



*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

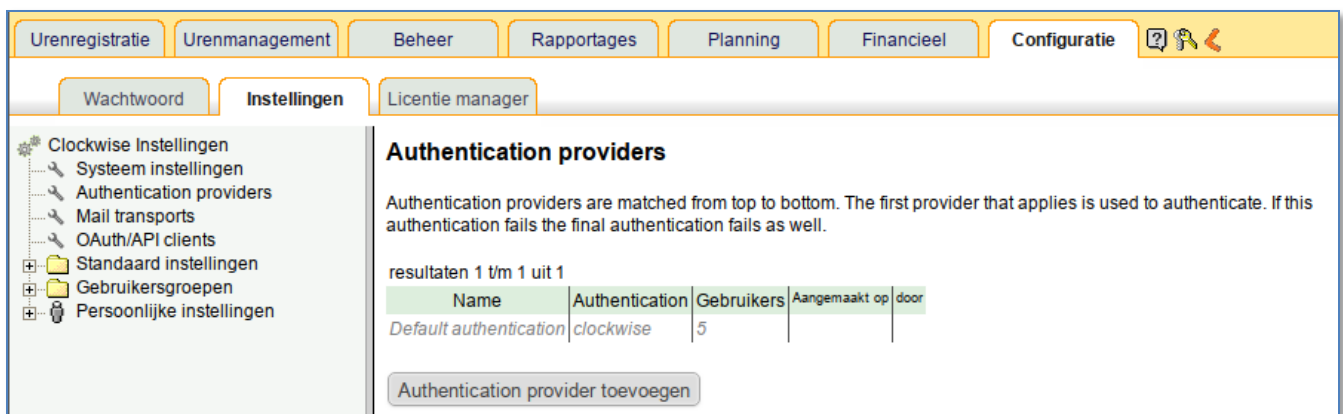
Entity ID – Identifier die de IdP of SP kenmerkt (kan een string of niet bestaande url zijn)

Attribute – De naam van een parameter waarvan de inhoud de unieke 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 gebeurt 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.



The screenshot shows the 'Configuratie' menu with 'Instellingen' selected. Under 'Instellingen', 'Authentication providers' is chosen. The main content area displays 'Authentication providers' with a descriptive text: 'Authentication providers are matched from top to bottom. The first provider that applies is used to authenticate. If this authentication fails the final authentication fails as well.' Below this, a table shows one provider:

Name	Authentication	Gebruikers	Aangemaakt op	door
Default authentication	clockwise	5		

A button 'Authentication provider toevoegen' is visible at the bottom of the configuration area.

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'

Authentication provider toevoegen

Naam

Authentication type

Een externe SAML provider wordt gebruikt voor de authenticatie van gebruikers.

Federated Metadata IdP

Identity Provider (IdP) which takes care of the external authentication of users in ClockWise. The IdP is configured using the 'Federated metadata' of the IdP, an xml file which can be found in the IdP.

i No metadata available

Initialize IdP metadata

Upload file

Use url

Federated Metadata SP

Service Provider (SP) makes use of the external authentication of users in ClockWise. The IdP is configured using the 'Federated metadata' of the IdP, an xml file which can be found in the IdP.

i No metadata available

Provider moet worden opgeslagen voordat de SP metadata beschikbaar is

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.

Initialize IdP metadata

Upload file

Use url

Authentication provider 'Saml IdP'

Naam

Authentication type

Een externe SAML provider wordt gebruikt voor de authenticatie van gebruikers.

Federated Metadata IdP

Identity Provider (IdP) which takes care of the external authentication of users in ClockWise. The IdP is configured using the 'Federated metadata' of the IdP, an xml file which can be found in the IdP.

Metadata XML

Entity ID	http://ipa.company.com/adfs/services/trust
SSO URI	https://ipa.company.com/adfs/ls/
SLS URI	https://ipa.company.com/adfs/ls/
Sign requests	yes
Sign certificate	MIIC4DCCAcigAwIB.....wwFGEggPANAEuoQ= (2048 bits, RSA, RSA-SHA256, valid until 09-02-2019)
Encrypt requests	yes
Encryption certificate	MIIC5jCCAc6gAwIB.....0qDFThtc02epBUE= (2048 bits, RSA, RSA-SHA256, valid until 09-02-2019)


Replace IdP metadata

Upload file

Use url

Federated Metadata SP

Service Provider (SP) makes use of the external authentication of users in ClockWise. The IdP is configured using the 'Federated metadata' of the IdP, an xml file which can be found in the IdP.

 No metadata available

Provider moet worden opgeslagen voordat de SP metadata beschikbaar is

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.

Federated Metadata SP

Service Provider (SP) makes use of the external authentication of users in ClockWise. The IdP is configured using the 'Federated metadata' of the IdP, an xml file which can be found in the IdP.

SP Metadata URL https://localhost/clockwise/modules/auth_saml/sp/metadata.php/clockwise-sp-3

Entity ID <https://web/clockwise/clockwise-sp-3>

ACS URI https://localhost/clockwise/modules/auth_saml/module.php/saml/sp/saml2-acis.php/clockwise-sp-3

SLS URI https://localhost/clockwise/modules/auth_saml/module.php/saml/sp/saml2-logout.php/clockwise-sp-3

Name ID Policy

External Attribute

Attribute that is used to match against the login code in ClockWise. If the value matches (case insensitive) for an active employee the user has access to the ClockWise account. Make sure this attribute is populated with the correct value at the IdP.

Sign requests

Encrypt requests

Certificate **MIIDfzCCAmegAwIB.....mfxT3ZJeQp0Mizw=**
(2048 bits, RSA, RSA-SHA256, valid until 30-01-2049)

Certificate fingerprint **3f617cb98eb990811be65f47ce9009f8347a7806**

Renew SP certificate

Size

Digest

Valid

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 authentication 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 aangemaakte authentication provider te gebruiken 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.

Authentication providers

Authentication providers are matched from top to bottom. The first provider that applies is used to authenticate. If this authentication fails the final authentication fails as well.

resultaten 1 t/m 2 uit 2

Name	Authentication	Gebruikers	Aangemaakt op	door
Saml IdP	saml		07-02-2019 13:53:21	Beheerder
Default authentication	clockwise	5		

Authentication provider toevoegen

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

The screenshot shows the 'Configuratie' (Configuration) section of the ClockWise system. The 'Instellingen' (Settings) tab is active, and the 'Standaard instellingen' (Standard settings) sub-tab is selected. The 'Algemene instellingen' (General settings) section is expanded, showing various system-wide settings. The 'Authentication provision' setting is highlighted, and its value is 'Saml IdP (saml)'. The page also includes a sidebar with a tree view of settings categories and a top navigation bar with tabs for different system functions.

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 prvision instelling zal de table met gebruikers per authentication provider er als volgt uit zien.

Authentication providers

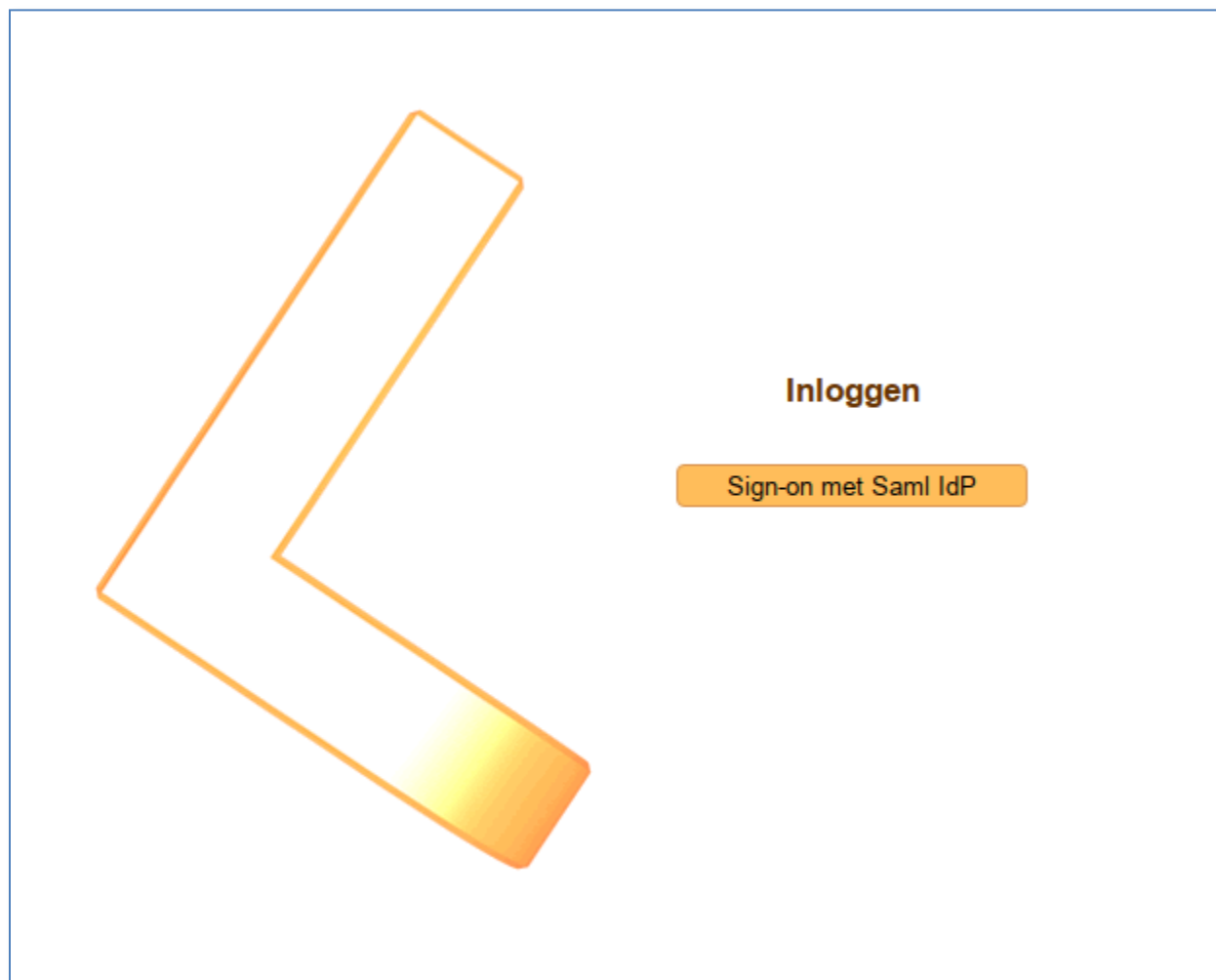
Authentication providers are matched from top to bottom. The first provider that applies is used to authenticate. If this authentication fails the final authentication fails as well.

resultaten 1 t/m 2 uit 2

Name	Authentication	Gebruikers	Aangemaakt op	door
Saml IdP	saml	5	07-02-2019 13:53:21	Beheerder
<i>Default authentication</i>	<i>clockwise</i>			

[Authentication provider toevoegen](#)

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.

The screenshot shows the configuration interface for the 'Beheerder' user group. The left sidebar contains a tree view of settings categories. The main content area is titled 'Instellingen voor gebruikersgroep 'Beheerder'' and includes a section for 'Algemene instellingen' with various toggle and dropdown options. The 'Authentication provision' section is expanded, showing 'Default authentication' as the selected option.

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

Authentication providers

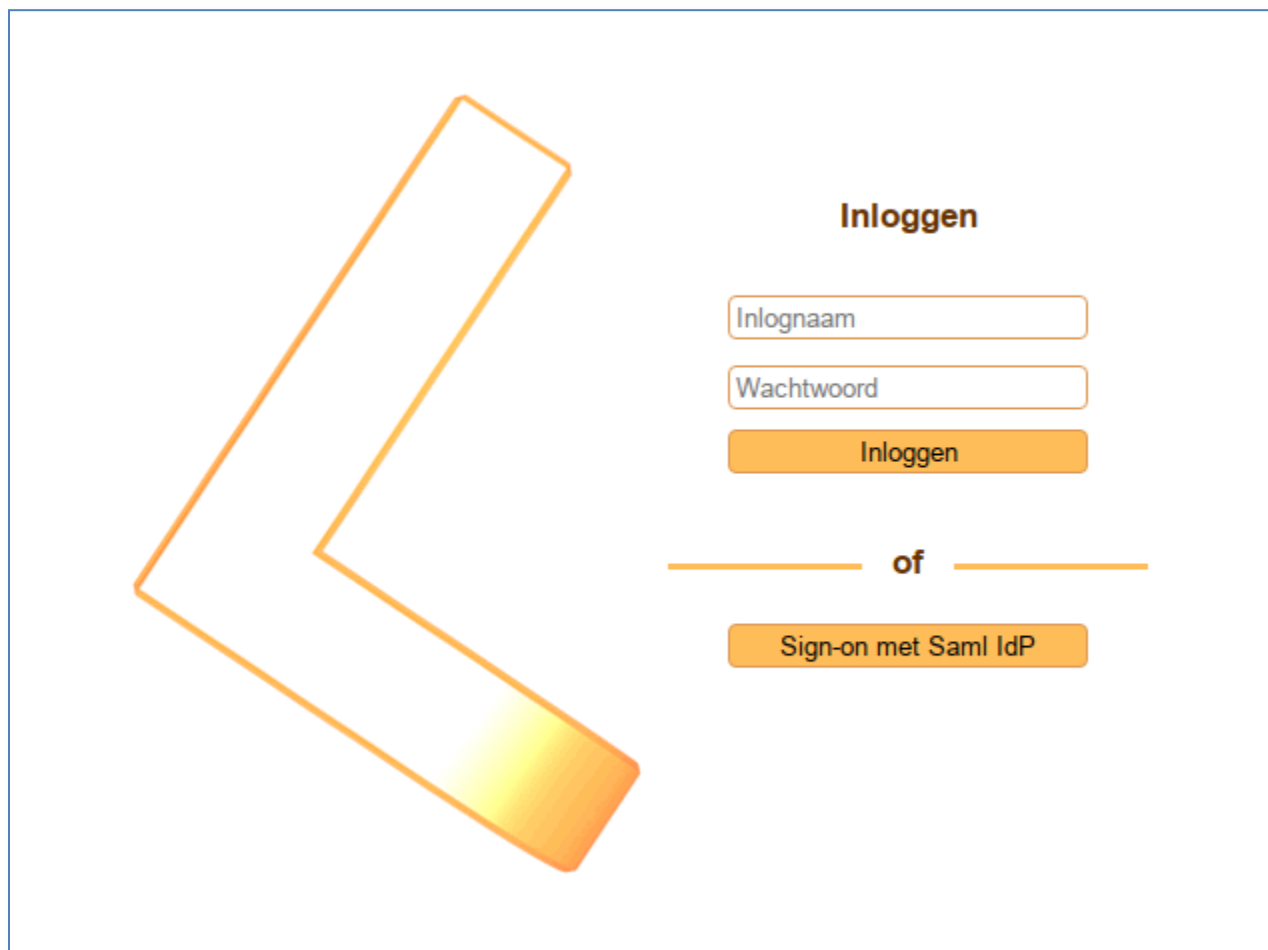
Authentication providers are matched from top to bottom. The first provider that applies is used to authenticate. If this authentication fails the final authentication fails as well.

resultaten 1 t/m 2 uit 2

Name	Authentication	Gebruikers	Aangemaakt op	door
Saml IdP	saml	4	07-02-2019 13:53:21	Beheerder
Default authentication	clockwise	1		

Authentication provider toevoegen

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.

Urenregistratie Urenmanagement Beheer Rapportages Planning Financieel Configuratie

Wachtwoord Instellingen Licentie manager

Clockwise Instellingen
 Systeem instellingen
 Authentication providers
 Mail transports
 OAuth/API clients
 Standaard instellingen
 Gebruikersgroepen
 Persoonlijke instellingen

Systeem instellingen

Instellingen die eenmalig voor het hele pakket ingesteld kunnen worden. Systeeminstellingen kunnen niet per gebruikersgroep of per gebruiker worden gewijzigd.

	default instelling	instelbaarper
Mogelijkheid om klantgroepen aan te maken	<input type="radio"/> Aan <input checked="" type="radio"/> Uit	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Mogelijkheid om records met 0-uren aan te maken	<input type="radio"/> Aan <input checked="" type="radio"/> Uit	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Globaal email adres van de applicatiebeheerder	<input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Managers kunnen ook gekoppeld worden op het niveau waar resource koppelingen staan	<input type="radio"/> Aan <input checked="" type="radio"/> Uit	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Verzonden facturen kunnen niet gewist of gewijzigd worden. Gefactureerde klanten en projecten kunnen niet gewist worden.	<input type="radio"/> Aan <input checked="" type="radio"/> Uit	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Startdatum van het pakket	<input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Klant voor stamgegevens	<input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Verberg default inlog methode als er andere authentication providers beschikbaar zijn	<input checked="" type="radio"/> Aan <input type="radio"/> Uit	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

De inlog pagina ziet er vervolgens als volgt uit:



Inloggen

[Sign-on met SAML IDP](#)

[Alternatieve inlog mogelijkheden »](#)