Multiple Application Platform Server

MAPS 6.3 Release Guide

Product version 6.3

Last updated 8/29/2019

Trademark, Publishing Statement, and Copyright Notice

Table of Contents

What's New in MAPS 6.3?

Evisions is pleased to announce the release of MAPS version 6.3, which includes the following changes:

Enhancements:

- Improved single sign-on support including adding support for SAML 2.0 authentication.
- Added support for MAPS group membership within CAS.
- Added support for Windows Server 2019.
- Additional enhancements and resolved issues.

We appreciate the feedback received from all of our users. Our products would not be what they are today without your continued support. If you have any comments or suggestions, please do not hesitate to open a HelpDesk ticket and let us know.

MAPS Updates

MAPS 6.3 is an update to the MAPS service (which includes the eLauncher) and the MAPS Config. You should upgrade both components concurrently.

Product versions

The latest versions of MAPS included in this release are:

- MAPS service 6.3.0.2152 / MAPS Config 6.3.0.1151 / eLauncher 6.3.0.33

Installation

1. Prepare test environment and ensure current backup

We highly recommend installing updates in a test environment before applying them to your production environment. You should make sure that a current backup is available in case of any unforeseen issues. To create a full backup of your MAPS environment, go to the **Server** -> **Backups** screen in MAPS and click **Backup Now**.

2. Check for updates

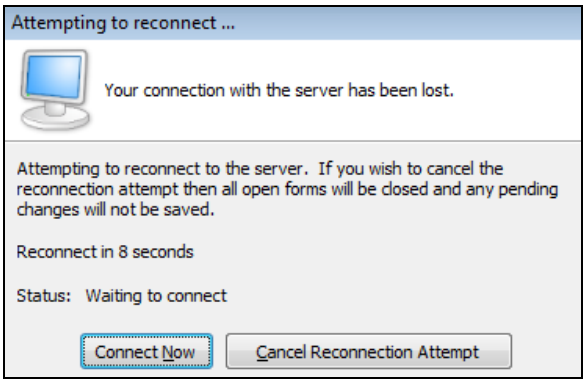
Click the **Check for Updates** button in the MAPS Configuration tool to view available updates.

> If you need to apply earlier updates prior to the 6.3 update, please refer to the appropriate release guide(s) before proceeding.

It is possible to apply updates when users are on the system; however, to avoid the possibility of losing unsaved work we recommend applying updates during off hours.

3. Allow update process to complete

When applying updates to the MAPS service you will be temporarily disconnected from the server:



The update process may take a few minutes to complete. **Do NOT cancel the reconnection attempt or manually restart the server.** You will automatically be reconnected to the server once the update has been applied.

4. Verify the latest version is installed

To ensure that you are on the most current version, continue clicking the **Check for Updates** button and applying the updates until no new updates are available.

Please Provide Us with Your Feedback!

As always, we welcome any feedback or suggestions you may have. We very much appreciate your thoughts and suggestions, so please keep the great ideas coming!

New Single Sign-on Features

Single sign-on (SSO) allows you to configure MAPS to use a common authentication server. There are two authentication methods supported: CAS authentication, and SAML 2.0 authentication. Single sign-on authentication can be used for eLauncher, Argos, and FormFusion. For security reasons, users are always prompted to log in when accessing IntelleCheck or MAPS Config.

There are two ways for users to login when SSO is used:

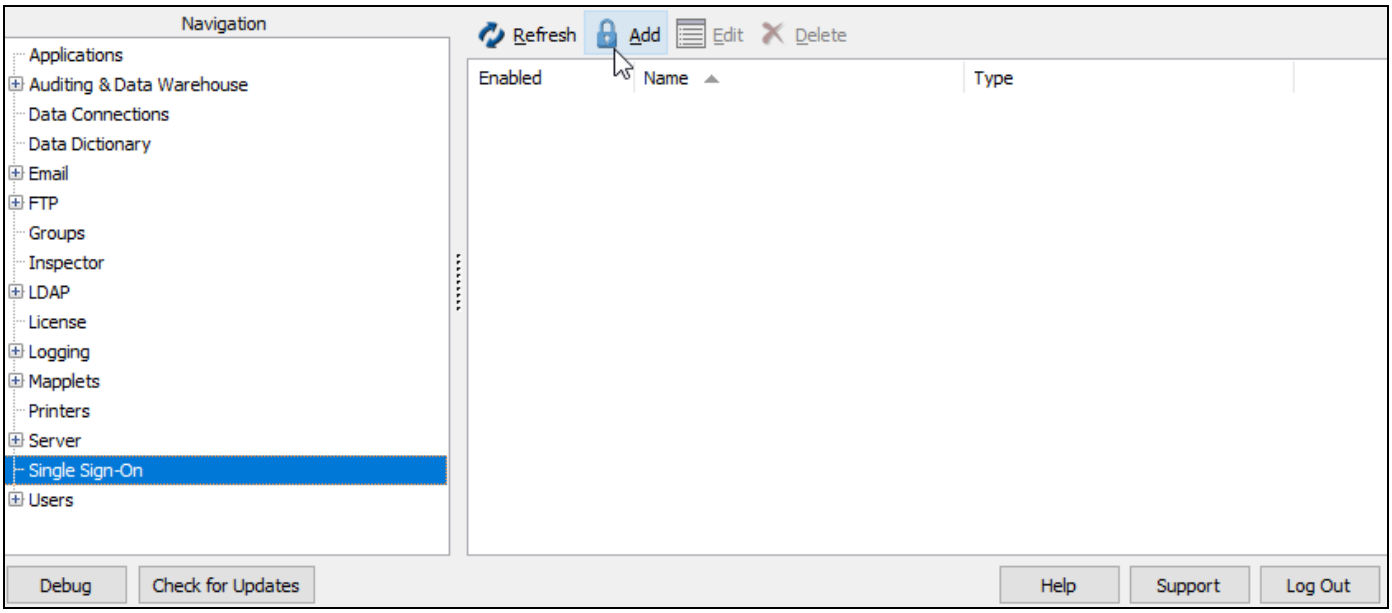
- Users log in once to a central portal and then click a link to access the MAPS eLauncher.
- With a SAML server, users may also access the eLauncher from a browser, select the Single Sign-On button from the login dialog, and then enter credentials on a central SSO login page for authentication.

The single sign-on server handles the authentication, and provides a secure login to the MAPS launch page. If you already use single sign-on for other web pages, this can save time when accessing the products because users do not need to log in a second time.

Adding a CAS or SAML Server

Select Single Sign-On from the Navigation pane. If one or more single sign-on servers have been added already, they will be listed here.

Click **Add** to display the Edit Single Sign-On Server configuration dialog.



Select the server type (**SAML** or **CAS**) from the Type menu.

The configuration dialog updates to show the configuration options for the type of server selected.

Maximum Number of CAS or SAML Servers

MAPS allows you to configure any number of CAS and SAML servers, but you can have only one CAS and one SAML server enabled at a time. If multiple CAS servers are enabled, MAPS will use the first enabled CAS server in the list. If multiple SAML servers are enabled, MAPS will use the first enabled SAML server in the list. To disable a configured server, un-check the **Enabled** box for the server on that server's configuration dialog.

SAML Servers

SAML stands for Security Assertion Markup Language, and is a single sign-on protocol. It is a standard method used to exchange authentication and authorization data between parties. SAML authentication allows your institution to provide SSO capability through your SAML Identity Provider (IdP). MAPS is added to the SAML IdP server as a service provider (SP).

SAML 2.0 can simplify access to applications for your users and eliminate the need to administer unique passwords and duplicate credentials for MAPS. Using SAML authentication with MAPS provides a unified user experience across the applications at your institution.

The SAML authentication feature for MAPS allows your users to authenticate to MAPS using the credentials from your SAML Identity Provider (IdP) server, which is also known simply as the IdP. During configuration, the SAML IdP server and the MAPS server (the service provider) exchange metadata files. These metadata files allow the SAML IdP to authenticate users who are members of the groups permitted to use the MAPS services.

Once the SAML authentication feature is installed and configured, users select a **Use Single Sign-On** button on the login dialog for the eLauncher. Users are redirected to your institution's SSO login page where they enter their credentials. When users are authenticated by the SAML server, they are granted access as usual.

SAML Server Configuration and Set Up

Prerequisites

- Your IdP server must support the SAML 2.0 protocol.
- You must be running MAPS version 6.3 or later.
- MAPS must be configured to run HTTPS (secure HTTP).

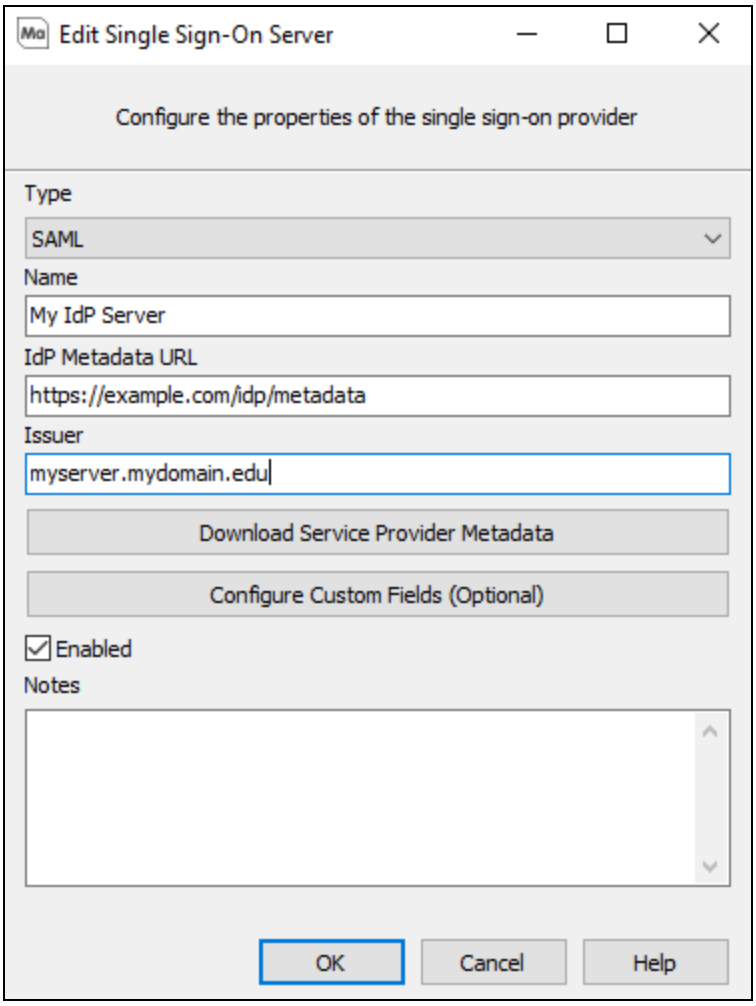
Configure SAML Single Sign-On Options

Before you can configure SAML authentication, gather the following information for your facility:

Option	Description	Examples
IdP Metadata URL	The URL of the metadata file (from the SAML IdP)	*https://example.com/idp/metadata*
Issuer	Domain name of the MAPS server	*internal.myservers.com*

Select **Single Sign-On** from the configuration menu to display the list of existing SSO servers.

Select a server from the list, or select **Add Server** to configure a new server. When the Edit Single Sign-On Server dialog box displays, select **SAML** as the server type from the first drop down.



Set the connection parameters as follows:

- **Name:** This is the name of the SSO server in MAPS, and will be used within connection messages and in logs.
- **IdP Metadata URL:** The location of the SAML IdP metadata file. You should be able to display the metadata file in your browser using this URL.
- **Issuer:** The domain name of MAPS. This domain must be accessible from the SAML IdP server. Otherwise, you need to use the fully qualified domain so that MAPS is accessible.
- **Enabled:** Use this check box to enable or disable use of the SAML IdP server. While you can configure multiple SAML IdP servers, you can have only one enabled at a time. When you enable a SAML IdP server, be sure to disable the others (un-check the Enabled box).
- **Notes:** Use this space to record any additional information.

Generate and Upload MAPS Metadata to the SAML IdP Server

1. Select the **Download Service Provider Metadata** button. This prepares the download of the MAPS metadata file so that it can be used by the SAML IdP server.
2. Name the file so that you can identify that it is associated with MAPS. (Use the MAPS server host name, for example.)
3. Save the file to a location where you can access it when you are ready to upload it to your SAML IdP server.
4. Upload the metadata file to the server. Refer to the documentation for your SAML IdP server for specific instructions.

Configure Users and Groups

When a user enters their username and password on the SAML login page, the SAML IdP server will return an assertion to MAPS if the user is validated. The response that the SAML IdP server sends to MAPS includes attributes that identify each LDAP and/or MAPS group that the user belongs to (within the IdP).

MAPS parses the assertion and examines each attribute with the value of `memberOf` for either the FriendlyName or Name.

If you are using LDAP groups, and the assertion provides the attributes in the format of a distinguished name (DN), MAPS parses each DN to determine if any LDAP groups in MAPS have a matching DN. If the LDAP group does include a matching DN, the user is granted the roles and permissions associated with that group. When there are multiple matching groups, the permissions associated with the roles in those groups accumulate.

If you only have MAPS groups, you must match the DN to a MAPS group. MAPS examines the assertion to see if the entire DN matches the name of a MAPS group. When the DN in the assertion returned for a user matches the name of the group defined in MAPS, the user is granted the roles and permissions associated with that group. When there are multiple matching groups, the permissions associated with the roles in those groups accumulate.

There may be additional attributes included in the assertion that MAPS can use as a custom field. These are explained in "Configuring Custom Fields" on the next page.

For more information on configuring groups to work with SAML authentications, see Using Groups with Single Sign-On, in the help.

Note: SAML authentication is not supported for users who are members of nested LDAP groups.

Troubleshooting Tip: You can look at the debug log in MAPS while attempting to log in through SAML to verify that the response from the SAML server is in the correct format.

SAML Authentication Example

The example below shows a portion of an assertion that the SAML server returns to MAPS for an authenticated user:

```
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="memberOf" Name="memberOf"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue>
      CN=Report Writer,OU=Groups,DC=Evisions,DC=Example
    </saml2:AttributeValue>
    <saml2:AttributeValue>
      CN=Report Viewer,OU=Groups,DC=Evisions,DC=Example
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

In this example, if you are using LDAP groups, the SAML response tells MAPS that the user is a member of the *Report Writer* LDAP group and the *Report Viewer* LDAP group. MAPS and associated applications grant this user the permissions defined for those two groups.

If you only using MAPS groups, the name of the MAPS group must be named **CN=Report Writer,OU=Groups,DC=Evisions,DC=Example** or **CN=Report Viewer,OU=Groups,DC=Evisions,DC=Example**.

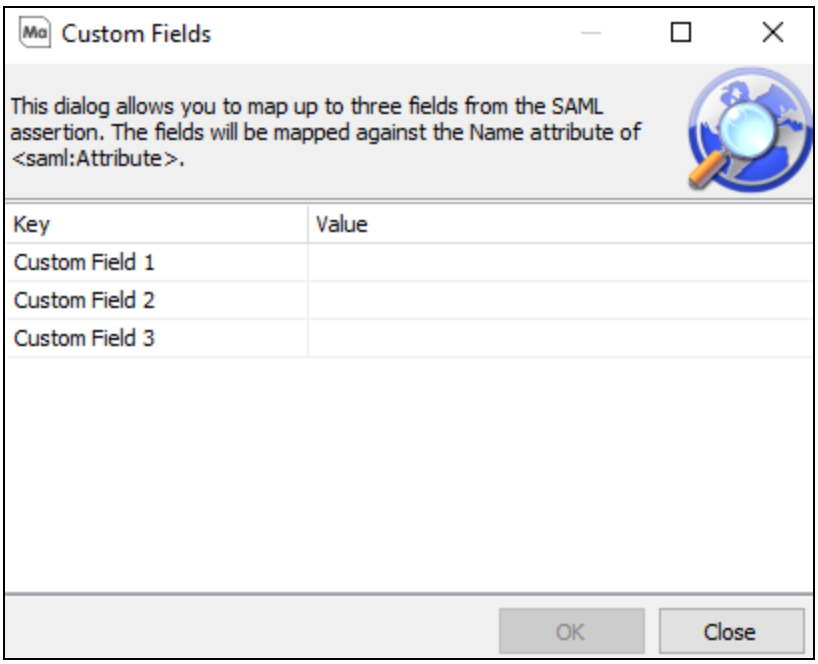
> **Note:** The assertion must include the value of "`memberOf`" for either the **FriendlyName=** or the **Name=** in the attribute statement. You may not be able to control the value for the Name statement that is sent from your server. If that is the case, edit the FriendlyName value so that it is `memberOf` which will allow it to be recognized by MAPS.

Note that the list of groups returned by the SAML server may include groups that are not defined in MAPS, but are used for other applications throughout the enterprise. MAPS ignores these attributes.

Configuring Custom Fields

Custom fields are used to map values from within the assertion sent from the IdP to variable values used by other applications such as Argos or proxy accounts (BANPROXY, for example).

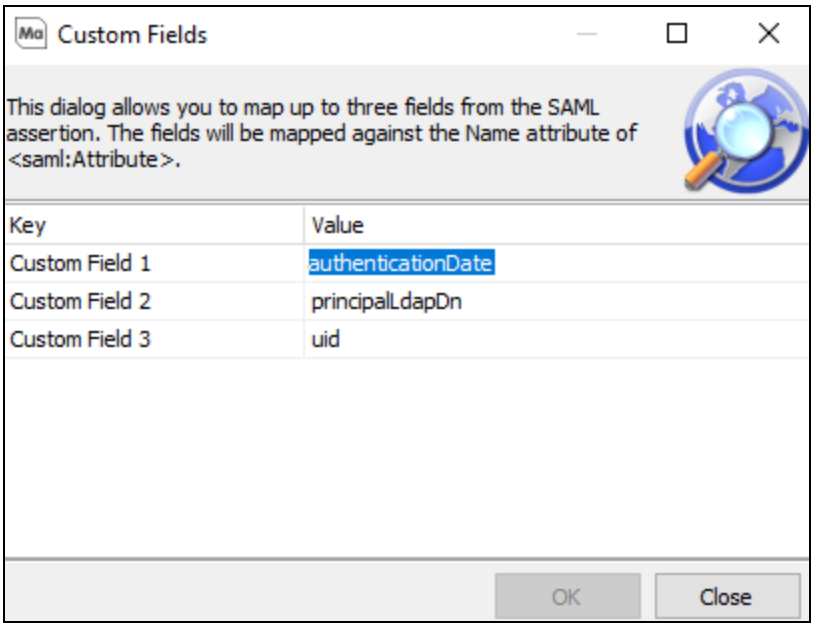
To configure custom fields, select the **Configure Custom Fields** button on the Edit Single Sign-On Server dialog. This displays the Custom Fields dialog:



You can enter up to three values.

MAPS examines the assertion from the SAML server, looking for a FriendlyName or Name attribute that matches the value for one of the Custom Fields. In the following example, MAPS will be looking for FriendlyName or Name field matching the following:

- authenticationDate
- principalLdapDn
- uid



The snippet below is from an assertion returned by the SAML server. In this snippet, the second and third custom field values (*uid* and *principalLdapDn*) are used as values for the FriendlyName of an attribute.

```
<saml2:Attribute
  FriendlyName="uid" Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml2:AttributeValue>
      Dex
   </saml2:AttributeValue>
</saml2:Attribute>

...

<saml2:Attribute
  FriendlyName="principalLdapDn" Name="principalLdapDn"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml2:AttributeValue>
      CN=dex,CN=Users,DC=Test,DC=Local
   </saml2:AttributeValue>
</saml2:Attribute>
```

- The attribute value of `principalLdapDn` (which is `CN=dex,CN=Users,DC=Test,DC=Local`) will be passed as *Custom Field 2*
- The attribute value of `uid` (which is `Dex`) will be passed as *Custom Field 3*

If the assertion does not include an attribute for `authenticationDate`, nothing is returned, and the Custom Field value is ignored.

If there are multiple values for an attribute, then only the first one in the list is set as the value for the custom field.

How Users Log On with SAML Single Sign-on

Once the SAML server and the MAPS server are properly configured and communicating with each other, users who attempt to sign in using the eLauncher see the **Use Single Sign-On** button on the sign in dialog.

When users select this button, they are redirected to the institution's IdP sign in page where they enter their credentials. If the authentication is successful, the users are redirected to the eLauncher and granted access to the MAPs pages and applications that they are authorized to access.

Note that for some sensitive applications, such as IntelleCheck and MAPS Config, users may be prompted to re-enter credentials.


evisions
Username:
Password:
Remember this user
Use Single Sign-On
Sign In

MAPS 6.3 Release Notes

MAPS Service 6.3.0.2152 / MAPS Config 6.3.0.1151 / eLauncher 6.3.0.33

MAPS

Enhancements

Area	Description	Issue number
Authentication	Added support for SAML 2.0 authentication to MAPS.	MAPS-1003
Authentication	Added a button for single sign-on from the eLauncher for institutions who use SAML authentication. Once the SAML server is configured properly, eLauncher users can use the Single Sign-On button to log in to the AWV, Argos, and FormFusion.	MAPS-2216
Authentication	The Argos Web Viewer now supports single sign-on and authentication through SAML servers.	MAPS-2281
Configuration	Added a new Single Sign-on entry in the MAPS Config Navigation pane which is used to configure both CAS and SAML authentication. The previous CAS entry has been removed and functionality replaced by this new Single Sign-On entry.	MAPS-2224
Groups	Added support for MAPS Groups with CAS SSO.	MAPS-2273
Security	Updated the OpenSSL .dll files packaged with MAPS to version 1.0.2r.	MAPS-1923
Security	Updated the OpenSSL .dll files packaged with MAPS Config to version 1.0.2r.	MAPS-2249
Server	Added Windows Server 2019 to the list of supported operating systems.	MAPS-2164
User interface	Updated the title bar to say "MAPS Config" instead of "MAP Server Configuration."	MAPS-2046

Resolved Issues

Area	Description	Issue Number
Clustered installations	The sorting of the boot date time for nodes in a cluster has been corrected.	MAPS-2107
Data connections	An error occurred when MAPS created a string variable of the default type WideString, but the database did not support the WideString variable type. To resolve this, MAPS Config now provides an option in the Data Connections configuration settings for SQL Formats. You can set the default string type to Auto, Narrow, or Wide to accommodate the database requirements.	MAPS-2359
Data dictionary	When an administrator used MAPS Config to delete an Argos-created Field Join, an Access Violation error could occur. The condition has been fixed.	MAPS-1402
Log files	The log creation dates/times shown on the Logging -> Logs screen were showing the GMT time instead of the local time.	MAPS-2166
Log files	The Created Date column for log files is now always displayed by default.	MAPS-2170
Product updater	When checking for updates, the link to the Product Version Matrix was not going to the correct page.	MAPS-2293

Area	Description	Issue Number
Stability	The error "Unable to add auditing records. Microsoft MSXML is not installed" was appearing in the internal logs. The underlying cause of the error has been fixed.	MAPS-1756

Getting Help

For information on using the software, please refer to the in-product Help, which contains detailed information on all aspects of the product.

If you are having problems with the installation or configuration, you can search our support site, which includes a knowledge base of common issues. If you are unable to find the solution, submit a HelpDesk request with a detailed explanation of the problem you are experiencing.

Please do not hesitate to contact the Evisions HelpDesk if any questions or problems arise. We are here to help you and want to ensure your success.

If you find that areas of this documentation could benefit from additional detail or clarification, please let us know. We are constantly trying to improve the installation process to make it as easy as possible.