SafeNet Keycloak Agent

SafeNet Keycloak Agent is used for integration of a Keycloak Identity provider function (IDP) with SAS PCE. With this integration, SAS PCE provides multi-factor authentication in context of authentication requests received by the Keycloak IDP from SAML or OIDC integrated applications. This agent is also a key component of STA Hybrid Access Management Add-On (https://thalesdocs.com/sta/operator/authentication/hybrid/index.html) based deployment.

SafeNet Keycloak Agent also supports Signal Sign-On (SSO) for applications integrated through Keycloak IDP. If an SSO exists for the same user and browser, SAS PCE is not invoked for token-based multi-factor authentication (MFA) and access is permitted when an access attempt reaches the Keycloak IDP. The access event is logged in the Keycloak IDP in this situation. If SSO is absent, SAS PCE is used for token-based MFA. If the authentication is successful, SSO is launched in the context of the users and the browser on the their system.

System Requirements

Operating System

The SafeNet Agent for Keycloak is supported by Java compatible operating systems (Linux or Windows).

Software Requirements

- Oracle JDK 8 – JDK 11, OpenJDK 11
- SAS PCE
- Keycloak Server

Prerequisites

Configuration of these components is necessary for the installation of SafeNet Keycloak Agent.

SAS PCE

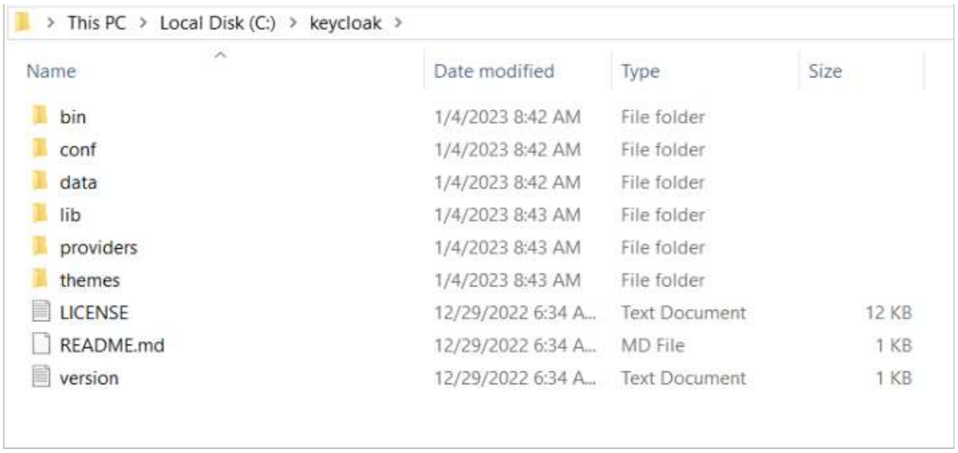
SafeNet Authentication Service PCE v3.16 and above is supported.

Caution

SAS API is not supported with SAS configured on PostgreSQL, hence SafeNet Keycloak Agent setup with SAS user federation does not work. But LDAP user federation works.

Keycloak Server

- Ensure that the Keycloak server version 19.0.3 is deployed on the system along with administrator user setup. For installation and configuration, refer to the server section in the Keycloak Server Guide (https://www.keycloak.org/guides#server).
- Refer to the Server Initialization (https://www.keycloak.org/docs/latest/server_admin/#server-initialization) section of the *Keycloak Server Administrator Guide* to setup the administrator user and master realm.
- Ensure the Keycloak server's directory structure contains "bin/", "conf/", "lib/", "data/", "providers/" and "themes/".



Name	Date modified	Type	Size
bin	1/4/2023 8:42 AM	File folder	
conf	1/4/2023 8:42 AM	File folder	
data	1/4/2023 8:42 AM	File folder	
lib	1/4/2023 8:43 AM	File folder	
providers	1/4/2023 8:43 AM	File folder	
themes	1/4/2023 8:43 AM	File folder	
LICENSE	12/29/2022 6:34 A...	Text Document	12 KB
README.md	12/29/2022 6:34 A...	MD File	1 KB
version	12/29/2022 6:34 A...	Text Document	1 KB

- You need to run Keycloak 19.0.3 with the old admin console. For that, you must disable the new console (admin2) by adding the following in your keycloak.conf file :

  ```
  features-disabled=admin2
  ```

  Note

  For more details, refer to https://www.keycloak.org/2022/07/keycloak-1900-released (https://www.keycloak.org/2022/07/keycloak-1900-released).

- Ensure the SAS Token Validator service is accessible from the system where the Keycloak is configured.
  `http(s):<sas-server-ip>:<port>/TokenValidator/TokenValidator.asmx`

Keycloak Server Migration

In Keycloak version 19, Quarkus distribution is the default distribution. For those who have been using Keycloak Wildfly distribution, it is required to migrate to Quarkus distribution.

If you are using **Keycloak Agent 1.2.0** with Keycloak version 15.0.2 (Wildfly), follow the steps below to migrate to **Keycloak Agent 1.3.0** with Keycloak version 19.0.3 (Quarkus):

1. Create a backup of the old installation, including configuration, themes, and others.
2. Create a backup of the database using the instructions in the documentation for your relational database.
3. Upgrade the Keycloak server. The database will no longer be compatible with the old server after the upgrade.
4. If you need to reverse the upgrade, restore the old installation first, and then restore the database from the backup.

For more detail on migration procedure, see the Upgrading Guide (https://www.keycloak.org/docs/19.0.3/upgrading/#intro) version 19.0.3.

Terminologies

- **Keycloak Directory**: Keycloak server installation directory.
- **Authentication Flow**: An authentication flow is a container for all authentications, screens, and actions that are mandatory during login, registration, and other Keycloak workflows.

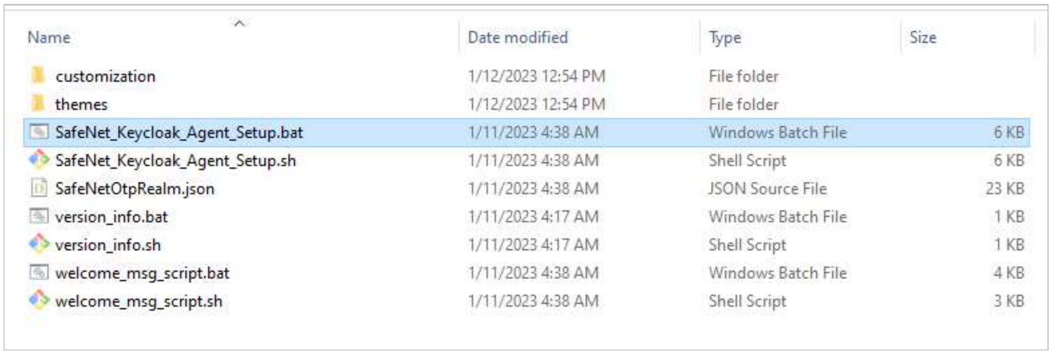
Package Contents

The SafeNet Keycloak Agent is a compressed **zip|tar.gz** file. The **SafeNetKeycloakAgent** Package contains:

- Setup scripts

- Binaries
- Themes resources
- SafeNet OTP Realm json file
- Realm configuration and Authentication flows defined for SAS OTP Validation.

To unpack this file, run the **unzip**, **gunzip** or **tar utilities**.



Name	Date modified	Type	Size
customization	1/12/2023 12:54 PM	File folder	
themes	1/12/2023 12:54 PM	File folder	
SafeNet_Keycloak_Agent_Setup.bat	1/11/2023 4:38 AM	Windows Batch File	6 KB
SafeNet_Keycloak_Agent_Setup.sh	1/11/2023 4:38 AM	Shell Script	6 KB
SafeNetOtpRealm.json	1/11/2023 4:38 AM	JSON Source File	23 KB
version_info.bat	1/11/2023 4:17 AM	Windows Batch File	1 KB
version_info.sh	1/11/2023 4:17 AM	Shell Script	1 KB
welcome_msg_script.bat	1/11/2023 4:38 AM	Windows Batch File	4 KB
welcome_msg_script.sh	1/11/2023 4:38 AM	Shell Script	3 KB

Keycloak SAS Providers (Keycloak SPIs)

On the functional level, the package updates the following modules on the pre-installed Keycloak server.

- **SafeNet OTP Authentication Flow** – Customized authentication flow for OTP validation with SAS Token Validator service.
- **SafeNet Theme** – Customized theme to define SafeNet HTML templates and stylesheets.

Set up SAS API for SAS PCE

Caution

This setup is mandatory when SAS is configured with MySQL database.

SAS API requests data from SAS PCE to dynamically update the SafeNet Keycloak Agent.

Note

SAS API encounters an issue with MySQL database (MySQL EF6 DLL in GAC missing). It is a limitation of MySQL Connector 8.0.27.

When SafeNet Keycloak Agent is configured with SAS using MySQL database, follow below steps.

Before installation ensure that the following steps are performed:

1. After installing SafeNet server, install MySQL 8.0.27 Connector.
2. Configure SafeNet server with MySQL database.
3. Copy the following text in a text file and save the file in the **.ps1** file format:

```
#Note that you should be running PowerShell as an Administrator
[System.Reflection.Assembly]::Load("System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a")

$publish = New-Object System.EnterpriseServices.Internal.Publish
$publish.GacInstall("C:\Program Files (x86)\MySQL\MySQL Connector Net 8.0.27\Assemblies\v4.5.2\MySql.Data.EntityFramework.dll")
```

```
#If installing into the GAC on a server hosting web applications in IIS, you need to restart IIS for the #applications to pick up the change.
Iisreset
```

4. Run the **.ps1** file, as an Administrator in the PowerShell.

5. Reset IIS.

Points to Remember

- Default location: `System Directory:\Program Files (x86)\MySQL\MySQL Connector Net 8.0.27\<locate MySql.Data.EntityFramework.dll file>`

- If someone changes the directory location while installing the MySQL Connector, the above path also needs to be updated in the script.

- Open the PowerShell script and change the path to where your DLL resides.

Configuration overview

- Setup of the SafeNet Agent for Keycloak (../../agents/keycloak/setup_safenet/index.html) and Realm Configuration (../../agents/keycloak/rc/index.html) are mandatory.

- User Federation Setup (../../agents/keycloak/user_federation_setup/index.html) (Either LDAP or SAS User Federation is mandatory).

- Customization (../../agents/keycloak/customization/index.html), Logging in SafeNet Agent for Keycloak (../../agents/keycloak/logging_in_safenet/index.html) and Testing the End User Login flow (../../agents/keycloak/testing/index.html) are optional.

Note

Set up of SAS PCE is required for end to end setup and validation for STA Hybrid (https://thalesdocs.com/sta/operator/authentication/hybrid/index.html) environment.