Configure Single Sign On

Last Modified on 24/02/2022 10:03 am AEDT

Single sign-on (SSO) allows centralised user management via an identity provider such as 'OpenID Connect' and 'SAML' (permissions are still configured in the ReadiNow tenant).

Note: SSO configuration is done on a per tenant basis, customers with multiple tenants can repeat the configure for each tenant as required.

This article explains how to:

- configure new identity providers
- update expired certificates
- troubleshoot common errors

Terminology

Identity Provider (IDP)

An identity provider is a service that stores and verifies user identities, such as Microsoft Azure, Okta or Ping. ReadiNow cannot assist with the configuration of your identity provider.

SAML and OIDC

Identity providers can be configured to use different protocols. ReadiNow supports both SAML and OIDC (OpenID Connect). The team responsible for your identity provider will advise you which protocol to use when configuring your ReadiNow tenant.

Internal versus external Identity Providers

When configuring your ReadiNow tenant you will need to know if your identity provider is internal or external as this changes the configuration. Internal and external are defined as follows:

- Internal - cannot be accessed by ReadiNow's servers, e.g. an ADFS server behind a company's firewall.
- External - is accessible by ReadiNow's servers, e.g. Microsoft Azure.

When configuring an internal provider, the identity provider's metadata must be entered in ReadiNow during the identity provider creation. An administrator will need to download the metadata from the identity provider and save it as a document.

Automatic Login

If automatic login is enabled and the user cannot log in, then navigating back to the login page again will present the user with an option to select a different identity provider. This is useful for users with multiple accounts, such as administrators. SSO will only fail if the identity provider is unavailable, or the user has been disabled by the identity provider.

SSO Auto Provisioning

Automatic user provisioning means that when an administrator creates or modifies a user account in your identity provider, then a corresponding account for that user will created or modified within your ReadiNow tenant.

SP- vs IDP-initiated SSO

Service Provider Initiated (SP-initiated) SSO gives your users the ability to sign into the ReadiNow login page. ReadiNow then sends an authorisation request to your IDP to authenticate the user. With Identity Provider Initiated (IdP-initiated) SSO, the user must first log into your IDP's SSO page and then click an icon to log into ReadiNow.

Claim Mappings

In SSO, a claim is an assertion that a particular user has a particular property. Claim or attribute mappings are used to map values that exist in your identity provider to the corresponding values within ReadiNow during user auto provisioning. For example, your identity provider may have a field called "Surname". The claim will map this field to the corresponding field in ReadiNow called "Last Name".

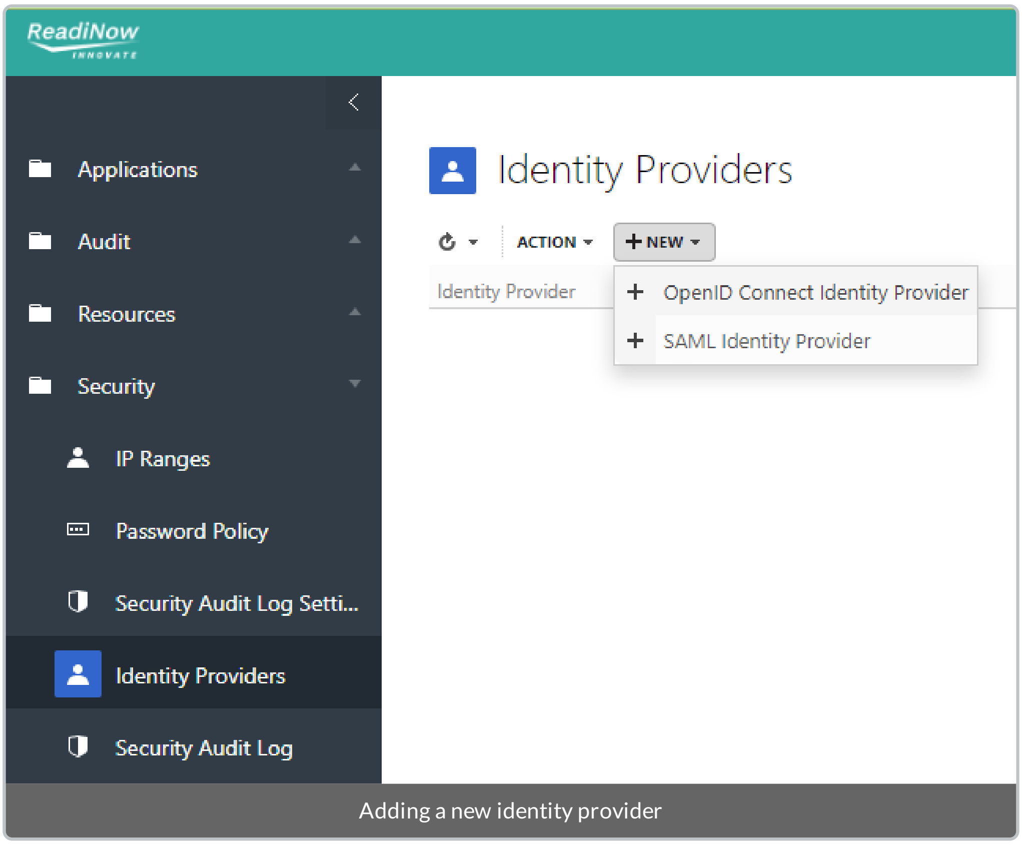
Quick Start Guide

Open the Identity Provider configuration screen

In the left menu, go to: ***Administration > Security > Identity Providers*** > *New*

Select the identity provider type:

- OIDC – OpenID Connect
- SAML



Adding a new identity provider

Common Options

Regardless of whether your identify provider uses SAML or OIDC:

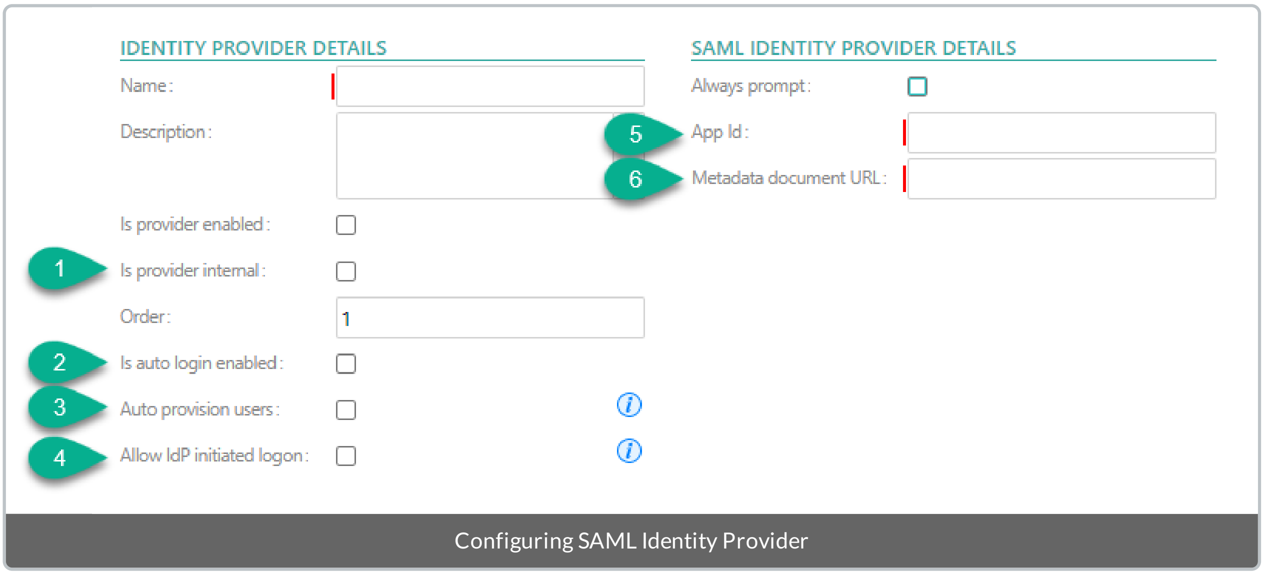
- The identity provider will need a Name, use a descriptive name of your choosing
- Add a Description to include any notes required to describe this configuration
- The identity provider will be enabled by default (to disable, uncheck: Is provider enabled).
- You can specify the Order of preference of the identity providers, if you have multiple providers configured.

SAML quick start

To configure your ReadiNow tenant for SAML SSO, the following information is necessary. Typically, this is provided by the team responsible for your IDP.

1. Whether your IDP is internal or external
2. Decide if users should be logged in automatically or prompted
3. Decide if users should be auto provisioned
4. Decide if SSO will be SP or IDP initiated
5. App Id (sometimes referred to as the Entity ID)
6. A copy of the federation metadata document if your IDP is internal OR the URL for the metadata if your IDP is external

Use this information to configure the SAML Identity Provider in your ReadiNow tenant



IDENTITY PROVIDER DETAILS

Name:

Description:

Is provider enabled: □

Is provider internal: □

Order: 1

Is auto login enabled: □

Auto provision users: □

Allow IdP initiated logon: □

SAML IDENTITY PROVIDER DETAILS

Always prompt: □

App Id:

Metadata document URL:

Configuring SAML Identity Provider

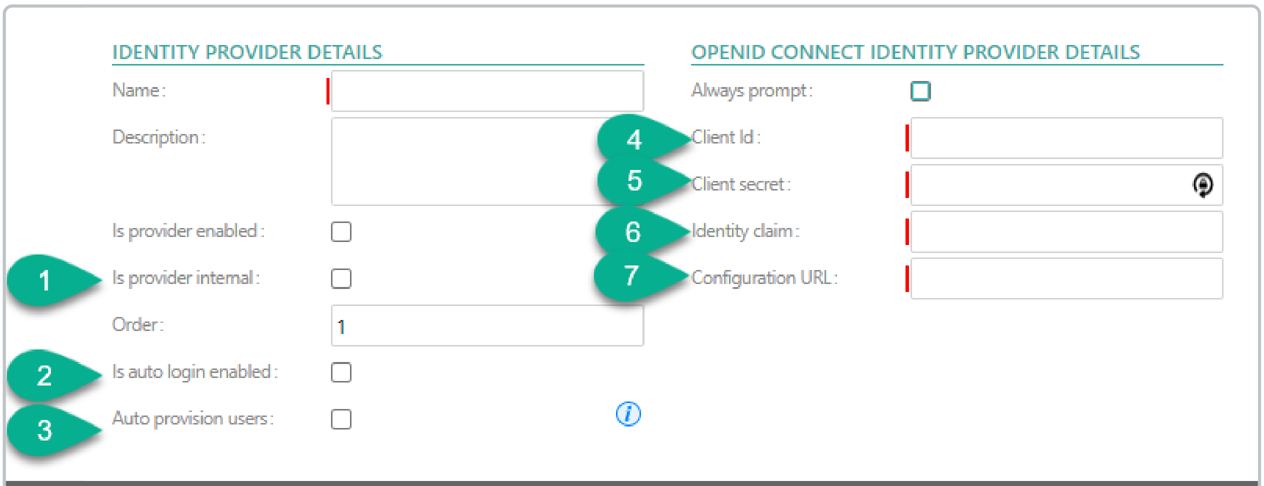
Once your tenant has been configured to connect to your identity provider, the next step is to configure your users unless auto provisioning has been enabled.

OIDC quick start

To configure your ReadiNow tenant for OIDC SSO, the following information is necessary. Typically, this is provided by the team responsible for your IDP.

1. Whether your IDP is internal or external
2. Decide if users should be logged in automatically or prompted
3. Decide if users should be auto provisioned
4. Client Id (sometimes referred to as the Application ID)
5. Client Secret (sometimes referred to as the Application Key) for external IDPs
6. Identity claim
7. The URL for the metadata if your IDP is external OR copies of the configuration document and JSON web key set document

Use this information to configure the OIDC Identity Provider in your ReadiNow tenant



IDENTITY PROVIDER DETAILS

Name :

Description :

Is provider enabled : □

Is provider internal : □

Order : 1

Is auto login enabled : □

Auto provision users : □

OPENID CONNECT IDENTITY PROVIDER DETAILS

Always prompt : □

Client Id :

Client secret :

Identity claim :

Configuration URL :

Configuring OIDC Identity Provider

Once your tenant has been configured to connect to your identity provider, the next step is to configure your users unless auto provisioning has been enabled.

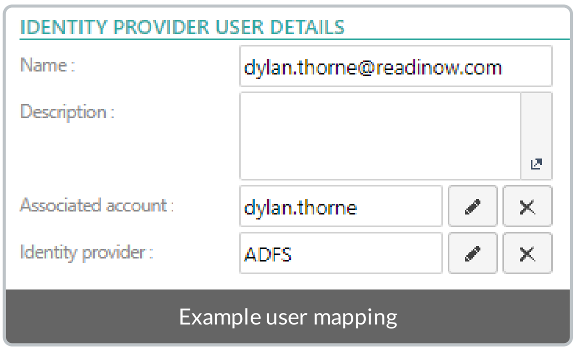
Users

Manual user provisioning

Note: This section can be ignored if 'auto provision users' is enabled.

The lower part of the configuration page contains mappings for the identity provider users. All users that login with SSO need to be added to this section.

To add a user, enter their 'email address' in the 'Name' field and select the Associated account



IDENTITY PROVIDER USER DETAILS

Name : dylan.thorne@readinow.com

Description :

Associated account : dylan.thorne

Identity provider : ADFS

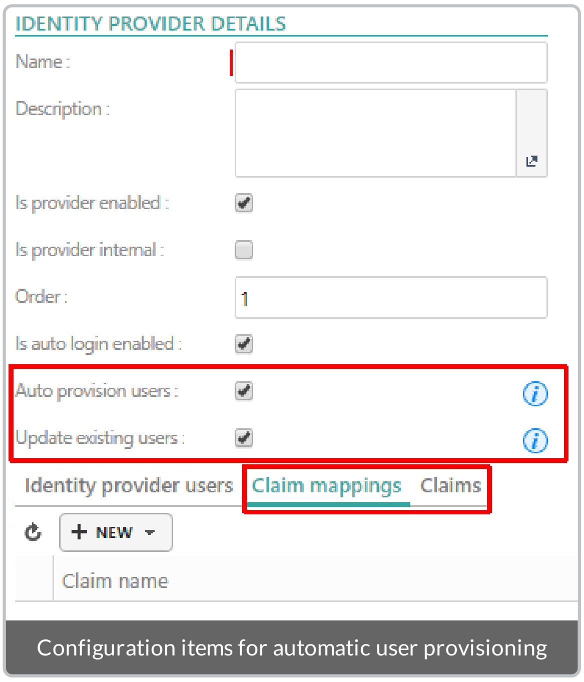
Example user mapping

Automatic User Provisioning

Automatic user provisioning will create or modify user accounts. Roles must already exist in ReadiNow. The auto-provisioning process does not create roles.

Users may not be able to log in if automatic provisioning is incorrectly configured. It is recommended to initially configure this in a non-production environment to verify the configuration.

Enable automatic user provisioning by checking Auto provision users. This will reveal the 'Update existing users' option and the Claim mappings and Claims tabs.



IDENTITY PROVIDER DETAILS

Name :

Description :

Is provider enabled : ☑

Is provider internal : □

Order : 1

Is auto login enabled : ☑

Auto provision users : ☑

Update existing users : ☑

Configuration items for automatic user provisioning

'Update existing users'

- If unchecked, only user accounts that do not exist will be created using the specified claim mappings.
- If checked, existing user accounts will also be updated based on the specified claim mappings.

Claim Mappings

Claim mappings need to be configured so that a user account can be successfully provisioned. Typically, this means that mappings are required for:

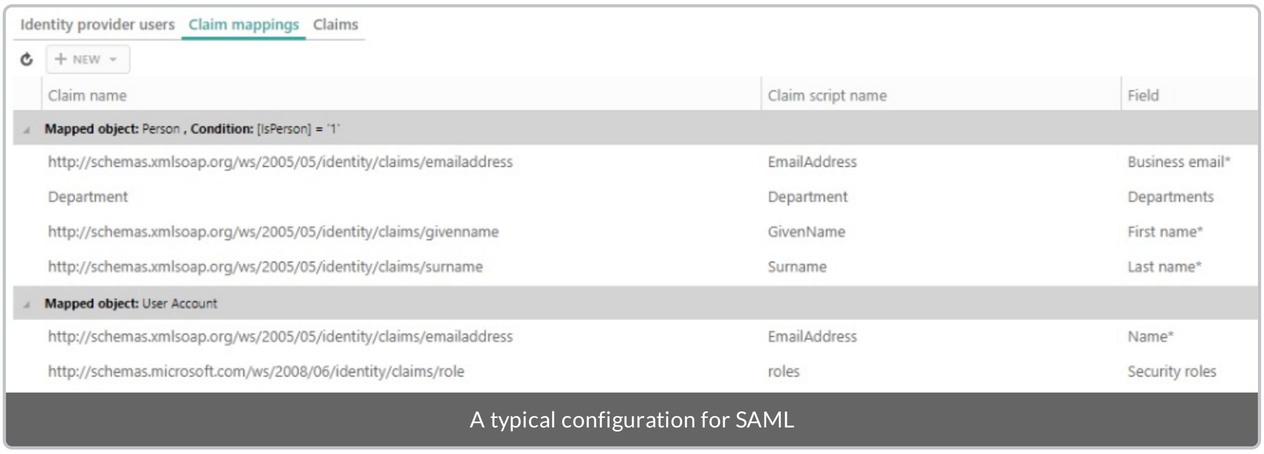
- email address
- first name
- last name
- security role

Mappings are used to map, or translate, between your identity provider and your ReadiNow tenant. For example, a field called 'Designation" in your identity provider may be called 'Title' in your ReadiNow tenant. The difference in the labels is not an issue, provide you create a mapping between the two values.

The names for these claims are typically as follows, although note that not all identity providers are configured in the same way. For example, although the list of OpenID Connect standard claims doesn't include the role, an additional field can sometimes be configured for that. Unfortunately, it must be observed that cloud identity providers may not give sufficient control to make that type of change. Note that without a role specified, the user will have very little permissions until the administrator can assign proper permissions manually.

OpenID Connect	SAML
email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
given_name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
family_name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
-	http://schemas.microsoft.com/ws/2008/06/identity/claims/role

To create the mappings, use the appropriate name from the table above- depending on whether the provider is OpenID or SAML - and create a row for each claim-field pair that is required. Note that the SAML names appear to be internet links.



Claim name	Claim script name	Field
Mapped object: Person , **Condition:** [IsPerson] = '1'		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	EmailAddress	Business email*
Department	Department	Departments
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	GivenName	First name*
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname	Last name*
Mapped object: User Account		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	EmailAddress	Name*
http://schemas.microsoft.com/ws/2008/06/identity/claims/role	roles	Security roles

A typical configuration for SAML

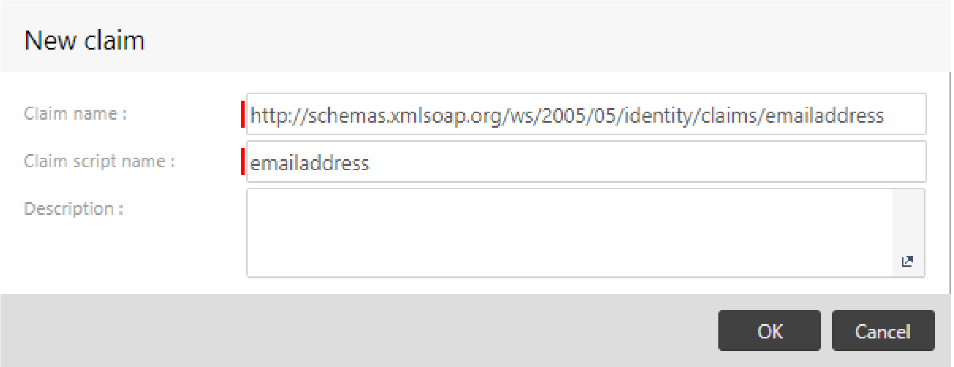
Note that the Name field on the *User Account* must be mapped to the unique identifier for each user. Typically this is the email address, but in some cases it may be a staff number or some other unique identifier; be sure to use the claim name that matches the existing users otherwise new accounts will be created when they attempt to log in.

Process to create claims and claim mappings

1. Navigate to the 'Claims mappings' tab. Click New.
2. Select the type of mapping to create. In this example, we will use Person
3. The 'Claim Mapping for Person' dialog appears. Under 'Source Claim' select [New Claim]
4. The 'New claim' dialog appears
5. For 'Claim name' field use the value for SAML or OIDC as appropriate.

   e.g. For SAML email address we would use

   http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
6. For 'Claim script name' enter a value that can be used to refer to this claim. This is used only if you are adding conditions to your claim import rules
7. 'Description' is optional
8. Click OK to save your new claim



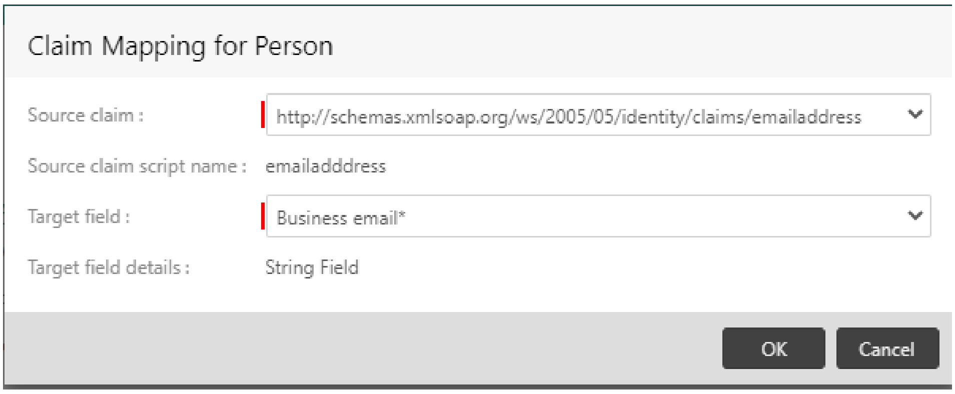
New claim

Claim name : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Claim script name : emailaddress

Description :

9. You are returned to the 'Claim Mapping for Person' dialog. The 'Target field' is the corresponding field in your ReadiNow tenant. E.g. 'Business email'
10. Click OK to save your new mapping



Claim Mapping for Person

Source claim : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Source claim script name : emailadddress

Target field : Business email*

Target field details : String Field

Further Notes on Claims and Claim Mappings

1. As the NameID is always first, the code will always use the value which is in the NameID field. The code will only look for the http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress if the NameID claim is missing.
2. (SAML) The claim for email must be named

   http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
3. The Person mapping must have all the default fields mapped. This includes First Name, Last Name and

Business Email. Other fields/claims may be defined but they are not required.

4. If a mapping is added for the Account Holder relationship for User Account, then the provisioning code will search to see if there are any existing Account Holders that match the mapped field.
   For example, the Business Email field of the User Account -> Account holder can be mapped to the email claim. If an Account Holder is found with the mapped field, this Account Holder will be assigned to the User Account. If no matching Account Holder is found, one will be created ONLY if claim mapping rules exist for Person.
   If there is no **Account holder** relationship from the **User Account** and claim mappings for **Person** exist, the code will attempt to lookup **Account holders** whose **Name = First name + " " + Last name**
5. ReadiNow supports multiple claims. For example, in your identity provider users may have been migrated from different systems. Some users may have an email address while others have an employee ID. Both these fields can be mapped to name.
6. Provided the mapping is correct, email address may have different domains. For example, as the result of a merger some users may have emails address from @salt.com while other users have @vinegar.com

Login Process for a New User

If the user account does not exist, then the provisioning process will run synchronously until the user account, account holder, and identity provider user entities have been created and the claim mappings have been applied. Once this is completed then the user will be signed in.

If there are errors when mapping fields for the user account or account holder the provisioning will fail and the user will not be signed in.

Login Process for an Existing User

If the 'Update existing users' check box is checked then existing User Account and Account Holder records may be updated if their mapped claims values differ from their field values.

If 'Update existing users' is unchecked then the User Account and Account holder records may get out of sync with the claim values.

NOTE: As long as a User Account is found based on the claim mappings the user will be allowed to login.

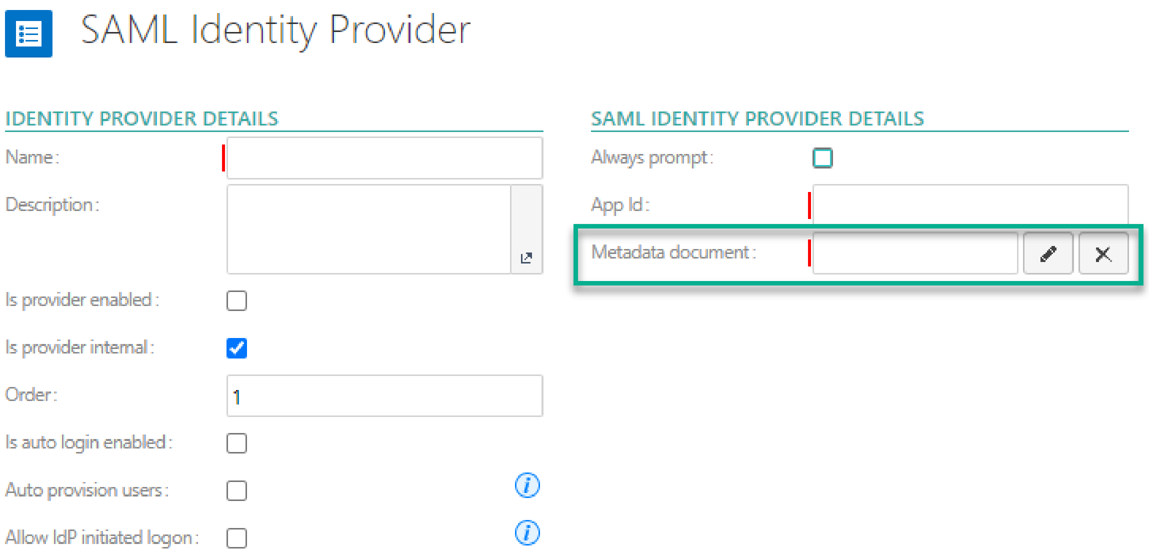
Update expiring/expired certificates

By design SSL certificates expire. Typically, before a certificate expires it will be replaced with a new one - this happens within the identity provider (i.e. external to your ReadiNow tenant). It is the tenant administrators' responsibility to update the metadata documents in their tenant. ReadiNow does not have access to the identity provider, and does not provide these documents or certificates.

The steps required for updating SSL certificates depends on whether your tenant is configured to use SAML or OpenID, and whether the certificate is accessible externally or only internally (see above). However, it is generally necessary to replace the metadata document. The following steps are an overview, for additional information refer to the configuration section.

NOTE: prior to replacing the metadata document, clear the existing documents from the picker using the 'X' button - this will ensure they are removed properly.

For an ***internal SAML*** provider updating a certificate involves replacing the metadata document in the document library and linking the new document in the identity provider configuration.



SAML Identity Provider

IDENTITY PROVIDER DETAILS

Name:

Description:

Is provider enabled: □

Is provider internal: ☑

Order: 1

Is auto login enabled: □

Auto provision users: □

Allow IdP initiated logon: □

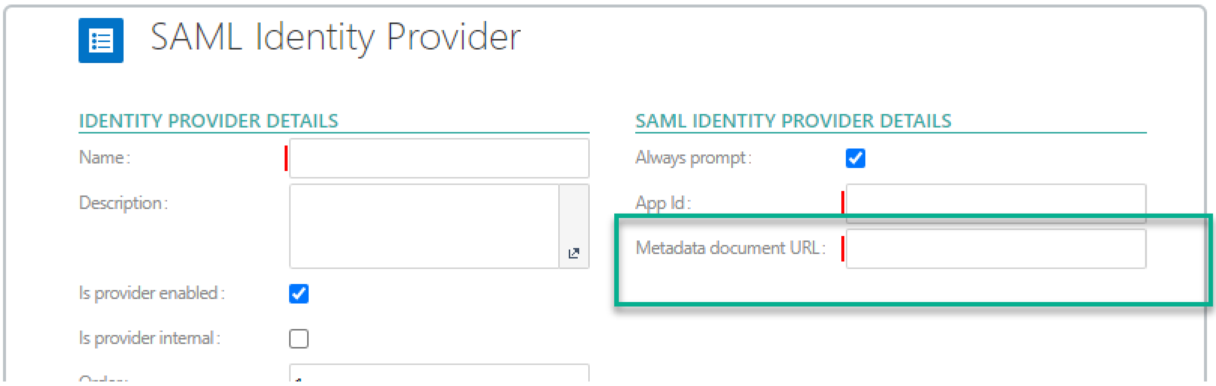
SAML IDENTITY PROVIDER DETAILS

Always prompt: □

App Id:

Metadata document:

For an ***external SAML*** provider the metadata document is found by URL - it may use the same URL. Check the metadata URL is still valid and update as necessary.



SAML Identity Provider

IDENTITY PROVIDER DETAILS

Name:

Description:

Is provider enabled: ☑

Is provider internal: □

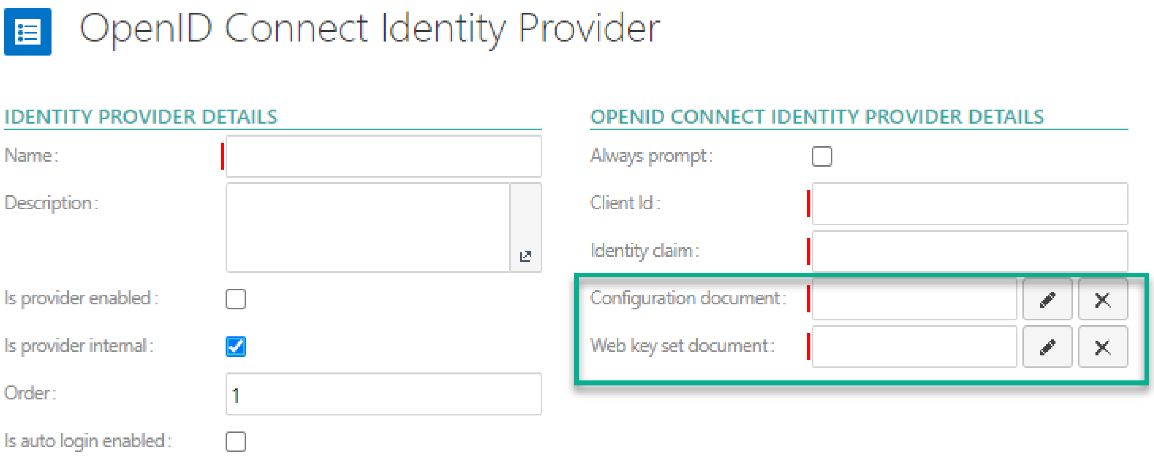
SAML IDENTITY PROVIDER DETAILS

Always prompt: ☑

App Id:

Metadata document URL:

For an ***internal OpenID*** provider updating a certificate involves replacing the configuration document and the web key set document and linking the new documents in the identity provider configuration.


OpenID Connect Identity Provider

IDENTITY PROVIDER DETAILS

Name:

Description:

Is provider enabled: □

Is provider internal: ☑

Order: 1

Is auto login enabled: □

OPENID CONNECT IDENTITY PROVIDER DETAILS

Always prompt: □

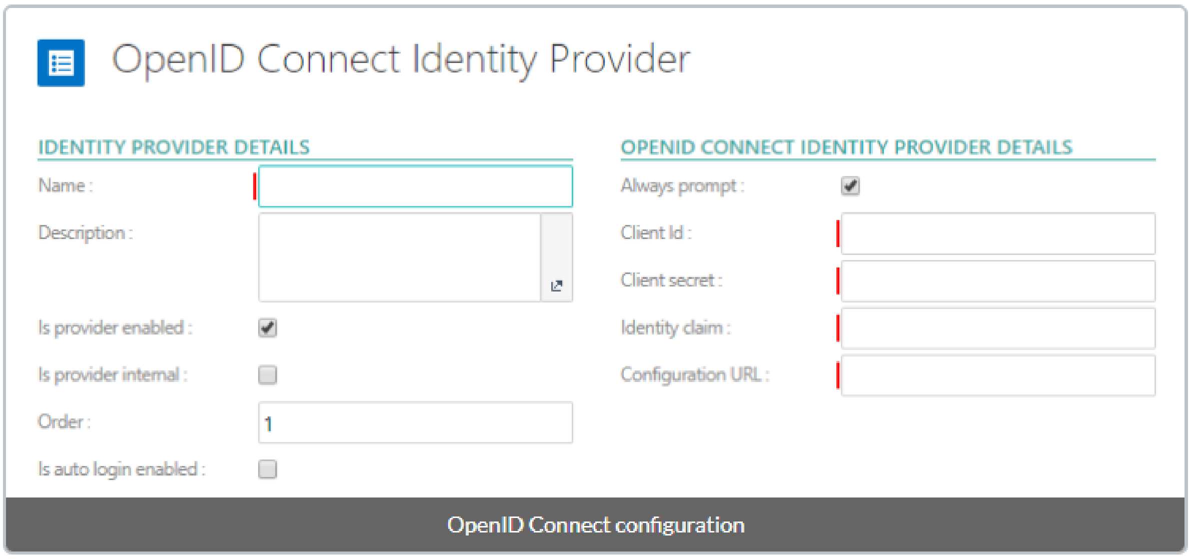
Client Id:

Identity claim:

Configuration document:

Web key set document:

For an ***external OpenID*** provider the metadata document is found by URL - it may use the same URL. Check the 'Configuration URL' is still valid and update as necessary.


OpenID Connect Identity Provider

IDENTITY PROVIDER DETAILS

Name:

Description:

Is provider enabled: ☑

Is provider internal: □

Order: 1

Is auto login enabled: □

OPENID CONNECT IDENTITY PROVIDER DETAILS

Always prompt: ☑

Client Id:

Client secret:

Identity claim:

Configuration URL:

OpenID Connect configuration

Further Information

SAML

Basic example of SAML identity provider configuration

Log into the identity provider administration and perform the following steps:

1. Create a new application registration
2. Select 'SAML-based Sign-on' for the Single Sign-on mode
3. Set the identifier (Entity ID) to be the host part of the tenant URL

   e.g. https://

   The Entity ID must match the App Id in the ReadiNow tenant.
4. Set the reply URL to:

   - SP Initiated logon:

https://[company].readinow.com/spapi/data/v1/login/saml/authresponse/[tenant]

Or

- IDP Initiated logon:

https://[company].readinow.com/spapi/data/v1/login/saml/authresponse/[tenant]/[identity_provider_name]

where [identity_provider_name] is the name of the identity provider within the ReadiNow tenant.

5. Set the Relay State to the URL *(note: loginRedirect is case sensitive and '//' is required)*:

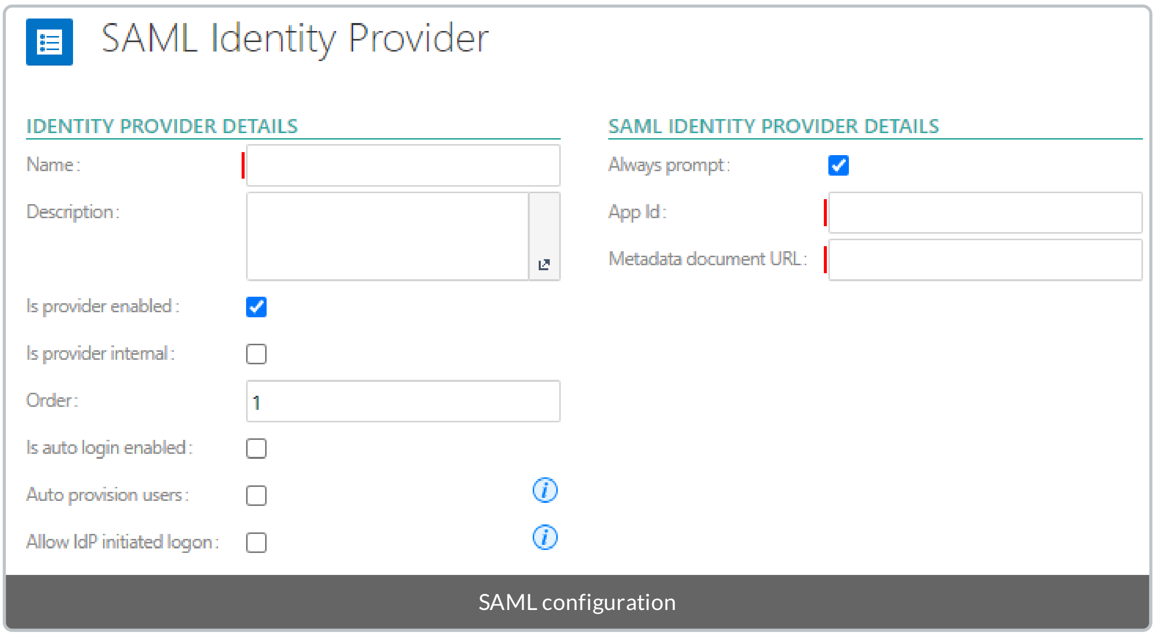
   https://[company]/sp/index.html#/[tenant]//loginRedirect
6. Leave the Logout URL blank
7. Select the email address as the user identifier
8. Adjust any attributes or claims as necessary for your use case
9. Grant access to the appropriate users and groups
10. Save the application registration

The identity provider will provide a metadata document URL which must be used to configure the tenant. If your identify provider is internal, download the metadata document as this will be needed to configure your ReadiNow tenant.

Configure the tenant for SAML SSO

Log into your ReadiNow tenant.
Go to: Administration > Security > Identity Providers > New. Select SAML.

1. Provide a name. This will be displayed to users on the login screen
2. [Optional] Enter a description
3. Check 'Is provider enabled'
4. Check 'Is provider internal' if required
5. If more than one identity provider is used, specify the Order of preference
6. Check 'Is auto login enabled' if required
7. Check 'Auto provision users' if this has been enabled in your identity provider
8. Check 'Allow IdP initiated logon' if this has been enabled in your identity provider. (Note: you can use SP and IdP initiated logon at the same time.)
9. Check 'Always prompt' if the user should always be prompted to re-enter their SSO credentials
10. Enter the App Id. This must match the Entity ID configured in the identity provider. For this example it would be: https://[company].readinow.com
11. For an external identity provider enter the metadata document URL
12. For an internal identity provider upload the metadata document itself



SAML Identity Provider

IDENTITY PROVIDER DETAILS

Name:

Description:

Is provider enabled: ☑

Is provider internal: □

Order: 1

Is auto login enabled: □

Auto provision users: □

Allow IdP initiated logon: □

SAML IDENTITY PROVIDER DETAILS

Always prompt: ☑

App Id:

Metadata document URL:

SAML configuration

OIDC

Basic example of OIDC identity provider configuration

Log into the identity provider administration console and perform the following steps:

1. Create a new application registration
2. Select 'OIDC-based Sign-on' for the Single Sign-on mode
3. Set the application ID URI (Entity ID) to be the host part of the tenant URL

   e.g. https://[company].readinow.com

   The application ID must match the App Id in the ReadiNow tenant.
4. Set the reply URL to: https:///spapi/data/v1/login/oidc/authresponse/

   e.g. https://[company].readinow.com/spapi/data/v1/login/oidc/authresponse/[tenant]
5. Leave the Logout URL blank
6. Create the client secret (password)
7. Grant access to the appropriate users and groups
8. Save the application registration

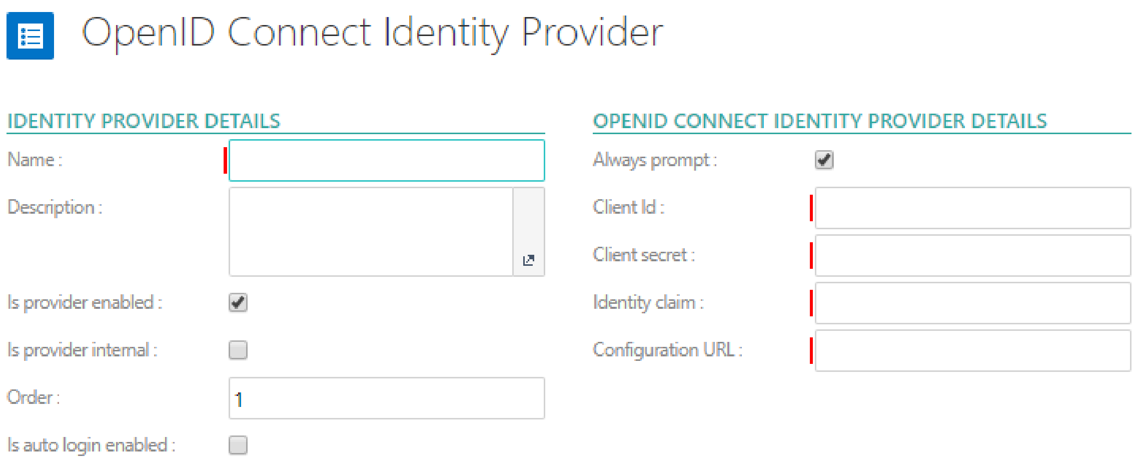
The identity provider will provide a metadata document URL which will be used to configure the tenant. If your identify provider is internal, download the configuration document and JSON web key set document as these will be needed to configure your ReadiNow tenant.

Configure the tenant for OIDC SSO

Log into your ReadiNow tenant.
Go to: Administration > Security > Identity Providers > New. Select OIDC.

1. Provide a name. This will be displayed to users on the login screen
2. [Optional] Enter description

3. Check ‘Is provider enabled’
4. Check ‘Is provider internal’ if required
5. If more than one identity provider is used, specify the Order of preference
6. Check ‘Is auto login enabled’ if required
7. Check ‘Always prompt’ if the user should always be prompted to re-enter their SSO credentials
8. Enter the Client Id. This must match the Entity ID configured in the identity provider. For this example it would be: https://[company].readinow.com
9. Enter the Client secret. This is the password or app key used in the configuration of the identity provider
10. Enter the identity claim. The name of the claim to use to map identity provider users to user accounts. The value of the claim must match the name of the identity provider user. For example, upn (user principal name) or email. (Refer to: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-optional-claims
11. For an external identity provider enter the Configuration URL
12. For an internal identity provider upload the configuration document and JSON web key set document



OpenID Connect Identity Provider

IDENTITY PROVIDER DETAILS

Name :

Description :

Is provider enabled : ☑

Is provider internal : □

Order : 1

Is auto login enabled : □

OPENID CONNECT IDENTITY PROVIDER DETAILS

Always prompt : ☑

Client Id :

Client secret :

Identity claim :

Configuration URL :

The Configuration URL for commonly used identity providers are:

Identity Provider	Example configuration URL (note: replace [xxx] as appropriate)
Google	https://accounts.google.com/.well-known/openid-configuration
Microsoft	https://login.microsoftonline.com/[xxx]/.well-known/openid-configuration
Okta	https://[instance].okta.com/.well-known/openid-configuration

Failure Logging

Errors will be written to the Event Log during the SSO login process.

Login page messages

The end user may see one of the following error messages on the login page.

The user name may be incorrect or the account may be locked, disabled or expired.

This indicates that the user successfully logged into the IDP and that the response was sent back successfully, however a valid identity provider user could not be found. The tenant event log will have a message containing the name of the user that the IDP has found. This name should match the name of the identity provider user. The log message is of the form **The request context could not be found for identity provider user ''. The user name may be incorrect or the account may be locked, disabled or expired.**

The identity provider configuration appears to be invalid, please contact your administrator.

This indicates that an error occurred during the processing of the authentication request to IDP or the or the processing of the response from the IDP.

Event log messages

SSO event log messages will have the following titles:

Failed to process SAML authorization response.

Failure occurred processing the SAML response. The error may have occurred at the IDP or ReadiNow. Details will have more information.

Failed to process SAML authorization request.

Failure occurred processing the SAML request.

Failed to process OpenID Connect authorization response.

Failure occurred processing the OpenID Connect response. The error may have occurred at the IDP or ReadiNow. Details will have more information.

Failed to process OpenID Connect authorization request.

Failure occurred processing the OpenID Connect request.

List of common errors and possible causes

Error	Solution
The SAML auth cookie does not exist. Ensure the ReadiNow URL is correct.	Cookies are used during the SSO login process so all user and IDP requests must be on the same domain.
The request context could not be found for SAML identity provider user ''. The user name may be incorrect or the account may be locked, disabled or expired.	The user successfully logged into the IDP and the response was sent back successfully. However a valid identity provider user could not be found. Check that a identity provider user whose name is exists and is not locked, disabled or expired.
The RelayState was not specified. Parameter name: RelayState	The SAML identity provider needs to be configured to return relay state.

Error	Solution
The OpenID Connect auth cookie does not exist. Ensure the ReadiNow URL is correct.	Cookies are used during the SSO login process so all requests must be on the same domain.
The identity provider configuration appears to be invalid. The remote server returned an error: (404) Not Found.	This indicates that the server did not find the metadata at the specified URL. Verify that the Metadata document URL is valid and accessible.
An error occurred validating the SAML response. The Saml2Response must have status success to extract claims. Status: Responder.	This message indicates that there is a configuration error on the IDP. Check that it is returning the NameID claim of type emailAddress or nameidentifier
An error occurred validating the SAML response. The Saml2Response must have status success to extract claims. Status: Requester. Second Level Status: urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy.	This message indicates that there is a configuration error on the IDP. Check that it is returning the NameID claim of type emailAddress or nameidentifier