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 8.1 og Windows Server 2012 R2





Sist oppdatert: april 2014

Disse hovedpunktene fra den fullstendige personvernerklæringen for Windows 8.1 og Windows Server 2012 R2 ("personvernerklæring for Windows") gir en høynivåforklaring av noe av datainnsamlings- og bruksprаksisen i Windows 8.1 og Windows Server 2012 R2 ("Windows"). De fokuserer på nettbaserte funksjoner og er ikke ment å være en uttømmende beskrivelse. De gjelder ikke andre nettsteder, produkter eller tjenester fra Microsoft, enten de er nettbaserte eller ikke.

Denne personvernerklæringen har følgende deler:

- **Hovedpunkt** (denne siden)
- Erklæring, som er hele personvernerklæringen for Windows 8.1, og som inneholder koblinger til personvernerklæringer for Windows-funksjoner med egne frittstående erklæringer
- Funksjonstillegg, som beskriver funksjonene som har innvirkning

på personvern i Windows 8.1 og Windows Server 2012 R2

- Apptillegg, som beskriver appene som påvirker personvernet i Windows 8.1
- Servertillegg, som beskriver tilleggsfunksjonene som har innvirkning på personvern i Windows Server 2012 R2

Hvis du vil ha mer informasjon om hvordan du kan bidra til å beskytte PC-en, personlige opplysninger og familien på nettet, kan du gå til sikkerhetssenteret.

Din informasjon

- Bestemte 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 den fullstendige Windows 8.1 personvernerklæringen, samt i Funksjonstillegg, Apptillegg og Servertillegg.
- Noen Windows-funksjoner kan dele personlige opplysninger via Internett med din tillatelse.
- 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. Ved aktivering sendes noen opplysninger om PC-en din til Microsoft.
- Hvis du velger å logge på Windows med en Microsoft-konto, synkroniserer Windows innstillingene på tvers av enheter og logger automatisk på enkelte apper og nettsteder. Windows krever ikke at du logger på med en Microsoft-konto for å få tilgang til e-posttjenester eller sosiale nettverkstjenester fra en tredjepart, men hvis denne tredjeparten tilbyr en app via Store, må du logge på Store med en Microsoft-konto for å installere appen. Hvis du oppretter en Microsoft-konto, blir du bedt om å angi noen personlige opplysninger, for eksempel geografisk

område og fødselsdato.

- Tilleggsdetaljer

Øverst på siden

Valgene dine

- Windows gir deg ulike metoder for å styre hvordan Windows-funksjoner overfører informasjon via Internett. Du finner mer informasjon om hvordan du styrer disse funksjonene, i Funksjonstillegg, Apptillegg og Servertillegg.

- Noen funksjoner som bruker Internett, er aktivert som standard. Dette forbedrer brukeropplevelsen.

- Tilleggsdetaljer

Øverst på siden

Bruk av informasjon

- Vi bruker informasjonen som samles inn, til å aktivere funksjonene du bruker, eller levere tjenestene du ber om. Vi bruker den også til å forbedre produktene og tjenestene. 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 noe annet formål.

- Tilleggsdetaljer

Øverst på siden

Hvordan du kontakter oss

Hvis du vil ha mer informasjon om personvernpraksisen vår, kan du gå til den fullstendige personvernerklæringen for Windows 8.1. Eller du kan skrive til oss ved å bruke nettskjemaet.

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 8.1 og Windows Server 2012 R2



På denne siden



Sist oppdatert: april 2014

Denne erklæringen gjelder for Windows 8.1 og Windows Server 2012 R2 ("Windows"). Visse Windows-komponenter har egne personvernerklæringer, som også er oppført på denne siden. Personvernerklæringer for programvare og tjenester som er relatert til Windows og for tidligere utgaver, er også oppført der.

Hvis du vil ha informasjon om bestemte funksjoner, kan du se Funksjonstillegg, Apptillegg, og Servertillegg. Hvis du vil ha informasjon om Windows Embedded Industry Pro og Windows Embedded Industry Enterprise, kan du se denne erklæringen.

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

## Innsamling og bruk av dine opplysninger

De personlige opplysningene vi mottar fra deg, blir brukt av

Microsoft og dets kontrollerte datterselskaper og tilknyttede selskaper til å aktivere funksjonene du bruker, og til å levere tjenestene eller utføre transaksjonene du har bedt om eller godkjent. Opplysningene kan også brukes til å analysere og forbedre Microsofts produkter og tjenester.

Med unntak av det som er beskrevet i denne erklæringen, overføres ingen personlige opplysninger du oppgir, til tredjeparter uten ditt samtykke. Vi leier av og til inn andre selskaper for å levere begrensede tjenester på våre vegne, for eksempel utføre statistisk analyse av tjenestene våre. Disse selskapene får bare tilgang til de personlige opplysningene de trenger for å levere tjenesten, og de har ikke lov til å bruke disse opplysningene til noe annet formål.

Microsoft kan få tilgang til eller utlevere informasjon om deg, inkludert innhold fra din kommunikasjon, for å (a) overholde loven eller svare på lovlige henvendelser eller juridiske prosesser, (b) beskytte rettighetene eller eiendom som tilhører Microsoft eller kundene våre, inkludert for å håndheve avtaler eller policyer som gjelder din bruk av programvaren, eller (c) handle i god tro på at slik tilgang eller utlevering er nødvendig for å beskytte den personlige sikkerheten til Microsoft-ansatte, kunder eller allmennheten.

Informasjon som samles inn eller sendes til Microsoft av Windows 8.1, kan bli lagret og behandlet i USA eller i et hvilket som helst annet land der Microsoft eller dets tilknyttede selskaper, datterselskaper eller Internett-leverandører har kontorer. Microsoft retter seg etter Safe Harbor-prinsippene som er utviklet av det amerikanske handelsdepartementet, og som omhandler innsamling, bruk og oppbevaring av data fra EU, EØS og Sveits.

Øverst på siden

## Innsamling og bruk av informasjon om datamaskinen din

Når du bruker programvare med Internett-aktiverte funksjoner, sendes informasjon om datamaskinen din ("standardinformasjon om datamaskinen") til nettstedene du besøker, og nettjenestene du bruker. Standardinformasjon om datamaskiner omfatter typisk informasjon som IP-adressen din, versjon av operativsystemet, nettleserversjon og innstillinger for område og språk. I noen tilfeller

omfatter den også en maskinvare-ID som angir enhetens produsent, enhetsnavn og versjon. Hvis en bestemt funksjon eller tjeneste sender informasjon til Microsoft, sendes også standardinformasjon om datamaskinen.

Personverndetaljene for hver Windows-funksjon i Funksjonstillegg, Apptillegg og Servertillegg samt funksjonene som er oppført andre steder på denne siden, beskriver tilleggsinformasjonen som samles inn, og hvordan den brukes.

Administratorer kan bruke Gruppepolicy til å endre mange av innstillingene for funksjonene som beskrives her. Hvis du vil ha mer informasjon, kan du se denne hvitboken for administratorer.

Øverst på siden

## Informasjonssikkerhet

Microsoft er opptatt av å ivareta sikkerheten til informasjonen din. Vi bruker en rekke sikkerhetsteknologier og prosedyrer for å beskytte informasjonen din mot uautorisert tilgang, bruk eller utlevering. Vi lagrer for eksempel opplysningene du oppgir på datasystemer med begrenset tilgang som befinner seg i kontrollerte fasiliteter. Når vi overfører sensitive opplysninger (for eksempel kredittkortnummer eller passord) over Internett, beskytter vi dem ved hjelp av kryptering, for eksempel Secure Sockets Layer-protokollen (SSL).

Øverst på siden

## Endringer i denne personvernerklæringen

Vi oppdaterer av og til denne personvernerklæringen for å gjenspeile endringer i produkter, tjenester og tilbakemeldinger fra kunder. Når vi gjør endringer, endrer vi Sist oppdatert-datoen øverst i denne erklæringen. Hvis det blir foretatt betydelige endringer i denne erklæringen eller i måten Microsoft bruker dine personlige opplysninger på, varsler vi deg, enten ved å legge ut en tydelig melding om slike endringer før de blir iverksatt, eller ved å sende et varsel om endringene direkte til deg. Vi anbefaler at du regelmessig ser gjennom denne erklæringen, slik at du er orientert om hvordan Microsoft beskytter informasjonen din.

Øverst på siden

## Mer informasjon

Microsoft vil gjerne ha dine kommentarer til denne personvernerklæringen. Hvis du har spørsmål til denne erklæringen eller mener at vi ikke har overholdt den, kan du skrive til oss ved å bruke nettskjemaet.

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

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 8.1 og Windows Server 2012 R2





Sist oppdatert: april 2014

Vær oppmerksom på at denne siden er et tillegg til personvernerklæringen for Windows 8.1 og Windows Server 2012 R2 ("personvernerklæring for Windows"), som har følgende deler:

- Hovedpunkt
- Erklæring, som er den fullstendige personvernerklæringen for Windows 8.1, inneholder koblinger til personvernerklæringer for Windows-funksjoner med egne frittstående erklæringer
- **Funksjonstillegg** (denne siden), som beskriver funksjonene som har innvirkning på personvern i Windows 8.1 og Windows Server 2012 R2
- Apptillegg, som beskriver appene som påvirker personvernet i Windows 8.1
- Servertillegg, som beskriver tilleggsfunksjonene som har innvirkning på personvern i Windows Server 2012 R2

DirectAccess

Hjelpemiddelsenter

Hendelsesliste

Tryggere for familien

Faks

Håndskrifttilpasning – automatisk læring

Hjemmegruppe

IME (Input Method Editor)

Deling av Internett-tilkobling

Internett-utskrift

Språkinnstillinger

Posisjonstjenester

Administrere legitimasjonen

Navn og kontobilde

Nettverkssporing

Varslinger, låseskjermapper og flisoppdateringer

Bestill kopier

Forhåndshenting og forhåndsstart

Program Compatibility Assistant

Egenskaper

Nærhet

For å forstå datainnsamlingen og bruksprakSisen som er relevant for en bestemt funksjon eller tjeneste i Windows, bør du lese hele personvernerklæringen og aktuelle tillegg eller frittstående erklæringer.

Aktivering

**Hva denne funksjonen gjør**

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 produktnøkkelen blir brukt til å aktivere den samme kopien av programvaren på flere PCer. Noen endringer i PC-maskinvaren eller -programvaren kan gjøre at du må aktivere Windows på nytt. Aktivering kan registrere og deaktivere aktiveringsutnyttelser (programvare som omgår eller hopper over programvareaktivering for Microsoft). Hvis en aktiveringsutnyttelse forekommer, kan det hende en programvare- eller maskinvareleverandør har redigert opprinnelig Microsoft-programvare for å opprette piratkopier av programvaren. Aktiveringsutnyttelser kan påvirke den vanlige driften av systemet ditt.

**Informasjon som samles inn, behandles eller overføres**

Under aktivering sendes følgende informasjon til Microsoft:

- Microsoft-produktkoden (en femsifret kode som identifiserer Windows-produktet du aktiverer).
- En kanal-ID eller områdekode som identifiserer hvordan Windows-produktet opprinnelig ble anskaffet. En kanal-ID eller områdekode identifiserer for eksempel om produktet opprinnelige ble kjøpt i en butikk, om det ble anskaffet som et evalueringseksempler, om det er anskaffet gjennom et Microsoft Volume Licensing-program eller ble forhåndsinstallert av en PC-produsent.
- Installasjonsdatoen og hvorvidt installasjonen var vellykket.

Eksterne tilkoblinger

Tilkoblinger til RemoteApp og skrivebord

Tilkobling til eksternt skrivebord

Logg på med en Microsoft-konto

OneDrive-nettlagring

Synkroniser innstillingene

Teredo-teknologi

TPM-tjenester (Trusted Platform Module)

Oppdater rotsertifikater

Oppdateringstjenester

Virtuelt privat nettverk

Windows Program for forbedret kundeopplevelse (CEIP)

Windows Defender

Windows-feilrapportering

Windows Filtilknytning

Windows Hjelp

Remote Assistance

Windows Search

- Informasjon som bekrefter at produktnøkkelen for Windows ikke har blitt endret.
- PCens merke og modell.
- Versjonsinformasjon om operativsystem og programvare.
- Innstillinger for region og språk.
- Et unikt tall som kalles en globalt unik identifikator (GUID) som er tilordnet PCen.
- Produktnøkkel (hashet) og produkt-ID.
- BIOS-navn, revisjonsnummer og revisjonsdato.
- Serienummer for harddiskvolum (hashet).
- Resultatet av aktiveringskontrollen. Dette inkluderer feilkoder og informasjon om aktiveringsutnyttelser og beslektet skadelig eller uautorisert programvare som blir funnet eller deaktivert:
    - Aktiveringsutnyttelsens ID.
    - Aktiveringsutnyttelsens gjeldende status, for eksempel renset eller satt i karantene.
    - PC-produsentens ID.
    - Aktiveringsutnyttelsens filnavn og hash-kode, og i tillegg en hash-kode for beslektede programvarekomponenter som kan angi tilstedeværelse av en aktiveringsutnyttelse.
- 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 datamaskinen sendes også.
- Hvis du bruker en volumlisensiert utgave av Windows som bruker en aktiveringsserver, blir IP-adressen for serveren sendt til Microsoft.

**Bruk av informasjon**

Installasjonsprogram for Windows

Windows-ressurs

Windows SmartScreen

Windows Talegjenkjenning

Windows Store

Tjenesten Windows Time

Windows Feilsøking

Arbeidsmapper

Arbeidsplass

Microsoft bruker informasjonen til å bekrefte at du har en lisensiert versjon av programvaren. Microsoft bruker ikke informasjonen til å kontakte enkeltkunder. Lisensserverinformasjon brukes for å sikre at lisensservere overholder lisensavtalen.

**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. For å kunne 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

Annonse-ID

**Hva denne funksjonen gjør**

Windows gir apper tilgang til en unik ID for hver bruker på en enhet for å levere mer relevante annonser. Du kan tilbakestille eller deaktivere tilgang til denne IDen når som helst.

**Informasjon som samles inn, behandles eller overføres**

Hvis du gir apper tilgang til annonse-IDen, vil Windows gi denne informasjonen til alle apper som ber om den. Apper kan lagre eller sende denne informasjonen.

**Bruk av informasjon**

Annonse-IDen brukes av apputviklere og reklamenettverk for å levere mer relevante annonser til deg ved å forstå hvilke apper du bruker og hvordan du bruker dem. Den kan også brukes av apputviklere til å forbedre tjenestekvaliteten ved å la dem fastslå hyppigheten og effektiviteten til annonser og oppdage svindel- og sikkerhetsproblemer.

Hvis du gir apper tilgang til annonse-IDen, er hver apps bruk av IDen underlagt appens personvernpraksis.

**Valg og kontroll**

Hvis du velger hurtiginnstillinger når du konfigurerer Windows, vil Windows la apper bruke annonse-IDen. Hvis du velger å tilpasse innstillingene, kan du styre tilgangen til annonse-IDen ved å velge **La apper bruke annonse-IDen for opplevelser på tvers av apper** under **Del informasjon med Microsoft og andre tjenester**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under

**Personvern** i PC-innstillinger. Hvis du deaktiverer denne innstillingen, sendes ikke annonse-IDen til apper som ber om den. Hvis du velger å aktivere innstillingen, blir det generert en ny ID.

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

Biometri

### Hva denne funksjonen gjør

Hvis PCen har en fingeravtrykksleser, kan du logge på Windows med fingeravtrykket ditt og identifisere deg for apper som støtter funksjonen.

### Informasjon som samles inn, behandles eller overføres

Når du setter opp et nytt fingeravtrykk, lagres avlesningene av fingeravtrykket lokalt på PCen din. Det sendes ingen informasjon til Microsoft. Når du bruker fingeravtrykket ditt til å identifisere deg for en app, sammenligner Windows fingeravtrykket med de lagrede fingeravtrykkene på PCen, og informerer appen om det skannede fingeravtrykket samsvarer med det som er knyttet til kontoen din. Windows gir ikke dataene til det skannede fingeravtrykket til appen.

### Bruk av informasjon

Windows bruker fingeravtrykksinformasjonen du velger å lagre på PCen, til å logge deg på Windows ved hjelp av fingeravtrykket ditt.

### Valg og kontroll

Du kan legge til eller fjerne fingeravtrykk i **Påloggingsalternativer** i **Kontoer** i PC-innstillinger.

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 MicrosoftOneDrive. 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 hashet 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 gjenopprettingsnøklene 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.

Du kan vise og administrere -gjenopprettingsnøklene som er lagret på OneDrive-kontoen.

Øverst på siden

Kontakter

**Hva denne funksjonen gjør**

Hvis du bruker Personer-appen eller en støttet tredjepartsapp til å håndtere kontaktene dine, kan du velge å dele bestemte kontakter med andre apper på PCen, vise kontaktinformasjon i et kontaktkort eller dele spesifikk kontaktinformasjon med andre apper på PCen for å utføre en handling, for eksempel foreta et anrop eller kartlegge en adresse.

**Informasjon som samles inn, behandles, lagres og overføres**

Når en app ber om kontaktinformasjon, lar Windows deg velge de bestemte kontaktene du vil dele med appen. Kontakter kan komme fra Personer-appen eller en støttet kontaktapp fra en tredjepart. Windows deler ikke hele kontaktlisten din med appen som ber om kontaktinformasjon.

Hvis en app har tilgang til bestemt informasjon om noen av kontaktene dine, for eksempel et telefonnummer eller en e-postadresse, kan Windows vise et kontaktkort med den ytterligere informasjonen for kontakten fra kontaktsinformasjonsappen. Windows deler ikke den ytterligere kontaktinformasjonene med appen som viser kontaktkortet.

Hvis du trykker eller klikker en kommando, for eksempel **Samtale**, **E-post**eller **Kart** , på kontaktkortet, åpner Windows den aktuelle appen for å utføre denne handlingen og gir tilgang til appen med

kontaktinformasjonen som er nødvendig for å fullføre handlingen, for eksempel telefonnummeret som skal ringes.

**Bruk av informasjon**

Windows bruker kontaktinformasjonen fra kontaktappen til å dele bestemte kontakter du velger, for å vise kontaktkort, åpne apper og dele kontaktinformasjon for å fullføre handlinger som er oppført på kontaktkortene, og for å vise kontaktene dine i Windows Search. Personer-appen bruker informasjon om kontaktene dine som beskrevet i personvernerklæringen for kommunikasjonsapper.

Hvis du deler kontaktinformasjon med en tredjepartsapp, vil måten appen bruker informasjonen på, være underlagt tredjepartens personvernpraksis. Hvis du deler kontaktinformasjon med en Microsoft-app, blir appens personvernpraksis beskrevet i personvernerklæringen for appen.

**Valg og kontroll**

Windows viser og deler kontaktinformasjon bare når du velger å dele bestemte kontakter med en app, viser et kontaktkort eller velger en handling fra kontaktkortet.

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 fullstendig funksjonalitet og brukeropplevelse på enheten. Hvis

enhetsprodusenten har levert en app for enheten, kan Windows automatisk laste ned og installere appen fra Windows Store hvis du er logget på Store.

**Informasjon som samles inn, behandles eller overføres**

Når Windows søker etter drivere, søkes det på Windows Update-tjenesten på Internett for å finne og laste ned enhetsdrivere, hvis en riktig driver ikke allerede er tilgjengelig på PCen. 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 en enhetsapp er tilgjengelig, laster Windows ned og installerer den fra Windows Store automatisk. Appen blir tilgjengelig på Windows Store-kontoen i listen over apper du eier.

**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 som er sendt, til å identifisere eller kontakte deg.

**Valg og kontroll**

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du automatisk nedlasting og installasjon av enhetsdrivere, enhetsinformasjon og enhetsapper. Hvis du velger å tilpasse innstillingene, kan du kontrollere automatisk nedlasting og installasjon av enhetsdrivere, apper og informasjon ved å velge **Hent enhetsdrivere, apper og informasjon for nye enheter automatisk** under **Beskytt og oppdater PCen**. 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, selv om du kanskje trenger appen for å kunne 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 hurtiginnstillinger 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, kan det hende at informasjon om PCen, for eksempel dens navn og nettverksadresse, kringkastes over lokalnettet, slik at andre 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 antall 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 nettverkssøk skal aktiveres i det hele tatt, og om automatisk konfigurasjon av nettverkstilkoblede enheter skal aktiveres, ved å velge **Endre innstillinger for avansert deling** i Nettverks- og delingssenter.

# Pare trådløse enheter

**Hva denne funksjonen gjør**

Windows lar deg pare 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, kringkaster Windows PCens navn via Bluetooth, slik at Bluetooth-aktiverte enheter kan oppdage og identifisere PCen.

Når du velger **Legg til en enhet** i 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 pares 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

Enhetskryptering

**Hva denne funksjonen gjør**

Enhetskryptering er med på å beskytte dataene ved hjelp av BitLocker-stasjonskryptering. Dette kan bidra til å forhindre frakoblede programvareangrep. Når du aktiverer enhetskryptering, krypterer Windows dataene på stasjonen der Windows er installert.

**Informasjon som samles inn, behandles eller overføres**

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

Windows bruker TPM (Trusted Platform Module) på PCen til å lagre og behandle de kryptografiske nøklene som brukes til å kryptere stasjonen. Når enhetskryptering er aktivert, krypterer Windows installasjonsstasjonen for Windows automatisk, og det blir generert en gjenopprettingsnøkkel. Gjenopprettingsnøkkelen gir deg tilgang til de beskyttede dataene i tilfelle det oppstår bestemte maskinvarefeil eller andre problemer.

BitLocker-gjenopprettingsnøkkelen for PCen sikkerhetskopieres automatisk til MicrosoftOneDrive-kontoen på Internett for hver administratorkonto som er koblet til en Microsoft-konto.

Datamaskinnavnet og en identifikator for gjenopprettingsnøkkelen blir også sikkerhetskopiert til samme OneDrive-konto. For å beskytte personvernet ditt blir informasjonen sendt kryptert via SSL.

**Bruk av informasjon**

Kryptografiske nøkler og GUIDer (globalt unik identifikator) lagres i minnet på PCen å støtte BitLocker-operasjoner. Ved hjelp av gjenopprettingsinformasjon får du tilgang til de beskyttede dataene dine i tilfelle det oppstår bestemte maskinvarefeil eller andre problemer, og BitLocker kan skille mellom autoriserte og uautoriserte brukere.

Microsoft sikkerhetskopierer gjenopprettingsinformasjonen til OneDrive-kontoen din slik at du har tilgang til informasjonen på Internett. Vi bruker ikke informasjonen om gjenopprettingsnøkkelen, og vi lagrer den ikke andre steder enn på denne OneDrive-kontoen. Vi kan bruke aggregerte data om gjenopprettingsnøkler til å analysere trender og forbedre våre produkter og tjenester. Vi kan for eksempel bruke informasjonen til å finne proporsjonene for PCer der enhetskryptering er aktivert.

**Valg og kontroll**

Hvis du velger å bruke en Microsoft-konto når du konfigurerer PCen og PCen støtter dette, aktiveres enhetskryptering, og gjenopprettingsnøkkelen blir sikkerhetskopiert til OneDrive-kontoen din. Hvis du velger å bruke en lokal konto når du konfigurerer PCen, deaktiveres enhetskryptering.

Hvis du senere kobler en Microsoft-konto til en administratorkonto på PCen:

- Hvis enhetskryptering ikke allerede er aktivert, aktiverer Windows dette automatisk og sikkerhetskopierer gjenopprettingsinformasjonen til brukerens OneDrive-konto.
- Hvis enhetskryptering allerede er aktivert, blir gjenopprettingsinformasjonen for PCen sikkerhetskopiert til brukerens OneDrive-konto.

Du kan vise og administrere gjenopprettingsnøklene som er lagret på OneDrive-kontoen, her.

Øverst på siden

DirectAccess

**Hva denne funksjonen gjør**

DirectAccess gjør at PCen uten problemer kan koble til nettverket på arbeidsplassen eksternt når PCen er koblet til Internett, uansett 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 Gruppepolicy. 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

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.

Utsagnene omfatter følgende:

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

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 hendelseslogginformasjon via Internett hvis du ikke samtykker i at den sendes. Administratorer kan bruke Gruppepolicy 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 forelderen 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 forelderen.

## 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 aktivitetsinnloggingsinformasjon 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 forelderen 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 faksserver.

**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 brukerkontorettighetene på PCen. Hvis ikke en faksadministrator har endret tilgangsinnstillingene, 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

Håndskrifttilpasning – automatisk læring

### Hva denne funksjonen gjør

Automatisk læring er et tilpasningsverktøy for håndskriftgjenkjenning som er tilgjengelig på PCer med berøring eller tavlepenn. Denne funksjonen samler inn data om ordene du bruker, og hvordan du skriver dem. Dette bidrar til at programvaren for håndskriftgjenkjenning kan forbedre tolkningen av håndskriftstilen og vokabularet, og det forbedrer også automatisk korrigering og tekstforslag 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.

Informasjonen som samles inn, inkluderer:

- Tekst fra meldinger du skriver og kalenderoppføringer du

oppretter ved hjelp av e-postapper (for eksempel Office Outlook eller Windows Live E-post), inkludert meldinger du allerede har sendt.

- Bokstaver du skriver i Inndatapanel.
- Gjenkjent tekst fra håndskrift du skriver i Inndatapanel eller skriver på berøringstastatur.
- Alternative tegn du velger for å korrigere den gjenkjente teksten.

**Bruk av informasjon**

Informasjonen som samles inn, brukes til å forbedre håndskriftgjenkjenning ved at det lages en versjon av gjenkjenningsprogramvaren som er tilpasset til din egen stil og ditt eget vokabular. Den brukes også til å aktivere automatisk korrigering og tekstforslag mens du skriver på berøringstastatur.

Teksteksemplene brukes til å opprette en utvidet ordliste. Håndskrifteksemplene brukes til å forbedre håndskriftgjenkjenning 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 strømme 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 enhver PC i hjemmegruppen. Når du slutter deg til en hjemmegruppe, deles kontoinformasjon (inkludert e-postadresse, visningsnavn og bilde) for alle Microsoft-kontoer på PCen med andre i hjemmegruppen for å aktivere deling med disse brukerne.

### 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** under **Nettverk** i PC-innstillinger.

Øverst på siden

IME (Input Method Editor)

Microsoft IME (Input Method Editor) brukes sammen 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.

## Kandidater til skybasert IME

### Hva denne funksjonen gjør

Når du bruker Microsoft Pinyin IME til å angi forenklede kinesiske tegn, kan IMEen bruke en onlinetjeneste til å søke etter ideogrammer for innskrevne data som ikke finnes i en lokal ordliste på PCen.

### Informasjon som samles inn, behandles eller overføres

Når du skriver inn forenklede kinesiske tegn ved hjelp av Microsoft Pinyin IME, foreslår IMEen ideogrammer du kan bruke. Hvis IMEen ikke finner et godt forslag i den lokale ordlisten, sender den tastaturinndataene til Microsoft for å finne ut om det finnes bedre ideogrammer for inndataene. Hvis det finnes bedre forslag, vises de i

listen over kandidater og legges til i den lokale ordlisten hvis du velger det. En tilfeldig generert unik identifikator sendes også for å hjelpe oss med å analysere bruken av denne funksjonen. Identifikatoren er ikke knyttet til Microsoft-kontoen, og brukes ikke til å identifisere, kontakte eller sende reklame til deg.

### Bruk av informasjon

Microsoft bruker den innsamlede informasjonen til å slå opp skyideogrammer og forbedre produktene og tjenestene våre. Vi bruker dem ikke til å identifisere, kontakte eller sende reklame til deg.

### Valg og kontroll

Kandidater til skybasert IME er deaktivert som standard for Microsoft Pinyin IME for forenklet kinesisk. Du kan vise eller endre denne innstillingen ved å åpne PC-innstillinger, klikke **Klokke, språk og område**, klikke **Region og språk**, velge språk, og deretter klikke **Alternativer**.

## 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

Funksjonene for automatisk læring og tekstforslag er aktivert som

standard i IMEer 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 feilkonverteringsrapport. Du kan også når som helst sende en konverteringsfeilrapport fra verktøyet for IME-feilkonverteringsrapport. 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 programvareversjonsnummeret 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

Deling av Internett-tilkobling

### Hva denne funksjonen gjør

Med deling av Internett-tilkobling kan du dele den mobile bredbåndstilkoblingen med andre enheter via Wi-Fi. Du kan også starte deling av Internett-tilkobling eksternt på enheten for mobilt bredbånd fra PCen hvis du er logget på begge med samme Microsoft-konto.

### Informasjon som samles inn, behandles eller overføres

Når du deler Internett-tilkoblingen for første gang, genererer og lagrer Windows automatisk et nettverksnavn og passord. Du kan når som helst endre disse.

Hvis PCen støtter dette og du har lagt til PCen på Microsoft-kontoen som en klarert enhet, synkroniserer Windows nettverksnavnet og passordet til Microsoft-kontoen. Windows synkroniserer også annen informasjon for å la deg starte deling av Internett-tilkobling eksternt fra andre klarerte enheter. Denne informasjonen inkluderer Bluetooth-

radioens maskinvareadresse og et tilfeldig nummer som brukes for å sikre tilkoblingen.

**Bruk av informasjon**

Denne informasjonen brukes til å konfigurere deling av Internett-tilkobling. Microsoft bruker ikke informasjonen til å identifisere, kontakte eller sende reklame til deg.

**Valg og kontroll**

Hvis du logger på en enhet som støtter deling av Internett-tilkobling med Microsoft-kontoen, og du legger til enheten som en klarert enhet, synkroniseres informasjonen som er nødvendig for å starte deling av Internett-tilkobling eksternt, til OneDrive. Du kan stoppe synkronisering av informasjonen ved å velge ikke å synkronisere passord. Hvis du vil ha mer informasjon, kan du se delen Synkroniser innstillingene på denne siden.

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 velge **Aktiver eller deaktiver Windows-funksjoner**.

Øverst på siden

Språkinnstillinger

**Hva denne funksjonen gjør**

Du kan legge til språkene du foretrekker å bruke, i språklisten i Windows 8.1. 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 foretrukne 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 foretrukne 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

Windows Posisjonstjenester lar deg avgjøre hvilke apper, nettsteder og Windows-funksjoner som har tillatelse til å fastslå PCens posisjon. Windows Posisjonstjenester består av to komponenter. Windows Lokasjonstjeneste kobler til en Microsoft-nettjeneste for å fastslå posisjonen din. Windows Location-plattform fastslår posisjonen til PCen ved hjelp av maskinvare (for eksempel en GPS-sensor) eller 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, og enkelte Windows-funksjoner, be om tillatelse til å fastslå PCens posisjon. Hvis du lar en app bruke posisjonen din, kan Windows Location-plattformen angi for appen når PCen flytter seg innenfor eller utenfor geografiske grenser som er angitt i appen, i tillegg til å gi posisjonen din når du bruker appen. En app kan for eksempel la deg angi en påminnelse om å handle dagligvarer når du slutter på arbeid. Avhengig av systemkonfigurasjonen kan Windows Location-plattformen fastslå posisjonen til PCen ved hjelp av maskinvare (for eksempel en GPS-sensor) eller programvare (for eksempel Windows Lokasjonstjeneste).

Windows Location-plattformen hindrer ikke at apper kan fastslå PCens posisjon på andre måter. Du kan for eksempel installere enheter (for eksempel en GPS-mottaker) som kan sende posisjonsinformasjon direkte til en app og omgå plattformen. Nettjenester kan bruke din IP-adresse til å fastslå omtrentlig posisjon, vanligvis byen PCen befinner seg i, uavhengig av innstillingene for Windows Location-plattformen.

### Informasjon som samles inn, behandles eller overføres

Windows Location-plattformen sender ikke selv noen informasjon fra PCen din, men enkeltstående lokasjonstjenester (for eksempel Windows Lokasjonstjeneste) kan overføre informasjon når Windows Location-plattformen ber dem om å fastslå PCens posisjon. Apper, nettsteder og funksjoner som er godkjent for å bruke plattformen til å fastslå PCens posisjon, kan også sende eller lagre den informasjonen.

Hvis en app konfigurerer geografiske grenser som skal overvåkes, blir disse grensene lagret kryptert på PCen. Informasjonen som lagres om disse grensene, omfatter et navn, en posisjon og om PCen var innenfor eller utenfor grensen sist gang posisjonen ble fastslått. Apper som konfigurerer geografiske grenser kan overføre eller lagre denne informasjonen.

**Bruk av informasjon**

Hvis du aktiverer Windows Location-plattformen, vil godkjente apper, nettsteder og Windows-funksjoner få tilgang til PCens posisjon og bruke den til å gi deg tilpasset innhold. Hvis du bruker en tredjeparts app eller posisjonstjeneste, vil tjenestens bruk av PCens posisjon 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 hurtiginnstillinger mens du konfigurerer Windows, aktiverer du Windows Location-plattformen. Hvis du velger å tilpasse innstillingene, kan du styre Windows Location-plattformen ved å velge La Windows og apper be om posisjonen min fra Windows Location-plattformen under Del informasjon med Microsoft og andre tjenester. Første gang hver Store-app ber om PCens posisjon, vil Windows spørre om du vil tillate at appen bruker din posisjon. Du kan vise og endre denne innstillingen for hver Store-app under Tillatelser i innstillingene for appen.

Hvis du bruker en skrivebordsapp som bruker Windows Location-plattformen, skal den be om din tillatelse til å bruke PCens posisjon, og når den bruker PCens posisjon, vil det vises et ikon i systemstatusfeltet for å varsle deg om at PCens posisjon har blitt brukt. Hver bruker kan styre sine egne posisjonsinnstillinger for apper under **Personvern** i PC-innstillinger. I tillegg kan administratorer velge å deaktivere Location-plattformen for alle brukere under **Plasseringsinnstillinger** i Kontrollpanel. Hvis du vil hindre at apper blir varslet når geografiske grenser, som er angitt av apper, blir krysset, kan en administratorbruker deaktivere Windows Location Framework Service i Kontrollpanel.

# Windows Lokasjonstjeneste

**Hva denne funksjonen gjør**

Windows Lokasjonstjeneste kobler til Microsoft Location Service på Internett for å finne den omtrentlige posisjonen til PCen basert på Wi-Fi-nettverk i nærheten av PCen samt PCens IP-adresse.

**Informasjon som samles inn, behandles eller overføres**

Når en app du har tillatt å motta posisjonen din, ber om det, vil Windows Location-plattformen be alle installerte posisjonstjenester (inkludert Windows Lokasjonstjeneste) om å finne din gjeldende posisjon. Windows Lokasjonstjeneste sjekker først om den har en liste over Wi-Fi-tilkoblingspunkter i nærheten lagret fra en tidligere spørring fra en app som forstår posisjonsinformasjon. Hvis det ikke allerede finnes en liste over Wi-Fi-tilgangspunkt i nærheten, eller listen er utdatert, sender leverandøren informasjon om Wi-Fi-tilgangspunkt i nærheten og GPS-informasjon (hvis tilgjengelig) til Microsoft Lokasjonstjeneste. Tjenesten sender din PCs omtrentlige posisjon tilbake til leverandøren, som videresender posisjonen til Windows Location-plattformen, slik at den i sin tur kan videresende den til appen som forespurte PCens posisjon. 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. For å bidra til å ivareta personvernet for eiere av Wi-Fi-nettverk sender ikke Windows informasjon om SSIDer (navn på Wi-Fi-tilgangspunkt) eller om skjulte Wi-Fi-nettverk. Av hensyn til personvern og sikkerhet sendes informasjon om Wi-Fi-nettverk kryptert via SSL.

Hvis du velger å hjelpe til med å forbedre Microsoft Location Service, kan det hende at Windows sender informasjon om nærliggende Wi-Fi-

tilgangspunkt til Microsoft på nytt etter at en app har bedt om posisjonen til PCen din. Hvis du bruker en Internett-tilkobling med forbruksmåling, begrenser Windows antallet ganger informasjonen sendes per dag, dette for å begrense bruken av Internett-tilkoblingen.

**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 være med på å forbedre Microsoft Location Service, blir informasjonen som sendes til Microsoft om Wi-Fi og GPS, brukt til å forbedre Microsofts posisjonstjenester, noe som igjen forbedrer posisjonstjenestene som leveres til appene dine. Microsoft lagrer ikke innsamlede data som kan brukes til å identifisere, kontakte eller sende reklame til deg eller til å spore PCen eller opprette en posisjonslogg for den.

**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 kan kontrollere om apper kan be om posisjonen til PCen din, kan du se delen om Windows Location-plattformen. Hvis du autoriserer apper til å be om posisjonen 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 innstillingene, kan du angi om du vil være med på å forbedre Microsoft Location Service. Det gjør du ved å velge **Send noen plasseringsdata til Microsoft når plassavhengige apper brukes** under **Hjelp til med å forbedre produktene og tjenestene til Microsoft**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under Plasseringsinnstillinger i Kontrollpanel. Hvis du velger ikke å være med på å forbedre tjenesten, kan du fortsatt bruke Windows Lokasjonstjeneste til å fastslå den omtrentlige posisjonen til PCen.

Du kan aktivere og deaktivere Windows Lokasjonstjeneste ved å åpne

**Aktiver eller deaktiver Windows-funksjoner** i Kontrollpanel. Hvis du deaktiverer Windows Location-plattformen, kan du fremdeles bruke andre lokasjonstjenester (for eksempel GPS) med Windows Location-plattformen.

Øverst på siden

Administrere legitimasjonen

**Hva denne funksjonen gjør**

Med Windows kan du koble Windows Store-apper til kontoer du bruker for nettsteder. Hvis du tidligere har lagret et passord for et nettsted i Internet Explorer, kan Windows bruke det lagrede passordet når du kobler en app til nettstedet.

**Informasjon som samles inn, behandles eller overføres**

Når en app ber deg om legitimasjon for å logge på et nettsted, kan du velge å lagre legitimasjonen. Hvis du allerede har logget på nettstedet i Internet Explorer og har valgt å lagre legitimasjonen, fyller Windows automatisk ut den lagrede legitimasjonen. Legitimasjonen lagres kryptert på PCen. Hvis du vil ha mer informasjon om hvordan denne og annen legitimasjon kan synkroniseres til OneDrive, kan du se delen Synkronisere innstillingene på denne siden.

**Bruk av informasjon**

Windows bruker bare den lagrede legitimasjonen til å hjelpe deg med å logge på nettstedene du har valgt. Hvis du lagrer legitimasjonen mens du kobler en app til et nettsted, vil ikke den lagrede legitimasjonen bli brukt i Internet Explorer eller andre apper.

**Valg og kontroll**

Du kan administrere lagret legitimasjon i Legitimasjonsbehandling i Kontrollpanel. Hvis du vil ha mer informasjon om hvordan denne og annen legitimasjon kan synkroniseres til OneDrive, kan du se delen Synkronisere innstillingene på denne siden.

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 vises under **Din konto** i **Kontoer** 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 sende 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 omfatter for eksempel brukerhovednavnet (som jack@contoso.com) og DNS-domenenavnet (som 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, vil hvordan appen bruker navnet og kontobildet ditt være 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 tilgangen til navnet og kontobildet ved å velge **La apper bruke navnet og kontobildet mitt** under **Del informasjon med Microsoft og andre tjenester**. Etter at du har konfigurert Windows, kan du angre endringen av denne innstillingen under **Personvern** i PC-innstillinger. Du kan endre

kontobildet under **Kontoer** i PC-innstillinger. Du kan også velge å tillate at enkelte apper endrer kontobildet.

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 varslingene 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 den elektroniske tjenesten til en app 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 deaktivere varslinger for alle apper eller hver enkelt app i **Varslinger** under **Søk og apper** 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 Windows Store-apper kan vise status og varslinger på skjermen når PCen din er låst. Låseskjermapper kan også utføre oppgaver mens PCen er låst. De kan for eksempel synkronisere e-post eller la deg svare på innkommende telefonsamtaler. Du kan også bruke PCens kamera direkte fra låseskjermen.

### 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 E-post-, Kalender- og Skype-appene automatisk som låseskjermapper. Du kan legge til eller fjerne disse eller andre apper fra låseskjermen og deaktivere bruken av kameraet i **Låseskjerm** under **PC og enheter** 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 varslinger på låseskjermen, under **Varslinger** under **Søk og apper** 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 den elektroniske tjenesten til en app 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 Filutforsker. 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

Forhåndshenting og forhåndsstart

**Hva denne funksjonen gjør**

Windows bidrar til at apper og Windows-funksjoner starter raskere ved å holde rede på når og hvor ofte appene og funksjonene brukes og hvilke systemfiler de laster inn.

**Informasjon som samles inn, behandles eller overføres**

Når du bruker en app eller Windows-funksjon, lagrer Windows noe informasjon på PCen om systemfilene som er brukt, og når og hvor ofte appen eller funksjonen er brukt.

**Bruk av informasjon**

Windows bruker informasjonen om app- og funksjonsbruk for å gjøre det raskere å starte apper og funksjoner. I noen tilfeller kan apper startes automatisk i en deaktivert tilstand.

**Valg og kontroll**

Apper som startes og deaktiveres automatisk, vises i Oppgavebehandling og kan avsluttes. Mens disse appene er deaktivert, får de ikke tilgang til webkameraet eller mikrofonen før du starter dem, selv om du tidligere har aktivert denne funksjonaliteten.

Øverst på siden

Program Compatibility Assistant

### Hva denne funksjonen gjør

Hvis det oppstår kompatibilitetsproblemer med en skrivebordsapp du prøver å kjøre, prøver Program Compatibility Assistant å hjelpe deg med å løse det.

### 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 Filutforsker 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 nærfeltskommunikasjon (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 informasjon om Bluetooth-paring, 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 websiden 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 nærhetstjenesten for nærfelt er aktivert, aktiveres Trykk og send også. 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 verts-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 ingen informasjon sendes 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 URL-adressen 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.

Hvis Microsoft er vert for PCen eller appen du kobler til, kan tilleggsinformasjon om tilkoblingen bli sendt til Microsoft av hensyn til kundestøtte.

**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. Ingen informasjon sendes til Microsoft med mindre Microsoft er vert for den eksterne tilkoblingen.

**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 **Få tilgang til RemoteApp og skrivebord**, og deretter skrive inn en tilkoblings-URL-adresse i dialogboksen. Du kan også bruke e-postadressen til å hente tilkoblings-URL-adressen. 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.

Øverst på siden

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. En liste lagres i registret. Denne listen lagres permanent med mindre den slettes av en administrator. Ingen informasjon sendes til Microsoft med mindre Microsoft er vert for den eksterne tilkoblingen.

**Bruk av informasjon**

Informasjon som samles inn av Tilkobling til eksternt skrivebord, lar deg koble til verts-PCer som kjører Eksterne skrivebordstjenester, 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) består av én enkelt e-postadresse og ett enkelt passord du kan bruke til å logge på apper, områder og tjenester fra Microsoft og utvalgte 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 logge på Windows med en Microsoft-konto eller velge å koble den lokale kontoen eller domenekontoen til en Microsoft-konto på produkter som støtter det. 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 et nettsted der du bruker en Microsoft-konto til pålogging, vil Windows også logge deg på nettstedet automatisk.

**Informasjon som samles inn, behandles eller overføres**

Når du angir en e-postadresse som skal brukes som en Microsoft-konto, under konfigurasjonen av PCen eller under **Kontoer** i PC-innstillinger, sender Windows e-postadressen til Microsoft for å finne ut om det allerede eksisterer en Microsoft-konto tilknyttet denne 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, kan det hende at vi først spør deg om mer sikkerhetsinformasjon, for eksempel et mobiltelefonnummer 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.

Når du logger på med en Microsoft-konto, sender Windows også standardinformasjon om datamaskinen til Microsoft, inkludert maskinvareprodusent, modellnavn og versjon.

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 en domenekonto som er tilknyttet Microsoft-kontoen:

- Enkelte Windows-innstillinger vil bli synkronisert mellom PCene du logger på med Microsoft-kontoen. Hvis du vil ha mer informasjon om hvilke innstillinger som synkroniseres og hvordan du styrer dem, kan du se avsnittet Synkronisere innstillingene på

denne siden.

- Microsoft-apper som bruker en Microsoft-konto til godkjenning (for eksempel E-post, Kalender, Personer, 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 Bing.com, kan du bli logget på automatisk uten at du må angi passordet for Microsoft-kontoen).

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. Siden domeneadministratorer har tilgang til informasjon på PCen din, vil de også ha tilgang til innstillinger og informasjon du har valgt å synkronisere med andre PCer via Microsoft-kontoen. Dette kan være innstillinger som navn, kontobilde og nettleserlogg. Hvis du vil ha mer informasjon om hvilke innstillinger som synkroniseres og hvordan du styrer dem, kan du se avsnittet Synkronisere innstillingene på denne siden.

**Bruk av informasjon**

Når du oppretter en ny Microsoft-konto i Windows, bruker vi informasjonen du oppgir, til å opprette og beskytte kontoen. Sikkerhetsinformasjonen (som telefonnummer eller alternativ e-postadresse) du angir, 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 ha mer informasjon om innvirkningen på personvernet ved å ha en Microsoft-konto, kan du lese personvernerklæringen for Microsoft-kontoer. Hvis du vil ha informasjon om hvordan individuelle Microsoft-apper bruker informasjon som er tilknyttet Microsoft-kontoen, kan du se personvernerklæringen for hver enkelt app. Du finner personvernerklæringen for en Microsoft-app ved å åpne Innstillinger i

appen eller i dialogboksen Om.

Standard enhetsinformasjon kan bli brukt til å tilpasse visse typer kommunikasjon til deg, for eksempel e-post med informasjon om hvordan du kommer i gang med enheten.

**Valg og kontroll**

Når du logger på Windows med en Microsoft-konto, synkroniseres noen innstillinger automatisk. Se delen Synkroniser innstillingene på denne siden hvis du vil lære hvordan du endrer hvilke Windows-innstillinger som synkroniseres, eller stopper synkroniseringen. 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 kan når som helst opprette en lokal konto eller Microsoft-konto i **Kontoer** i PC-innstillinger på produkter som støtter det. Hvis du logger på Windows med en domenekonto, kan du når som helst koble til eller koble fra Microsoft-kontoen under **Kontoer** 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

OneDrive-nettlagring

**Hva denne funksjonen gjør**

Når du logger på med en Microsoft-konto på enheten, kan du velge å automatisk lagre bestemt innhold og innstillinger til Microsoft-servere, slik at du har en sikkerhetskopi hvis noe skjer med enheten.

**Informasjon som samles inn, behandles eller overføres**

Hvis du under installasjonen velger å bruke OneDrive til nettlagring, vil Windows automatisk sende innhold til Microsoft-servere, herunder:

- Bilder og videoer på enheten som er lagret i **kamerabildemappen** .
- Innstillinger som gjelder for enheten, og som ikke er delt mellom enhetene.

- Beskrivelsesinformasjon for enheten, for eksempel enhetsnavn og -type.

Du kan også velge å lagre innhold på Microsoft-servere, og apper kan velge å bruke Microsoft-servere som standard lagringsplassering for filene.

**Bruk av informasjon**

Windows bruker dette innholdet til å levere nettlagringstjenesten. Microsoft bruker ikke innholdet eller informasjonen til å identifisere, kontakte eller sende reklame til deg.

**Valg og kontroll**

Hvis du velger "Bruk OneDrive" når du konfigurerer PCen, vil Windows lagre innholdet som er beskrevet i dette avsnittet, på OneDrive. Du kan endre disse innstillingene når som helst i OneDrive-delen i PC-innstillinger.

Øverst på siden

Synkroniser innstillingene

**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. Når du har logget på én eller flere PCer med en Microsoft-konto og deretter logger på en annen PC med samme Microsoft-konto første gang, laster Windows ned og bruker innstillingene og informasjonen du velger å synkronisere fra de andre PCene. 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 enkelte innstillinger med Microsoft-servere. Disse innstillingene omfatter følgende:

- Oppsettet for startskjermen

- Apper du har installert fra Windows Store
- Språkinnstillinger
- Hjelpemiddelinnstillinger
- Tilpassingsinnstillinger, for eksempel kontobildet, låseskjermbildet, bakgrunnen og museinnstillingene
- Innstillinger for Windows Store-apper
- Ordlister for stavekontroll, IME-ordlister og personlige ordlister
- Nettleserlogg, favoritter og åpne nettsteder
- Lagrede passord for apper, nettsteder og nettverk
- Adresser for delte nettverksskrivere som du er tilkoblet

For å beskytte personvernet ditt blir alle synkroniserte innstillinger sendt kryptert via SSL. 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. Siden domeneadministratorer har tilgang til informasjon på PCen din, vil de også ha tilgang til innstillinger og informasjon du har valgt å synkronisere med andre PCer via Microsoft-kontoen.

**Bruk av informasjon**

Windows 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, synkroniseres innstillingene som standard. Du kan velge å synkronisere innstillingene og angi hva som skal synkroniseres, ved å gå til **Synkroniser innstillingene** i delen OneDrive 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 version 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 om Internet Protocol version 6, Teredo og relaterte teknologier 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 enhetskryptering, 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 brukerhandlinger, 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, opprettelsesbrukeren og opprettelsesdatoen for å gjøre det enklere å gjenkjenne filen.

I et domenemiljø 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-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. Enhetskryptering 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 også 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 tilbakestille 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.

**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 støtteprogramvare, f.eks. drivere fra enhetsprodusenter.
- **Microsoft Update** er en tjeneste som sender deg

programvareoppdateringer for Windows-programvare og annen Microsoft-programvare, for eksempel Microsoft Office.

**Informasjon som samles inn, behandles eller overføres**

Informasjonen som oppdateringstjenestene samler inn fra PCen, gjør det mulig for Microsoft å drive og forbedre tjenestene, for eksempel følgende:

- Microsoft-programvaren og annen støtteprogramvare (for eksempel drivere og fastvare som leveres av enhetsprodusenter) som er installert på PCen, og som oppdateringstjenestene har oppdateringer for. Dette hjelper oss med å finne ut hvilke oppdateringer du trenger.

- Konfigurasjonsinnstillingene for Windows Update og/eller Microsoft Update, for eksempel om du vil at oppdateringer skal lastes ned og installeres automatisk.

- Om tilgangen til og bruken av oppdateringstjenestene er vellykket, mislykket eller forårsaker feil.

- Plug and Play-ID-nummer for maskinvareenheter – en kode som er tilordnet av enhetsprodusenten og identifiserer enheten (for eksempel en bestemt type tastatur).

- Globalt unik identifikator (GUID) – et tilfeldig generert nummer som ikke inneholder personlige opplysninger. GUIDer brukes til å identifisere individuelle PCer uten å identifisere brukeren.

- BIOS-navn, revisjonsnummer, leverandør og revisjonsdato – informasjon om settet med vesentlige programvarerutiner som tester maskinvaren, starter operativsystemet på PCen og overfører data mellom maskinvareenheter som er koblet til PCen.

- Produsent, modell, plattformrolle og SKU-nummer – informasjon om PCen for bruk i forbindelse med diagnostikk av driverinstallasjon.

Hvis du vil bruke disse oppdateringstjenestene, går du til Windows Update i Kontrollpanel og ser etter oppdateringer eller endrer innstillingene for å tillate at Windows automatisk installerer oppdateringer etter hvert som de blir tilgjengelige (anbefales). I

Windows Update-funksjonen kan du velge om du vil bruke Microsoft Update.

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 søk etter skadelig programvare blir det sendt en rapport til Microsoft med spesifikk informasjon om den skadelige programvaren som blir funnet, feil og annen informasjon om PCen. Hvis du vil ha mer informasjon, kan du lese personvernerklæringen for Windows Verktøy for fjerning av skadelig programvare .

**Bruk av informasjon**

Dataene som sendes til Microsoft, blir brukt til å drive og vedlikeholde oppdateringstjenestene. Dataene brukes også til å generere samlet statistikk som hjelper oss med å analysere trender og forbedre produkter og tjenester, inkludert oppdateringstjenestene.

Oppdateringstjenestene genererer samlet statistikk ved å bruke den innsamlede GUIDen til å spore og registrere hvor mange enkeltmaskiner som bruker oppdateringstjenestene, og finne ut om nedlasting og installasjon av bestemte oppdateringer var vellykket eller mislykket. Oppdateringstjenestene registrerer GUIDen for datamaskinen som prøvde å laste ned og installere oppdateringer, IDen til det forespurte elementet, om oppdateringer var tilgjengelige samt standard datamaskininformasjon.

MSRT-informasjonen som er beskrevet ovenfor, brukes til å hjelpe oss med å forbedre beskyttelsen mot skadelig programvare og andre sikkerhetsprodukter og -tjenester. Ingen informasjon i MSRT-rapportene blir brukt til å identifisere eller kontakte deg.

**Nødvendige oppdateringer**

Hvis du aktiverer oppdateringstjenestene, må du fra tid til annen oppdatere enkelte programvarekomponenter som utgjør eller er direkte knyttet til oppdateringstjenestene på systemet, for at

tjenestene skal fungere som de skal. Disse oppdateringene må utføres før tjenestene kan se etter, laste ned eller installere andre oppdateringer. De nødvendige oppdateringene retter feil, sørger for løpende forbedringer og opprettholder kompatibilitet med Microsoft-serverne som støtter tjenestene.

Hvis oppdateringstjenestene er deaktivert, vil du ikke motta disse oppdateringene.

Programvareoppdateringer som er nødvendig for å installere eller oppdatere Windows Store-apper, blir lastet ned og installert automatisk. Disse oppdateringene må utføres for at apper skal fungere riktig.

**Informasjonskapsler og tokener**

Et token ligner en informasjonskapsel. Det lagrer informasjon i en liten fil som er plassert på harddisken av oppdateringstjenesteserveren, og brukes når datamaskinen kobles til denne serveren for å opprette en gyldig tilkobling. Tokenet lagres bare på datamaskinen, ikke på serveren. Informasjonskapselen eller tokenet inneholder informasjon (for eksempel tidspunkt for siste skanning) for å finne de nyeste oppdateringene. Det inneholder også informasjon som angir hvilket innhold som skal lastes ned til datamaskinen, når nedlastingen skal skje samt en GUID for å identifisere datamaskinen på serveren.

Innholdet i informasjonskapselen eller tokenet krypteres av serveren (med unntak av utløpstiden for informasjonskapselen eller tokenet). Informasjonskapselen eller tokenet er ikke en informasjonskapsel for nettleser og kan derfor ikke styres med nettleserinnstillingene. Informasjonskapselen eller tokenet kan ikke fjernes, men hvis du ikke bruker oppdateringstjenestene, brukes heller ikke informasjonskapselen eller tokenet.

**Valg og kontroll**

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiveres Windows Update-tjenesten og konfigureres til å installere oppdateringer automatisk.

Hvis du aktiverer oppdateringstjenestene, uansett hvilken innstilling du har valgt, blir nødvendige oppdateringer til enkelte tjenestekomponenter lastet ned og installert automatisk uten at du

varsles ytterligere. Hvis du ikke vil motta nødvendige oppdateringer, deaktiverer du oppdateringstjenestene.

Du kan også velge om systemet skal se etter eller automatisk installere viktige og anbefalte oppdateringer for datamaskinen, eller bare viktige oppdateringer. Valgfrie oppdateringer installeres aldri automatisk. Etter konfigurasjonen av Windows kan du endre innstillingene for Windows Update i Kontrollpanel eller PC-innstillinger.

Hvis du har valgt å se etter og installere viktige oppdateringer og motta MSRT som en del av disse oppdateringene for datamaskinen, kan du deaktivere programvarens rapporteringsfunksjonalitet.

Øverst på siden

Virtuelt privat nettverk

**Hva denne funksjonen gjør**

Med et virtuelt privat nettverk (VPN) kan du koble til et privat nettverk, for eksempel et firmanettverk, via Internett. En VPN-tilkobling kan leveres av Windows VPN-klienten, eller av en VPN-app fra en tredjepart.

**Informasjon som samles inn, behandles eller overføres**

Når du kobler til et VPN, sendes legitimasjonen du angir i VPN-klienten, til det eksterne nettverket. Du kan kanskje lagre denne legitimasjonen på PCen. Når du er koblet til, rutes noe eller all nettverksaktivitet via det eksterne nettverket, avhengig av hvordan VPN er konfigurert. Administratorer kan konfigurere bestemte apper slik at trafikken alltid rutes gjennom VPN, og slik at de alltid kobles til VPN når disse appene startes. Det sendes ingen informasjon til Microsoft.

VPN-programvare fra tredjeparter kan samle inn tilleggsinformasjon. Innsamling og bruk av denne informasjonen er underlagt tredjepartens personvernpraksis.

**Bruk av informasjon**

VPN-klienter bruker legitimasjonen du oppgir, til å godkjenne deg på det eksterne nettverket, og til å rute nettverkstrafikk til og fra det eksterne nettverket. Hvis en VPN-klient fra en tredjepart samler inn

tilleggsinformasjon, er tredjepartens bruk av denne informasjonen underlagt tredjepartens personvernpraksis.

**Valg og kontroll**

Du kan legge til eller fjerne en VPN-tilkobling og se statusen til eksisterende tilkoblinger under **Nettverk** i PC-innstillinger. Når en VPN-tilkobling er konfigurert, kan du koble den til eller fra manuelt ved å velge nettverket fra listen i Innstillinger.

Øverst på siden

Windows Program for forbedret kundeopplevelse (CEIP)

**Hva denne funksjonen gjør**

Windows-programmet for forbedret kundeopplevelse kan samle inn informasjon om hvordan du bruker appene dine, PCene dine, tilkoblede enheter og Windows. Det kan også samle inn informasjon om problemer som kan oppstå med ytelse og pålitelighet. 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, herunder hvor mange prosessorer PCen din har, antallet nettverksforbindelser i bruk, skjermoppløsninger for skjermenheter og hvilken versjon av Windows som kjører på PCen.

- Ytelses- og pålitelighetsinformasjon, som for eksempel hvor raskt en app svarer når du trykker en knapp, hvor mange problemer du opplever med en app eller en enhet, og hvor raskt informasjon blir sendt eller mottatt over en nettverksforbindelse.

- Appbrukinformasjon, inkludert informasjon om 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 kan også inneholde informasjon om hendelser (hendelsesloggdata) på PCen fra opptil sju dager før du velger 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. Hvis du mottar enkeltstående IDer, bruker ikke Microsoft dem til å identifisere eller kontakte deg.

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. Noen rapporter fra programmet for forbedret kundeopplevelse kan også inneholde GUIDer som er avledet fra din Microsoft-konto.

CEIP kan også regelmessig laste 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 komprimert CEIP-informasjon med Microsoft-partnere slik at de kan forbedre sine produkter og tjenester, men den delte informasjonen 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-apper fra Windows Store kan sende CEIP-rapporter for alle brukere på PCen. Hvis du velger å tilpasse innstillingene, kan du kontrollere programmet for forbedret kundeopplevelse ved å velge **Send informasjon til Microsoft om hvordan jeg bruker PCen min, som en del av programmet for forbedret kundeopplevelse** under **Hjelp til med å forbedre produktene og tjenestene til Microsoft**. Etter konfigurasjonen av Windows kan administratorer endre denne innstillingen i **Handlingssenter** i Kontrollpanel.

Hvis du vil ha mer informasjon, kan du se vanlige spørsmål om Program for forbedret kundeopplevelse.

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

Hvis du bruker Windows Defender, kan Microsoft Active Protection Service (MAPS) bidra til bedre beskyttelse av PCen ved automatisk å laste ned nye signaturer for nyoppdaget, skadelig programvare og overvåke sikkerhetsstatusen for PCen. MAPS vil sende informasjon om skadelig programvare og andre former for potensielt uønsket programvare til Microsoft, og kan også sende filer som inneholder skadelig programvare. Hvis MAPS oppdager at PCen er infisert med bestemte typer skadelig programvare, kan MAPS automatisk kontakte deg via din Microsoft-konto for å bidra til å løse problemet.

**Informasjon som samles inn, behandles eller overføres**

MAPS-rapporter omfatter informasjon om potensielt skadelige programvarefiler, for eksempel filnavn, kryptografisk hash, programvareutgiver, størrelse og datostempler. MAPS kan i tillegg samle inn fullstendige URL-adresser for å angi opphavet til filene og IP-adressene som de potensielt skadelige filene kobler til. Disse URL-adressene kan i enkelte tilfeller inneholde personlig informasjon som søkeord eller data som er angitt 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 hjelp 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 iverksetter tiltak mot skadelig programvare når den oppdages (som et ledd i den automatiske viderebehandlingen).
- Windows Defender fullfører et planlagt søk og utfører tiltak automatisk i forhold til programvare som oppdages basert på dine innstillinger.
- Windows Defender skanner en ActiveX-kontroll i Internet Explorer.

Hvis du velger å bli med i MAPS når du konfigurerer Windows, deltar du med et grunnleggende medlemskap. Rapporter for grunnleggende medlemskap inneholder informasjonen beskrevet i dette avsnittet. Rapporter for avansert medlemskap er mer omfattende og kan av og til inneholde personlige opplysninger, 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 for skadelig programvare blir deretter opprettet, og de oppdaterte definisjonene blir gjort tilgjengelige for alle brukere via Windows Update.

Hvis du blir med i MAPS, kan det hende Windows Defender sender bestemte filer eller nettinnhold fra PCen som Microsoft mistenker kan være potensielt uønsket programvare. Eksempelrapporten brukes til videre analyse. Hvis en fil mest sannsynlig inneholder personlige opplysninger, blir du spurt før den sendes. Hvis Windows Update ikke kan hente oppdaterte signaturer for Windows Defender i en periode, prøver Windows Defender å bruke MAPS til å laste ned signaturer fra en alternativ nedlastingsplassering.

For å beskytte personvernet ditt blir all informasjon til MAPS sendt kryptert via SSL.

Windows Defender sender regelmessig informasjon til MAPS om sikkerhetsnivået til PCen for å bidra til å oppdage og reparere bestemte typer infeksjoner av skadelig programvare. Dette omfatter informasjon om PCens sikkerhetsinnstillinger og loggfiler som beskriver drivere og programvare som lastes inn når datamaskinen starter. Det sendes også en unik identifikator som identifiserer PCen.

**Bruk av informasjon**

Rapporter som sendes til MAPS, brukes til å forbedre Microsoft-programvaren og -tjenestene. Rapportene kan også bli brukt til statistiske formål og andre test- eller analyseformål, og til å generere 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.

Informasjonen om PCen sikkerhetsnivå, som MAPS samler inn, brukes til å fastslå om bestemte typer skadelig programvare har infisert PCen. I slike tilfeller bruker Microsoft kontaktinformasjonen i din Microsoft-konto til å kontakte deg med detaljer om problemet og hvordan du kan løse det.

**Valg og kontroll**

Hvis du velger hurtiginnstillinger mens du konfigurerer Windows, aktiverer du MAPS. Hvis du velger å tilpasse innstillingene, kan du

styre MAPS ved å velge **Få bedre beskyttelse mot skadelig programvare ved å sende informasjon og filer til Microsoft Active Protection Service når Windows Defender er aktivert** under **Del informasjon med Microsoft og andre tjenester**. Etter konfigurasjonen av Windows kan du endre MAPS-medlemskap eller -innstillinger, for eksempel deaktivere MAPS, på **Innstillinger** -menyen i Windows Defender.

Hvis du mottar Verktøy for fjerning av skadelig programvare gjennom Windows Update, kan det hende det sender lignende informasjon til MAPS selv om Windows Defender er deaktivert. Hvis du vil ha mer informasjon, kan du lese personvernerklæringen for Windows Verktøy for fjerning av skadelig programvare .

# 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. Noen løsninger vil også være inkludert i oppdateringspakker og fremtidige versjoner av programvaren for å bidra til å forhindre problemer med programvaren og gjøre den mer pålitelig.

**Informasjon som samles inn, behandles eller overføres**

Mange programvareprodukter er utformet til å fungere med Windows-feilrapportering. Hvis det oppstår et problem med ett av disse produktene, kan du bli spurt om du ønsker å rapportere det.

Windows-feilrapportering samler inn informasjon som er nyttig for analyse og løsing av et problem som har oppstått, for eksempel hvor i programvaren eller maskinvaren problemet oppstod, problemets type eller alvorsgrad, 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 kan omfatte navn på appens kjørbare filer. Informasjon om enheter og drivere kan omfatte navn på enhetene som er installert på PCen, og de kjørbare filene som er knyttet til disse enhetsdriverne. Det kan hende det blir samlet inn informasjon om firmaet som publiserte en app eller driver.

Hvis du velger å aktivere automatisk rapportering under konfigurasjonen av Windows, vil rapporteringstjenesten automatisk sende grunnleggende informasjon om hvor problemer oppstår. I

enkelte tilfeller vil rapporteringstjenesten automatisk sende tilleggsinformasjon for å bidra til å diagnostisere problemet, for eksempel et øyeblikksbilde av en del av PC-minnet. Enkelte feilrapporter kan utilsiktet inneholde visse personopplysninger. En rapport som inneholder et øyeblikksbilde av PC-minnet, kan for eksempel omfatte navnet ditt, deler av et dokument du jobbet på, eller data du nettopp sendte inn til et nettsted.

Det kan hende at Windows-feilrapportering oppretter en rapport som inneholder tilleggsinformasjon, for eksempel loggfiler, for å bidra til å diagnostisere bestemte typer problemer. Før det blir sendt en rapport som inneholder denne tilleggsinformasjonen, vil Windows spørre om du vil sende rapporten, selv om du har aktivert automatisk rapportering.

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 ingen personlige opplysninger.

For å beskytte personvernet ditt blir informasjonen sendt kryptert via SSL.

**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 vi bruke 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 på nettet etter løsninger på problemer** under **Se etter løsninger på Internett**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under Handlingssenter i Kontrollpanel.

Hvis du vil ha mer informasjon, kan du se personvernerklæringen for Microsoft-feilrapporteringstjenesten.

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 bestem 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 Hjelp og støtte på weben er slått på for Windows, 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 nettstedsdata**, 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 (HEIP) 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 PC over tid. GUIDen inneholder ingen 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 finne ut hvor utbredte problemene vi mottar tilbakemeldinger om, 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 med hensikt inn informasjon som kan brukes til å identifisere deg personlig. Hvis du skriver inn slike opplysninger i søke- eller tilbakemeldingsboksen, blir opplysningene sendt, men Microsoft bruker dem ikke 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 innstillingene, kan du angi innstillinger for produktforbedringsprogrammet for Hjelp ved å velge **Send informasjon til Microsoft om hvordan jeg bruker Hjelp, som en del av produktforbedringsprogrammet for Hjelp** under **Hjelp til med å forbedre produktene og tjenestene til Microsoft**. Etter at du har konfigurert Windows, kan du endre denne innstillingen i Windows Hjelp og støtte.

Øverst på siden

Remote Assistance

**Hva denne funksjonen gjør**

Du kan bruke Fjernhjelp til å invitere noen til å koble til datamaskinen din og hjelpe deg med et PC-problem, selv om 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 datamaskinen din med Fjernhjelp, kan denne personen se skrivebordet og eventuelle

åpne dokumenter, inkludert eventuell privat informasjon som vises. 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. Når tilkoblingen 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 merket for disse alternativene i innstillingene for Fjernhjelp.

Øverst på siden

Windows Search

**Hva denne funksjonen gjør**

Med Windows Search kan du søke på enheten og på Internett fra ett sted. Det kan hende at Windows Search bruker Bing og Windows Location-plattformen for å levere bedre søkeresultater. Vær oppmerksom på at andre søkefunksjoner på enheten leveres av Microsoft, for eksempel søk i Windows Store, Internet Explorer, og andre Microsoft-produkter.

**Informasjon som samles inn, behandles eller overføres**

Hvis du velger å hente nettsøkresultater, sender Windows det du skrev i Windows Search, til Microsoft. Det kan også hende at Windows Search sender informasjon til Microsoft om hvordan du samhandler med funksjonen for å bidra til å forbedre søkeresultatene. Windows Search sender også en ID for å levere tilpassede søkeresultater basert på din samhandling med Bing og andre Microsoft-produkter og -

tjenester. Hvis du logger på Windows med en Microsoft-konto, vil IDen bli tilknyttet din Microsoft-konto. Du kan velge ikke å tilpasse resultatene i Windows Search, og da sendes ikke denne IDen.

Hvis du lar Windows Search bruke posisjonen din, vil den fysiske posisjonen til enheten, som angitt av Windows Location-plattformen, bli sendt til Microsoft som en del av hver søkeforespørsel. Det kan også hende vil prøver å fastslå din omtrentlige fysiske posisjon basert på IP-adressen.

Når du bruker Windows Search til å søke i en app, sendes søkeordene til appen.

**Bruk av informasjon**

Hvis du velger å bruke Windows Search til å få nettsøkresultater, bruker vi søkeordet du angav, søkeloggen lokalt og på nettet, informasjon tilknyttet din Microsoft-konto og posisjonen til enheten, for å levere relevante søkeforslag, tilpassede søk og tilpassede opplevelser i andre Microsoft-produkter og -tjenester. Hvis du vil lære mer om hvordan dataene brukes, kan du lese personvernerklæringen for Bing.

Når du bruker Windows Search til å søke 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**

Hvis du velger hurtiginnstillinger når du konfigurerer Windows, tillater du at Windows Search henter søkeforslag og nettresultater og at Microsoft bruker data fra Windows Search (herunder posisjon) for å tilpasse Windows Search og andre Microsoft-opplevelser. Hvis du velger å tilpasse innstillinger, kan du avgjøre om du vil endre disse innstillingene for Windows Search. Etter konfigurasjonen av Windows kan du endre disse innstillingene under **Søk** i PC-innstillinger.

Du kan slette den lokale søkeloggen og deler av Bing-søkeloggen som brukes til å tilpasse Windows Search-opplevelsen i **Søk** i **Søk og apper** i PC-innstillinger. Hvis du sletter søkeloggen, angir du at Microsoft ikke skal bruke noen tidligere innsamlede søkelogger til å tilpasse søkeforslag eller søkeresultater. Dette sletter ikke reklame

eller annen informasjon om bruk av personlige data (herunder informasjon avledet fra søkeloggen). Det sletter heller ikke aggregert informasjon som brukes av Microsoft til å forbedre søkeresultater og andre Microsoft-opplevelser. Denne informasjonen beholdes og anonymiseres som beskrevet i personvernerklæringen for Bing. Du kan administrere Microsoft-reklame og annen informasjon om bruk av personlige data på nettet.

Øverst på siden

Installasjonsprogram for Windows

Dette avsnittet beskriver funksjoner som er tilgjengelig som en del av installasjonsprosessen for Windows.

# Dynamisk oppdatering

**Hva denne funksjonen gjør**

Dynamisk oppdatering gjør det mulig for Windows å utføre en engangssjekk i Windows Update for å få tak i de siste oppdateringene til PCen din 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 innboksdriver.** Viktige driveroppdateringer for versjonen av Windows du installerer.

Hvis du installerer Windows fra Windows Store, vil Dynamisk oppdatering i tillegg laste ned og installere de nyeste oppdateringene for Windows og bestemte maskinvaredrivere som PCen behøver.

**Bruk av informasjon**

Dynamisk oppdatering sender informasjon til Microsoft om maskinvaren på PCen for å kunne finne de riktige driverne for systemet.

### Valg og kontroll

Hvis du installerer Windows fra Windows Store, vil installasjonsprogrammet automatisk laste ned og installere oppdateringer. Hvis du installerer Windows fra et fysisk medium, blir du spurt om du vil koble til Internett for å installere oppdateringer.

## Program for installasjonsforbedring

### Hva denne funksjonen gjør

Denne funksjonen sender én rapport til Microsoft med grunnleggende informasjon om PCen din og hvordan du installerte Windows. Microsoft bruker denne informasjonen til å forbedre installasjonsopplevelsen og finne løsninger på vanlige installasjonsproblemer.

### Informasjon som samles inn, behandles eller overføres

Rapporten omfatter generelt sett opplysninger om din installasjonsopplevelse, f.eks. dato for installasjon, tiden det tok hver installasjonsfase å fullføre, om installasjonen var en oppgradering eller en ny installasjon av produktet, versjonsdetaljer, operativsystemets språkinnstillinger, medietype, PC-konfigurasjon og om installasjonen var vellykket eller mislykket, sammen med eventuelle feilmeldinger.

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 GUID til å samholde disse dataene med data samlet inn av Windowss Program for forbedret kundeopplevelse (CEIP), et program du kan velge å delta i når du bruker Windows.

### Valg og kontroll

Du kan velge å delta i programmet når du installerer Windows ved å velge **Jeg vil gjøre Windows-installasjonen bedre** .

Hvis du vil ha mer informasjon, kan du se avsnittet Program for forbedret kundeopplevelse for Windows.

## Kompatibilitetskontroll for installasjon

### Hva denne funksjonen gjør

Når du installerer Windows, hjelper installasjonsprogrammet deg med å fastslå om den gjeldende PCen er klar for oppgradering til Windows 8.1, og gir kompatibilitetsinformasjon om programmene og enhetene dine.

### Informasjon som samles inn, behandles eller overføres

Ved fastslåelse av kompatibilitet samler vi inn bestemte opplysninger om hva slags oppgradering du trenger, for eksempel maskinvarens kapasitet, enhetene du har koblet til datamaskinen, og programmene som er installert på den. Av og til kan det hende at opplysninger om programutgiveren inneholder informasjon som utgiverens navn eller e-postadresse.

### Bruk av informasjon

Vi bruker informasjonen vi samler inn, til å finne de riktige driverne for PCen og finne ut om PCen, programmene og enhetene dine er kompatible med Windows 8.1. Vi kan også bruke den til å forbedre produktene og tjenestene. Vi bruker ikke denne informasjonen til å identifisere, kontakte eller sende reklame til deg.

### Valg og kontroll

Hvis du installerer Windows fra Windows Store eller fra et fysisk medium i en eksisterende Windows-installasjon, sendes informasjonen som er beskrevet i denne delen, til Microsoft. Hvis du starter fra et fysisk installasjonsmedium for å installere Windows, ser ikke installasjonsprogrammet etter kompatibilitetsinformasjon på Internett.

Øverst på siden

### Hva denne funksjonen gjør

Du kan bruke Windows Del 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 stoppe lagringen av denne informasjonen eller slette alle lagrede mål i **Del** under **Søk og apper** i PC-innstillinger.

Øverst på siden

## Windows SmartScreen

### Hva denne funksjonen gjør

Windows SmartScreen bidrar til å holde PCen sikker ved å kontrollere nedlastede filer og nettinnhold i apper for å beskytte deg mot skadelig programvare og potensielt usikkert nettinnhold. Windows viser en advarsel før en nedlastet fil som er ukjent eller potensielt usikker, blir åpnet. Hvis SmartScreen oppdager potensielt usikkert nettinnhold i en app, vil Windows vise en advarsel i stedet for innholdet.

### Informasjon som samles inn, behandles eller overføres

Hvis du velger å bruke Windows SmartScreen til å kontrollere nedlastede filer, sender Windows informasjon til SmartScreen-nettjenesten. Denne informasjonen kan omfatte et filnavn, en filidentifikator (hash-kode) og informasjon om digitale sertifikater samt standard PC-informasjon og versjonsnummeret for Windows SmartScreen. Informasjonen krypteres via SSL før den sendes til Microsoft slik at personvernet beskyttes.

Hvis du velger å bruke Windows SmartScreen til å blokkere potensielt usikkert innhold i apper, sender Windows informasjon til SmartScreen-nettjenesten, herunder adressene og typen innhold som noen Windows Store-apper har tilgang til når du bruker dem. Nettjenesten sender svar til PCen som angir om innholdet som er rapportert til Microsoft, er usikkert eller mistenkelig. Rapporter som blir sendt til Microsoft, omfatter informasjon som navn eller identifikator for appen, og fullstendige adresser for nettinnhold som appen bruker.

For å ivareta personvernet krypteres informasjonen som sendes til Microsoft. Informasjon som kan være tilknyttet en webside som åpnes i en app, for eksempel søkeord, kan være inkludert i adressen som sendes til Microsoft. Hvis du for eksempel slår opp et ord i en ordbokapp, kan ordet du slo opp, kanskje bli sendt 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.

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.

**Bruk av informasjon**

Microsoft bruker informasjonen som er beskrevet ovenfor, til å sende deg varsler om potensielt usikre, nedlastede filer og innhold i apper. Hvis SmartScreen for eksempel oppdager en potensiell fare i en app som støtter SmartScreen, vil Windows vise en advarsel i stedet for innholdet. Vi bruker også informasjonen til å forbedre SmartScreen og andre produkter og tjenester. Microsoft bruker ikke informasjonen til å 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 **Bruk nettjenester for SmartScreen til å beskytte mot skadelig innhold på nettsteder som lastes inn av Windows Store-apper og Internet Explorer, og skadelige nedlastinger** under **Beskytte PCen og ditt personvern**. Etter at du har konfigurert Windows, kan du endre denne innstillingen under Handlingssenter i Kontrollpanel. Hvis du vil ha informasjon om Internet ExplorerSmartScreen, kan du se avsnittet SmartScreen-filter i personvernerklæringen for Internet Explorer.

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 dokumentgjennomgang i Windows Talegjenkjenning er aktivert, blir tekst fra Microsoft Office Word-dokumenter (med DOC- eller DOCX-filtypen) og e-post (fra alle e-postmapper unntatt Slettede elementer og Søppelpost) på PCen og på eventuelle tilkoblede delte filressurser som er inkludert i Windows-søkeindeksplasseringer, samlet inn og lagret i fragmenter på ett, to eller 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. Profilinformasjonen 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 tilpasningsdata som ble brukt til tilpasning 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**(Help improve speech recognition). 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 foretar appinterne kjøp med Store-kontoen.

- Apper du har installert. Listen over apper du har installert fra Store, 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 evalueringsversjon, 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.

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 nettsteder analyserer surfedataene til besøkende.

**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 varsling i Store, og flisen 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.

## Automatiske appoppdateringer

### Hva denne funksjonen gjør

Denne funksjonen ser etter, laster ned og installerer oppdateringer for Windows Store-apper for å sikre at du har de nyeste versjonene. Appoppdateringer kan omfatte sikkerhetsoppdateringer, ytelsesoppdateringer eller nye funksjoner og nytt innhold. 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 lære om funksjonsendringer på siden for produktbeskrivelse for appen i Windows Store.

### Informasjon som samles inn, behandles eller overføres

For å levere automatiske appoppdateringer sender Store følgende informasjon til Microsoft:

- En liste over alle appene som er installert fra Store av alle brukerne på PCen.
- Lisensinformasjonen for hver app.
- Om oppdateringene for appene fra Store var vellykket, mislykket eller forårsaket feil
- Globalt unik identifikator (GUID) – et tilfeldig generert nummer som ikke inneholder personlige opplysninger.
- BIOS-navn, revisjonsnummer og revisjonsdato
- Grunnleggende informasjon om PCen, for eksempel produsent, modell og Windows-utgaven du bruker

### Bruk av informasjon

Denne informasjonen brukes til å levere oppdateringstjenesten. Dataene brukes også til å generere samlet statistikk som hjelper oss med å analysere trender og forbedre produkter og tjenester. De brukes ikke til å identifisere, kontakte eller sende reklame til deg.

### Valg og kontroll

Hvis du velger hurtiginnstillinger når du konfigurerer Windows, vil Windows Store automatisk se etter, laste ned og installere appoppdateringer, selv om du er logget av Windows Store. Hvis du deaktiverer automatiske appoppdateringer, kan du velge om du vil installere en appoppdatering når du logger på Windows Store.

Slik deaktiverer du automatiske appoppdateringer:

1. Åpne Windows Store.
2. Sveip inn fra høyre kant på skjermen, og trykk deretter **Innstillinger**.

   Hvis du bruker en mus, plasserer du markøren nederst til høyre på skjermen, og deretter klikker du **Innstillinger**.
3. Trykk eller klikk **Appoppdateringer**.
4. Trykk eller klikk **Oppdater appene automatisk** for å deaktivere automatiske appoppdateringer.

Hvis du vil lære mer om hva den nyeste versjonen av appen kan gjøre og når en app sist ble oppdatert, kan du se gjennom siden for produktbeskrivelse for appen i Windows Store.

## 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 gjennom 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
- Biblioteker for bilder, videoer, musikk eller dokumenter. Gjør at appen kan få tilgang til, endre eller slette filer i bibliotekene dine. Dette omfatter tilgang til eventuelle tilleggsdata som er innebygd i disse filene, for eksempel posisjonsinformasjon 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.
- Windows-legitimasjonen din. Gjør at appen kan bruke legitimasjonen din 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 kan når som helst endre om appen kan bruke den.

I tillegg til tillatelsene ovenfor gjelder at hvis en app ber om informasjon fra en enhet som lagrer informasjon om deg eller oppførselen din, spør Windows deg om du vil tillate appen å bruke den. Hvis du for eksempel kobler en trimenhet som sporer posisjonen din, spør Windows deg om du vil tillate at appen får tilgang til 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. Du kan gjøre dette ved å åpne appen, åpne **Innstillinger**og deretter velge **Tillatelser**.

## Tilpasset Store-søk og appanbefalinger

### Hva denne funksjonen gjør

Når du blar eller søker etter apper i Windows Store, gir Microsoft anbefalinger og søkeresultater for å hjelpe deg med å finne apper som er relevante for deg.

### Informasjon som samles inn, behandles eller overføres

Windows Store sender informasjon til Microsoft om hvordan du samhandler med den, inkludert hva du søker etter og hvilke søkeresultater du velger, for å bidra til å forbedre søkeresultatene. Windows Store sender også en ID knyttet til Microsoft-kontoen for å gi tilpassede søkeresultater basert på samhandlingene dine med Bing og andre Microsoft-produkter og -tjenester. Du kan velge ikke å tilpasse resultatene, og da sendes ikke denne IDen.

### Bruk av informasjon

Store bruker IDen knyttet til Microsoft-kontoen for å gi tilpassede søkeresultater og anbefalinger basert på din samhandling med Store og andre Microsoft-produkter og -tjenester, for eksempel Bing og Windows Phone Store. Dette omfatter informasjon om for eksempel apper du har kjøpt, profilinformasjon du har angitt i Microsoft-kontoen, og dine vurderinger av apper. Denne informasjonen kan også brukes til å tilpasse andre Microsoft-produkter og -tjenester.

### Valg og kontroll

Når du er logget på Windows med en Microsoft-konto, er tilpassede resultater og anbefalinger for Windows Store aktivert som standard. Du kan velge ikke å få tilpassede resultater og anbefalinger fra Store i **Innstillinger** -delen i Store-innstillinger.

## Bidra til å forbedre Windows Store ved å sende URL-adresser for nettinnhold som apper bruker

### Hva denne funksjonen gjør

Noen apper fra Store fungerer som nettsteder og kan utsette datamaskinen for potensielt usikker programvare, for eksempel skadelig programvare. Hvis du velger å slå denne funksjonen på,

samler den inn informasjon om nettinnholdet som ble brukt av disse appene til å hjelpe Microsoft med å analysere potensielt utrygg virkemåte. Microsoft 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 nettinnholdet 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 URL-adresser som appen går til, og fullstendige URL-adresser 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 URL-adresser 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 **Bruk nettjenester for SmartScreen til å beskytte mot skadelig innhold på nettsteder som lastes inn av Windows Store-apper og Internet Explorer, og skadelige nedlastinger** under **Hjelp til med å forbedre produktene og tjenestene til Microsoft**. 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**

Informasjonen brukes av tjenesten Windows Time til å synkronisere klokken på PCen automatisk.

**Valg og kontroll**

Tjenesten Windows Time er aktivert som standard. Du kan deaktivere denne funksjonen under **Dato og klokkeslett** i PC-innstillinger. Hvis du deaktiverer tjenesten Windows Time, har ikke dette noen direkte virkning på apper eller andre tjenester, men klokken på 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 vil feilsøkingsresultater, går du til Feilsøking i Kontrollpanel. Klikk **Vis logg**, velg et resultat, og klikk deretter **Slett**.

Øverst på siden

Arbeidsmapper

**Hva denne funksjonen gjør**

Arbeidsmapper er mapper på PCen som synkroniseres automatisk med filserveren på arbeidsplassen.

**Informasjon som samles inn, behandles, lagres eller overføres**

Når du lagrer en fil i en arbeidsmappe, synkroniseres filen automatisk til en filserver som administreres av arbeidsplassen. Filer som lagres i arbeidsmappen fra andre PCer, synkroniseres til PCen.

**Bruk av informasjon**

Windows sender og mottar filene i arbeidsmappene for å holde mappene synkronisert. Bruk av informasjonen som er lagret på serverne på arbeidsplassen, er underlagt arbeidsplassens personvernpolicy.

**Valg og kontroll**

Du kan administrere PCens tilkobling til arbeidsmapper under **Arbeidsplass** i PC-innstillinger.

Øverst på siden

Arbeidsplass

Med Arbeidsplass kan du koble enheten til Windows Intune (krever et eget abonnement fra Microsoft) eller en annen tredjepartstjeneste for enhetsbehandling. Hvis du tillater at firmaadministratoren din kan administrere PCen ved å bruke Arbeidsplass, kan han eller hun utføre oppgaver som for eksempel å håndheve sikkerhetspolicyer, installere apper, vise bestemte konfigurasjoner og annen informasjon på PCen samt utføre andre administrasjonsoppgaver. Se firmaets personvernpolicy, eller sjekk med systemadministratoren for å få mer informasjon om firmaets bruk av denne funksjonen.

**Informasjon som samles inn, behandles eller overføres**

Når du konfigurerer og bruker Arbeidsplass, kommuniserer PCen med enhetsbehandlingstjenesten firmaet bruker, som Microsoft kan være vert for. Legitimasjonen du angir for å koble til arbeidsplassen, sendes til tjenesten.

**Bruk av informasjon**

Informasjonen som sendes til enhetsbehandlingstjenesten, brukes til å opprette en tilkobling mellom tjenesten og PCen og til å la deg installere en selvbetjeningsappen fra Windows Store. Se selskapets personvernpolicy, eller sjekk med systemadministratoren for å få mer

informasjon om selvbetjeningsappen.

**Valg og kontroll**

Hvis firmaet bruker Arbeidsplass, kan du koble til eller fra i Arbeidsplass i PC-innstillinger under **Nettverk**. Når du har koblet PCen til tjenesten, kan du vise informasjon om tilkoblingen eller koble fra når som helst.

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 8.1 og Windows Server 2012 R2



Vær oppmerksom på at denne siden er et tillegg til personvernerklæringen for Windows 8.1 og Windows Server 2012 R2 ("personvernerklæring for Windows"), som har følgende deler:

- Hovedpunkt
- Erklæring, som er hele personvernerklæringen for Windows 8.1, inneholder koblinger til personvernerklæringer for Windows-funksjoner med egne frittstående erklæringer
- Funksjonstillegg, som beskriver funksjonene som har innvirkning på personvern i Windows 8.1 og Windows Server 2012 R2
- **Apptillegg** (denne siden), som beskriver appene som har innvirkning på personvern i Windows 8.1, og inneholder koblinger til personvernerklæringer som gjelder for hver app
- Servertillegg, som beskriver tilleggsfunksjonene som har innvirkning på personvern i Windows Server 2012 R2

For å forstå datainnsamlingen og bruksprаksisen som er relevant for

en bestemt funksjon eller tjeneste i Windows, bør du lese hele personvernerklæringen og aktuelle tillegg eller frittstående erklæringer.

Hvis du valgte å delta i programmet for forbedret kundeopplevelse (CEIP) da du konfigurerte PCen, samler disse appene inn informasjon i en rapport om hvordan du bruker hver app, i tillegg til appens ytelse og pålitelighet. Microsoft bruker informasjonen i programmet for forbedret kundeopplevelse til å forbedre produktene og tjenestene sine. Informasjonen vil ikke bli brukt til å identifisere, kontakte eller sende reklame til deg. Du kan deaktivere Program for forbedret kundeopplevelse i PC-innstillinger. Hvis du vil ha mer informasjon, kan du se Personvernerklæring for Program for forbedret kundeopplevelse.

Følgende koblinger går til personvernerklæringer som gjelder for hver av de oppførte appene:

Alarm

Kalkulator

Kalender

Kamera

Økonomi

Mat

Spill

Helse

Hjelp og tips

Mail

Kart

Musikk

Nyheter

Personer

Leser

Leseliste

Skann

Skype

Lydinnspilling

Sport

Reise

Video

Vær

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 8.1 og Windows Server 2012 R2



På denne siden



Denne siden er et tillegg til personvernerklæringen for Windows 8.1 og Windows Server 2012 R2 ("personvernerklæring for Windows"). Personvernerklæringen har følgende deler:

- Hovedpunkt
- Erklæring, som er hele personvernerklæringen for Windows 8.1, og som inneholder koblinger til personvernerklæringer for Windows-funksjoner med egne frittstående erklæringer
- Funksjonstillegg, som beskriver funksjonene som har innvirkning på personvern i Windows 8.1 og Windows Server 2012 R2
- Apptillegg, som beskriver appene som påvirker personvernet i Windows 8.1
- **Servertillegg** (denne siden), som beskriver tilleggsfunksjonene som har innvirkning på personvern i Windows Server 2012 R2

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

feilrapportering (WER)

Software Inventory Logging

personvernerklæringen for Windows og aktuelle tillegg. I tillegg bør du lese denne hvitboken for administratorer.

Hvis du vil ha informasjon om hvilken innvirkning funksjoner som er inkludert i Windows Server 2012 R2 Essentials, har på personvernet, kan du se personvernerklæringen for Windows Server 2012 R2 Essentials og Windows Server Essentials Experience.

UAL (User Access Logging)

**Hva denne funksjonen gjør**

UAL (User Access Logging) samler inn og aggregerer poster med klientforespørsler for serverroller (både bruker- og enhetsforespørsler) og installerte produkter (hvis de 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 poster med unike klientforespørsler er kritiske.

**Informasjon som samles inn, behandles eller overføres**

IP-adresser, brukernavn og i enkelte tilfeller vertsnavn (hvis DNS-rolle er installert) samt virtuelle maskinidentiteter (hvis Hyper-V-rolle 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. Du kan stoppe og starte UAL-tjenesten mens serveren kjører. Hvis du vil deaktivere UAL permanent, åpner du Windows PowerShell, skriver inn Disable-UAL og starter serveren på nytt. En administrator kan slette alle historiske data som samles inn,

ved først å deaktivere UAL og deretter slette alle filene i mappen %SystemRoot%\System32\LogFiles\SUM\.

Øverst på siden

Serveradministrasjon

**Hva denne funksjonen gjør**

Serveradministrasjon er et administrasjonsverktøy som administratorer kan bruke til å overvåke én eller flere servere og å vise generell eller rollespesifikk status, slik at de kan 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 administratoren kontrollerer:

- **Generell serverinformasjon:** NetBios-navn og fullstendig domenenavn (FQDN), kontolegitimasjon som angis i Manage as-funksjonen, IPv4-adresse, IPv6-adresse, administrasjonsstatus, beskrivelse, operativsystemversjon, type, sist oppdatering, prosessorer, minne, klyngenavn, klyngeobjekttype, aktiveringsstatus, SKU, operativsystemarkitektur, produsent, konfigurasjon av Program for forbedret kundeopplevelse (CEIP) og konfigurasjon av Windows-feilrapportering.

- **Hendelser:** ID, alvorsgrad, kilde, logg, dato og klokkeslett for hver hendelse fra Windows og andre logger som administratoren 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 CPU-bruk og tilgjengelig minne.

**Bruk av informasjon**

Denne informasjonen lagres i Serveradministrasjon og sendes ikke til Microsoft. Den vises i Serveradministrasjon for å gjøre det enklere for

administratorer å overvåke systemer.

### Valg og kontroll

Administratorer kan velge om de vil samle inn data fra servere, unntatt den lokale serveren, ved å legge til eller fjerne serveren i Serveradministrasjon. Administratorer kan eksplisitt oppgi legitimasjon for å koble til en ekstern server. Serveradministrasjon ber administratoren om eksplisitt å samtykke i at legitimasjonen lagres lokalt i Serveradministrasjon, og administratoren kan når som helst slette denne legitimasjonen.

Øverst på siden

Active Directory Federation Services

### Hva denne funksjonen gjør

Active Directory Federation Services (AD FS) er en organisasjonsklar forbundsløsning med enkel pålogging for lokalnettbaserte eller andre nettverksbaserte apper. AD FS er til hjelp når administratorer vil gjøre det mulig for brukere å samarbeide på tvers av organisasjoner og å få enkel tilgang til apper på lokalnett eller andre nettverk samtidig som appsikkerheten ivaretas. 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 hver eller enhver kombinasjon av AD DS, Lightweight Directory Access Protocol (LDAP), SQL Server eller et egendefinert lager.

### Informasjon som samles inn, behandles eller overføres

En brukers legitimasjon samles inn når brukeren godkjennes med AD FS. Legitimasjonen sendes øyeblikkelig til godkjenning i Active Directory Domain Services, og AD FS lagrer den ikke lokalt. Brukerens attributter i Active Directory Domain Services kan bli brukt 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 til. Det blir ikke sendt noen informasjon til Microsoft.

### Bruk av informasjon

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

### Valg og kontroll

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

Øverst på siden

IPAM (IP Address Management)

### Hva denne funksjonen gjør

IPAM (IP Address Management) gjør at serveradministratorer kan spore IP-adressen, vertsnavnet og klientidentifikatoren (for eksempel MAC-adressen i IPv4 og DUID i IPv6) til 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 lagrer deretter IP-adressen, vertsnavnet, klientidentifikatoren og brukernavnet til den påloggede brukeren. En serveradministrator kan søke etter de innsamlede loggene basert på IP-adresse, klientidentifikator, 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 for kunden.

### Valg og kontroll

IPAM installeres ikke som standard og må installeres av serveradministratoren. 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 deaktiverer deretter oppgaven.

Øverst på siden

Unified Remote Access

### Hva denne funksjonen gjør

Unified Remote Access gjør at eksterne brukere kan 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 gjennomsiktig tilkobling til firmanettverk. Den gir også RAS-funksjonalitet (Remote Access Service), som er tradisjonelle VPN-tjenester, inkludert lokalnettilkobling eller annen nettverkstilkobling fra område til område.

### Informasjon som samles inn, behandles eller overføres

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

### Bruk av informasjon

Denne informasjonen brukes av administratoren til å feilsøke klienttilkobling og også til overvåkings- eller samsvarsformål. Det blir ikke sendt noen informasjon til Microsoft.

### Valg og kontroll

Overvåking av ekstern klient er aktivert som standard og kan ikke deaktiveres. Overvåkingsdataene lagres i WID-en eller på RADIUS-servere bare hvis en administrator har konfigurert kontobehandling slik at den bruker et av disse alternativene. Hvis en administrator ikke har konfigurert kontobehandling, lagres ikke noe av denne informasjonen. En administrator kan også konfigurere kontobehandling på en RAS-server slik at brukernavn og IP-adresse ikke lagres.

Øverst på siden

## Eksterne skrivebordstjenester

### Hva denne funksjonen gjør

Eksterne skrivebordstjenester (RDS) gir en plattform som firmaer kan bruke til å implementere en sentralisert skrivebordsstrategi, administrere skrivebord og apper og forbedre fleksibilitet og samsvar samtidig med datasikkerhet.

### Informasjon som samles inn, behandles eller overføres

Når det gjelder RDS-brukerovervåking, lagrer vertsservere for ekstern skrivebordsøkt informasjon om eksterne brukere som kobler til RDS-ressurser. Dette omfatter informasjon som vertsnavnet på den eksterne brukeren, Active Directory-brukernavnet og den offentlige IP-adressen til den eksterne klienten (hvis klienten er bak Network Address Translation (NAT), er det den offentlige IP-adressen). Disse dataene lagres automatisk i den interne Windows-databasen (WID) eller på SQL-serverne når brukere kobler til. Ingen informasjon sendes til Microsoft. Det er bare en domenebruker med en lokal administratorkonto som har tilgang til og kan vise denne informasjonen.

### Bruk av informasjon

Denne informasjonen brukes av administratoren til å feilsøke klienttilkobling og også til interne overvåkings- eller samsvarsformål. Det blir ikke sendt noen informasjon til Microsoft.

### Valg og kontroll

Klientovervåking er aktivert som standard og kan ikke deaktiveres. Overvåkingsinformasjonen lagres på WID-/SQL-serveren.

Øverst på siden

## Windows-programmet for forbedret kundeopplevelse (CEIP) og Windows-feilrapportering (WER)

### Hva denne funksjonen gjør

Hvis du vil ha mer informasjon om disse funksjonene, kan du se kategorien Funksjonstillegg eller denne hvitboken for administratorer.

**Informasjon som samles inn, behandles eller overføres**

Hvis du vil vite mer om spesifikk informasjon som samles inn, behandles og sendes av disse funksjonene, kan du se CEIP og Windows-feilrapportering i kategorien Funksjonstillegg .

**Bruk av informasjon**

Hvis du vil vite hvordan vi bruker informasjon som samles inn av disse funksjonene, kan du se CEIP og Windows-feilrapportering i kategorien Funksjonstillegg .

**Valg og kontroll**

CEIP er deaktivert som standard, og WER ber deg som standard om bekreftelse før krasjrapporter sendes til Microsoft. Du kan aktivere og deaktivere CEIP fra Serveradministrasjon i Kontrollpanel, og ved å bruke kommandolinjemetoder. WER kan bare styres med kommandolinjemetoder.

Hvis du vil aktivere eller deaktivere CEIP ved å bruke Kontrollpanel, klikker du **System og vedlikehold**og deretter **Problemrapporter og -løsninger**. Deretter klikker du **Innstillinger for program for forbedret kundeopplevelse**, klikke **Se også** for å velge alternativet for å aktivere eller deaktivere CEIP.

## Kontroller for Serveradministrasjon

Lokal server

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

- Deaktivere CEIP
  Åpne Serveradministrasjon og velg **Lokal server**. Klikk koblingen Program for forbedret kundeopplevelse, velg **Nei, jeg ønsker ikke å delta i programmet** i dialogboksen, og klikk deretter **OK**.

- Aktivere WER
  Åpne Serveradministrasjon og velg **Lokal server**. Klikk koblingen Windows-feilrapportering, velg **Ja, send sammendragsrapporter automatisk**, og klikk deretter **OK**.

- Deaktivere WER
  Åpne Serveradministrasjon og velg **Lokal server**. Klikk koblingen Windows-feilrapportering, velg **Jeg ønsker ikke å delta, og ikke spør meg igjen**, og klikk deretter **OK**.

Flere datamaskiner

- Aktivere CEIP
  Åpne Serveradministrasjon og velg **Alle servere**. Velg alle serverne (CTRL+A) i Servere-flisen, høyreklikk og velg **Konfigurer Automatisk tilbakemelding for Windows** . Velg **Ja, jeg ønsker å delta (anbefales)**i kategorien Program for forbedret kundeopplevelse. Bruk denne innstillingen på alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter **OK**.

- Deaktivere CEIP
  Åpne Serveradministrasjon og velg Alle servere. Velg alle serverne (CTRL+A) i Servere-flisen, høyreklikk og velg **Konfigurer Automatisk tilbakemelding for Windows** . Velg **Nei, jeg ønsker ikke å delta i programmet**i kategorien Program for forbedret kundeopplevelse. Bruk denne innstillingen på alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter **OK**.

- Aktivere WER
  Åpne Serveradministrasjon og velg **Alle servere**. Velg alle serverne (CTRL+A) i Servere-flisen, høyreklikk og velg **Konfigurer Automatisk tilbakemelding for Windows** . Velg **Ja, send sammendragsrapporter automatisk (anbefales)**i kategorien Program for forbedret kundeopplevelse. Bruk denne innstillingen på alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter **OK**.

- Deaktivere WER
  Åpne Serveradministrasjon og velg **Alle servere**. Velg alle

serverne (CTRL+A) i Servere-flisen, høyreklikk og velg **Konfigurer Automatisk tilbakemelding for Windows** . Velg **Nei, jeg ønsker ikke å delta i programmet**i kategorien Program for forbedret kundeopplevelse. Bruk denne innstillingen på alle serverne ved å merke av for Servernavn i Velg servere-kontrollen, og klikk deretter **OK**.

Øverst på siden

Software Inventory Logging

**Hva denne funksjonen gjør**

Software Inventory Logging (SIL) omfatter et nytt sett med WMI-klasser og PowerShell-cmdleter som gjør det enklere å få en grunnleggende oversikt over Windows Server-operativsystemet, programvaren som er installert i Windows Server, og egenskapene til serveren som programvaren kjører på. En administrator kan også aktivere en SIL-funksjon for å samle inn data fra WMI-leverandøren hver time og videresende dem over nettverket til en aggregasjonsserver, hvis en angis med cmdleten Set-SilLogging -TargetUri.

**Informasjon som samles inn, behandles eller overføres**

Data kan sendes til en aggregasjonsserver over nettverket hvis dette konfigureres av en administrator. Som standard blir ingenting samlet inn, behandlet eller sendt. Disse dataene omfatter følgende:

- Navnet på og utgaven av det installerte Windows Server-operativsystemet.
- En liste over navn på, versjoner av og utgivere av all programvaren som er installert på serveren, og installasjonsdatoen for programvaren.
- Det fullstendige domenenavnet på serversystemet.
- Antall, type og produsent av prosessorer, logiske prosessorer og kjerner som er installert på eller tilordnet serversystemet.

Data som samles inn og behandles, men som standard ikke sendes, selv om den timebaserte oppgaven er aktivert og en målaggregator er

angitt av administratoren:

- Klassen MsftSil_UalAccess og cmdleten Get-SilUalAccess behandler tellingen av totalt antall unike brukere og enheter for hver rolle eller hvert produkt som er registrert med funksjonen User Access Logging (UAL), fra to dager før spørringen. Dette er bare antall, ingen informasjon om brukere eller enheter produseres eller sendes. SIL må behandle bruker- og enhetsinformasjonen fra UAL-klasser for å kunne beregne selve antallene. Disse dataene er bare tilgjengelige for administratorer på den lokale maskinen. SIL endrer ikke tilgangen som trengs for UAL-API-ene.

Ingen innsamlede data sendes til Microsoft.

**Bruk av informasjon**

SIL WMI-leverandørene aggregerer data fra andre API-er som allerede finnes i systemet. Data kan sendes til en server for ytterligere aggregasjon over nettverket hvis dette konfigureres av en administrator. Som standard blir ingenting samlet inn, behandlet eller sendt. Når det gjelder klassen MsftSil_UalAccess og cmdleten Get-SilUalAccess, gir de behandlede dataene en telling av totalt antall unike brukere og enheter for hver rolle eller hvert produkt som er registrert med funksjonen User Access Logging (UAL), fra to dager før innsamlingen, men produserer ingen data som kan identifisere brukere eller enheter. Selv om denne WMI-klassen og cmdleten finnes på systemet, er de ikke en del av SIL-datanyttelasten som samles inn og videresendes til en aggregator hver time, når en administrator for systemet har konfigurert SIL slik at den gjør dette.

**Valg og kontroll**

Den timebaserte SIL-oppgaven er deaktivert som standard. Alle SIL-API-er er som standard tilgjengelige for spørring av administratorer for det lokale systemet. Den timebaserte SIL-oppgaven kan startes og stoppes mens serveren kjører, ved hjelp av cmdletene Start-SilLogging og Stop-SilLogging. Administratorer for serveren kan bruke cmdleten Set-SilLogging til å angi dato og klokkeslett for når den timebaserte oppgaven skal starte (standardverdien er 3 AM lokal systemtid), URI-en (Uniform Resource Identifier) for en målaggregasjonsserver og sertifikatavtrykket som er nødvendig for å sikre en klarert sending av

dataene.

Alle SIL-konfigurasjonsinnstillinger, inkludert start og stopp av den timebaserte oppgaven, kan endres i registret. Dette er ment å gjøres bare når systemet er en virtuell maskin, og bare før den første oppstarten av systemet.

Øverst på siden