



# Implementeringsguide för Chrome-enheter

Konfigurera och implementera Chrome-enheter i organisationen

# Innehåll

## Om den här guiden

### Inledning

- Förutsättningar
- Hantera Chrome-enheter

### Uppkoppling

- Viktiga funktioner
- Utvärdering och implementeringstips
- Hantera nätverksprofiler
- Konfigurera wifi
  - Lägga till wifi-konfigurering på enhetsnivå
  - Konfigurera wifi
  - Implementering via 802.1x
  - Webbfiltrering

### Konfigurera konton och Chrome-principer

- Viktiga överväganden gällande policyer
- Rekommenderade inställningar

### Förbereda enheterna inför implementeringen

- Uppdatera Chrome-enheterna till den senaste versionen
- Skapa en systemavbildning av Chrome OS
- Förbereda enheterna för registrering
- Förberedelsejänst (valfritt)

### Skriva ut med Chrome-enheter

- Överväganden för organisationer
- Integrering med befintlig infrastruktur

### Fjärråtkomst och virtualisering (valfritt)

- Viktiga funktioner
- Överväganden vid appvärdskap

### Särskilda implementeringsscenarier för Chrome-enheter

- Kioskapp med en enda uppgift
- Kiosker för sessioner med hanterade gäster
- Digital skyltning
- Tentor och prov

### Checklista inför implementering

### Ytterligare resurser och support

- Håll koll på vad som är nytt i Chrome-enheterna
- Söka i hjälpcentret
- Självhjälpstips
- Få support

## Om den här guiden

Den här guiden är ett komplement till [femstegsguiden för Chrome-enheter](#) och ger en mer detaljerad beskrivning av följande:

- De viktigaste beslutspunkterna när du driftsätter Chrome-enheter inom större skolor eller företag.
- [Molnbaserade principer](#), Chrome-appar och specifika användningsområden. Du hittar mer fördjupad dokumentation i [hjälpcentret för Chrome Enterprise](#).

I den här guiden fokuserar vi på följande:

- **Konfigurering och registrering** – hur du ansluter varje enhet till nätverket, registrerar enheterna på domänen och uppdaterar dem till den senaste versionen av Chrome OS.
- **Hantering** – hur du inför policyer för att domänen ska uppfylla IT-kraven och hur du konfigurerar och hanterar enheter som kör den senaste versionen av Chrome OS.

**Obs!** Rekommendationerna för att implementera Chrome-enheter på skolor och företag har sammanställts utifrån vårt arbete med en rad olika kunder och partner. Vi vill tacka dem för att de delat med sig av sina erfarenheter och insikter. Läs om att [implementera Chrome](#) om du vill veta mer om att implementera en hanterad Chrome-webbläsare.

<b>Det här ingår i beskrivningen</b>	Anvisningar, rekommendationer och viktiga överväganden för att implementera Chrome-enheter i en skol- eller företagsmiljö
<b>Primär målgrupp</b>	IT-administratörer
<b>IT-miljö</b>	Chrome OS, webbaserad miljö
<b>Tänk på följande</b>	De bästa metoderna för viktiga överväganden och beslut inför implementeringen av Chrome-enheter

*Senast uppdaterad: 10 september 2019*

*Dokumentets plats: <https://support.google.com/chrome/a/answer/6149448>*

## Inledning

Chrome-enheter är datorer som utvecklats av Google och körs med Chrome OS. Det som gör dessa datorer unika är att de körs i en ren webbmiljö, vilket innebär att de uppdateras automatiskt och att du slipper installera programkorrigeringar och göra nya utbildningar av datorerna regelbundet. De startar snabbt och har flera inbyggda [säkerhetsfunktioner](#).

Chrome-enheterna kan hanteras centralt via Googles administratörskonsol. Du kan konfigurera över 200 inställningar från den webbaserade konsolen. Exempelvis kan du välja wifi-inställningar och vilka appar som ska förinstalleras, samt tvinga enheterna att uppdateras automatiskt till den senaste versionen av Chrome OS.

## Förutsättningar

1. Även om Google Identity (ett Google Workspace-konto) inte krävs för att använda en hanterad Chrome-enhet rekommenderar vi att du förser användarna med Google-konton. Läs mer om att [lägga till nya användare på domänen](#).
2. Du måste ha Chromebook Enterprise-enheter eller en uppgradering, till exempel Chrome Enterprise Upgrade eller Chrome Education Upgrade, för varje fristående Chrome-enhet som du vill hantera. Köp uppgraderingar för en [skola eller ett företag](#). Organisationer i USA och Kanada kan även [köpa Chrome Enterprise Upgrade](#) online.
3. Om du planerar att implementera ett stort antal Chrome-enheter eller vill implementera dem samtidigt som du implementerar Google Workspace rekommenderar vi att du samarbetar med en [Google Cloud Partner](#).

## Hantera Chrome-enheter

Chrome-enheter kan konfigureras så att de fungerar i nästan alla skol- eller företagsmiljöer. När du implementerar Chrome-enheter kan du (administratören) styra åtkomsten till wifi-nätverk, webbfiltrering, förinstallerade appar och en rad andra saker med hjälp av följande:

- **Device Policies** – kan användas för att tillämpa inställningar och principer på organisationens hanterade Chrome-enheter oavsett vem som loggar in. Till exempel kan du begränsa inloggningen till specifika användare, blockera gästläget och konfigurera inställningar för automatiska uppdateringar. [Läs mer](#).
- **Användarpolicyer** – kan användas för att tillämpa inställningar och policyer för organisationens användare, oavsett vilken Chrome-enhet de använder. Till exempel kan en IT-administratör förinstallera appar för specifika användare, tillämpa Säker webbsökning, konfigurera Enkel inloggning (SSO), blockera specifika pluginprogram, svartlista specifika webbadresser, hantera bokmärken och tillämpa många andra inställningar för användare inom hela organisationen. [Läs mer](#).
- **Policyer för hanterade gästsessioner** – kan användas för att konfigurera inställningar för delade enheter på domänen. Med hanterade gästsessioner kan flera användare dela Chrome-enhet utan

att behöva logga in eller autentisera. Du kan tillämpa inställningar, till exempel för att se till att en användare loggas ut efter en viss tid. [Läs mer](#).

## Uppkoppling

När du konfigurerar en trådlös anslutning i ett klassrum eller på ett företag ska du se till att du har tillräcklig täckning i hela byggnaden och att du har tillräckligt med bandbredd för att alla enheterna ska fungera online.

## Viktiga funktioner

Chrome-enheter har stöd för de vanligaste wifi-protokollen: WEP, WPA, WPA2, EAP-TLS, EAP-TTLS, EAP-PEAP och LEAP. Dessutom har vissa Chrome-enheter maskinvara för mobilt internet via 3G eller 4G som fungerar om det finns mobiltäckning och ett mobildataabonnemang.

## Utvärdering och implementeringstips

Det är viktigt att göra en ordentlig utvärdering och att förbereda organisationens nätverksinfrastruktur för att ge användarna en så bra upplevelse som möjligt. IT-administratörerna ska se till att det finns en adekvat anslutning och bandbredd, särskilt på områden med många användare, till exempel på ett kontor eller en skola där många Chrome-enheter används samtidigt.

- **Testa wifi-täckningen och användningsfrekvensen** för att utvärdera var det kan behövas ytterligare åtkomstpunkter. Du kan göra detta med [tredjepartsappen Wifi Analyzer](#) på en Android-enhet.
- **Gör en trådlös infrastruktur- och topologiundersökning** i alla byggnader innan du implementerar enheterna på hela skolan eller företaget för att se till att du har tillräckligt med trådlös täckning. Det är oftast bäst att låta en partner som specialiserar sig på trådlös topologi göra följande:
  - **Platsundersökning** – du måste först analysera både det befintliga wifi-nätverket och störningar i omgivningen från enheter eller andra wifi-nätverk.
  - **Implementera** – implementera eller flytta åtkomstpunkter med korrekt säkerhet, kanalval och mottagarström/sändarström (Rx/Tx).
- **Se till att Chrome-enheterna har åtkomst till de webbadresser som krävs.** Chrome-enheterna behöver ha åtkomst till Googles nätverk för att fungera ordentligt och för att ta emot policy- och säkerhetsuppdateringar. Om du begränsar internetåtkomsten i miljön måste du se till att de implementerade enheterna fortfarande har åtkomst till dessa specifika Google-[webbadresser](#) utan att gå via en autentiserad proxy eller SSL-inspektion.

Läs [Enterprise-nätverk för Chrome-enheter](#) om du vill veta mer.

## Hantera nätverksprofiler

Wifi-nätverk kan när som helst läggas till på en Chrome-enhet manuellt, men Google rekommenderar att du använder [administratörskonsolen för att skicka wifi-profiler](#). Dessa profiler laddas ned och

tillämpas på Chrome-enheten under registreringsprocessen.

Uppdateringar i wifi-nätverksprofilerna

skickas även under den automatiska policyuppdateringen på Chrome-enheten. Fördelarna med att använda administratörskonsolen för att skicka dessa konfigurationer är att den i förväg delade nyckeln (PSK:n) kan vara tillräckligt komplex och aldrig behöver delas med slutanvändarna.

## Konfigurera wifi

Många kunder med Chrome-enheter använder WPA2-PSK på grund av den enkla konfigurationen. Chrome-enheter kan dock fungera i en rad olika skol- och företagsmiljöer, inklusive under komplexa wifi-implementeringsscenarier som kräver klientcertifikat, SSO och där lösningar för webbfiltrering har implementerats. Nedan hittar du tips om hur du konfigurerar wifi och valfria nätverksinställningar.

## Lägga till wifi-konfigurering på enhetsnivå

Underordnade organisationsenheter ärver wifi-nätverksprofiler från den överordnade organisationen. Om du vill konfigurera en profil behöver du ange nätverksinformation som SSID och säkerhetstyp. Var extra noga när du anger service set identifier (SSID) och lösenfras, eftersom båda är skiftlägeskänsliga. När du anger en ny wifi-nätverksprofil behöver du även markera rutorna **Anslut automatiskt** och **Chromebook** i avsnittet **Begränsa åtkomst till det här wifi-nätverket efter plattform**. Du hittar ytterligare teknisk information för nätverkskonfigurering [här](#).

Device management > Networks > Wi-Fi

ORGANIZATIONS
SETTINGS for solarmora.com

solarmora.com

- Cloud Identity
- Development
- Finance
- Legal
- Marketing
- Sales
- Support
- Vault
- XEdu
- XInfoX

**Name** Help

**Service set identifier (SSID)**

This SSID is not broadcast

Automatically connect

**Security type**

None

**Proxy settings**

Direct Internet Co

**Restrict access to this Wi-Fi network by platform**

This Wi-Fi network will be available to users using:

Mobile devices

Chromebooks

Google meeting room hardware

**Apply network**

by user

Users in this Organizational Unit will automatically get access to this network when signed in.

ADD
CANCEL

## Konfigurera wifi

Det är oftast enklast att använda ett öppet eller ofiltrerat nätverk för att registrera Chrome-enheterna och göra en första synkronisering av hanteringspolicyerna. Med den här konfigurationen kan Chrome-enheterna ta emot de nätverksprofiler som IT-administratören angett. När du har konfigurerat enheterna tar du bort det tillfälliga registreringsnätverket från listan över önskade nätverk. Läs mer i [Glöm ett nätverk](#).

## Implementering via 802.1x

Chrome-enheterna har stöd för 802.1x-autentisering. Kontakta nätverksleverantören om du vill veta hur du konfigurerar [Chrome-enheter med klientcertifikat](#). Till exempel är [ClearPass Onboard](#) från Aruba Networks ett tillägg som hanterar onboarding av Chrome-enheter och installerar certifikaten på ett säkert sätt. Systemadministratörer och partner som använder Google Cloud hittar dokumentation för avancerad wifi-nätverkskonfiguration med 802.1x för företag på [Google Cloud Connect](#).

Du måste vara ansluten till nätverket om du vill ladda ner 802.1x-certifikat. Med andra ord kan du antingen konfigurera ett öppet WPA/WPA2-PSK-nätverk eller använda USB till Ethernet-adaptrar för att hämta certifikatet på enheten. Se [Hantera nätverk](#).

Mer information om ämnet finns i [Hantera klientcertifikat på Chrome-enheter](#).

## Webbfiltrering

Inom organisationer med nätverksfilter som genomsöker SSL-trafik krävs i allmänhet att ett anpassat rotcertifikat läggs till på fliken **Auktoriteter** i `chrome://settings/Certificates`. Även om detta fungerar för de flesta användarutlösta webbbegäranden använder vissa begäranden på systemnivå inte detta certifikat för att skydda användaren mot vissa typer av säkerhetsrisker. I den här [listan med värddar](#) ser du vilka som måste undantas från SSL-inspektion.

Om du vill att Chrome-enheterna ska fungera i ett nätverk med SSL-inspektion läser du [Konfigurera nätverk med SSL-innehållsfilter](#), som förklarar hur du installerar ett anpassat rotcertifikat för alla domänanvändare som loggar in på organisationens registrerade Chromebook-enheter.

## Konfigurera konton och policyer för Chrome OS

Med Googles administratörskonsol kan du organisera och hantera organisationens Chrome-enheter centralt. När du hanterar användare via administratörskonsolen kan du konfigurera enheter och användarpolicyer per organisationsenhet via avsnittet för Chrome-hantering i administratörskonsolen.

Du kan visa en lista över Chrome-enheterna, söka efter enheter och visa information om enheterna (serienummer, registreringsstatus, slutdatum för support, användarnamn vid registrering och manuellt skrivna anteckningar, t.ex. om plats) via administratörskonsolens enhetslista. Genom att gå in på varje enhet efter serienummer kan du även visa information som vilken OS-version som har installerats på enheten, MAC-adressen och den senaste inloggade användaren.

Dessa enhetspolicyer tillämpas på alla Chrome-enheter som registrerats för hantering på domänen.

Användarpolicyerna tillämpas överallt där användarna loggar in, inklusive på registrerade och icke-registrerade Chrome-enheter. I inställningarna ingår en möjlighet för dig att ange säkerhetspolicyer och styra vilka appar användarna får ladda ned och använda. Läs mer i [Om Chrome OS-enhetshantering](#).



## Viktiga överväganden gällande policyer

Tänk på följande när du väljer inställningar för skolan eller företaget:

1. Anteckna hur du vill att Chrome-enhetsmodellen ska konfigureras i miljön.
2. Ange samma inställningar som policyer i administratörskonsolen och använd en och samma organisationsenhet för testning.
3. När inställningarna har konfigurerats och verifierats på Chrome-enheterna i den organisationsenheten (t.ex. vilken startsida som ska visas som standard, vilka appar som ska förinstalleras eller vilka webbadresser som ska svartlistas) kan du kopiera inställningarna till hela domänen.

Om du vill veta mer om att använda organisationsenheter med Chrome-enheter läser du artikeln [Flytta en Chrome-enhet till en organisationsenhet](#).

## Rekommenderade inställningar

På administratörskonsolen under **Enhetshantering > Chrome-hantering** har du åtkomst till många inställningar under **Användarinställningar** och **Enhetsinställningar**. Även om de flesta organisationer använder standardinställningarna hittar du några inställningar som vissa organisationer väljer att anpassa nedan.

<b>Tillåt att användare som är inloggade på enheten ändrar sina konton i webbläsarfönstret</b>	Du kan välja om du vill tillåta eller blockera användare från att logga in på eller ut från sina Google-konton i webbläsaren. Eller så kan du tillåta användarna att logga in enbart på specifika Google Workspace-domäner. Läs mer om <a href="#">att logga in i webbläsaren</a> .
<b>Tvingad återregistrering</b>	Google rekommenderar inte att du stänger av den här inställningen. När den är aktiv tvingar den en rensad enhet att återregistrera sig på domänen. Om du inte vill att en Chrome-enhet ska återregistreras på din domän ska du <a href="#">avadministrera</a> enheten. <a href="#">Läs mer om tvingad återregistrering</a> .
<b>Skärmlås</b>	Välj <b>Lås alltid skärmen automatiskt vid viloläge</b> för att höja säkerheten och minska risken för att någon använder dina användares datorer när de är borta.
<b>Förinstallerade appar och tillägg</b>	Välj de webbappar som gäller för dina användare, till exempel Gmail Offline eller Google Drive. Du kan även svartlista och vitlista appar från <a href="#">Chrome Web Store</a> om du behöver ha mer kontroll över vilka appar som användarna får installera.
<b>Fästa appar</b>	Välj vilka appar som ska döljas eller visas i systemets aktivitetsfält. <b>Obs!</b> Med den här inställningen tillåts endast appar som angetts av administratören, vilket innebär att användarna inte kan ha egna uppsättningar av appar synliga i systemets aktivitetsfält.

Sidor som ska läsas in vid start	Här väljs vanligtvis en portal för intranätet eller en startsida. Nackdelen med den här inställningen är att Chrome-enheterna inte kan återställa flikarna från den föregående sessionen nästa gång de startar.
Begränsa inloggning till lista på användare	Om du begränsar inloggningarna till *@dindomän.se hindrar du användarna från att logga in med privata Gmail-konton eller andra konton som inte är specifika för domänen. Du kan styra vilka som får logga in på en hanterad (registrerad) Chrome-enhet.
Radera alla inställningar för användaruppgifter och status efter varje utloggning	Aktivera inte detta om du inte vill att Chrome-enheten ska rensas på användardata mellan varje session. Inställningen innebär att användarnas policyer laddas ned på nytt vid varje inloggning.
Inställningar för automatisk uppdatering	Använd standardinställningarna för automatisk uppdatering. Chrome-enheterna uppdateras automatiskt med ett intervall på mellan sex och åtta veckor och hämtar då nya funktioner, felkorrigeringar och programkorrigeringar vid säkerhetsbrister. Vi rekommenderar även att du behåller 5 procent av organisationen i beta- eller utvecklingskanalen för att testa hur framtida Chrome OS-versioner fungerar i organisationen. Du hittar en fullständig lista över rekommendationer i <a href="#">Implementera automatiska uppdateringar för Chrome-enheter</a> . <b>Obs!</b> Stoppa bakgrundshämtningen av uppdateringar innan enheten har registrerats och startat om genom att trycka på Ctrl + Alt + E på skärmen Licensavtal för slutanvändare. Annars kan nedladdade uppdateringar som borde ha blockerats av principen tillämpas när användaren startar enheten.
Enkel inloggning	I organisationer som ska använda Enkel inloggning (SSO) rekommenderar vi att du först testar med ett litet antal användare för att se till att de kan logga in på sina Chrome-enheter innan du aktiverar SSO för hela organisationen. Om du använder SSO för Google Workspace-inloggning på befintliga enheter kan du överväga att börja använda <a href="#">Lösenordssynkronisering i Google Workspace</a> .

## Förbereda enheterna inför implementeringen

Innan du distribuerar Chrome-enheter till slutanvändarna måste de förberedas för att ge användarna en optimal upplevelse. Som minst behöver du registrera Chrome-enheter på domänen för hantering. På så sätt tillämpas alla framtida enhetspolicyuppdateringar på alla Chrome-enheter.

Om du implementerar ett litet antal enheter hittar du anvisningar om hur du smidigt registrerar och implementerar enheterna i [snabbstartsguiden](#). Om du implementerar Chrome-enheter till en större användargrupp, till exempel flera klassrum eller skolor, eller på flera olika kontor, läser du anvisningarna nedan.

## Uppdatera Chrome-enheterna till den senaste versionen

Enheter som körs med Chrome OS söker efter och laddar ned uppdateringar automatiskt när de är anslutna till wifi eller Ethernet. Enheterna uppdateras till den senaste versionen om inte administratören ställt in en begränsning i [inställningarna för enhetsuppdatering](#). Om du behöver uppdatera många enheter och samtidigt vill spara bandbredd i nätverket kan du dock använda ett USB-minne med den senaste versionen av Chrome OS.

När du ska avbilda hundratals eller tusentals Chrome-enheter är uppdatering via USB-enheter det effektivaste sättet. Att uppdatera via USB är ett bra sätt att spara bandbredd, eftersom det kan gå åt mer än 400 MB per enhet för att ladda ned en fullständig operativsystemuppdatering.

## Skapa en systemavbildning av Chrome OS

Om du vill uppdatera Chrome-enheterna till den senaste versionen av Chrome OS manuellt med ett USB-minne behöver du följande:

1. Information om tillverkare och modell för den Chrome-enhet du vill uppdatera.
2. Ett USB 2.0-minne eller senare, ett flashminne på minst 4 GB
3. Webbläsaren Chrome, som körs med Chrome OS, Microsoft Windows eller macOS
4. Installera [Återställningsverktyg för Chromebook](#) och välj korrekt serie och modell för enheten för att skapa en USB-återställningsenhet.

Läs [här](#) om du vill ha mer information om att uppdatera, återställa eller rensa enheter.

**Obs!** Det kan ta en vecka innan en stabil version är tillgänglig i verktyget för att bränna avbildningar.

## Förbereda enheterna för registrering

Så här förbereder och implementerar du enheterna:

1. [Skapa USB-återställningsenheter](#) eller uppdatera enheterna over-the-air. Vi rekommenderar USB-metoden om du har mer än 10 enheter.
2. Efter omstarten väljer du språk, typ av tangentbord och wifi-nätverk.
3. När du godkänt användarvillkoren och *innan du loggar in på Chrome-enheten* trycker du på **Ctrl + Alt + E**. Då visas "företagsregistrering" uppe till vänster.
4. Ange ett användarnamn och lösenord (antingen administratören eller den registrerade användaren på domänen) och klicka på **Registrera enhet**.  
När du registrerat enheten får du ett meddelande om att enheten har registrerats för företagshantering.
5. Klicka på **Klar** så kommer du tillbaka till den första inloggningsskärmen. Där står det "Den här enheten hanteras av *dindomän.se*" längst ned på sidan.

Upprepa de här stegen för alla Chrome-enheter i organisationen. Om du vill ha mer information om enhetsregistrering läser du [Registrera Chrome-enheter](#).

## Använda en förberedelsejänst (valfritt)

Förberedelsejänsten har utformats för att implementera Chrome-enheterna utan att IT-avdelningen behöver göra något. Fördelen med att låta en återförsäljare använda en förberedelsejänst är att Chromebook-enheterna är klara att använda direkt. Användarna kan öppna förpackningen till sin egen Chrome-enhet och vara produktiva direkt, utan att någon konfiguration behövs. Men precis som alla enheter för slutanvändare behöver även Chrome-enheterna viss konfiguration för att kopplas till rätt hanteringspolicyer i administratörskonsolen. Den tjänsten tillhandahålls av många officiella återförsäljare av Google Chrome-enheter före leverans.

Återförsäljaren eller en annan organisation som tillhandahåller förberedelsejänsten för Chromebook och utför förberedelserna på sin anläggning kan få ett användarkonto på din Google Workspace-domän (inte ett administratörskonto). Det här registreringskontot kan placeras i en organisationsenhet där alla tjänster är inaktiverade.

De faktiska stegen som ingår i förberedelsejänsten kan vara följande:

- uppdatering av Chrome OS-versioner
- registrering för Chrome OS-hantering
- policyverifiering, inklusive förkonfigurerade wifi-nätverk
- resurstaggning
- lasermärkning
- paketering av kringutrustning.

Kontakta återförsäljaren av Google Chrome-enheten om du vill veta mer. Om du inte har någon partner kan du söka efter en [Google Cloud Partner](#) i ditt område.

## Implementera Android-appar på Chrome-enheter

Om organisationen använder [Chrome-enheter med stöd för Android-appar](#) kan du tvångsinstallera eller bestämma vilka Android-appar som användarna får ladda ned. Det finns tre sätt att göra appar tillgängliga:

- Du kan tvångsinstallera appar på enheter.
- Du kan skapa ett urval av appar som du tillåter att användarna laddar ned.
- Du kan ge användarna åtkomst till allt innehåll i en hanterad Google Play-butik (detta stöds inte för Chrome Education-kunder).

Om du vill veta mer om hur du aktiverar Android-appar på domänens Chrome-enheter och godkänner appar för användarna läser du [Använda Android-appar på Chrome-enheter](#).

## Innan du börjar

- Google rekommenderar att du testar Android-appar för Chrome-enheterna i en provorganisationsenhet innan du lanserar dem för alla. Om du inte längre vill använda dem kan du inaktivera dem och fortsätta att använda enheterna på samma sätt som förut.
- Läs [Vanliga frågor om Android-appar på Chrome](#) om du vill veta mer om sådant som kan vara relevant för din implementering.

## Köra Android-appar i kioskläge

Du kan använda [Googles administratörskonsol](#) för att installera [Android-appar på hanterade Chrome-enheter i låst kioskläge](#). På så sätt kan du implementera en Android-app på en kioskenhet och konfigurera den så att den startar automatiskt.

## Integrerad utskrift med Chrome-enheter

Chrome OS har stöd för integrerad utskrift, vilket innebär att användarna enkelt kan ansluta till skrivare och skrivarservrar direkt, utan åtkomst till en molnbaserad infrastruktur. Chrome använder Common UNIX Printing System (CUPS) som stöd för integrerad utskrift och Internet Printing Protocol (IPP) som stöd för utskrift på lokala skrivare och nätverksskrivare.

Som administratör kan du använda Googles administratörskonsol för att konfigurera CUPS. När du lägger till en skrivare visas den automatiskt på användarnas lista över Chrome-skrivare så att de kan börja skriva ut utan ytterligare konfiguration. Läs mer i artikeln [Hantera lokala skrivare och nätverksskrivare](#).

För CUPS-utskrifter finns det stöd för skrivare från många olika tillverkare och det finns även stöd för utskrift på lokala skrivare och nätverksskrivare.

Om du vill veta mer om andra utskriftsalternativ på Chrome OS läser du [Skriva ut på Chrome-enheter](#).

## Fjärråtkomst och virtualisering (valfritt)

Du kan använda Chrome-enheter för att komma åt traditionella, äldre appar i situationer då användarna behöver åtkomst till

- äldre klientappar som Microsoft® Office®
- webbsidor som kräver äldre tekniker eller endast Microsoft-tekniker (t.ex. Internet Explorer)
- pluginprogram utöver Flash (t.ex. Java®-pluginprogram eller Silverlight) för webbappar.

### Viktiga funktioner

Med virtualiseringsappar kan du köra äldre appar på Chrome-enheter eller använda Chrome-enheter med din befintliga virtualiserade appinfrastruktur. Det finns flera tillgängliga lösningar som använder vanliga protokoll för fjärråtkomst. Till exempel:

- [Citrix Workspace](#)
- [VMware Horizon Client för Chrome](#)
- [ChromeRDP](#)

Det finns även appvirtualiseringslösningar som [Chromotif](#) och [Fra.me](#) som fungerar bra med Chrome OS.

### Överväganden vid appvärdskap

Om det inte gör något att apparna du vill använda finns på en annan plats (t.ex. Microsoft® Office 365, Oracle® Cloud-appar eller värd-baserade SaaS-appar) är det oftast enklast att implementera en värdlösning, vilken inte kräver någon serverkonfiguration.

Men om appen du vill använda måste finnas innanför organisationens brandvägg, eller om du vill använda befintliga servrar eller lösningar för en virtuell skrivbordsinfrastruktur (VDI) kan följande lösningar fungera bättre:

- [VMware Horizon™ DaaS®](#)
- [Chrome Remote Desktop](#)

## Särskilda implementeringsscenarier för Chrome-enheter

Chrome-enheter kan användas i en rad olika situationer, och tack vare den låga kostnaden, fjärrhanteringen och lite eller inget underhållsbehov har de blivit populära att implementera för specifika användningsscenarier på skolor och företag. Dessa scenarier kan innefatta allt från att visa en skolkalender på en skärm för digital skyltning till att dela datorer på ett bibliotek eller administrera prov. Nedan hittar du länkar till ytterligare resurser om hur du implementerar Chrome-enheter för att tillgodose just era behov.

### Molnbaserade anställda

Chrome-enheter passar utmärkt för anställda på företag. En Chrome-enhet kan tilldelas en viss användare för åtkomst till webbappar och produktivitetstverkyg och för samarbete med kollegor. Om du vill veta mer om hur du kan använda Chrome Enterprise för att underlätta för molnbaserade anställda hittar du videor om detta på [Cloud Worker Live](#).

### Kioskapp med en enda uppgift

Du kan skapa en kioskapp med en enda uppgift, till exempel för att låta kunderna fylla i en kreditansökan, svara på en butiksenkät eller läsa information om elevregistrering. [Läs mer](#)

### Kiosker för sessioner med hanterade gäster

Du kan konfigurera kiosker för sessioner med hanterade gäster i till exempel fikarummet, på butiksskärmar eller på delade enheter på biblioteket, där användarna inte behöver logga in för att använda Chrome-enheten. [Läs mer](#)

### Digital skyltning

Du kan använda Chromebox-enheter för digital skyltning, t.ex. för skolkalendrar, digitala affischtavlor, restaurangmenyer och interaktiva spel. Du kan skapa en värdaserad app eller en paketerad app och starta den i helskärm via Kioskläge för enskild app. [Läs mer](#).

### Tentor och prov

Med Chromebooks får du en säker plattform där du kan administrera tentor och prov åt eleverna. När enheterna har konfigurerats på rätt sätt uppfyller de kraven för bedömningar av elever enligt standarden för grund- och gymnasieskolor. Med Chromebooks kan du inaktivera elevernas tillgång till internet under pågående prov. Du kan dessutom inaktivera externt lagringsutrymme och möjligheten att ta skärmdumpar och göra utskrifter.

Det finns en rad olika sätt att konfigurera Chromebook-enheter inför prov, t.ex. som kiosker för en enskild app, på en domän som tillhandahålls av provleverantören eller som kiosker för sessioner med hanterade gäster. Läs mer i [Använda Chromebook vid tentor och prov](#).

## Checklista inför implementering

<input type="checkbox"/> <b>Nätverksinfrastruktur</b>	<p>Har du den wifi-infrastruktur som behövs, och tillräckligt med bandbredd för att alla enheter ska kunna ansluta till internet samtidigt?</p> <ul style="list-style-type: none"> <li>• Hur ser bandbreddsanvändningen ut i dagsläget, utan Chrome-enheterna? Klarar den aktuella bandbredden att tillgodose det förväntade behovet?</li> <li>• Finns det platser i byggnaden som saknar wifi-täckning?</li> </ul>
<input type="checkbox"/> <b>Inventering av äldre appar och webbappar</b>	<p>Hur många av användarna behöver äldre appar jämfört med webbappar? Vill ni införa fler webbappar och onlineresurser för användarna? Hur ser tidsplanen ut i så fall?</p>
<input type="checkbox"/> <b>Pluginanvändning</b>	<p>Vet du vilka pluginprogram som krävs för att komma åt de webbplatser som användarna behöver? Behöver du konfigurera en fjärrlösning för detta? <a href="#">Läs mer</a></p>
<input type="checkbox"/> <b>Skrivare</b>	<p>Har du konfigurerat skrivarna för integrerad utskrift (CUPS)? Ska du tillåta utskrift för alla eller bara några av användarna?</p>
<input type="checkbox"/> <b>Kringutrustning</b>	<p>Har du verifierat att kringutrustningen som användarna behöver fungerar med Chrome-enheterna? Testa t.ex. headset, streckodsläsare och annan kringutrustning som måste implementeras innan användarna ska börja använda dem.</p>
<input type="checkbox"/> <b>Verifieringsschema</b>	<p>Hur ska användarna logga in på sina datorer? Hur ska du hantera wifi-lösenord och åtkomst till wifi-nätverket? Använder ni SSO för Chrome-enhetsautentisering? Använder ni även Lösenordssynkronisering i Google Workspace (GSPS)? Använder ni <a href="#">Cloud Identity</a>?</p>
<input type="checkbox"/> <b>Datum för projektets milstolpar</b>	<p>Har du en tidsplan för lanseringen? Finns det något sätt för användarna att lämna feedback om hur de upplever Chrome-enheterna? Hur lång ska utvärderingsperioden vara, vilka typer av enkäter ska du skicka till användarna och hur ofta ska du samla in data om användningen och feedback från användarna?</p>
<input type="checkbox"/> <b>Utbildning av användare</b>	<p>Ska ni utbilda användarna om ni flyttar från en annan plattform till Chromebook? Om ni har en utbildningsavdelning kan ni utforma utbildningen på plats. I annat fall erbjuder vissa <a href="#">Google Cloud Premier Partner</a> Chromebook-utbildning.</p>
<input type="checkbox"/> <b>Kundtjänstförberedelser</b>	<p>Är kundtjänstmedarbetarna bekanta med <a href="#">hjälpcentret för Chrome Enterprise</a>? Att läsa igenom resurserna som anges på nästa sida och gå utbildningar kan hjälpa kundtjänstmedarbetarna och IT-personalen att hantera Chromebook-relaterade frågor.</p>



## Ytterligare resurser och support

### Håll koll på vad som är nytt i Chrome-enheterna

- Följ [Google Chrome-bloggen](#) och [Chrome-versionsbloggen](#)
- Följ [Viktig information om Chrome Enterprise](#)

Google Workspace-kunder kan också läsa

- [nyhetswebbplatsen om](#) Google Workspace
- [Google Cloud-bloggen](#)

### Söka i hjälpcentret

- [Chrome Enterprise](#)
- [Chromebook \(slutanvändare\)](#)
- [Chromebox för möten](#)
- [Läs mer om hur du loggar in på administratörskonsolen](#)

### Självhjälpstips

- [Så här samlar du in enhetsloggar för Chrome](#)
- [Åtgärda Chromebook-problem \(Chromebook-kunder\)](#)
- [Kända problem \(Chrome Enterprise\)](#)
- [Log Analyzer](#) (verktyg för Google Workspace) – Analysera `/var/log/messages` och `/var/log/chrome/` för att hitta fel
- [Administrera prov på Chromebook](#)

### Få support

Vi erbjuder support via e-post och telefon för problem med Chrome-enheternas programvara och tjänster. [Se våra supportalternativ för Chrome-enheter.](#)