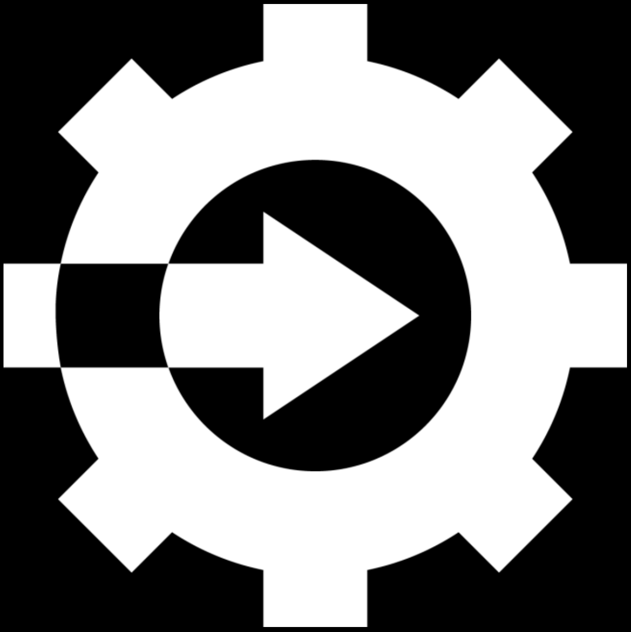
DXC Assure Claims

Sisense Single Sign-On (SSO)

September 2019



Legal Disclaimer: This document contains trade secrets and confidential information, which are proprietary to DXC Technology. The use, reproduction, distribution or disclosure of the documentation, in whole or part, without the express written permission of DXC is prohibited. The information in this document is subject to change.

DXC Technology, 1775 Tysons Blvd,
Tysons, VA 22102, USA. All rights reserved.
Printed in U.S.A.

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

GENERAL OVERVIEW

Introduction

Single Sign-On (SSO) is a mechanism that allows a system to authenticate users and subsequently tells Sisense that the user has been authenticated. The user is, then, allowed to access Sisense without being prompted to enter separate login credentials.

The SSO security mechanism allows Sisense to trust the login requests, it gets from your corporate authentication system, and grant access to the users that have been authenticated by it. An SSO session begins when the authenticated user requests a secured resource from Sisense while logged into the site or application. The user's browser sends an HTTP request to Sisense that includes a cookie which contains session and authentication information. This information is then used for session validation.

The user who already have Sisense account can continue to access Sisense via the Sisense Login page with their current account. To prevent users from directly logging in to Sisense instead of the login page, the Sisense administrator can change the passwords of the current users forcing them to log in with the company's credentials in the respective company's login page.

DXC recommends that administrators always keep a Sisense password, so that, the administrator can access Sisense in case the SSO server is not available.

TABLE OF CONTENTS

DXC.technology

DXC Assure Claims

Sisense Single Sign-On (SSO)

September 2019

SISENSE SSO VIA SAML 2.0

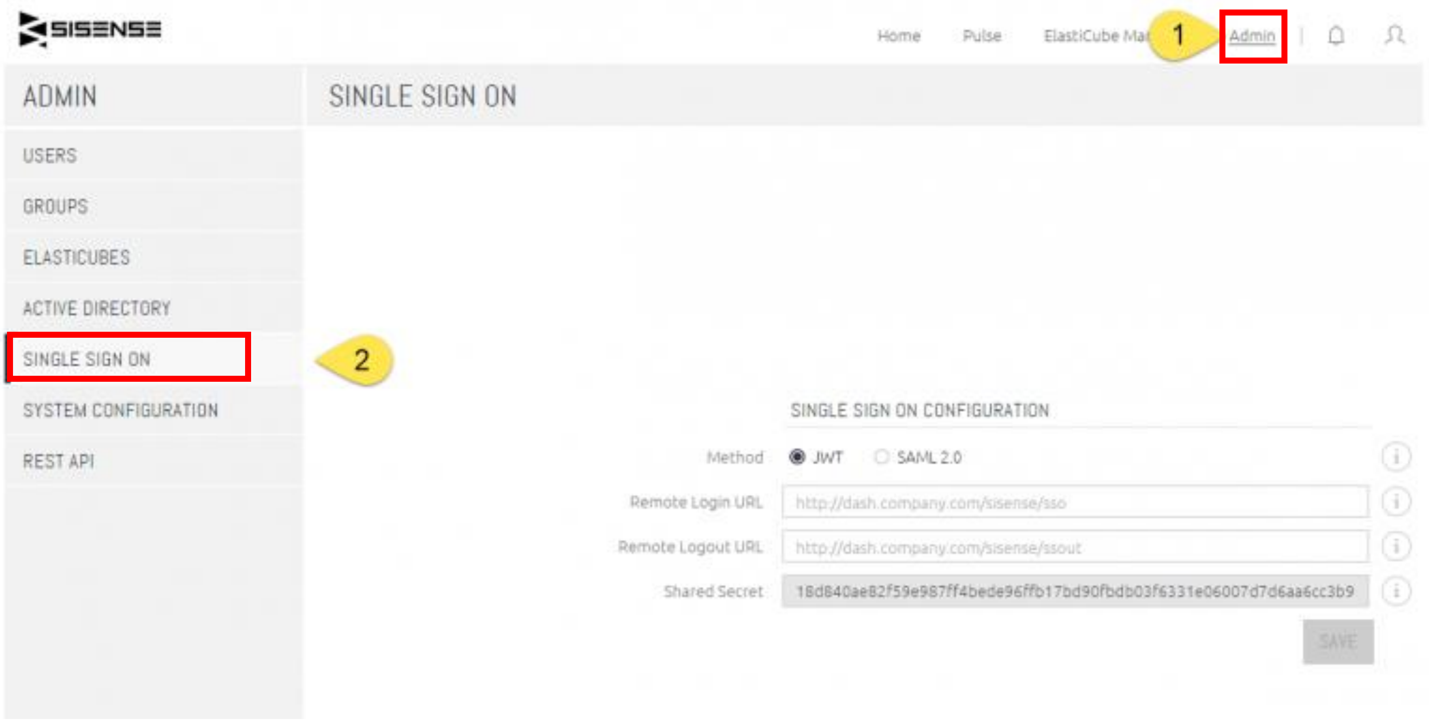
SISENSE SSO VIA SAML 2.0

The Sisense SAML authentication process is based on the SAML 2.0

After you have configured your SAML server, sign in to Sisense as an Administrator and follow the instructions below.

Follow the steps mentioned below to enable SAML in Sisense:

1. In the Sisense Web Application, click **Admin** and select **Single Sign On**.



Method ● JWT ○ SAML 2.0

Remote Login URL: http://dash.company.com/sisense/sso

Remote Logout URL: http://dash.company.com/sisense/ssout

Shared Secret: 18d840ae82f59e987ff4bede96ffb17bd90fbdb03f6331e06007d7d6aa6cc3b9

2. In the Single Sign On page, select SAML 2.0.
3. In the Remote Login URL field, enter the SAML Login endpoint. Sisense redirects the user to this field when they sign in. This value should be provided by the IdP Service.
4. In the Remote Logout URL field, enter the SAML Logout endpoint. Sisense redirects the user to this field when they sign out. This value should be provided by the IdP Service.
5. In the **Public X.509 Certificate** field, enter your public key for your SAML configuration. This value should be provided by the IdP Service.
6. Click **Save**. SSO via SAML 2.0 is configured.

DXC Assure Claims

Sisense Single Sign-On (SSO)

September 2019

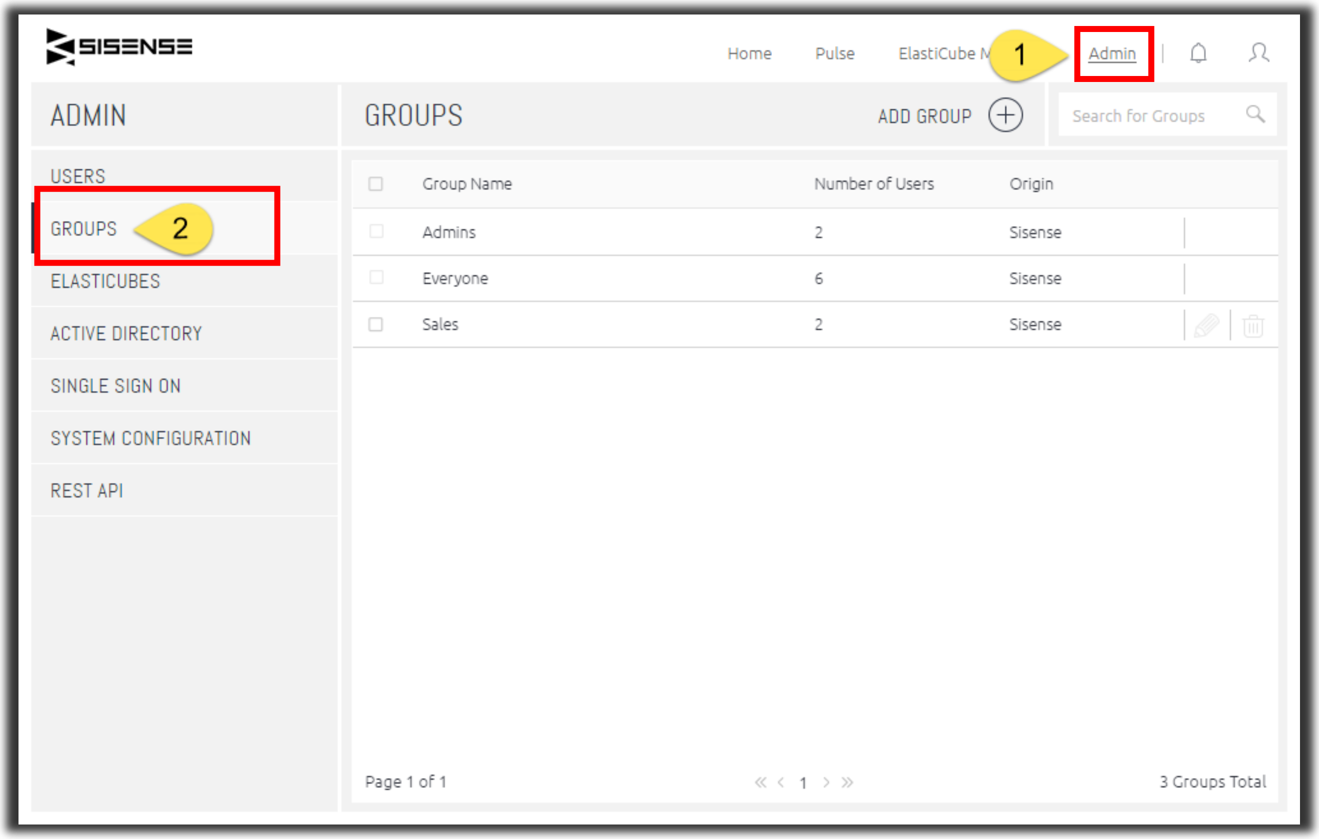
SISENSE DEFAULT ROLE SET-UP

SISENSE DEFAULT ROLE SET-UP

When an authenticated user is not found in the Sisense database, a new account is created. The user role is specified based on the user group/groups default role.

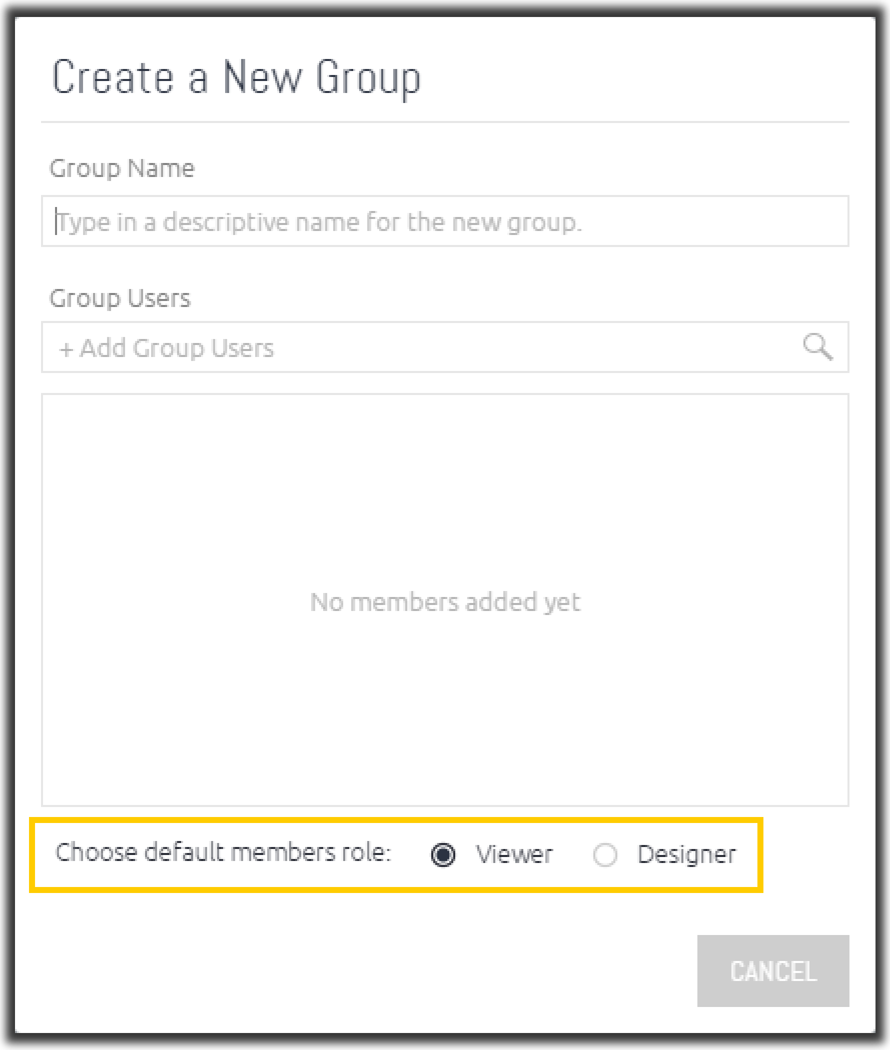
Follow the steps mentioned below to define a group's role:

1. In the Sisense Web Application, click **Admin** and select **Groups**.



☐	Group Name	Number of Users	Origin
☐	Admins	2	Sisense
☐	Everyone	6	Sisense
☐	Sales	2	Sisense

2. Click **Add Group**. The Create a New Group window is displayed.
3. In the **Create a New Group** window, select the default role of the group.



Create a New Group

Group Name

Type in a descriptive name for the new group.

Group Users

+ Add Group Users

No members added yet

Choose default members role: ● Viewer ○ Designer

CANCEL

4. Click **Save**.

Note

Changes to the group’s default role are applied when new users are created, and do not affect existing users. After a user is created in the system, an administrator can modify the user role, if needed.

DXC.technology

DXC Assure Claims

Sisense Single Sign-On (SSO)

September 2019

ABOUT & CONTACT

DXC TECHNOLOGY:
NEW. BUT NOT BORN YESTERDAY.

About DXC Technology

The company was formed on April 1, 2017, by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise. DXC Technology has successfully guided the world's largest enterprises and government agencies through successful change cycles. With some 137,000 employees worldwide, the company's deep experience gives it a clear and confident vision to help clients navigate the future.

DXC Technology is a Fortune 500 company and represented in the S&P 500 Index. The company works to create greater value for clients, partners and shareholders, and to present growth opportunities for its people. DXC Technology is ranked among the world's best corporate citizens.

DXC Technology's extensive partner network helps us drive collaboration and leverage technology independence. The company has established more than 250 industry-leading global Partner Network relationships, including 15 strategic partners: Amazon Web Services, AT&T, Dell EMC, HCL, Hitachi Vantara, HP, HPE, IBM, Lenovo, Micro Focus, Microsoft, Oracle, PwC, SAP and ServiceNow.

Click Here **To read more about DXC Technology.**

DXC Blog – Insurance and Technology

About DXC Insurance RISKMASTER^{TM}

DXC Insurance RISKMASTER^{TM} 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.

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

Click Here **To visit the Insurance RISKMASTER website.**

Click Here **To read more about Insurance RISKMASTER on the DXC website.**

Contact

DXC Technology
3000 University Drive,
Auburn Hills,
Michigan 48326

1-877-275-3676

risksupp@dxc.com

DXC.technology

Follow **DXC Technology** on social Media

Get the insights that matter.

Keep up-to-date with technology and innovation, now and in the future.

Get the insights that matter.