Integrating IdentityIQ with File Access Manager for Enrichment

Version: 8.2 Revised: July 01, 2021

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. https://www.sailpoint.com/patents

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Contents ..... **iii**

Connector Overview ..... **iv**

Supported Versions iv

Setup Procedures iv

Prerequisites ..... **v**

Active Directory Application Setup v

Setting Account Mappings v

IdentityIQ User for File Access Manager x

Enrichment Connector Setup ..... **xii**

Connector Overview

> The IdentityIQ 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.

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

IdentityIQ 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:

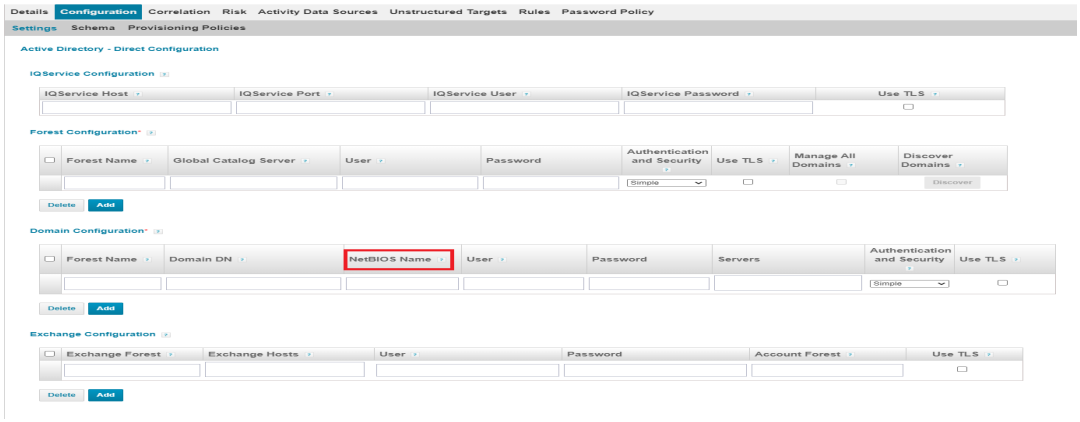
1. Set up the IdentityIQ Active Directory application(s)
2. Assign a user to connect to IdentityIQ File Access Manager
3. Set up the enrichment connector in IdentityIQ File Access Manager

Prerequisites

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

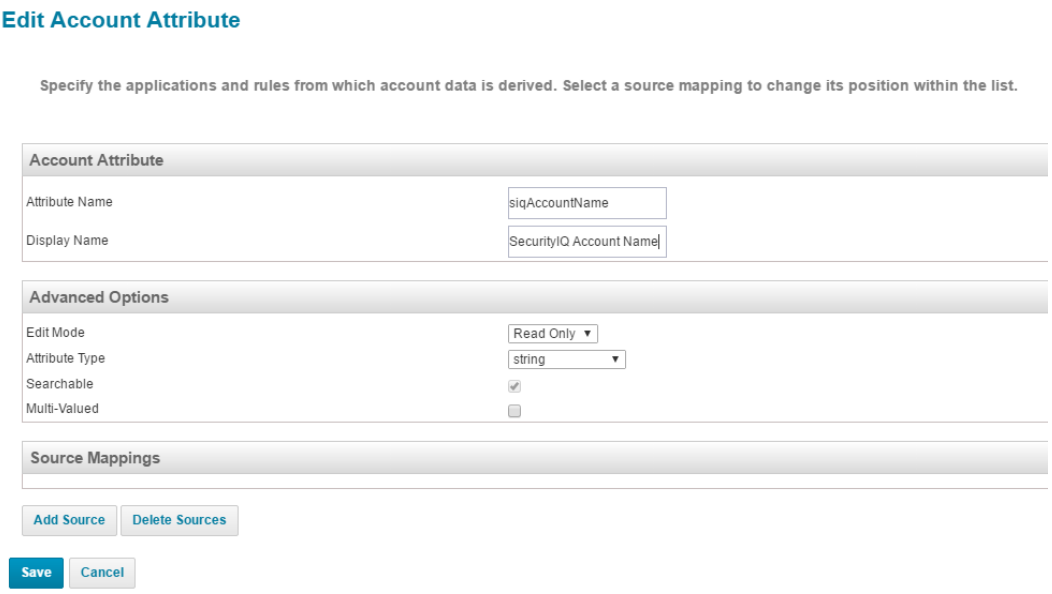
Active Directory Application Setup

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.

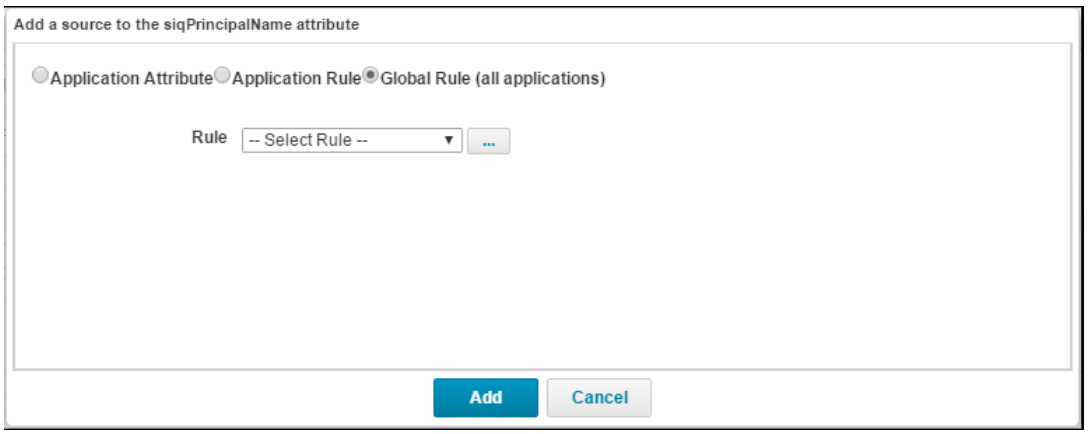


Setting Account Mappings

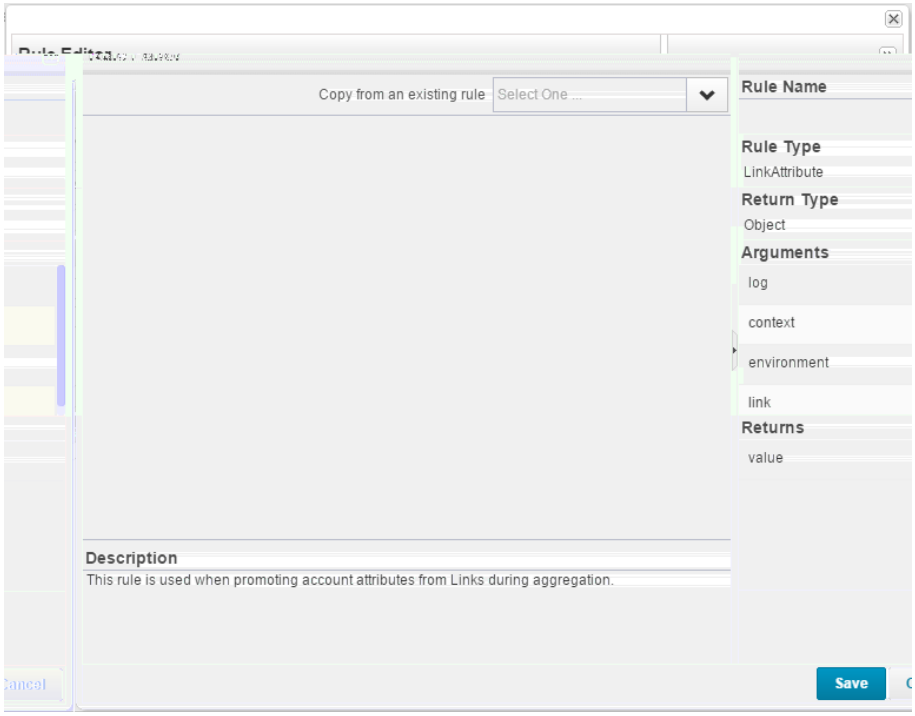
1. Navigate to Global Settings > Account Mappings.
2. Create a new attribute by clicking **Add New Attribute.**
3. Set the following values:
    a. Attribute Name (with the same character case): siqAccountName
    b. Display Name: IdentityIQ File Access ManagerAccount Name



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.



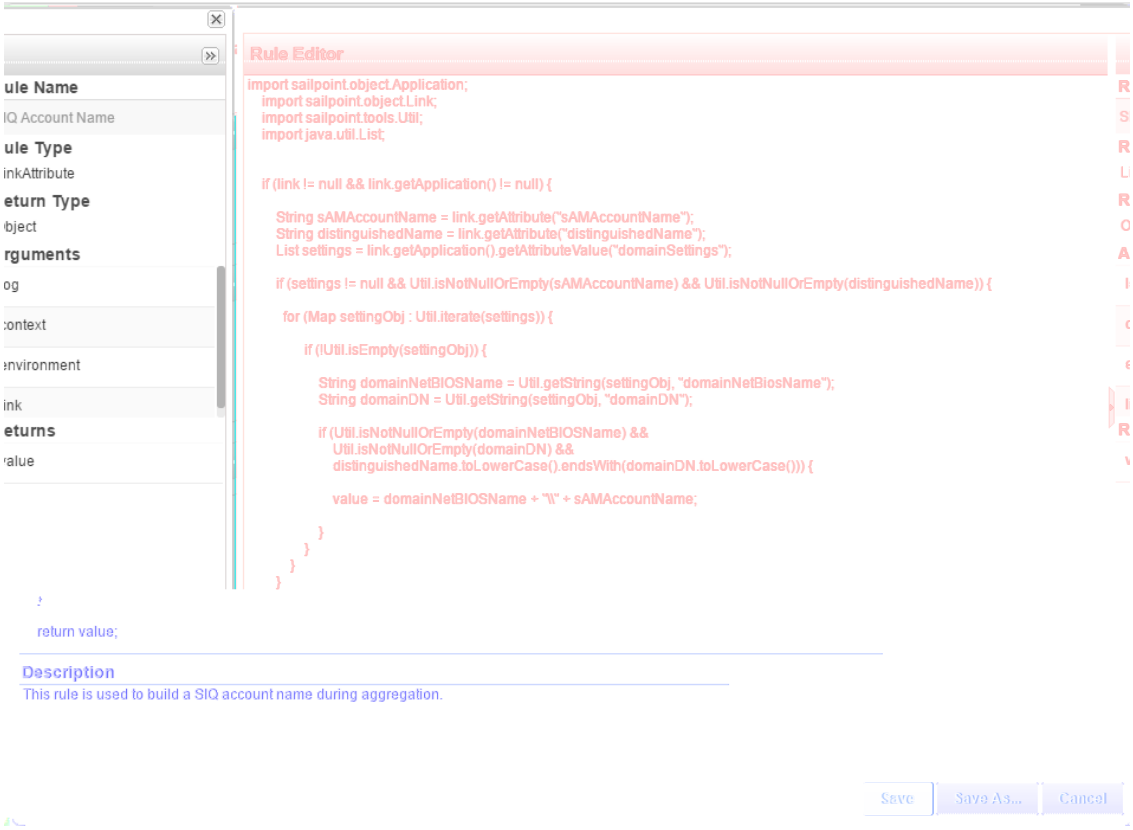
7. Set the following values:

   a. Rule Name: SIQ Account Name

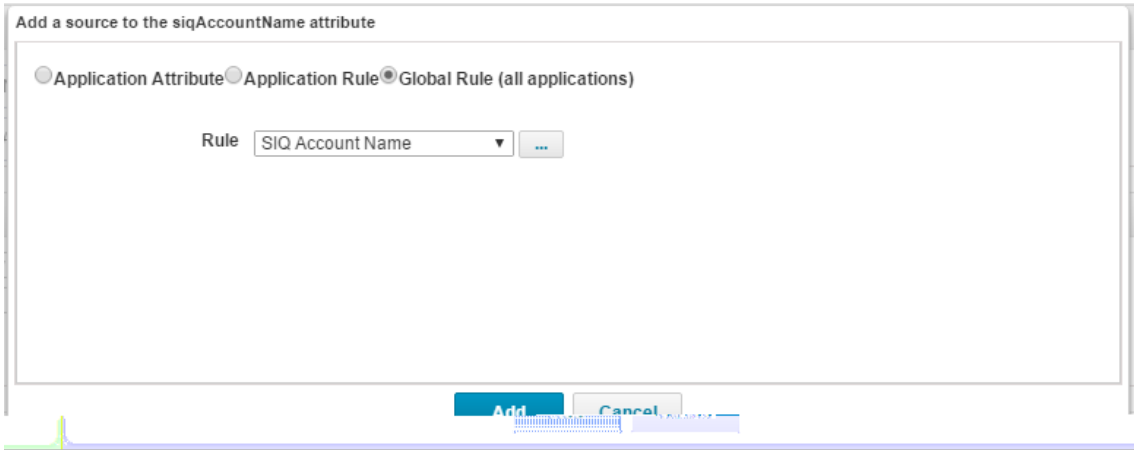
   b. Source code:

```
import sailpoint.object.Application;
import sailpoint.object.Link;
import sailpoint.tools.Util;
import java.util.List;
if (link != null && link.getApplication() != null) {
String sAMAccountName = link.getAttribute("sAMAccountName");
String distinguishedName = link.getAttribute("distinguishedName");
List settings = link.getApplication().getAttributeValue("domainSettings");
if (settings != null && Util.isNotNullOrEmpty(sAMAccountName) &&
Util.isNotNullOrEmpty(distinguishedName)) {
  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) &&
        distinguishedName.toLowerCase().endsWith(domainDN.toLowerCase())) {
        value = domainNetBIOSName + "\\" + sAMAccountName;
        }
    }
    }
  }
}
```

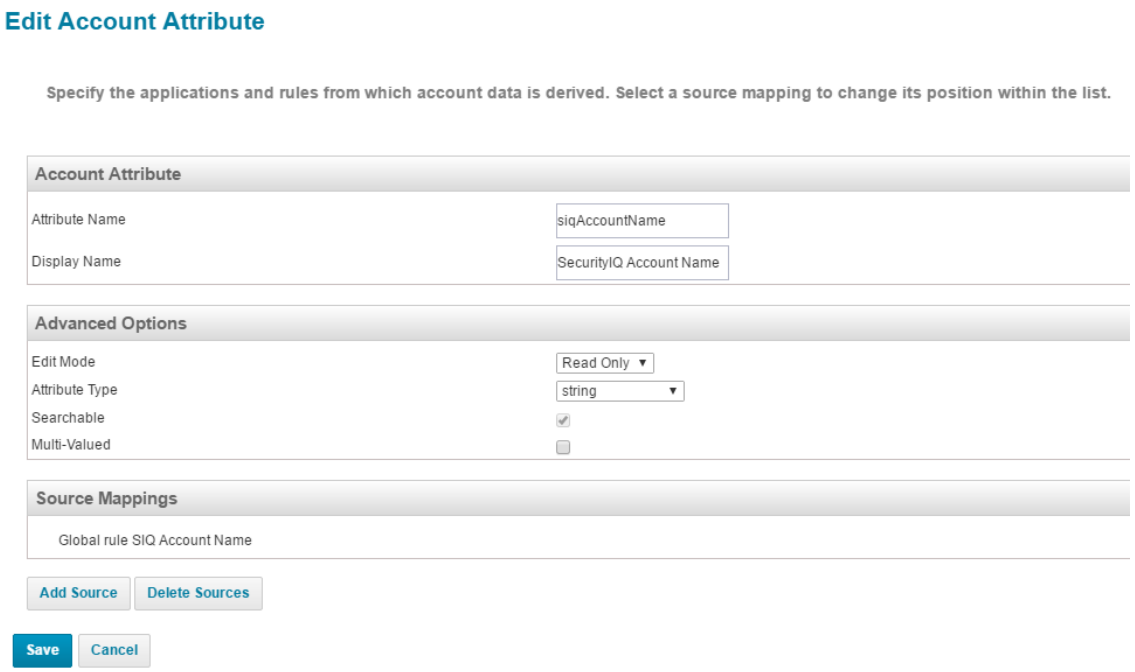
```
return value;
```



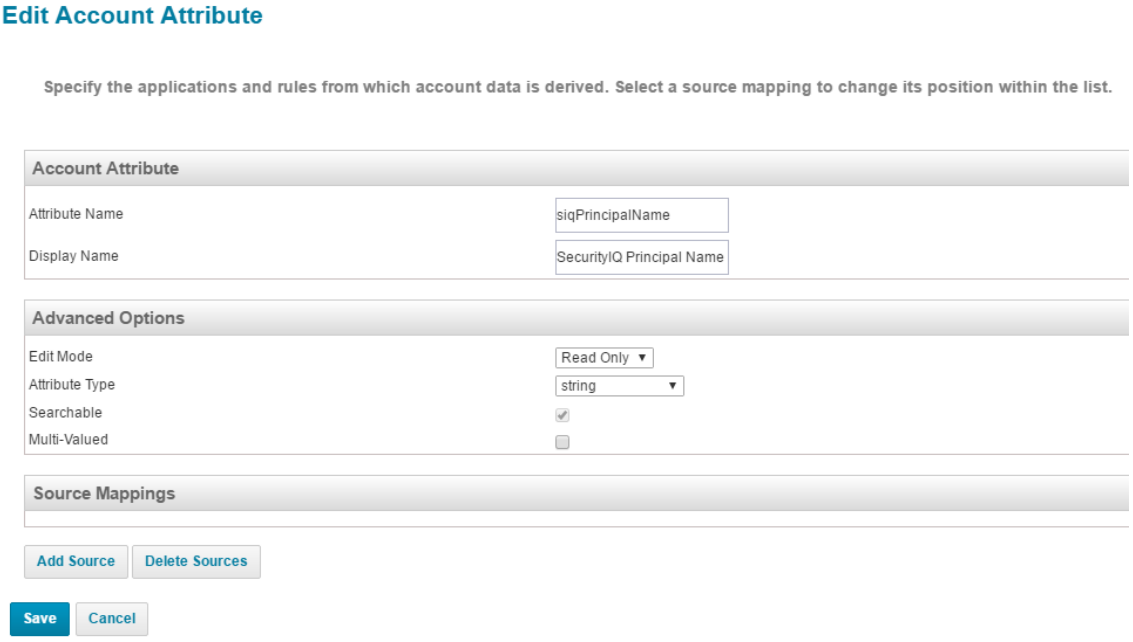
8. Click **Save.**
9. Select *SIQ Account Name* from the Rules selection.



10. Click **Add**

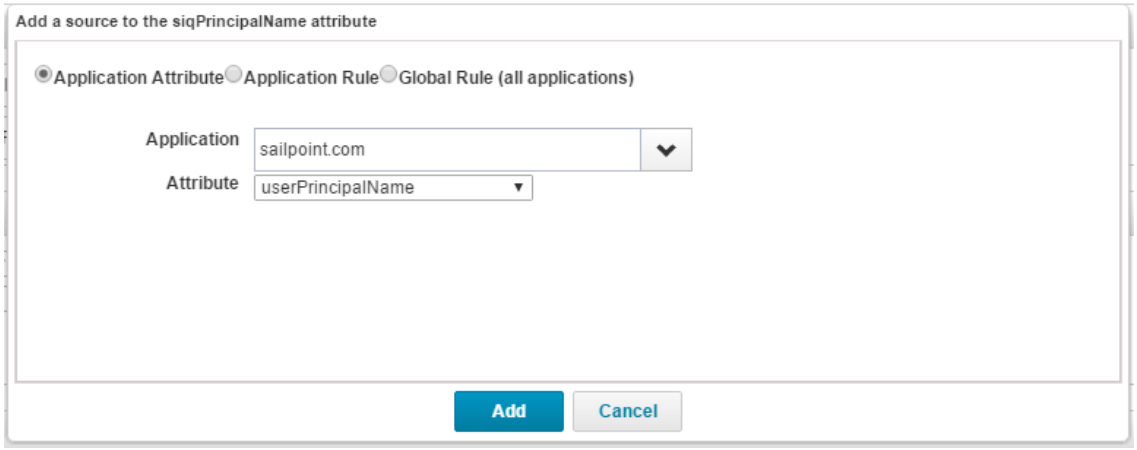


11. Click **Save.**
12. Create a new attribute by clicking **Add New Attribute**.
13. Set the following values:
14. Attribute Name (with the same character case): siqPrincipalName
15. Display Name: IdentityIQ File Access Manager Principal Name

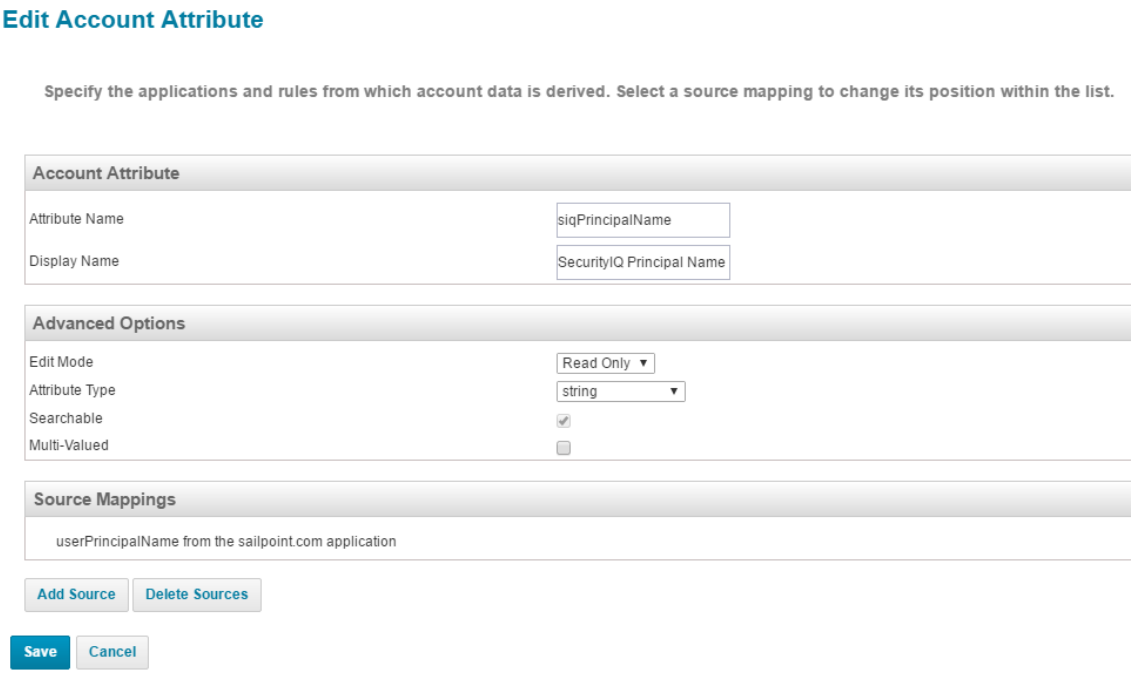


16. Click **Add Source** to add a new source.

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



18. Click **Add**.



19. Click **Save**.

IdentityIQ User for File Access Manager

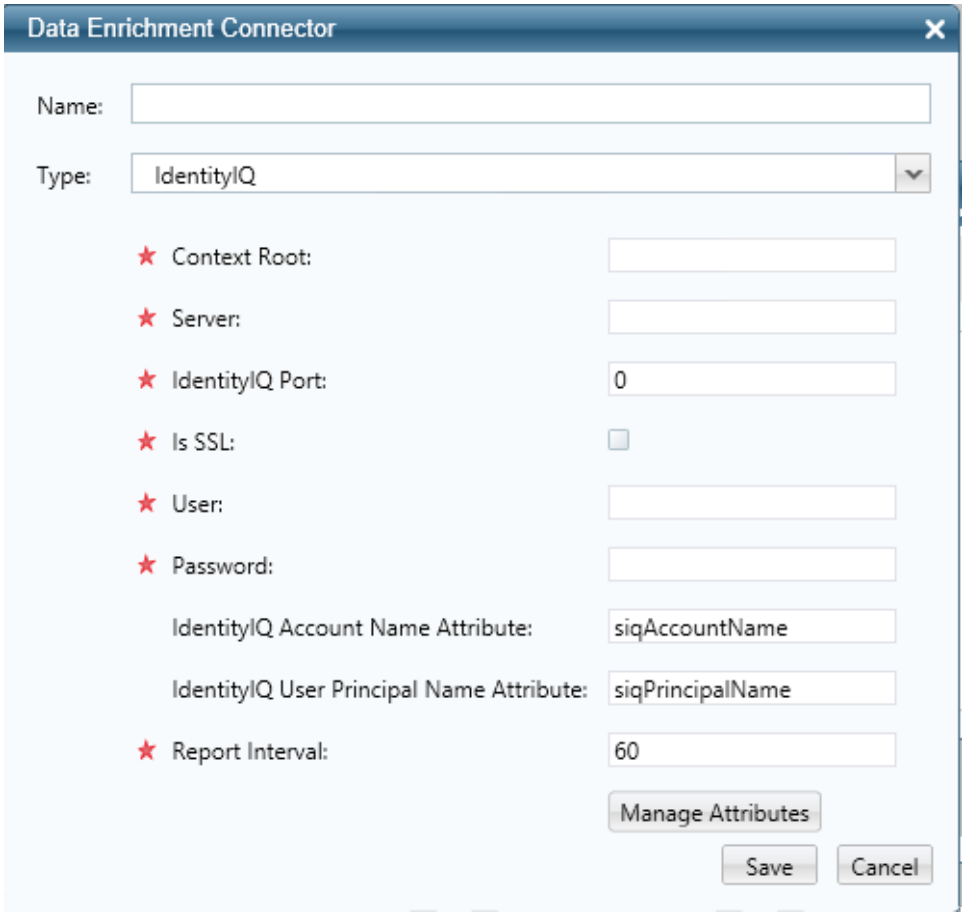
IdentityIQ File Access Manager connects to IdentityIQ, using the basic authentication mechanism to retrieve data from IdentityIQ.

Basic authentication requires a user name and a password.

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

Enrichment Connector Setup

1. On the IdentityIQ 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 IdentityIQ 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 IdentityIQ 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).

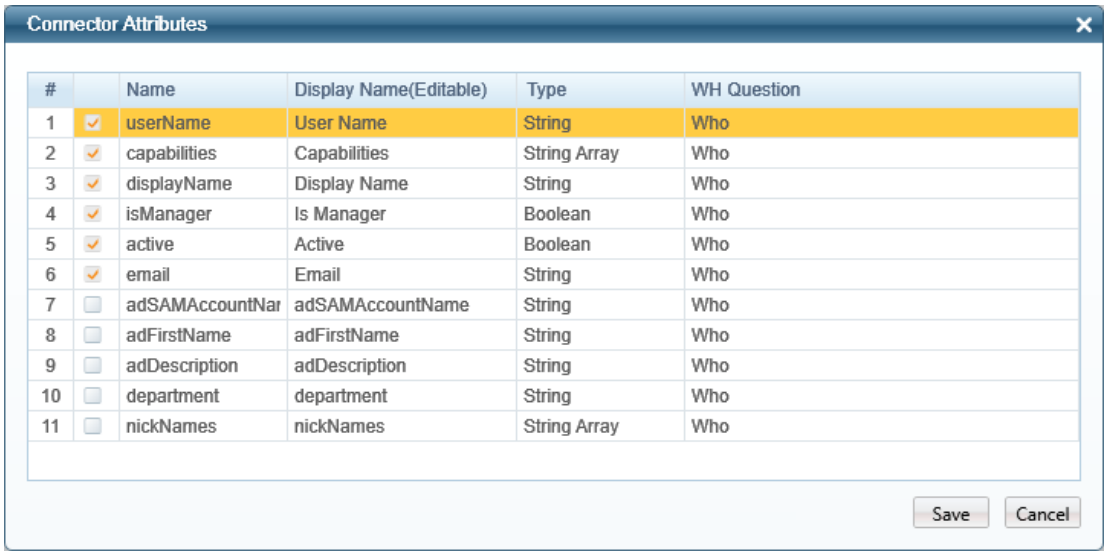
5. Click **Manage Attributes**.

> 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 IdentityIQ 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.