SAML

Last Modified on 17/12/2024 1:54 pm ACDT

CareRight now supports SAML as an authentication mechanism.

When correctly configured; it allows your users to login to the CareRight system via the configured Identity Provider.

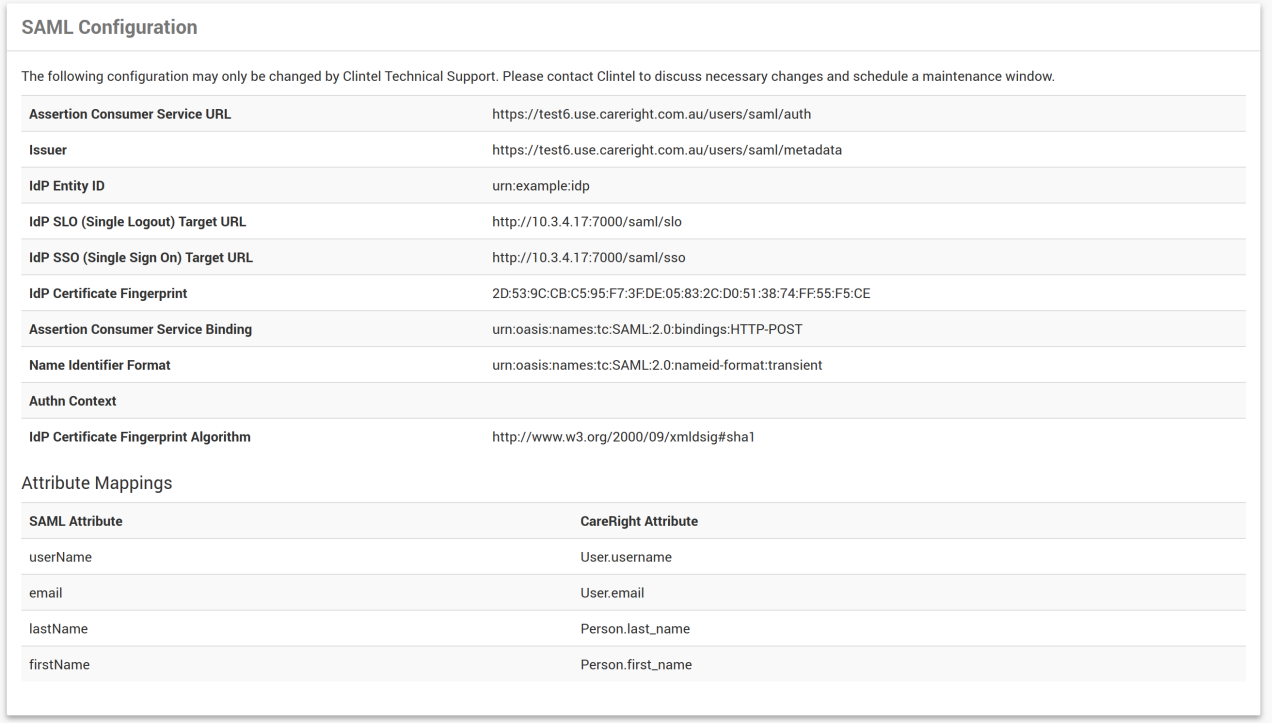
Testing

We recommend the use of browser plugins such as saml-tracer to assist in tracing and determining problems.

Configuration

Navigate to System Administration > Users and Groups > SAML.

Typically, Clintel Systems will have configured your deployment, and you can view your settings:



SAML Configuration

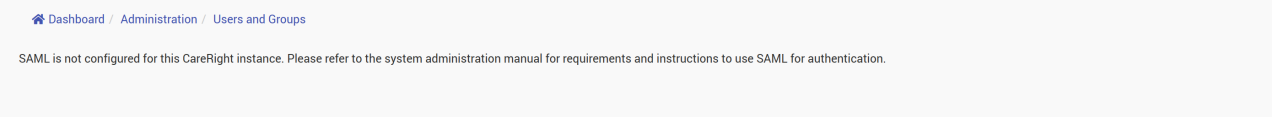
The following configuration may only be changed by Clintel Technical Support. Please contact Clintel to discuss necessary changes and schedule a maintenance window.

Assertion Consumer Service URL	https://test6.use.careright.com.au/users/saml/auth
Issuer	https://test6.use.careright.com.au/users/saml/metadata
IdP Entity ID	urn:example:idp
IdP SLO (Single Logout) Target URL	http://10.3.4.17:7000/saml/slo
IdP SSO (Single Sign On) Target URL	http://10.3.4.17:7000/saml/sso
IdP Certificate Fingerprint	2D:53:9C:CB:C5:95:F7:3F:DE:05:83:2C:D0:51:38:74:FF:55:F5:CE
Assertion Consumer Service Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
Name Identifier Format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Authn Context	
IdP Certificate Fingerprint Algorithm	http://www.w3.org/2000/09/xmldsig#sha1

Attribute Mappings

SAML Attribute	CareRight Attribute
userName	User.username
email	User.email
lastName	Person.last_name
firstName	Person.first_name

If it has not yet been configured, you will see:



Dashboard / Administration / Users and Groups

SAML is not configured for this CareRight instance. Please refer to the system administration manual for requirements and instructions to use SAML for authentication.

The full list of attributes that can be mapped via claims:

Refer to Admin > Documentation Items for the applicable list for your version of CareRight.

- All core User fields
- All core Person fields

- All core Staff Member fields (as of 6.96 or higher)
- Job Title
- Groups

Recommended configuration for Azure

https://docs.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol

```
assertion_consumer_service_url: https://sandbox1.use.careright.com.au/users/saml/auth

# our test azure instance:
idp_slo_target_url: https://login.microsoftonline.com/(instance id)/saml2
idp_sso_target_url: https://login.microsoftonline.com/(instance id)/saml2
idp_cert_fingerprint: (fingerprint)

# this is the their entity ID.  from XML. (EntityDescriptor#entityID).  In Azure is called "Azure AD Identifier"
idp_entity_id: https://sts.windows.net/(id)/

# this is OUR entity ID, previously referred to as issuer
sp_entity_id: https://sandbox1.use.careright.com.au/users/saml/metadata

assertion_consumer_service_binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
name_identifier_format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
authn_context:
idp_cert_fingerprint_algorithm: http://www.w3.org/2000/09/xmldsig#sha1
```

```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress: "User.email"
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname: "Person.first_name"
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name: "User.username"
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname: "Person.last_name"


# Optional claims
http://schemas.microsoft.com/identity/claims/displayname: "Person.primary_display_name"
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/jobtitle: "Other.job_title"

# Either map users by department (singular) or
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department: "Group.name"
# Map by groups
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups: "Group.name"
```

Multiple Groups - Configuring Azure

We recommend following guides such as https://wiki.resolution.de/doc/saml-sso/5.0.x/jira/knowledgebase-articles/technical/jit-and-azure-ad-sending-groups-via-saml-attributes

Ensure you are sending:

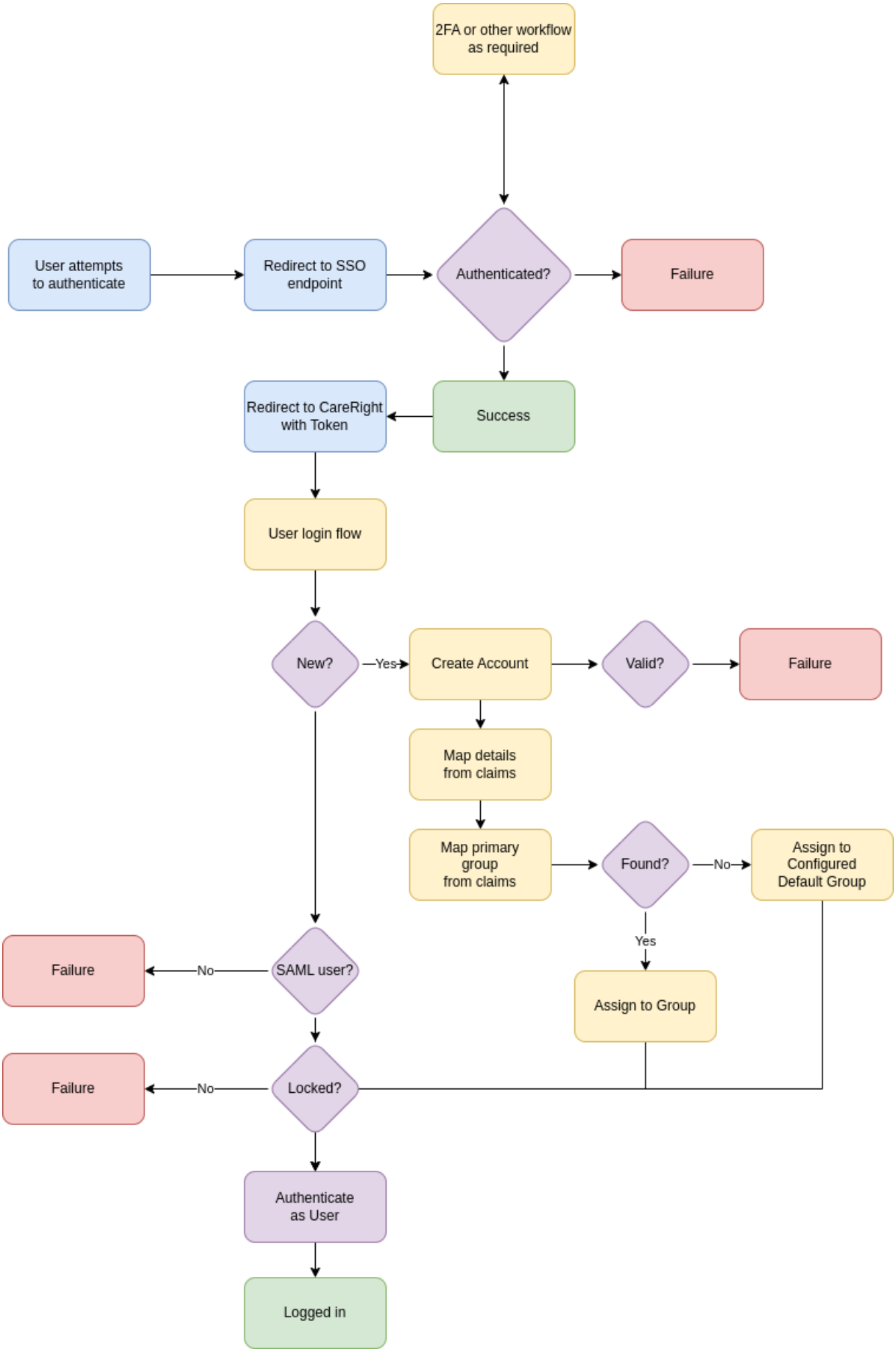
- A group claim
- Group names, not group IDs

Recommended configuration for Okta

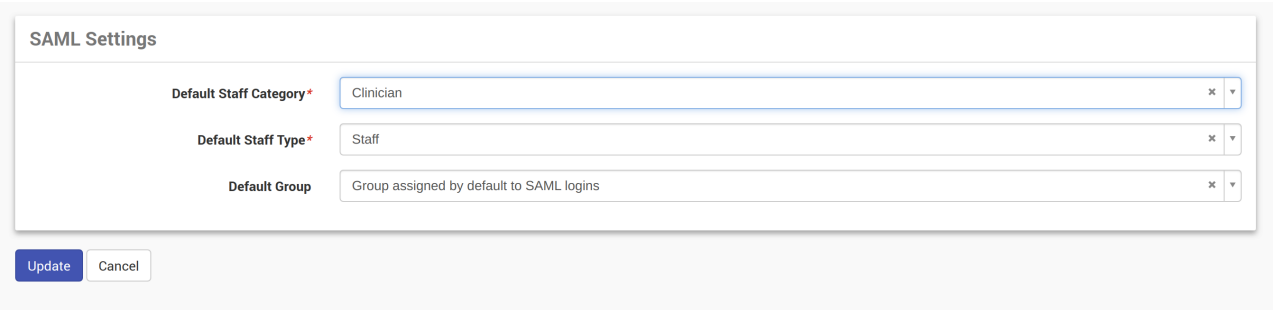
```
set :saml_enabled, true
set :saml_assertion_consumer_service_url,     "https://example-test.use.careright.com.au/users/saml/auth"
set :saml_issuer,                             "http://www.okta.com/unique_id_here"
set :saml_sp_entity_id,                       "https://example-test.use.careright.com.au/users/saml/metadata"
set :saml_assertion_consumer_service_binding, "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
set :saml_name_identifier_format,             "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
set :saml_authn_context,                      "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
set :saml_idp_cert_fingerprint_algorithm,     "http://www.w3.org/2000/09/xmldsig#sha1"


# attribute mappings - this is the default for OKTA SSO
set :saml_username_attribute,   "name"
set :saml_email_attribute,      "emailaddress"
set :saml_last_name_attribute,  "surname"
set :saml_first_name_attribute, "givenname"
set :saml_group_name_attribute, "division"
set :saml_job_title_attribute, "jobtitle"


# SAML - OKTA:
set :saml_idp_entity_id,                      "http://www.okta.com/unique_id_here"
set :saml_idp_slo_target_url,                 "https://login.company.com.au/app/application_name/unique_id_here/sso/saml
"
set :saml_idp_sso_target_url,                 "https://login.company.com.au/app/application_name/unique_id_here/sso/saml
"
set :saml_idp_cert_fingerprint,               "00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00"
```

Default Behaviours

CareRight's workflow is as per the below diagram



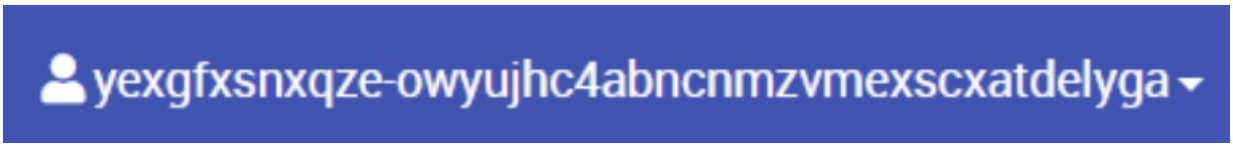
When a new user is registered, they will be created as a particular staff type, and optionally assigned roles.



User display

Some identity providers generate long user identifiers, which aren't suitable.

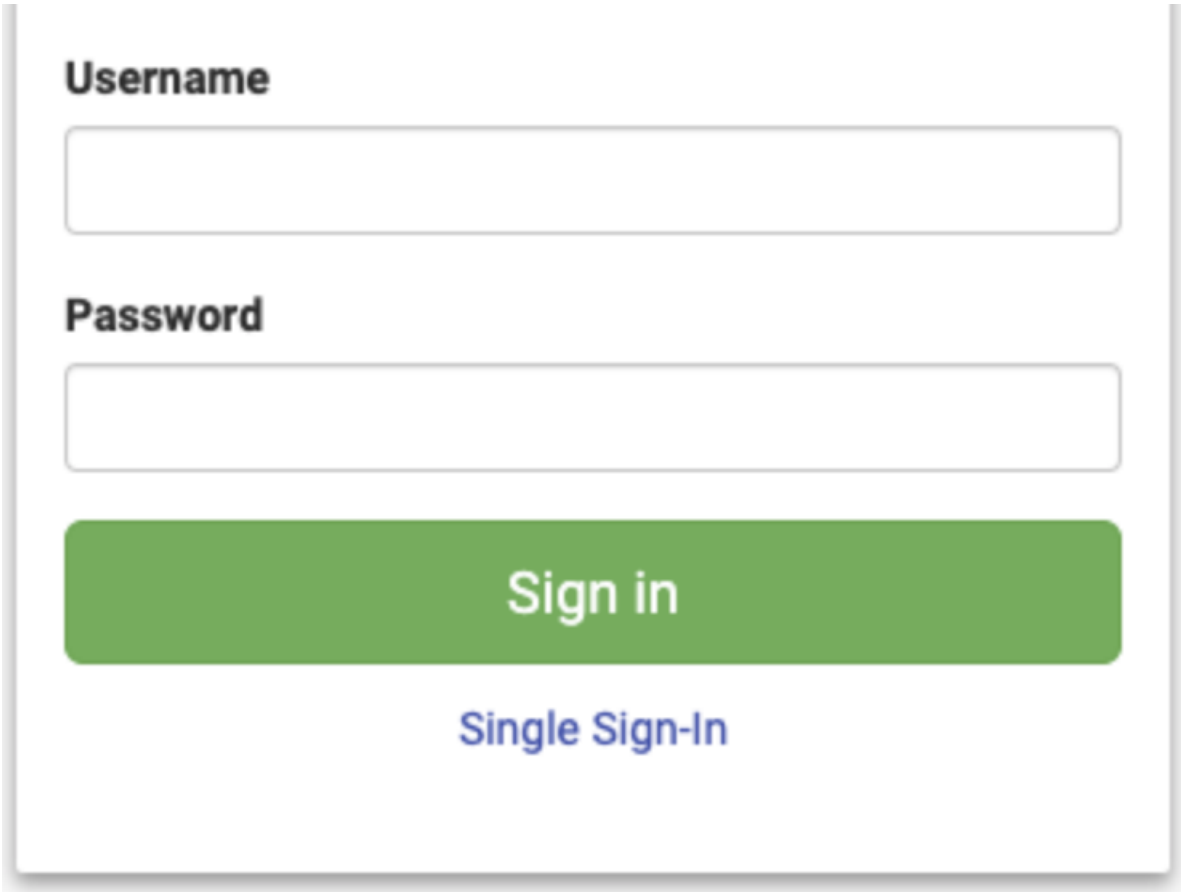
Example:



To change this behaviour, under **System Administration > Global Settings** you can swap to 'Username', 'Email' or'Display name'

Account Login

When configured, users can simply choose to *Single Sign In* to start the authentication process.



Common problems

Multiple user accounts with the same email

Within Careright, a user account must have a unique email. This means if you create a *Standard* user account for example@example.com; when authenticating with SAML it will not allow a user to be created with that email.

Users must re-authenticate with their password credentials to link accounts.

Bespoke behaviour

User group mapping to staff type

As of CareRight 6.97.20; the following groups are detected on authentication and automatically add a corresponding staff type

- CareRight-Exercise Physiology-Student -> Exercise Physiology Student
- CareRight-Nutrition & Dietetics-Student -> Nutrition Student
- CareRight-Optometry-Student -> Optometry Student
- CareRight-Podiatry-Student -> Podiatry Student
- CareRight-Psychology & Counselling-Student -> Psychology Student