, og i tillegg tredjepartsprogramvare og -maskinvare som er utformet for bruk med disse produktene og tjenestene. Vi deler kanskje også CEIP-informasjon med Microsoft-partnere slik at de kan forbedre sine produkter og tjenester, men den delte informasjonen er i komprimert utgave og kan ikke brukes til å identifisere, kontakte eller sende reklame til deg.

Vi bruker GUID til å fastsette hvor utbredte tilbakemeldingene vi mottar, er, og hvordan vi skal prioritere dem. GUIDen lar for eksempel Microsoft skille mellom én kunde som opplever et problem hundre ganger, og hundre kunder som opplever det samme problemet én gang. Microsoft bruker ikke informasjonen som er samlet inn av CEIP, til å identifisere eller kontakte deg.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du Windows CEIP: Windows og Microsoft-appene som er lisensiert med Windows, kan sende CEIP-rapporter for alle brukere på PCen. Hvis du velger å tilpasse innstillinger, kan du kontrollere CEIP ved å velge **Bli med i programmet for forbedret kundeopplevelse og hjelp til med å forbedre Microsofts programvare og tjenester** under **Send Microsoft-informasjon for å bidra til å gjøre Windows og apper bedre**. Etter at administratorer har konfigurert Windows, kan de endre denne innstillingen under Handlingscenter i Kontrollpanel.

Hvis du vil ha mer informasjon, kan du se [vanlige spørsmål om Program for forbedret kundeopplevelse](#) på nettet.

[Øverst på siden](#)

Windows Defender

Windows Defender søker etter skadelig programvare og annen potensielt uønsket programvare på PCen. Programmet inkluderer funksjonene Microsoft Active Protection Service og History.

Microsoft Active Protection Service

Hva denne funksjonen gjør

Fellesskapet for beskyttelse mot skadelig programvare for Microsoft Active Protection Service (MAPS) er et frivillig og verdensomspennende fellesskap, inkludert Windows Defender-brukere. Ved hjelp av MAPS kan brukere sende informasjon om skadelig programvare og annen potensielt uønsket programvare til Microsoft i en rapport. MAPS kan beskytte PCen ved automatisk å laste ned nye signaturer for nylig oppdaget skadelig programvare.

Informasjon som samles inn, behandles eller overføres

MAPS-rapporter inkluderer informasjon om potensielle filer med skadelig programvare, for eksempel filnavn, kryptografiske hash-koder, programvareutgivere, størrelser og datostempler. I tillegg kan MAPS samle inn fullstendige nettadresser for å angi filenes opprinnelse. Disse nettadressene kan av og til inneholde personlige opplysninger, for eksempel søketermer og data som er registrert i skjemaer. Rapporter inneholder kanskje også handlingene du utførte da Windows Defender varslet deg om at potensielt uønsket programvare ble oppdaget. MAPS inkluderer denne informasjonen for å hjelpe Microsoft med å måle hvor effektivt Windows Defender kan oppdage og fjerne skadelig programvare og potensielt uønsket programvare, og å forsøke å identifisere nye tilfeller av skadelig programvare.

Rapporter sendes automatisk til Microsoft når:

- Windows Defender oppdager programvare som ikke har blitt analysert for risikoer.

- Windows Defender oppdager endringer på PCen din av programvare som ikke har blitt analysert for risikoer.
- Windows Defender utfører tiltak i forhold til skadelig programvare ved oppdaging (som en del av den automatiske utbedringen).
- Windows Defender fullfører et planlagt søk og utfører tiltak automatisk i forhold til programvare som oppdages basert på dine innstillinger.

Du kan bli med i MAPS med et grunnleggende eller et avansert medlemskap. Hvis du vil aktivere MAPS mens du konfigurerer Windows, registrerer du deg med et grunnleggende medlemskap. Grunnleggende medlemskapsrapporter inneholder informasjonen som er beskrevet i denne delen. Avanserte medlemskapsrapporter er mer omfattende, og kan av og til inneholde personlige opplysninger fra, for eksempel filbaner og delvise minnedumper. Disse rapportene, sammen med rapporter fra andre Windows Defender-brukere som deltar i MAPS, hjelper våre forskere å oppdage nye trusler raskere. Definisjoner på skadelig programvare blir deretter opprettet, og deretter blir disse oppdaterte definisjonene gjort tilgjengelig for alle brukere via Windows Update.

Hvis du registrerer deg for MAPS med et grunnleggende eller avansert medlemskap:

- Ber kanskje Microsoft om en eksempelrapport. Denne rapporten inneholder bestemte filer fra PCen din som Microsoft mistenker for å kunne være potensielt uønsket programvare. Eksempelrapporten brukes til videre analyse. Hver gang blir du spurt om du vil sende eksempelrapporten til Microsoft.
- Hvis Windows Update ikke har kunnet hente oppdaterte signaturer for Windows Defender en stund, forsøker Windows Defender å bruke MAPS til å laste ned signaturer fra en alternativ plassering.

All informasjon som sendes til MAPS, sendes kryptert via SSL for å beskytte personvernet ditt.

Bruk av informasjon

Rapporter som sendes til MAPS, brukes til å forbedre Microsoft-programvaren og -tjenestene. Rapportene brukes kanskje også til statistikk, testing eller analyse samt til generering av definisjoner. MAPS samler ikke inn personlige opplysninger med hensikt. I den grad MAPS tilfeldigvis samler inn personlige opplysninger, bruker ikke Microsoft den informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du MAPS. Hvis du velger å tilpasse innstillinger, kan du kontrollere MAPS ved å velge **Hjelp Microsoft med å reagere mot ondsinnede apper og skadelig programvare ved å bli med i Microsoft Active Protection Service** under **Send Microsoft-informasjon for å bidra til å gjøre Windows og apper bedre**. Etter at du har konfigurert Windows, kan du endre MAPS-medlemskapet eller -innstillingene, inkludert deaktivering av MAPS. Dette gjør du på Tools-menyen i Windows Defender.

Loggfunksjon

Hva denne funksjonen gjør

Funksjonen History inneholder en liste over alle apper på PCen som Windows Defender oppdager, og i tillegg tiltakene som ble utført da appene ble oppdaget.

I tillegg kan du vise en liste over apper som Windows Defender ikke overvåker, mens de kjører på PCen (disse kalles tillatte elementer). Du kan også vise apper som Windows Defender forhindrer fra å kjøre, til du velger å fjerne dem eller tillate at de kjører (disse kalles elementer i karantene).

Informasjon som samles inn, behandles eller overføres

Listen over programvare som Windows Defender gjenkjenner, tiltakene som du og andre brukere iverksetter, og tiltakene som Windows Defender iverksetter automatisk, lagres på PCen. Alle brukere kan vise loggen i Windows Defender for å vise skadelig programvare og annen potensielt uønsket programvare som har prøvd å installere seg eller kjøre på PCen, eller som en annen bruker har tillatt å kjøre. Hvis du for eksempel blir klar over en ny trussel

om skadelig programvare, kan du sjekke loggen for å se om Windows Defender har hindret at den har infisert PCen din. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Logglister kan slettes av en administrator.

[Øverst på siden](#)

Windows-feilrapportering

Hva denne funksjonen gjør

Windows-feilrapportering hjelper Microsoft og Microsoft-partnere med å analysere problemer i programvaren du bruker, samt å formidle løsninger. Ikke alle problemer kan løses, men når løsningene blir tilgjengelige, tilbys de som fremgangsmåter for å løse et problem du har rapportert eller som oppdateringer som kan installeres. For å unngå problemer og gjøre programvaren mer pålitelig blir enkelte løsninger også inkludert i oppdateringspakker og fremtidige versjoner av programvaren.

Informasjon som samles inn, behandles eller overføres

Mange programvareprodukter er utformet til å fungere med Windows-feilrapportering. Hvis et problem oppstår i ett av disse produktene, blir du kanskje spurt om du vil rapportere det.

Windows-feilrapportering samler inn informasjon som er nyttig for analyse og løsning av et problem som har oppstått, for eksempel hvor i programvaren eller maskinvaren problemet oppstod, problemets type eller alvorgrad, filer som beskriver problemet, grunnleggende informasjon om programvare og maskinvare, eller mulige problemer med programvareytelse og -kompatibilitet. Hvis du bruker Windows til å drifte virtuelle maskiner, kan det hende feilrapporter som sendes til Microsoft, inneholder informasjon om virtuelle maskiner.

Windows-feilrapportering samler også inn informasjon om apper, drivere og enheter for å hjelpe Microsoft med å forstå og forbedre app- og enhetskompatibilitet. Informasjon om en app inneholder kanskje navnet på appens kjørbare filer. Informasjon om enheter og drivere inneholder kanskje navnet på enhetene du har installert på

PCen, og de kjørbare filene som er knyttet til driverne for de enhetene. Informasjon om selskapet som gav ut en app eller driver, samles kanskje inn.

Hvis du velger å aktivere automatisk rapportering mens du konfigurerer Windows, sender rapporteringstjenesten automatisk grunnleggende informasjon om hvor problemene forekommer. Noen feilrapporter kan utilsiktet inneholde personlige opplysninger. En rapport med et øyeblikksbilde av PCens minne kan for eksempel omfatte navnet ditt, deler av et dokument du jobbet på, eller data du nettopp sendte inn til et nettsted. Hvis en rapport skal kunne inneholde denne typen informasjon, spør Windows deg om du vil sende denne informasjonen, selv om du har aktivert automatisk rapportering. Rapporter som inkluderer filer og data, blir kanskje lagret på PCen til etter at de har blitt sendt eller slettet.

Etter at du har sendt en rapport, kan rapporteringstjenesten be deg om mer informasjon om problemet som oppstod. Hvis du velger å oppgi telefonnummer eller e-postadresse i denne informasjonen, blir feilrapporten personlig identifiserbar. Microsoft kan kontakte deg for å be om tilleggsinformasjon for å bidra til å løse problemet du rapporterte.

Windows-feilrapportering genererer et tilfeldig tall kalt GUID (globalt unik identifikator) som sendes til Microsoft med hver feilrapport. GUIDen lar oss fastslå hvilke data som sendes fra en bestemt datamaskin over tid. GUIDen inneholder ikke personlige opplysninger.

Informasjonen sendes kryptert via SSL for å beskytte personvernet ditt.

Bruk av informasjon

Microsoft bruker informasjon om feil og problemer som er rapportert av Windows-brukere, til å forbedre Microsoft-produkter og -tjenester, og i tillegg tredjepartsprogramvare og -maskinvare som er utformet for bruk med disse produktene og tjenestene. Vi bruker GUIDen til å fastsette hvor utbredte tilbakemeldingene vi mottar, er, og hvordan vi skal prioritere dem. GUIDen lar for eksempel Microsoft skille mellom én kunde som opplever et problem hundre ganger, og hundre kunder som opplever det samme problemet én gang.

Microsoft-ansatte, -kontraktører, -leverandører og -partnere får kanskje tilgang til relevante deler av den innsamlede informasjonen, men de har bare tillatelse til å bruke informasjonen til å reparere eller forbedre Microsoft-produkter og -tjenester, eller tredjepartsprogramvare og -maskinvare som er utformet for bruk med Microsoft-produkter og -tjenester. Hvis en feilrapport inneholder personlige opplysninger, bruker ikke Microsoft den informasjonen til å identifisere, kontakte eller sende reklame til deg. Hvis du imidlertid velger å oppgi kontaktinformasjon som beskrevet ovenfor, kan det hende vi bruker denne informasjonen til å kontakte deg.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, sender Windows-feilrapportering automatisk grunnleggende rapporter for å søke på Internett etter løsninger på problemer. Hvis du velger å tilpasse innstillingene, kan du styre Windows-feilrapportering ved å velge **Bruk Windows-feilrapportering til å se etter løsninger på problemer** under **Se etter problemløsninger på Internett**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under Handlingscenter i Kontrollpanel.

Hvis du vil ha mer informasjon, kan du se [personvernerklæringen for Microsofts feilrapporteringstjeneste](#) .

[Øverst på siden](#)

Windows Filtilknytning

Hva denne funksjonen gjør

Windows Filtilknytning bidrar til at brukere kan knytte filtyper til bestemte apper. Hvis du prøver å åpne en filtype uten en tilknyttet app, får du spørsmål i Windows om du vil bruke Windows Filtilknytning til å finne en app for filen, som omfatter søk i Windows Store etter en kompatibel app. Apper som vanligvis knyttes til filtypen, vises.

Informasjon som samles inn, behandles eller overføres

Hvis du velger å bruke Windows Filtilknytning, sendes filtypen (for

eksempel DOCX eller PDF) og PC-visningsspråket til Microsoft. Resten av filnavnet sendes ikke til Microsoft. Når det opprettes en filtilknytning til en bestemt app, sendes en unik identifikator for appen for å identifisere standardappen for hver filtype.

Bruk av informasjon

Når du sender inn en filtype, returnerer tjenesten en liste over appene som Microsoft vet kan åpne filer med denne filtypen. Hvis ikke du velger å laste ned og installere en app, endres ingen filtypetilknytninger.

Valg og kontroll

Når du prøver å åpne en filtype uten en tilknyttet app, kan du velge om du vil bruke Windows Filtilknytning. Det sendes ingen filtilknytningsinformasjon til Microsoft hvis du ikke bruker tjenesten.

[Øverst på siden](#)

Windows Hjelp

Windows Hjelp og støtte på weben

Hva denne funksjonen gjør

Når Windows Hjelp og støtte på weben er slått på, kan du få oppdatert hjelpe- og støtteinnhold, som er tilgjengelig når du er koblet til Internett.

Informasjon som samles inn, behandles eller overføres

Når du bruker Windows Hjelp og støtte på weben, sendes søketermer til Microsoft, og i tillegg dine forespørsler om hjelpeinnhold når en kobling klikkes. Windows sender informasjon om PCens konfigurasjon for å finne mer relevant hjelpeinnhold. Windows Hjelp og støtte på weben bruker også standard netteknologier, for eksempel informasjonskapsler.

Bruk av informasjon

Microsoft bruker informasjonen til å returnere hjelpeemner som svar på dine søk, til å returnere de mest relevante resultatene, til å utvikle nytt innhold, og til å forbedre eksisterende innhold. Vi bruker informasjonen om PCens konfigurasjon til å vise riktig hjelpeinnhold

for den konfigurasjonen. Vi bruker informasjonskapsler og andre netteknologier til å gjøre det enklere å navigere i hjelpeinnholdet, og slik at vi bedre forstår hvordan våre brukere bruker Windows Hjelp på weben.

Valg og kontroll

Hjelp og støtte på weben er aktivert som standard. Hvis du vil endre denne innstillingen, trykker eller klikker du **Innstillinger** -ikonet øverst i vinduet Hjelp og støtte, og deretter merker du av for eller fjerner merket for **Få elektronisk hjelp**. Hvis du vil fjerne informasjonskapsler som brukes av Windows Hjelp, åpner du Alternativer for Internett i Kontrollpanel, klikker eller trykker **Slett** -knappen under **Leserlogg**, velger **Informasjonskapsler og nettstedssdata**, og klikker eller trykker **Slett**. Hvis du velger å blokkere alle informasjonskapsler (i Personvern-delen i Alternativer for Internett), angir ikke Windows Hjelp noen informasjonskapsler.

Produktforbedringsprogram for Hjelp

Hva denne funksjonen gjør

Produktforbedringsprogrammet for Hjelp hjelper Microsoft med å identifisere trender på måten som våre kunder bruker Windows Hjelp og støtte på weben på, slik at vi kan forbedre våre søkeresultater og relevansen i innholdet.

Informasjon som samles inn, behandles eller overføres

HEIP sender Microsoft-informasjon om versjonen av Windows som PCen kjører, og om hvordan du bruker Windows Hjelp og støtte, inkludert spørringer du registrerer når du søker i Windows Hjelp og støtte, og eventuelle evalueringer eller tilbakemeldinger om hjelpeemnene som vises. Når du søker i, blar gjennom eller oppgir vurderinger av eller tilbakemeldinger på emnene i Hjelp som blir presentert for deg, sendes denne informasjonen til Microsoft.

HEIP genererer et tilfeldig nummer kalt GUID (globalt unik identifikator) som sendes til Microsoft sammen med hver HEIP-rapport. GUIDen lar oss fastslå hvilke data som sendes fra en bestemt maskin over tid. GUIDen inneholder ikke personlige opplysninger. GUIDen er atskilt fra GUIDene som brukes av Windows-feilrapportering og Windows CEIP.

Bruk av informasjon

Dataene brukes til å identifisere trender og bruksmønstre, slik at Microsoft kan forbedre kvaliteten på innholdet vi leverer, og relevansen i søkeresultatene. Vi bruker GUIDen til å fastsette hvor omfattende problemene vi mottar, er, og hvordan vi skal prioritere dem. GUIDen lar for eksempel Microsoft skille mellom én kunde som opplever et problem hundre ganger, og hundre kunder som opplever det samme problemet én gang.

Produktforbedringsprogrammet for Hjelp samler ikke inn informasjon med hensikt som kan brukes til å identifisere deg. Hvis du skriver inn slik informasjon i søk- eller tilbakemeldingsboksen, sendes informasjonen, men Microsoft bruker ikke denne eller annen informasjon til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, blir du med i produktforbedringsprogrammet for Hjelp. Hvis du velger å tilpasse innstillinger, kan du kontrollere innstillingene for produktforbedringsprogrammet for Hjelp ved å velge **Hjelp med å forbedre innholdet i Hjelp for Windows ved å sende informasjon til produktforbedringsprogrammet for Hjelp** under **Send Microsoft-informasjon for å bidra til å gjøre Windows og apper bedre**. Etter at du har konfigurert Windows, kan du endre denne innstillingen i Windows Hjelp og støtte.

[Øverst på siden](#)

Fjernhjelp

Hva denne funksjonen gjør

Du kan bruke Fjernhjelp til å invitere noen til å koble til PCen din og hjelpe deg med et PC-problem, selv om den personen ikke er i nærheten. Når den andre personen har koblet til, kan vedkommende vise PCen din. Med din tillatelse kan den andre personen bruke sin egen mus og sitt eget tastatur til å styre PCen din, og slik vise deg hvordan du løser et problem.

Informasjon som samles inn, behandles eller overføres

Fjernhjelp oppretter en kryptert tilkobling mellom de to PCene via Internett eller det lokale nettverket. Når noen kobler til PCen din med Fjernhjelp, kan vedkommende se skrivebordet og alle åpne dokumenter, inkludert synlig privat informasjon. Hvis du tillater at den andre personen styrer PCen din med musen sin og tastaturet sitt, kan denne personen gjøre ting som å slette filer eller endre innstillinger. Etter at en tilkobling er opprettet, utveksler Fjernhjelp kontaktinformasjon, inkludert brukernavn, PC-navn og kontobilde. En øktloggfil inneholder et register over alle Fjernhjelp-tilkoblingene.

Bruk av informasjon

Informasjonen brukes til å opprette en kryptert tilkobling og gi den andre personen tilgang til skrivebordet. Det sendes ingen informasjon til Microsoft.

Valg og kontroll

Før du lar noen koble til PCen din, lukker du alle åpne apper eller dokumenter du ikke vil at den andre personen skal se. Hvis du føler deg ukomfortabel med det den andre personen ser eller gjør på PCen din, kan du når som helst trykke ESC-tasten for å avslutte økten. Du kan deaktivere øktlogging og utveksling av kontaktinformasjon ved å fjerne disse alternativene i innstillingene for Fjernhjelp.

[Øverst på siden](#)

Windows Søk

Hva denne funksjonen gjør

Windows Søk er et raskt og konsekvent inngangspunkt du kan bruke til å søke etter apper, innstillinger, filer eller innhold i apper.

Informasjon som samles inn, behandles eller overføres

Når du bruker Windows Søk, blir tegnene du skriver inn i søkefeltet (etter hvert som du skriver dem inn), og den endelige søkestrengen du sender, bare sendt til Windows og alle apper du søker i, og dermed kan Windows eller appen formidle søkeforslag og vise søkeresultater. Windows lagrer søkespørringer og data om hvor ofte du søker i appene.

Bruk av informasjon

Windows bruker lagrede tidligere søk til å gi søkeforslag i søkeruten. Den lagrede informasjonen om hvor ofte du søker i apper, brukes til å sortere listen over søkbare apper i søkeruten etter frekvens. Hvis du søker i en tredjepartsapp, er bruk av innsamlet informasjon underlagt tredjepartens personvernpraksis. Hvis du søker i en Microsoft-app, blir appens personvernpraksis forklart i denne personvernerklæringen.

Valg og kontroll

Windows lagrer denne informasjonen som standard. Du kan deaktivere lagringen av denne informasjonen eller slette alle tidligere lagrede søk under Søk i PC-innstillinger.

[Øverst på siden](#)

Windows-ressurs

Hva denne funksjonen gjør

Du kan bruke Windows-ressurs til å dele innhold mellom Windows Store-apper som støtter deling. Du kan også bruke den til å dele innhold med venner.

Informasjon som samles inn, behandles eller overføres

Når du deler, sender kildeappen innhold til målappen bare etter at du har valgt målet i delingsruten. Hvis kildeappen ikke har deling implementert, kan du dele et bilde av det som vises på skjermen. Målapper og personer du ofte deler innhold med, vises i en liste i delingsruten, slik at det blir enklere å få tilgang til dem. Det sendes ingen informasjon til Microsoft.

Bruk av informasjon

Informasjonen som lagres om hvor ofte du deler med målapper, og personer du ofte deler innhold med, brukes til å sortere listen i delingsruten etter frekvens. Hvis du deler informasjon med en tredjepartsapp, er bruk av innsamlet informasjon underlagt tredjepartens personvernpolicy. Hvis du deler med en Microsoft-app, blir appens personvernpraksis forklart i denne

personvernerklæringen.

Valg og kontroll

Som standard lagrer Windows informasjon om din bruk av Windows-ressurs. Du kan deaktivere lagringen av denne informasjonen eller slette alle tidligere lagrede målene under Ressurs i PC-innstillinger.

[Øverst på siden](#)

Windows SmartScreen

Hva denne funksjonen gjør

Windows SmartScreen holder PCen trygg ved å sjekke filer og apper med Microsoft før du åpner eller kjører dem. På den måten blir du beskyttet mot potensielt usikre filer og apper. Windows spør deg om hva du vil gjøre hvis en fil eller app er ukjent eller potensielt farlig, før den åpnes.

Informasjon som samles inn, behandles eller overføres

Hvis du velger å bruke denne funksjonen, sendes det informasjon om noen av appene du bruker, og noen av filene du laster ned fra Internett, til Microsoft. Denne informasjonen kan omfatte et filnavn, en filidentifikator (hash-kode) og informasjon om digitale sertifikater samt standard PC-informasjon og versjonsnummeret for Windows SmartScreen-filtret. Informasjonen krypteres via SSL før den sendes til Microsoft slik at personvernet beskyttes.

Windows SmartScreen genererer et tilfeldig nummer kalt GUID (globalt unik identifikator) som sendes til Microsoft sammen med SmartScreen-bruksdataene. GUIDen lar oss fastslå hvilke data som sendes fra en bestemt PC over tid. GUIDen inneholder ikke personlige opplysninger.

Bruk av informasjon

Microsoft bruker informasjonen beskrevet over til å advare deg om potensielt usikre filer og apper. Vi bruker også informasjonen til å analysere funksjonens ytelse og til å forbedre kvaliteten på våre produkter og tjenester. Vi bruker GUIDen til å fastsette hvor utbredte tilbakemeldingene vi mottar, er, og hvordan vi skal prioritere dem. GUIDen lar for eksempel Microsoft skille mellom én

kunde som opplever et problem hundre ganger, og hundre kunder som opplever det samme problemet én gang. Microsoft bruker ikke informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du Windows SmartScreen. Hvis du velger å tilpasse innstillingene, kan du kontrollere Windows SmartScreen ved å velge **Bruke Windows SmartScreen-filer til å kontrollere filer og apper med Microsoft** under **Beskytte personvernet ditt og PCen**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under Handlingscenter i Kontrollpanel.

[Øverst på siden](#)

Windows Talegjenkjenning

Hva denne funksjonen gjør

Windows Talegjenkjenning gir talegjenkjenning i Windows og for alle apper som velger å bruke den. Windows Talegjenkjenning øker nøyaktigheten ved å lære hvordan du bruker språk, inkludert lydene og ordene du liker å bruke.

Informasjon som samles inn, behandles eller overføres

Windows Talegjenkjenning lagrer en liste over ord og uttalen deres på PCen. Ord og uttale legges til i denne listen ved hjelp av taleordboken, og ved å bruke Windows Talegjenkjenning til å diktere og rette ord.

Når funksjonen for gjennomgang av dokumenter for Windows Talegjenkjenning aktiveres, samles tekst fra Microsoft Office Word-dokumenter (med filtypen DOC eller DOCX) og e-post (fra andre e-postmapper enn Slettede elementer eller Sjøppelpost) på PCen og på andre tilkoblede filressurser, inkludert i søkeindeksplasseringer for Windows, inn i fragmenter på ett, to og tre ord. Fragmenter på ett ord omfatter bare ord du har lagt til i egendefinerte ordlister, og fragmenter på to eller tre ord omfatter bare ord som finnes i standardordlister.

All innsamlet informasjon lagres i den personlige taleprofilen din på

PCen. Egne taleprofiler lagres for hver bruker, og brukerne har ikke tilgang til profilene til andre brukere på PCen. Administratorer har imidlertid tilgang til alle profiler på PCen. Profilinformatjonen sendes ikke til Microsoft med mindre du velger å sende den når du får spørsmål av Windows Talegjenkjenning. Du kan gå gjennom dataene før de sendes. Hvis du velger å sende denne informasjonen, sendes også akustiske tilpassingsdata som ble brukt til tilpassing til dine lydegenskaper.

Hvis du fullfører en taleopplæringsøkt, får du spørsmål av Windows Talegjenkjenning om du vil sende taleprofilinformasjonen til Microsoft. Du kan gå gjennom informasjonen før den sendes. Denne informasjonen kan omfatte innspillinger av stemmen din mens du fullførte opplæringsøkten, og annen informasjon fra den personlige taleprofilen din.

Bruk av informasjon

Windows Talegjenkjenning bruker ord fra taleprofilen til å konvertere tale til tekst. Microsoft bruker informasjon fra den personlige taleprofilen til å forbedre produktene og tjenestene. Vi bruker ikke denne informasjonen til å identifisere, kontakte eller sende reklame til deg.

Valg og kontroll

Du kan velge om du vil kjøre Windows Talegjenkjenning. Hvis du kjører Windows Talegjenkjenning, er funksjonen for gjennomgang av dokumenter aktivert som standard. Du kan endre innstillingene for dokumentgjennomgang første gang du kjører Windows Talegjenkjenning. Du kan endre innstillingene for dokumentgjennomgang eller slette personlige taleprofiler (og det meste av informasjonen om dokumentgjennomgang) ved å gå til Talegjenkjenning i Kontrollpanel og klikke **Avanserte talealternativer**. Du kan også bruke alternativet for endring av eksisterende ord i taleordboken til å slette ord du har lagt til i taleprofilen. Hvis du sletter taleprofilen, slettes imidlertid ikke ord som ble lagt til ved hjelp av taleordboken.

Du kan kontrollere hvor denne dokumentgjennomgangen skal samle inn ordfragmenter fra, ved å endre plasseringene som er inkludert i Windows-søkeindeksen. Hvis du vil vise eller endre hvilke

plasseringer som er inkludert i Windows-søkeindeksen, åpner du Indekseringsalternativer i Kontrollpanel.

På slutten av opplæringsøkten kan du velge om du vil sende opplæringen og annen profilinformasjon til Microsoft. Du kan også sende informasjon når Windows Talegjenkjenning startes, ved å høyreklikke **Mikrofon** og deretter klikke **Bidra til å forbedre talegjenkjenning**. I hvert tilfelle kan du vise alle datafiler før de sendes, og du kan velge å ikke sende dem.

[Øverst på siden](#)

Windows Store

Du kan bruke Windows Store til å søke etter, administrere og installere apper for PCen. Avsnittene nedenfor beskriver hvordan Store-funksjonene og appene du anskaffer via Store, kan påvirke personvernet ditt, og hva du kan gjøre for å kontrollere dette.

Store-app og -tjeneste

Hva denne funksjonen gjør

Du kan bruke Store til å søke etter og installere apper for PCen. Den holder også rede på Store-appene du har installert, slik at du kan få oppdateringer for dem og installere dem på flere PCer.

Informasjon som samles inn, behandles eller overføres

Du kan finne og installere apper ved å logge på Store med en Microsoft-konto. Dette gir Store tilgang til informasjon i Microsoft-kontoprofilen din, for eksempel navn, e-postadresse og kontobilde. Store samler inn og knytter følgende tilleggsinformasjon til Store-kontoen:

- Betalinger til Store. Informasjon om hva du kjøper, hvor mye du betaler, og hvordan du betaler når du kjøper apper eller kjøper produkter i apper med Store-kontoen.
- Apper du har installert. Listen over apper du har installert, lisenspolicyen for hver app (permanent lisens eller tidsbegrenset prøveversjon) og en liste over kjøp du har foretatt med Store-kontoen i hver app. I tillegg til å lagre denne informasjonen på nettet i Store-kontoen din lagrer Store

lisensinformasjon på PCen for hver app du installerer. Denne informasjonen identifiserer deg som eier av lisensen.

- PCer du har installert apper på. Merket, modellen og datamaskinnavnet på hver PC du installerer apper på, sammen med et nummer som identifiserer PCen entydig. Dette nummeret genereres basert på maskinvarekonfigurasjonen for PCen og inneholder ikke informasjon om deg.
- Vurderinger, omtaler og problemrapporter. Når du har installert en app, kan du skrive en omtale eller angi en vurdering for den i Store. Microsoft-kontoen tilknyttes disse vurderingene. Hvis du skriver en omtale, blir navnet og kontobildet fra Microsoft-kontoen publisert sammen med omtalen din.
- Store-innstillinger. Innstillinger du angir for visning av apper i Store, for eksempel at bare apper som er tilgjengelige på morsmålet, skal vises.

Du kan velge om du vil lagre betalingsinformasjon, for eksempel et kredittkortnummer, i Store-kontoen. Denne informasjonen overføres av sikkerhetshensyn over SSL, og alle unntatt de fire siste sifrene i kredittkortnummeret lagres kryptert.

Store samler inn en del informasjon om Windows-eksemplaret ditt for å finne ut om det ble solgt i butikk, er en evalueringssversjon, er en del av et volumlisensprogram eller ble forhåndsinstallert av PC-produsenten. Når du kobler til Store for første gang, sendes en liste over alle apper som er forhåndsinstallert på PCen din, til Store, som deretter knytter lisenser til de appene med Store-kontoen din.

Store ser automatisk etter oppdateringer for appene, og den kan varsle deg når nye oppdateringer er tilgjengelige. Store sender følgende informasjon til Microsoft for å tilby oppdateringer:

- En liste over alle appene som er installert fra Store av alle brukerne på PCen.
- Lisensinformasjonen for hver app, inkludert eieren av hver lisens.
- Konfigurasjonsinnstillingene for Windows Update og/eller

Microsoft Update, for eksempel om du vil at oppdateringer skal lastes ned og installeres automatisk.

- Om oppdateringene for appene fra Store var vellykket, mislykket eller forårsaket feil.
- Globalt unik identifikator (GUID) – et tilfeldig generert nummer som ikke inneholder personlig informasjon. GUIDer brukes til å identifisere individuelle PCer uten å identifisere brukeren.
- BIOS-navnet, -revisjonsnummeret og -revisjonsdatoen – informasjon om settet med vesentlige programvarerutiner som tester maskinvaren, starter operativsystemet på datamaskinen og overfører data mellom maskinvareenheter som er koblet til datamaskinen.

Når du blar gjennom Store og bruker apper fra den, samler Microsoft inn en del informasjon som hjelper oss å forstå bruksmønstre og trender, omtrent slik mange nettstedet analyserer surfedataene til besøkende. Ingen av disse aktivitetsdataene brukes til å identifisere eller kontakte deg.

Bruk av informasjon

Microsoft bruker kontaktinformasjonen til å sende deg e-post som er nødvendig for å kunne tilby Store-tjenestene, for eksempel kvittering for apper du kjøper. Den bruker betalingsinformasjonen til å la deg betale for kjøp. Hvis du velger å lagre denne informasjonen, trenger du ikke å skrive den inn hver gang. Microsoft bruker informasjon om kjøp til å holde Store i drift og gi kundestøtte.

Store holder rede på alle appene du har installert. Du kan bruke Store til å administrere listen over enheter du har installert apper på, og kundestøtte kan også hjelpe deg å administrere denne informasjonen. Når du har installert en app, kan du alltid vise den i Store-kjøpsloggen, selv om du senere avinstallerer appen. Store bruker også denne listen til å sikre at grensen for antall PCer du kan installere apper på, ikke overskrides, slik som beskrevet i vilkårene for bruk for Windows Store. Når du skriver en omtale for en app, blir navnet og kontobildet som er knyttet til Windows-kontoen, publisert ved siden av omtalen i Store. Hvis du rapporterer et problem med en app, blir problemrapporten gjort tilgjengelig for Store-

representanter, slik at de kan vurdere den og følge den opp. De kan kanskje bruke navnet og e-postadressen som er knyttet til Store-kontoen, for om nødvendig å kontakte deg når de går gjennom rapporten.

Når oppdateringer er tilgjengelige for appene du har installert, vises en varslingsmelding i Store, og appflisen for Store angir antall tilgjengelige oppdateringer. Du kan deretter vise listen over tilgjengelige oppdateringer og velge hvilke du vil installere. Det kan hende at oppdaterte apper bruker andre Windows-funksjoner enn tidligere versjoner. Dette kan gi dem tilgang til andre ressurser på PCen. Du kan se de oppdaterte listene over funksjoner på sidene for appbeskrivelse, som det går en kobling til fra siden med tilgjengelige oppdateringer.

Store bruker informasjonen den samler inn om Windows-eksemplaret ditt, til å finne ut hvordan Windows ble installert på PCen (for eksempel om PC-produsenten forhåndsinstallerte det). Denne informasjonen kan Store bruke til å gi deg tilgang til apper som produsenten har gjort tilgjengelig eksklusivt for sine kunder. Den brukes også til å gi informasjon til Microsoft (og i enkelte tilfeller i aggregert form til produsenten) om Windows-bruksmønstre.

Microsoft bruker i enkelte tilfeller noen appkjøp- og bruksdata til å finne ut hvordan personer bruker Store (for eksempel hvordan brukere finner appene de installerer). Microsoft kan kanskje dele en del av denne aggregerte statistikken med apputviklere. Microsoft deler ikke personlige opplysninger med apputviklere. Vi bruker søke- og bruksdata som er samlet inn av Store, til bedre å forstå hvordan personer bruker Store, og til å forbedre Store-funksjoner og -tjenester.

Valg og kontroll

Hvis du velger å bruke Store, sendes informasjonen som beskrives i denne delen, til Microsoft som beskrevet ovenfor.

Hvis du vil fjerne en omtale du har publisert for en app, går du til appbeskrivelsen i Store, redigerer omtalen, og sletter all teksten.

Tillatelse for Store-apper

Hva denne funksjonen gjør

Mange apper du installerer fra Windows Store, er utviklet for å bruke bestemte maskinvare- og programvarefunksjoner på PCen. En bildeapp må kanskje bruke webkameraet ditt, og en restaurantguide må kanskje vite hvor du er, for å kunne komme med anbefalinger i nærheten.

Informasjon som samles inn, behandles eller overføres

Her er en liste over funksjoner som apper må oppgi at de bruker:

- Internett-tilkoblingen. Gjør at appen kan koble til Internett.
- Innkommende tilkoblinger via en brannmur. Tillater at appen sender informasjon til eller fra PCen via en brannmur.
- Et hjemme- eller arbeidsnettverk. Tillater at appen sender informasjon mellom PCen og andre PCer i samme nettverk
- Dine bilder, videoer, musikk eller dokumentbiblioteker. Tillater at appen bruker, endrer eller sletter filer i bibliotekene dine. Dette inkluderer tilgang til tilleggsdata som er innebygd i disse filene, for eksempel plasseringsinformasjon i bilder.
- Flyttbare lagringsmedier. Gjør at appen kan få tilgang til, endre eller slette filer på en ekstern harddisk, USB-flash-enhet eller bærbar enhet.
- Din Windows-legitimasjon. Tillater at appen bruker din legitimasjon til å godkjenne og gi tilgang til et firmaintranett.
- Sertifikater som er lagret på PCen eller et smartkort. Gjør at appen kan bruke sertifikater til å koble til organisasjoner, for eksempel banker, offentlige kontorer eller arbeidsgiveren din, på en sikker måte.
- Tekstmeldingsfunksjonen på PCen. Gjør at appen kan sende og motta tekstmeldinger.
- Webkameraet og mikrofonen. Gjør at appen kan ta bilder og spille inn lyd og video.
- Din geografiske posisjon. Gjør at appen kan fastslå din omtrentlige posisjon basert på en GPS-sensor eller

nettverksinformasjon.

- Funksjonen for nærfeltskommunikasjon på PCen. Gjør at appen kan koble til andre enheter i nærheten som samme app kjører på.
- De bærbare enhetene dine. Gjør at appen kan kommunisere med enheter, for eksempel mobiltelefonen, det digitale kameraet eller den bærbare musikkspilleren.
- Informasjonen på en bærbar enhet. Gjør at appen kan få tilgang til, endre eller slette kontakter, kalendere, oppgaver, notater, status eller ringetoner på den bærbare enheten.
- Den mobile bredbåndskontoen. Gjør at appen kan administrere den mobile bredbåndskontoen.

Funksjonene som brukes av en app, vises på siden med appbeskrivelsen. Hvis du installerer en app, tillater Windows at den bruker disse funksjonene, bortsett fra plassering, tekstmeldinger og webkamera og mikrofon, som anses å være spesielt sensitive. Når en app ber om tilgang til én av disse sensitive funksjonene for første gang, spør Windows deg om du vil tillate appen å bruke funksjonen. Du kan når som helst endre om appen kan bruke den.

Bruk av informasjon

Hver apps bruk av disse funksjonene er underlagt leverandørens personvernpraksiser. Hvis en app bruker én av de sensitive funksjonene som er beskrevet ovenfor, vises det en kobling til apputgiverens personvernerklæring på siden Appbeskrivelse i Store.

Valg og kontroll

Du kan se hvilke funksjoner en app krever, i Store før du installerer appen. Du får spørsmål i Windows om du vil gi eller nekte tilgang til de mest sensitive av disse funksjonene – posisjon, tekstmeldingsfunksjon, webkamera og mikrofon – før hver app bruker dem for første gang.

Når du ser på siden med appbeskrivelsen i Windows Store, er det en forkortet liste over funksjonene som brukes av appen, nederst i venstre kolonne. Du kan vise den fullstendige listen på detaljsiden

for appbeskrivelsen. Når du har installert en app, kan du når som helst vise den fullstendige listen over funksjoner den bruker, og kontrollere appens tilgang til de mest sensitive funksjonene. Dette gjøre du ved å åpne appen, klikke eller trykke Innstillinger-perlen, og deretter velge **Tillatelser**.

Bidra til å forbedre Windows Store ved å sende nettadresser for nettinhold som apper bruker

Hva denne funksjonen gjør

Noen apper du henter fra Store, fungerer som nettsted og kan dermed utsette datamaskinen for potensielt usikker programvare, for eksempel skadelig programvare. Hvis du velger å slå denne funksjonen på, samler den inn informasjon om nettinholdet som ble brukt av disse appene til å hjelpe Microsoft med å analysere potensielt utrygg virkemåte. Vi kan for eksempel bruke denne informasjonen til å fjerne en app fra Store.

Informasjon som samles inn, behandles eller overføres

Hvis du velger å sende informasjon om nettinholdet som ble brukt av appene dine, samler Microsoft inn informasjon om nettadressene og innholdstypene som disse appene har tilgang til når du bruker dem. Dette kan hjelpe oss å identifisere appene som mottar innhold fra skadelige eller usikre nettsteder. Rapporter som blir sendt til Microsoft, omfatter informasjon som navn eller identifikator for appen, fullstendige nettadresser som appen går til, og fullstendige nettadresser som angir plasseringen for eventuelle JavaScript som appen bruker. Windows genererer et tilfeldig nummer kalt GUID (globalt unik identifikator) som sendes til Microsoft sammen med hver rapport. GUIDen lar oss fastslå hvilke data som sendes fra en bestemt datamaskin over tid. GUIDen inneholder ingen personlige opplysninger og brukes ikke til å identifisere deg.

For å ivareta personvernet krypteres informasjonen som sendes til Microsoft. Informasjon som kan være knyttet til en nettside som disse appene bruker, for eksempel søkeord eller data du har skrevet inn i apper, kan bli inkludert. Hvis du for eksempel slår opp et ord i en ordbokapp, kan ordet du slo opp, kanskje bli inkludert i informasjonen som sendes til Microsoft, som en del av den

fullstendige adressen appen går til. Microsoft filtrerer disse adressene for å prøve å fjerne personlige opplysninger der dette er mulig.

Bruk av informasjon

Microsoft går regelmessig gjennom informasjonen som sendes for å bidra til å gjenkjenne apper som kan kommunisere med usikkert nettinnhold, for eksempel skadelige nettadresser eller skript. Vi kan for eksempel bruke denne informasjonen til å iverksette tiltak mot potensielt skadelige apper. Adresser til nettinnhold kan utilsiktet inneholde personlige opplysninger, men disse opplysningene blir ikke brukt til å identifisere, kontakte eller sende reklame til deg. Vi bruker GUIDen til å fastsette hvor utbredte tilbakemeldingene vi mottar, er, og hvordan vi skal prioritere dem. GUIDen gjør for eksempel at Microsoft kan skille mellom en potensielt usikker virkemåte som oppstår hundre ganger på én PC, og den samme virkemåten som forekommer én gang på hundre PCer.

Valg og kontroll

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, sender Windows informasjon om nettinnholdet som brukes av appene fra Store som er utviklet ved hjelp av JavaScript. Hvis du velger å tilpasse innstillinger, kan du kontrollere denne innstillingen ved å velge **Bidra til å forbedre Windows Store ved å sende nettadresser for nettinnhold som apper bruker** under **Send Microsoft-informasjon for å bidra til å gjøre Windows og apper bedre**. Etter installasjonen kan du endre denne innstillingen under Personvern i PC-innstillinger.

[Øverst på siden](#)

Tjenesten Windows Time

Hva denne funksjonen gjør

Tjenesten Windows Time synkroniserer PCens klokkeslett automatisk med en tidsserver på et nettverk.

Informasjon som samles inn, behandles eller overføres

Tjenesten kobler til en tidsserver over Internett eller et lokalnett ved

å bruke bransjestandarden Network Time Protocol. Som standard synkroniseres denne tjenesten med time.windows.com én gang i uken. Det sendes ikke annet enn standard PC-informasjon til tidsserveren.

Bruk av informasjon

Informasjon brukes av tjenesten Windows Time til automatisk å synkronisere klokkeslettet på den lokale PCen.

Valg og kontroll

Tjenesten Windows Time er aktivert som standard. Du kan deaktivere denne funksjonen eller velge foretrukket tidskilde ved å gå til Dato og klokkeslett i Kontrollpanel, velge kategorien Internett-klokke og klikke **Endre innstillinger**. Hvis du deaktiverer tjenesten Windows Time, har ikke dette noen direkte virkning på apper eller andre tjenester, men klokken på den lokale PCen kan slutte å gå synkront med klokker på andre PCer på nettverket eller Internett. Apper og tjenester som er avhengige av klokkeslett, kan slutte å fungere riktig hvis det er et betydelig tidsavvik mellom PCer på et nettverk.

[Øverst på siden](#)

Windows Feilsøking

Hva denne funksjonen gjør

Ved hjelp av Windows Feilsøking kan du analysere og løse vanlige problemer på PCen.

Informasjon som samles inn, behandles eller overføres

Når du har kjørt en feilsøkingspakke, lagres resultatene på PCen. Disse resultatene kan inneholde personlige opplysninger, for eksempel brukernavnet eller navnet på en enhet. Windows Feilsøking kan hjelpe deg å søke etter problemløsninger i Windows Hjelp og i Windows-grupper på nettet. Nøkkelord som er knyttet til problemet, sendes til Microsoft for å bidra til å finne en løsning. Hvis skriveren for eksempel ikke fungerer som den skal, og du ser etter hjelp, sendes ordene "skriver", "skrive ut" og "utskrift" til Microsoft.

Bruk av informasjon

Microsoft bruker informasjonen som er samlet inn fra Windows Feilsøking, til å løse problemer som våre kunder opplever.

Valg og kontroll

Hvis du velger hurtiginnstillinger under Windows-installasjonen, søker Windows Feilsøking som standard etter feilsøkingspakker på nettet. Hvis du vil endre disse innstillingene eller slette feilsøkingsresultater, går du til Feilsøking i Kontrollpanel. Klikk **Vis logg**, velg et resultat, og klikk deretter **Slett**.

[Øverst på siden](#)

Hvis du vil ha oppdatert informasjon om Microsofts databehandlingspraksis, kan du se [Microsofts personvernerklæring](#). Her kan du også finne ut mer om de nyeste verktøyene vi tilbyr for åpne og kontrollere data, og hvordan du kontakter oss hvis du har et spørsmål om personvern.

Personvernerklæring for Windows 8 og Windows Server 2012

Høydepunkt Erklæring Funksjonstillegg **Servertillegg**

På denne siden Sist oppdatert: **August 2012**

Brukertilgangslogging Denne siden er et tillegg til [Personvernerklæring for Windows 8 og Windows Server 2012](#) ("Personvernerklæring for Windows").

Serveradministrasjon Personvernerklæringen har fire deler:

Active Directory
Federation Services

- [Hovedpunkter](#)

IP Address
Management

- Erklæring, som er [fullstendig personvernerklæring for Windows](#) som inneholder koblinger til Windows-funksjoner med egne frittstående erklæringer

Unified Remote
Access

- [Funksjonstillegg](#), som beskriver funksjonene som har innvirkning på personvern i Windows 8 og Windows Server 2012

Eksterne
skrivebordstjenester

- [Servertillegg](#) (dette dokumentet), som beskriver tilleggsfunksjonene som har innvirkning på personvernet i Windows Server 2012

Windows-program
for forbedret
kundeopplevelse

(CEIP) og Windows-feilrapportering (WER)

For å forstå datainnsamlingen og brukspraksisen som er relevant for en bestemt funksjon eller tjeneste i Windows, bør du lese hele personvernerklæringen for Windows og aktuelle tillegg. I tillegg bør du lese [denne hvitboken for administratorer](#).

Brukertilgangslogging

Hva denne funksjonen gjør

Brukertilgangslogging (UAL) samler inn og aggregerer oppføringer med klientforespørsler om serverroller (både bruker- og enhetsforespørsler) og installerte produkter (hvis det er registrert med brukertilgangslogging) på den lokale serveren. Disse dataene, i form av IP-adresser, brukernavn, og i enkelte tilfeller vertsnavn og/eller virtuelle maskinidentiteter, lagres i de lokale ESE-databasene (Extensible Storage Engine) og er bare tilgjengelige for administratorer. UAL har en WMIv2-leverandør og tilknyttede Windows PowerShell-cmdleter for å hente brukertilgangsdata som er beregnet på frakoblet administrasjon av rettigheter for klientadgangslisens (CAL), der faktiske oppføringer med unike klientforespørsler er kritisk.

Informasjon som samles inn, behandles eller overføres

IP-adresser, brukernavn, og i enkelte tilfeller vertsnavn (hvis DNS-rollen er installert), og virtuelle maskinidentiteter (hvis Hyper-V-rollen er installert), samles inn lokalt på serveren når UAL er aktivert. Ingen innsamlede data sendes til Microsoft.

Bruk av informasjon

UAL-data gjøres tilgjengelige for administratorer gjennom lokale ESE-databaser, WMI-leverandøren og Windows PowerShell-cmdleter. Windows bruker ikke disse dataene utenfor selve UAL-funksjonen.

Valg og kontroll

UAL er aktivert som standard. UAL-tjenesten kan stoppes og startes mens serveren kjører. Hvis du vil deaktivere UAL permanent, åpner du Windows PowerShell, skriver inn `Disable-UAL` og starter serveren på nytt. Administrator kan slette alle historiske data som samles inn, ved først å stoppe tjenesten, deaktivere UAL

og deretter slette alle filene i mappen
%SystemRoot%\System32\LogFiles\SUM\.

[Toppen av siden](#)

Serveradministrasjon

Hva denne funksjonen gjør

Serveradministrasjon er et administrasjonsverktøy som lar administratorer overvåke én eller flere servere og vise generell eller rollespesifikk status, for å utføre administrasjonsoppgaver og få tilgang til andre verktøy for serveradministrasjon.

Informasjon som samles inn, behandles eller overføres

Serveradministrasjon samler inn følgende typer informasjon fra en server som administrator administrerer:

- **Generell serverinformasjon:** NetBios-navn og fullstendig domenenavn (FQDN), kontolegitimasjon som er angitt i "Administrer som"-funksjonen, IPv4-adresse, IPv6-adresse, administrasjonsstatus, beskrivelse, operativsystemversjon, type, siste oppdatering, prosessorer, minne, klyngenavn, klyngeobjekttype, aktiveringsstatus, SKU, operativsystemarkitektur, produsent, konfigurasjon av Program for forbedret kundeopplevelse (CEIP-Customer Experience Improvement Program) og konfigurasjon av Windows-feilrapportering (WER).
- **Hendelser:** ID, alvorsgrad, kilde, logg, dato og klokkeslett for hver hendelse fra Windows og andre logger som administrator velger.
- **Alle tjenester:** navn, status og starttype.
- **Informasjon om serverrolle:** BPA-resultater (Best Practice Analyzer) for roller som er installert på serveren.
- **Ytelsesinformasjon:** eksempler for ytelsestellere og varslinger for prosessorbruk og tilgjengelig minne.

Bruk av informasjon

Denne informasjonen lagres i Serveradministrasjon og sendes ikke til Microsoft. Den vises i Serveradministrasjon for å hjelpe administratorer med å overvåke systemer.

Valg og kontroll

Administrator kan velge å samle inn data fra servere, unntatt den lokale serveren, ved å legge til eller fjerne serveren i Serveradministrasjon. Administrator kan eksplisitt angi legitimasjon for å koble til en ekstern server. Serveradministrasjon ber administrator om eksplisitt å samtykke i lagring av legitimasjonen lokalt i Serveradministrasjon, og administrator kan slette denne legitimasjonen når som helst.

[Toppen av siden](#)

Active Directory Federation Services

Hva denne funksjonen gjør

Active Directory Federation Services (AD FS) er en virksomhetsklar løsning for forbund og enkel pålogging for lokale eller andre nettverksbaserte programmer. AD FS gjør det mulig for administratorer å la brukere å samarbeide på tvers av organisasjoner og gi enkel tilgang til programmer på lokale nettverk eller andre nettverk, og samtidig opprettholde programsikkerhet. AD FS bruker en sikkerhetstokentjeneste som bruker Active Directory Domain Services (AD DS) til å godkjenne brukere og gi dem sikkerhetstokener ved hjelp av ulike protokoller. Tokenet signeres digitalt og inneholder påstander om brukeren, som kommer fra alle eller enhver kombinasjon av AD DS, Lightweight Directory Access Protocol (LDAP), SQL Server eller et egendefinert lager.

Informasjon som samles inn, behandles eller overføres

Legitimasjonen til en bruker samles inn når brukeren godkjennes med AD FS. Legitimasjonen sendes umiddelbart til Active Directory Domain Services for godkjenning, og AD FS lagre den ikke lokalt. Brukerens attributter i Active Directory Domain Services kan brukes til å generere utgående påstander, avhengig av

påstandsreglene som en AD FS-administrator har konfigurert. Utgående påstander sendes til klarerte partnere som en AD FS-administrator har et tillitsforhold med. Ingen informasjon sendes tilbake til Microsoft.

Bruk av informasjon

Microsoft har ikke tilgang til denne informasjonen. Denne informasjonen er bare ment for bruk av kunden.

Valg og kontroll

Bruk AD FS hvis du vil at AD FS skal samle inn og sende data til klarerte partnere.

[Toppen av siden](#)

IP Address Management

Hva denne funksjonen gjør

IP Address Management (IPAM) lar serveradministratorer spore IP-adresse, vertsnavn og klient-ID (for eksempel MAC-adressen i IPv4 og DUID i IPv6) for datamaskiner eller enheter på et nettverk, med brukerpåloggingsinformasjon.

Informasjon som samles inn, behandles eller overføres

IPAM-serveren samler inn overvåkingslogger og hendelser fra DHCP-servere, domenekontrollere og nettverkspolicyservere, og deretter blir IP-adressen, vertsnavnet, klientidentifikatoren og brukernavnet til den påloggede brukeren, lagret lokalt.

Serveradministrator kan søke i de innsamlede loggene basert på IP-adresse, klient-ID, vertsnavn og brukernavn, ved å bruke IPAM-konsollen. Ikke noe av denne informasjonen sendes til Microsoft.

Bruk av informasjon

Microsoft har ikke tilgang til denne informasjonen. Denne informasjonen er bare ment for bruk av kunden.

Valg og kontroll

IPAM er ikke installert som standard og må installeres av serveradministrator. Etter at IPAM er installert, aktiveres IP-adresseovervåking automatisk. Hvis du vil deaktivere IP-

adresseovervåking på en server der IPAM er installert, starter du Oppgaveplanlegging på IPAM-serveren, går til Audit Task under Microsoft\Windows\IPAM, og deretter deaktiverer du oppgaven.

[Toppen av siden](#)

Unified Remote Access

Hva denne funksjonen gjør

Unified Remote Access lar eksterne brukere koble til et privat nettverk, for eksempel et firmanettverk, via Internett. Unified Remote Access bruker DirectAccess til å gi eksterne klientdatamaskiner, som kjører Windows 8, uavbrutt og transparent tilkobling til firmanettverk. Den leverer også tjeneste for ekstern pålogging (RAS-Remote Access Service), som er tradisjonelle VPN-tjenester, inkludert node-til-node-tilkobling lokalt eller annen nettverkstilkobling.

Informasjon som samles inn, behandles eller overføres

For Unified Remote Access-brukerovervåking lagrer DirectAccess-serveren detaljene for eksterne brukere som kobler til det private nettverket. Dette omfatter informasjon som vertsnavnet til den eksterne brukeren, Active Directory-brukernavnet og den offentlige IP-adressen til den eksterne klienten (hvis klienten er bak NAT (Network Address Translation), vil dette være den offentlige IP-adressen). Disse dataene kan også lagres i Intern Windows-database (WID) eller på RADIUS-servere, og bare med samtykke fra administrator. Bare DirectAccess-administrator (en domenebruker med en lokal administratorkonto) har tilgang til og kan vise denne informasjonen ved tilgang til en server.

Bruk av informasjon

Denne informasjonen brukes av administrator til å feilsøke klienttilkobling og også til overvåkings- eller samsvarsformål. Ingen informasjon sendes tilbake til Microsoft.

Valg og kontroll

Overvåking av ekstern klient er aktivert som standard og kan ikke deaktiveres. Overvåkingsdataene lagres i WID eller på RADIUS-

servere bare hvis administrator har konfigurert kontobehandling til å bruke noen av disse alternativene. Hvis administrator ikke har konfigurert kontobehandling, lagres ikke noe av denne informasjonen. Administrator kan også konfigurere kontobehandling på en server for ekstern pålogging til ikke å lagre informasjon om brukernavn og IP-adresse.

[Toppen av siden](#)

Eksterne skrivebordstjenester

Hva denne funksjonen gjør

Eksterne skrivebordstjenester (RDS) gir en plattform som lar firmaer implementere en sentralisert skrivebordsstrategi, administrere skrivebord og programmer, forbedre fleksibilitet og samsvar, og samtidig forbedre datasikkerhet.

Informasjon som samles inn, behandles eller overføres

For RDS-brukerovervåking lagrer vertsserver for en ekstern skrivebordsøkt informasjon om eksterne brukere som kobler til RDS-ressurser. Dette omfatter informasjon som vertsnavnet til den eksterne brukeren, Active Directory-brukernavnet og den offentlige IP-adressen til den eksterne klienten (hvis klienten er bak NAT (Network Address Translation), vil det være den offentlige IP-adressen). Disse dataene lagres automatisk i Intern Windows-database (WID) eller på SQL-servere når brukere kobler til. Ingen informasjon sendes tilbake til Microsoft. Bare domenebrukere med lokal administratorkonto har tilgang til og kan vise denne informasjonen.

Bruk av informasjon

Denne informasjonen brukes av administrator til å feilsøke klienttilkobling og også til interne overvåkings- eller samsvarsformål. Ingen informasjon sendes tilbake til Microsoft.

Valg og kontroll

Klienovervåking er aktivert som standard og kan ikke deaktiveres. Overvåkingsinformasjonen lagres i WID eller på SQL-server.

[Toppen av siden](#)

Windows-program for forbedret kundeopplevelse (CEIP) og Windows-feilrapportering (WER)

Hva denne funksjonen gjør

Hvis du vil ha mer informasjon om disse problemene, kan du se [Funksjonstillegg](#)-fanen eller [denne](#) [hvitboken for administratorer](#).

Informasjon som samles inn, behandles eller overføres

Hvis du vil vite mer om den spesifikke informasjonen som samles inn, behandles og overføres av disse funksjonene, kan du se CEIP og WER i [Funksjonstillegg](#) -fanen.

Bruk av informasjon

Hvis du vil vite mer om hvordan vi bruker informasjon som samles inn av disse funksjonene, kan du se CEIP og WER i [Funksjonstillegg](#) -fanen.

Valg og kontroll

CEIP er deaktivert som standard, og WER er som standard satt til å be om bekreftelse før krasjrapporter sendes til Microsoft. Du kan aktivere og deaktivere CEIP fra Serveradministrasjon og Kontrollpanel, og ved å bruke kommandolinjemetoder. WER kan bare kontrolleres ved hjelp av kommandolinjemetoder.

Hvis du vil aktivere eller deaktivere CEIP ved hjelp av kontrollpanelet, klikker du på **System og vedlikehold** og **Problemrapportering og løsninger**. Under Se også i venstre rute, klikker du på **Innstillinger for program for forbedret kundeopplevelse** for alternativet for å aktivere eller deaktivere CEIP.

Kontroller for Serveradministrasjon

Lokal server

- Aktiver CEIP
Åpne Serveradministrasjon, og velg **Lokal server**. Klikk på koblingen Program for forbedret kundeopplevelse, velg **Ja, jeg ønsker å delta i CEIP** i dialogboksen, og klikk deretter på **OK**.

- Deaktiver CEIP
Åpne Serveradministrasjon, og velg **Lokal server**. Klikk på koblingen Program for forbedret kundeopplevelse, og velg **Nei, jeg ønsker ikke å delta** i dialogboksen, og klikk deretter på **OK**.
- Aktiver WER
Åpne Serveradministrasjon, og velg **Lokal server**. Klikk på koblingen for Windows-feilrapportering, velg **Ja, send sammendragsrapporter automatisk**, og klikk deretter på **OK**.
- Deaktiver WER
Åpne Serveradministrasjon, og velg **Lokal server**. Klikk på koblingen for Windows-feilrapportering, velg **Velg Jeg ikke ønsker å delta, og ikke spør meg igjen**, og klikk deretter på **OK**.

Flere datamaskiner

- Aktiver CEIP
Åpne Serveradministrasjon, og velg **Alle servere**. Velg alle servere (Ctrl+A) i Servere-flisen, høyreklikk og velg **Konfigurer automatisk tilbakemelding for Windows** . I fanen Program for forbedret kundeopplevelse velger du **Ja, jeg ønsker å delta (anbefales)**. Bruk denne innstillingen for alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter på **OK**.
- Deaktiver CEIP
Åpne Serveradministrasjon, og velg Alle servere. Velg alle servere (Ctrl+A) i Servere-flisen, høyreklikk og velg **Konfigurer automatisk tilbakemelding for Windows** . I fanen Program for forbedret kundeopplevelse velger du **Nei, jeg ønsker ikke å delta**. Bruk denne innstillingen for alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter på **OK**.
- Aktiver WER
Åpne Serveradministrasjon, og velg **Alle servere**. Velg alle servere (Ctrl+A) i Servere-flisen, høyreklikk og velg **Konfigurer automatisk tilbakemelding for Windows** . I

fanen Windows-feilrapportering velger du **Ja, send sammendragsrapporter automatisk (anbefales)**. Bruk denne innstillingen for alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter på **OK**.

- Deaktiver WER

Åpne Serveradministrasjon, og velg **Alle servere**. Velg alle servere (Ctrl+A) i Servere-flisen, høyreklikk og velg **Konfigurer automatisk tilbakemelding for Windows** . I fanen Windows-feilrapportering velger du **Nei, jeg ønsker ikke å delta**. Bruk denne innstillingen for alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter på **OK**.

[Toppen av siden](#)

Hvis du vil ha oppdatert informasjon om Microsofts databehandlingspraksis, kan du se [Microsofts personvernerklæring](#). Her kan du også finne ut mer om de nyeste verktøyene vi tilbyr for åpne og kontrollere data, og hvordan du kontakter oss hvis du har et spørsmål om personvern.

Personvernerklæring for Windows 8 og Windows Server 2012

Høydepunkt Erklæring Funksjonstillegg Servertillegg

På denne siden Sist oppdatert: **August 2012**

Dine opplysninger Disse hovedpunktene fra fullstendig [Personvernerklæring for Windows 8 og Windows Server 2012](#) ("Personvernerklæring for Windows") forklarer på et overordnet nivå noe av datainnsamlingen og brukspraksisen i Windows 8 og Windows Server 2012 ("Windows"). De fokuserer på funksjoner som kommuniserer med Internett, og de er ikke ment å være fullstendige beskrivelser. De gjelder ikke for andre av Microsofts tilkoblede eller frakoblede nettsteder, produkter eller tjenester.

Dine valg

Bruk av informasjon

Slik kontakter du oss

Denne personvernerklæringen har fire deler:

- Hovedpunkter (denne siden)
- Erklæring, som er den fullstendige personvernerklæringen for Windows som inneholder koblinger til Windows-funksjoner med egne frittstående erklæringer
- Funksjonstillegg, som beskriver funksjonene som har

innvirkning på personvernet i Windows 8 og Windows Server 2012

- [Servertillegg](#), som beskriver tilleggsfunksjonene som har innvirkning på personvernet i Windows Server 2012

Hvis du vil ha mer informasjon om hvordan du kan bidra til å beskytte den personlige datamaskinen din, dine personlige opplysninger og familien på Internett, kan du gå til vårt [Sikkerhetssenter](#).

Dine opplysninger

- Enkelte Windows-funksjoner ber deg kanskje om tillatelse til å samle inn eller bruke informasjon fra PC-en din, inkludert personlige opplysninger. Windows bruker denne informasjonen som beskrevet i fullstendig [Personvernerklæring for Windows](#), i [Funksjonstillegg](#) og [Servertillegg](#).
- Noen Windows-funksjoner kan, med din tillatelse, dele personlige opplysninger via Internett.
- Hvis du velger å registrere programvaren, blir du bedt om å oppgi personlige opplysninger.
- Windows krever aktivering for å redusere piratkopiering av programvare og bidra til å sikre at kundene våre får programvarekvaliteten de forventer. Aktivering sender informasjon om PC-en din til Microsoft.
- Du kan velge å logge på Windows med en [Microsoft-konto](#), som lar deg synkronisere Windows-innstillinger og automatisk logge på apper og nettsteder. Når du oppretter en Microsoft-konto, blir du bedt om å angi noen personlige opplysninger.
- [Tilleggsdetaljer](#)

[Toppen av siden](#)

Dine valg

- Windows inneholder en rekke metoder for å kontrollere

hvordan Windows-funksjoner overfører informasjon via Internett. Du finner mer informasjon om hvordan du styrer disse funksjonene i funksjonstillegget og servertillegget.

- Noen funksjoner som bruker Internett, er aktivert som standard for å bidra til å forbedre opplevelsen.
- [Tilleggsdetaljer](#)

[Toppen av siden](#)

Bruk av informasjon

- Vi bruker den innsamlede informasjonen til å aktivere funksjonene du bruker eller levere tjenestene du ber om. Vi bruke den også til å forbedre våre produkter og tjenester. For å bidra til å levere tjenestene våre gir vi av og til informasjon til andre firmaer som arbeider på våre vegne. Bare firmaer som trenger informasjonen i virksomheten får tilgang til den. Disse firmaene er forpliktet til å holde informasjonen konfidensiell og har ikke lov til å bruke den til andre formål.
- [Tilleggsdetaljer](#)

[Toppen av siden](#)

Slik kontakter du oss

Hvis du vil ha mer informasjon om vår personvernpraksis, kan du gå til fullstendig [Personvernerklæring for Windows](#). Du kan også skrive til oss ved hjelp av vår [nettskjema](#).

[Toppen av siden](#)