



SailPoint IdentityIQ

Version: 8.0

File Access Manager Generic Table Connector Installation Guide

Copyright ©2019 SailPoint Technologies, Inc., All Rights Reserved.

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.

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. Government's Specially Designated Nationals (SDN) List; 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.

Copyright and Trademark Notices.

Copyright ©2019 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 web site 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 Technologies & Design,” “SailPoint,” “IdentityIQ,” “IdentityNow,” “SecurityIQ,” “IdentityAI,” “AccessIQ,” “Identity Cube” and “Managing the Business of Identity” are registered trademarks of SailPoint Technologies, Inc. “Identity is Everything” and “The Power of Identity” are 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.

Table of Contents

Chapter 1: Connector Installation & Configuration	1
Overview.....	1
Installation Flow.....	1
Chapter 2: General	1
Connector Operation Principles	1
Chapter 3: Prerequisites.....	1
Software Requirements.....	1
Communications Requirements	1
Chapter 4: Add New Application Wizard	2
Chapter 5: Installation of Services	5
Collector Installation.....	5
Chapter 6: Verification	7
Services.....	7
Collectors' Installation Status	7
Logs.....	7
Monitored Activities.....	7

List of Figures

Figure 1. Generic Table configuration panel	3
Figure 2. Collector Installation Manager	5
Figure 3. Service Configuration	6

List of Tables

Table 1. Communications Requirements	1
--	---

Table of Revisions

Ver. #	Description	Author	Date
5.0	Final Version	Jonathan Rappeport	10 Jan 2017
5.1	First Draft	Jonathan Rappeport	08 Feb 2017
5.1	Second Draft	Jonathan Rappeport	13 Jun 2017
5.1	Third Draft	Jonathan Rappeport	26 Sep 2017
6.0	First Draft	Jonathan Rappeport	31 Jul 2017
6.1	Formatting changes only	SailPoint	1 Nov 2018
8.0	Formatting Rebranding to IdentityIQ File Access Manager	SailPoint	30 Jul 2019

Chapter 1: Connector Installation & Configuration

Overview

Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Admin Client.
3. Install the Activity Monitor service.

Chapter 2: General

Connector Operation Principles

IdentityIQ File Access Manager Admin Client Connector for Generic Table queries a database table (either SQL Server or Oracle) for activity monitoring.

Chapter 3: Prerequisites

Software Requirements

- Activity Monitor
 - ◆ Microsoft .Net Framework 4.5

Communications Requirements

Table 1. Communications Requirements

Requirement	Source	Destination	Port
IdentityIQ File Access Manager Admin Client Access	Activity Monitor	IdentityIQ File Access Manager Admin Client Servers	8000-8008
Activity Monitoring	Activity Monitor	Monitored database table	Database port

Chapter 4: Add New Application Wizard

1. **Admin Client** Navigate to **System** → **Applications** → **New** → **Application**.
2. The New Application Wizard window of the New Application Wizard displays under the Welcome tab.
3. Select Standard Application
4. Select Generic Table from the Application Type dropdown menu.
5. Click **Next**

The General Details window of the New Application Wizard displays under the General tab.
6. Type the logical name of the Generic Table application in the *Name* field.
7. Type a description of the application in the *Description* field.
8. Select a logical container for the application from the **Container** dropdown menu.
9. Click **Next**

The Monitor Configuration window of the New Application Wizard displays under the Configuration tab.

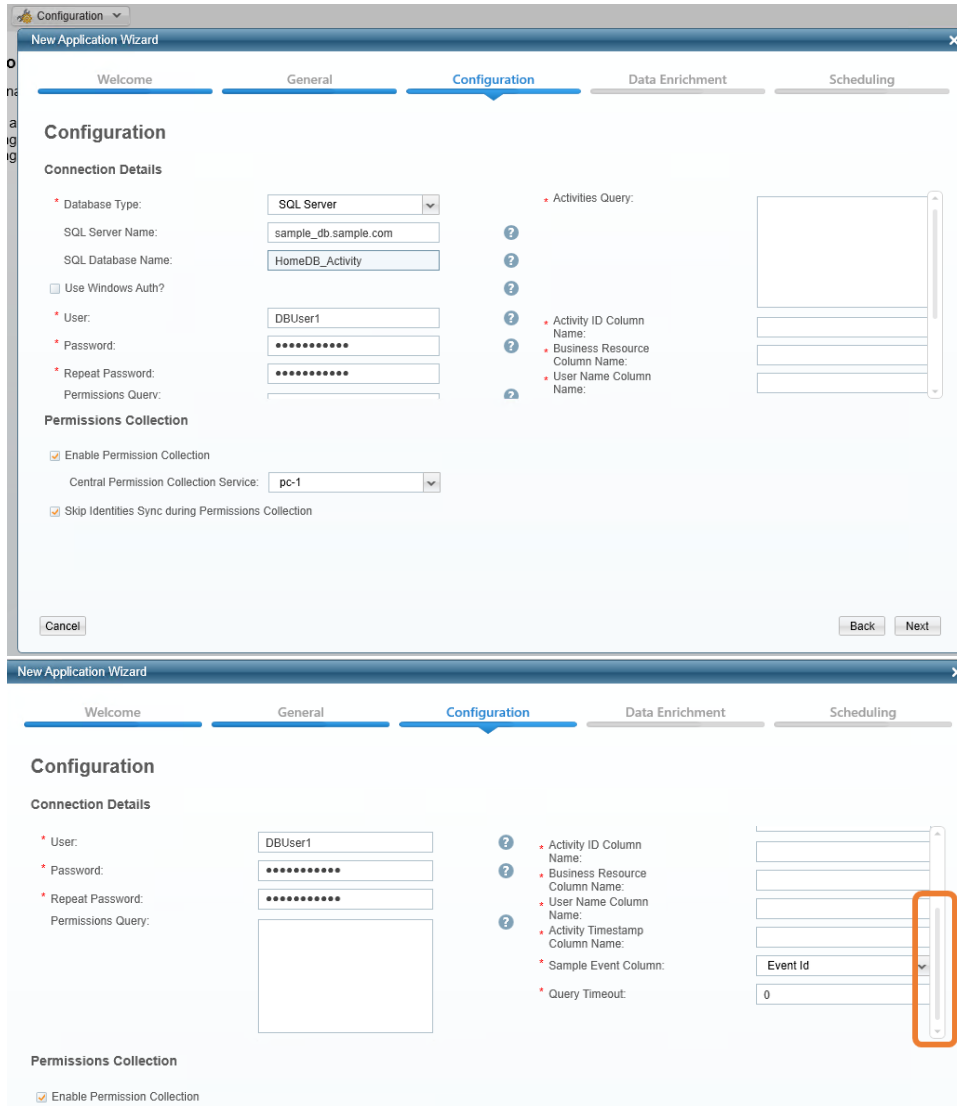


Figure 1. Generic Table configuration panel

10. Complete the Connection Details fields:

Database Type

The type of database, either SQL Server or Oracle.

SQL Server Name

The SQL Server

SQL Database Name

The SQL database

Use Windows Authentication

The default is not to use Windows authentication

User credentials

The user to connect to the database

Activities Query

This query will periodically run to fetch new activities

Permissions Query

This query will periodically run to fetch new permissions

Activity ID Column Name

The column name in the *Activities Query* which identifies the unique id of the activity. This column is used to query for new activities periodically

Business Resource Column Name

The column name in the *Activities Query* which will be displayed to the user as the Business Resource Full Path in the Activities Forensics

User Name Column Name

The column name in the *Activities Query* which will be displayed to the user as the User Name in the Activities Forensics

Activity Timestamp Column Name

The column name in the *Activities Query* which represents the time the activity occurred

Sample Event Column

Either by Event ID or by date

Note: The Generic Table connector will add a condition for each query to fetch only new events. This condition is created with the Sample Event Column.

Query Timeout

In minutes, the default being 0, which means wait indefinitely

11. Complete the Monitor Behavior fields:

- ◆ *Polling interval* (Activity fetching interval [in seconds])
- ◆ *Report Interval* (Activity Monitor Health reporting interval [in seconds])
- ◆ *Local Buffer Size* (Local buffer size for activities [in MB])

Note: This cyclic buffer stores activities on the Activity Monitor machine in case network errors prevent activities from being sent.

12. Although the *Permissions Collection* section appears, the Generic Table connector does not support permissions collection

13. Click **Next**

The Data Enrichment Connectors window of the New Application Wizard displays under the Data Enrichment tab.

14. Select the data enrichment connectors (DECs) to enrich monitored activities from the Available DECs text box and use the > or >> arrows to move them to the Current DECs text box.

Note: The chapter *Activities* of the IdentityIQ File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

15. Click **Next**.

Although the Permissions Collector Scheduling window appears under the Scheduling tab, the Generic Table connector does not support scheduling.

16. Click **Finish**.

Chapter 5: Installation of Services

Collector Installation

1. Run the “**Collector Installation Manager**” as an Administrator.
The installation files are located in the installation package under the folder **Collectors**.

The Collector Installation Manager window displays.

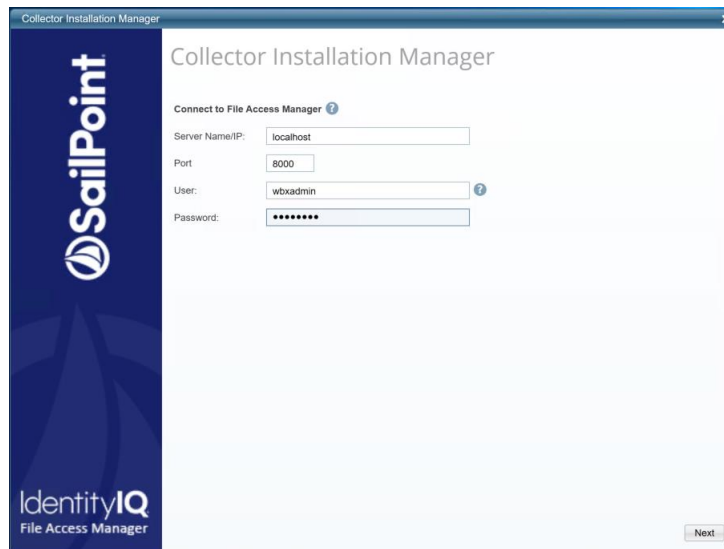


Figure 2. Collector Installation Manager

2. Enter the credentials to connect to IdentityIQ File Access Manager.
 - a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
 - b. An IdentityIQ File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.
3. Click **Next**.

The Service Configuration window displays.

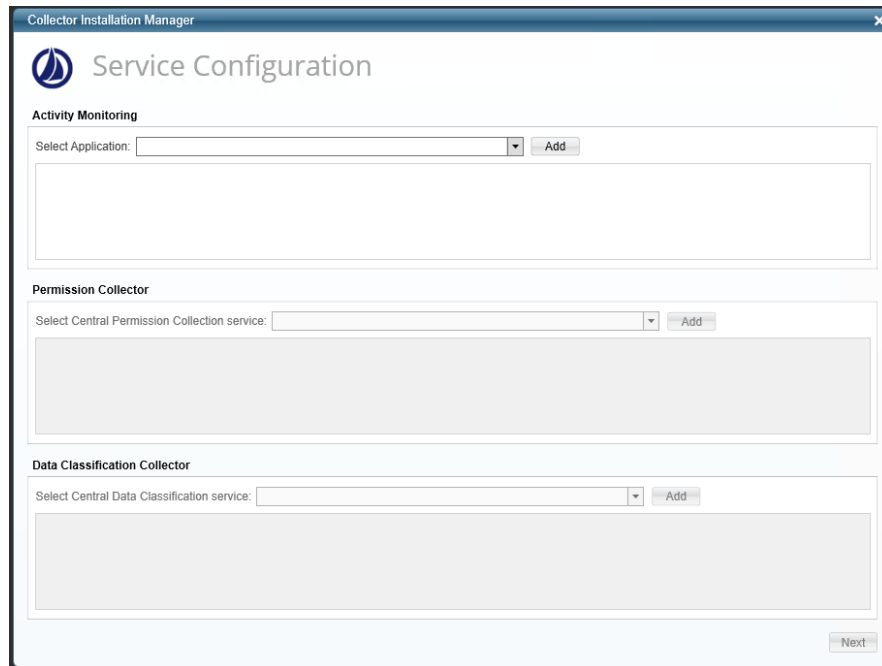


Figure 3. Service Configuration

4. If you are installing the Activity Monitoring collector, select the application from the dropdown list, and click **Add**.
5. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**.
6. Click **Next**.

The Installation Folder window displays.

Note: If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

7. Browse and select the location of the target folder for installation.
8. Browse and select the location of the folder for system logs.
9. Click **Next**.
10. The system begins installing the selected components.
11. After all the selected components have been installed Click **Finish**.

Note: For more information, see the chapter *Permissions* in the IdentityIQ File Access Manager Administrator Guide .

Chapter 6: Verification

Services

Collectors' Installation Status

Verify in windows Service manager or other tool, that the IdentityIQ File Access Manager services are running. For example,

- **File Access Manager Central Activity Monitor** - <Service Name> service is running.

Logs

- "%SAILPOINT_HOME_LOGS%\GenericDBTable_<Application_Name>.log" does not contain errors.

Monitored Activities

1. Simulate activities by inserting them into the Generic Table on the database selected during the connector configuration.
2. Wait a minute (approximately).
3. Query for activities in the Administrative Client by <Application_Name>.
4. Verify that the activities display in the Administrative Client.