

SSO Partner User Manual

© eFileReady LTD	v1.0	12/07/2023	Page 1 of 14
------------------	------	------------	--------------

Table of contents

[SSO Partner User Manual](#)

[Table of contents](#)

[1. Introduction](#)

[2. Steps for implementing eFileReady's SSO](#)

[2.1. Creating an eFileReady Account](#)

[2.2. Designation of an SSO Administrator](#)

[2.3. SSO Activation and Setup by the Administrator](#)

[2.4. Configuring SSO Details](#)

[2.4.1. Section 1: eFileReady SSO details](#)

[2.4.2. Section 2: eFileReady Partner SSO Federation Details](#)

[2.4.3. Section 3: SSO Implementation Important Note](#)

[2.4.3.1. Transitioning to 'ACCESS BY SSO ONLY'](#)

[2.4.3.2. Company-Level SSO Implementation](#)

[2.4.4. Verifying SSO setup configuration](#)

[2.4.4.1. Accessing eFileReady through Your Federation](#)

[2.4.4.2. Authenticating SSO Administrator Access](#)

[2.4.4.3. Confirmation of Successful SSO Authentication](#)

[2.4.4.4. Cross-verification by the Application System Administrator](#)

[2.4.4.5. Onboarding Additional Users via SSO](#)

[2.4.5. Onboarding Additional Users through SSO](#)

[2.4.6. Modifying & Upgrading SSO Settings](#)

[2.4.7. Seeking Assistance from eFileReady Support](#)

[2.4.8. Activating the SSO System](#)

[3. eFileReady SSO Guidelines and Contingency Measures](#)

[3.1. SSO Guidelines](#)

[3.2. Contingency Measures](#)

[4. Configuration of Sign In URL](#)

[4.1. For Dedicated eFileReady Servers](#)

[4.2. For Shared eFileReady Servers](#)

[5. Managing User Access Rights](#)

© eFileReady LTD	v1.0	12/07/2023	Page 2 of 14
------------------	------	------------	--------------

[5.1. Role of the Application System Administrator](#)

[5.2. Defining User Roles at the SSO Provider](#)

[6. Appendix](#)

[6.1. Legend](#)

[6.2. eFileReady logos](#)

© eFileReady LTD	v1.0	12/07/2023	Page 3 of 14
------------------	------	------------	--------------

1. Introduction

eFileReady offers two distinct methods for customers to access our service:

- Traditional username and password authentication.
- Single Sign-On (SSO) authentication.

We support SSO through various providers, including Keycloak, OpenAM, AzureAD, Ping, Google, and Yahoo.

Our proven SSO implementation is OpenID Connect with any SSO provider. We are currently looking into supporting SAML as an alternative.

2. Steps for implementing eFileReady's SSO

2.1. Creating an eFileReady Account

Begin by registering an account with eFileReady using the standard username and password method. The Application System Administrator should create a new company account, entering company and personal details, and setting up the usual sign-in credentials.

2.2. Designation of an SSO Administrator

The Application System Administrator designates an SSO Administrator. This is achieved by navigating to Employer/Contractor (in the top menu) → User Accounts Manager → Manage System Users → Add New User. Ensure that "SSO Setup" is chosen as the exclusive user access right for this SSO Administrator.

2.3. SSO Activation and Setup by the Administrator

Once appointed, the SSO Administrator activates their account and logs into eFileReady conventionally. From the dashboard, they should select the "View/Edit Single Sign-On (SSO)" button to initiate the SSO setup process.

© eFileReady LTD	v1.0	12/07/2023	Page 4 of 14
------------------	------	------------	--------------

2.4. Configuring SSO Details

Within the Single Sign-On Details page, there are three sections that the SSO Administrator must review and configure appropriately to finalise the SSO integration with eFileReady.

2.4.1. Section 1: eFileReady SSO details

eFileReady automatically generates and displays the Sign-In URL and associated Redirect URIs, which should be set up on the SSO provider's end. The SSO Administrator should input these Redirect URIs into the "Valid Redirect URIs" section of the OpenID Connect client record specifically tailored for eFileReady on the SSO provider's portal.

For a comprehensive understanding of the required values for SSO integration, we suggest referencing the "SSO Partner Manual" (this document).

An example list of automatically generated URIs is provided below:

#	Generated item description	Sample value
1	Sign In URL	https://www1.efileready.com/portal/signin/sso/6c093ee8-b7ed-4217-ab06-46cee2425579
2	Redirect URI - public	https://www1.efileready.com/portal/login/oauth2/code/6c093ee8-b7ed-4217-ab06-46cee2425579
3	Redirect URI - private	https://www1.efileready.com/portal/login/sso/code/6c093ee8-b7ed-4217-ab06-46cee2425579

2.4.2. Section 2: eFileReady Partner SSO Federation Details

Based on the SSO protocol selection:

For "SAML": The SSO Administrator needs to provide SAML-specific details.

For "OpenID Connect": OpenID Connect-specific details are required.

Below details are needed when OpenID Connect is chosen as the SSO protocol.

© eFileReady LTD	v1.0	12/07/2023	Page 5 of 14
------------------	------	------------	--------------

Input field required	Description
SSO Protocol	<p>We hope your SSO federation supports OpenID Connect which works best for our eFileReady system.</p> <p>However, if for whatever reason you cannot use OpenID Connect, please choose SAML as the alternative.</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 identity our eFileReady application
Client Secret	The secret value that gets generated at your SSO portal
Re-enter Client Secret	The secret value that needs to be entered again to confirm it
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 Discovery URL".</p> <p>If you want to provide your SSO provider URIs explicitly then you would choose "To Provide URIs individually".</p>
Client Authentication Method	You can choose only client_secret_basic as the authentication method.
Scope	By default, openid , email and profile scopes are preselected and can't be changed at present
Grant Type	We support only authorization_code grant type at present.
Discovery URL	The URI that you can get from an SSO provider portal. It's typically named as "well-known openid configuration" URI.
Authorization	This endpoint is responsible for authenticating the end-user and obtaining consent for the

© eFileReady LTD	v1.0	12/07/2023	Page 6 of 14
------------------	------	------------	--------------

Endpoint	requested claims or scopes.
Token Endpoint	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.
JWKS URI (JSON Web Key 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 Endpoint	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.

Below details are needed when SAML is chosen as the SSO protocol.

Input field required	Description
SSO Protocol	We hope your SSO federation supports OpenID Connect which works best for our eFileReady system. However, if for whatever reason you cannot use OpenID Connect, please choose SAML as the alternative.
SSO Federation	Select your SSO provider that would act as the authorization server.
Access Setup	Select the access setup. You can choose either Public or Private. You would choose Public if your SSO provider is publicly accessible. You would choose Private if your SSO provider is accessible only within your intranet network.
SSO Provider Metadata Location	Single Sign-On (SSO) provider metadata location is a URL endpoint or a file that contains necessary configuration information for the Service Provider (SP) to communicate with the Identity Provider (IdP).
SSO Provider Entity ID	The Entity ID is used within the SAML federation to identify the SSO provider. It's often a URI (Uniform Resource Identifier), but it does not need to point to an actual resource on the web. It's not used as a location, but rather as a unique name.
Application Entity ID	The Entity ID is used within the SAML federation to identify the service provider.

© eFileReady LTD	v1.0	12/07/2023	Page 7 of 14
------------------	------	------------	--------------

	It's often a URI (Uniform Resource Identifier), but it does not need to point to an actual resource on the web. It's not used as a location, but rather as a unique name.
Sign Authentication Request	Whether to sign the SAML authentication request or not. You would choose Yes if you want eFileReady to sign the authentication request, else a No value.

2.4.3. Section 3: SSO Implementation Important Note

The SSO Administrator determines user access preference by choosing between "SSO Sign In Only" or "Conventional Sign In Only" and then confirming the choice with a password.

"SSO Sign In Only": Users from the respective company can exclusively access via the SSO method.

"Conventional Sign In Only": Users can solely access through the traditional method.

However, the exception is the SSO Administrator, who has the flexibility to use both sign-in methods.

Essential points for the SSO implementation:

2.4.3.1. Transitioning to 'ACCESS BY SSO ONLY'

- The decision to transition users to 'ACCESS BY SSO ONLY' rests with the SSO System Administrator.
- At any stage, the SSO System Administrator can switch between 'Access by SSO only' and 'Access by CONVENTIONAL Sign In'.
- To determine the access method for all users, the SSO Administrator merely selects the preferred option and verifies with a password.
- This transition can occur during either the testing phase or actual live operation.

© eFileReady LTD	v1.0	12/07/2023	Page 8 of 14
------------------	------	------------	--------------

2.4.3.2. Company-Level SSO Implementation

- It's imperative to understand that no mixed access option is available for different authorised users. In other words, it's an all-or-nothing approach: either all users access via Conventional Sign In, or all access via SSO Sign In method.
- Only the SSO System Administrators can interchange between SSO or Conventional Sign In methods while signing in.

2.4.4. Verifying SSO setup configuration

It's imperative to rigorously test and validate the established SSO setup before it's deployed for broader use.

The SSO Administrator should link the Sign In URL, previously mentioned in section 1, with the eFileReady icon provided in the Appendix.

Consider this analogy

An example company has its primary dashboard portal with several application icons representing various services like "Holidays," "Benefits," and others. If the company wishes to include eFileReady as one of these services, they would position the eFileReady icon on the dashboard and tie it to the Sign In URL. Consequently, users would be directed to the SSO provider's authentication page upon clicking the eFileReady icon.

Steps to Verify the SSO Setup:

2.4.4.1. Accessing eFileReady through Your Federation

Upon linking the Sign In URL to the eFileReady icon, the SSO Administrator should initiate by clicking on the eFileReady icon, which will navigate them to the SSO provider's authentication page.

2.4.4.2. Authenticating SSO Administrator Access

The SSO Administrator will enter their allocated company credentials (typically a username and password). Following a successful authentication, they'll seamlessly be redirected to eFileReady to utilise its offerings.

© eFileReady LTD	v1.0	12/07/2023	Page 9 of 14
------------------	------	------------	--------------

2.4.4.3. Confirmation of Successful SSO Authentication

If the authentication process completes without any hitches, the SSO Administrator will be greeted with the authenticated eFileReady page. This landing page is indicative of a successful login process.

2.4.4.4. Cross-verification by the Application System Administrator

Post the SSO Administrator's successful sign-in, other users, especially the Application System Administrator, should attempt an SSO login to ensure complete compatibility. If any sign-in issues arise, they should collaborate with the SSO Administrator to make necessary adjustments.

2.4.4.5. Onboarding Additional Users via SSO

Once the Application System Administrator successfully accesses eFileReady via SSO, they should proceed to onboard other system users, ensuring they too can employ the SSO method for sign-ins.

2.4.5. Onboarding Additional Users through SSO

The Application System Administrator can add more users by navigating through:
Employer/Contractor → User Accounts Manager → Manage System Users → Add New User.

All Application System Administrators on eFileReady are responsible for managing their team members, be it adding a new user or suspending one, via the eFileReady system user manager.

2.4.6. Modifying & Upgrading SSO Settings

If users encounter issues during the SSO sign-in, the SSO Administrator should adjust settings on both the eFileReady and SSO provider's end, then attempt sign-in again.

Moreover, if an upgrade to the SSO setting is needed, such as switching from OIDC to SAML or changing providers from OpenAM to Ping, the SSO Administrator can proceed with the changes.

2.4.7. Seeking Assistance from eFileReady Support

While most SSO sign-in challenges should be resolved during the initial setup or after making necessary adjustments, persistent issues should be escalated to the eFileReady support team for resolution.

© eFileReady LTD	v1.0	12/07/2023	Page 10 of 14
------------------	------	------------	---------------

2.4.8. Activating the SSO System

Once users can consistently sign in via SSO, the setup is deemed complete. The SSO Administrator can then set user access to "SSO Sign In Only", thereby requiring all users to authenticate solely through SSO.

Important Note: Care should be taken before selecting "SSO Sign In Only." Once activated, the conventional sign-in method becomes inaccessible, compelling all users to rely exclusively on SSO.

3. eFileReady SSO Guidelines and Contingency Measures

3.1. SSO Guidelines

Below are the guidelines for implementing and utilising eFileReady with SSO:

- **SSO Administrator Control:** Only the SSO Administrator has the authority to transition to SSO or revert to the conventional sign-in method.
- **Application System Administrator Sign-up:** They must initially sign up for a new company account conventionally, using credentials such as a password and pattern word.
- **Access Rights Selection:** The Application System Administrator is not permitted to amalgamate access rights from "User Operation Rights", "User Management Rights", and "Single Sign-On (SSO) Rights".
- **Appointment of SSO Administrators:** The Application System Administrator has the discretion to nominate multiple SSO Administrators for SSO setup.
- **Static URLs:** Regardless of how often the SSO Administrator accesses the SSO Setup page, the initially generated Sign In URL and Redirect URIs remain unchanged.
- **Email Notifications:** The eFileReady system abstains from emailing the Sign In URL or Redirect URIs (both public and private) to any administrators. This information is available only after successful sign-in on eFileReady.
- **Visibility Based on Sign-in Model:**

© eFileReady LTD	v1.0	12/07/2023	Page 11 of 14
------------------	------	------------	---------------

- When “SSO Sign In Only” is activated by the SSO Administrator, certain columns in the Manage Account and Manage System Users pages will be concealed due to their irrelevance during the SSO period.
- Conversely, activating the “Conventional Sign In Only” option retains visibility of all columns.
- **Account Activation Email:** Additional users, when created under the “Conventional Sign In Only” setting, will receive activation emails detailing the conventional activation method. Otherwise, the email will guide them through the SSO sign-in process.
- **Transaction Password:** For enhanced security, users logging in through SSO for the first time are prompted to establish a Transaction Password, which will subsequently be required for significant updates, like modifying employer information.

3.2. Contingency Measures

In the event of SSO malfunction, the SSO Administrator retains the capability to access the platform conventionally and may grant conventional sign-in permissions to all users.

4. Configuration of Sign In URL

4.1. For Dedicated eFileReady Servers

While we handle the configuration of the sign-in URL for dedicated server users, you must set up the redirect URI on your SSO provider portal.

4.2. For Shared eFileReady Servers

Here, it's your responsibility to link the sign-in URL to the eFileReady icon. This ensures that when your users click the icon, they'll initiate the SSO sign-in process.

© eFileReady LTD	v1.0	12/07/2023	Page 12 of 14
------------------	------	------------	---------------

5. Managing User Access Rights

5.1. Role of the Application System Administrator

Within the eFileReady tool, the user access rights are determined and adjusted. Initially, a designated representative from the client's side registers for a company account on eFileReady, earning the title 'Application System Administrator'. This individual has the authority to introduce multiple system users subsequently and designate varying access rights to them.

It's essential to note that every Application System Administrator is accountable for their user management, be it adding new users or revoking access to existing ones. All these actions are executed via the eFileReady system user manager interface.

5.2. Defining User Roles at the SSO Provider

For every account sign-up, there exists a single 'Application System Administrator'. This person then nominates an SSO Administrator responsible for orchestrating the SSO setup on the eFileReady platform.

An important distinction to make is that eFileReady does not require the return of role details from the SSO provider following an SSO sign-in. The reason for this is that eFileReady internally manages user access rights.

6. Appendix

6.1. Legend

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

Term	Meaning
Application System Administrator	The Application System Administrator, designated by your company, will register and establish a company account on eFileReady. After signing in, this individual will then introduce and oversee access rights for additional users.

© eFileReady LTD	v1.0	12/07/2023	Page 13 of 14
------------------	------	------------	---------------

SSO Administrator	The SSO Administrator is the individual responsible for managing your SSO provider. This administrator configures the integration between eFileReady and your SSO portal, ensuring seamless communication between the two platforms.
Additional User	Additional User is an user that is designated by the Application System Administrator to serve either as an SSO Administrator or as a Functional User.

6.2. eFileReady logos

Logo name	Transparent	Non-Transparent
eFileReady		