Microsoft Entra ID-oppsett

Guide for IT-ansvarlig i kunde-organisasjonen som skal aktivere Microsoft-pålogging for sine DigiReq-admin- og godkjenner-brukere.

> **Sluttbrukere** trenger ikke gjøre noe. Etter at oppsettet er ferdig, ser de en "Logg inn med Microsoft"-knapp på `https://digireq.no/admin/login`.

1. Hva blir aktivert

- Admin- og godkjenner-roller logger inn med sin Entra ID-konto i stedet for (eller i tillegg til) SMS-OTP
- Ansatt-rollen (felt-app) beholder SMS-OTP — Entra ID gjelder kun admin-dashboardet
- Per-organisasjon valg: SMS-OTP kan slås av helt for admin/godkjenner ("Entra ID-only"-modus)

2. Hva DigiReq ber om — minimum-rettigheter

Tre standard OIDC-scopes:

- `openid` — bekreft at brukeren er logget inn (standard OIDC)
- `profile` — navn og brukernavn (vises i admin-UI)
- `email` — e-postadresse (knytte Entra-bruker til en forhåndsinvitert DigiReq-bruker)

Vi leser **ikke** kalender, filer, mailbox eller Teams. Vi lagrer Microsoft-konto-IDen (`oid` claim) som en referanse — ingen passord eller token settes til hvile hos oss utover sesjonen.

Tekstsamtykke vises av Microsoft når en Global Administrator klikker gjennom samtykke-flyten — det er Microsoft som beskriver scopes, ikke DigiReq.

3. Forutsetninger

- **Global Administrator** eller **Privileged Role Administrator** i kundens Entra ID-tenant
- Kundens **Tenant ID** (UUID-format, finnes i Entra admin senter → Overview)
- DigiReq-konto med rolle = `super_admin` på leverandør-siden (Markus) må aktivere tenant ID-en i DigiReq-systemet etter at samtykke er gitt

4. Steg 1 — Generer samtykke-URL

Åpne `https://digireq.no/admin/consent` i nettleseren. Skriv inn tenant ID-en (eller la feltet stå tomt for å bruke `common`-endepunktet — Microsoft ruter da til den tenanten du er logget inn på).

Siden bygger en samtykke-URL i format:

```
https://login.microsoftonline.com/<TENANT_ID>/adminconsent
  ?client_id=b4e5540c-b264-4cfe-b358-0f6572b8e875
  &redirect_uri=https://api.digireq.no/auth/oidc/callback
```

Klikk "Åpne i Microsoft" eller kopier URL-en og send den til IT-admin via intern kanal.

5. Steg 2 — Godkjenn samtykke i Microsoft

1. Microsoft ber deg logge inn (hvis du ikke er logget inn fra før)
2. Du blir bedt om å logge inn som Global Administrator
3. Microsoft viser de tre rettighetene fra forrige seksjon
4. Klikk "Godta"

Microsoft sender deg deretter til `https://api.digireq.no/auth/oidc/callback` — det er normalt at den siden viser en feilmelding eller hvit side. Selve samtykket er allerede registrert i Entra; redirect-en er bare et teknisk artefakt.

6. Steg 3 — Aktivér i DigiReq

Send tenant ID-en til DigiReq:

- E-post: info@digireq.no
- Emne: `Aktivér Entra ID for <organisasjonsnavn>`

Vi aktiverer tenanten i DigiReq-systemet (felt: `entra_tenant_id`) og gir tilbakemelding samme dag i pilot-fasen. Etter aktivering kan admin/godkjenner- brukere logge inn med

Microsoft umiddelbart.

Du kan også be om at SMS-OTP slås helt av for admin-rollene ("Entra ID-only"-modus). Standard er at begge metodene er aktive parallelt — det er anbefalt for de første ukene som fallback.

7. Steg 4 — Test innlogging

1. Gå til `https://digireq.no/admin/login`
2. Klikk "Logg inn med Microsoft"
3. Skriv inn organisasjonskoden din (Narvik Vann KF = `NV`)
4. Microsoft viser kontovelger; velg organisasjonskontoen
5. Du sendes til DigiReq admin-oversikten

Hvis innlogging feiler (URL `?oidc_error=…`):

- `tenant_mismatch` — Microsoft-kontoen tilhører en annen tenant enn DigiReq har på filen
- `not_invited` — DigiReq-brukeren din er ikke pre-invitert. Få admin til å invitere e-posten din via `/admin/users` først
- `role_not_allowed_for_oidc` — du har ansatt-rolle; bruk mobil-appen, ikke admin-dashboardet
- `oidc_validation_failed` — teknisk problem; kontakt sikkerhet@digireq.no

8. Anbefalt Conditional Access-policy (MFA)

For å håndheve MFA på alle admin-/godkjenner-påloggинger, sett opp en Conditional Access-policy i kundens egen Entra-tenant for DigiReq-app-en (`b4e5540c-b264-4cfe-b358-0f6572b8e875`):

- **Krav om MFA** ved hver pålogging eller på risiko-basert nivå (Identity Protection)
- **Sesjons-kontroll:** tidsbegrenset pålogging (f.eks. 8-12 timer) og re-autentisering ved nye enheter
- **Valgfritt:** krav om kompatible/registrerte enheter (Intune-managed) for ekstra device-binding
- **Valgfritt:** lokasjons-restriksjon hvis kommunal IT har geografiske krav
- **Anbefalt:** blokker legacy-autentisering

Se også /sikkerhet § 4.3 for vår MFA-policy-anbefaling.

9. Trekke samtykke tilbake

1. Entra admin senter → **Enterprise applications**
2. Søk etter **DigiReq**
3. **Properties** → **Delete**

Samme øyeblikk slutter alle DigiReq-påloggинger via Entra å fungere for din organisasjon. Eksisterende SMS-OTP-brukere er ikke berørt.

10. Sikkerhets-detaljer for revisjons-teamet

- **Tenant-isolasjon:** validert per pålogging. Et token signert av en annen tenant blir avvist selv om signaturen ellers er gyldig (`iss` og `tid` claims sjekkes mot kundens registrerte tenant ID).
- **PKCE S256** + signed state cookie (10 min TTL, HttpOnly, Secure, SameSite=Lax) for CSRF/replay-beskyttelse
- **JWKS host-pinning** til `login.microsoftonline.com` — discovery-doc-poisoning kan ikke omdirigere oss
- **Klokke-skew-toleranse** 60 sekunder på `exp`/`iat`/`nbf`
- **Audit-logg:** alle påloggинger logges med Entra-OID, rolle, tenant. Append-only, retention 12 måneder
- **Token-utstedelse:** access-token TTL 60 min, refresh-token TTL 60 dager. Token revokeres umiddelbart ved deaktivering av brukeren i DigiReq

11. Hvis dere går fra "Entra ID-only" tilbake til SMS

Kontakt info@digireq.no. Vi snur policy-flagget umiddelbart. SMS-OTP-funksjonalitet er aldri fjernet for`super_admin`— DigiReq-leverandøren beholder backdoor-tilgang via SMS for support-formål, men det er kun Markus' personlige bruker.

12. Tekniske spørsmål

sikkerhet@digireq.no — vi svarer innen 24 timer i pilot-fasen.

Dokument-versjon 1.0 · Sist oppdatert 29. mai 2026 (redirect-URI til api.digireq.no) · sikkerhet@digireq.no

OM LEVERANDØREN

Tjenesten DigiReq leveres av **Påvakt AS** (org.nr. **937 620 187**), heretter omtalt som «Leverandør». DigiReq er registrert som virksomhet under Påvakt AS (**Digireq**, org.nr. **937 700 539**). Avtaler signeres med Påvakt AS som juridisk enhet; EHF-fakturaer fra DigiReq utstedes på Digireqs virksomhets-org-nr.

Kontakt: info@digireq.no · Sikkerhet: sikkerhet@digireq.no · Personvern: personvern@digireq.no