



Micro Focus File Reporter 4.0 Administration Guide

January 8, 2021

Legal Notices

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

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

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

Copyright © 2021 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion without the express written consent of the publisher.

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

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

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	7
1 What's New	9
1.1 New in Version 4.0	9
2 Overview	11
2.1 Micro Focus File Reporter	11
2.2 How File Reporter Works	11
2.2.1 Core Components	12
2.2.2 File System Scanning	13
2.2.3 File Content Scanning	14
2.2.4 Microsoft 365 Cloud Scanning	15
2.2.5 Reporting	15
2.2.6 Client Tools	18
3 The Administrative Interface	23
3.1 Supported Browsers	23
3.2 Launching the Administrative Interface	23
3.3 Using the Administrative Interface	25
3.3.1 Viewing Notifications	25
3.3.2 Configuring the Web Interface	26
3.3.3 Viewing System Information	27
4 Performing Setup Procedures	29
4.1 Viewing Storage Resources	29
4.2 Assigning Proxy Targets	31
4.3 Configuring Notifications	32
4.4 Integrating with File Dynamics	33
5 Scheduling and Performing File System Scans	35
5.1 Scans	35
5.1.1 Scan Retention	36
5.2 Adding a Scan Target	36
5.3 Removing a Scan Target	38
5.4 Creating Scan Policies	38
5.5 Establishing a Baseline Scan	42
5.6 Clearing a Baseline Scan	43
5.7 Editing a Scan Policy	43
5.8 Deleting a Scan Policy	43
5.9 Scheduling Scans	43
5.10 Editing a Scheduled Scan	45

5.11	Clearing a Schedule on a Scheduled Scan	45
5.12	Conducting an Immediate Scan	45
5.13	Viewing Scans in Progress	45
5.14	Retrying Failed Scans	46
5.15	Viewing Scan Data	47
5.16	Viewing Scan History	47
5.17	Troubleshooting a Failed Scan	48
5.18	Scanning Your Microsoft 365 Tenant	48
5.18.1	Scan the Microsoft 365 Tenant	49
5.18.2	Scan Selected Drives	50

6 Generating File System Reports 51

6.1	Overview	51
6.2	Changing Your Cover Sheet Branding	52
6.3	Changing the Report Data Font	54
6.4	Built-in Report Types	55
6.5	Directory Data Reports	56
6.5.1	Generating a Summary Report	56
6.5.2	Generating a Directory Quota Report	63
6.5.3	Generating a Storage Cost Report	64
6.5.4	Generating a Comparison Report	65
6.6	Permissions Reports	66
6.6.1	Generating an Assigned NTFS Permissions Report	66
6.6.2	Generating a Permissions by Path Report	68
6.6.3	Generating a Permissions by Identity Report	69
6.7	File Data Reports	70
6.7.1	Generating a Filename Extension Report	70
6.7.2	Generating a Detailed Filename Extension Report	71
6.7.3	Generating an Owner Report	73
6.7.4	Generating a Detailed Owner Report	74
6.7.5	Generating a Duplicate File Report	75
6.7.6	Generating a Detailed Duplicate File Report	76
6.7.7	Generating a Date-Age Report	78
6.7.8	Generating a Detailed Date-Age Report	79
6.8	Historic Comparison Reports	81
6.8.1	Generating a Historic File System Comparison Report	81
6.8.2	Generating a Historic NTFS Permissions Comparison Report	83
6.9	Trending Report	85
6.9.1	Generating a Volume Free Space Report	85
6.10	Unformatted Reports	86
6.10.1	Generating Unformatted Reports	86
6.11	Custom Query Reports	87
6.11.1	Generating a Content Hashed Duplicate File Report	90
6.11.2	Generating Microsoft 365 Reports	97
6.12	Micro Focus File Dynamics Policy Reports	100
6.13	Scheduling Reports	101
6.14	Editing a Scheduled Report	103
6.15	Clearing a Schedule on a Scheduled Report	103
6.16	Copying a Report Definition	103
6.17	Viewing Reports in Progress	104
6.18	Troubleshooting Reports	105

7	Content Scanning and Reporting	107
7.1	Creating File Content Classifications	107
7.1.1	Creating a New Classification	107
7.1.2	Editing a Classification	108
7.2	Creating File Content Categories	108
7.2.1	Creating a New Category	108
7.2.2	Editing a Category	109
7.3	Creating Search Patterns	109
7.3.1	Creating a New Search Pattern	109
7.3.2	Editing a Search Pattern	111
7.4	Creating Job Definitions	111
7.4.1	Creating a New Job Definition	111
7.4.2	Editing a Job Definition	114
7.5	Viewing Jobs in Progress	114
7.6	Viewing Scanned Data Jobs	115
7.7	Viewing Search Results	115
7.8	Viewing AgentFC Configuration Registrations	116
8	Performing Other Administrative Tasks	117
8.1	Stopping and Restarting Services	117
8.2	Using Folder Summary	118
8.3	Considerations for Reporting on NAS Devices	119
8.3.1	NetApp filer	119
8.3.2	EMC Isilon	120
8.3.3	Other NAS Devices	120
8.4	Changing the Default Path for Stored Reports	120
8.5	Changing the Life Span of Stored Reports	121
8.6	Resetting the Proxy User Password	121
9	Using the Report Viewer	123
9.1	Use the Report Viewer	123
10	Using the Data Analytics Tools	127
10.1	Launching the Analytics Tools	127
10.2	Using the Dashboard	129
10.3	Using the Tree Map	131
10.4	Using the Pivot Grid	132
11	Using Report Designer	137
11.1	Using the Report Designer Interface	137
11.2	Creating a Custom Query Report	139
11.3	Designing a Custom Query Report	142
11.4	Saving the Layout as a Template	152
11.5	Using a Saved Template for Custom Query Reports	152

A	Filtering for Built-in Reports	155
A.1	Filters Tab	155
A.1.1	Filter Expression Builder	156
A.1.2	Relative Date Filtering Parameters	157
A.2	Single Entry Filter Conditions	157
A.2.1	Using the Filter Expression Builder	157
A.2.2	Using the Relative Date Filtering Settings	159
A.3	Multi-Condition Filtering	159
B	Security Settings	161
B.1	Rights and Privileges on Scanned Storage	161
B.1.1	Granting Rights	161
B.2	Firewall Requirements	161
B.3	Local Security Authority Rights and Privileges	162
B.4	Proxy Rights Group	163
B.5	Windows Clustering through Proxy Agents	163
C	Log File Locations	165
D	AgentFS Scan Capabilities	167
D.1	Server Platform and NAS Device Support	167
D.2	File System Metadata	168
D.3	Security Scans — Active Directory File Systems	169
D.4	Other Microsoft Supported Features	169
D.5	Current Limitations	169
E	Glossary	171

About This Manual

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

- ♦ Chapter 1, “What’s New,” on page 9
- ♦ Chapter 2, “Overview,” on page 11
- ♦ Chapter 3, “The Administrative Interface,” on page 23
- ♦ Chapter 4, “Performing Setup Procedures,” on page 29
- ♦ Chapter 5, “Scheduling and Performing File System Scans,” on page 35
- ♦ Chapter 6, “Generating File System Reports,” on page 51
- ♦ Chapter 7, “Content Scanning and Reporting,” on page 107
- ♦ Chapter 8, “Performing Other Administrative Tasks,” on page 117
- ♦ Chapter 9, “Using the Report Viewer,” on page 123
- ♦ Chapter 10, “Using the Data Analytics Tools,” on page 127
- ♦ Chapter 11, “Using Report Designer,” on page 137
- ♦ Appendix A, “Filtering for Built-in Reports,” on page 155
- ♦ Appendix B, “Security Settings,” on page 161
- ♦ Appendix C, “Log File Locations,” on page 165
- ♦ Appendix D, “AgentFS Scan Capabilities,” on page 167
- ♦ Appendix E, “Glossary,” on page 171

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, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Micro Focus File Reporter 4.0 Administration Guide*, visit the [Micro Focus File Reporter Documentation website](#).

Additional Documentation

For additional File Reporter 4.0 documentation, see the following guides at the [Micro Focus File Reporter Documentation website](#):

- ◆ *[Micro Focus File Reporter 4.0 Installation Guide](#)*
- ◆ *[Micro Focus File Reporter 4.0 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 4.0

Reporting for Microsoft 365

File Reporter is now enabled to scan Microsoft 365 cloud repositories for data and associated permissions for OneDrive for Business, SharePoint Online, and Teams.

Advanced Duplicate File Detection

A new scanning option allows for Agents to produce a content-based hash for specific files for complete duplicate detection and aggregate reporting. New packaged Custom Query reports can then generate a report of duplicate files based on hash comparisons.

Pre-built Custom Queries and Report Layouts

For reporting on files and permissions in the Microsoft 365 cloud, File Reporter includes pre-built custom queries and report layouts that you can utilize.

Reporting Exclusive to the Microsoft Network and 365 Cloud Platforms

Previous versions of File Reporter reported on both Microsoft and Micro Focus Open Enterprise Server (OES) platforms. While the release of File Reporter 4.0 discontinues this multi-platform reporting, File Reporter continues to provide OES reporting through File Reporter 3.6. File Reporter customers have entitlements to both product versions. Micro Focus will continue to support OES and eDirectory through the File Reporter 3.x product line.

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.

- ♦ [Section 2.1, “Micro Focus File Reporter,” on page 11](#)
- ♦ [Section 2.2, “How File Reporter Works,” on page 11](#)

2.1 Micro Focus File Reporter

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.

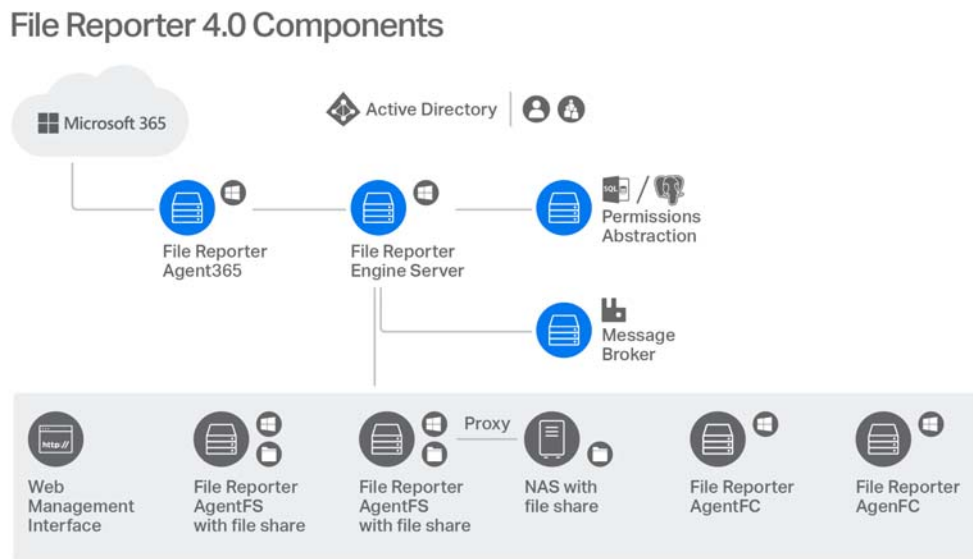
2.2 How File Reporter Works

- ♦ [Section 2.2.1, “Core Components,” on page 12](#)
- ♦ [Section 2.2.2, “File System Scanning,” on page 13](#)
- ♦ [Section 2.2.3, “File Content Scanning,” on page 14](#)
- ♦ [Section 2.2.4, “Microsoft 365 Cloud Scanning,” on page 15](#)
- ♦ [Section 2.2.5, “Reporting,” on page 15](#)
- ♦ [Section 2.2.6, “Client Tools,” on page 18](#)

File Reporter was developed to examine, report and analyze Windows 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



2.2.1 Core Components

The following are core components of Micro Focus File Reporter.

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

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

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

2.2.2 File System Scanning

The following are components associated with file system scanning.

Scan Processor

The Scan Processor does the following:

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

Agents

Agents are compact programs that run on Microsoft Windows Server hosts. Agents can examine and report on NTFS file systems and OneDrive for Business, SharePoint Online, and Teams files stored in the Microsoft 365 cloud. Additionally, Agents examine and report on security, including file and folder permissions. For more information, see [Appendix D, “AgentFS Scan Capabilities,” on page 167](#).

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 type of devices, Agents can be set up as proxy agents.

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

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 analyzing 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 [Chapter 5, “Scheduling and Performing File System Scans,”](#) on page 35.

2.2.3 File Content Scanning

The following are components associated with file content scanning.

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

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.

Scans

Through AgentFC, the RabbitMQ messaging broker, 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 or credit card numbers.

2.2.4 Microsoft 365 Cloud Scanning

With the release of version 4.0, File Reporter extends the ability to report what files are being stored on your enterprise storage devices and who has access to these files, to 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 Custom Queries and report layouts available at filequerycookbook.com. The process is as easy as searching through the cookbook to see what type of report you want to generate, downloading it, pasting the query into the File Reporter Report Designer Query Editor, defining any needed paths or making desired modifications, and then laying out the report.

2.2.5 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

Built-in Reports

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

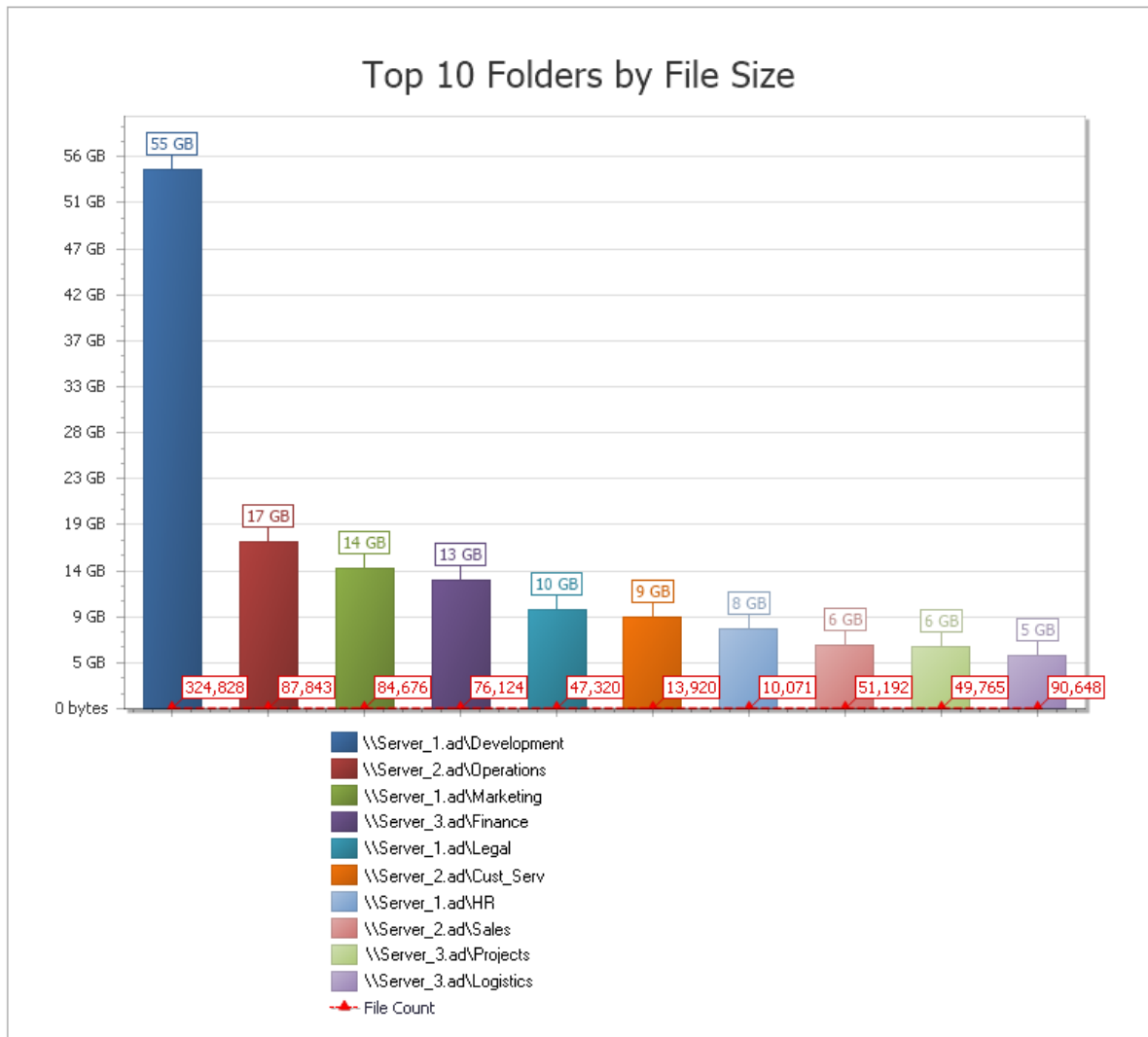
To generate a report, the Engine takes all of the needed scans that are applicable to the specifications of the report and consolidates them into a single report by indexing the applicable scans.

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	
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



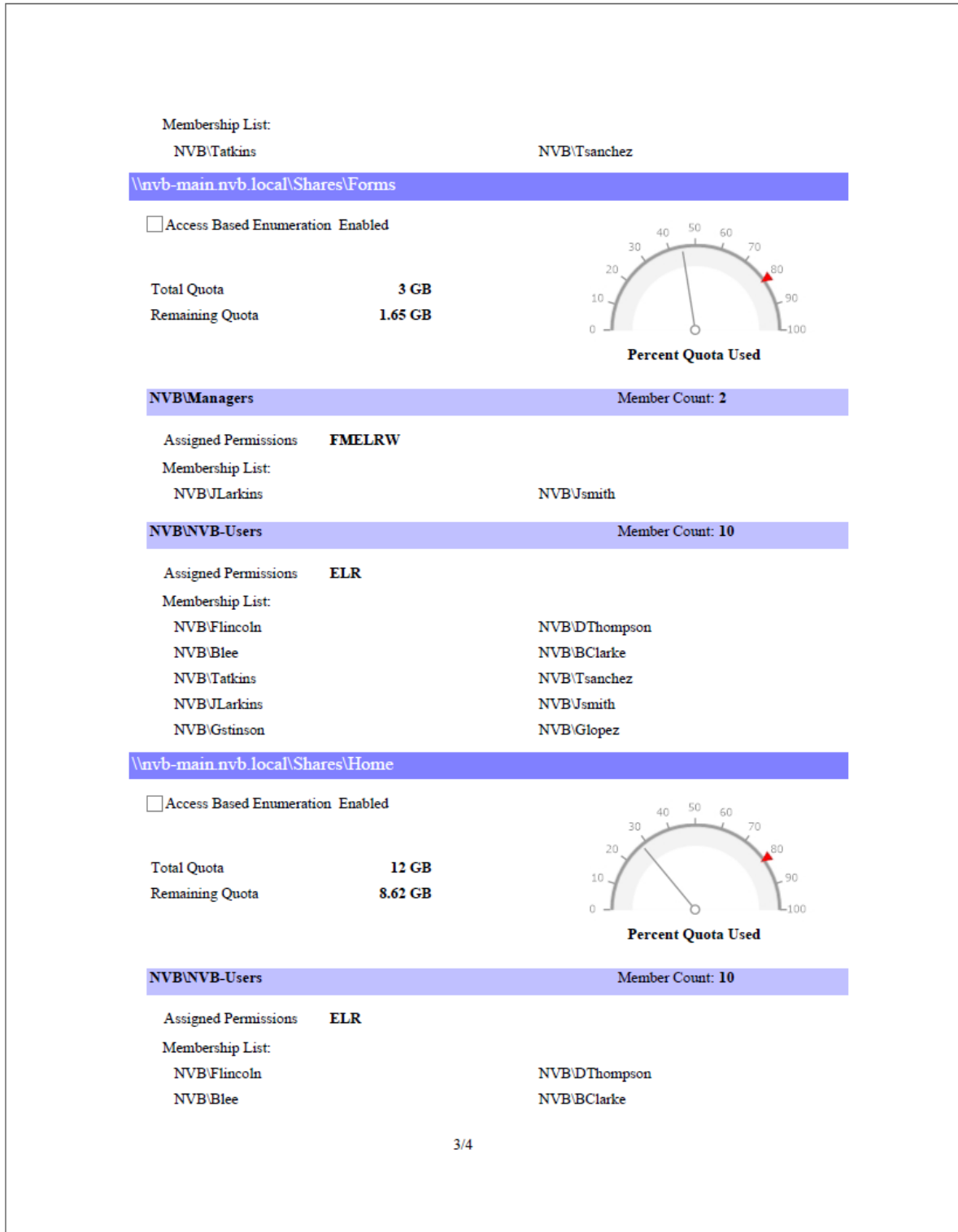
Custom Query Reports

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.



2.2.6 Client Tools

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

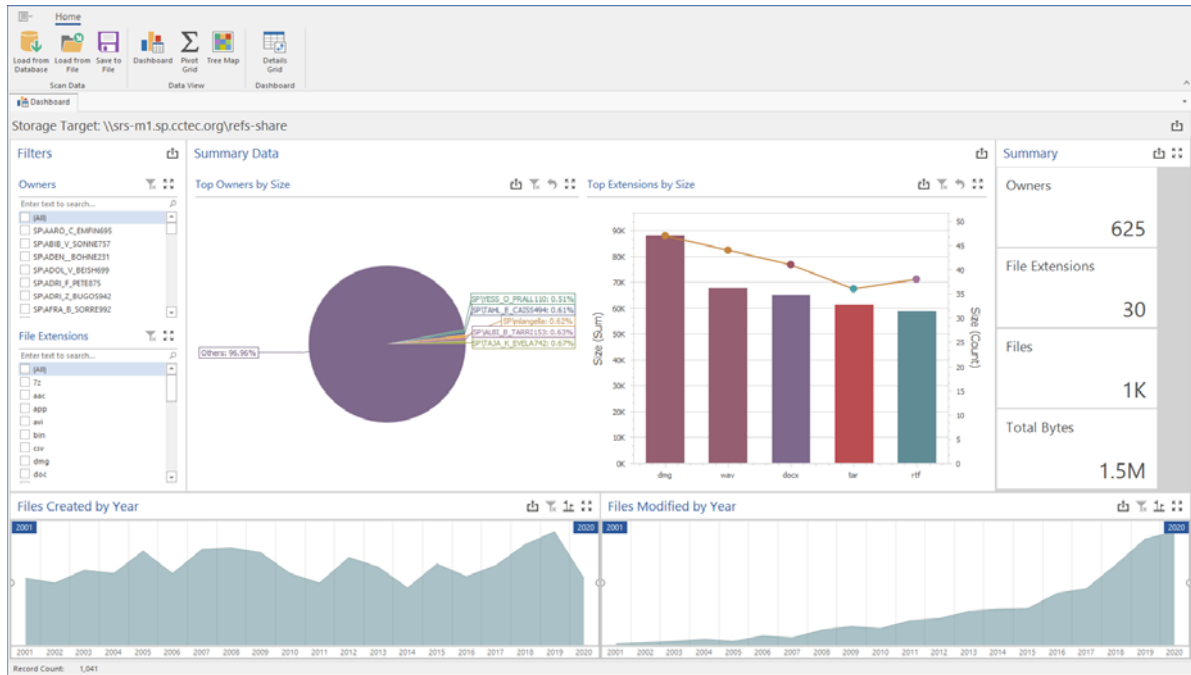
Data Analytics

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

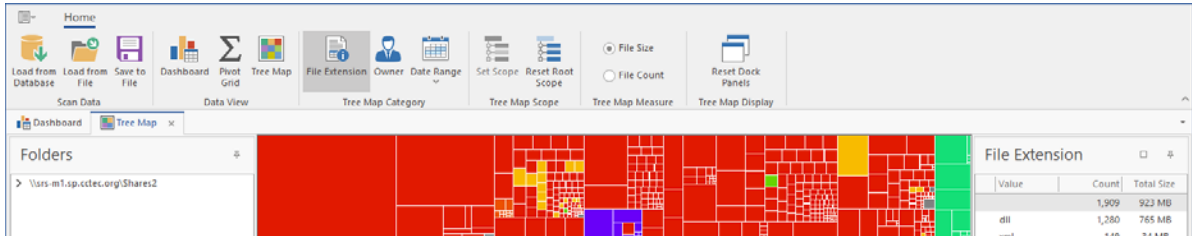
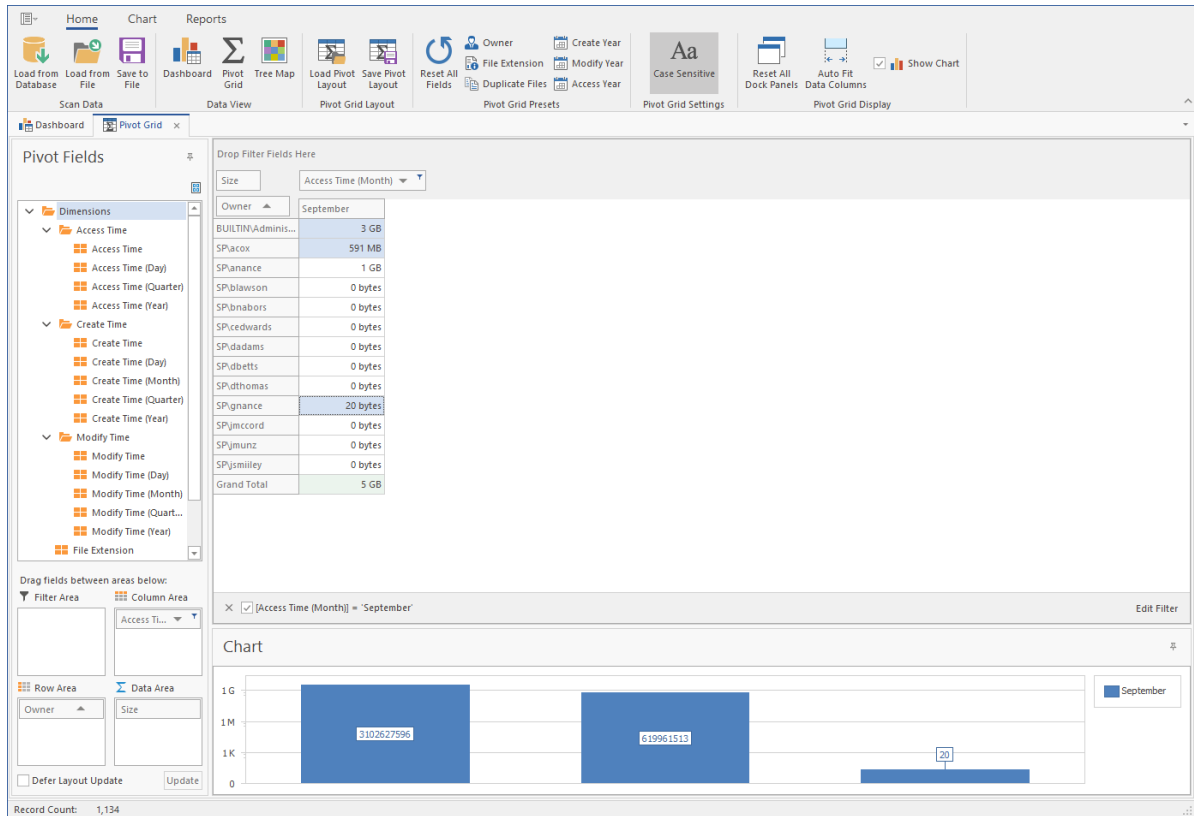


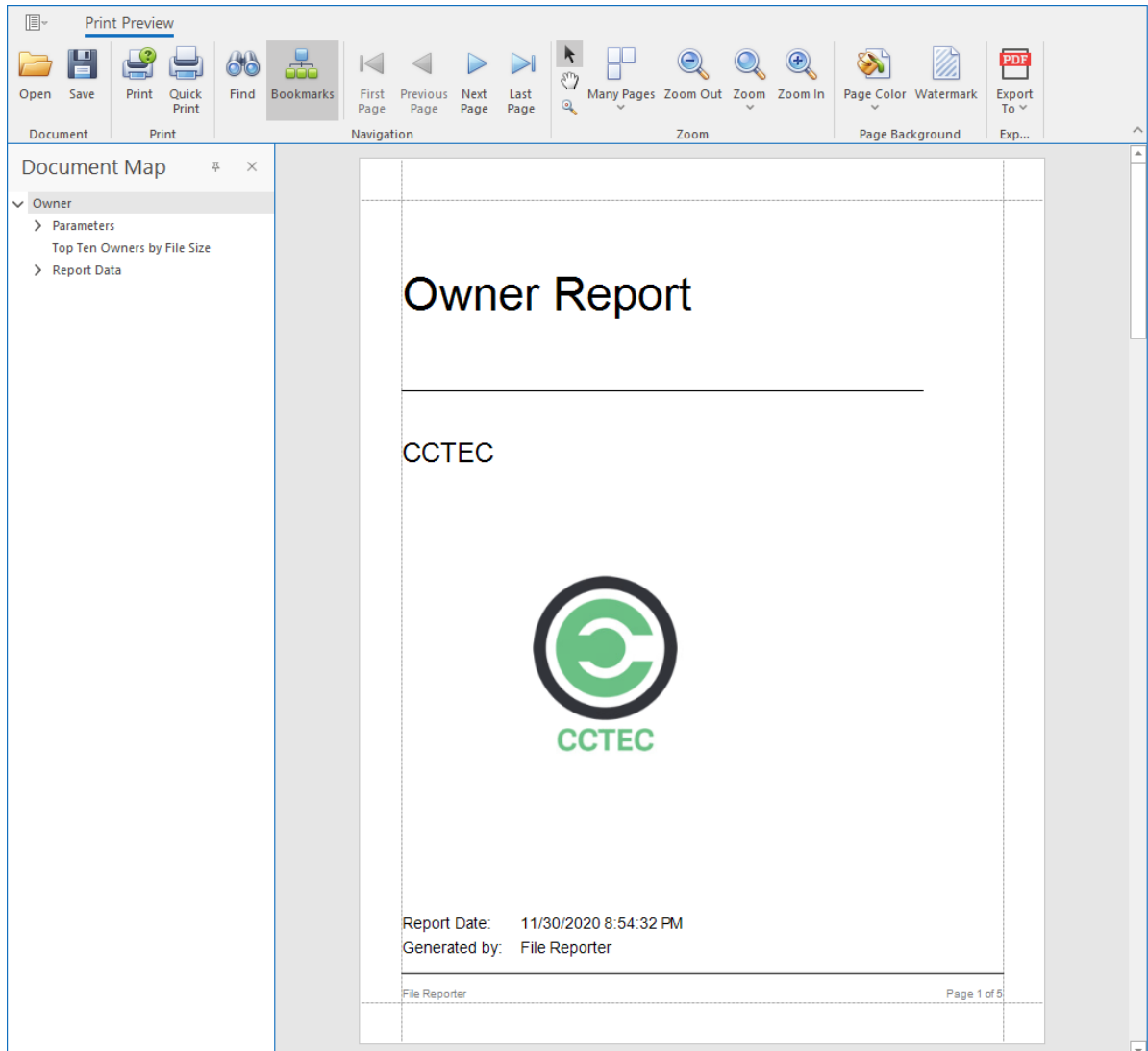
Figure 2-6 Pivot Grid



Report Viewer

The Report Viewer lets you to 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 The Administrative Interface

- ♦ Section 3.1, “Supported Browsers,” on page 23
- ♦ Section 3.2, “Launching the Administrative Interface,” on page 23
- ♦ Section 3.3, “Using the Administrative Interface,” on page 25

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 in the “[Micro Focus File Reporter 4.0 Installation Guide](#).”

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

The login screen appears.

File Reporter 4.0

User Account

Password

[Sign In](#)

- 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@ad.test.lab)

LDAP(CN=user1,OU=home,DC=ad,DC=test,DC=lab)

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

The File Reporter Home page appears:

File Reporter 4.0		Main	File Systems	File Content	Governance	Microsoft 365	Reports	Configuration	SPUAdministrator																																																		
<div style="display: flex; justify-content: space-between;"> <div style="width: 33%; border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin-top: 0;">✔ General</p> <p>Version Info</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Web Application</td><td>4.0.0.12</td></tr> <tr><td>Engine</td><td>4.0.0.24</td></tr> <tr><td>Scan Processor</td><td>4.0.0.21</td></tr> <tr><td>Operating System</td><td>Microsoft Windows Server 2019 Standard</td></tr> <tr><td>Database</td><td>Microsoft SQL Server 2017 (RTM-GDR) (KB4505224) - 14.0.2027.2</td></tr> </table> <p>License Info</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>License Type</td><td>Production</td></tr> <tr><td>Identity System</td><td>sp.cctec.org</td></tr> <tr><td>Expiration Date</td><td>11/5/2022</td></tr> <tr><td colspan="2">▶ Licensed Features</td></tr> <tr><td colspan="2">▶ Licensed Microsoft 365 Tenants</td></tr> </table> <p>Server Local Time</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Current Time</td><td>2020-11-24 16:50:20 PM</td></tr> <tr><td>Time Zone</td><td>Coordinated Universal Time (UTC +00:00)</td></tr> </table> </div> <div style="width: 33%; border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin-top: 0;">📁 Scans</p> <p>File System Scan Policies 5</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Scans In Progress</td><td style="text-align: right;">0</td></tr> <tr><td># Scans Last Day</td><td style="text-align: right;">0</td></tr> <tr><td># Scans Last Week</td><td style="text-align: right;">0</td></tr> </table> <p>File System Agents 1</p> <p>Total Agents</p> <p>File System Scans Data Path</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Total Space</td><td style="text-align: right;">79.4 GB</td></tr> <tr><td>Free Space</td><td style="text-align: right;">34.55 GB</td></tr> </table> <p>File Content</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Job Definitions</td><td style="text-align: right;">2</td></tr> <tr><td>Classifications</td><td style="text-align: right;">4</td></tr> <tr><td>Search Patterns</td><td style="text-align: right;">2</td></tr> <tr><td>Agents</td><td style="text-align: right;">2</td></tr> </table> </div> <div style="width: 33%; border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin-top: 0;">📊 Reports</p> <p>Report Definitions 9</p> <p>Report Generation</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Reports In Progress</td><td style="text-align: right;">0</td></tr> <tr><td># Stored Reports</td><td style="text-align: right;">0</td></tr> </table> <p>Stored Report Storage</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Bytes In Use</td><td style="text-align: right;">0 bytes</td></tr> <tr><td>Free Bytes Remaining</td><td style="text-align: right;">34.55 GB</td></tr> </table> </div> </div>										Web Application	4.0.0.12	Engine	4.0.0.24	Scan Processor	4.0.0.21	Operating System	Microsoft Windows Server 2019 Standard	Database	Microsoft SQL Server 2017 (RTM-GDR) (KB4505224) - 14.0.2027.2	License Type	Production	Identity System	sp.cctec.org	Expiration Date	11/5/2022	▶ Licensed Features		▶ Licensed Microsoft 365 Tenants		Current Time	2020-11-24 16:50:20 PM	Time Zone	Coordinated Universal Time (UTC +00:00)	Scans In Progress	0	# Scans Last Day	0	# Scans Last Week	0	Total Space	79.4 GB	Free Space	34.55 GB	Job Definitions	2	Classifications	4	Search Patterns	2	Agents	2	Reports In Progress	0	# Stored Reports	0	Bytes In Use	0 bytes	Free Bytes Remaining	34.55 GB
Web Application	4.0.0.12																																																										
Engine	4.0.0.24																																																										
Scan Processor	4.0.0.21																																																										
Operating System	Microsoft Windows Server 2019 Standard																																																										
Database	Microsoft SQL Server 2017 (RTM-GDR) (KB4505224) - 14.0.2027.2																																																										
License Type	Production																																																										
Identity System	sp.cctec.org																																																										
Expiration Date	11/5/2022																																																										
▶ Licensed Features																																																											
▶ Licensed Microsoft 365 Tenants																																																											
Current Time	2020-11-24 16:50:20 PM																																																										
Time Zone	Coordinated Universal Time (UTC +00:00)																																																										
Scans In Progress	0																																																										
# Scans Last Day	0																																																										
# Scans Last Week	0																																																										
Total Space	79.4 GB																																																										
Free Space	34.55 GB																																																										
Job Definitions	2																																																										
Classifications	4																																																										
Search Patterns	2																																																										
Agents	2																																																										
Reports In Progress	0																																																										
# Stored Reports	0																																																										
Bytes In Use	0 bytes																																																										
Free Bytes Remaining	34.55 GB																																																										
Copyright 2020 Condrey Corporation																																																											

3.3 Using the Administrative Interface

- ◆ Section 3.3.1, “Viewing Notifications,” on page 25
- ◆ Section 3.3.2, “Configuring the Web Interface,” on page 26
- ◆ Section 3.3.3, “Viewing System Information,” on page 27

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 Micro Focus 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 Viewing 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.

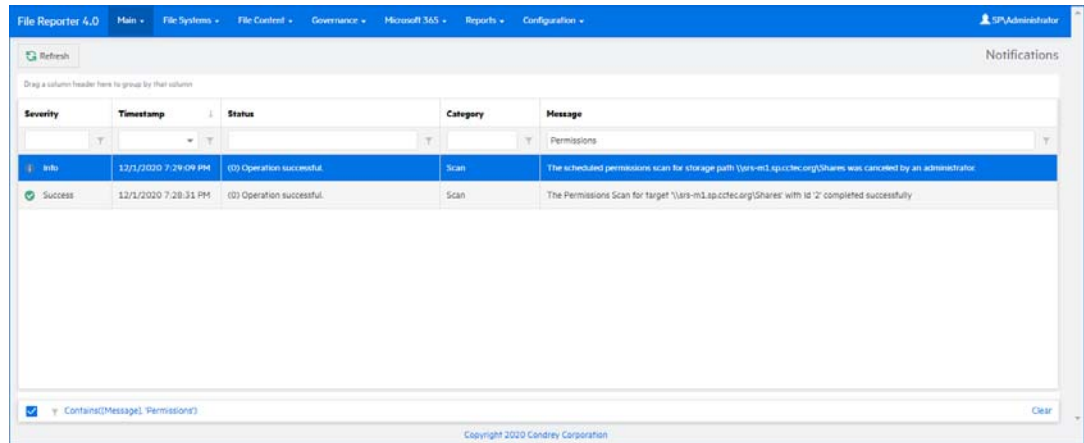
- 1 From the **Main** menu, select **Notifications**.

Severity	Timestamp	Status	Category	Message
Error	12/1/2020 5:35:21 PM	(-1) An unspecified error has occurred.	Scan	The scheduled data scan for storage path \\ars-m1.spictec.org\test-125 (Scan ID 320) was unable to complete. The following error occurred: (-1) An unspecified error has occurred. There are 3 retry attempts remaining. The next attempt will be made in 3579 seconds.
Success	11/30/2020 8:54:33 PM	(0) Operation successful.	Report	The report owner report has been successfully generated and is ready to be viewed.
Success	11/30/2020 8:48:30 PM	(0) Operation successful.	Report	The report owner report has been successfully generated and is ready to be viewed.
Success	11/30/2020 5:00:37 PM	(0) Operation successful.	Report	The report File Extensions by Category Summary has been successfully generated and is ready to be viewed.
Error	11/24/2020 8:51:01 PM	(-1) An unspecified error has occurred.	Scan	The File System Data Scan for target \\ars-m1.spictec.org\test-119 with id 267 failed with the following error: Invalid column name 'ms365_hash'. Updating fullpath_hash on 'import_scan_data_267' for scan '267'

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**.

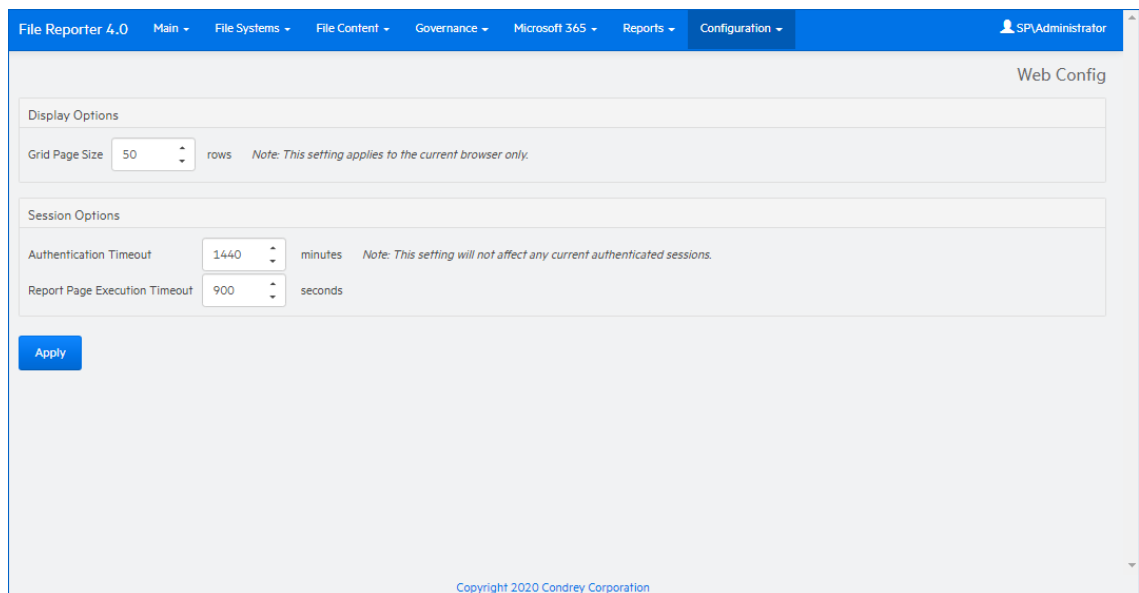
- 4c In the field to the left of the “pin” icon, enter the distinguishing word or letter for the filter. For example, Permissions. The page is updated according to the filtering parameters.



3.3.2 Configuring the Web Interface

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 Viewing 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.

The screenshot displays the 'System Info' page in the File Reporter 4.0 interface. The page is divided into two main sections: 'Database Statistics' and 'Referenced Web Application Assemblies'.

Database Statistics

Database Version String	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 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
Permission 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
Condreyl/Product	2.0.7.0	None
Condreyl/Srs.Core	4.0.8.0	None
Condreyl/Srs.Core.Database	4.0.0.2	None
Condreyl/Srs.Core.Ext	4.0.0.6	None
Condreyl/Srs.Product	4.0.12.0	None

Copyright 2020 Condreyl Corporation

4 Performing Setup Procedures

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

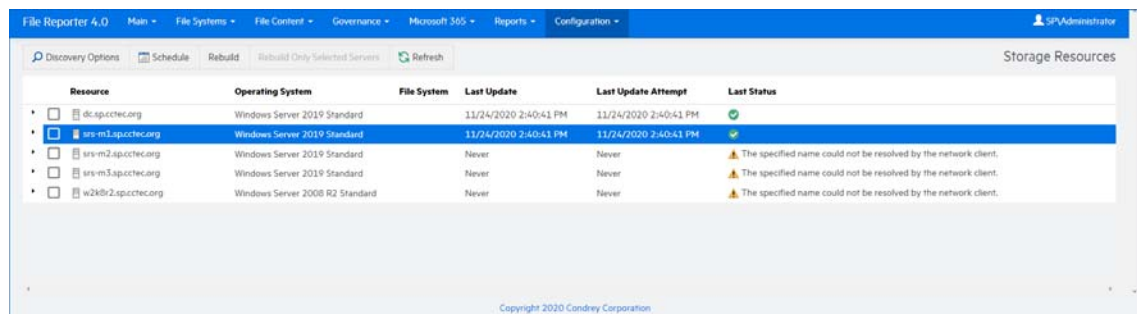
- ◆ Section 4.1, “Viewing Storage Resources,” on page 29
- ◆ Section 4.2, “Assigning Proxy Targets,” on page 31
- ◆ Section 4.3, “Configuring Notifications,” on page 32
- ◆ Section 4.4, “Integrating with File Dynamics,” on page 33

4.1 Viewing 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**.



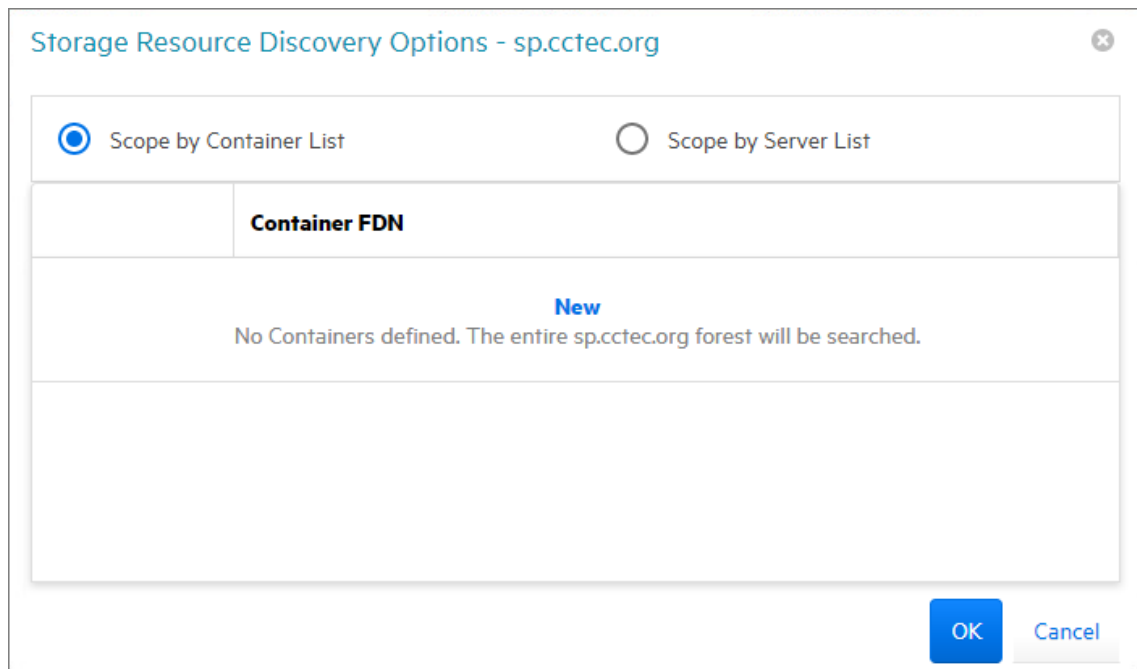
The screenshot shows the File Reporter 4.0 interface with the Configuration > Storage Resources page open. The table below lists the storage resources discovered in the Active Directory forest.

Resource	Operating System	File System	Last Update	Last Update Attempt	Last Status
<input type="checkbox"/> dc.spctec.org	Windows Server 2019 Standard		11/24/2020 2:40:41 PM	11/24/2020 2:40:41 PM	
<input checked="" type="checkbox"/> srv-m1.spctec.org	Windows Server 2019 Standard		11/24/2020 2:40:41 PM	11/24/2020 2:40:41 PM	
<input type="checkbox"/> srv-m2.spctec.org	Windows Server 2019 Standard		Never	Never	The specified name could not be resolved by the network client.
<input type="checkbox"/> srv-m3.spctec.org	Windows Server 2019 Standard		Never	Never	The specified name could not be resolved by the network client.
<input type="checkbox"/> w2k8r2.spctec.org	Windows Server 2008 R2 Standard		Never	Never	The specified name could not be resolved by the network client.

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 need added.



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**.

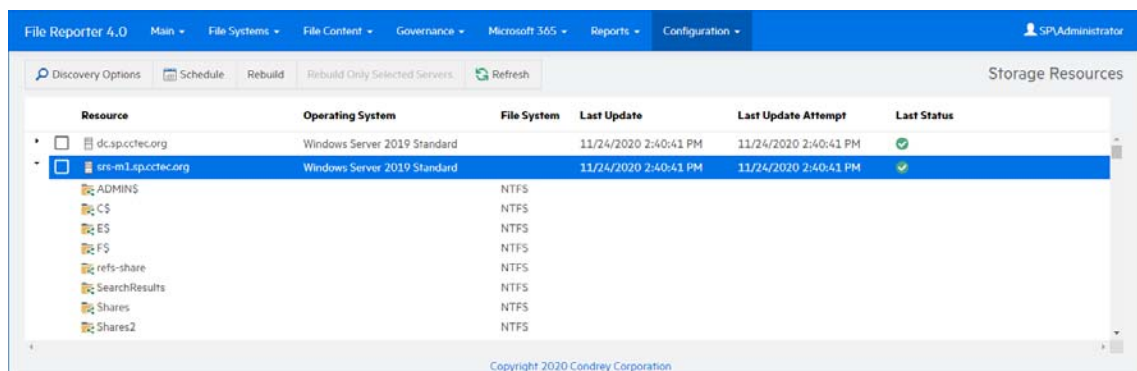
Schedule: By default, File Reporter rebuilds Active Directory's storage resources at 12:00 AM each day. Larger sites might want change this setting to weekly or on a specific day of the month. To do so, click this option and modify the settings in the dialog box.

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.

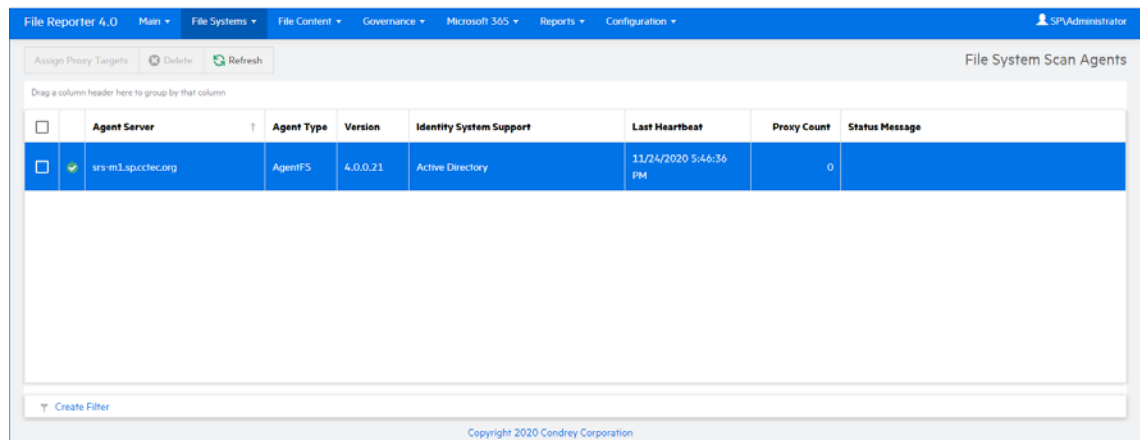


4.2 Assigning Proxy Targets

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**.

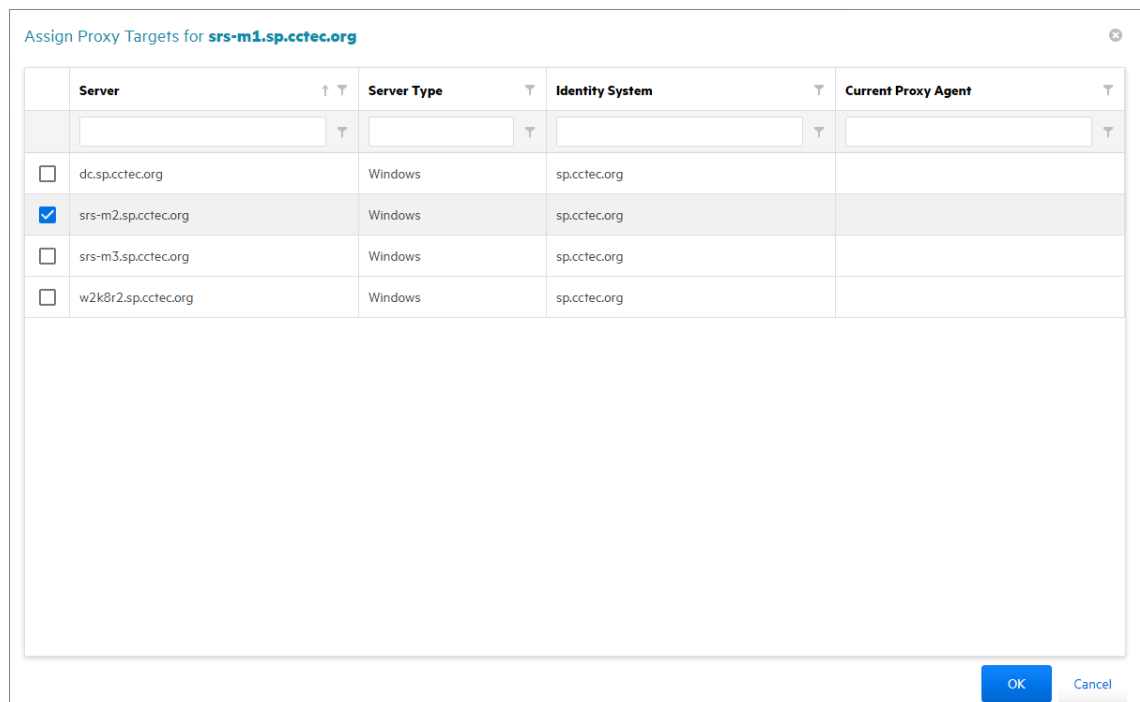
All of the Agents are listed.



The screenshot shows the 'File System Scan Agents' table in the File Reporter 4.0 interface. The table has the following columns: Agent Server, Agent Type, Version, Identity System Support, Last Heartbeat, Proxy Count, and Status Message. One agent is listed: srs-m1.spccotec.org, AgentFS, 4.0.0.21, Active Directory, 11/24/2020 5:46:36 PM, 0, and Status Message.

<input type="checkbox"/>	Agent Server	Agent Type	Version	Identity System Support	Last Heartbeat	Proxy Count	Status Message
<input checked="" type="checkbox"/>	srs-m1.spccotec.org	AgentFS	4.0.0.21	Active Directory	11/24/2020 5:46:36 PM	0	

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



The screenshot shows the 'Assign Proxy Targets for srs-m1.spccotec.org' dialog box. It contains a table with the following columns: Server, Server Type, Identity System, and Current Proxy Agent. The table lists four servers: dc.spccotec.org, srs-m2.spccotec.org, srs-m3.spccotec.org, and w2k8r2.spccotec.org. The srs-m2.spccotec.org row is selected with a blue checkmark.

<input type="checkbox"/>	Server	Server Type	Identity System	Current Proxy Agent
<input type="checkbox"/>	dc.spccotec.org	Windows	spccotec.org	
<input checked="" type="checkbox"/>	srs-m2.spccotec.org	Windows	spccotec.org	
<input type="checkbox"/>	srs-m3.spccotec.org	Windows	spccotec.org	
<input type="checkbox"/>	w2k8r2.spccotec.org	Windows	spccotec.org	

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**.

The screenshot shows the 'Notification Configuration' interface. The top navigation bar includes 'File Reporter 4.0', 'Main', 'File Systems', 'File Content', 'Governance', 'Microsoft 365', 'Reports', and 'Configuration'. The user is logged in as 'SPAdministrator'. The main content area is titled 'Notification Configuration' and contains two sections: 'Notification Settings' and 'Mail Settings'. In the 'Notification Settings' section, there is a dropdown menu for 'Only notify me about events of at least this severity level' set to 'Success', a spinner for 'Days to display notifications in the dashboard' set to '30', and an unchecked checkbox for 'Enable Mail Notifications'. The 'Mail Settings' section includes fields for 'Mail Server' (IP Address or Hostname), 'Port' (25), 'Connection Type' (TLS), and 'From Email Address' (noreply@cctec.org). There is also an unchecked checkbox for 'Use Authentication', fields for 'Username' (mailuser) and 'Password', and a spinner for 'Minutes to buffer multiple notifications for a single email' set to '1'. A 'Save Changes' button is located at the bottom left of the form area. The footer of the page reads 'Copyright 2020 Condrey Corporation'.

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.

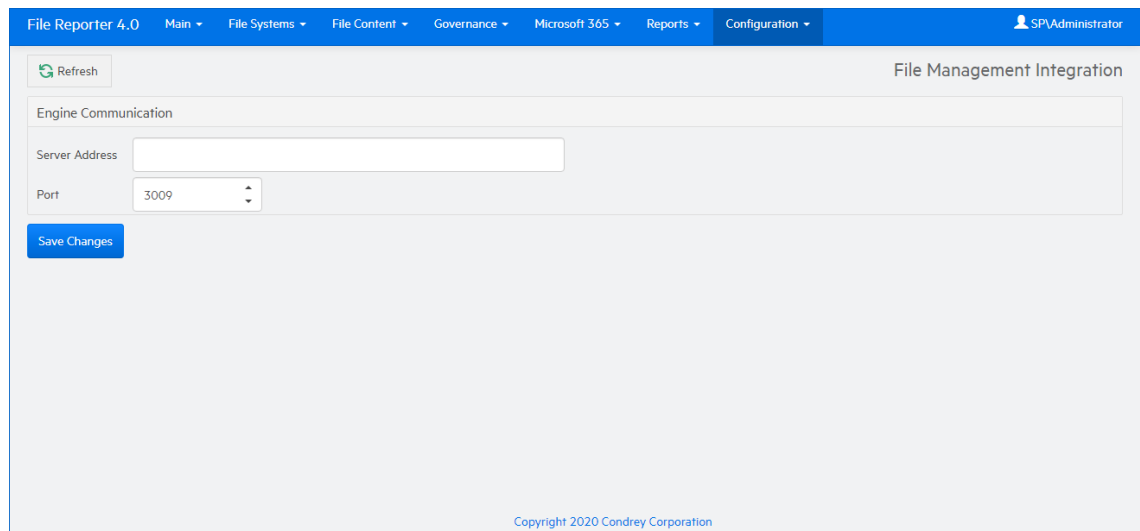
- 2 Specify your notification parameters and click **Save Changes**.

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 4.0 integrates with File Dynamics 6.0 and above.

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



The screenshot shows the File Reporter 4.0 Configuration page for File Management Integration. The page has a blue header with navigation tabs: File Reporter 4.0, Main, File Systems, File Content, Governance, Microsoft 365, Reports, and Configuration. The user is logged in as SP Administrator. The main content area is titled "File Management Integration" and contains a "Refresh" button and a "Save Changes" button. Under the "Engine Communication" section, there is a "Server Address" text input field and a "Port" dropdown menu currently set to "3009".

- 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 Scheduling and Performing File System Scans

- ◆ Section 5.1, “Scans,” on page 35
- ◆ Section 5.2, “Adding a Scan Target,” on page 36
- ◆ Section 5.3, “Removing a Scan Target,” on page 38
- ◆ Section 5.4, “Creating Scan Policies,” on page 38
- ◆ Section 5.5, “Establishing a Baseline Scan,” on page 42
- ◆ Section 5.6, “Clearing a Baseline Scan,” on page 43
- ◆ Section 5.7, “Editing a Scan Policy,” on page 43
- ◆ Section 5.8, “Deleting a Scan Policy,” on page 43
- ◆ Section 5.9, “Scheduling Scans,” on page 43
- ◆ Section 5.10, “Editing a Scheduled Scan,” on page 45
- ◆ Section 5.11, “Clearing a Schedule on a Scheduled Scan,” on page 45
- ◆ Section 5.12, “Conducting an Immediate Scan,” on page 45
- ◆ Section 5.13, “Viewing Scans in Progress,” on page 45
- ◆ Section 5.14, “Retrying Failed Scans,” on page 46
- ◆ Section 5.15, “Viewing Scan Data,” on page 47
- ◆ Section 5.16, “Viewing Scan History,” on page 47
- ◆ Section 5.17, “Troubleshooting a Failed Scan,” on page 48
- ◆ Section 5.18, “Scanning Your Microsoft 365 Tenant,” on page 48

5.1 Scans

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, “Establishing a Baseline Scan,” on page 42](#).

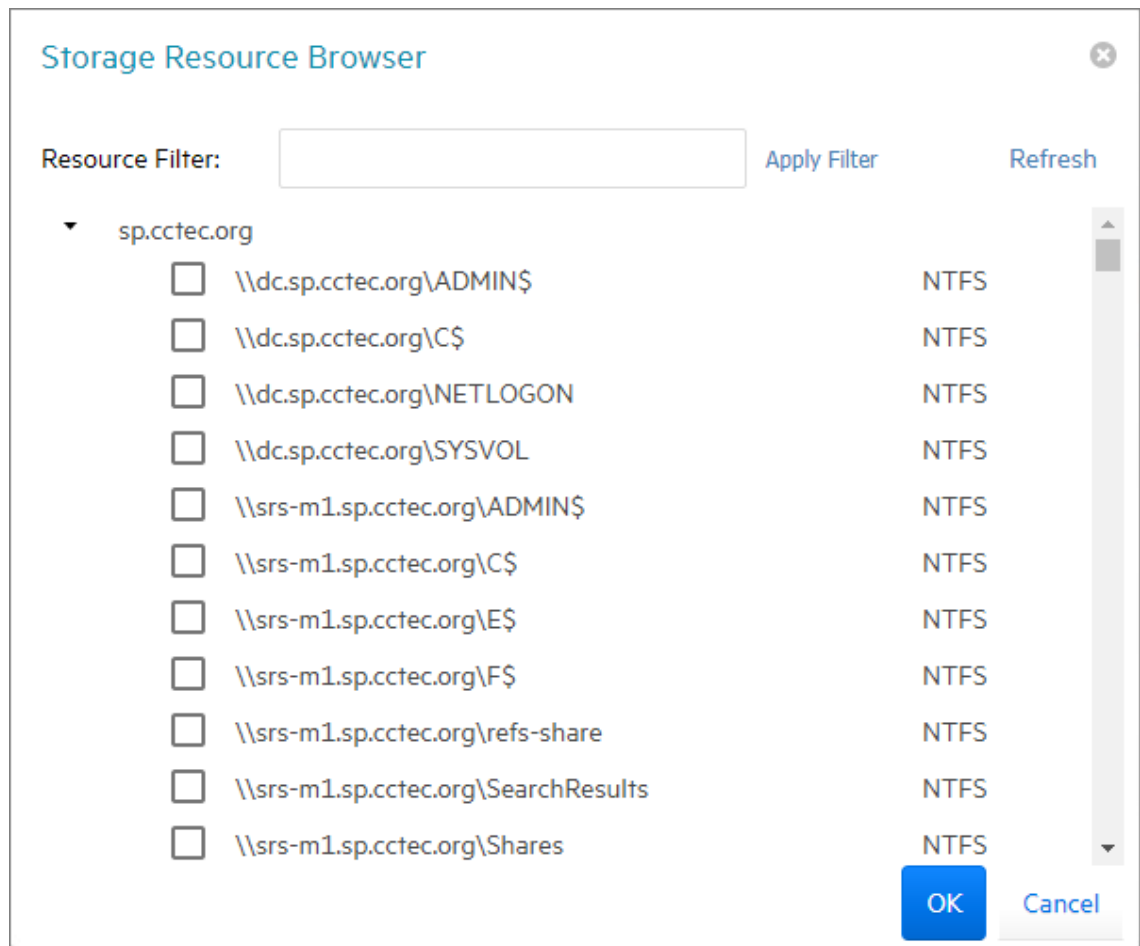
Automatic Retention

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 5.4, “Creating Scan Policies,” on page 38](#).

5.2 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.

File Reporter 4.0 Main File Systems File Content Governance Microsoft 365 Reports Configuration SPSAdministrator

Add Delete Refresh Rebuild Storage Resources File System Scan Targets

Drag a column header here to group by that column

<input type="checkbox"/>	Identity System	Target Path	File System	Id
<input checked="" type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\refs-share	NTFS	47
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\Shares	NTFS	1
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\Shares2	NTFS	2
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-1	NTFS	3
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-10	NTFS	4
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-100	NTFS	5
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-101	NTFS	6
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-102	NTFS	7
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-103	NTFS	8
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-104	NTFS	9
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-105	NTFS	10
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-106	NTFS	11
<input type="checkbox"/>	sp.cctec.org	\\srs-m1.sp.cctec.org\test-107	NTFS	12

Page 1 of 1 (47 items) < 1 >

Create Filter

Copyright 2020 Condrey Corporation

5.3 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**.

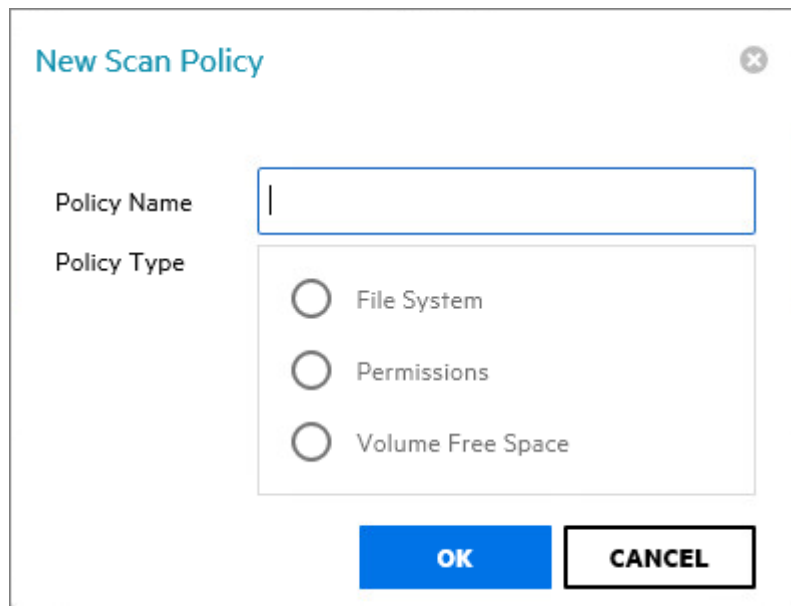
5.4 Creating Scan Policies

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**.

The image shows a dialog box titled "New Scan Policy" with a close button (X) in the top right corner. It contains two main sections: "Policy Name" with an empty text input field, and "Policy Type" with three radio button options: "File System", "Permissions", and "Volume Free Space". At the bottom, there are two buttons: a blue "OK" button and a white "CANCEL" button with a black border.

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**.

Scan Policy Editor

Name: FS Scan Policy

Description: File System scan for current share

Retry Count: 3

Retry Interval: 60 Minutes

Directory Quotas: Scan Directory Quotas

Previous Scans: Save Previous Scan

Content Hash: Generate file content hashes

All Files

Files updated since last scan

Add Remove

Target Path

OK Cancel

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 6.8, “Historic Comparison Reports,” on page 81.](#)

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, “Establishing a Baseline Scan,” on page 42](#).

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 hash comparisons can be much more accurate.

For more information on generating a duplicate file report through content-based hashes, see [Section 6.11.1, “Generating a Content Hashed Duplicate File Report,” on page 90](#).

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

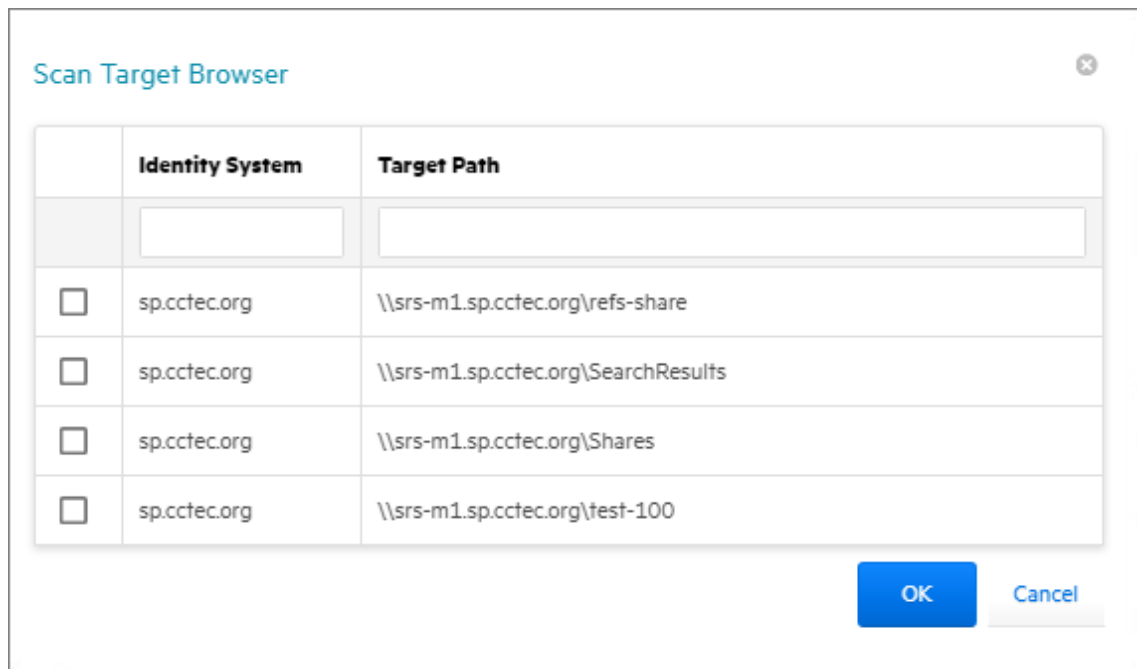
Files updated since last scan: Selecting this check box creates an individual hash for each file that does not already have a previously created hash or for files updated since the hash was created.

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.

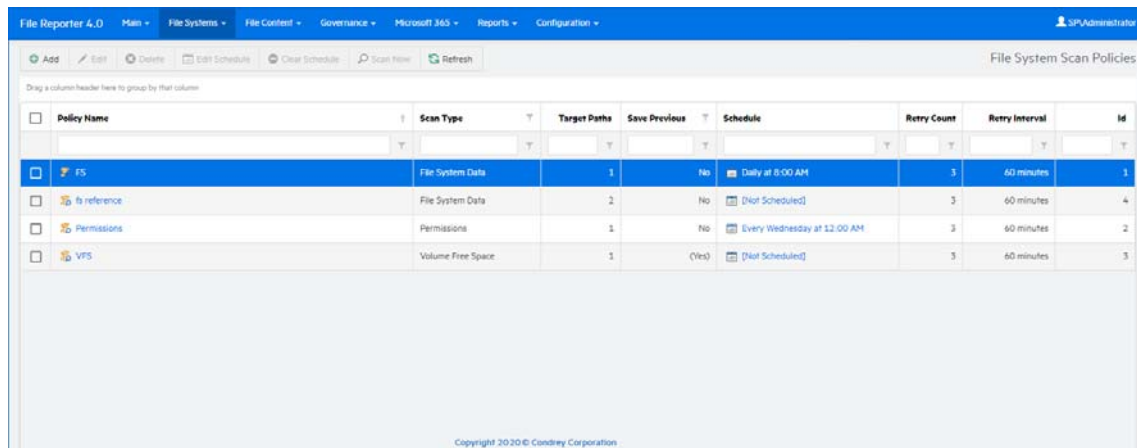
IMPORTANT: After a target has been added to a scan policy, the same target cannot be added to another scan policy of the same scan policy type.

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 5.9, “Scheduling Scans,”](#) on page 43.

5.5 Establishing a Baseline Scan

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.

- 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**.

5.6 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**.

5.7 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**.

5.8 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**.

5.9 Scheduling Scans

- 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**.

Schedule for Munich Users FS Scan Policy ✕

SCHEDULE START

Engine Local Time:*

Engine Local Start Date:*

SCHEDULE RECURRENCE

Once

Daily

Weekly

Monthly

Day of every month

The of every month

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**.

5.10 Editing a Scheduled Scan

- 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**.

5.11 Clearing a Schedule on a Scheduled Scan

- 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**.

5.12 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**.

5.13 Viewing 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**.

Scan ID	Scan Target	Scan Policy	Scan Type	Agent	Start Time	Status	Try Count	Next Retry Time	Last Error
<input type="checkbox"/>	288 \\sars-m1.lap.cctec.org\test-00	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	287 \\sars-m1.lap.cctec.org\test-137	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	286 \\sars-m1.lap.cctec.org\test-136	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	285 \\sars-m1.lap.cctec.org\test-135	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	284 \\sars-m1.lap.cctec.org\test-134	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	283 \\sars-m1.lap.cctec.org\test-133	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input checked="" type="checkbox"/>	282 \\sars-m1.lap.cctec.org\test-132	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	281 \\sars-m1.lap.cctec.org\test-131	test fs	File System Data	SRS-M1	11/24/2020 6:49:22 PM	Scan in Progress	0		(0) Operation successful.

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

5.14 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**.

5.15 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**.

File Reporter 4.0 Main File Systems File Content Governance Microsoft 365 Reports Configuration SP Administrator

File System Scan Data

Drag a column header here to group by that column

Scan Id	Scan Target	Scan Type	State	Baseline	Triggered Scan Time	Policy	Agent	Status
242	\\srs-m1.sp.cctec.org\Shares2	File System Data	Current	False	9/21/2020 6:41:23 PM	shares2	SRS-M1	(0) Operation successful.
241	\\srs-m1.sp.cctec.org\Shares2	File System Data	Previous	False	9/21/2020 6:33:21 PM	shares2	SRS-M1	(0) Operation successful.
239	\\srs-m1.sp.cctec.org\test-99	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
238	\\srs-m1.sp.cctec.org\test-137	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
237	\\srs-m1.sp.cctec.org\test-136	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
236	\\srs-m1.sp.cctec.org\test-135	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
235	\\srs-m1.sp.cctec.org\test-134	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
234	\\srs-m1.sp.cctec.org\test-133	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
233	\\srs-m1.sp.cctec.org\test-132	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
232	\\srs-m1.sp.cctec.org\test-131	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
231	\\srs-m1.sp.cctec.org\test-130	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
230	\\srs-m1.sp.cctec.org\test-13	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.
229	\\srs-m1.sp.cctec.org\test-129	File System Data	Current	False	9/21/2020 6:15:24 PM	test fs	SRS-M1	(0) Operation successful.

Page 1 of 2 (93 items) < 1 2 >

(State) is any of (Current, Previous, Retained) Clear

Copyright 2020 Condrey Corporation

5.16 Viewing 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**.

Scan Id	Start Time	Scan Target	Scan Policy	Scan Type	Agent	Scan Duration	Database Duration	File Count	Folder Count	Status
246	11/24/2020 6:49:22 PM	\\vars-m1.lap.cctec.org\test-10	test fs	File System Data	SRS-M1	00:00:00:00.000	00:00:00:00.000	53	2	{-1} - Invalid column name 'ms365_hash'. Updating fullpath_hash on 'importscan_data_246' for scan '246'
245	11/24/2020 6:49:22 PM	\\vars-m1.lap.cctec.org\test-1	test fs	File System Data	SRS-M1	00:00:00:00.000	00:00:00:00.000	5	2	{-1} - Invalid column name 'ms365_hash'. Updating fullpath_hash on 'importscan_data_245' for scan '245'
244	11/24/2020 6:49:22 PM	\\vars-m1.lap.cctec.org\Shares	Share fs	File System Data	SRS-M1	00:00:00:01.000	00:00:00:00.000	30	1,104	{-1} - Invalid column name 'ms365_hash'. Updating fullpath_hash on 'importscan_data_244' for scan '244'
243	11/24/2020 6:49:22 PM	\\vars-m1.lap.cctec.org\ref-share	ref-share fs	File System Data	SRS-M1	00:00:00:01.000	00:00:00:00.000	1,000	41	{-1} - Invalid column name 'ms365_hash'. Updating fullpath_hash on 'importscan_data_243' for scan '243'
242	9/21/2020 6:41:23 PM	\\vars-m1.lap.cctec.org\Shares2	shares2	File System Data	SRS-M1	00:00:00:01.000	00:00:00:01.297	5,897	1,224	(0) - Success
241	9/21/2020 6:33:21 PM	\\vars-m1.lap.cctec.org\Shares2	shares2	File System Data	SRS-M1	00:00:00:01.000	00:00:00:01.423	5,897	1,224	(0) - Success
240	9/21/2020 6:18:28 PM	\\vars-m1.lap.cctec.org\Shares2	shares2	File System Data	SRS-M1	00:00:00:02.000	00:00:00:01.359	5,894	1,224	(0) - Success
239	9/21/2020 6:15:24 PM	\\vars-m1.lap.cctec.org\test-99	test fs	File System Data	SRS-M1	00:00:01:05.000	00:00:00:00.207	49	2	(0) - Success

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.

5.17 Troubleshooting a Failed Scan

- 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 or the local 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.

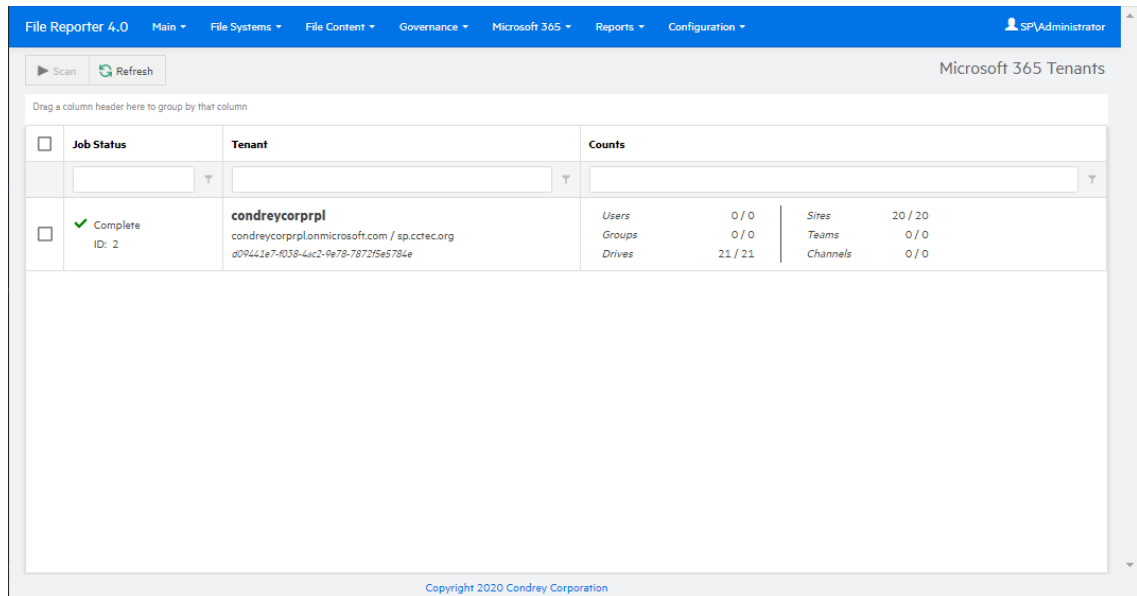
For more information on the Windows Firewall, see [Section B.2, "Firewall Requirements,"](#) on page 161.

5.18 Scanning Your Microsoft 365 Tenant

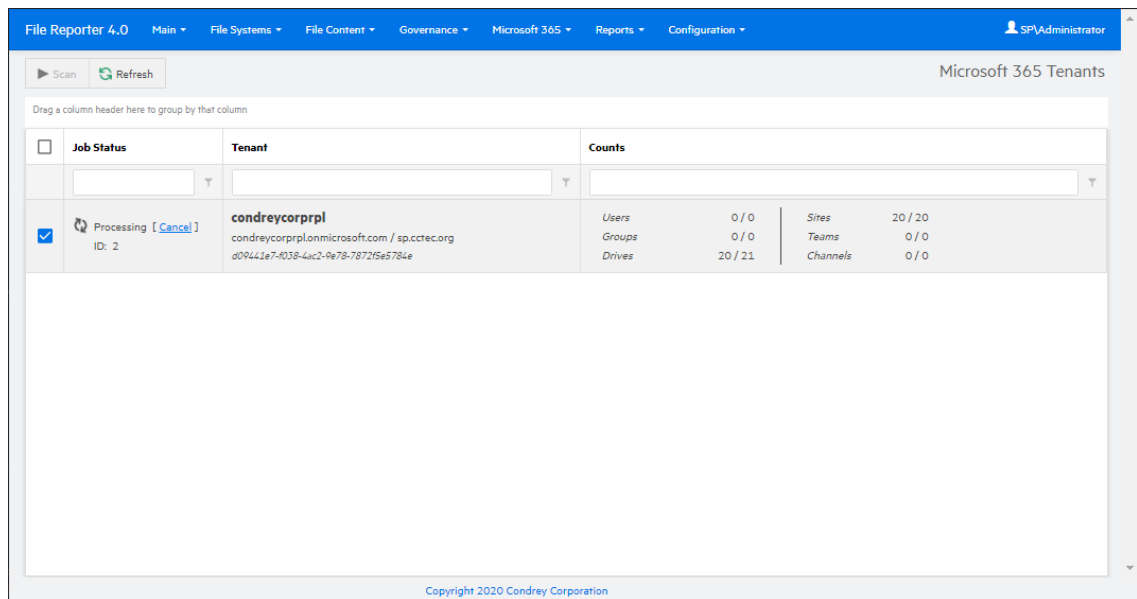
Scanning your Microsoft 365 tenant identifies all users and groups, the associated drives, sites and associated libraries, teams and their associated libraries, and channels and their associated libraries. A tenant scan includes details pertaining to the file system structure, individual files, and file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

5.18.1 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**.

File Reporter 4.0 Main File Systems File Content Governance Microsoft 365 Reports Configuration SP Administrator

Microsoft 365 Drive Scans

Drag a column header here to group by that column

Scan Status	Drive Type	Counts	URL	Scan Id
		Permissions 10		
<input type="checkbox"/> Complete	Document Library	Files 0 Folders 2 Permissions 6	https://condreycorprpl.sharepoint.com/sites/created-to-be-deleted/Shared%20Documents	13
<input type="checkbox"/> Complete	Document Library	Files 0 Folders 1 Permissions 0	https://condreycorprpl.sharepoint.com/sites/contentTypeHub/Shared%20Documents	14
<input type="checkbox"/> Complete	Business	Files 3 Folders 3 Permissions 6	https://condreycorprpl-my.sharepoint.com/personal/rflagger_condreycorprpl_onmicrosoft_com/Documents	15
<input checked="" type="checkbox"/> Processing [Cancel]	Document Library	Files 438 Folders 21 Permissions 1,835	https://condreycorprpl.sharepoint.com/sites/condreycorprpl/Shared%20Documents	16
<input type="checkbox"/> Complete	Document Library	Files 0 Folders 1 Permissions 1	https://condreycorprpl.sharepoint.com/sites/TestTeam1/Shared%20Documents	17
<input type="checkbox"/> Complete	Business	Files 22 Folders 4 Permissions 37	https://condreycorprpl-my.sharepoint.com/personal/gnance_sp_cctec_org/Documents	18
<input type="checkbox"/> Complete	Document Library	Files 3 Folders 6 Permissions 34	https://condreycorprpl.sharepoint.com/sites/Finance_Team/Shared%20Documents	19
<input type="checkbox"/> Complete	Document Library	Files 1 Folders 1 Permissions 6	https://condreycorprpl.sharepoint.com/sites/condreycorprpl/musings/Shared%20Documents	20
		Files 1		

Copyright 2020 Condrey Corporation

Once the Job Status column indicates that the scan is complete, you can then generate a Microsoft 365 report. For procedures for doing so, see [Section 6.11.2, “Generating Microsoft 365 Reports,”](#) on page 97.

5.18.2 Scan Selected Drives

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**.

6 Generating File System Reports

- [Section 6.1, “Overview,” on page 51](#)
- [Section 6.2, “Changing Your Cover Sheet Branding,” on page 52](#)
- [Section 6.3, “Changing the Report Data Font,” on page 54](#)
- [Section 6.4, “Built-in Report Types,” on page 55](#)
- [Section 6.5, “Directory Data Reports,” on page 56](#)
- [Section 6.6, “Permissions Reports,” on page 66](#)
- [Section 6.7, “File Data Reports,” on page 70](#)
- [Section 6.8, “Historic Comparison Reports,” on page 81](#)
- [Section 6.9, “Trending Report,” on page 85](#)
- [Section 6.10, “Unformatted Reports,” on page 86](#)
- [Section 6.11, “Custom Query Reports,” on page 87](#)
- [Section 6.12, “Micro Focus File Dynamics Policy Reports,” on page 100](#)
- [Section 6.13, “Scheduling Reports,” on page 101](#)
- [Section 6.14, “Editing a Scheduled Report,” on page 103](#)
- [Section 6.15, “Clearing a Schedule on a Scheduled Report,” on page 103](#)
- [Section 6.16, “Copying a Report Definition,” on page 103](#)
- [Section 6.17, “Viewing Reports in Progress,” on page 104](#)
- [Section 6.18, “Troubleshooting Reports,” on page 105](#)

6.1 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 [Appendix A, “Filtering for Built-in Reports,” on page 155](#).

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.

6.2 Changing Your Cover Sheet Branding


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**.

Report Branding ✕

Company Name:

Company Logo:

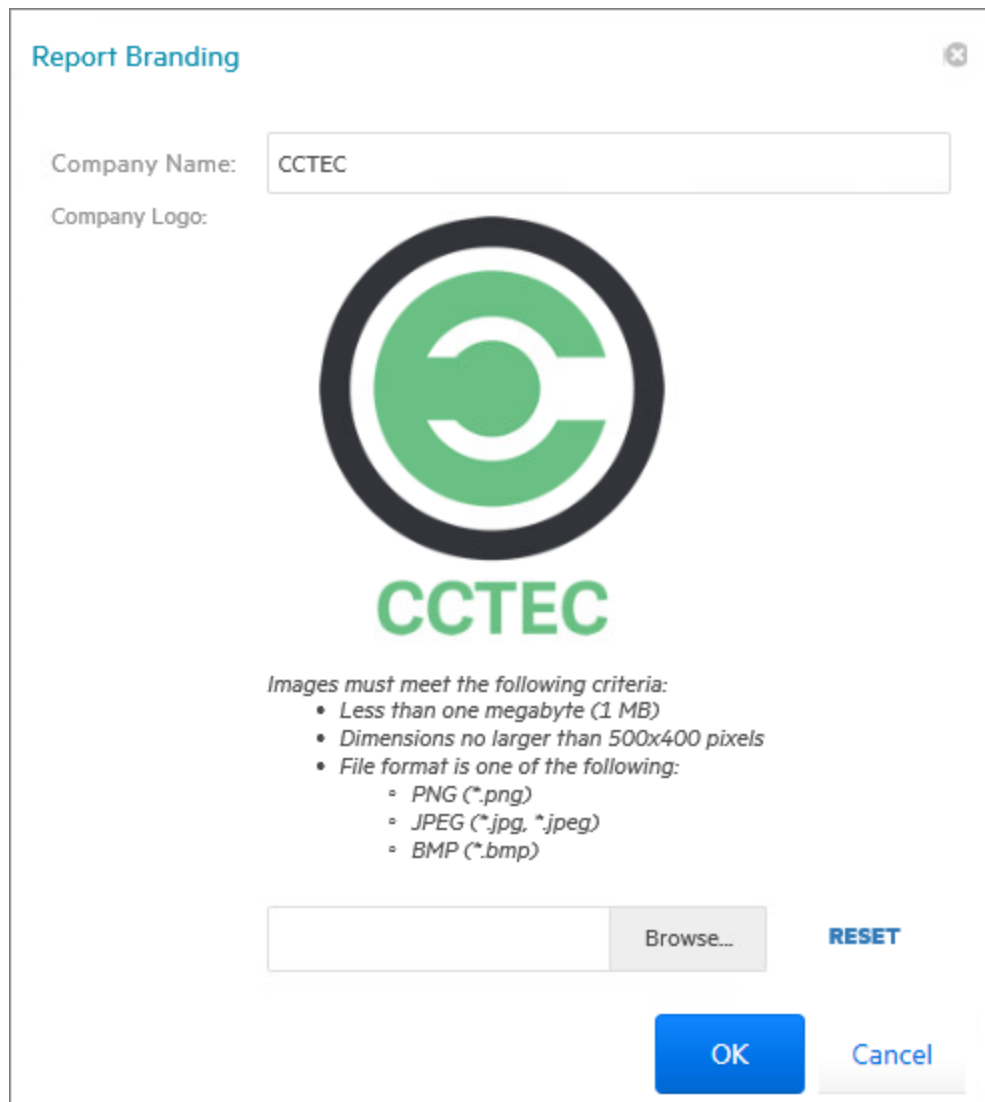


Images must meet the following criteria:

- Less than one megabyte (1 MB)
- Dimensions no larger than 500x400 pixels
- File format is one of the following:
 - PNG (*.png)
 - JPEG (*.jpg, *.jpeg)
 - BMP (*.bmp)

RESET

- 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**.

6.3 Changing the 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**.

6.4 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.

For more information about the procedures for generating built-in reports according to classification, see the following sections:

- ◆ [Section 6.5, “Directory Data Reports,” on page 56](#)
- ◆ [Section 6.6, “Permissions Reports,” on page 66](#)
- ◆ [Section 6.7, “File Data Reports,” on page 70](#)
- ◆ [Section 6.9, “Trending Report,” on page 85](#)
- ◆ [Section 6.10, “Unformatted Reports,” on page 86](#)

6.5 Directory Data 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.

- ◆ [Section 6.5.1, “Generating a Summary Report,” on page 56](#)
- ◆ [Section 6.5.2, “Generating a Directory Quota Report,” on page 63](#)
- ◆ [Section 6.5.3, “Generating a Storage Cost Report,” on page 64](#)
- ◆ [Section 6.5.4, “Generating a Comparison Report,” on page 65](#)

6.5.1 Generating a 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**.

Add Report Definition

Name:*

Unformatted: Create report as Unformatted (for use with Text, Csv, or Xls exports)

Directory Data

- Summary
- Directory Quota
- Storage Cost
- Comparison

File Data

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

Permissions

- Assigned NTFS Permissions
- Permissions by Path
- Permissions by Identity

Historic Comparison

- File System Comparison
- NTFS Permissions Comparison

Trending

- Volume Free Space

Custom Query

- Custom Query Report

OK **Cancel**

- 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**.

The screenshot shows a dialog box titled "Report Definition Editor - Atlanta User Share Summary Report". It contains the following fields and controls:

- Name:** Atlanta User Share Summary Report
- Type:** Summary Report
- Description:** Report Definition created on 12/2/2020 8:07:05 PM by SP\Administrator
- Report Path Depth:** 0
- Initial Chart Path Depth:** 0
- Info:** A Report Path Depth greater than 3 or 4 may result in significant report size and processing time.
- Tabs:** TARGET PATHS (selected), FILE MANAGEMENT POLICIES
- Buttons:** Add, Remove
- Table:** A table with one column labeled "Target Path" and an empty body.
- Bottom Buttons:** OK, Cancel

- 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.

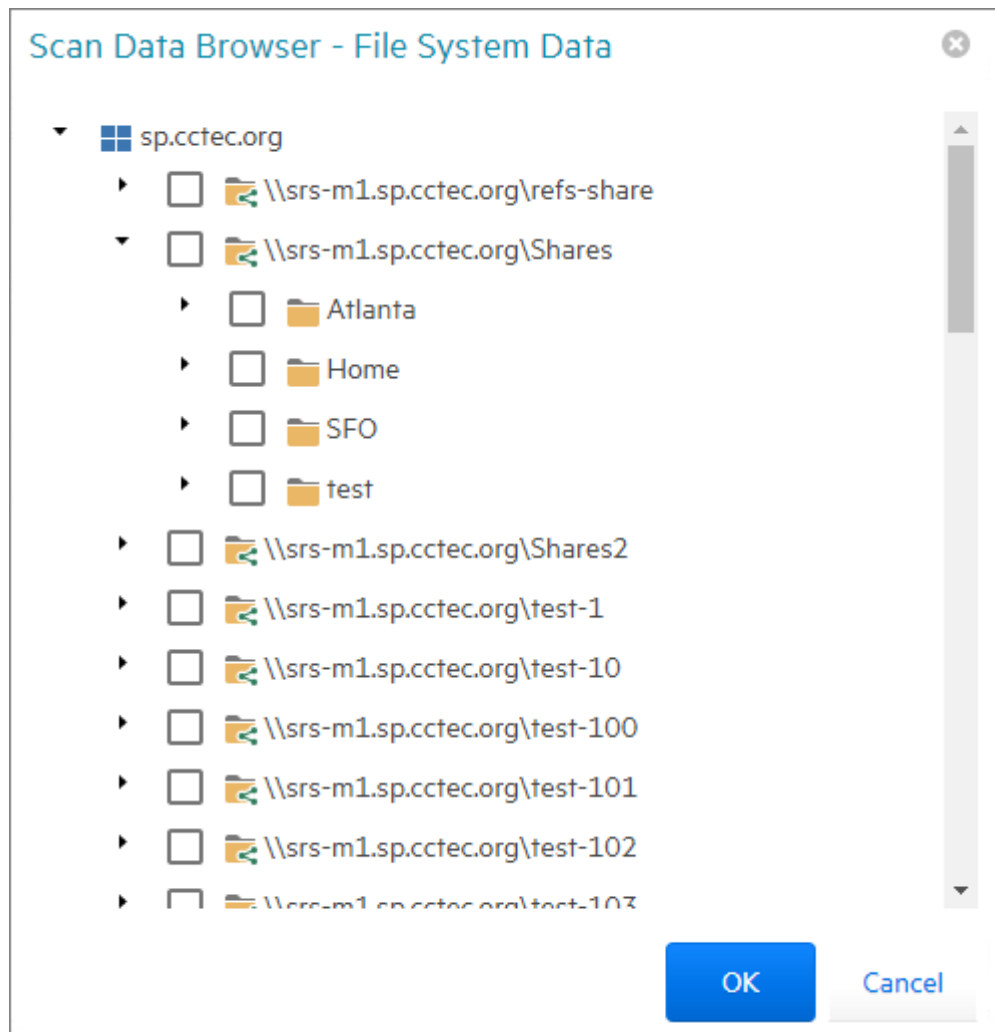
For example, for a server named srs-mlsp, the Summary report would list the contents of these paths:

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

The screenshot shows the 'Report Definitions' page in File Reporter 4.0. The page has a blue header with navigation tabs: File Reporter 4.0, Main, File Systems, File Content, Governance, Microsoft 365, Reports, and Configuration. The user is logged in as 'SPUAdministrator'. Below the header is a toolbar with icons for Add, Edit, Rename, Copy, Delete, Schedule, Generate, Report Branding and Styling, and Refresh. A sub-header says 'Drag a column header here to group by that column'. The main content is a table with the following columns: Name, Report Type, Targets, File Management Policies, Report Owner, Schedule, and Id. The table contains 10 rows of report definitions. The first row is selected and highlighted in blue.

<input type="checkbox"/>	Name	Report Type	Targets	File Management Policies	Report Owner	Schedule	Id
<input checked="" type="checkbox"/>	Copy Of Security - Find Compromized File	Custom Query	0	0	sp\administrator	[Not Scheduled]	4
<input type="checkbox"/>	duplicate file hash test query	Custom Query	0	0	sp\administrator	[Not Scheduled]	1
<input type="checkbox"/>	File create-time in future	Custom Query	0	0	sp\administrator	[Not Scheduled]	0
<input type="checkbox"/>	File Extensions by Category Summary	Custom Query	0	0	sp\administrator	[Not Scheduled]	2
<input type="checkbox"/>	num of Files with Mod-time greater than create-time	Custom Query	0	0	sp\administrator	[Not Scheduled]	8
<input type="checkbox"/>	Security - File Decrypt Virus Files	Custom Query	0	0	sp\administrator	[Not Scheduled]	5
<input type="checkbox"/>	Security - Find Compromized File	Custom Query	0	0	sp\administrator	[Not Scheduled]	3
<input type="checkbox"/>	Summary Report	Summary	0	0	sp\administrator	[Not Scheduled]	10
<input type="checkbox"/>	top 5 files per path	Custom Query	0	0	sp\administrator	[Not Scheduled]	7
<input type="checkbox"/>	vfs	Custom Query	0	0	sp\administrator	[Not Scheduled]	6

Page 1 of 1 (10 items) < 1 >

Create Filter

Copyright 2020 Condrey Corporation

10 Do one of the following:

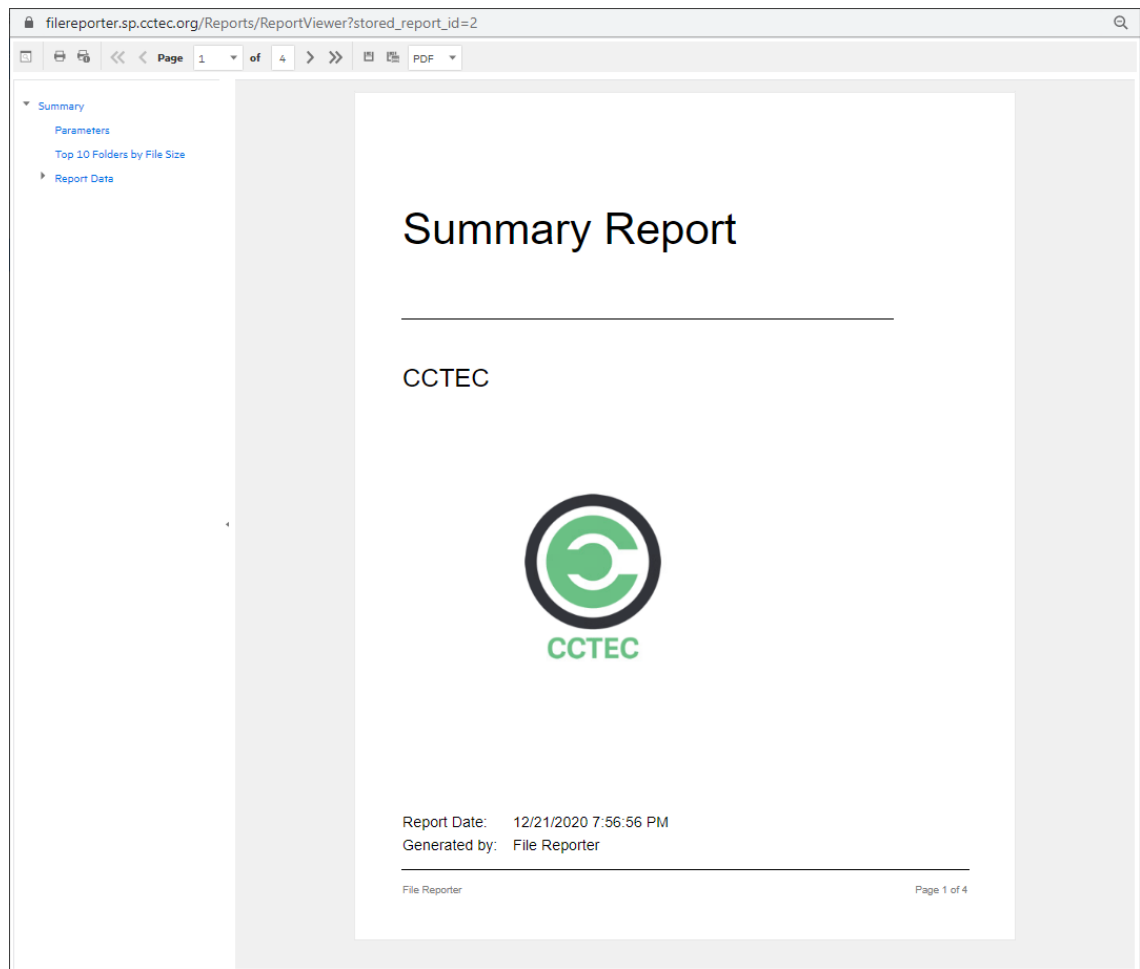
- ◆ Generate the report in Preview mode by following the procedures under “[Generating a Preview Report](#)” on page 59.
- ◆ Generate the report in Stored mode by following the procedures under “[Generating a Stored Report](#)” on page 61.

Generating a Preview Report

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.

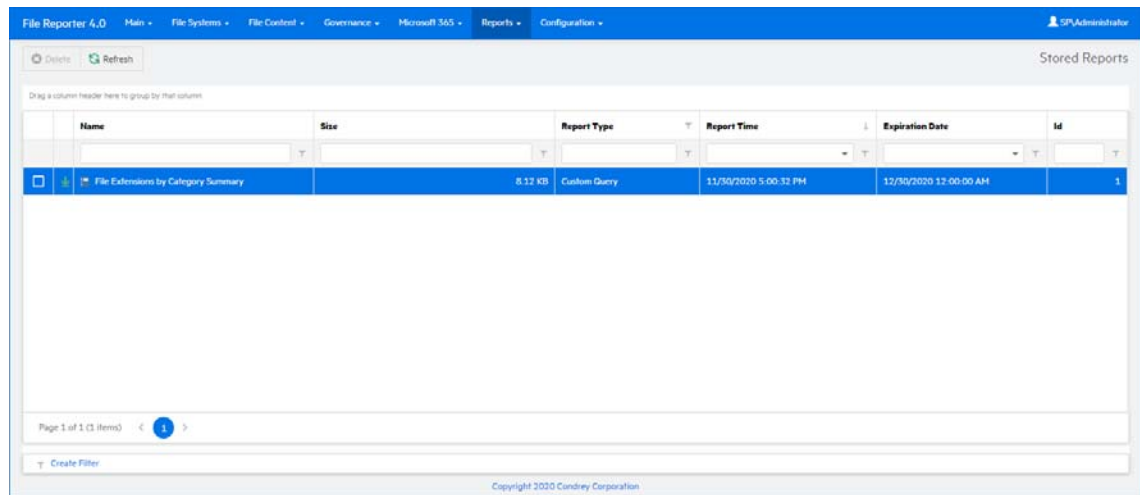
Document Navigation: Lists the contents of the report. You can click any item to advance within the preview report.

- 4 Export, save, or print the preview report.

Generating a Stored Report

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**.

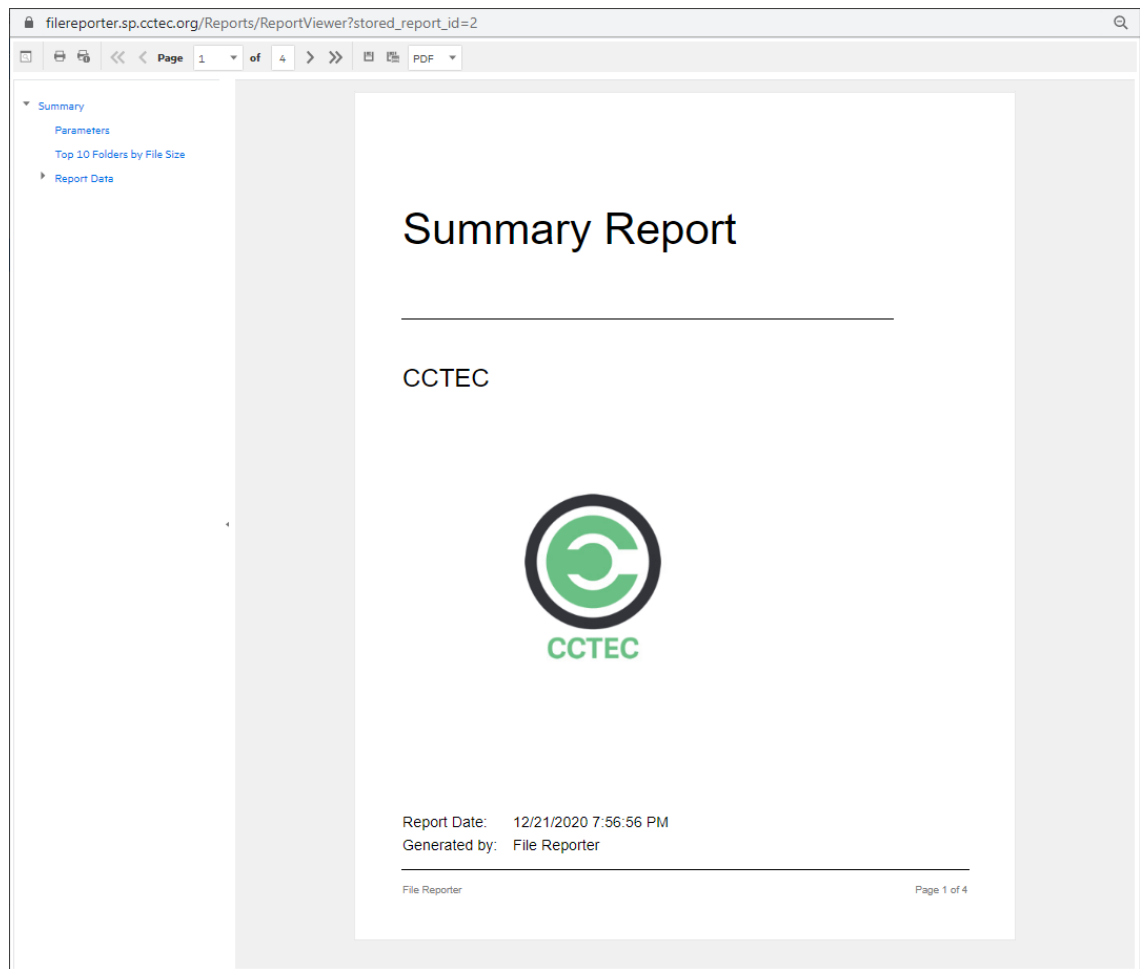


The screenshot shows the File Reporter 4.0 interface. The top navigation bar includes 'Main', 'File Systems', 'File Control', 'Governance', 'Microsoft 365', 'Reports', and 'Configuration'. The user is logged in as 'SPAdmin'. The main area is titled 'Stored Reports' and contains a table with the following data:

Name	Size	Report Type	Report Time	Expiration Date	Id
File Extensions by Category Summary	8.12 KB	Custom Query	11/30/2020 5:00:12 PM	12/30/2020 12:00:00 AM	1

At the bottom of the table, it says 'Page 1 of 1 (1 Items)' and 'Create Filter'. The footer of the page reads 'Copyright 2020 Conduley Corporation'.

- 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.

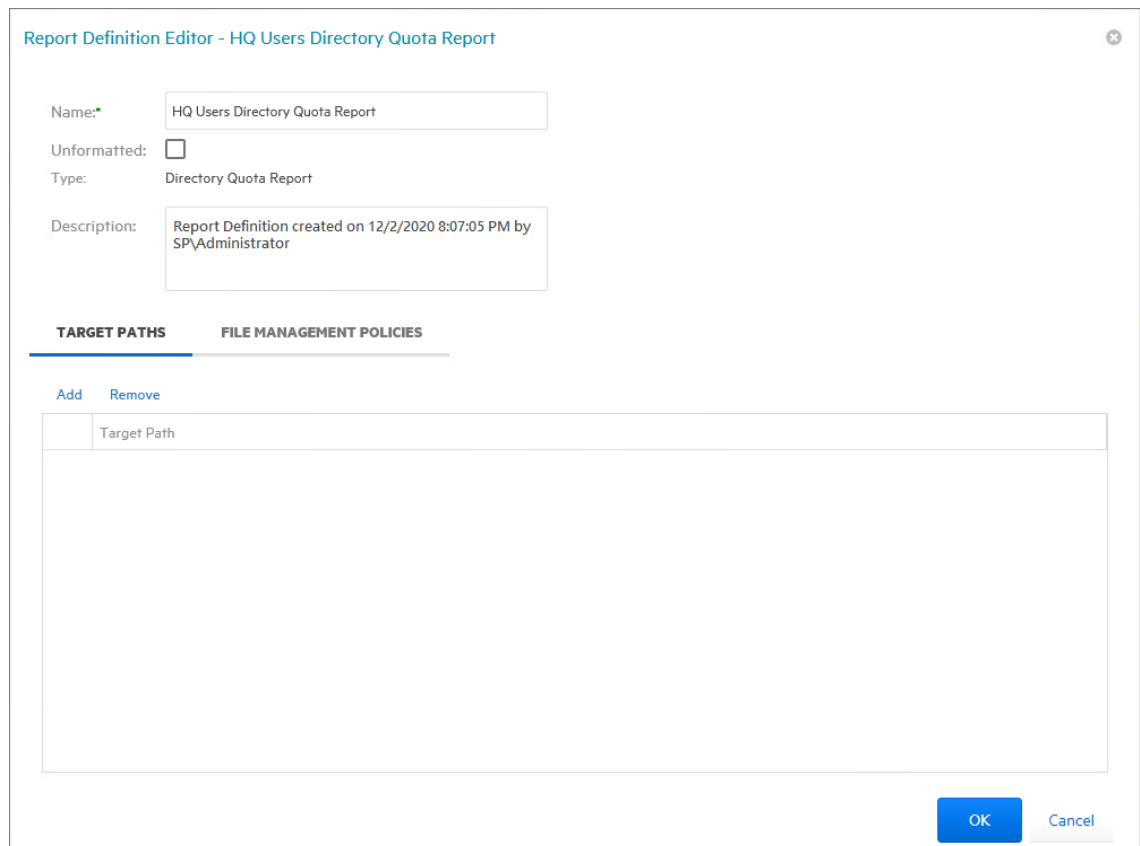
- 5 Save or print the stored report.

6.5.2 Generating a 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**.



The screenshot shows a dialog box titled "Report Definition Editor - HQ Users Directory Quota Report". It contains the following fields and options:

- Name:** HQ Users Directory Quota Report
- Unformatted:**
- Type:** Directory Quota Report
- Description:** Report Definition created on 12/2/2020 8:07:05 PM by SP\Administrator

Below these fields are two tabs: **TARGET PATHS** (selected) and **FILE MANAGEMENT POLICIES**. Under the **TARGET PATHS** tab, there are **Add** and **Remove** buttons above a table with one column labeled "Target Path". The table is currently empty. At the bottom right of the dialog are **OK** and **Cancel** buttons.

- 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 “Generating a Preview Report” on page 59.

For procedures on generating a Stored report, see “Generating a Stored Report” on page 61.

6.5.3 Generating a 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**.

Report Definition Editor - Atlanta Users Storage Cost Report

Name:* Atlanta Users Storage Cost Report Unit: GB

Unformatted: Cost per Unit:* 1.0

Type: Storage Cost Report

Description: Report Definition created on 12/2/2020 8:07:05 PM by SPAdministrator

TARGET PATHS FILE MANAGEMENT POLICIES

Add Remove

Target Path

OK Cancel

- 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 [“Generating a Preview Report” on page 59](#).
 - For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).

6.5.4 Generating a 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**.

Report Definition Editor - HQ Share Users Comparison Report

Name:* Results:

Unformatted:

Type: Comparison Report

Description:

TARGET PATHS

Add Remove

Target Path	Index

OK Cancel

- 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 [“Generating a Preview Report” on page 59](#).

For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).

6.6 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.

- ♦ [Section 6.6.1, “Generating an Assigned NTFS Permissions Report,” on page 66](#)
- ♦ [Section 6.6.2, “Generating a Permissions by Path Report,” on page 68](#)
- ♦ [Section 6.6.3, “Generating a Permissions by Identity Report,” on page 69](#)

6.6.1 Generating an 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 [“Generating a Preview Report”](#) on page 59.

For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.

6.6.2 Generating a 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**.

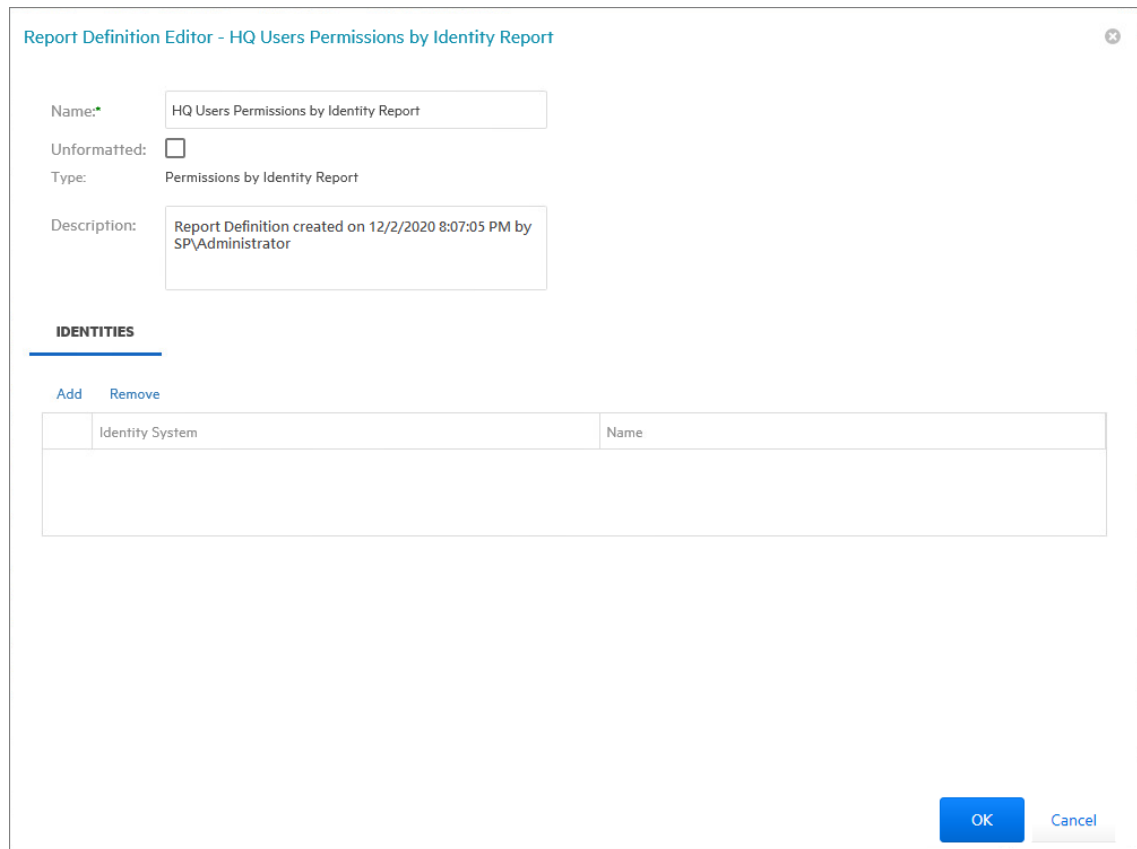
The screenshot shows the 'Report Definition Editor' window for a report named 'London Users Permissions by Path Report'. The window has a title bar with the text 'Report Definition Editor - London Users Permissions by Path Report' and a close button. The main content area is divided into two sections: 'Name' and 'Description'. The 'Name' field contains the text 'London Users Permissions by Path Report'. The 'Unformatted' checkbox is unchecked. The 'Type' is set to 'Permissions by Path Report'. The 'Description' field contains the text 'Report Definition created on 12/2/2020 8:07:05 PM by SP\Administrator'. Below these fields are two tabs: 'TARGET PATHS' (which is selected) and 'FILE MANAGEMENT POLICIES'. Under the 'TARGET PATHS' tab, there are 'Add' and 'Remove' buttons. Below these buttons is a table with one column header 'Target Path' and an empty body. At the bottom right of the window are 'OK' and 'Cancel' buttons.

- 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 [“Generating a Preview Report”](#) on page 59.
For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.

6.6.3 Generating a 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**.



The screenshot shows a dialog box titled "Report Definition Editor - HQ Users Permissions by Identity Report". It contains the following fields and options:

- Name:** HQ Users Permissions by Identity Report
- Unformatted:**
- Type:** Permissions by Identity Report
- Description:** Report Definition created on 12/2/2020 8:07:05 PM by SPAdministrator

Below these fields is a section titled **IDENTITIES** with a blue underline. It includes "Add" and "Remove" links. A table is present with the following structure:

Identity System	Name

At the bottom right of the dialog box are "OK" and "Cancel" buttons.

- 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 [“Generating a Preview Report” on page 59](#).
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).

6.7 File Data Reports

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.

- ◆ [Section 6.7.1, “Generating a Filename Extension Report,” on page 70](#)
- ◆ [Section 6.7.2, “Generating a Detailed Filename Extension Report,” on page 71](#)
- ◆ [Section 6.7.3, “Generating an Owner Report,” on page 73](#)
- ◆ [Section 6.7.4, “Generating a Detailed Owner Report,” on page 74](#)
- ◆ [Section 6.7.5, “Generating a Duplicate File Report,” on page 75](#)
- ◆ [Section 6.7.6, “Generating a Detailed Duplicate File Report,” on page 76](#)
- ◆ [Section 6.7.7, “Generating a Date-Age Report,” on page 78](#)
- ◆ [Section 6.7.8, “Generating a Detailed Date-Age Report,” on page 79](#)

6.7.1 Generating a 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 [Appendix A, “Filtering for Built-in Reports,”](#) on page 155.
- 8 Click **Save**.
- 9 Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see [“Generating a Preview Report”](#) on page 59.
For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.
- 10 (Optional) Generate a Detailed report on an individual file extension by clicking a file extension name in the report.

6.7.2 Generating a 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 [Appendix A, “Filtering for Built-in Reports,”](#) on page 155.
- 9 Click **Save**.
- 10 Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see [“Generating a Preview Report”](#) on page 59.
For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.

6.7.3 Generating an 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**.

The screenshot shows a window titled "Report Definition Editor - Atlanta Users Owner Report". It contains the following fields and options:

- Name:** Atlanta Users Owner Report
- Unformatted:**
- Type:** Owner Report
- Description:** Report Definition created on 12/2/2020 8:07:05 PM by SPAdministrator

Below these fields are three tabs: **TARGET PATHS** (selected), **FILE MANAGEMENT POLICIES**, and **FILTERS**. Under the **TARGET PATHS** tab, there are "Add" and "Remove" buttons above a table with one header row: "Target Path". The table body is currently empty. At the bottom right of the window are "OK" and "Cancel" buttons.

- 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 [Appendix A, "Filtering for Built-in Reports,"](#) on page 155.
- 8 Click **Save**.
- 9 Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see ["Generating a Preview Report"](#) on page 59.
For procedures on generating a Stored report, see ["Generating a Stored Report"](#) on page 61.
- 10 (Optional) Generate a Detailed report on an individual owner by clicking an owner's name in the report.

6.7.4 Generating a 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**.

The screenshot shows the 'Report Definition Editor - Munich Users Owner Detail Report' dialog box. It has a title bar with a close button. The main area contains the following fields and controls:

- Name:** A text input field containing 'Munich Users Owner Detail Report'. To its right is an information icon and the text 'See Owners tab below for selected identities.'
- Unformatted:** A checkbox that is currently unchecked.
- Type:** A dropdown menu set to 'Owner Detail Report'.
- Description:** A text area containing 'Report Definition created on 12/2/2020 8:07:05 PM by SPAdministrator'.

Below these fields are four tabs: **OWNERS** (selected), **TARGET PATHS**, **FILE MANAGEMENT POLICIES**, and **FILTERS**. Under the **OWNERS** tab, there are 'Add' and 'Remove' buttons. Below these is a table with the following structure:

#	Identity System	Owner
No data to display		

At the bottom of the table area, there is a pagination control showing 'No data to paginate' and navigation arrows. At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

- 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 [Appendix A, "Filtering for Built-in Reports,"](#) on page 155.
- 8 Click **Save**.
- 9 Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see ["Generating a Preview Report"](#) on page 59.
For procedures on generating a Stored report, see ["Generating a Stored Report"](#) on page 61.

6.7.5 Generating a 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 hash comparisons. For more details, see [Section 6.11.1, “Generating a Content Hashed Duplicate File Report,”](#) on page 90.

- 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**.

Report Definition Editor - Atlanta Duplicate File Report

Name:* Atlanta Duplicate File Report

Unformatted:

Type: Duplicate File Report

Description: Report Definition created on 12/2/2020 8:07:05 PM by SP\Administrator

Match Size

Match Name

Match Create Time

Match Modify Time

Minimum Duplicates: 2

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path

OK Cancel

- 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 [Appendix A, “Filtering for Built-in Reports,”](#) on page 155.
- 8 Click **Save**.
- 9 Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see [“Generating a Preview Report”](#) on page 59.
For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.
- 10 (Optional) Generate a Detailed report on a duplicate file by clicking a specific file name in the report.

6.7.6 Generating a 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**.

Report Definition Editor - HQ Duplicate File Detail Report

Name: HQ Duplicate File Detail Report

Unformatted:

Type: Duplicate File Detail Report

Description: Report Definition created on 12/2/2020 8:07:05 PM by SPAdministrator

Duplicate Criteria

Name

Size 0 bytes

Create Time

Modify Time

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path

OK Cancel

- 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 [Appendix A, “Filtering for Built-in Reports,” on page 155.](#)

- Browse to and specify the file paths you want included in the report and click **OK**.
- (Optional) Click the **Filters** tab and set the filters for the report.
For information on using the filtering capabilities of File Reporter, refer to [Appendix A, “Filtering for Built-in Reports,” on page 155.](#)
- Click **Save**.
- Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see [“Generating a Preview Report” on page 59.](#)
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61.](#)

6.7.7 Generating a 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**.

The screenshot shows a dialog box titled "Report Definition Editor - HQ Users Date-Age Report". It contains the following fields and options:

- Name:** HQ Users Date-Age Report
- Date Type:** Create Time (dropdown menu)
- Unformatted:**
- Type:** Date-Age Report
- Detail Level:** Year (dropdown menu)
- Description:** Report Definition created on 12/2/2020 8:07:05 PM by SP\Administrator

Below these fields are three tabs: **TARGET PATHS** (selected), **FILE MANAGEMENT POLICIES**, and **FILTERS**. Under the **TARGET PATHS** tab, there are "Add" and "Remove" buttons and a table with one header row "Target Path". At the bottom right of the dialog are "OK" and "Cancel" buttons.

- 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 [Appendix A, “Filtering for Built-in Reports,”](#) on page 155.
- 9 Click **Save**.
- 10 Generate the report as either a Preview report or a Stored report.
For procedures on generating a Preview report, see [“Generating a Preview Report”](#) on page 59.
For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.
- 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.

6.7.8 Generating a 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**.

Report Definition Editor - Atlanta Shares Detailed Date-Age Report

Name: Atlanta Shares Detailed Date-Age Report

Unformatted:

Type: Date-Age Detail Report

Description: Report Definition created on 12/2/2020 8:07:05 PM by SPAdministrator

Date Type: Create Time

Detail Level: Year

Selected Dates:

Enter one or more dates with the format yyyy-mm-dd, one per line.

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path

OK Cancel

- 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 [Appendix A, "Filtering for Built-in Reports,"](#) on page 155.
- 10 Click **Save**.
- 11 Generate the report as either a Preview report or a Stored report.

For procedures on generating a Preview report, see [“Generating a Preview Report”](#) on page 59.

For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.

6.8 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.

- ◆ [Section 6.8.1, “Generating a Historic File System Comparison Report,”](#) on page 81
- ◆ [Section 6.8.2, “Generating a Historic NTFS Permissions Comparison Report,”](#) on page 83

6.8.1 Generating a 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**.

Report Definition Editor - Atlanta Historic File System Comparison Report

Name: Atlanta Historic File System Comparison Report

Unformatted:

Type: Historic File System Comparison Report

Description: Report Definition created on 12/2/2020 8:07:05 PM by SPVAdministrator

Limit Path Depth: 100

Scans to Compare: Current and Previous

QUERY FILTERS

Added Entries

Removed Entries

Modified Entries

DETAIL DISPLAY OPTIONS

Files

Folders

Include entries modified by:

File Size Create Time Directory Quota

Attributes Modify Time

Owner Access Time

TARGET PATHS

Add Remove

Target Path

OK Cancel

- (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.

- 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.

- 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 [“Generating a Preview Report” on page 59](#).

For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).

6.8.2 Generating a 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**.

Report Definition Editor - Atlanta Users Historic NTFS Comparison Report

Name: Atlanta Users Historic NTFS Comparison Report

Unformatted:

Type: Historic NTFS Permissions Comparison Report

Description: Report Definition created on 12/2/2020 8:07:05 PM by SP\Administrator

Limit Path Depth: 100

Scans to Compare: Current and Previous

Include Inherited ACEs

Include Removed Paths

TARGET PATHS

Add Remove

Target Path

OK Cancel

- (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.

- 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.

- (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.

- (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.
- 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 [“Generating a Preview Report”](#) on page 59.

For procedures on generating a Stored report, see [“Generating a Stored Report”](#) on page 61.

6.9 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.

6.9.1 Generating a 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**.

The screenshot shows the 'Report Definition Editor - SFO Volume Free Space Report' window. It contains the following fields and controls:

- Name:** SFO Volume Free Space Report
- Last number of days to include:** 365
- Unformatted:**
- Type:** Volume Free Space Trending Report
- Description:** Report Definition created on 12/2/2020 8:07:05 PM by SPVAdministrator

Below these fields is a section titled **TARGET PATHS** with **Add** and **Remove** buttons. A table with one column labeled 'Target Path' is present but empty.

At the bottom right, there are **OK** and **Cancel** buttons.

- 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 [“Generating a Preview Report” on page 59](#).
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).

6.10 Unformatted Reports

File Reporter allows you to generate unformatted reports. In some instances, having an unformatted report might be useful for doing extensive sorting and filtering of the report data using a product such as Microsoft Excel.

File Reporter can generate an unformatted report for all built-in report types except for Summary reports.

You can generate unformatted reports by selecting the option in the Add Report Definition dialog box or by selecting the **Unformatted** check box in the Report Definition Editor dialog box.

6.10.1 Generating Unformatted Reports

- 1 Select **Reports > Report Definitions**.
- 2 Click **Add**.
- 3 In the **Name** field, specify a descriptive name of the report definition.
- 4 Select the report type you want to generate.
- 5 Select **Create report as Unformatted**.

- 6 Click **OK**.
- 7 In the Report Definition Editor, specify the settings and the file paths you want included in the report, then click **OK**.
- 8 Click **Save**.
- 9 Generate the report as either a Preview report or a Stored report.
 For procedures on generating a Preview report, see [“Generating a Preview Report” on page 59](#).
 For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).
- 10 From the file type drop-down menu, select either **XLS**, **XLSX**, **Text**, or **CSV**.
- 11 Click the **Export a Report and Save it to the Disk** button.
- 12 Select **Save File** and click **OK**.

6.11 Custom Query Reports

Custom Query Reports are reports that are generated through a series of SQL commands that you enter. 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 commands must be specific to the database (Microsoft SQL Server or PostgreSQL) that your deployment of File Reporter is utilizing.

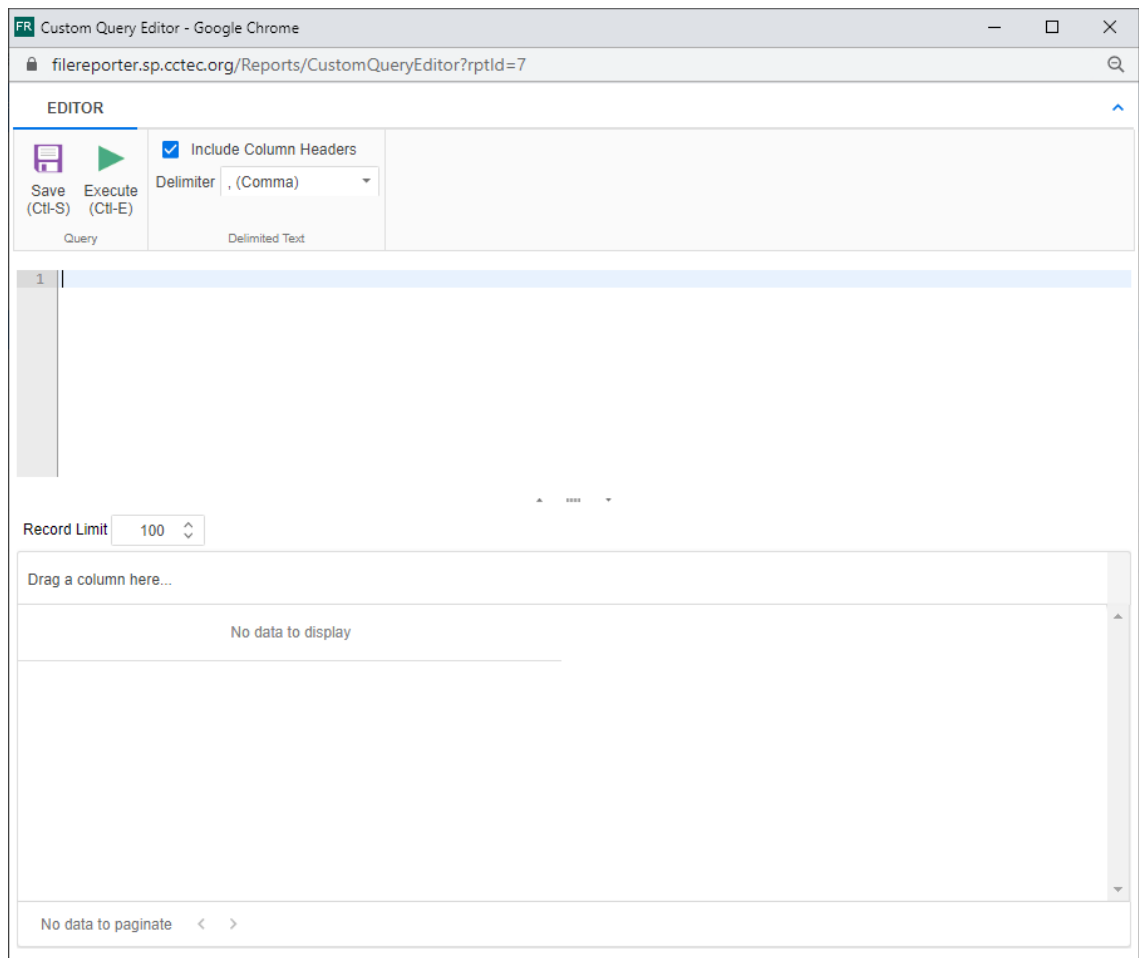
NOTE: For details and examples of the supported database functions, tables, and views that you can utilize in Custom Query reports, refer to the *Micro Focus File Reporter 4.0 Database Schema and Custom Queries Guide*.

SQL commands 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 [Section 11.3, “Designing a Custom Query Report,”](#) on page 142.

TIP: Don't forget to utilize File Query Cookbook as a resource for obtaining SQL commands and sample report layouts that have been submitted by the File Reporter community. 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>.

- 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 commands according to what information you want included in your report. As you enter commands, 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.

The screenshot shows the Custom Query Editor interface. At the top, there are buttons for 'Save (Ctl-S)' and 'Execute (Ctl-E)'. A checkbox for 'Include Column Headers' is checked, and the 'Delimiter' is set to '(Comma)'. Below this is a text area containing a SQL query:

```

1 WITH
2     x(filename_extension, size, category) AS (SELECT sd.filename_extension,
3         sd.size,
4         CASE WHEN sd.filename_extension IN ('lan', 'ncp', 'nlm', 'nlk', 'vlm') THEN 'Novel
5         FROM srs.current_fs_scandata AS sd
6         WHERE (sd.fullpath LIKE '\\sp.cctec.org\DFS\HQ\HQShare\%' ESCAPE '#') AND
7             (sd.path_type = 1))
8
9 SELECT
10    x.category,
11    Sum(x.size) AS cat_size.
12

```

Below the query editor, there is a 'Record Limit' dropdown set to 100. The results are displayed in a table:

#	category	cat_size	file_count	cat_size_strir
1	Configuration Files	59832	1	58.43 KB
2	Document Files	1331905	9	1.27 MB

At the bottom, there is a pagination control showing 'Page 1 of 1 (8 items)' with a page number '1' in a blue circle.

- 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 [“Generating a Preview Report” on page 59](#).
 - For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).

6.11.1 Generating a Content Hashed Duplicate File Report

- ♦ [“Using the Query Editor” on page 91](#)
- ♦ [“Using the Report Designer” on page 93](#)

A Content Hashed Duplicate File report provides more advanced duplicate file detection over the Duplicate File built-in report which compares only filenames and metadata.

With the introduction of File Reporter 4.0, a new scanning option allows for Agents to produce a content based hash for specific files. These hashes can then be compared to identify duplicate files.

NOTE: For information on the content based hashing option, see [Section 5.4, “Creating Scan Policies,”](#) on page 38.

Through [filequerycookbook](#), you can copy and paste the Content Hashed Duplicate File Report custom query into the Query Editor and export a report layout into the Report Designer. This custom query and associated report identifies duplicate files based on hash comparisons and the parameters you set.

Prerequisites

- ◆ Create a file system scan policy for each of the target paths on which you want to report.
- ◆ With the **Generate content file hashes** option selected in the Scan Policy Editor of each scan policy, conduct a file system scan on each target path.
- ◆ Install the Client Tools.

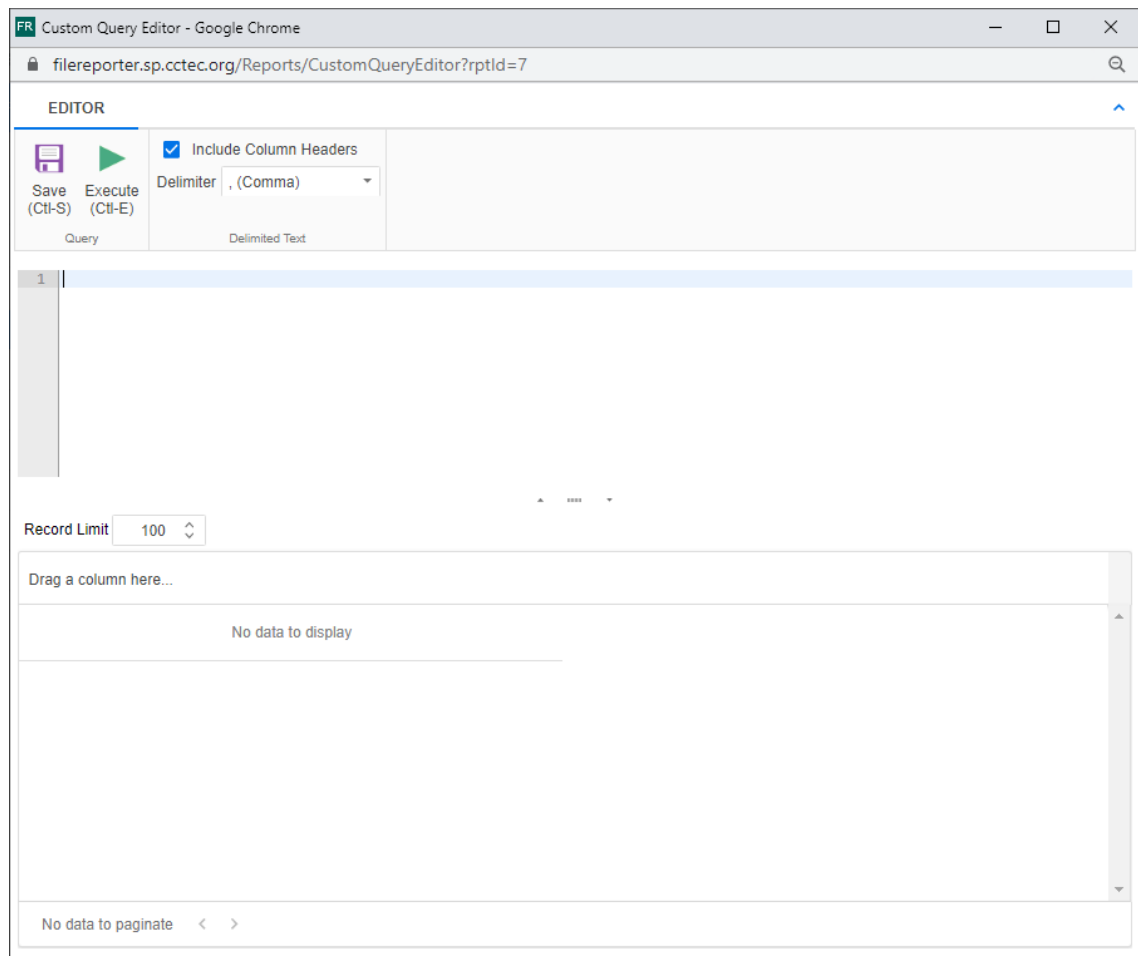
The Client Tools include the Query Editor and the Report Designer that will be used in these procedures.

- ◆ Decide how you want the report to be generated and follow the applicable procedures.
 - ◆ To generate a .CSV file that you can take into Microsoft Excel for customized searching and presentations or to import as a workload file in the File Dynamics Data Owner Client, you can copy or create an SQL query either with the browser based query editor covered in [“Using the Query Editor”](#) on page 91, or with the query editor in the Report Designer covered in [“Using the Report Designer”](#) on page 93.
 - ◆ To generate the report using the Report Designer and export the report as either a .PDF, .HTML, .MHT, .RTF, .DOCX, .XLS, .XLSX, .CSV, Text, or Image file, proceed with [“Using the Report Designer”](#) on page 93

Both the Query Editor and the Report Designer options provide the ability to generate a .CSV file, but for efficiency and capabilities, Micro Focus recommends that .CSV files be generated using the Query Editor option.

Using the Query Editor

- 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 Using File Query Cookbook located at <https://www.filequerycookbook.com>, locate and download the “Content Hashed Duplicate File Report.”

The file is saved as zipped file.

- 6 Unzip the downloaded file and open it in a text editor such as Notepad++.
- 7 From the text editor, copy the custom query and past it into the Query Editor.
- 8 In the line beginning with `WHERE`, edit the UNC paths so that they are specific to the content file hashed shares on which you want to report.

The custom query only includes two paths so if you want more, extend the line to include more paths by adding `srs.path_hash('\\server\share\path')` to the comma delimited `sd.fullpath_hash IN` portion of the where clause for each desired path.

- 9 (Conditional) At the bottom of the custom query, modify the `q.item_count` and `q.size` settings to the minimum number of duplicates and file sizes (in bytes), respectively, to include in the report.
- 10 Click **Execute** to get a preview in the bottom portion of the editor of how the report will appear.

The screenshot shows the Custom Query Editor interface. At the top, there are buttons for 'Save (Ctl-S)' and 'Execute (Ctl-E)'. A checkbox labeled 'Include Column Headers' is checked. Below it, a 'Delimiter' dropdown menu is set to '(Comma)'. The main area contains a SQL query:

```

1 WITH
2   root_path(fullpath, fullpath_hash, ns_left, ns_right, path_type, scan_id) AS (SELECT sd.
3     sd.fullpath_hash,
4     sd.ns_left,
5     sd.ns_right,
6     sd.path_type,
7     sd.scan_id
8   FROM srs.scan_data AS sd
9   INNER JOIN srs.scans AS s ON s.id = sd.scan_id
10  WHERE (sd.fullpath_hash IN (srs.path_hash('\srs-m1.sp.cctec\Shares'), srs.path_
11         (sd.path_type = 2) AND
12

```

Below the query, there is a 'Record Limit' dropdown set to '100'. The results are displayed in a table:

#	fullpath	size	create_time	modify_time	access_time	name	item_count	total_size	c
1	\\srs-m1.sp.cctec. Visual Studio	1081656	2020-09-21 17:26:56	2015-07-01 22:59:20	2020-09-21 17:26:56	msdia140.dll	2	2163312	C

At the bottom, it shows 'Page 1 of 1 (100 items)' with a blue circle containing the number '1' and navigation arrows.

- 11 When you are satisfied with the report and the previewed results, click **Save**.
- 12 Close the Custom Query Report Editor.
- 13 Select **Reports > Report Definitions**.
- 14 Select the Custom Query Report you just saved and generate the report as a Stored report.
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 61](#).
- 15 From the **Reports** menu, select **Stored Reports**.
- 16 Click the download icon associated with the new report.
- 17 Save the report to a desired location.
From here you can open the .CSV file into Microsoft Excel and sort through the report data as desired. If you have Micro Focus File Dynamics, you can import the .CSV file as a workload.

Using the Report Designer

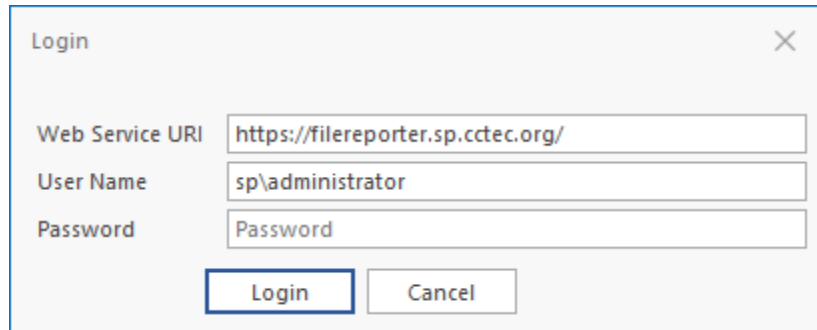
This option lets you utilize both the custom query *and* the associated report layout design for the “Content Hashed Duplicate File Report” from filequerycookbook.com.

NOTE: A detailed discussion of the Report Designer, along with procedures for familiarizing yourself with the interface are available in [Chapter 11, “Using Report Designer,”](#) on page 137.

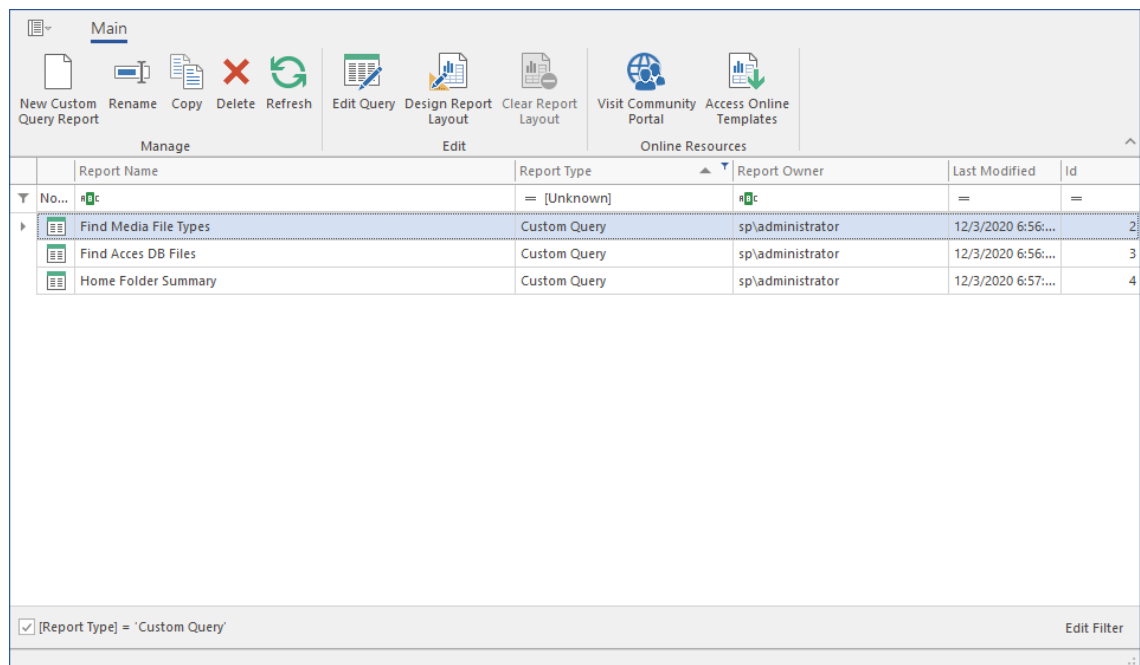
- 1 Using File Query Cookbook located at <https://www.filequerycookbook.com>, locate and download the “Content Hashed Duplicate File Report.”

The file is saved as zipped file.

- 2 Unzip the downloaded file and open the .SQL file in a text editor such as Notepad++.
You will eventually paste this custom query into the Query Editor.
- 3 From the **Start** menu, launch the **File Reporter 4.0 Report Designer**.



- 4 Enter the login credentials and click **Login**.

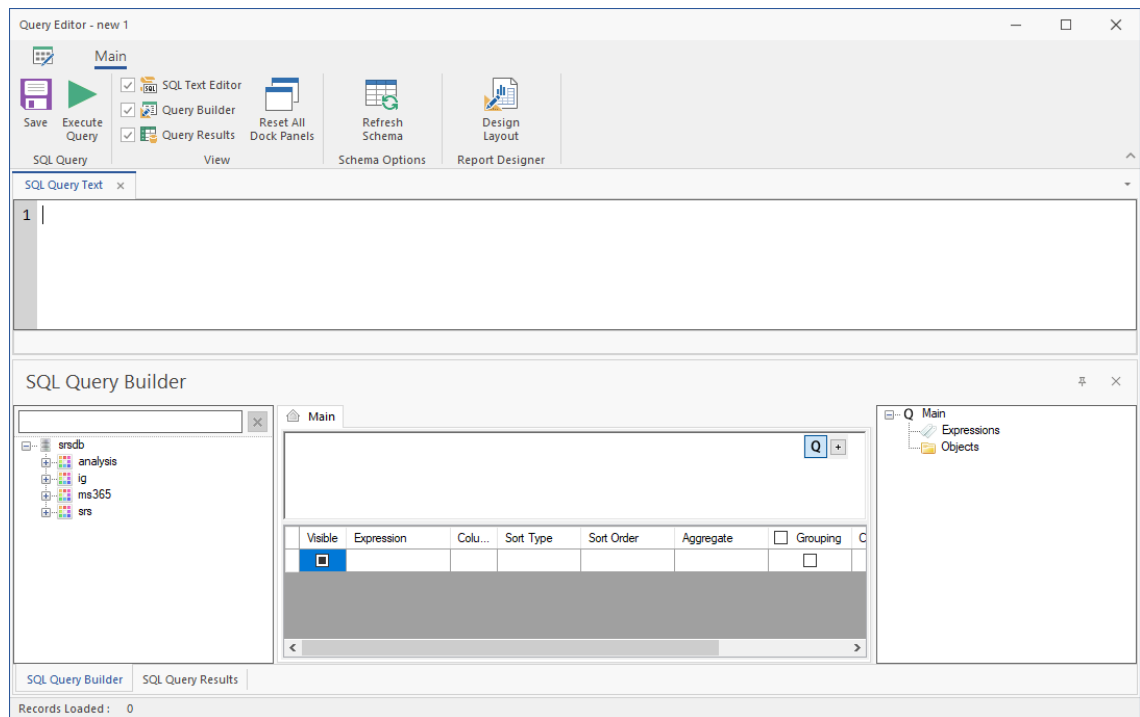


No...	Report Name	Report Type	Report Owner	Last Modified	Id
		= [Unknown]		=	=
2	Find Media File Types	Custom Query	sp\administrator	12/3/2020 6:56...	
3	Find Acces DB Files	Custom Query	sp\administrator	12/3/2020 6:56...	
4	Home Folder Summary	Custom Query	sp\administrator	12/3/2020 6:57...	

[Report Type] = 'Custom Query' Edit Filter

All of your saved Custom Query reports are listed.

- 5 Click **New Custom Query**, give it a name, then click **Create**.
The Report Designer Query Editor is launched.



- 6 From the text editor you used in Step 2, copy the custom query and past it into the Query Editor.
- 7 In the line beginning with `WHERE`, edit the UNC paths so that they are specific to the content file hashed shares on which you want to report.

The custom query only includes two paths so if you want more, extend the line to include more paths by adding `srs.path_hash('\\server\share\path')` to the comma delimited `sd.fullpath_hash` IN portion of the where clause for each desired path.
- 8 (Conditional) At the bottom of the custom query, modify the `q.item_count` and `q.size` settings to the minimum number of duplicates and file sizes (in bytes), respectively, to include in the report.
- 9 Click **Execute** to get a preview in the bottom portion of the editor of how the report will appear.

Query Editor - new 1

Main

Save Execute Query SQL Text Editor Query Builder Reset All Dock Panels Refresh Schema Design Layout

SQL Query View Schema Options Report Designer

```

31 srs.byte_string(CAST((q.total_size - q.size) AS BIGINT)) AS wasted_space_string
32 FROM
33 q
34 WHERE
35 (q.size > 0) AND
36 (q.item_count >= 2)
37

```

SQL Query Results - Limited to 10,000 Records

Drag a column header here to group by that column

fullpath	size	create_time	modify_time	access_time	name	item_count	total_size	content_ha...	size_string	total_size_s...	wasted_spa...	wasted_spa...
\\srs-m1.sp...	1081656	2020-09-21...	2015-07-01...	2020-09-21...	msdia140.dll	2	2163312	00721b85b...	1.03 MB	2.06 MB	1081656	1.03 MB
\\srs-m1.sp...	1081656	2020-09-21...	2015-07-01...	2020-09-21...	msdia140.dll	2	2163312	00721b85b...	1.03 MB	2.06 MB	1081656	1.03 MB
\\srs-m1.sp...	31592	2020-09-21...	2019-04-13...	2020-09-21...	Microsoft...	3	94776	02b62eac1...	30.85 KB	92.55 KB	63184	61.7 KB
\\srs-m1.sp...	31592	2020-09-21...	2019-04-13...	2020-09-21...	Microsoft...	3	94776	02b62eac1...	30.85 KB	92.55 KB	63184	61.7 KB
\\srs-m1.sp...	31592	2020-09-21...	2019-04-13...	2020-09-21...	Microsoft...	3	94776	02b62eac1...	30.85 KB	92.55 KB	63184	61.7 KB
\\srs-m1.sp...	20021	2020-09-21...	2019-09-18...	2020-09-21...	as90.xsl	2	40042	037831bb4...	19.55 KB	39.1 KB	20021	19.55 KB
\\srs-m1.sp...	20021	2020-09-21...	2019-06-03...	2020-09-21...	as90.xsl	2	40042	037831bb4...	19.55 KB	39.1 KB	20021	19.55 KB
\\srs-m1.sp...	637	2020-09-21...	2019-04-13...	2020-09-21...	MobileFor...	2	1274	042c7fb844...	637 bytes	1.24 KB	637	637 bytes
\\srs-m1.sp...	637	2020-09-21...	2015-07-06...	2020-09-21...	MobileFor...	2	1274	042c7fb844...	637 bytes	1.24 KB	637	637 bytes
\\srs-m1.sp...	18624	2020-09-21...	2019-04-13...	2020-09-21...	api-ms-win...	2	37248	057b0483f...	18.19 KB	36.38 KB	18624	18.19 KB
\\srs-m1.sp...	18624	2020-09-21...	2019-04-13...	2020-09-21...	api-ms-win...	2	37248	057b0483f...	18.19 KB	36.38 KB	18624	18.19 KB

SQL Query Builder SQL Query Results

Records Loaded: 1,078

10 Click Save.

11 Click Design Layout.

Report Designer Print Preview

Open... Save Refresh Data Bindings Download All Data Edit Query Cut Copy Paste Undo Redo Times New Roman 9.75 B I U Alignment Layout Zoom Out Zoom In View Scripts

Report Report Data Edit Font Alignment Layout View Scripts

Toolbox

Standard Controls

- Pointer
- Label
- Check Box
- Rich Text
- Picture Box
- Panel
- Table
- Character Comb
- Line
- Shape
- Bar Code
- Chart
- Cross Tab
- Gauge

Custom Permissions

Field List

Report Data

- Query Results

Properties

CustomQueryReportBase Report

- Background...
- Border Color
- Border Das...
- Border Width
- Borders
- Font

Background Color

Gets or sets the control's background color.

Group and Sort

Add a Group Add a Sort Delete Move Up Move Down

Field Name	Sort Order	Show Header	Show Footer

Group and Sort Scripts Errors

CustomQueryReportBase (PaperKind: Letter) Record Count: 0 Partial query results in use 100%

12 Click Open.

- 13 Locate the `.REPX` file that you saved and unzipped in Step 2 and click **Open**.
The layout template appears in the Report Designer.
- 14 Click **Download All Data**.
- 15 In the subsequent dialog box, click **Yes**.
This runs the query in the database and loads data into the report template.
- 16 Click **Print Preview** to review the report findings.
Note how the hashes are listed with a total number for each and the location of each, meaning the total number of duplicate files and their locations.
- 17 Save the report by doing one of the following:
 - ♦ From the **Export To** drop-down menu, select the file type you want to save the report layout to.
 - ♦ Click **Save Report** to save the report as a `.PRNX` file that you can open in the Report Viewer and if you want later, export the report to the desired file type.

6.11.2 Generating Microsoft 365 Reports

Once Agent365 has scanned the data and associated permissions for Microsoft 365 file repositories, including OneDrive for Business, SharePoint Online document libraries, and Teams document libraries, you can use the pre-built custom queries and associated report layouts in [filequerycookbook.com](https://www.filequerycookbook.com) to generate reports.

Prerequisites

- ♦ Install and configure Agent365.
 - ♦ Scan the tenant.
For procedures, see [Section 5.18, “Scanning Your Microsoft 365 Tenant,” on page 48](#).
 - ♦ Install the Client Tools.
The Client Tools include the Query Editor and the Report Designer that will be used in these procedures.
- 1 Using File Query Cookbook located at <https://www.filequerycookbook.com>, locate and download one of the custom queries and associated reports for Microsoft 365.
The file is saved as zipped file.
 - 2 Unzip the downloaded file and open the `.SQL` file in a text editor such as Notepad++.
You will eventually paste this custom query into the Query Editor.
 - 3 From the **Start** menu, launch the **File Reporter 4.0 Report Designer**.

Login

Web Service URI

User Name

Password

4 Enter the login credentials and click **Login**.

Main

New Custom Query Report Rename Copy Delete Refresh Edit Query Design Report Layout Clear Report Layout Visit Community Portal Access Online Templates

Manage Edit Online Resources

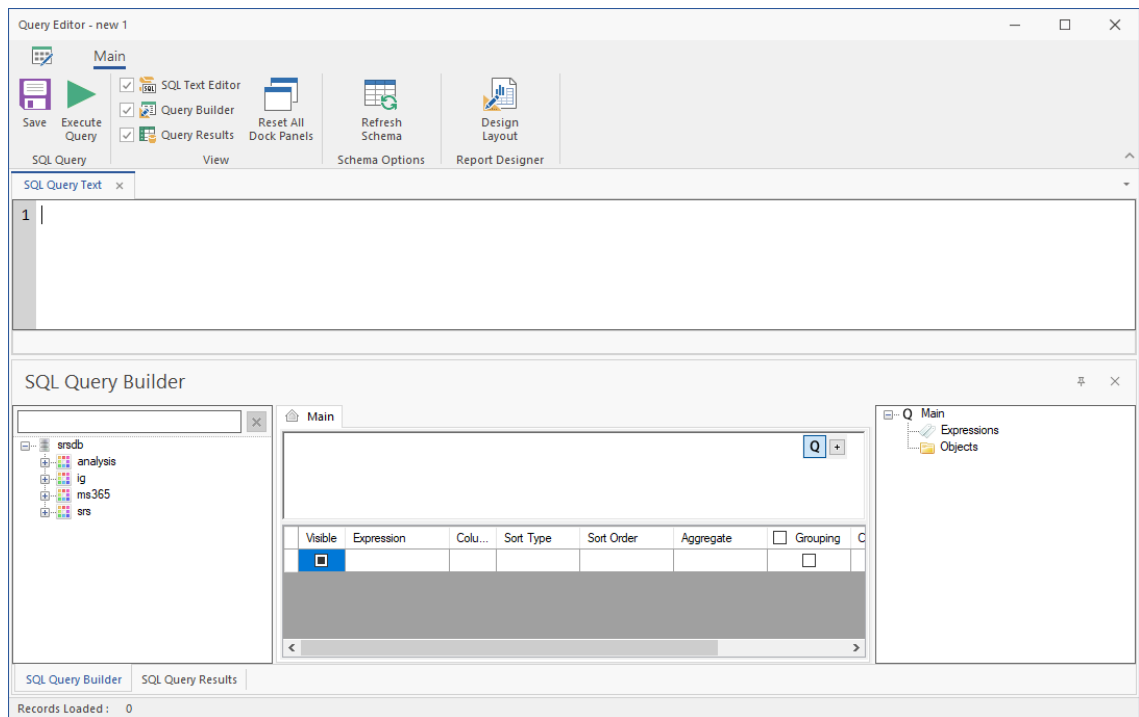
	Report Name	Report Type	Report Owner	Last Modified	Id
▼	No...	= [Unknown]	#Dc	=	=
▶	Find Media File Types	Custom Query	sp\administrator	12/3/2020 6:56:...	2
	Find Acces DB Files	Custom Query	sp\administrator	12/3/2020 6:56:...	3
	Home Folder Summary	Custom Query	sp\administrator	12/3/2020 6:57:...	4

[Report Type] = 'Custom Query' Edit Filter

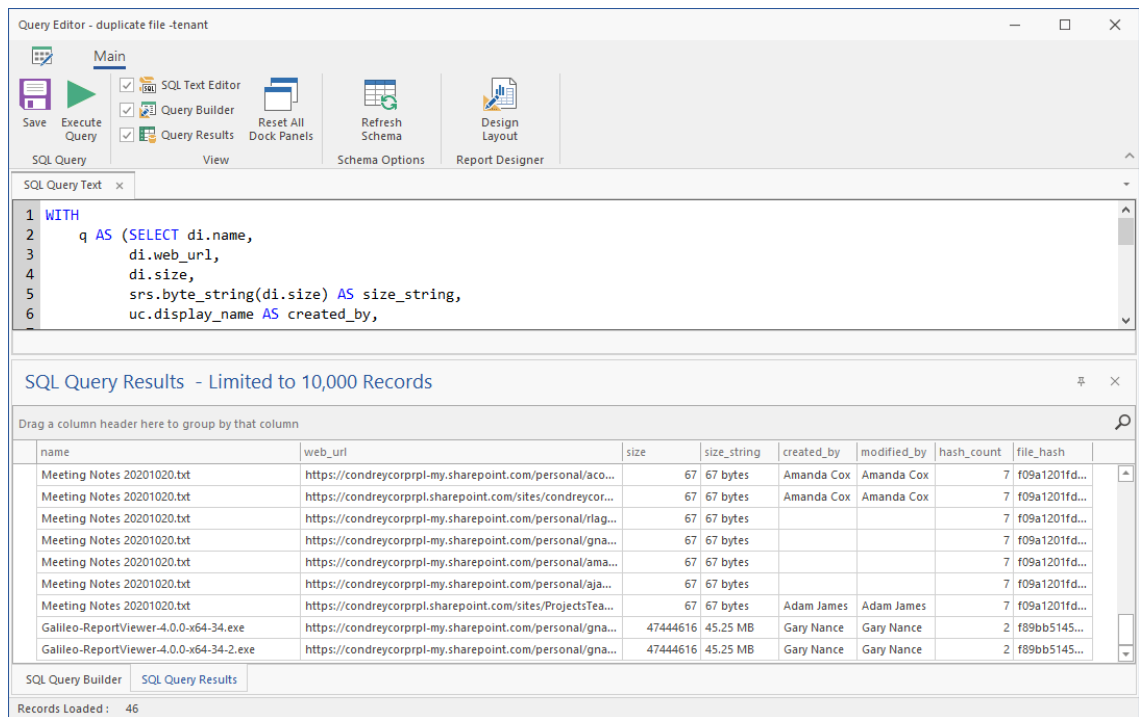
All of your saved Custom Query reports are listed.

5 Click **New Custom Query**, give it a name, then click **Create**.

The Report Designer Query Editor is launched.

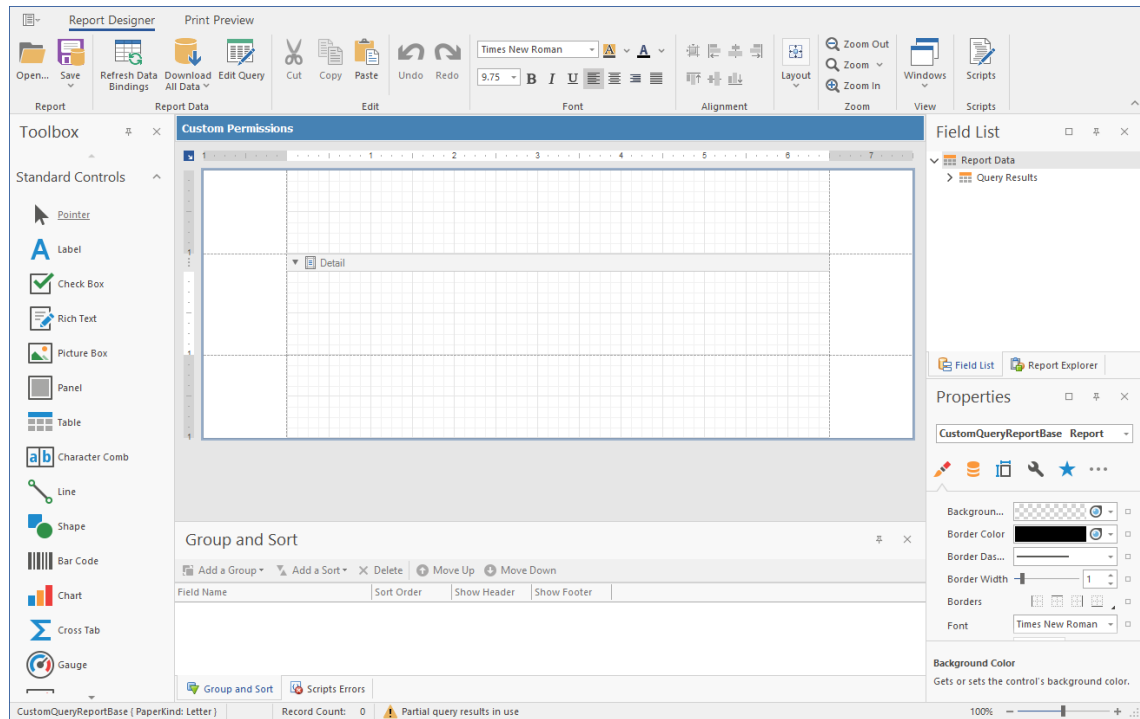


- 6 From the text editor you used in Step 2, copy the custom query and paste it into the Query Editor.
- 7 (Conditional) If there are target paths or other modifications that need to be made for your environment, follow the procedures for the “recipe.”
- 8 Click **Execute** to get a preview in the bottom portion of the editor of how the report will appear.



- 9 Click **Save**.

10 Click Design Layout.



11 Click **Open**.

12 Locate the .REPX file that you saved and unzipped in Step 2 and click **Open**.

The layout template appears in the Report Designer.

13 Click **Download All Data**.

14 In the subsequent dialog box, click **Yes**.

This runs the query in the database and loads data into the report template.

15 Click **Print Preview** to review the report findings.

16 Save the report by doing one of the following:

- ◆ From the **Export To** drop-down menu, select the file type you want to save the report layout to.
- ◆ Click **Save Report** to save the report as a .PNRX file that you can open in the Report Viewer and if you want later, export the report to the desired file type.

6.12 Micro Focus File Dynamics Policy Reports

In most reports, you browse to and specify a file path for the report through the **Target Paths** tab. If you have Micro Focus 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 4.0 supports File Dynamics 6.0 and above.

The advantages 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.

6.13 Scheduling Reports

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**.

Schedule for Atlanta Shares Detailed Date-Age Report ✕

SCHEDULE START

Engine Local Time:*

Engine Local Start Date:*

SCHEDULE RECURRENCE

Once

Daily

Weekly

Monthly

Day of every month

The of every month

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.

6.14 Editing a Scheduled Report

- 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**.

6.15 Clearing a Schedule on a Scheduled Report

- 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**.

6.16 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:

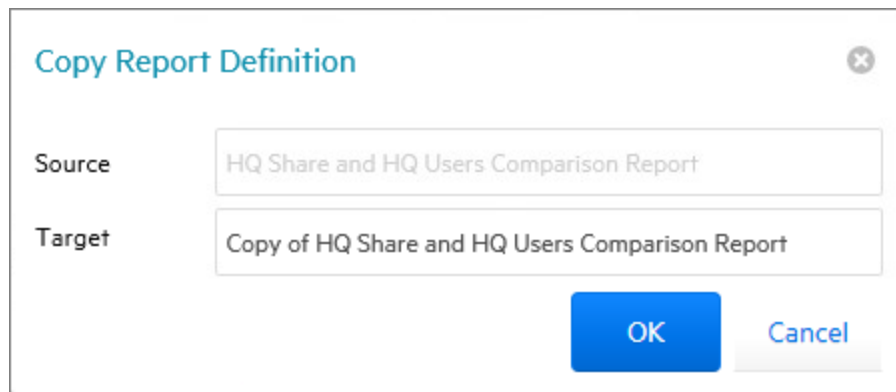
- ♦ Report Parameters
- ♦ Report Targets Paths
- ♦ Report Identity Targets
- ♦ Filters
- ♦ File Dynamics Policies

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**.



Copy Report Definition

Source: HQ Share and HQ Users Comparison Report

Target: Copy of HQ Share and HQ Users Comparison Report

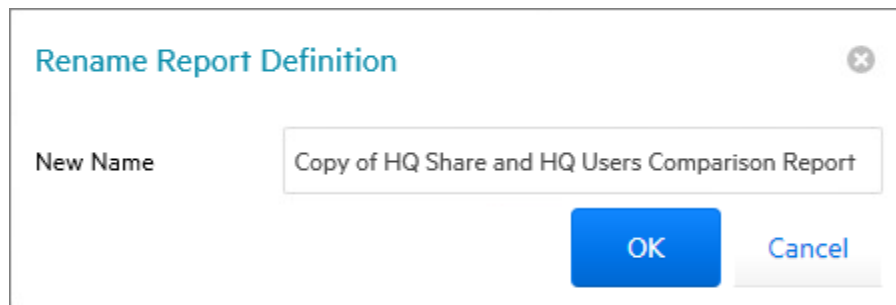
OK Cancel

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**.



Rename Report Definition

New Name: Copy of HQ Share and HQ Users Comparison Report

OK Cancel

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**.

6.17 Viewing 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.

6.18 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 reports include too much data to be useful, narrow the scope of the report by implementing filters. For more information, see [Appendix A, “Filtering for Built-in Reports,”](#) on [page 155](#).

7 Content Scanning and Reporting

In addition to generating file system, permissions, and trending reports, File Reporter customers also have the ability to 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.

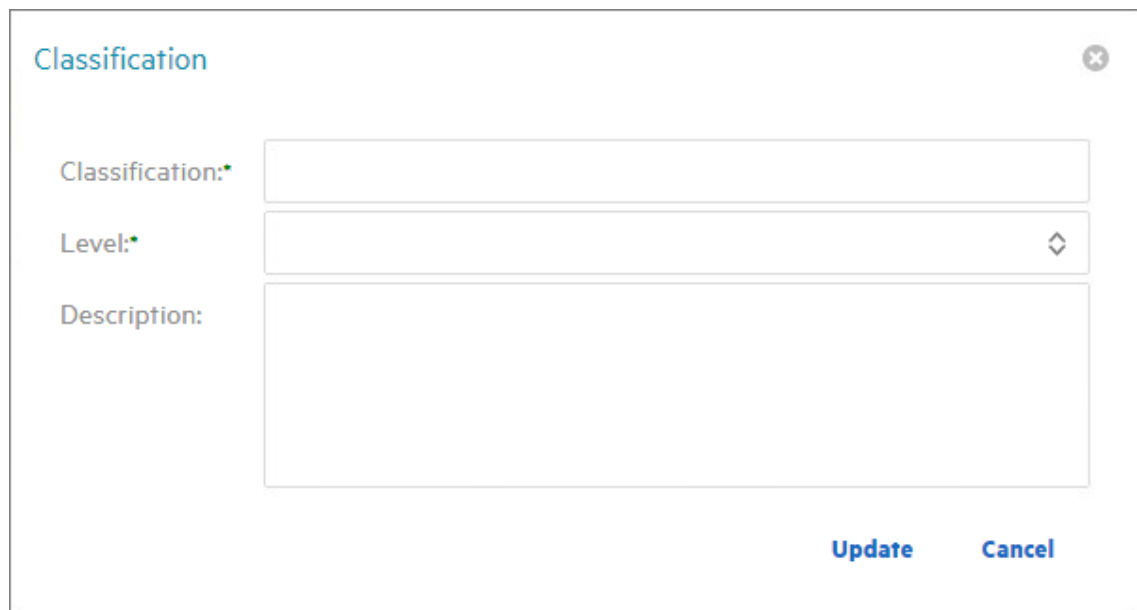
All File Content procedures are performed through the **File Content** menu options.

7.1 Creating 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**.



The screenshot shows a dialog box titled "Classification" with a close button in the top right corner. The dialog contains three input fields: "Classification:" (a text box), "Level:" (a dropdown menu), and "Description:" (a larger text box). At the bottom right, there are "Update" and "Cancel" buttons.

- 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 for public disclosure.

- 6 Click **Update**.

7.1.2 Editing a Classification

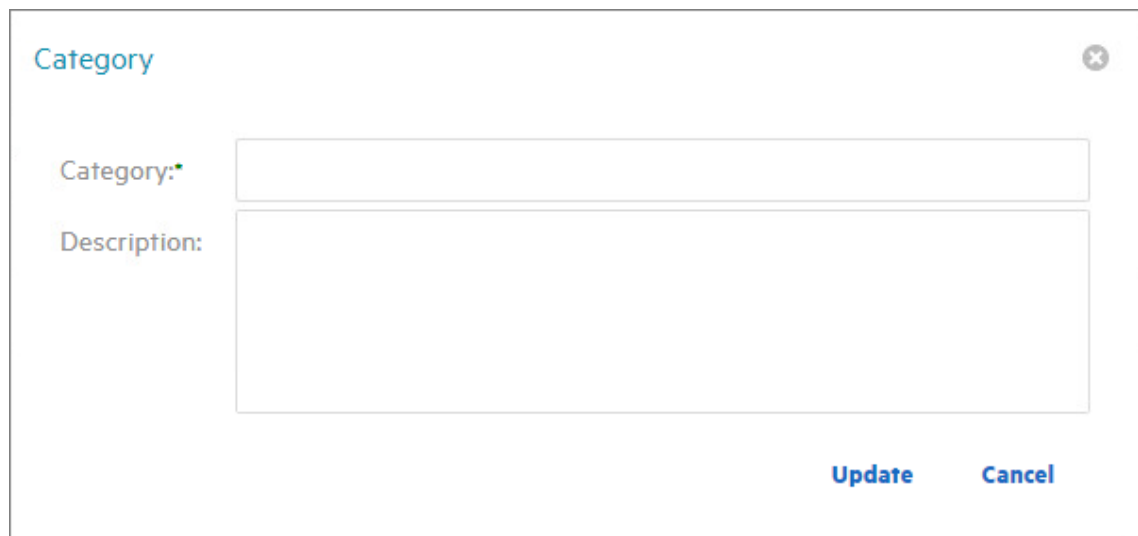
- 1 Select **File Content > Classifications**.
- 2 Select the classification you want to edit.
- 3 Click **Edit**.
- 4 Edit the fields.
- 5 Click **Update**.

7.2 Creating 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**.



The screenshot shows a dialog box titled "Category" with a close button in the top right corner. Inside the dialog, there are two input fields: "Category:" followed by a single-line text box, and "Description:" followed by a multi-line text area. At the bottom right of the dialog, there are two buttons: "Update" and "Cancel".

- 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 SSNs 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**.

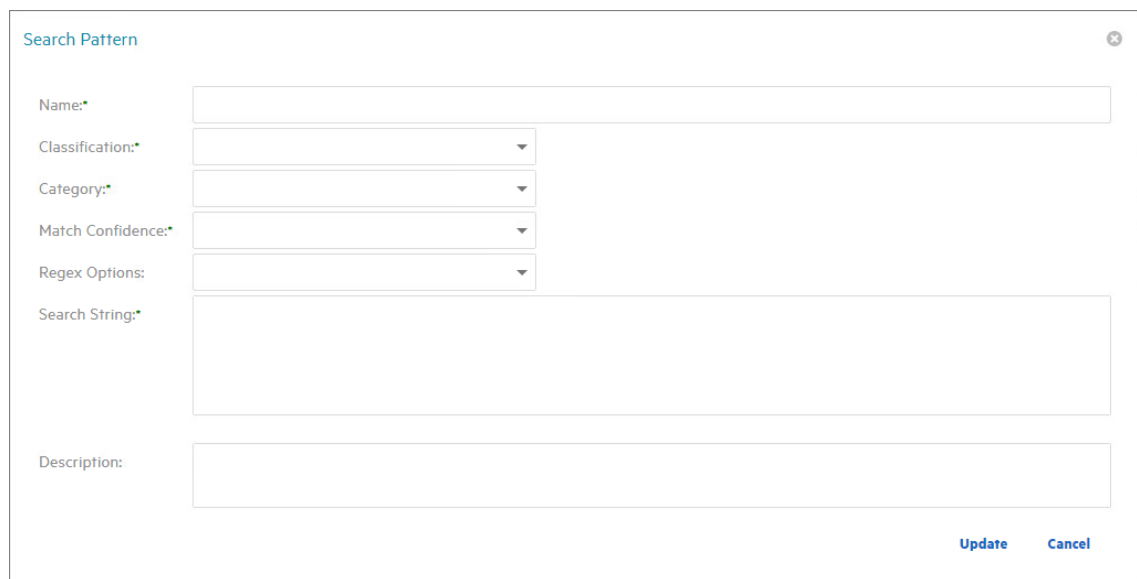
7.3 Creating Search Patterns

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.

7.3.1 Creating a New Search Pattern

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



The screenshot shows a form titled "Search Pattern" with a close button (X) in the top right corner. The form contains the following fields:

- Name:** A text input field.
- Classification:** A dropdown menu.
- Category:** A dropdown menu.
- Match Confidence:** A dropdown menu.
- Regex Options:** A dropdown menu.
- Search String:** A large text area for entering the search pattern.
- Description:** A text input field.

At the bottom right of the form, there are two buttons: **Update** and **Cancel**.

- 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.

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 Creating Job Definitions

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**.

Job Definition

Name: Result Type:

TARGET PATHS **SEARCH PATTERNS** **FILTERS**

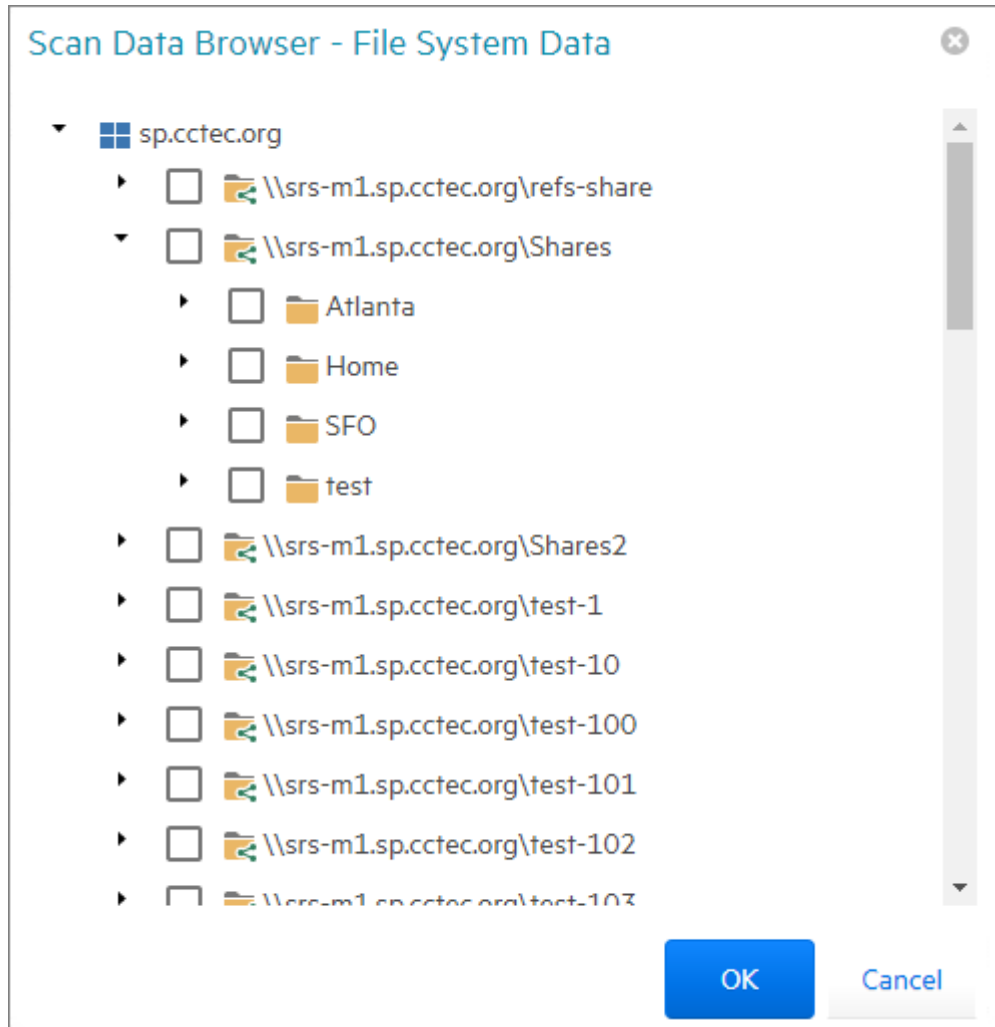
Add Remove

Target

Update Cancel

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

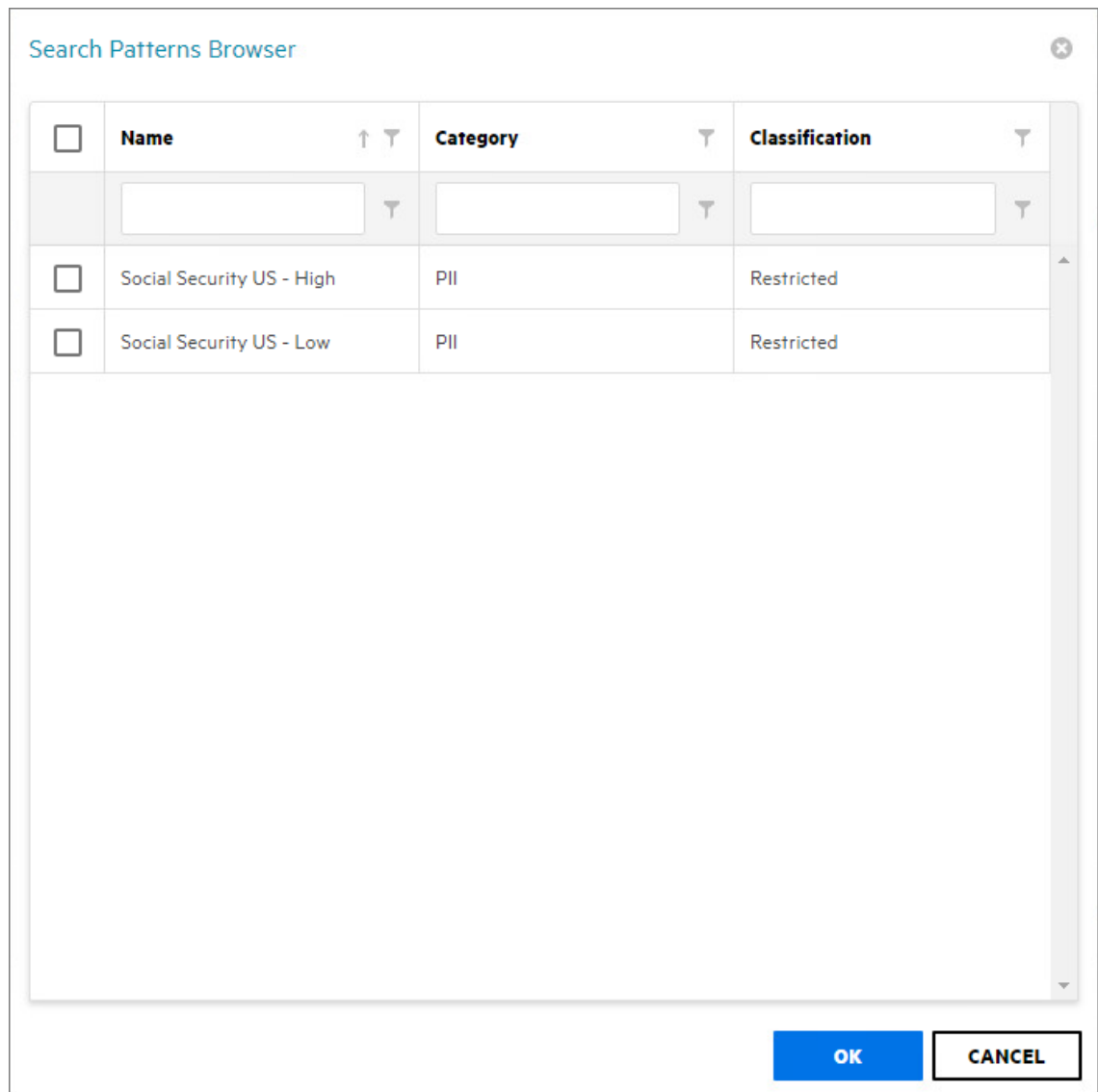
- 4 From the **Result Type** menu, select from the following options:
 - ◆ **Database:** This option saves the results of the content scan to the database, where you can use it to generate a report using the Report Designer. Having the scan in the database also allows you to search and report utilizing 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.

Job Definition ✕

Name: Result Type:

TARGET PATHS **SEARCH PATTERNS** **FILTERS**

Maximum File Size: MB (Value of 0 is unlimited size)

File Extensions:

pptx
ppt
docx
doc
xls
xlsx
pdf
txt
rtf
xps

Enter filename extensions, one per line, without a leading period.

Update **Cancel**

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 Viewing Jobs in Progress

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

The screenshot shows the 'File Content Jobs in Progress' section of the File Reporter 4.0 interface. It features a table with the following columns: Job ID, Job Definition, Files Submitted, Files Processed, Status Code, and Status Message. A single job is listed with Job ID 4, Job Definition 'Amanda Cox', 25 Files Submitted, 25 Files Processed, and a Status Code of 'Processing'. The Status Message is also 'Processing'. The interface includes a 'Refresh' button and a 'Page 1 of 1 (1 items)' indicator at the bottom.

Job ID	Job Definition	Files Submitted	Files Processed	Status Code	Status Message
4	Amanda Cox	25	25	Processing	Processing

7.6 Viewing Scanned Data Jobs

You can view a list of file content scan jobs by selecting **File Content > Scan Data**.

The screenshot shows the 'File Content Scan Data' section of the File Reporter 4.0 interface. It displays a table with columns: Full Path, Scan Time, Classification, Category, Matched Search Pattern, and Confidence. The data is grouped by job definition. Two jobs are shown: 'Job Amanda Cox - 4 (3 entries - Completed)' and 'Job adam james - 3 (1 entries - Completed)'. The Amanda Cox job has three entries with file paths, scan times, classifications (Sensitive), categories (PI), and matched search patterns (acox (2 matches)). The adam james job has one entry with a file path, scan time, classification (Sensitive), category (PI), and matched search pattern (Adam James (1 match)).

Full Path	Scan Time	Classification	Category	Matched Search Pattern	Confidence
Job Amanda Cox - 4 (3 entries - Completed)					
\\ms-m3.sp.octec.org\Shares\Atlanta\employees\lance\New Text Document.txt	11/30/2020 7:51:30 PM	Sensitive	PI	acox (2 matches)	Medium
\\ms-m3.sp.octec.org\Shares\Atlanta\employees\jacob\New Text Document.txt	11/30/2020 7:51:07 PM	Sensitive	PI	acox (2 matches)	Medium
\\ms-m3.sp.octec.org\Shares\Atlanta\employees\jacob\finding names.txt	11/30/2020 7:50:43 PM	Sensitive	PI	acox (2 matches)	Medium
Job adam james - 3 (1 entries - Completed)					
\\ms-m3.sp.octec.org\Shares\Atlanta\employees\jacob\finding names.txt	9/14/2020 1:33:38 PM	Sensitive	PI	Adam James (1 match)	Medium

7.7 Viewing 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.

File Reporter 4.0 Main File Systems File Content Governance Microsoft 365 Reports Configuration SP Administrator

Delete Refresh File Content Search Results

Drag a column header here to group by that column

<input type="checkbox"/>	Result File	Job Status	File Size	Last Modify Time
<input type="checkbox"/>	adam.james-3.csv	Completed	342 bytes	9/14/2020 1:33:38 PM
<input type="checkbox"/>	Amanda Cox-2.csv	Completed	521 bytes	9/14/2020 1:13:41 PM

Page 1 of 1 (2 Items) 1

Copyright 2020 Condrey Corporation

7.8 Viewing AgentFC Configuration Registrations

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

File Reporter 4.0 Main File Systems File Content Governance Microsoft 365 Reports Configuration SP Administrator

Delete Refresh File Content Scan Agents

Drag a column header here to group by that column

<input type="checkbox"/>	Host Name	Version	Last Heartbeat	OS Version	OS Description	Java Version	Tika Version	OCR	Status
<input type="checkbox"/>	<input checked="" type="checkbox"/> sfs-m1.sp.cctec.org	4.0.0.11	11/30/2020 7:53:57 PM	10.0.17763.0	Windows Server 2019 Standard (Build 17763) Release 1809	openjdk version "11.0.7" 2020 OpenJDK Runtime Environment OpenJDK 64-Bit Server VM Ad	Apache Tika 1.24.1	<input type="checkbox"/>	Ready

Create Filter

Copyright 2020 Condrey Corporation

8

Performing Other Administrative Tasks

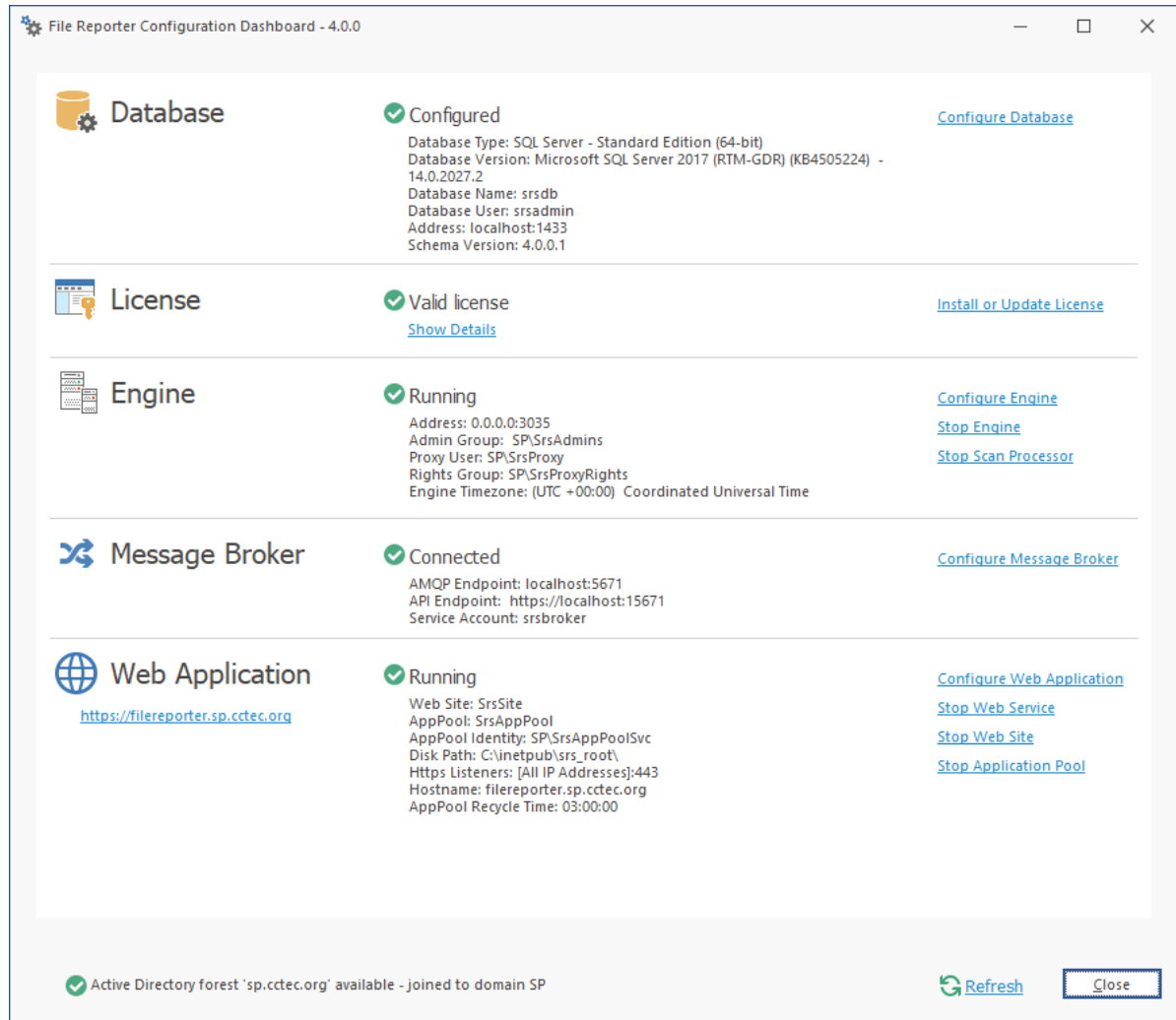
This section provides procedures for performing administrative tasks not covered in the previous sections.

- ♦ [Section 8.1, “Stopping and Restarting Services,” on page 117](#)
- ♦ [Section 8.2, “Using Folder Summary,” on page 118](#)
- ♦ [Section 8.3, “Considerations for Reporting on NAS Devices,” on page 119](#)
- ♦ [Section 8.4, “Changing the Default Path for Stored Reports,” on page 120](#)
- ♦ [Section 8.5, “Changing the Life Span of Stored Reports,” on page 121](#)
- ♦ [Section 8.6, “Resetting the Proxy User Password,” on page 121](#)

8.1 Stopping and Restarting Services

Use the Configuration Dashboard to stop and restart the Engine, Web Application, Web Service, Web Site, and Application Pool.

Figure 8-1 Configuration Dashboard



8.2 Using Folder Summary

The Folder Summary feature provides you 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 8-2 Folder Summary

Path	Scan Start Time	File Size	File Count	Folder Count	Folder Quota	% of Parent Folder Size	% of Total Size
sp-ctec.org	9/24/2020 2:33:09 PM			1,103			
\\sp-ctec.org\share	9/28/2020 7:47:36 PM						
Atlanta		1 GB	30		100	100	
Employees		1 GB	29		100	100	
Files...		1 GB	27		100	100	
Files...		223 bytes	1		0	0	
alex		893 MB	15	1	30	30	
finance		593 MB	11	0	50	50	
areid		0 bytes	0	0	0	0	
stawson		0 bytes	0	0	0	0	
brubors		0 bytes	0	0	0	0	
cedwards		0 bytes	0	0	0	0	
clarkams		0 bytes	0	0	0	0	
clibeth		0 bytes	0	0	0	0	
othomas		0 bytes	0	0	0	0	
jphocod		0 bytes	0	0	0	0	
jhurst		0 bytes	0	0	0	0	
jamilley		0 bytes	0	0	0	0	
sparks		0 bytes	0	0	0	0	
hanson		0 bytes	0	0	0	0	
lones		0 bytes	0	0	0	0	
pdavis		0 bytes	0	0	0	0	
Groups		919 KB	2	11	0	0	
Home		0 bytes	0	6	0	0	
ajames		0 bytes	0	0	0	0	
anance		0 bytes	0	0	0	0	
stark		0 bytes	0	0	0	0	
lbanmer		0 bytes	0	0	0	0	
sparker		0 bytes	0	0	0	0	
soofth		0 bytes	0	0	0	0	
SFO		0 bytes	0	1,063	0	0	
Employees		0 bytes	0	1,000	0	0	
Groups		0 bytes	0	61	0	0	
test		36 bytes	1	0	0	0	
\\sp-ctec.org\share2	9/28/2020 6:43:23 PM						
\\sp-ctec.org\test-1	9/23/2020 6:58:41 PM						
\\sp-ctec.org\test-10	9/23/2020 6:15:24 PM						
\\sp-ctec.org\test-100	9/23/2020 6:15:24 PM						

You can print, save, or export the data as a PDF or XLS file.

8.3 Considerations for Reporting on NAS Devices

File Reporter can report on the contents of Network Attached Storage (NAS) devices. Integration information for reporting on specific NAS device types is found below.

- ◆ Section 8.3.1, “NetApp filer,” on page 119
- ◆ Section 8.3.2, “EMC Isilon,” on page 120
- ◆ Section 8.3.3, “Other NAS Devices,” on page 120

8.3.1 NetApp filer

For a NetApp filer device, 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 rights and privileges to grant on a NetApp filer NAS device.

8.3.2 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.

8.3.3 Other NAS Devices

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

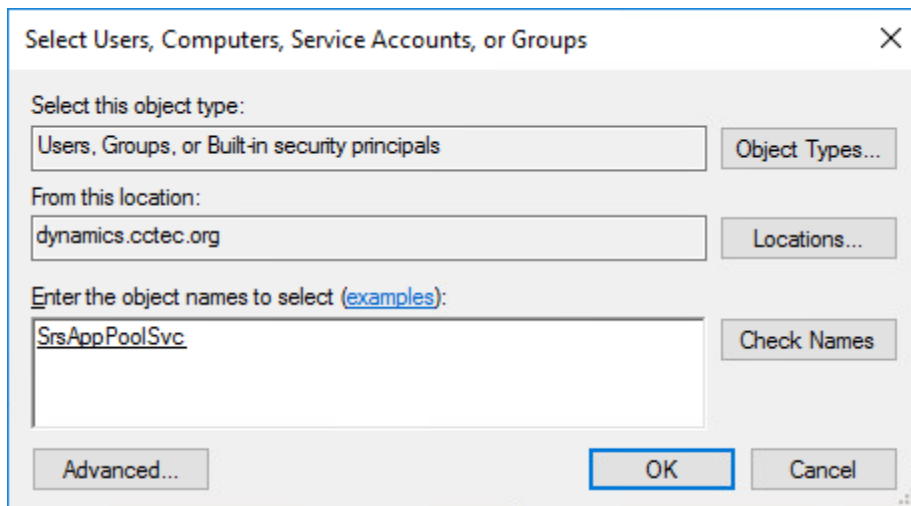
- 1 In the associated Computer object in Active Directory, add the following text somewhere in the description attribute for that object:
`***SRGenericNASDevice***`
- 2 Rebuild the storage resources and verify that the NAS device is displayed on the list.
- 3 Perform any needed steps for giving the proxy rights group access to the desired shares and folders on the NAS device.

8.4 Changing the Default Path for Stored Reports

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:



File Reporter does not move previously generated reports to the new location.

- 1 Select **Configuration > Stored Reports**.
- 2 In the **Stored Reports Folder** field, specify a new path.
- 3 Click **Save Changes**.

8.5 Changing the Life Span of Stored Reports

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**.

8.6 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.

9 Using the Report Viewer

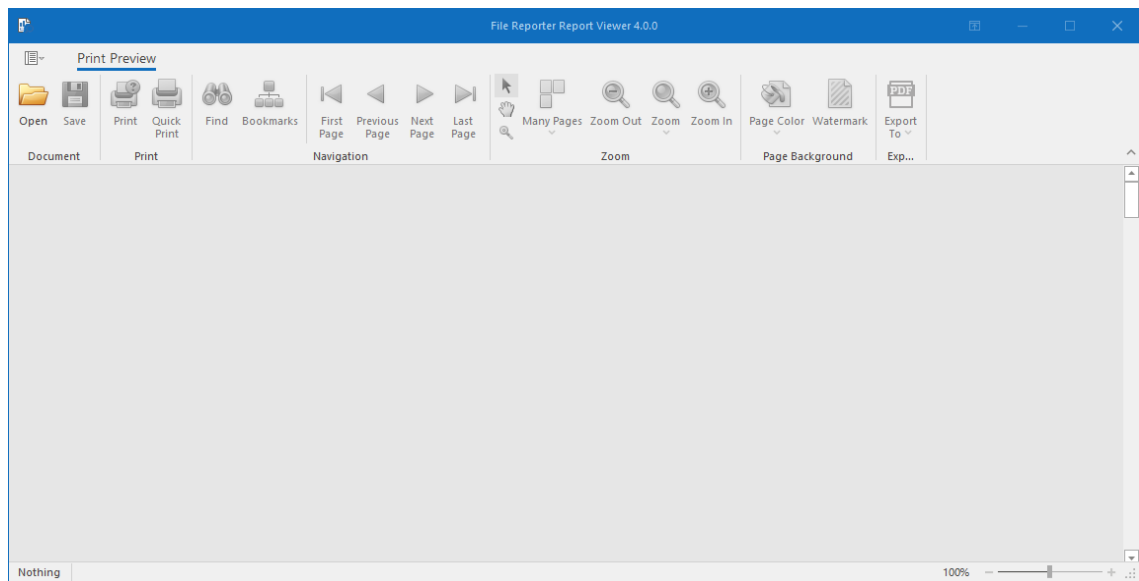
NOTE: The Report Viewer is installed as a separate application, rather than part of the Client Tools. This is so both administrators and other users who need access to the reports can access saved reports.

9.1 Use the Report Viewer

The Report Viewer lets you to 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.

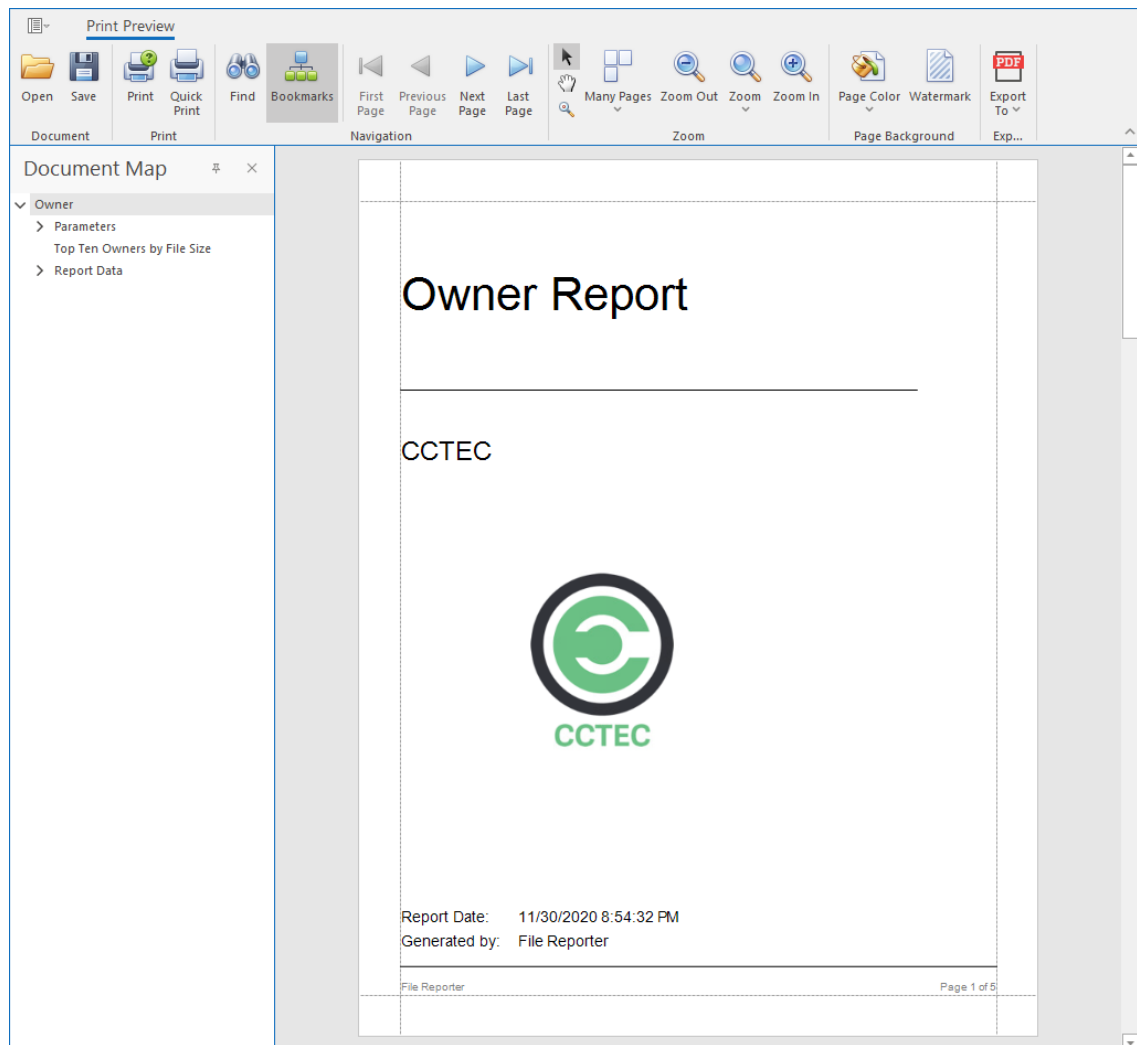
In comparison to the viewing capabilities of the browser-based administrative interface, the Report Viewer offers more capabilities. For example, with the Report Viewer you can change the visual display parameters of the report.

- 1 Launch the File Reporter File Viewer application.



- 2 Click **Open**, browse to the location of your stored reports, then click **Open**.

To determine where stored reports are located, in the File Reporter administrative interface, select **Configuration > Stored Reports** and view the location in the **Stored Reports Folder** field.



3 (Optional) Adjust the view to your preferences using the tools discussed below.

Bookmarks: Click to toggle between the report **Document Map** being displayed and not displayed.

Many Pages: Click to specify the number of pages you want displayed.

Zoom Out: Click to see more of the report page at a reduced size.

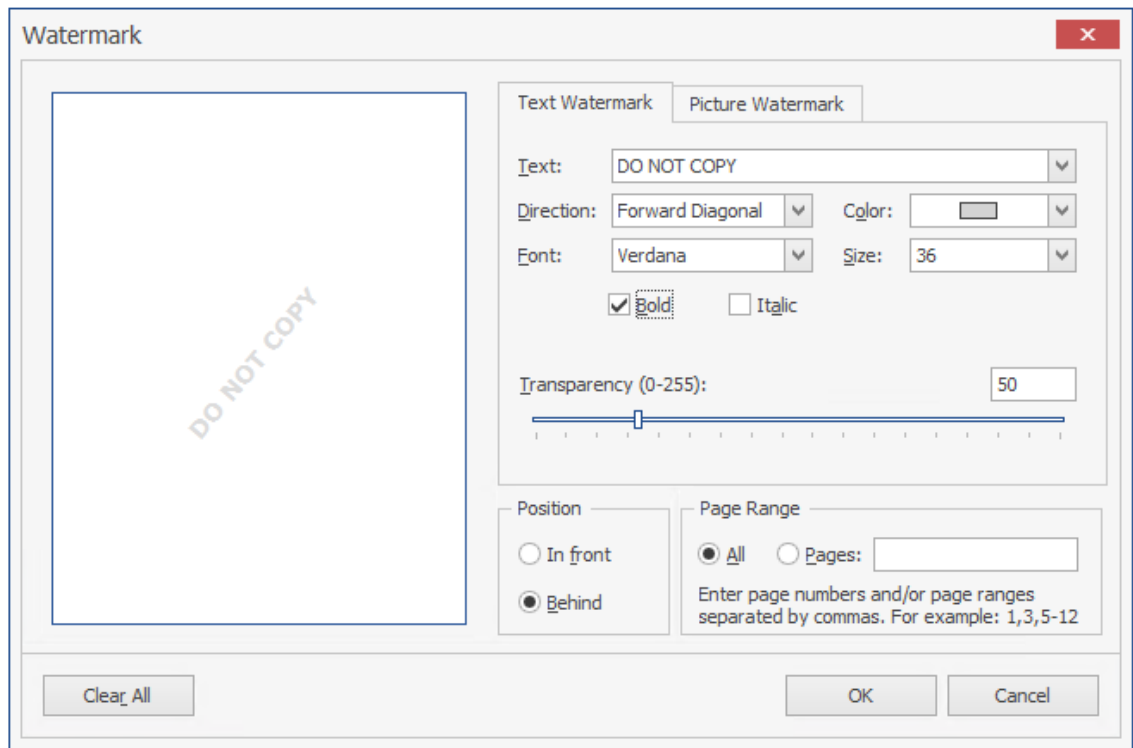
Zoom: Click to change the zoom level of the report preview.

Zoom In: Click to get a close-up view of the report.

Page Color: Click to change the color for the background of the report pages.

Watermark: Click to insert a ghosted text or image behind the content of each page of the report. A watermark is often used to indicate how a document is to be treated specifically.

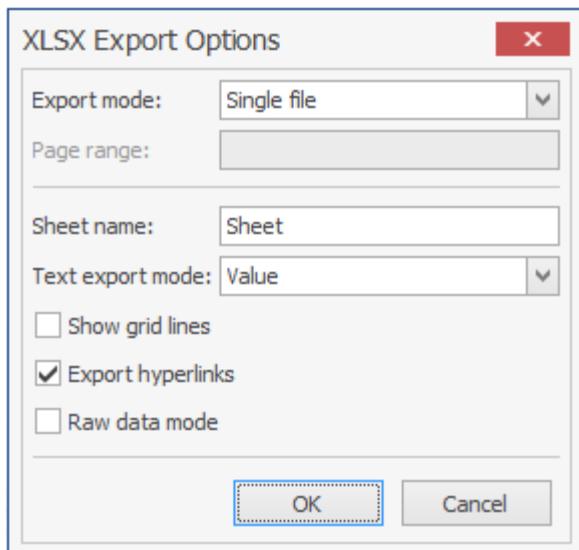
The Watermark dialog box lets you specify your watermark settings. Your watermark can either be in text or graphic form.



4 (Optional) Save the Report using the tools discussed below.

Save: Click to save the report. The report is saved as a .PNRX file, meaning that in this format, the report can only be opened through the Report Viewer.

Export To: Click to export the report to a new format. Each selected format option brings up a dialog box where you can provide specifics on how you want the report exported.



10 Using the Data Analytics Tools

The Micro Focus File Reporter Client Tools are designed to provide members of the administrators group expanded abilities in analyzing data and designing reports. The Client Tools are run from a Windows workstation.

The analytics tools are an integrated set of data visualization applications that include a Dashboard, Pivot Grid, and Tree Map.

The Report Designer allows you to design reports locally from a Windows workstation while offering significantly more reporting design capabilities to those of the browser-based administrative interface.

- ♦ [Section 10.1, “Launching the Analytics Tools,” on page 127](#)
- ♦ [Section 10.2, “Using the Dashboard,” on page 129](#)
- ♦ [Section 10.3, “Using the Tree Map,” on page 131](#)
- ♦ [Section 10.4, “Using the Pivot Grid,” on page 132](#)

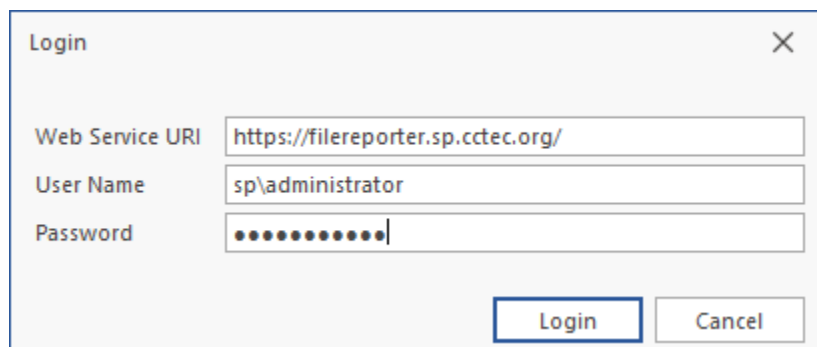
10.1 Launching the Analytics Tools

These procedures briefly introduce you to some of the capabilities of each of the applications. You will discover more capabilities as you work with each of the applications on your own.

- 1 From the **Start** menu, select **File Reporter 4.0 Data Analytics**.

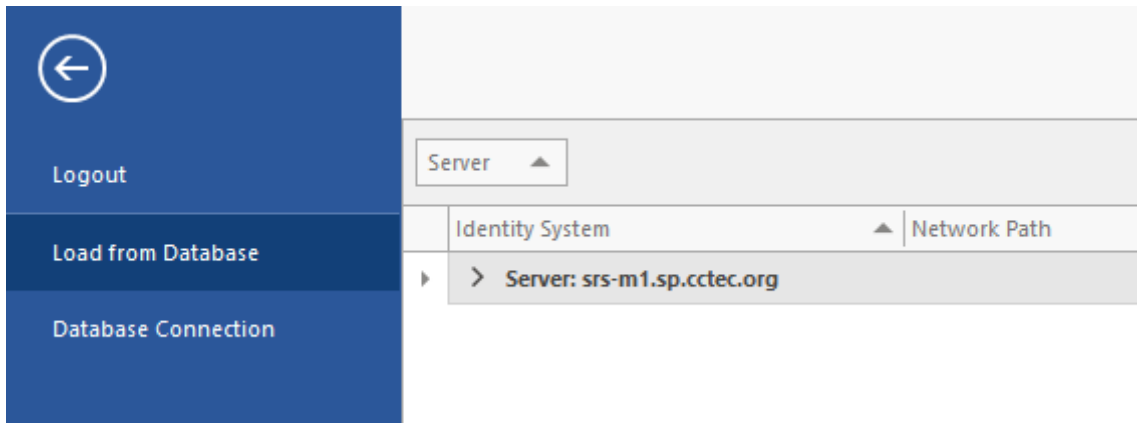
The following login screen appears:

- 2 Enter your login credentials and click **Login**.



The screenshot shows a standard Windows-style dialog box titled "Login". It features a close button (X) in the top right corner. The dialog contains three text input fields: "Web Service URI" with the text "https://filerreporter.sp.cctec.org/", "User Name" with the text "sp\administrator", and "Password" with masked characters represented by a series of dots. At the bottom right of the dialog, there are two buttons: "Login" and "Cancel".

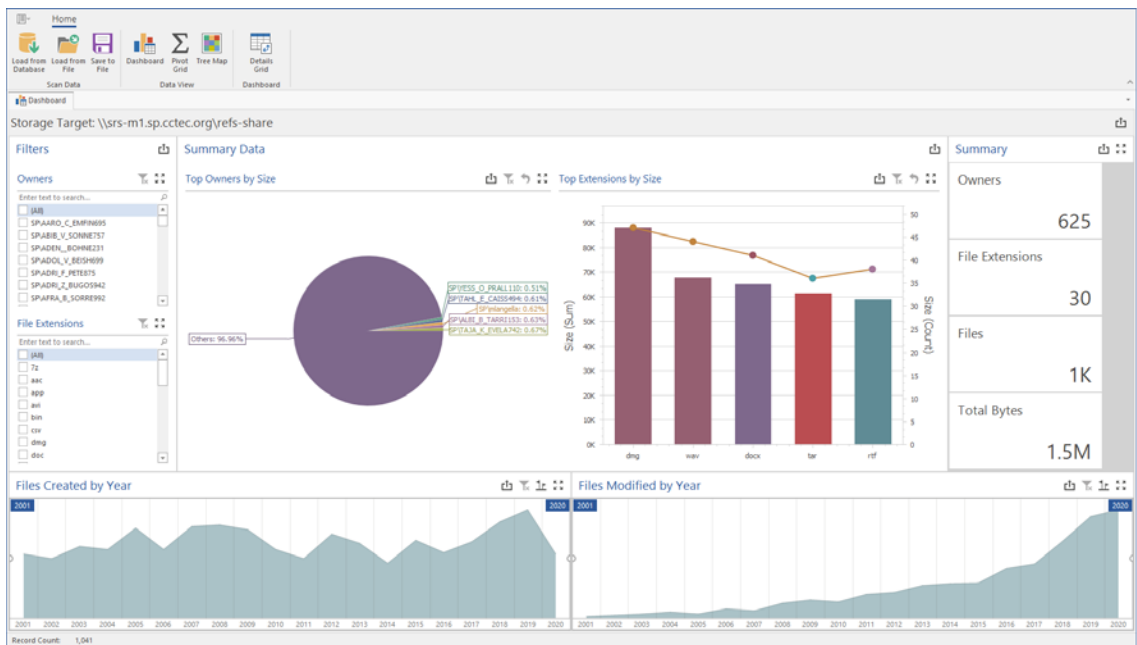
A selection dialog box similar to the following appears:



3 Expand the shares and volumes.

Identity System	Network Path
Server: srs-m1.sp.ctec.org	
sp.ctec.org	\\srs-m1.sp.ctec.org\refs-share
sp.ctec.org	\\srs-m1.sp.ctec.org\Shares
sp.ctec.org	\\srs-m1.sp.ctec.org\Shares
sp.ctec.org	\\srs-m1.sp.ctec.org\Shares2
sp.ctec.org	\\srs-m1.sp.ctec.org\Shares2

4 Double-click the File System scan you want to analyze.
The data from the scan is presented in the Dashboard.



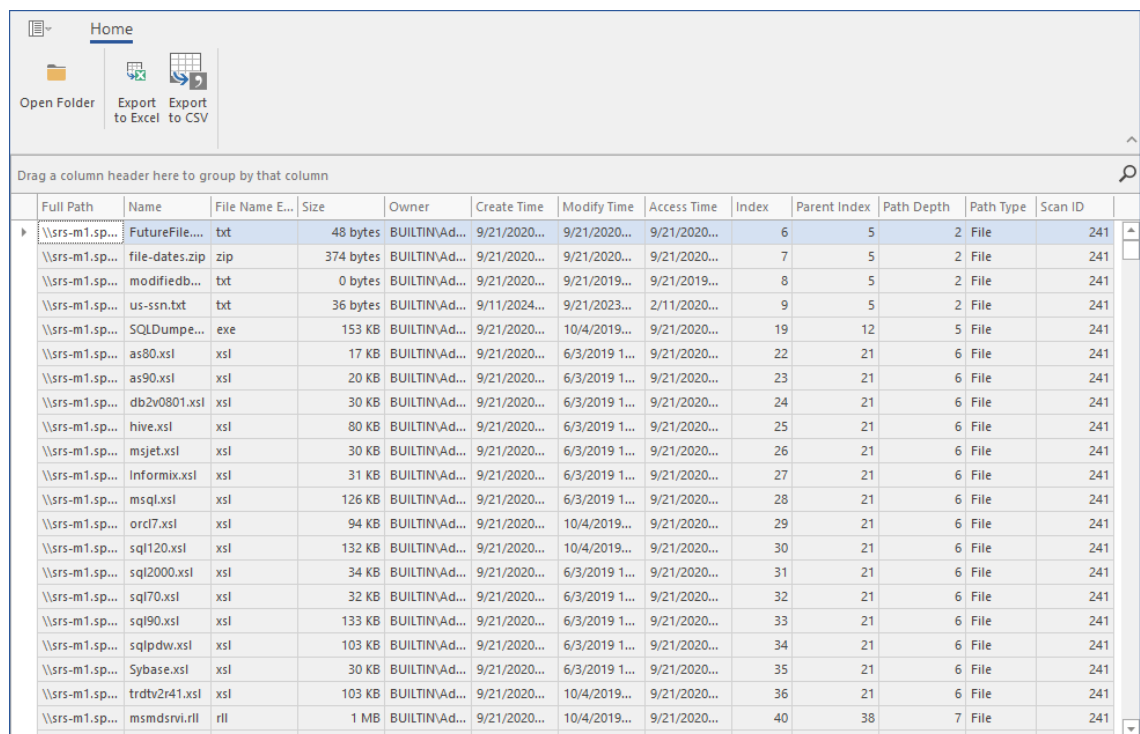
10.2 Using the Dashboard

NOTE: The exercises in the remainder of this chapter introduces you to some of the very basic analytical features of the Analytics Tools. Through familiarizing yourself with these basic features, you will become proficient enough with these tools to try more advanced features.

- 1 In the **Filters** region of the Dashboard, deselect one or two of the check boxes and observe how the changes are reflected in the **Summary Data**, **Top Extensions by Size**, and **Summary** regions of the Dashboard.
- 2 In the **Files Created by Year** region, click a specific year.
- 3 Observe the changes in the **Summary Data**, **Top Extensions by Size**, and **Summary** regions of the Dashboard.

The graphical displays in the **Summary Data**, **Top Extensions by Size**, and **Summary** regions of the Dashboard are driven by the **Filters** region and the selected years from the **Files Created by Year** and **Files Modified by Year** regions.

- 4 In the **Summary Data** region, place the cursor over a pie graph section and observe how sectional-specific information appears in a balloon.
- 5 Double-click the pie graph section and observe how the Dashboard drills down to show data specific to the selected section in the **Summary Data**, **Top Extensions by Size**, and **Summary** regions.
- 6 Right-click a section of the new pie graph and select **Details Grid** to view the individual filenames.



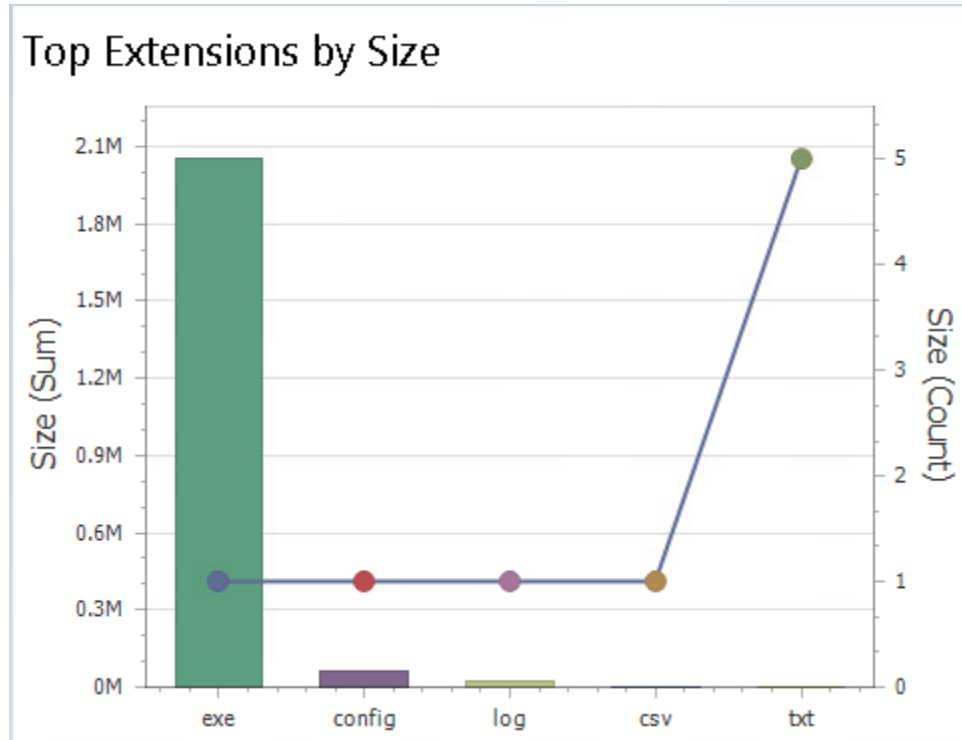
	Full Path	Name	File Name Extension	Size	Owner	Create Time	Modify Time	Access Time	Index	Parent Index	Path Depth	Path Type	Scan ID
▶	\\srs-m1.sp...	FutureFile...	txt	48 bytes	BUILTIN\Ad...	9/21/2020...	9/21/2020...	9/21/2020...	6	5	2	File	241
	\\srs-m1.sp...	file-dates.zip	zip	374 bytes	BUILTIN\Ad...	9/21/2020...	9/21/2020...	9/21/2020...	7	5	2	File	241
	\\srs-m1.sp...	modifiedb...	txt	0 bytes	BUILTIN\Ad...	9/21/2020...	9/21/2019...	9/21/2019...	8	5	2	File	241
	\\srs-m1.sp...	us-ssn.txt	txt	36 bytes	BUILTIN\Ad...	9/11/2024...	9/21/2023...	2/11/2020...	9	5	2	File	241
	\\srs-m1.sp...	SQLDumpe...	exe	153 KB	BUILTIN\Ad...	9/21/2020...	10/4/2019...	9/21/2020...	19	12	5	File	241
	\\srs-m1.sp...	as80.xsl	xsl	17 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	22	21	6	File	241
	\\srs-m1.sp...	as90.xsl	xsl	20 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	23	21	6	File	241
	\\srs-m1.sp...	db2v0801.xsl	xsl	30 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	24	21	6	File	241
	\\srs-m1.sp...	hive.xsl	xsl	80 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	25	21	6	File	241
	\\srs-m1.sp...	msjet.xsl	xsl	30 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	26	21	6	File	241
	\\srs-m1.sp...	Informix.xsl	xsl	31 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	27	21	6	File	241
	\\srs-m1.sp...	msql.xsl	xsl	126 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	28	21	6	File	241
	\\srs-m1.sp...	orcl7.xsl	xsl	94 KB	BUILTIN\Ad...	9/21/2020...	10/4/2019...	9/21/2020...	29	21	6	File	241
	\\srs-m1.sp...	sql120.xsl	xsl	132 KB	BUILTIN\Ad...	9/21/2020...	10/4/2019...	9/21/2020...	30	21	6	File	241
	\\srs-m1.sp...	sql2000.xsl	xsl	34 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	31	21	6	File	241
	\\srs-m1.sp...	sql70.xsl	xsl	32 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	32	21	6	File	241
	\\srs-m1.sp...	sql90.xsl	xsl	133 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	33	21	6	File	241
	\\srs-m1.sp...	sqlpdw.xsl	xsl	103 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	34	21	6	File	241
	\\srs-m1.sp...	Sybase.xsl	xsl	30 KB	BUILTIN\Ad...	9/21/2020...	6/3/2019 1...	9/21/2020...	35	21	6	File	241
	\\srs-m1.sp...	trdtv2r41.xsl	xsl	103 KB	BUILTIN\Ad...	9/21/2020...	10/4/2019...	9/21/2020...	36	21	6	File	241
	\\srs-m1.sp...	msmdsrvi.rll	rll	1 MB	BUILTIN\Ad...	9/21/2020...	10/4/2019...	9/21/2020...	40	38	7	File	241

- 7 From the grid, right-click a file and select **Open Folder** to open the folder where the file is located.

The Dashboard gives you the ability to easily access any files you might want to know about.

- 8 Close the grid.
- 9 Drill up to the originally displayed data by clicking the Drill Up arrow pertaining to the **Summary Data** region of the Dashboard.
- 10 In the **Top Extensions by Size** region, place the cursor over one of the bars and observe how sectional-specific information appears in a balloon.
- 11 In the **Top Extensions by Size** region, right-click and select **Export to Image**.
- 12 Save the image to a location on your desktop.

The graphic can now be used in a presentation or report.

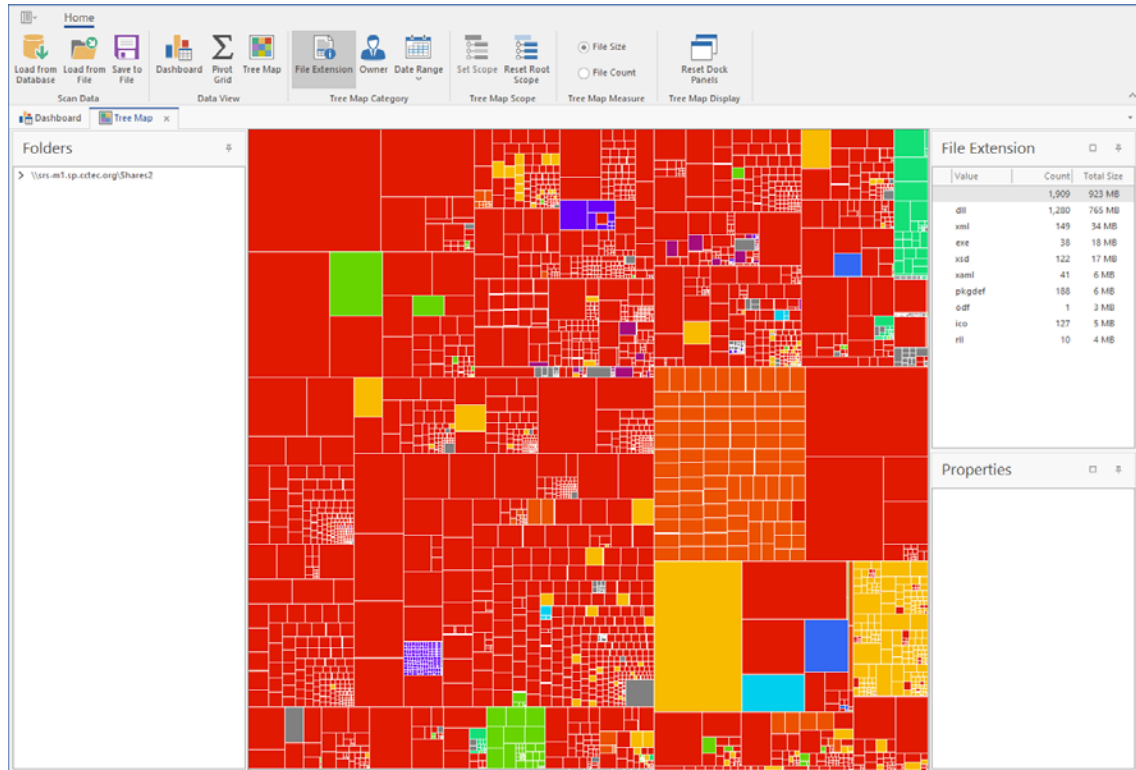


- 13 In the **Files Created by Year** region, double-click a year span and observe how the displayed data in the other regions is updated to data pertaining to the selected year.
- 14 Right-click the selected year span and select **Clear Master Filter** to have the graph span all of the years again.
- 15 In the **Files Modified by Year** region, double-click a year span and observe the change in the displayed data in the Dashboard.
- 16 Place the cursor over a bar in the **Top Extensions by Size** region, right-click and select **Print Preview**.
- 17 Observe that in addition to printing, you can save the graph as a PDF or email the graph.
- 18 Close the Print Preview page.

10.3 Using the Tree Map

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

- 1 From the Dashboard, click **Load from Database**.
- 2 Browse to select the file system scan you want and double-click it.
- 3 Click **Tree Map**.



- 4 Observe how the Tree Map is presented according to file extension type with the specific color assignments detailed in the **File Extension** region.
Each of the squares in the Tree Map represents a single file in the scanned storage resource. The squares are represented according to the file size, relative to all of the other files in the scan.
- 5 Click one of the larger squares to view the details of the file in the **Properties** region.
- 6 Right-click the file and select **Open Parent Folder** to open the folder where the file resides.
This gives you the ability to easily access any files you might want to know more about.
- 7 Expand the file system so it is displayed in the **Folders** region.
- 8 Click one of the folders to see the group of files that reside in that folder.
The files belonging to a selected folder are outlined by a magenta colored outline.
- 9 Right-click a folder and select **Set Scope** to drill down and view the contents of the folder in the Tree Map.
- 10 In the **Folders** region, right click the listed scan and select **Reset Root Scope**.
- 11 Click **Owner**.

The Tree Map now displays files according to owners.

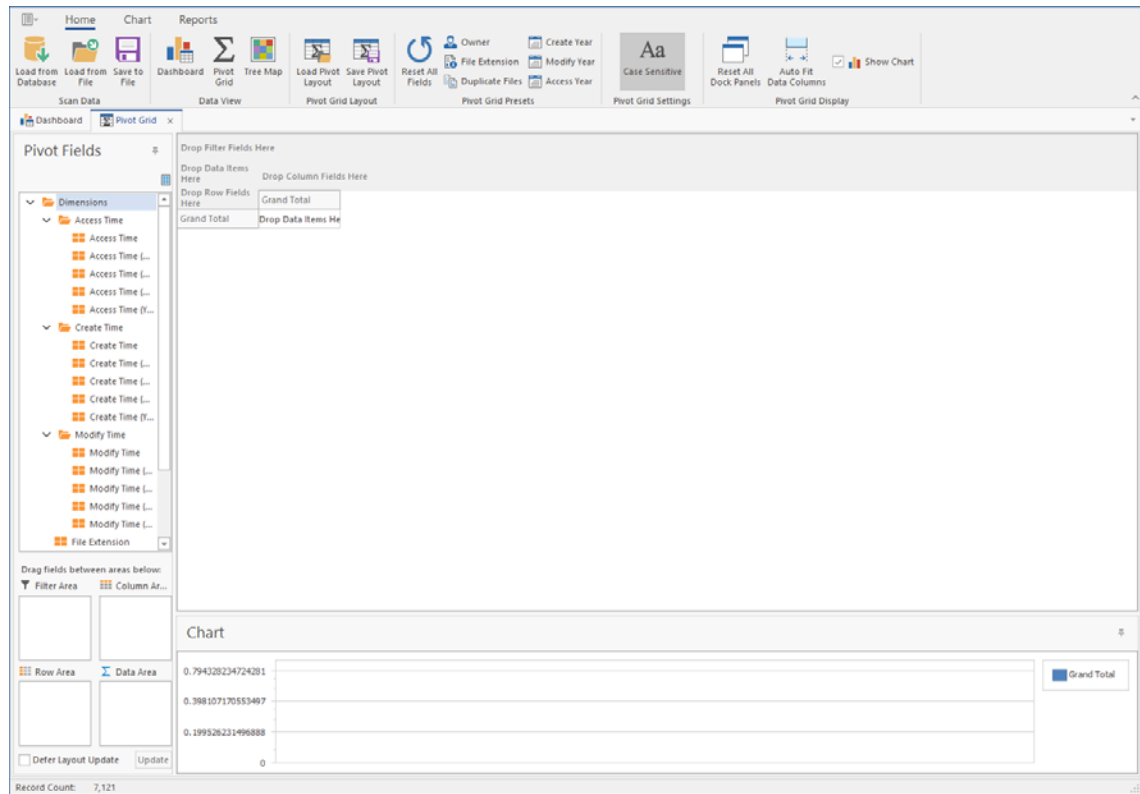
- 12 Using the color classifications in the **Owner** region, observe which users are storing the largest files.
- 13 Click **Date Range > Access Date**.
- 14 Observe how the data in the Tree Map is now classified according to when files were last accessed.

This is one of the most powerful means in File Reporter of quickly determining the relevance of data being stored on network storage resources.

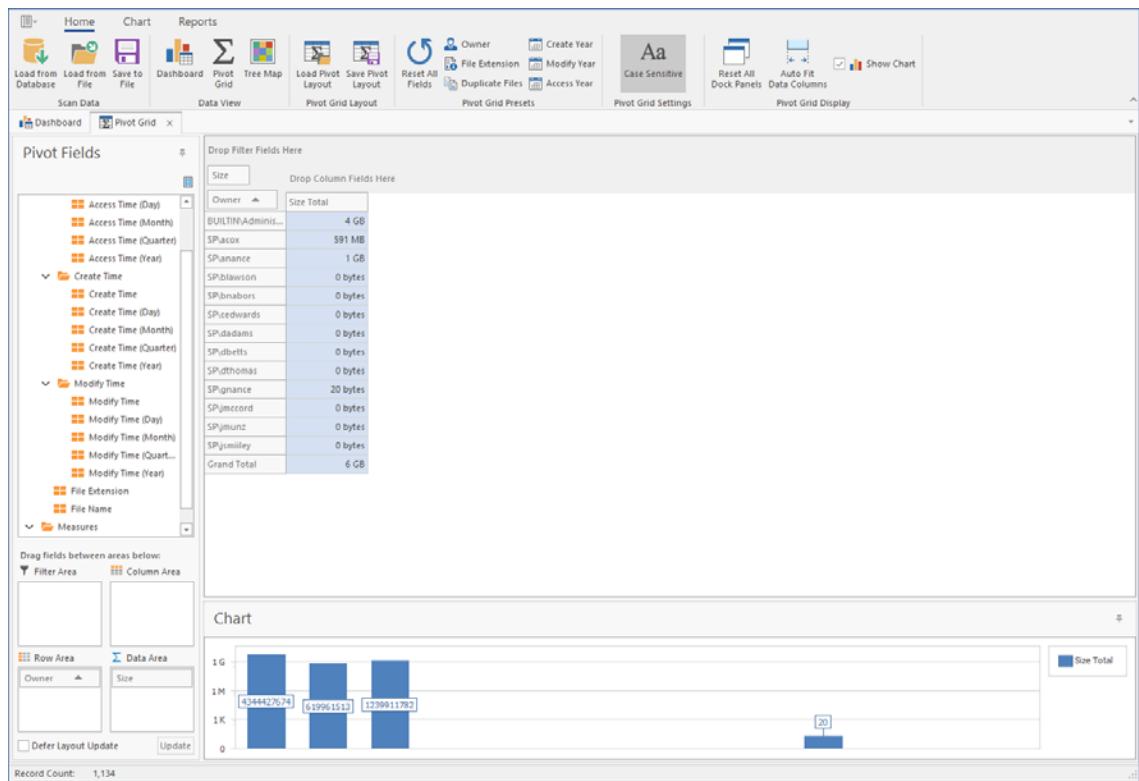
10.4 Using the Pivot Grid

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

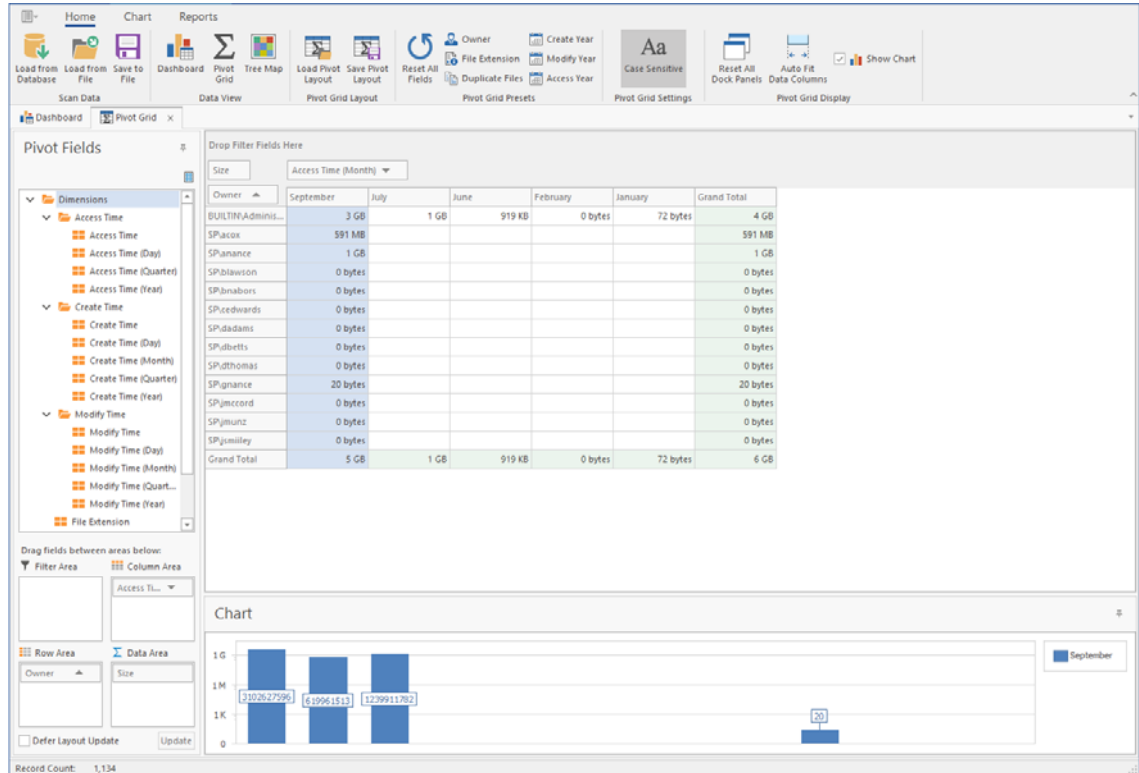
- 1 From the Dashboard, click **Load from Database**.
- 2 Browse to select the file system scan you want and double-click it.
- 3 Click **Pivot Grid**.



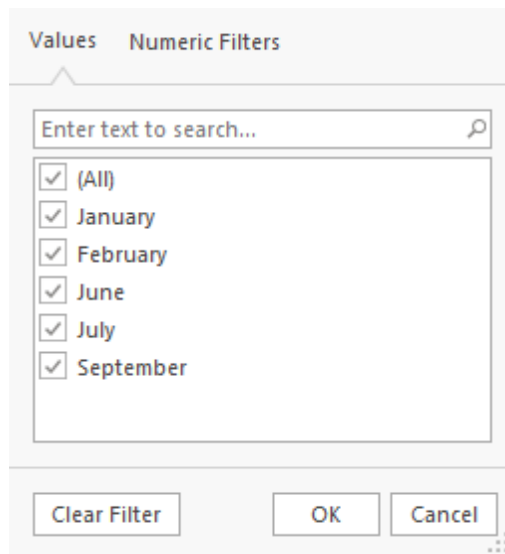
- 4 From the **Pivot Fields** region, select **Size** (residing in the **Measures** folder) and drag it up to the area marked **Drop Data Items**.
- 5 Again in the **Pivot Fields** region, select **Owner** and drag and place it in the area marked **Drop Row Fields Here**.
- 6 Observe the totals now calculated for the two data variables.



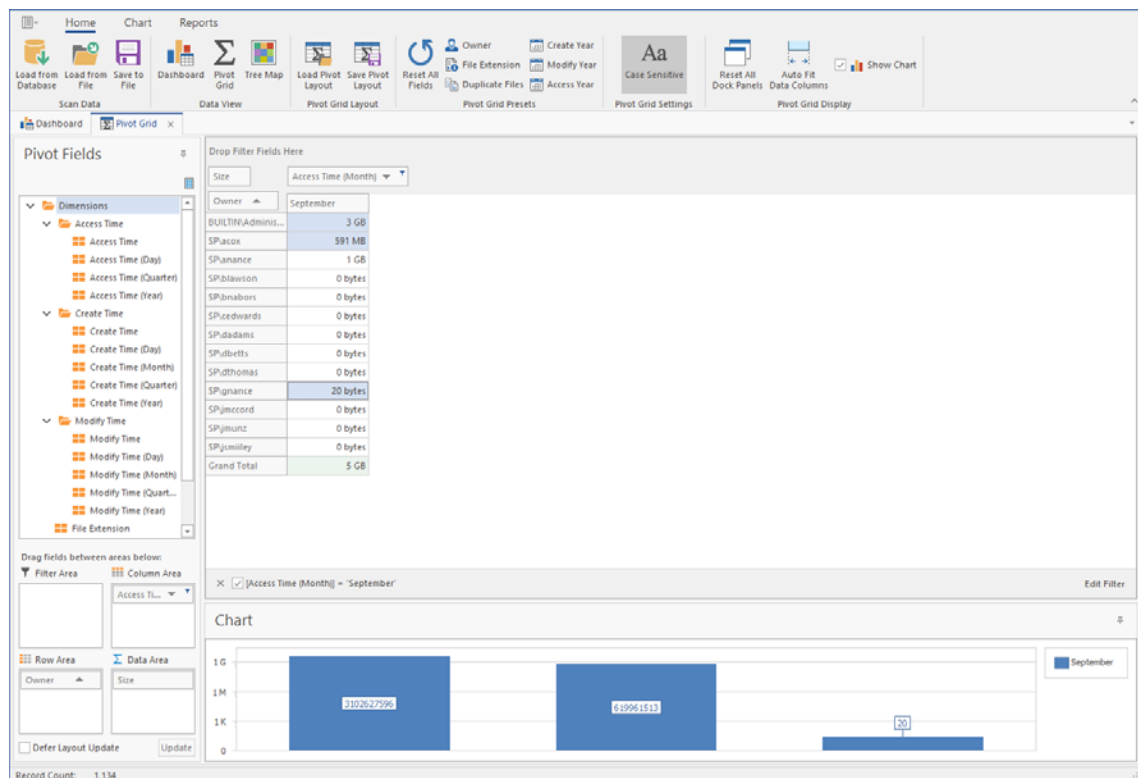
7 From the Pivot Fields region, expand Access Time to locate Access Time (Month) and drag it up to the area marked Drop Column Fields Here.



8 Click the filter icon from the Access Time (Month) filter that you just placed.



- 9 Deselect all but one month and **OK**.
- 10 Click the **Chart** tab.
- 11 Highlight three consecutive rows to view the data analyzed as graphs in the **Chart** region.



- 12 From the **Chart Presets** options, experiment with different chart views of the data.
- 13 Double-click a selected cell from the table to access the Scan Data Details table specifying all of the files accessed by that user during that month.
- 14 From the Scan Data Details table, right-click a file and select **Open Folder** to open the parent folder of the file.

With the parent folder open, you can examine the file, move it to another location, or delete it.

- 15 Click the **Reports** tab.
- 16 Again, highlight three consecutive rows.
- 17 Click **Generate Report**.
- 18 Observe that you have the option to print the report or export it to a number of different formats.

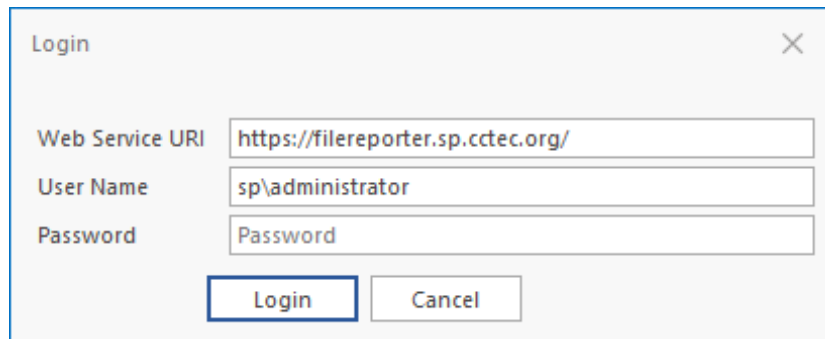
11 Using Report Designer

Report Designer allows you to design reports locally from a Windows workstation while offering significantly more reporting design capabilities to those of the browser-based administrative interface.

11.1 Using the Report Designer Interface

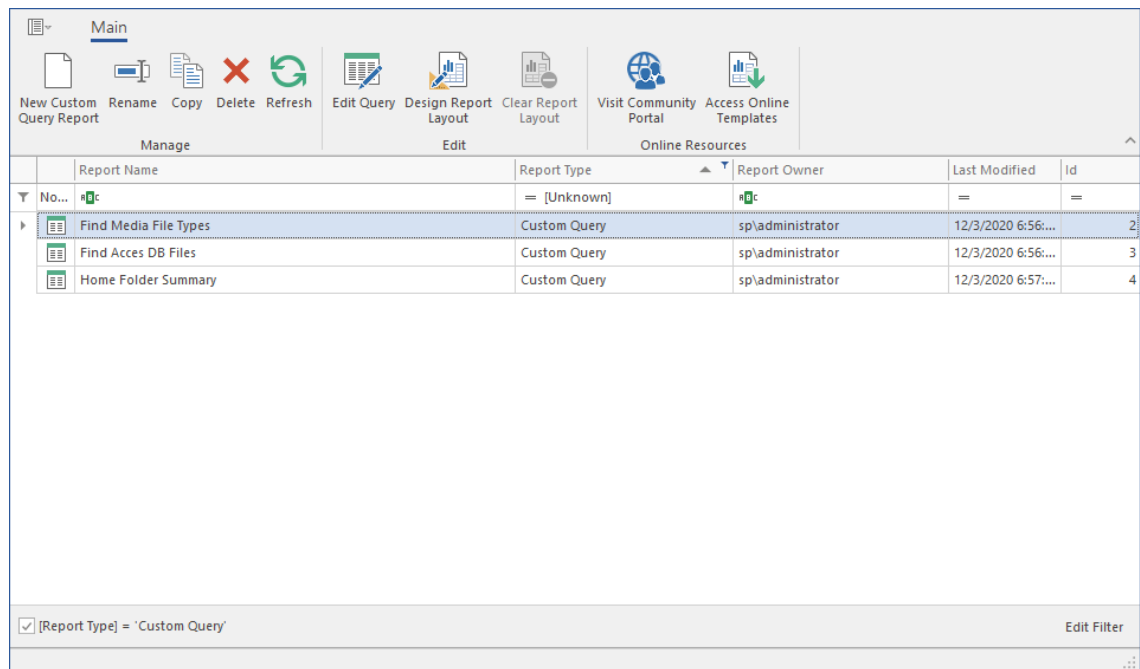
NOTE: You must be a member of the SrsAdmins group to design reports using Report Designer. The name SrsAdmins is the default name (which you can change) of the File Reporter administrators group created during the installation of the Engine.

- 1 From the **Start** menu, launch the **File Reporter 4.0 Report Designer**.



The screenshot shows a standard Windows-style dialog box titled "Login". It features a close button (X) in the top right corner. Below the title bar, there are three text input fields. The first field is labeled "Web Service URI" and contains the text "https://filereporter.sp.ctec.org/". The second field is labeled "User Name" and contains "sp\administrator". The third field is labeled "Password" and contains "Password". At the bottom of the dialog, there are two buttons: "Login" and "Cancel".

- 2 Enter the login credentials and click **Login**.



3 Familiarize yourself with the Report Designer interface.

All Custom Query Reports are listed. Those that have *not* been designed using the Report Designer Layout interface are displayed with the green-bannered text icon, while those designed using the Report Designer have the blue notebook icon.

All of the options on the toolbar are available by selecting a report and right-clicking.

New Custom Query Report: Click to create a new Custom Query Report by launching the Query Editor.

Rename: Click to rename a selected Custom Query Report.

Copy: Click to create a copy of the report definition of a selected report.

Delete: Click to delete a selected Custom Query Report.

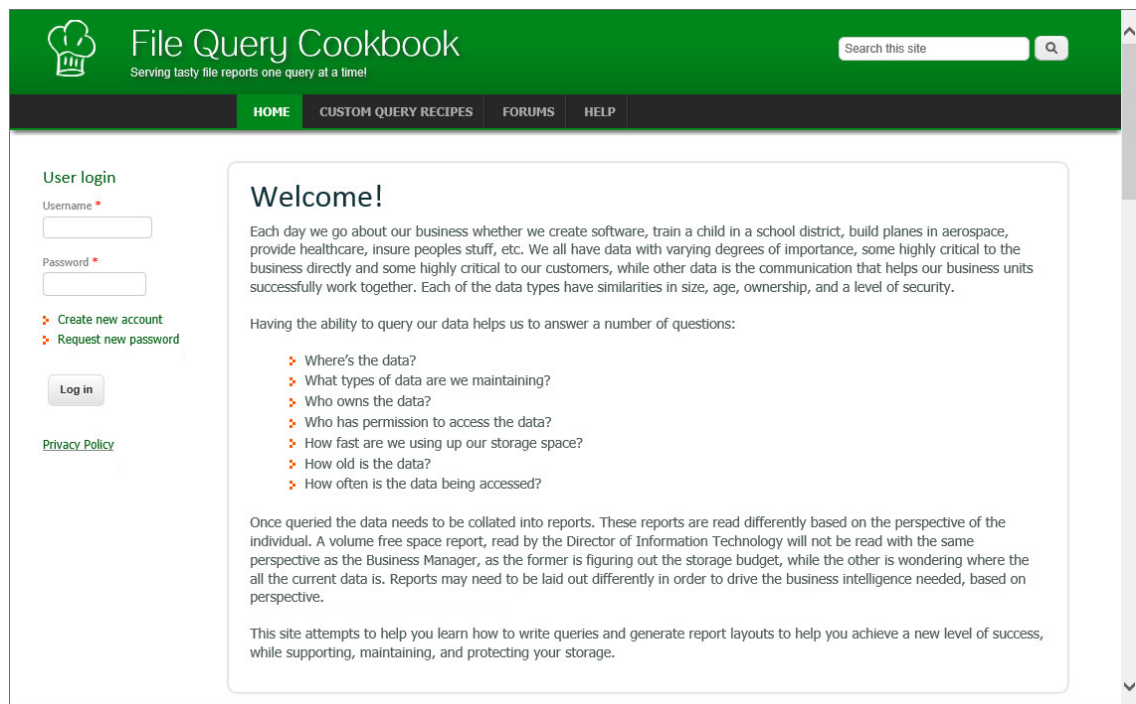
Refresh: Click to refresh the list of saved reports.

Edit Query: Click to edit the SQL commands pertaining to a selected Custom Query Report through the Report Designer's Query Editor.

Design Report Layout: Launches the Report Designer Layout interface. For more information on the Report Designer Layout interface, see [Section 11.3, "Designing a Custom Query Report," on page 142](#).

Clear Report Layout: Click to clear custom design settings created using the Report Designer Layout interface. This is a nonreversible procedure.

Visit Community Portal: Click to access the File Query Cookbook website.



File Query Cookbook is a community website for sharing Custom Query reports and layouts created through the Report Designer. You can utilize a shared Custom Query report by simply copying the SQL commands in a shared Custom Query report “recipe.” You can also download shared layouts created through the Report Designer.

Access Online Templates: Click to directly access the list of all available Custom Query reports shared on the File Query Cookbook website. From the Custom Query Recipes page, you can filter your search by category, database host, and more.

Filter: The cell directly below the **Report Name** column heading is a report filter that lists saved Custom Query reports according what you enter. For example, if you were to enter the word `access`, the listed Custom Query reports would be only those with the word `access` in the report name.

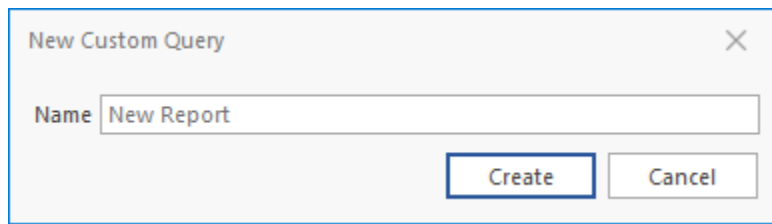
[Report Type]: By default, this check box is selected so that it displays only Custom Query Reports, which are the only reports that can be designed using the Design Editor. You can deselect the check box to view all of your reports.

Edit Filter: Use this button to further refine your filtering using Boolean operators.

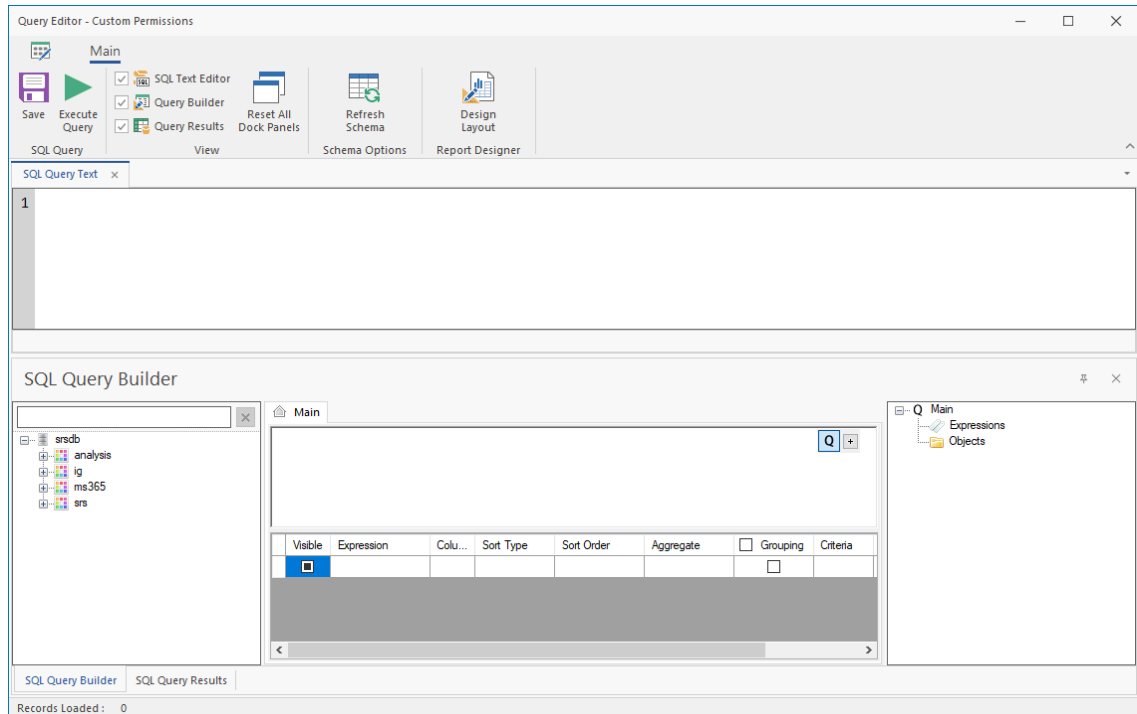
11.2 Creating a Custom Query Report

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 4.0 Database Schema and Custom Queries Guide](#).

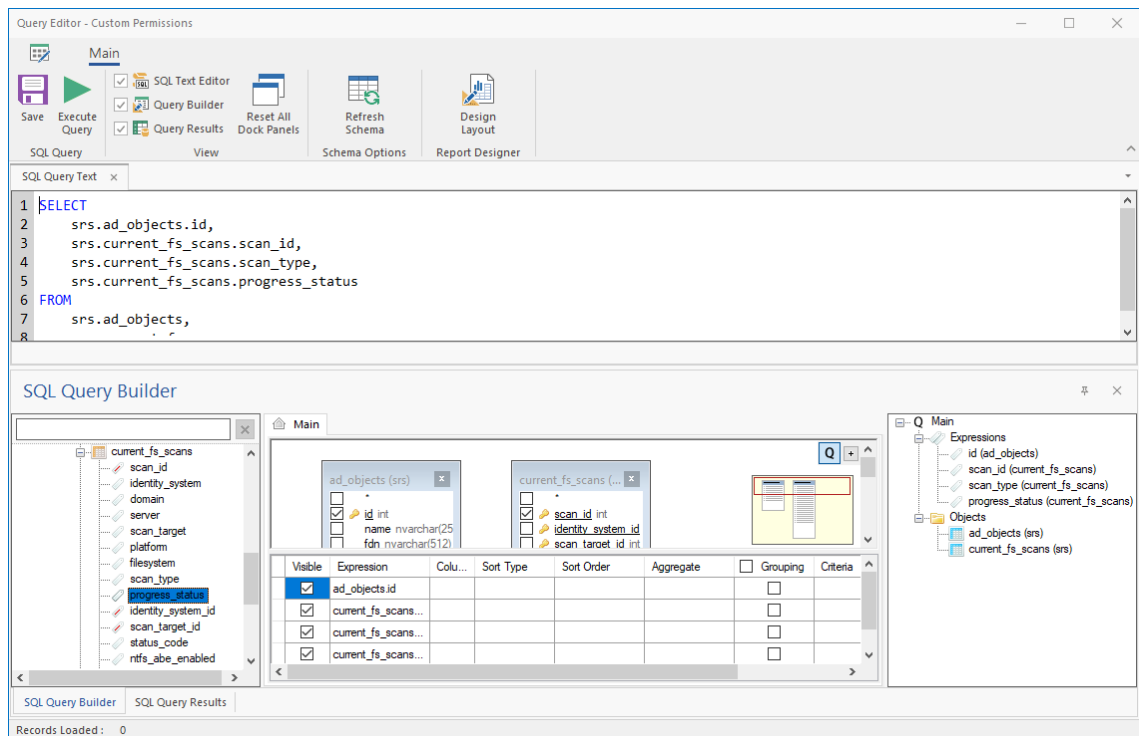
- 1 Click **New Custom Query Report**.



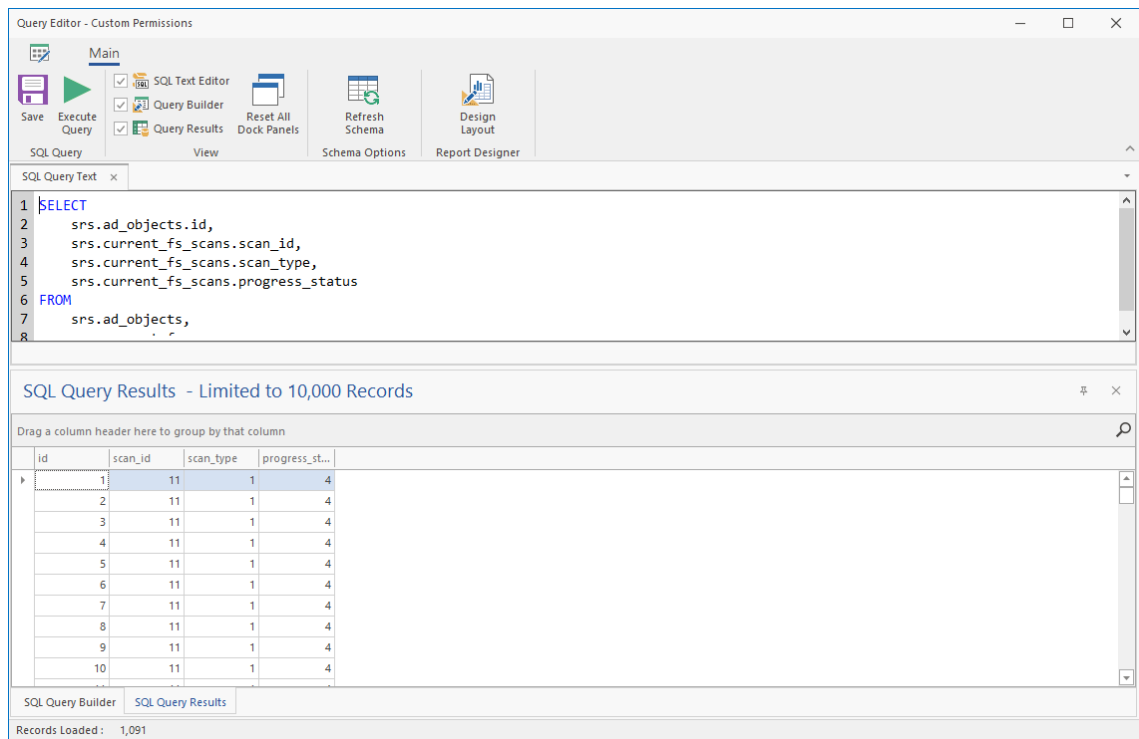
- 2 Specify a descriptive name, then click **Create**.
The Report Designer Query Editor is launched.



- 3 In the **SQL Query Builder** region, expand **srs** to see the **Tables** and **Views** folders.
- 4 Expand either the **Tables** or **Views** folder.
- 5 Expand a displayed table or view.
- 6 Select the tables and fields you want included in the query by double-clicking each.



- 7 Append the query with any additional SQL commands in the text editor.
- 8 Click **Execute Query** to get a preview of the Custom Query Report.



- 9 Click **Save**.
- 10 Close the Query Editor.

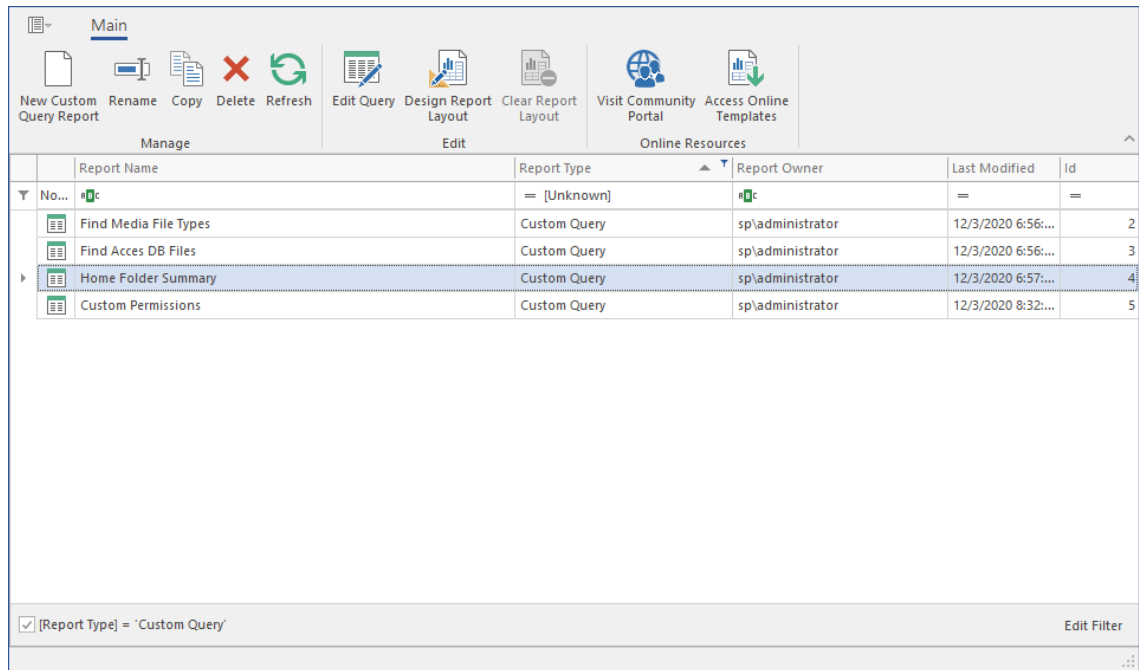
11.3 Designing a Custom Query Report

After you have created a Custom Query Report, either through the Report Designer Query Editor or the Query Editor built into the browser-based administration interface, you can design the layout of the report.

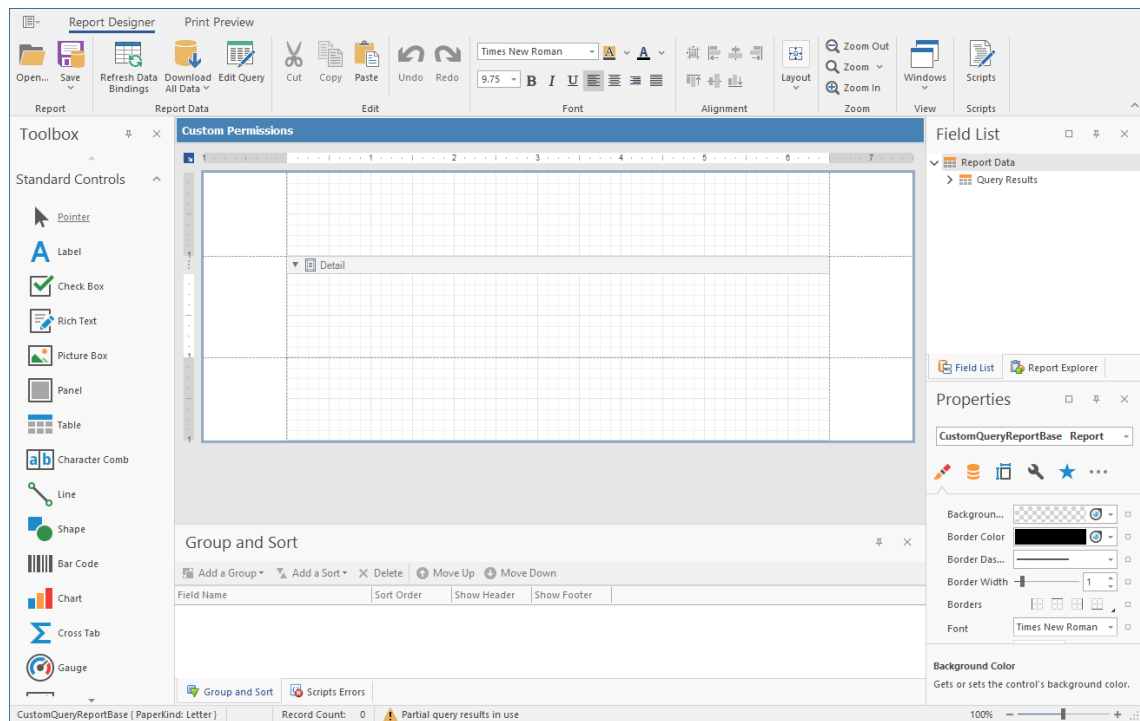
NOTE: This exercise introduces you to some of the very basic design features of the Report Designer. Through familiarizing yourself with the basic features, you will become proficient enough in the interface to try more advanced features.

For a more detailed explanation of features in the Report Designer, refer to: <https://devexpress.github.io/dotnet-eud/interface-elements-for-desktop/articles/report-designer/report-designer-for-winforms.html>.

- 1 From the listed Custom Query Reports, select the one you want to design.



- 2 Click Design Report Layout.



3 Create a report header.

3a Place the pointer in the upper section of the layout grid.

3b Right click and select **Insert Band > Report Header**.

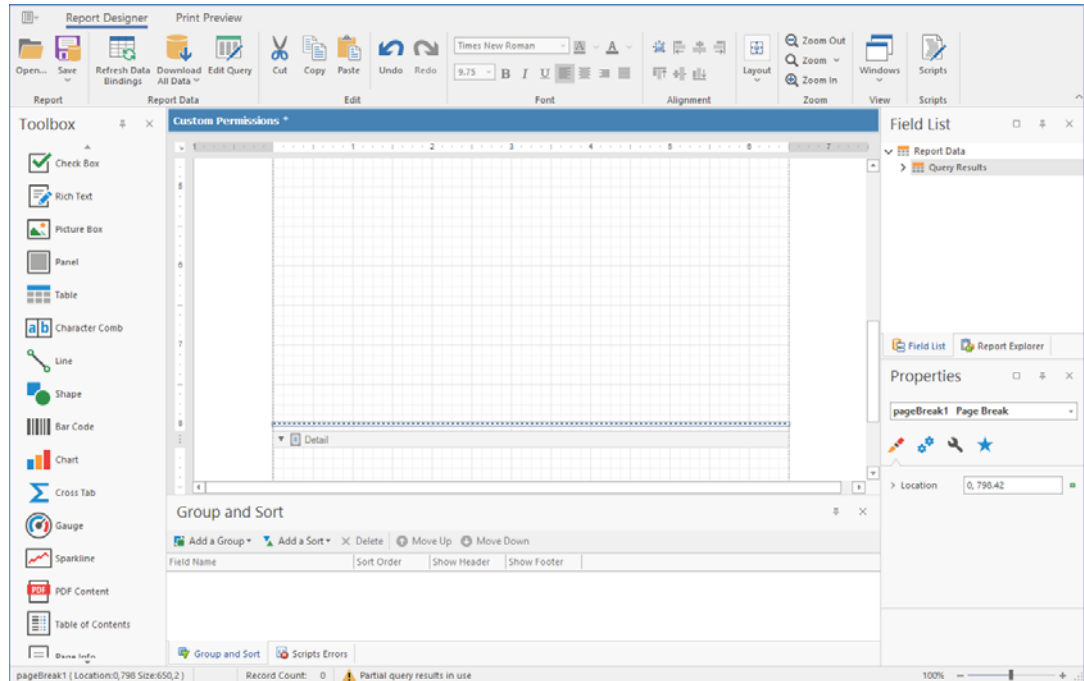
A new ReportHeader band appears on the grid.

4 Resize Page 1 and add a page break.

4a Place the pointer on the bottom border of the new band and using the vertical ruler as a guide, extend the band to fill the first page.

For example, to fill the first page, you might extend the border down to the 8" mark.

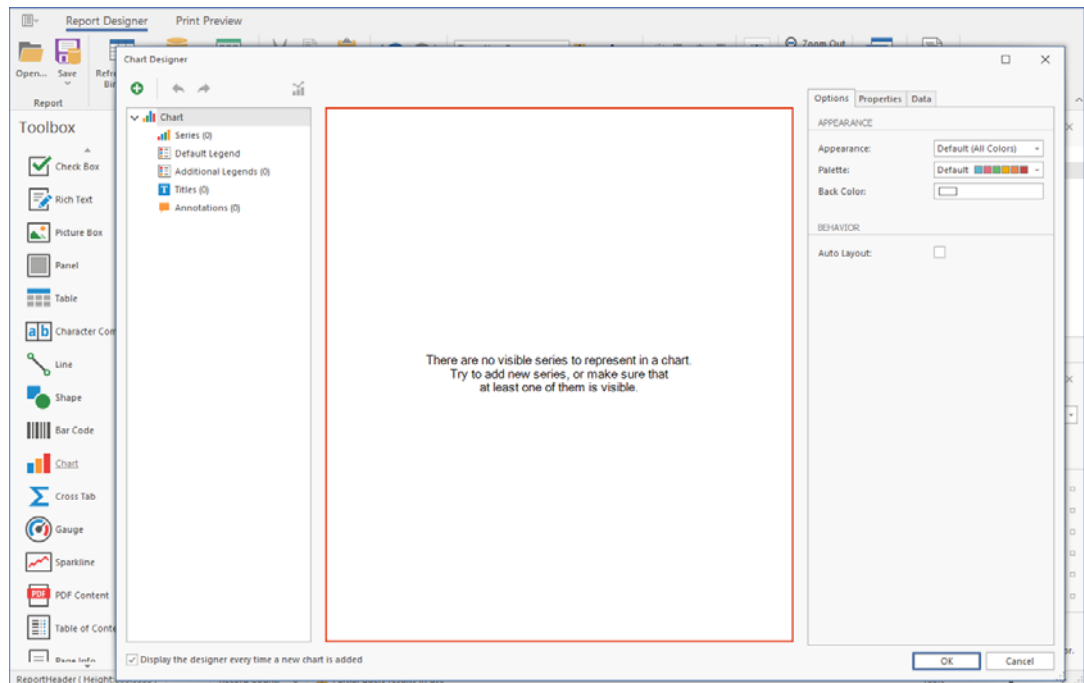
4b From the **Standard Controls** region, click and drag a **Page Break** to the bottom of the band.



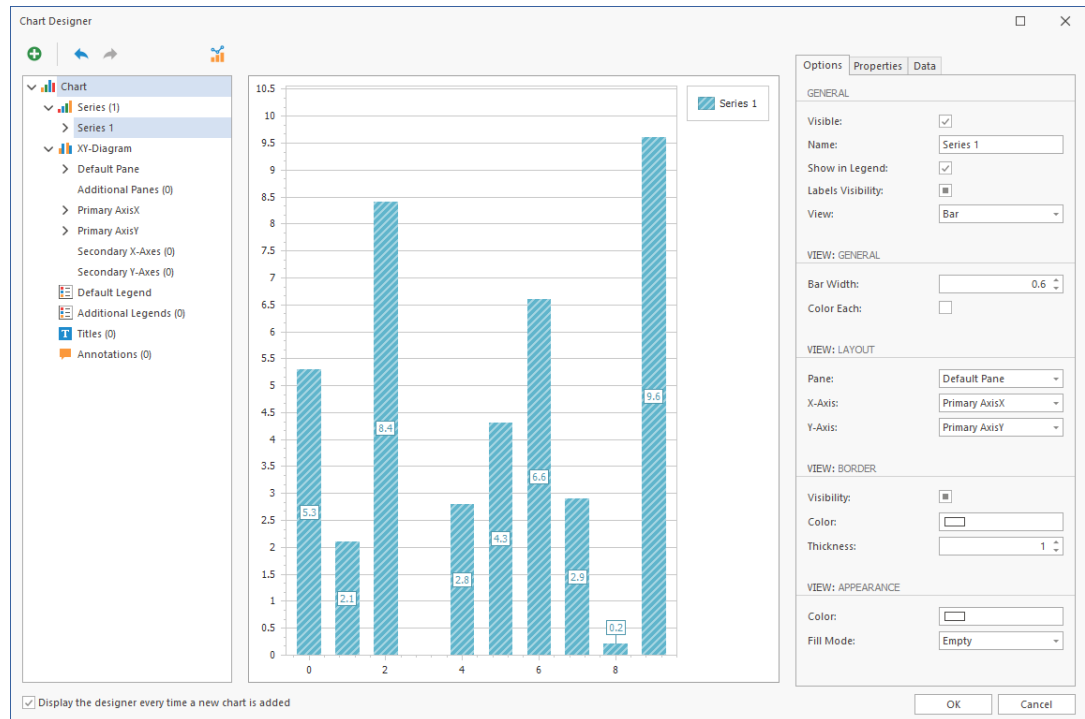
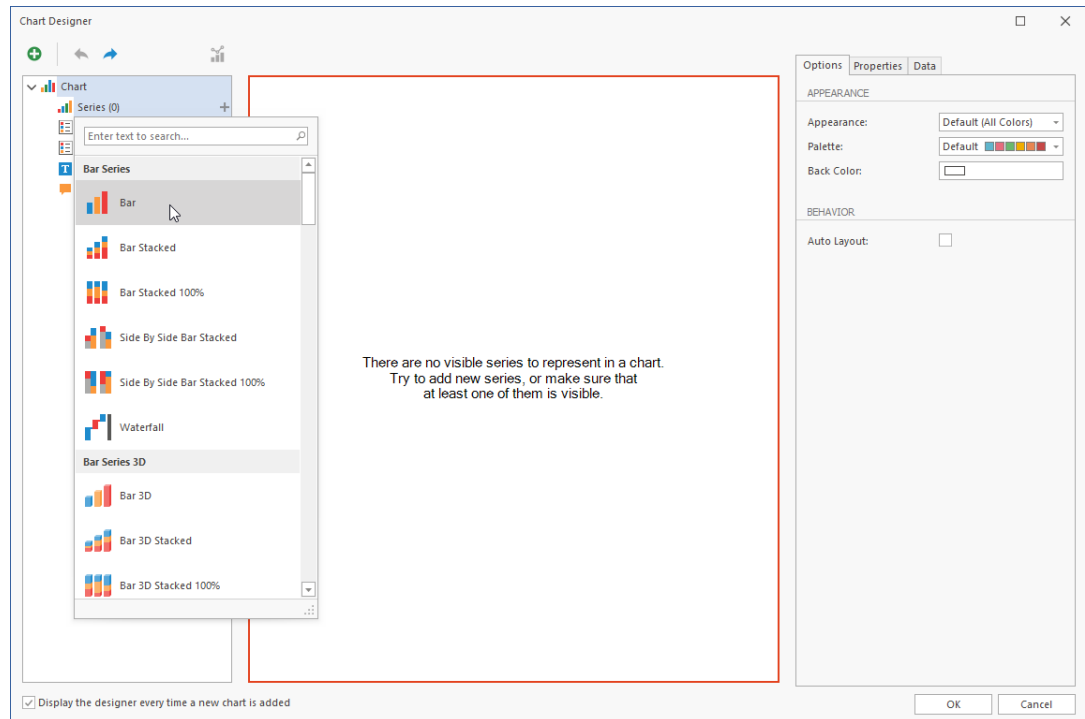
5 Insert and design a chart.

5a From the **Standard Controls** region, click and drag a **Chart** to the band.

The Chart Designer is launched.



5b In the Chart Designer, below the **Chart** menu, click the **+** that pertains to the **Series** option and select the **Bar** option.



5c Click the **Date** tab and expand **Query Results**.

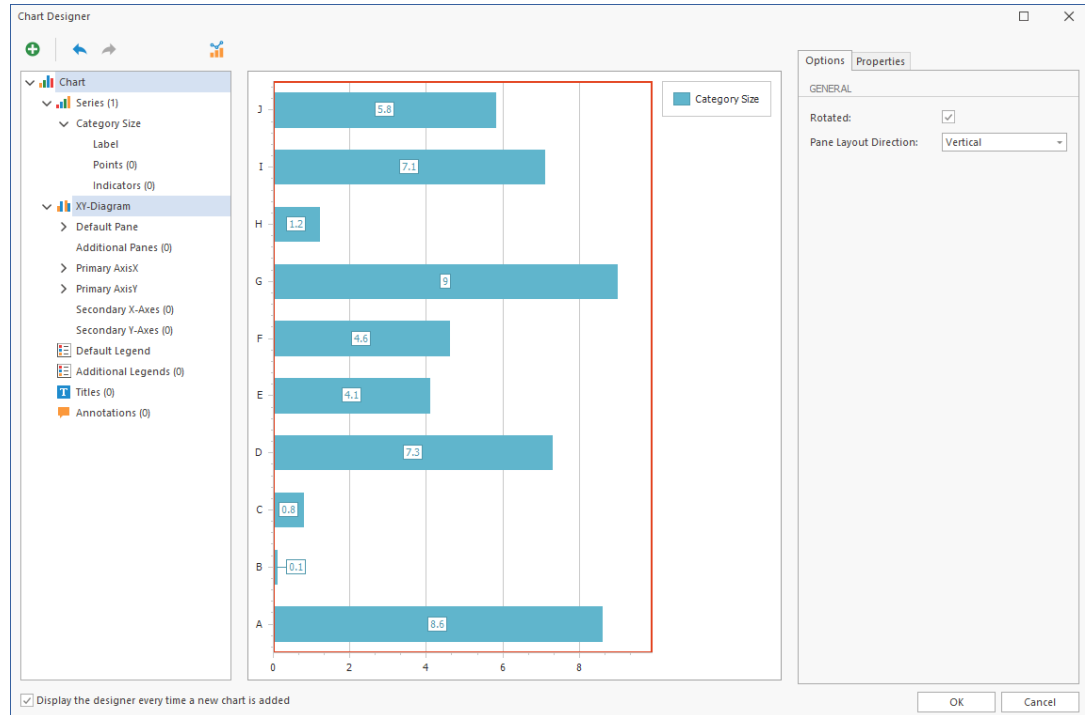
5d Click and drag **Category** to the **Argument** cell.

5e Click and drag **cat_size** to the **Value** cell.

5f Click the **Options** tab and in the **Name** field, replace **Series 1** with **Category Size**.

5g Below the **Chart** menu, click the **XY-Diagram** option.

5h In the **Options** tab, select the **Rotated** check box.



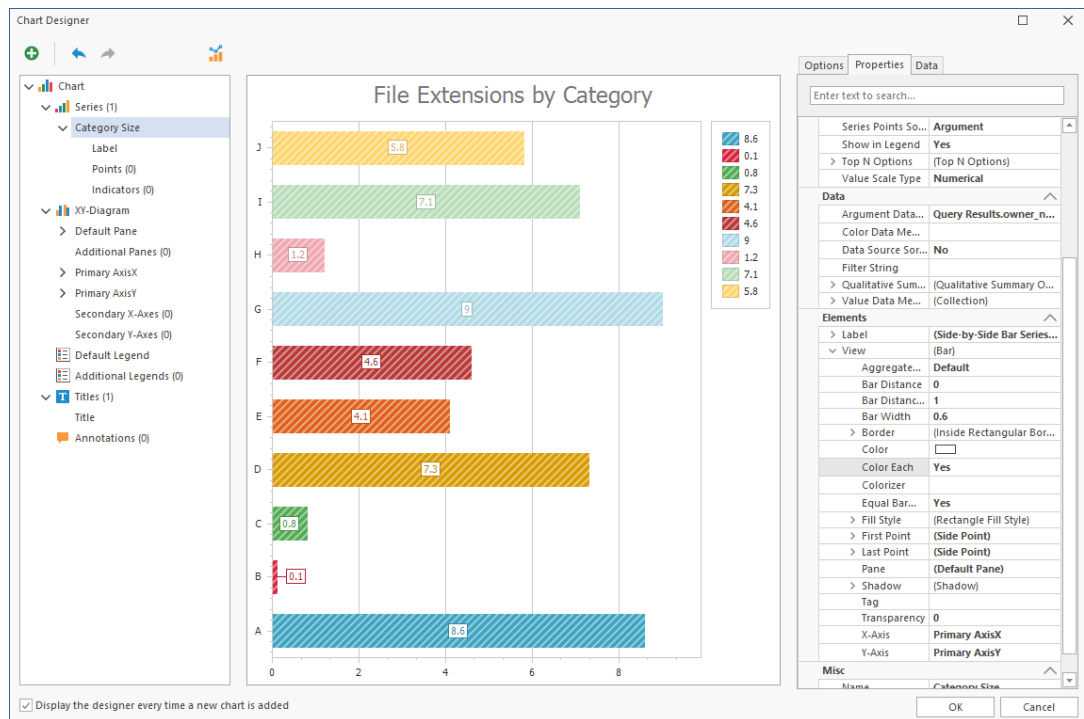
5i Below the **Chart** menu, select **Titles**, click the **+**, and select **Title**.

5j In the **Options** tab, in the **Lines** field, replace **Chart Title** with a more descriptive name. For example, **File Extensions by Category**.

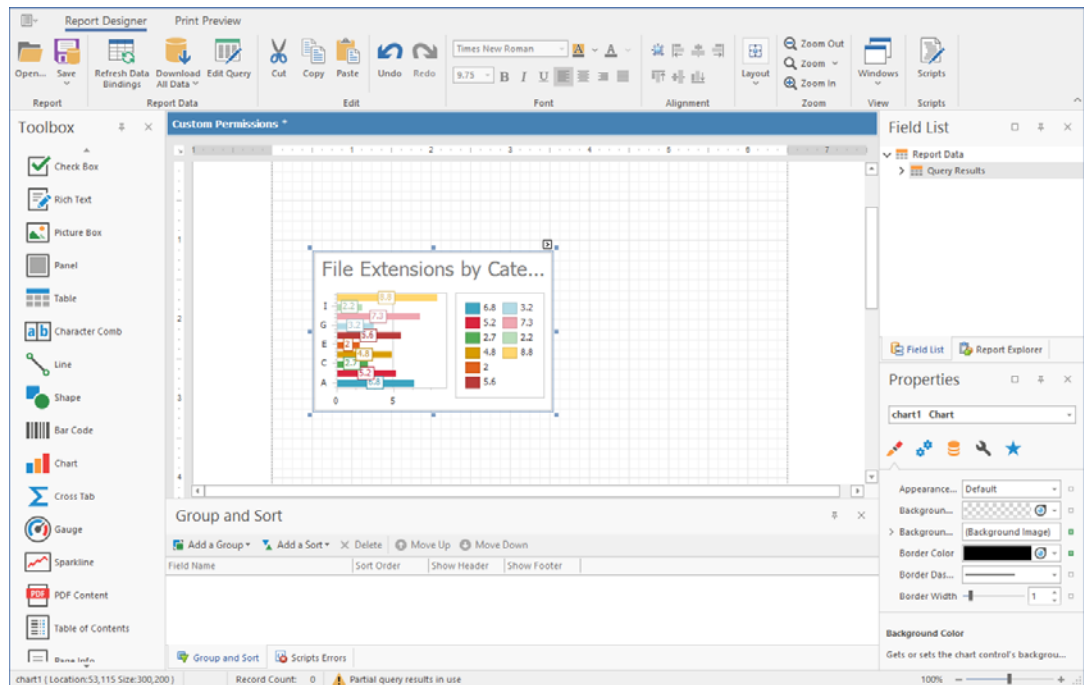
5k Below the **Chart** menu, select **Category Size**.

5l Click the **Properties** tab, scroll down and under the **Elements** heading and expand **View**.

5m Change the **Color Each** setting to **Yes**.



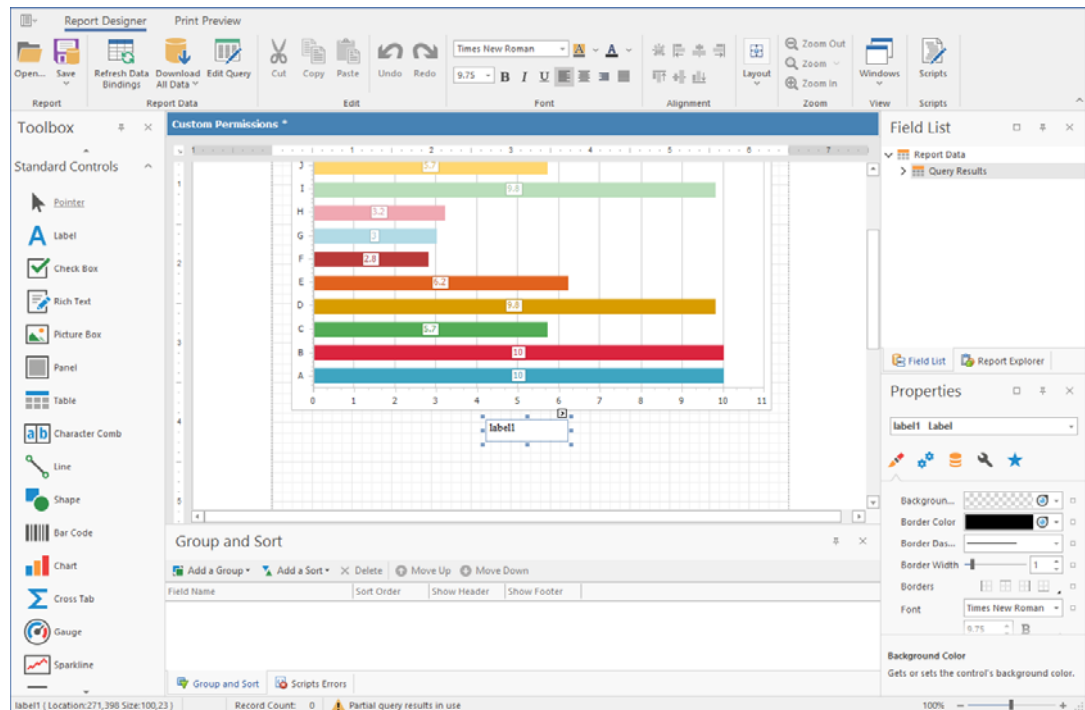
5n Click OK.



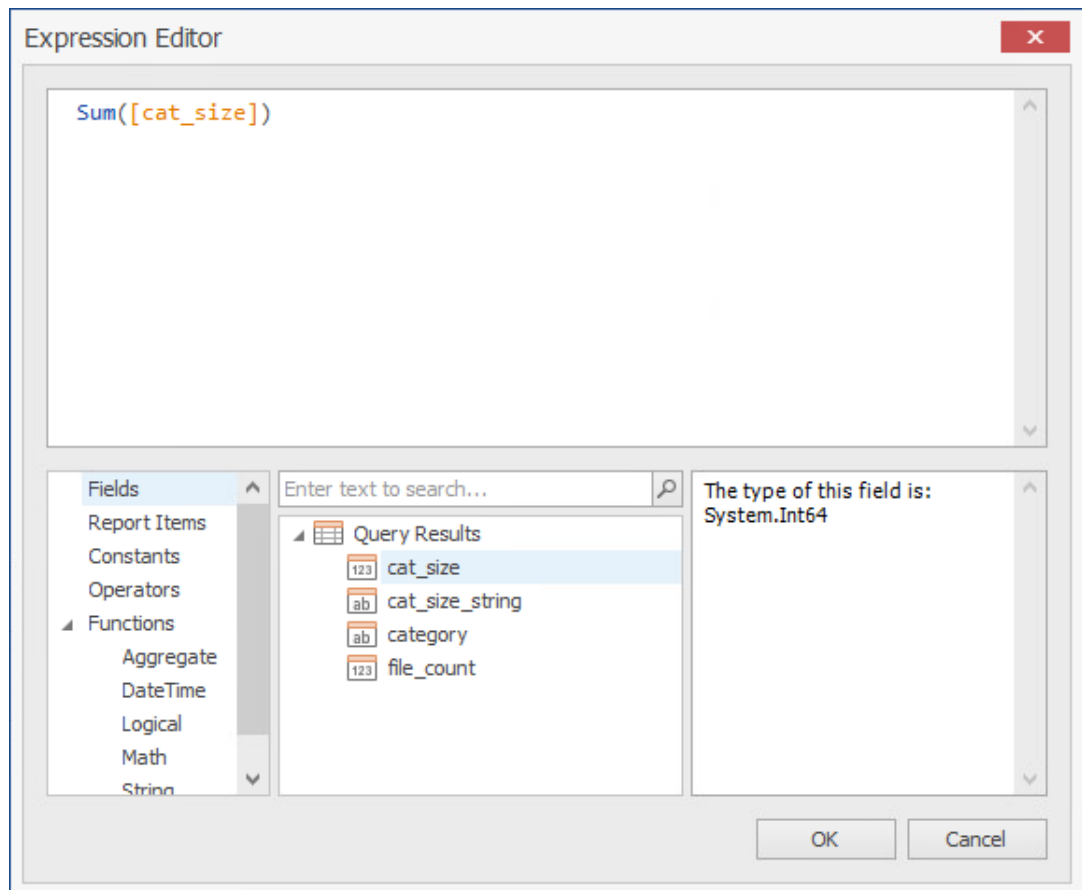
5o In the upper right-hand corner of the newly-placed chart, click the arrow to access the **Chart Tasks** menu and select **Run Designer**.

5p Click the legend and from the **Options** tab, deselect the **Visibility** check box so the legend no longer appears.

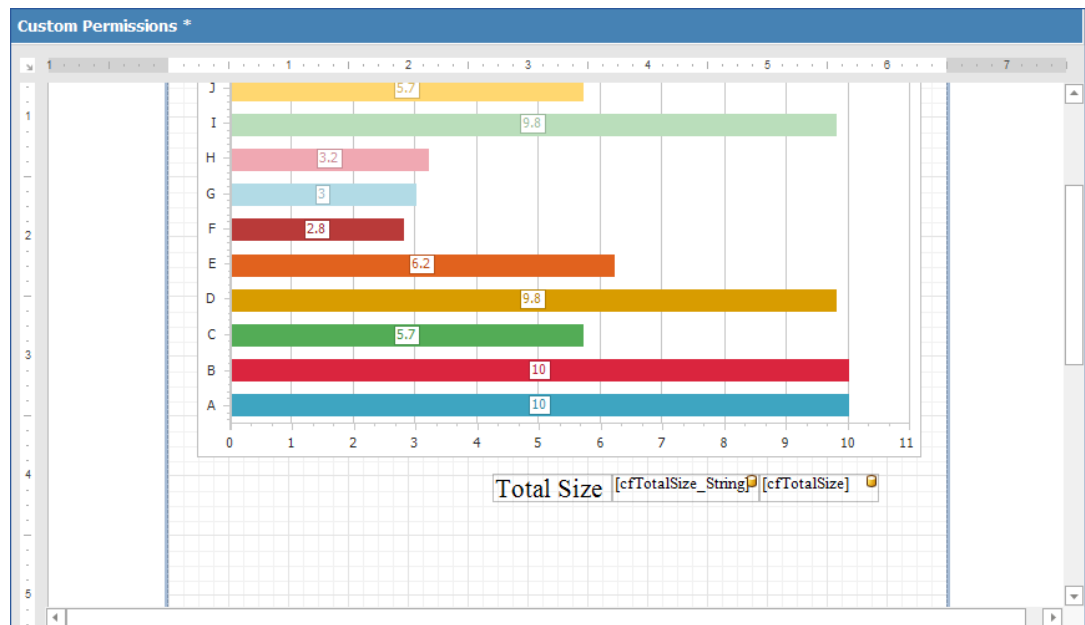
- 5q Click **OK**.
- 5r In the Report Designer, expand the view of the chart to take up more of the page.
- 6 Insert labels.
 - 6a From the **Toolbox**, click and drag **Label** to a position centered below the chart.



- 6b Double-click within the label and specify the label name.
For example, `Total Size`.
- 6c Adjust the font size and style to your preferences.
- 7 Create new fields.
 - 7a From the **Field List**, expand the **Query Results**.
 - 7b Right-click **Query Results** and select **Add Calculated Field**.
 - 7c In the **Design** region of the **Property Grid** for `calculatedField1`, change the **(Name)** setting to `cfTotalSize`.
 - 7d While still in the **Property Grid**, under the **Data** heading, click the ellipses (...) pertaining to the **Expression** field.
This launches the Expression Editor.
 - 7e In the bottom-left column, select **Functions**.
 - 7f In the empty field at the top of the middle column, type `sum` to locate the **Sum** function, then double click **Sum** to place the function in the top text box of the Expression Editor.
 - 7g In the bottom-left column, select **Fields** and then in the middle column, double-click `cat_size`.

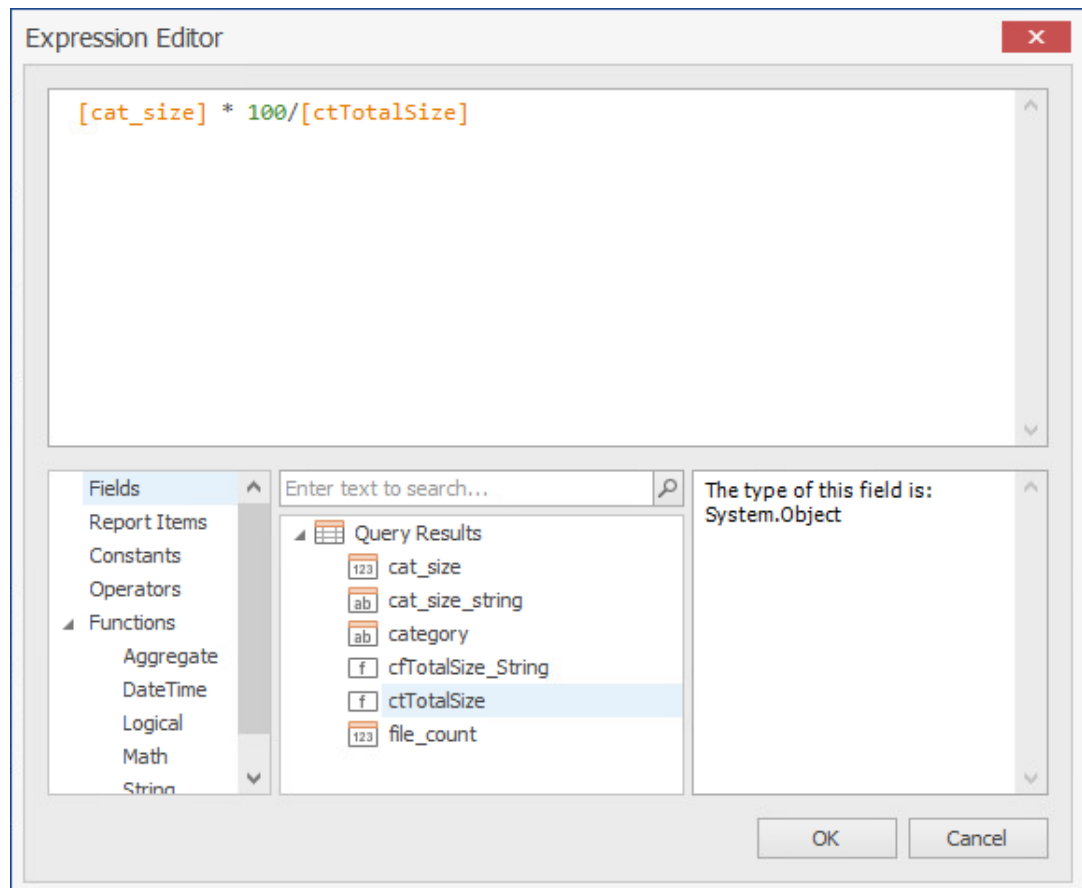


- 7h Click **OK** to save the new field and close the Expression Editor.
- 7i Right-click **Query Results** and select **Add Calculated Field**.
- 7j In the **Design** region of the **Property Grid** for `calculatedField1`, change the **(Name)** setting to `cfTotalSize_String`.
- 7k While still in the **Property Grid**, under the **Data** heading, click the ellipses (...) pertaining to the **Expression** field.
- 7l In the top text box of the Expression Editor, type `Byte` so that **ByteString()** appears.
- 7m From the middle column, double-click `cfTotalSize` that you created earlier and click **OK**.
- 8 Place the new fields.
 - 8a From the **Field List**, hold down the Control key, select the two new fields you just created, then drag them to the `Total Size` label on the grid.
 - 8b Adjust the size so that both fields will appear to the right of the `Total Size` label.



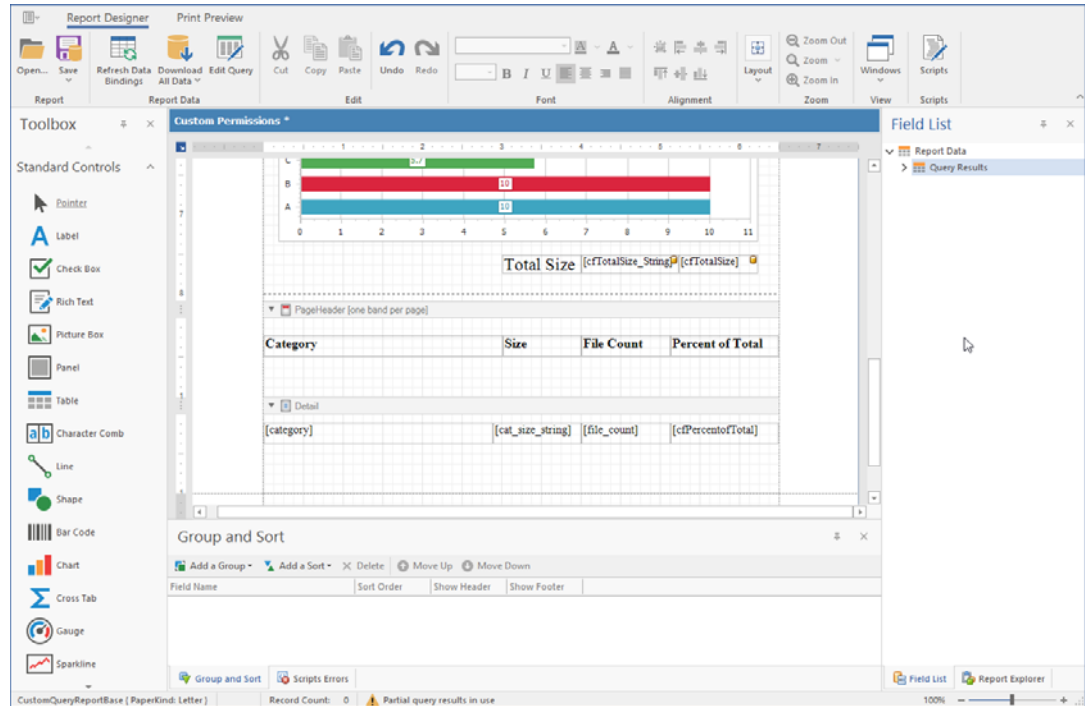
- 8c Adjust the font size and style to your preferences.
- 9 Preview the report.
 - 9a Click **Download All Data**.
 - 9b When the warning dialog box appears, click **Yes**.
 - 9c Click the **Print Preview** tab to observe how the report is going to look at this point.
 - 9d Make any desired format changes.
- 10 Create a header for Page 2.
 - 10a Click the **Report Designer** tab.
 - 10b In the Report Designer, scroll down below the page break so that you are working on Page 2 of the report.
 - 10c At the top of the page, right-click and select **Insert Band > PageHeader**.
 - 10d From the **Tool Box**, click and drag a **Table** to the location of the new page header.
 - 10e Replace the names of the three new table cells with the following names:
 - ◆ Category
 - ◆ Size
 - ◆ File Count
 - 10f Select the **File Count** cell, right-click, then select **Insert > Column to Right**.
 - 10g Change the table cell name to **Percent of Total**.
 - 10h Resize the table cells to your preferred width.
 - 10i Adjust the font size and style to your preferences.
 - 10j Resize the depth of the page header so it is limited to the depth of the table.

- 11 Create a new calculated field for Percent of Total.
 - 11a Right-click **Query Results** and select **Add Calculated Field**.
 - 11b In the **Design** region of the **Property Grid** for `calculatedField1`, change the **(Name)** setting to `cfPercentofTotal`.
 - 11c While still in the **Property Grid**, under the **Data** heading, click the ellipses (...) pertaining to the **Expression** field.
 - 11d From the middle column of the Expression Editor, double-click `cat_string`.
 - 11e Hit the space bar and then enter the following string: `* /100`
 - 11f Complete the string by double-clicking `cfTotalSize` from the middle column of the Expression Editor.



- 11g Click **OK**.
- 12 Insert the table content.
 - 12a Click below the header, hold down the Control key, and from the **Field List**, select the following fields in this order:
 - ♦ category
 - ♦ cat_size_string
 - ♦ file_count
 - ♦ cfPercentofTotal
 - 12b Drag the fields to a location below the header.

12c Line up the tables cells with the headings.



12d Click the **Print Preview** tab to view how the report will look.

12e Make any needed adjustments.

13 Click **Save > Save to Database**.

By saving the report to the database you enable the File Reporter Report Generator to use the report design for updated reports.

In addition to saving the report to the database, you can save the report as a file where you can import it into another file, such as a Word file or PowerPoint presentation.

11.4 Saving the Layout as a Template

When working with the Report Designer, you might create a layout design that you want to utilize as a template for future Custom Query Reports. You can do so using **Save As File**.

- 1 In Report Designer, open the Custom Query Report whose design you want to save as a template.
- 2 Select **Save > Save As File**.
- 3 Name and save the layout.

The layout is saved as a `.repx` (Report Layout XML) file.

11.5 Using a Saved Template for Custom Query Reports

You can use saved `.repx` files as design templates for Custom Query Reports.

TIP: You can also use the sample report layouts and SQL commands that are available from the File Query Cookbook, the collaborative community portal for accessing and sharing Custom Query reports. 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 <http://www.filequerycookbook.com> (<https://www.filequerycookbook.com>).

- 1 In Report Designer, open the Custom Query Report you want to design using a saved template.
- 2 Click **Open**, then select the `.repx` file you want to use for designing your report.
The report is updated with the design from the `.repx` file.

A

Filtering for Built-in Reports

- ◆ [Section A.1, “Filters Tab,” on page 155](#)
- ◆ [Section A.2, “Single Entry Filter Conditions,” on page 157](#)
- ◆ [Section A.3, “Multi-Condition Filtering,” on page 159](#)

Micro Focus 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

A.1 Filters Tab

- ◆ [Section A.1.1, “Filter Expression Builder,” on page 156](#)
- ◆ [Section A.1.2, “Relative Date Filtering Parameters,” on page 157](#)

All filtering takes place in the **Filters** tab of the Report Definition Editor.

Figure A-1 Filters Tab

Report Definition Editor - Atlanta Users Owner Report

Name: Atlanta Users Owner Report

Unformatted:

Type: Owner Report

Description: Report Definition created on 12/7/2020 7:46:06 PM by SP\Administrator

TARGET PATHS FILE MANAGEMENT POLICIES **FILTERS**

EXPRESSION | And +

RELATIVE DATE

Save Cancel

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.

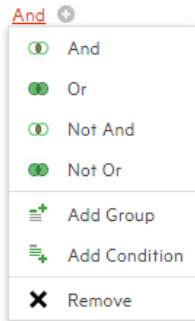
You can filter according to size, dates, or both.

A.1.1 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 A-2 And Drop-Down Menu



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

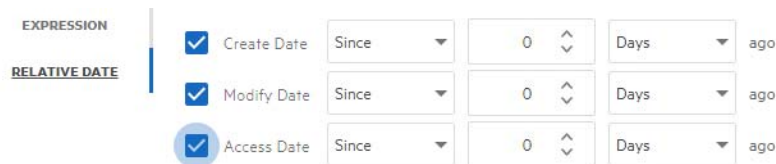
Figure A-3 Parameters for Filter



A.1.2 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 A-4 Relative Date Filtering Parameters



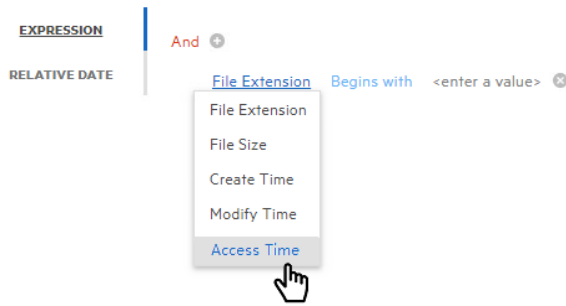
A.2 Single Entry Filter Conditions

- ◆ [Section A.2.1, "Using the Filter Expression Builder," on page 157](#)
- ◆ [Section A.2.2, "Using the Relative Date Filtering Settings," on page 159](#)

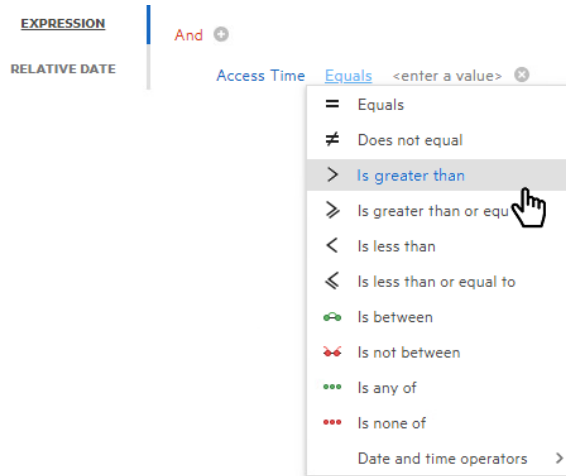
You can use either the **And** drop-menu and + button, or the **Relative Date** filtering settings to create single entry filter conditions.

A.2.1 Using the Filter Expression Builder

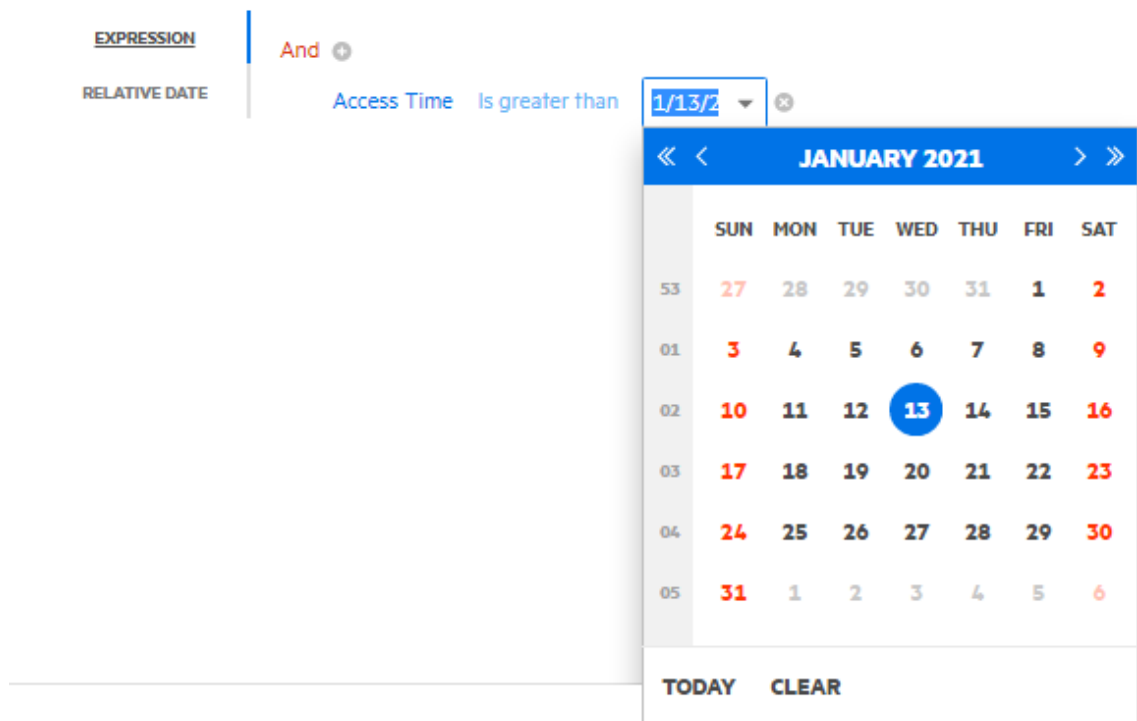
- 1 From the **And** drop-down menu, select a Boolean operator.
- 2 Click the + button to add an entry.
- 3 From the **File Extension** drop-down menu, select a Boolean operator.



4 From the **Equals** drop-down menu, select a Boolean operator.



5 In the **<enter a value>** field, enter a value.



File size 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 x1024). A more practical entry might be 500000000. Do not attempt to enter commas; they are placed automatically.

- 6 Click **OK** to save the settings in the Report Definition Editor.

Using the settings in this procedure as an example, when you generate a report, the data would include only files that have been accessed after May 17, 2017.

A.2.2 Using the Relative Date Filtering Settings

- 1 From the **Filters** tab, click the **Relative Date** option.
- 2 Select from the **Create Date**, **Modify Date**, or **Access Date** check boxes.
- 3 From the first drop-down menu, select either **Since** or **Before**.
- 4 From the numeric field to the right, enter a numeric setting.
- 5 From the drop-down menu to the right, select from the options.



- 6 Click **Save** to save the settings in the Report Definition Editor.

Using the setting in this procedure as an example, when you generate a report, the data would include only files that have been accessed in the last week.

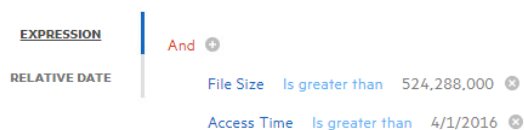
A.3 Multi-Condition Filtering

You can set multi-conditioned filters by:

- ♦ Entering parameters for more than one entry using the **And** drop-down menu
- ♦ Specifying multiple **Relative Date** filtering settings
- ♦ Combining parameters specified through the **And** drop-down menu and the **Relative Date** filtering settings

IMPORTANT: Be aware that when you set multiple entries in a condition for filtering, that all entries must be met in order for File Reporter to report on the file.

For example, in the example below, the files would appear in the report only if they were greater than 500 MB and had been accessed after April 1, 2012.



B Security Settings

- ◆ [Section B.1, “Rights and Privileges on Scanned Storage,” on page 161](#)
- ◆ [Section B.2, “Firewall Requirements,” on page 161](#)
- ◆ [Section B.3, “Local Security Authority Rights and Privileges,” on page 162](#)
- ◆ [Section B.4, “Proxy Rights Group,” on page 163](#)
- ◆ [Section B.5, “Windows Clustering through Proxy Agents,” on page 163](#)

B.1 Rights and Privileges on Scanned Storage

Micro Focus File Reporter must have the proper rights set on each network share that it scans. In addition, certain privileges must be granted to File Reporter on the machine hosting the Engine and on each server where storage is managed.

B.1.1 Granting Rights

Every Windows network share to be scanned by File Reporter must have proper rights assigned to the File Reporter proxy rights group.

- 1 As an Active Directory domain administrator, authenticate to the server where the storage is located.
- 2 Grant Read Only sharing privileges to the proxy rights group for each share that File Reporter will scan.

B.2 Firewall Requirements

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.

B.3 Local Security Authority Rights and Privileges

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 rights and privileges are modified through `secpol.msc` or 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 In the table of **Privileges** and the objects to which they apply located on the right, verify that the File Reporter proxy rights group has the following privileges:

- ◆ 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 of some of these privileges causes the Engine and Agent components to not function properly. Removal of these rights and privileges via Group Policy Object (GPO) results in the Engine and Agent not functioning properly.

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.

B.4 Proxy Rights Group

By default, whenever any of the components of File Reporter are installed on a server in a domain, the proxy rights universal 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.

As explained previously, 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.

IMPORTANT: The proxy rights group for Active Directory must be a member of the built-in Administrators group on each Windows server that File Reporter scans.

Certain functions, such as collection of quotas via FSRM (File Server Resource Manager) do not work without this membership despite the assignment of other rights and privileges.

B.5 Windows Clustering through Proxy Agents

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. In particular, the File Reporter proxy rights group must be granted membership in the built-in Administrators group and it must also be granted all of the LSA rights and privileges that are granted at 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.

C 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 C-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\SRManagerFC.log
AgentFC	C:\ProgramData\Micro Focus\SRS\AgentFC\log\SRSAgentFC.log
Agent365	C:\ProgramData\Micro Focus\SRS\Agent365\log\SRSAgent365.log

D AgentFS Scan Capabilities

- ◆ Section D.1, “Server Platform and NAS Device Support,” on page 167
- ◆ Section D.2, “File System Metadata,” on page 168
- ◆ Section D.3, “Security Scans — Active Directory File Systems,” on page 169
- ◆ Section D.4, “Other Microsoft Supported Features,” on page 169
- ◆ Section D.5, “Current Limitations,” on page 169

D.1 Server Platform and NAS Device Support

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

Table D-1 Supported Scan Target Hosts

Server Platform	File Reporter 4.0
Windows Server 2008	✓ ¹
Windows Server 2008 R2	✓
Windows Server 2012	✓
Windows Server 2012 R2	✓
Windows Server 2016	✓
Windows Server 2019	✓

1. Older Windows servers including Windows 2003 or 2003 R2 might work, but are not supported.

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

Table D-2 Supported Scan Target NAS Hosts

NAS Device	File Reporter 4.0
NetApp Filer with OnTAP 8.x (7 mode or Cluster mode)	✓ ¹
NetApp Filer with OnTAP 9.x	✓
Isilon OneFS 7.2	✓ ¹
Isilon OneFS 8.x	✓

1. Older versions of NetApp OnTAP and Isilon OneFS might work but are not supported.
2. Other NAS devices not listed here might work with limited support if running a vendor supported version of the device and management software.

D.2 File System Metadata

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

Table D-3 File System Metadata Support

Metadata Feature	Windows NTFS	Windows ReFS
File Name / Extension	✓	✓
File Size	✓	✓
File Sparse Size	✓	✓
File Compressed Size	✓	✗
File Size on Disk ²	✓	✓
Create Time	✓	✓
Modify Time ³	✓	✓
Access Time ³	✓	✓
Directory Quota	✓	✗
Owner	✓	✓

1. File size-on-disk calculations are currently performed using an assumed 4 KB block size, except when using AgentFS, which attempts retrieval of the actual allocation size.

2. Access and Modify time stamps for directories are not consistently defined across file system types. These time stamps should only be considered for file entries.
3. 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.

D.3 Security Scans — Active Directory File Systems

Table D-4 Permission Scan Capabilities for Active Directory Environments

Windows Component	Supported	Notes
Share Permissions	✓	
Security Descriptors	✓	Includes the ACLs and ACEs, 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.

D.4 Other Microsoft Supported Features

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

D.5 Current Limitations

The following are scan limitations of File Reporter 4.0:

- ◆ Microsoft Environments
 - ◆ No scanning for 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

E Glossary

Agent365: Agent enabled to perform scanning of data and associated permissions for Microsoft 365 file repositories, including OneDrive for Business, SharePoint Online document libraries, and Teams document libraries

AgentFC: Agent enabled to perform file content scanning.

AgentFS: Agent enabled to perform file system scanning.

Analytics Tools: Windows workstation application included in the Client Tools designed to analyze data from scans. The current Analytics Tools include the Dashboard, Pivot Grid, and Tree Map.

Baseline Scan: A scan that you save as a reference for a comparison with another scan via a Historical Comparison report. You can have one File System Baseline scan and one Permissions Baseline scan for each storage resource.

Built-in Reports: With the exception of Custom Query reports, all of the report types that you can generate through the options displayed on the Add Report Definition page.

Current Scan: The most recent scan of a storage resource.

Custom Query Reports: Custom reports generated through SQL commands to the database. Custom Query reports can be generated both from the File Reporter browser-based administrative interface and from the Report Designer client tool.

Engine: The component that runs File Reporter.

The Engine does the following:

- ◆ Schedules the scans that the Agents conduct
- ◆ Compiles scans for inclusion in a report
- ◆ Provides the report information to the user interface
- ◆ Determines that a condition has been met to start a triggered report
- ◆ Runs scheduled reports
- ◆ Monitors how many agents are online
- ◆ Sends notifications that File Reporter has completed a scan or generated a report

File Content Scan: The process of scanning file content for specified patterns (e.g. U.S Social Security numbers, credit card numbers, etc.). File Content scans are performed by an AgentFC on a Windows storage device.

Historic Comparison Report: File system or permissions reports that specify the differences between two similar scan types of the same target system. Historic Comparison reports can compare Baseline scans to Previous scans, Baseline scans to Current scans, and Previous scans to Current scans.

ManagerFC: Service that 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

Micro Focus File Dynamics: A Windows network file management system utilizing Microsoft Active Directory to enacted policies. Identity-driven policies automate tasks that are traditionally done manually, resulting in cost savings and the assurance that tasks are being performed properly. Target-driven policies offer data migration, cleanup, workload, and protection from data corruption and downtime through nearline storage backup of high-value targets, enabling quick recovery of files and their associated permissions. File Reporter can output reports that can be imported into File Dynamics Workload policies for remediation.

Preview Report: A report generated through the **Generate Preview** option. Might also be referred to as “viewing the report in Preview mode.”

Previous Scan: When the **Retain existing Previous scan** option is selected in the Scan Policy Editor, the status of the Current scan becomes the Previous scan. You can then use the Previous scan as a reference for a Historic Comparison report. There is only one File System Previous scan and one Permissions Previous scan for each storage resource.

Proxy Agent: An Agent that performs agent services on a storage resource through a proxy association. NAS devices and clustered systems require proxy agents.

Proxy Target: Servers, clustered systems, and NAS devices that are not hosting an Agent but are being scanned through a proxy agent.

Report: The result of a report request specified through the report definition. Reports are first presented on-screen in either Preview or Stored mode. You can save reports in a number of different formats.

Scan: Comprehensive file information pertaining to a storage resource at a specific time. Information from scans is the means of generating reports.

Scan Policy: Specifies how and where the scan is conducted. All network file system scans are managed through a scan policy.

Scan Processor: Introduced in File Reporter 3.0, the Scan Processor alleviates some of the workload that was previously performed by the Engine. This workload includes storing the scans in the database and processing the scans.

Scan Target: The storage resource on the network that can be scanned by File Reporter.

Storage resource: A resource within the network environment that File Reporter monitors and reports on. A storage resource can be a Windows server share, a NAS device, or a network folder path.

Stored Report: A report that is stored in the `Reports` folder of the Engine. By default, a stored report is only stored for 30 days, but this setting can be adjusted through the Stored Reports Configuration page.

Unformatted Report: Report data generated as “raw” text rather than formatted and presented in a formatted report. In some instances, having an unformatted report might be useful for doing extensive sorting and filtering of the report data through a product such as Microsoft Excel.

Web Application: The File Reporter administrative interface that runs on top of Microsoft IIS.

