

Micro Focus Data Access Governance 3.6 Identity Governance Integration and Administration Guide

December 21, 2017

Legal Notices

Condrey Corporation makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2018 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion with out the express written consent of the publisher.

Condrey Corporation
122 North Laurens St.
Greenville, SC, 29601
U.S.A.
<http://condrey.co>

For information about Micro Focus legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Contents

About This Guide	5
1 Overview	7
1.1 Unstructured Data Repositories	7
1.2 Terminology	7
2 Component Integration	9
2.1 File Reporter Components and Constructs	9
2.2 Identity Governance Components and Constructs	10
3 Conceptual Model	11
3.1 File System Access Permissions in Identity Governance	11
3.2 Virtual Entitlements	12
4 Requirements	13
4.1 Identity Governance 3.5	13
4.2 File Reporter 3.6	13
4.3 Licensing	13
4.4 Windows File Systems	13
5 Configuring File Reporter	15
5.1 Managing File Reporter	15
5.2 Updating the License (Conditional)	15
5.3 Performing File System Scans	15
5.3.1 Adding Scan Targets	15
5.3.2 Defining Scan Policies	17
5.3.3 Executing Scans	19
5.3.4 Viewing Scans in Progress	19
5.3.5 View Current Scans List and Scan History	20
5.4 Managing Data Access Governance Target Paths	20
5.4.1 Adding a Target Path	20
5.4.2 Editing a Target Path	21
5.4.3 Deleting a Target Path	21
5.4.4 Processing a Target Path	22
5.4.5 Understanding the Target Path Status Indicators	22
5.5 Reviewing Governance Target Path Data	22
6 Configuring Identity Governance	25
6.1 Managing Identity Governance	25
6.2 Understanding the File System Access Permission Attributes	25
6.3 Configuring Database Connectivity	26
6.3.1 General JDBC Driver Requirements	26
6.3.2 Configuring Data Access Governance for Microsoft SQL Server	26
6.3.3 Configuring Data Access Governance for PostgreSQL	26

6.4	Importing the File System Access Permission Attributes	27
6.5	Importing the File System Access Collector Template	27
6.6	Defining a File System Access Collector	29
7	Collecting and Publishing File System Access Permissions	35
7.1	Manually Collecting and Publishing File System Access Data	35
8	Performing File System Access Reviews	37
8.1	Customizing Review Display Options for File System Access	37
8.2	Defining a File System Access Review	38
8.3	Running a File System Access Review	41
9	Exploring Detailed Access Reports with File Reporter	43
9.1	Reviewing Built-in File System Access Reports in File Reporter	43
9.2	Creating Custom File System Access Reports in File Reporter	43
A	Collection Strategies	45
A.1	Using a Single Collector	45
A.2	Using Multiple Collectors	45
A.2.1	Scoping Collection by Target Path	46
A.2.2	Scoping Collection by Target Path Category	46
B	File Reporter Schema Extensions	49
B.1	Schema Namespace	49
B.2	Tables	49
B.2.1	ig.dag_permission_entries	49
B.2.2	ig.dag_permissions	49
B.2.3	ig.dag_target_paths	50
B.2.4	ig.dag_target_paths_job_queue	51
B.3	Views	51
B.3.1	ig.dag_entitlement_entries	51
B.3.2	ig.dag_entitlements	52
B.3.3	ig.dag_permission_entries_view	52
B.3.4	ig.dag_target_paths_view	53
B.4	Functions	54
B.4.1	ig.dag_get_aggregate_access_string	54

About This Guide

This document is for system administrators needing to provide a Data Access Governance solution for review and certification of users' access to unstructured file system data.

Audience

Administrators should have a working knowledge of application data collection and review processes in NetIQ Identity Governance as well as a basic knowledge of performing file system permissions scans in Micro Focus File Reporter.

Feedback

We want to hear your comments and suggestions about this guide. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Micro Focus Data Access Governance 3.6 Identity Governance Integration and Administration Guide*, visit the [Micro Focus File Reporter web site \(http://www.novell.com/documentation/filereporter3/\)](http://www.novell.com/documentation/filereporter3/).

1 Overview

- ◆ [Section 1.1, “Unstructured Data Repositories,” on page 7](#)
- ◆ [Section 1.2, “Terminology,” on page 7](#)

Micro Focus Data Access Governance 3.6 extends the existing capabilities of NetIQ Identity Governance by providing an integrated solution for the collection, review, and certification of user access in unstructured data repositories.

The Data Access Governance solution is the integration of the following products:

- ◆ NetIQ Identity Governance
- ◆ Micro Focus File Reporter

This integration combines file system security scans in File Reporter with the user access review and certification processes in Identity Governance.

1.1 Unstructured Data Repositories

Unlike structured data repositories (such as databases) that are typically associated with applications, unstructured data is often associated with projects and workgroups alongside application data, but outside the control of the applications themselves. This data may live as files in a network file share, attachments in email, in synchronized cloud-based repositories, or other general document and file repositories both on and off-premises.

This initial Data Access Governance solution targets CIFS-based file shares such as shares on Windows server or Network Attached Storage (NAS) devices, with other targets planned for later releases, including both on-premises and cloud-based data repositories.

1.2 Terminology

In NetIQ Identity Governance, a *permission* represents an application entitlement for review.

In file systems, the word *permission* is sometimes used to describe an access right that an identity (user or group) is granted to a file system resource (file, folder, share), such as Read Access or Write permissions.

To avoid confusion, the terms *access* and *rights* are used in place of *permission* when referring to file system access in Data Access Governance. For example, the Identity Governance collector used with File Reporter is referred to as the File System Access collector.

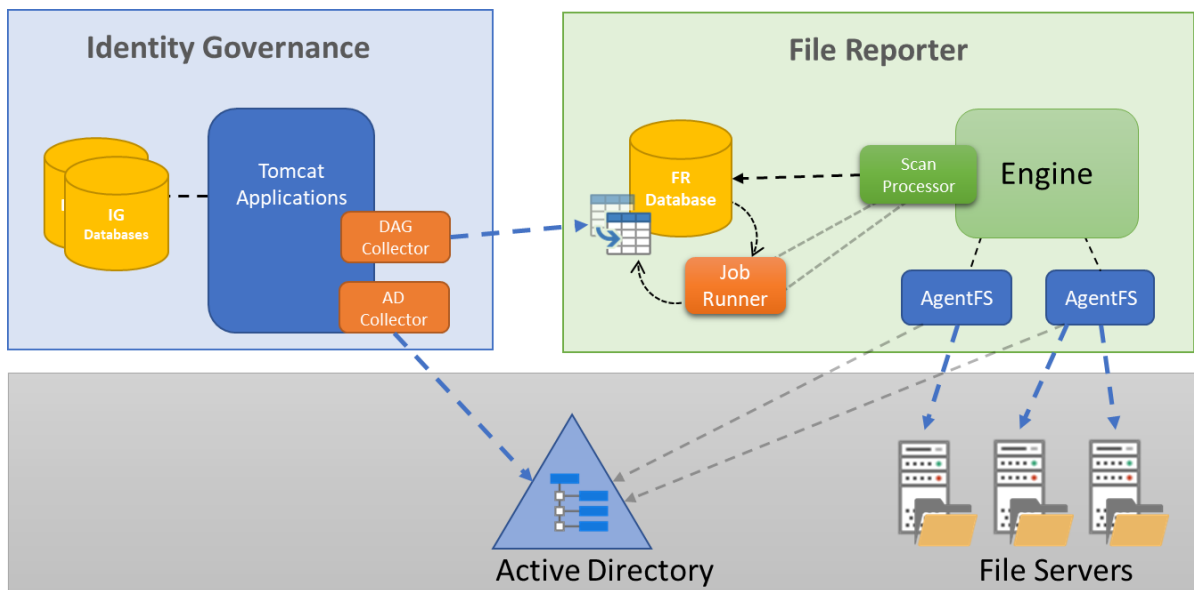
2 Component Integration

- ◆ Section 2.1, “File Reporter Components and Constructs,” on page 9
- ◆ Section 2.2, “Identity Governance Components and Constructs,” on page 10

File Reporter is responsible for the collection and aggregation of file system access data. File system rights summary data is calculated for a set of defined *Target Paths* and stored in tables for use with Identity Governance.

Identity Governance imports this data via a custom *File System Access* collector template. In addition, new Identity Governance *Permission* attributes are defined to assist with the permission definitions and associated metadata for use with reviews.

Figure 2-1 Component Integration



2.1 File Reporter Components and Constructs

Data Access Governance makes use of the following components in File Reporter:

- ◆ **Engine:** The File Reporter Engine coordinates and manages the delegation of file system scans for each scan target based on policy.
- ◆ **Scan Processor:** The Scan Processor imports file system scan data from AgentFS scan agents. In addition, it hosts the Job Runner used to process the aggregated file system access data for use with Identity Governance.
- ◆ **AgentFS:** Scan agents are used to perform the actual collection of file system metadata for selected scan targets.
- ◆ **Database:** The File Reporter database holds all definitions for scan targets, scan policies, as well as the collected file system scan data and aggregated file system access data for Identity Governance.

Data Access Governance also requires a basic understanding of these constructs in File Reporter:

- ♦ **Identity System:** For Data Access Governance, an Active Directory identity system is required. The identity system provides access to the various identities and resources for collection in File Reporter and for association with Identity Governance.
- ♦ **Scan Targets:** Each scan target represents a file share where one or more Data Access Governance Target Paths exist.
- ♦ **Scan Policies:** Scan policies define the type of scan and a schedule for scanning the file system metadata needed for Data Access Governance.

For more detail on the various File Reporter components and constructs please refer to the [Micro Focus File Reporter 3.6 Administration Guide](#).

2.2 Identity Governance Components and Constructs

Data Access Governance uses the following components in Identity Governance:

- ♦ **Identity Governance Tomcat Application:** This is the primary Identity Governance application that provides the management interface along with collection and review of defined identity and application data.
- ♦ **Database:** Identity Governance makes use of its own set of databases for management and storage of collected data.
- ♦ **Collector Templates:** Collector templates provide the interface for collection of data specific to application endpoints. Data Access Governance provides a custom file system access collector template for use with a File Reporter data store.

Data Access Governance also requires an understanding of the following Identity Governance constructs:

- ♦ **Identity Governance Catalog:** The catalog is the set of identities and permissions collected and curated via Identity Governance.
- ♦ **Identity Sources:** These are the sources where identities originate such as Active Directory.
- ♦ **Collectors:** Collectors are configured instances of collector templates defined within an Identity Governance Application or identity source. Collectors are responsible for the retrieval of the actual data in identity and application endpoints.
- ♦ **Applications:** Applications provide context for one or more collectors and generally reference a specific type of endpoint, such as a database or web service.
- ♦ **Permissions:** a permission in Identity Governance is like an entitlement as defined in Identity Manager and defines a resource right held by one or more identities. Each permission may have metadata attributes associated with it. Data Access Governance provides a set of custom Permission Attributes for use with the file system access collector template.

3 Conceptual Model

3.1 File System Access Permissions in Identity Governance

For each Target Path defined in File Reporter, the Identity Governance File System access collector provides three permissions:

- ♦ [Target Path] - Read Access
- ♦ [Target Path] - Write Access
- ♦ [Target Path] - Full Control

The following table shows the mapping of specific NTFS access mask flags to a corresponding generic file system access right for use with Data Access Governance.

NTFS Access Mask Flag	Data Access Governance File System Access
List Folder / Read Data	Read
Read Attributes	Read
Read Extended Attributes	Read
Read Permissions	Read
Create Files / Write Data	Write
Create Folders / Append Data	Write
Write Attributes	Write
Write Extended Attributes	Write
Delete Subfolders and Files	Write
Delete	Write
Change Permissions	Change Permissions
Take Ownership	Change Permissions
Traverse Folder / Execute File	-
Synchronize	-

3.2 Virtual Entitlements

Identity Governance Permissions are like Identity Manager's concept of Entitlements. As such, the review process for these entitlements are binary – “yes,” the user should have the Permission (Entitlement) or “no,” the user should not. These entitlements are not the actual rights to resources themselves, but rather a group or role which is directly assigned a set of rights for a resource represented by the entitlement.

File system rights are not intrinsically as simple:

- ◆ Different rights might exist for the same user on different folders in the hierarchy.
- ◆ The number of discrete file system rights and the combination of those rights for a given file or folder can be rather extensive.
- ◆ The exact meaning of many file system rights is too in-depth for a business-level review.

To map these low-level file system rights to identities, and not just groups, roles, or entitlements, we need a way to model those rights as an entitlement construct. Data Access Governance aggregates any assigned file access rights in the Target Path's hierarchy into a single set of projected or “virtual” entitlements represented at the Target Path level. These virtual entitlements are displayed as Permissions in an Identity Governance review providing a simple binary approval process for Read, Write and Change Permissions access for each defined Target Path.

4 Requirements

4.1 Identity Governance 3.5

For requirements related to Identity Governance 3.5 see the [NetIQ Identity Governance User Guide \(https://www.netiq.com/documentation/identity-governance-35/user-guide/data/front.html\)](https://www.netiq.com/documentation/identity-governance-35/user-guide/data/front.html).

4.2 File Reporter 3.6

For requirements related to File Reporter 3.6 see the [Micro Focus File Reporter 3.6 Installation Guide](#).

4.3 Licensing

Licensing for Data Access Governance integration is included with the base products.

NOTE: File Reporter 3.6 is licensed as a maintenance update under the File Reporter 3.5 license scheme. An updated license might be required however to enable Data Access Governance features. Current File Reporter customers with active maintenance are eligible for this updated license at no additional cost. To obtain an updated license visit the [Micro Focus Customer Center \(https://www.novell.com/cchelp/\)](https://www.novell.com/cchelp/).

4.4 Windows File Systems

Data Access Governance 3.6 provides support for the collection and review of summarized file system permissions in Windows file systems. General requirements for Windows file system repositories include:

- ◆ File servers running Windows 2008 R2 or later
- ◆ File servers joined to an Active Directory domain
- ◆ Network Attached Storage (NAS) devices joined to an Active Directory domain
- ◆ Target folders located on an NTFS or ReFS file system or a CIFS share using NTFS-compatible security

For other requirements specific to Windows file system scans, see the [Micro Focus File Reporter 3.6 Administration Guide](#).

5 Configuring File Reporter

5.1 Managing File Reporter

You will need to access the File Reporter administrative web interface to set up and manage the various aspects of Data Access Governance Target Paths. Using a supported web browser, enter the address for File Reporter and when prompted, log in to the web application using an account that is a member of the File Reporter Administrators group (typically SrsAdmins) in Active Directory.

For details on accessing and authenticating to the File Reporter web interface, see [Launching the Administrative Interface](#) in the *Micro Focus File Reporter 3.6 Administration Guide*.

5.2 Updating the License (Conditional)

If you are upgrading from File Reporter 3.5, you will need an updated license to enable the Data Access Governance features. See [Section 4.3, “Licensing,” on page 13](#) and [Licensing the Product](#) in the *Micro Focus File Reporter 3.6 Installation Guide* for details on obtaining and installing this license.

5.3 Performing File System Scans

Data Access Governance relies on data from file system scans in File Reporter to define Target Paths and to process the aggregated file system access data.

Preparing File Reporter for Data Access Governance Target Paths management and processing includes:

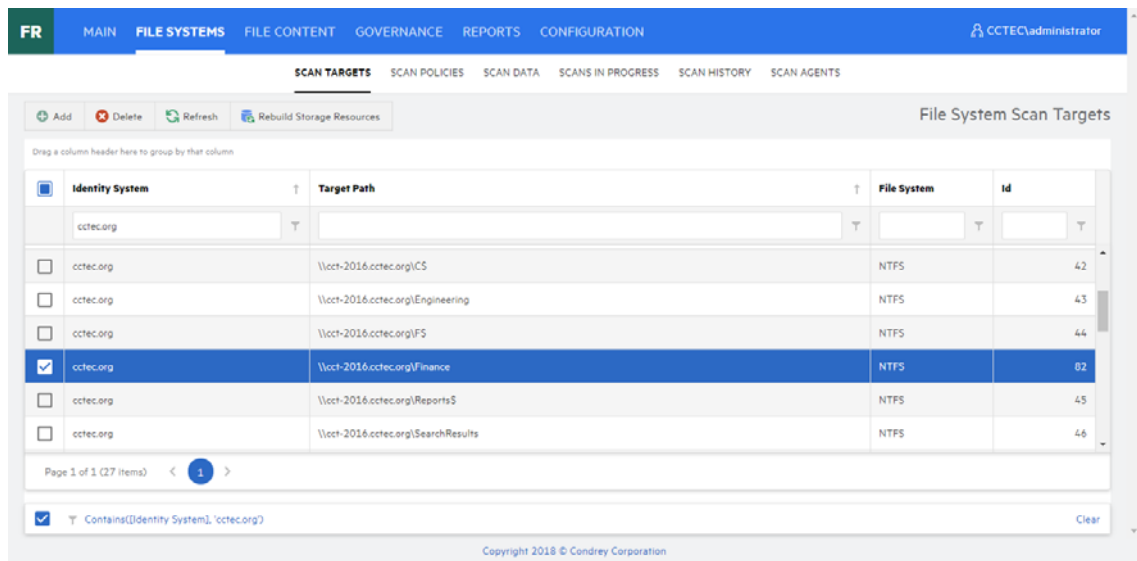
1. Adding required scan targets.
2. Defining appropriate scan policies.
3. Executing scans based on those scan policies.

Details on each of these steps can be found in the [tMicro Focus File Reporter 3.6 Administration Guide](#).

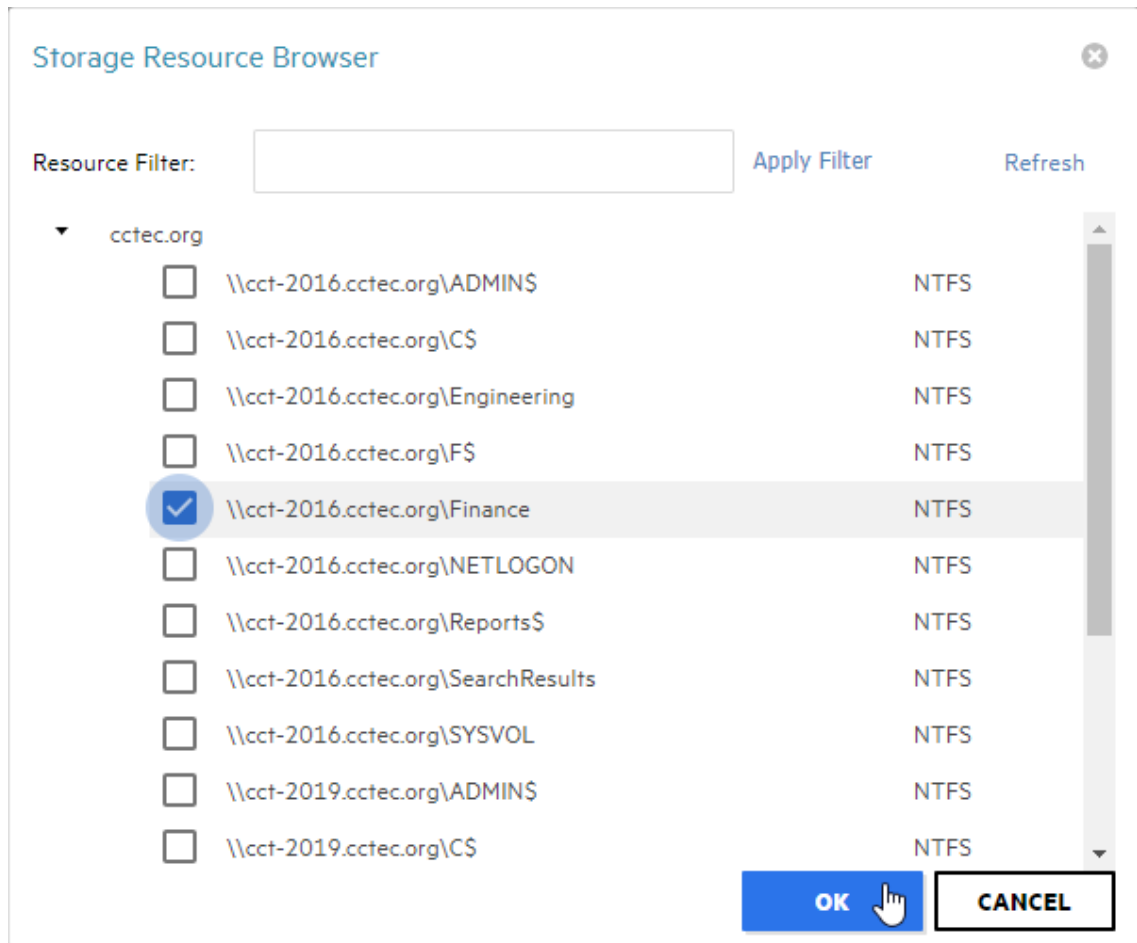
The following sections provide a quick-setup guide to configure File Reporter for Data Access Governance.

5.3.1 Adding Scan Targets

- 1 In the File Reporter web application, select **File Systems > Scan Targets**.



2 Click Add to display the Storage Resource Browser.



3 Select the Windows file shares to add as scan targets.

Each file share containing a Target Path for Data Access Governance should be added to File Reporter's scan targets list.

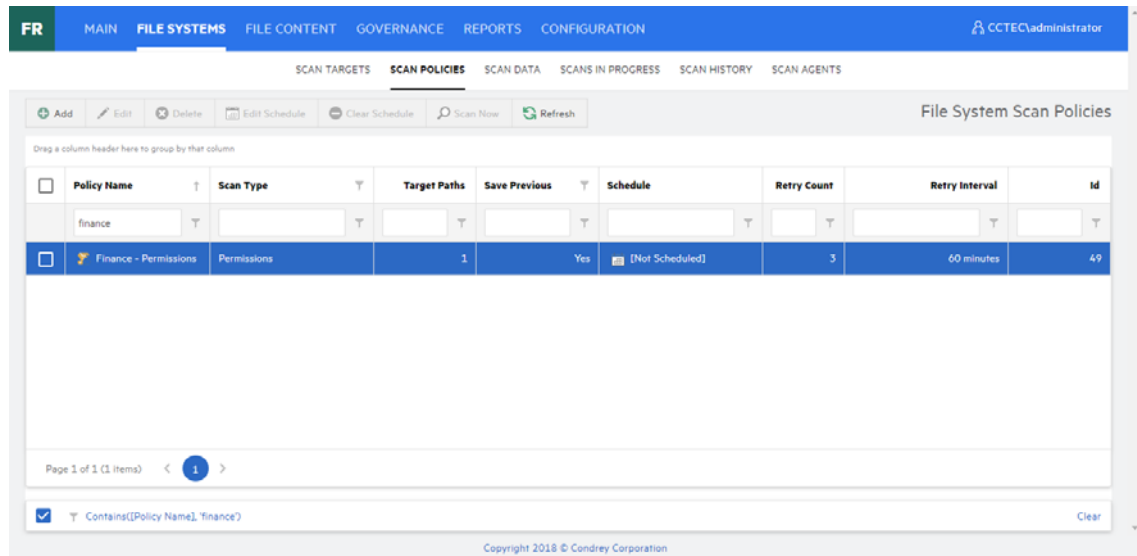
File system scans are performed for an entire share, but any path under the share may later be defined for Data Access Governance review.

If you do not see a file share you are looking for, you might need to perform a Rebuild Storage Resources operation or verify File Reporter proxy user rights. For details, refer to the [Micro Focus File Reporter 3.6 Administration Guide](#).

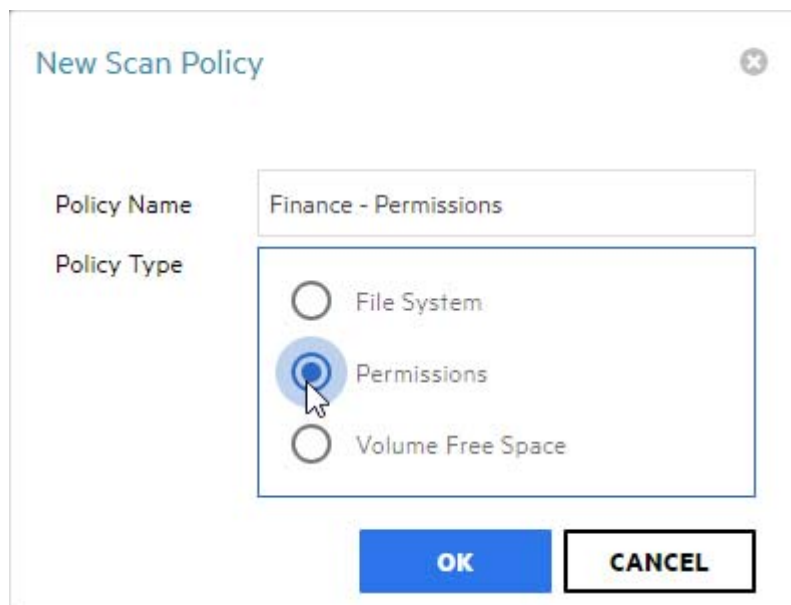
- 4 Click **OK** to add the selected file shares to the list of scan targets.

5.3.2 Defining Scan Policies

- 1 In the File Reporter web application, select **File Systems > Scan Policies**.



- 2 Click **Add** to display the New Scan Policy dialog.



- 3 Fill in the required fields.
 - ♦ **Policy Name:** Provide a name for the scan policy.

- ◆ **Policy Type:** Select **Permissions** to configure the scan policy for collecting file system access data.

4 Click **OK** to save the scan policy and display the Scan Policy Editor dialog.

Scan Policy Editor

Name: Finance - Permissions

Description: Enter a policy description

Retry Count: 3

Retry Interval: 60 Minutes

Previous Scans: Save Previous Scan

Add Remove

	Target Path
<input type="checkbox"/>	\\cct-2016.cctec.org\Finance

OK CANCEL

5 Complete the fields:

- ◆ **Name:** Optionally change the name of the scan policy.
- ◆ **Description:** Provide an optional description for the scan policy.
- ◆ **Retry Count:** Specify the number of times to retry on scan failure.
- ◆ **Retry Interval:** Specify the time to wait between retries.
- ◆ **Previous Scans:** Check to save the previous scan when a new scan completes.

6 In the **Target Path** list, click **Add** to display the Scan Target Browser dialog.

Scan Target Browser ✕

	Identity System	Target Path
	<input type="text"/>	finance
<input checked="" type="checkbox"/>	cctec.org	\\cct-2016.cctec.org\Finance

- 7 Select each scan target to scan in the list.
- 8 Click **OK** to save the list of scan targets.
- 9 Click **OK** to save the scan policy.

5.3.3 Executing Scans

- 1 In the File Reporter web application, select **File Systems > Scan Policies**.
- 2 Select each scan policy you want to execute.
- 3 Click **Scan Now**.
- 4 Click **Yes** in the confirmation dialog to start the scans.

5.3.4 Viewing Scans in Progress

- 1 In the File Reporter web application, select **File Systems > Scans in Progress**.
- 2 View the progress and status for each scan in progress.
- 3 Click **Refresh** to see any updated status.

5.3.5 View Current Scans List and Scan History

- 1 In the File Reporter web application, select **File Systems > Scan Data**.
- 2 View the status and job details of the completed scans.
- 3 (Optional) Select **File Systems > Scan History** to see the history of all scan jobs (both completed and failed).

5.4 Managing Data Access Governance Target Paths

In the File Reporter web application, **Select Governance > Target Paths**.

FR MAIN FILE SYSTEMS FILE CONTENT GOVERNANCE REPORTS CONFIGURATION CCTEC\Administrator

TARGET PATHS TARGET PATH DATA

Add Edit Delete Process Refresh Data Access Governance Target Paths

Drag a column header here to group by that column

Status	Target Path	Process on Scan	Category	Identities	Last Processed Scan	ID
<input checked="" type="checkbox"/> Queued [Cancel]	\\cct-2012.cctec.org\Engineering	<input type="checkbox"/>	Engineering	2	2018-11-29 14:00:00 ID: 984	10
<input type="checkbox"/> Processing [Cancel]	\\cct-2016.cctec.org\Engineering	<input type="checkbox"/>	Engineering	11,297	2018-11-29 14:00:00 ID: 983	6
<input type="checkbox"/> Processed	\\cct-2016.cctec.org\Finance	<input type="checkbox"/>	Financial	3	2018-11-29 11:36:51 ID: 978	7

Copyright 2018 © Condrey Corporation

5.4.1 Adding a Target Path

- 1 In the File Reporter web application, select **Governance > Target Paths**.
- 2 In the Target Paths page, click **Add**.

3 In the Target Path Editor dialog, specify the details for the Target Path.

- ◆ **Target Path:** Click **Browse** and from the Target Path Browser, select a folder.
- ◆ **Process on Scan:** Select this option to automatically process this Target Path whenever new scan data is collected.
 Selecting this option will automatically start a job for this Target Path if unprocessed scan data is available when you save this entry.
- ◆ **Category:** (Optional) Category name for use with filtering and review processes in Identity Governance. This field maps to the file system category permission attribute in Identity Governance.
- ◆ **Description:** (Optional) Description for this Target Path. This description maps to the permission description attribute in Identity Governance.

5.4.2 Editing a Target Path

- 1 In the File Reporter web application, select **Governance > Target Paths**.
- 2 Double-click the Target Path to edit or select the checkbox in the **Target Path** row and click **Edit** in the menu.

The same options apply as in [Section 5.4.1, “Adding a Target Path,” on page 20](#) with the notable exception that once a Target Path entry has been added, the Target Path itself is read-only.

To modify the Target Path itself, you will need to delete the current Target Path entry then add a new one.

5.4.3 Deleting a Target Path

- 1 In the File Reporter web application, select **Governance > Target Paths**.
- 2 Select each Target Path in the list you want to delete.
- 3 Click **Delete**.

- 4 Review the confirmation dialog, then click **Delete**.

Performing a delete for a Target Path places a `delete` entry in the Scan Processor's Job Runner queue. The Target Path entries will show as `Marked for Delete` until the Job Runner processes the action.

5.4.4 Processing a Target Path








Target Paths that are configured for Process on Scan will automatically process the Target Path when new scan data is available.

To manually start processing a Target Path's file system access data:

- 1 In the File Reporter web application, select **Governance > Target Paths**.
- 2 Select each Target Path in the list you want to process.
- 3 Click **Process**.
- 4 Review the confirmation dialog then click **Yes** to start processing.

5.4.5 Understanding the Target Path Status Indicators

Status indicators for a Target Path specify the current state of processing, and whether any new scan data is available for processing.

Icon	Status	Description
	Scan Data Available	New scan data is available for this Target Path but has not yet been processed.
	New Scan Pending	A file system scan was recently imported, but post-import processing such as group membership calculations are in progress.
	Queued	The Target Path has been queued for processing file system access data for associated identities.
	Processing	Calculation of file system access data is currently in progress for identities on the Target Path.
	Processed	The latest scan data for this Target Path has been fully processed for collection and review.
	Marked for Delete	The Target Path has been marked for delete. No further actions can be taken against this Target Path.
	Scan Incomplete	The current scan data for this Target Path is missing or invalid.

5.5 Reviewing Governance Target Path Data

To review the processed file system access summary data, in the File Reporter administration web application, from the **Governance** tab, click **Target Path Data**.

FR MAIN FILE SYSTEMS FILE CONTENT GOVERNANCE REPORTS CONFIGURATION CCTEC\administrator

TARGET PATHS TARGET PATH DATA

Refresh Target Path Permissions Data

Target Path ↑ ▾

Trustee	Access	Category	
Target Path: \\cct-2016.cctec.org\Finance (3)			
▾ CCTEC\alice	Read, Write, Change Permissions	Financial	
Record ID: 63927 Associated Scan ID: 978			
Trustee:		Permissions	
SAM Account: CCTEC\alice		Read, Write, Change Permissions	
FDN: CN=Alice Donovan,OU=Employees,DC=cctec,DC=org			
GUID: a34281bb-51bc-4f46-aa2d-a593667038f4			
SID: S-1-5-21-2842228899-2166691306-2690483865-4117			
> CCTEC\bob	Read	Financial	
> CCTEC\johnson	Read	Financial	

Copyright 2018 © Condrey Corporation

This page presents a view of the data to be collected by Identity Governance.

To see the identities associated with a given Target Path, click the arrow next to the entry in the grid or double-click the Target Path row.

To see the detail data for a given identity, click the arrow next to the user entry, or double-click the user entry row.

6 Configuring Identity Governance

6.1 Managing Identity Governance

Performing tasks in Identity Governance requires logging in with an account that has the appropriate authorization assignments.

Identity Governance provides multiple levels of delegation for the tasks defined in this guide, such as Global Administrator, Data Administrator, and Review Administrator.

For details on setting up the required access to each of the tasks defined in this section, see Adding Identity Governance Users and Assigning Authorizations in the [NetIQ Identity Governance 3.5 User Guide](https://www.netiq.com/documentation/identity-governance-35/user-guide/data/front.html) (<https://www.netiq.com/documentation/identity-governance-35/user-guide/data/front.html>).

6.2 Understanding the File System Access Permission Attributes

The file system access collector template requires the following Permission Attributes.

Display Name	Attribute Key	Data Type	Description
File System Access	<code>ext_fileSystemAccess</code>	string (255)	Access rights string having one of the following values: <ul style="list-style-type: none">◆ Read◆ Write◆ Change Permissions
File System Path	<code>ext_fileSystemPath</code>	string (2000)	Target Path in UNC format such as <code>\\cct-2016.cctec.org\Finance</code>
File System Category	<code>ext_fileSystemCategory</code>	string (255)	Optional category name for organization and grouping purposes. NOTE: This attribute is unrelated to Categories in Identity Governance.

Each of these attributes play a role in providing organization, filter criteria, and key metadata for use with reviews in Identity Governance.

6.3 Configuring Database Connectivity

File System Access data is retrieved from the File Reporter database using an SQL connection provided by a JDBC driver. Depending on the current configuration of Identity Governance, an additional JDBC driver file might be required in the Identity Governance Application Server class path.

If Identity Governance and File Reporter are configured for the same type of database (for example, both are configured for PostgreSQL), then no further configuration of JDBC drivers is required, and you can continue with configuration of the File System Access Collector.

However, if both systems are running with different database types (for example, Identity Governance is configured for PostgreSQL and File Reporter is configured for Microsoft SQL Server), then an additional JDBC driver might be required.

6.3.1 General JDBC Driver Requirements

Identity Governance 3.5 runs with Java 8. Any additional JDBC drivers installed must be:

- ◆ Compiled for Java 8
- ◆ Built for the JDBC 4.2 specification

6.3.2 Configuring Data Access Governance for Microsoft SQL Server

If Identity Governance is configured for Microsoft SQL Server, no other JDBC dependencies are needed.

To install the Microsoft SQL Server JDBC driver:

- 1 Download an appropriate driver from Microsoft.

For a list of supported drivers and databases, see <https://docs.microsoft.com/en-us/sql/connect/jdbc/microsoft-jdbc-driver-for-sql-server-support-matrix?view=sql-server-2016>.

Generally, you should install the latest version that supports Java 8 with JDBC 4.2.

- 2 Extract the driver file from the archive, paying attention to find the one built for Java 8.
- 3 Copy the JDBC driver to the Identity Governance application server's `lib` folder.

For installations on Linux, this is in a folder such as `/opt/netiq/idm/apps/tomcat/lib`.

For installations on Windows, this is in a folder such as `C:\netiq\idm\apps\tomcat\lib`.

- 4 Restart the Identity Governance Tomcat service.

For example, with the Microsoft JDBC driver 7.0 archive `sqljdbc_7.0.0.0_enu.tar.gz`, copy the included file from `sqljdbc_7.0/enu/mssql-jdbc-7.0.0.jre8.jar` to the application folder listed above, then restart Tomcat.

6.3.3 Configuring Data Access Governance for PostgreSQL

If Identity Governance is configured for PostgreSQL, no other JDBC dependencies are needed.

To install the PostgreSQL JDBC driver:

- 1 Download an appropriate driver for PostgreSQL.

For a list of supported drivers see <https://jdbc.postgresql.org/about/about.html> and <https://jdbc.postgresql.org/download.html>.

Generally, you should install the latest version supports Java 8 with JDBC 4.2.

- 2 Copy the JDBC driver to the Identity Governance application server's lib folder.

For installations on Linux, this is in a folder such as `/opt/netiq/idm/apps/tomcat/lib`.

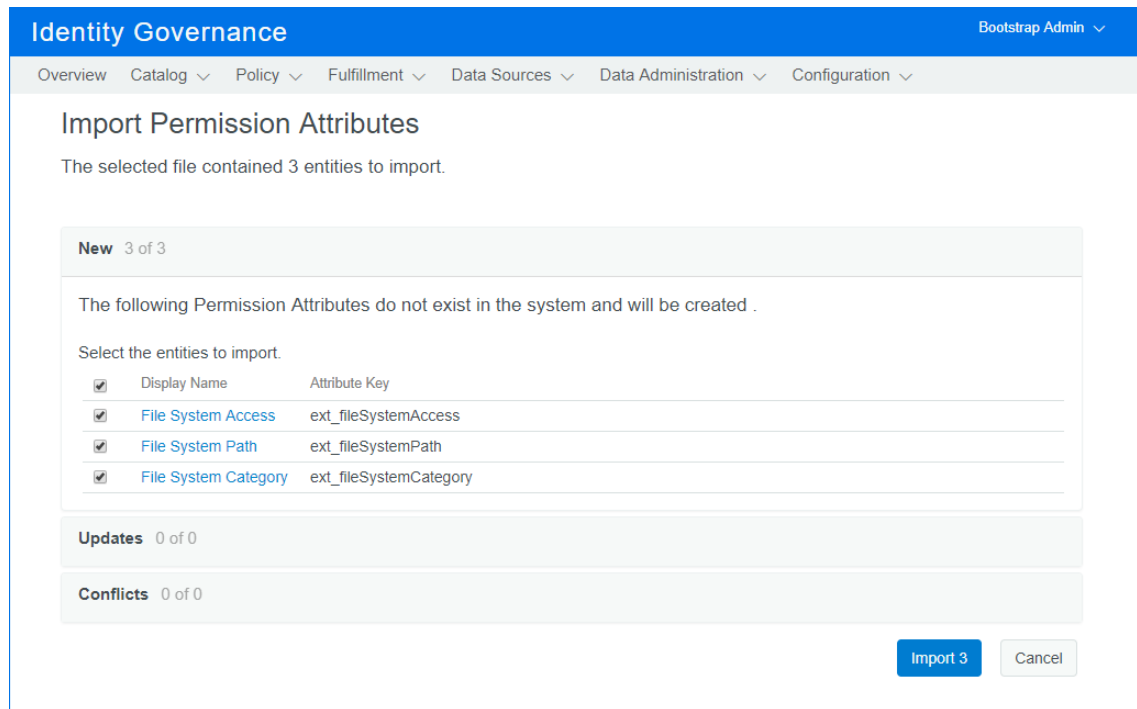
For installations on Windows, this is in a folder such as `C:\netiq\idm\apps\tomcat\lib`.

- 3 Restart the Identity Governance Tomcat service.

For example, download the PostgreSQL JDBC driver file `postgresql-42.2.5.jar` and copy it to the application folder listed above, then restart Tomcat.

6.4 Importing the File System Access Permission Attributes

- 1 In Identity Governance select **Data Administration** > **Permission Attributes**.
- 2 Click the **Import Attributes** link at the top of the page.
- 3 In the Open File dialog, select the `FileSystemAccess-Permission-Attributes.json` file included in the `DAG` folder of the File Reporter ISO.



- 4 Review the attributes to import, then click **Import**.

6.5 Importing the File System Access Collector Template

- 1 Verify that the required Permission Attributes have been imported.

For details, see [Section 6.4, “Importing the File System Access Permission Attributes,”](#) on [page 27](#).

- 2 In Identity Governance, select **Configuration > Application Source Collector Templates**.
- 3 In the **Application Source Collector Templates** section click **+** to display the Add new collector template dialog.

Add new collector template [X]

Template name
File System Access

Description
Permission collector template for File System Access via File Reporter


Type
Permission ▾

JSON file
Choose File FileSystemAc...mplate.json

Save Cancel

- 4 Fill in the criteria for this template:
 - ◆ **Template Name:** Provide a name for this template. For example, `File System Access`.
 - ◆ **Description:** Provide an optional description for this template.
 - ◆ **Type:** Select **Permission** as the type.
 - ◆ **JSON file:** Click **Choose File** then select the `FileSystemAccess-Collector-Template.json` file included in the `DAG` folder of the File Reporter ISO.

5 Click **Save** to save the template.

Application Source Collector Templates	
These JSON text files are templates for creating new application source collectors. Select the filename to view details or use the select boxes and action menu to download the template. Add a customized JSON file as a new template.	
Actions ▾ +	
<input type="checkbox"/> Name ^	Description
<input type="checkbox"/> AD Account	Account collector template for Active Directory
<input type="checkbox"/> AD Permission	Permission collector template for Active Directory
<input type="checkbox"/> CSV Account	Account collector template for delimited text file
<input type="checkbox"/> CSV Permission	Permission collector template for delimited text file
<input type="checkbox"/> * File System Access 	Permission collector template for File System Access via File Reporter
<input type="checkbox"/> Identity Manager AE Permission	Permission collector template for NetIQ IDM Advanced Edition
<input type="checkbox"/> JDBC Account (DB2)	Account collector template for DB2 JDBC Driver

6.6 Defining a File System Access Collector

A File System Access collector may be added to a new or existing Identity Governance Application.

To add the collector to a new Application:

- 1 In Identity Governance, select **Data Sources > Applications**.
- 2 Click **+** to add a new Application source.
- 3 In the New Application Source form, complete the following fields:
 - ♦ **Name:** Provide a name for this Application. For example, `File System Access Data`.
 - ♦ **Description:** (Optional) Provide a description for this Application.
- 4 Select **New Application Source > New Collector**.

File System Access Collector ⓘ
This data will be collected ▼

File System Access Collector

Collector name

File System Access Collector
✔

Collector template

File System Access
▼

Collect this data?

Yes

Service Parameters ⓘ

Collect Permission ✔ This data will be collected

Collect Permission to Holders ✔ This data will be collected

5 Complete the following fields:

- ◆ **Collector name:** Provide a name for the collector. For example, `File System Access Collector`.
- ◆ **Collector template:** Select **File System Access** from the drop-down list.
- ◆ **Collect this data:** Select **Yes**.

6 Click **Service Parameters**.

Service Parameters ✔

Database Type

Host Server
 ✔

Host Server Port
 ✔

Database Instance Name
 ✔

User Name
 ✔

Password
 ✔

7 Complete the following fields:

- ◆ **Database Type:** Select the database type of SQL Server or PostgreSQL used with your File Reporter installation.
- ◆ **Host Server:** Enter the IP address or hostname for the File Reporter database.
- ◆ **Host Server Port:** Enter the TCP port for the File Reporter database.
- ◆ **Database Instance Name:** Enter the name of the File Reporter database instance.
This will typically be `srssdb`.
- ◆ **User Name:** Enter the name of a database user with read access to the File Reporter scan data.
You can use the File Reporter Report user (typically `srsreport_user`) or any other database account in the File Reporter Database Report Role (typically `srsreport_role`).
- ◆ **Password:** Enter the password for the database user.
- ◆ **Batch Collection Session Timeout:** Enter the number of seconds before an idle batch collection session times out.
The default setting is 60 seconds.

8 Click **Test connection** to verify the database connection parameters.

9 Click **Collect Permission**.

Collect Permission ✔
This data will be collected

Permission Query

✔

Collect Permission attributes **Mapped attribute**

Permission ID from Source {}

Permission Name {}

Permission Description {}

File System Access {}

File System Category {}

File System Path {}

10 Complete the following fields:

- ◆ **Permission Query:** Use the provided SQL query for collecting File System Access Permissions from File Reporter.
- ◆ **Permission ID from Source:** Use the provided value `entitlement_id`.
- ◆ **Permission Name:** Use the provided value `entitlement`.
- ◆ **Permission Description:** Use the provided value `description`.
- ◆ **File System Access:** Use the provided value `permission`.
- ◆ **File System Category:** Use the provided value `category`.
- ◆ **File System Path:** Use the provided value `target_path`.

11 Click **Collect Permission to Holders Attribute**.

Collect Permission to Holders ✔
This data will be collected

Collect this data? Yes

Permissions to Holders Query ✔

Collect Permission to Holders attributes **Mapped attribute**

Permission ID(s) from Source {}

Permission Account or User Mapping {}

This attribute is used to join permissions to a specific account or identity in the Identity Governance system. Specify the attribute this value should match to associate this permission to an identity or account. For example, if each permission record contained the ID of the identity with that permission then you would select the User ID from Source in this field.

This mapping is used for all of the collectors in this Application Source.

Map to attribute

12 Complete the following fields:

- ◆ **Collect this data:** Select **Yes**.
- ◆ **Permissions to Holders Query:** Use the provided SQL query.
- ◆ **Permission ID(s) from Source:** Use the provided value `entitlement_id`.
- ◆ **Permission Account or User Mapping:** Use one of the following mappings:

Use this value...	to map to this Permissions to Holders attribute
<code>trustee_guid</code>	Object GUID
<code>trustee_fdn</code>	User ID from Source or any Identity attribute mapped to the <code>distinguishedName</code> attribute in Active Directory.
<code>trustee_sid</code>	Custom Identity attribute mapped to <code>objectSid</code> in Active Directory.

7 Collecting and Publishing File System Access Permissions

Staging File System Access Permissions for review requires collecting and then publishing the associated data.

7.1 Manually Collecting and Publishing File System Access Data

- 1 In Identity Governance, select **Data Sources** > **Application Sources**.

- 2 Click the **Collect Now**  link for an Application configured to collect File System Access Permissions from File Reporter.

- 3 Once collection is complete, click the **Publish Now**  link for the Application.

For more details on the collection process and scheduling options refer to the [NetIQ Identity Governance 3.5 User Guide \(https://www.netiq.com/documentation/identity-governance-35/user-guide/data/front.html\)](https://www.netiq.com/documentation/identity-governance-35/user-guide/data/front.html).

8 Performing File System Access Reviews

Once you have successfully collected and published relevant File System Access data from File Reporter, you are ready to set up and perform reviews in Identity Governance.

8.1 Customizing Review Display Options for File System Access

File System Access Permissions make use of the following custom Permission Attributes:

- **File System Access:** One of Read, Write, or Change Permissions
- **File System Path:** Target Path in UNC format
- **File System Category:** (Optional) Category specified in File Reporter for the Target Path

Each of these attributes are initially configured for use in reviews and searches.

To include these attributes in review display data, configure the display options for reviews:

- 1 In Identity Governance, select **Configuration > Review Display Customization**.

The screenshot shows the 'Review Display Customization' interface for 'User Access Review'. The page title is 'Review Display Customization' and the subtitle is 'Select default columns for reviewers per review type.' The main heading is 'User Access Review' with a checkmark icon. Below this, there are two panels: 'Selected Columns' and 'Available Columns'. The 'Selected Columns' panel contains buttons for 'Type', 'Review Item', 'User', 'Action*', 'Activity*', 'File System Path', and 'File System Category'. The 'Available Columns' panel contains a list of buttons: 'Account Description', 'Account Disabled', 'Last Login Date', 'Privileged Account', 'Account Risk', 'Account State', 'Account Type', 'Permission Cost', 'Permission Description', 'Permission Risk', 'Permission Type', and 'Permission Value'. A mouse cursor is hovering over the 'File System Access' button in the 'Available Columns' panel. Below the panels, there is a note: 'Drag-and-drop to rearrange, add, or remove columns. Columns with a * are required. Available attributes are single valued with limited data types. Selected attributes appear in reviewer list options. To show attributes in expanded details, set quick info in the Attributes area.'


- 2 In the **User Access Review** section, select attributes from the **Available Columns** list and drag them to the **Selected Columns** panel.

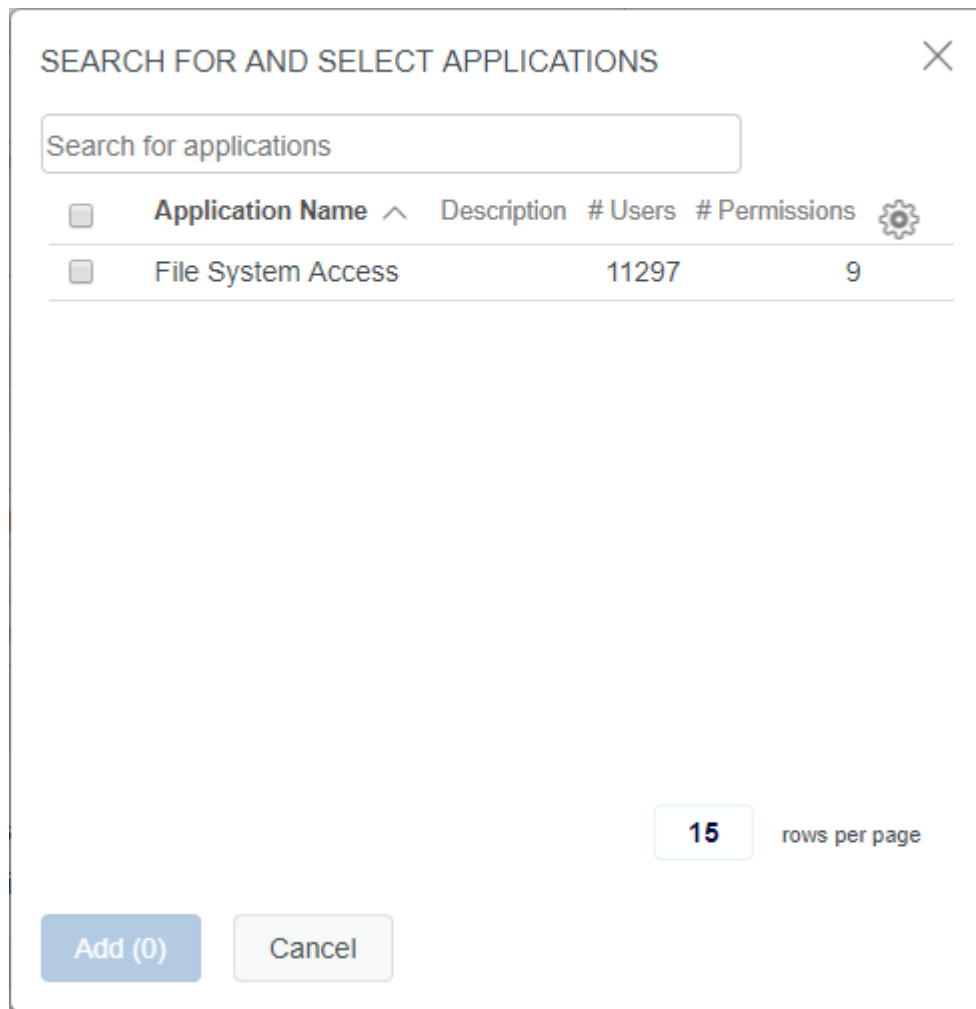
- 3 Click **Save**  to commit the changes.

8.2 Defining a File System Access Review

- 1 Authenticate to Identity Governance with an account having Review Administrator access.
- 2 In Identity Governance, select **Reviews > Definitions**.
- 3 Click **+** to add a new Review Definition.

The screenshot shows the 'New Review Definition' form in Identity Governance. The form is titled 'Review Definitions' and 'New Review Definition'. It contains four fields: 'Review type' (User Access Review), 'Name' (Finance File System Access Review), 'Description' (Reviews access to various file shares and folders for the Finance department), and 'Review instructions' (Review the file system access identified for each user and target path).


- 4 Complete the following general fields:
 - ♦ **Review type:** Select **User Access Review** from the drop-down list.
 - ♦ **Name:** Provide a name. For example, `Finance File System Access Review`.
 - ♦ **Description:** (Optional) Provide a description for this review.
 - ♦ **Review instructions:** (Optional) Provide any instructions for this review.
- 5 Set the scope and filter for **User Access Review** items as needed.
 - 5a **Select Applications:** Select the applications containing the File System Access collectors of interest for review.
 - 5b Click **Search**  to display the Search for and Select Applications dialog.

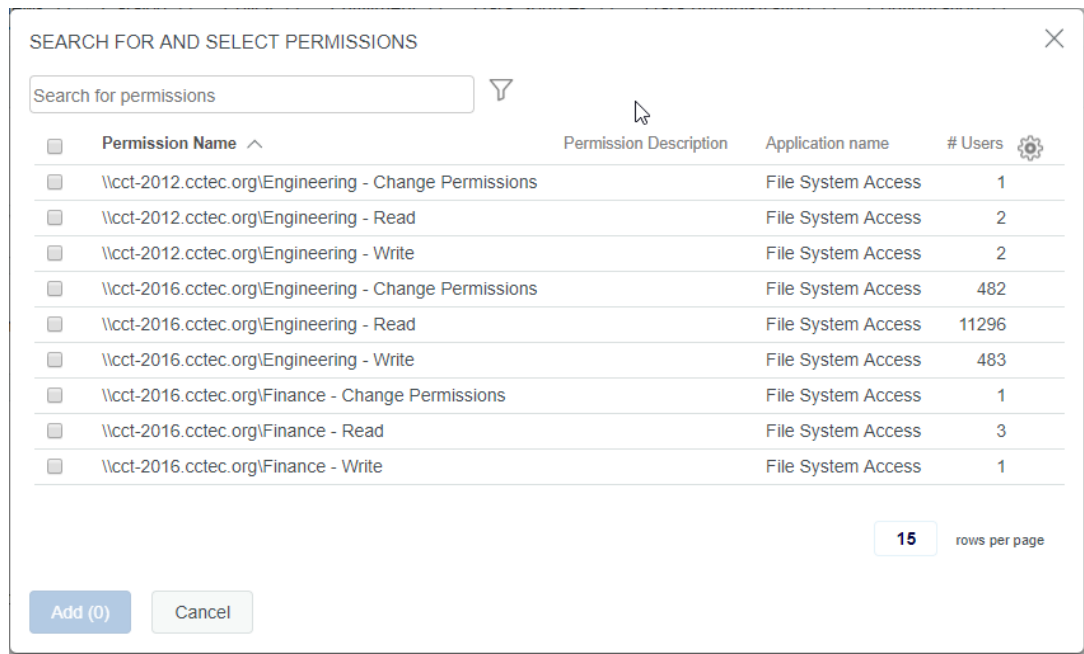


5c Select one or more applications from the list then click **Add**.

5d Select Permissions: Select this option to specify which permissions to review.

To select specific permissions:

Click **Search**  to display the Search for and Select Permissions dialog.



5e Select one or more permissions from the list, then click **Add**.

5f To filter by Permission Attributes, select **any** or **all** for the **permissions that match** criteria,

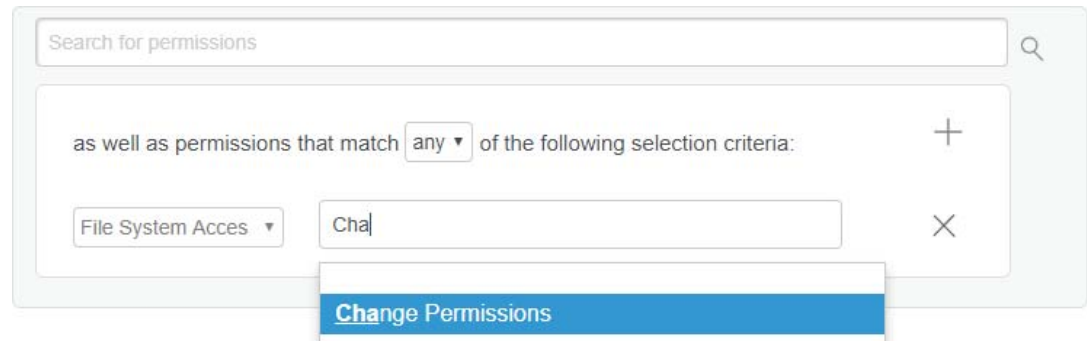
then click **Add Condition** .

5g In the drop-down list, select from any of the Permission Attributes, including the custom attributes defined for File System Access.



5h For the custom attributes, start typing in the **Search for catalog attribute value** text box to find available values.

For example, if the **File System Access** attribute is selected, start typing **change** to see the value **Change Permissions**, then press **Enter** to select it.



- 6 Specify other desired criteria for the Review Definition, such as **Reviewers**, **Review Options**, and **Default Reviewer Display Preferences**.

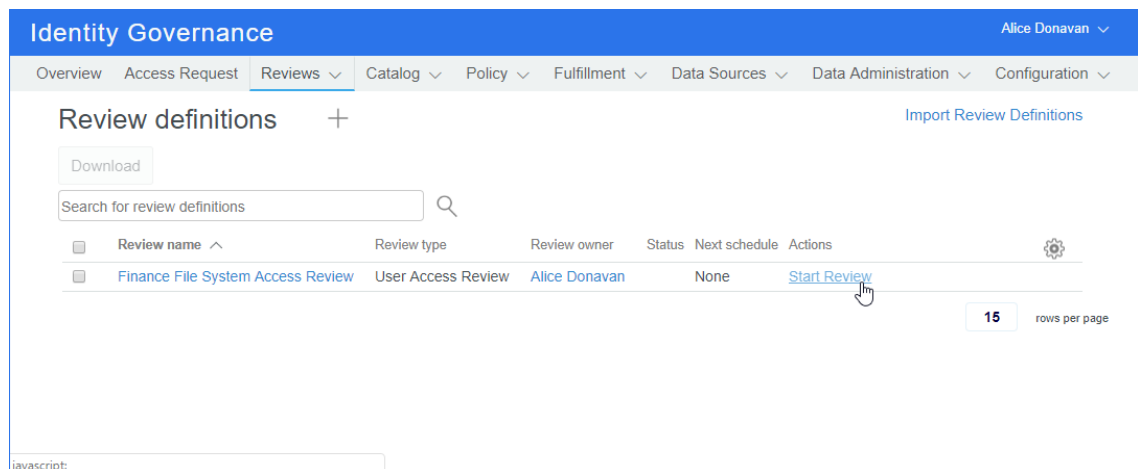


- 7 Click **Save** to commit the changes for the Review Definition.

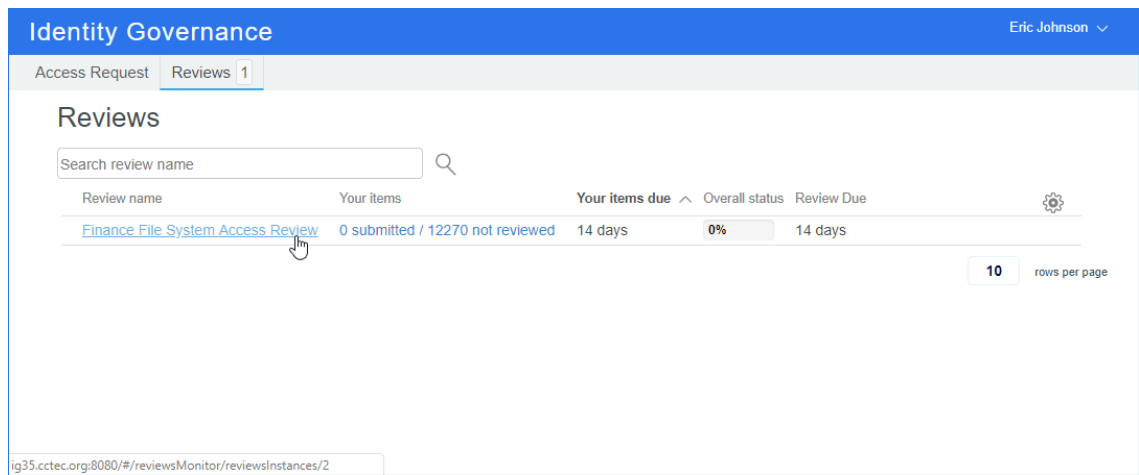
8.3 Running a File System Access Review

Once you have created a Review Definition, you can initiate the review process itself.

- 1 In Identity Governance, select **Reviews** > **Review Definitions**.
- 2 Click **Start Review** to initiate the review.



- 3 Click **Start and Go Live**.
- 4 Once the review is listed as **In Progress**, log in to Identity Governance as a user assigned as a Reviewer in the Review Definition.
- 5 Select **Reviews**, then click the review name.



The **Review Item** for File System Access shows the permission listed as the **Target Path – Access** such as `\\cct-2016.cctec.org\Finance - Change Permissions`.

The File System Access custom Permission Attributes provide additional criteria for grouping and filtering within the review itself. For example, to group by the **File System Access**, right-click the **Show all** drop-down and select **Group by File System Access**.



9 Exploring Detailed Access Reports with File Reporter

The File System Access integration and review criteria that define Data Access Governance provide a summarized business-level view of file system rights for identities.

To complete fulfillment and change process management, a detailed view of a Target Path's specific file system rights in the folder hierarchy is often required. File Reporter provides a detailed view of specific folder access rights for both users and groups and provides details as to whether those rights are inherited as well as displaying where the rights originate, such as a parent group.

9.1 Reviewing Built-in File System Access Reports in File Reporter

File Reporter provides the following built-in security reports related to detailed folder permissions:

- ◆ Assigned NTFS Permissions
- ◆ Permissions by Path
- ◆ Permissions by Identity
- ◆ NTFS Permissions Comparison

Each of these reports provides a unique perspective on file system access that can assist with making decisions for changes to users' folder access.

For details on each of these reports, refer to [Permissions Reports](#) in the *Micro Focus File Reporter 3.6 Administration Guide*.

9.2 Creating Custom File System Access Reports in File Reporter

In addition to the built-in reports, File Reporter provides tools to design and generate custom reports and report layouts. File Reporter includes a report designer tool as well as a complete reference to the database schema holding the file system scan data.

For details on using the File Reporter Report Designer, refer to [Using Report Designer](#) in the *Micro Focus File Reporter 3.6 Administration Guide*.

For details on the custom database schema available, refer to the [Micro Focus File Reporter 3.6 Database Schema and Custom Queries Guide](#).

In addition, [Appendix B, "File Reporter Schema Extensions,"](#) on page 49 provides details on database schema that may be referenced in custom queries along with the standard database schema.

A

Collection Strategies

A.1 Using a Single Collector

In cases where there are few Target Paths defined or in cases where all Target Paths should be collected at the same time, use a single File System Access Collector.

Advantages

- ♦ Minimal configuration required
- ♦ Out-of-the-box configuration of collector templates – no custom SQL editing required
- ♦ All Target Path data collected at one time

Disadvantages

- ♦ Larger data sets with a significant number of Target Paths might take longer to collect
- ♦ All defined Target Paths must be collected at the same time

To set up collection of File System Access data using a single collector, simply define the collector in an application, leaving the SQL query contents with the default values.

A.2 Using Multiple Collectors

In cases where separate application scopes are required or when a significant number of Target Paths has been defined, consider using multiple applications with separate collectors.

Advantages

- ♦ Separate scopes (Applications) might be associated with specific Target Paths
- ♦ Quicker collection times based on scope of each collector

Disadvantages

- ♦ Complex configuration required with multiple collectors defined
- ♦ Custom editing of collector SQL queries required

To set up multiple collectors, define a separate File System Access collector in each desired application. To set the scope for each collector, modify the SQL query for both the Permissions and Permissions to Holders section of each collector's definition, being sure to specify the same conditions for both queries in the same collector.

A.2.1 Scoping Collection by Target Path

To scope a File System Access Collector by one or more Target Paths, simply add the appropriate `WHERE` condition to the SQL queries in the collector's definition:

For example, to set a File System Access Collector to only include the Target Paths:

- ♦ `\\cct-2016.cctec.org\Finance`
- ♦ `\\cct-2012.cctec.org\Finance`

- 1 In Identity Governance, select **Data Sources > Applications**.
- 2 Select the application containing the File System Access collector to modify.
- 3 Select the collector in the application's configuration page to expand its configuration details.
- 4 Click **Collect Permission** to expand the permission settings.
- 5 Modify the Permission Query by adding an appropriate `WHERE` condition to the query:

```
SELECT
    e.id AS entitlement_id,
    e.entitlement,
    e.description,
    e.permission,
    e.target_path,
    e.category
FROM ig.dag_entitlements AS e
WHERE e.target_path IN ('\\cct-2016.cctec.org\Finance',
                       '\\cct-2012.cctec.org\Finance')
```

- 6 Click **Collect Permission to Holders** to expand the **Permission to Holders** settings.
- 7 Modify the **Permissions to Holders Query** by adding the appropriate `WHERE` condition to the query:

```
SELECT
    e.entitlement_id,
    e.trustee_fdn,
    e.trustee_guid,
    e.trustee_sid
FROM ig.dag_entitlement_entries AS e
WHERE e.target_path IN ('\\cct-2016.cctec.org\Finance',
                       '\\cct-2012.cctec.org\Finance')
```

- 8 Click **Save**  to commit the changes.

A.2.2 Scoping Collection by Target Path Category

To scope a File System Access Collector by one or more Target Paths, simply add the appropriate `WHERE` condition to the SQL queries in the collector's definition:

For example, to set a File System Access Collector to only include the Target Paths assigned the Finance category:


- 1 In Identity Governance, select **Data Sources > Applications**.
- 2 Select the application containing the File System Access collector to modify.

- 3 Select the collector in the application's configuration page to expand its configuration details.
- 4 Click **Collect Permission** to expand the permission settings.
- 5 Modify the **Permission Query** by adding an appropriate `WHERE` condition to the query:

```
SELECT
  e.id AS entitlement_id,
  e.entitlement,
  e.description,
  e.permission,
  e.target_path,
  e.category
FROM ig.dag_entitlements AS e
WHERE e.category = 'Finance'
```

- 6 Click **Collect Permission to Holders** to expand the Permission to Holders settings.
- 7 Modify the **Permissions to Holders Query** by adding the appropriate `WHERE` condition to the query:

```
SELECT
  e.entitlement_id,
  e.trustee_fdn,
  e.trustee_guid,
  e.trustee_sid
FROM ig.dag_entitlement_entries AS e
WHERE e.category = 'Finance'
```

- 8 Click **Save**  to commit the changes.

B File Reporter Schema Extensions

B.1 Schema Namespace

All File Reporter database objects related to Data Access Governance exist in the `ig` schema namespace.

Read access to this namespace and relevant tables and views is granted to the `Report Role` (typically named `srsreport_role`) in the database.

B.2 Tables

B.2.1 `ig.dag_permission_entries`

Provides the set of raw aggregated file system access data for use with Identity Governance.

Table B-1 Permission Entries Table Definition

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
<code>id</code>	big integer	big integer	Primary key
<code>scan_id</code>	integer	integer	Reference to <code>srs.scans</code> table
<code>target_path_id</code>	integer	integer	Reference to <code>ig.dag_target_paths</code>
<code>target_path</code>	nvarchar(max)	text	Target Path in UNC format
<code>target_path_hash</code>	binary(20)	bytea	SHA-1 hash of Target Path
<code>category</code>	nvarchar(64)	varchar(64)	Category assigned to Target Path
<code>trustee</code>	nvarchar(256)	varchar(256)	Trustee name in <code>Domain\SAMAccountName</code> format
<code>trustee_fdn</code>	nvarchar(256)	varchar(256)	Trustee full distinguished name
<code>trustee_guid</code>	nvarchar(36)	varchar(36)	Trustee GUID
<code>trustee_sid</code>	nvarchar(256)	varchar(256)	Trustee Security Identifier
<code>aggregate_access_mask</code>	integer	integer	Aggregate access mask for this identity and Target Path

B.2.2 `ig.dag_permissions`

Provides static table for permissions lookup.

Table B-2 Permissions Table Definition

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
id	integer	integer	Primary key
permission	nvarchar(32)	varchar(32)	One of: <ul style="list-style-type: none"> ◆ Read ◆ Write ◆ Change Permissions
access_mask	integer	integer	ACE mask that corresponds to the specific permission
description	nvarchar(128)	varchar(128)	Description of the permission

B.2.3 ig.dag_target_paths

Provides the set of Target Paths defined for Data Access Governance.

Table B-3 Target Paths Table Definition

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
id	integer	integer	Primary key
target_path	nvarchar(max)	text	Target Path in UNC format
target_path_hash	binary(20)	bytea	SHA-1 hash of Target Path
scan_target_path	nvarchar(256)	varchar(256)	Associated network path from srs.scan_targets
category	nvarchar(64)	varchar(64)	Optional category name
description	nvarchar(1024)	varchar(1024)	Optional description
scan_id	integer	integer	Reference to srs.scans table
scan_time	datetime2(0)	timestamp without time zone	UTC timestamp copied from scan_start_time in srs.scans
process_time	datetime2(0)	timestamp without time zone	UTC Time when aggregate processing completes
identity_count	integer	integer	Number of processed identities
option_flags	integer	integer	Processing options: 0 = None 1 = Automatic processing after scan
status	integer	integer	0 = Disabled 1 = Enabled 2 = Marked for delete

B.2.4 ig.dag_target_paths_job_queue

Provides the job queue for Data Access Governance Target Path processing.

Table B-4 Target Paths Job Queue Table Definition

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
id	big integer	big integer	Primary key
target_path_id	integer	integer	Reference to ig.dag_target_paths
queue_time	datetime(2)	timestamp without time zone	UTC timestamp when job queued
state	integer	integer	0 = Unknown 1 = Queued 2 = Processing 3 = Canceling 4 = Complete

B.3 Views

B.3.1 ig.dag_entitlement_entries

Provides an extended view of permission entries.

This view is referenced by the File System Access Permissions collector in Identity Governance.

Table B-5 Entitlement Entries View

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
entitlement_id	nvarchar	text	Composite "key" composed of: <ul style="list-style-type: none">◆ dag_target_paths id◆ dag_permission_entries id Example: 3-1
trustee_guid	nvarchar(36)	varchar(36)	Trustee GUID
trustee_sid	nvarchar(256)	varchar(256)	Trustee Security Identifier
trustee_fdn	nvarchar(256)	varchar(256)	Trustee full distinguished name
target_path	nvarchar(max)	text	Target Path in UNC format
category	nvarchar(64)	varchar(64)	Optional category name

B.3.2 ig.dag_entitlements

Provides a simple view of mappings between Data Access Governance Target Paths and identities. This view is referenced by the File System Access Permissions collector in Identity Governance.

Table B-6 Entitlements View

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
id	nvarchar	text	Composite "key" composed of: <ul style="list-style-type: none"> ◆ dag_target_paths id ◆ dag_permissions id Example: 3-1
entitlement	nvarchar	text	Composite value consisting of: <ul style="list-style-type: none"> ◆ target_path ◆ dag_permissions id Example: \\server.lab\Share - 3
description	nvarchar(1024)	varchar(1024)	Optional description
target_path	nvarchar(max)	text	Target Path in UNC format
permission	nvarchar(32)	varchar(32)	One of: <ul style="list-style-type: none"> ◆ Read ◆ Write ◆ Change Permissions
category	nvarchar(64)	varchar(64)	Optional category name

B.3.3 ig.dag_permission_entries_view

Provides an extended view of `ig.dag_permission_entries` and includes data from `ig.dag_target_paths` as well as the converted string value for the aggregate access mask.

Table B-7 Permission Entries View

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
id	big integer	big integer	Primary key
scan_id	integer	integer	Reference to srs.scans table
scan_time	datetime2(0)	timestamp without time zone	UTC timestamp copied from scan_start_time in srs.scans
category	nvarchar(64)	varchar(64)	Optional category name

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
target_path	nvarchar(max)	text	Target Path in UNC format
target_path_hash	binary(20)	bytea	SHA-1 hash of Target Path
target_path_id	integer	integer	References ig.dag_target_paths
trustee	nvarchar(256)	varchar(256)	Trustee name in <i>Domain\SAMAccountName</i> format
trustee_fdn	nvarchar(256)	varchar(256)	Trustee full distinguished name
trustee_guid	nvarchar(36)	varchar(36)	Trustee GUID
trustee_sid	nvarchar(256)	varchar(256)	Trustee Security Identifier
aggregate_access_mask	integer	integer	Aggregate access mask for this identity and Target Path
access_string	nvarchar(64)	varchar(64)	Converted text for aggregate access mask containing one or more of the following: <ul style="list-style-type: none"> ◆ Read ◆ Write ◆ Change Permissions
target_path_status	integer	integer	0 = Disabled 1 = Enabled 2 = Marked for delete

B.3.4 ig.dag_target_paths_view

Provides an expanded view of Target Paths and includes data from job queue as well as `permissions_status` from any new scan data referenced in the `srs.scans` table.

Table B-8 s View

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
id	integer	integer	Primary key
target_path	nvarchar(max)	text	Target Path in UNC format
target_path_hash	binary(20)	bytea	SHA-1 hash of Target Path
scan_target_path	nvarchar(256)	varchar(256)	Associated network path from <code>srs.scan_targets</code>
category	nvarchar(64)	varchar(64)	Optional category name
description	nvarchar(1024)	varchar(1024)	Optional description
scan_id	integer	integer	Reference to <code>srs.scans</code> table
scan_time	datetime2(0)	timestamp without time zone	UTC timestamp copied from <code>scan_start_time</code> in <code>srs.scans</code>

Column Name	SQL Server Data Type	PostgreSQL Data Type	Notes
process_time	datetime2(0)	timestamp without time zone	Time when aggregate processing completes
identity_count	integer	integer	Number of processed identities
option_flags	integer	integer	Processing options: 0 = None 1 = Automatic processing after scan
status	integer	integer	0 = Disabled 1 = Enabled 2 = Marked for delete
queue_time	datetime2(0)	timestamp without time zone	Timestamp when processing job was queued
permissions_status	integer	integer	Status of membership post-processing on permission scans: 0 = Unknown 1 = Queued 2 = Processing 3 = Complete
current_scan_id	integer	integer	References srs.scans.id from last processed scan data
job_state	integer	integer	0 = Unknown 1 = Queued 2 = Processing 3 = Canceling 4 = Complete
job_num	integer	integer	Count of queued jobs for a Target Path – internal processing

B.4 Functions

B.4.1 ig.dag_get_aggregate_access_string

Table B-9 Get Aggregate Access String Function

Parameter	SQL Server Data Type	PostgreSQL Data Type
access_mask	integer	integer
Return Value	nvarchar(64)	varchar(64)

Description:

Converts an aggregate access mask to a string value containing one or more of the following:

- ◆ Read
- ◆ Write
- ◆ Change Permissions

Example:

```
SELECT ig.dag_get_aggregate_access_string(255)
```

Returns: "Read, Write"

