## LISTSERV Maestro Admin Tech Doc 22

# SAML Single Sign-On

August 21, 2024 | 
**lsoft.com**

This document is a LISTSERV Maestro Admin Tech Doc. Each admin tech doc documents a certain facet of the LISTERV Maestro administration on a technical level. This document is number 22 of the collection of admin tech docs and explains the topic “SAML Single Sign-On”.

Last updated for LISTSERV Maestro 11.1-1 on August 21, 2024. The information in this document also applies to later LISTSERV Maestro versions, unless a newer version of the document supersedes it.



All of L-Soft's manuals are also available at: **http://www.lsoft.com/manuals.html**

L-Soft invites comment on its manuals. Please feel free to send your comments by e-mail to: MANUALS@LSOFT.COM

# Table of Contents

# 1 Introduction

SAML is a standard to exchange authentication information between parties, usually in the context of the world wide web and to implement single sign-on. In addition to the users themselves, there are two other main players in a SAML setup:

The **Service Provider (SP)** is the entity that provides a (web based) service to the user. In our scenario, LISTSERV Maestro is such a service provider. It provides its various email and subscriber related services.

The **Identity Provider (IdP)** is the entity that verifies the identity of the user (e.g. via a password check, possibly supported with an additional 2-factor authentication [2FA]), and which transfers an assertion about the identity to the service provider, so that the SP knows to trust the user and allow him access to its services.

There are usually several SPs using the same IdP, thus creating a **Single Sign-On (SSO)** framework, often also with Single Log-Out (SLO).

For the user, such a single sign-on setup has two main benefits:

- The user does not have to maintain login credentials at every single SP. Instead, he only has to maintain his login credentials at the IdP, in one place.
- If the user accesses one of the SPs, and the user is already logged in at the IdP (for example because he already logged in earlier, possibly while accessing one of the other SPs), then he can immediately start using the SP's services, without even having to enter his login credentials.

# 2 Configure SAML Single Sign-On in LISTSERV Maestro

## *2.1 Identity Provider Preconditions*

To be usable as an IdP for SAML SSO with LISTSERV Maestro, the identity provider must meet the following criteria:

- The IdP must support SAML SSO (support for single log-out [SLO] is optional).
- The IdP must have a publicly accessible SAML metadata URL.
- The IdP must specify the user's email address as the "Name ID" attribute (aka. "name identifier", or "Unique User Identifier", or similar) of the returned identity assertion.
- The IdP, in the configuration that applies to Maestro as a SP, must digitally sign messages with a valid server certificate. This requirement is fulfilled by default for many IdP vendors, but some have this disabled by default, so make sure that you enable this during your configuration at the IdP.

## *2.2 Configure the Identity Provider*

If an IdP meets the preconditions described above, then you can configure it for SAML SSO in LISTSERV Maestro as follows.

(Note, that the parts of the description related to the IdP must be relatively vague, as they differ between IdPs.)

### 2.2.1 Prepare the IdP

In the IdP, it is usually necessary to create a new “SSO Application” (or “Enterprise application”, or “Cloud application”, or similar). This is referred to as the “SSO app” in the following.

As a first step, go into the IdP and create such an SSO app for LISTSERV Maestro as the SP.

At this early stage, you will likely not be able to finish the creation of the SSO app, as there is some data related to the LISTSERV Maestro SP that you do not have at this time. This is, however, OK. You only need to proceed far enough into the creation of the SSO app to get access to the IdP’s SAML metadata URL (possibly also called SSO metadata URL, federation metadata URL, or similar).

Take note of this metadata URL, as you will need it in the next step.

### 2.2.2 Register the IdP in LISTSERV Maestro

To register the IdP in LISTSERV Maestro, log into the HUB as an administrator and select **SAML Identity Providers** from the menu. Then click on **New Identity Provider**.

On the next screen, enter the following values:

**Identity Provider Settings**

These settings define the IdP in LISTSERV Maestro.

- **Display Name:** Specify a name that later allows you to recognize this IdP in the list of available IdPs.
- **Metadata URL:** Supply the metadata URL of the IdP. This is the metadata URL from the SSO app configuration as described in the previous sub-section. Copy & paste it from the SSO app configuration into the field here in the HUB. LISTSERV Maestro will access this URL and read the metadata from it.
- **Single Log Out:** Configure if Maestro as Service Provider shall also initiate SLO when a user logs out from Maestro.

**LISTSERV Maestro as Service Provider (SP), when using the above IdP**

*Contact Details for SP Metadata*

As a SAML SP, LISTSERV Maestro creates its own SAML metadata which must be supplied to the IdP to establish the trust relationship between IdP and SP. Most of this metadata is technical in nature and automatically generated by Maestro, but the contact information for the SP must be supplied here.

- **Organization:** Specify the name of your organization (as the entity that runs LISTSERV Maestro) that shall be included in the SP metadata. E.g. your company name.
- **Email Address:** Specify a contact email address that shall be included in the SP metadata. E.g. for a technical contact.

*Details for SP Certificate*

To establish a trusted communication between the IdP and the SP, the SAML protocol uses digital signatures with digital certificates. The necessary certificate for this is automatically created by LISTSERV Maestro, based on the details you supply here.

- **Common Name:** Specify the common name of the certificate. E.g. "SAML Certificate".

- **Organizational Unit:** Specify the organizational unit in your organization that is responsible for LISTSERV Maestro. E.g. "IT" or "Operations".
- **Organization:** Specify your organization. E.g. your company name.
- **Two-Letter Country Code:** Specify the two-letter country code as per ISO3166-1 of the country where your organization is located. E.g. US or SV.

When finished with the input, click **[OK]** to save the settings. You are now returned to the overview list of all identity providers that are currently defined in LISTSERV Maestro, with the newly defined IdP shown in the list.

As explained above, for each IdP, LISTSERV Maestro creates a dedicated metadata URL corresponding to its role as the SP for this IdP. This **SAML SP Metadata URL** is shown together with the IdP entry in the list, as a clickable link. Click on the URL to download the metadata as an XML file. You will need it in the next step.

### 2.2.3 Finish Setup at the IdP

Now go back to the SSO app configuration at the IdP that you started, but didn't complete, in the "Prepare the IdP" step above.

This configuration is still missing the details about LISTSERV Maestro as the SP. The quickest way to configure all these details is to upload them in form of the SAML SP metadata file that you downloaded in the previous step.

Somewhere in the SSO app configuration at the IdP there should be an "Upload metadata file" button, or a link, or similar. Look for this feature and use it to upload the XML file that you downloaded in the previous step. Make sure to save the changes that are applied by this upload.

SAML usage is now configured both on the IdP and on the SP end, except for the configuration of the actual user accounts. This is explained in the following sub-sections.

**Tip:** When configuring the SSO app, many IdPs allow you to upload an image as the logo for this SSO app, which is then for example shown to users on their dashboard at the IdP. If you need a LISTSERV Maestro logo for this purpose, you can download this one:

https://maestro.lsoft.com/lui/images/maestroLogoForSAML.png

(This is a relatively large image with transparent background, in PNG format. You may have to resize it and/or add a non-transparent background and/or change the file format, depending on your IdP's requirements.)

## *2.3 Configure Users for SAML SSO*

For a user to be able to login to LISTSERV Maestro via SAML SSO, the user account must be configured correctly both in the IdP and in LISTSERV Maestro.

### 2.3.1 Configure IdP Accounts for SAML SSO

After a new SSO app has been created, most IdPs will not automatically grant all known IdP user accounts access to this new app. Instead, you will usually have to add the accounts (from the pool of accounts known to your IdP) that you want to be able to login to the new app.

For this, the IdP has, in some way or the other, a feature to associate the allowed IdP accounts with the SSO app. You now need to use this feature with all IdP accounts that you want to be able to log in to LISTSERV Maestro.

### 2.3.2 Configure LISTSERV Maestro Accounts for SAML SSO

In LISTSERV Maestro, you need to configure which accounts are supposed to use SAML SSO in the first place (and if so, via which IdP), and how LISTSERV Maestro shall map from the IdP account to its own internal accounts. This is described in the following.

#### *2.3.2.1 Set "SAML SSO" as the Authentication Method*

SAML SSO as the authentication method can be configured on different levels in LISTSERV Maestro:

- **SAML SSO for the whole LISTSERV Maestro server**

  To configure SAML SSO for the whole LISTSERV Maestro server, configure SAML SSO authentication on the application default level:

  In the HUB menu, go to **LUI Settings → Application Default Settings → User Authentication**. Then set the **Default User Authentication** to **Authenticate Through SAML SSO**. Then select the desired **Identity Provider** from the available drop-down list. Finally, click **[Save]**.

  **Important:** If configured on the default application level like this, SAML SSO with the selected IdP is active for **all** accounts on the whole LISTSERV Maestro server, including administrator accounts (except for the default "admin" account, to which this never applies). It is not possible for individual accounts to override this setting to use a different IdP or a different authentication method.

- **SAML SSO for a specific group**

  Unless SAML SSO is already configured on the whole server (see above), you can instead configure it for only a specific user group:

  In the menu, go to **Accounts and Identities**, then in the list of user accounts, select the desired group. Then in the menu, go to **Group Settings → User Authentication**. Then set the first drop-down list to **Use custom settings** and the second to **Authenticate Through SAML SSO**. Then select the desired **Identity Provider** from the available drop-down list. Finally, click **[Save]**.

  **Important:** If configured on group level like this, SAML SSO with the selected IdP is active for **all** accounts this group. It is not possible for an individual group member to override this setting to use a different IdP or a different authentication method. It can only be configured for the whole group. And of course this is only possible if SAML SSO is not already configured for the whole server.

- **SAML SSO for a specific non-group user**

  Unless SAML SSO is already configured on the whole server (see above), you can instead configure it for only a specific single user account (i.e. an account that is not member of a group):

  In the menu, go to **Accounts and Identities**, then in the list of user accounts, select the desired user account. Then in the menu, go to **Account Settings → User Authentication**. Then set the first drop-down list to **Use custom settings** and the second to **Authenticate Through SAML SSO**. Then select the desired **Identity Provider** from the available drop-down list. Finally, click **[Save]**.

  **Important:** Only accounts that do not belong to a group at all can be configured in this way. Accounts that belong to a group cannot have SAML SSO configured individually. For them, it can only be configured for the whole group (see above). And of course this is only possible if SAML SSO is not already configured for the whole server.

#### *2.3.2.2 Map IdP Accounts to LISTSERV Maestro Accounts*

After the user has logged in at the IdP, the IdP sends a so called SAML identity assertion to LISTSERV Maestro. With this assertion, the IdP tells LISTSERV Maestro, that someone with this IdP account is currently logged in for this browser session and that LISTSERV Maestro can go ahead and grant the user access to its services.

But to be able to do so, LISTSERV Maestro must know which internal LISTSERV Maestro account corresponds with this logged in IdP account, so that it can grant access to the correct internal account.

This is determined by looking up the email address from the IdP account, as provided by the IdP in the assertion data. LISTSERV Maestro looks for an internal account that is configured to use the given IdP (see sub-section above) and that has the same email address from the identity assertion configured as its account address.

**Example:** If the IdP "Sample Provider" sends an identity assertion that says that the user with the email address "joe@example.com" is logged in, then LISTSERV Maestro will look for an internal account where the account address is also "joe@example.com", where the account must be configured to "Authenticate Through SAML SSO", with "Sample Provider" as the IdP.

Therefore, for any IdP account that you grant access to the LISTSERV Maestro SSO app in the IdP (see previous sub-section), you must make sure that there exists a LISTSERV Maestro account that has the same email address (as the account address) and that is configured to use this IdP for SAML SSO (as described in the previous sub-section).

**Note:** It is possible, and may even be desired, that multiple internal LISTSERV Maestro accounts have the same account address assigned and use the same IdP. See section 5 for more details.

# 3 Log In with Single Sign-On (SSO)

So, how does it work for the user if SAML SSO is enabled?

This depends a bit on if SAML SSO is configured for the whole server or only for some groups or accounts.

- **SAML SSO for the whole LISTSERV Maestro server**

  If SAML SSO is configured for the whole LISTSERV Maestro server, then the access URL for the LISTSERV Maestro login is the same as before, something like this:

  ```
  https://maestro.example.com/lui
  ```

  Only that when a user goes to this URL, he does not see the normal LISTSERV Maestro login page. Instead, if the user is already logged in at the IdP, he does not see a login page at all but is seamlessly sent into the LISTSERV Maestro user interface. If he is not already logged in, then he sees the IdP's login page and is sent into the LISTSERV Maestro user interface after the login.

- **SAML SSO only for some groups or accounts**

  If SAML SSO is configured only for some groups or accounts, then the default access URL for the login (as shown above) works only for the *other* accounts, i.e., those that do *not* have SAML SSO configured. For these accounts, the default access URL shows the normal LISTSERV Maestro login page, from where they can login normally, without SAML SSO.

The groups and accounts that *have* SAML SSO configured must now use a different login URL, that looks something like this:

```
https://maestro.example.com/lui/login/idp/IDP_ID
```

where `IDP_ID` is a unique ID that identifies the IdP that the group (or account) is configured to use.

For any given group or account, you can find this IDP-specific login URL by looking up the group or account settings in the HUB: Go to **Accounts and Identities**, then in the list of user accounts, select the desired group or user account. Then on the overview page, look for the **Generic Login URL**.

When the user goes to this URL, then if the user is already logged in at the corresponding IdP, he does not see a login page at all but is seamlessly sent into the LISTSERV Maestro user interface. If he is not already logged in, then he sees the IdP's login page and is sent into the LISTSERV Maestro user interface after the login.

# 4 Log Out with Single Log-Out (SLO)

Some IdPs also support single log-out (SLO). LISTSERV Maestro automatically detects if this is the case for the given IdP and behaves accordingly:

- **SLO not supported**

  If the IdP does not support SLO, then if you log out of a LISTSERV Maestro session, then you are only logged out of this one session where you selected to log out. You are not logged out of any other LISTSERV Maestro sessions (if you have any open) and are also not logged out of any other service providers (SPs) that are connected to the same IdP.

- **SLO supported and enabled in the IdP settings**

  If the IdP supports SLO and you have enabled SLO in the settings, and if you log out of a LISTSERV Maestro session, then this also logs you out of all other LISTSERV Maestro sessions that you have opened for the same IdP account, and you are logged out of the sessions of any other service providers (SPs) that are connected to the same IdP (and that support SLO), and you are also logged out of the related IdP session itself.

  This means, that if you later want to access LISTSERV Maestro or any of the other connected SPs again, you will have to do a proper login at the IdP first.

  This can be desired, for example when you are wrapping up your work for the day and want to quickly logout everywhere.

  In other cases, where you only want to stop working with the current LISTSERV Maestro session but want to stay logged in in general at the IdP (and in other SPs), it may not be desired. In such situations, the recommended method is to not use the "Logout" option in LISTSERV Maestro, but simply close the LISTSERV Maestro browser window.

  **Note:** If a LISTSERV Maestro session simply expires because of inactivity, then only the expired session is affected. This does not trigger an SLO at the IdP, i.e. all other sessions that are currently active via the IdP remain active.

# 5 Multiple Accounts Mapped to Same Identity

It is possible, and sometimes desired, that multiple internal LISTSERV Maestro accounts use the same IdP and are also configured with the same account address.

This means that the IdP account with this email address maps to all these internal accounts at once.

For the user this means that when he accesses the login URL, then after the login at the IdP, he is presented with a **Select User Account** page. This page lists all LISTSERV Maestro accounts that are mapped to the IdP account. The user can now select the account he wants to start working with. At any later time, he can then switch to any of the other accounts (and back, as often as he wants) via the **Switch Account** entry in the user menu.

If this **Select User Account** page is not desired right after the login, then the initial account can also be preselected by specifying it in the access URL. If you want this, then you should not use the generic access URL for LISTSERV Maestro (as described in section 3), but instead you should use the user specific login URL. The format of this URL is like this:

```
https://maestro.example.com/lui/login/u/USERNAME

https://maestro.example.com/lui/login/u/USERNAME/GROUPNAME
```

where the first is for users that are not members of a group, while the second is for users in a group, where you replace `USERNAME` and `GROUPNAME` accordingly.

If you use this user specific login URL, then after login at the IdP you immediately see the LISTSERV Maestro user interface with the internal account active that was specified in the URL, without first being presented with the **Select User Account** page. You can however still switch to any of the other mapped accounts with the **Switch Account** entry in the user menu.

For most user and group names, it should be simple to build this user specific login URL yourself.

But if you are in doubt about the correct URL for a given LISTSERV Maestro account, you can easily find it, like this:

- **As an administrator, in the HUB:**

  Go to **Accounts and Identities**, then in the list of user accounts, select the desired user account. Then on the overview page, look for the **User Login URL**.

- **As a normal user, in LUI:**

  Go to **User Menu** → **Preferences** → **User Interface**. Your **Individual Login URL** is shown near the top of this page.

- **As a normal user, without logging in:**

  Access the following URL:

  ```
  https://maestro.example.com/lui/login
  ```

  (only of course with your proper host name instead)

  This will always show the standard LISTSERV Maestro login page. Now fill in your username (and group, if applicable) but leave the password field empty, and click **[Log In]**. The next page will tell you the user specific login URL for the specified account (but only if the account has SAML SSO enabled).

Note: Building the user specific login URL from the user and group name as described above only works for user and group names that do not contain the slash character "`/`". If any of the two names contains this character, then the user specific login URL is instead built with an internal user code. If

this applies to your user account, then you will likely not be able to build the URL yourself, as you do not know this internal code. You will instead have to use one of the methods described above to find out the correct user specific login URL.

# 6 Troubleshooting

## 6.1 HUB Login as an Administrator

Direct HUB login (via the HUB login URL) is not possible with administrator accounts that are configured for SAML SSO.

What does this mean?

In normal situations, an administrator logs in to LISTSERV Maestro with the same LUI access URL as normal users. This gives access both to LUI and HUB, and the administrator can freely switch between the two. This normal login works fine for administrators that have SAML SSO configured.

If LUI is however currently not running, but the HUB is running, and the administrator needs to login to the HUB (possibly to fix the problem that stops LUI from starting, for example a problem with the system database), then the administrator cannot use the normal LUI access URL, but must use the direct HUB access URL instead, like this:

```
https://maestro.example.com/hub
```

This login via the direct HUB access URL however does not work for administrators that use SAML SSO. Consequently, this means that you cannot use such an administrator account if you need to troubleshoot a problem in the HUB while LUI is not running. You must use a different administrator account that uses an authentication method other than SAML SSO.

At any time, at least the default “admin” account is such an administrator account, as it always uses the “internal passwords” method for authentication, even if SAML SSO is configured for server wide use. You should therefore take care to always have the password for this default “admin” account handy for such emergencies (and it goes without saying that this password must be a very secure password).

## 6.2 Login Error: “Authentication Data Invalid”

This error is shown if the IdP does not return the user’s email address as the so called “Name ID” attribute in the SAML identity assertion (or claim). If you get this error after logging in via the IdP, then you need to change the IdP configuration to make sure that the email address is properly returned as the “Name ID” attribute (aka. “name identifier”, or “Unique User Identifier”, or similar).

## 6.3 Debugging SAML Messages

If necessary, you can tell LISTSERV Maestro to log out the SAML XML messages that are sent to and returned from the IdP during SSO and SLO. You do this by adding the following line to the `lui.ini` file:

```
SamlDebugLogging=true
```

Then restart LISTSERV Maestro.

While this line is active in the `lui.ini`, LISTSERV Maestro will log the SAML XML data to its log file, prefixed with the text “`SAML DEBUG:`”, for easy recognition.

**Note:** As this may expose sensitive user data in the log file, it is not recommended to have this debug option active during normal production. It should only be used for troubleshooting.