

## INNOMATE HR Single Sign-On

Det er muligt at oprette Single Sign-On (SSO) forbindelser til INNOMATE HR.

Det betyder, at man undgår, at brugerne skal vedligeholde og huske passwords til INNOMATE HR, men kan bruge eksisterende brugeradgang til at få adgang til systemet.

Der understøttes for nærværende følgende SSO identitets-leverandører:

- UNI•Login
- WAYF
- ADFS
- INNOMATE Windows Authentication
- Andre leverandører efter aftale

I alle tilfælde kræves det, at brugernavnene, som vi modtager fra identitets-leverandøren er de samme som dem, der sættes op i INNOMATE HR.

### UNI•Login og WAYF

Hvis I allerede bruger UNI•Login eller WAYF, kan vi umiddelbart etablere løsningen, så brugerne vil kunne logge ind i INNOMATE HR gennem pågældende leverandør.

### ADFS

Vi kan oprette tillidsrelationer mellem INNOMATE HR og jeres ADFS, således at brugerne vil få adgang via dette. Der vil være lidt opsætning og installation af certifikater forbundet med løsningen.

### INNOMATE Windows Authentication

Der skal her installeres en applikation på jeres netværk. Applikationen er en ASP.NET-applikation baseret på Microsoft Windows Identity Foundation. Al kommunikation foregår med SAML protokollen og er krypteret. Der skal installeres nogle X.509 certifikater på jeres server til brug for denne kryptering. Applikationen kræver en Microsoft Windows Server med Microsoft .NET 4.5

### Andre leverandører

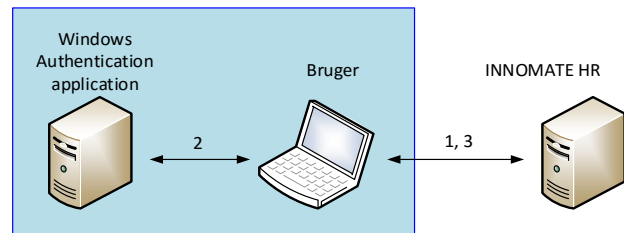
Hvis I ønsker at bruge en leverandør, som vi ikke allerede understøtter, så kontakt os. Vi kan muligvis etablere løsningen.

### Flere leverandører

Det er muligt at bruge flere leverandører på én gang. Der vil så skulle angives en række IP-adresser for hvilke den enkelte leverandør skal bruges. Hvis en bruger ikke er logget på INNOMATE HR, men forsøger at tilgå en side – f.eks. med et dybt link – vil dette afgøre hvilken identitets-leverandør, der bruges.

I kan også vælge at beholde muligheden for normal login med brugernavn og password, der vedligeholdes i INNOMATE HR, og kombinere dette med en eller flere SSO identitets-leverandører.

## Logon-processen



Når en bruger på kundens netværk først forsøger at tilgå en URL i INNOMATE HR systemet (1), redirectes brugeren over på WindowsAuthentication applikation (2). Her registreres brugerens Windows-login, og der oprettes et login-token, der sendes tilbage til brugeren. Brugeren bliver derefter redirectet tilbage til INNOMATE HR (3). Her tjekkes login-tokenet, og hvis alt stemmer, logges brugeren ind i systemet.

Brugeren kan derefter navigere rundt i systemet som normalt. Logon-processen er gennemsigtig for brugeren, der blot vil opleve at blive sendt hurtigt forbi en tom side, inden man kommer ind til den rigtige side.