ITA_ System Configuration/ Environment Construction Guide

SSO(Single Sign-On)

—Version 1.7 —

Disclaimer

Trademark

※「Exastro IT Automation」is written as「ITA」in this document.

Table of Contents

Introduction

This document explains the system configuration and environment construction to use Single Sign-On authentication function (referred to as SSO hereafter) in ITA.

To use the SSO authentication driver, it is assumed that the basic ITA functions have been built. Please refer to "System Configuration/Environment Construction Guide - Basics" for constructing ITA basic function.

1 Function

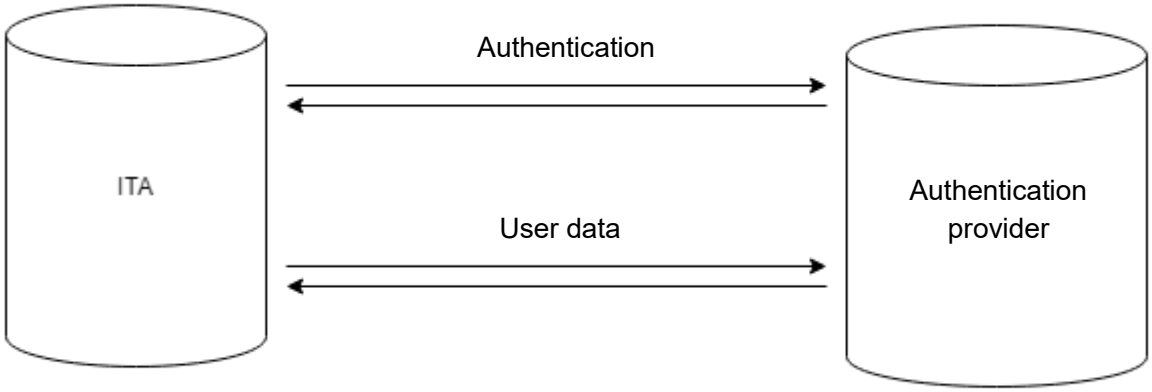
SSO authentication function provides the following functions.

Table 1-1 Function name

No	Function name	Use	WEB Content	BackYard Content
1	SSO authentication function	Perform ITA authentication via external authentication provider.	○	—

2 System configuration

Concept of SSO



3 System requirements

Since Ansible driver is based on system requirements of ITA system, please refer to "System Configuration/Environment Construction Guide - Basics".

To use SSO authentication function, it is required for the system which ITA system is installed and the client device of user to connect SSO authentication provider via HTTP/HTTPS.

ITA system supports HTTP/HTTPS and Proxy connection. However, authentication that needs proxy is not supported.

HTTP / HTTPS connection on the client side of user needs to be able to authenticate normally to the SSO authentication provider regardless of SSO authentication.

4 SSO authentication that ITA supports

No	Authentication name on ITA	Overview
1	OAuth2	OAuth version2.0

5 Setting flow

① Register client to authentication provider

In order to use the authentication provider, it is required to register the client for the authentication method supported by ITA and acquire the information required for authentication.

No	Authentication method	Information required for authentication
1	OAuth2	・clientId ・clinentSecret

Please set the following URL as the callback URL (redirect URL) for the provider.

No	Authentication method	Callback URL(Redirect URL)
1	oauth2	https//(FQDN of ITA)/common/common_sso_auth.php?oauth2&callback

※Please set http://... for callback URL if ITA connection is http (Not recommended)

② Register SSO basic preference in ITA

Main menu >> Management console >> Single Sign-On basic preference

Set the displayed information and authentication method in login screen.

No	Item name	Setting content	Required	Remarks
1	Provider ID	Auto-numbered	○	
2	Provider name	Provider name	○	The provider name displayed on login screen
3	Authentication Method	Select the authentication method	○	OAuth2 only
4	Logo	Upload the logo file		The logo of provider displayed on login screen
5	Display flags	Flag that decides to display on login screen or not	○	Select: Display or Hide ※Not displayed if required information for authentication is insufficient. Refer to「④About display on login screen」

③ Register SSO attribute preference in ITA

Main menu >> Management console >> Single Sign-On attribute preference

Set the authentication setting and the user information acquired form provider.

No	Item name	Setting content	Required	Remarks
1	Attribute ID	Auto-numbered	○	
2	Provider name	Provider name	○	Select provider registered in “SSO basic preference” from the pulldown menu
3	Item name	Setting item	○	Select the item to be set from the pulldown menu. ※Please refer to “Setting item list” in the follows.
4	Setting value	Setting value		The setting value for the setting item

※Provider and Setting item have to be unique.

Setting item list

Authentication method	Item name	Setting content	Required	Remarks
OAuth2	clientId	authentication client id	○	Set the value obtained from authentication provider
	clientSecret	authentication client secret	○	Set the value obtained from authentication provider
	authorizationUri	User authentication endpoint	○	Please check the specification of authentication provider and set
	accessTokenUri	accessToken acquisition endpoint	○	Please check the specification of authentication provider and set
	resourceOwnerUri	User information acquisition endpoint	○	Please check the specification of authentication provider and set
	scope	User information acquisition scope		Please check the specification of authentication provider and set
	id	User id key name	○	Key name of user data obtained from resourceOwnerUri
	name	User name key name	○	Key name of user data obtained from resourceOwnerUri
	email	User email key name		Key name of user data obtained from resourceOwnerUri
	imageUrl	User image URL key name		Key name of user data obtained from resourceOwnerUri ※Separate with “>” if key is stored in array.
	ignoreSslVerify	SSL Certificate verification option		Enables/Disables SSL server certificate validation. SSL Server certificate validation is enabled by default. ※By setting ”1”, SSL Certificate validation will be turned off.
Others	proxy	Specify proxy for external connection		tcp://(host name or IP address):(Port number) or http://(host name or IP address):(Port number)
Others	debug	Debug flag		Display the details on the screen if SSO login failed. ※Set ”1” to active the debug flag.

④ About the display on login screen

The following condition are required for information to be displayed on the login screen

・The “Display flag” is set to “Display” in “②Register SSO basic preference in ITA”

・All required item of authentication method in “③Register SSO attribute preference in ITA” are

registered

・All end point Uri are registered with string that starts from “https://” or “http://”

・Proxy is registered in the format described in the remarks if registered

⑤ How to check if the settings are correct without displaying on the login screen

If SSO is displayed on the login screen, the login operation will be performed even if users do not know whether the setting is correct.

It is recommended to set the "Display flag" of "②Register SSO basic preference in ITA " to "Display" after confirming whether users can log in.

If the display flag on the login screen is set to "Hide", users can verify the operation by entering the following URL directly into the browser.

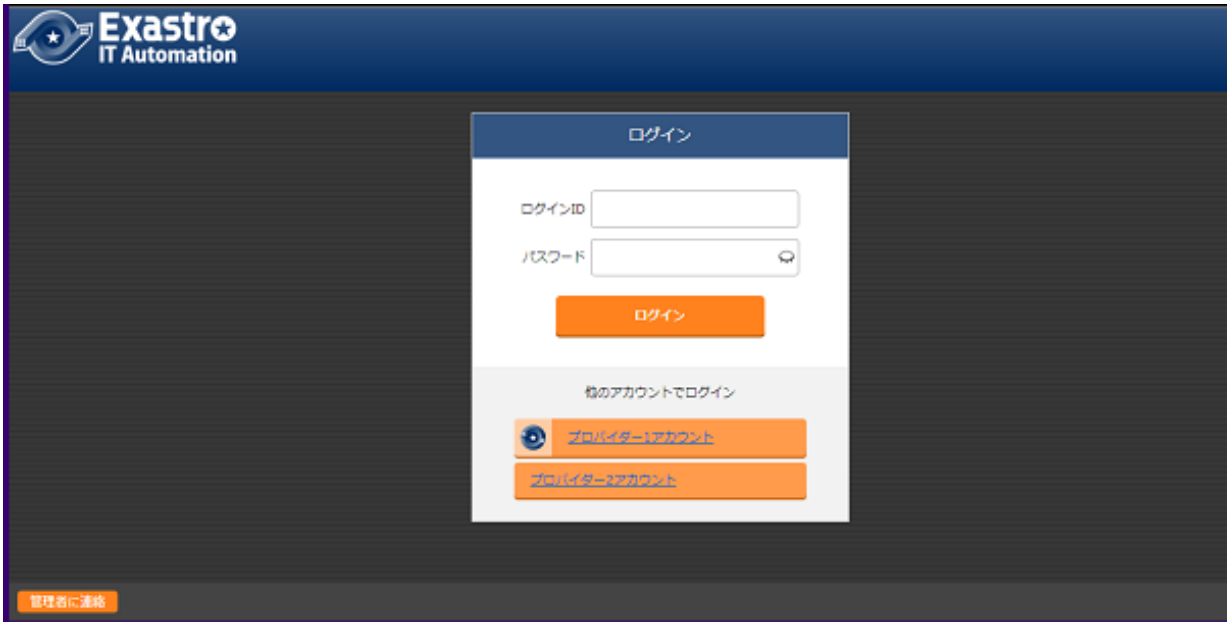
No	Authentication method	Operation checking URL
1	oauth2	https://(FQDN of ITA)/common/common_sso_auth.php?oauth2&providerId=(provider ID) ※Provider ID is the item in “SSO basic preference” menu

6 About role

ITA user are automatically created when user is authenticated by SSO
Furthermore, the user is automatically linked to SSO default role (Role ID: 210000001) when logging in for the first time.
※Role linkage is performed only for the first time.
The role is not linked to any menu on default so please link the role to proper menu beforehand.
Please set the role linkage in Main menu >> Management console >> Role/User link list

7 Login screen

After completing the above setting flow and setting the display flag on the login screen to "Display", SSO information will be displayed at the bottom of the login screen.
SSO authentication will be performed by clicking the provider.
The logo registered in “Single Sign-On basic preference” is displayed before the provider name.



8 Screen after login

SSO provider information will be displayed as the login user information on the top-right of screen after SSO login.
The logo of provider registered in “Single Sign-On basic preference” will be displayed if registered. Provider name will be displayed if not registered.
The user icon will be displayed on the right side of provider information if “imageUrl” is registered in “Single Sign-on Attribute preference” and acquired from provider.

Provider logo is registered and user icon can be acquired.

Provider logo is not registered and user icon can’t be acquired.

9 About SSO authentication user management

The name and email address of SSO authenticated user which obtained from authentication provider.
Even though the information can be changed in ITA management screen, the information will be rewritten by the information acquired from authentication provide after next login.
However, login ID will not be changed if it is set in ITA user list.
Also, even if the user is discarded in ITA management console menu, if the user can log in on the provider side, it will be automatically restored when logging in to ITA. But, it is not linked to the SSO default role.
If you do not want to use a specific user, please restrict the use of ITA by deleting the user on the provider side or preventing the user from logging in, or by not assigning it to any role on the ITA side.

10 About using with AD (Active Directory) together

SSO authentication can be used with AD authentication simultaneously.
Normally, if AD authentication is enabled in ITA, users and roles other than the system administrator (user ID: 1) and system administrator role (role ID: 1) are automatically discarded if they are not listed in the Active Directory configuration file, but the SSO authenticated user (authentication method: sso) and SSO default role (role ID: 2100000001) will not be discarded.

12.Important points regarding Reverse PROXY Environment

※Any problems written in this section will not occur if you are not using Reverse PROXY

If you are using Reverse PROXY for load balancing when users access ITA, You will need to configure additional settings on the reverse PROXY server for SSH Authentication in the following cases.

- HTTPS (Client(Browser)<->Reverse PROXY Server) is not used.
- AWS ELB(ALB,CLB) is not used。
  ※This problem does not occur with AWS ELB (ALB,CLB)
- Reverse PROXY ⇒ The requestor protocol information header (X_FORWARDED_PROTO) is not being sent between ITA servers.

If all the conditions above are met, there is a possibility that a protocol other than the original will be substituted during the SSO Authentication flow. If only one of the two is being used when switching, an error will occur.
While it is possible to do reverse PROXY with open source software such as Apache, The request protocol information might not be sent by default.
Below, we have an example of using Reverse PROXY in Apache to configure additional headers.
※Other cases will be skipped.

Access URL: http://example.com
Reverse Proxy URL: http://192.168.100.1

```
<VirtualHost *:80>
    ServerName   example.com
    ErrorLog     (Abbr.)
    CustomLog    (Abbr.)
    ProxyRequests Off
    ProxyPass / http://192.168.100.1/
    ProxyPassReverse / http://192.168.100.1/
    RequestHeader set X-Forwarded-Proto http
</VirtualHost>
```

※Add the underlined lined to the settings.