*Handleiding Single-Sign-On koppelingen met **SAML 2.0***

februari 2019

SAML Handleiding

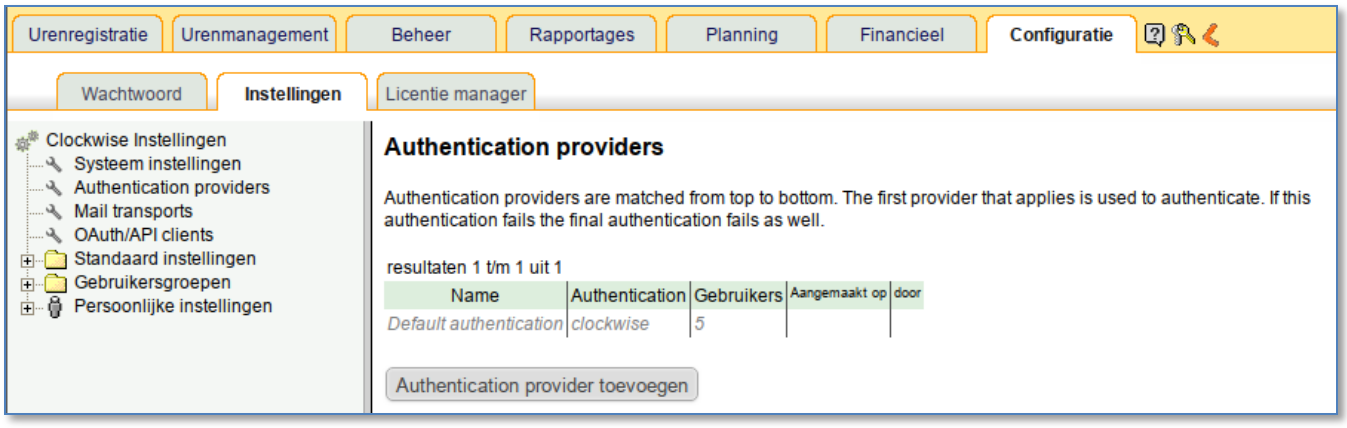
In ClockWise is het mogelijk Single Sign On te realiseren via het SAML 2.0 protocol. Deze methode wordt onder andere gebruikt bij Azure Active Directory, ADFS, SecureAuth, SimpleSAML en vele andere systemen. Om een koppeling te realiseren wordt in ClockWise gebruik gemaakt van Authentication providers, waarbij per gebruikersgroep of zelfs gebruiker een eigen authentication provision kan worden ingesteld. Naast de bestaande standaard inlog methode in ClockWise, zijn er ook 2-factor, Google, Facebook en dus ook SAML authentication providers beschikbaar. Deze handleiding beschrijft het instellen van een SAML authentication provider.

Gebruikte terminologie

SAML – Een veelgebruikte standaard voor identity federation; het koppelen van inlog procedures
Single Sign On (SSO) – Netwerkarchitectuur waarbij inlog van gebruikers op een centrale plek plaats vindt
Identity Provider (IdP) – De server die via SAML authenticatie uitdeelt aan de SP
Service Provider (SP) – Het ClockWise account dat extern authenticatie vraagt van een IdP
Metadata – XML file die de configuratie beschrijft van een IdP of SP
Entity ID – Identifier die de IdP of SP kenmerkt (kan een string of niet bestaande url zijn)
Attribute – De naam van een parameter waarvan de inhoud deunieke koppeling van medewerkers tussen de IdP en SP definieert
Authentication provider – Configurabele methode binnen ClockWise die de login van een medewerker regelt

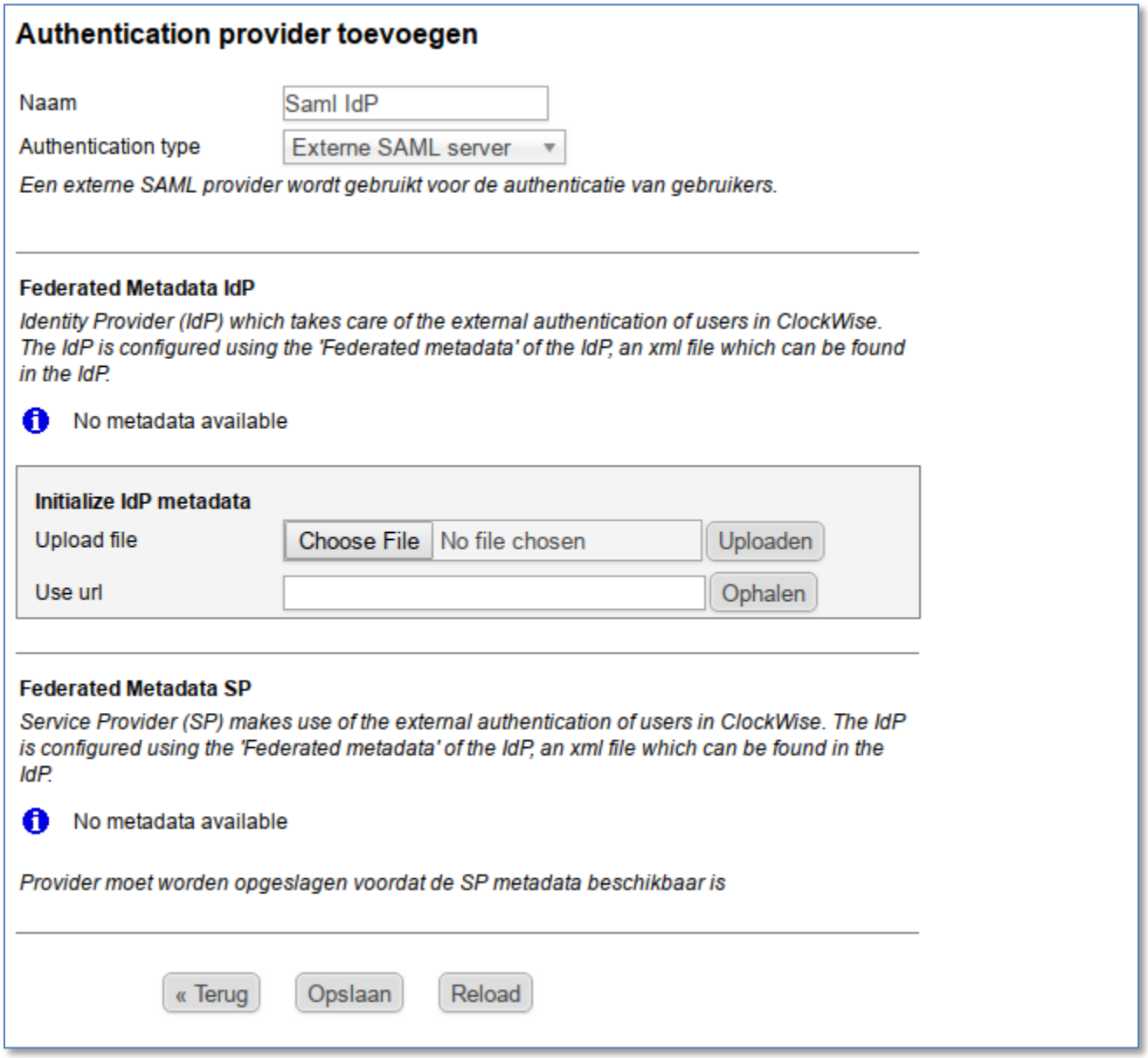
Authentication provider instellen

Het instellen van een nieuwe authentication provider gebeurd in Configuratie -> Instellingen -> Authentication providers. Hier zit een knop genaamd ‘Authentication provider toevoegen’. Mocht er op deze pagina de melding staan met de tekst ‘Authentication providers is not enabled on this system’, dan kunt u contact op nemen met ClockWise om het systeem voor het instellen van authentication providers geschikt te maken.

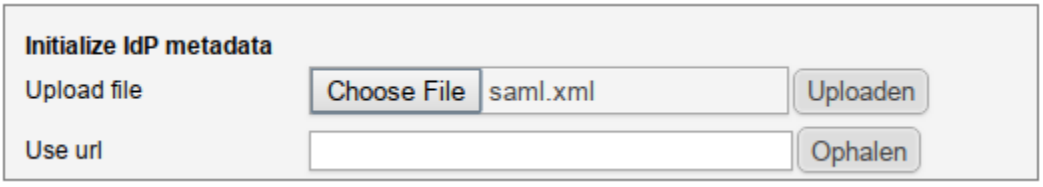


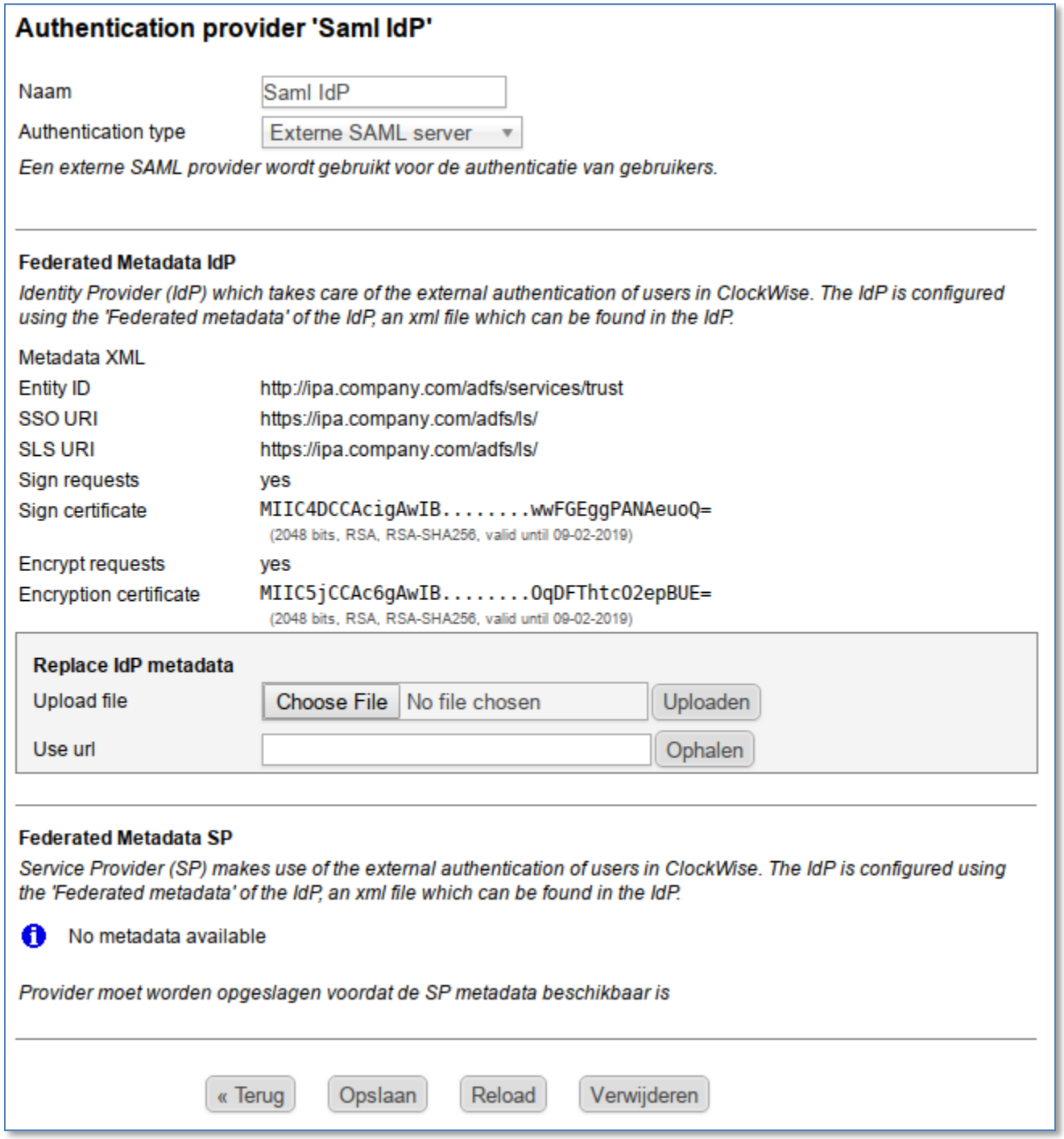
Na het drukken op de knop voor het aanmaken kan een **Naam** worden ingevoerd. Deze naam zal ook getoond worden op het inlog scherm, dus dient voor de gebruiker begrijpelijk te zijn. De naam kan op

een later moment gewijzigd worden. Vervolgens dient men te kiezen voor het **Authentication type** 'Externe SAML server'

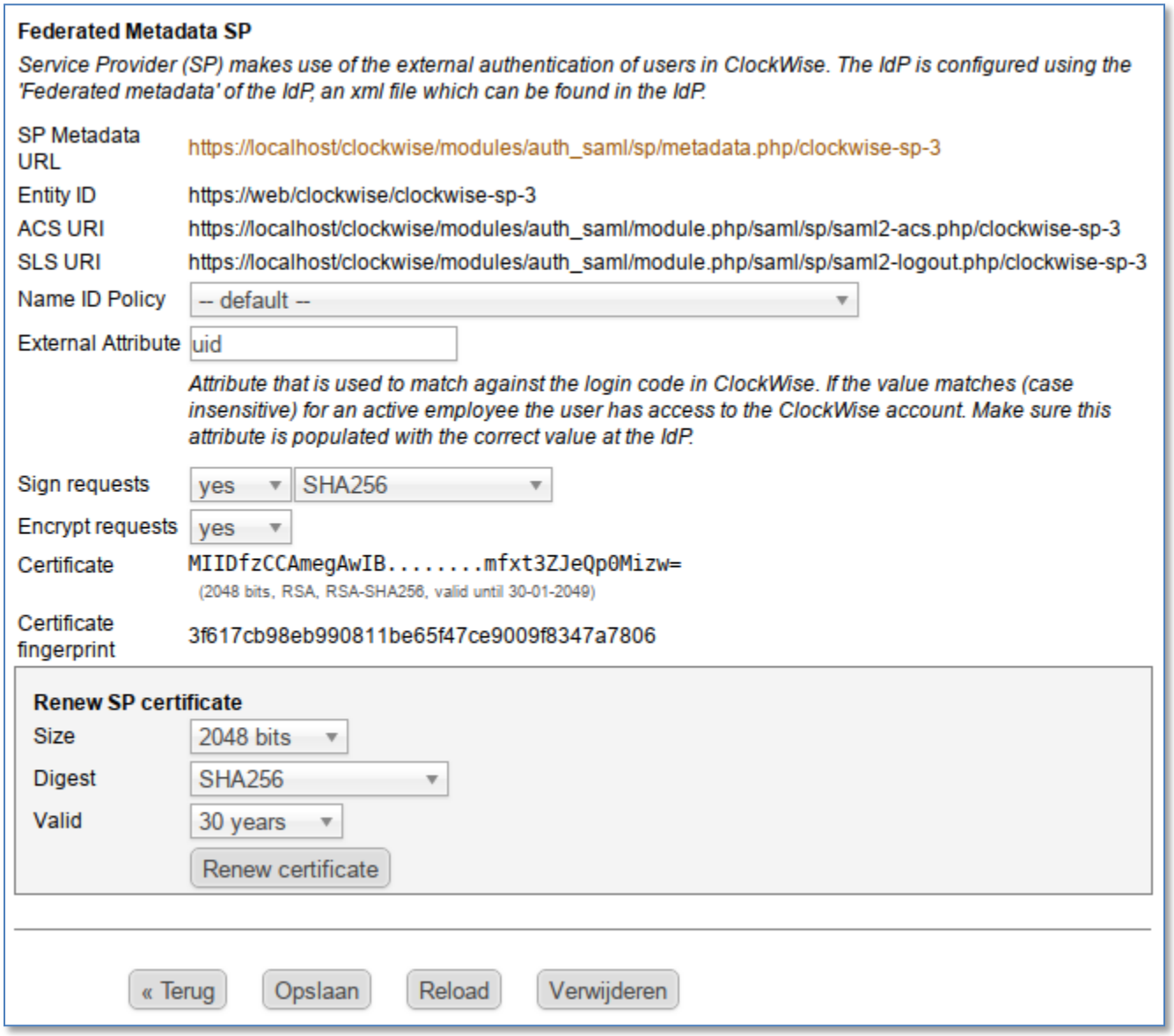


Na het kiezen van het Authentication type verschijnen er nieuwe opties. Eerst dient de metadata van de IdP ingeladen te worden. Dit kan via het uploaden van een XML bestand, of via het invoeren van een url waar de metadata in het XML formaat is te downloaden.





Na het uploaden van de IdP metadata worden de endpoints en certificaten van de IdP getoond. Als de authentication provider vervolgens wordt opgeslagen zal ook de metadata van de SP voor deze authentication provider aangemaakt en getoond worden.



Bij de instellingen van de SP zijn nog een aantal dingen te wijzigen zoals of er wel of niet signed of encrypted dataverkeer nodig is, welk attribuut gebruikt worden om de logins in de IdP en ClockWise te koppelen en het type certificaat. De standaard instellen zijn doorgaans voldoende om de koppeling tot stand te brengen. De metadata kan worden gedownload via de link '**SP Metadata URL**'. Deze metadata samen met de attribuut toekenning dient in de IdP ingeladen of ingesteld te worden. De precieze wijze van instellen verschilt per applicatie en kan in de handleiding van de IdP gevonden worden.

Het attribute, in bovenstaande voorbeeld en als standaard waarde 'uid', is het veld waarmee de gebruiker gematched wordt. De waarde van dit veld moet gelijk zijn aan de waarde van de **Loginnaam** bij de medewerker. Er wordt bij het vergelijken niet gelet op hoofd-/kleine letters. Het kan dus zijn dat voor de verdere inrichting de Loginnaam van de medewerkers moeten worden gelijkgetrokken met de 'uid' die gebruikt wordt in de IdP. Vaak is de 'uid' overigens hetzelfde als de loginnaam bij de IdP. Dit kan ook een email adres zijn. Het veld Wachtwoord bij de medewerker wordt niet meer gebruikt.

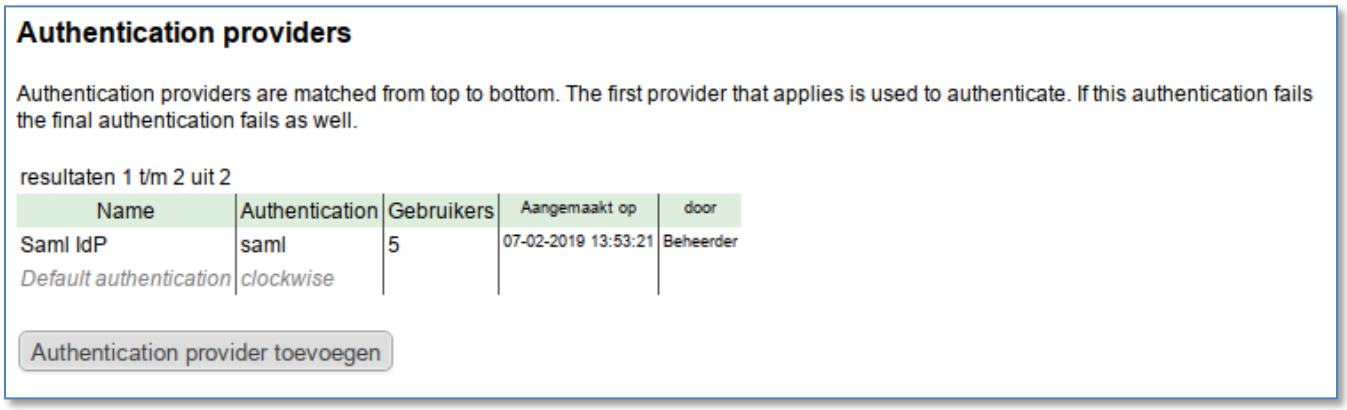
Na het aanmaken van de authentication provider zal deze verschijnen in het lijstje met authentification providers. In de kolom Gebruikers is te zien door hoeveel gebruikers de authentication provider gebruikt wordt. Elke gebruiker kan maar via één authentication provider inloggen. Alle authentication providers die tenminste door één gebruiker gebruikt wordt is weergegeven op de inlog pagina.

Om deze aangemaakt authentication provider te gebruiker dient een gebruiker via de gebruikersgroep nog ingesteld worden om de authentication provider te gebruiken. Op deze manier kan ClockWise zo ingericht worden dat verschillende afdelingen of zelfs locaties hun eigen authentication provision heeft.

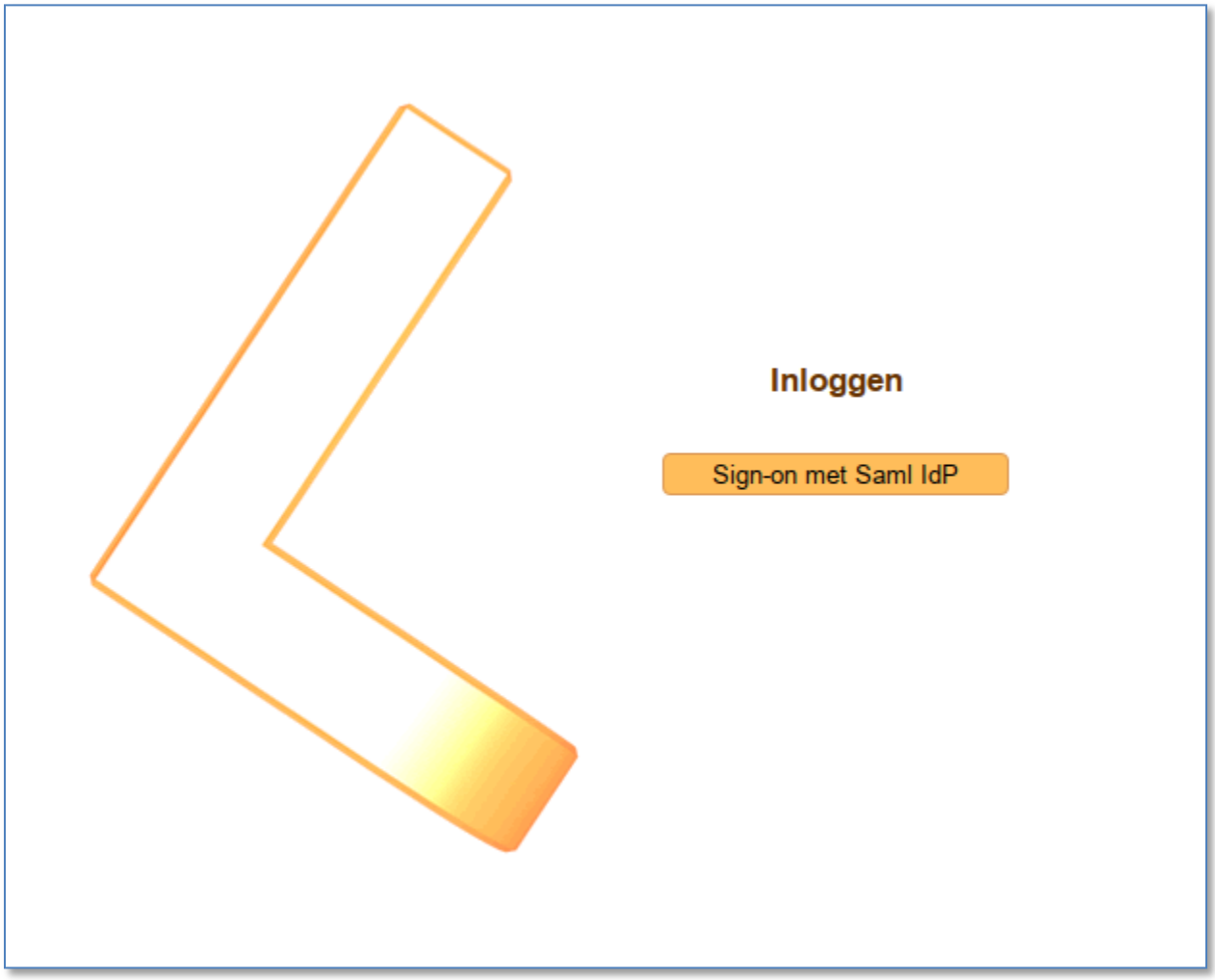
Het instellen ven de authentication provider voor iedereen gaat via Standaard instellingen -> Algemene instellingen onder het item ‘Authentication provision’. Hier kan de naam van de net aangemaakte authentiocation provider geselecteerd worden.

Log nog niet uit, want als de instelling niet goed is kan er niet meer als beheerder worden ingelogd om dingen te herstellen.

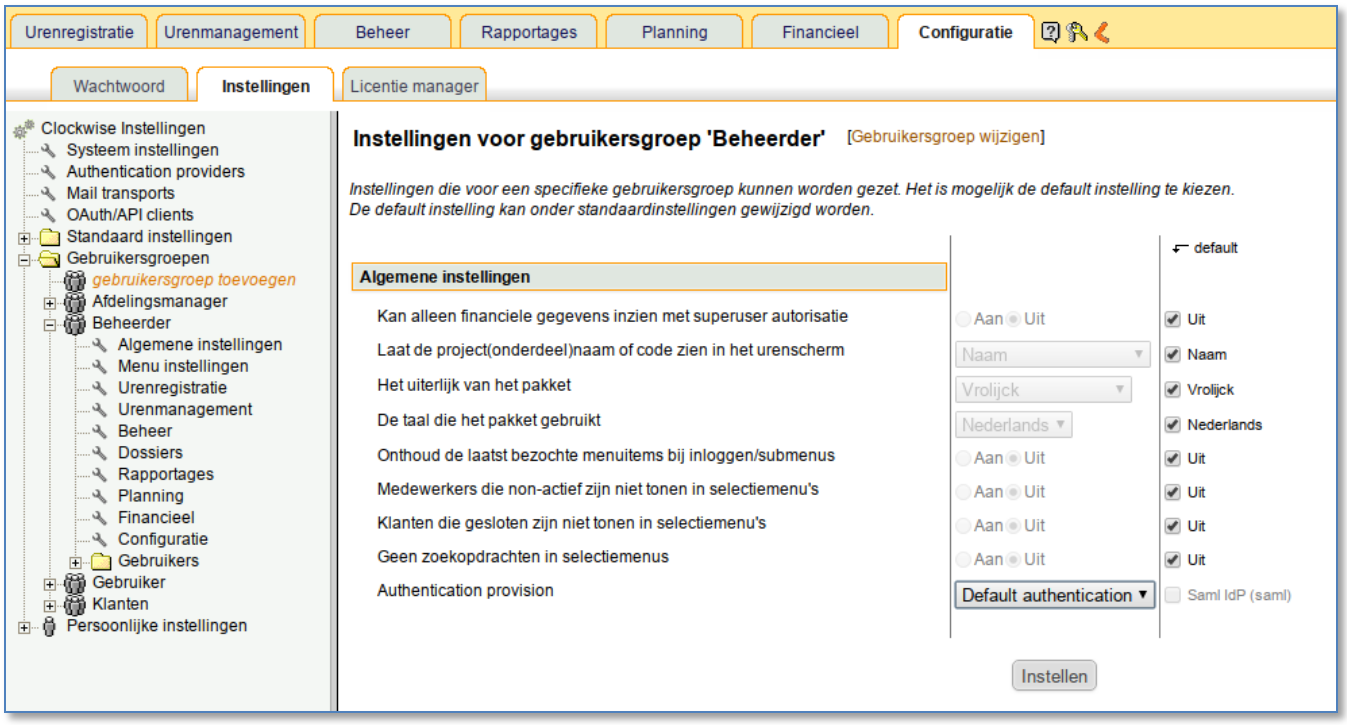
Na het instellen van deze standard authentication privision instelling zal de table met gebruikers per authentication provider er als volgt uit zien.



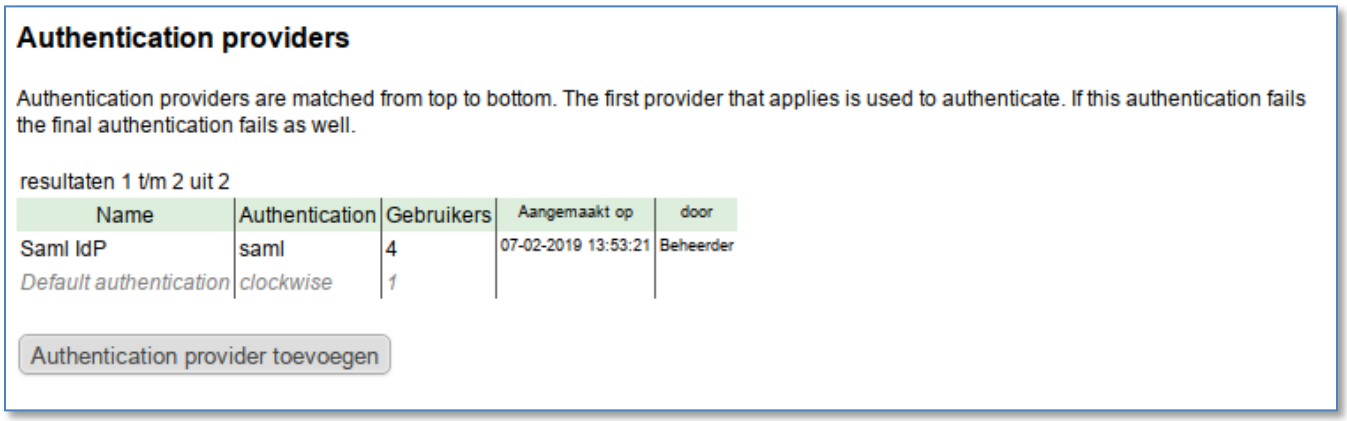
De inlog pagina toont nu maar één optie om in te loggen. Om wijzigingen aan te brengen is het verstandig om de beheerder te kunnen laten inloggen via de standaard ClockWise inlog methode.



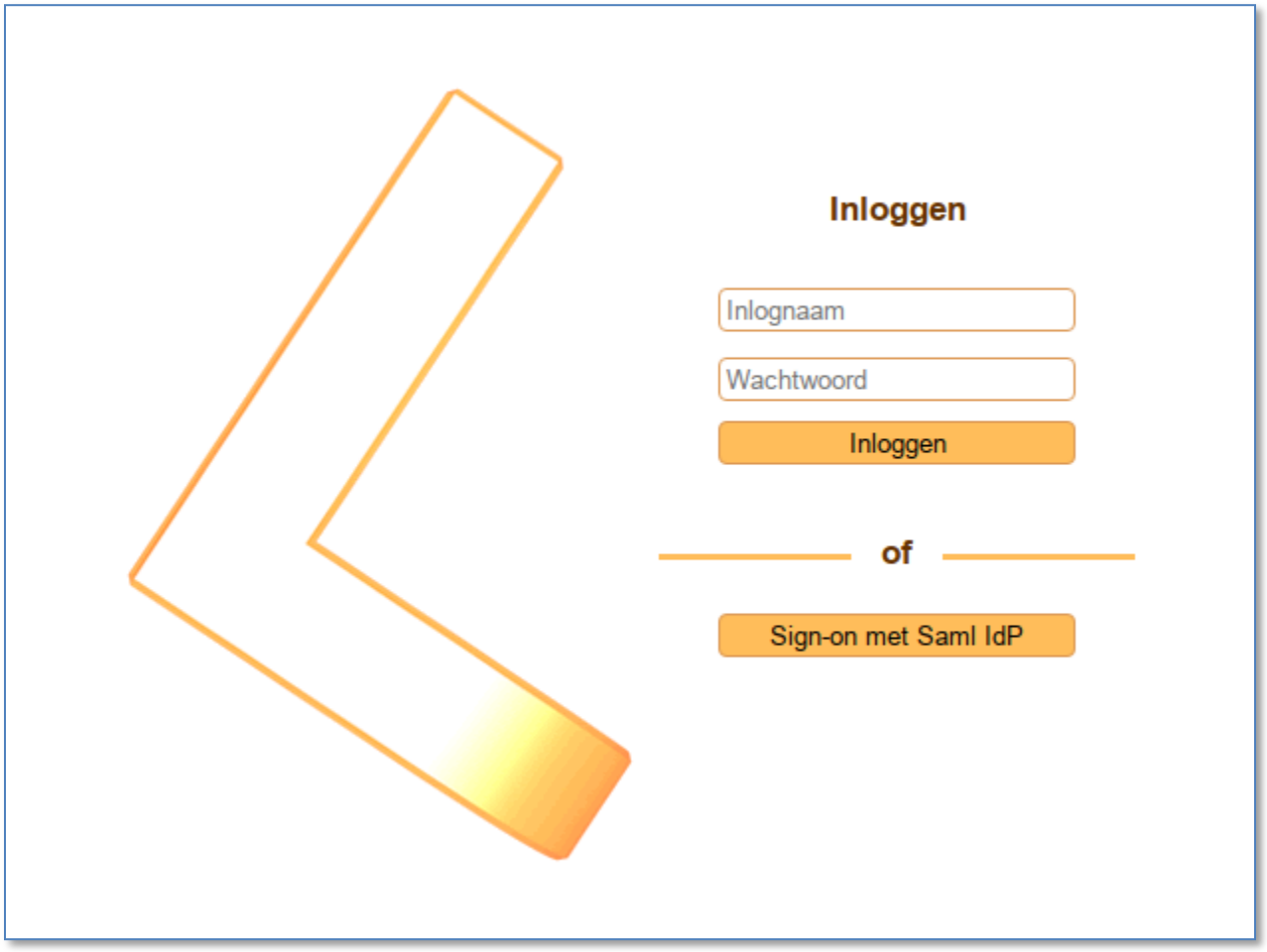
Dit kan door de gebruikersgroep ‘Beheerder’ bij onder Configuratie -> Instellingen -> Gebruikersgroepen -> Beheerder -> Algemene instellingen onder het kopje ‘Authentication provision’ de instelling ‘Default authentication’ te geven.



De lijst met gebruikers per authentication provider ziet er vervolgens als volgt uit:



En de inlog pagina toont nu twee optie om in te loggen.



In de gevallen waarbij de standaard ClockWise inlog methode als fallback optie gebruikt wordt en maar door enkele personen gebruikt wordt kan de standaard inlog, die als eerste getoond wordt en mogelijk nogal prominent als optie wordt aangeboden, naar de achtergrond verplaatst worden via een link ‘Alternatieve inlog mogelijkheden’.

Dit kan via de instelling Configuratie -> Instellingen -> Systeem instellingen onder het kopje ‘Verberg default inlog methode als er andere authentication providers beschikbaar zijn’ de optie ‘Aan’ aan te vinken.

De inlog pagina ziet er vervolgens als volgt uit: