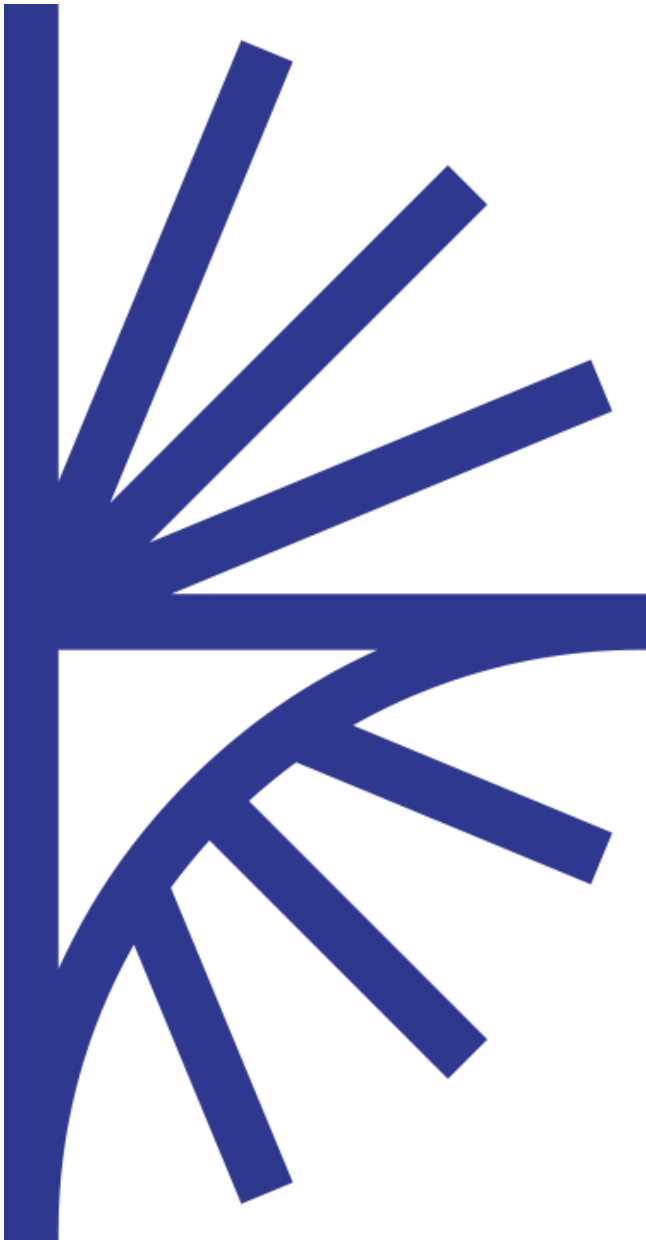


f



FUSION REGISTRY LDAP SETTINGS

FUSION REGISTRY
VERSION 9

LDAP Settings

CONTENTS

1	Overview	3
2	LDAP Configuration	4
2.1	Settings Page	4
2.2	Role Template	5
2.3	Role mapping	5

Version History

Version #	Implemented By	Revision Date	Reason
201909528	Phil Lazarou	28 th May 2019	Initial version
20190927	Phil Lazarou	27 th Sep 2019	Minor typographical fixes

1 Overview

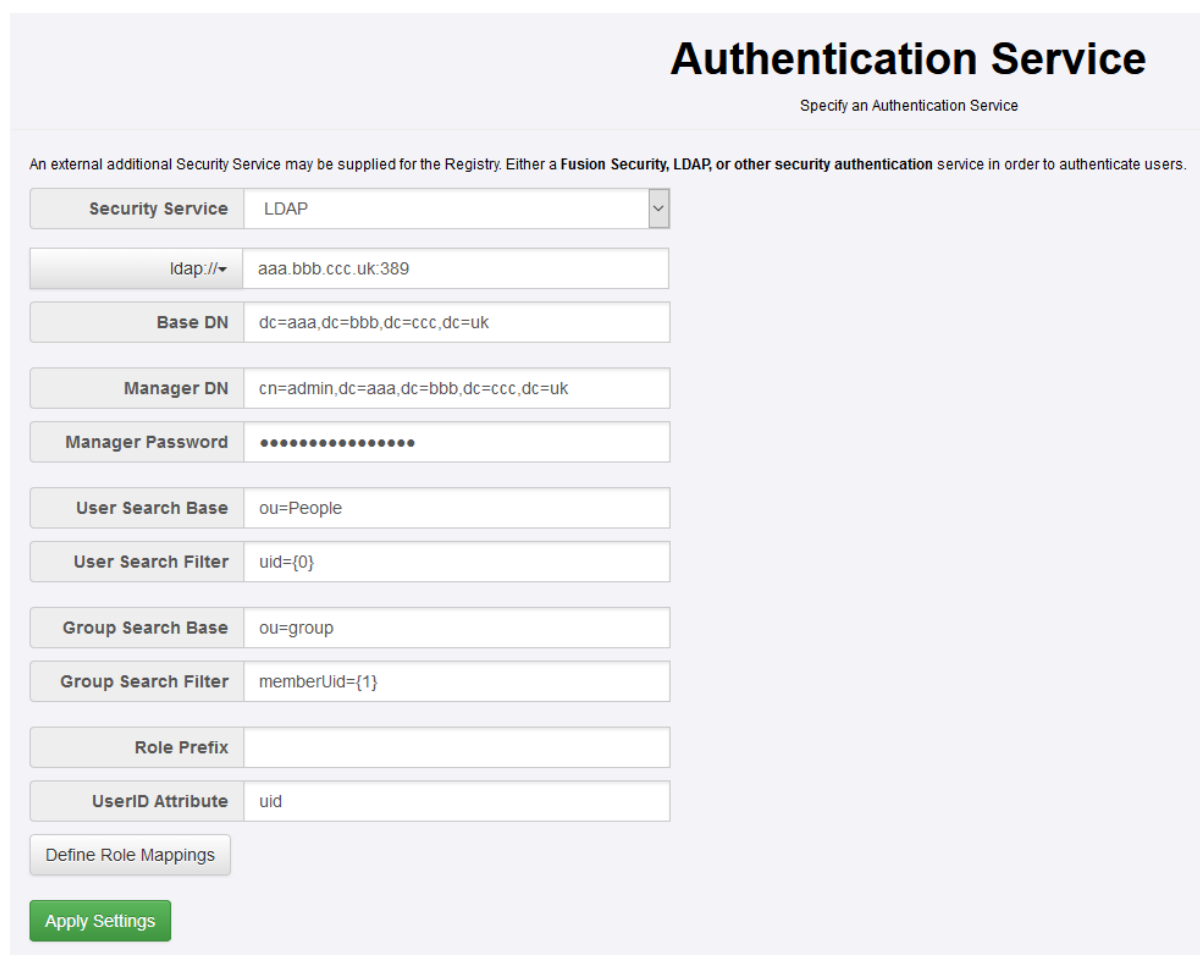
A running LDAP instance, such as Open LDAP may be used as the Authentication and Authorisation provider for Fusion Registry. This requires an LDAP server running on a network that Fusion Registry can communicate to. Fusion Registry can communicate with LDAP either using a Role Template or else a Role Mapping can be defined.

This document does not explain how to deploy an LDAP system nor does it explain how to create the required users or groups within it.

2 LDAP Configuration

2.1 Settings Page

In the Authentication Service settings page of the Fusion Registry, there is a drop-down option for LDAP. Selecting this option will display the controls allowing specification of your LDAP system.



The screenshot shows the 'Authentication Service' configuration page. At the top, it says 'Specify an Authentication Service'. Below that, a note states: 'An external additional Security Service may be supplied for the Registry. Either a Fusion Security, LDAP, or other security authentication service in order to authenticate users.' The main configuration area consists of several input fields:

- Security Service:** A dropdown menu with 'LDAP' selected.
- ldap://:** A text field containing 'aaa.bbb.ccc.uk:389'.
- Base DN:** A text field containing 'dc=aaa,dc=bbb,dc=ccc,dc=uk'.
- Manager DN:** A text field containing 'cn=admin,dc=aaa,dc=bbb,dc=ccc,dc=uk'.
- Manager Password:** A password field with masked characters (dots).
- User Search Base:** A text field containing 'ou=People'.
- User Search Filter:** A text field containing 'uid={0}'.
- Group Search Base:** A text field containing 'ou=group'.
- Group Search Filter:** A text field containing 'memberUid={1}'.
- Role Prefix:** An empty text field.
- UserID Attribute:** A text field containing 'uid'.

At the bottom of the form, there is a 'Define Role Mappings' button and a green 'Apply Settings' button.

Figure 1 showing the LDAP settings page with some placeholder values

To establish the connection between Fusion Registry and the LDAP server, the following information needs to be supplied:

1. Protocol – either LDAP or LDAPS.
2. URL of LDAP server – either the IP address or server name of the LDAP server. This may include the port number if necessary.

The following information is optional, but it is highly likely that some, if not all, of these values will need to be specified to enable communication between Fusion Registry and LDAP:

Base DN	The root Distinguished Name (DN) for the Registry to search for entities under.
Manager DN	
Manager Password	The password for the manger
User Search Base	

User Search Filter	
Group Search Base	
Group Search Filter	
Role Prefix	
UserID Attribute	

2.2 Role Template

If no Role Mappings are defined then the Registry will communicate to the LDAP server using the Role Template. In this scenario, users are given permission by assigning them to groups and the names of the groups follows a specific pattern to provide authorisation.

To set up roles permitting Agency level authorisation, groups for the appropriate agency must be named "ACY_" and then be followed by the agency name. E.g. A group which permits users assigned to that group to modify SDMX structures, must be named "ACY_SDMX"

To assign a Data Provider role to a user, then the group must be named "DP_" followed by the "Agency Id" of the Data Provider, an underscore, and then the Data Provider ID. For example, to create a group of Data Providers for the Data Provider "DP1" owned by the Agency "ACY", the group must be named: "DP_ACY_DP1"

To assign a Data Consumer role to a user, then the group must be named "DP_" followed by the "Agency Id" of the Data Provider, an underscore, and then the Data Provider ID. For example, to create a group of Data Providers for the Data Provider "DP1" owned by the Agency "ACY", the group must be named: "DP_ACY_DP1".

To create a group that permits Administrator access to the Registry, the group needs to be named "Administrators" (this is not case sensitive).

2.3 Role mapping

If you do not want to map roles to users using the default naming template, you can define your own mapping values. Custom Role Mapping allows an association between a group in the LDAP server to permissions in the Registry. For example, you can specify that any users assigned to the group named "ABC" have permission to be Agencies for "ACY1".

To setup a mapping, click the "Define Role Mappings" button and you will be presented with a dialog titled: "Define Role Mappings". This modal has controls allowing the creation of custom mappings.

Figure 2 showing the LDAP role mappings

Clicking “Add Role Mapping” presents the user with an input field, and a dropdown:

Figure 3 showing the input field with dropdown

The key is what will be looked up when parsing your roles on the LDAP server, the key needs to match the name of the group. The second part is the type of role this mapping value equates to. If for example you want to map “ABC” with the Agency “ACY1”, then you would type “ABC” as the key, and select agency “ACY1” as the value.

When you have added all your required mapping values, clicking “OK” will inform the Registry to use your mapping values and not use the template. Any groups that your LDAP server is connected to and not defined in the mapping will be ignored.

If you wish to define a custom name for an Administrator mapping, click the “Add Administrator Role Mapping”. This will only allow you to specify a key since an admin does not associate with organisations.