Micro Focus File Reporter 4.1

Administration Guide

February 28, 2022

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.

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/.

Third Party Systems

The software is designed to run in an environment containing third party elements meeting certain prerequisites. These may include operating systems, directory services, databases, and other components or technologies. See the accompanying prerequisites list for details.

The software may require a minimum version of these elements in order to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth in order for the software to be able to perform in a way that meets the customer requirements. The download, installation, performance, upgrade, backup, troubleshooting, and management of these elements is the responsibility of the customer using the third party vendor’s documentation and guidance.

Third party systems emulating any these elements must fully adhere to and support the appropriate APIs, standards, and protocols in order for the software to function. Support of the software in conjunction with such emulating third party elements is determined on a case-by-case basis and may change at any time.

Contents

About This Manual

This administration guide is written to provide network administrators the conceptual and procedural information for administering Micro Focus File Reporter 4.1.

Audience

This guide is intended for network administrators who manage network storage resources.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Micro Focus File Reporter 4.1 Administration Guide*, visit the Micro Focus File Reporter Documentation website.

Additional Documentation

For additional File Reporter 4.1 documentation, see the following guides at the Micro Focus File Reporter Documentation website:

- Micro Focus File Reporter 4.1 Installation Guide

- Micro Focus File Reporter 4.1 Client Tools Guide
- *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*

1 What's New

With each product update, Micro Focus File Reporter introduces significant architectural and feature enhancements.

1.1 New in Version 4.1

1.1.1 Enhanced Reporting for Microsoft 365

File Reporter 4.1 includes the following additional data when scanning Microsoft 365 tenants:

- SharePoint site-specific users, groups, and permission levels.
- SharePoint site-level permissions.
- SharePoint permission level bindings for folders, files and document libraries.
- Group Owners for Microsoft 365 Groups.
- Improved identification of SharePoint site-specific groups and users for existing drive item permissions definitions.

1.1.2 Identity Enrichment for Active Directory

File Reporter 4.1 provides extended collection of attributes for associated security principals in Active Directory.

The data collected by this new system extends the basic identity data already collected for file system owners and permission holders.

Features for this enhancement include:

- Independently scheduled scan of all security principals in the Active Directory forest.
- Basic set of identity and extended attributes related to security principal types (user, group, etc.).
- Initial support for specifying additional attributes for collection.

1.1.3 Custom Query Report Enhancements

File Reporter 4.1 adds initial management of File System target paths for Custom Query reports.

Users can now select and assign one or more target paths from File System or Permissions scans and associate them with a specific Custom Query report in a similar fashion as built-in reports.

2 Overview

This section provides an understanding of Micro Focus File Reporter, the supported databases, the Engine, and Agents, along with how reports and analytics information are generated.

2.1 Introduction

Micro Focus File Reporter inventories Microsoft network file systems and Microsoft 365 cloud storage to deliver the detailed file storage intelligence you need to optimize and secure your network and Microsoft 365 cloud for efficiency and compliance. Engineered for enterprise system reporting, File Reporter gathers data across the millions of files and folders scattered among the various network storage devices and OneDrive for Business, SharePoint Online, and Teams cloud storage areas that make up your network and cloud storage. Flexible reporting, filtering, and querying options then present the exact findings you need so you can demonstrate compliance or take corrective action.

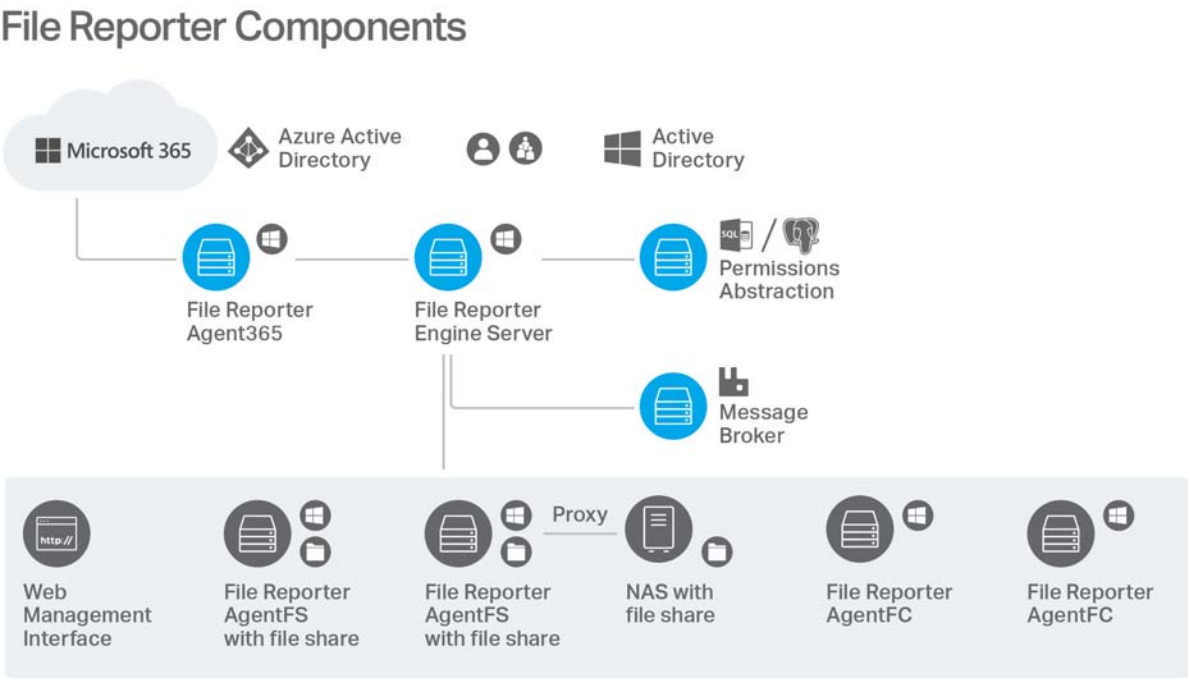
File Reporter identifies files currently stored, the size of the files, whether these files contain personal or other sensitive information, when users last accessed or modified the files, the locations of duplicate files, and more. File Reporter can also help you calculate department or individual storage costs. File Reporter can even identify access rights to folders and consequently, the files that are contained within.

2.2 How File Reporter Works

File Reporter was developed to examine, report, and analyze Windows network file systems and the Microsoft 365 cloud and its potential petabytes of data—in other words, millions of files, folders and shares, scattered among the various storage devices and Microsoft 365 applications that make up your network. This reporting includes file content and the associated rights of these files, folders, and network shares.

To examine, report, and analyze this data efficiently, File Reporter disperses the work among a Web Application, Engine, Agents, a Scan Processor, the RabbitMQ messaging broker, either a PostgreSQL or Microsoft SQL Server database, Microsoft Active Directory, and Microsoft Azure Active Directory.

Figure 2-1 *File Reporter Work Process*



2.3 Core Components

The following are core components of File Reporter.

2.3.1 Web Application

The Web application runs on top of Microsoft Internet Information Services (IIS) and is the means of all administrative interaction. Among other things, the Web application is responsible for:

- Management of scan policies and report definitions
- Generating Preview reports
- Access to stored reports
- All other management functions

2.3.2 Engine

The Engine is the mechanism that runs File Reporter and runs from a Windows Server host. The Engine does the following:

- Schedules the scans that the Agents conduct
- Compiles scans for inclusion in a report

- Runs scheduled reports
- Manages scan delegations to Agents
- Sends notifications that File Reporter has completed a scan or generated a report

2.3.3 Database

The database stores information needed for generating reports. This information includes:

- Cached Active Directory objects
- Scans
- Identity system information such as names of Active Directory domains and forests
- Schedule information pertaining to scans and reports
- Notification information
- Report definitions
- Scan history
- Scan policies
- Free space on shares

2.4 File System Scanning

The following are components associated with file system scanning.

2.4.1 Scan Processor

The Scan Processor does the following:

- Processes file system scan files
- Updates file system scan information in the database

2.4.2 AgentFS

AgentFS is a compact program that runs on Microsoft Windows Server hosts. AgentFS can examine and report on NTFS file systems hosted through shares. AgentFS can collect and scan data related to file system metadata and permissions. For more information, see Appendix C, “AgentFS Scan Capabilities,” on page 127.

IMPORTANT: For optimal results, you should install an Agent on every server that has a share you want to report on.

Agents cannot be installed on NAS devices or clustered storage. For File Reporter to report on these types of devices, Agents can be set up as proxy agents.

For performing file system scans (rather than file content scans), File Reporter provides AgentFS.

2.4.3 Scans

Through AgentFS, File Reporter scans a storage resource. A storage resource can be a Microsoft network share or a Network Attached Storage (NAS) device.

File system scans are indexed data that are specific to a storage resource. They are the means of generating a storage report or the means of reviewing data using the analytics tools. File system scans include comprehensive information on the file types users are storing, when files were created, when they were last modified, permission data on the folders where these files reside, and much more.

File Reporter collects file system scans from the Agents and sends them to the Engine. The Engine then sends the scans to the Scan Processor, which stores the scans in the database.

You can conduct scans at any time, but we recommend using a scheduled time after normal business hours to minimize the effect on network performance.

NOTE: Procedures for performing scans are documented in Section 5.4, “Scan Scheduling,” on page 43.

2.5 File Content Scanning

The following are components associated with file content scanning.

2.5.1 ManagerFC

The ManagerFC service is responsible for the execution and management of file scan jobs. The service performs the following tasks when processing a scan job:

- Enumeration of files in target paths
- Submission of files to scan queues in the message broker based on filter criteria
- Processing of scan results and update of result data to the database and scan result files

2.5.2 AgentFC

AgentFC performs file content scans. AgentFC is hosted on a Windows Server and performs content scans on files stored on Windows servers and NAS devices.

2.5.3 Scans

Through AgentFC and ManagerFC, File Reporter performs, classifies, and categorizes file content scans. For example, content scans can identify files containing specified patterns such as U.S. Social Security numbers or credit card numbers.

2.6 Microsoft 365 Cloud Scanning

File Reporter extends the ability to report what files are being stored on your enterprise storage devices and who has access to these files, with reporting on the files and associated permissions located in Microsoft 365 cloud repositories for OneDrive for Business, SharePoint Online document libraries, and Teams document libraries.

Unlike scanning the network file system separately for File System, Permissions, and Volume Free Space, scans for files and associated permissions stored in the Microsoft 365 cloud are conducted simultaneously.

Reporting on Microsoft 365 is done through the development of custom queries and report layouts or by using report templates available at https://filequerycookbook.com. For instructions on creating a Custom Query report from a predefined template, see the *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*.

2.7 Reporting

When File Reporter has a scan, you can utilize it to generate a report. You can generate reports through the following means:

- Built-in Reports
- Custom Queries

2.7.1 Built-in Reports

Generating a built-in report is as simple as selecting the report type from a menu.

To generate a report, the Engine takes all of the needed scans that apply to the specifications of the report and consolidates them into a single report by indexing the applicable scans.

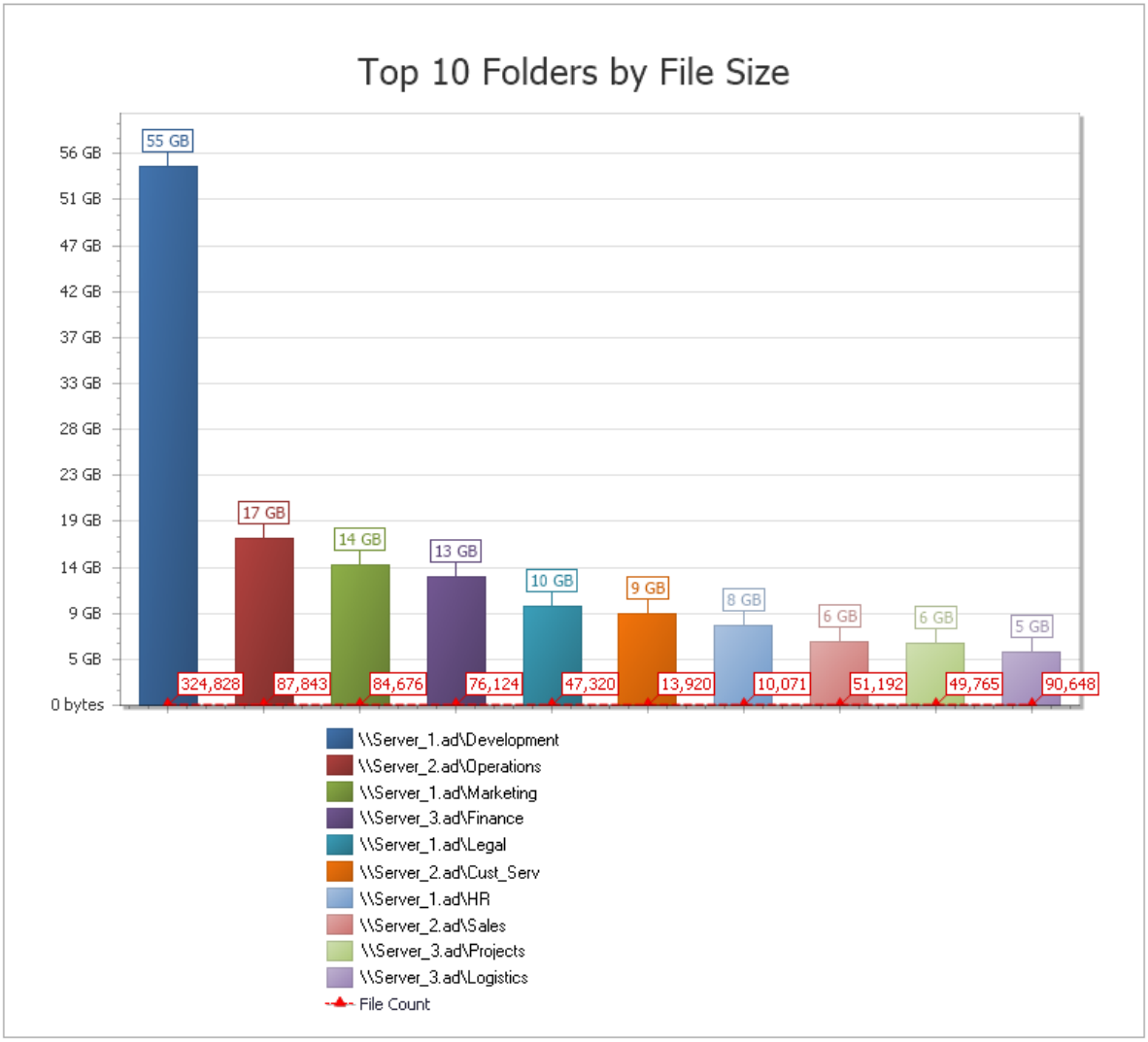
Table 2-1 *Built-in Report Types*

File System Reports	Security Reports	Trending Reports
Folder Summary	Assigned NTFS Permissions	Volume Free Space
Detail Reports	Permissions by Path	
File Extension	Permissions by Identity	

File System Reports	Security Reports	Trending Reports
Duplicate Files	Historic NTFS Permissions	
Date-Age		
Owner		
Storage Cost		
Comparison		
Directory Quota		
Historic File System Comparison		

File Reporter lets you present built-in reports in various formats including PDF, Microsoft Excel, RTF, HTML, TXT, and CSV. The product also includes built-in graphs for certain report types.

Figure 2-2 *Sample Report in Graphical Format*



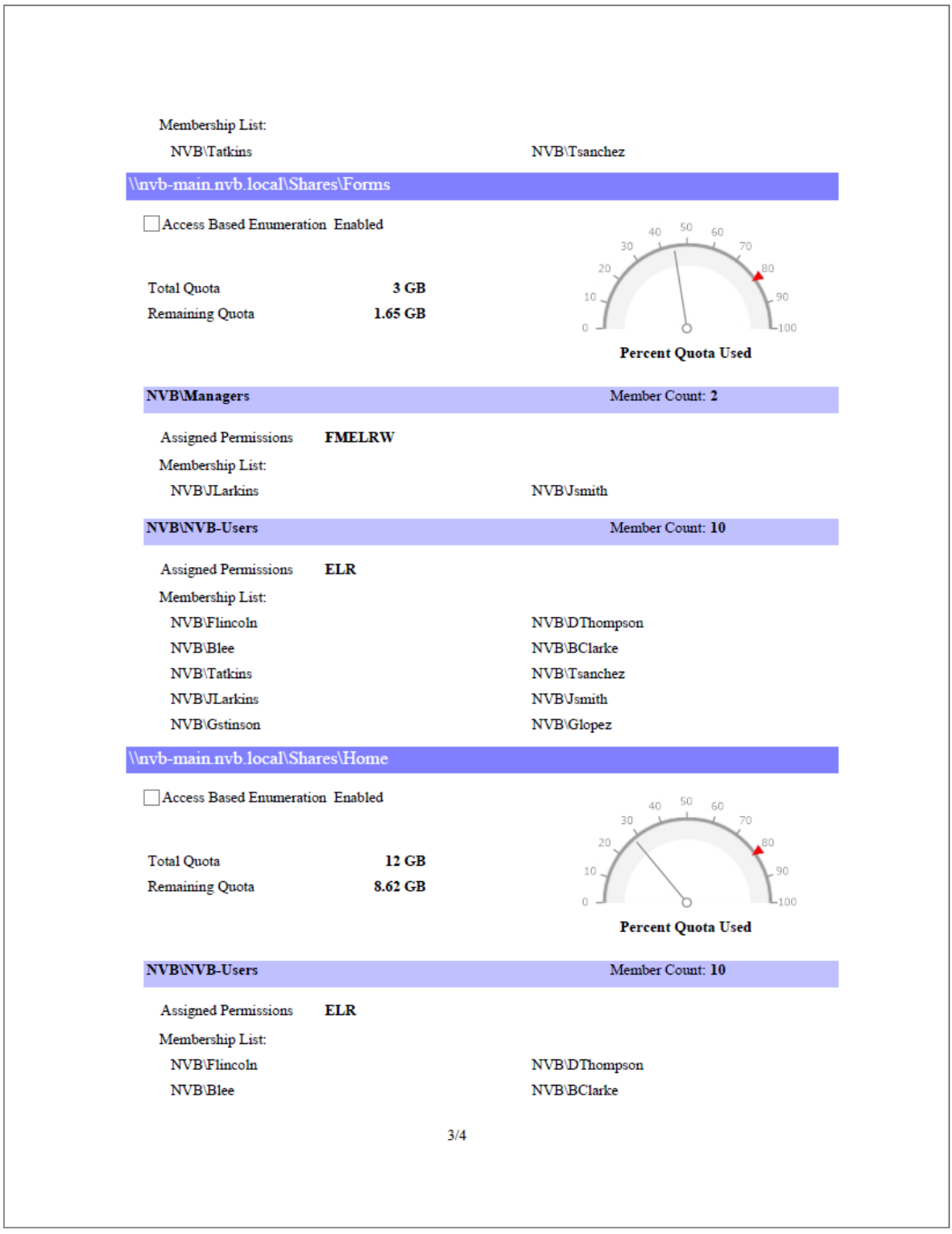
2.7.2 Custom Query Reports

These reports allow administrators who are familiar with querying the database to generate very specific report data that might not be available through one of the built-in report types.

Custom Query report data can be further customized for layout and presentation from a Windows workstation with the Report Designer.

File content and Microsoft 365 reports are delivered as Custom Query reports.

Figure 2-3 *Page from a Custom Query Report Designed with the Report Designer.*



2.8 Client Tools

File Reporter provides the following Client Tools, designed to be run from a Windows workstation.

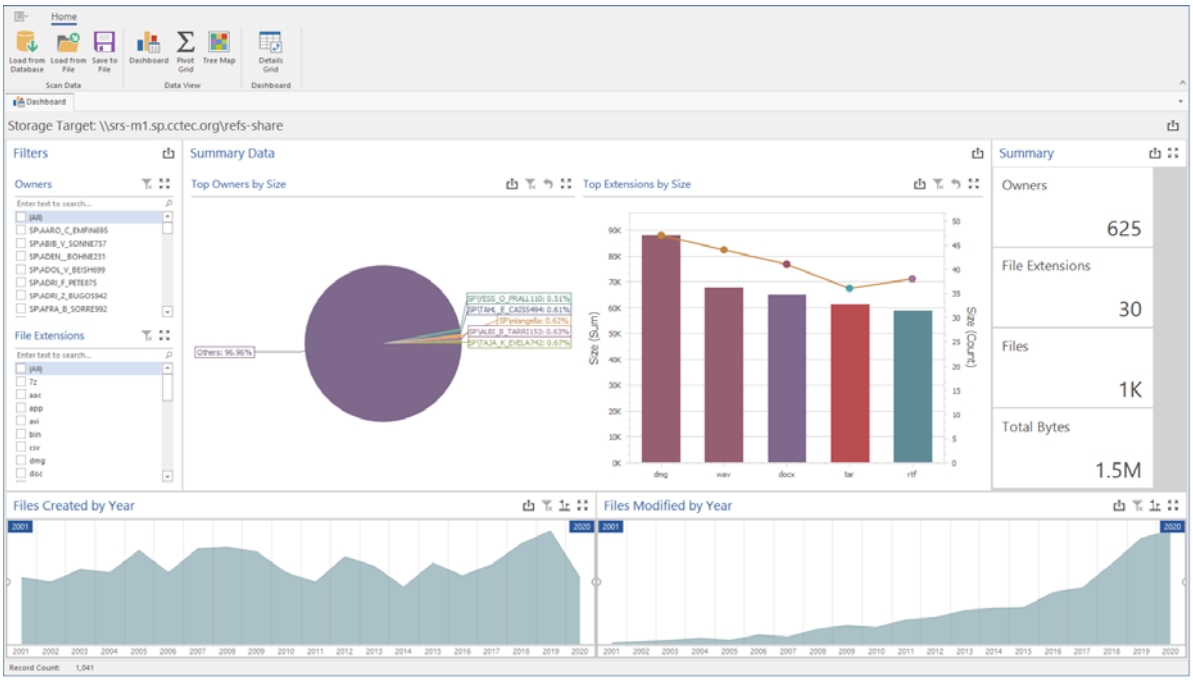
2.8.1 Data Analytics

In addition to extensive reporting options, File Reporter provides the ability to graphically analyze file system data using a variety of analytics tools that are available to administrators through the Client Tools.

Dashboard

The Dashboard lets you graphically analyze data from file system scans according to the filters that you specify.

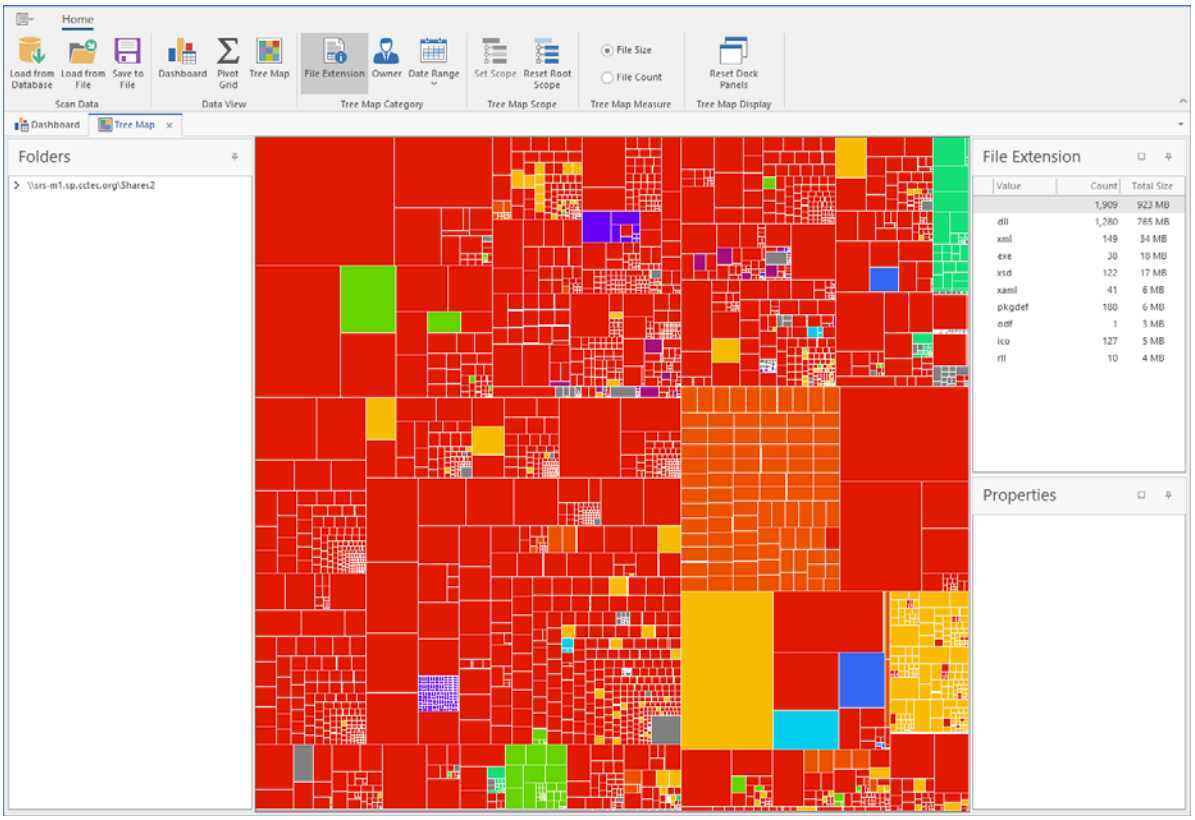
Figure 2-4 *Dashboard*



Tree Map

The Tree Map lets you view graphical representations of hierarchical file system data and in the process, gain insight very quickly.

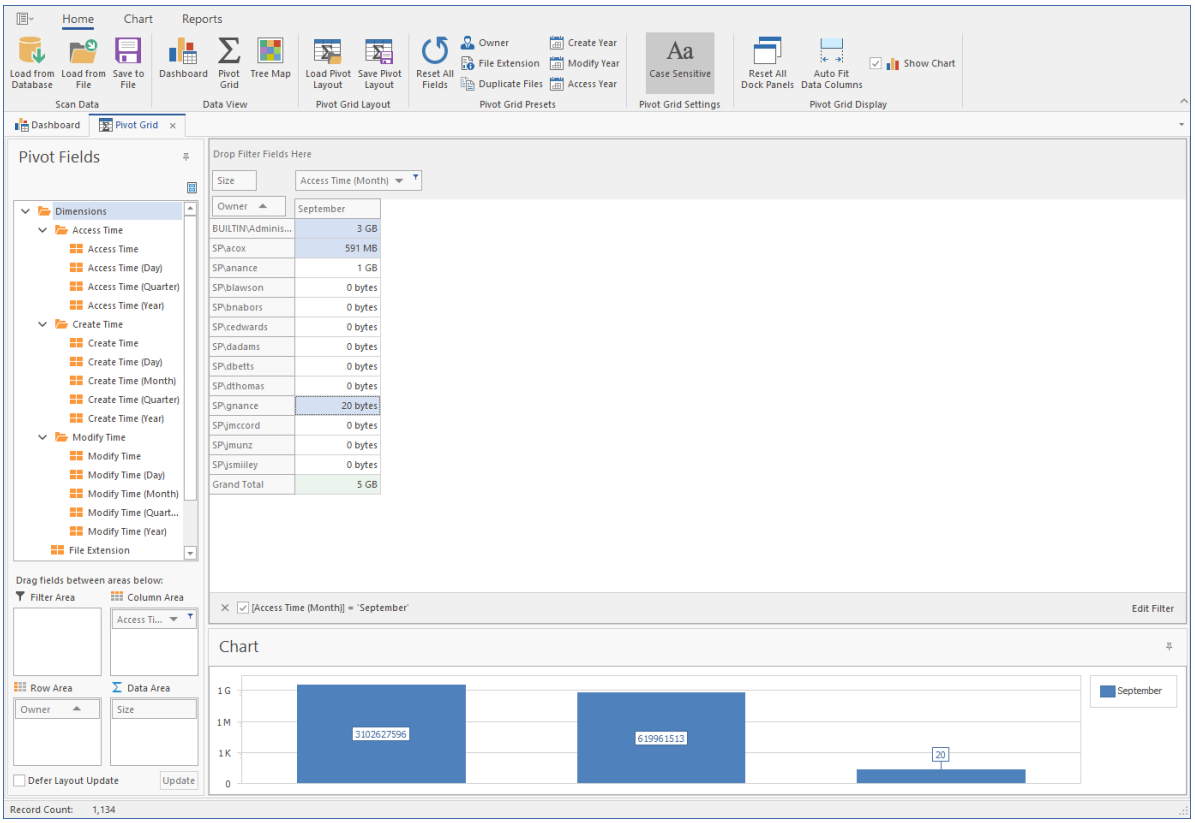
Figure 2-5 *Tree Map*



Pivot Grid

The Pivot Grid gives you the ability to visually analyze data according to combinations of variables.

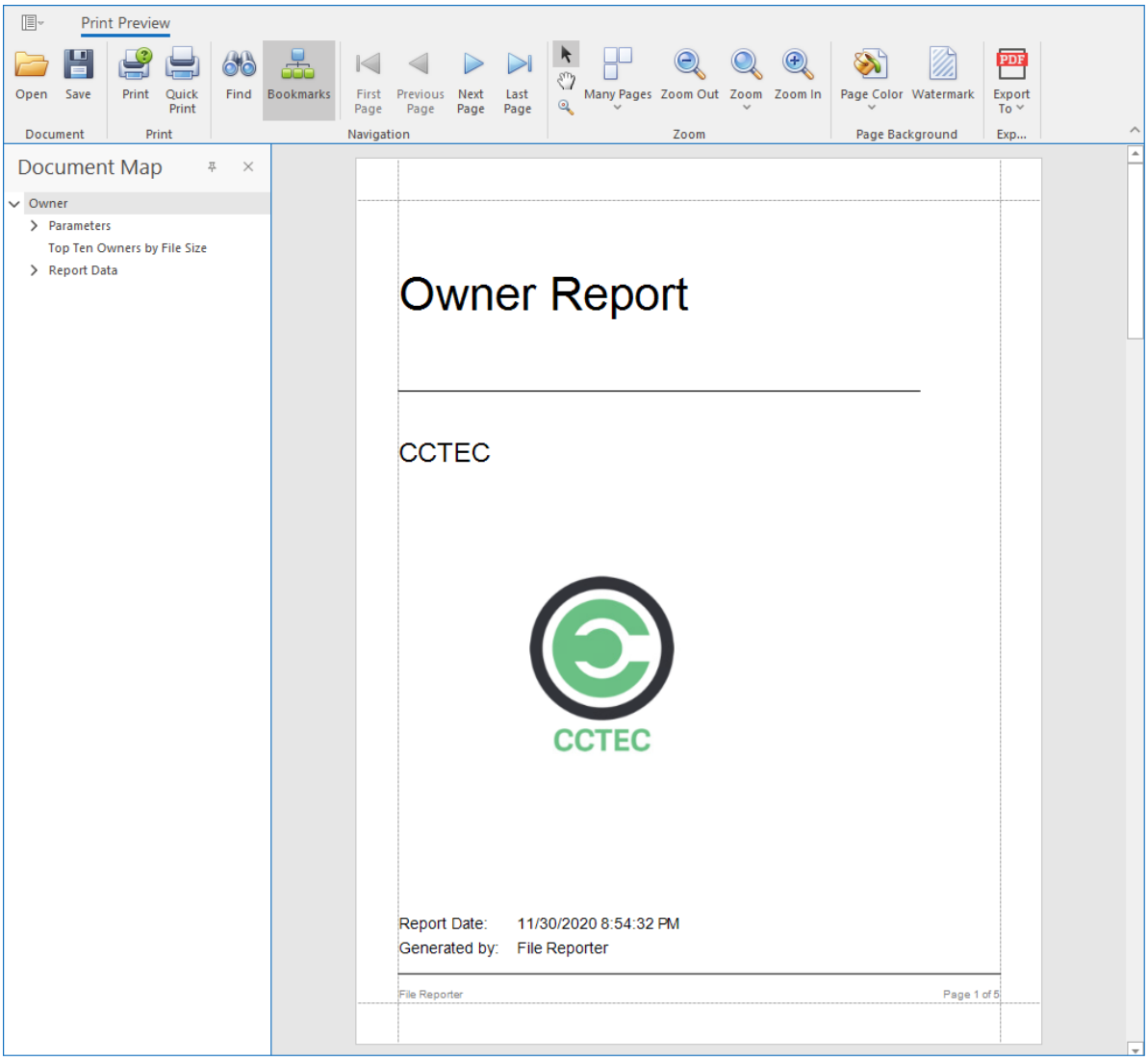
Figure 2-6 *Pivot Grid*



Report Viewer

The Report Viewer lets you view all stored reports locally from a Windows workstation. Because the Report Viewer utilizes the resources of the Windows workstation, rather than those of the Engine, the Report Viewer can display stored reports much faster in most instances.

Figure 2-7 *Report Viewer*



3 Web Application

This section provides procedures for enabling and using the web browser-based File Reporter administrative interface.

3.1 Supported Browsers

Micro Focus File Reporter is managed through a web browser-based interface and is supported on the latest versions of the following browsers:

Table 3-1 *Supported Browsers*

Windows	Linux	Mac OS X
Firefox	Firefox	Firefox
Chrome		Chrome
Edge		

3.2 Launching the Administrative Interface

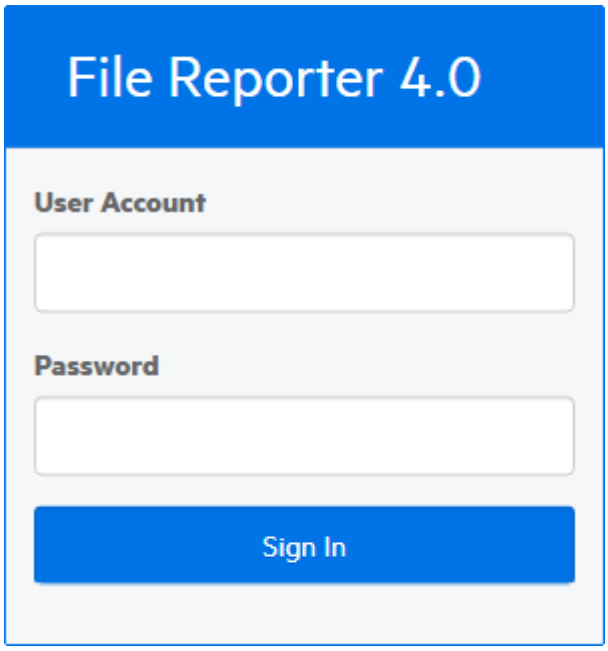
1 In the browser’s address bar, type:

`https://file_reporter_web_server_dns_name`

The DNS name is the one you created during the File Reporter installation.

You must enter the DNS name. You cannot log in with an IP address.

The login screen appears.



2 Enter the username and password of a member of the SRsAdmins group that you created and click **Log In**.

The username can be entered in any of the standard Active Directory formats:

*domain**SAMAccountName* (AD\User1)

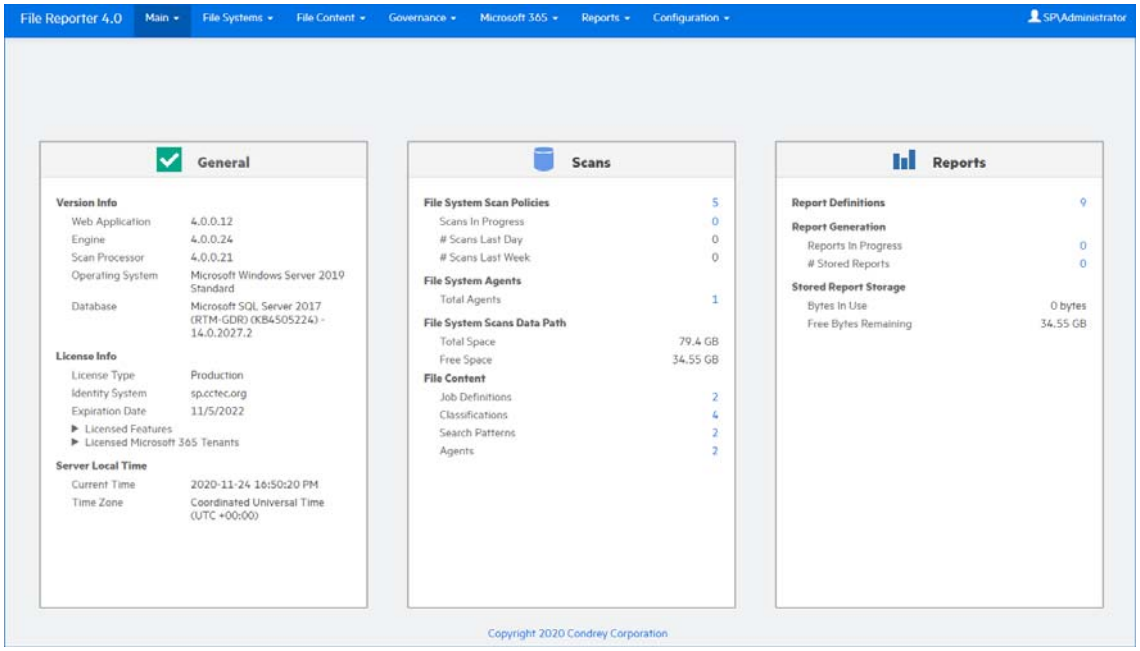
UPN(user1@sp.cctec.lab)

LDAP(CN=user1,OU=home,DC=sp,DC=cctec,DC=org)

NOTE: With LDAP, there may be partial case sensitivity, especially with the domain (DC=) components

---

The File Reporter Home page appears:



3.3 Overview

All tasks are conducted by selecting an option from one of the menus at the top of the page.

The **Main** menu provides access to notifications and system information.

The **File Systems** menu is the means to setting up and viewing the progress of file system scans.

The **File Content** menu provides options for setting up and conducting file content scans.

The **Governance** menu is for enabling the conducting of access reviews on unstructured data through NetIQ Identity Governance.

The **Microsoft 365** menu provides the means of scanning OneDrive for Business, SharePoint Online document libraries, and Team libraries.

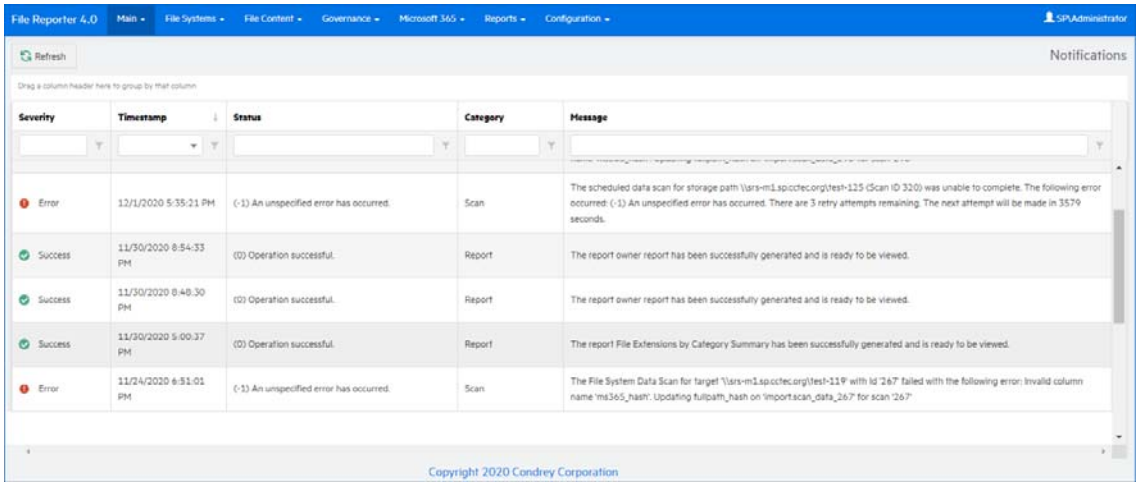
The **Reports** menu is the means of generating and accessing reports.

The **Configuration** menu is the means of establishing and modifying configuration settings within File Reporter.

3.3.1 Notifications

File Reporter displays notifications for successfully completed scans, failed scans, completed reports, failed reports, errors, warnings, and other information. You can use the filtering options to list only the notification types you want.

1 From the **Main** menu, select **Notifications**.



Like many pages in the administrative interface, you can modify the current display.

2 (Optional) Display columns in the order you want by dragging them to the desired location.

3 (Optional) List the most recent notification by clicking the column heading twice.

4 (Optional) Filter the notifications to display only the information you want:

4a At the desired column heading, click the “pin” icon.

For example, the **Message** column.

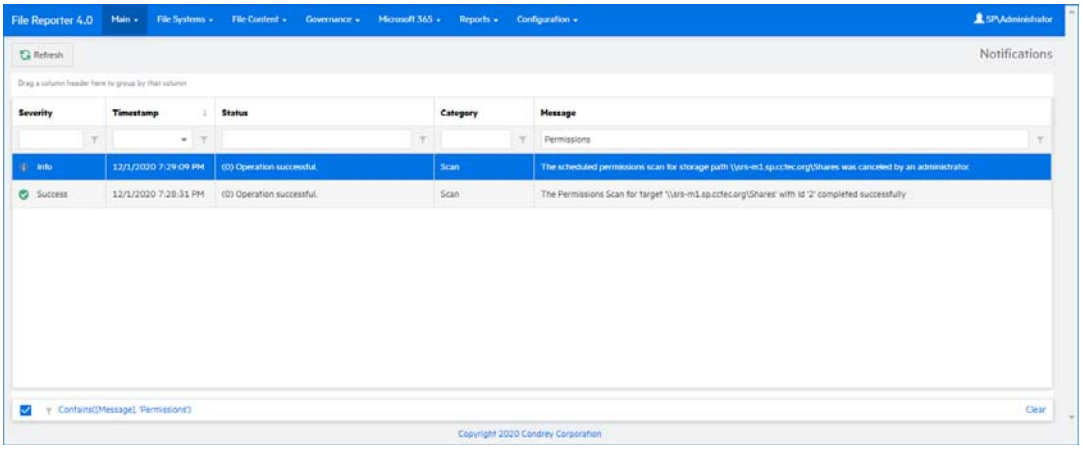
4b Select the desired filter option.

For example, **Contains**.

4c In the field to the left of the “pin” icon, enter the distinguishing word or letter for the filter.

For example, `Permissions`.

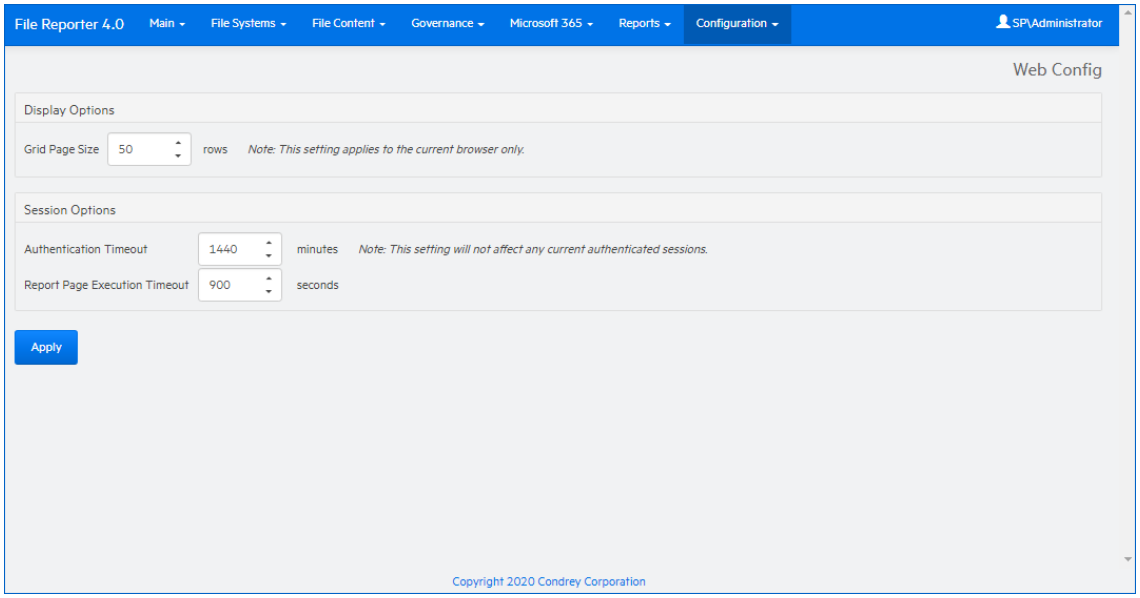
The page is updated according to the filtering parameters.



3.3.2 Web Client Options

After 20 minutes of inactivity in the administrative interface, you are required to log in again. You can adjust this setting and specify the number of items displayed per page through the **Web Application** option of the **Configuration** menu.

1 From the **Configuration** menu, select **Web Application**.



2 In the **Grid Page Size** field, specify the number of entries you want displayed.

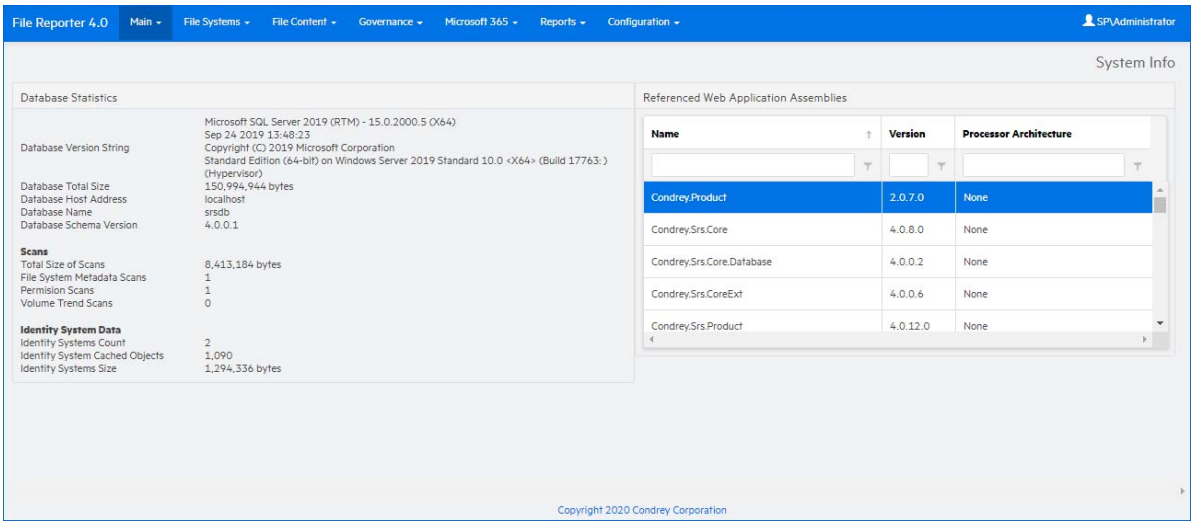
3 In the **Authentication Timeout** field, specify the minutes of inactivity before you will need to log in again.

4 Click **Apply**.

5 When you are notified that the Web interface configuration was saved, click **OK**.

3.3.3 System Information

When you work with a Micro Focus Support representative to diagnose the source of a problem, you might be asked to access the System Info page. To do so, simply select **System Configuration** from the **Main** menu.


File Reporter 4.0
Main
File Systems
File Content
Governance
Microsoft 365
Reports
Configuration
SP\Administrator
System Info
Database Statistics
Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64)
Sep 24 2019 13:48:23
Copyright (C) 2019 Microsoft Corporation
Standard Edition (64-bit) on Windows Server 2019 Standard 10.0 <X64> (Build 17763:) (Hypervisor)
Database Version String
Database Total Size 150,994,944 bytes
Database Host Address localhost
Database Name srsdb
Database Schema Version 4.0.0.1
Scans
Total Size of Scans 8,413,184 bytes
File System Metadata Scans 1
Permision Scans 1
Volume Trend Scans 0
Identity System Data
Identity Systems Count 2
Identity System Cached Objects 1,090
Identity Systems Size 1,294,336 bytes
Referenced Web Application Assemblies
Name
Version
Processor Architecture
Condrey.Product 2.0.7.0 None
Condrey.Srs.Core 4.0.8.0 None
Condrey.Srs.Core.Database 4.0.0.2 None
Condrey.Srs.CoreExt 4.0.0.6 None
Condrey.Srs.Product 4.0.12.0 None
Copyright 2020 Condrey Corporation

4 Setup Procedures

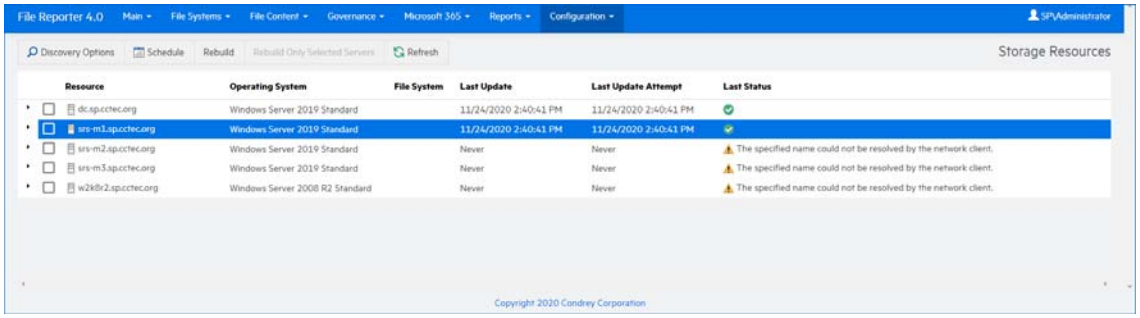
Before you can start scanning storage resources and generating reports, you first need to perform some setup procedures.

4.1 Storage Resources

When Active Directory has been enabled, the associated storage resources are available for scanning and reporting.

File Reporter cannot see a Windows network disk drive that is not shared.

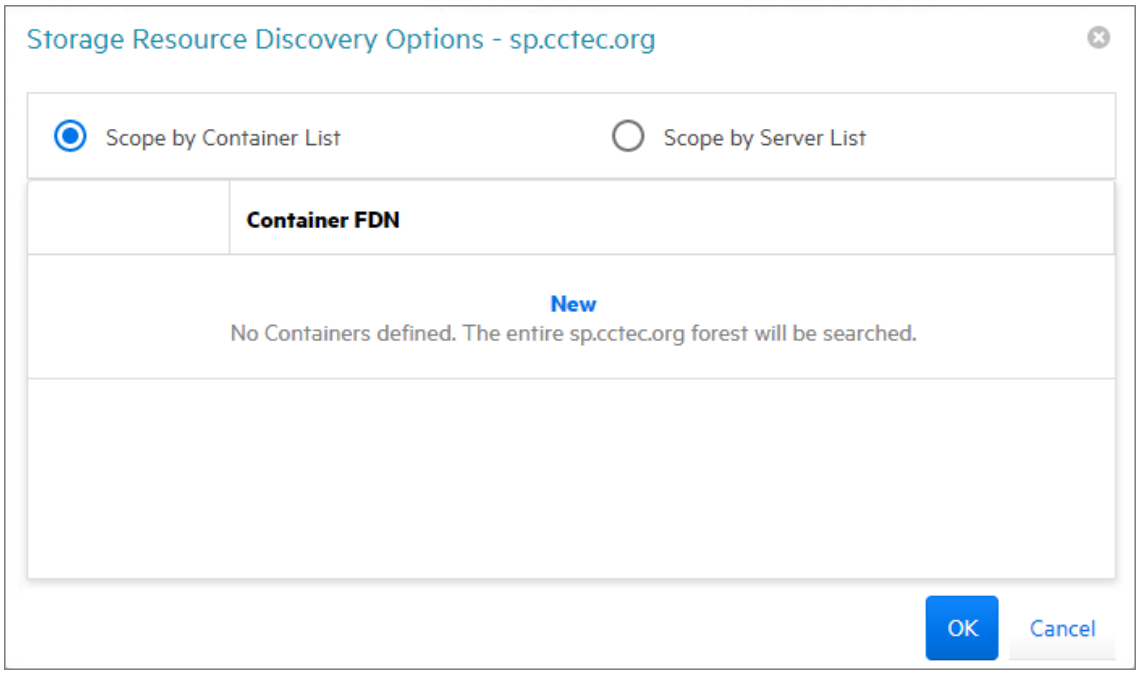
1 Select **Configuration** > **Storage Resources**.



All of the servers in the Active Directory forest are displayed.

2 Click each button to view options.

Discovery Options: For large organizations with Active Directory forests spanning multiple geographic areas, rebuilding the storage resources can take many hours. Rather than rebuilding the storage resources, you can select this to create a scope that specifies just those new containers or servers that should be included.



Select whether to specify the servers through a container FDN or server FDN, then click **New** to enter the paths. Specify the FDN path and click **Update**. When all of the paths you want to be searched are listed, click **OK**.

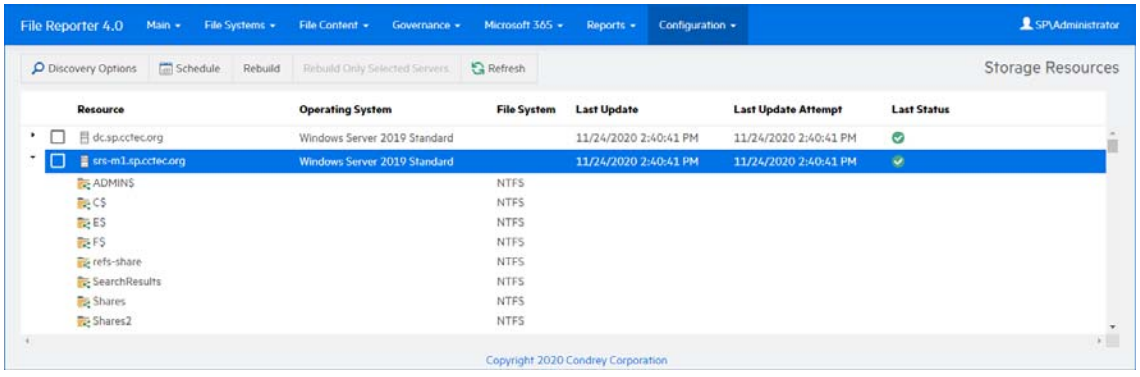
Schedule: By default, File Reporter rebuilds Active Directory's storage resources at 12:00 AM each day. Larger sites might want to change this setting to weekly or monthly. To do so, click this option and modify the settings in the dialog box.

Rebuild: Clicking this button automatically rebuilds Active Directory's storage resources.

Rebuild Only Selected Servers: Use this option to rebuild the selected servers.

Refresh: Refreshes the resource list.

3 Click the > for each server to browse the storage resources.

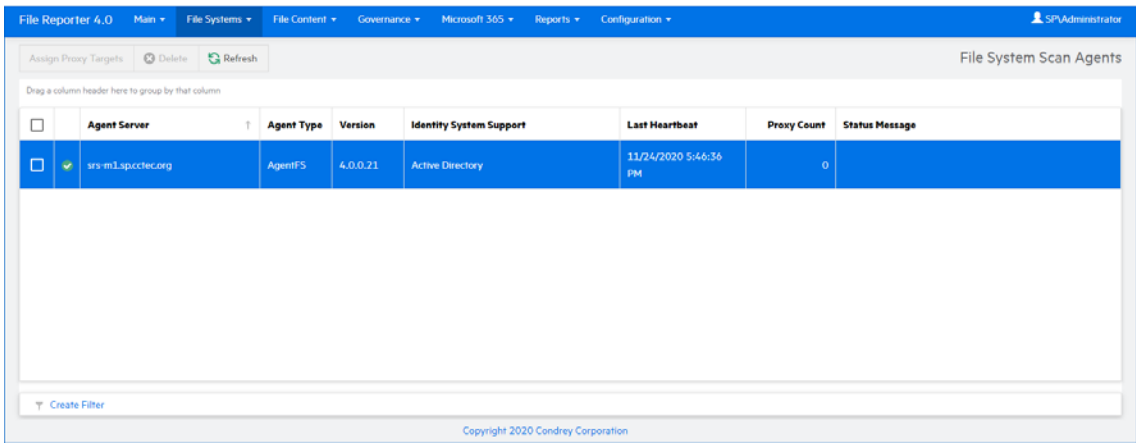


4.2 Assigning Proxy Targets

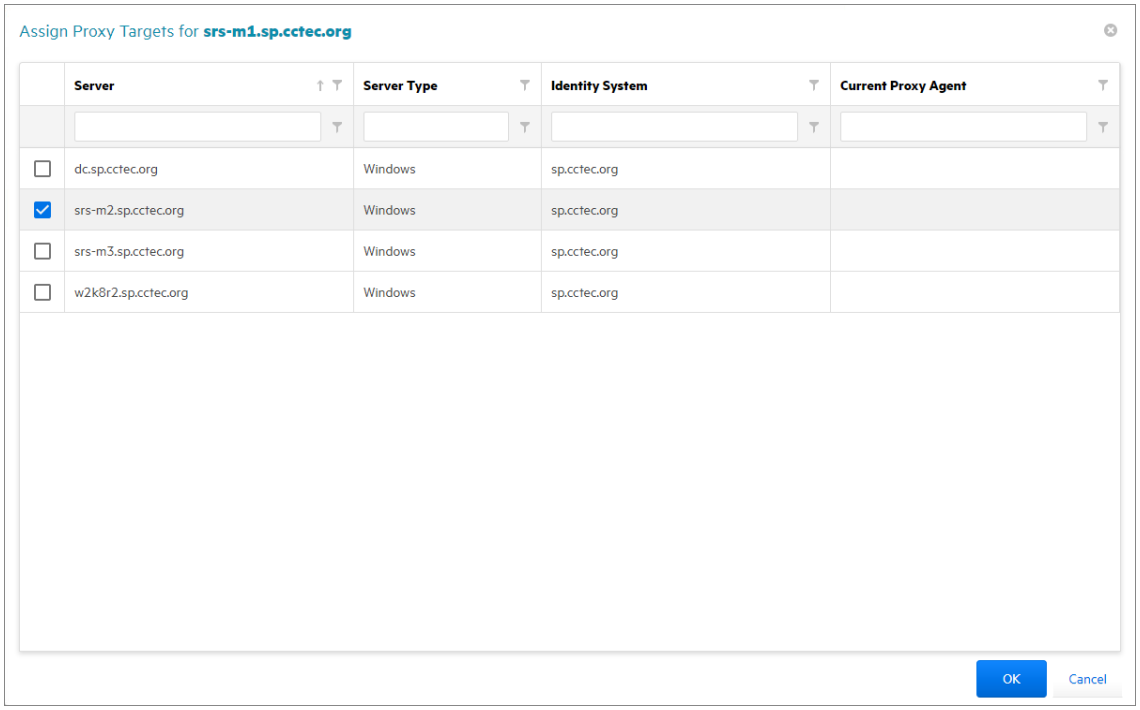
An Agent cannot be deployed on a NAS device or storage cluster. Additionally, only one Agent type (AgentFS, AgentFC, or Agent365) can be hosted on a server. Finally, some organizations might not want Agents deployed on every server. In situations such as these, you can have a deployed Agent on another server function as a proxy agent.

1 Select **File Systems** > **Scan Agents**.

All of the Agents are listed.



2 Select the Agent you want to set up as a proxy agent and click **Assign Proxy Targets**.

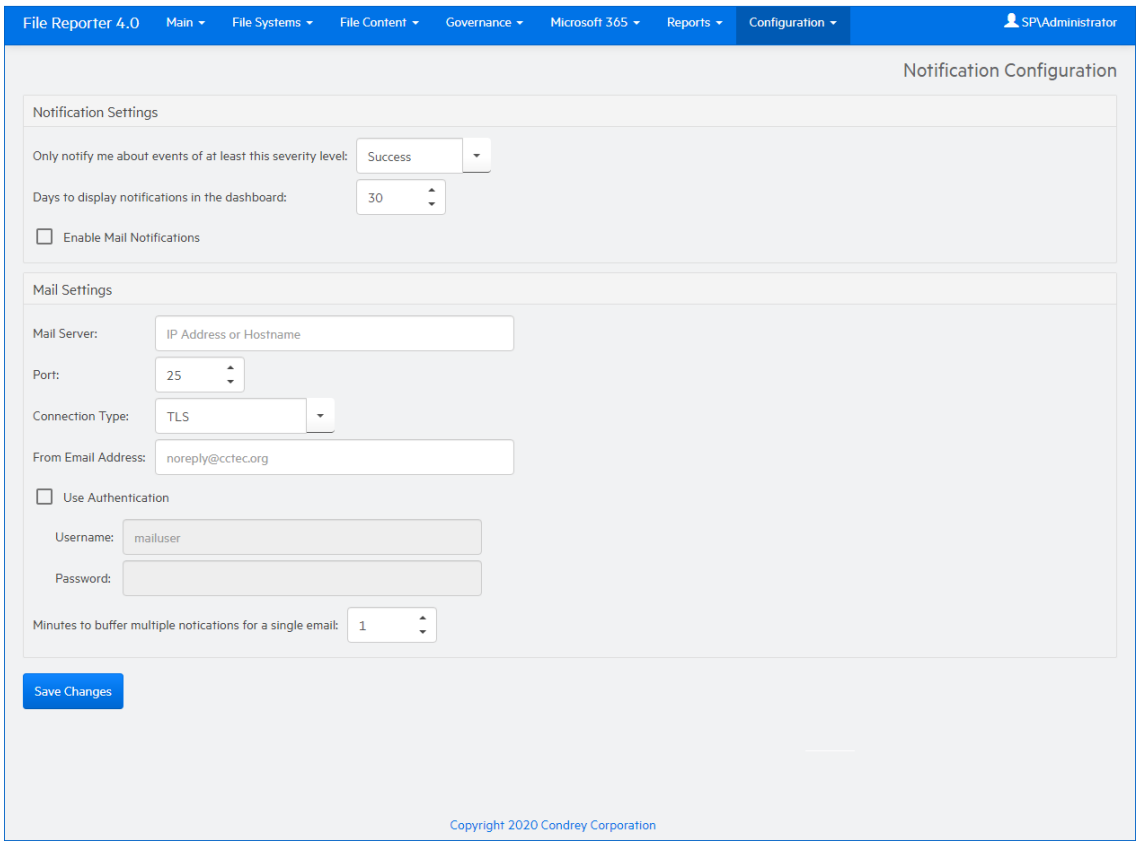


3 Select the proxy targets and click **OK**.

4.3 Configuring Notifications

Notification parameters specify what types of notifications are listed and how email notifications are sent.

1 Select **Configuration** > **Notifications**.



Only notify me about events of at least this severity level: This field lets you specify the severity level of events that are recorded and displayed in the Notifications page and through email notifications.

The severity levels are listed from lowest to highest, with **Success** being the default setting.

If you change the severity level, File Reporter records and displays only the events for that severity level and higher. Older notifications from formerly recorded severity levels continue to be displayed in the Notifications page. For example, if you change the setting from **Success** to **Warning**, only warning and error events are recorded, but the formerly recorded success and info events are still displayed, unless you filter them out.

To avoid receiving emails for every successful event, you should modify this setting to a more restrictive level.

Days to display notifications in the dashboard: This field indicates the number of days an event is listed in the Notifications page.

Enable Mail Notifications: Clicking this activates the fields in the **Mail Settings** region of the page.

Email notifications are sent to all members of the SrsAdmins group. File Reporter finds each member's email address from Active Directory.

Mail Server: Specify the IP address or hostname of the mail server to use for sending the email notifications.

Port: Specify the port number used by the mail server.

Connection Type: Specify the encryption type used by the mail server.

From Email Address: Specify the address you want displayed in the **From** field of the email notifications that are sent.

Use Authentication: If your mail server requires authentication, select this.

Username: Specify the mail server username.

Password: Specify the mail server password.

Minutes to buffer multiple notifications in a single email: File Reporter can consolidate messages into a single email notification. If you change this setting to 5, File Reporter consolidates all of the events that took place in 5 minutes and emails you a notification.

2 Specify your notification parameters and click **Save Changes**.

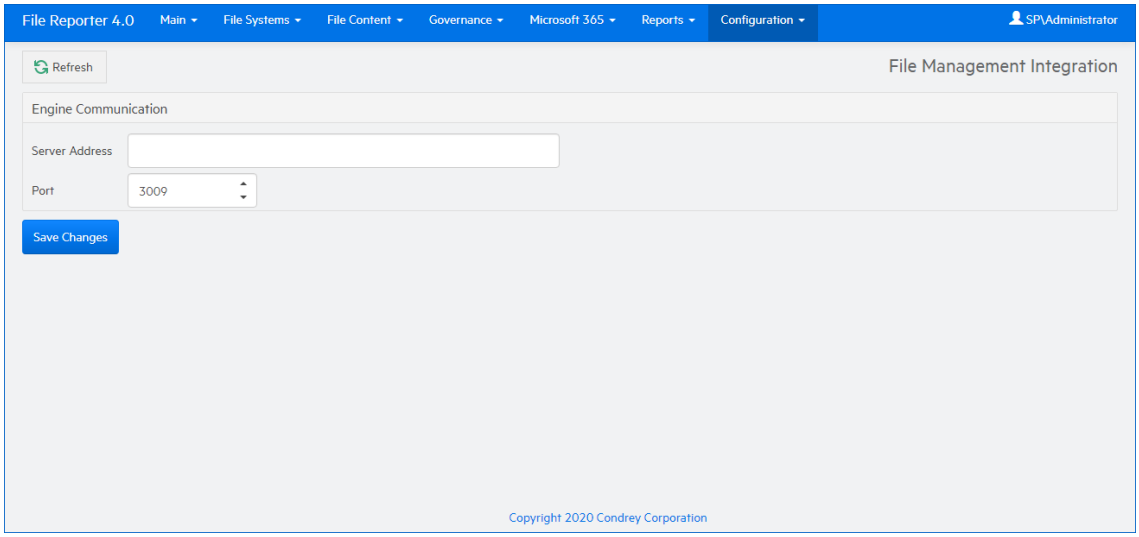
4.4 Integrating with File Dynamics

If you have Micro Focus File Dynamics deployed, you can use Micro Focus File Reporter to report on File Dynamics policies. Before you can do so, you must first specify the server address and port number of the server hosting the File Dynamics Engine.

IMPORTANT: File Reporter 4.1 integrates with File Dynamics 6.5 and above.

---

1 Select **Configuration** > **File Management**.



2 Specify the IP address or DNS name of the server hosting the File Dynamics Engine.

3 Specify the port number that the Engine is using.

The default port number is 3009.

4 Click **Save Changes**.

5 File System Scans

This chapter provides procedures for scanning your Microsoft network file systems.

5.1 Overview

Through AgentFS, Micro Focus File Reporter takes a file system “scan” of the file system’s storage resource at a given moment. A storage resource is a Microsoft network share.

File system scans are indexed data that are specific to a storage resource. They are the means of generating a storage report or analytics views. Scans include comprehensive information on the file types users are storing, when files were created, when they were last modified, permission data on the folders where these files reside, and much more.

File Reporter collects file system scans from the Agents, compresses them, and sends them to the Engine, where the Scan Processor takes them and uploads them to the database.

File system scans can be taken at any time, but we recommend using a scheduled time after normal business hours to minimize the effect on network performance.

You should consider a number of factors as you decide how often to conduct a file system scan:

- Although daily scanning always provides the most up-to-date information, scanning is not throttled and might place a considerable load on the server hosting the Agent.
- Most storage resources do not change rapidly enough to justify daily scanning.
- Monthly scanning places the least total load on individual servers and on the network, but scans are not as up-to-date as they could be.
- You can scan frequently-changing shares more often and scan the more static shares less often.
- Part of the decision concerning scanning frequency involves the primary purpose of the reporting. Reporting on storage trending can generally use less frequent scans, but reporting that is intended to solve immediate problems, such as “Who filled up this volume?” needs more frequent scans.

- When information is needed immediately, you can manually trigger a scan.
- For installations where you are not sure of the optimal scanning frequency, you can start with weekly scanning, and then adjust that interval based on the needs of the particular site.

5.1.1 Scan Retention

By default, File Reporter only retains the most current file system scan and permissions scan of a storage resource. However, if you want to generate Historic Comparison reports, which let you compare two scans of the same storage resource over two points in time, you will need to specify that scans be retained. Depending on the retained scan type, this is done either manually or automatically.

Manual Retention

You can specify that a file system or permissions scan be retained indefinitely as a "Baseline scan" by manually specifying it in the Scan Data page. For procedures and more information on Baseline scans, see Section 5.5, "Baseline Scans," on page 45.

Automatic Retention

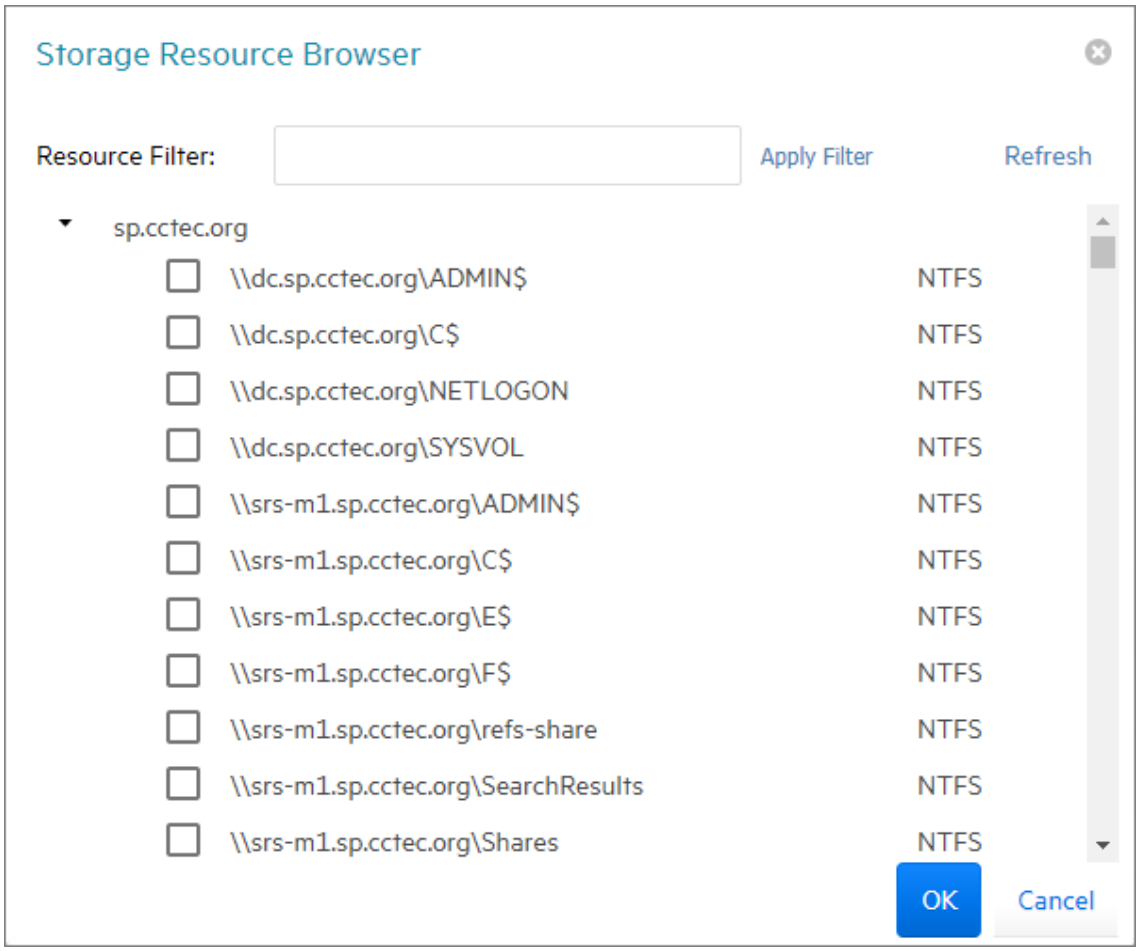
Within the scan policy, you can specify that the last file system scan or permissions scan be retained when a new file system scan or permissions scan is conducted. This version is known as a "Previous scan." For procedures and more information on Previous scans, see Section 5.3, "Scan Policies," on page 38.

5.2 Scan Targets

5.2.1 Adding a Scan Target

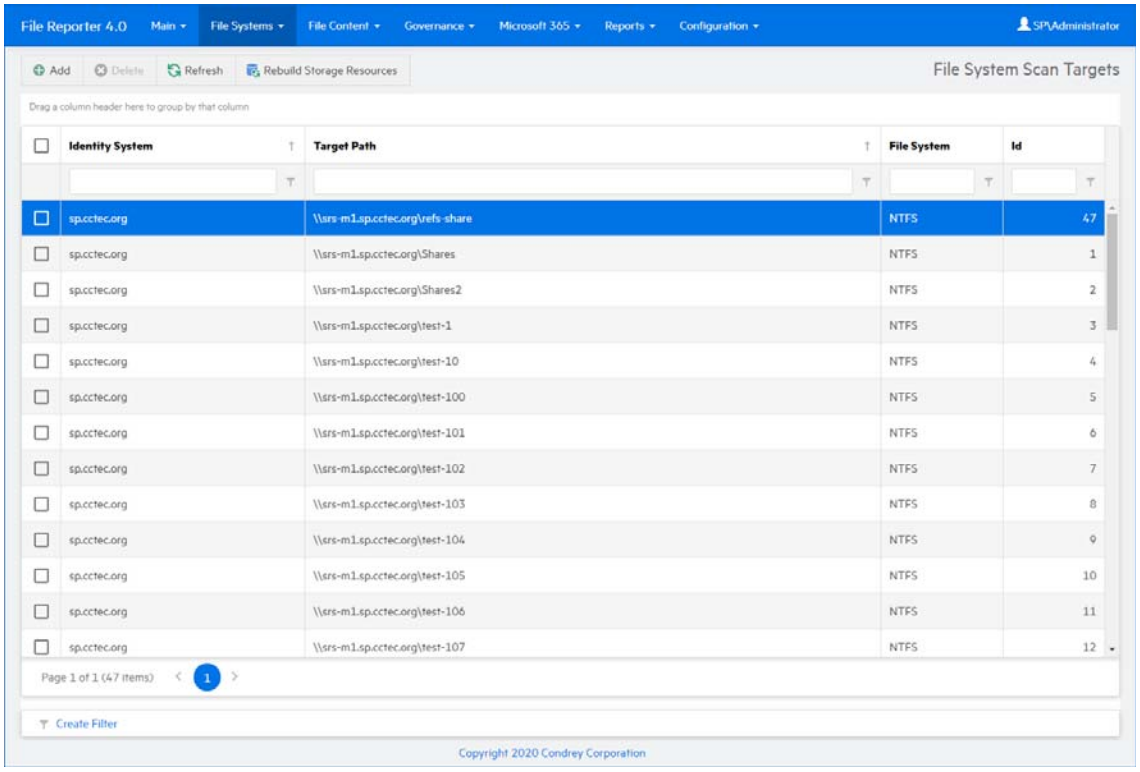
All shares must first be specified as a scan target before they can be scanned.

1. Select **File Systems** > **Scan Targets**.
2. Click **Add**.
3. Click the > to view the shares of the listed servers.



4 Select the shares you want File Reporter to be able to scan and click **OK**.

The scan targets are added.



5.2.2 Removing a Scan Target

1. Select **File Systems** > **Scan Targets**.
2. Select the check box pertaining to the share you want to remove as a scan target and click **Delete**.
3. When the confirmation dialog box appears, click **Yes**.

5.3 Scan Policies

5.3.1 Creating a Scan Policy

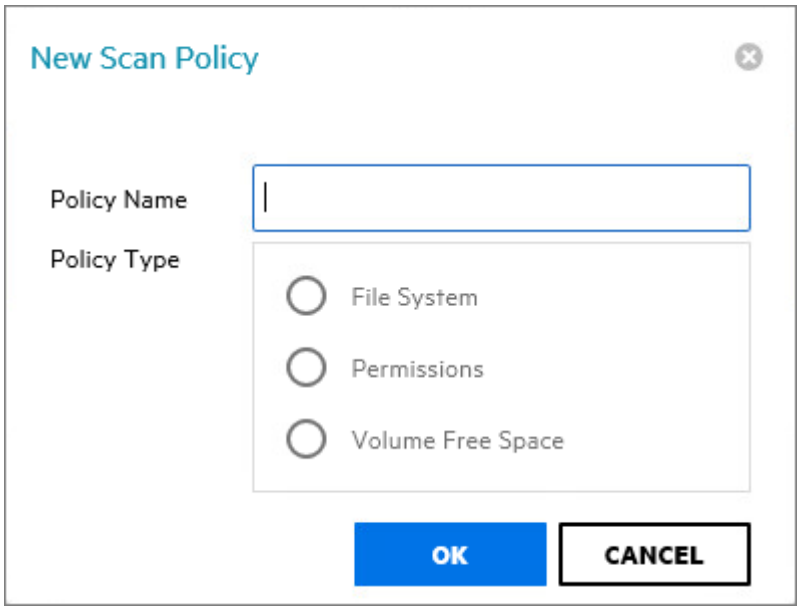
The specifications for a scan are established in a scan policy. The scan policy specifies the following parameters:

- What type of scan to conduct (File System, Permissions, or Volume Free Space)
- The scan targets
- Scan retry settings
- The scan schedule

IMPORTANT: The scan policy name must be unique. If you attempt to give the scan policy an existing name, File Reporter generates an error.

1 Select **File Systems** > **Scan Policies**.

2 Click **Add**.



3 In the **Scan Policy Name** field, specify a name for the scan policy.

You can provide a description of the policy in the next dialog box.

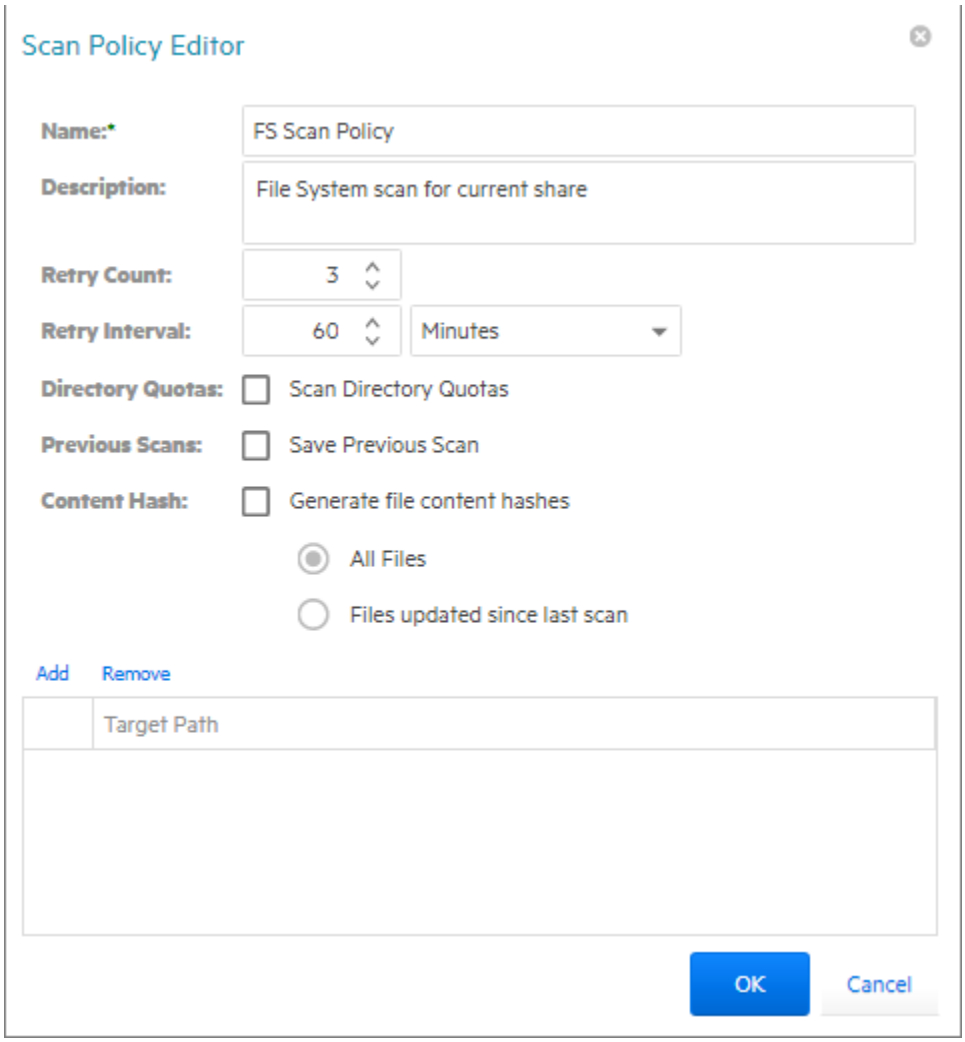
4 Select the type of scan that File Reporter is to conduct.

File System: Scans the files currently stored on the network share, the size of those files, when the files were last accessed, the locations of duplicate versions, and so forth.

Permissions: Scans the permissions pertaining to the folders stored on the shares.

Volume Free Space: Scans the availability of free space on the shares.

5 Click **OK**.



Name: Displays the name of the scan policy.

Description: Specify a description of the scan policy in this field.

Retry Count: Specify the number of times File Reporter attempts to scan the storage resource targets listed in the scan policy if there is a failure.

Retry Interval: Specify the amount of time before File Reporter retries scanning the storage resource targets listed in the scan policy if there is a failure.

Directory Quotas: By default, a scan does not include home folder quota information, because gathering this information on Windows shares can extend the scan time significantly. Unless you plan to generate a Directory Quota report, we recommend that you leave this option deselected.

This option applies only to File System scans.

Previous Scans: This option lets you specify whether to keep the previous version of a scan generated through this policy. This scan is known as the "Previous scan" which you can then use to generate a Historic Comparison report through a comparison with either a Baseline scan or a "Current scan." For more information, see Section 10.9, "Historic Comparison Reports," on page 110.

Previous scans are designated whenever a new scan is performed. The new scan is the Current scan and the earlier scan becomes the Previous scan. When the target paths are eventually scanned again, the new scan becomes the Current scan, the earlier Current scan becomes the Previous scan, and the former Previous scan is deleted.

NOTE: If you want to maintain a scan indefinitely, you can do so by specifying it as a Baseline scan. For more information, see Section 5.5, “Baseline Scans,” on page 45.

The management of Previous scan retention occurs when processing a new scan. This means that if you deselect **Retain existing Previous scan**, no existing Previous scan will be removed at that time, but it will be removed when a new scan is processed.

Content Hash: Selecting this check box enables File Reporter to create a content-based hash for each file in the specified target path. These hashes can then be compared through a Custom Query report to find duplicate files based on hash comparisons.

While File Reporter has always had a Duplicate File report option in its built-in reports, its reporting is based solely on metadata comparisons. Generating a duplicate file report through content has comparisons can be much more accurate.

For more information on generating a duplicate file report through content-based hashes, see the *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*.

All Files: Selecting this check box creates a new individual hash for each file in the specified target path.

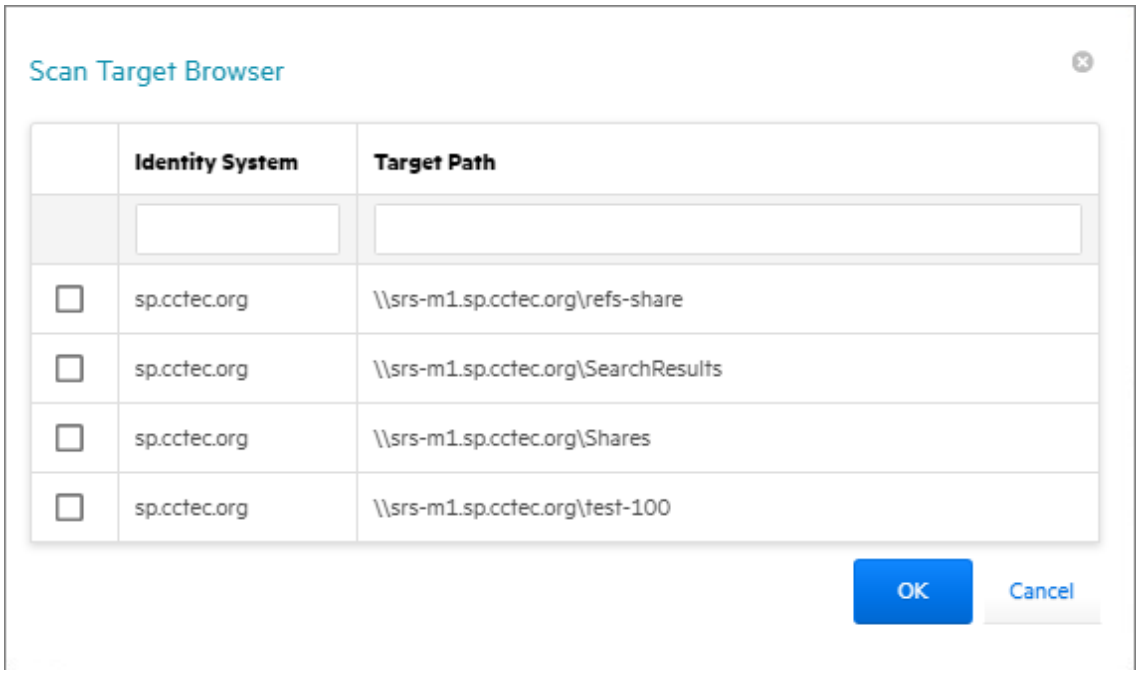
Files updated since last scan: Selecting this check box creates an individual hash for each file that does not already have a previously created hash or for files updates since the hash was created.

NOTE: Generating a content hash for each file will cause AgentFS to take longer to perform the scan. Generating hashes only for new or updated files can save a significant amount of time for subsequent scans.

Add: Click this option to specify the scan targets for the scan policy.

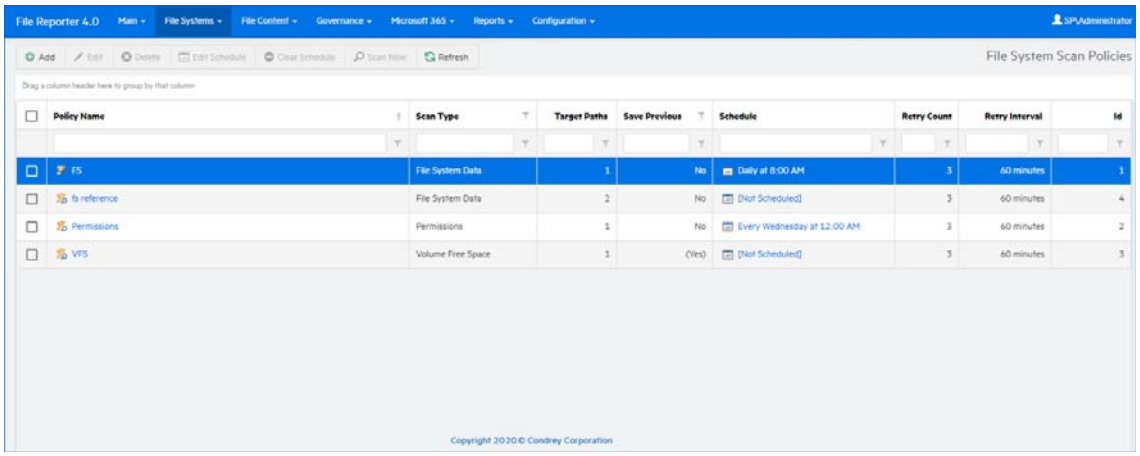
IMPORTANT: After a target has been added to a scan policy, the same target cannot be added to another scan policy of the same scan policy type.

Clicking **Add** brings up a dialog box like the one below where you can select available storage resources.



6 Click **OK** to save the scan policy.

The scan policy is now displayed on the Scan Policies page.



The scan policy still needs to be scheduled. For procedures on scheduling scans, go to Section 5.4, “Scan Scheduling,” on page 43.

5.3.2 Editing a Scan Policy

1 Select **File Systems** > **Scan Policies**.

2 Click the check box that pertains to the scan policy that you want to edit.

3 Click **Edit**.

4 Change any of the settings you wish.

5 Click **OK**.

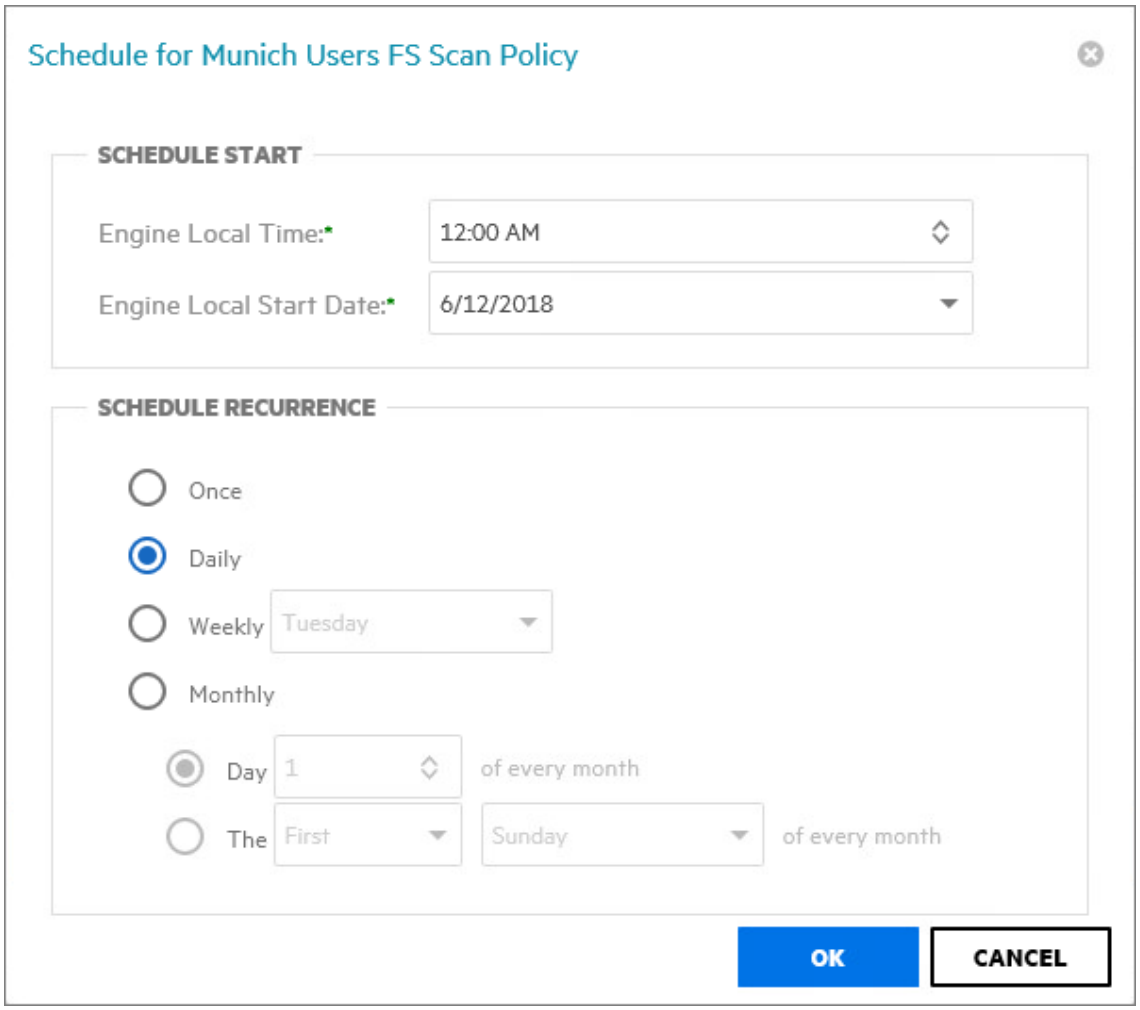
5.3.3 Deleting a Scan Policy

1. Select **File Systems** > **Scan Policies**.
2. Click the check box that pertains to the scan policy that you want to delete.
3. Read the warning and click **Yes**.

5.4 Scan Scheduling

5.4.1 Setting a Scan Schedule

1. Select **File Systems** > **Scan Policies**.
2. Click the check box that pertains to the scan policy for which you want to create a schedule.
3. Click **Edit Schedule**.



Engine Local Time: Specify the time that you want the scan to begin.

The time you select is based on the time zone where the Engine is located and not the Agent that conducts the scan.

Engine Local Start Date: Specify the date when you want the scan schedule to take effect.

Be aware that entering a date does not mean that the scan takes place on that date. If the **Engine Local Start Date** is set for today, which is a Monday, but the **Schedule Recurrence** setting is set for **Weekly** on Sunday, the scan does not take place until Sunday.

Once: Select this option to scan the storage resources specified in the scan policy only once.

Daily: Select this option for a daily scan of the storage resources specified in the scan policy.

Weekly: Select this option and specify a weekday for a weekly scan of the storage resources specified in the scan policy.

Monthly: Select this option and specify a day for a monthly scan of the storage resources specified in the scan policy.

4 Specify the scheduling parameters and click **OK**.

5.4.2 Editing a Scan Schedule

1. Select **File Systems** > **Scan Policies**.
2. Click the check box that pertains to the scan policy for which you want to edit a schedule.
3. Click **Edit Schedule**.
4. Make the schedule changes you want.
5. Click **OK**.

5.4.3 Clearing a Scan Schedule

1. Select **File Systems** > **Scan Policies**.
2. Click the check box that pertains to the scan policy for which you want to clear a schedule.
3. Click **Clear Schedule**.
4. When the confirmation prompt appears, click **Yes**.

5.4.4 Conducting an Immediate Scan

1. Select **File Systems** > **Scan Policies**.
2. Click the check box that pertains to the scan policy for which you want to conduct an immediate scan.
3. Click **Scan Now**.
4. When the confirmation prompt appears, click **Yes**.

5.5 Baseline Scans

A Baseline scan is a scan that you save as a reference for a comparison with another scan. You compare scans when you generate a Historical Comparison report. Unlike a Previous scan, which gets replaced as a new Current scan is created, a Baseline scan is retained indefinitely until you decide to delete it. You can have only one Baseline scan per scan target.

IMPORTANT: Because you can have only one Baseline scan per scan type for a scan target, establishing a scan as a Baseline will override any established Baseline scan of the same scan type for the same scan target.

5.5.1 Establishing a Baseline Scan

1. Select **File Systems** > **Scan Data**.
2. In the far left column, select the check box pertaining to the scan you want to set as a Baseline scan.

3 Click **Set Baseline**.

4 When the confirmation dialog box appears, click **Yes**.

5.5.2 Clearing a Baseline Scan

Scans designated as Baseline scans are retained until the baseline designation is cleared. If a Baseline scan that is in the Retained state has its Baseline status removed, that scan will be immediately marked for deletion.

1 Select **File Systems** > **Scan Data**.

2 In the far left column, deselect the check box pertaining to the scan you want to clear as a Baseline scan.

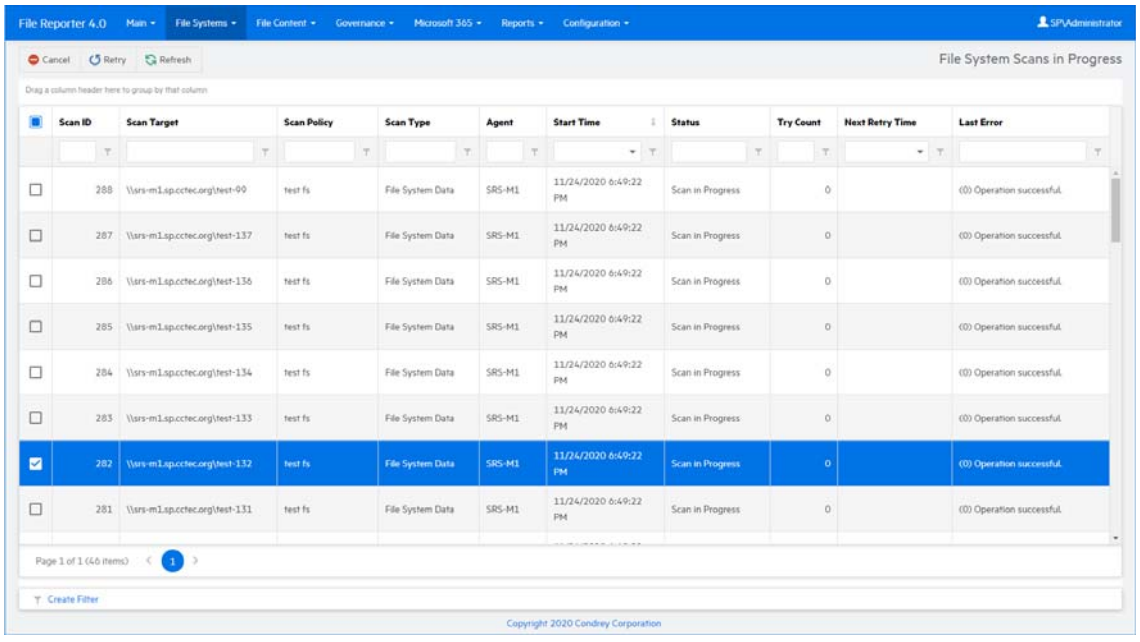
3 Click **Clear Baseline**.

4 When the confirmation dialog box appears, click **Yes**.

5.6 Scans in Progress

You can view details on the scans that are in progress through the Scans in Progress page. When the scan has been completed, you can view the details in the Scan History page.

1 Select **File Systems** > **Scans in Progress**.



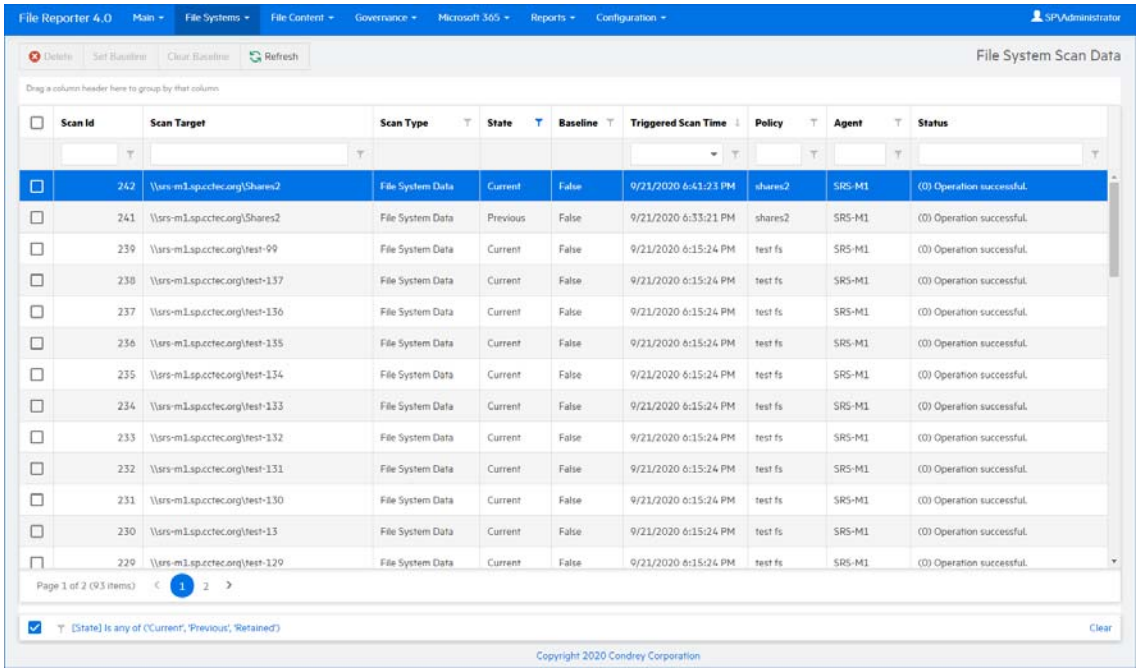
As you click **Refresh**, the completed scan listings are removed and listed in the Scan Data and Scan History pages.

5.7 Scan Data

5.7.1 Viewing Scan Data

The Scan Data page lets you view a minimal set of details pertaining to the currently available scans for each scan target.

1 Select **File Systems** > **Scan Data**.



5.7.2 Deleting Scan Data

To delete specific scan data:

1 Select **File Systems** > **Scan Data**.

2 In the far left column, select the check boxes of the scans you want to delete.

3 Click **Delete** in the menu at the top of the page.

A confirmation dialog box appears.

4 (Optional) Check the check box for **Delete Immediately** in the dialog box to perform the data cleanup immediately, instead of waiting for the next scheduled cleanup interval.

IMPORTANT: Consider leaving the **Delete Immediately** option unselected.

By default, the Delete Scans operation marks the selected scans for cleanup on the next maintenance interval and is performed by the Engine. This is the recommended option.

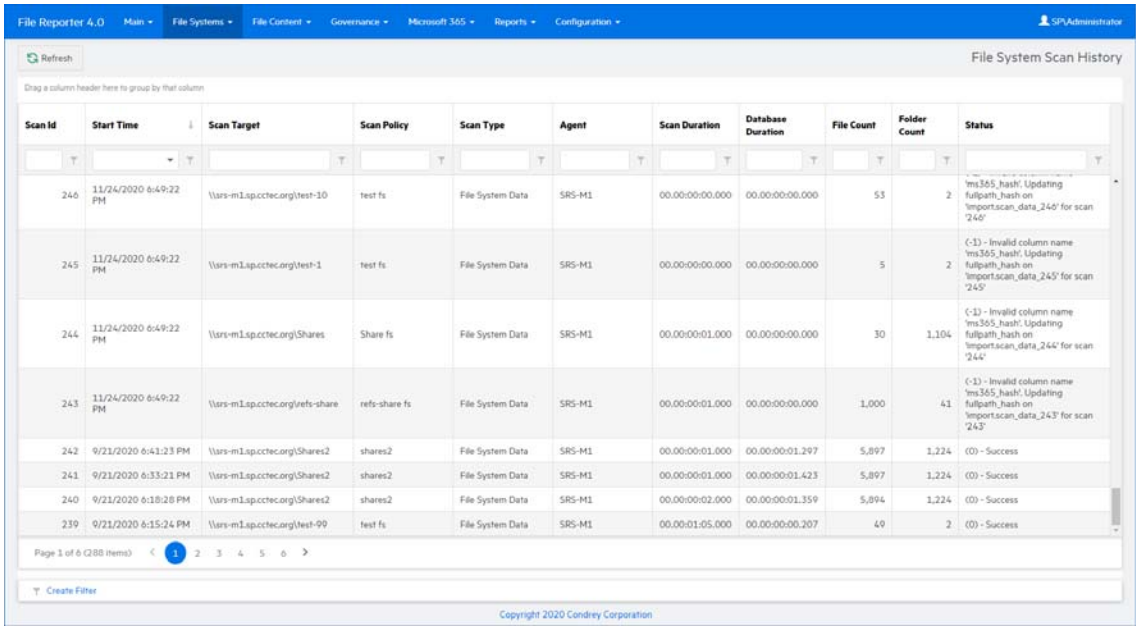
Deleting scans with the **Delete Immediately** option selected is performed by the Web Application directly and may result in timeout errors if the operation takes too long, especially with large scan sets.

5 Click **Yes** to confirm and close the dialog.

5.8 Scan History

The Scan History page displays a complete history of all scans, along with details of the scan and some basic information of the storage resource at the time of the scan, including the file and folder count.

1 Select **File Systems** > **Scan History**.



You can click the columns to list the data in ascending or descending order.

Because the Scan History page logs each successful scan, the most efficient way of locating a scan is using a filter.

5.9 Retrying Failed Scans

In the Scan Policy Editor dialog box, the default scan policy settings for **Retry Count** is three and the **Retry Interval** is 60 minutes. You can adjust each of these settings. Assuming the default settings are not adjusted, File Reporter retries the scan in 60 minutes and only retries to scan up to three times.

Until File Reporter has attempted all three retries, the failed scans remain listed on the Scans in Progress page. After all retries have been performed, the scan listing is moved to the Scan History page.

As long as a failed scan is listed on the Scans in Progress page, you can retry the scan manually by doing the following:

1. From the Scans in Progress page, select the check box corresponding to the failed scan.
2. Click **Retry**.

5.10 Troubleshooting

1. Verify that the Agent service is running properly on its host machine.
2. Verify that the host machine where the Agent is installed has enough free disk space to temporarily store a copy of the scan in its uncompressed and compressed form.
3. If an Agent is not installed directly on the server with the storage resource you want to scan, verify that a proxy assignment for the storage resource has been established.
4. If the proxy agent is not scanning, assign the storage resource from a different proxy agent and try scanning again.
5. Verify that the proxy rights group has been assigned the proper rights to the share.

   The proxy rights group must be assigned to the Builtin\Administrators group on the server where the scan is being conducted.
6. Verify that the Windows Firewall is configured to permit network traffic to flow between the Engine and the Agent.

   For more information on the Windows Firewall, see Section A.1, “Windows Firewall Settings,” on page 121.

6 Active Directory Identity Scans

File Reporter 4.1 performs scans across an extended collection of identities (security principals) in your Active Directory forest. The extended data collected with this process is available for use with Custom Query reports, direct review via the Identities page, or for use with other customer-defined processes that query the database directly.

6.1 Overview

6.1.1 Scope

Active Directory Identity Scan service scans for all identities across all domains in the associated Active Directory forest. Identities are classified as any object in Active Directory that has a valid Security Identifier (objectSid) attribute.

6.1.2 Collected Data

The collected data includes a predefined set of single-value attributes that enrich the basic identity metadata for users, groups, and other security principals found in Active Directory.

For a list of the currently included attributes, refer to the *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*.

NOTE: Multi-value attributes are currently not supported, except the objectClass attribute for which only the primary structural class value is collected.

Support for multi-value attributes such as group members, direct reports, and SID history will be added in a future release.

6.2 Performing Scans

6.2.1 Scheduling Identity Scans

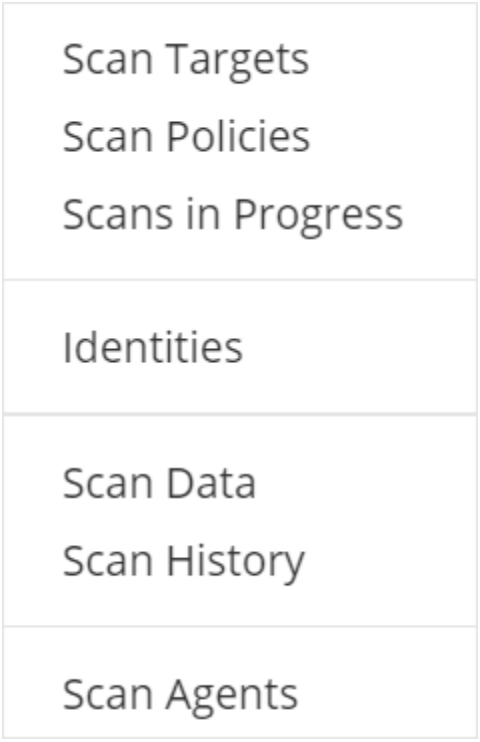
Active Directory Identity Scans run once per day at midnight.

Support for custom schedules will be added in a future release.

6.2.2 Performing an Immediate Scan

To perform an immediate scan of Active Directory identity objects:

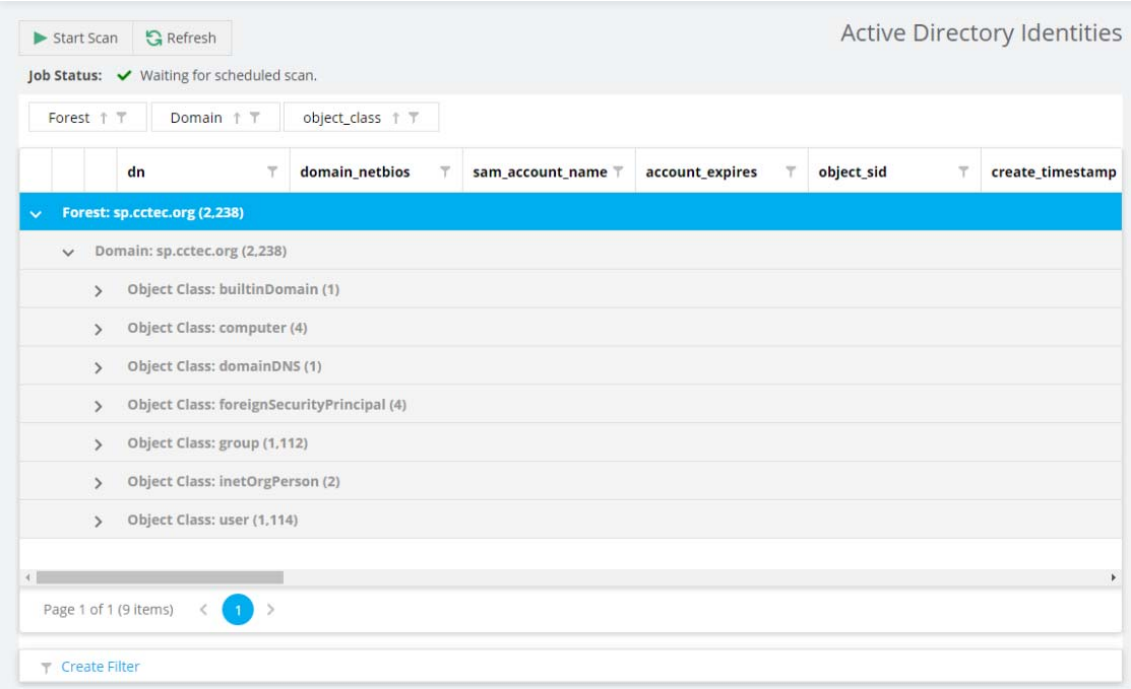
1. Log in to the File Reporter Web Application.
2. Select **File Systems** > **Identities**.



3. Click **Start Scan**.

6.3 Viewing Collected Identities

1. Log in to the File Reporter Web Application.
2. Select **File Systems** > **Identities**.



By default, the collected identities are grouped by domain and object type.

3 Use the search filters and grouping capabilities of the grid display to gain insight into the collected identities and assist with Custom Query reports.

6.4 Extending Custom Query Reports

For an example of creating a Custom Query report with extended identity information, refer to the Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide.

7 File Content Scanning

In addition to generating file system, permissions, and trending reports, File Reporter customers can also analyze their files based on content. By analyzing content, organizations can locate files containing confidential, sensitive, and personal information that should be given restricted access, moved to a more secure location, or deleted.

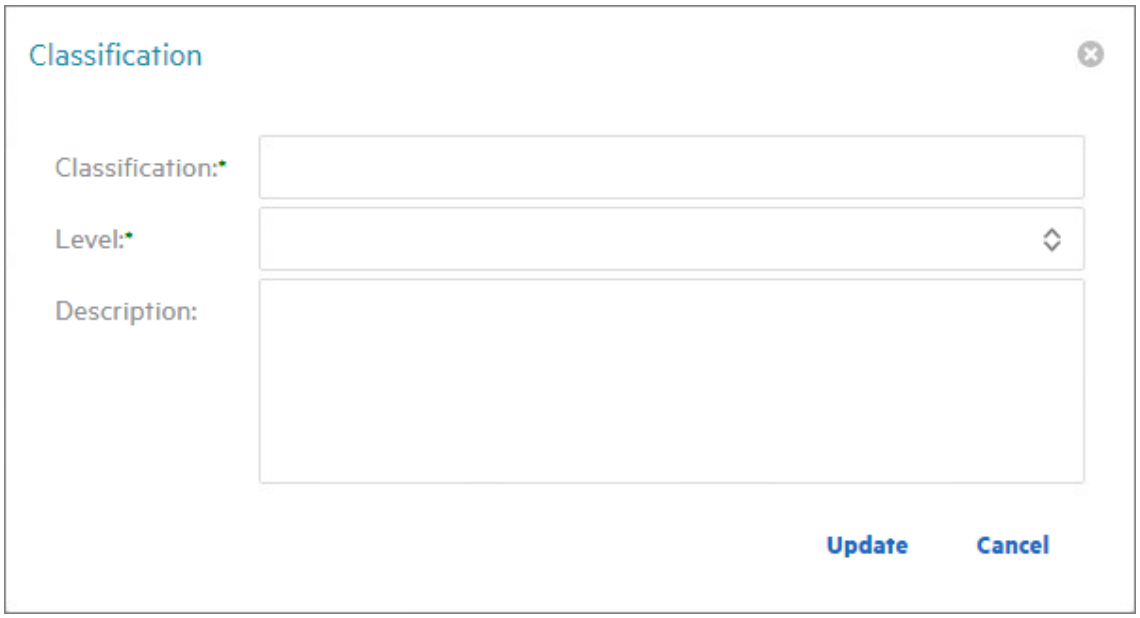
All File Content procedures are performed through the **File Content** menu options.

7.1 File Content Classifications

File content classifications are needed by File Reporter as a search parameter. For your convenience, File Reporter includes three classifications and severity levels. You can modify this list by editing the settings or creating your own classifications.

7.1.1 Creating a New Classification

1. Select **File Content** > **Classifications**.
2. Click **Add**.



3 In the **Classification** field, enter a name.

   For example, Private.

4 From the **Level** field, specify a severity level for the new classification.

   For example, 400.

5 In the **Description** text box, enter a description for the new classification.

   For example, High-risk private information, not intended for public disclosure.

6 Click **Update**.

7.1.2 Editing a Classification

1 Select **File Content** > **Classifications**.

2 Select the classification you want to edit.

3 Click **Edit**.

4 Edit the fields.

5 Click **Update**.

7.2 File Content Categories

Categories are an additional way of refining your search parameters. For your convenience, File Reporter includes three standard categories. You can modify this list by creating your own classifications.

7.2.1 Creating a New Category

1 Select **File Content** > **Categories**.

2 Click **Add**.

3 In the **Category** field, enter a name.

For example, National ID.

4 In the Description text box, enter a description for the new category.

For example, US Social Security Numbers as well as other national ID schemes.

5 Click **Update**.

7.2.2 Editing a Category

1 Select **File Content** > **Categories**.

2 Select the category you want to edit.

3 Click **Edit**.

4 Edit the fields.

5 Click **Update**.

7.3 File Content Search Patterns

Search patterns specify the conditions for the content scanning, along with how you want to classify and categorize the results.

File Reporter utilizes regex search strings for conducting content scanning. Regex is short for “regular expression,” a special text string describing and defining a search pattern. Regex search strings are ideal for locating files containing specified patterns (e.g. Social Security numbers, credit card numbers, etc.) or other user-defined patterns.

File Reporter currently makes use of Microsoft's .NET regular expressions engine. For basic information and tutorials on compiling regular expression search strings, see the following sites:

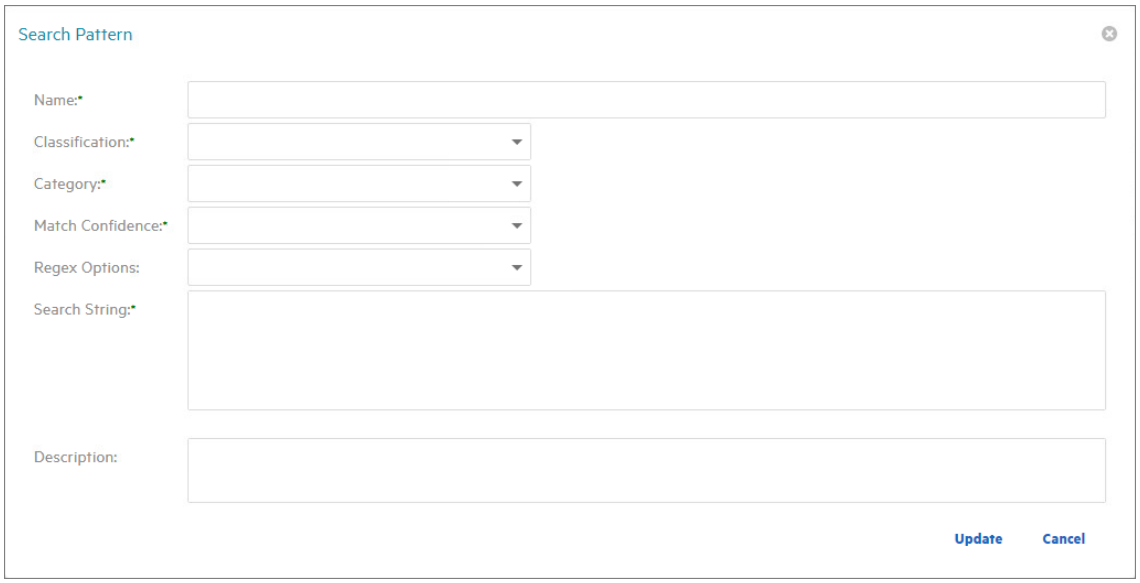
- https://regexone.com
- https://www.regular-expressions.info/tutorial.html
- https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expressions

---

NOTE: For cases where different regex engines or languages are mentioned, note that this version of File Reporter makes use of the C# (.NET) regular expression variant.

7.3.1 Creating a New Search Pattern

1. Select **File Content** > **Search Patterns**.
2. Click **Add**.



3. In the **Name** field, enter a descriptive name for the search pattern.

   For example, Social Security US - High.

   Names are restricted to A-Z, a-z, 0-9, space, - (hyphen), and_ (underscore).
4. From the **Classification** drop-down menu, select a classification.
5. From the **Category** drop-down menu, select a category.
6. From the **Match Confidence** drop-down menu, select either **Low**, **Medium**, or **High**.

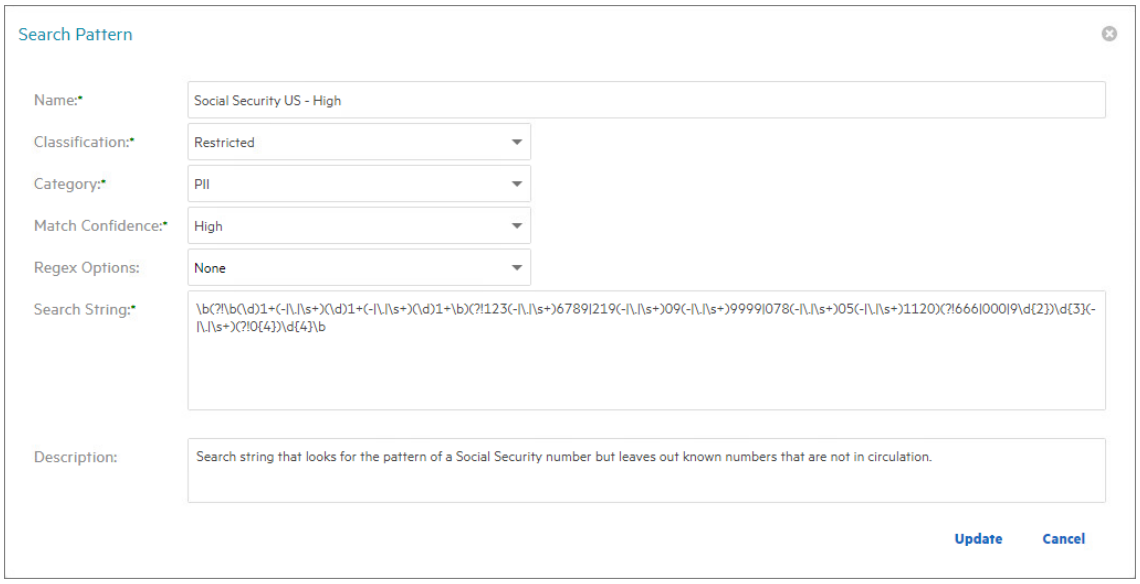
These designations allow you to indicate your confidence in the search pattern. Selecting **High** does not necessarily make the match confidence better than selecting **Low**. It simply indicates your confidence in results of the search, based on the depth of the Regex search string. For example, a search for all Social Security numbers might be **Low**, while a search for a particular Social Security number specified in the regex string would be **High**.

7 In the **Regex Options** drop-down menu, select any applicable options.

For an explanation of these options, we recommend referring to the following: https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-options.

8 In the **Search String** text box, enter or paste the search string.

9 In the **Description** text box, enter a description of the search pattern.



10 Click **Update**.

7.3.2 Editing a Search Pattern

1 Select **File Content** > **Search Patterns**.

2 Select the search pattern you want to edit.

3 Click **Edit**.

4 Edit the fields.

5 Click **Update**.

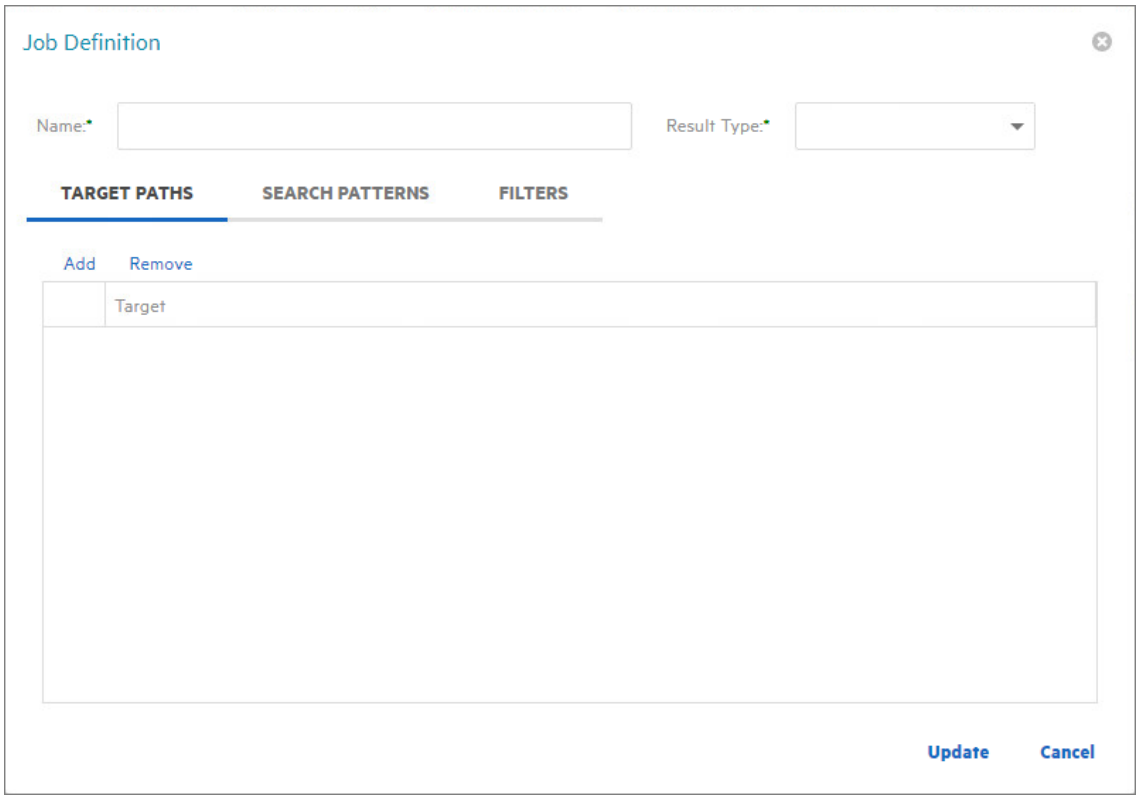
7.4 File Content Jobs

A job definition specifies the file system paths where the content scanning will take place, the search patterns that will be applied, the filters for the search, and where the content scanning results will be stored.

7.4.1 Creating a New Job Definition

1 Select **File Content** > **Job Definitions**.

2 Click **Add**.

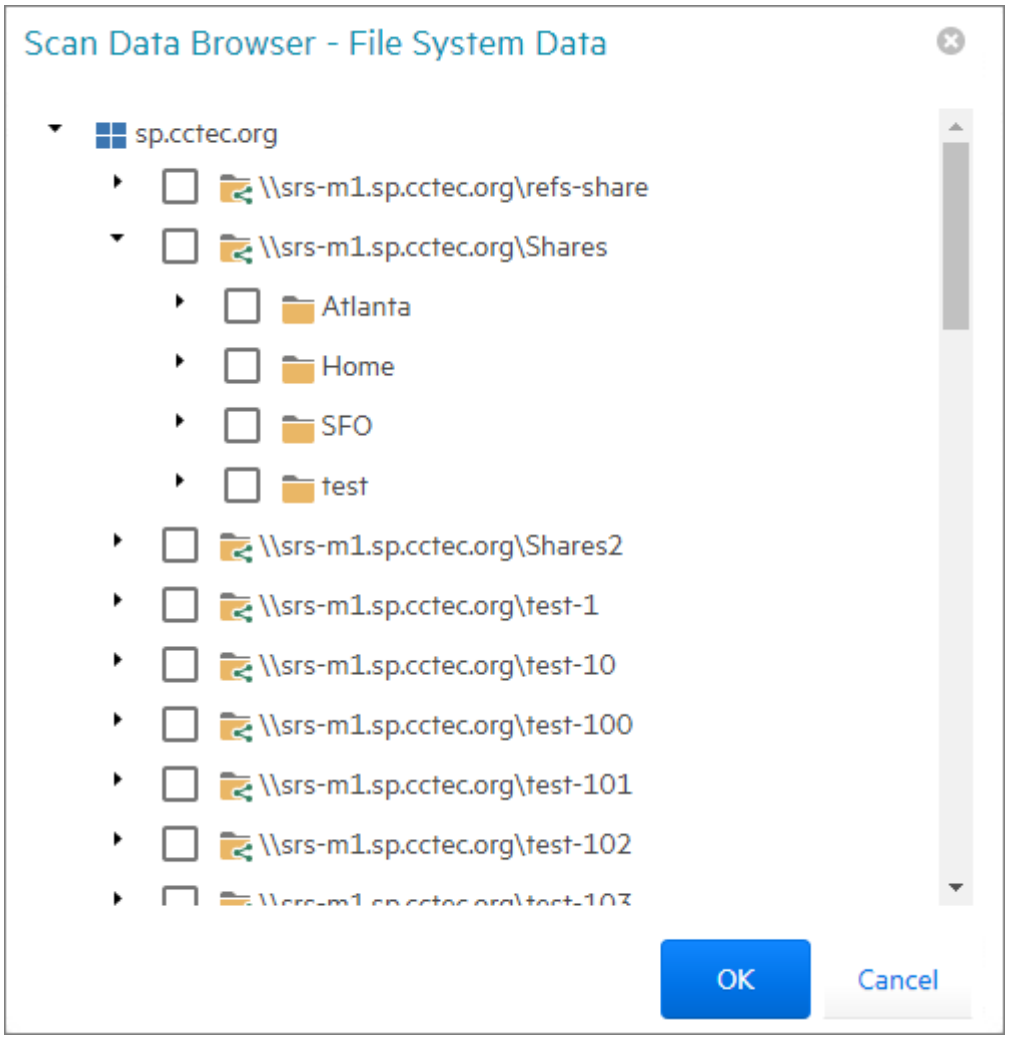


3 In the **Name** field, enter a descriptive name for the job definition.

4 From the **Result Type** menu, select from the following options:

- **Database:** This option saves the results of the content scan to the database, where you can use it to generate a report using the Report Designer. Having the scan in the database also allows you to search and report utilizing the established classifications and categories.
- **File:** This option saves the results of the content scan as a file in the `Search Results` share. You can access all saved files through the Search Results page.

5 From the Target Paths tab, click **Add**.



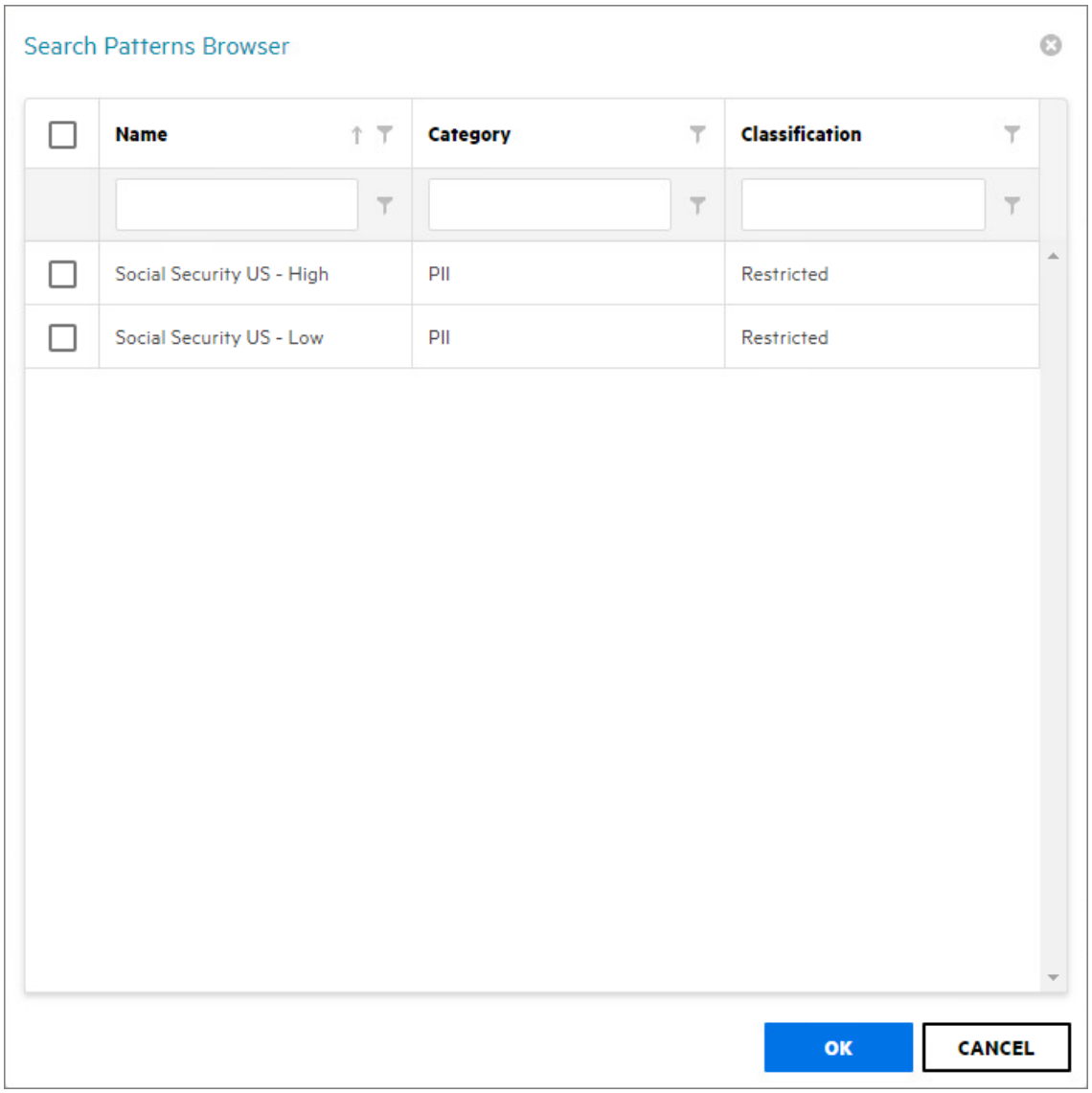
6 Select the targets where you want the file content to be scanned.

IMPORTANT: File paths appear in the Scan Data Browser - File System Data dialog box only if the paths have had a previous file system scan. If the path you want does not appear in the dialog box, you must first conduct a file system scan on the path.

7 Click **OK**.

8 Click the **Search Patterns** tab.

9 Click **Add**.



10 From the Search Pattern Browser, specify your search patterns and click **OK**.

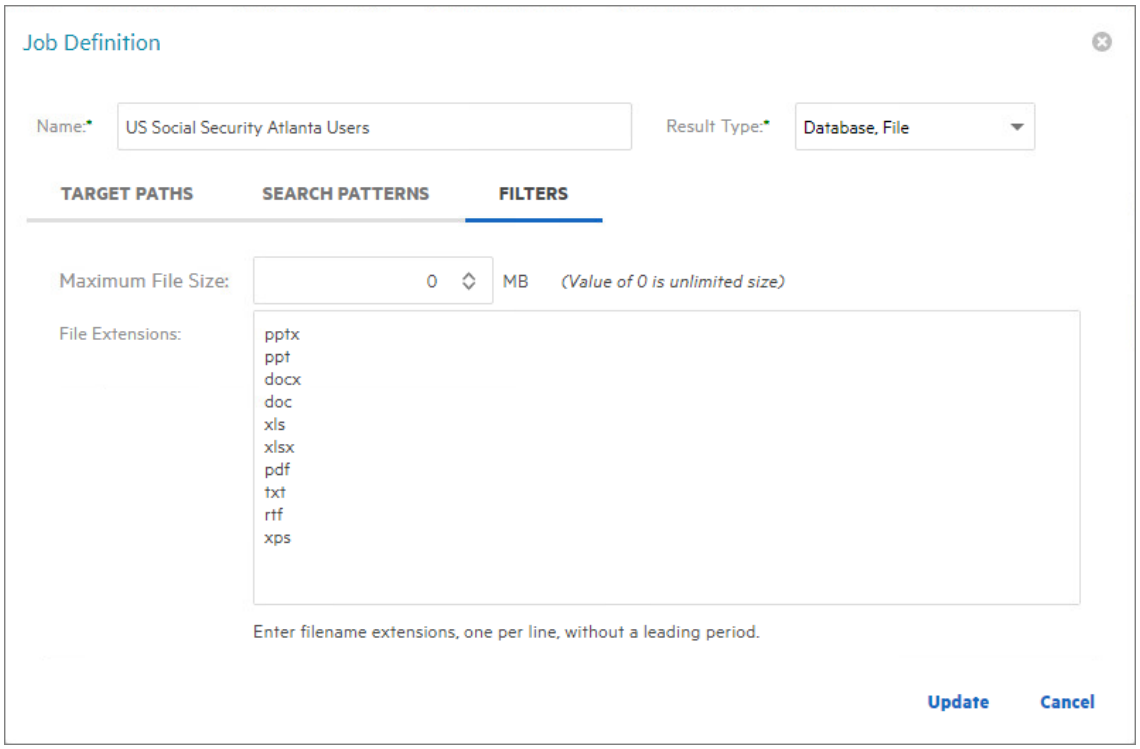
11 Click the **Filters** tab.

12 In the **Maximum File Size** field, specify the size of files that will not be scanned for content.

For example, large files such as ISO files should probably not be scanned. If you do not enter a setting in this field, all files in the file path will be scanned.

13 In the **File Extensions** text box, specify the file types that you want scanned.

If you do not specify file extensions, all files in the file path will be scanned.



14 Click **Update** to save the job definition settings.

7.4.2 Editing a Job Definition

1 Select **File Content** > **Job Definitions**.

2 Select the job definition you want to edit.

3 Click **Edit**.

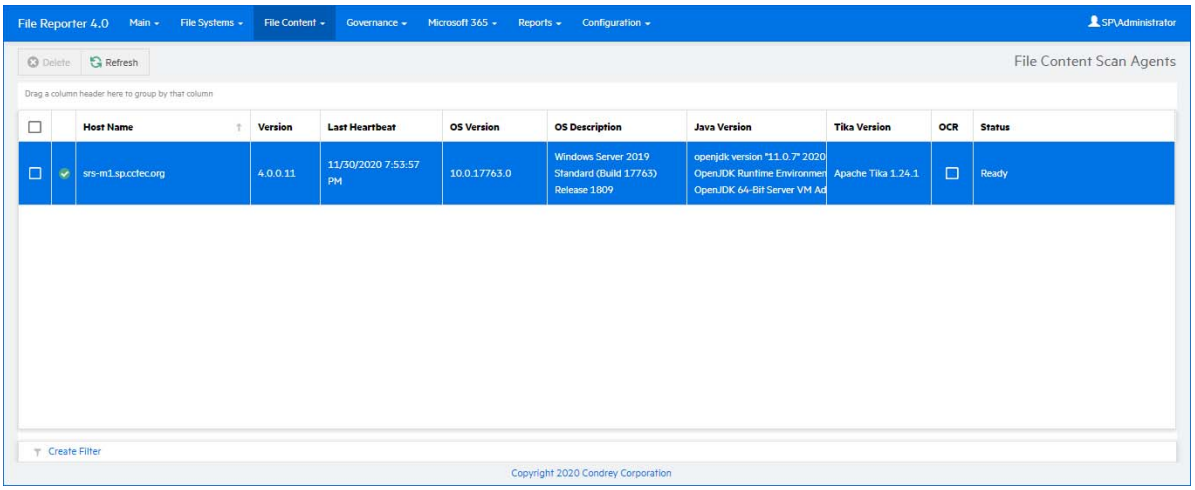
4 Edit the fields.

5 Click **Update**.

7.5 Managing File Content Scans

7.5.1 Verify AgentFC Registrations

You can view the version and the last heartbeat for each deployed AgentFC by selecting **File Content** > **Agents**.



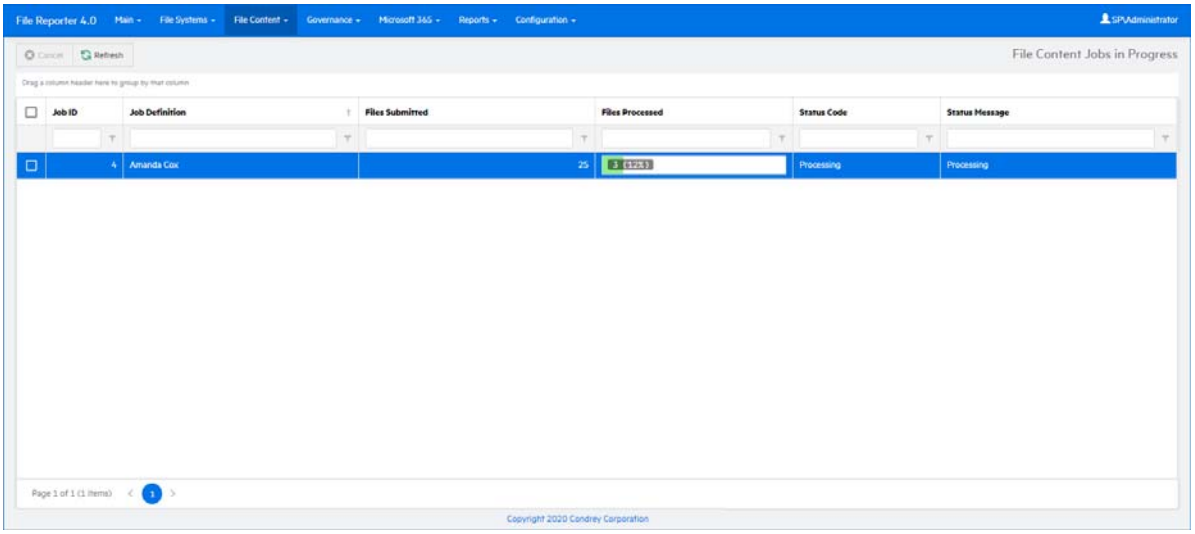
This page can be used to verify the consistency of AgentFC deployments and configuration parameters.

7.5.2 Start a File Content Scan Job

1. Select **File Content** > **Job Definitions**.
2. Select the check box for the job definition to run.
3. Click **Scan Now** in the toolbar to initiate the selected File Content Scan Job.

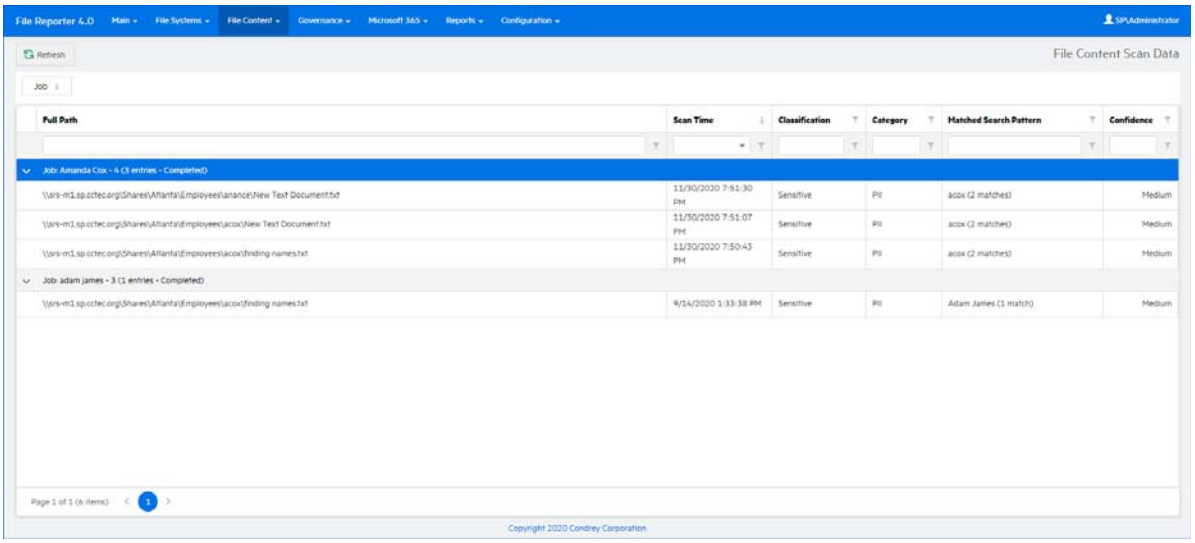
7.5.3 Viewing Jobs in Progress

You can view the status of file content scanning jobs in progress by selecting **File Content** > **Jobs in Progress**.



7.5.4 Viewing Scanned Data Matches

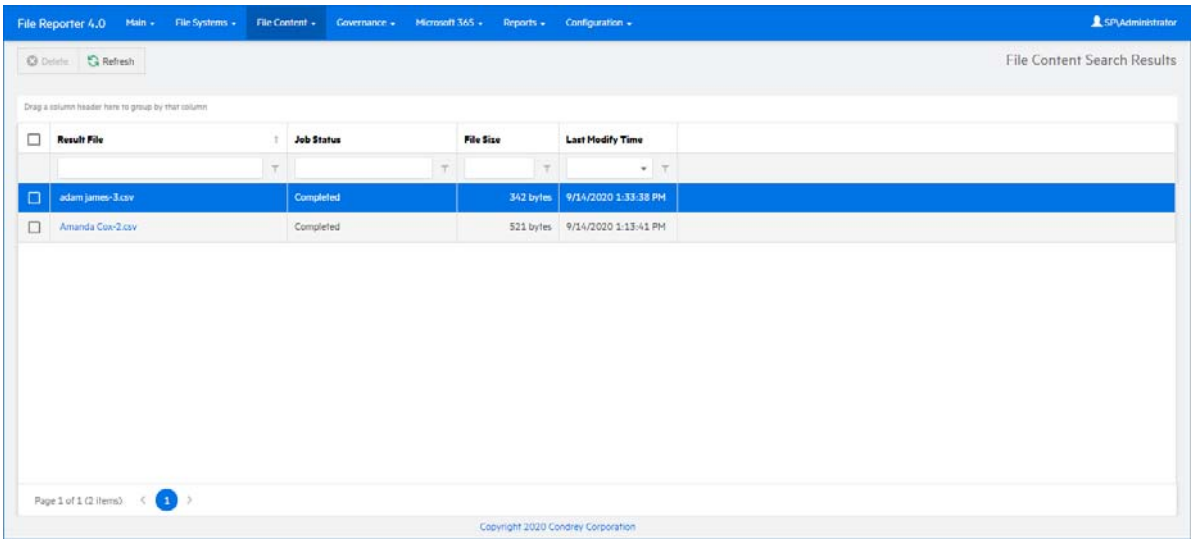
You can view the set of matched results data by selecting **File Content** > **Scan Data.**



7.5.5 Download Search Results

For those job definitions where the **Result Type** setting is set to **File**, you can download the file content scan file from the Search Results page.

File Reporter outputs the file as a CSV file so that if you desire, you can import the file into the Micro Focus File Dynamics Data Owner Client where a Data Owner can perform remediation work.



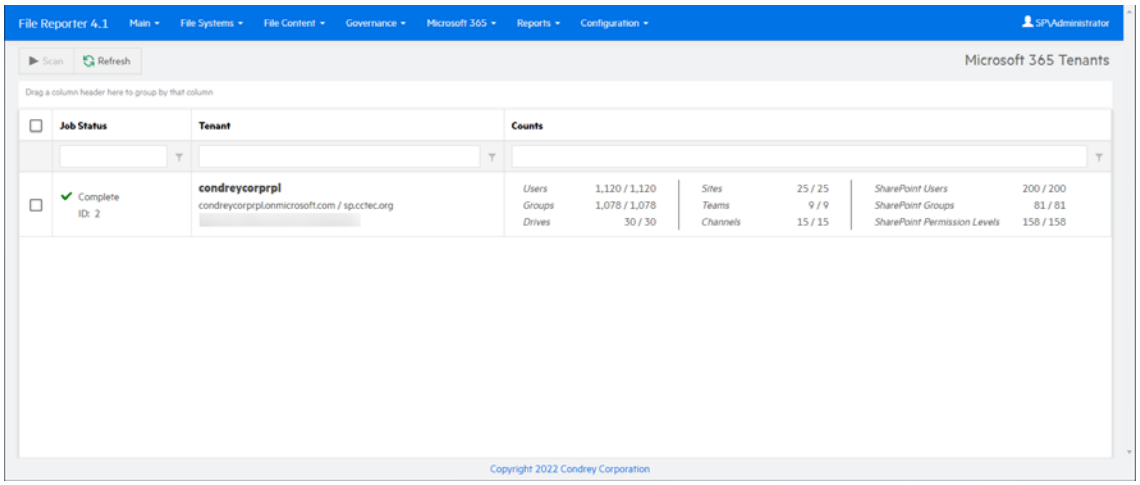
8 Microsoft 365 Scans

Scanning your Microsoft 365 tenant identifies all users and groups, the associated drives, sites and associated libraries, teams and their associated libraries, and channels and their associated libraries. A tenant scan includes details pertaining to the file system structure, individual files, and file and folder permissions.

8.1 Tenants

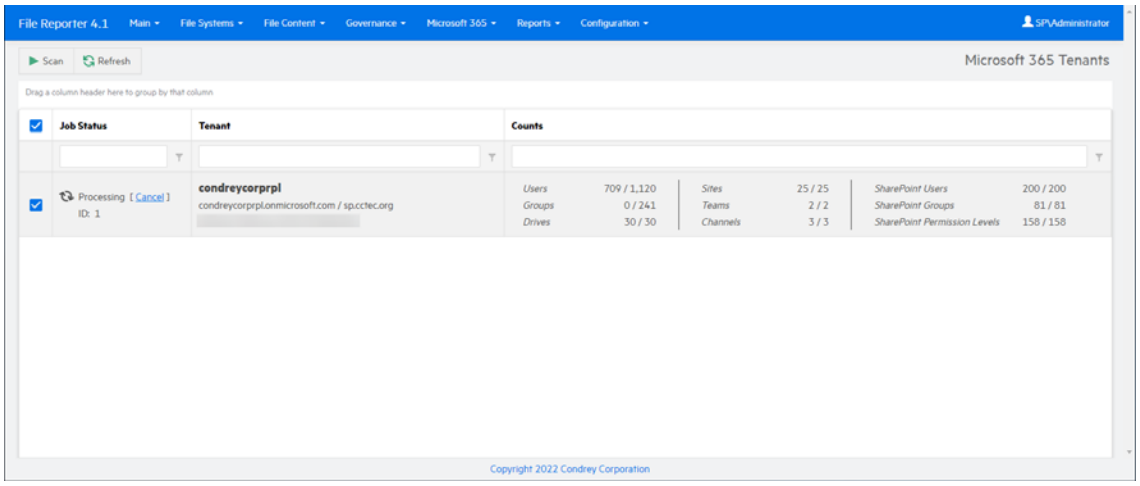
To scan the Microsoft 365 Tenant:

1 Select **Microsoft 365** > **Tenant.**

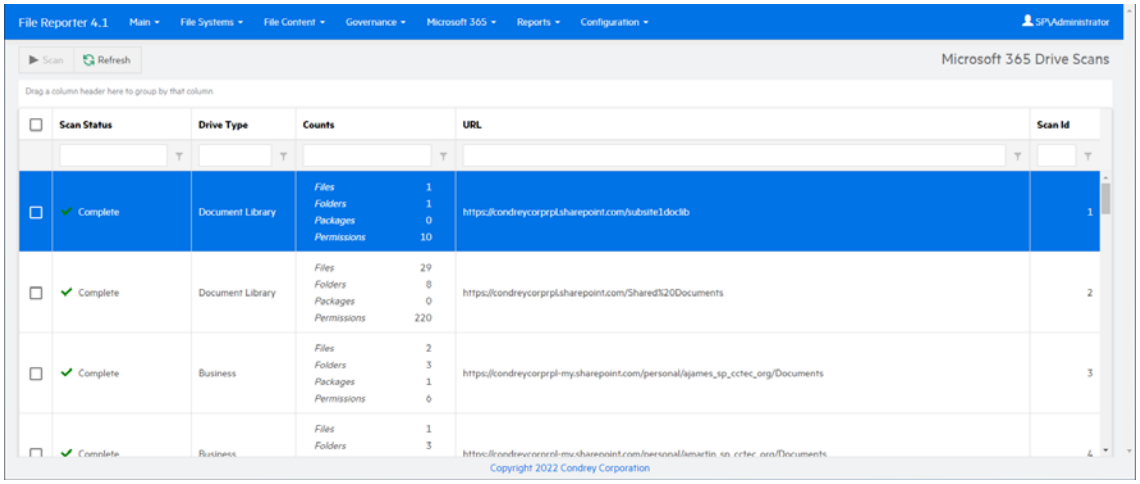


2 Select the check box associated with the listed tenant, then click **Scan**.

The progress of the scan is displayed in the **Counts** column.



You can also monitor the progress of the scan among the various drives by selecting **Microsoft 365** > **Drives**.



Once the Job Status column indicates that the scan is complete, you can then generate a Microsoft 365 report. For details, see the *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*.

8.2 Drives and Document Libraries

There might be instances where after the initial tenant scan, that changes were made to only a select number of libraries. Rather than rescan the entire tenant, you can select the specific drives to scan.

NOTE: More significant changes, such as the addition of a new team and consequently the creation of a new drive, requires a tenant scan for the drive to be scanned.

---

1. Select **Microsoft 365** > **Drives**.
2. Select the check boxes associated with the listed drives you want to scan, then click **Scan**.

9 Reporting

File Reporter provides an extensive set of reporting options for each of the supported repository types and targets.

9.1 Built-in Reports

File Reporter provides several built-in report templates for Windows file system targets. Each template includes customizable parameters specific to the report type and includes categories such as:

- File system metadata reporting
- Permissions reporting
- Historic comparison reporting for changes in permissions or metadata over time
- Volume free space trending

NOTE: For details on built-in reports, see Chapter 10, “Built-in Reports,” on page 81.

9.2 Custom Query Reports

For cases where customized file system reporting is required or for repository types where built-in reports are not available, such as Microsoft 365, Custom Query reporting provides an advanced interface for querying collected scan data and laying out report data results.

A Custom Query report may be configured as just a simple SQL query with delimited text output, or it may include both the SQL query as well as a detailed report layout definition to assist with the presentation of charts, grouping, and custom layouts, as well as provide exports for various formats including PDF, HTML, and Excel spreadsheet exports.

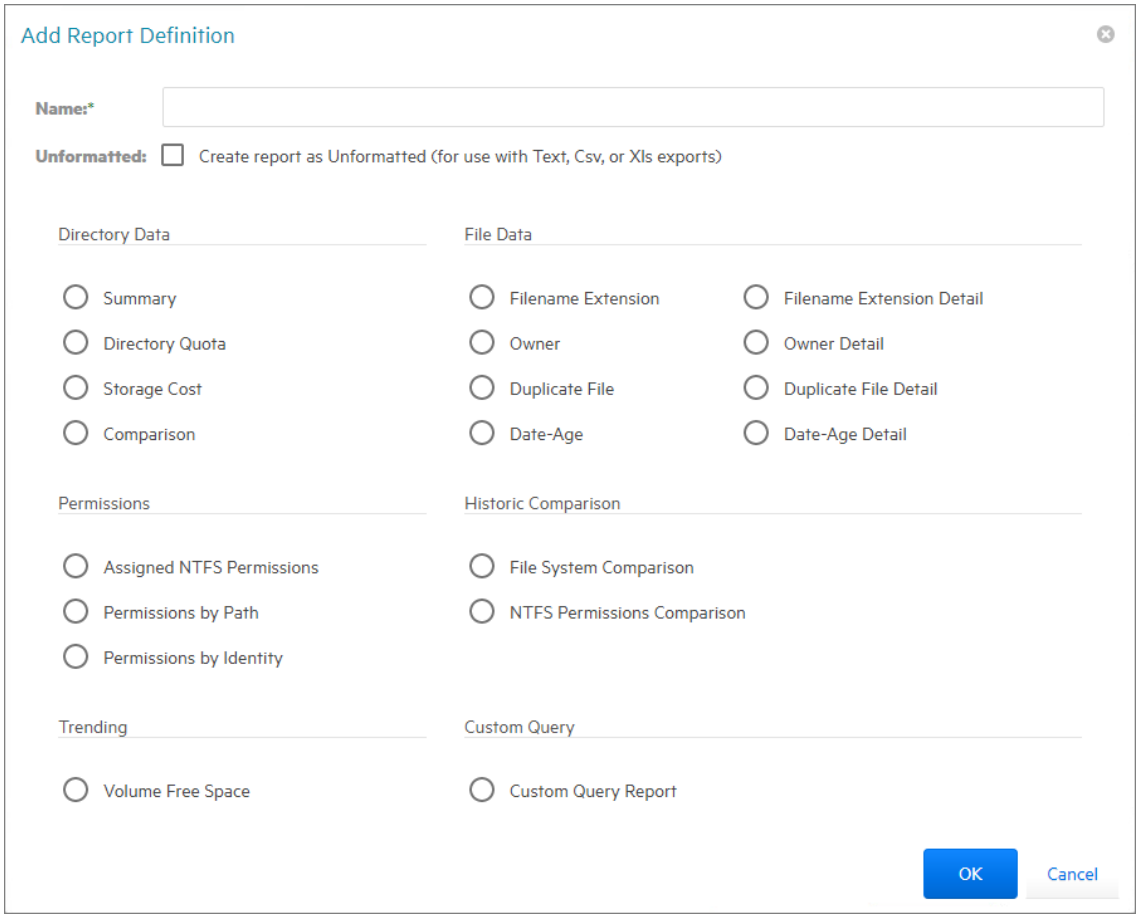
NOTE: For details on Custom Query reports, see Chapter 11, “Custom Query Reports,” on page 117.

9.3 Report Definitions

9.3.1 Creating a Report Definition

1 Select **Reports** > **Report Definitions.**

2 Click **Add** in the toolbar.



3 In the **Name** field, enter a name for the report.

4 (Optional) Select **Unformatted** to create a report that is delimited text only, with no report layout assigned.

5 Select a report type by clicking one of the options.

NOTE: For users who are familiar with writing SQL queries, a Custom Query report definition may provide better control and performance than a comparable unformatted report definition.

---

6 Click **OK** to create the report definition.

Depending on the report definition type, set any remaining report definition parameters, or for Custom Query reports, write the necessary SQL query and report definition layout.

For details on the various Built-in reports and their parameters, see Chapter 10, “Built-in Reports,” on page 81.

For details on Custom Query reports, see Chapter 11, “Custom Query Reports,” on page 117.

9.3.2 Deleting a Report Definition

1. Select **Reports** > **Report Definitions**.
2. From the list of report definitions, select the one that you want to delete.
3. From the toolbar, select **Delete**.
4. Click **Yes** in the confirmation dialog to confirm the report definition deletion.

NOTE: Editing or deleting a Report Definition, does not affect any Stored Reports previously generated from that Report Definition.

9.3.3 Copying a Report Definition

To save time in creating a new report definition and its associated properties, you can copy an existing report definition.

When you copy a built-in report, the following properties are included:

- Report Parameters
- Report Targets Paths
- Report Identity Targets
- Filters
- File Dynamics Policies

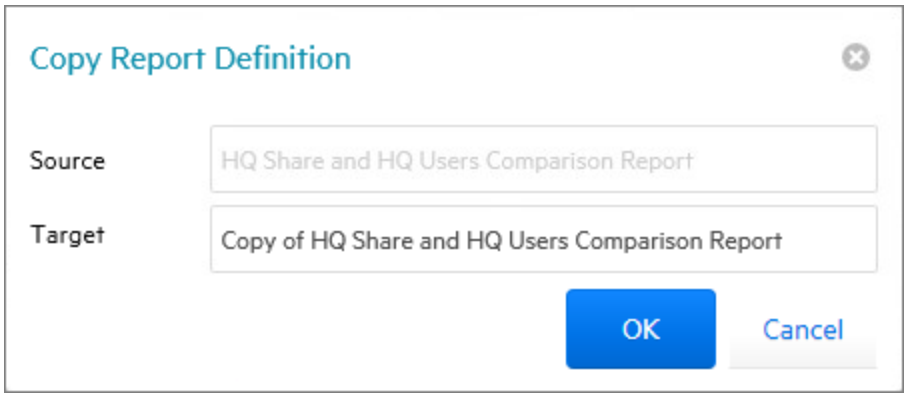
When you copy a Custom Query report, the following properties are included:

- SQL Query
- Report Layout

NOTE: Copying a report definition does not copy the content in the **Description** field, nor does it copy the report schedule.

---

1. Select **Reports** > **Report Definitions.**
2. From the list of report definitions, select one that you want to copy.
3. From the taskbar, click **Copy**.

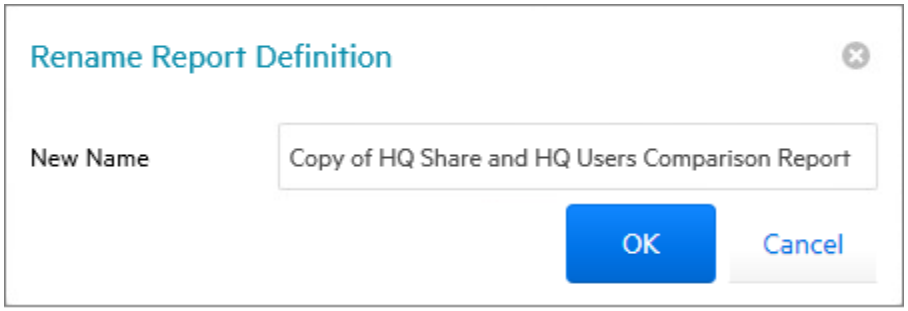


4 Click **Copy**.

The new report definition is added to the list of report definitions with the name *Copy of* preceding the name of the original report definition.

5 Select the copy of the report definition.

6 From the taskbar, select **Rename**.



7 In the **New Name** field, specify a name for the new report definition, then click **Rename**.

8 From the taskbar, select **Schedule** > **Edit Schedule**.

9 Set the scheduling parameters for the new report definition, then click **OK**.

10 From the taskbar, click **Edit**.

11 In the **Description** field, enter a new description.

12 Click **Save**.

9.4 Preview Reports

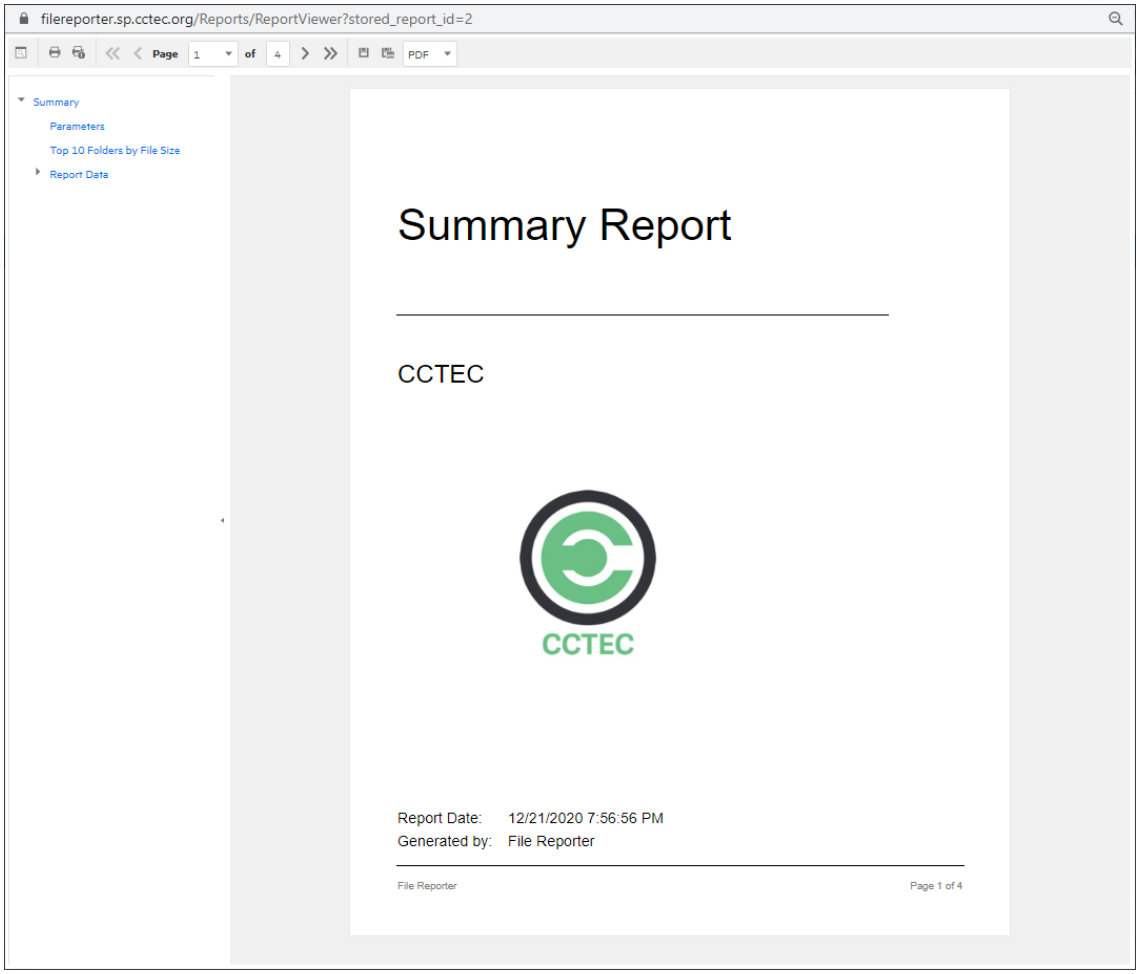
A preview report is generated from scan data in the database and is temporarily cached in the Web application's data folder. When you close a preview report, you cannot access the report again until you generate a new one using the same report definition.

When you view a report in Preview mode, you can print the report or save the report locally.

1 From the Report Definitions page, select the report definition from which you want to generate a report.

2 Select **Generate** > **Generate Preview**.

3 (Conditional) If you get a message stating that your browser prevented pop-up windows from appearing, enable pop-ups for this site.



All reports are structured similarly, with a title page, report parameters, for some report types a Top Ten summary, followed by a comprehensive breakdown of the data in the pages that follow.

Display the Search Window button: Lets you conduct a search within the preview report.

Print the Report button: Prints the entire preview report.

Print the Current Page button: Prints the currently displayed page.

First Page button: Takes you to the first page of the preview report.

Previous Page button: Takes you to the page that precedes the page you are viewing.

Page drop-down menu: Lets you advance to a page number by selecting it.

Next Page button: Takes you to the page that follows the page you are viewing.

Last Page button: Takes you to the last page of the preview report.

Export a Report and Save it to the Disk button: Exports the preview report to the file type listed in the drop-down menu and lets you view or save it in the new format.

Export a Report and Show it in a New Window button: Exports the preview report to the file type listed in the drop-down menu.

File Type drop-down menu: Lets you select the file type format to export the report to.

Document Navigation: Lists the contents of the report. You can click any item to advance within the preview report.

4 Export, save, or print the preview report.

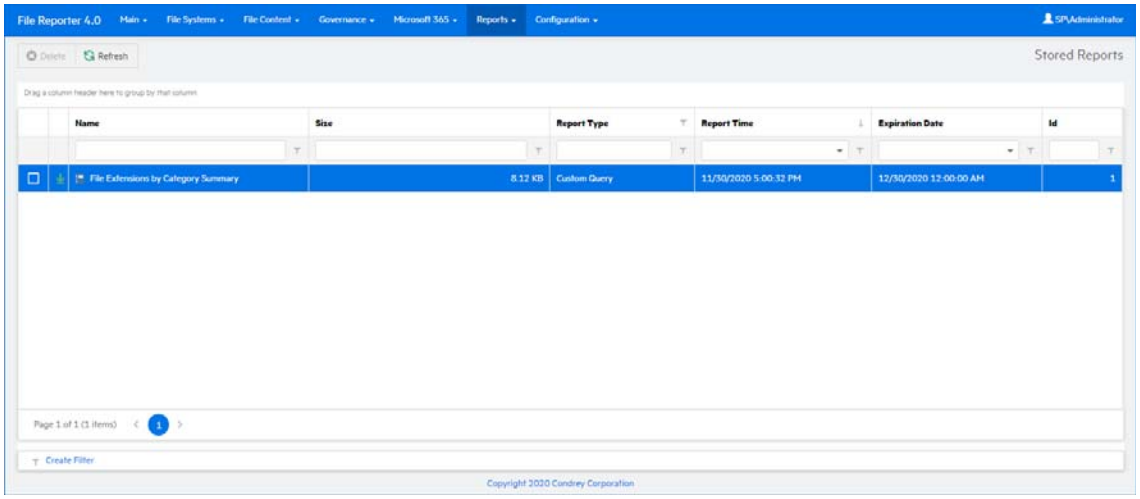
9.5 Stored Reports

9.5.1 Generating Stored Reports

Generating a report in Stored mode means that the report is saved and available for access for a set number of days from the time it is generated. Of course, you can save the report locally where you can keep it indefinitely.

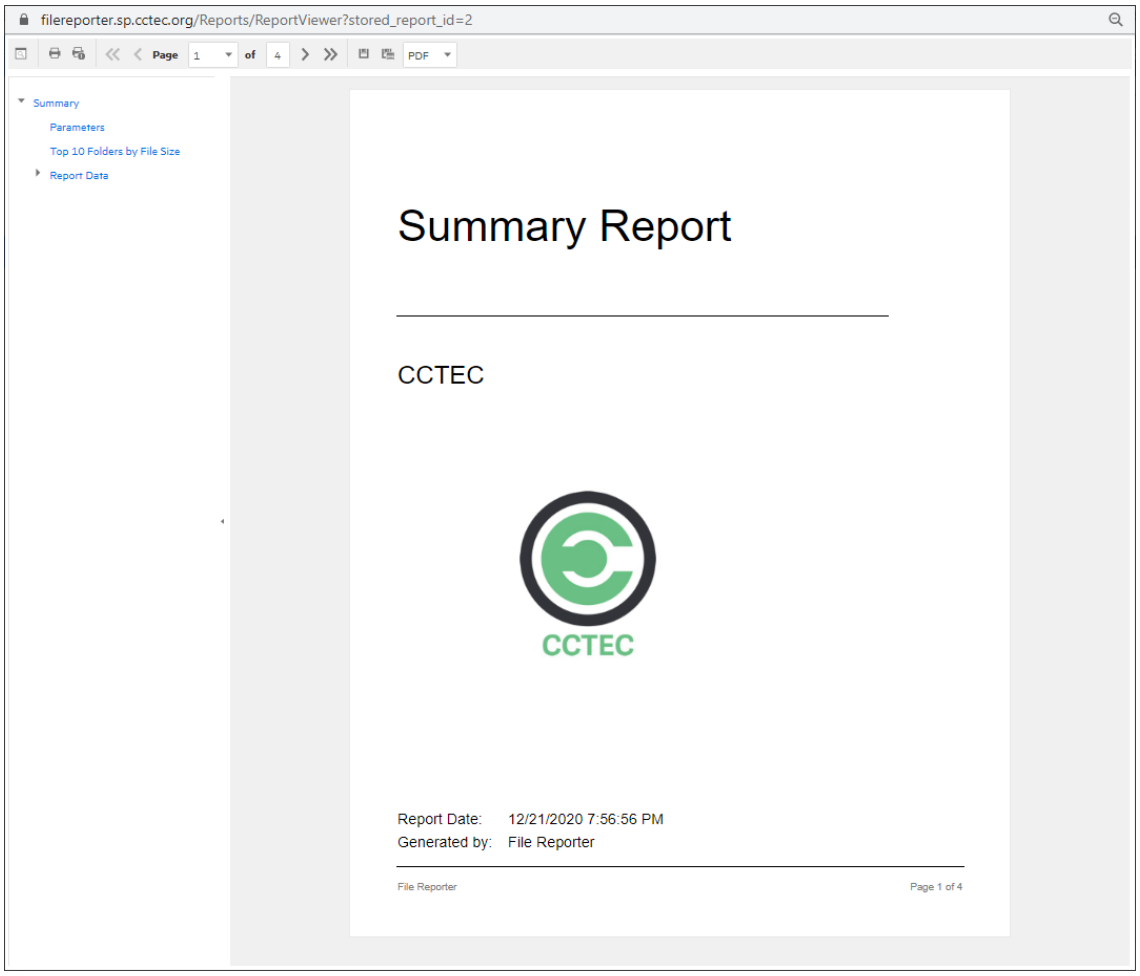
1 From the Report Definitions page, select **Generate** > **Generate Stored Report.**

2 Select **Reports** > **Stored Reports**.



3 Click the report you want to view.

4 (Conditional) If you get a message stating that your browser prevented pop-up windows from appearing, enable pop-ups for this site.



All reports are structured similarly, with a title page, report parameters, for some report types a Top Ten summary, followed by a comprehensive breakdown of the data in the pages that follow.

Display the Search Window button: Lets you conduct a search within the preview report.

Print the Report button: Prints the entire preview report.

Print the Current Page button: Prints the currently displayed page.

First Page button: Takes you to the first page of the preview report.

Previous Page button: Takes you to the page that precedes the page you are viewing.

Page drop-down menu: Lets you advance to a page number by selecting it.

Next Page button: Takes you to the page that follows the page you are viewing.

Last Page button: Takes you to the last page of the preview report.

Export a Report and Save it to the Disk button: Exports the preview report to the file type listed in the drop-down menu and lets you view or save it in the new format.

Export a Report and Show it in a New Window button: Exports the preview report to the file type listed in the drop-down menu.

File Type drop-down menu: Lets you select the file type format to export the report to.

Document Navigation: Lists the contents of the report. You can click any item to advance within the report.

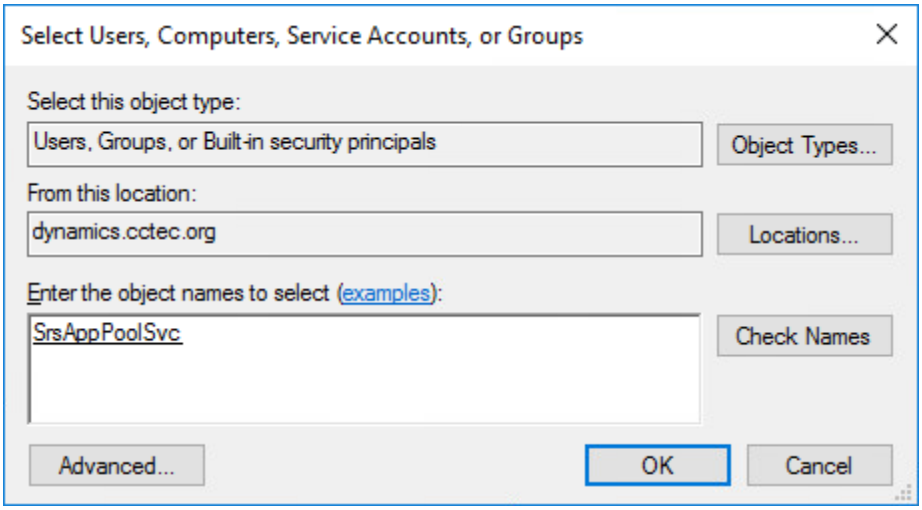
5 Save or print the stored report.

9.5.2 Stored Reports Path

The default path for stored reports is established during the installation of the Engine. If you want to change the file path, you can do so if the new path is on the server hosting the Engine and Web application.

Because both the Web application and the Engine via the Stored Reports DLL need access to the report files, the service accounts those processes run as must have both Read and Write access to the specified path. For the Engine, this is the Windows Proxy Account and for the Web Application, this is the associated IIS AppPool Identity, which is a hidden account created by Windows and tied to the Application Pool when the Web service was configured.

If you create a new folder for the stored reports, you must assign Read and Write access for the associated Windows server/proxy account to that folder, as well as the AppPool Identity. Because you cannot browse for the AppPool Identity, you need to use the name of the AppPool itself:



1 Select **Configuration** > **Stored Reports**.

2 In the **Stored Reports Folder** field, specify a new path.

3 Click **Save Changes**.

IMPORTANT: When reconfiguring the Stored Reports path, File Reporter does not move previously generated reports to the new location—you will need to move these yourself.

9.5.3 Stored Reports Lifespan

By default, stored reports are available for access for 30 days. You can adjust this setting by following the procedures below.

NOTE: You can always save a Preview or Stored report locally so it remains accessible indefinitely.

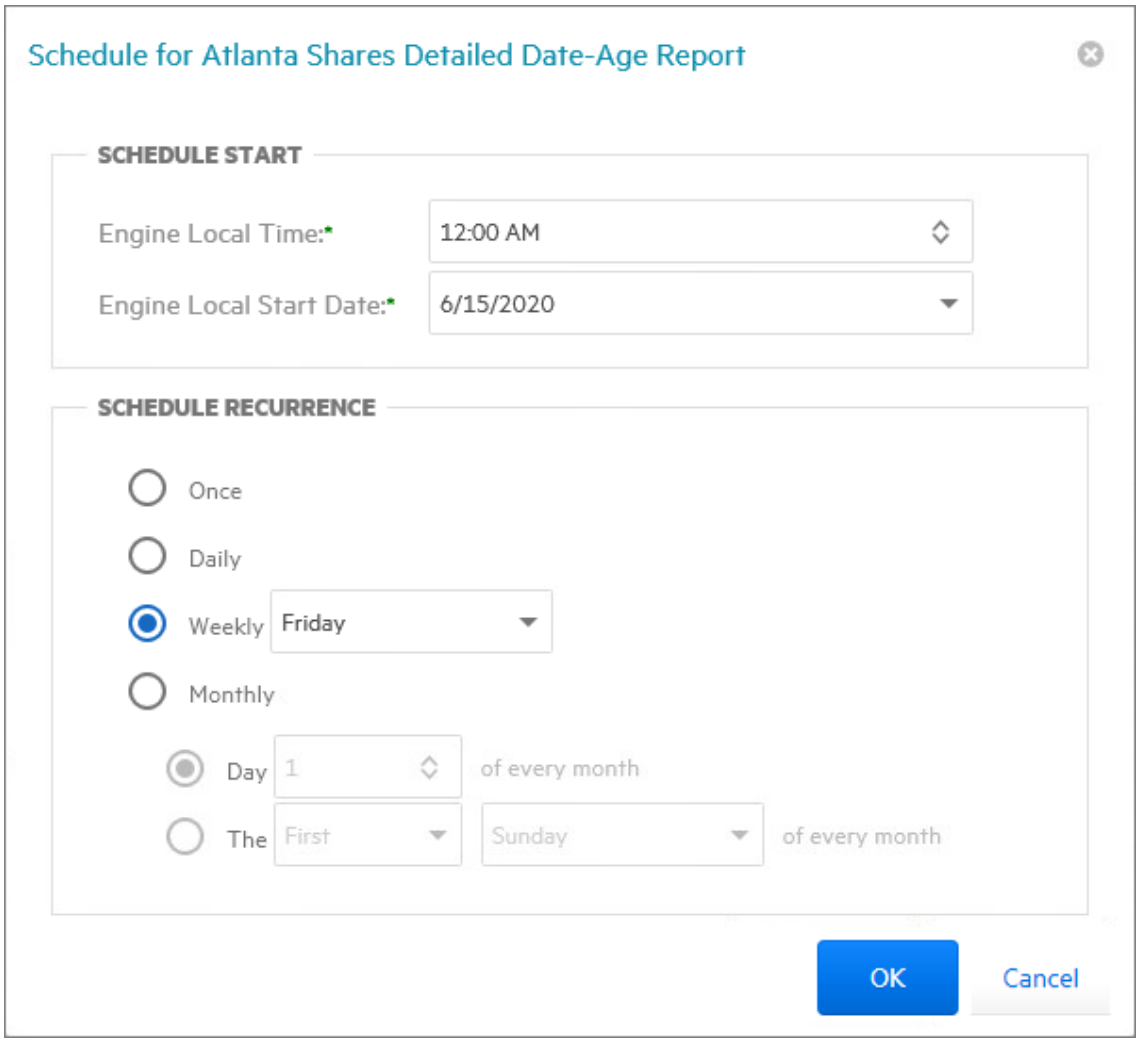
1. Select **Configuration** > **Stored Reports**.
2. In the **Default Expiration** field, adjust the setting.
3. Click **Save Changes**.

9.6 Report Scheduling

9.6.1 Setting a Report Schedule

You can generate reports on a one-time or regularly scheduled basis.

1. Select **Reports** > **Report Definitions**.
2. From the list of report definitions, select one that is not scheduled.
3. Select **Schedule** > **Edit Schedule**.



Engine Local Time: Specify the time that you want the report to generate.

The time you select should be based on the time zone where the Engine is located and not the workstation where you are accessing the Web application.

Engine Local Start Date: Specify the date when you want the report schedule to take effect.

Be aware that entering a date does not mean that the report generates on that date. If the **Engine Local Start Date** is set for today, which is a Monday, but the **Schedule Recurrence** setting is set for Weekly on Sunday, the report does not generate until Sunday.

Once: Select this option to schedule the report to be generated only once.

Daily: Select this option to schedule the report to be generated daily.

Weekly: Select this option and specify a weekday to generate the report.

Monthly: Select this option and specify a day to generate the report each month.

4 Specify the scheduling parameters and click **OK**.

The new schedule is displayed in the **Schedule** column of the Report Definitions page.

9.6.2 Editing a Report Schedule

1. Select **Reports** > **Report Definitions**.
2. From the list of report definitions, select one whose schedule you want to edit.
3. Select **Schedule** > **Edit Schedule**.
4. Make the schedule changes you want.
5. Click **OK**.

9.6.3 Clearing a Report Schedule

1. Select **Reports** > **Report Definitions**.
2. From the list of report definitions, select one whose schedule you want to clear.
3. Select **Schedule** > **Clear Schedule**.
4. When the confirmation screen appears, click **Yes**.

   The status of the report definition appears in the **Schedule** column as **Not Scheduled**.

9.7 Reports in Progress

9.7.1 View Reports in Progress

When you generate large reports, you can view the progress in the Reports in Progress page.

1. Select **Reports** > **Reports in Progress**.
2. Click **Refresh**.

   When the report disappears from the list, the report generation has completed.

9.7.2 Cancel a Report in Progress

1. Select **Reports** > **Reports in Progress**.
2. Click the check box for the report in progress that you want to cancel.
3. Click **Cancel** in the toolbar.

9.8 Troubleshooting Reports

If there is potential for a reporting problem, File Reporter provides notifications to help resolve the issue. The following points might also be helpful.

1. Verify that a scan exists for the storage resources you want to report on.
2. If your built-in reports include too much data to be useful, narrow the scope of the report by implementing filters or by reducing the number of report target paths for built-in reports.

   For more information on built-in report filters, see Section 10.5, “Built-in Report Filtering,” on page 85.

10 Built-in Reports

This chapter provides overview information and procedures for generating reports applicable to your Microsoft network, including built-in reports and Custom Query reports.

10.1 Overview

After you have conducted scans on storage resources, Micro Focus File Reporter has the content needed to generate reports. The type of report you can generate depends on the type of scan that you have conducted. For example, in order to create an Assigned NTFS Permissions report, a Permissions scan on a Windows share must first be conducted.

All reports are created by first creating report definitions. The report definition specifies the report name, type, target path to the scans, and more.

IMPORTANT: The report definition name must be unique. If you attempt to give the report definition an existing name, File Reporter generates an error.

File Reporter has built-in aggregate reporting capabilities, meaning that you can specify multiple target paths in the same report. Additionally, File Reporter has built-in scoping, which allows you to browse through the file path or Active Directory and specify the level where you want to start reporting data. Finally, Boolean filtering is available for all File Data Reports. For more information, see Section 10.5, “Built-in Report Filtering,” on page 85.

When the definition has been saved, you can generate the report immediately or schedule it to be generated.

You can generate reports in either Preview or in Stored Report mode. Preview lets you view the report where you can save it locally if you want to. Stored Report saves the report to the server hosting the Engine, where it remains for a set amount of days.

You can generate Detailed Reports from certain built-in report types. For example, a File Extension Report can be the means of generating a Detailed Report that includes the specific details of all of the `*.mov` files.

All built-in reports include a cover sheet that you can customize to include your organization's logo.

10.2 Built-in Report Types

File Reporter has five different built-in report type classifications:

- Directory Data
- Permissions
- File Data
- Historic Comparison
- Trending

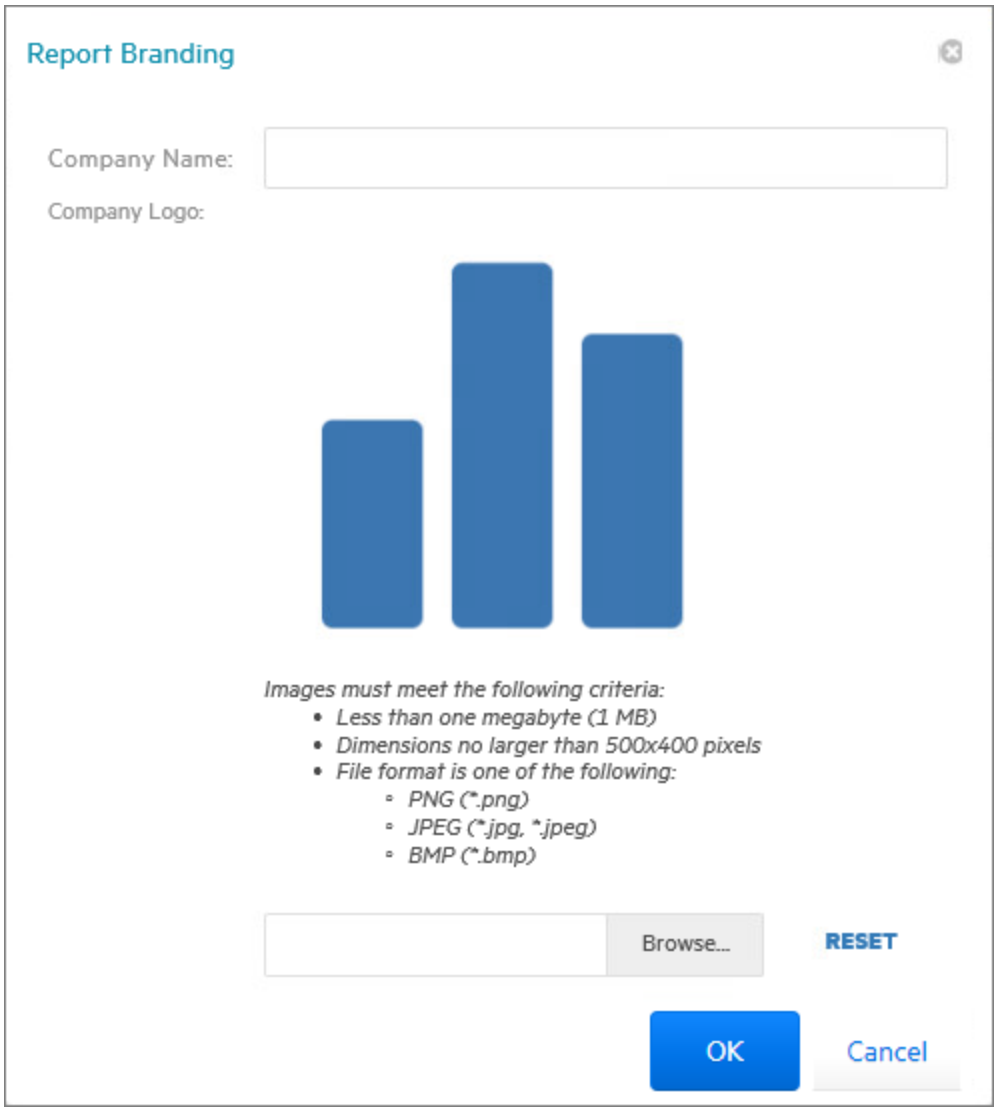
Each classification includes one or more report types. For example, in the Permissions category, there are three different reports that can be generated.

10.3 Branding and Style

10.3.1 Cover Sheet Logo

All generated built-in reports include a cover sheet that includes a default graphic. If you want, you can replace it with your organization's logo.

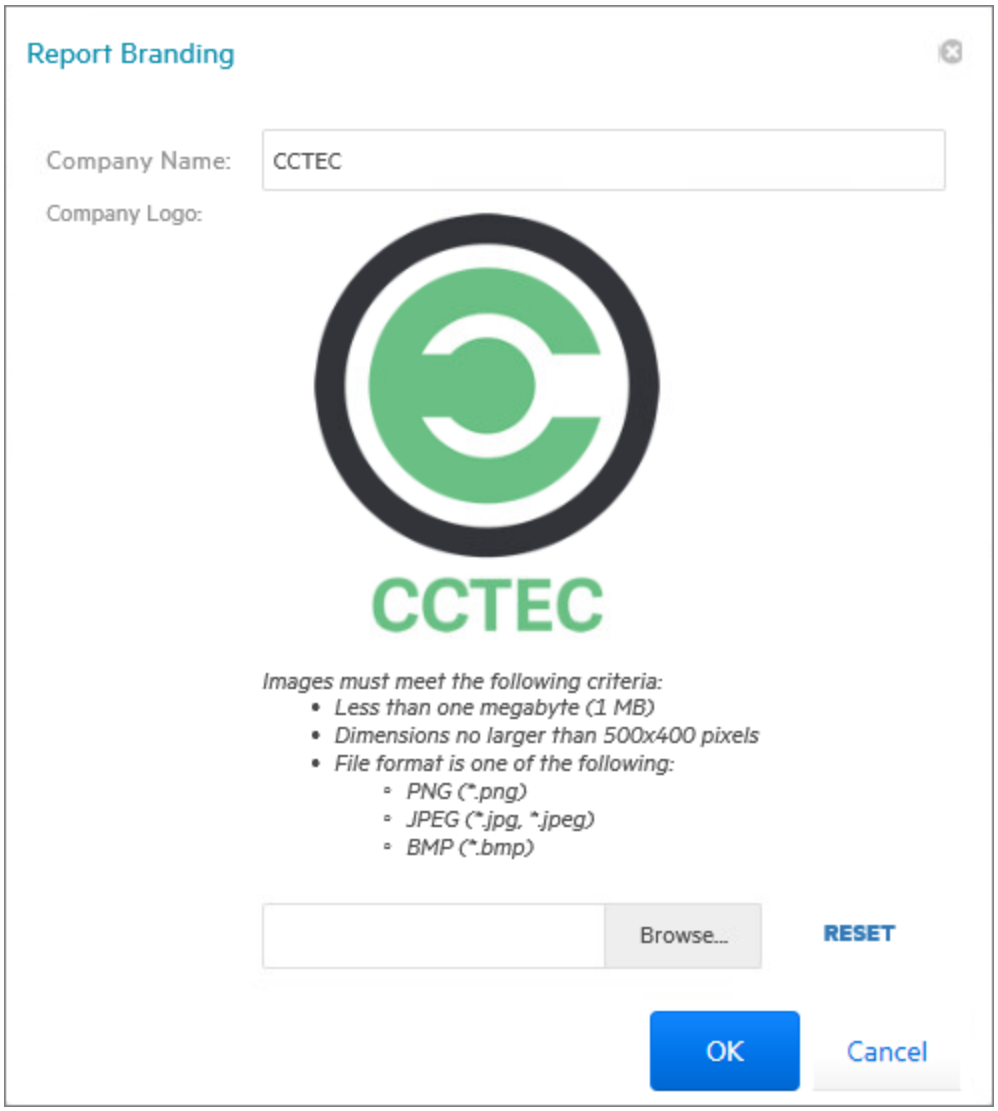
1. Select **Reports** > **Report Definitions**.
2. Select **Report Branding and Styling** > **Report Branding**.



3 In the **Company Name** field, specify the name of your organization.

This is the name that appears on the front cover.

4 Click **Browse**, then browse to and replace the default logo with a new logo.



5 Click Save.

10.3.2 Report Data Font

Due to limitations of font encoding in PDF files, you might need to specify an alternate report data font. Locales that have multi-byte characters or characters outside the Latin-1 set of characters supported by the default font are especially at risk.

If you know the collected data is limited to a specific locale or language, choose a font that properly displays all characters for that locale or language.

If the collected data might contain characters that span multiple locales or that include both multi-byte and Latin-1 characters, for example, choose an appropriate Unicode Font that can accurately display most characters from the Unicode set and not just a specific locale.

Two Unicode fonts known for having both good Unicode character coverage and good glyph presentation are MS Arial Unicode (a sans-serif font) and CODE2000 (a serif font).

For more information on these fonts and on Unicode fonts in general, see http://en.wikipedia.org/wiki/Unicode_font.

NOTE: You can change the data font to any font that is available on the server hosting the Web Application.

Headers and parameters in the reports remain in the default Arial font.

To change the report data font:

1. From the **Reports** menu, select **Report Definitions**.
2. From the **Report Branding and Styling** drop-down menu, select **Report Data Font**.
3. From the **Report Data Font Name** drop-down menu, select the font you want displayed in the report.
4. Click **Save**.

10.4 File Management Policy Reports

In most built-in reports, you browse to and specify a file path for the report through the **Target Paths** tab. If you have File Dynamics managing your organization's user and collaborative storage, you can have File Reporter report on the storage according to the target paths of the File Dynamics policies, rather than through a specific file path.

IMPORTANT: File Reporter 4.1 supports only File Dynamics 6.5.

The advantage to specifying a File Dynamics policy rather than a file path is that a policy can include many different target paths. For example, in a large organization that utilizes File Dynamics' load balancing capabilities, a single policy might have 10 or more target paths. If you chose to specify the paths through the **Target Paths** tab, you would need to list all 10 paths. But if you have each of the target paths listed in a single policy, through the **File Management Policies** tab, all you need to do is add the single policy.

Another important advantage is that File Reporter reads the associated policy target paths each time a report is generated, so that it dynamically responds to changes in assigned target paths for File Dynamics policies.

NOTE: Procedures for integrating File Reporter with File Dynamics are included in Section 4.4, "Integrating with File Dynamics," on page 33.

You can specify policies for all File Reporter reports with the exception of Comparison reports, Permissions by Identity reports, and Volume Free Space reports.

10.5 Built-in Report Filtering

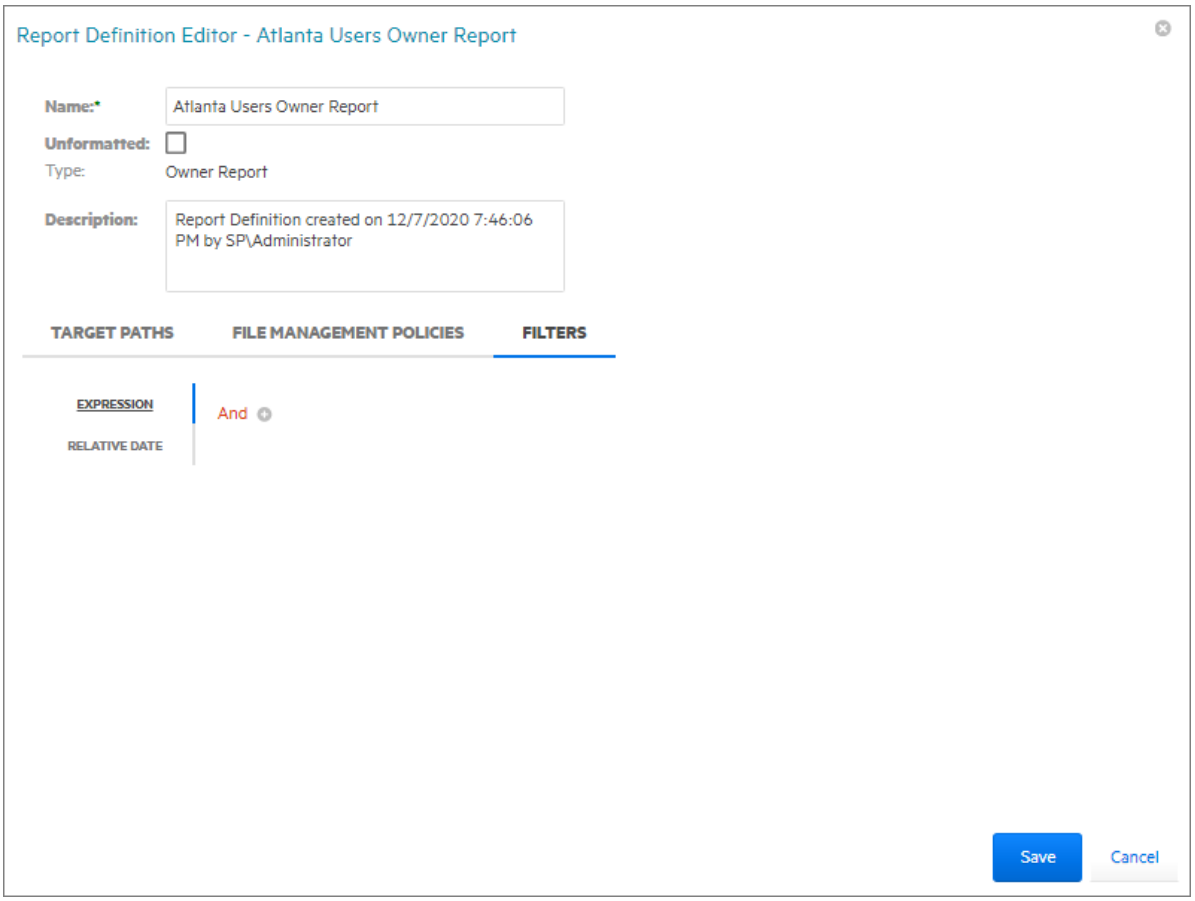
File Reporter enables you to utilize advanced filtering capabilities so that your reports include only the data you want. File Reporter provides this advanced filtering capability for all File Data Reports, which include:

- Filename Extension Reports
- Filename Extension Detail Reports
- Owner Reports
- Owner Detail Reports
- Duplicate File Reports
- Duplicate File Detail Reports
- Date-Age Reports
- Date-Age Detail Reports

10.5.1 Filters Tab

Built-in report filtering is available in the **Filters** tab of the Report Definition Editor.

Figure 10-1 *Filters Tab*



You set filter parameters using the Boolean operators available through the **And** drop-down menu, and adding the search parameters with the **+** button. Alternatively, you set date filters using the **Relative Date** filter parameters on the right-hand portion of the page.

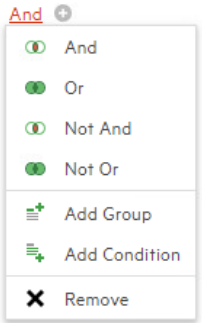
You can filter according to size, dates, or both.

10.5.2 Filter Expression Builder

The **And** drop-down menu is used to:

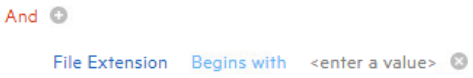
- Select Boolean operators for creating a search filter
- Create additional groups or conditions
- Delete search filters, groups, or conditions

Figure 10-2 *And Drop-Down Menu*



The **+** button next to the **And** drop-down menu are used to create parameters for a search condition.

Figure 10-3 *Parameters for Filter*

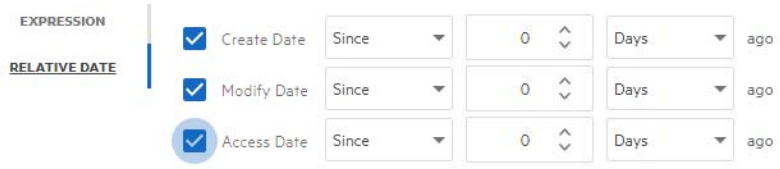


NOTE: File size filter values must be entered in bytes. For example, if your filtering parameters were for all files larger than 500 MB, you would enter 524288000 (500 x 1024 x 1024). A more practical entry might be 500000000. Do not attempt to enter commas; they are placed automatically.

10.5.3 Relative Date Filtering Parameters

Click **Relative Date** and then select the **Create Date**, **Modify Date**, and **Access Date** check boxes to enable the corresponding drop-down menus and fields.

Figure 10-4 *Relative Date Filtering Parameters*



NOTE: Use of both the Filter Expression Builder and Relative Date Filter in the same report definition are logically joined with a Boolean **AND**.

10.6 Directory Reports

Reports in this classification include Summary, Directory Quota, Storage Cost, and Comparison Reports.

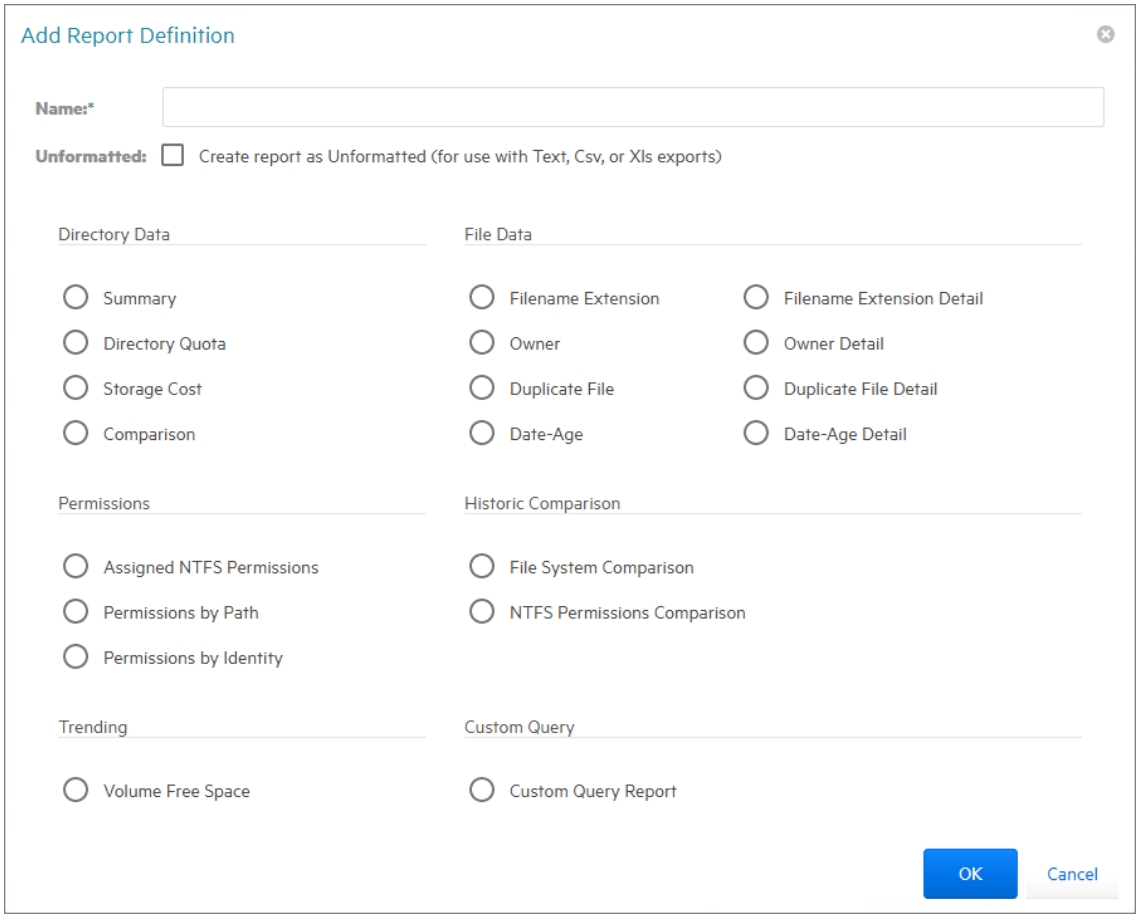
Before generating any type of Directory Data report, you must first conduct a File System scan on the shares you want to report on.

10.6.1 Summary Report

Summary reports provide a summary of the contents of folders according to a specified level in the file system.

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

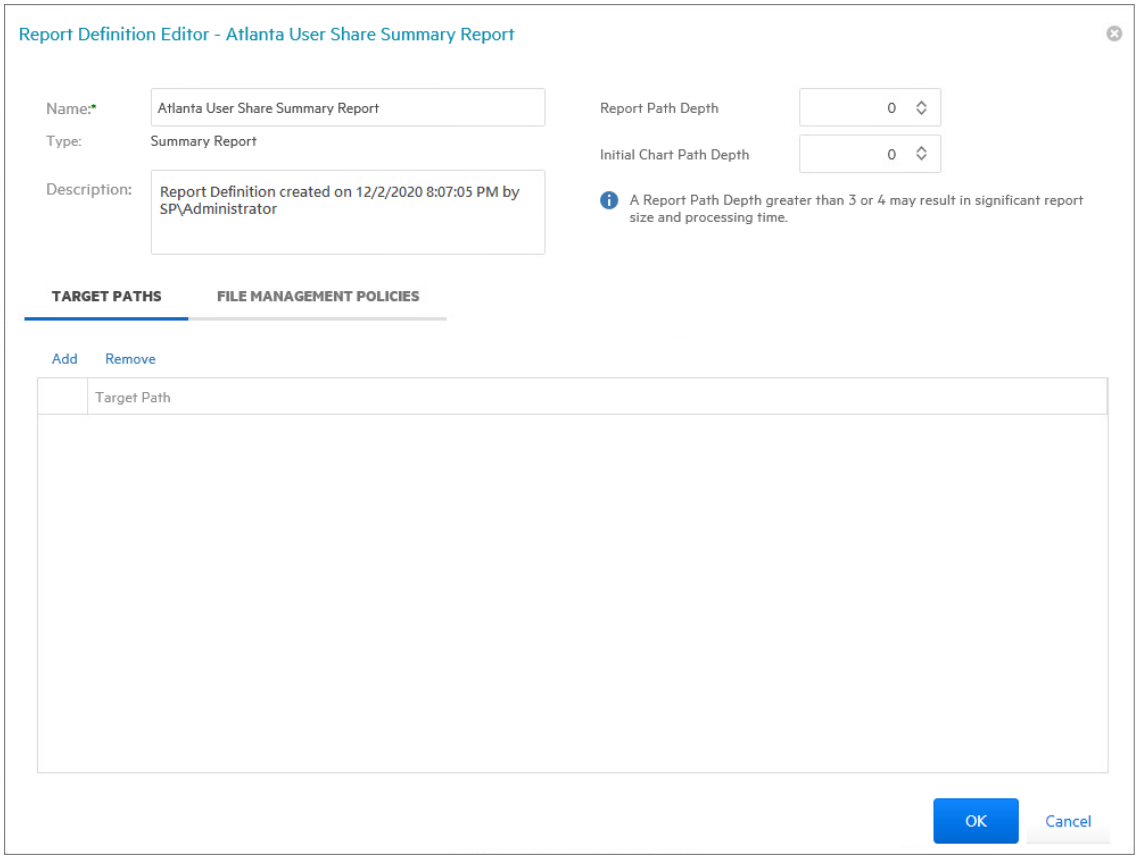


3 In the **Name** field, specify a descriptive name of the report definition.

For example, User Volume Summary Report.

The name can contain up to 64 alphanumeric characters.

4 Select the **Summary** option and click **OK**.



5 In the **Report Path Depth** field, specify the depth of reporting.

For example, if you select 3, the Summary report lists the file contents of all file paths in the specified shares up to 3 levels in the file structure.

For example, for a server named srs-mlsp, the Summary report would list the contents of these paths:

`\\srs-m1sp.cctec.org\Shares\Home\Users1`

`\\srs-m1sp.cctec.org\Shares\Home\Users1\a`

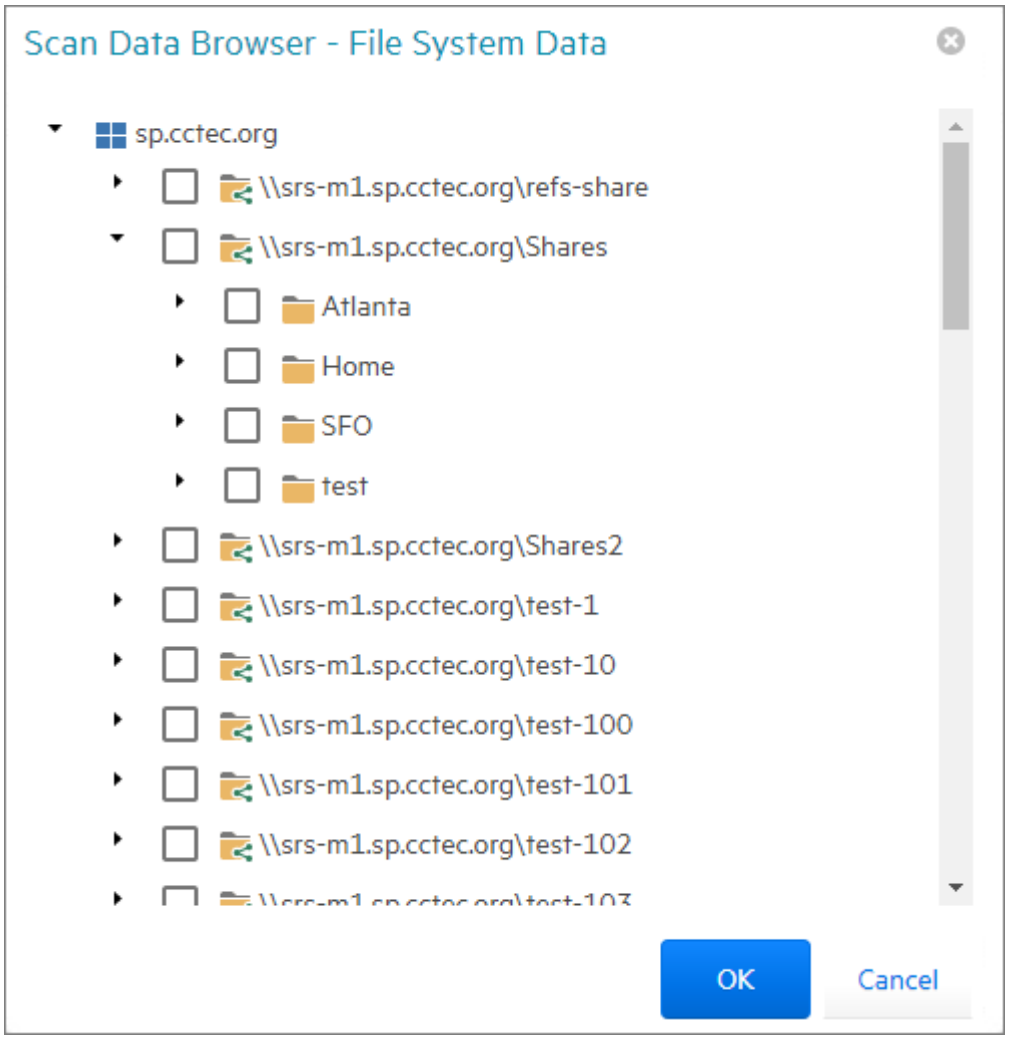
`\\srs-m1sp.cctec.org\Shares\Home\Users1\a\stuff`

`\\srs-m1sp.cctec.org\Shares\Home\Users1\a\stuff\morestuff`

6 In the **Initial Chart Path Depth** field, specify the initial path depth for inclusion in the Top Ten Folders by Size chart that is displayed in the report header section.

This is important so that when the **Report Path Depth** is greater than zero, the top level folders are now conditionally included. The **Chart Path Depth** parameter is not allowed to be greater than the currently specified **Report Path Depth**.

7 From the **Target Paths** tab, click **Add**.

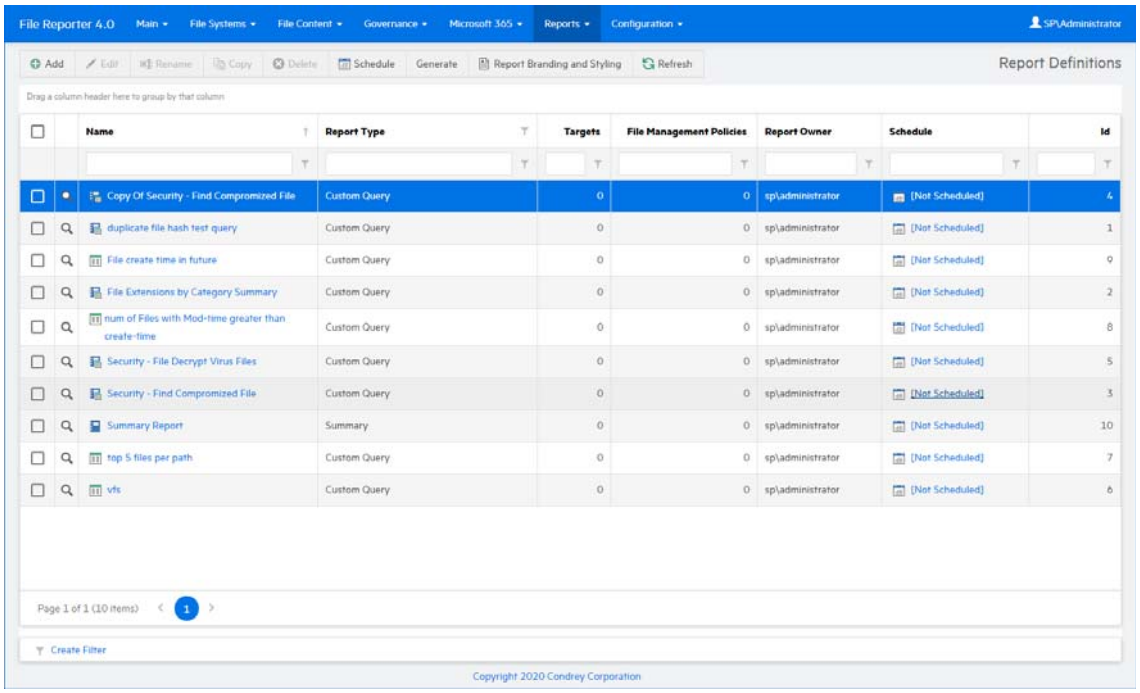


8 Click the > to browse to and select the file paths you want included in the report, then click **OK**.

You must expand the Active Directory forest to be able to select the shares, even if you want to select the root of the Active Directory forest.

9 Click **Save**.

The report definition is added to the list.



10 Do one of the following:

- Generate the report in Preview mode by following the procedures under Section 9.4, “Preview Reports,” on page 72.
- Generate the report in Stored mode by following the procedures under Section 9.5, “Stored Reports,” on page 74.

10.6.2 Directory Quota Report

Directory Quota reports specify folders with assigned quota, the amount of quota assigned, and the amount of quota consumed.

NOTE: Quota information is only available if the file system scan policy was configured to collect quota information.

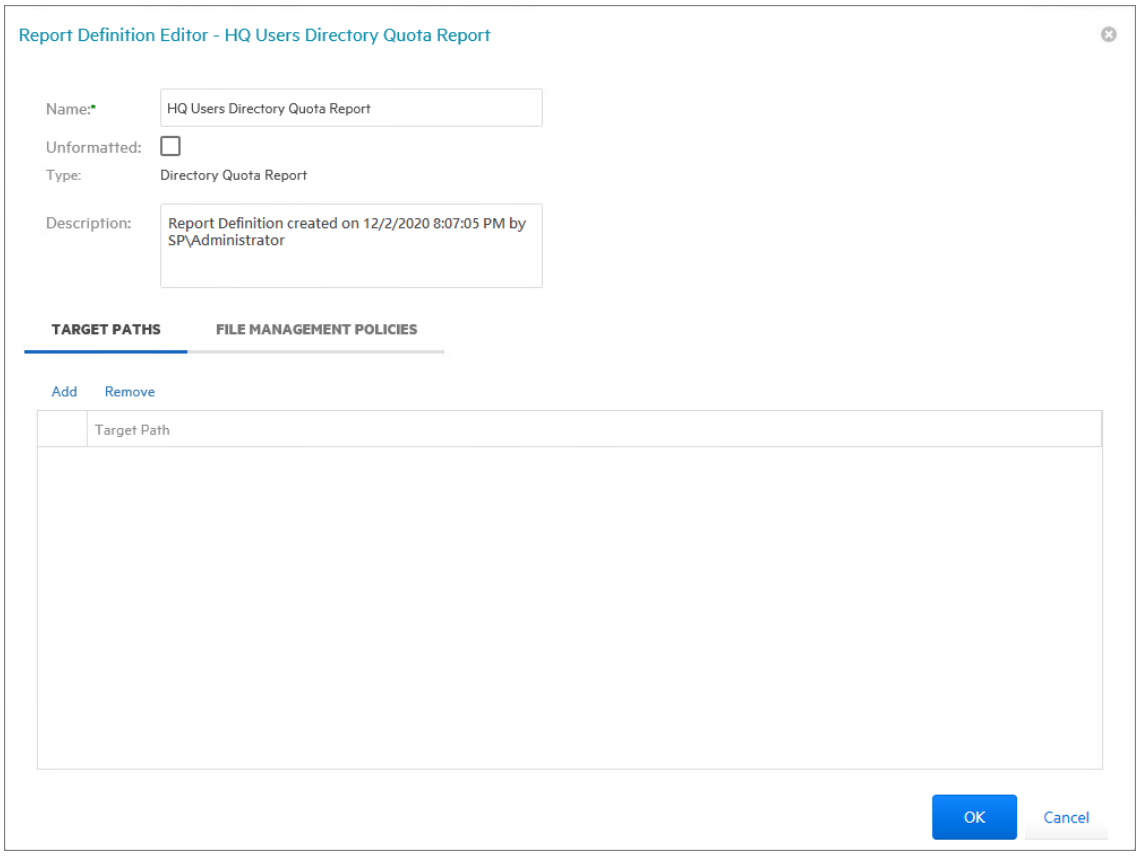
---

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Directory Quota** option and click **OK**.



5 From the **Target Paths** tab, click **Add**.

6 Browse to and select the file paths you want included in the report and click **OK**.

7 Click **Save**.

8 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.6.3 Storage Cost Report

Storage Cost reports indicate storage costs according to prices established in the **Cost per Unit** setting of the Report Definition editor. You can use this report to determine which users or groups are being irresponsible with network storage practices.

NOTE: When the report is generated, the monetary symbol that is displayed comes from the local Engine/Web server's Windows locale and region settings. For example, if the Windows server hosting the engine and Web application is set up using US locale and region, it will show a $ for costing displays in the report.

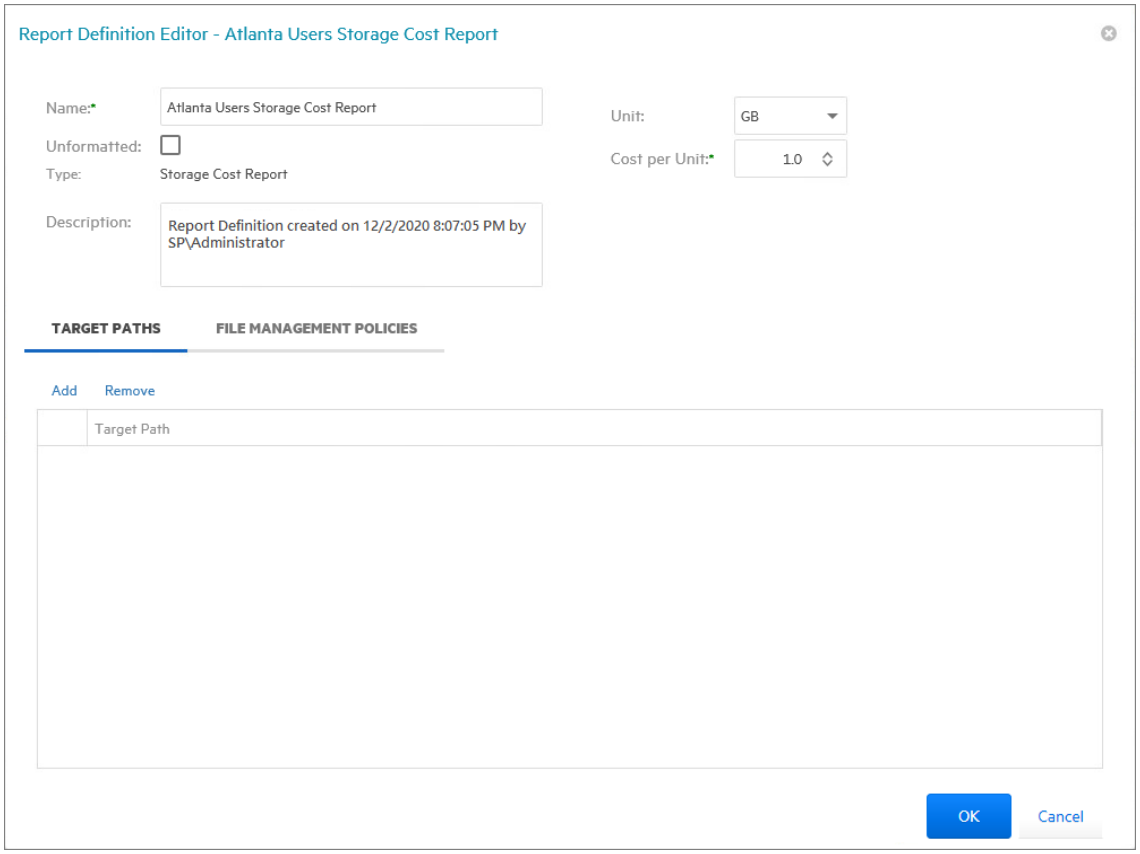
---

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Storage Cost** option and click **OK**.



5 In the **Unit** drop-down menu, select the storage unit value for which you want to establish a cost.

6 In the **Cost per Unit** field, indicate the cost of the selected storage unit.

7 From the **Target Paths** tab, click **Add**.

8 Browse to and select the file paths you want included in the report and click **OK**.

9 Click **Save**.

10 Generate the report as either a Preview report or as a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.6.4 Comparison Report

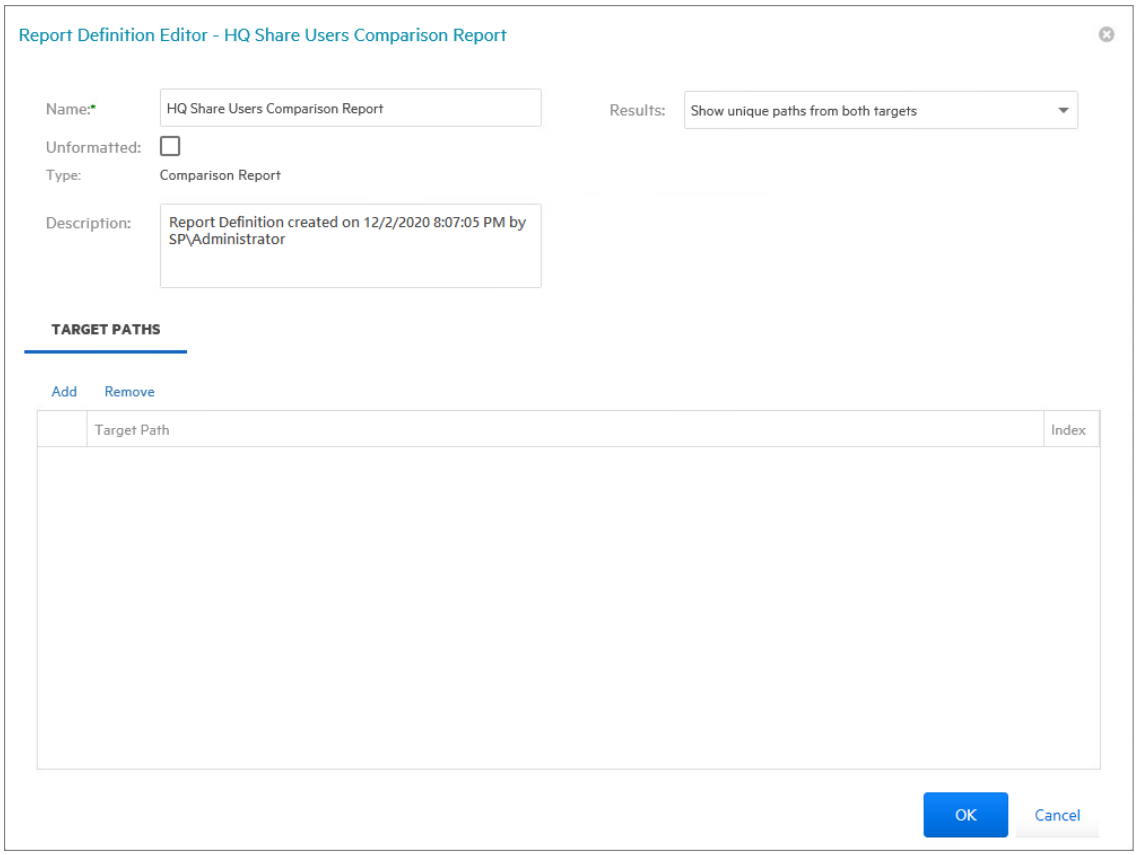
A Comparison report specifies the differences between two selected folders on the network. This is useful if you want to verify that servers are hosting the same version of software, library files on servers are the same, and so forth.

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Comparison** option and click **OK**.



5 In the **Comparison Results** drop-down menu, select an option.

Show unique paths from both targets: The report indicates the differences in folder and file names for the compared target paths.

Show paths unique to the first target: The report indicates only the unique folder and file names found in the first target path.

Show paths unique to the second target: The report indicates only the unique folder and file names found in the second target path.

6 From the **Target Paths** tab, click **Add.**

7 Browse to and select two shares or folders whose data you want to compare and click **OK**.

8 Click **Save**.

9 Generate the report as either a Preview report or as a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.7 File Data Reports

- Section 10.7.5, “Duplicate File Report,” on page 100
- Section 10.7.6, “Detailed Duplicate File Report,” on page 101
- Section 10.7.7, “Date-Age Report,” on page 103
- Section 10.7.8, “Detailed Date-Age Report,” on page 104

Reports in this classification include Filename Extension, Owner, Duplicate File, and Date-Age, along with detailed versions of each of these reports.

Before generating any type of File Data report, you must first conduct a File System scan on the shares you want to report on.

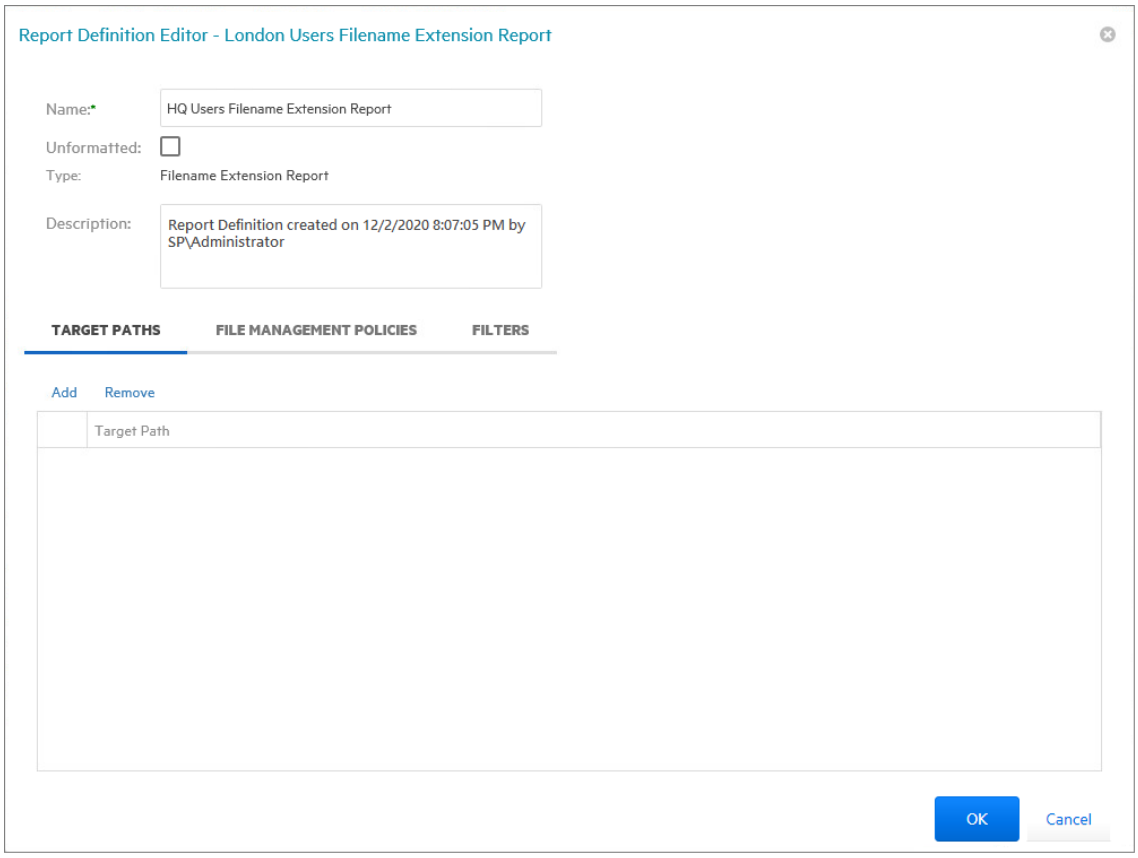
10.7.1 Filename Extension Report

The Filename Extension report presents data grouped according to filename extension. This report is helpful for determining file types that you do not want stored on your network drives. For example, you can easily identify who is storing .MP3 or .MOV files.

NOTE: File extensions in File Reporter are limited to 32 characters. File extensions longer than 32 characters are considered part of the file name and not as an extension.

---

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Filename Extension** option and click **OK**.



5 From the **Target Paths** tab, click **Add**.

6 Browse to and specify the file paths you want included in the report and click **OK**.

7 (Optional) Click the **Filters** tab and set the filters for the report.

For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.

8 Click **Save**.

9 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10 (Optional) Generate a Detailed report on an individual file extension by clicking a file extension name in the report.

10.7.2 Detailed Filename Extension Report

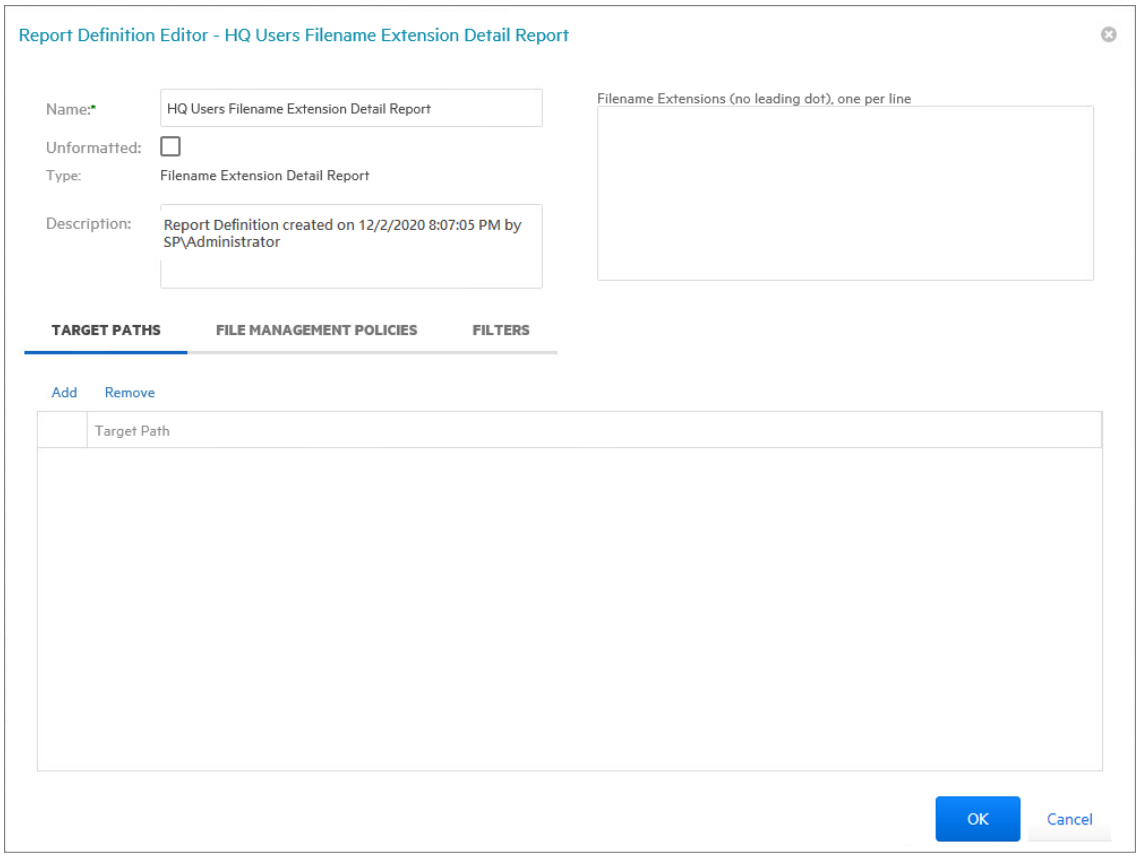
A Detailed Filename Extension report is similar to a standard Filename Extension report, except you can filter the report to include only the files with the extension types you want.

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Filename Extension Detail** option and click **OK**.



5 In the **Filename Extension** field, specify the filename extensions you want included in the report by listing each on an individual line. Do not precede the filename extension with a period.

   For example:

   ```
   mov
   jpg
   tmp
   ```

6 From the **Target Paths** tab, click **Add**.

7 Browse to and specify the file paths you want included in the report and click **OK**.

8 (Optional) Click the **Filters** tab and set the filters for the report.

   For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.

9 Click **Save**.

10 Generate the report as either a Preview report or a Stored report.

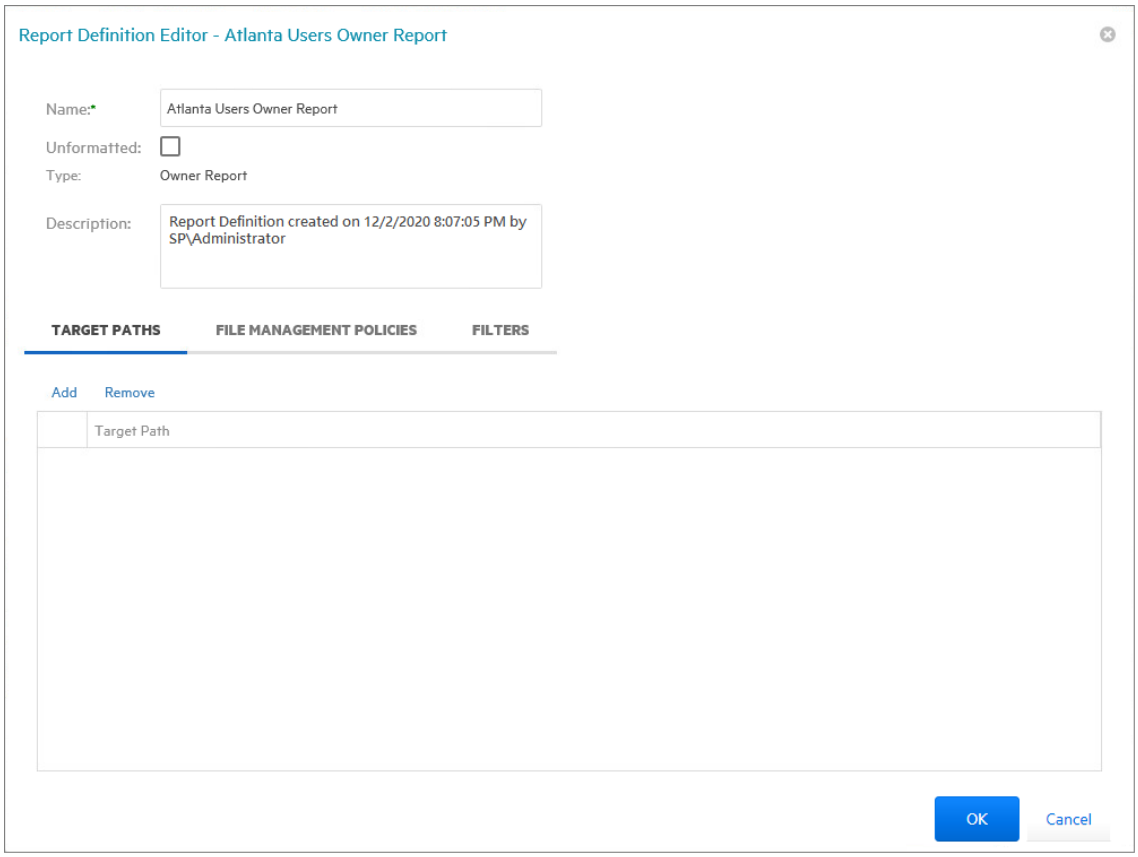
   For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

   For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.7.3 Owner Report

An Owner report groups data according to file owners. If it is determined that certain users are using a disproportionate amount of storage, you can see what these users are storing and if they are justified in doing so.

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Owner** option and click **OK**.



5. From the **Target Paths** tab, click **Add**.
6. Browse to and specify the file paths you want included in the report and click **OK**.
7. (Optional) Click the **Filters** tab and set the filters for the report.

   For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.
8. Click **Save**.
9. Generate the report as either a Preview report or a Stored report.

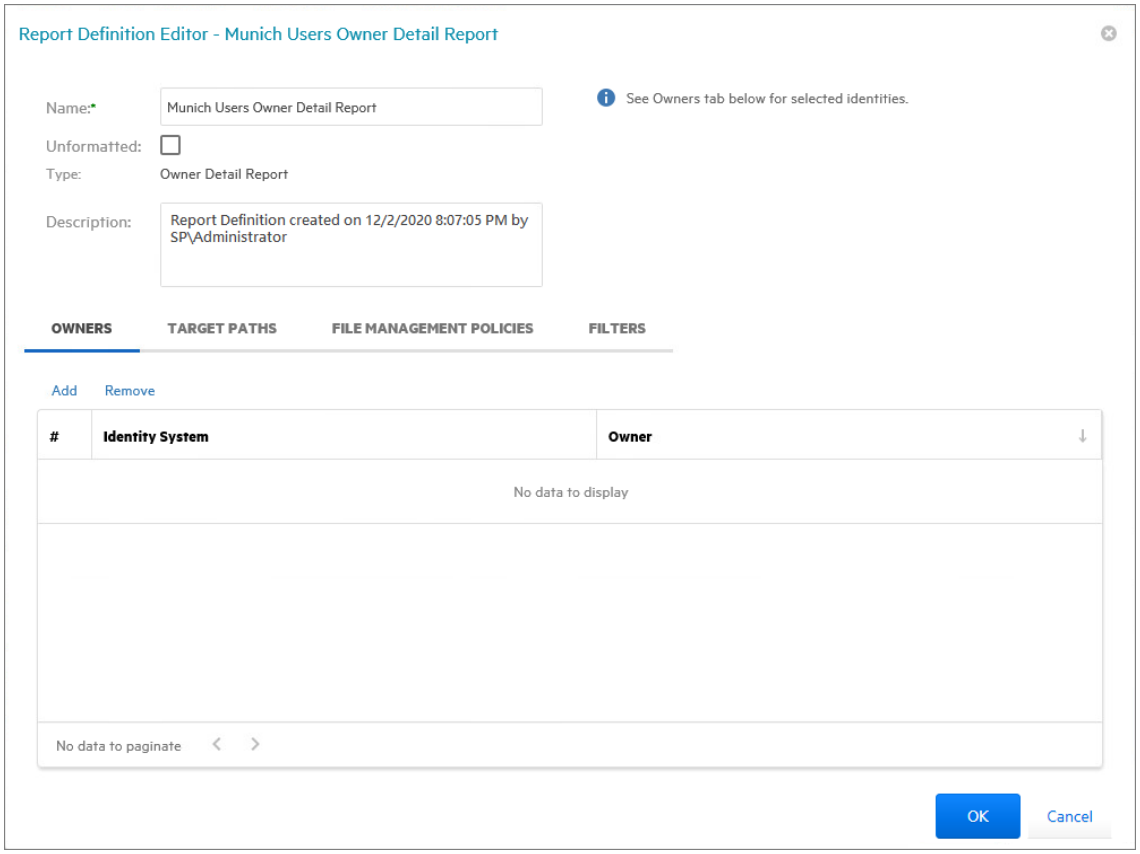
   For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

   For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.
10. (Optional) Generate a Detailed report on an individual owner by clicking an owner’s name in the report.

10.7.4 Detailed Owner Report

A Detailed Owner report is similar to a standard Owner report, except you can specify the users you want information on.

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Owner Detail** option and click **OK**.



5. From the **Owners** tab, click **Add**, then browse to and specify the owners you want in the report and click **OK**.
6. From the **Target Paths** tab, click **Add**, then browse to and specify the file paths you want included in the report and click **OK**.
7. (Optional) Click the **Filters** tab and set the filters for the report.

   For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.
8. Click **Save**.
9. Generate the report as either a Preview report or a Stored report.

   For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

   For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

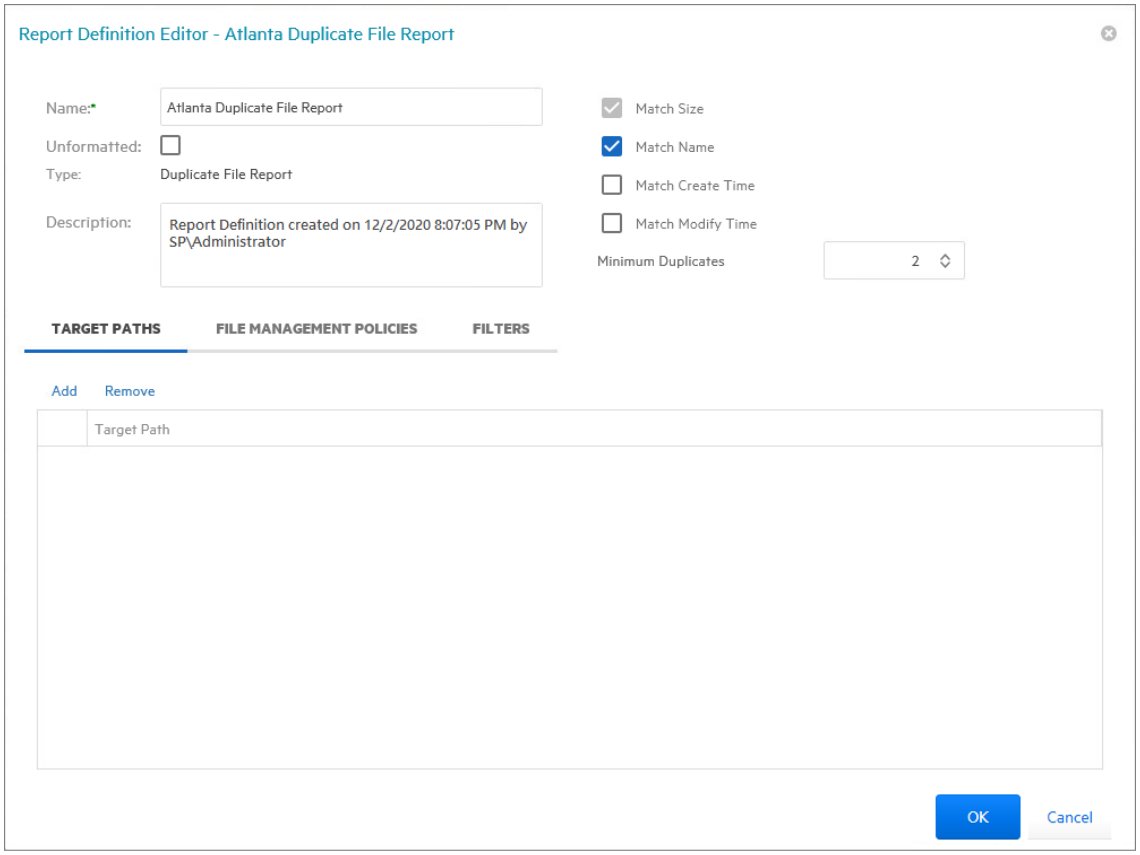
10.7.5 Duplicate File Report

A Duplicate File report indicates duplicate versions of files being stored and their locations. A principle objective for any organization determined to limit network storage usage should be the elimination of duplicate versions of files.

NOTE: This Duplicate File report option is generated by comparing filenames and other metadata. File Reporter offers a more advanced Duplicate File report generated through content hashed comparisons. For more details, refer to the *Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide*.

---

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Duplicate File** option and click **OK**.



5. Use the check boxes and **Minimum Duplicates** field to specify the parameters for reporting.

   The more check boxes you select, the more likely it is that File Reporter can identify definitive duplicate files.

   Match Size: Specifies that files reported must have duplicate file sizes. This option cannot be deselected.

   Match Name: Specifies that files reported must have duplicate names with other files.

Match Create Time: Specifies that files reported must have duplicate file creation times with other files.

Match Modify Time: Specifies that files reported must have duplicate file modification times with other files.

Minimum Duplicates: Specifies the minimum number of duplicate files, according to the parameters selected above, for inclusion in the report.

6 Browse to and specify the file paths you want included in the report and click **OK**.

7 (Optional) Click the **Filters** tab and set the filters for the report.

For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.

8 Click **Save**.

9 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10 (Optional) Generate a Detailed report on a duplicate file by clicking a specific file name in the report.

10.7.6 Detailed Duplicate File Report

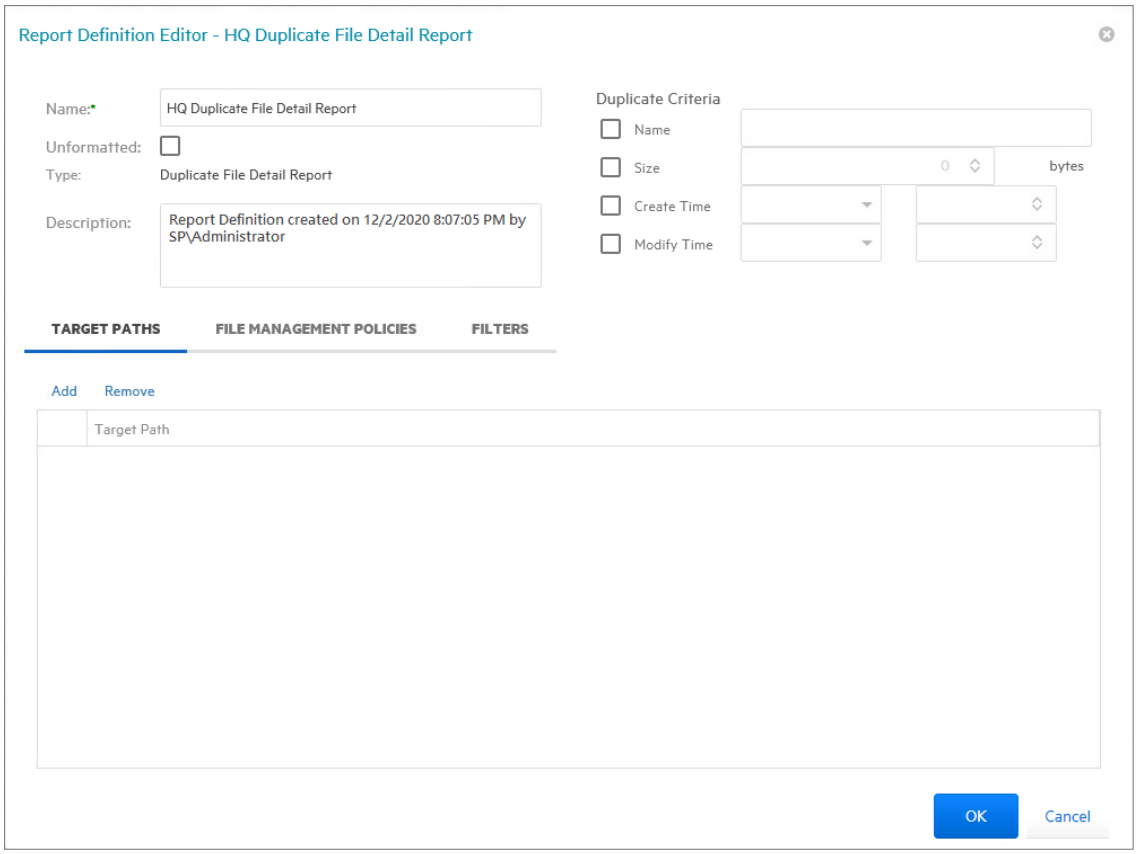
A Detailed Duplicate File report is similar to a standard Duplicate File report, except you can specify the exact filename to search for, along with exact create and modify times.

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Duplicate File Detail** option and click **OK**.



5 In the **Duplicate Criteria** region, specify the file name size, and the dates and times that the file was created or modified.

IMPORTANT: When specifying Create or Modify times, the time entered must be exact down to the second. If a date range is required, do not enable the Create or Modify criteria here, but use the date filters in the **Filters** tab. For more information on filters, see Section 10.5, “Built-in Report Filtering,” on page 85.

---

6 Browse to and specify the file paths you want included in the report and click **OK**.

7 (Optional) Click the **Filters** tab and set the filters for the report.

For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.

8 Click **Save**.

9 Generate the report as either a Preview report or a Stored report.

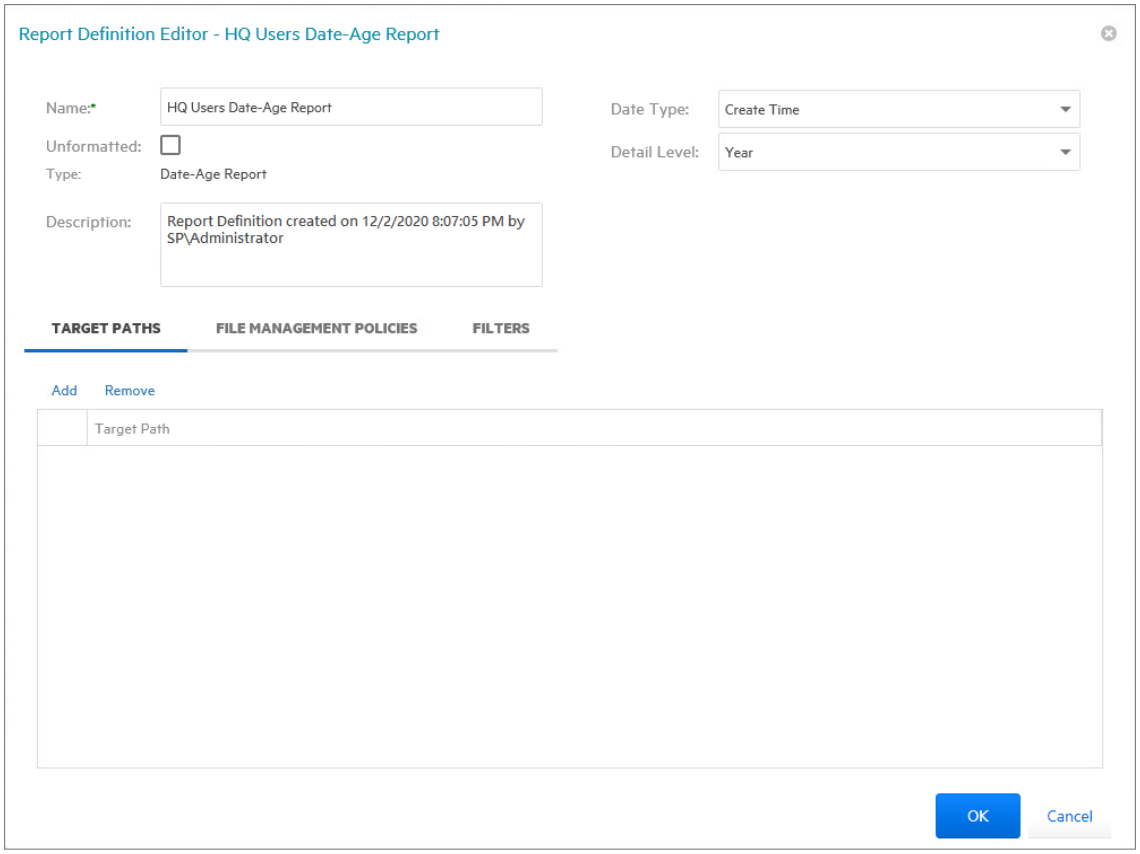
For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.7.7 Date-Age Report

The Date-Age report presents file count data according to when files were created, last accessed, or last modified. You can use this report to help you determine which files have not been accessed for a given amount of time and then decide whether to delete, archive, or move those files to less expensive storage.

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Date-Age** option and click **OK**.



5. In the **Date Type** drop-down menu, select an option.

   Create Time: Reports when files were created.

   Modify Time: Reports when files were last modified.

   Access Time: Reports when files were last accessed.

6. In the **Detail Level** drop-down menu, select an option.

   Year: Groups the file count in the report according to the year they were created, last modified, or last accessed.

   Month: Groups the file count in the report according to the month they were created, last modified, or last accessed.

Day: Groups the file count in the report according to the calendar date they were created, last modified, or last accessed.

7 Browse to and specify the file paths you want included in the report and click **OK**.

8 (Optional) Click the **Filters** tab and set the filters for the report.

For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.

9 Click **Save**.

10 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

11 (Optional) Generate a Detailed report by clicking a specific year, month, or date in the report.

Unlike the original Date-Age report that lists the data by file count, the generated Detailed report lists individual files.

10.7.8 Detailed Date-Age Report

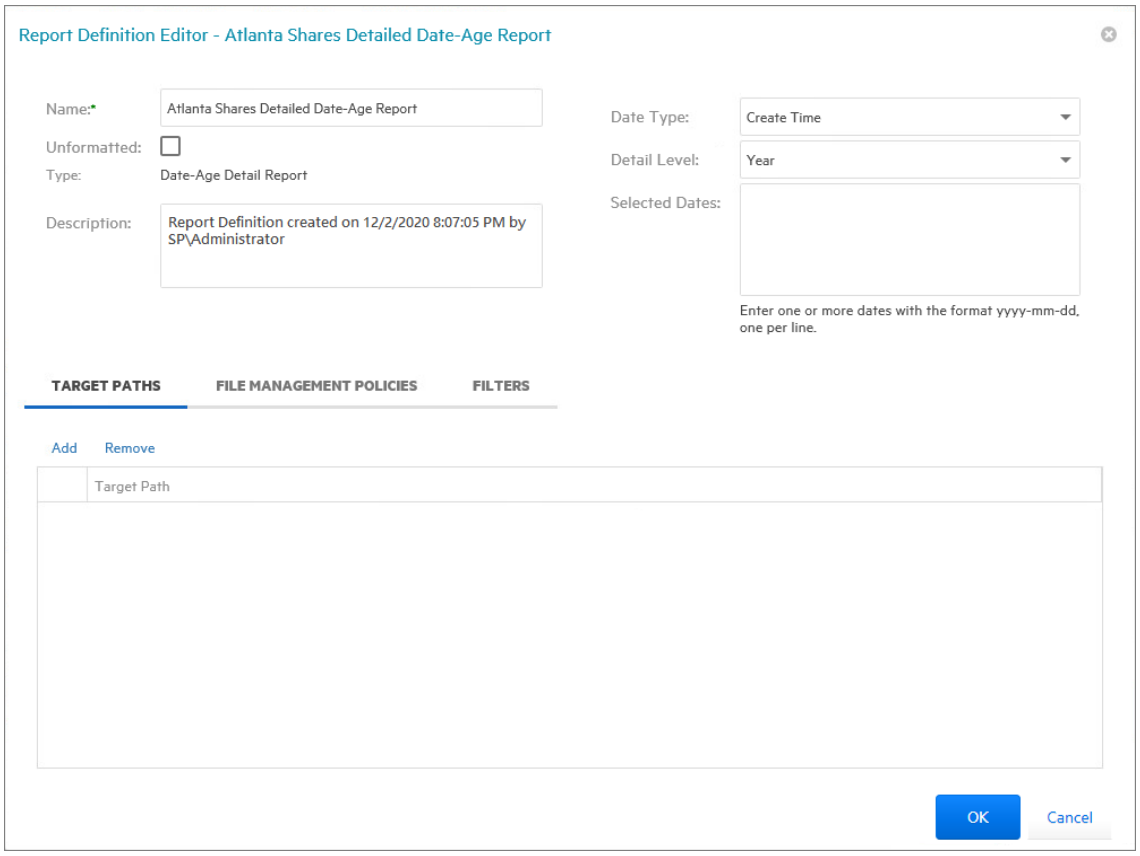
A Detailed Date-Age report is similar to a standard Date-Age report, except you can specify the exact create, modify, or access date parameters.

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Date-Age Detail** option and click **OK**.



5 In the **Date Type** drop-down menu, select an option.

Create Time: Reports when files were created.

Modify Time: Reports when files were last modified.

Access Time: Reports when files were last accessed.

6 In the **Detail Level** drop-down menu, select an option.

Year: Groups the file count in the report according to the year they were created, last modified, or last accessed.

Month: Groups the file count in the report according to the month they were created, last modified, or last accessed.

Day: Groups the file count in the report according to the calendar date they were created, last modified, or last accessed.

7 In the **Selected Dates** field, specify the dates you want.

This indicates that only the files created, last modified, or last accessed on those dates will be included in the report.

8 Browse to and specify the file paths you want included in the report and click **OK**.

9 (Optional) Click the **Filters** tab and set the filters for the report.

For information on using the filtering capabilities of File Reporter, refer to Section 10.5, “Built-in Report Filtering,” on page 85.

10 Click **Save**.

11 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.8 Permissions Reports

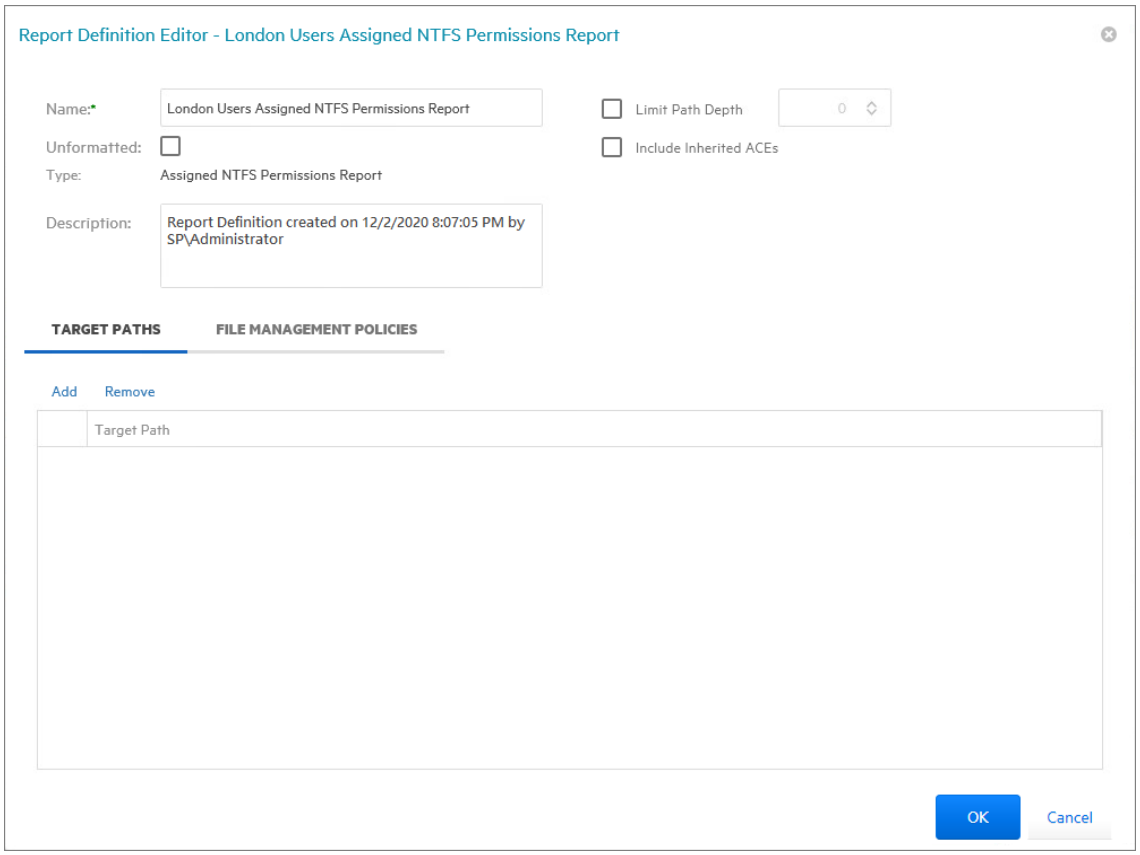
Reports in this classification include Assigned NTFS Permissions, Permissions by Path, and Permissions by Identity.

Before generating any type of Permissions report, you must first conduct a Permissions scan on the volumes or shares you want to report on.

10.8.1 Assigned NTFS Permissions Report

The Assigned NTFS Permissions report indicates the assigned Microsoft file system user permissions for all folders and subfolders from a specified path.

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Assigned NTFS Permissions** option and click **OK**.



5 (Conditional) If you want to limit the scope of the report to a set depth in the file structure, click the **Limit Path Depth** check box and specify the depth level.

   For example, if you specify 3, the report lists the file contents of all file paths in the specified target paths up to 3 levels in the file structure.

   If you do not specify a path depth, File Reporter will report on all levels of the specified target path.

6 (Conditional) If you don't want the report to include inherited ACEs (Access Control Entries), deselect the **Include Inherited ACEs** check box.

7 From the **Target Paths** tab, click **Add**.

8 Browse to and specify the file paths you want included in the report and click **OK**.

9 Click **Save**.

10 Generate the report as either a Preview report or a Stored report.

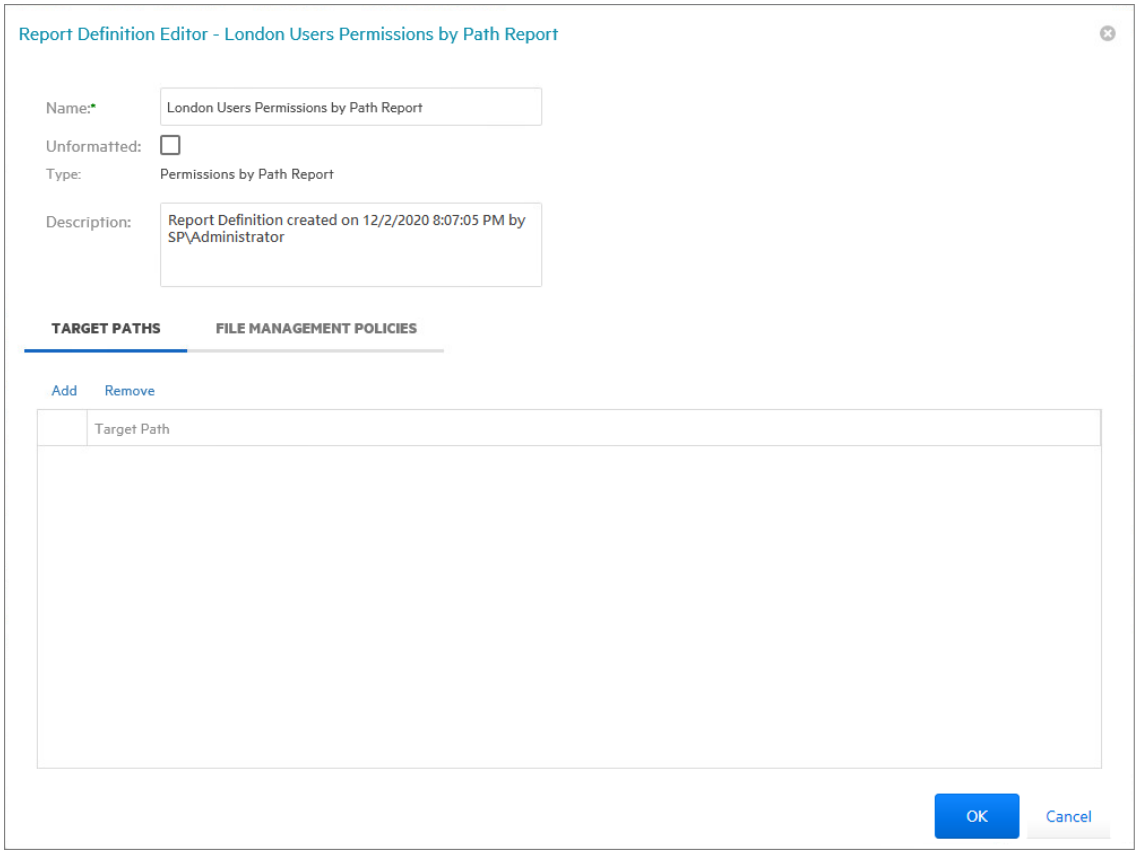
   For procedures on generating a Preview report, see Section 9.4, "Preview Reports," on page 72.

   For procedures on generating a Stored report, see Section 9.5, "Stored Reports," on page 74.

10.8.2 Permissions by Path Report

The Permissions by Path report indicates the effective permissions to the Microsoft file system according to the paths you specify.

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Permissions by Path** option and click **OK**.



5. From the **Target Paths** tab, click **Add**.
6. Browse to and specify the file paths you want included in the report and click **OK**.
7. Click **Save**.
8. Generate the report as either a Preview report or a Stored report.

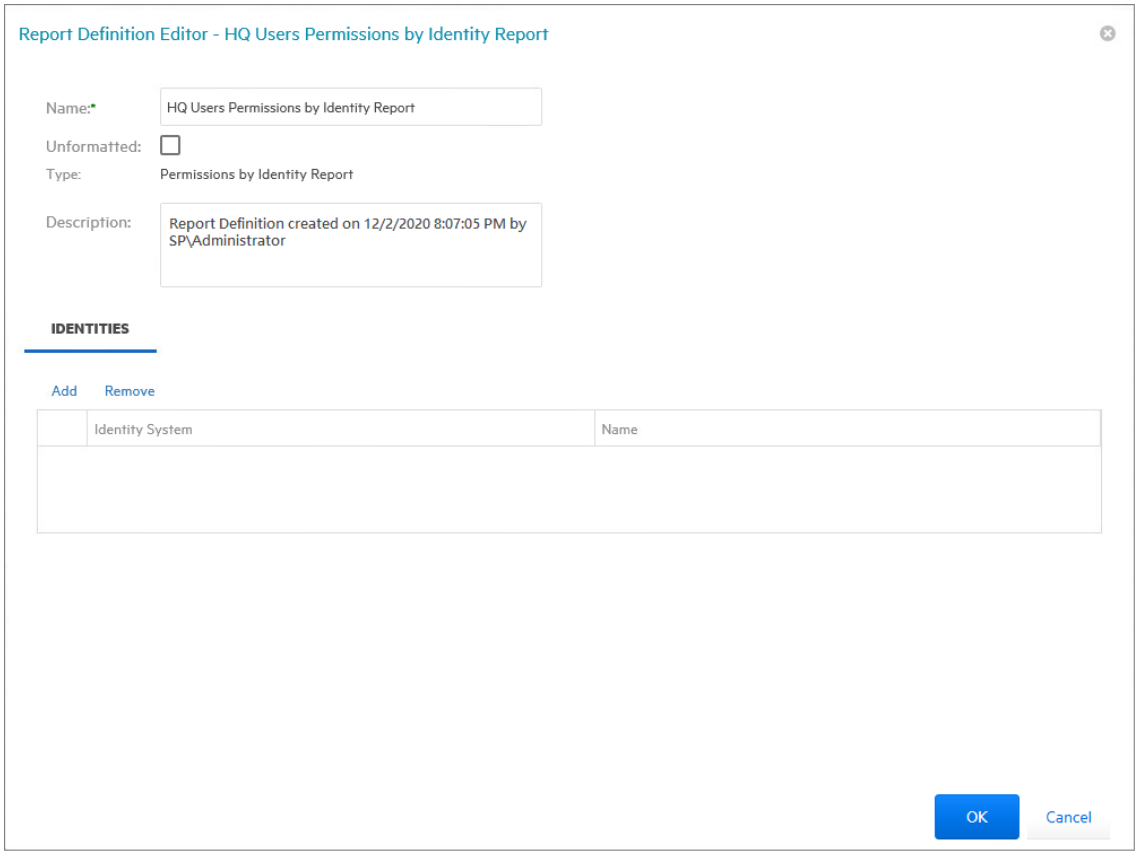
   For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

   For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.8.3 Permissions by Identity Report

The Permissions by Identity report indicates the effective permissions to the Microsoft file system according to the identities you specify.

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Select the **Permissions by Identity** option and click **OK**.



5. From the **Identities** tab, click **Add**.
6. Browse to and specify the identities you want included in the report.
7. Click **OK** to close the Identity Browser.
8. Click **Save** to close the Report Definition Editor.
9. Generate the report as either a Preview report or a Stored report.

   For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

   For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.9 Historic Comparison Reports

Historic Comparison reports specify the differences between two similar scan types of the same target system. For example, if you had a Previous Permissions scan of a Windows share and a Current Permissions scan of the same share, you could generate a Historic NTFS Permissions Comparison report that would specify the differences in permissions between the two points in time that the scans were taken.

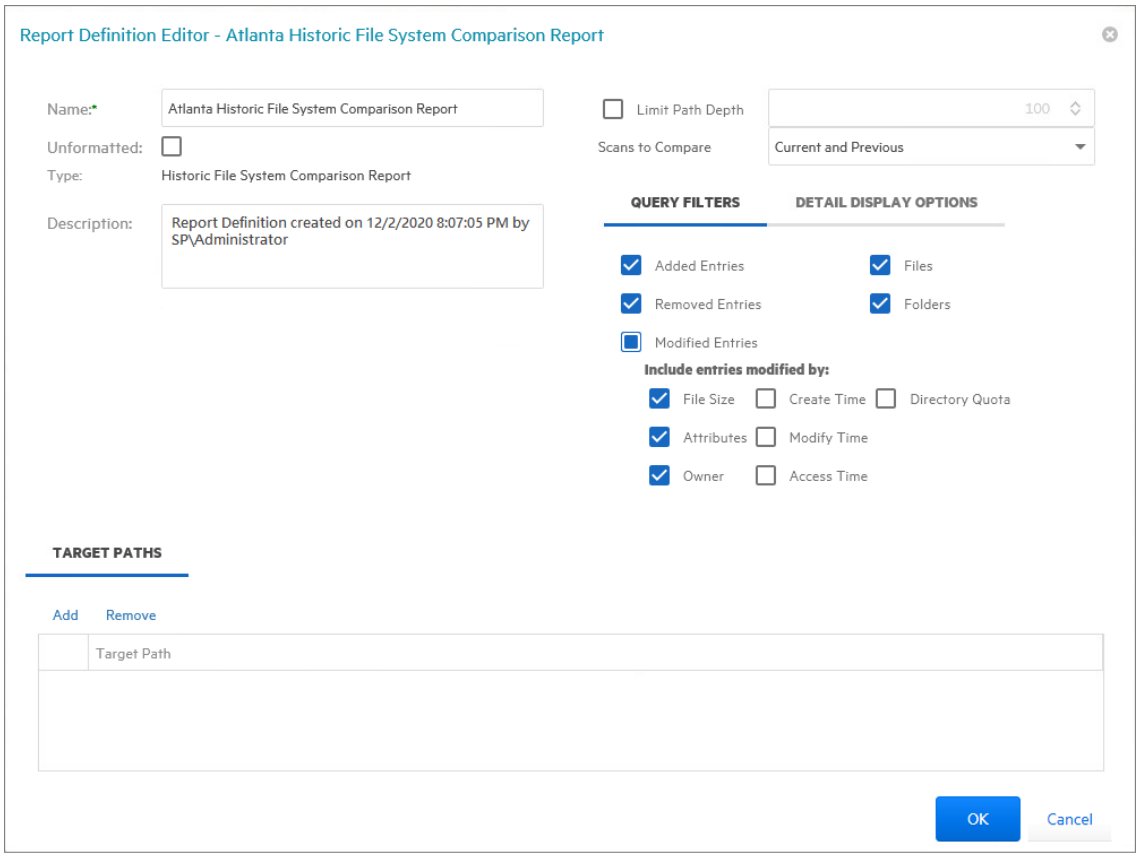
Historic Comparison reports can compare the following:

- Baseline scans to Previous scans
- Baseline scans to Current scans
- Historic scans to Current scans

Reports in this classification include Historic File System Comparison and Historic NTFS Permissions Comparison.

10.9.1 Historic File System Comparison Report

1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name of the report definition.
4. Under **Historic Comparison**, select the **File System Comparison** option, then click **OK**.



5 (Conditional) If you want to limit the scope of the report to a set depth in the file structure, click the **Limit Path Depth** check box and specify the depth level.

For example, if you specify 3, the report lists the file contents of all file paths in the specified target paths up to 3 levels in the file structure.

If you do not specify a path depth, File Reporter will report on all levels of the specified target path.

6 From the **Scans to Compare** drop-down menu, select one of the following options:

Current and Previous: Compares the Current scan of the storage resource to the Previous scan of the storage resource.

Current and Baseline: Compares the Current scan of the storage resource to the Baseline scan of the storage resource.

Previous and Baseline: Compares the Previous scan of the storage resource to the Baseline scan of the storage resource.

All options appear whether you have scans or not. If you do not have scans, File Reporter will generate an empty report.

7 In the **Query Filters** region, specify whether to include the following metadata categories in the report:

Added Entries: If you want the report to list files or folders that have been added since the older scan, leave this check box selected.

Removed Entries: If you want the report to list files or folders that have been removed since the older scan, leave this check box selected.

Modified Entries: If you want the report to list files or folders that have been modified since the older scan, leave this check box selected.

Files: If you want the report to list files, leave this check box selected.

Folders: If you want the report to list folders, leave this check box selected.

8 In the **Include entries modified by:** region of the **Query Filters**, specify which of the attributes modified between the older and newer scan you want included in the report.

9 In the **Detail Display Options** region, identify whether to display the metadata categories specified below in the **Detail Data** section of the report.

The categories below pertain to the **Detail Data** section of the report only, and not the **Summary Data** section.

Added Entries: If you want the report to display this category, whether there are added entries to list or not, select this check box.

Removed Entries: If you want the report to display this category, whether there are removed entries to list or not, select this check box.

Modified Entries: If you want the report to display this category, whether there are modified entries to list or not, select this check box.

10 (Conditional) If you selected the **Modified Entries** check box, in the **Always show modify detail for:** region, select any of the category options you want displayed in the report *whether these metadata categories have been changed between the two scans or not*.

By default, the **Modified Entries** section of the report only shows metadata that has changed. The options in this region of the dialog box are to force the display of one or more particular metadata properties.

Any metadata for an entry that File Reporter has determined has changed is displayed in bold font. Any optional data that has not changed is displayed in regular font.

11 Browse to and specify the file paths you want included in the report, then click **OK**.

12 Click **Save** to close the Report Definition Editor.

13 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

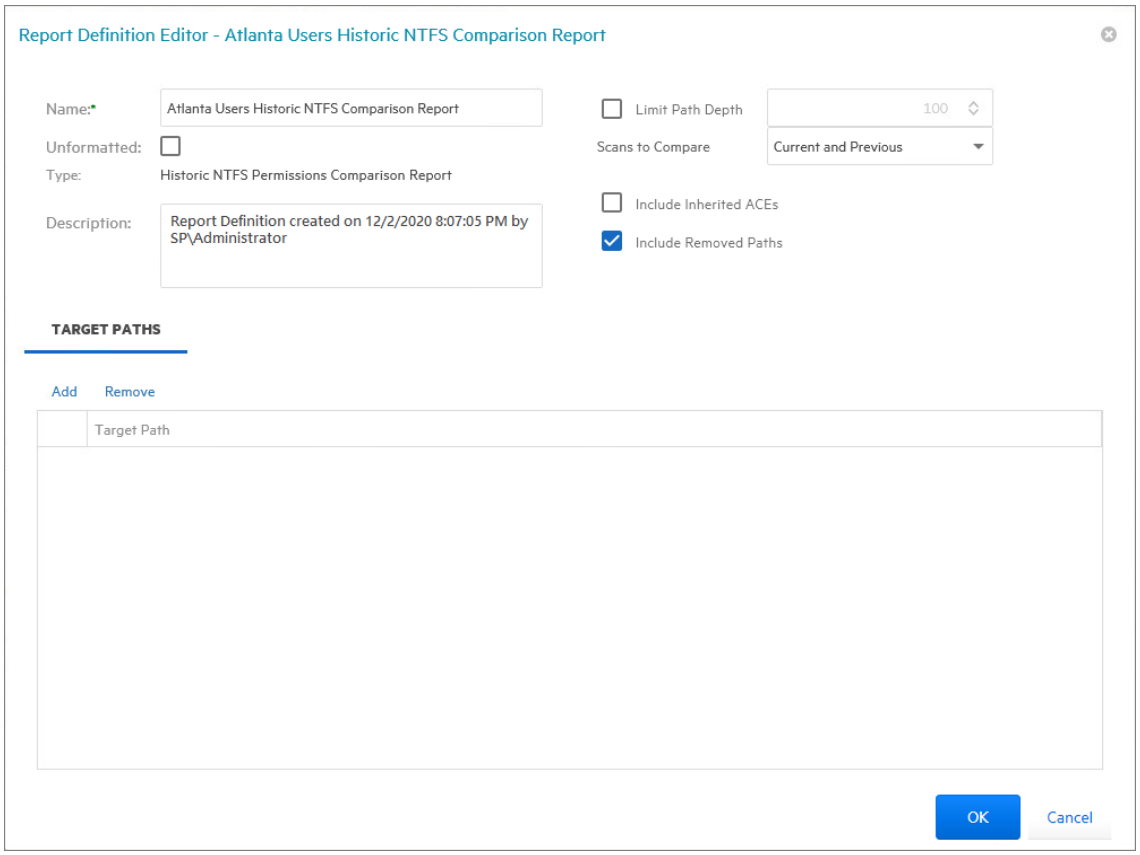
10.9.2 Historic NTFS Permissions Comparison Report

1 Select **Reports** > **Report Definitions.**

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Historic NTFS Permissions** option, then click **OK**.



5 (Conditional) If you want to limit the scope of the report to a set depth in the file structure, click the **Limit Path Depth** check box and specify the depth level.

For example, if you specify 3, the report lists the permissions of file contents of all file paths in the specified target paths up to 3 levels in the file structure.

If you do not specify a path depth, File Reporter will report on all levels of the specified target path.

6 From the **Scans to Compare** drop-down menu, select one of the following options:

Current and Previous: Compares the Current scan of the storage resource to the Previous scan of the storage resource.

Current and Baseline: Compares the Current scan of the storage resource to the Baseline scan of the storage resource.

Previous and Baseline: Compares the Previous scan of the storage resource to the Baseline scan of the storage resource.

All options appear whether you have scans or not. If you do not have scans, File Reporter will generate an empty report.

7 (Conditional) If you want your report to include not only direct permissions, but inherited permissions, select the **Include Inherited ACEs** check box.

Reporting inherited permissions could make the report significantly larger.

8 (Conditional) If you do not want the report to list any paths that have been deleted or removed, deselect the **Include Removed Paths** check box.

9 Browse to and specify the file paths you want included in the report, then click **OK**.

10 Click **Save** to close the Report Definition Editor.

11 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.10 Trending Report

Currently, the only report in this classification is the Volume Free Space report. Before generating a Volume Free Space report, you must first conduct a Volume Free Space scan on the volumes or shares you want to report on.

10.10.1 Volume Free Space Report

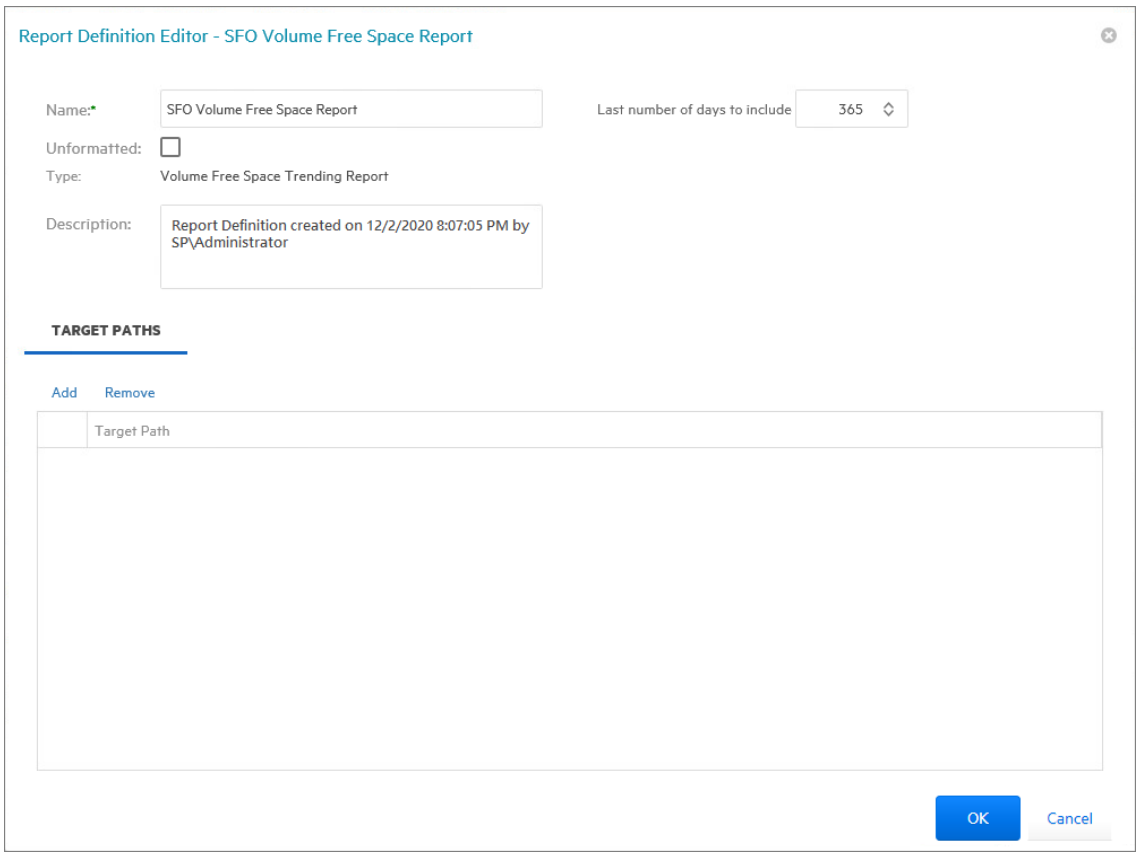
The Volume Free Space report lets you view available Windows share disk space over a set amount of time. For best results, you should conduct regularly scheduled Volume Free Space scans on specific shares. File Reporter then has the data it needs to graph the pattern of free space on the share.

1 Select **Reports** > **Report Definitions**.

2 Click **Add**.

3 In the **Name** field, specify a descriptive name of the report definition.

4 Select the **Volume Free Space** option and click **OK**.



5 In the **Last number of days to include** field, specify the last number of days you want the report to include.

   For example, if you want the report to graph the last month, enter 30.

   The lowest number you can specify is 7.

6 Browse to and specify the shares you want included in the report and click **OK**.

7 Click **Save**.

8 Generate the report as either a Preview report or a Stored report.

   For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

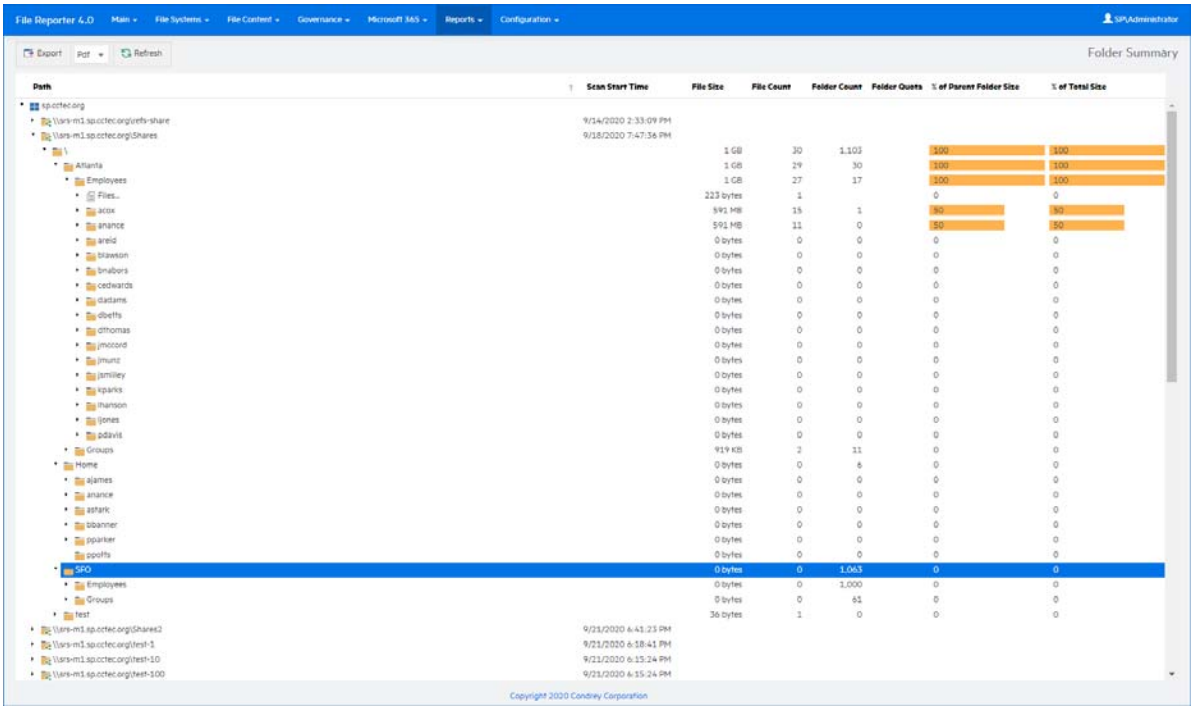
   For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

10.11 Folder Summary Reports

The Folder Summary feature provides you with a visual folder structure according to the latest scanned file system data. Folder Summary also provides extensive summary information for the folders and files.

You can access Folder Summary by selecting **Reports** > **Folder Summary**.

Figure 10-5 *Folder Summary*



11 Custom Query Reports

11.1 Overview

Custom Query reports are generated through SQL queries that you enter. Furthermore, you have the option to display the results in report layouts. These commands enable you to generate very specific detail in reports that are not available through the built-in report types in File Reporter.

The SQL queries must be specific to the database (Microsoft SQL Server or PostgreSQL) that your deployment of File Reporter is utilizing.

NOTE: For details and examples of the supported database functions, tables, and views that you can utilize in Custom Query reports, refer to the Micro Focus File Reporter 4.1 Database Schema and Custom Queries Guide.

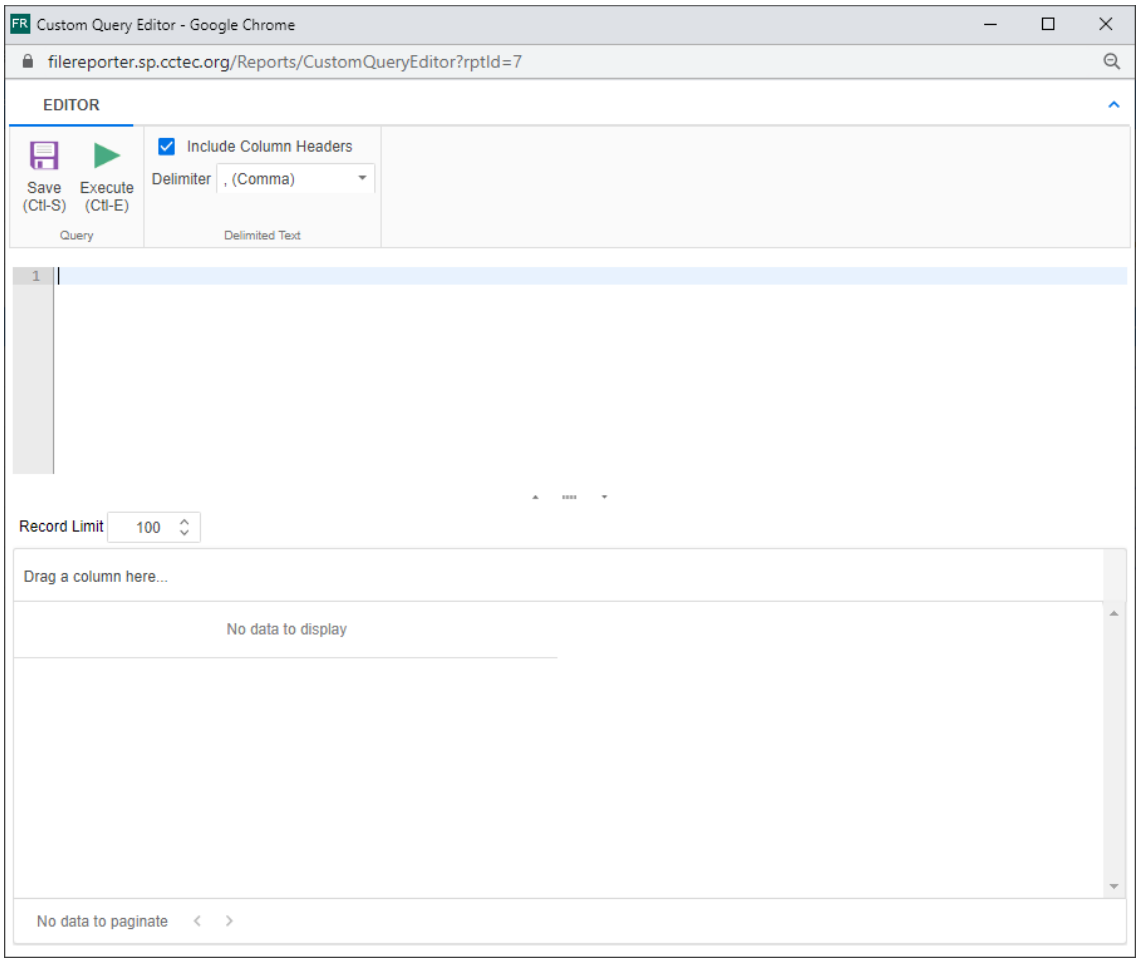
SQL queries are entered through report editors available from the File Reporter browser-based administrative interface and from the Report Designer client tool.

NOTE: For details on using the report editor in the Report Designer, see Report Designer in the *Micro Focus File Reporter 4.1 Client Tools Guide*.

TIP: Don't forget to utilize File Query Cookbook as a resource for obtaining SQL queries and sample report layouts. Both the SQL commands and report layouts can be customized as needed. You can access the File Query Cookbook directly through the Report Designer interface, or at https://www.filequerycookbook.com.

11.1.1 Build a Custom Query Report

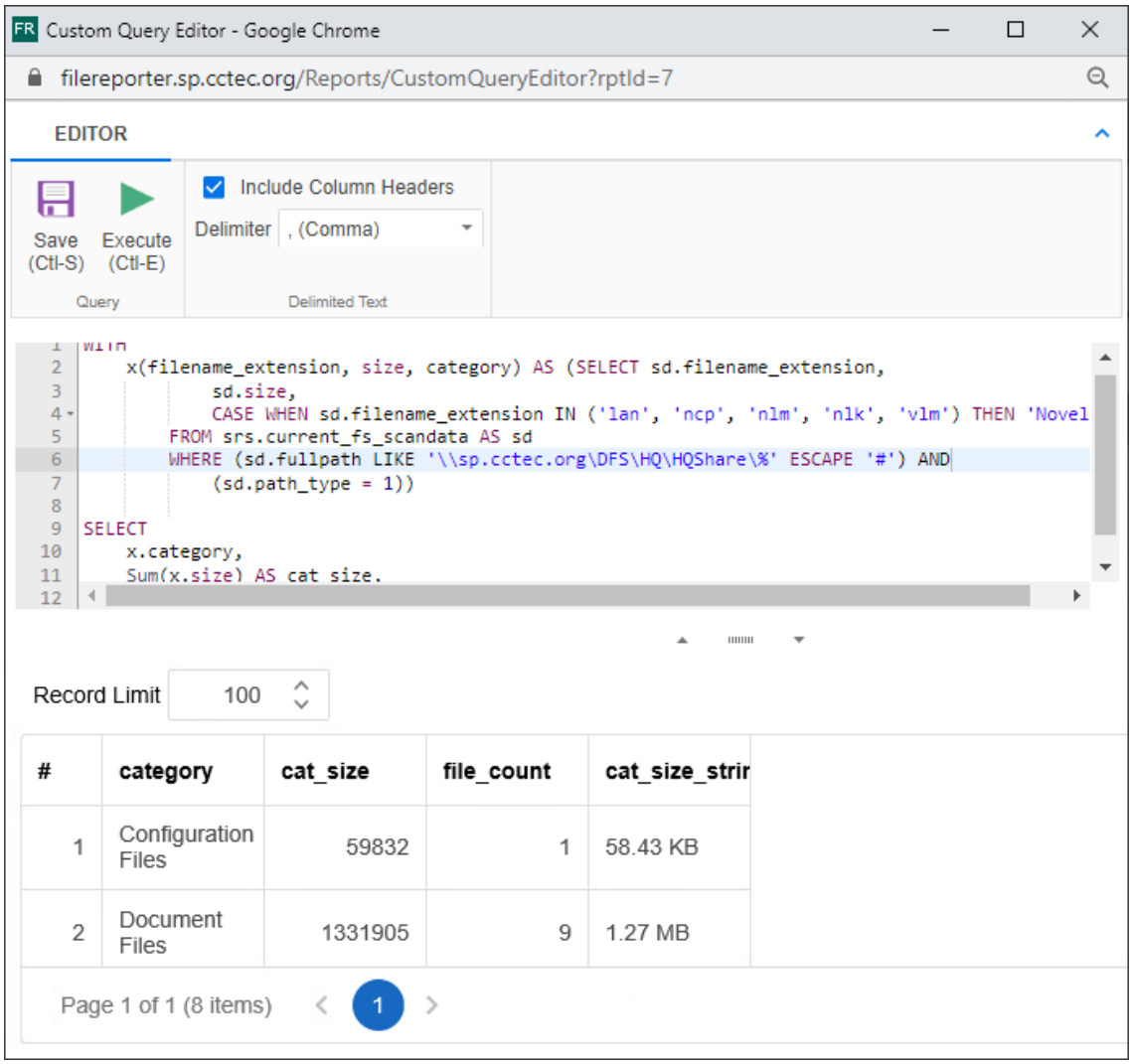
1. Select **Reports** > **Report Definitions**.
2. Click **Add**.
3. In the **Name** field, specify a descriptive name for the report definition.
4. Select **Custom Query Report**.
5. Click **OK**.



6 Enter the SQL query according to what information you want included in your report.

As you update the query, you can click **Execute** to get a preview in the bottom portion of the editor of how the report will appear.

The **Row Limit** setting does not limit the size of the report. Instead, it limits how much can be previewed.



7 When you are satisfied with the report and the previewed results, click **Save**.

8 Close the Custom Query Report Editor.

9 Select **Reports** > **Report Definitions**.

10 Select the Custom Query Report you just saved and generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see Section 9.4, “Preview Reports,” on page 72.

For procedures on generating a Stored report, see Section 9.5, “Stored Reports,” on page 74.

A Security Settings

A.1 Windows Firewall Settings

Depending on the host system, exceptions must be added to the firewall rules for that host. The following are needed for successful operation of File Reporter tasks.

NOTE: Inbound firewall exceptions for File Reporter components installed on Windows are set up automatically during configuration of each component.

- The Engine must remain permitted to make outbound connections.
- The Engine must remain able to listen on port 3035.

  This is the default port choice that is presented during the installation and configuration.
- AgentFS must be permitted to make outbound connections.
- AgentFS must remain able to listen on TCP port 3037.

  This is the default port choice that is presented during the installation and configuration.
- The Web Application hosted on IIS must be allowed to listen on TCP ports 80 and 443.
- On each server hosting storage that you wish to collect quota via proxy, you must enable the Remote File Server Resource Manager Management - FSRM Service (RPC-In) firewall rule.
- If File Content Analysis is enabled:
  - ManagerFC must remain permitted to make outbound connections.
  - AgentFC must remain permitted to make outbound connections.
  - RabbitMQ must remain permitted to make outbound connections.
  - RabbitMQ must remain permitted to listen on TCP port 15671 for the management interface.

    This is the default port that RabbitMQ is configured for with TLS.
  - RabbitMQ must remain permitted to listen on TCP port 5671.

    This is the default port that RabbitMQ is configured for with TLS.

A.2 Windows LSA User Rights

Windows Local Security Authority (LSA) rights and privileges are assigned to accounts or groups, and they determine how those accounts or group members may access the system. The User Rights are modified through the Local Security Policy from:

Start > Administrative Tools > Local Security Policy

1. In Local Security Policy, go to the following:

   Security Settings > Local Policies > User Rights Assignments

2. Verify that the File Reporter proxy rights group has the following assignments:
   - Access this computer from the network
   - Back up files and directories
   - Bypass traverse checking
   - Create a token object
   - Create symbolic links
   - Impersonate a client after authentication
   - Log on as a batch job
   - Manage auditing and security log

IMPORTANT: Absence or removal of these privileges may prevent the Engine and Agent components from functioning properly.

In some cases, Group Policy Object (GPO) settings may remove or override the necessary Local Security Policy settings and revoke the membership of the File Reporter proxy object from one or more required LSA privileges.

If GPO conflicts are detected, set up an additional GPO with just the privileges listed above and assign it to the proxy rights group for the appropriate servers.

A.3 Proxy Rights Group

By default, whenever any of the components of File Reporter are installed on a server in a domain, the proxy rights security group is granted membership in that server's built-in Administrators security group. This grants File Reporter certain permissions needed in addition to the LSA privileges required for successful scanning of file system metadata.

On other servers in the domain that are hosting storage to be scanned by File Reporter through a proxy agent, you must also grant the proxy rights group membership in the built-in Administrators group. This is necessary because there are many actions performed that require membership in this group regardless of the LSA privileges that the user has been granted—in particular, reading directory quotas.

Additionally, the other servers in the domain that are not hosting components, but are hosting storage to be scanned, must have the necessary rights and privileges, along with some file share and NTFS permissions. The easiest way of granting these rights and privileges is through Group Policy objects in Active Directory.

At a minimum, you must grant read-only sharing and security privileges to the proxy rights group for each share that File Reporter will scan.

A.4 Windows File Server Cluster

File Reporter supports clustering of Windows Server through Proxy Agents. Configuring a cluster to be scanned through a proxy agent is similar to configuring an individual server to be scanned by a proxy agent.

To support proxy-based scanning, the File Reporter proxy rights group must be granted membership in the built-in Administrators group and granted all of the required LSA user rights on each cluster node. When this is done, the folder share permissions and NTFS permissions that are required must be granted to the proxy rights group for all shares and NTFS volumes that will be scanned by File Reporter.

B Log File Locations

When troubleshooting Micro Focus File Reporter, you might need to refer to component log files. The locations for each are specified in the table below.

Table B-1 *Log File Locations*

Component	Typical Log File Path
Engine	`C:\ProgramData\Micro Focus\SRS\Engine\log\srsengine.log`
Scan Processor	`C:\ProgramData\Micro Focus\SRS\Engine\log\scanprocessor.log`
AgentFS	`C:\ProgramData\Micro Focus\SRS\AgentFS\log\SRSAgentFS.log`
Web Application	`C:\inetpub\srs_root\AppData\logs\webui.log`
ManagerFC	`C:\ProgramData\Micro Focus\SRS\ManagerFC\log\SRSManagerFC.log`
AgentFC	`C:\ProgramData\Micro Focus\SRS\AgentFC\log\SRSAgentFC.log`
Agent365	`C:\ProgramData\Micro Focus\SRS\Agent365\log\SRSAgent365.log`

C AgentFS Scan Capabilities

C.1 Server Platform and NAS Device Support

The following platforms are supported as server hosts for scan targets.

Table C-1 *Supported Server Hosts for Scan Targets*

Server Platform	Local Scan or Proxy Scan	Proxy Scan Only
Windows Server 2022	✔	
Windows Server 2019	✔	
Windows Server 2016	✔	
Windows Server 2012 R2	✔	
Windows Server 2012		✔
Windows Server 2008 R2		✔
Windows Server 2008		✔

Older Windows servers including Windows Server 2003 or 2003 R2 might work but are not supported as scan target hosts.

The following NAS devices are supported as hosts for scan targets.

Table C-2 *Supported Scan Target NAS Hosts*

NAS Device	Scan Type
NetApp Filer with OnTAP 9.*x*	Proxy scan only
Isilon OneFS 8.2, 9.*x*	Proxy scan only

NOTE: Older versions of NetApp OnTAP and Isilon OneFS might work but are not supported.

NOTE: Other NAS devices not listed here might work with limited support if running a vendor supported version of the device and management software.

C.2 File System Feature Support

The following table lists file system scanning capabilities of File Reporter.

Table C-3 *File System Metadata Support*

Feature	NTFS	ReFS
File Name / Extension	✔	✔
File Size	✔	✔
File Sparse Size	✔	✔
File Compressed Size	✔	✘
File Size on Disk[1]	✔	✔
Create Time	✔	✔
Modify Time	✔	✔
Access Time	✔	✔
Directory Quota2	✔	✘
Owner	✔	✔
Encrypting File System (EFS)	✘	✘

1. File size-on-disk calculations default to an assumed 4 KB block size in cases where AgentFS cannot retrieve the actual allocation size.
2. Directory Quotas are only available on Windows 2008 R2 and later servers, and only if the File Server Resource Manager (FSRM) Role has been installed.

C.3 Security Scans

Table C-4 *Permission Scan Capabilities*

Windows Component	Supported	Notes
Share Permissions	✔	

Windows Component	Supported	Notes
Security Descriptors	✔	Includes the DACLs, owner, and all ACE and security descriptor flags. However, only security descriptors for folders are currently collected. Additionally, deny ACEs are not factored into calculations for Permission by Identity or Permission by Path reports.
Universal Security Groups	✔	
Global Security Groups	✔	
Local Security Groups	✘	The local security groups themselves are collected, but group memberships for local security groups are not currently processed.
Nested Group Memberships	✔	Nested group membership is collected as a flat list of all intermediate and leaf groups, users, and other security principals. The hierarchy of group nesting is not currently preserved.
Primary Groups	✔	
Local Security Authority (LSA) Privileges	✘	LSA privileges are not currently collected.

C.4 Other Microsoft Supported Features

- Multiple domains in a single forest
- Distribute File System (DFS) running in domain-based mode

C.5 Current Limitations

- No scanning of workstations
- No scanning for standalone servers
- No support for Distributed File System (DFS) in standalone mode
- No support for Single Label Domains
- No support for FAT or FAT32 file systems
- No support for Trusted Forests

D NAS Device Considerations

D.1 NetApp Filer

For a NetApp Filer device, the configuration is very simple because the device does not fully emulate a Windows Server at the operating system level.

1. Use the NetApp Filer administration utility to join the NAS device to a domain where File Reporter can report.
2. Grant the proxy rights group membership in the NAS device’s built-in Administrators group.
3. Grant the proxy rights group the folder share permissions that are required to access the storage.

   There are no LSA privileges to grant on a NetApp Filer NAS device.

D.2 EMC Isilon

Perform the following steps to integrate an EMC Isilon device. You can use these same steps to see if other NAS devices integrate with File Reporter.

1. Rebuild the storage resources and verify that the NAS device is displayed on the list.
2. Perform any needed steps for giving the proxy rights group access to the desired shares and folders on the NAS device.

D.3 Other NAS Devices

Perform the following steps to see if other NAS devices integrate with File Reporter.

1. In the associated Computer object in Active Directory, add the following text somewhere in the description attribute for that object:

   ```
   ***SRGenericNASDevice***
   ```
2. Rebuild the storage resources and verify that the NAS device is displayed on the list.
3. Perform any needed steps for giving the proxy rights group access to the desired shares and folders on the NAS device.

E Resetting the Proxy User Password

If the proxy user password is not working, you can reset it through the Engine Configuration Utility. As part of the configuration process, it resets the proxy user password.