



# Sikkerhetswebinar

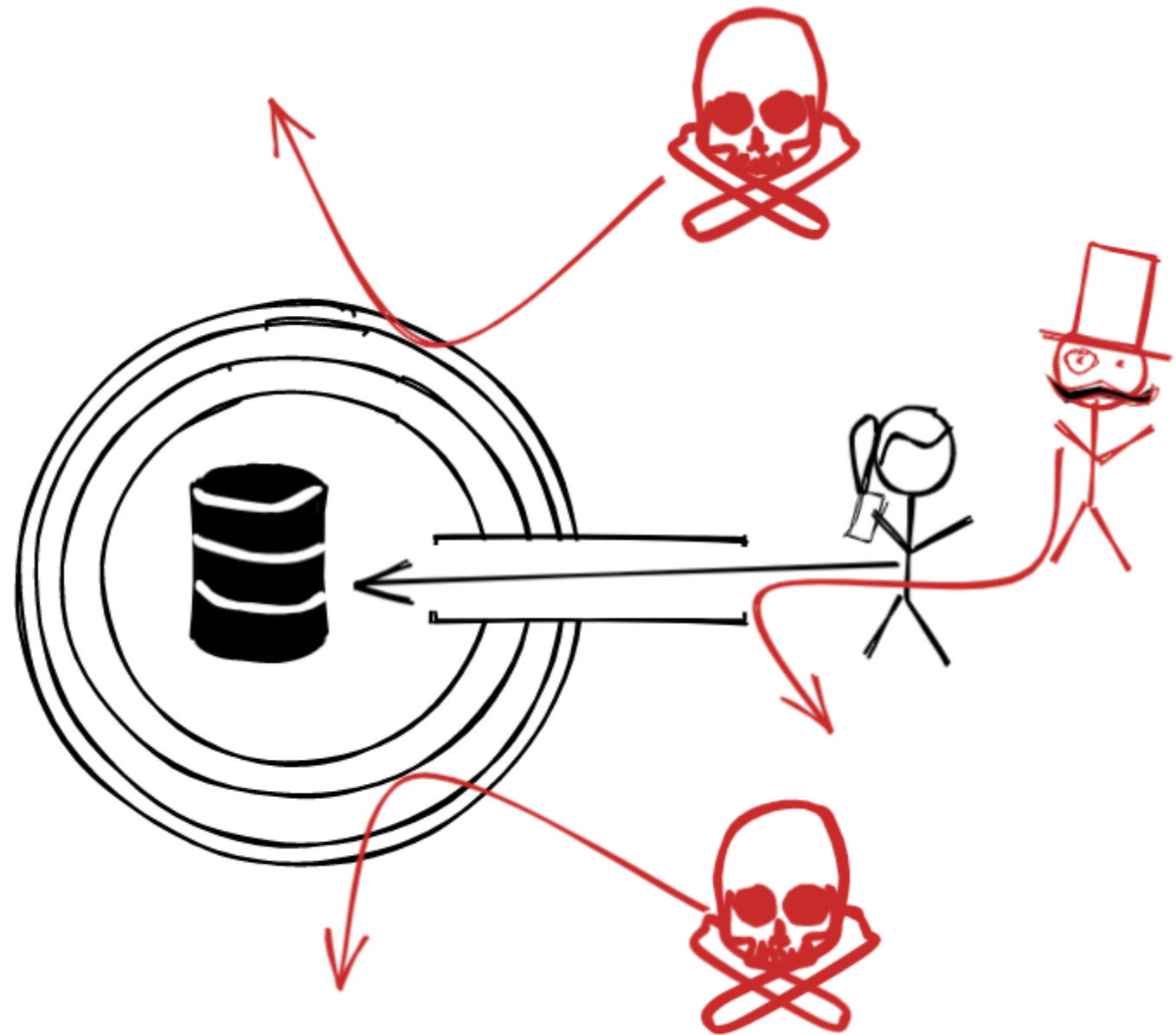
## 27.04.22

### Tema

- Generelt om data sikkerhet
- Passord
- Vitec Planias tiltak for sikkerhet
- Autentifikasjons alternativer med Plania



Espen Sigmundstad  
Prosjektleder BIM



# Passord

## Phishing - Nettfisking

- Lurer deg til å gi fra deg passordet
  - Via mail
  - Via telefon
  - Via SMS
  - Via annen nett tjeneste

## Cracking

- Prøver å “beregne” ditt passord med tilfeldige kombinasjoner
- Prøver typisk brukte password som “123456789”



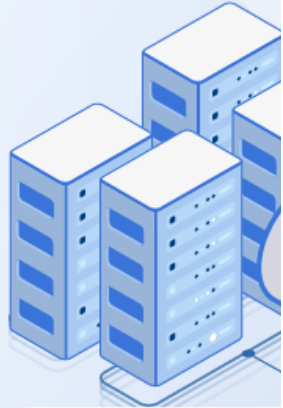
# Passord



632.000.000.000 komb/sekund

# Passord

CLOUD



Compute

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %\$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

# Passord

## Credential stuffing

- Bruker navnet ditt er nødvendigvis ikke hemmelig
- Kan testes over mange tjenester

## Tiltak

- Unike sterke passord
- To-faktor autorisasjon

haveibeenpwned.com

3 Jysla Tåsjne Bisletutar

# Passord

## Tiltak

### Password manager

- Samling av unike password
- Tjenestene har strenge sikkerhets barrierer
- Kan ligge innenfor din organisasjons nettverk

### Andre muligheter

- Windows Hello
- Passwordless



# Vitec Planias tiltak for sikkerhet

## Vitec IT

- Brannmur and IPS (Intrusion Protection System)
- Søker etter sårbarheter
- Kontinuerlig vedlikehold

## Vitec Plania

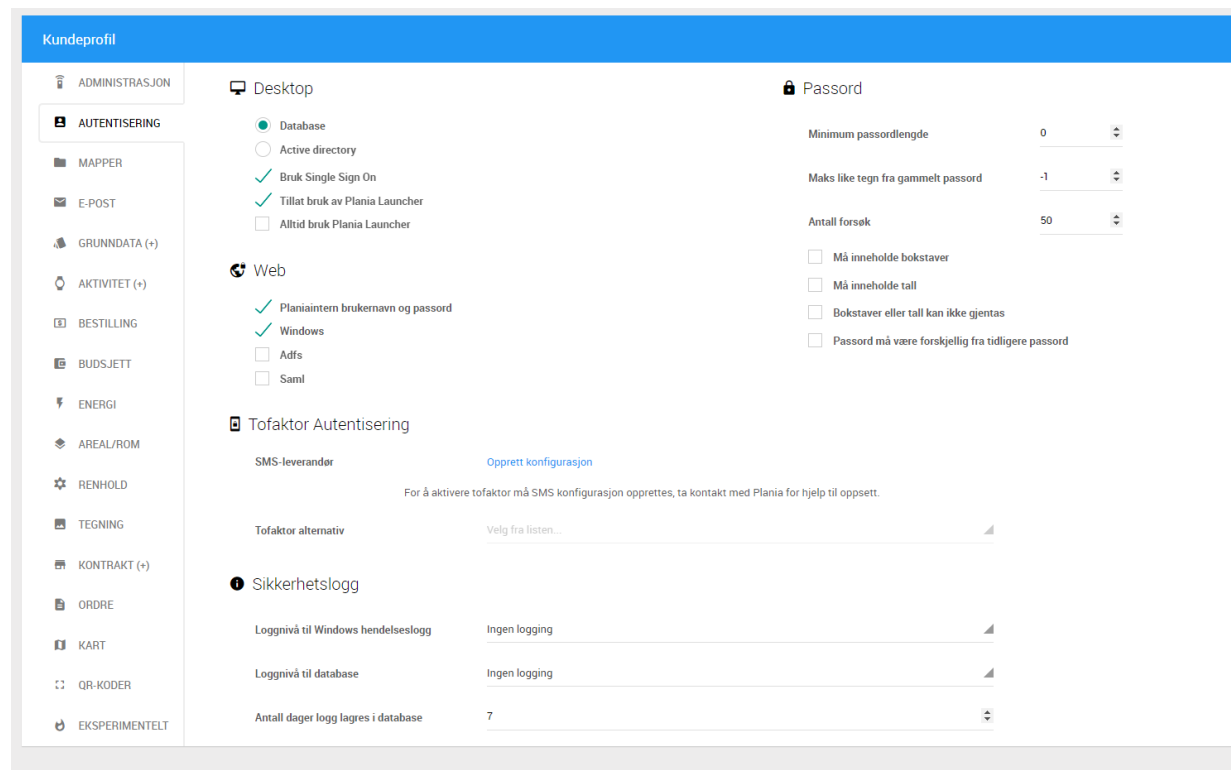
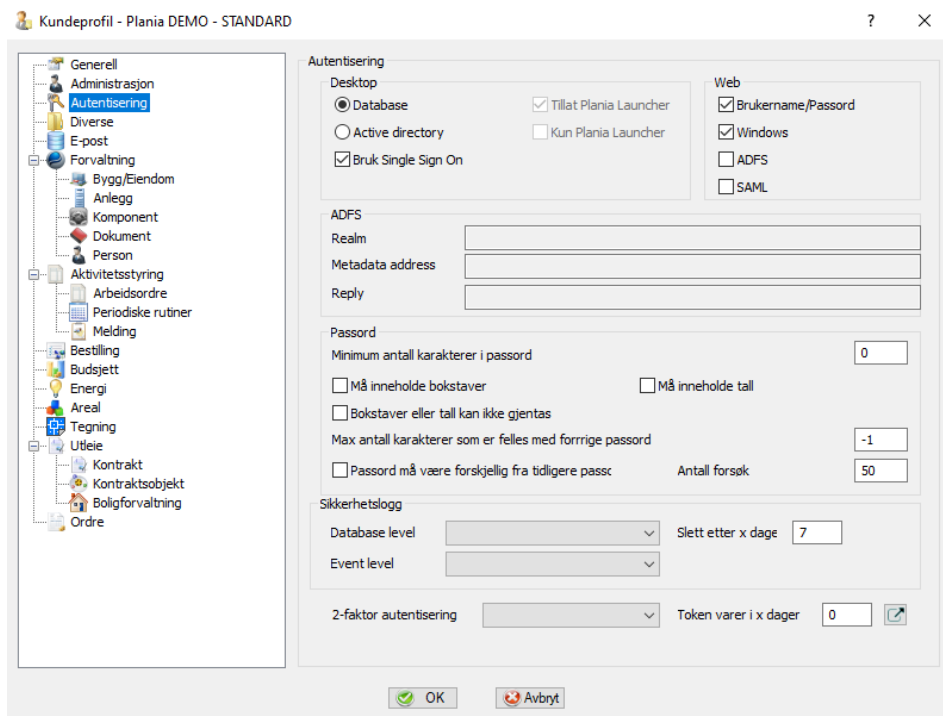
- Penetrasjonstest
- Ny hovedrelease av Plania, minstekrav til passord
- Tilbyr forskjellige muligheter for autentisering



# Autentifikasjons alternativer med Plania

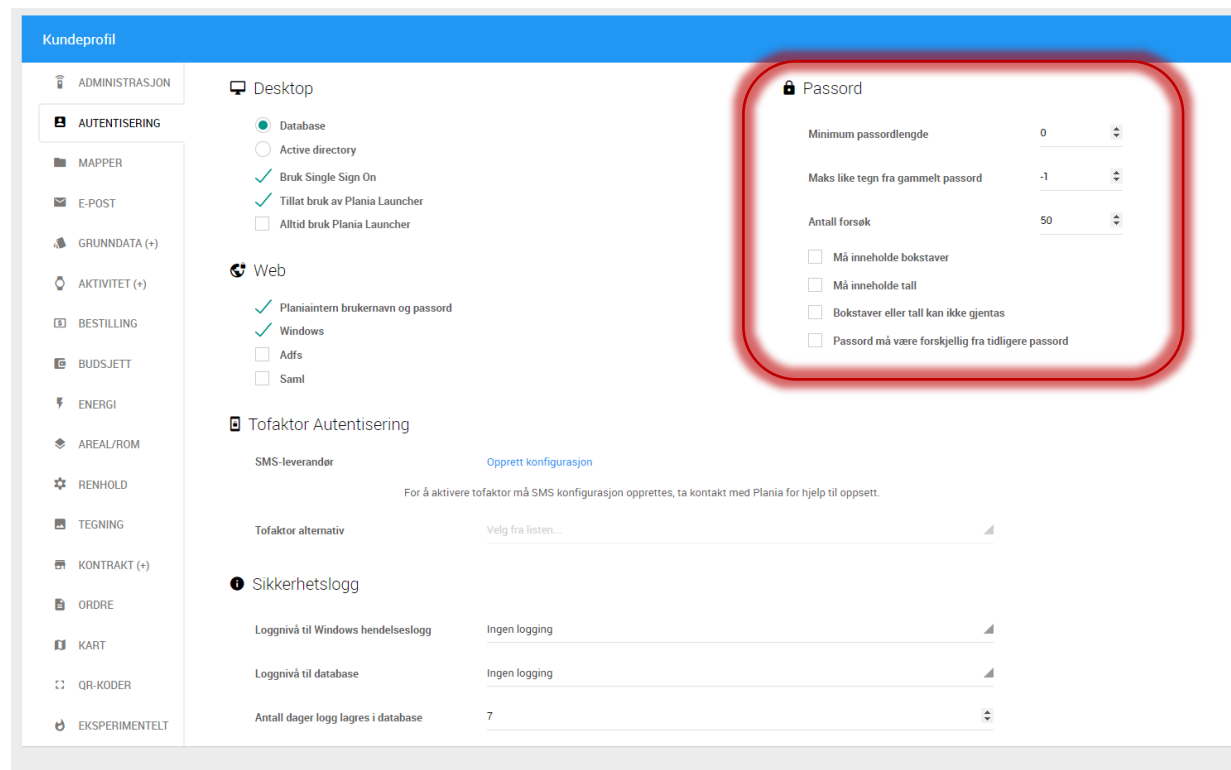
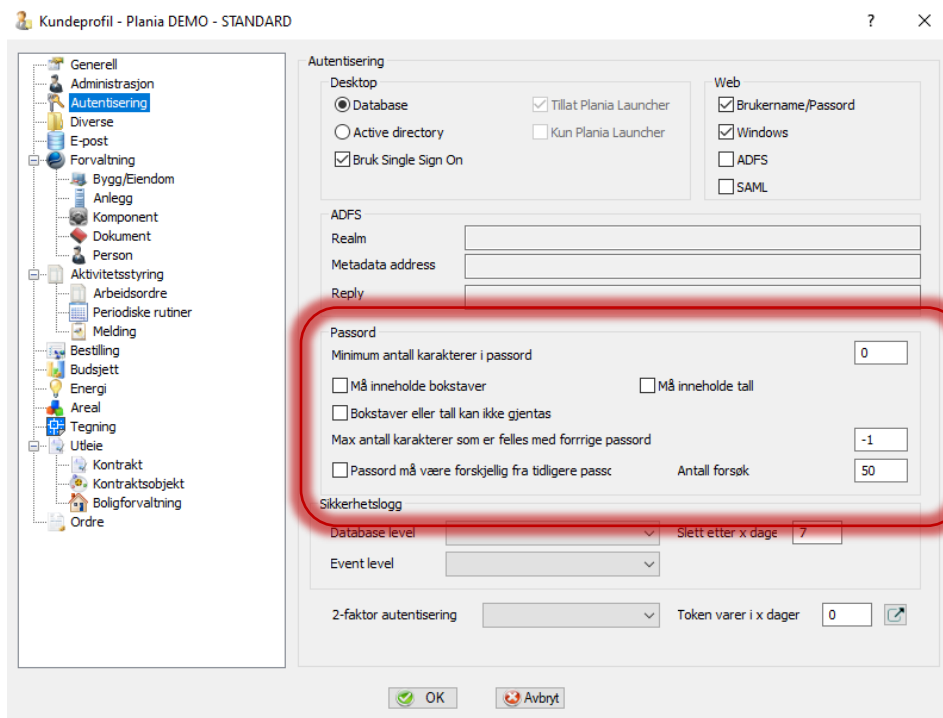
1. Sette passord krav
2. To-faktor autentifikasjon
3. Administrere innlogging via egen IT avdeling (SAML)

# Autentifikasjons alternativer med Plania



# Autentifikasjons alternativer med Plania

## 1. Sette passord krav



# Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon

Kundeprofil - Plania DEMO - STANDARD

Autentisering

Desktop

Database  Tillat Plania Launcher

Active directory  Kun Plania Launcher

Bruk Single Sign On

Web

Brukernavn/Passord

Windows

ADFS

SAML

ADFS

Realm

Metadata address

Reply

Passord

Minimum antall karakterer i passord 0

Må inneholde bokstaver  Må inneholde tall

Bokstaver eller tall kan ikke gjentas

Max antall karakterer som er felles med forrige passord -1

Passord må være forskjellig fra tidligere pass

Antall forsøk 50

Sikkerhetslogg

Database level Slett etter x dage 7

Event level

2-faktor autentisering Token varer i x dager 0

OK Avbryt

Kundeprofil

ADMINISTRASJON

AUTENTISERING

Desktop

Database

Active directory

Bruk Single Sign On

Tillat bruk av Plania Launcher

Alltid bruk Plania Launcher

Web

Planiaintern brukernavn og passord

Windows

Adfs

Saml

Passord

Minimum passordlengde 0

Maks like tegn fra gammelt passord -1

Antall forsøk 50

Må inneholde bokstaver

Må inneholde tall

Bokstaver eller tall kan ikke gjentas

Passord må være forskjellig fra tidligere passord

Tofaktor Autentisering

SMS-leverandør [Opprett konfigurasjon](#)

For å aktivere tofaktor må SMS konfigurasjon opprettes, ta kontakt med Plania for hjelp til oppsett.

Tofaktor alternativ [Velg fra listen...](#)

Sikkerhetslogg

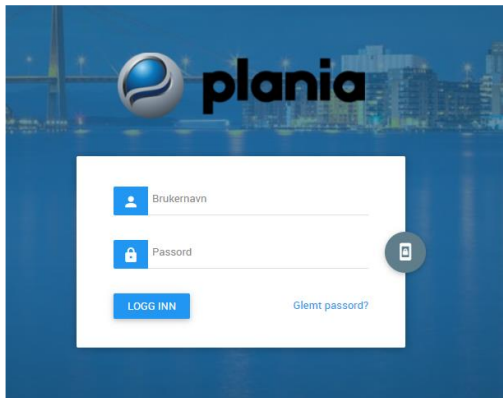
Loggnivå til Windows hendelseslogg Ingen logging

Loggnivå til database Ingen logging

Antall dager logg lagres i database 7

# To-faktor autentisering

- Noe man vet (passord)
- Noe man har (kodebrikke, enhet)
- Noe man er (biometri)



# Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon

Kundeprofil - Plania DEMO - STANDARD

Autentisering

Desktop

Database  Tillat Plania Launcher

Active directory  Kun Plania Launcher

Bruk Single Sign On

Web

Brukernavn/Passord

Windows

ADFS

SAML

ADFS

Realm

Metadata address

Reply

Passord

Minimum antall karakterer i passord 0

Må inneholde bokstaver  Må inneholde tall

Bokstaver eller tall kan ikke gjentas

Max antall karakterer som er felles med forrige passord -1

Passord må være forskjellig fra tidligere pass

Antall forsøk 50

Sikkerhetslogg

Database level

Slett etter x dage 7

Event level

2-faktor autentisering

Token varer i x dager 0

OK Avbryt

Kundeprofil

ADMINISTRASJON

Desktop

Database

Active directory

Bruk Single Sign On

Tillat bruk av Plania Launcher

Alltid bruk Plania Launcher

Web

Planiaintern brukernavn og passord

Windows

Adfs

Saml

Tofaktor Autentisering

SMS-leverandør [Opprett konfigurasjon](#)

For å aktivere tofaktor må SMS konfigurasjon opprettes, ta kontakt med Plania for hjelp til oppsett.

Tofaktor alternativ [Velg fra listen...](#)

Sikkerhetslogg

Loggnivå til Windows hendelseslogg Ingen logging

Loggnivå til database Ingen logging

Antall dager logg lagres i database 7

# Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon
3. SAML

Kundeprofil - Plania DEMO - STANDARD

Autentisering

Desktop

Database  Tillat Plania Launcher

Active directory  Kun Plania Launcher

Bruk Single Sign On

Web

Brukernavn/Passord

Windows

ADFS

SAML

ADFS

Realm:

Metadata address:

Reply:

Passord

Minimum antall karakterer i passord:

Må inneholde bokstaver  Må inneholde tall

Bokstaver eller tall kan ikke gjentas

Max antall karakterer som er felles med forrige passord:

Passord må være forskjellig fra tidligere pass

Antall forsøk:

Sikkerhetslogg

Database level:

Slett etter x dage:

Event level:

2-faktor autentisering:

Token varer i x dager:

OK Avbryt

Kundeprofil

ADMINISTRASJON

AUTENTISERING

Desktop

Database

Active directory

Bruk Single Sign On

Tillat bruk av Plania Launcher

Alltid bruk Plania Launcher

Web

Planiaintern brukernavn og passord

Windows

Adfs

Saml

Tofaktor Autentisering

SMS-leverandør: [Opprett konfigurasjon](#)

For å aktivere tofaktor må SMS konfigurasjon opprettes, ta kontakt med Plania for hjelp til oppsett.

Tofaktor alternativ: Velg fra listen...

Sikkerhetslogg

Loggnivå til Windows hendelseslogg: Ingen logging

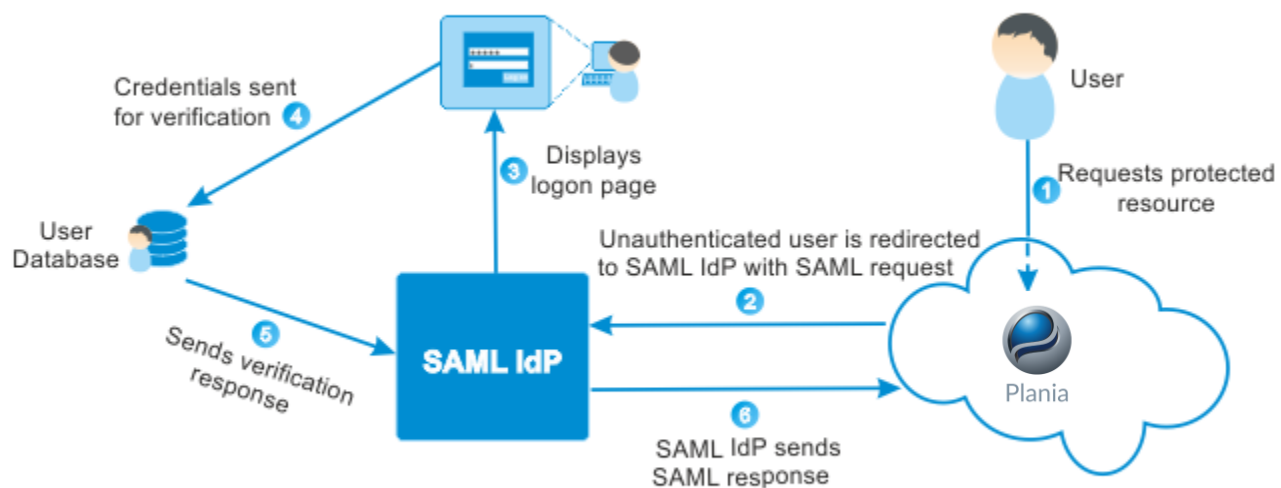
Loggnivå til database: Ingen logging

Antall dager logg lagres i database:



# SAML

- Bruker organisasjonens identifikasjons biblioteker for å gi tilganger til forskjellige systemer.
- Må ordnes gjennom organisasjonenes IT avdeling og Plania Support.
- Sikrer god sikkerhet, og enkelt for brukerne.



# Oppsummering

- Generelt om data sikkerhet
- Passord
- Vitec Planias tiltak for sikkerhet
- Autentifikasjons alternativer med Plania

<https://kunde.plania.no/hc/no/articles/4758696472092-God-passordsikkerhet-i-systemet>

Spørsmål?



Espen Sigmundstad  
Prosjektleder BIM