



DeliverHealth

eScripture One SSO Configuration and User Guide

Table of contents

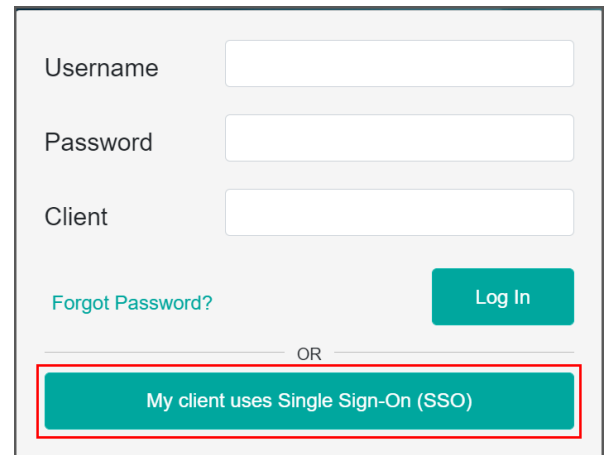
- Introduction 3**
- Prerequisites to Using SSO 4
- IT Steps - Configuring SSO 4**
 - Object IDs..... 4
 - Workflow 4
 - Additional Notes..... 5
- Admin Steps – Inviting Users to Join SSO..... 5**
 - Additional Notes..... 6
- User Steps - Logging in with SSO 7**
 - Accepting the SSO Invitation..... 7
 - Logging in with SSO 8
- Support..... 10**

Introduction

Single sign-on (SSO) allows users to securely log into eScription One with credentials provided by their own organization rather than those created in DeliverHealth. With single sign-on, users have fewer user names and passwords to remember, and clients can impose stricter or more consistent password policies and procedures across multiple applications. Note that users will be required to re-enter their organization credentials when signing into a new application.

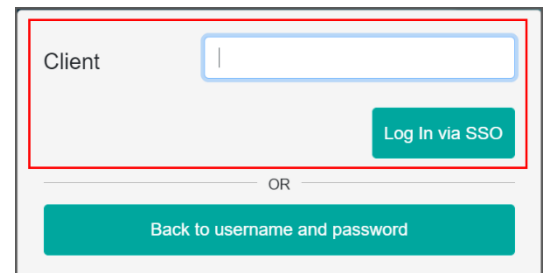
Note: DeliverHealth currently supports only those clients using Microsoft Azure Active Directory.

Once set up for SSO, users will log in by selecting a new SSO option on the eScription One login screen.



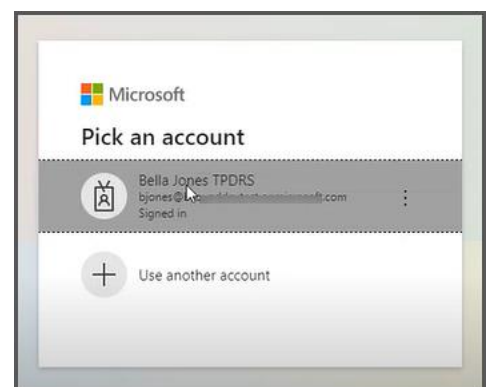
The screenshot shows the eScription One login interface. It features three input fields: 'Username', 'Password', and 'Client'. Below these fields are two links: 'Forgot Password?' and a teal 'Log In' button. A horizontal line with 'OR' in the center separates this section from the SSO option. The SSO option is a teal button labeled 'My client uses Single Sign-On (SSO)', which is highlighted with a red rectangular border.

Next, they will enter their organization's name and click the 'Log In via SSO' button.



The screenshot shows the eScription One login interface. It features a 'Client' input field and a teal 'Log In via SSO' button. Below these fields is a horizontal line with 'OR' in the center, and a teal button labeled 'Back to username and password'. The 'Log In via SSO' button is highlighted with a red rectangular border.

Lastly, they will select their Microsoft account on the Microsoft Sign in page to be automatically logged into their eScription One application (after having successfully signed in during the initial setup).



The screenshot shows the Microsoft Sign in page. It features the Microsoft logo and the text 'Pick an account'. Below this, there is a list of accounts. The first account is 'Bella Jones TPDRS' with the email address 'bjones@tpdr.com' and the text 'Signed in'. Below the list is a plus sign icon and the text 'Use another account'.

Prerequisites to Using SSO

To use SSO, a client must meet the following requirements:

- The client must be active on eScription One
- The client must be using Microsoft Azure Active Directory (AAD) as an identity provider

Once these prerequisites are established, eScription One will work with your organization's IT department to establish SSO as a sign on method.

IT Steps - Configuring SSO

To establish the connection to a customer's SSO, eScription One requires the customer's Azure AD Tenant ID. The Tenant ID is added (manually) to the eScription One database. eScription One uses OpenID Connect to integrate with the Azure AD Tenant.

No Enterprise Application needs to be created on the customer's end in advance; an Enterprise Application will appear once we establish a connection. The app registration name will be **eScription One**.

Object IDs

For each user, the Object ID is a requirement for our configuration as we need the unique identifier for the individual user in our platform.

Sign-ins that use OpenID Connect return an access token and an ID token. The ID token contains claims about the user, and ID tokens returned from Azure AD include the Tenant ID and the Object ID.

Prior to the first time a user signs in to an eSOne application using SSO, we create a link between their existing eSOne user profile in our database and these claims. Then, whenever the user signs in with SSO, we can use those two claims to know which user has signed in.

Note: Our implementation does not currently support Azure AD Groups.

Workflow

Currently, linking large groups of users must be done on the backend via script.

For smaller groups of users, an eScription One client admin will link a user to the organization's Microsoft Azure Tenant without a backend script. The high-level workflow is as follows:

- **Invite** – the client admin invites a user to join SSO via a new SSO Invite button in InCommand
- **Accept** – the user receives the Invite through their organization's email and clicks the link to accept
- **Link** – after a successful 'linking', the user is directed to log into their organization's MS login page. The user's profile is now linked to the organization's MS Tenant ID.

- **SSO Login** – the user selects a new SSO Login button when logging into an eScription One app, and logs in with MS credentials

Additional Notes

- Microsoft Graph API permissions are required for SSO functionality. These permissions are typically granted through user consent. When the user first signs in with SSO they are shown a consent screen and are asked to grant permission to access their basic profile information to sign them in. The required permissions are "openid", "profile", "email", and "offline_access".
- Automated user-provisioning is not necessary/desired for the application.
- A client can activate SSO for just one user. Users not yet enrolled in SSO within the client will continue to log in through the current eSOne Username and Password process.

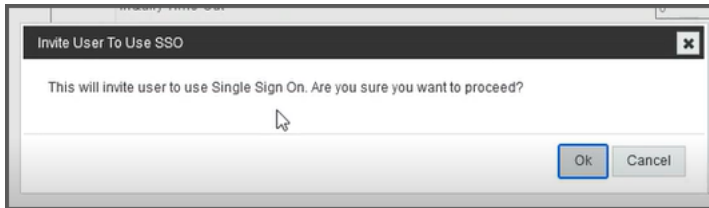
Admin Steps – Inviting Users to Join SSO

Note: Prior to sending invites, an organization must be configured and registered to use SSO.

1. To invite a user to use SSO, open InCommand and go to Client Maintenance> Maintenance> Users (Add/Edit).
2. In the 'Users' section, select the user you want to invite.
3. Expand the + **Password and Security** section.
4. Click the 'invite user to use SSO' button.

The screenshot shows the InCommand interface for user management. On the left, a list of users is displayed, with 'Jones, Bella - bjones' selected and highlighted in blue. An arrow points from the text 'Select the user to be invited' to this user. On the right, the 'Password and Security Options' section is expanded, and the 'invite user to use SSO' button is highlighted with a red box. An arrow points from the text 'Then click the "invite" button' to this button.

5. A message will pop up. Click **Ok** to confirm that you want to invite this user.



A confirmation appears.



An email will be sent to the verified email address listed in the Client Maintenance > User > User Information section. This must be the email assigned to the user by the organization. It cannot be a personal email.

	<input type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday
User E-Mail	<input type="text" value="bjones@DeliverHealth.com"/> <input type="button" value="verify"/>
User Active	<input checked="" type="checkbox"/>
National Provider Identifier	<input type="text"/>

Additional Notes

An invite will 'expire' after 3 days. At that time, the invite can be re-sent.

If you want to revoke an invite (before it is accepted) or check on the status of an invite, you must contact eScript One.

You will receive an error if:

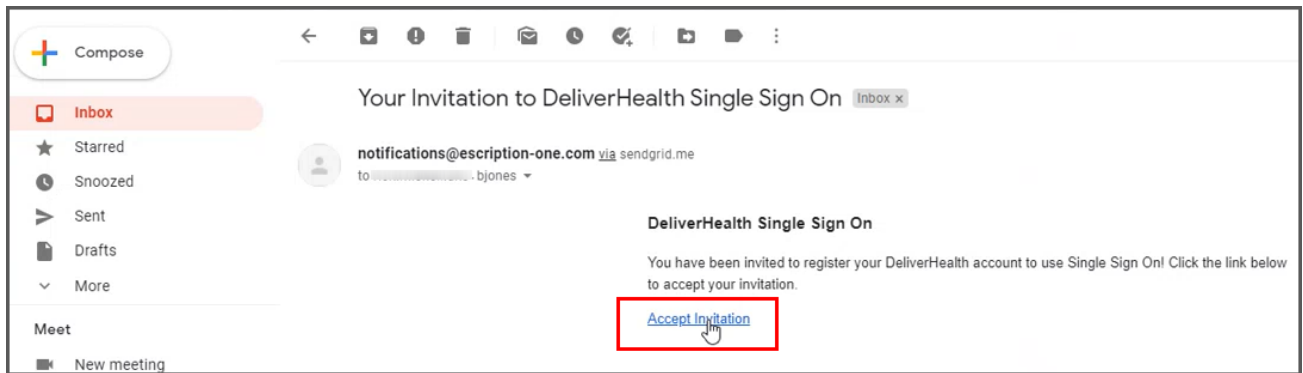
- you send the invite more than once
- there is no email in the 'User E-Mail' field
- the invite has already been sent and accepted

User Steps - Logging in with SSO

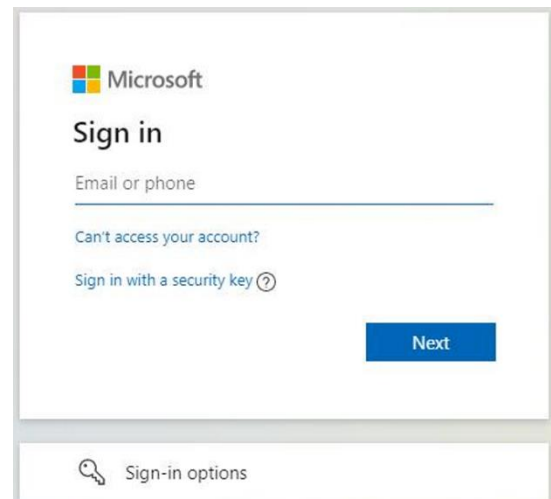
As a user, you will receive an email stating that you have been invited to join Single Sign-on. The email will contain a link.

Accepting the SSO Invitation

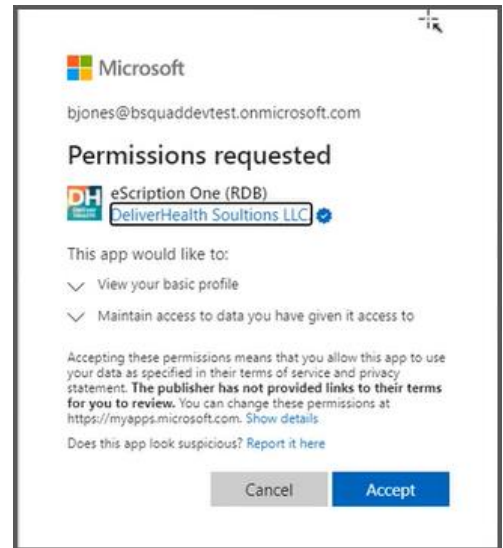
1. Click the **Accept Invitation** link in the email, which will link your organization's account to eScripton One.



2. The Microsoft Login page appears next. Enter the login credentials you use to log into your organization.



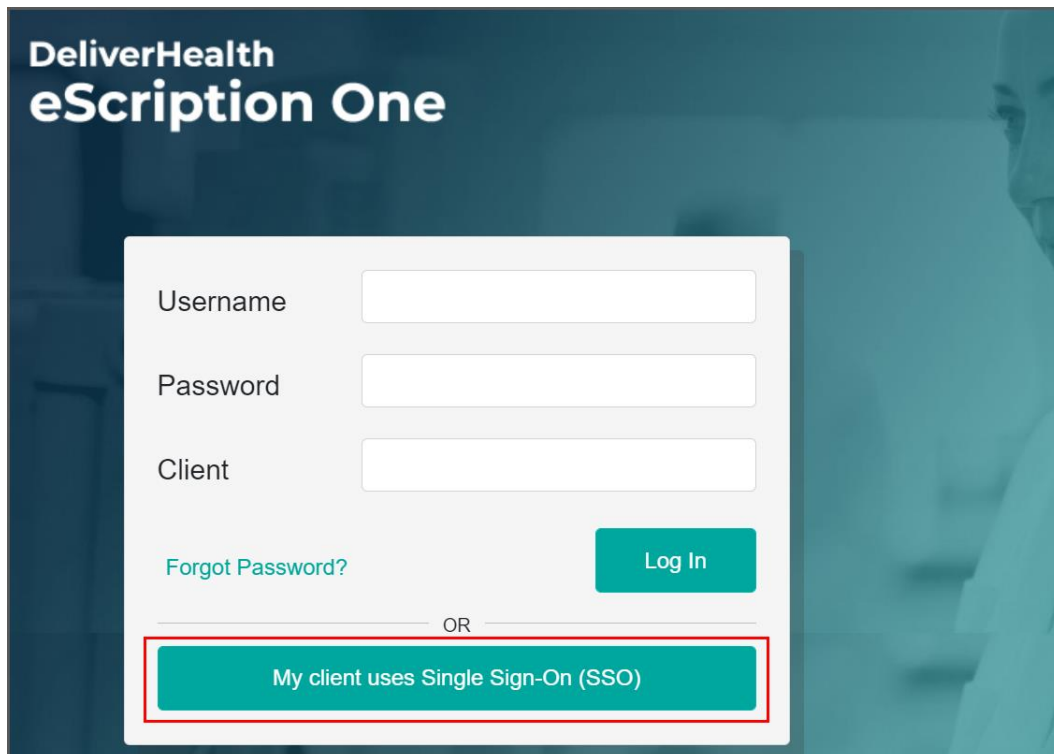
3. During the login process, you may be asked for your consent. Press **Accept** to continue logging in. This is a one-time consent and appears the first time using SSO.
4. After clicking Accept, you will receive a message stating: 'Your invite has been successfully accepted!'



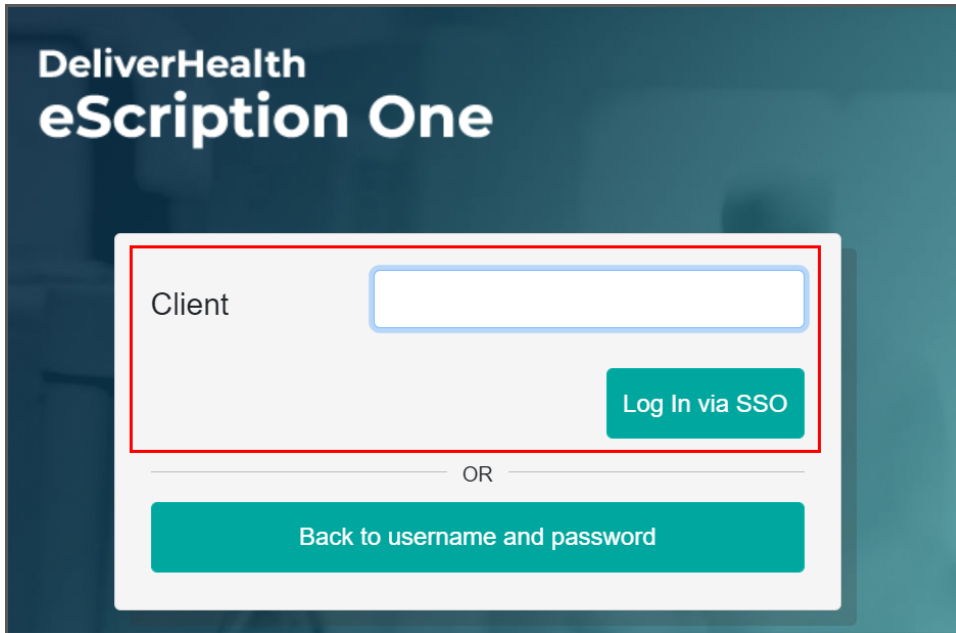
Logging in with SSO

To log in after accepting an SSO invite, open your eSOne app as usual. On the login screen, a new option appears for SSO users.

1. Select the option called '**My client uses single sign-on (SSO)**' or '**My company uses single sign-on (SSO)**'.



2. On the next screen, enter your Client or Company name and then select **Log In via SSO**.



DeliverHealth
eScripton One

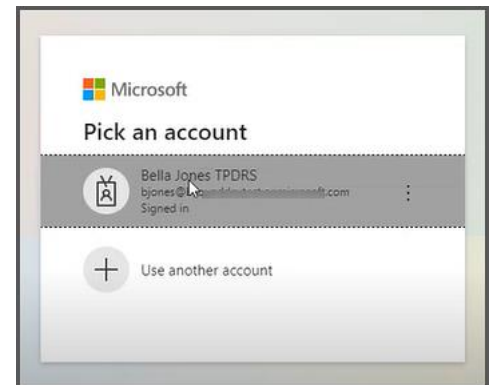
Client

Log In via SSO

OR

Back to username and password

3. Select your name on the Microsoft login page to be logged in.



Support

Get assistance for SSO, and all other eScripton One applications, here:

- Phone Support: 1-800-858-0080
- Support Email: esone.support@DeliverHealth.com