

SÅDAN NAVIGERER DU I ANDROID MDM- LANDSKABET

Do's and Don'ts – Best practices



I dag er mobile enheder en uundværlig del af de fleste virksomheders arbejdsgange. Android-enheder er især populære blandt medarbejdere, da de er overkommelige, nemme at bruge og tilgængelige i en række forskellige former og størrelser.

Men med populariteten af mobile enheder – herunder Android-enheder – kommer naturligvis også visse udfordringer. Som virksomhed skal det sikres, at medarbejdernes Android-enheder er sikre og at de bruges på en måde, der er i overensstemmelse med virksomhedens politikker.

Dette er præcis her, hvor **Android MDM** kommer ind i billedet.

Android MDM (Mobile Device Management) giver virksomheder mulighed for at administrere og beskytte deres Android-enheder.

Med Android MDM kan du blandt andet:



Overvåge enheder og data



Håndhæve politikker




Sikkerhedskopiere og gendanne data



Fjerninstallere apps



Blokere adgang til bestemte websteder og apps



Android MDM er altså et vigtigt værktøj for virksomheder, der ønsker at sikre deres Android-enheder og beskytte deres data.

Ved at implementere **Android MDM** kan du:

- Forbedre jeres sikkerhed
- Øge jeres produktivitet
- Reducere jeres omkostninger
- Og meget mere

Hvis din virksomhed bruger Android-enheder, bør du overveje at prioritere **Android MDM**. Det er en investering, der vil betale sig i sidste ende.

Sikkerhed, sikkerhed og sikkerhed

Med fokus på sikkerhed, er der nogle ting, som du bør overveje, når du vælger en **Android MDM**:

- Sørg for, at MDM-løsningen tilbyder stærke sikkerhedsfunktioner, såsom kryptering og appkontrol.
- Sørg for, at MDM-løsningen er kompatibel med de Android-enheder, som din virksomhed bruger.
- Sørg for, at MDM-løsningen er nem at implementere og bruge.
- Sørg for, at MDM-løsningen er overkommelig for din virksomhed.

Ved at overveje disse faktorer kan du vælge en Android MDM, der hjælper dig med at beskytte dine Android-enheder og data.

Vi har her kort listet yderligere detaljer om nogle af de sikkerhedsfunktioner, som du også bør kigge efter i en Android MDM:

- **Kryptering:** Kryptering beskytter dine data mod uautoriseret adgang, selvom enheden går tabt eller stjæles.
- **Appkontrol:** Appkontrol giver dig mulighed for at blokere eller tillade bestemte apps på dine Android-enheder.

Ved at vælge en Android MDM med stærke sikkerhedsfunktioner kan du hjælpe med at beskytte dine Android-enheder og data mod hackere og andre cybertrusler.



VALG AF ANDROID MDM

Do's



Overvej dine behov: Hvad er dine vigtigste behov for en Android MDM-løsning? Skal du kunne administrere enheder, overvåge data, håndhæve politikker eller noget andet? Når du ved, hvad du har brug for, kan du begynde at indsnævre dine muligheder.



Undersøg forskellige løsninger: Der er mange forskellige Android MDM-løsninger på markedet, så det er vigtigt at undersøge dine muligheder grundigt, før du træffer en beslutning. Sammenlign priser, funktioner og brugertilgængelighed for at finde den bedste løsning til dine behov.



Prøv det af: De fleste Android MDM-udbydere tilbyder gratis prøveperioder, så du kan prøve en løsning, før du køber den. Dette er en god måde at se, om løsningen opfylder dine behov, og om den er nem at bruge.



Tal med andre virksomheder: Spørg andre organisationer, der bruger en Android MDM-løsning, om deres anbefalinger. De kan dele deres erfaringer og give dig indsigt i, hvad der er vigtigt at overveje, når du vælger en løsning.



Vælg ikke en løsning, der ikke opfylder dine behov: Det er vigtigt at vælge en Android MDM-løsning, der opfylder dine behov. Hvis du ikke vælger en løsning, der er kraftfuld nok, kan du ikke beskytte dine data eller administrere dine enheder effektivt.



Glem ikke at overveje dine brugeres behov: En Android MDM-løsning skal være nem at bruge for dine brugere. Hvis løsningen er for kompliceret, vil dine brugere ikke bruge den, og du vil ikke kunne opnå de ønskede resultater.



Glem ikke at implementere løsningen korrekt: Når du har valgt en Android MDM-løsning, skal du implementere den korrekt. Dette omfatter at konfigurere løsningen til at opfylde dine behov og at træne dine brugere i, hvordan de bruger den.



Glem ikke at overvåge løsningen: Efter at du har implementeret en Android MDM-løsning, skal du overvåge den for at sikre, at den fungerer korrekt. Dette omfatter at overvåge enheder, data og politikker.

Ved at følge disse do's og don'ts kan du vælge den bedste Android MDM-løsning til dine behov og sikre, at den implementeres og overvåges korrekt.



CapaSystems er en dansk software- og konsulentvirksomhed, der siden 1996 har været dedikeret til at skabe softwareløsninger, som giver bedre overblik, lavere omkostninger, højere slutbrugertilfredshed samt større fleksibilitet for vores kunder. Det gør CapaSystems ved at levere ekspertise og 'smart technology', som kan udnytte potentialet i vores kunders IT-systemer. Hos CapaSystems er du sikret en løsning, der tilgodeser dine behov.

CapaSystems står bag udviklingen af de to on-premise softwareløsninger **CapaInstaller** og **PerformanceGuard** samt cloudløsningen **CapaOne**, der understøtter alle deployment tools. Der udvikles konstant nye produkter til CapaOne bl.a. **Android** (styring af virksomhedens Android-enheder) **AdminOnDemand** (Privileged Access Management), **Drivers** (automatisk opdatering af drivere), **Reliability** (muligheden for at få det fulde overblik og finde løsningen på virksomhedens IT-udfordringer) samt **Updater** (strømlinet opdatering af 3. parts programmer). CapaSystems beskæftiger i dag +30 medarbejdere, der er placeret i Taastrup og Skanderborg. CapaSystems' løsninger anvendes i en lang række danske og internationale virksomheder – over 25% af danske kommuner har valgt at benytte CapaSystems' software.

Book et møde

Vil du vide mere så ring til os og book en præsentation af vores produkter, der kan spare dig og virksomheden vital tid!

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup
Tel. (+45) 70 10 70 55
www.capasystems.dk