

Client's guide to set up SSO with eFileReady

© eFileReady LTD	v1.0	12/07/2023	Page 1 of 13
------------------	------	------------	--------------

Document Control

Date Approved:	12/07/2023	Date or Frequency of Next Review:	
Approved by:	Juan Ho		
Author:		Date of Creation:	
Reviewer:			
Policy/Document Owner:	Juan Ho, Director of Company		
Supporting Documents	Not applicable		

Revision History

Version Control	Effective Date	Author	Approved by	Amendment
1.0	12/07/2023		Juan Ho	Initial Version

Table of contents

[Client's guide to set up SSO
with eFileReady](#)

[Table of contents](#)

[1. Introduction](#)

[1.1. Overview](#)

[1.2. Document overview](#)

[1.3. Target audience](#)

[2. SSO set up at client's side](#)

[2.1. Steps to be followed by Application System Administrator and SSO Administrator to set up SSO at client's side](#)

[2.1.1. Creating a new company account](#)

[2.1.2. Activating the account](#)

[2.1.3. Providing Application System Administrator and company details](#)

[2.1.4. Creating a Dummy Redirect URI](#)

[2.1.5. Providing SSO provider details](#)

[2.1.6. Capturing the Sign In URL and Redirect URI](#)

[3. Configuring Sign In URL](#)

[3.1. Dedicated eFileReady server](#)

[3.2. Shared eFileReady server](#)

[4. User Access Rights](#)

[4.1. Application System Administrator managing additional users](#)

[4.2. User roles at SSO provider](#)

[5. Appendix](#)

[5.1. Legend](#)

© eFileReady LTD	v1.0	12/07/2023	Page 3 of 13
------------------	------	------------	--------------

1. Introduction

1.1. Overview

At present, our users login into the eFileReady application (henceforth, known as “the application” for brevity) using the application provided user credentials like User Sign In ID, User Sign In Password. The application is web based and accessed using any modern web browser like Chrome, Firefox etc. on desktops, laptops and mobile devices.

The user id and password based sign in process has been in effect since a long time ago and no technical or security issue has ever been found so far. Users are able to login to our application and conduct all necessary activities related to eFiling to HMRC without hurdles. However, users need to remember another set of user credentials to login into our application.

We need a solution to help our users remember only one set of account credentials to access their internal applications and our eFileReady application too. This would make the login more seamless.

Hence, in the target state, the users would transition to a more seamless Single-Sign On process by leveraging their enterprise provided account credentials to access and use our application. This would enable users to remember only one set of credentials given by their enterprise.

With OpenID Connect or SAML, we can cater to below needs:

- Need 1: Understand required user information returned by SSO provider. This would enable us to verify the extracted email etc. as needed within our application.
- Need 2: Understand authentication response returned by SSO provider. This would help us to determine if the user was successfully authenticated.

© eFileReady LTD	v1.0	12/07/2023	Page 4 of 13
------------------	------	------------	--------------

- Need 3: Retire username and password based login into our application. This would help users remember only their enterprise provided account credentials to access and use our application.

1.2. Document overview

This document explains the steps that the SSO provider team needs to take in order to successfully integrate their SSO with eFileReady.

1.3. Target audience

This document is mainly targeted towards SSO administrators, application managers on both eFileReady and client side.

© eFileReady LTD	v1.0	12/07/2023	Page 5 of 13
------------------	------	------------	--------------

2. SSO set up at client's side

2.1. Steps to be followed by Application System Administrator and SSO Administrator to set up SSO at client's side

We expect SSO configuration at client side to be active and working successfully to enable live communication between eFileReady and SSO provider. Only then, users will be able to sign in using SSO.

To facilitate this, the SSO administrator would need to configure an appropriate OpenID Connect or SAML based record for eFileReady at their side. They need to follow below steps to help them create such a record:

2.1.1. Creating a new company account

It all starts with a designated Application System Administrator at client's side visiting eFileReady application website and signing up for an account.

During the signup process, the Application System Administrator provides company details and continues to get an email containing "Account Email Verification Code".

2.1.2. Activating the account

The Application System Administrator needs to enter the "Account Email Verification Code" within the eFileReady application to successfully activate the account.

2.1.3. Providing Application System Administrator and company details

At this point, the Application System Administrator provides their personal details and then their company's registered office and business address details and continues.

© eFileReady LTD	v1.0	12/07/2023	Page 6 of 13
------------------	------	------------	--------------

2.1.4. Creating a Dummy Redirect URI

We understand that for the SSO Administrator to provide Client Id and Client Secret they require Redirect URI to be available especially when the access type is Confidential.

Since eFileReady generates the Redirect URI after taking Client Id and Client Secret as inputs, we suggest that the SSO Administrator create a dummy redirect URI first at their SSO provider portal page for e.g., something like "dummy.redirect.uri".

Then, they can get Client Id and Client Secret from their portal page. These are required to be provided in the next step below.

2.1.5. Providing SSO provider details

Here, the Application System Administrator needs to provide below SSO details for the eFileReady application to understand SSO requirements and be able to generate an unique "Sign In URL" and "Redirect URI".

Application System Administrator needs to discuss with SSO Administrator as needed to understand the values required to be provided as inputs below.

These generated details would need to be configured at client's side to allow their users to sign in using SSO.

SSO details required by eFileReady:

Input field required	Description
SSO Administrator Name	Enter your SSO Administrator full name
SSO Administrator Email	Enter your SSO Administrator Email address
SSO Administrator Mobile No.	Enter your SSO Administrator Mobile number
SSO Protocol	Select your preferred protocol to integrate eFileReady

	<p>with SSO provider. You can either choose OpenID Connect or SAML.</p> <p>Based on the selection you make here, either SAML related fields or OIDC related fields will show up for you to further enter.</p>
SSO Federation	Select your SSO provider that would act as the authorization server.
Access Setup	<p>Select the access setup. You can choose either Public or Private.</p> <p>You would choose Public if your SSO provider is publicly accessible.</p> <p>You would choose Private if your SSO provider is accessible only within your intranet network.</p>
Client Id	The unique identifier that you want to use at your SSO portal to identify our eFileReady application
Client Secret	The secret value that gets generated at your SSO portal
Username Attribute	The attribute within the ID token carrying the user name. For e.g., sub attribute is such an attribute that carries user name
SSO Setup Preference	<p>If you want to provide your SSO provider discovery URI and let the application derive other URIs like tokenURI, authURI etc. then you would choose "To Provide OIDC Discovery URI".</p> <p>If you want to provide your SSO provider URIs explicitly then you would choose "To Provide URIs individually".</p>
Client Authentication Method	<p>You can choose different authentication methods, like client_secret_basic etc.</p> <p>TODO: Other methods are yet to be supported yet.</p>
Scope	By default, openid , email and profile scopes are

	preselected and can't be changed at present
Discovery URI	The URI that you can get from an SSO provider portal. It's typically named as "well-known openid configuration" URI.
Authorization URI	This endpoint is responsible for authenticating the end-user and obtaining consent for the requested claims or scopes.
Token URI	After the client application has received an authorization code from the Authorization Endpoint, it will make a request to the Token Endpoint to exchange this code for an access token and/or an ID token.
JWK Set URI	The endpoint which exposes a set of public keys that the client application can use to verify any JWTs (JSON Web Tokens) issued by the authorization server.
Userinfo URI	The Userinfo URI, also known as the Userinfo Endpoint, is an endpoint in OpenID Connect from which client applications can retrieve claims about the authenticated end-user. These claims can contain profile information about the user, such as their name, email, and so forth.

2.1.6. Capturing the Sign In URL and Redirect URI

After the Application System Administrator provides SSO details and continues, they would get below details from eFileReady which are automatically generated.

SSO details generated by eFileReady:

Output field generated	Description
SignIn URL	An unique URL generated by eFileReady after providing all the inputs above.

	This will be used by the client users to get redirected to their SSO provider to authenticate themselves.
Redirect URI	An unique URI generated by eFileReady. This is where the SSO Federation would send the user after they have authenticated successfully using SSO.

At this point, the SSO administrator can override the dummy redirect URI value provided earlier at their SSO provider portal page with the eFileReady generated redirect URI above.

3. Configuring Sign In URL

3.1. Dedicated eFileReady server

If you are using a dedicated eFileReady server, then we shall configure the sign in URL for you with the above automatically generated sign in URI.

However, you still need to configure the redirect URI at your SSO provider portal.

3.2. Shared eFileReady server

If you are using a shared eFileReady server, then <TODO: ADD HERE OUR APPROACH>

4. User Access Rights

4.1. Application System Administrator managing additional users

The user's access rights are managed within the eFileReady application tool.

At first, the client's designated user signs up for a company account at our eFileReady.

This user is termed a 'Application System Administrator' and can later create multiple additional system users and assign various access rights.

The SSO set up with eFileReady system, regardless of which SSO Federation, generally involve the following:

- 1) The Application System Administrator needs to click on SIGN UP at www.efileready.com to create an account.
- 2) After the Application System Administrator given email has been verified the Application System Administrator will be requested to fill in the SSO details based on the protocol (OIDC or SAML) used.
- 3) Upon completion of the SSO setup the Application System Administrator will be able to sign in to www.efileready.com via SSO.
- 4) All eFileReady Application System Administrator users are required to manage their own users, either appointing a user or suspending an additional user for the system by logging on to eFileReady system user manager.

4.2. User roles at SSO provider

There is only ever one 'Application System Administrator' to an account sign up.

Hence, eFileReady doesn't need SSO provider roles details returned to eFileReady post SSO sign in.

© eFileReady LTD	v1.0	12/07/2023	Page 12 of 13
------------------	------	------------	---------------

5. Appendix

5.1. Legend

This section provides general guidance understanding various terms we have used throughout this document.

Term	Meaning
Application System Administrator	<p>The user designated by your company will sign up and create a company account with eFileReady.</p> <p>This user will later add additional users and manage their access rights after signing in.</p>
SSO Administrator	<p>The user that typically manages your SSO provider. They will be the one that configures eFileReady at SSO portal to enable communication between eFileReady and your SSO provider.</p>