SailPoint IdentityIQ

Version: 8.0

File Access Manager CIFS Connector Installation Guide

This document and the information contained herein is SailPoint Confidential Information.

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

List of Figures

List of Tables

Table of Revisions

Ver. #	Description	Author	Date
8.0	First Release	Josh Lewin	4 June 2019

Chapter 1: Connector Installation & Configuration

Overview

General

The CIFS connector enables crawling, permissions collection (without local users and local groups) and data classification but does not provide activity monitoring.

Note: IdentityIQ File Access Manager provides dedicated specified connectors for common application types. You should check for specified connector, if we provide it, before trying to install a generic connector. See the section on Business Resource Structure in the IdentityIQ File Access Manager Administrator Guide for a full list of supported application types.

Installation Flow

1. Configure all the prerequisites.
2. Add a new application to the IdentityIQ File Access Manager Admin Client.
3. Install the Permissions Collector/Data Classification services.

Note: Permission Collector and Data Classification services installation is optional and should only be installed by someone with a full understanding of IdentityIQ File Access Manager deployment architecture. The IdentityIQ File Access Manager Administrator Guide has additional information on IdentityIQ File Access Manager architecture.

Chapter 2: General

Permissions Collector Operation Principle

IdentityIQ File Access Manager connects to the CIFS server through CIFS and analyzes the share and file system permissions on all the folders.

File Access Manager will not analyze local users and local groups. If a folder contains permissions to a local user/group it will appear in IdentityIQ File Access Manager but the entity (user or group) type will be Orphan.

Supported Versions

- Any CIFS compliant file server

Chapter 3: Prerequisites

Software Requirements

Permissions Collector

- Microsoft .Net Framework 4.5

Data Classification

- Microsoft .Net Framework 4.5

Permissions

IdentityIQ File Access Manager requires different permissions, based on the tasks that require those permissions. The user configured in the Application Configuration Wizard must have the following permissions:

Crawling

- Requires a user with Shared Read access, who has permissions to enumerate all shares on the CIFS server.
- Requires a user with File Read access, with permissions to read file attributes.

Typically, in most systems, this would be a member of the local Backup Operators group on the CIFS server.

Permission Collection

- Requires a user with Shared Read access, who has permissions to enumerate all shares on the CIFS server.
- Requires a user with permissions for enumeration of CIFS share-level permissions.

Typically, in most systems, this would be a member of the local Backup Operators group on the CIFS server.

Data Classification

- Requires a user with Shared Read access, who has permissions to enumerate all shares on the CIFS server.
- Requires a user with File Read access, with permissions to read the file contents.

Typically, in most systems, this would be a member of the local Backup Operators group on the CIFS server.

Communications Requirements

Table 1. Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector/Data Classification Collector	RabbitMQ	5671
Permissions Collector & Data Classification Analysis	Permissions Collector/Data Classification Server	Monitored server	CIFS/SMB (139, 445)

Chapter 4: Add New Application Wizard

1. Admin Client Navigate to **System** → **Applications**.
2. Select New → Application.

   The **New Application Wizard** window displays under the Welcome tab.
3. Select Standard Application.
4. Select CIFS (Connector) 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 CIFS 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. Optionally select an Active Directory Identity Collector from the **Identity Collector** dropdown menu.
10. Click **Next**

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

11. Complete the Connection Details fields:

    - *Server Name* (the name of the CIFS server to which users connect)
    - *User Domain* (the user defined in the prerequisites)
    - *User* (the user defined in the prerequisites)
    - *Password* (the password of the user defined in the prerequisites)
    - *Repeat Password* (the password of the user defined in the prerequisites)
12. Click to enable Permission Collection, select a central permissions collection service and complete the relevant Permissions Collection items:

    - *Skip Identities Sync* (Skip identity synchronization before running permission collection tasks when the identity collector is common to many different connectors.)
13. Click to enable Data Classification and select a central data classification service from the list.
14. Click **Next**.

Note: The Scheduling tab contains the Permissions Collection, Crawler, and Data Classification (if supported) scheduling windows. You can navigate among those windows, using the Next and Back buttons.

The Permissions Collection scheduling window of the New Application Wizard displays under the Scheduling tab.

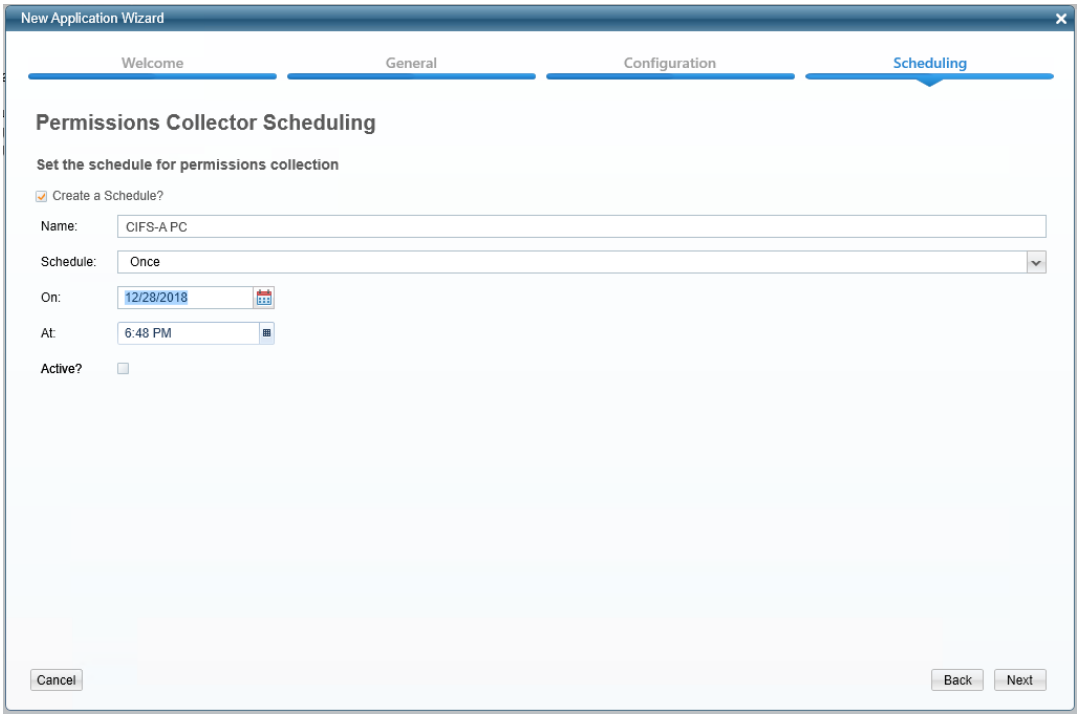

Figure 1. Permissions Collection Scheduling Window

15. Check the **Create a Schedule** check box
16. Type a name for the permissions collection scheduling task in the *Name* field
17. Select a scheduling frequency from the **Schedule** dropdown menu
18. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected)
19. Check the **Active** check box if relevant
20. Click **Next**

The Crawler window of the New Application Wizard displays under the Scheduling tab.

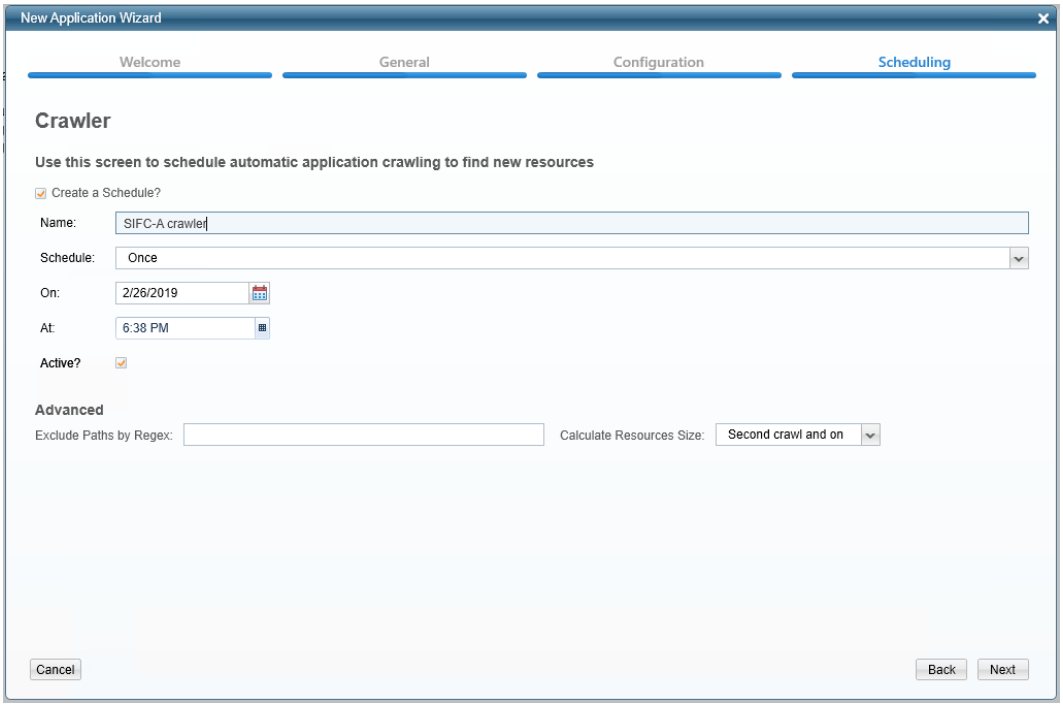

Figure 2. Crawler scheduling Window

21. Check the **Create a Schedule** check box.
22. Type a name for the crawling scheduling task in the *Name* field.
23. Select a scheduling frequency from the **Schedule** dropdown menu.
24. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
25. Check the **Active** check box if relevant.
26. Type in the names of folders to exclude from the crawling process in the *Exclude Paths by Regex* field.

    Note: See the chapter *Crawling* of the IdentityIQ File Access Manager Administrator Guide for more information.

27. Click **Next**.

The Data Classification scheduling window of the New Application Wizard displays under the Scheduling tab.

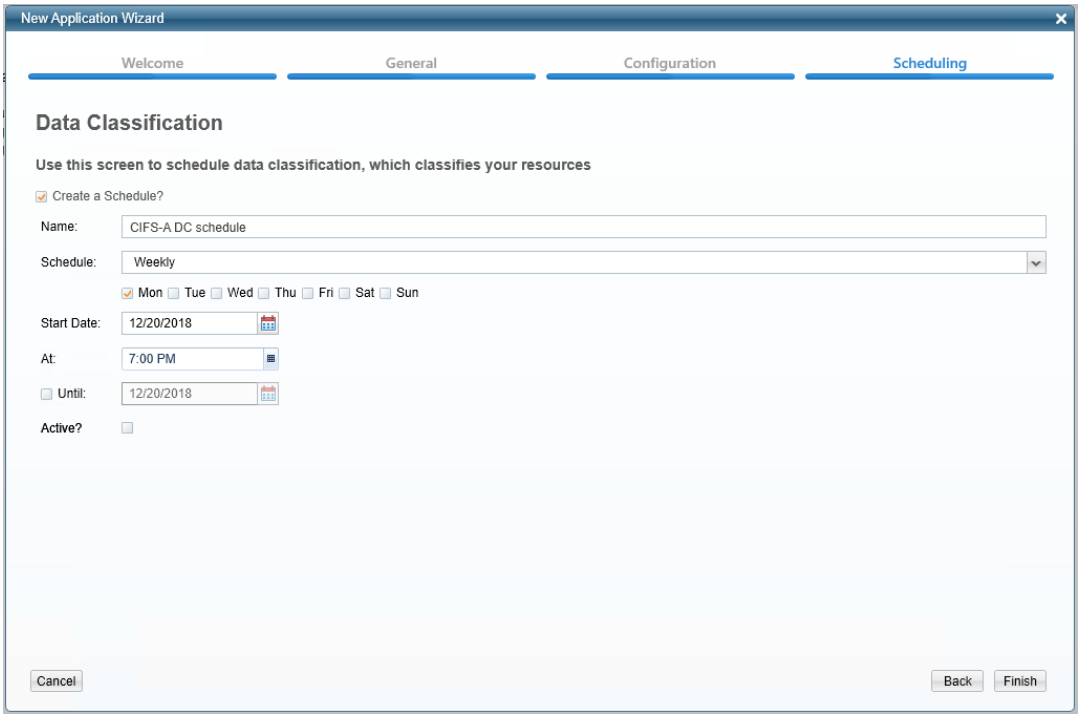

Figure 3. Data Classification Window

28. Check the **Create a Schedule** check box.
29. Type a name for the data classification scheduling task in the *Name* field.
30. Select a scheduling frequency from the **Schedule** dropdown menu.
31. Fill in the relevant date and time fields (which differ, depending upon the scheduling frequency selected).
32. Check the **Active** check box if relevant.

    Note: See the chapter Data Classification of the IdentityIQ File Access Manager Administrator Guide for further information.

33. Click **Finish**.

Chapter 5: Verification

Services

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

- **File Access Manager Central Permissions Collection - <Service_Name>** service is running.
- **File Access Manager Central Data Classification - <Service_Name>** service is running.

Logs

- "%SAILPOINT_HOME_LOGS%\PermissionsCollection_<Service_Name>.log" does not contain errors.
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Service_Name>.log" does not contain errors.

Permissions Collection

1. Run the Crawler and Permissions Collector tasks in the IdentityIQ File Access Manager Admin Client.
2. Verify that:
   - The tasks completed successfully.
   - Business resources were created on the BRs tree.
   - Permissions display in the Permission Forensics window.