Single Sign-On (SSO)

Configuration Guide

(For DXC Assure Claims v.19.1 onwards)

(Document updated: November 2022)

DXC Assure Claims

Empowering Corporate Claims and Self-Insured Organizations with an integrated RMIS solution

General Claims

Non-Occupational Claims

Property Claims

Vehicle Accident Claims

Workers' Compensation Claims

Life Claims

Events

DXC Assure Claims Support Helpdesk: All questions regarding this documentation should be routed through customer assistance, Blythewood, SC, on Phone: 800-420-6007 or Email: risksupp@dxc.com

Document Overview

This document is a Configuration Guide to assist with setting up of the Single Sign-On (SSO) feature.

However, you may require DXC's consulting services team's assistance setting this up. Please reach out to your sales representative for further information & assistance in this regard.

Table of contents

Single Sign-On (SSO)*

THIS SECTION CONTAINS DESCRIPTIONS OF A MORE SECURE WORKING EXPERIENCE WITH THE INTRODUCTION OF SINGLE SIGN-ON (SSO) AUTHENTICATION.

Single Sign-On (SSO)*

DXC Assure Claims offers a more secure working experience with the introduction of Single sign-on (SSO) authentication. SSO is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

SSO is a licensed feature and must be procured separately. The SSO feature is available to users operating at v. 19.1 and over of DXC Assure Claims.

It is now possible to enable SAML2.0 based Single Sign-On in DXC Assure Claims. Any identity providers supporting SAML2.0 standard SSO can be configured in Assure Claims to enable Single Sign-On.

* Procuring this feature may involve additional cost/ consulting/ agreement/ licensing considerations.
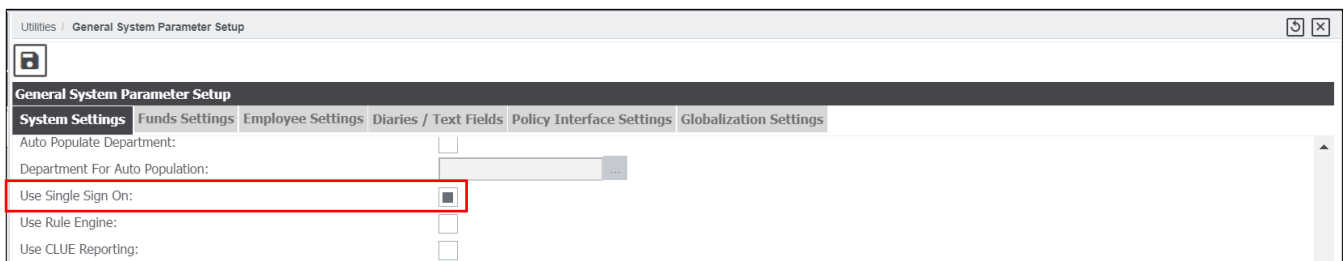
Prerequisite Settings

The following are the prerequisite settings that must be enabled for the functioning of SSO in DXC Assure Claims

- ➢ https:// must be enabled for DXC Assure Claims
- ➢ Domain name must be specified for the server
- ➢ The checkbox "Use Single Sign On" must be selected under Utilities > General System Parameter Setup > System Settings (tab) [Fig. 1]

DXC Assure Claims screen

| Utilities / General System Parameter Setup		
General System Parameter Setup		
System Settings Funds Settings Employee Settings Diaries / Text Fields Policy Interface Settings Globalization Settings		
Auto Populate Department:	☐	
Department For Auto Population:		...
Use Single Sign On:	☑	
Use Rule Engine:	☐	
Use CLUE Reporting:	☐	

[Fig. 1]

Configuring SSO on Providers/Identity Providers in DXC Assure Claims

Follow the following steps to configure SSO on Providers/Identity Providers in Assure Claims:

1. Navigate to Security Management System (SMS) and select the Authentication Provider Settings button. **[Fig. 2]**
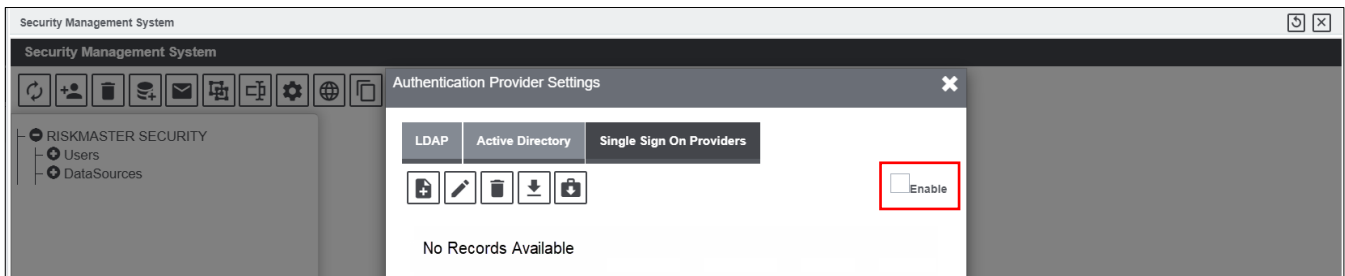
DXC Assure Claims screen
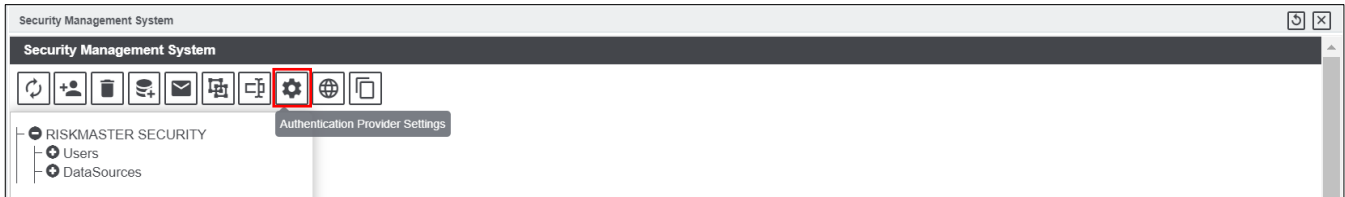
[Fig. 2]

2. Select the "Authentication Provider Settings" button to open the "Authentication Provider Settings" window and click on the "Single Sign On Providers" tab.
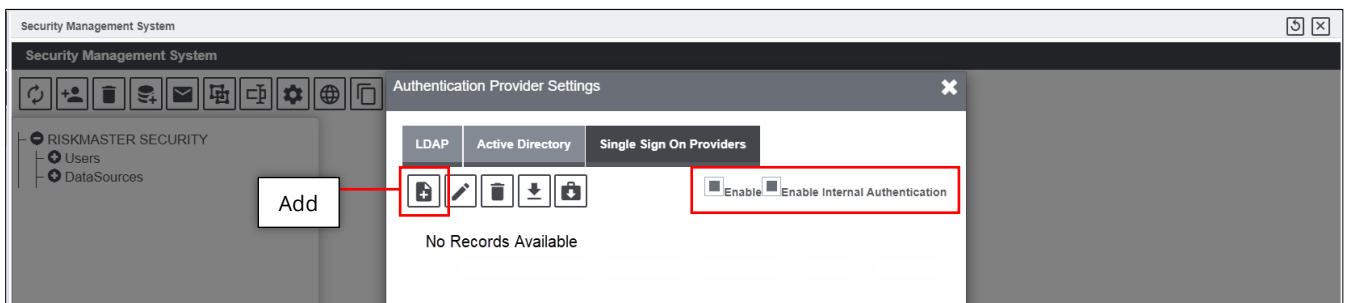
DXC Assure Claims screen

[Fig. 3]

3. Select the checkbox labelled "Enable" **[Fig. 3]** on the "Authenticate Provider Settings" window (to enable SSO). This makes the "Enable Internal Authorization" checkbox available for selection. **[Fig. 4]**
   - Select the "Enable Internal Authorization" checkbox as well.

DXC Assure Claims screen

[Fig. 4]

- Selecting the "Enable Internal Authorization" checkbox allows using the Assure Claims authentication module as well which enables logging into the Assure Claims application.
- This feature can be used as a fallback in case the "Identity Providers" are down or not configured properly.
- To enable "Internal Assure Claims Authentication", it is imperative that users are already created in DXC Assure Claims using "Add New User" feature in Security Management System.

4. Select the "Add" button [Fig. 4] on the "Authentication Provider Settings" popup window to open the "Add Identity Provider and SAML Settings" popup window. **[Fig. 5]**

DXC Assure Claims screen
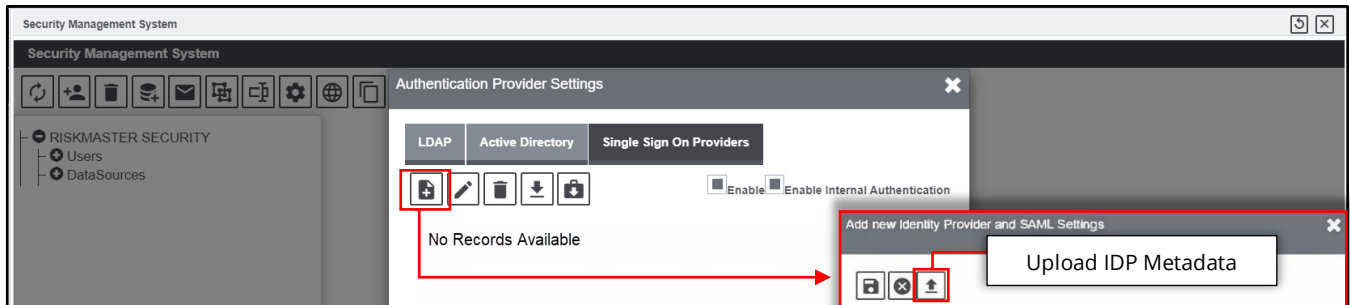
[Fig. 5]

Add Identity Provider

ADFS is being taken as an example to show the configuration of an Identity Provider. **[Fig. 5]**

There are two options to populate data in "Add New Identity Provider and SAML Settings" window. They are, by:

1. Consuming IDP's Metadata XML and populate. (Select the "Upload IDP Metadata File" button **[Fig. 5]** and browse to select an appropriate XML file to upload.
2. Manually fill in the information as explained below:
   - **Identity Provider Name:** This is the display name of the Identity provider.
   - **Identity Provider URL:** this is the URL of Identity Provider where users can authenticate themselves. For ADFS Example, the IDP URL is https://rmaadfspoc.csc-rmcl.com/adfs/ls/IdpInitiatedSignon.aspx
   - **Single Sign On Protocol:** Currently, we are only supporting SAML2.0 based SSO Authentication
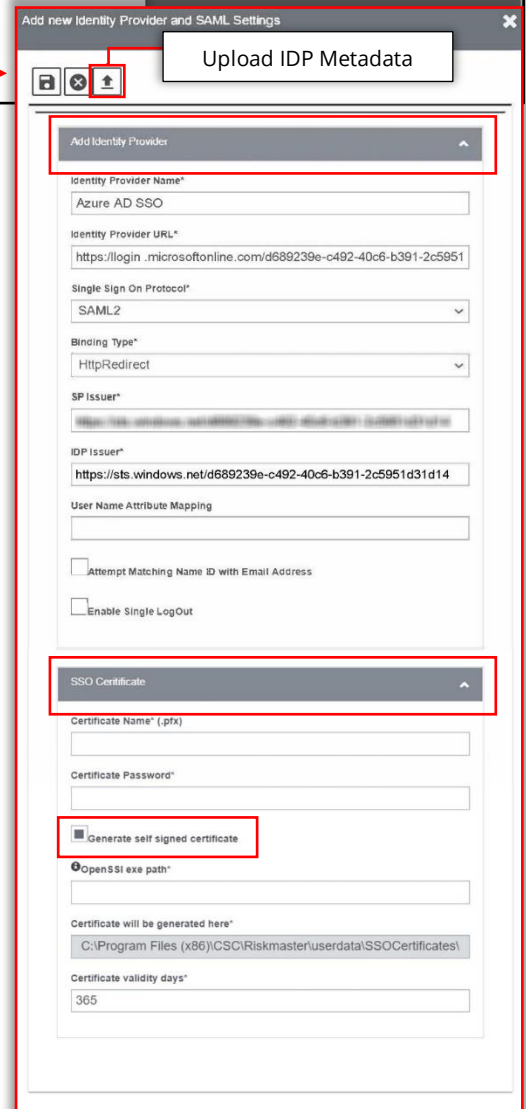
- **Binding Type:** Currently, we are only supporting "HttpRedirect" binding for Assure Claims to IDP redirection for authentication. (SP to IDP redirection).
- **SP Issuer:** Service Provider (SP) Issuer. This is generally the domain name of the service provider, Assure Claims, in our case. This is required to establish a trust between Service Provider and Identity Provider during the SSO Handshake.
- **IDP Issuer:** Identity Provider Issuer is required to establish the trust between Identity Provider and Service Provider. Assure Claims will be able to trust the authentication assertion from the Identity Provider by looking at the "IDP Issuer" in the assertion. This is provided by your Identity Provider.
- **User Attribute Mapping:** Assure Claims generally looks for the "Name ID" subject in the SAML Assertion received from the identity provider to find out "UserName" but if User Name is not supplied in the "NameID" subject, then clients may define User Name attribute here and Assure Claims will look for the specific attribute in the assertion to find out "UserName".
- **Enable Single Logout:** When this is enabled, log out request from Assure Claims will be sent to IDP and user will be logged out from the Assure Claims as well as IDP. When this is disabled, user will be logged out only from Assure Claims application
- **Single Log Out URL:** This is the IDP's single logout URL where Assure Claims users will be redirected for single logout.

SSO Certificate

Please refer to the "SSO Certificate" accordion of "Add New Identity Provider and SAML Settings" window. **[Fig. 5]**

Select the "Generate Self Signed Certificate" checkbox **[Fig. 5]**, to generate an SSL certificate. For this, the "Open SSL exe" needs to be placed on the Application Server and path of the same needs to be entered along with the validity of the certificate.

A Certificate Name and Password must also be entered in their respective fields and a .pfx file with same Name and Password will get generated and be placed at the location mentioned in the field labelled "Certificate will be generated here".

If the "Generate Self Signed Certificate" checkbox is not selected, then, the private key of the certificate on which DXC Assure Claims is hosted over https can be exported and its Name and Password can be mentioned in the "Certificate Name (.pfx)" and "Certificate Password" fields. **[Fig. 5]** Please note that the .pfx file needs to be placed at the same location.

Certificate Name: this is the name of the Certificate that will be used to sign SAML Authentication Request sent to Identity Provider for authentication. The Private key of this certificate will be used to sign the SAML Authentication request.

Certificate Password: Password of the .pfx certificate

Downloading Service Provider Metadata XML & Certificate

Once all the details are filled and saved, the Service Provider (Assure Claims) Metadata XML can be downloaded to IDP to consume by selecting the added "Authentication Provider" and select the "Download Service Provider Metadata" button on the "Single Sign On Providers" tab **[Fig. 6]** to download the metadata XML. This XML file can then be consumed by the IDP.

DXC Assure Claims screen
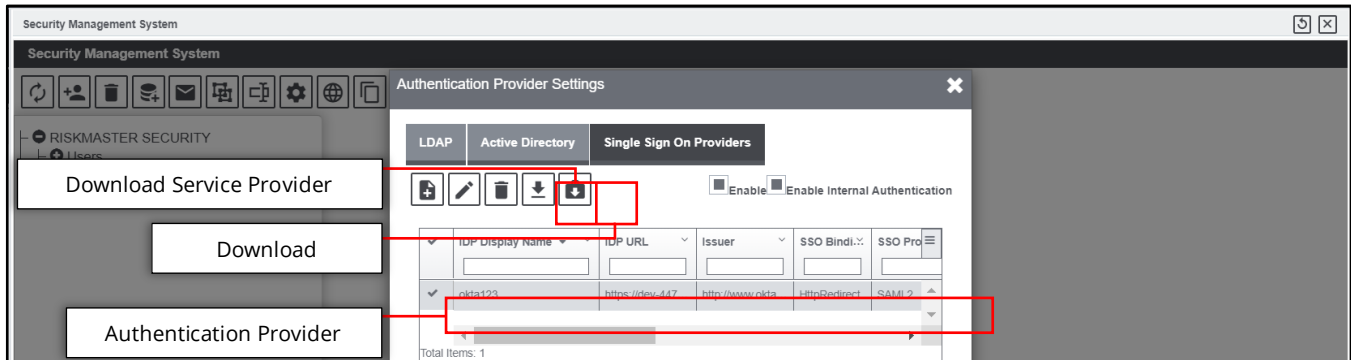
[Fig. 6]

➢ The Certificate File (.pfx) can be downloaded via the "Download Certificate" button on the "Single Sign On Providers" tab. **[Fig. 6]**

Assure Claims Metadata supplied to IDP to complete SAML settings for SSO

The following are details of the Assure Claims Metadata that needs to be supplied to IDP to complete SAML settings for SSO:

1. **Consume Assertion API Route**
   https://<domain name>/RiskmasterAPI/dashboard/consumeasertion/{EncryptedClientId}

   {EncryptedClientId} is the ClientId which should be 0 if not applicable

2. **Log Out Response API Route**
   https://<domain name>/RiskmasterAPI/dashboard/getlogoutresponse/{EncryptedClientId}

   {EncryptedClientId} is the ClientId which should be 0 if not applicable

3. **Supported binding To consume SAML Assertion**
   Currently we only support HttpPost binding to receive saml assertion from IDP

4.   **Supported Binding For Single Logout Request to IDP**
Currently, we only support HttpRedirect binding to send Single Log Out Request to IDP

5.   **Supported Binding To Receive Log Out Response from IDP**
Currently, we only support HttpPost binding to receive Log Out Response from IDP

About Us & Contact Info

DXC TECHNOLOGY IS A FORTUNE 500 GLOBAL IT SERVICES LEADER. OUR MORE THAN 130,000 PEOPLE IN 70-PLUS COUNTRIES ARE ENTRUSTED BY OUR CUSTOMERS TO DELIVER WHAT MATTERS MOST. WE USE THE POWER OF TECHNOLOGY TO DELIVER MISSION CRITICAL IT SERVICES ACROSS THE ENTERPRISE TECHNOLOGY STACK TO DRIVE BUSINESS IMPACT

DXC Technology

We deliver the mission critical IT services that move the world.

70+	130,000+	240+	60+
countries	employees	fortune 500 customers	years of innovation

Delivering eXcellence for our Customers and Colleagues

DXC Technology is a Fortune 500 global IT services leader. Our more than 130,000 people in 70-plus countries are entrusted by our customers to deliver what matters most. We use the power of technology to deliver mission critical IT services across the Enterprise Technology Stack to drive business impact. DXC is an employer of choice with strong values, and fosters a culture of inclusion, belonging and corporate citizenship. We are DXC.

READ MORE ABOUT DXC TECHNOLOGY

DXC Assure Claims

DXC Assure Claims is an integrated Claims Administration Platform that consolidates multiple functions into one cohesive solution to provide accurate and up-to-date business functions using the latest technology.

This browser-based software provides real-time analytics to help you spot trends and mitigate future losses. It gives your staff a highly efficient system that simplifies workflows and promotes best practices throughout your organization. It helps ensure that your claimants receive first-class service, besides providing your management team with a means to track key metrics to control costs and improve performance.

> **READ MORE ON THE DXC CLAIMS MICROSITE**

> **DXC BLOG – INSURANCE & TECHNOLOGY**

Thousands of Risk and Claim professionals rely on DXC Assure Claims to manage all types of Claims, making it one of the industry's leading Claims Management Systems. This active client community ensures that DXC Assure Claims is continually supported and enhanced – keeping your Claims processing running smoothly today and in the future.

Contact Us

The Assure Claims Support Center provides manned telephone support services at these times –

8:00 AM – 8:30 PM, EST, Monday through Friday.

Additional and after-hours coverage may be available upon request.

risksupp@dxc.com

1-877-275-3676

DXC TECHNOLOGY

EXPLORE DXC INSURANCE
SOFTWARE

Assure Claims Support Helpdesk

Phone: 1-877-275-3676
Email: risksupp@dxc.com