Integrating IdentityIQ with File Access Manager for Enrichment

Version: 8.3 Revised: March 30, 2022

Contents

Connector Overview

> The File Access Manager is an independent application installed on the IdentityIQ platform. This Data Enrichment Connector connects to the IdentityIQ application, which is also installed on the IdentityIQ platform.

The IdentityIQ Enrichment connector retrieves complementary identity information regarding an Active Directory user, if that user created activities in a monitored application connected to the enrichment connector.

File Access Manager uses an IdentityIQ API to connect to the IdentityIQ application and platform.

File Access Manager uses this API to search for an Active Directory account and retrieve that account's identity information.

Supported Versions

This connector supports IdentityIQ versions 7.1 and up.

Setup Procedures

The main setup procedures are:

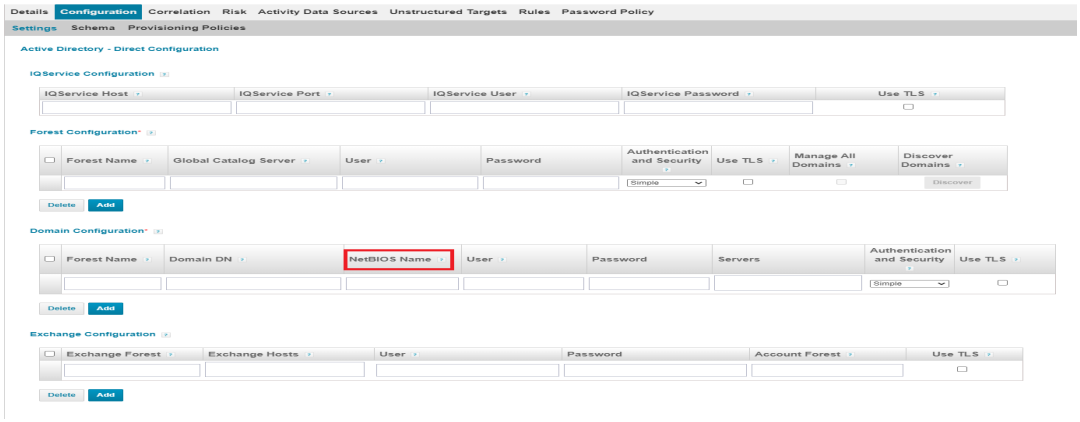
1. Set up the IdentityIQ Active Directory application(s)
2. Assign a user to connect to File Access Manager
3. Set up the enrichment connector in File Access Manager

Prerequisites

Make sure your system fits the descriptions below before starting the installation.

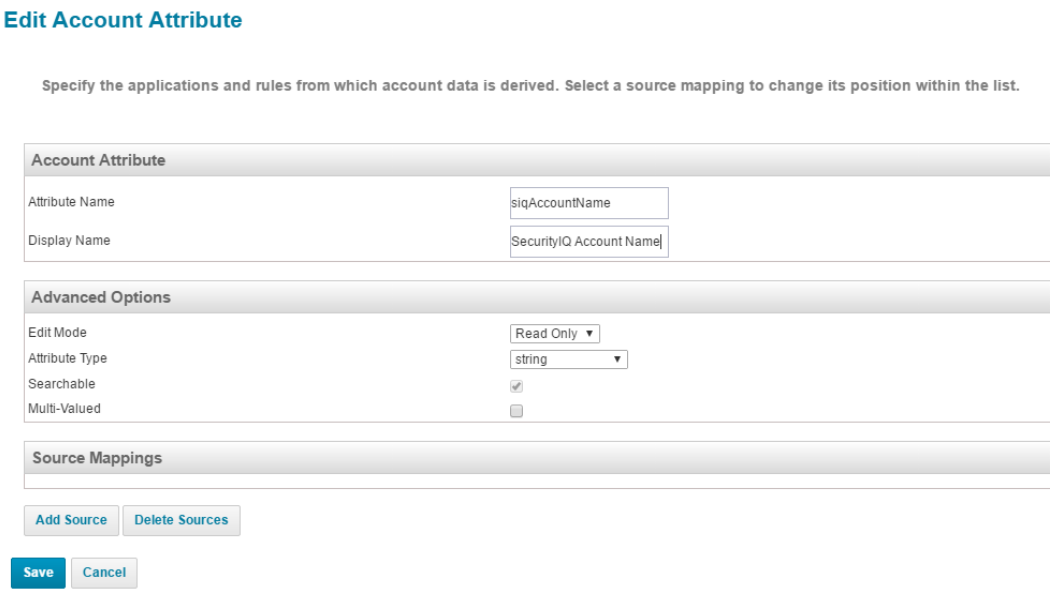
Active Directory Application Setup

1. Create an Active Directory application in IdentityIQ if one does not already exist.
2. Navigate to *Application Configuration* > *Domain Configuration*, and fill in the “NetBIOS Name” column for each domain.

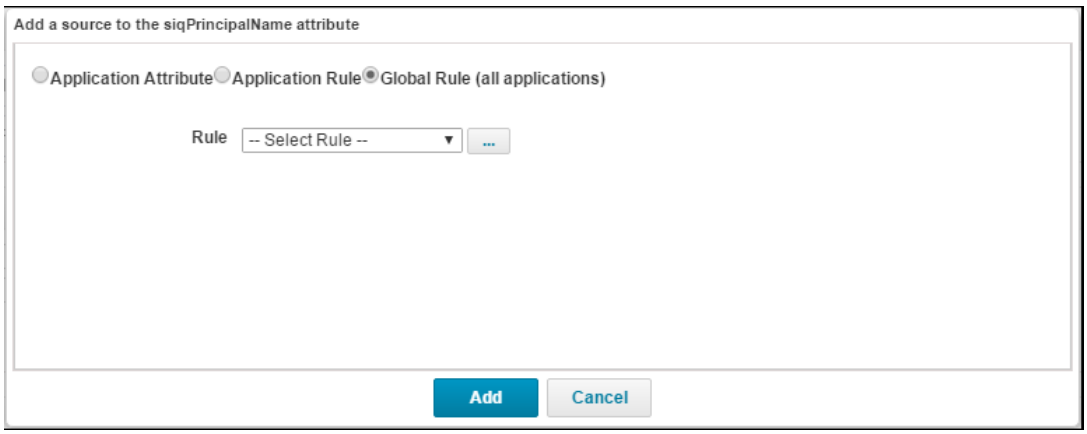


Setting Account Mappings

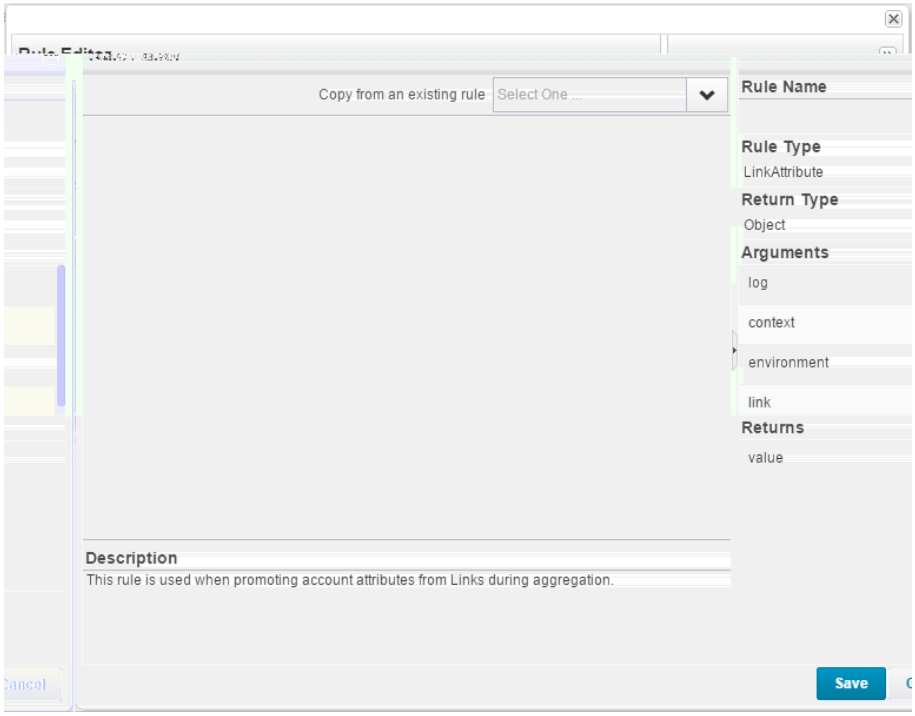
1. Navigate to Global Settings > Account Mappings.
2. Create a new attribute by clicking **Add New Attribute.**
3. Set the following values:
    a. Attribute Name (with the same character case): siqAccountName
    b. Display Name: File Access ManagerAccount Name



4. Click **Add Source** to add a new source.
5. Select *Global Rule*.



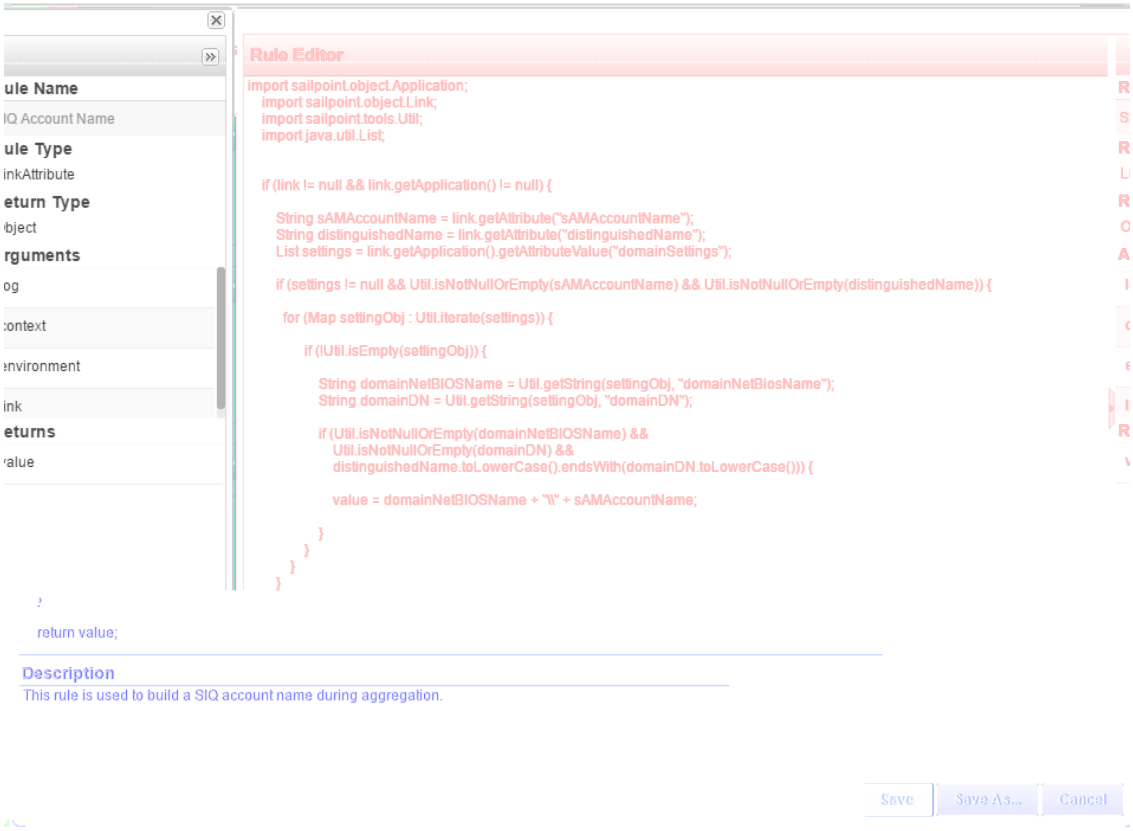
6. Click the ellipsis button (**...**) to the right of the Rule field.



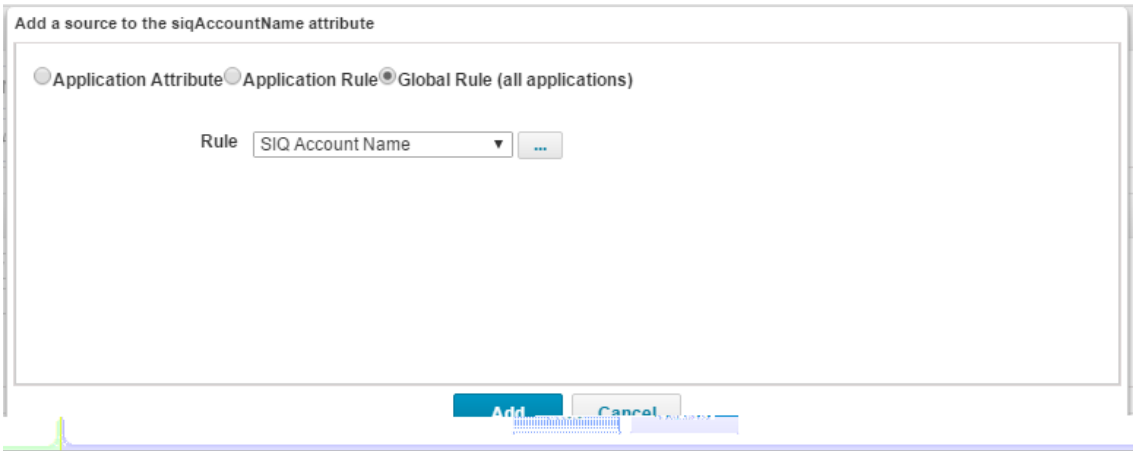
7. Set the following values:
    a. Rule Name: SIQ Account Name
    b. Source code:

```
import sailpoint.object.Application;
import sailpoint.object.Link;
import sailpoint.tools.Util;
import java.util.List;

value = null;

if (link != null) {

    Application app = link.getApplication();

    if (app != null && app.type.equalsIgnoreCase("Active Directory - Direct")) {

        String msDSPrincipalName = link.getAttribute("msDS-PrincipalName");
        if (Util.isNotNullOrEmpty(msDSPrincipalName) && msDSPrincipalName.contains
("\\") ) {
          value = msDSPrincipalName;
        }
        else {
            String sAMAccountName = link.getAttribute("sAMAccountName");
            String distinguishedName = link.getAttribute("distinguishedName");
            List settings = app.getAttributeValue("domainSettings");
```

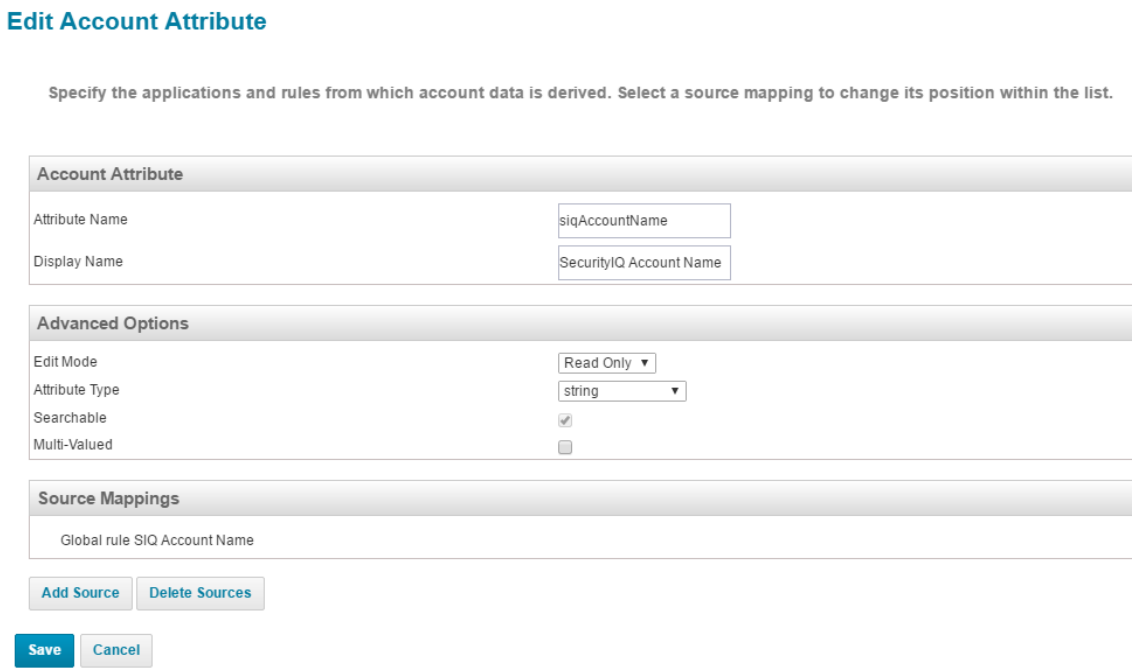
```
            if (settings != null && Util.isNotNullOrEmpty(sAMAccountName) &&
Util.isNotNullOrEmpty(distinguishedName)) {

                distinguishedName = distinguishedName.toLowerCase();
                String userDomainDN = distinguishedName.substring(dis-
tinguishedName.indexOf(",dc=") + 1);

                for (Map settingObj : Util.iterate(settings)) {
                    if (!Util.isEmpty(settingObj)) {

                        String domainNetBIOSName = Util.getString(settingObj,
"domainNetBiosName");
                        String domainDN = Util.getString(settingObj, "domainDN");
                        if (Util.isNotNullOrEmpty(domainNetBIOSName) &&
Util.isNotNullOrEmpty(domainDN) && userDomainDN.equalsIgnoreCase(domainDN)) {
                            value = domainNetBIOSName + "\\" + sAMAccountName;
                        }
                    }
                }
            }
        }
    }

return value;
```



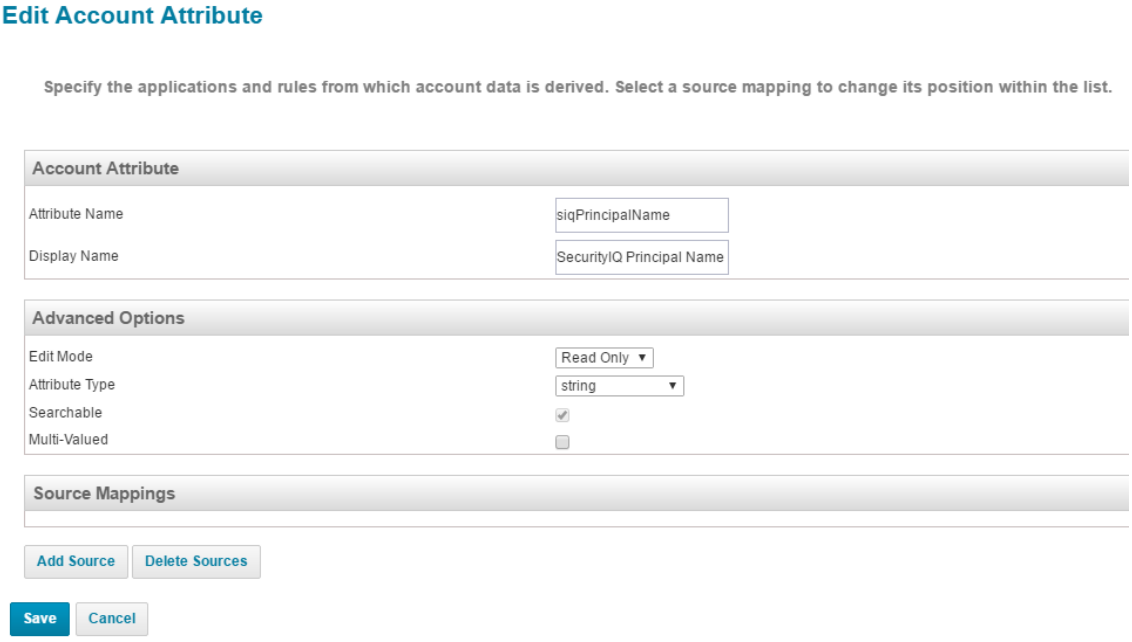
8. Click **Save.**
9. Select *SIQ Account Name* from the Rules selection.



10. Click **Add**

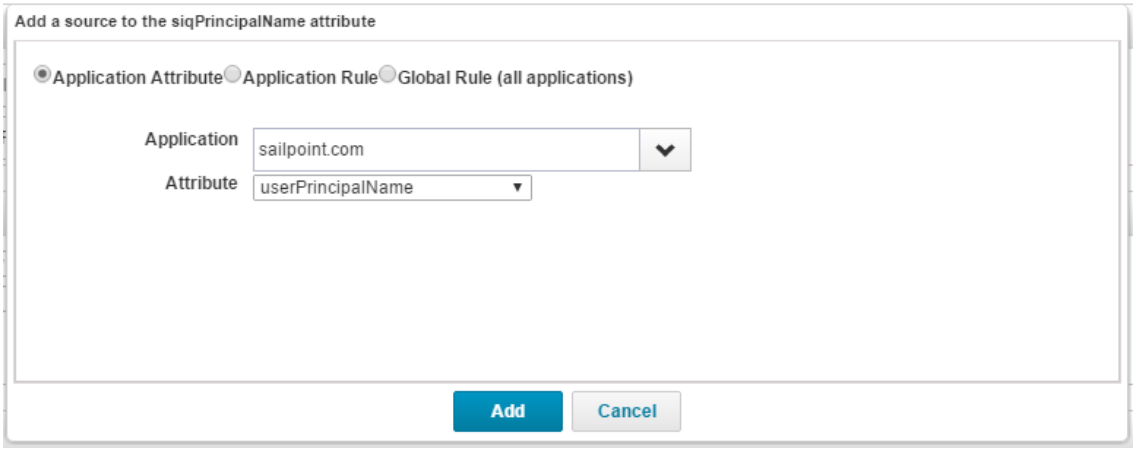


11. Click **Save.**
12. Create a new attribute by clicking **Add New Attribute**.
13. Set the following values:
14. Attribute Name (with the same character case): siqPrincipalName
15. Display Name: File Access Manager Principal Name

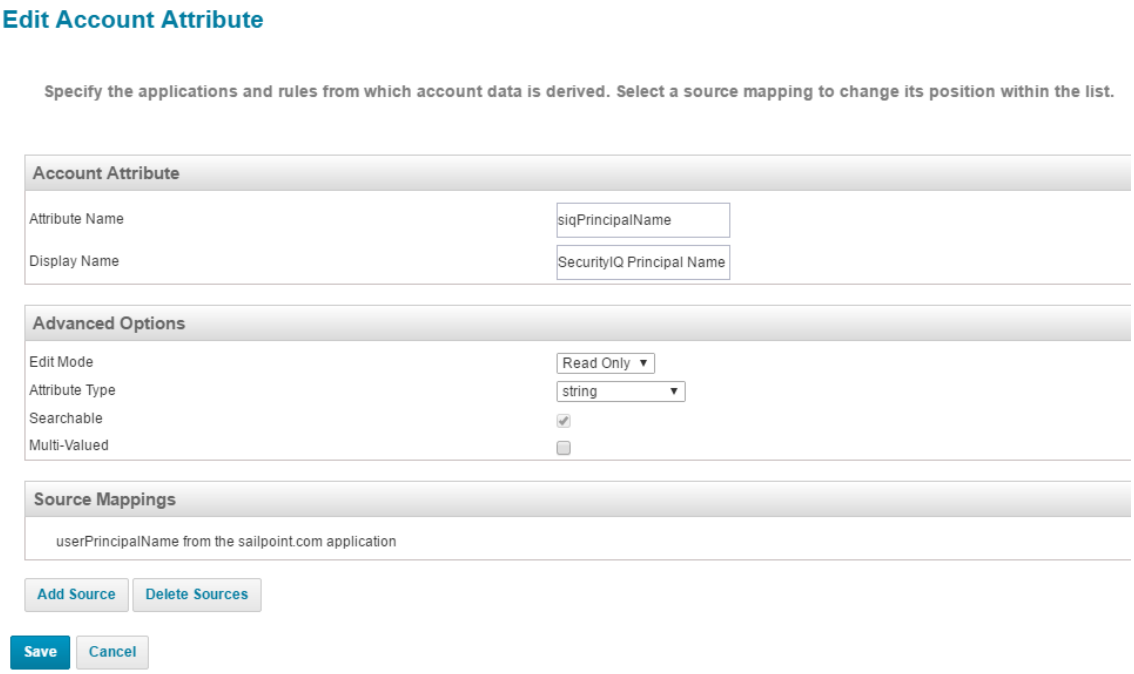


16. Click **Add Source** to add a new source.

17. Set the following values:
    a. Application: The Active Directory application name
    b. Attribute: userPrincipalName



18. Click **Add**.



19. Click **Save**.

> To force IdentityIQ account mappings to be updated, run the Active Directory Account Aggregation task with option "Disable optimization of unchanged accounts" checked.

IdentityIQ User for File Access Manager

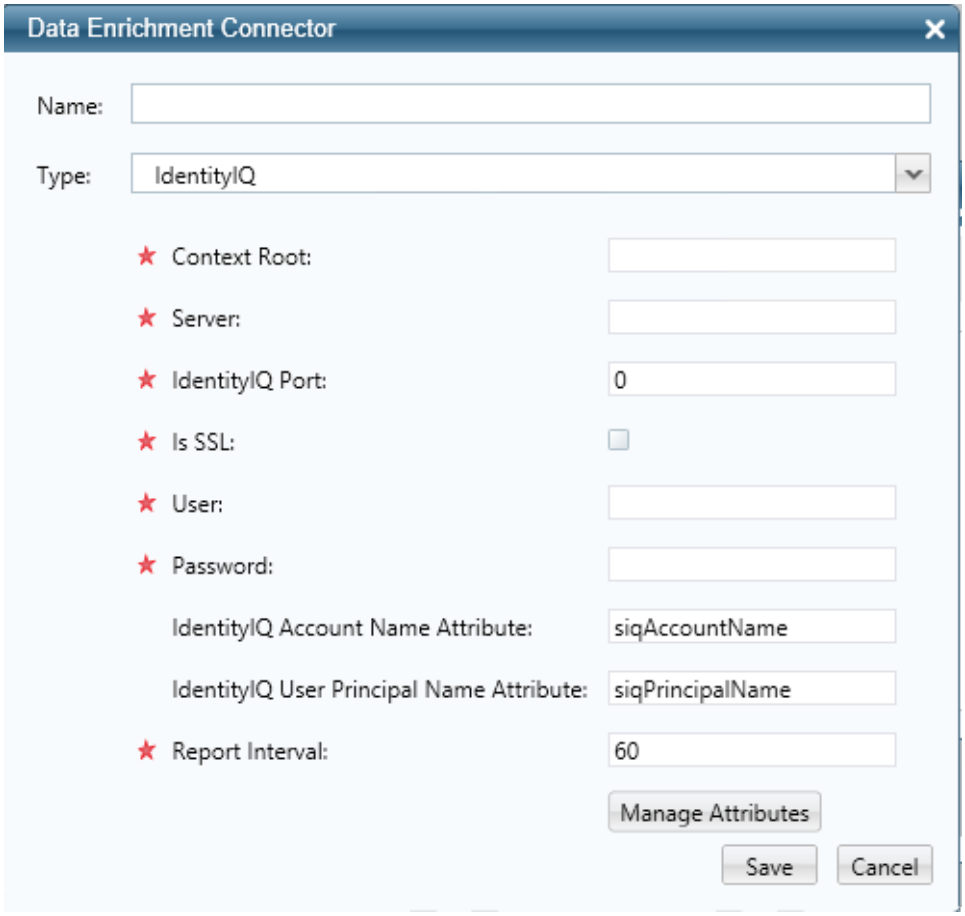
File Access Manager connects to IdentityIQ, using the basic authentication mechanism to retrieve data from IdentityIQ.

Basic authentication requires a user name and a password.

Assign an IdentityIQ user (with *SCIM Executor* capability) to File Access Manager so that the user has access to, and can retrieve data from,IdentityIQ.

Enrichment Connector Setup

1. On the File Access Manager Administrative Client navigate to *Applications* > *Configuration* > *Activity Monitoring* > *Data Enrichment Connectors*.
2. Click **New**.
3. Select Type: IdentityIQ.



4. Complete the following IdentityIQ Enrichment connector fields as follows:

Name

The connector's logical name.

Context Root

The IdentityIQ context root is part of the IdentityIQ address. The default context root when installing IdentityIQ is "IdentityIQ", as in the URL: *http://localhost:8080/**IdentityIQ***

> The context root can be changed from the default value during the IdentityIQ installation stage. If so, type in the updated value.

Server

The IdentityIQ server name.

Port

The IdentityIQ port.

Is SSL

Select if IdentityIQ uses SSL.

User/Password

The IdentityIQ credentials (from the account in Section IdentityIQ User for File Access Manager).

IdentityIQ *Account Name Attribute*: The Account Mapping attribute name (from the File Access Manager Account Name mapping created in section Setting Account Mappings).

> If the names are the same as those in this guide, the attribute will be siqAccountName.

IdentityIQ User Principal Name Attribute

Type the Principal Name Mapping attribute name, as defined in File Access Manager Principal Name mapping created in section Setting Account Mappings.

> If the names are the same as those in this guide, the attribute will be siqPrincipalName.

Report Interval

Set the connector Health reporting interval (in seconds).

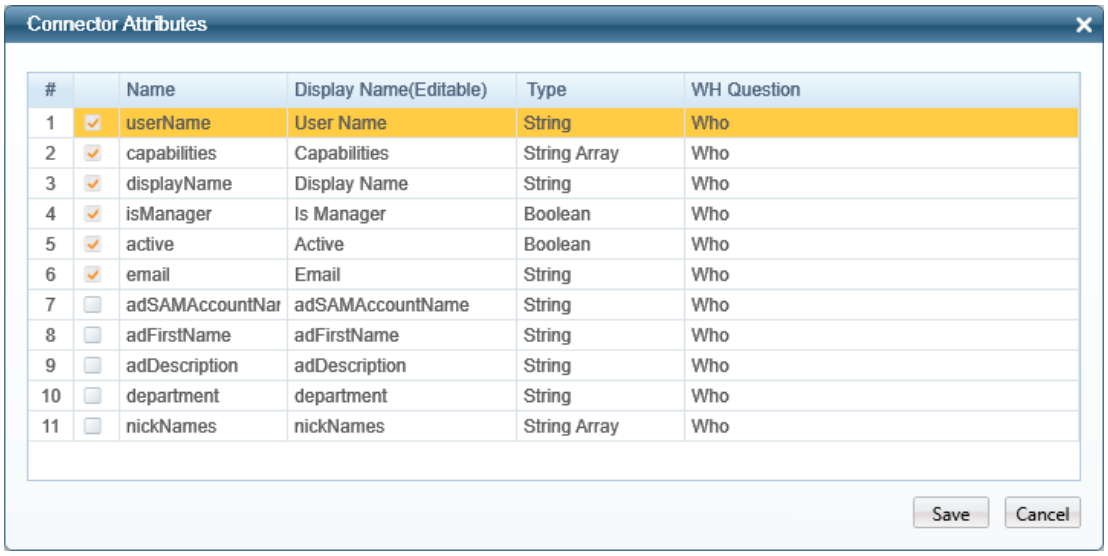
5. Click **Manage Attributes**.

> This screen displays the attributes that can be fetched from the IdentityIQ Enrichmentconnector. Some are predefined attributes, while others are custom attributes (defined in IdentityIQ Identity Mappings).

The predefined attributes displayed the first time this screen is displayed are:

- userName
- capabilities
- displayName
- isManager
- active
- email

> Other attributes will be displayed after the predefined attributes, with the same Name and Display Name, and will be unmarked by default.



6. Each marked attribute will be fetched from IdentityIQ and stored in each File Access Manager activity.
7. Mark an attribute to add it, or unmark an attribute to remove it.

> Predefined attributes cannot be unmarked.

8. You can edit the display name of any attribute by clicking on it and typing a new Display Name.
9. Click **Save** after editing the attributes.
10. Click **Save** (again) to save the connector.