



# Micro Focus File Reporter 3.6 Administration Guide

November 27, 2018

## Legal Notices

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

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

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

Copyright © 2018 Condrey Corporation. All Rights Reserved.

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

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

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

## 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

<b>About This Manual</b>	<b>7</b>
<b>1 What's New</b>	<b>9</b>
1.1 New in Version 3.6	9
1.2 New in Version 3.5	9
1.3 New in Version 3.0	10
1.4 New in Version 2.6	10
1.5 New in Version 2.5	11
1.6 New in Version 2.0.2	11
1.7 New in Version 2.0.1	12
1.8 New in Version 2.0	12
<b>2 Overview</b>	<b>15</b>
2.1 Micro Focus File Reporter	15
2.2 How File Reporter Works	15
2.2.1 Core Components	16
2.2.2 File System Scanning	17
2.2.3 File Content Scanning	18
2.2.4 Reporting	19
2.2.5 Client Tools	21
<b>3 The Administrative Interface</b>	<b>25</b>
3.1 Supported Browsers	25
3.2 Launching the Administrative Interface	25
3.3 Using the Administrative Interface	27
3.3.1 Viewing Notifications	27
3.3.2 Configuring the Web Interface	28
3.3.3 Viewing System Information	29
<b>4 Performing Setup Procedures</b>	<b>31</b>
4.1 Enabling Other Identity Systems	31
4.1.1 Enabling eDirectory	31
4.1.2 Enabling Active Directory	33
4.2 Viewing Storage Resources	35
4.3 Assigning Proxy Targets	37
4.4 Configuring Notifications	38
4.5 Integrating with File Dynamics or Storage Manager	40
<b>5 Scheduling and Performing File System Scans</b>	<b>41</b>
5.1 Scans	41
5.1.1 Scan Retention	42
5.2 Adding a Scan Target	42
5.3 Removing a Scan Target	44
5.4 Creating Scan Policies	44

5.5	Establishing a Baseline Scan	49
5.6	Clearing a Baseline Scan	50
5.7	Editing a Scan Policy	50
5.8	Deleting a Scan Policy	50
5.9	Scheduling Scans	50
5.10	Editing a Scheduled Scan	52
5.11	Clearing a Schedule on a Scheduled Scan	52
5.12	Conducting an Immediate Scan	52
5.13	Viewing Scans in Progress	52
5.14	Retrying Failed Scans	53
5.15	Viewing Scan Data	54
5.16	Viewing Scan History	54
5.17	Troubleshooting a Failed Scan	55

## **6 Generating File System Reports 57**

6.1	Overview	57
6.2	Changing Your Cover Sheet Branding	58
6.3	Changing the Report Data Font	59
6.4	Built-in Report Types	60
6.5	Directory Data Reports	60
6.5.1	Generating a Summary Report	61
6.5.2	Generating a Directory Quota Report	68
6.5.3	Generating a Storage Cost Report	69
6.5.4	Generating a Comparison Report	70
6.6	Permissions Reports	71
6.6.1	Generating an Assigned NCP Permissions Report	71
6.6.2	Generating an Assigned NTFS Permissions Report	73
6.6.3	Generating a Permissions by Path Report	74
6.6.4	Generating a Permissions by Identity Report	75
6.7	File Data Reports	76
6.7.1	Generating a Filename Extension Report	77
6.7.2	Generating a Detailed Filename Extension Report	78
6.7.3	Generating an Owner Report	79
6.7.4	Generating a Detailed Owner Report	80
6.7.5	Generating a Duplicate File Report	81
6.7.6	Generating a Detailed Duplicate File Report	82
6.7.7	Generating a Date-Age Report	84
6.7.8	Generating a Detailed Date-Age Report	85
6.8	Historic Comparison Reports	86
6.8.1	Generating a Historic File System Comparison Report	86
6.8.2	Generating a Historic NCP Permissions Comparison Report	88
6.8.3	Generating a Historic NTFS Permissions Comparison Report	90
6.9	Trending Report	91
6.9.1	Generating a Volume Free Space Report	91
6.10	Custom Query Reports	92
6.11	Unformatted Reports	95
6.11.1	Generating Unformatted Reports	95
6.12	Micro Focus File Dynamics and Storage Manager Policy Reports	96
6.13	Scheduling Reports	96
6.14	Editing a Scheduled Report	98
6.15	Clearing a Schedule on a Scheduled Report	98
6.16	Copying a Report Definition	98
6.17	Viewing Reports in Progress	99
6.18	Troubleshooting Reports	100

<b>7</b>	<b>Content Scanning and Reporting</b>	<b>101</b>
7.1	Creating File Content Classifications . . . . .	101
7.1.1	Creating a New Classification . . . . .	101
7.1.2	Editing a Classification . . . . .	102
7.2	Creating File Content Categories . . . . .	102
7.2.1	Creating a New Category . . . . .	102
7.2.2	Editing a Category . . . . .	103
7.3	Creating Search Patterns . . . . .	103
7.3.1	Creating a New Search Pattern . . . . .	103
7.3.2	Editing a Search Pattern . . . . .	104
7.4	Creating Job Definitions . . . . .	105
7.4.1	Creating a New Job Definition . . . . .	105
7.4.2	Editing a Job Definition . . . . .	108
7.5	Viewing Jobs in Progress . . . . .	108
7.6	Viewing Scanned Data Jobs . . . . .	109
7.7	Viewing Search Results . . . . .	109
7.8	Viewing AgentFC Configuration Registrations . . . . .	110
<b>8</b>	<b>Performing Other Administrative Tasks</b>	<b>111</b>
8.1	Stopping and Restarting Services . . . . .	111
8.2	Using Folder Summary . . . . .	112
8.3	Considerations for Reporting on NAS Devices . . . . .	113
8.3.1	NetApp filer . . . . .	113
8.3.2	EMC Isilon . . . . .	114
8.3.3	Other NAS Devices . . . . .	114
8.4	Changing the Default Path for Stored Reports . . . . .	114
8.5	Changing the Life Span of Stored Reports . . . . .	115
8.6	Resetting the Proxy User Password . . . . .	115
<b>9</b>	<b>Using the Report Viewer</b>	<b>117</b>
9.1	Use the Report Viewer . . . . .	117
<b>10</b>	<b>Using the Client Tools</b>	<b>121</b>
10.1	Launching the Analytics Tools . . . . .	121
10.2	Using the Dashboard . . . . .	123
10.3	Using the Tree Map . . . . .	125
10.4	Using the Pivot Grid . . . . .	127
<b>11</b>	<b>Using Report Designer</b>	<b>131</b>
11.1	Using the Report Designer Interface . . . . .	131
11.2	Creating a Custom Query Report . . . . .	133
11.3	Designing a Custom Query Report . . . . .	135
11.4	Saving the Layout as a Template . . . . .	145
11.5	Using a Saved Template for Custom Query Reports . . . . .	145
<b>A</b>	<b>Filtering</b>	<b>147</b>
A.1	Filters Tab . . . . .	147
A.1.1	Filter Expression Builder . . . . .	148
A.1.2	Relative Date Filtering Parameters . . . . .	149
A.2	Single Entry Filter Conditions . . . . .	149

A.2.1	Using the Filter Expression Builder	149
A.2.2	Using the <b>Relative Date</b> Filtering Settings	151
A.3	Multi-Condition Filtering	151
<b>B</b>	<b>Security Settings</b>	<b>153</b>
B.1	Rights and Privileges on Scanned Storage	153
B.1.1	Granting Rights	153
B.2	Firewall Requirements	153
B.3	Local Security Authority Rights and Privileges	154
B.4	Proxy Rights Group	155
B.5	Windows Clustering through Proxy Agents	155
<b>C</b>	<b>Log File Locations</b>	<b>157</b>
<b>D</b>	<b>Agent Scan Capabilities</b>	<b>159</b>
D.1	Server Platform and NAS Device Support	159
D.2	File System Metadata	160
D.3	Security Scans — Active Directory File Systems	161
D.4	Security Scans — eDirectory File Systems	161
D.5	Volume Free Space Scans	162
D.6	Other Microsoft Supported Features	162
D.7	Current Limitations	162
<b>E</b>	<b>Glossary</b>	<b>165</b>
<b>F</b>	<b>Documentation Updates</b>	<b>169</b>
F.1	November 27, 2018	169
F.2	July 2, 2018	169
F.3	July 19, 2016	169
F.4	August 5, 2015	170
F.5	April 27, 2015	170
F.6	October 7, 2014	170
F.7	February 18, 2014	171
F.8	November 26, 2013	171
F.9	April 25, 2013	171
F.10	February 13, 2013	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 15
- ◆ Chapter 3, “The Administrative Interface,” on page 25
- ◆ Chapter 4, “Performing Setup Procedures,” on page 31
- ◆ Chapter 5, “Scheduling and Performing File System Scans,” on page 41
- ◆ Chapter 6, “Generating File System Reports,” on page 57
- ◆ Chapter 7, “Content Scanning and Reporting,” on page 101
- ◆ Chapter 8, “Performing Other Administrative Tasks,” on page 111
- ◆ Chapter 9, “Using the Report Viewer,” on page 117
- ◆ Chapter 10, “Using the Client Tools,” on page 121
- ◆ Chapter 11, “Using Report Designer,” on page 131
- ◆ Appendix A, “Filtering,” on page 147
- ◆ Appendix B, “Security Settings,” on page 153
- ◆ Appendix C, “Log File Locations,” on page 157
- ◆ Appendix D, “Agent Scan Capabilities,” on page 159
- ◆ Appendix E, “Glossary,” on page 165
- ◆ Appendix F, “Documentation Updates,” on page 169

## 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](http://www.novell.com/documentation/feedback.html) and enter your comments there.

## Documentation Updates

For the most recent version of the *Micro Focus File Reporter 3.6 Administration Guide*, visit the [Micro Focus File Reporter Documentation website \(http://www.novell.com/documentation/filereporter3\)](http://www.novell.com/documentation/filereporter3).

## **Additional Documentation**

For additional File Reporter 3.6 documentation, see the following guides at the [Micro Focus File Reporter Documentation website](http://www.novell.com/documentation/filereporter3): (<http://www.novell.com/documentation/filereporter3>)

- ◆ *Micro Focus File Reporter 3.6 Installation Guide*
- ◆ *Micro Focus File Reporter 3.6 Database Schema and Custom Queries Guide*



# 1 What's New

- ◆ Section 1.1, “New in Version 3.6,” on page 9
- ◆ Section 1.2, “New in Version 3.5,” on page 9
- ◆ Section 1.3, “New in Version 3.0,” on page 10
- ◆ Section 1.4, “New in Version 2.6,” on page 10
- ◆ Section 1.5, “New in Version 2.5,” on page 11
- ◆ Section 1.6, “New in Version 2.0.2,” on page 11
- ◆ Section 1.7, “New in Version 2.0.1,” on page 12
- ◆ Section 1.8, “New in Version 2.0,” on page 12

With each product update, Micro Focus File Reporter introduces significant architectural and feature enhancements. Starting with the release of Version 2.0, we have provided a timeline summarizing some of the more notable changes in architecture, performance, and features.

## 1.1 New in Version 3.6

### Data Access Governance

This release introduces support for integration with Micro Focus Identity Governance 3.5 (IG 3.5) to provide an initial Data Access Governance solution. For details on configuration and setup of Data Access Governance, see the *Data Access Governance 3.6 Integration and Administration Guide*.

## 1.2 New in Version 3.5

### File Content Scanning and Reporting

In addition to reporting on security and metadata, on files located on Windows storage devices, File Reporter can now report on the content of the files themselves. Through file content scanning, organizations can identify files containing specified patterns such as U.S. Social Security numbers, credit card numbers, or other user-defined patterns. Furthermore, these organizations can define and apply classifications and categories to these identified files.

File content reports that identify files containing personal, confidential, or sensitive information can be imported into Micro Focus File Dynamics where the location of these files can be remediated.

### New Agents

A new AgentFS replaces the previous Windows Agent, now known as the legacy Agent for Windows. The latter is still available for serving as a Proxy Agent for OES storage devices. For file content scanning there is the new AgentFC.

### Support for OES 2018

This includes the ability for OES 2018 servers to host File Reporter Linux Agents, as well as for File Reporter 3.5 to perform file system scans on OES 2018 servers.

## 1.3 New in Version 3.0

### Micro Focus Branding

Micro Focus File Reporter 3.0 is the first File Reporter release to implement the Micro Focus branding elements. These are most apparent in the management and installation interfaces. In some cases, the names of files and folders have changed to reflect the new product name.

### Scan Processor

This new .NET application greatly improves the rate at which scans are added to the database. The Scan Processor resides on the server hosting the Engine and is installed during the Engine installation process.

### Direct Upgrading from Various 2.x Versions

You can upgrade to File Reporter 3.0 directly from versions 2.5, and 2.6.

### Updated Analytic Tools

No longer offered as a “Technology Preview,” these tools are now fully developed 64-bit applications. The Heat Map has been renamed to the more applicably descriptive Tree Map.

## 1.4 New in Version 2.6

### Baseline and Previous Scans

Previous versions of Novell File Reporter 2 let you keep only the most recent File System and Permissions scans of a storage resource. With the release of Version 2.6, you can now designate a particular scan to be retained as a “Baseline scan” and keep the existing scan as a “Previous scan.” This means that you can now retain up to three scans for each storage resource: a Baseline scan, a Previous scan, and a “Current scan.” Any combination of two scans are the means of generating new built-in Historic Comparison reports being introduced in Version 2.6.

### Historic Comparison Reports

This new built-in report lets you view the changes to a storage resource through a comparison of any two of the following scans: Baseline, Previous, or Current.

Historic Comparison reports include:

- ◆ Historic File System Comparison reports
- ◆ Historic NCP Permissions Comparison reports
- ◆ Historic NTFS Permissions Comparison reports

### Custom Query Report Designer Updates

The Custom Query Report Designer has been updated to support views for Previous and Baseline scan data, as well as a number of other updates and bug fixes.

### Ability to Delete a Scan Immediately

A scan can be manually deleted immediately, or it can be marked for deletion at the next maintenance interval (by default, currently 12:00 midnight local time).

## Ability to Copy a Report Definition

The ability to copy Report Definitions has been added to both the Web Application and the Report Designer. The Web Application is able to copy any report definition type, and the Report Designer is able to copy any Custom Query report definitions.

## File Query Cookbook

Coinciding with the release of Novell File Reporter 2.6 is the introduction of a new collaborative community portal for accessing and sharing Custom Query reports. The SQL commands for these reports are included so all that you have to do is simply copy the commands and paste them into the Report Designer. In addition, sample report layouts (.repx files) are also included for some reports which can be opened via the Report Designer report layout interface. Both the SQL and the report layouts may be customized as needed. You can access the File Query Cookbook directly through the Report Designer interface, or at <http://www.filequerycookbook.com> (<http://www.filequerycookbook.com>).

# 1.5 New in Version 2.5

## Custom Reports through Database Querying

In addition to the built-in report types, you can generate custom reports by crafting your own database query. The report data is extracted from the scan and generated into a report in delimited text format or a custom report layout via the new Report Designer.

## Custom Query Report Designer

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

## Desktop Report Viewer

Stored reports can now be downloaded and viewed from a Windows workstation with the Report Viewer application.

## Early Access to Analytic Tools in Development

The release of Version 2.5 includes early access to analytic features in a new tool set that can be run from a Windows workstation.

# 1.6 New in Version 2.0.2

## Support for Microsoft SQL Server 2012

With the release of Novell File Reporter 2.0.2, supported databases now include both PostgreSQL and Microsoft SQL Server 2012. For procedures on properly configuring a new SQL Server 2012 instance that is compatible with Novell File Reporter, see the *Novell File Reporter 2.0.2 Installation Guide*.

## Configuration Dashboard

A new configuration dashboard is the means of managing the product licensing and sequentially configuring and administering the database, Engine, and Web Application.

## Reporting on Administrative Shares

Novell File Reporter can now report on administrative shares in Windows file systems.

## Support for Microsoft Server 2012 R2

Novell File Reporter 2.0.2 fully supports Microsoft Server 2012 R2.

# 1.7 New in Version 2.0.1

## Advanced Filtering

With the introduction of Novell File Reporter 2.0.1, you can use advanced filtering capabilities so that your File Data reports include only the data you want. Boolean filtering is available through a new **Filters** tab. For more information, see [Appendix A, "Filtering," on page 147](#).

## Microsoft DFS Namespace Support

Distributed File System (DFS) namespace technology helps Microsoft network administrators group shared folders located on different servers and presents them to users as a virtual tree of folders known as a namespace. Novell File Reporter now presents these namespaces as available storage resources that can be reported on.

# 1.8 New in Version 2.0

## Advanced Architecture

To provide expanded reporting capabilities Novell File Reporter 2.0 was built on a new advanced architecture that supports:

- ♦ Simultaneous integration with eDirectory and Active Directory
- ♦ An SQL database
- ♦ Web-based administration

## Easier Configuration and Management

All of the complex DSI installation and configuration tasks have been replaced with a simple installation and configuration wizard. Once installed, all management tasks are performed through a browser-based interface.

## New Reporting Capabilities

Novell File Reporter 2.0 has a much stronger tie-in to network directory services. File Reporter 2.0 authenticates to a primary identity system (either eDirectory or Active Directory) and then through a proxy, establishes a connection to the other identity system. You can be connected to one Active Directory domain and many eDirectory trees at the same time.

## New Reports

In addition to the extensive file report types in Version 1, Novell File Reporter 2.0 introduces:

- ♦ Permissions reports that identify who has access to a particular file or the access rights of a particular user

- ◆ Trending reports that show the growth of data on a Novell volume or Windows share over a period of time
- ◆ Detail reports that are specific to an individual user, file type, file, and more
- ◆ Aggregate reports that report on file and folders located on storage resources in eDirectory and Active Directory



# 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 15](#)
- ♦ [Section 2.2, “How File Reporter Works,” on page 15](#)

## 2.1 Micro Focus File Reporter

Micro Focus File Reporter inventories network file systems and delivers the detailed file storage intelligence you need to optimize and secure your network for efficiency and compliance. Engineered for enterprise file system reporting, File Reporter gathers data across the millions of files and folders scattered among the various network storage devices that make up your network. 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 on the network, 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.

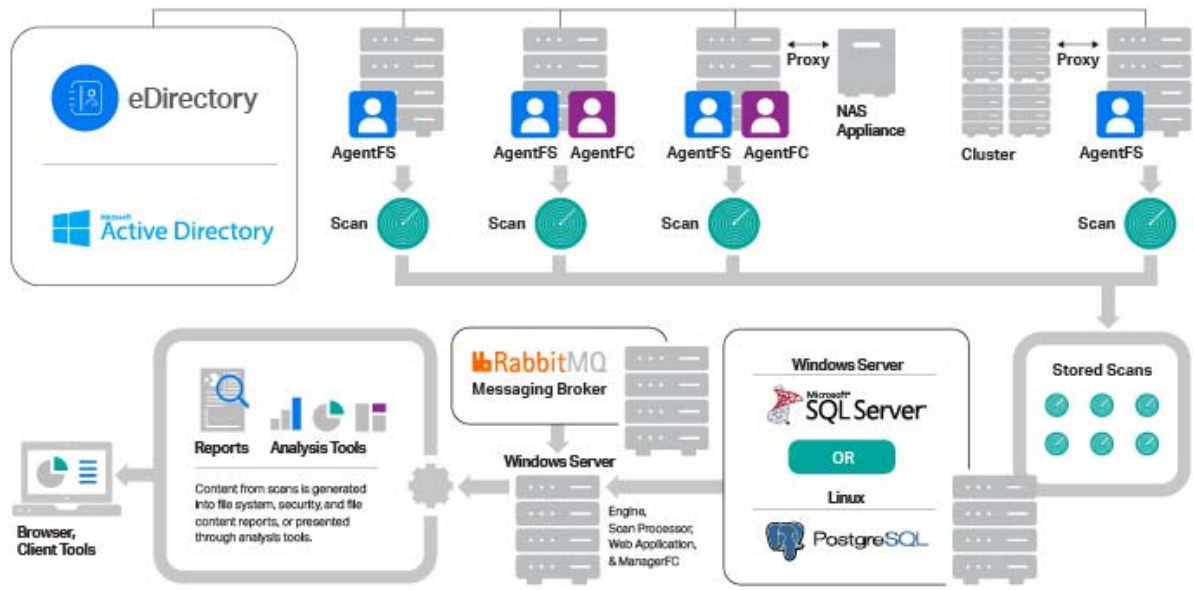
## 2.2 How File Reporter Works

- ♦ [Section 2.2.1, “Core Components,” on page 16](#)
- ♦ [Section 2.2.2, “File System Scanning,” on page 17](#)
- ♦ [Section 2.2.3, “File Content Scanning,” on page 18](#)
- ♦ [Section 2.2.4, “Reporting,” on page 19](#)
- ♦ [Section 2.2.5, “Client Tools,” on page 21](#)

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

To examine, report, and analyze this data efficiently, File Reporter disperses the work among a Web application, Engine, Agents, a Scan Processor, either a PostgreSQL or Microsoft SQL Server database, and either eDirectory or 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 and eDirectory objects
- ◆ Scans
- ◆ Identity system information such as names of eDirectory trees and Active Directory domains and forests
- ◆ Schedule information pertaining to scans and reports
- ◆ Notification information
- ◆ Report definitions
- ◆ Scan history
- ◆ Scan policies
- ◆ Volume free space

### 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 can run on Micro Focus Open Enterprise Server and Microsoft Windows Server hosts. Agents can examine and report on NSS and NTFS file systems. Additionally, Agents examine and report on file system security, including file and folder rights, trustee assignments, and permissions. For more information, see [Appendix D, "Agent Scan Capabilities," on page 159](#).

---

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

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

---

File Reporter includes the following file system Agents:

- ◆ **AgentFS:** Windows file system Agent that in most cases should replace any previous File Reporter Agents on Windows Server hosts. AgentFS performs file system scans (rather than file content scans) on Windows storage devices.
- ◆ **Legacy Agent for Windows:** Previous File Reporter Agent for performing file system scans on Windows Server hosts. You should only use this Agent when you need an Agent hosted on a Windows Server to function as a Proxy Agent for a Micro Focus Open Enterprise Server (OES) or NetWare server, as AgentFS cannot perform that function.

- ♦ **Agent for OES Linux:** Micro Focus OES hosted Agent that performs file system scans on OES or NetWare servers.

## Scans

Through one of the file system Agents (AgentFS, legacy Agent for Windows, or Linux Agent), File Reporter scans a storage resource. A storage resource can be a Micro Focus (formerly Novell) network server volume or 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 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 41.

---

### 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 only on a Windows Server and performs content scans only on files stored on Windows storage 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 Reporting

When File Reporter has a file system or file content 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.

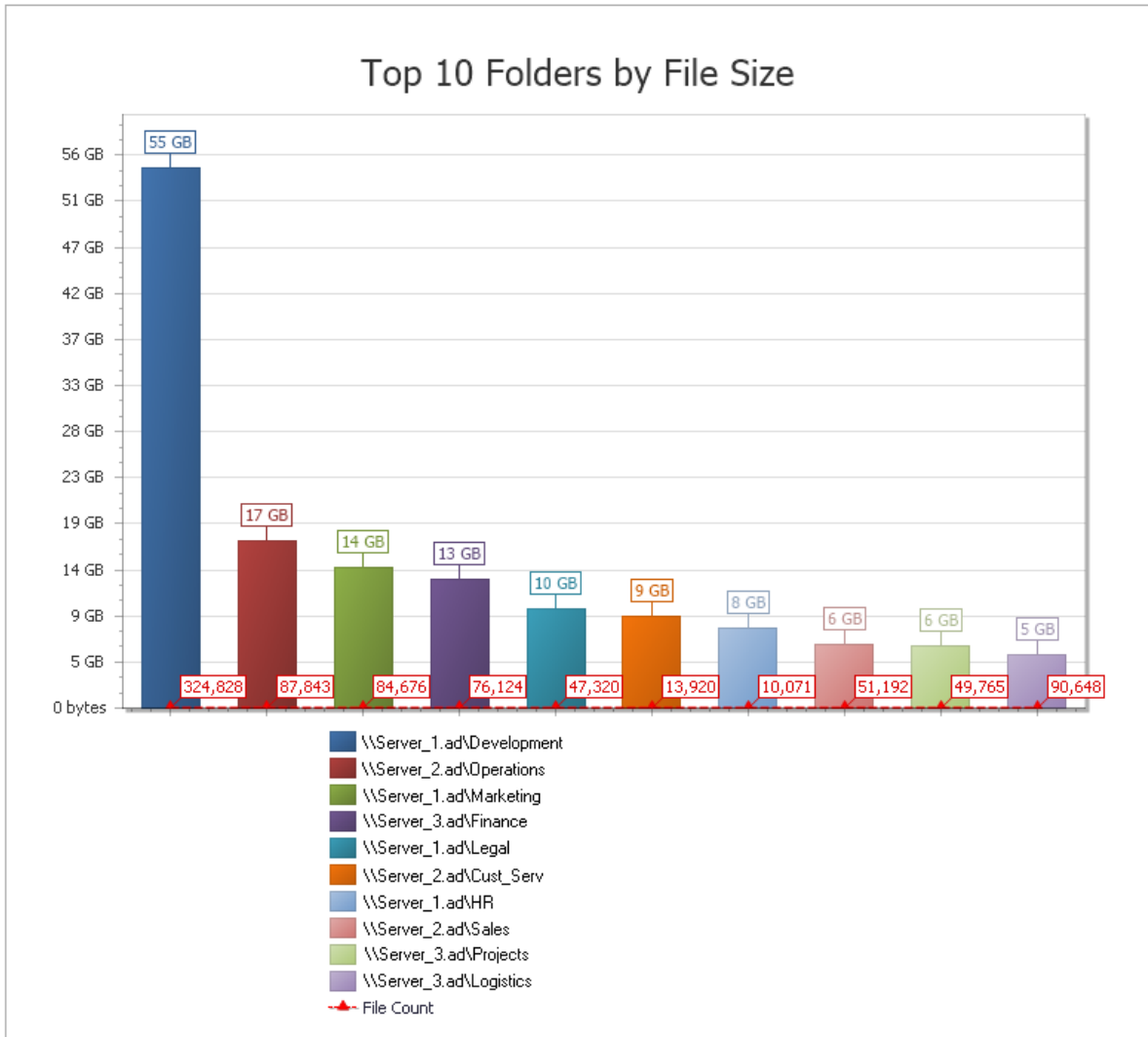
To generate a report, the Engine takes all of the needed scans that are applicable to the specifications of the report and consolidates them into a single report by indexing the applicable scans.

*Table 2-1 Built-in Report Types*

<b>File System Reports</b>	<b>Security Reports</b>	<b>Trending Reports</b>
Folder Summary	Assigned NCP Permissions	Volume Free Space
Detail Reports	Assigned NTFS Permissions	
File Extension	Permissions by Path	
Duplicate Files	Permissions by Identity	
Date-Age	Historic NCP Permissions Comparison	
Owner	Historic NTFS Permissions Comparison	
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



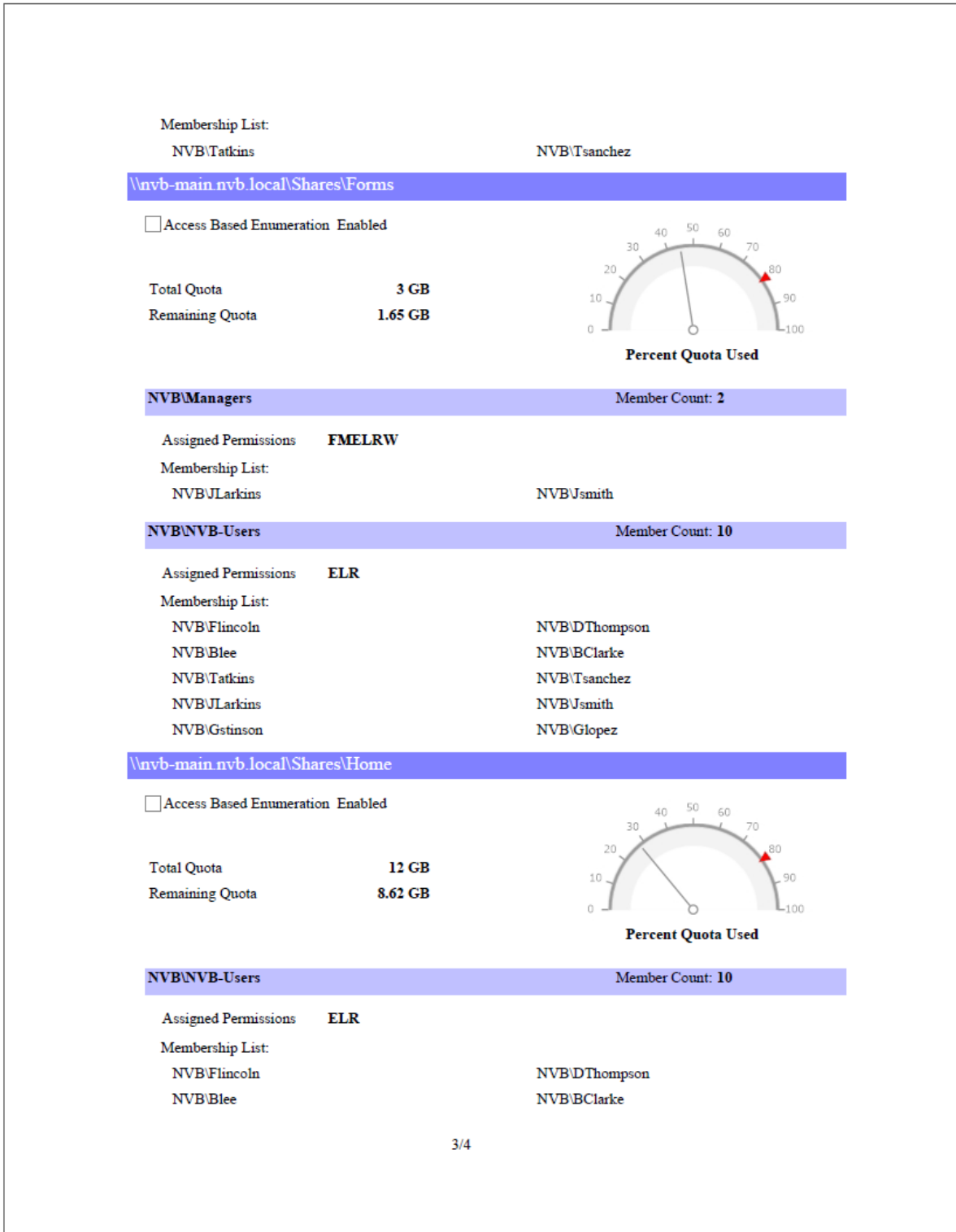
## Custom Query Reports

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 reports are delivered as Custom Query reports.

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



## 2.2.5 Client Tools

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

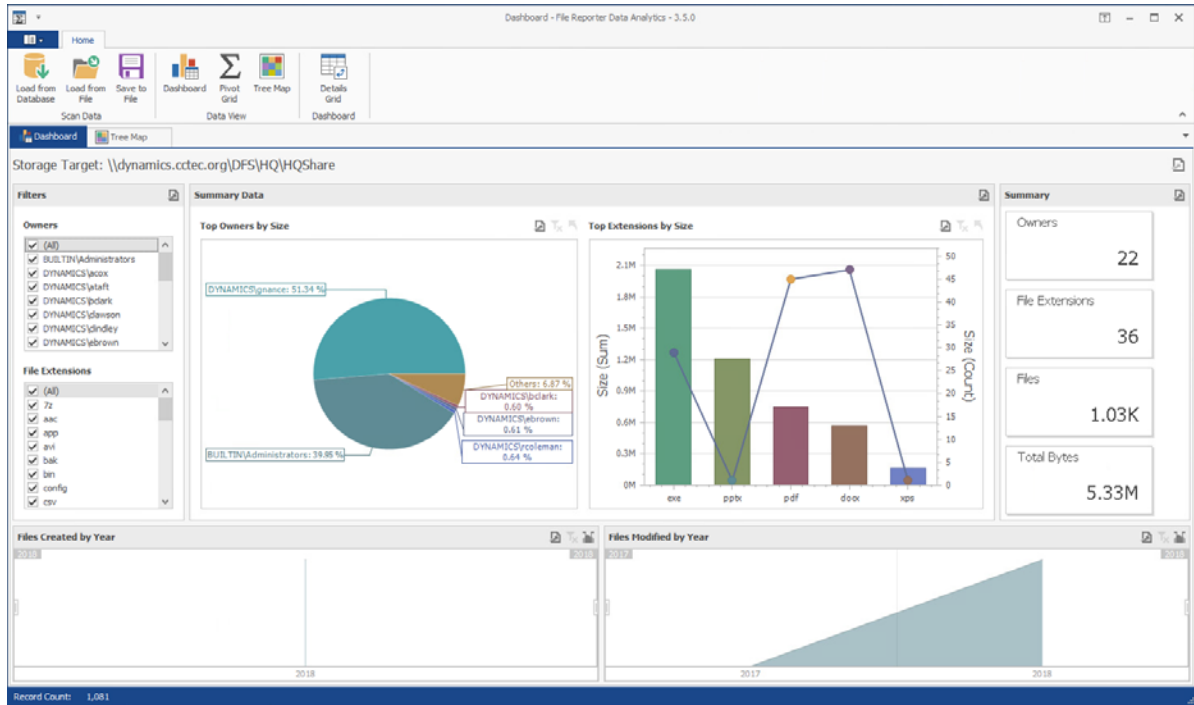
# Data Analytics

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.

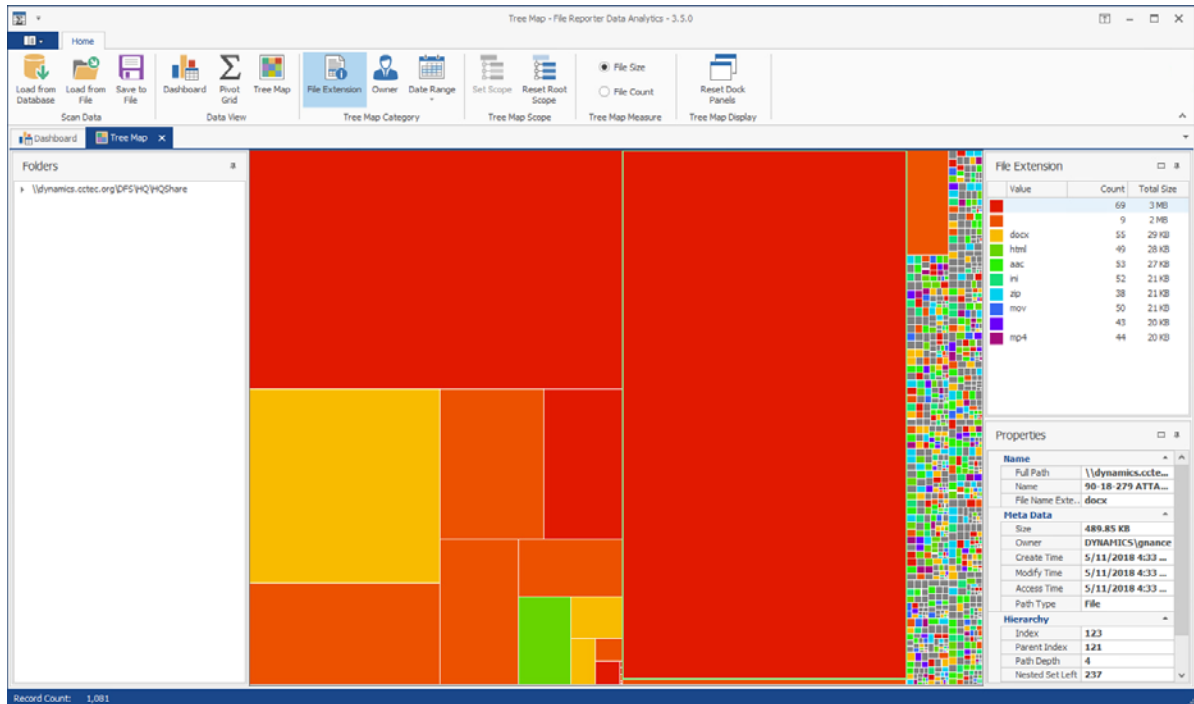
Figure 2-4 Dashboard



## Tree Map

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

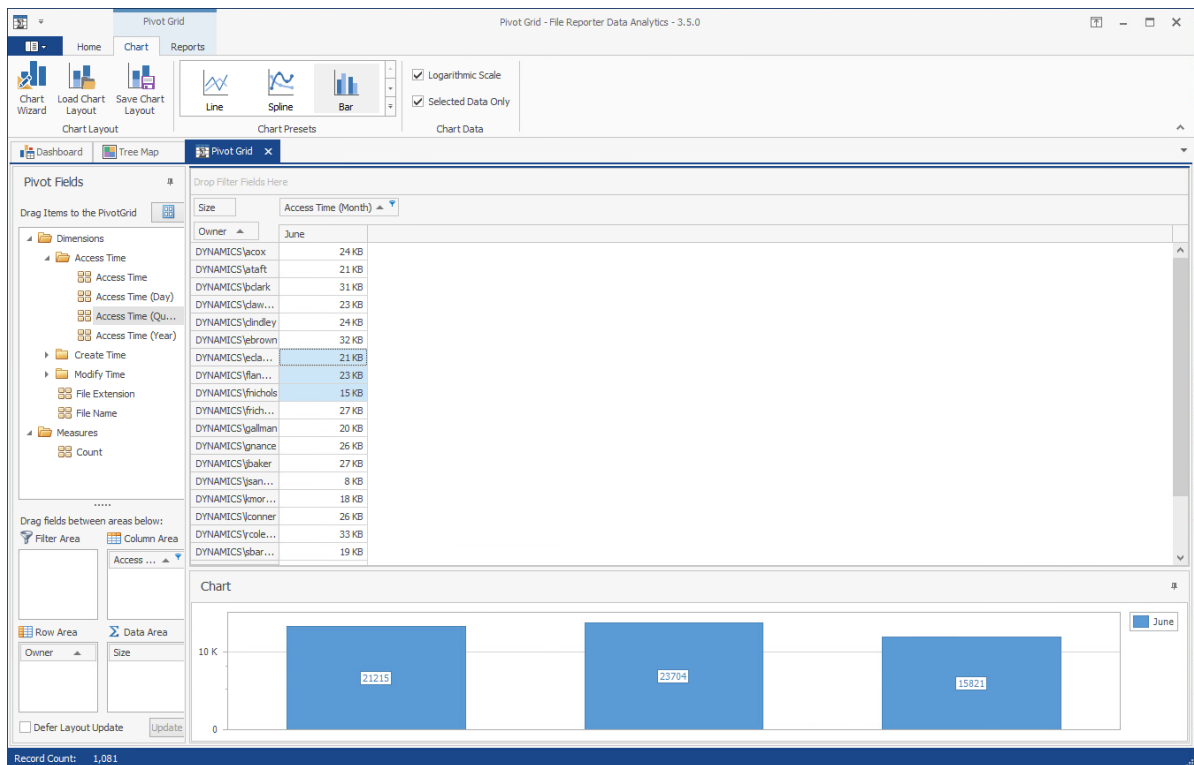
Figure 2-5 Tree Map



## Pivot Grid

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

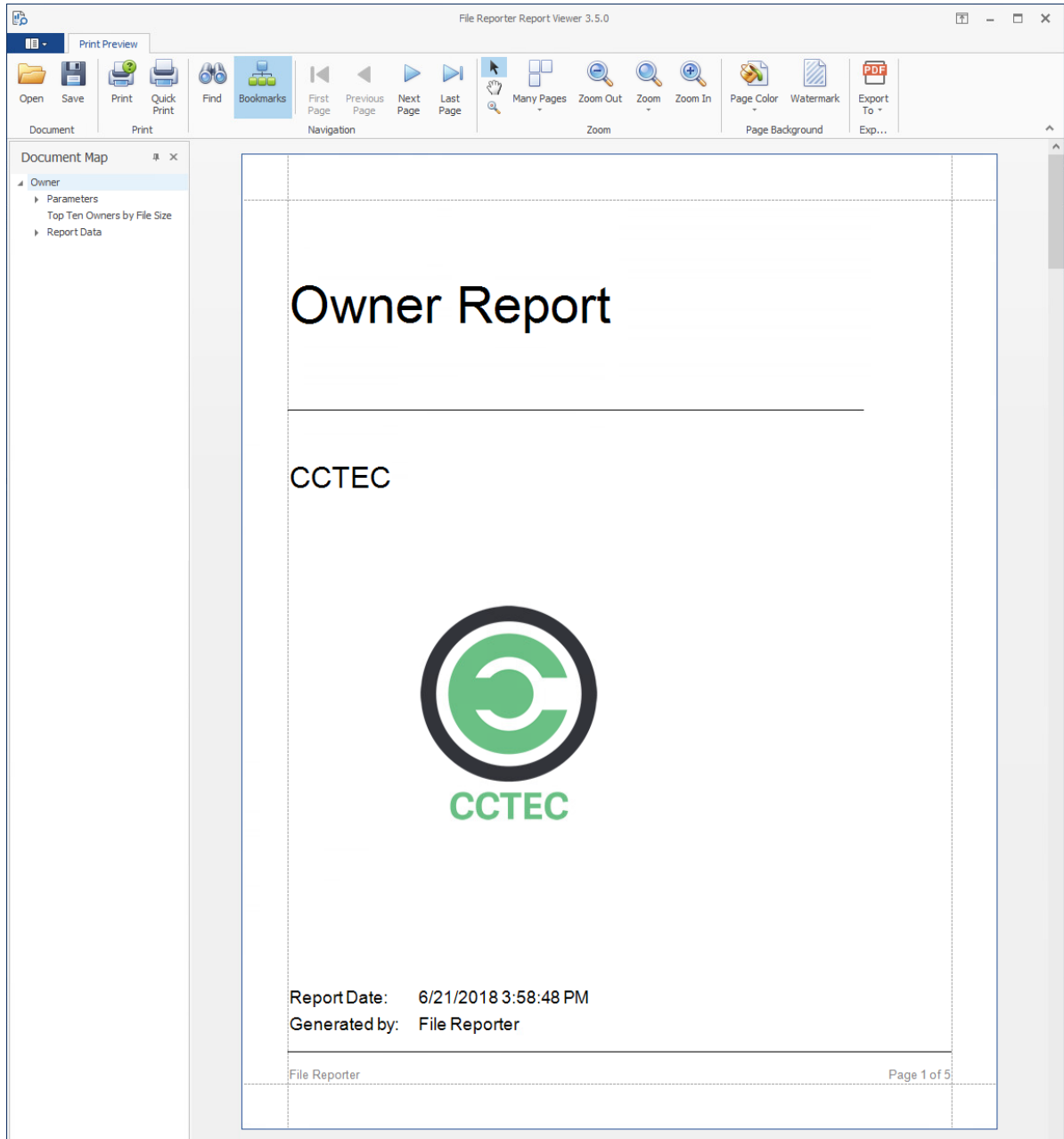
Figure 2-6 Pivot Grid



# Report Viewer

The Report Viewer lets you 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 25
- ◆ Section 3.2, “Launching the Administrative Interface,” on page 25
- ◆ Section 3.3, “Using the Administrative Interface,” on page 27

## 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

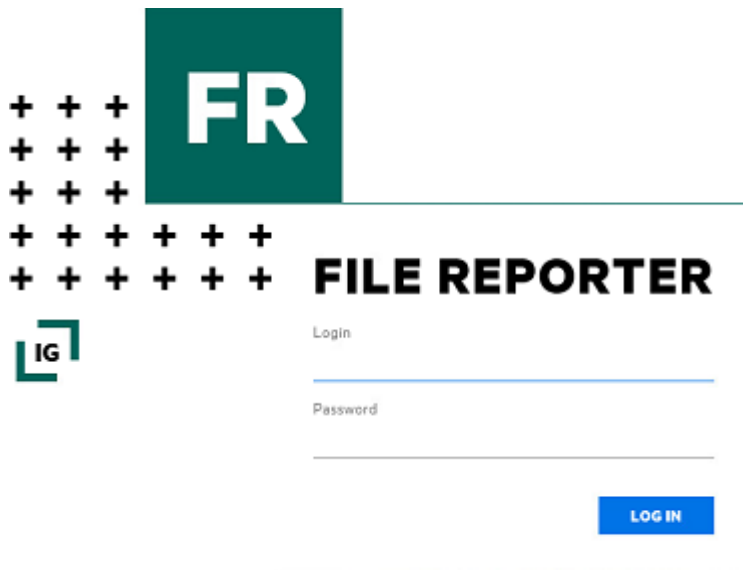
- 1 In the browser’s address bar, type:

`https://file_reporter_web_server_dns_name`

The DNS name is the one you created in “[Micro Focus File Reporter 3.6 Installation Guide](#).”

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

The login screen appears.



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

If you are authenticating to Active Directory, 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.

If you are authenticating to eDirectory, the username must be entered in typeless FDN:

*admin.mcirofocus*

The File Reporter Home page appears:

General	
<b>Version Info</b>	
Web Application	3.5.0.30
Engine	3.5.0.16
Scan Processor	3.5.0.2
Operating System	Microsoft Windows Server 2016 Standard
Database	SQL Server 14.0.1000.169
<b>License Info</b>	
License Type	Production
Identity System	DYNAMICS.CCTEC.ORG
Expiration Date	5/25/2019
Licensed Features	
<ul style="list-style-type: none"> <li>Active Directory Reporting</li> <li>eDirectory Reporting</li> <li>Content Analysis</li> <li>NSS AD Support</li> </ul>	
<b>Server Local Time</b>	
Current Time	2018-06-07 12:28:00 PM
Time Zone	Eastern Daylight Time (UTC -04:00)

Scans	
<b>File System Scan Policies</b>	
Scans In Progress	0
# Scans Last Day	0
# Scans Last Week	0
<b>File System Agents</b>	
Total Agents	2
<b>File System Scans Data Path</b>	
Total Space	99.51 GB
Free Space	73.95 GB
<b>File Content</b>	
Job Definitions	0
Classifications	4
Search Patterns	0
Agents	0

Reports	
<b>Report Definitions</b>	
<b>Report Generation</b>	
Reports In Progress	0
# Stored Reports	0
<b>Stored Report Storage</b>	
Bytes In Use	Not available
Free Bytes Remaining	Not available

Copyright 2018 © Condrey Corporation

## 3.3 Using the Administrative Interface

- ◆ Section 3.3.1, “Viewing Notifications,” on page 27
- ◆ Section 3.3.2, “Configuring the Web Interface,” on page 28
- ◆ Section 3.3.3, “Viewing System Information,” on page 29

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 **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.

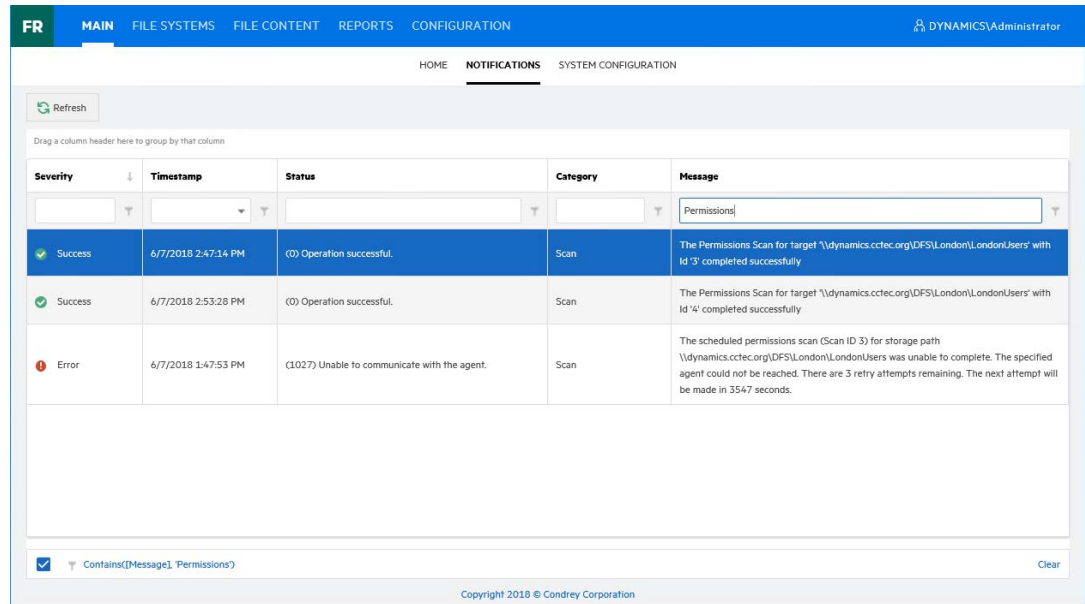
- 1 From the **Main** menu, select **Notifications**.

Severity	Timestamp	Status	Category	Message
Success	6/7/2018 2:53:59 PM	(0) Operation successful.	Scan	The File System Data Scan for target '\\dynamics.cctec.org\DFS\Atlanta\AtlantaShare' with Id '5' completed successfully
Info	6/7/2018 2:53:39 PM	(0) Operation successful.	Scan	The scheduled data scan for storage path '\\dynamics.cctec.org\DFS\Atlanta\AtlantaUsers' was canceled by an administrator.
Info	6/7/2018 2:53:39 PM	(0) Operation successful.	Scan	The scheduled data scan for storage path '\\dynamics.cctec.org\DFS\Atlanta\AtlantaShare' was canceled by an administrator.
Success	6/7/2018 2:53:28 PM	(0) Operation successful.	Scan	The Permissions Scan for target! '\\dynamics.cctec.org\DFS\London\LondonUsers' with Id '4' completed successfully
Success	6/7/2018 2:47:14 PM	(0) Operation successful.	Scan	The Permissions Scan for target! '\\dynamics.cctec.org\DFS\London\LondonUsers' with Id '3' completed successfully
Error	6/7/2018 2:38:00 PM	(1038) The specified agent name could not be found.	Scan	The scheduled data scan for storage path '\\dynamics.cctec.org\DFS\Atlanta\AtlantaUsers (Scan ID 2)' was unable to complete. The following error occurred: (1038) The specified agent name could not be found. There are 2 retry attempts remaining. The next attempt will be made in 3600

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 twice the column heading.
- 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**.

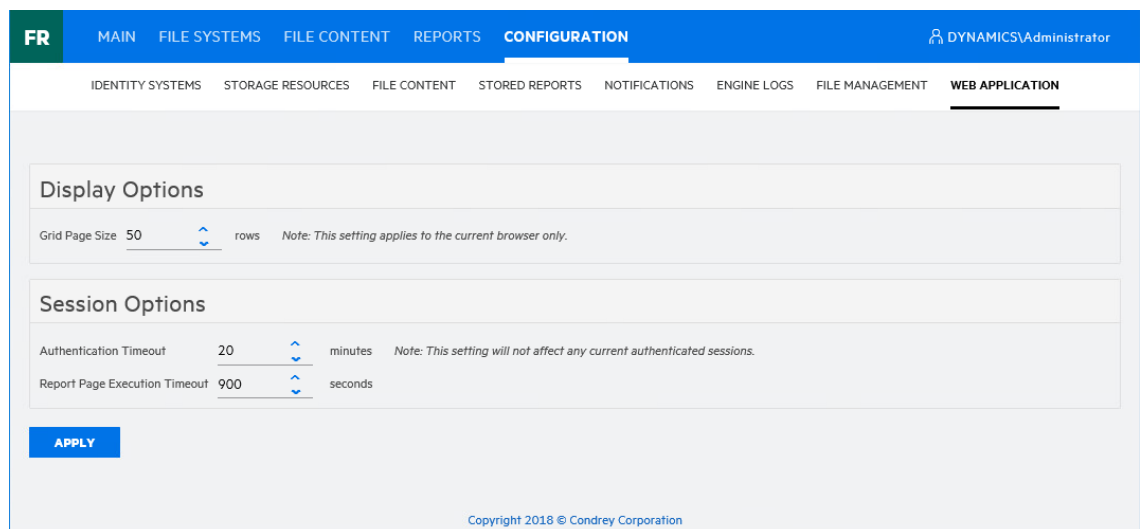
- 4c In the field to the left of the “pin” icon, enter the distinguishing word or letter for the filter.  
For example, Permissions.  
The page is updated according to the filtering parameters.



### 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 CONFIGURATION' page. The top navigation bar includes 'FR', 'MAIN', 'FILE SYSTEMS', 'FILE CONTENT', 'REPORTS', and 'CONFIGURATION'. The user is logged in as 'DYNAMICS\Administrator'. The main content area is divided into two sections:

- Database Statistics:** A table showing database details.

Category	Value
Microsoft SQL Server 2017 (RTM) - 14.0.1000.169 (X64)	Aug 22 2017 17:04:49
Database Version String	Copyright (C) 2017 Microsoft Corporation Standard Edition (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)
Database Total Size	83,886,080 bytes
Database Host Address	172.17.2.21
Database Name	srsdb
Database Schema Version	3.5.0.1
<b>Scans</b>	
Total Size of Scans	1,400,832 bytes
File System Metadata Scans	2
Permission Scans	2
Volume Trend Scans	0
<b>Identity System Data</b>	
Identity Systems Count	3
Identity System Cached Objects	44
Identity Systems Size	442,368 bytes
- Referenced Web Application Assemblies:** A table listing assemblies.

Name	Version	Processor Architecture
AlphaFS	2.2.0.0	None
Condrey.Srs.Core	3.5.0.2	None
Condrey.Srs.CoreExt	3.5.0.9	None
Condrey.Srs.Product	3.5.0.5	None
Condrey.Srs.ReportLibrary	3.5.0.1	None

The footer of the page reads 'Copyright 2018 © Condrey 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, “Enabling Other Identity Systems,” on page 31](#)
- ◆ [Section 4.2, “Viewing Storage Resources,” on page 35](#)
- ◆ [Section 4.3, “Assigning Proxy Targets,” on page 37](#)
- ◆ [Section 4.4, “Configuring Notifications,” on page 38](#)
- ◆ [Section 4.5, “Integrating with File Dynamics or Storage Manager,” on page 40](#)

## 4.1 Enabling Other Identity Systems

- ◆ [Section 4.1.1, “Enabling eDirectory,” on page 31](#)
- ◆ [Section 4.1.2, “Enabling Active Directory,” on page 33](#)

Your license file for File Reporter is either for Active Directory or eDirectory. If the File Reporter license file is for Active Directory, then Active Directory is the primary identity system. If the license file is for eDirectory, then eDirectory is the primary identity system.

File Reporter lets you enable other identity systems so that you can scan and report on the storage resources that are within those systems.

- ◆ [Section 4.1.1, “Enabling eDirectory,” on page 31](#)
- ◆ [Section 4.1.2, “Enabling Active Directory,” on page 33](#)

### 4.1.1 Enabling eDirectory

File Reporter allows you to enable multiple eDirectory trees as identity systems.

---

**IMPORTANT:** If you have Universal Passwords set up for all users in your tree, you must have the proper settings for File Reporter to work. Refer to [“Micro Focus File Reporter 3.6 Installation Guide”](#) for more information.

---

---

**IMPORTANT:** If your primary identity system is Active Directory and you want to enable eDirectory, you must first install the Client for Open Enterprise Server on the Windows server that is hosting the Engine.

---

- 1 Select **Configuration > Identity Systems**.

FR MAIN FILE SYSTEMS FILE CONTENT REPORTS CONFIGURATION DYNAMICS Administrator						
IDENTITY SYSTEMS STORAGE RESOURCES FILE CONTENT STORED REPORTS NOTIFICATIONS ENGINE LOGS FILE MANAGEMENT WEB APPLICATION						
Primary	Name	Type	Default Server	Proxy Credentials	Authenticated	
<input checked="" type="radio"/>	dynamics.ctec.org	Active Directory			<input checked="" type="checkbox"/>	

Copyright 2018 © Condrey Corporation

2 Click Add.

### Add eDirectory Identity System

eDirectory Authentication:

Default Server Address:

Username:

Password:

Tree Name:

Proxy Object FDN:

Assign Supervisor rights to [Root] for Proxy Account

**Default Server Address:** Specify the IP address of any server in the directory tree.

**Username:** Use typeless FDN format naming to specify an administrator name.

**Password:** Specify the administrator password.

**Tree Name:** Specify the name of the eDirectory tree.

**Proxy Object FDN:** Use typeless FDN format naming to specify a name for the proxy object that you are creating.

For example, MFRProxyObject.system



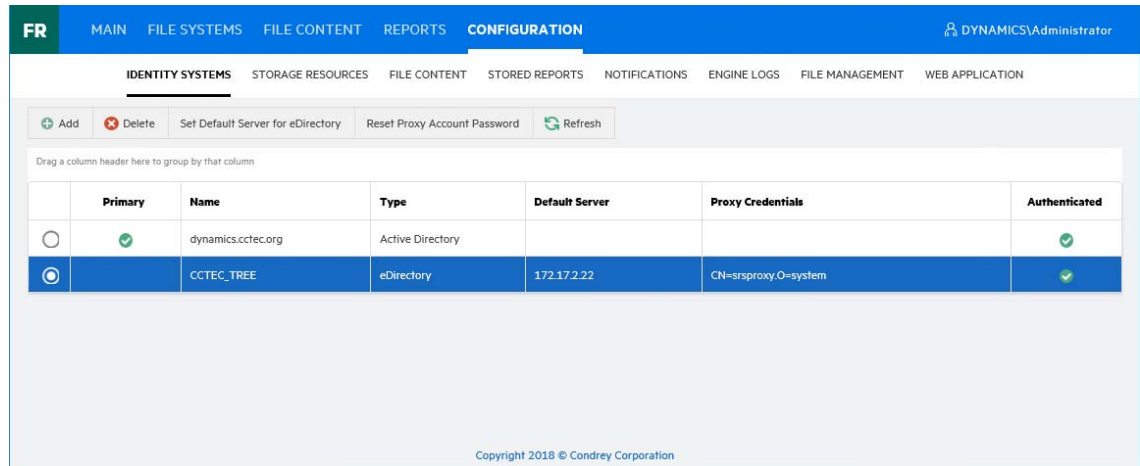
**Assign Supervisor rights to [Root] for Proxy Account:** Leaving this check box selected enables File Reporter to scan all volumes in the directory tree. If you deselect this option, the Agent can scan only those volumes to which the File Reporter proxy object has been given supervisor rights.

When this option is deselected, storage resources might not build properly.

We therefore recommend that this option remain selected.

**3** Complete the fields and click **OK**.

The eDirectory identity system is added.

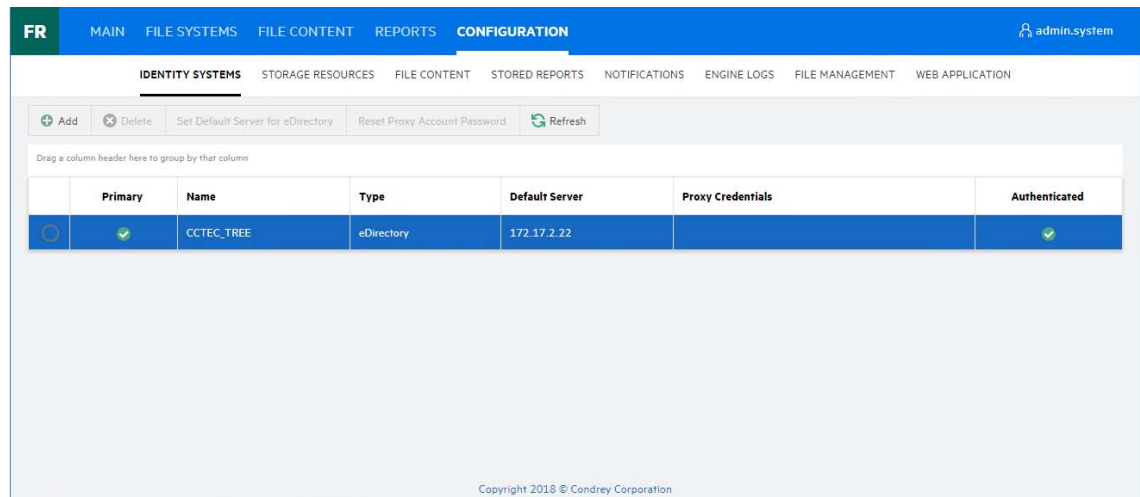


**4** (Optional) Repeat these steps to add additional eDirectory identity systems.

## 4.1.2 Enabling Active Directory

File Reporter allows you to enable only one Active Directory forest as an identity system.

**1** Select **Configuration > Identity Systems**.



**2** Click **Add**.

**3** In the **Identity System Type** region, click the **Active Directory** option.

**Add Identity System**

Identity System Type:

eDirectory  Active Directory

Domain Administrator Credentials:

Username:

Password:

Forest Root:

Proxy User: DYNAMICS\

Proxy Rights Group: DYNAMICS\

**OK** **CANCEL**

**Username:** Specify a username for an administrator in Active Directory.

**Password:** Specify the password for the administrator.

**Forest Root:** Because the Windows Engine host server is already part of a domain, the forest name is entered automatically.

**Proxy User:** Name the proxy user.

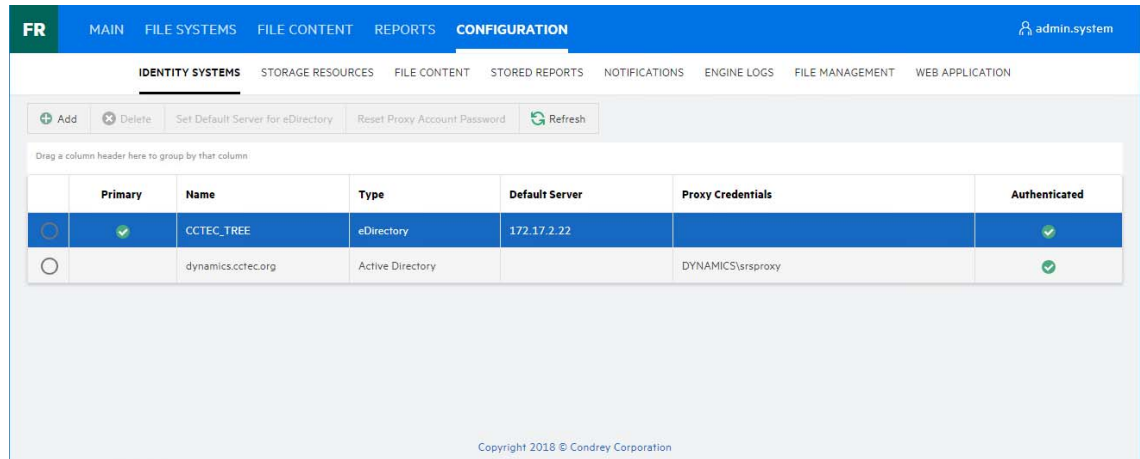
For example, `srsproxy`.

**Proxy Rights Group:** Name the proxy rights group.

For example, `srsproxyrights`.

**4** Click **OK**.

The Active Directory identity system is added.

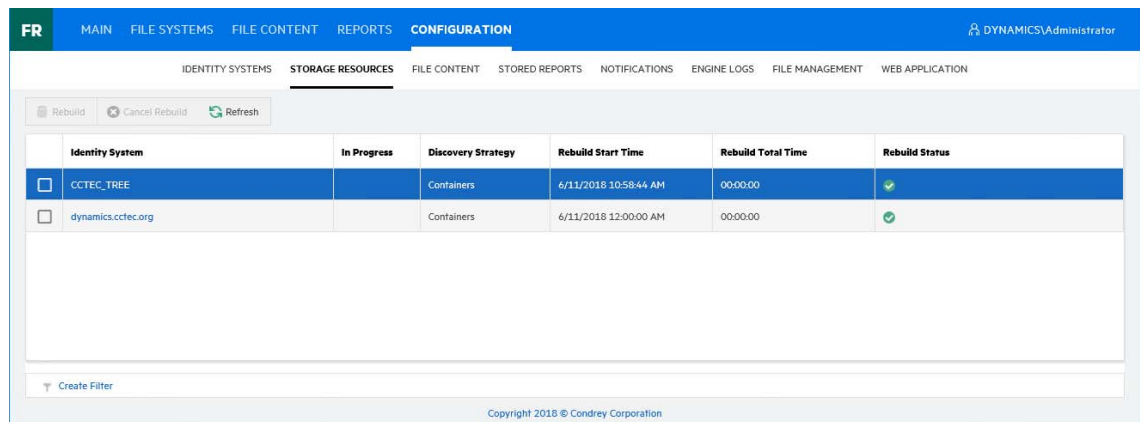


## 4.2 Viewing Storage Resources

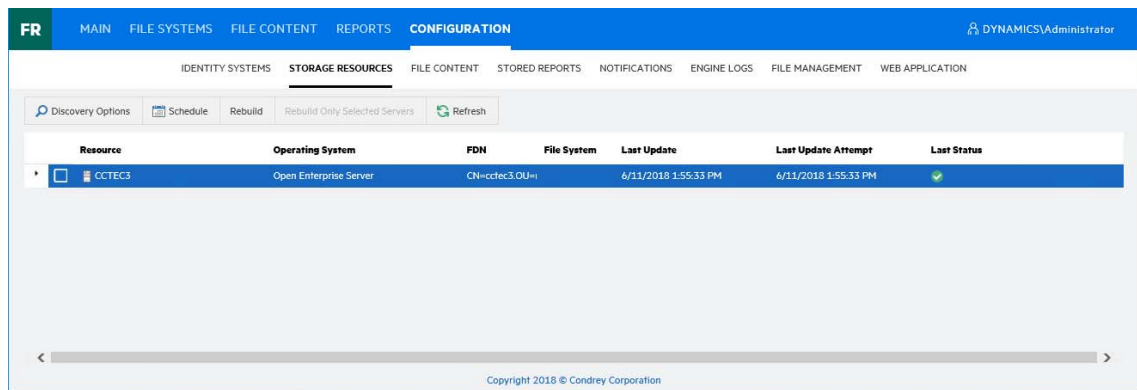
When an identity system has been enabled, the associated storage resources, which include Micro Focus volumes and Microsoft shares, are available for scanning and reporting.

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

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



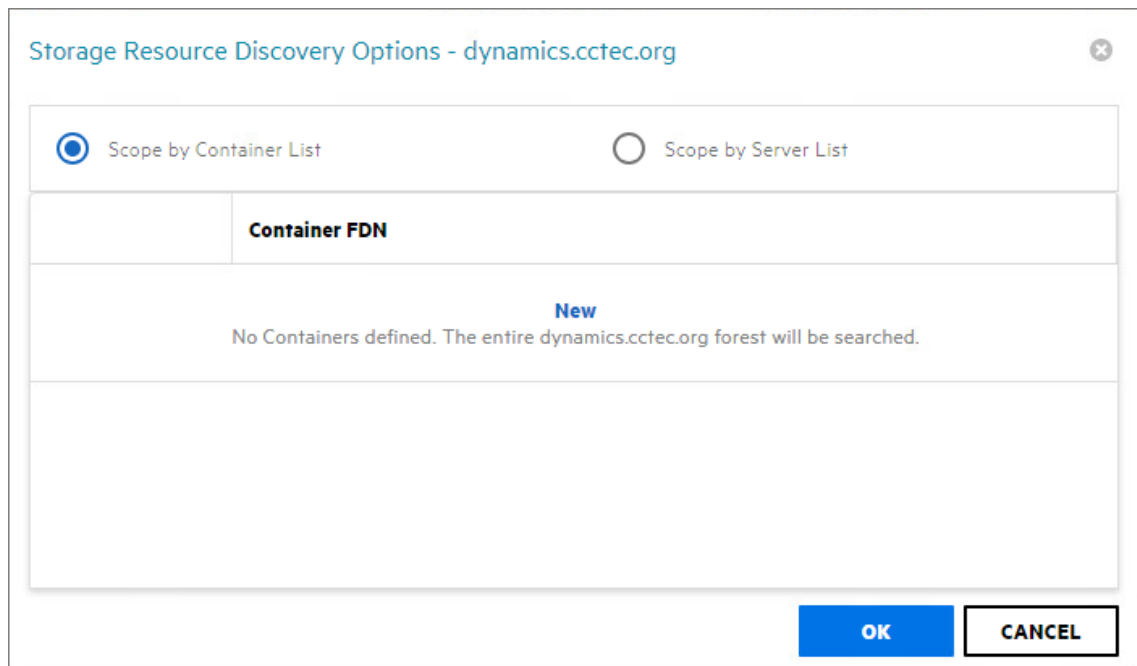
- 2 Select a check box pertaining to one of the listed eDirectory trees or Active Directory forests. The **Rebuild** button is enabled, allowing you to rebuild the storage resources for the selected eDirectory tree or Active Directory forest. You should rebuild the storage resources whenever you add a new server.
- 3 (Optional) Click **Rebuild** to rebuild the storage resources for the eDirectory tree or Active Directory forest.
- 4 Click one of the listed eDirectory trees or Active Directory forests.



All of the servers in the selected eDirectory tree or Active Directory forest are displayed.

5 Click each button to view options.

**Discovery Options:** For large organizations with eDirectory trees or Active Directory forests spanning multiple geographic areas, rebuilding the storage resources can take many hours. Rather than rebuilding the storage resources for the identity system, 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**.

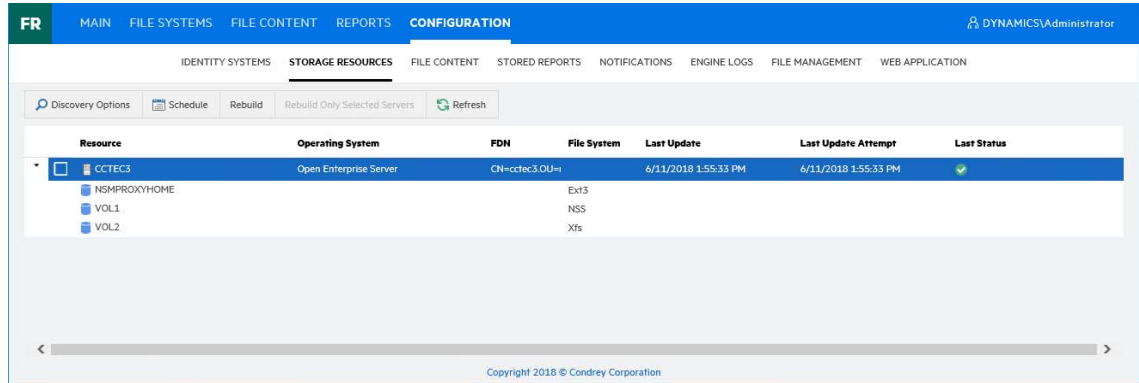
**Schedule:** By default, File Reporter rebuilds the identity system’s storage resources at 12:00 AM each day. Larger sites might want change this setting to weekly or on a specific day of the month. To do so, click this option and modify the settings in the dialog box.

**Rebuild:** Clicking this button automatically rebuilds the identity system’s storage resources.

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

**Refresh:** Refreshes the resource list.

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

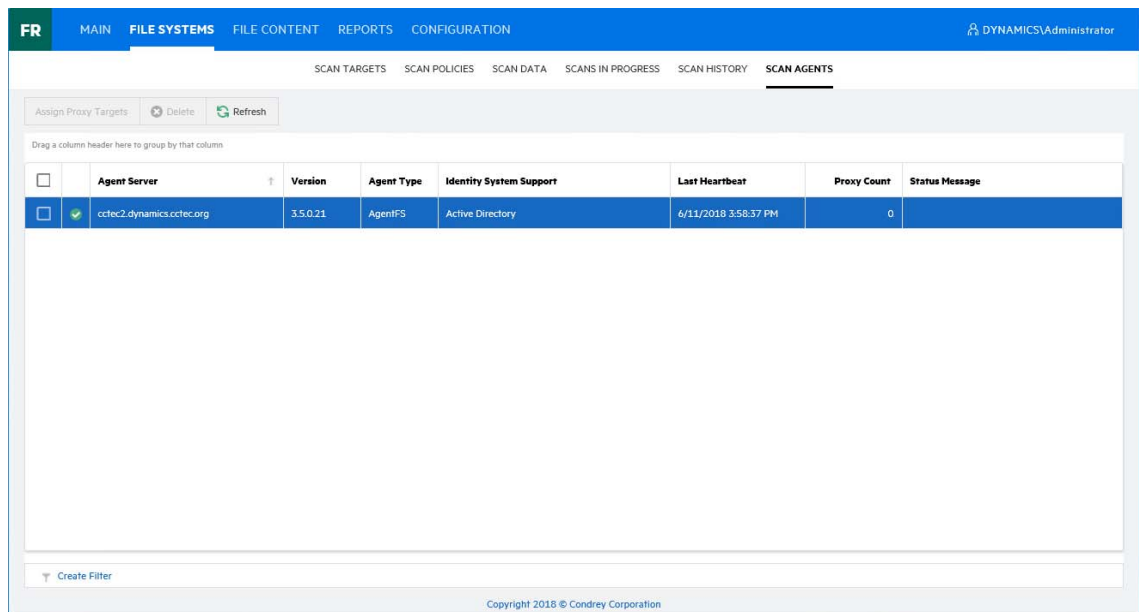


## 4.3 Assigning Proxy Targets

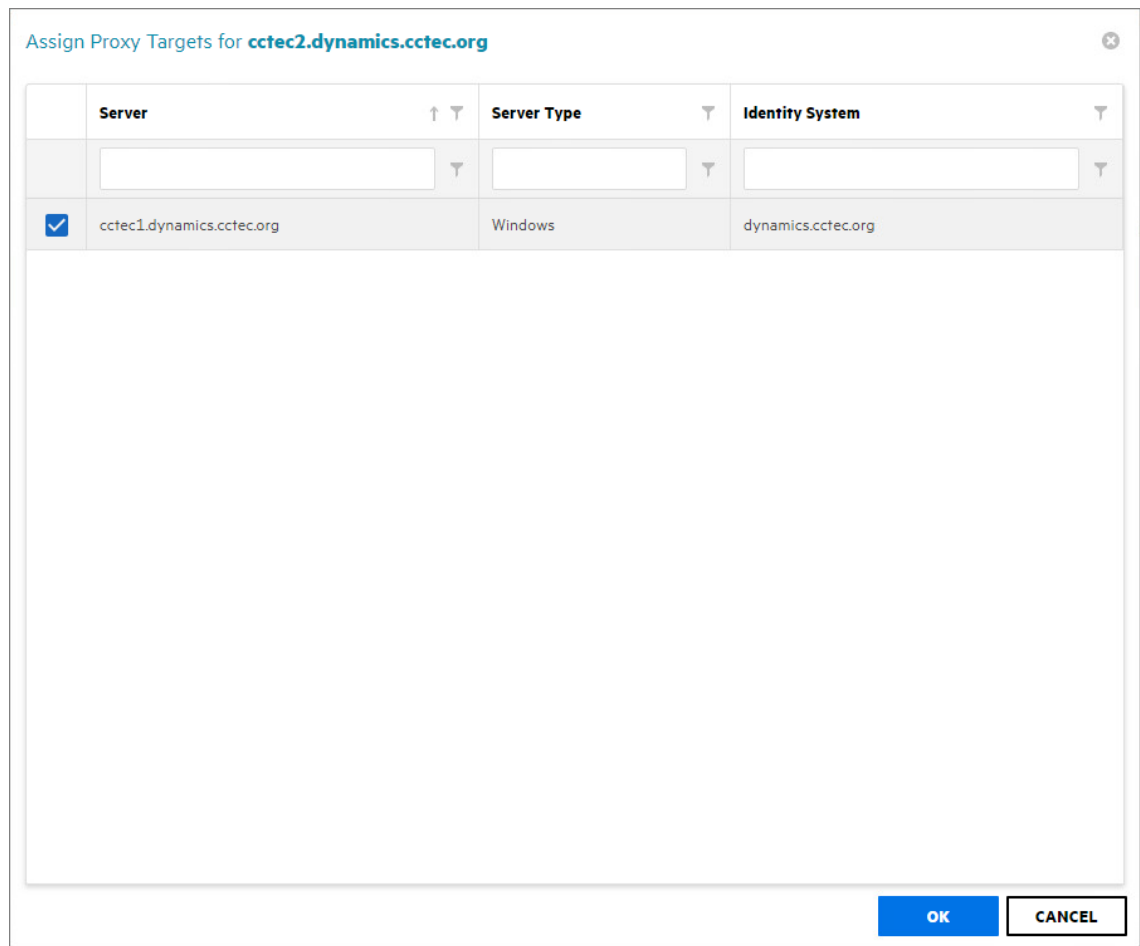
File Reporter does not include a NetWare Agent. Furthermore, an Agent cannot be deployed on a NAS device or server cluster. Additionally, only one Agent type (Legacy Agent, AgentFS, or AgentFC) can be hosted on a server. Finally, some organizations might not want Agents deployed on every server. In situations such as these, you can have a deployed Agent on another server function as a proxy agent.

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

All of the Agents are listed.



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



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

## 4.4 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 'CONFIGURATION' page in File Reporter. The 'NOTIFICATIONS' tab is selected. The 'Notification Settings' section includes a dropdown 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), 'From Email Address' (noreply@cctec.org), an unchecked checkbox for 'Use Authentication', 'Username' (mailuser), 'Password', and a spinner for 'Minutes to buffer multiple notifications for a single email' set to 1. A 'SAVE CHANGES' button is at the bottom left, and a copyright notice 'Copyright 2018 © Condrey Corporation' is at the bottom right.

**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 the primary identity system.

**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**.

## 4.5 Integrating with File Dynamics or Storage Manager

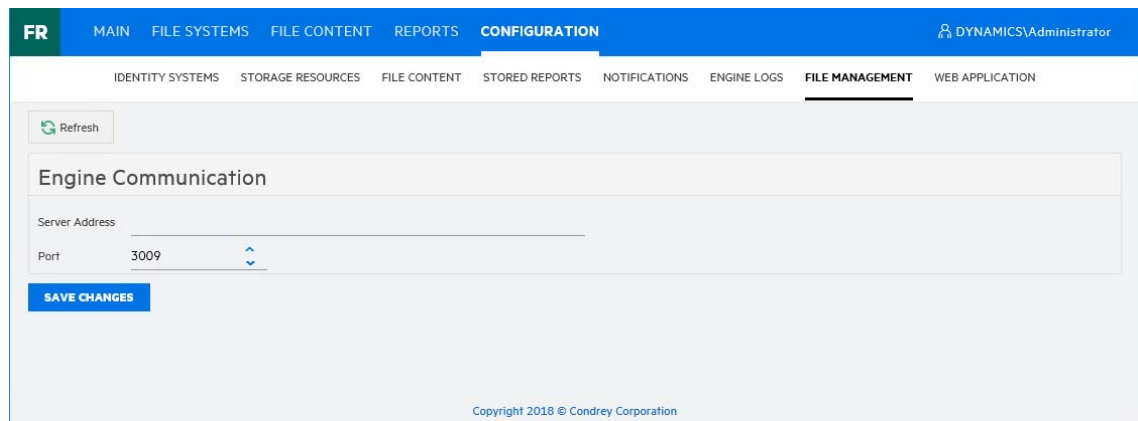
If you have Micro Focus File Dynamics or Micro Focus Storage Manager deployed, you can use Micro Focus File Reporter to report on File Dynamics or Storage Manager policies. Before you can do so, you must first specify the server address and port number of the server hosting the File Dynamics or Storage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

---

**IMPORTANT:** File Reporter 3.6 integrates with File Dynamics 6.0 and above and Storage Manager 5.0 or above.

---

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



The screenshot shows the File Reporter (FR) web interface. The top navigation bar includes 'MAIN', 'FILE SYSTEMS', 'FILE CONTENT', 'REPORTS', and 'CONFIGURATION'. The 'CONFIGURATION' menu is expanded, showing sub-menus: 'IDENTITY SYSTEMS', 'STORAGE RESOURCES', 'FILE CONTENT', 'STORED REPORTS', 'NOTIFICATIONS', 'ENGINE LOGS', 'FILE MANAGEMENT', and 'WEB APPLICATION'. The 'FILE MANAGEMENT' sub-menu is selected. The main content area is titled 'Engine Communication' and contains a 'Refresh' button, a 'Server Address' text input field, and a 'Port' dropdown menu currently set to '3009'. A blue 'SAVE CHANGES' button is located below the form. The footer of the page reads 'Copyright 2018 © Condrey Corporation'.

- 2 Specify the IP address or DNS name of the server hosting the File Dynamics or Storage Manager 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 41
- ◆ Section 5.2, “Adding a Scan Target,” on page 42
- ◆ Section 5.3, “Removing a Scan Target,” on page 44
- ◆ Section 5.4, “Creating Scan Policies,” on page 44
- ◆ Section 5.5, “Establishing a Baseline Scan,” on page 49
- ◆ Section 5.6, “Clearing a Baseline Scan,” on page 50
- ◆ Section 5.7, “Editing a Scan Policy,” on page 50
- ◆ Section 5.8, “Deleting a Scan Policy,” on page 50
- ◆ Section 5.9, “Scheduling Scans,” on page 50
- ◆ Section 5.10, “Editing a Scheduled Scan,” on page 52
- ◆ Section 5.11, “Clearing a Schedule on a Scheduled Scan,” on page 52
- ◆ Section 5.12, “Conducting an Immediate Scan,” on page 52
- ◆ Section 5.13, “Viewing Scans in Progress,” on page 52
- ◆ Section 5.14, “Retrying Failed Scans,” on page 53
- ◆ Section 5.15, “Viewing Scan Data,” on page 54
- ◆ Section 5.16, “Viewing Scan History,” on page 54
- ◆ Section 5.17, “Troubleshooting a Failed Scan,” on page 55

## 5.1 Scans

Through a Legacy Agent or AgentFS, Micro Focus File Reporter takes a file system “scan” of the file system’s storage resource at a given moment. A storage resource can be a Micro Focus network server volume or 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 volumes more often and scan the more static volumes 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 49](#).

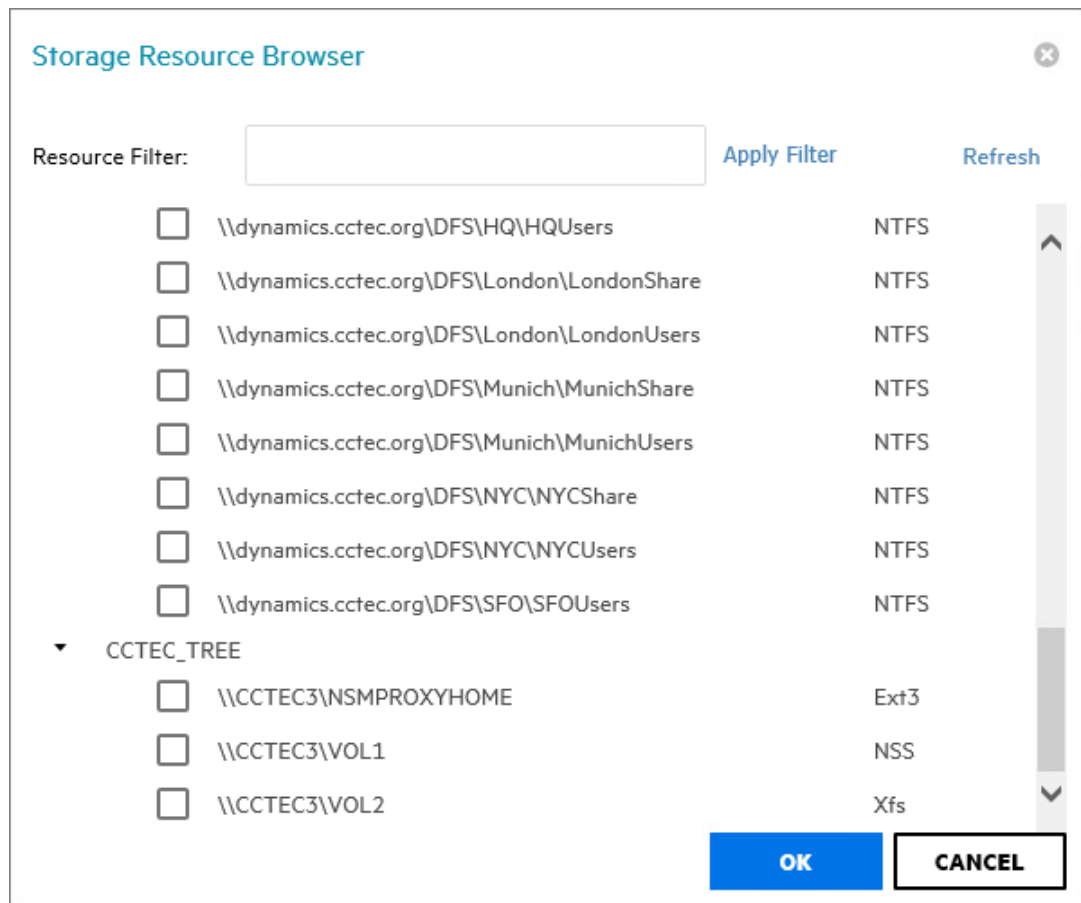
### Automatic Retention

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 44](#).

## 5.2 Adding a Scan Target

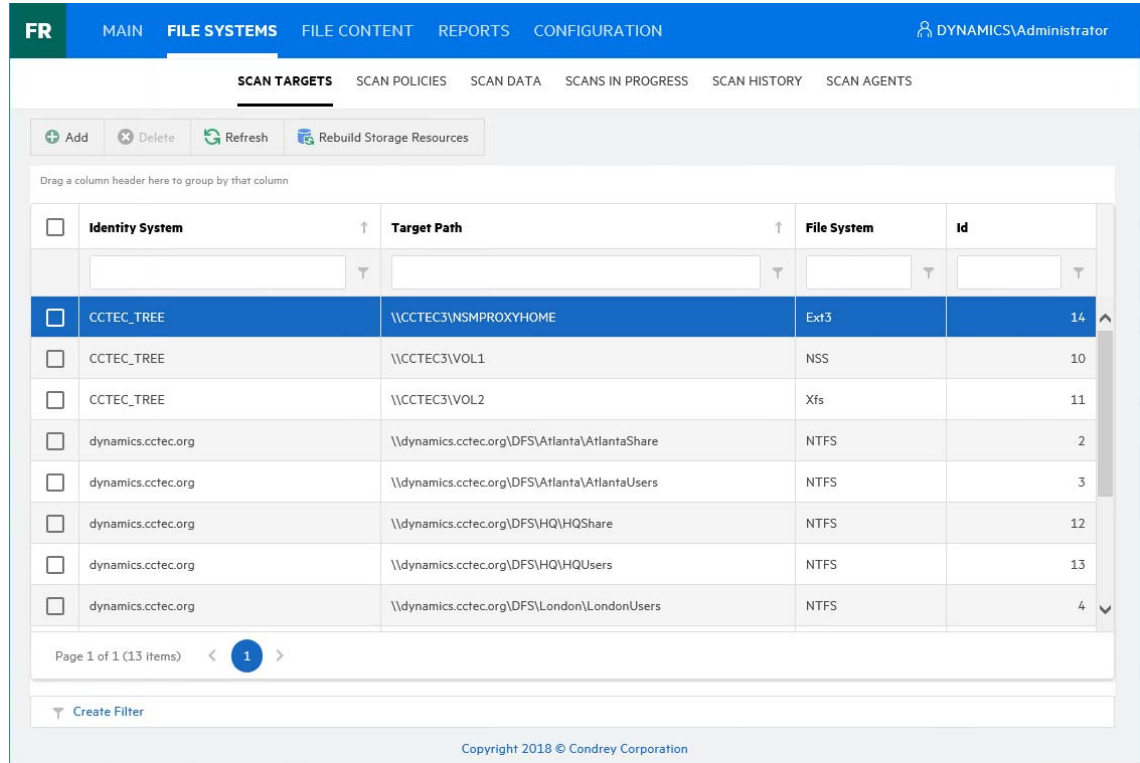
All volumes and shares must first be specified as a scan target before they can be scanned.

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



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

The scan targets are added.



## 5.3 Removing a Scan Target

- 1 Select **File Systems > Scan Targets**.
- 2 Select the check box pertaining to the volume or 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". It has a close button in the top right corner. The dialog contains the following elements:

- Policy Name:** A text input field with a vertical cursor.
- Policy Type:** A section containing three radio button options:
  - File System
  - Permissions
  - Volume Free Space
- Buttons:** A blue "OK" button and a white "CANCEL" button with a black border, located at the bottom right.

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 volume or share, the size of those files, when the files were last accessed, the locations of duplicate versions, and so forth.

**Permissions:** Scans the rights, trustee assignments, and permissions pertaining to the folders stored on the volumes or shares.

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

5 Click **OK**.

### Scan Policy Editor ✕

Name:

Description:

Retry Count:  ↕

Retry Interval:  ↕  ▼

Directory Quotas:  Scan Directory Quotas  
*Note that this may take a significant amount of time.*

Previous Scans:  Save Previous Scan

[Add](#) [Remove](#)

	Target Path

**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 86](#).

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 49](#).

---

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.

**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. For example, if you specify \\Pinyon\Vol1 in one File System scan, you cannot specify the same volume in another File System scan.

---

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

Scan Target Browser ✕

	Identity System	Target Path
	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	CCTEC_TREE	\\CCTEC3\NSMPROXYHOME
<input type="checkbox"/>	CCTEC_TREE	\\CCTEC3\VOL1
<input type="checkbox"/>	CCTEC_TREE	\\CCTEC3\VOL2
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\Atlanta\AtlantaShare
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\Atlanta\AtlantaUsers
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\HQ\HQShare
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\HQ\HQUsers
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\London\LondonUsers
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\Munich\MunichShare
<input type="checkbox"/>	dynamics.cctec.org	\\dynamics.cctec.org\DFS\Munich\MunichUsers

Page 1 of 2 (13 items) < **1** 2 >

- Click **OK** to save the scan policy.  
The scan policy is now displayed on the Scan Policies page.



FR MAIN FILE SYSTEMS FILE CONTENT REPORTS CONFIGURATION DYNAMICS Administrator									
SCAN TARGETS SCAN POLICIES SCAN DATA SCANS IN PROGRESS SCAN HISTORY SCAN AGENTS									
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Edit Schedule"/> <input type="button" value="Clear Schedule"/> <input type="button" value="Scan Now"/> <input type="button" value="Refresh"/>									
Drag a column header here to group by that column									
<input type="checkbox"/>	Policy Name ↑	Scan Type ↓	Target Paths	Save Previous	Schedule	Retry Count	Retry Interval	Id	
<input type="checkbox"/>	Atlanta File System	File System Data	2	No	[Not Scheduled]	3	60 minutes	1	
<input type="checkbox"/>	Atlanta User Permissions	Permissions	1	No	[Not Scheduled]	3	60 minutes	5	
<input type="checkbox"/>	CCTec Vol 1 Permissions	Permissions	1	Yes	[Not Scheduled]	3	60 minutes	8	
<input type="checkbox"/>	HQ File System	File System Data	1	No	[Not Scheduled]	3	60 minutes	7	
<input type="checkbox"/>	HQ Users File System	File System Data	1	No	[Not Scheduled]	3	60 minutes	6	
<input type="checkbox"/>	London Users Permissions	Permissions	1	No	[Not Scheduled]	3	60 minutes	3	
<input checked="" type="checkbox"/>	Munich Users FS Scan Policy	File System Data	1	No	Daily at 12:00 AM	3	60 minutes	4	
<input type="checkbox"/>	SFO Trending	Volume Free Space	1	(Yes)	[Not Scheduled]	3	60 minutes	9	

Page 1 of 1 (8 Items) < 1 >

Create Filter

Copyright 2018 © Condrey Corporation

The scan policy still needs to be scheduled. For procedures on scheduling scans, go to [Section 5.9, “Scheduling Scans,”](#) on page 50.

## 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 create a 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 C	Next Retry Time	Last Error	
<input type="checkbox"/>	11	\\dynamics.ctec.org\DFS\Atlanta\AtlantaUsers	Atlanta User Permissions	Permissions	CTEC2	6/12/2018 12:15:34 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	10	\\dynamics.ctec.org\DFS\Munich\MunichUsers	Munich Users FS Scan Policy	File System Data	CTEC2	6/12/2018 12:15:34 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	9	\\dynamics.ctec.org\DFS\London\LondonUsers	London Users Permissions	Permissions		6/12/2018 12:15:34 PM	Waiting for Retry	1	6/12/2018 1:15:00 PM	(-1) An unspecified error has occurred.
<input type="checkbox"/>	8	\\dynamics.ctec.org\DFS\Atlanta\AtlantaUsers	Atlanta File System	File System Data	CTEC2	6/12/2018 12:15:34 PM	Scan in Progress	0		(0) Operation successful.
<input type="checkbox"/>	7	\\dynamics.ctec.org\DFS\Atlanta\AtlantaShare	Atlanta File System	File System Data	CTEC2	6/12/2018 12:15:34 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**.

Scan Id	Scan Target	Scan Type	State	Baseline	Triggered Scan Time	Policy	Agent	Status
10	\\dynamics.cctec.org\DFS\Munich\MunichUsers	File System Data	Current	False	6/12/2018 12:15:34 PM	Munich Users FS Scan Policy	CCTEC2	(0) Operation successful.
11	\\dynamics.cctec.org\DFS\Atlanta\AtlantaUsers	Permissions	Current	False	6/12/2018 12:15:34 PM	Atlanta User Permissions	CCTEC2	(0) Operation successful.
8	\\dynamics.cctec.org\DFS\Atlanta\AtlantaUsers	File System Data	Current	False	6/12/2018 12:15:34 PM	Atlanta File System	CCTEC2	(0) Operation successful.
7	\\dynamics.cctec.org\DFS\Atlanta\AtlantaShare	File System Data	Current	False	6/12/2018 12:15:34 PM	Atlanta File System	CCTEC2	(0) Operation successful.
4	\\dynamics.cctec.org\DFS\London\LondonUsers	Permissions	Current	True	6/7/2018 2:53:18 PM	London Users Permissions	CCTEC2	(0) Operation successful.

## 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
8	6/12/2018 12:15:34 PM	\\dynamics.cctec.org	Atlanta File System	File System Data	CCTEC2	00:00:00:00:00	00:00:00:00:253	5	35	(0) - Success
7	6/12/2018 12:15:34 PM	\\dynamics.cctec.org	Atlanta File System	File System Data	CCTEC2	00:00:00:00:00	00:00:00:00:564	0	8	(0) - Success
6	6/7/2018 2:53:52 PM	\\dynamics.cctec.org	Atlanta File System	File System Data	CCTEC2	00:00:00:01:00	00:00:00:00:333	5	35	(0) - Success
5	6/7/2018 2:53:52 PM	\\dynamics.cctec.org	Atlanta File System	File System Data	CCTEC2	00:00:00:01:00	00:00:00:00:207	0	8	(0) - Success
4	6/7/2018 2:53:18 PM	\\dynamics.cctec.org	London Users Permissions	Permissions	CCTEC2	00:00:00:03:00	00:00:00:00:560	0	1	(0) - Success
3	6/7/2018 1:47:52 PM	\\dynamics.cctec.org	London Users Permissions	Permissions	CCTEC2	00:00:00:04:00	00:00:00:02:890	0	1	(0) - Success
2	6/7/2018 1:38:42 PM	\\dynamics.cctec.org	Atlanta File System	File System Data		00:00:00:00:00	00:00:00:00:00	0	0	(68) - Scan canceled by user.
1	6/7/2018 1:38:42 PM	\\dynamics.cctec.org	Atlanta File System	File System Data		00:00:00:00:00	00:00:00:00:00	0	0	(68) - Scan canceled by user.

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 When scanning Windows storage resources, 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 153](#).





# 6 Generating File System Reports

- ◆ Section 6.1, “Overview,” on page 57
- ◆ Section 6.2, “Changing Your Cover Sheet Branding,” on page 58
- ◆ Section 6.3, “Changing the Report Data Font,” on page 59
- ◆ Section 6.4, “Built-in Report Types,” on page 60
- ◆ Section 6.5, “Directory Data Reports,” on page 60
- ◆ Section 6.6, “Permissions Reports,” on page 71
- ◆ Section 6.7, “File Data Reports,” on page 76
- ◆ Section 6.8, “Historic Comparison Reports,” on page 86
- ◆ Section 6.9, “Trending Report,” on page 91
- ◆ Section 6.10, “Custom Query Reports,” on page 92
- ◆ Section 6.11, “Unformatted Reports,” on page 95
- ◆ Section 6.12, “Micro Focus File Dynamics and Storage Manager Policy Reports,” on page 96
- ◆ Section 6.13, “Scheduling Reports,” on page 96
- ◆ Section 6.14, “Editing a Scheduled Report,” on page 98
- ◆ Section 6.15, “Clearing a Schedule on a Scheduled Report,” on page 98
- ◆ Section 6.16, “Copying a Report Definition,” on page 98
- ◆ Section 6.17, “Viewing Reports in Progress,” on page 99
- ◆ Section 6.18, “Troubleshooting Reports,” on page 100

## 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 identity system 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,” on page 147](#).

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.

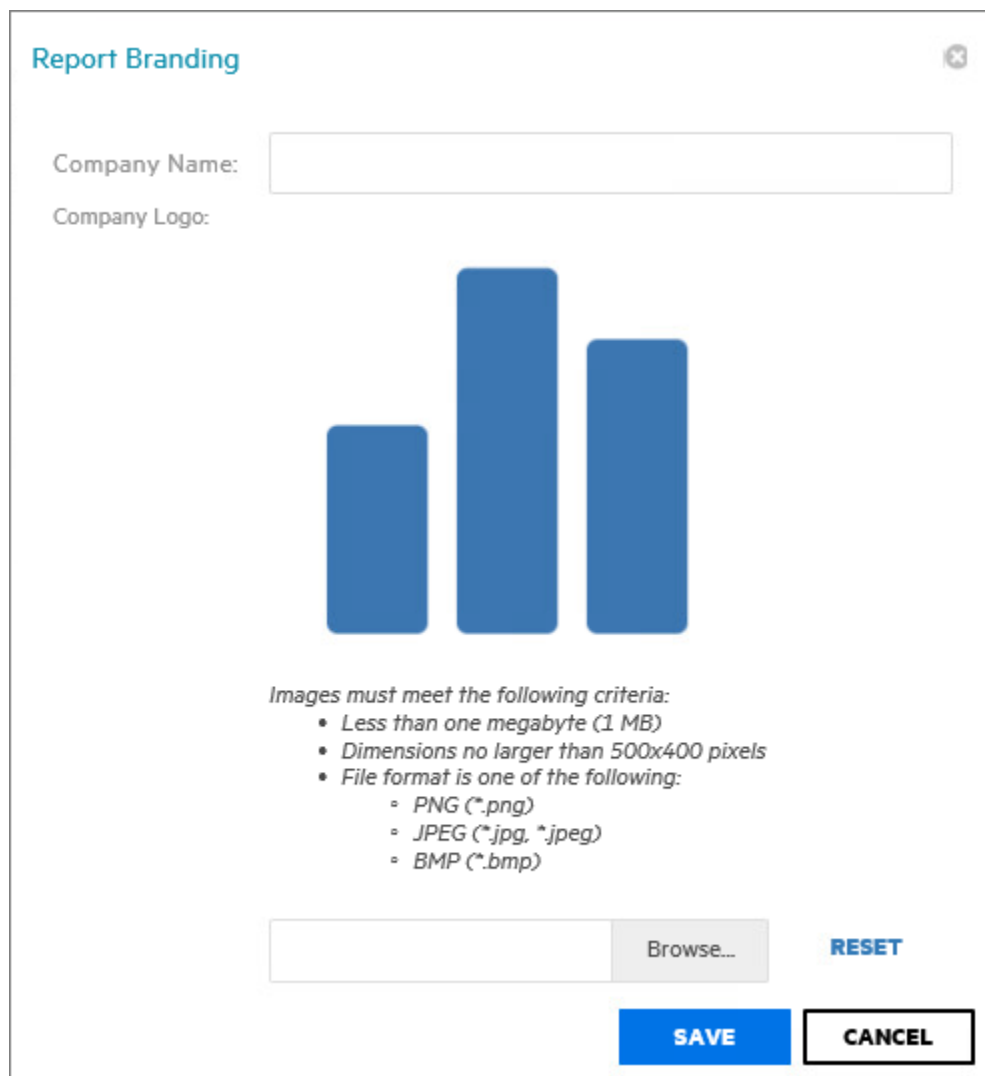
You can generate Detailed Reports from certain built-in report types. For example, a File Extension Report can be the means of generating a Detailed Report that includes the specific details of all of the \*.mov files.

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

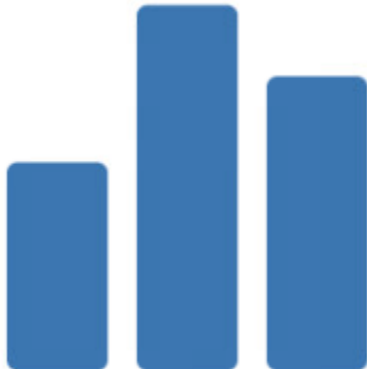
All generated built-in reports include a cover sheet that includes a default graphic. If you want, you can replace it with your organization's logo.

- 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)

Browse... **RESET**

**SAVE** **CANCEL**

- 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.

**Report Branding**

Company Name: CCTEC

Company Logo:

**CCTEC**

*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)

Browse... RESET SAVE CANCEL

- 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](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 four 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 60](#)
- ◆ [Section 6.6, “Permissions Reports,” on page 71](#)
- ◆ [Section 6.7, “File Data Reports,” on page 76](#)
- ◆ [Section 6.9, “Trending Report,” on page 91](#)
- ◆ [Section 6.11, “Unformatted Reports,” on page 95](#)

## 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 volumes or shares you want to report on.

- ◆ [Section 6.5.1, “Generating a Summary Report,” on page 61](#)
- ◆ [Section 6.5.2, “Generating a Directory Quota Report,” on page 68](#)

- ♦ [Section 6.5.3, “Generating a Storage Cost Report,”](#) on page 69
- ♦ [Section 6.5.4, “Generating a Comparison Report,”](#) on page 70

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

**Permissions**

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

**Historic Comparison**

- File System Comparison
- NCP Permissions 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**.

Report Definition Editor - Atlanta User Share Summary Report

Name: Atlanta User Share Summary Report

Type: Summary Report

Description: Report Definition created on 6/13/2018 9:15:15 AM by DYNAMICS\Administrator

Report Path Depth: 0

Initial Chart Path Depth: 0

**i** A Report Path Depth greater than 3 or 4 may result in significant report size and processing time.

**TARGET PATHS**    **FILE MANAGEMENT POLICIES**

Add    Remove

Target Path

**SAVE**    **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.

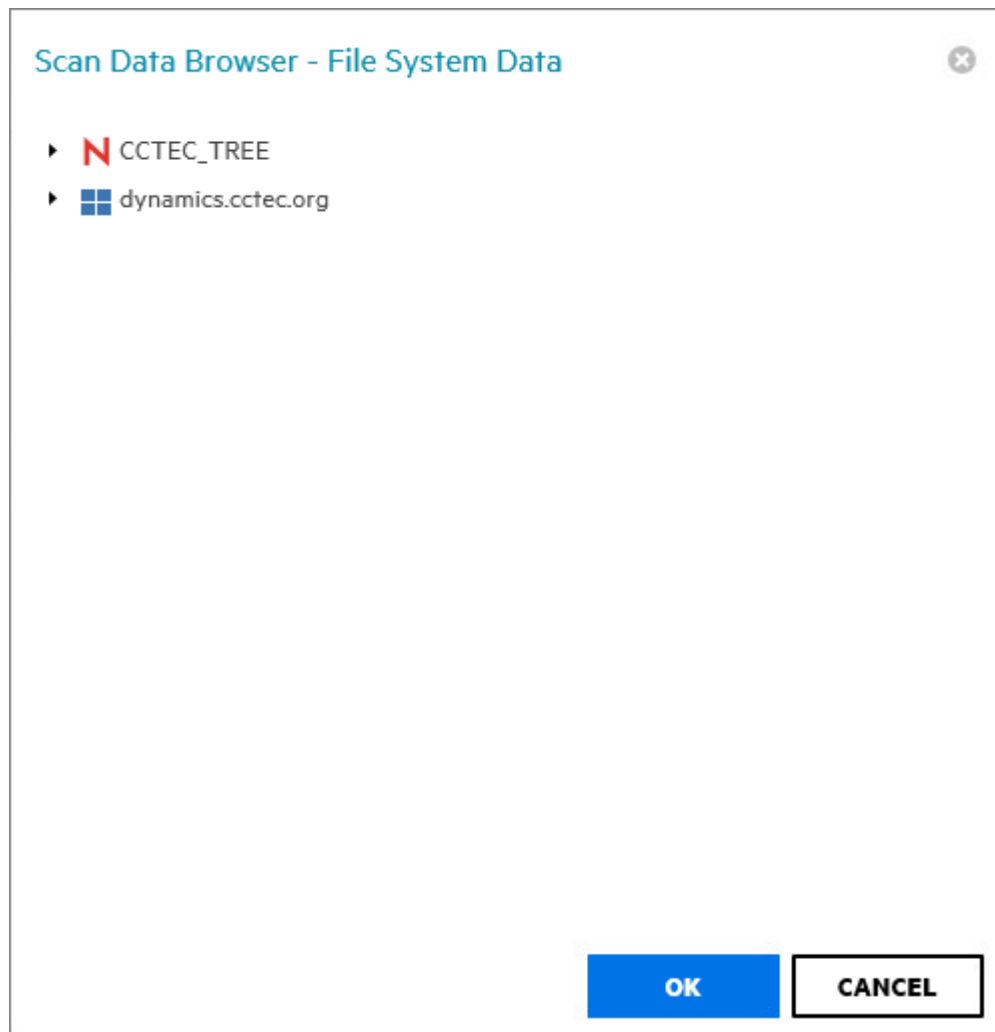
For example, for a server named Las Vegas, the Summary report would list the contents of these paths:

```
\\lasvegas.nvb.local\Users1
\\lasvegas.nvb.local\Users1\a
\\lasvegas.nvb.local\Users1\a\stuff
\\lasvegas.nvb.local\Users1\a\stuff\morestuff
```

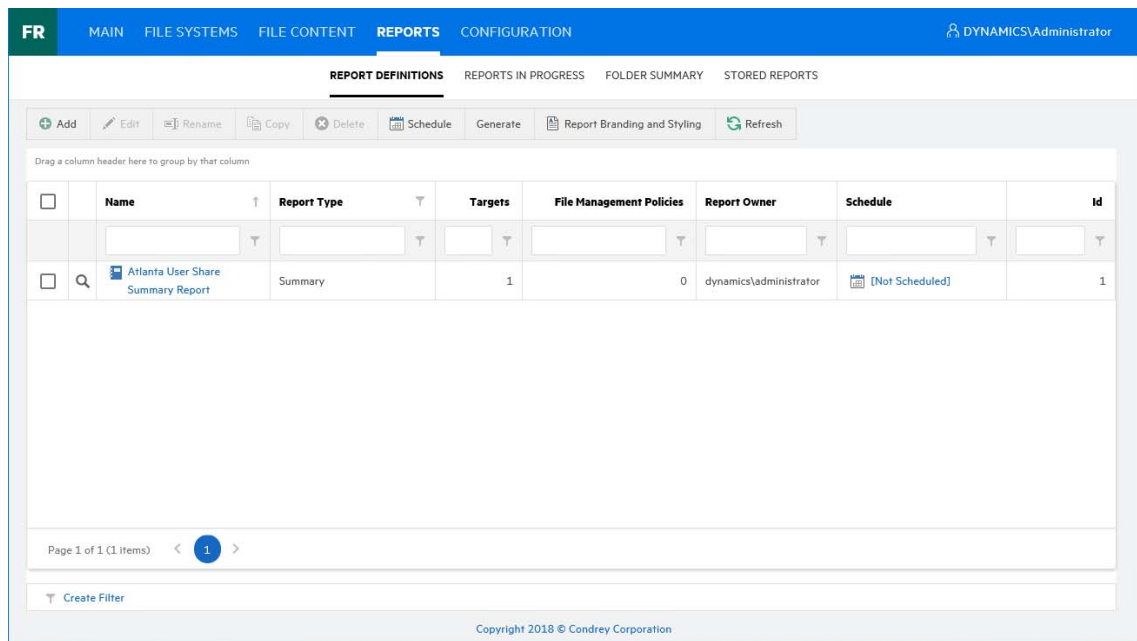
6 In the **Initial Chart Path Depth** field, specify the initial path depth for inclusion in the Top Ten Folders by Size chart that is displayed in the report header section.

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 eDirectory tree or Active Directory forest to be able to select the volumes or shares, even if you want to select the root of the eDirectory tree or Active Directory forest.
- 9 Click **Save**.  
The report definition is added to the list.



10 Do one of the following:

- ◆ Generate the report in Preview mode by following the procedures under [“Generating a Preview Report” on page 64](#).
- ◆ Generate the report in Stored mode by following the procedures under [“Generating a Stored Report” on page 66](#).

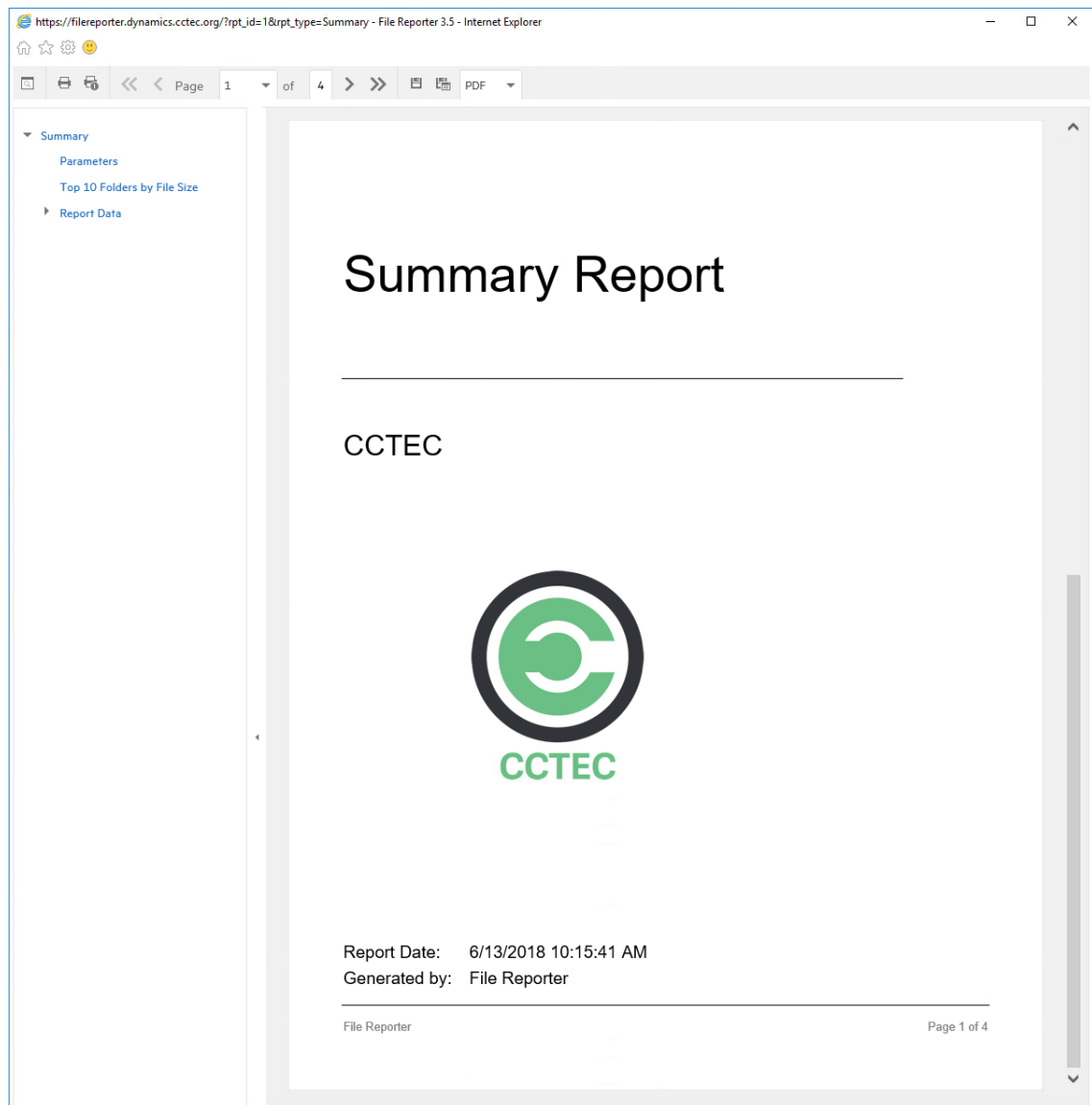
## Generating a Preview Report

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.

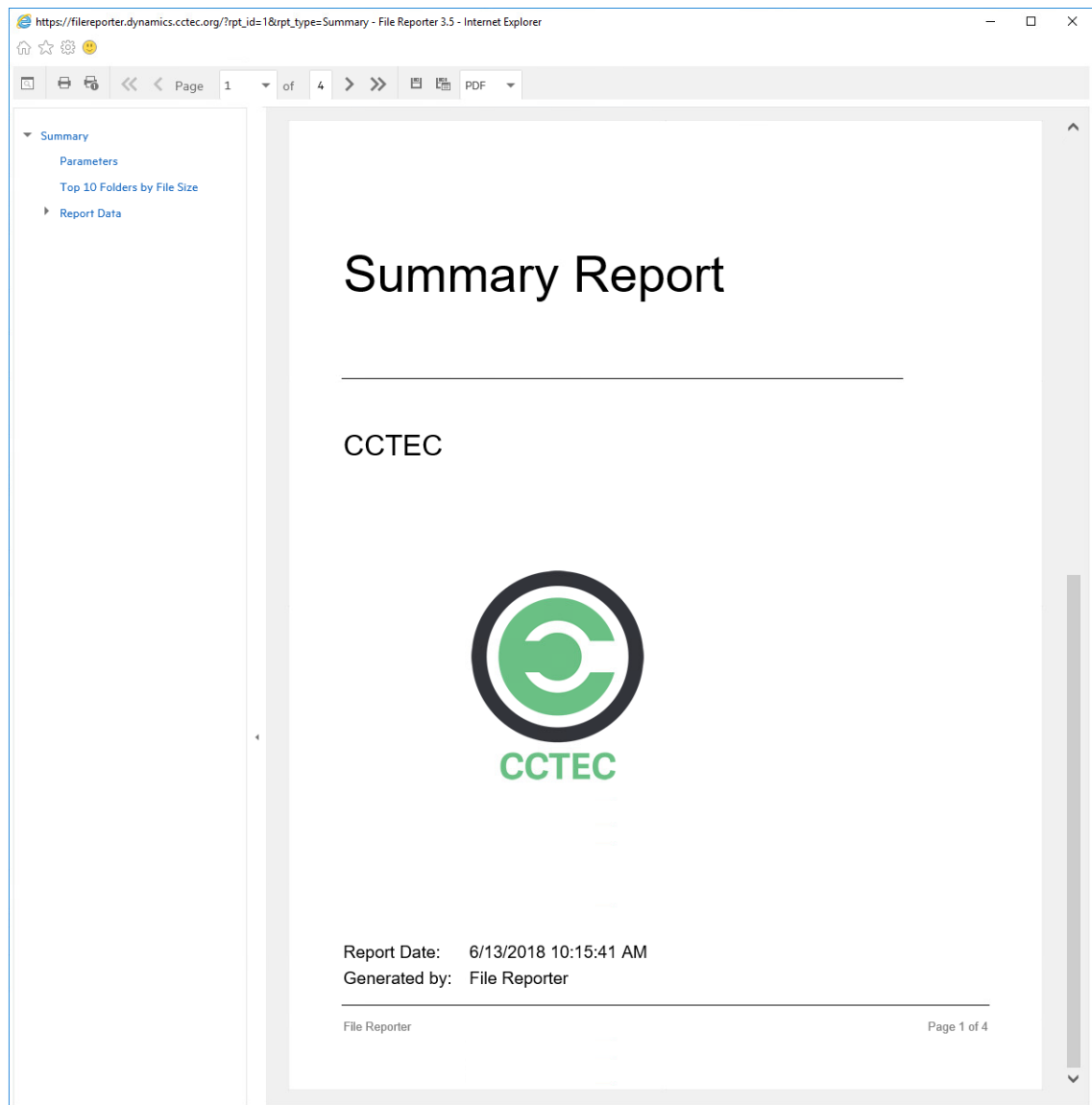
## Generating a Stored Report

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**.

	Name	Size	Report Type	Report Time	Expiration Date	Id
<input type="checkbox"/>	 Atlanta User Share Summary Report	20.35 KB	Summary	6/13/2018 10:57:48 AM	7/13/2018 12:00:00 AM	1

- 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.

- 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**.

Report Definition Editor - HQ Users Directory Quota Report

Name:\*

Unformatted:

Type: Directory Quota Report

Description: Report Definition created on 6/13/2018 11:45:53 AM by DYNAMICS\Administrator

**TARGET PATHS** FILE MANAGEMENT POLICIES

Add Remove

Target Path
-------------

SAVE CANCEL

- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 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 6/13/2018 12:16:55 PM by DYNAMICS\Administrator

**TARGET PATHS** FILE MANAGEMENT POLICIES

Add Remove

Target Path
-------------

SAVE 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 64.

For procedures on generating a Stored report, see “Generating a Stored Report” on page 66.

## 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: HQ Share Users Comparison Report

Results: Show unique paths from both targets

Unformatted:

Type: Comparison Report

Description: Report Definition created on 6/13/2018 12:44:45 PM by DYNAMICS\Administrator

**TARGET PATHS**

Add Remove

Target Path	Index
-------------	-------

SAVE 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 volumes, 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 6.6 Permissions Reports

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

---

**NOTE:** The term “Permissions” in File Reporter includes NTFS permissions as well as NCP rights and trustee assignments.

---

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 NCP Permissions Report,” on page 71](#)
- ♦ [Section 6.6.2, “Generating an Assigned NTFS Permissions Report,” on page 73](#)
- ♦ [Section 6.6.3, “Generating a Permissions by Path Report,” on page 74](#)
- ♦ [Section 6.6.4, “Generating a Permissions by Identity Report,” on page 75](#)

### 6.6.1 Generating an Assigned NCP Permissions Report

The Assigned NCP Permissions report indicates the assigned Micro Focus (formerly Novell) file system rights and trustee assignments 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 NCP Permissions** option and click **OK**.

Report Definition Editor - CCTEC3 Volume 1 NCP Permissions Report

Name: CCTEC3 Volume 1 NCP Permissions Report  Limit Path Depth 0

Unformatted:

Type: Assigned NCP Permissions Report

Description: Report Definition created on 6/13/2018 1:56:46 PM by DYNAMICS\Administrator

**TARGET PATHS** FILE MANAGEMENT POLICIES

Add Remove

Target Path

SAVE CANCEL

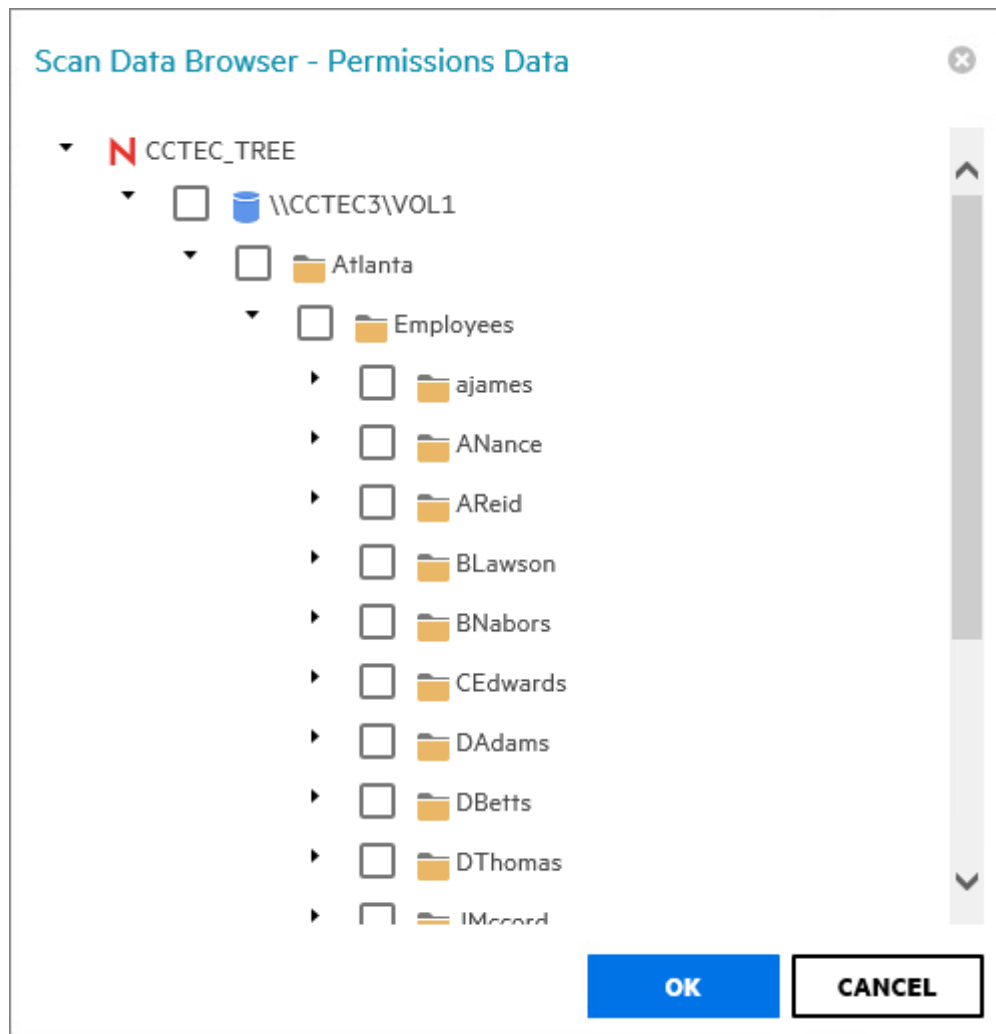
- 5 (Conditional) If you want to limit the scope of the report to a set depth in the file structure, click the **Limit Path Depth** check box and specify the depth level.

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

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

- 6 From the **Target Paths** tab, click **Add**.
- 7 Browse to and specify the file paths you want included in the report.





- 8 Click **OK** to close the Scan Data Browser.
- 9 Click **Save** to close the Report Definition Editor.
- 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 64.](#)  
 For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66.](#)

## 6.6.2 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**.

Report Definition Editor - London Users Assigned NTFS Permissions Report

Name: London Users Assigned NTFS Permissions Report  Limit Path Depth 0

Unformatted:   Include Inherited ACEs

Type: Assigned NTFS Permissions Report

Description: Report Definition created on 6/13/2018 3:16:21 PM by DYNAMICS\Administrator

**TARGET PATHS** FILE MANAGEMENT POLICIES

Add Remove

Target Path
-------------

SAVE CANCEL

- 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 64](#).  
For procedures on generating a Stored report, see ["Generating a Stored Report" on page 66](#).

### 6.6.3 Generating a Permissions by Path Report

The Permissions by Path report indicates the effective rights to the Micro Focus (formerly Novell) file system or the 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. Below the title bar, there are several fields: 'Name:' with the value 'London Users Permissions by Path Report', 'Unformatted:' with an unchecked checkbox, 'Type:' with the value 'Permissions by Path Report', and 'Description:' with the text 'Report Definition created on 6/14/2018 9:16:19 AM by DYNAMICSAdministrator'. Below these fields, there are two tabs: 'TARGET PATHS' (which is selected and underlined) and 'FILE MANAGEMENT POLICIES'. Under the 'TARGET PATHS' tab, there are 'Add' and 'Remove' buttons above a table. The table has a single header row with the text 'Target Path' and an empty body. At the bottom right of the window, there are two buttons: 'SAVE' (in a blue box) and 'CANCEL' (in a white box with a black border).

- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 6.6.4 Generating a Permissions by Identity Report

The Permissions by Identity report indicates the effective rights to the Micro Focus (formerly Novell) file system or the 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**.

Report Definition Editor - HQ Users Permissions by Identity Report

Name: HQ Users Permissions by Identity Report

Unformatted:

Type: Permissions by Identity Report

Description: Report Definition created on 6/14/2018 9:32:54 AM by DYNAMICS\Administrator

**IDENTITIES**

Add Remove

Identity System	Name

SAVE CANCEL

- 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 64](#).  
 For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 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 volumes or shares you want to report on.

- ◆ [Section 6.7.1, “Generating a Filename Extension Report,” on page 77](#)
- ◆ [Section 6.7.2, “Generating a Detailed Filename Extension Report,” on page 78](#)
- ◆ [Section 6.7.3, “Generating an Owner Report,” on page 79](#)
- ◆ [Section 6.7.4, “Generating a Detailed Owner Report,” on page 80](#)
- ◆ [Section 6.7.5, “Generating a Duplicate File Report,” on page 81](#)
- ◆ [Section 6.7.6, “Generating a Detailed Duplicate File Report,” on page 82](#)

- [Section 6.7.7, “Generating a Date-Age Report,”](#) on page 84
- [Section 6.7.8, “Generating a Detailed Date-Age Report,”](#) on page 85

## 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**.

The screenshot shows the 'Report Definition Editor' window for a report named 'London Users Filename Extension Report'. The 'Name' field contains 'HQ Users Filename Extension Report'. The 'Unformatted' checkbox is unchecked. The 'Type' is set to 'Filename Extension Report'. The 'Description' field contains the text: 'Report Definition created on 6/14/2018 10:06:40 AM by DYNAMICS\Administrator'. Below the description 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' and an empty body. At the bottom right of the window are 'SAVE' 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,”](#) on page 147.
- 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 64.  
For procedures on generating a Stored report, see “Generating a Stored Report” on page 66.
- 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**.

Report Definition Editor - HQ Users Filename Extension Detail Report

Name:\* HQ Users Filename Extension Detail Report

Unformatted:

Type: Filename Extension Detail Report

Description: Report Definition created on 6/14/2018 10:36:23 AM by DYNAMICS\Administrator

Filename Extensions (no leading dot), one per line

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path

SAVE CANCEL

- 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,” on page 147](#).
- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

### 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**.

Report Definition Editor - Atlanta Users Owner Report

Name:\* Atlanta Users Owner Report

Unformatted:

Type: Owner Report

Description: Report Definition created on 6/14/2018 11:05:53 AM by DYNAMICS\Administrator

**TARGET PATHS** FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path
-------------

SAVE CANCEL

- 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,” on page 147](#).

- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).
- 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' window. It has a title bar with a close button. The main area contains several fields: 'Name' (Munich Users Owner Detail Report), 'Unformatted' (checkbox), 'Type' (Owner Detail Report), and 'Description' (Report Definition created on 6/14/2018 11:17:18 AM by DYNAMICS\Administrator). Below these fields are four tabs: OWNERS, TARGET PATHS, FILE MANAGEMENT POLICIES, and FILTERS. The OWNERS tab is active. Under the OWNERS tab, there are 'Add' and 'Remove' buttons. Below these is a table with columns '#', 'Identity System', and 'Owner'. The table is empty, showing 'No data to display'. At the bottom of the table, there is a pagination bar with 'No data to paginate' and navigation arrows. At the bottom right of the window, there are 'SAVE' 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,” on page 147.](#)
- 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 64.](#)  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66.](#)

## 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.

- 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 6/14/2018 11:37:59 AM by DYNAMICS\Administrator

Match Size:

Match Name:

Match Create Time:

Match Modify Time:

Minimum Duplicates: 2

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path
-------------

SAVE 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," on page 147](#).
- 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 64](#).  
For procedures on generating a Stored report, see ["Generating a Stored Report" on page 66](#).
- 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 6/14/2018 12:05:04 PM by DYNAMICS\Administrator

Duplicate Criteria

Name

Size 0 bytes

Create Time

Modify Time

**TARGET PATHS** FILE MANAGEMENT POLICIES FILTERS

Add Remove

Target Path

SAVE 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,” on page 147](#).

- 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,” on page 147](#).
- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 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**.

Report Definition Editor - HQ Users Date-Age Report

Name:\*  Date Type:

Unformatted:  Detail Level:

Type:

Description:

**TARGET PATHS** FILE MANAGEMENT POLICIES FILTERS

[Add](#) [Remove](#)

Target Path
-------------

- 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,” on page 147](#).
- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).
- 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 6/14/2018 1:44:30 PM by DYNAMICS\Administrator

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

**SAVE** **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," on page 147](#).
  - 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 64](#).  
For procedures on generating a Stored report, see ["Generating a Stored Report" on page 66](#).

## 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, Historic NCP Permissions Comparison, and Historic NTFS Permissions Comparison.

- ◆ [Section 6.8.1, "Generating a Historic File System Comparison Report," on page 86](#)
- ◆ [Section 6.8.2, "Generating a Historic NCP Permissions Comparison Report," on page 88](#)
- ◆ [Section 6.8.3, "Generating a Historic NTFS Permissions Comparison Report," on page 90](#)

### 6.8.1 Generating a Historic File System Comparison Report

- 1 Select **Reports > Report Definitions**.
- 2 Click **Add**.

- In the **Name** field, specify a descriptive name of the report definition.
- 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 6/14/2018 2:39:18 PM by DYNAMICS\Administrator

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

**SAVE** **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 64](#).

For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 6.8.2 Generating a Historic NCP 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 NCP Permissions** option, then click **OK**.



**Report Definition Editor - CCTEC Vol 1 NCP Permissions Comparison**

Name: CCTEC Vol 1 NCP Permissions Comparison

Unformatted:

Type: Historic NCP Permissions Comparison Report

Description: Report Definition created on 6/14/2018 2:57:04 PM by DYNAMICS\Administrator

Limit Path Depth 100

Scans to Compare: Current and Previous

Include Removed Paths

**TARGET PATHS**

Add Remove

Target Path

**SAVE** **CANCEL**

- 5 (Conditional) If you want to limit the scope of the report to a set depth in the file structure, click the **Limit Path Depth** check box and specify the depth level.  
 For example, if you specify 3, the report lists the permissions of file contents of all file paths in the specified target paths up to 3 levels in the file structure.  
 If you do not specify a path depth, File Reporter will report on all levels of the specified target path.
- 6 From the **Scans to Compare** drop-down menu, select one of the following options:
  - Current and Previous:** Compares the Current scan of the storage resource to the Previous scan of the storage resource.
  - Current and Baseline:** Compares the Current scan of the storage resource to the Baseline scan of the storage resource.
  - Previous and Baseline:** Compares the Previous scan of the storage resource to the Baseline scan of the storage resource.
 All options appear whether you have scans or not. If you do not have scans, File Reporter will generate an empty report.
- 7 (Conditional) If you do not want the report to list any paths that have been deleted or removed, deselect the **Include Removed Paths** check box.
- 8 Browse to and specify the file paths you want included in the report, then click **OK**.
- 9 Click **Save** to close the Report Definition Editor.
- 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 64](#).  
 For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 6.8.3 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**.

The screenshot shows the 'Report Definition Editor' window for a report named 'Atlanta Users Historic NTFS Comparison Report'. The window title is 'Report Definition Editor - Atlanta Users Historic NTFS Comparison Report'. The form contains the following fields and options:

- Name:** Atlanta Users Historic NTFS Comparison Report
- Unformatted:**
- Type:** Historic NTFS Permissions Comparison Report
- Description:** Report Definition created on 6/14/2018 3:18:31 PM by DYNAMICS\Administrator
- Limit Path Depth:**  Limit Path Depth: 100
- Scans to Compare:** Current and Previous
- Include Inherited ACEs:**
- Include Removed Paths:**

Below these fields is a section titled **TARGET PATHS** with 'Add' and 'Remove' buttons. A table with one column 'Target Path' is present but empty. At the bottom right are 'SAVE' and 'CANCEL' buttons.

- 5 (Conditional) If you want to limit the scope of the report to a set depth in the file structure, click the **Limit Path Depth** check box and specify the depth level.  
For example, if you specify 3, the report lists the permissions of file contents of all file paths in the specified target paths up to 3 levels in the file structure.  
If you do not specify a path depth, File Reporter will report on all levels of the specified target path.
- 6 From the **Scans to Compare** drop-down menu, select one of the following options:
  - Current and Previous:** Compares the Current scan of the storage resource to the Previous scan of the storage resource.
  - Current and Baseline:** Compares the Current scan of the storage resource to the Baseline scan of the storage resource.
  - Previous and Baseline:** Compares the Previous scan of the storage resource to the Baseline scan of the storage resource.All options appear whether you have scans or not. If you do not have scans, File Reporter will generate an empty report.

- 7 (Conditional) If you want your report to include not only direct permissions, but inherited permissions, select the **Include Inherited ACEs** check box.  
Reporting inherited permissions could make the report significantly larger.
- 8 (Conditional) If you do not want the report to list any paths that have been deleted or removed, deselect the **Include Removed Paths** check box.
- 9 Browse to and specify the file paths you want included in the report, then click **OK**.
- 10 Click **Save** to close the Report Definition Editor.
- 11 Generate the report as either a Preview report or a Stored report.  
For procedures on generating a Preview report, see [“Generating a Preview Report” on page 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 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 volume or share disk space over a set amount of time. For best results, you should conduct regularly scheduled Volume Free Space scans on specific volumes and shares. File Reporter then has the data it needs to graph the pattern of free space on the volume or 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**.

**Report Definition Editor - SFO Volume Free Space Report**

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 6/14/2018 3:55:00 PM by DYNAMICS\Administrator

**TARGET PATHS**

Add Remove

Target Path

SAVE CANCEL

- 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 volumes or 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 6.10 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 3.6 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.

---

**IMPORTANT:** Prior to the release of version 3.0, File Reporter supported the `active_fs_scandata` view, which was then deprecated, but not removed. That view has now been removed to support File Reporter's current and previous naming parameters. If you have existing Custom Query reports that include the `active_fs_scandata` view, you will need to replace each instance with `current_fs_scandata`.

---

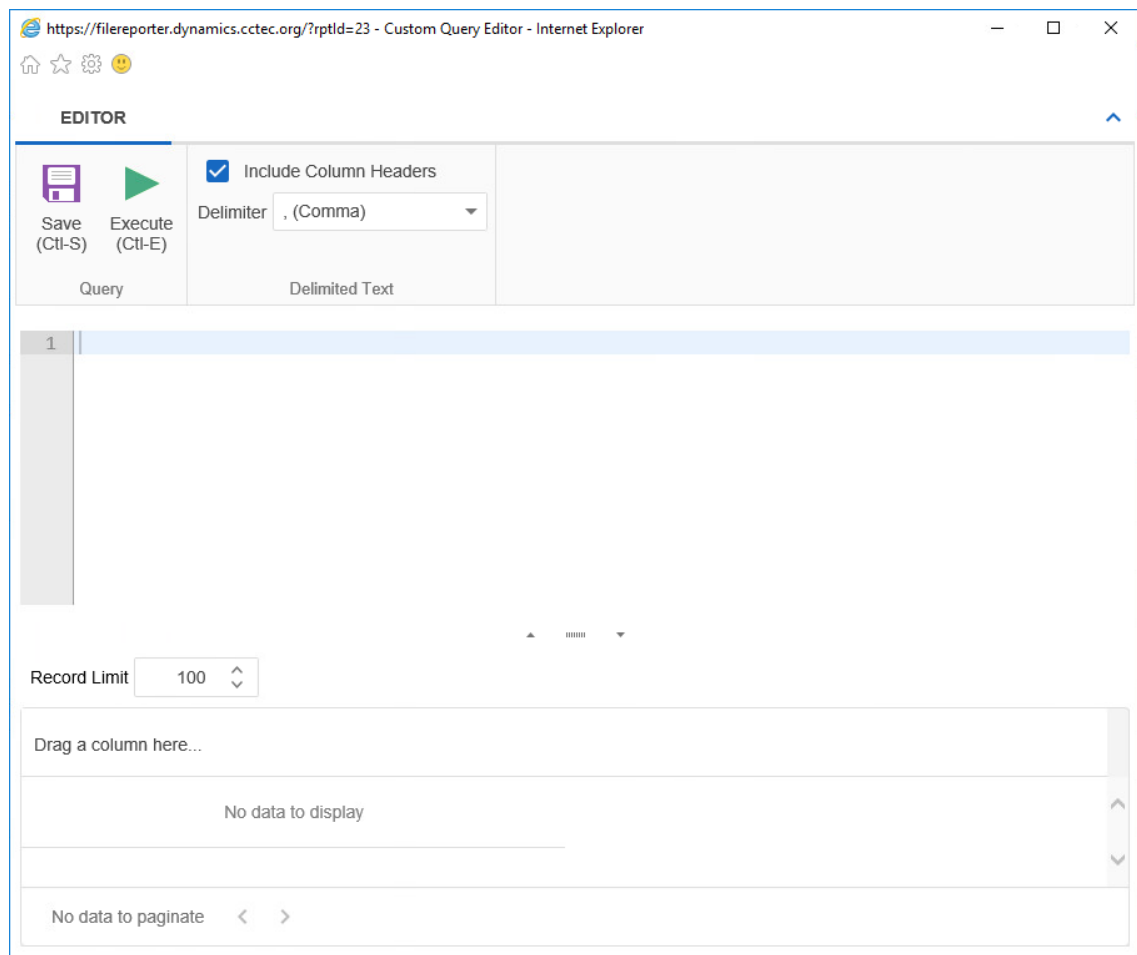
**NOTE:** For details on using the report editor in the Report Designer, see [Section 11.3, "Designing a Custom Query Report,"](#) on page 135.

---

**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 <http://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 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 the how much can be previewed.

The screenshot shows the Custom Query Editor interface. At the top, there are navigation icons and a title bar. Below that is the 'EDITOR' section with a 'Save (Ctrl-S)' button, an 'Execute (Ctrl-E)' button, and a 'Delimited Text' section with a checked 'Include Column Headers' option and a 'Delimiter' dropdown set to ', (Comma)'. The main area contains SQL code:

```
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 'Novell'
5         FROM srs.current_fs_scandata AS sd
6         WHERE (sd.fullpath LIKE '\\dynamics.cctec.org\DFS\HQ\HQShare\%' ESCAPE '#') AND
7             (sd.path_type = 1))
8 SELECT
9     x.category,
10    Sum(x.size) AS cat_size,
11    count(*) AS file count,
```

Below the code is a 'Record Limit' dropdown set to 100. A preview table is shown with the following data:

#	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)' and a page number '1' in a blue circle.

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

7 Close the Custom Query Report Editor.

8 Select **Reports > Report Definitions**.

9 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 64](#).

For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).

## 6.11 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.

### 6.11.1 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**.

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

**Permissions**

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

**Historic Comparison**

- File System Comparison
- NCP Permissions Comparison
- NTFS Permissions Comparison

**Trending**

- Volume Free Space

**Custom Query**

- Custom Query Report

**OK** **CANCEL**

- 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 64](#).  
For procedures on generating a Stored report, see [“Generating a Stored Report” on page 66](#).
- 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**.

## 6.12 Micro Focus File Dynamics and Storage Manager Policy Reports

In most reports, you browse to and specify a file path for the report through the **Target Paths** tab. If you have either Micro Focus File Dynamics or Micro Focus Storage Manager 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 or Storage Manager policies, rather than through a specific file path.

---

**IMPORTANT:** File Reporter 3.6 supports File Dynamics 6.0 and Storage Manager 4.0 or above.

---

The advantages to specifying a File Dynamics or Storage Manager 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’ or Storage Manager’s 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 or Storage Manager policies.

---

**NOTE:** Procedures for integrating File Reporter with File Dynamics or Storage Manager are included in [Section 4.5, “Integrating with File Dynamics or Storage Manager,” on page 40](#).

---

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 or Storage Manager 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** [Close]

Source: HQ Share and HQ Users Comparison Report

Target: Copy of HQ Share and HQ Users Comparison Report

[COPY] [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** [Close]

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

[RENAME] [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,” on page 147](#).

# 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 input field), "Level:\*" (a dropdown menu with a diamond icon), and "Description:" (a text area). At the bottom right of the dialog are two buttons: "Update" and "Cancel".

- 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

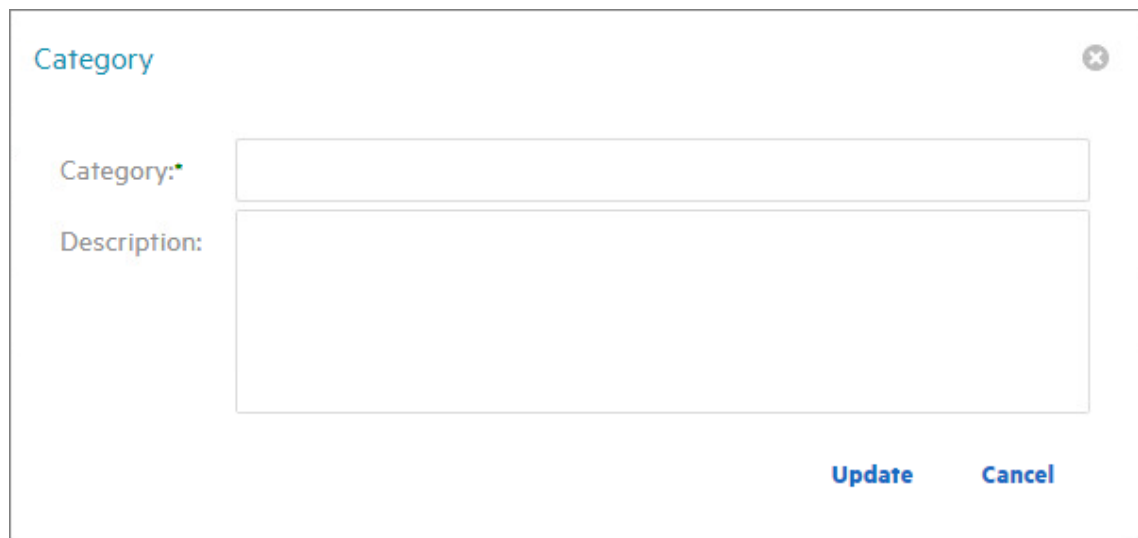
- 1 Select **File Content > Classifications**.
- 2 Select the classification you want to edit.
- 3 Click **Edit**.
- 4 Edit the fields.
- 5 Click **Update**.

## 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:\*" (a single-line text box) and "Description:" (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**.

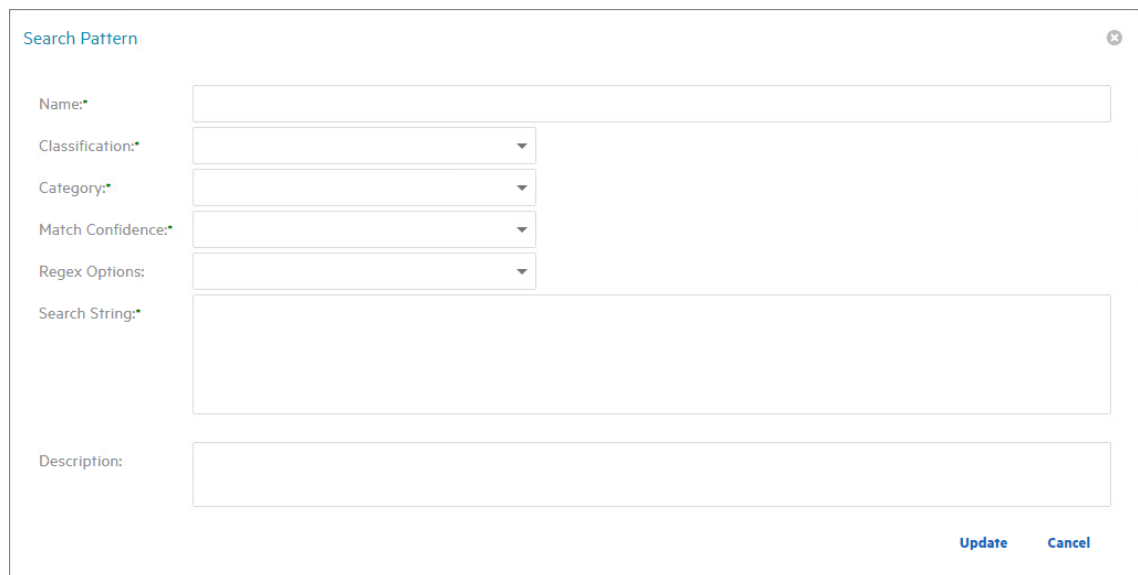
## 7.3 Creating Search Patterns

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 'Search Pattern' form with 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 regex 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.
- 6 From the **Match Confidence** drop-down menu, select either **Low**, **Medium**, or **High**.





- 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.

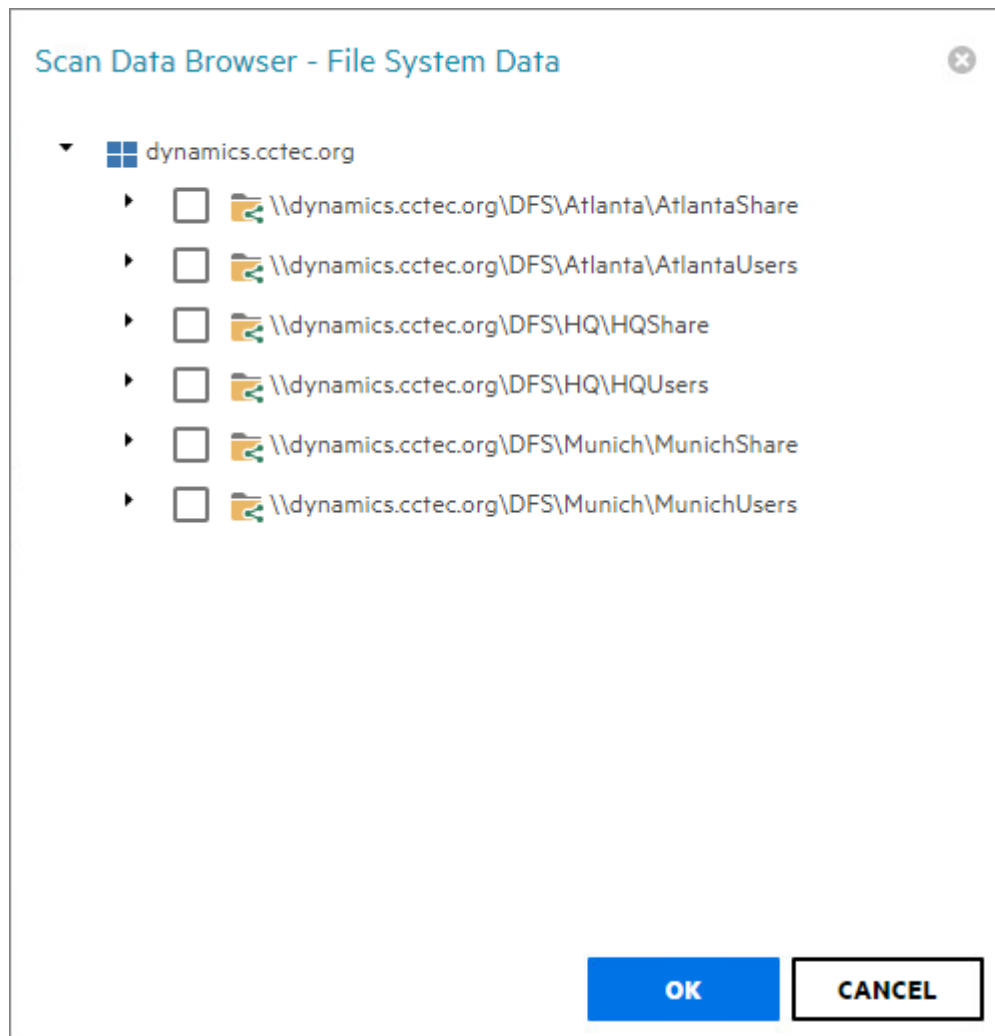
### 7.4.1 Creating a New Job Definition

- 1 Select **File Content > Job Definitions**.
- 2 Click **Add**.

The screenshot shows a 'Job Definition' form with the following elements:

- Name:** A text input field.
- Result Type:** A dropdown menu.
- Tabs:** Three tabs labeled 'TARGET PATHS', 'SEARCH PATTERNS', and 'FILTERS'. The 'TARGET PATHS' tab is selected.
- Buttons:** 'Add' and 'Remove' buttons are located above the table.
- Table:** A table with one row containing the text 'Target'.
- Footer:** 'Update' and 'Cancel' buttons are located at the bottom right.

- 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**.



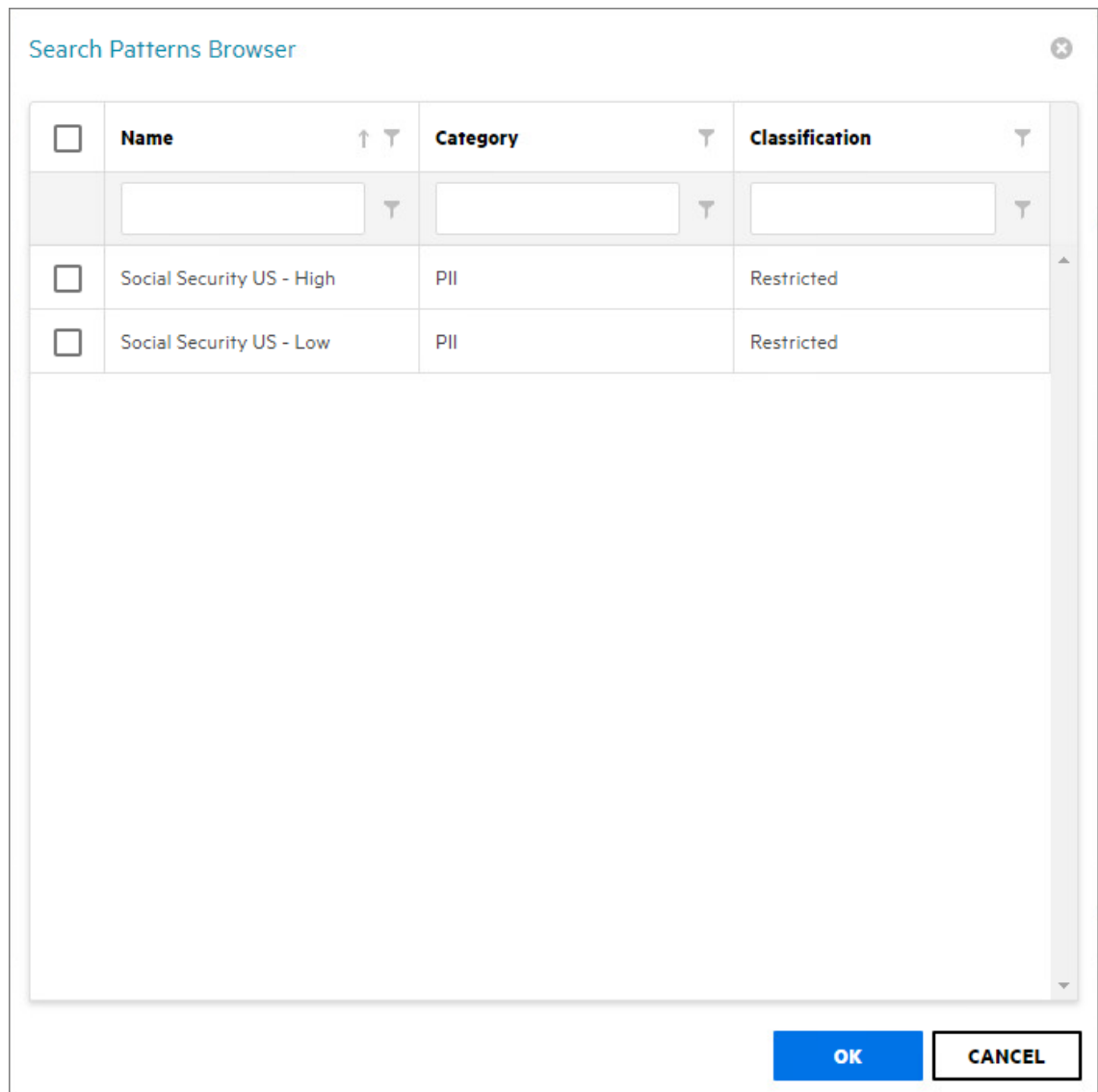
- 6 Select the targets where you want the file content to be scanned.

---

**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, select 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**

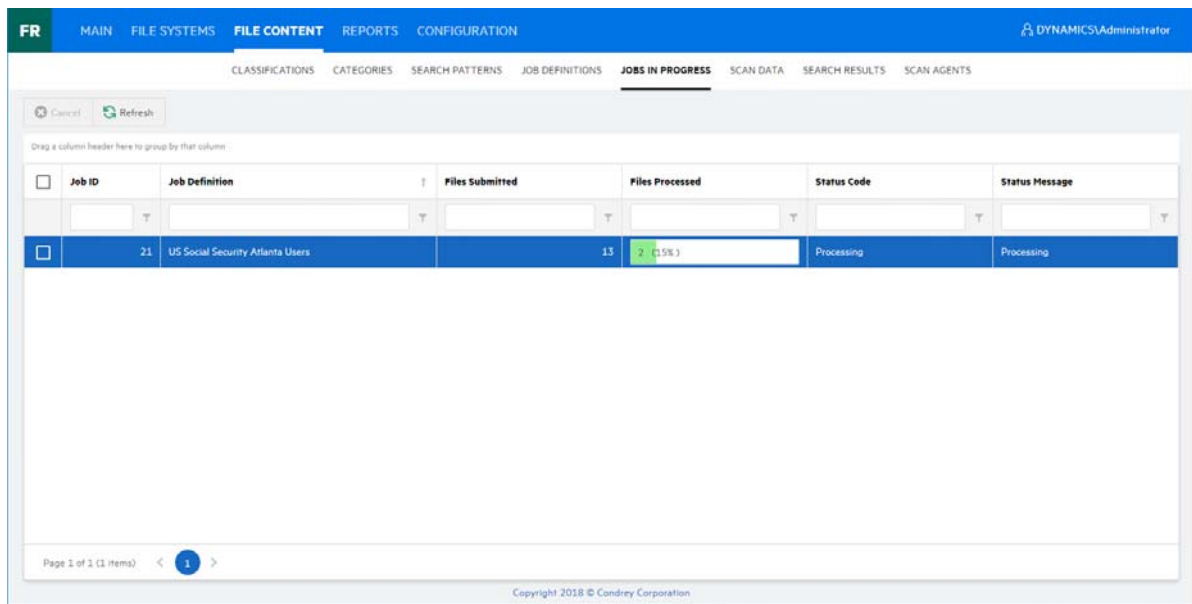
- 14 Click **Update** to save the job definition settings.

## 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**.

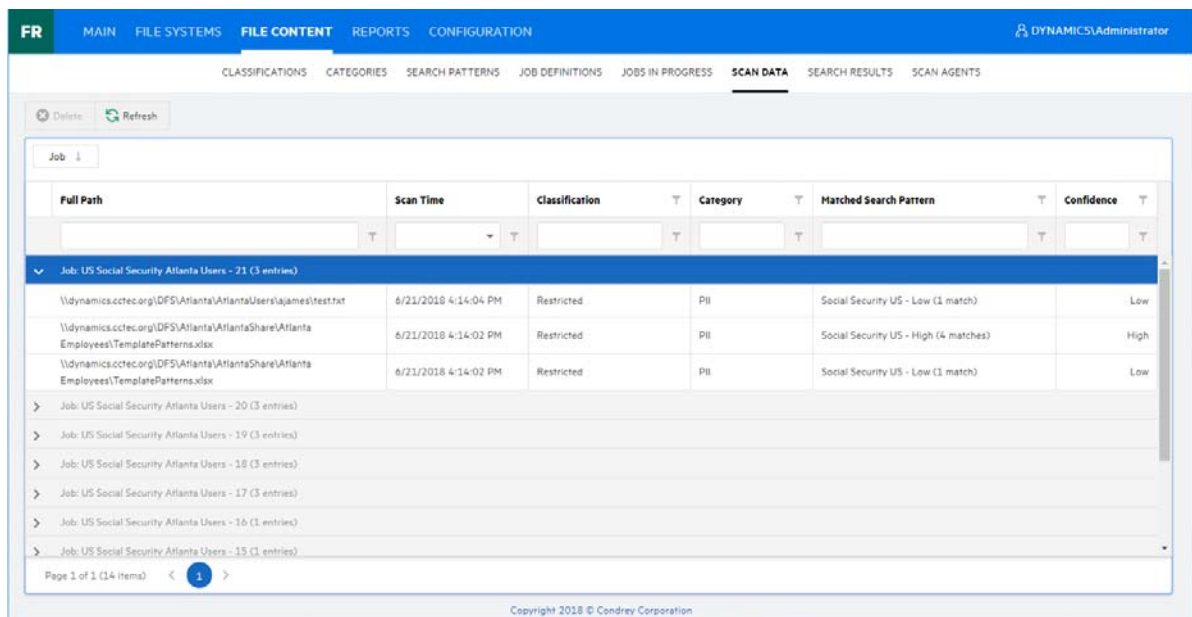
## 7.5 Viewing Jobs in Progress

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



## 7.6 Viewing Scanned Data Jobs

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



## 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.

FR MAIN FILE SYSTEMS FILE CONTENT REPORTS CONFIGURATION DYNAMICS\Administrator

CLASSIFICATIONS CATEGORIES SEARCH PATTERNS JOB DEFINITIONS JOBS IN PROGRESS SCAN DATA SEARCH RESULTS SCAN AGENTS

Delete Refresh

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"/>	US Social Security Atlanta Users-10.csv	Completed	340 bytes	6/19/2018 3:14:22 PM
<input type="checkbox"/>	US Social Security Atlanta Users-12.csv	Completed	340 bytes	6/19/2018 5:34:39 PM
<input type="checkbox"/>	US Social Security Atlanta Users-13.csv	Completed	340 bytes	6/19/2018 5:48:53 PM
<input type="checkbox"/>	US Social Security Atlanta Users-14.csv	Completed	346 bytes	6/19/2018 5:58:43 PM
<input type="checkbox"/>	US Social Security Atlanta Users-15.csv	Completed	346 bytes	6/19/2018 5:59:01 PM
<input type="checkbox"/>	US Social Security Atlanta Users-16.csv	Completed	346 bytes	6/19/2018 5:59:16 PM
<input type="checkbox"/>	US Social Security Atlanta Users-17.csv	Completed	941 bytes	6/19/2018 6:00:07 PM
<input type="checkbox"/>	US Social Security Atlanta Users-18.csv	Completed	938 bytes	6/20/2018 10:05:01 AM
<input type="checkbox"/>	US Social Security Atlanta Users-19.csv	Completed	938 bytes	6/21/2018 12:13:08 PM

Page 1 of 1 (11 items) < 1 >

Copyright 2018 © 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 > Scan Agents**.

FR MAIN FILE SYSTEMS FILE CONTENT REPORTS CONFIGURATION DYNAMICS\Administrator

CLASSIFICATIONS CATEGORIES SEARCH PATTERNS JOB DEFINITIONS JOBS IN PROGRESS SCAN DATA SEARCH RESULTS SCAN AGENTS

Delete Refresh

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"/>	cctec2.dynamics.cctec.org	3.5.0.20	6/21/2018 1:53:12 PM	10.0.14393.0	Windows Server 2016 Standard (Build 14393) Release 1607	openjdk version "1.8.0_adoptopenjdk" OpenJDK Runtime Environment (build 1.8.0_adoptop OpenJDK 64-Bit Server VM (build 25.71-b00, mixed r	Apache Tika 1.18	<input type="checkbox"/>	Ready

Create Filter

Copyright 2018 © Condrey Corporation

# 8

## Performing Other Administrative Tasks

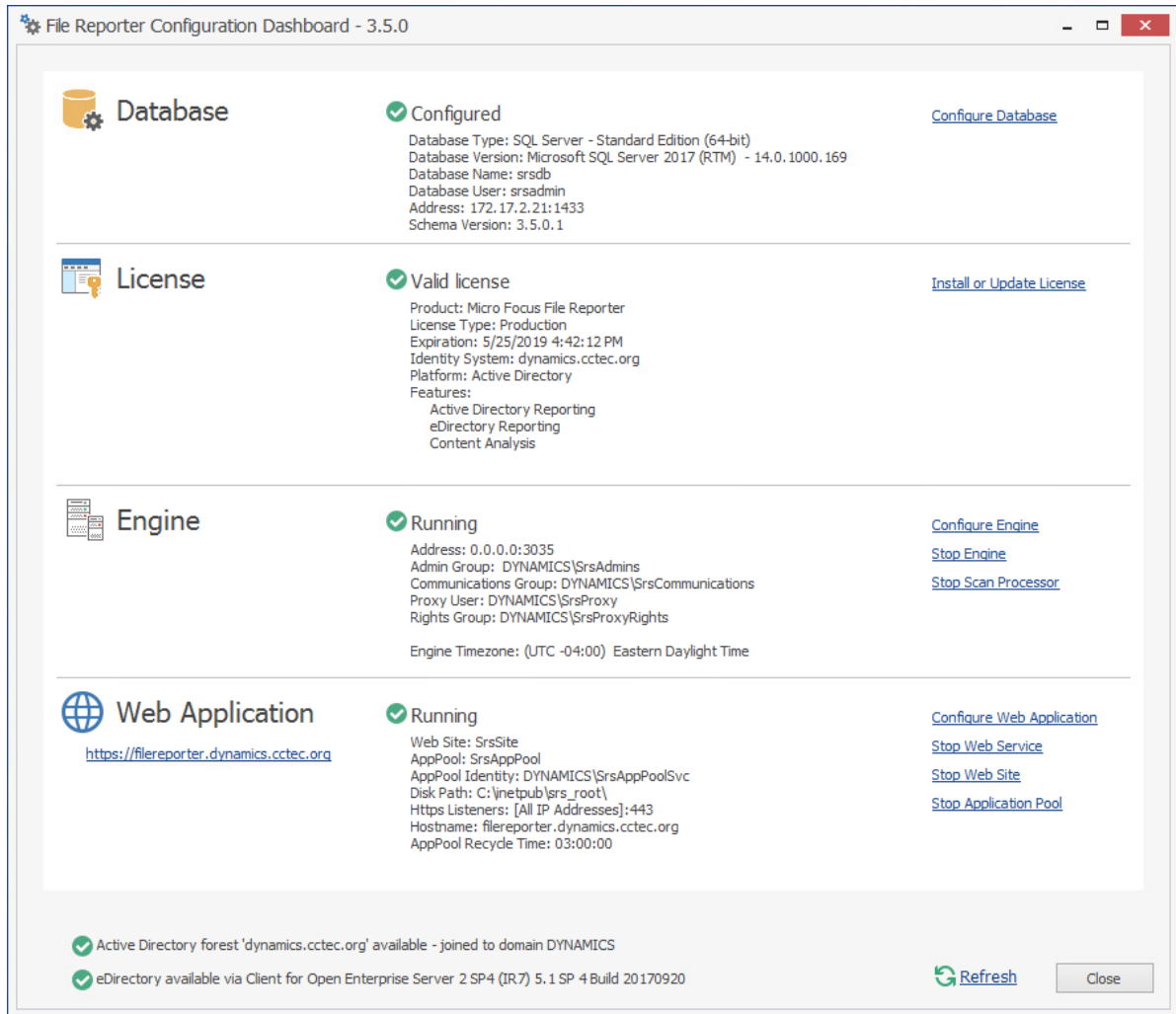
This section provides procedures for performing administrative tasks not covered in the previous sections.

- ◆ [Section 8.1, “Stopping and Restarting Services,” on page 111](#)
- ◆ [Section 8.2, “Using Folder Summary,” on page 112](#)
- ◆ [Section 8.3, “Considerations for Reporting on NAS Devices,” on page 113](#)
- ◆ [Section 8.4, “Changing the Default Path for Stored Reports,” on page 114](#)
- ◆ [Section 8.5, “Changing the Life Span of Stored Reports,” on page 115](#)
- ◆ [Section 8.6, “Resetting the Proxy User Password,” on page 115](#)

### 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
<b>CCTEC_TREE</b>							
dynamics.cctec.org							
\dynamics.cctec.org\DFS\Atlanta\AtlantaShare	6/15/2018 12:48:26 PM						
\dynamics.cctec.org\DFS\Atlanta\AtlantaUsers	6/15/2018 12:48:26 PM	222 MB	5	34		100	100
\dynamics.cctec.org\DFS\HQ\HQShare	6/15/2018 12:48:27 PM	56 MB	60	269		100	100
\dynamics.cctec.org\DFS\HQ\HQUsers	6/15/2018 12:48:27 PM	93 MB	2	22		100	100
\dynamics.cctec.org\DFS\Munich\MunichShare	6/18/2018 12:00:00 AM						
\dynamics.cctec.org\DFS\Munich\MunichUsers	6/15/2018 12:00:00 AM						

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

## 8.3 Considerations for Reporting on NAS Devices

In Active Directory network environments, 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 113](#)
- ◆ [Section 8.3.2, “EMC Isilon,” on page 114](#)
- ◆ [Section 8.3.3, “Other NAS Devices,” on page 114](#)

### 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***
```

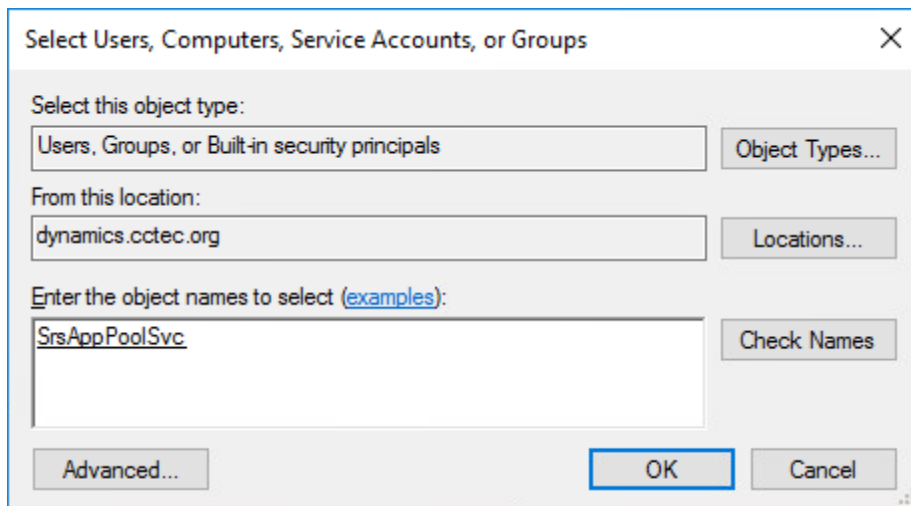
- 2 Rebuild the storage resources and verify that the NAS device is displayed on the list.
- 3 Perform any needed steps for giving the proxy rights group access to the desired shares and folders on the NAS device.

## 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; for eDirectory (or the “service account” when running in eDirectory mode) 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

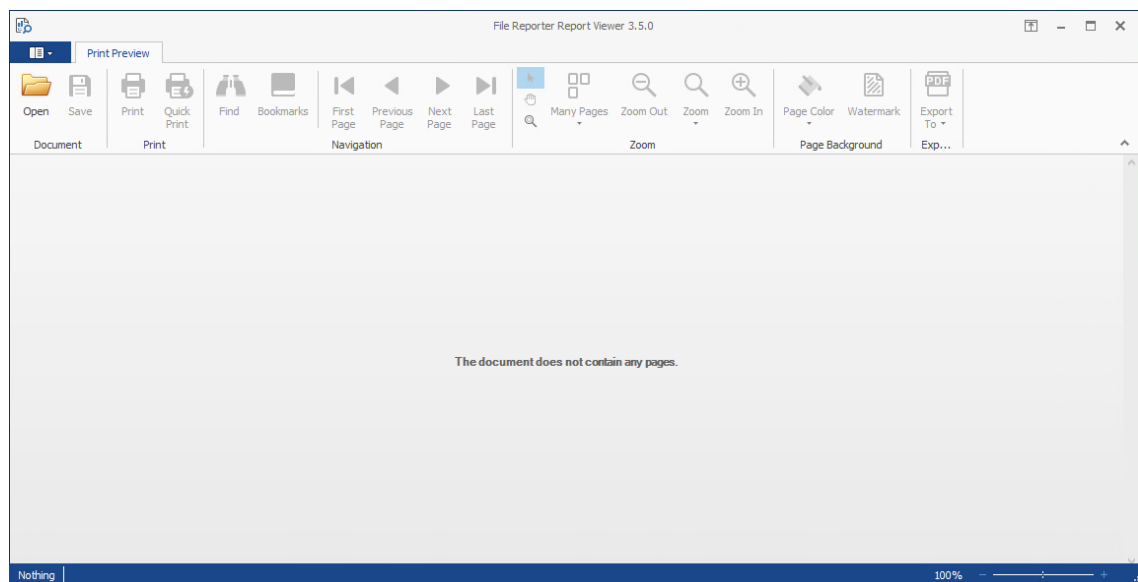
**NOTE:** The Report Viewer is installed as a separate application, rather than part of the Client Tools. This is so both administrators and other users who need access to the reports, can access saved reports.

## 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.

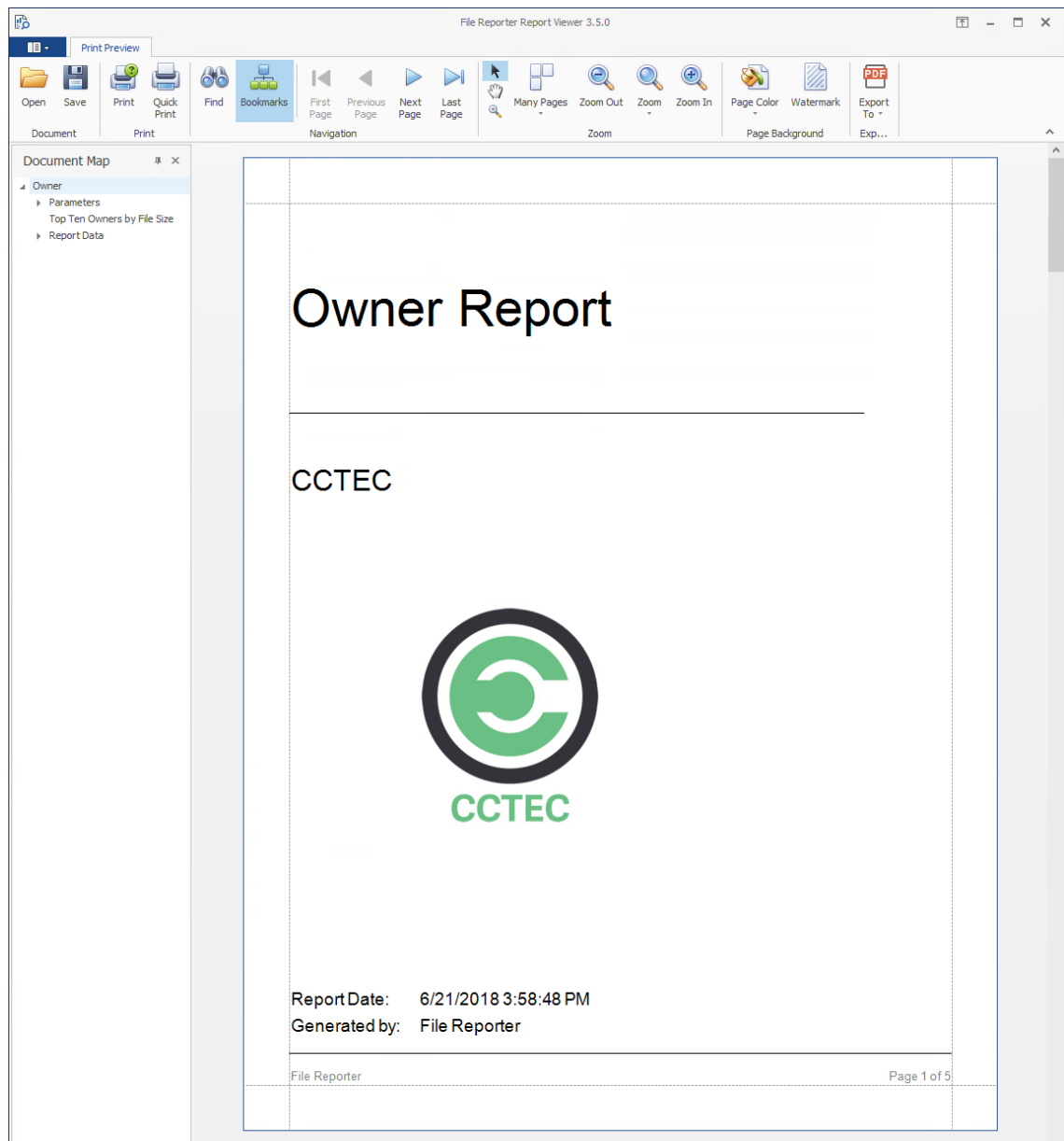
In comparison to the viewing capabilities of the browser-based administrative interface, the Report Viewer offers more capabilities. For example, with the Report Viewer you can change the visual display parameters of the report.

- 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.

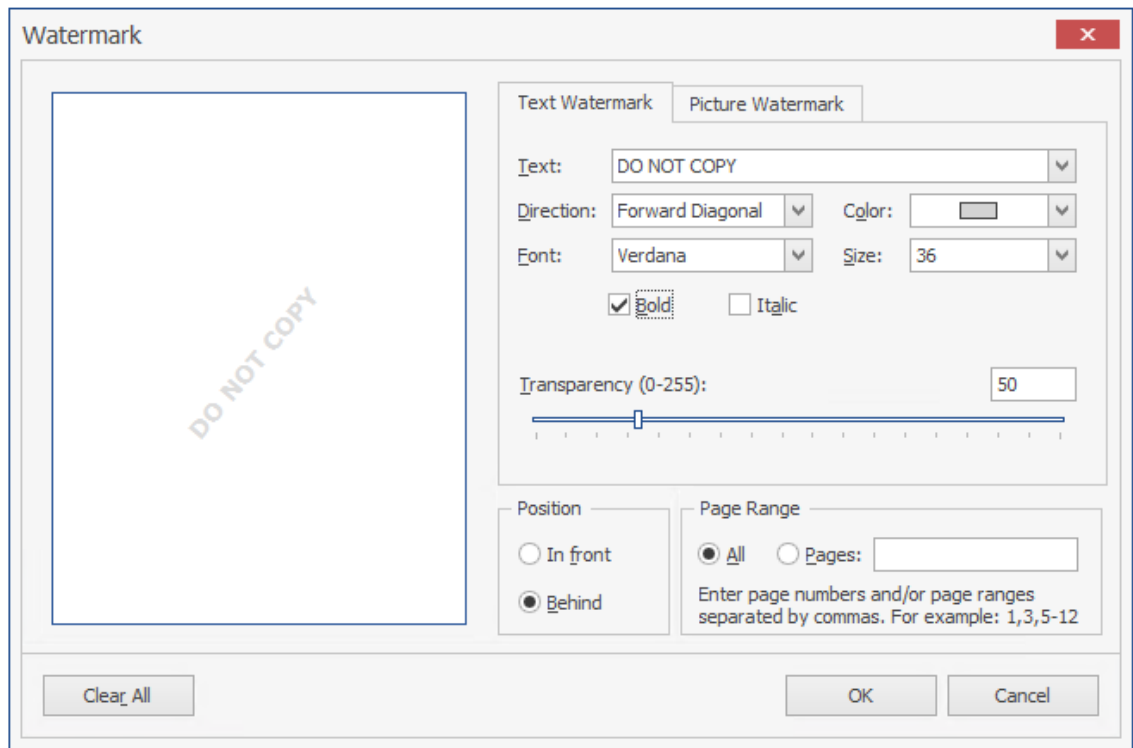
**Zoom:** Click to change the zoom level of the report preview.

**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.

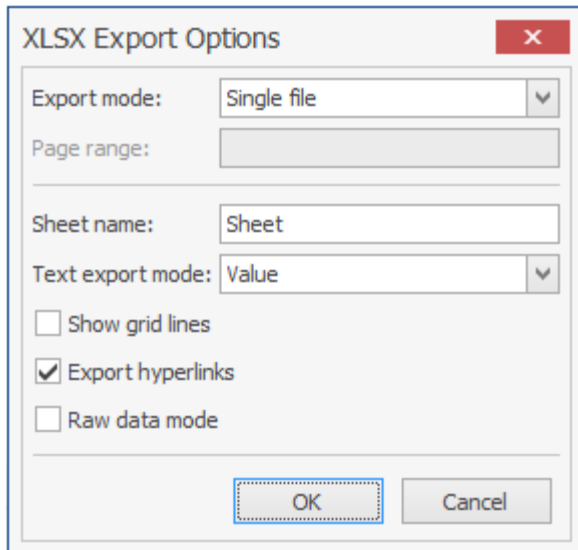
The Watermark dialog box lets you specify your watermark settings. Your watermark can either be in text or graphic form.



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 Client 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 121](#)
- ♦ [Section 10.2, “Using the Dashboard,” on page 123](#)
- ♦ [Section 10.3, “Using the Tree Map,” on page 125](#)
- ♦ [Section 10.4, “Using the Pivot Grid,” on page 127](#)

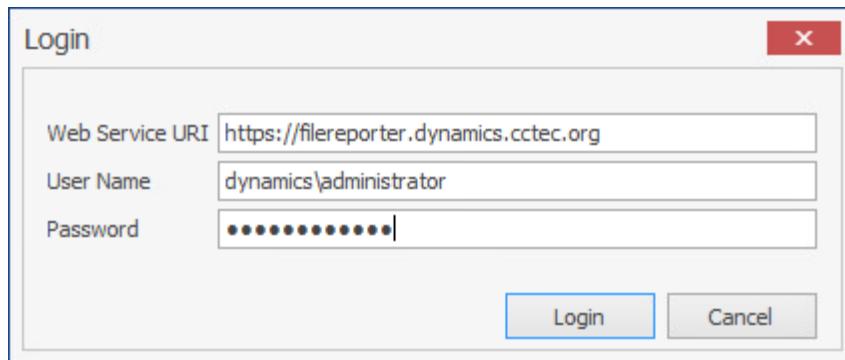
## 10.1 Launching the Analytics Tools

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 3.6 Data Analytics**.

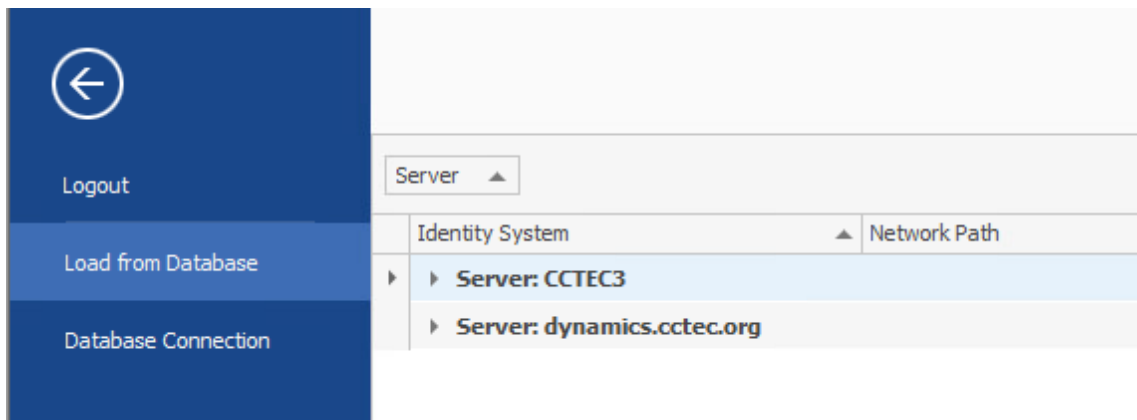
The following login screen appears:

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

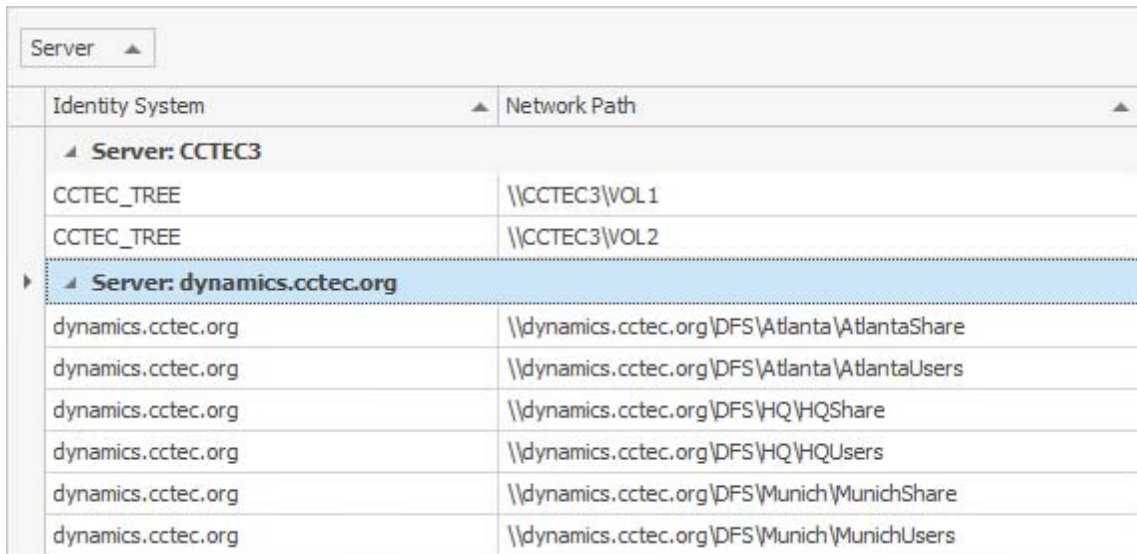


The screenshot shows a standard Windows-style dialog box titled "Login". It features a close button (X) in the top right corner. The dialog contains three text input fields: "Web Service URI" containing "https://filereporter.dynamics.cctec.org", "User Name" containing "dynamics\administrator", and "Password"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

A selection dialog box similar to the following appears:

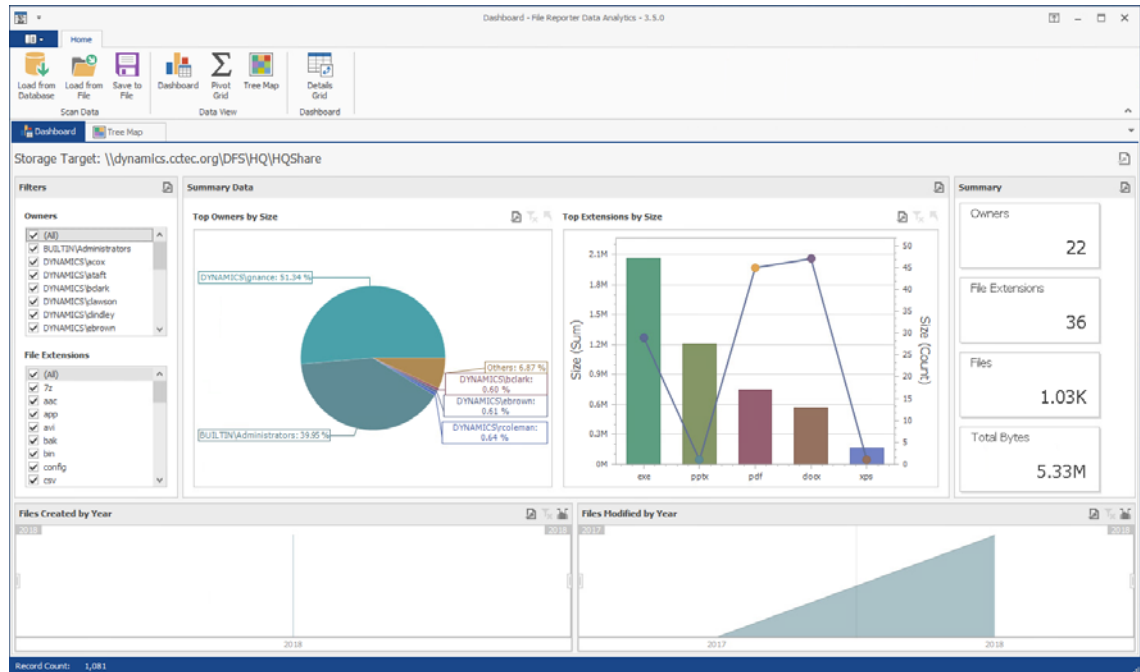


3 Expand the shares and volumes.



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.

Filtered by: DYNAMICS\Ignance

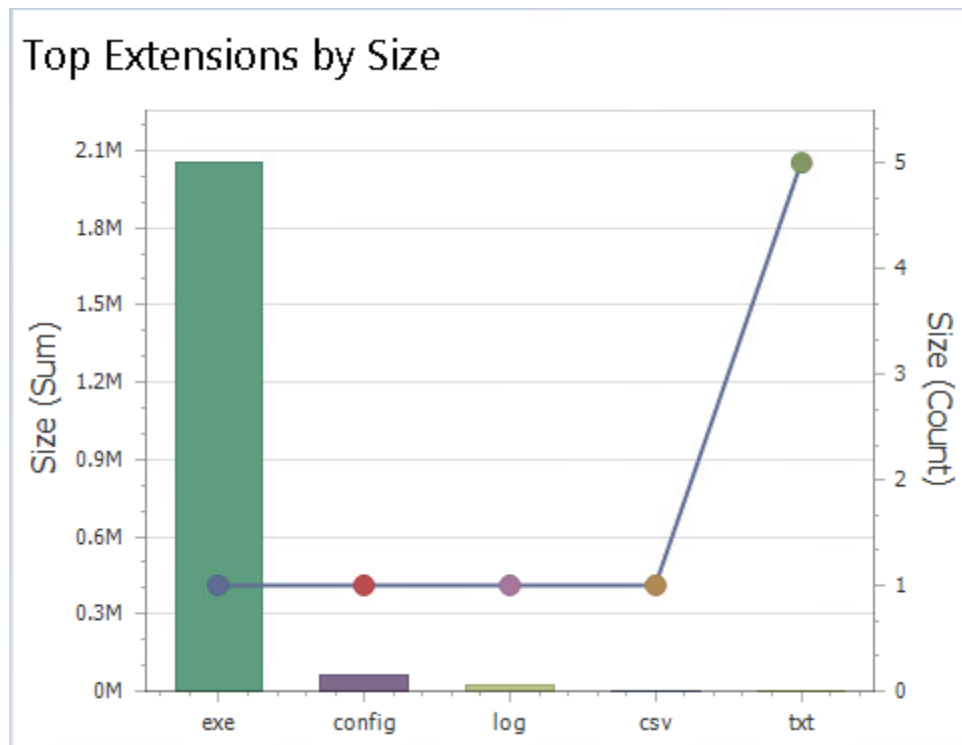
Home

Open Folder    Export to Excel    Export to CSV

Drag a column header here to group by that column

Full Path	Name	File Name E...	Size	Owner	Create Time	Modify Time	Access Time	Index	Parent Inde
\\dynamics...	conusee.mov	mov	152 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	671	^
\\dynamics...	eventual.avi	avi	688 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	674	
\\dynamics...	burns.bin	bin	504 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	696	
\\dynamics...	scratch.docx	docx	422 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	714	
\\dynamics...	sorbets.m4a	m4a	474 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	715	
\\dynamics...	outrun.app	app	443 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	732	
\\dynamics...	mobilized.w...	wma	89 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	791	
\\dynamics...	gum.avi	avi	911 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	811	
\\dynamics...	releasable.rtf	rtf	833 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	818	
\\dynamics...	overcoat.mp4	mp4	433 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	835	
\\dynamics...	perches.gz	gz	581 bytes	DYNAMICS...	6/22/2018 ...	6/22/2018 ...	6/22/2018 ...	837	v
Total Cou...			SUM=3 MB						

- 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.

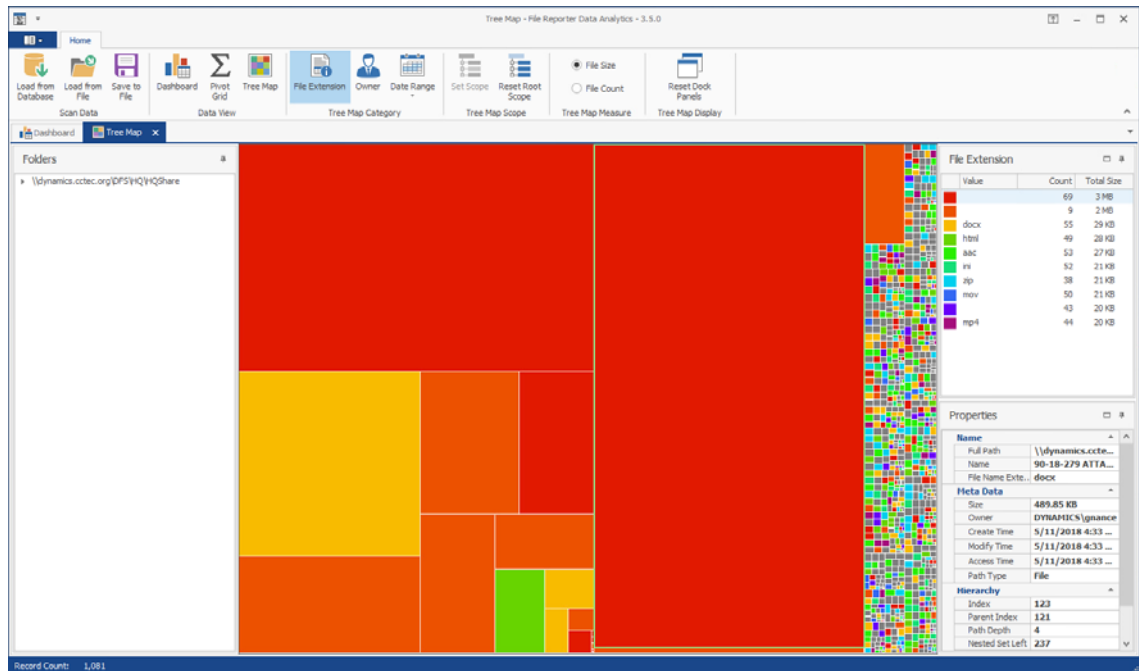


- 13 In the **Files Created by Year** region, double-click a year span and observe how the displayed data in the other regions is updated to data pertaining to the selected year.
- 14 Right-click the selected year span and select **Clear Master Filter** to have the graph span all of the years again.
- 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**.

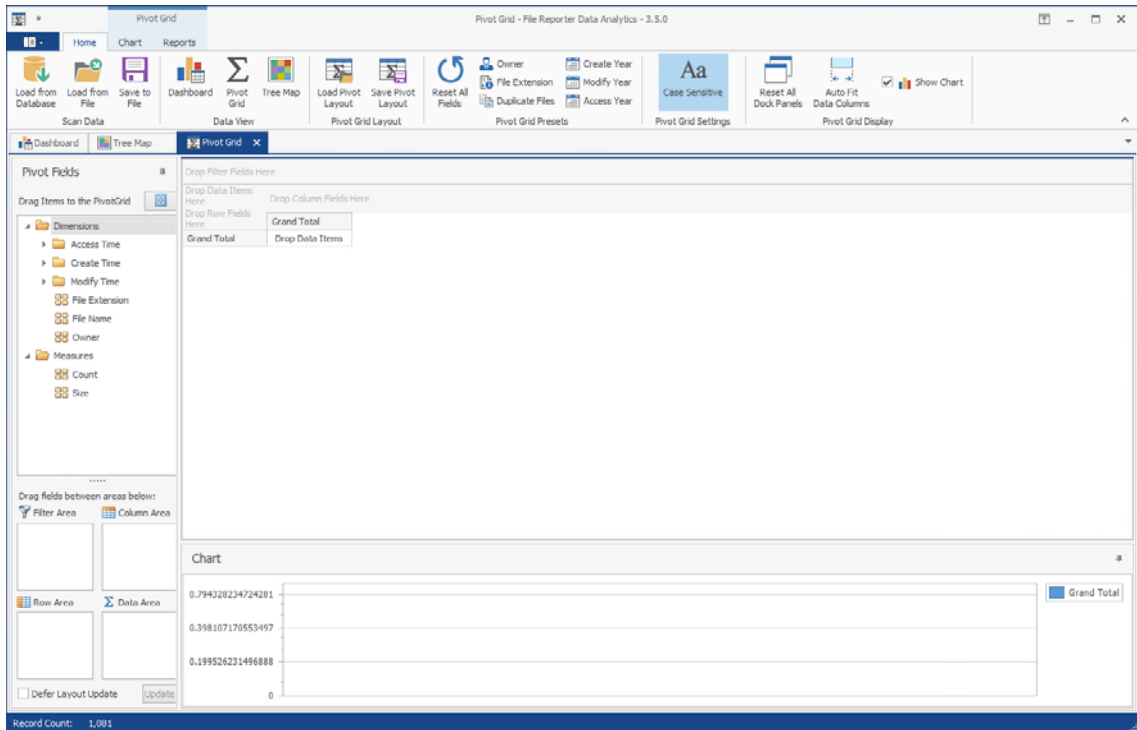


- 4 Observe how the Tree Map is presented according to file extension type with the specific color assignments detailed in the **File Extension** region.  
Each of the squares in the Tree Map represents a single file in the scanned storage resource. The squares are represented according to the file size, 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.

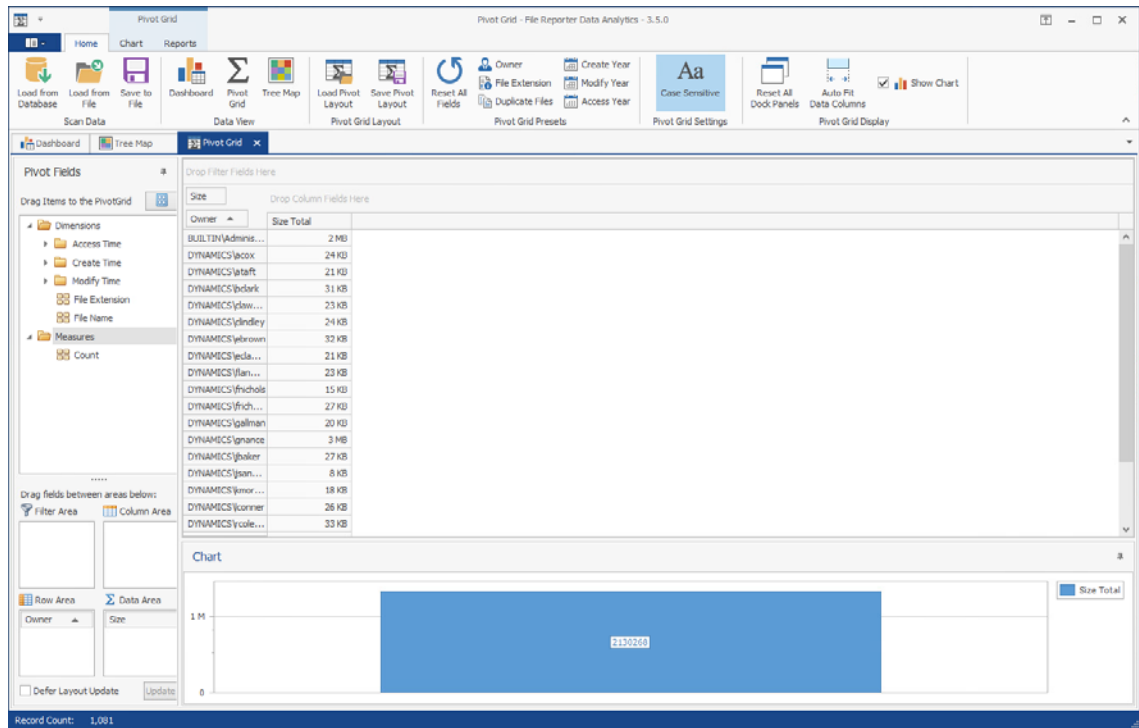
## 10.4 Using the Pivot Grid

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

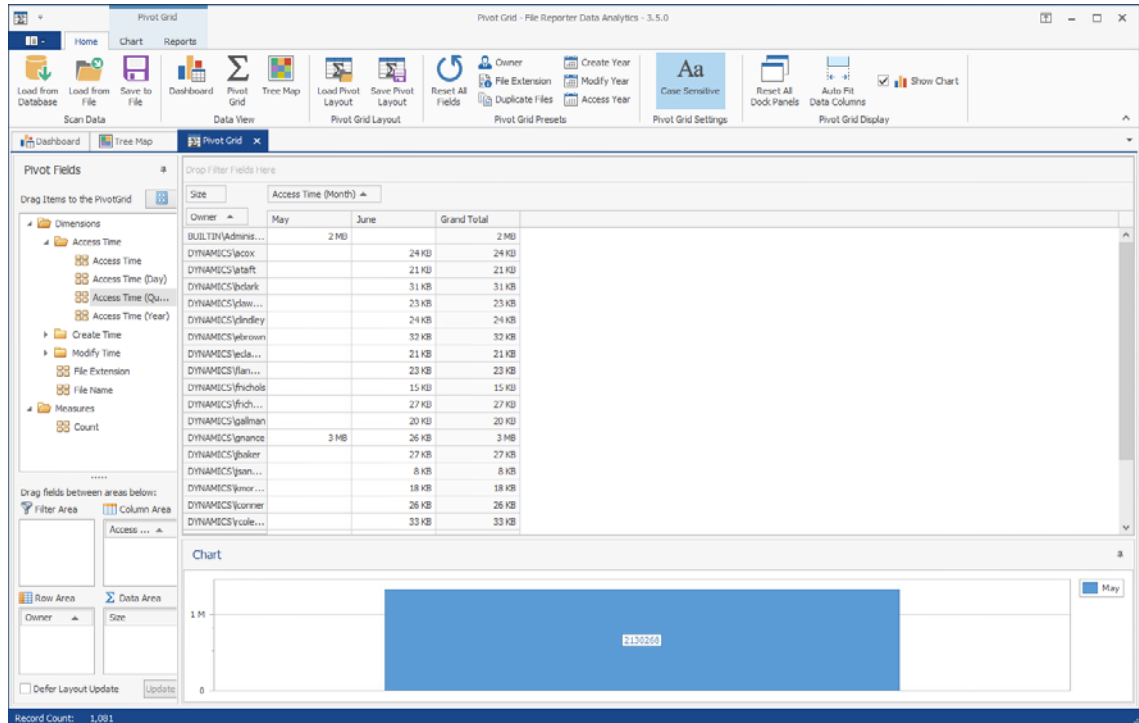
- 1 From the Dashboard, click **Load from Database**.
- 2 Browse to select the file system scan you want and double-click it.
- 3 Click **Pivot Grid**.



- 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.

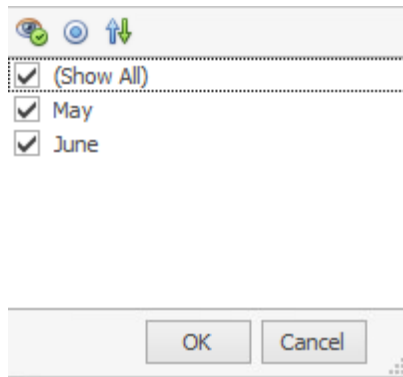


7 From the Pivot Fields region, expand Access Time to locate Access Time (Month) and drag it up to the area marked Drop Column Fields Here.

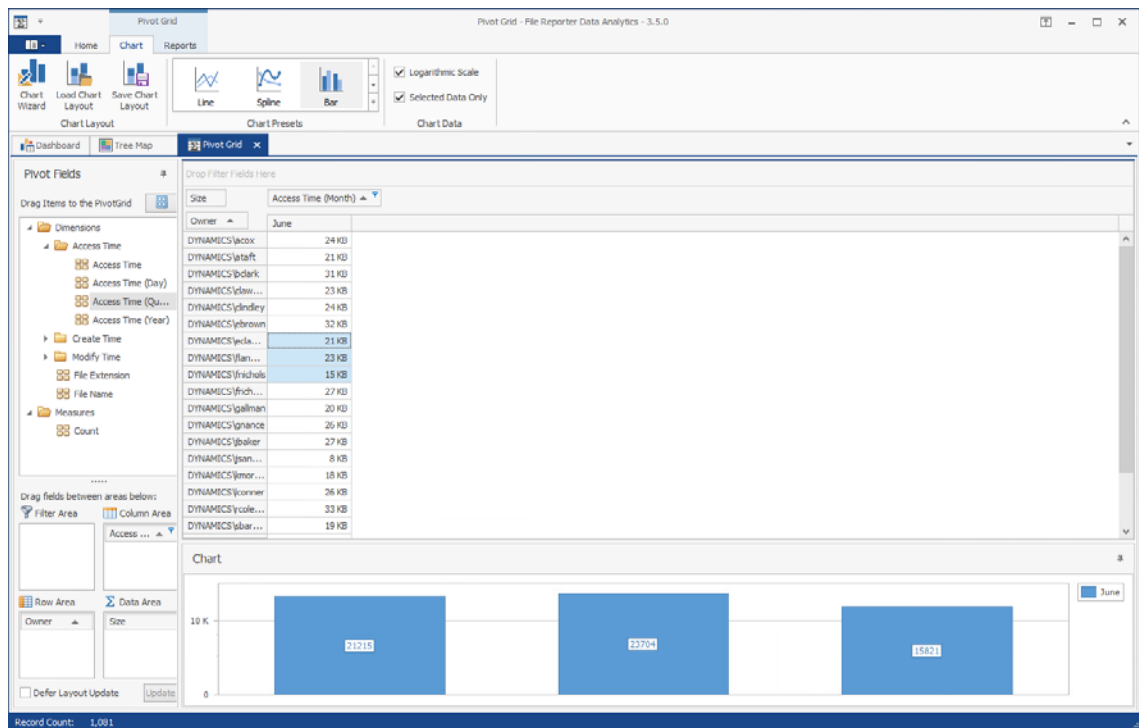


8 Click the filter icon from the Access Time (Month) filter that you just placed.





- 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.



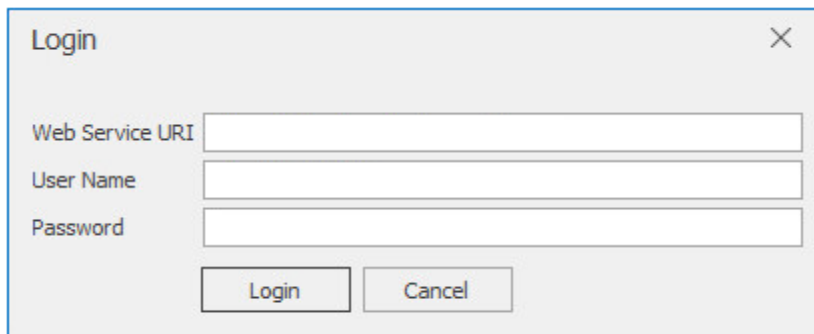
# 11 Using Report Designer

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.

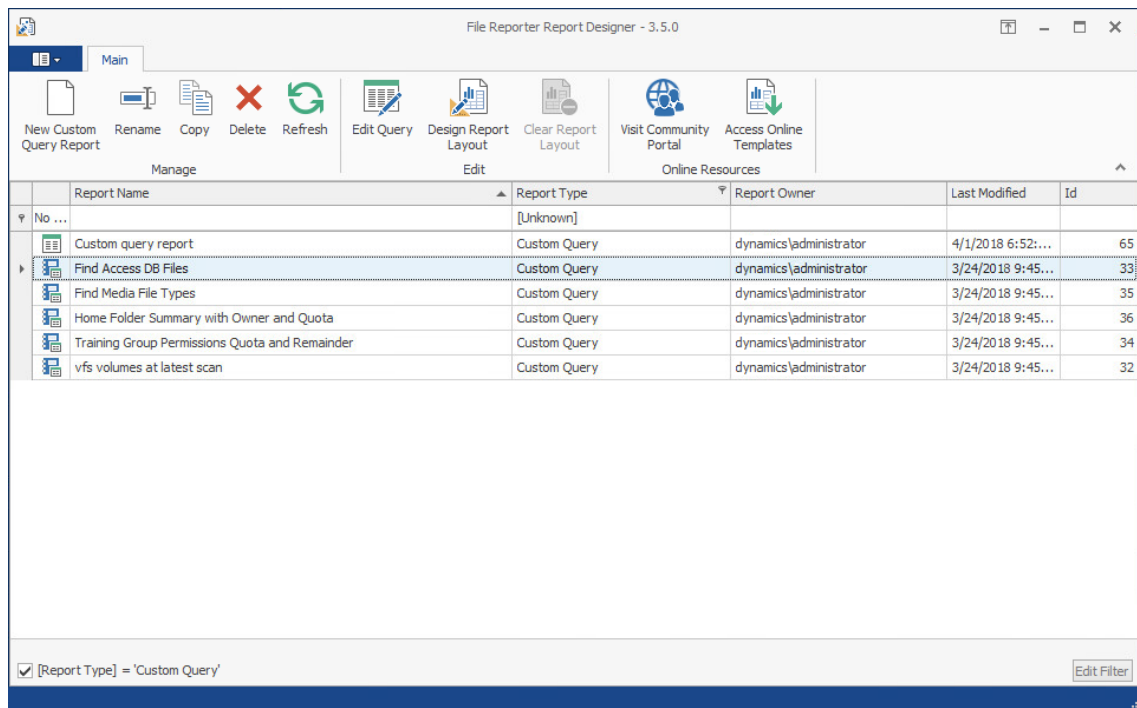
## 11.1 Using the Report Designer Interface

**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 3.6 Report Designer**.



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



Report Name	Report Type	Report Owner	Last Modified	Id
No ...	[Unknown]			
Custom query report	Custom Query	dynamics\administrator	4/1/2018 6:52:...	65
Find Access DB Files	Custom Query	dynamics\administrator	3/24/2018 9:45...	33
Find Media File Types	Custom Query	dynamics\administrator	3/24/2018 9:45...	35
Home Folder Summary with Owner and Quota	Custom Query	dynamics\administrator	3/24/2018 9:45...	36
Training Group Permissions Quota and Remainder	Custom Query	dynamics\administrator	3/24/2018 9:45...	34
vfs volumes at latest scan	Custom Query	dynamics\administrator	3/24/2018 9:45...	32

[Report Type] = 'Custom Query' Edit Filter

### 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.

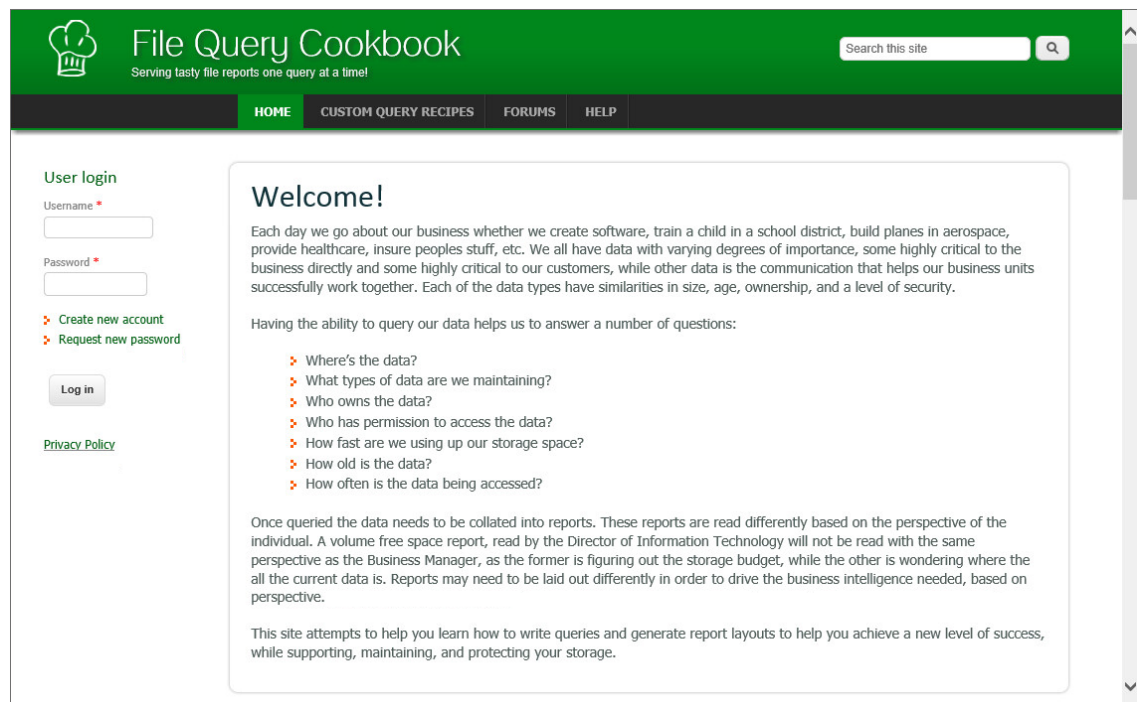
**Refresh:** Click to refresh the list of saved reports.

**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 135](#).

**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.



The screenshot shows the homepage of the File Query Cookbook website. The header is green with the site logo and name, and a search bar. Below the header is a dark navigation bar with links for HOME, CUSTOM QUERY RECIPES, FORUMS, and HELP. The main content area is white and features a 'User login' section on the left with input fields for username and password, and links for 'Create new account' and 'Request new password'. A 'Log in' button is also present. The central 'Welcome!' section contains a paragraph about data management, a list of questions about data querying, and a paragraph about report generation. At the bottom, there is a statement about the site's purpose in helping users learn to write queries and generate report layouts.

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 to 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.

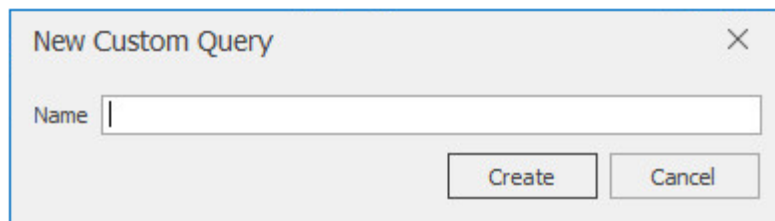
## 11.2 Creating a Custom Query Report

---

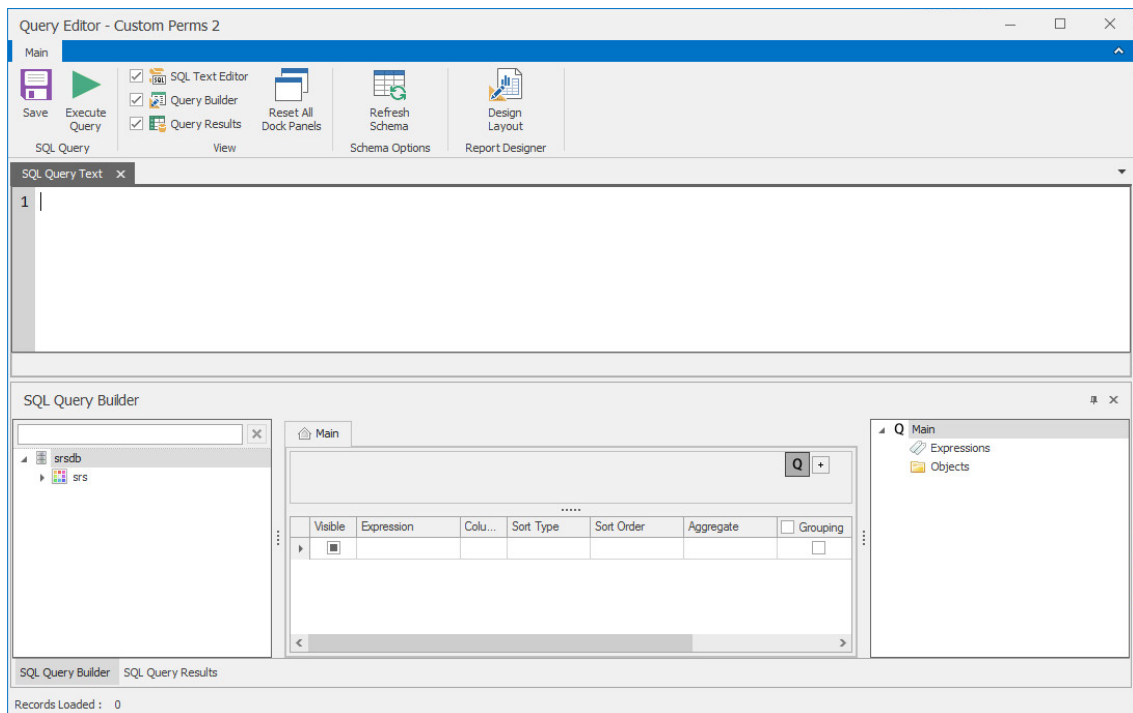
**NOTE:** For details and examples of the supported database functions, tables, and views that you can utilize in Custom Query reports, refer to the *Micro Focus File Reporter 3.6 Database Schema and Custom Queries Guide*.

---

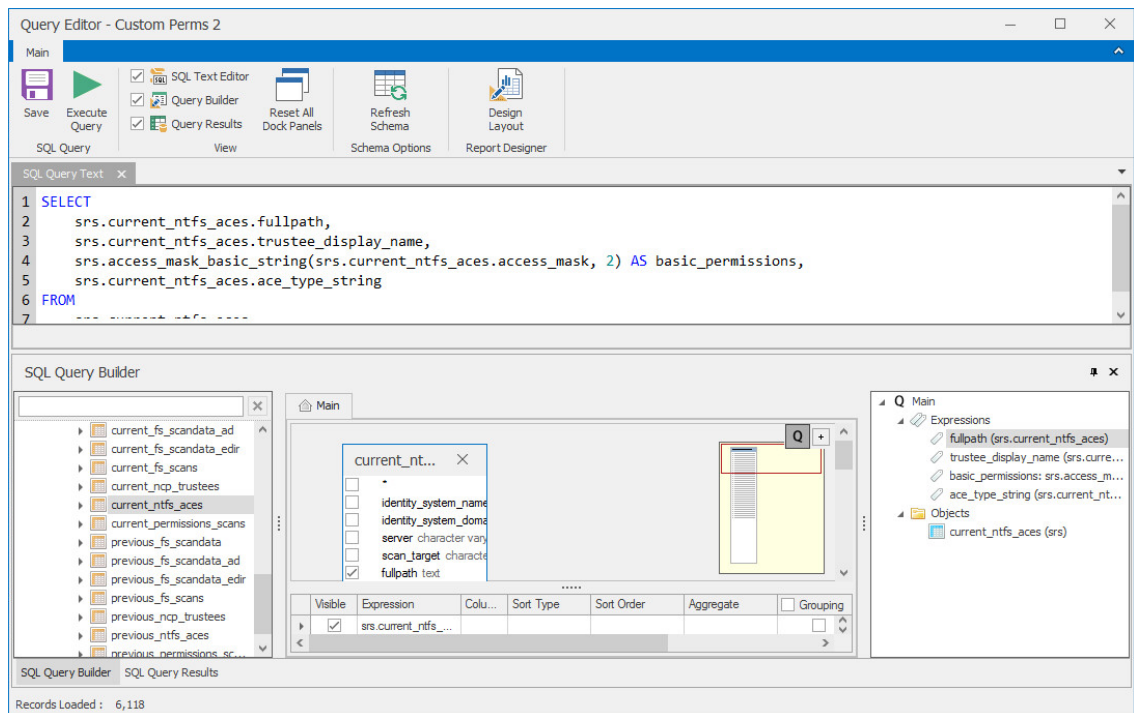
- 1 Click **New Custom Query Report**.



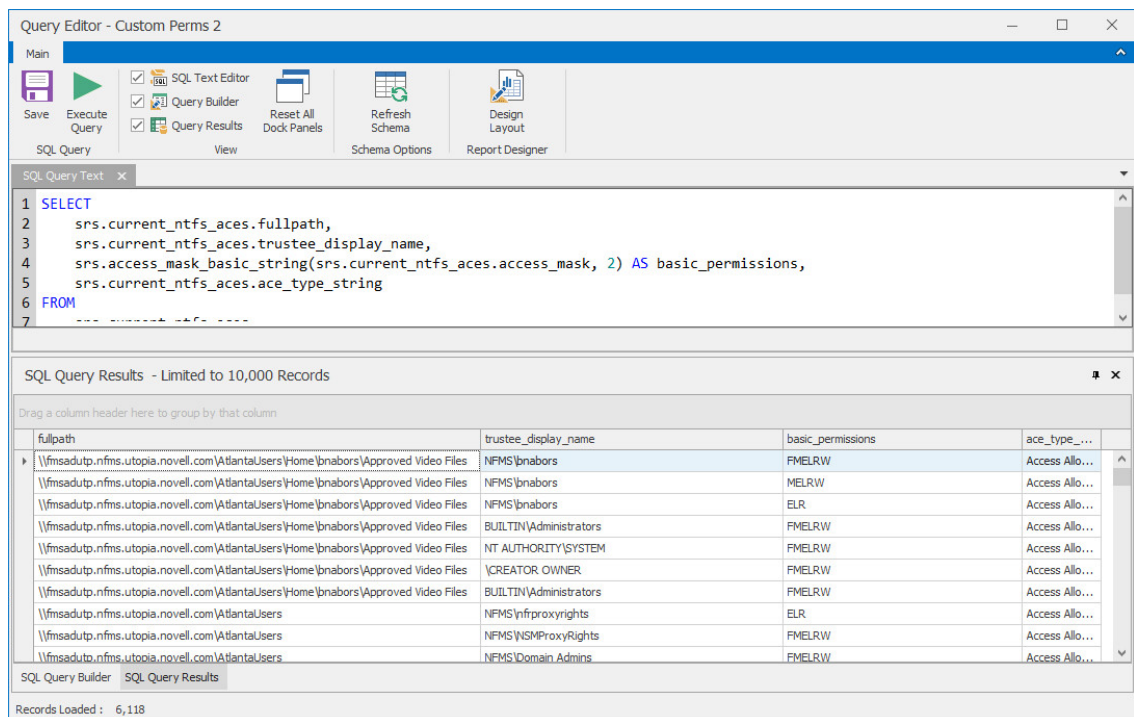
- 2 Specify a descriptive name, then click **Create**.  
The Report Designer Query Editor is launched.



- 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.

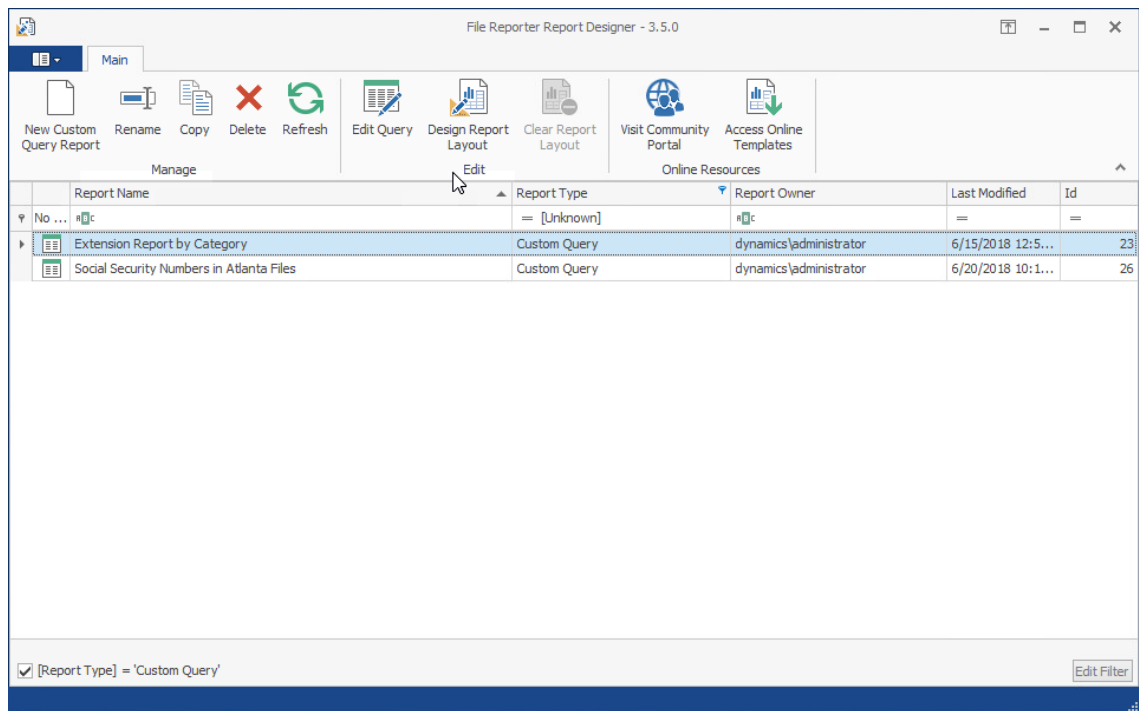
## 11.3 Designing a Custom Query Report

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.

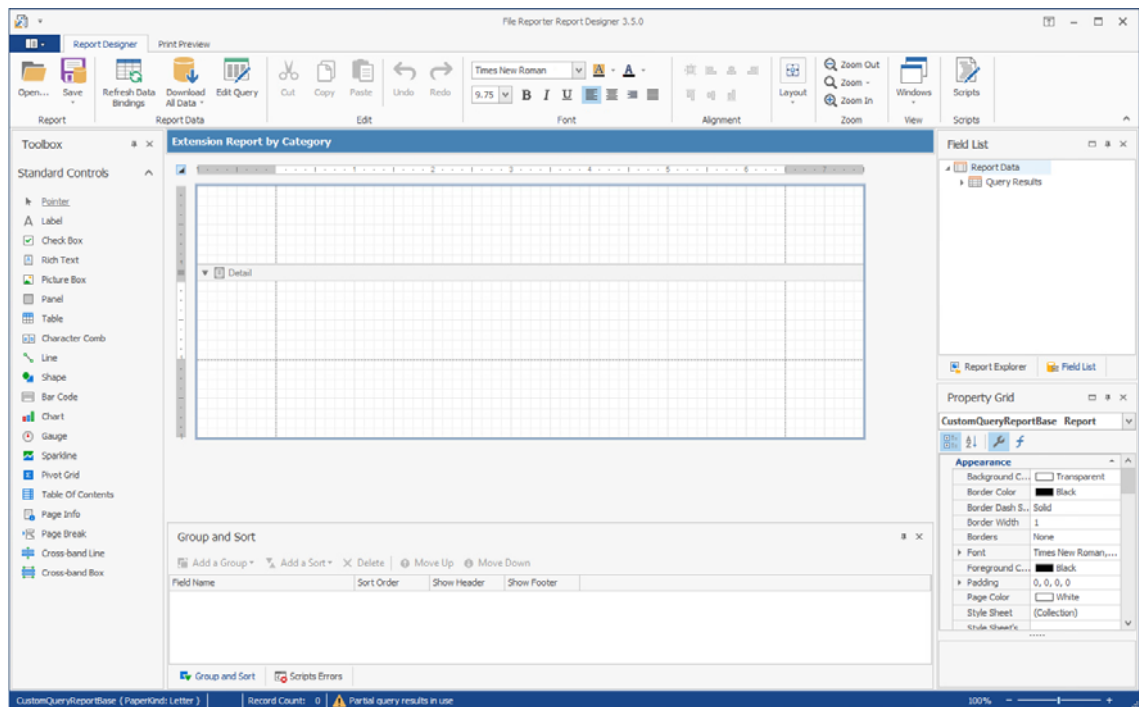
**NOTE:** This exercise introduces you to some of the very basic design features of the Report Designer. Through familiarizing yourself with the basic features, you will become proficient enough in the interface to try more advanced features.

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.



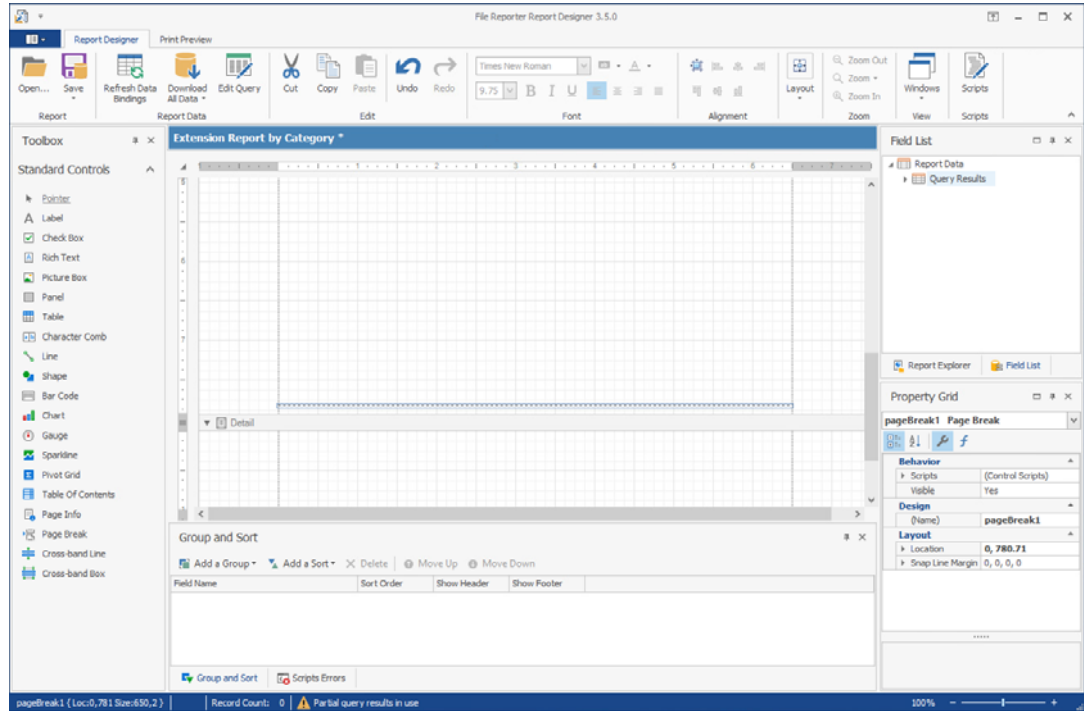
- 2 Click **Design Report Layout**.



- 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.



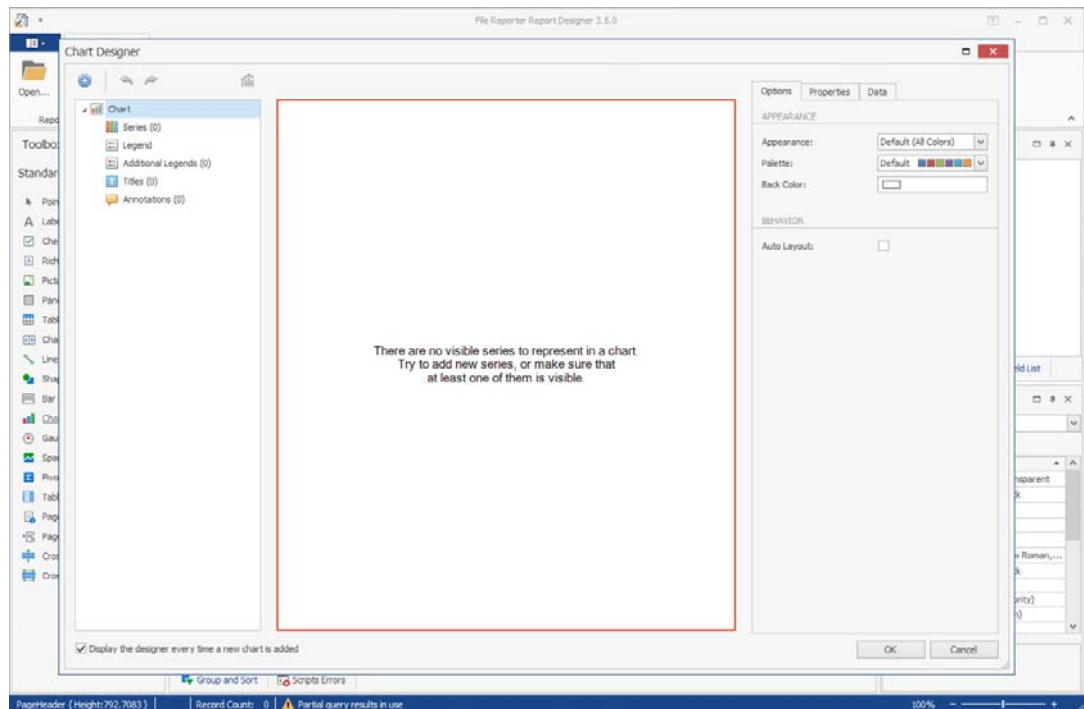
4b From the **Standard Controls** region, click and drag a **Page Break** to the bottom of the band.



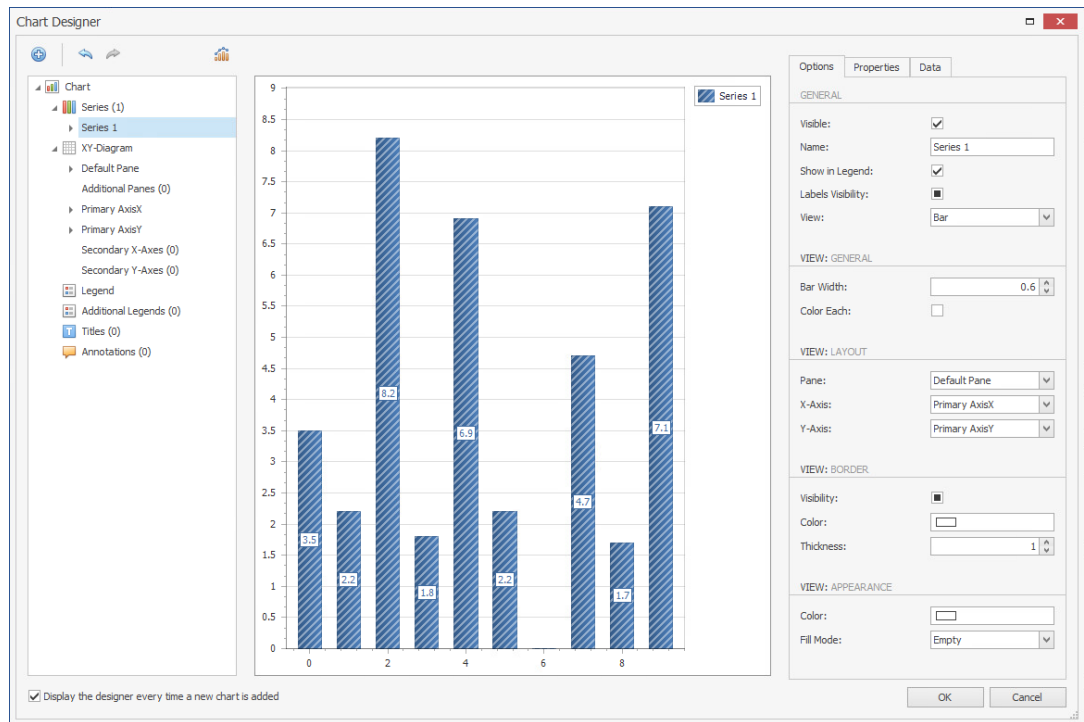
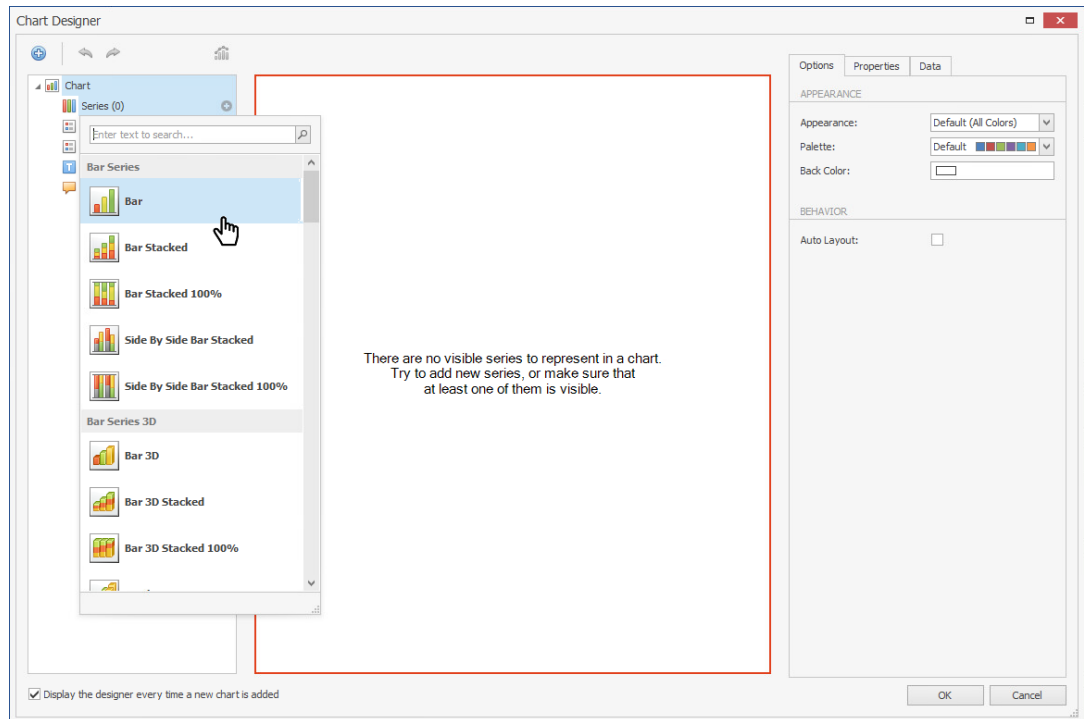
5 Insert and design a chart.

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

The Chart Designer is launched.

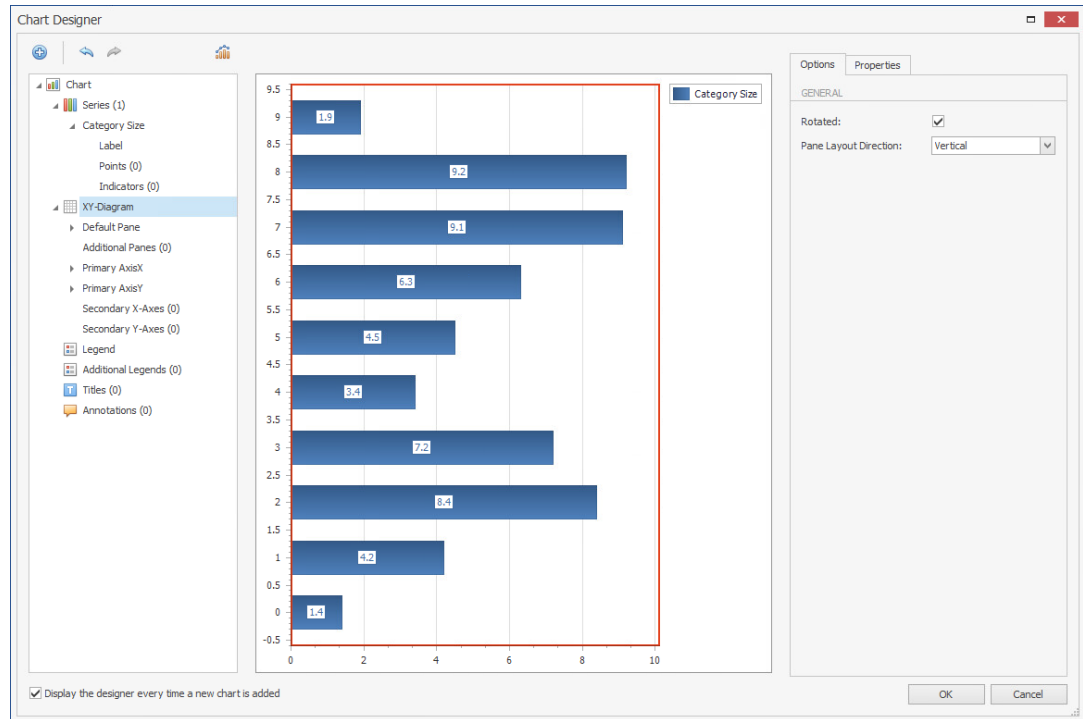


5b In the Chart Designer, below the **Chart** menu, click the **+** that pertains to the **Series** option and select the **Bar** option.



- 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.



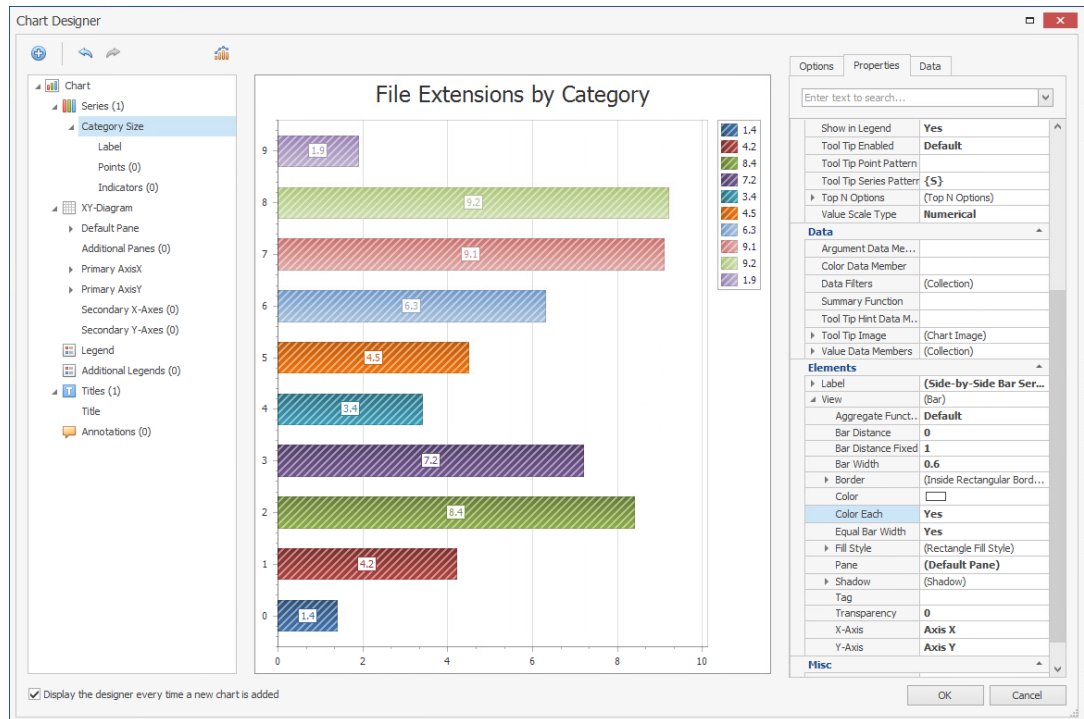
**5i** Below the **Chart** menu, select **Titles**, click the **+**, and select **Title**.

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

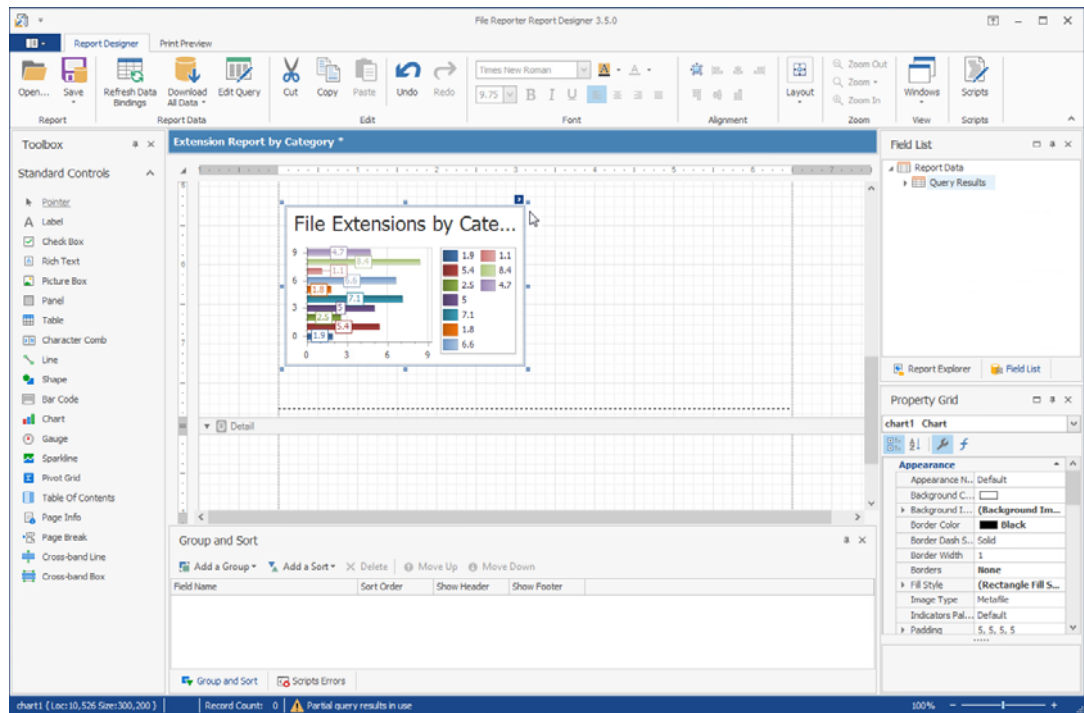
**5k** Below the **Chart** menu, select **Category Size**.

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

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



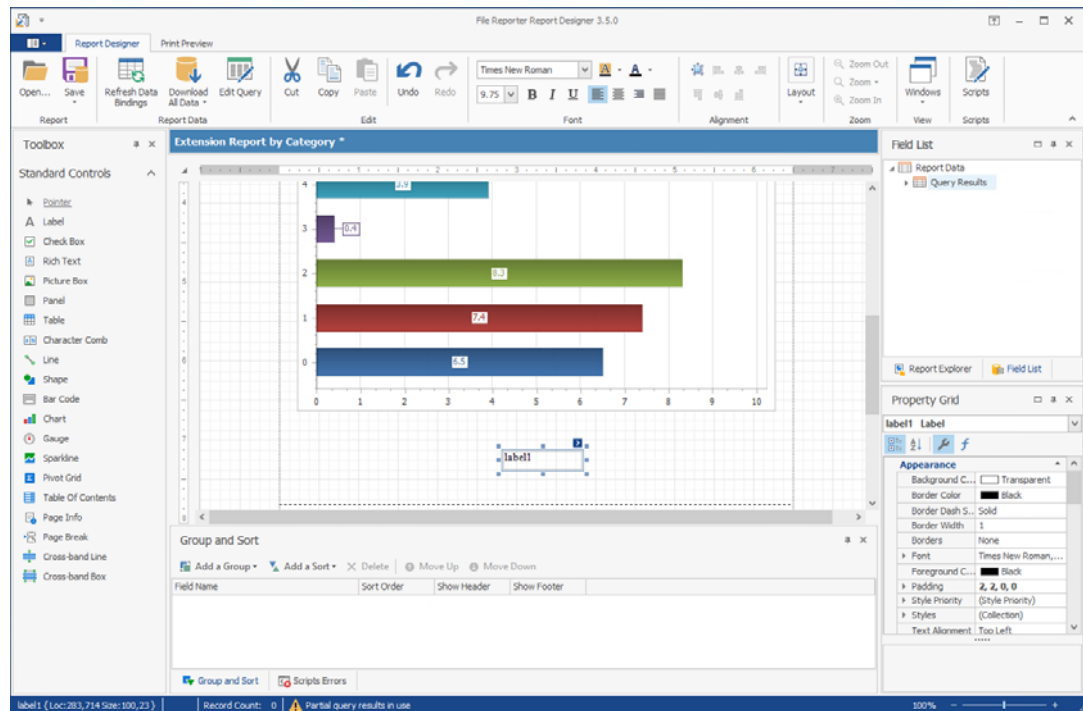
5n Click OK.



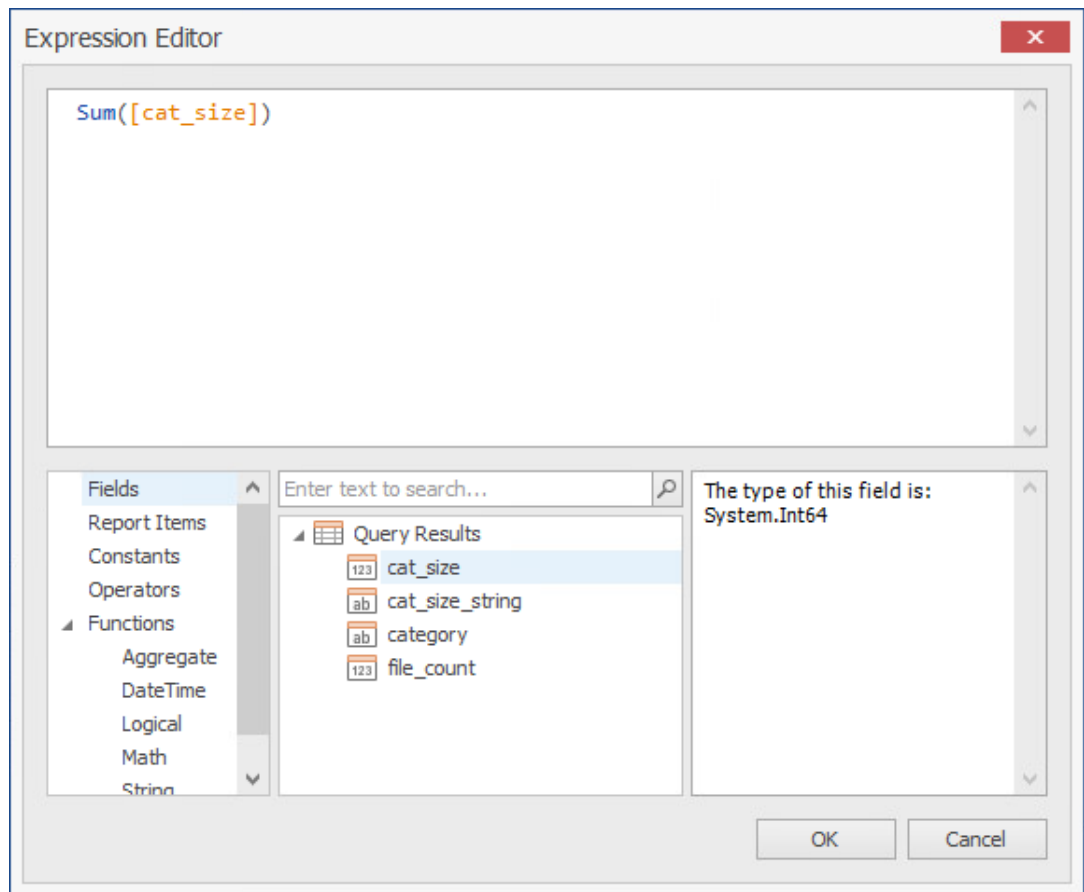
5o In the upper right-hand corner of the newly-placed chart, click the arrow to access the **Chart Tasks** menu and select **Run Designer**.

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

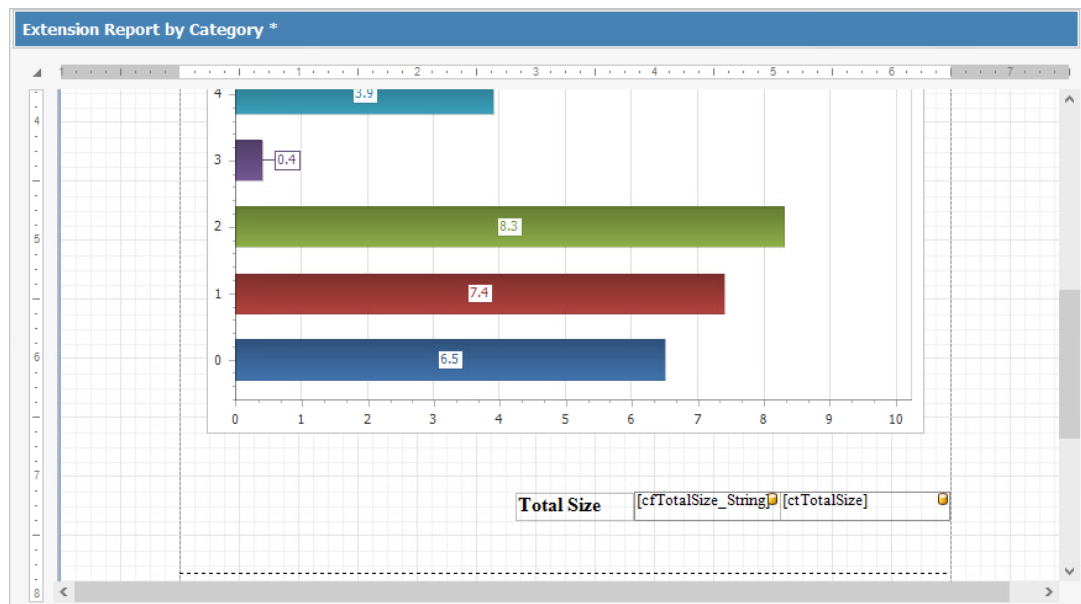
- 5q Click **OK**.
- 5r In the Report Designer, expand the view of the chart to take up more of the page.
- 6 Insert labels.
  - 6a From the Toolbox, click and drag **Label** to a position centered below the chart.



- 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`.

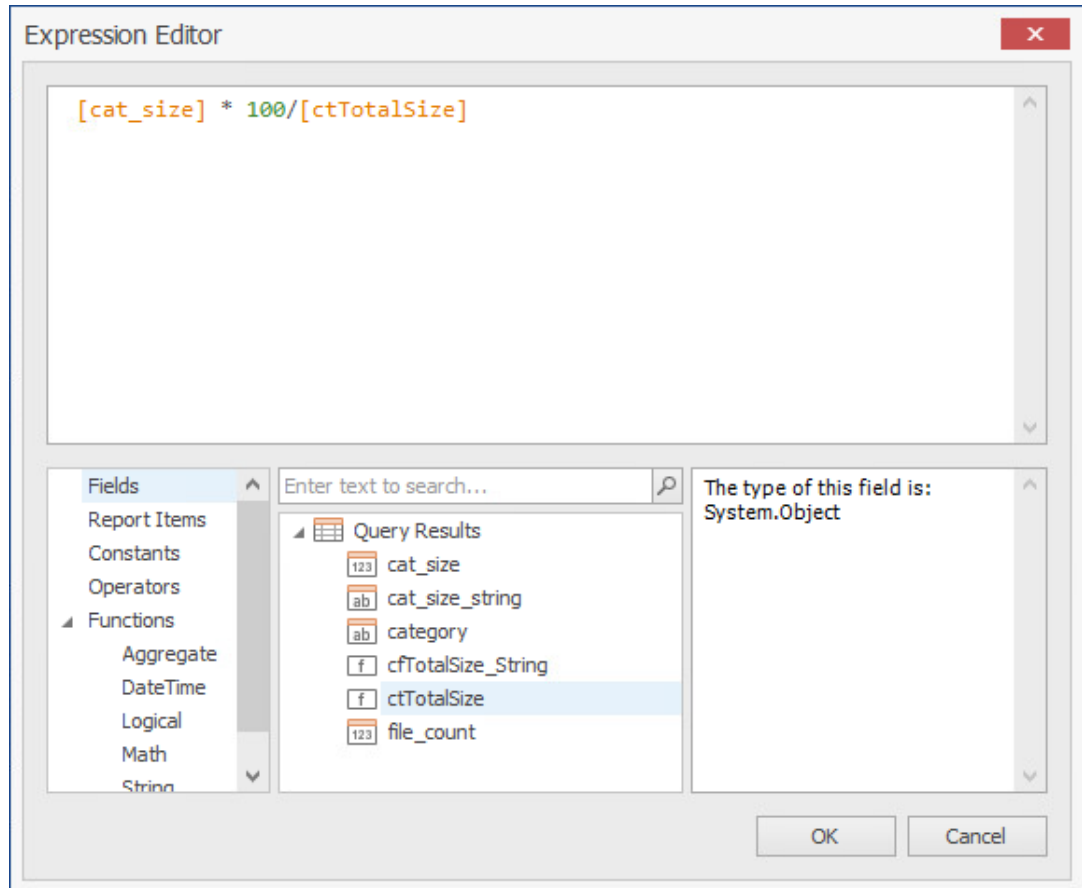


- 7h Click **OK** to save the new field and close the Expression Editor.
- 7i Right-click **Query Results** and select **Add Calculated Field**.
- 7j In the **Design** region of the **Property Grid** for `calculatedField1`, change the **(Name)** setting to `cfTotalSize_String`.
- 7k While still in the **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.



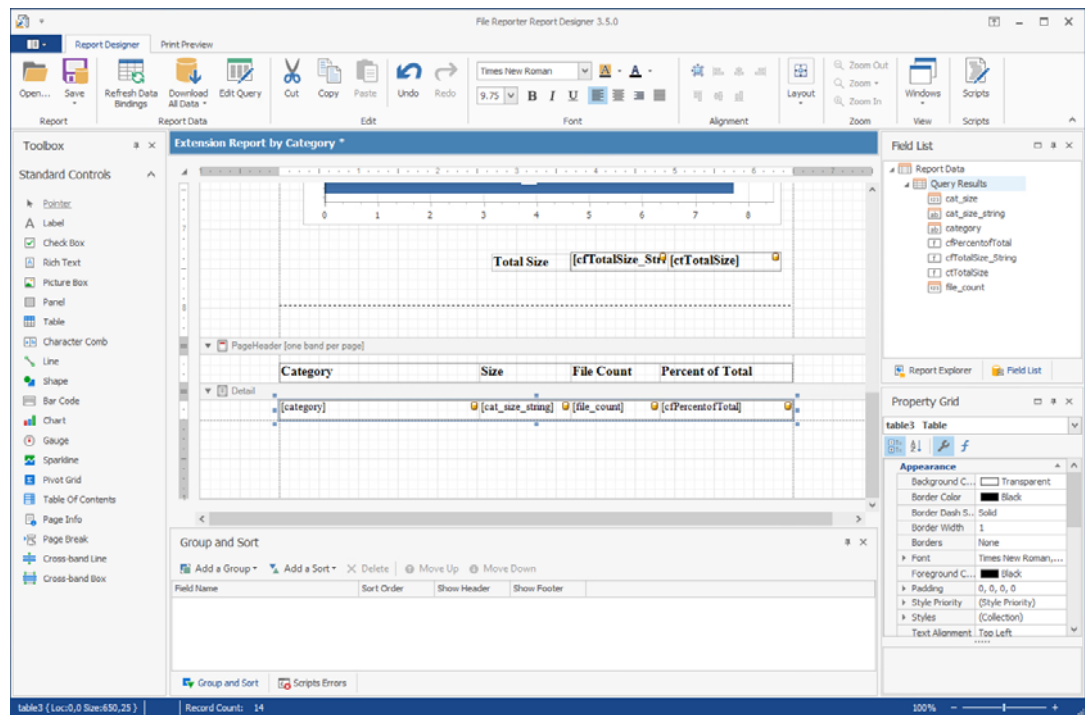
- 8c Adjust the font size and style to your preferences.
- 9 Preview the report.
  - 9a Click **Download All Data**.
  - 9b When the warning dialog box appears, click **Yes**.
  - 9c Click the **Print Preview** tab to observe how the report is going to look at this point.
  - 9d Make any desired format 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> (<http://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

- ◆ [Section A.1, “Filters Tab,” on page 147](#)
- ◆ [Section A.2, “Single Entry Filter Conditions,” on page 149](#)
- ◆ [Section A.3, “Multi-Condition Filtering,” on page 151](#)

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 148](#)
- ◆ [Section A.1.2, “Relative Date Filtering Parameters,” on page 149](#)

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 6/14/2018 11:05:53 AM by DYNAMICS\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.

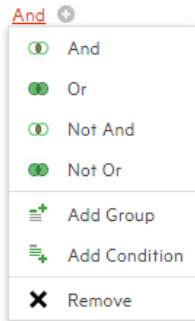
You can filter according to size, dates, or both.

## 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.

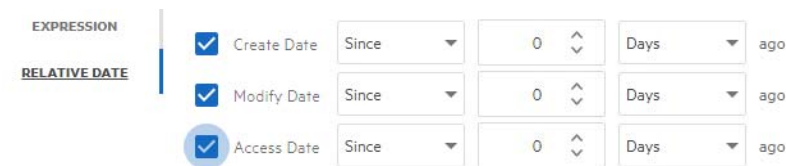
Figure A-3 Parameters for Filter



## 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



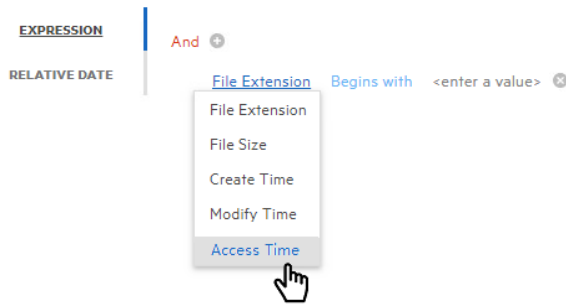
## A.2 Single Entry Filter Conditions

- ◆ [Section A.2.1, “Using the Filter Expression Builder,” on page 149](#)
- ◆ [Section A.2.2, “Using the Relative Date Filtering Settings,” on page 151](#)

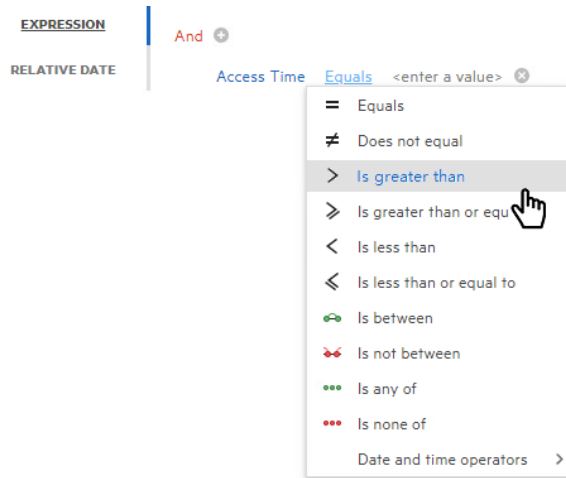
You can use either the **And** drop-menu and + button, or the **Relative Date** filtering settings to create single entry filter conditions.

### A.2.1 Using the Filter Expression Builder

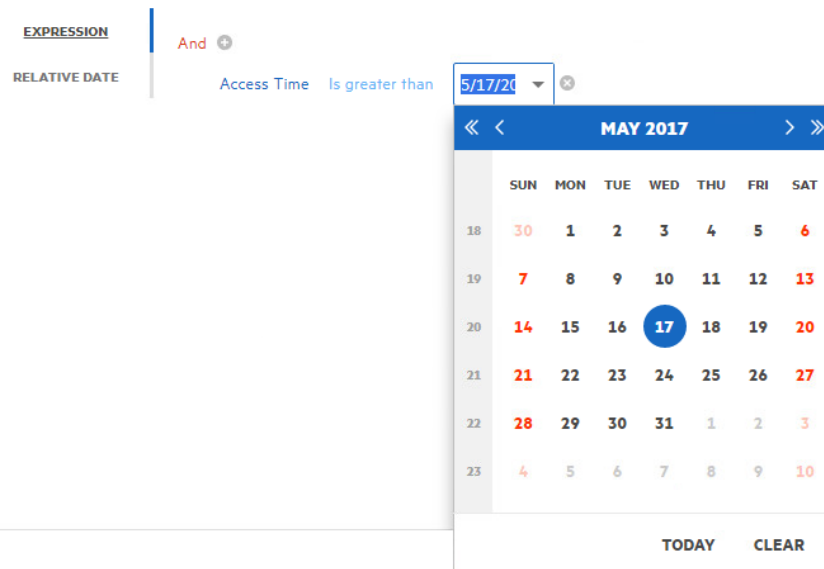
- 1 From the **And** drop-down menu, select a Boolean operator.
- 2 Click the + button to add an entry.
- 3 From the **File Extension** drop-down menu, select a Boolean operator.



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 x 1024). 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:

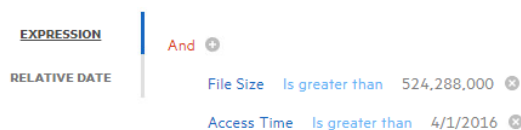
- ♦ Entering parameters for more than one entry using the **And** drop-down menu
- ♦ Specifying multiple **Relative Date** filtering settings
- ♦ Combining parameters specified through the **And** drop-down menu and the **Relative Date** filtering settings

---

**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 153
- ◆ Section B.2, “Firewall Requirements,” on page 153
- ◆ Section B.3, “Local Security Authority Rights and Privileges,” on page 154
- ◆ Section B.4, “Proxy Rights Group,” on page 155
- ◆ Section B.5, “Windows Clustering through Proxy Agents,” on page 155

## B.1 Rights and Privileges on Scanned Storage

Micro Focus File Reporter must have the proper rights set on each network volume or 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:** 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.
- ◆ File System Agents (legacy Agent for Windows, AgentFS, Agent for OES Linux) must be permitted to make outbound connections.
- ◆ File System Agents (legacy Agent for Windows, AgentFS, Agent for OES Linux) 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 15672 for the management interface.

This is the default port that RabbitMQ management interface listens on.
  - ◆ 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*

<b>Component</b>	<b>Typical Log File Path</b>
Engine	C:\ProgramData\Micro Focus\SRS\Engine\log\srsengine.log
Scan Processor	C:\ProgramData\Micro Focus\SRS\Engine\log\scanprocessor.log
Legacy Agent for Windows	C:\ProgramData\Micro Focus\SRS\Agent\log\srsagent.log
AgentFS	C:\ProgramData\Micro Focus\SRS\AgentFS\log\SRSAgentFS.log
Agent for OES Linux	/var/opt/microfocus/srs/agent/log/srsagentd.log
Web Application	C:\inetpub\srs_root\AppData\logs\webui.log
ManagerFC	C:\ProgramData\Micro Focus\SRS\ManagerFC\log\SRSManagerFC.log
AgentFC	C:\ProgramData\Micro Focus\SRS\AgentFC\log\SRSAgentFC.log



# D Agent Scan Capabilities

- ◆ Section D.1, “Server Platform and NAS Device Support,” on page 159
- ◆ Section D.2, “File System Metadata,” on page 160
- ◆ Section D.3, “Security Scans — Active Directory File Systems,” on page 161
- ◆ Section D.4, “Security Scans — eDirectory File Systems,” on page 161
- ◆ Section D.5, “Volume Free Space Scans,” on page 162
- ◆ Section D.6, “Other Microsoft Supported Features,” on page 162
- ◆ Section D.7, “Current Limitations,” on page 162

## 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 3.6
Windows Server 2008	✓ <sup>1</sup>
Windows Server 2008 R2	✓
Windows Server 2012	✓
Windows Server 2012 R2	✓
Windows Server 2016	✓
Open Enterprise Server 2015 SP1	✓ <sup>2,3</sup>
Open Enterprise Server 2018	✓

1. Older Windows servers including Windows 2003 or 2003 R2 might work, but are not supported.
2. Older editions of Open Enterprise Server including OES 2 SP4 and OES 11 SP1 might work, but are not fully supported.
3. NetWare 6.5 SP8 might work with limited support.

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

**Table D-2** Supported Scan Target NAS Hosts

NAS Device	File Reporter 3.6
NetApp Filer with OnTAP 8.x (7 mode or Cluster mode)	✓ <sup>1</sup>
NetApp Filer with OnTAP 9.x	✓
Isilon OneFS 7.2	✓ <sup>1</sup>
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	OES NSS <sup>1</sup>	OES NCP Volumes
File Name / Extension	✓	✓	✓	✓
File Size	✓	✓	✓	✓
File Sparse Size	✓	✓	✗	✗
File Compressed Size	✓	✗	✗ <sup>1</sup>	✗
File Size on Disk <sup>2</sup>	✓	✓	✓	✓
Create Time	✓	✓	✓	✓
Modify Time <sup>3</sup>	✓	✓	✓	✓
Access Time <sup>3</sup>	✓	✓	✓	✓
Directory Quota	✓ <sup>4</sup>	✗	✓	✗
Owner	✓	✓	✓	✓

1. Even though NSS volumes support compression, they only report compression metrics at the volume level, not on a per-file basis.
2. File size-on-disk calculations are currently performed using an assumed 4 KB block size, except when using AgentFS for Windows file systems, which attempts retrieval of the actual allocation size.



3. 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.
4. Directory Quotas for Windows NTFS volumes are only available on Windows 2008 R2 and later servers, and only if the File Server Resource Manager (FSRM) Role has been installed.
5. Scanning of NSS 64 volumes is supported only by:
  - ♦ Agent for OES Linux running on OES 2015 SP1 or later
  - ♦ Legacy Agent for Windows running on Windows Server 2008 R2 or later with OES Client 2 SP4 or later

## 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 Security Scans — eDirectory File Systems

**Table D-5** *Permission Scan Capabilities for eDirectory Environments*

Novell Component	Supported	Notes
Trustees	✓	Only trustees for directories are currently collected.

Novell Component	Supported	Notes
Inherited Rights Masks (IRMs)		These are fully scanned and collected, but reporting does not calculate them for Permissions by Path or Permissions by Identity reports.
Security Equivalence		For calculation of effective rights, security equivalence is collected for all objects that are direct trustees of any file system folder entry, as well as implicit trustees.
Rights Inherited from eDirectory		All users in eDirectory that have Write or Supervisor access to the server object automatically have Supervisor rights to all volumes on that server.
eDirectory Inherited Rights Filters (IRFs)		IRFs are not currently collected nor reported.

## D.5 Volume Free Space Scans

- ♦ Free space for NSS volumes is currently calculated as volume free space + purgeable space.
- ♦ Used space for NSS volumes is currently calculated as total size – calculated free space. This means that the volume compressed size is included along with actual space used.
- ♦ For NSS volumes that are oversubscribed on a shared NSS Pool, the volume total size of each volume in the pool will change as data is added or removed from other volumes in the pool. This is known behavior for oversubscribed volumes.

Oversubscribed NSS volumes are defined as two or more NSS volumes that are set to grow to the size of a shared NSS Pool.

- ♦ NSS 64 volumes are supported by Agents running on OES 2015 servers or Windows Server 2008 R2 or later with Open Enterprise Server Client 2 SP4 or later.

## D.6 Other Microsoft Supported Features

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

## D.7 Current Limitations

The following are scan limitations of File Reporter 3.6:

- ♦ 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
- ◆ Micro Focus (Novell) Environments
  - ◆ NetWare Traditional File System (TFS) volumes are not supported.





# Glossary

**Agent:** A service that can run on Micro Focus Open Enterprise Server and Microsoft Windows Server hosts. Agents can examine and report on NSS and NTFS file systems and content. Additionally, Agents examine and report on file system security, including folder rights, trustee assignments, and permissions.

**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.

**Identity System:** Refers to the supported directory services, which are eDirectory and Active Directory. File Reporter can report on storage resources that reside in either identity system.

**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.

**Micro Focus Storage Manager:** A network file management system that utilizes directory services enacted policies to automatically manage user and group network storage. When installed and configured in the same network, File Reporter can report on Storage Manager policies.

**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, clustered configurations, and NetWare servers require proxy agents.

**Proxy Target:** Servers, clusters, 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 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. Depending on the environment in which File Reporter is deployed, a storage resource can be a server volume, a Windows server share, a Micro Focus Storage Manager policy, 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.





# F

## Documentation Updates

This section contains information about documentation content changes that were made in this *Micro Focus File Reporter 3.6 Administration Guide* after the initial release of File Reporter 2.0. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

### F.1 November 27, 2018

Updates were made to the following section:

Location	Update Description
<a href="#">Section 2.2, "How File Reporter Works," on page 15.</a>	Updated diagram.

### F.2 July 2, 2018

Updates were made to the following sections:

Location	Update Description
<a href="#">Chapter 7, "Content Scanning and Reporting," on page 101.</a>	New chapter.
<a href="#">Appendix B, "Security Settings," on page 153.</a>	Various updates.
<a href="#">Appendix C, "Log File Locations," on page 157.</a>	Log file locations to new components.
<a href="#">Appendix D, "Agent Scan Capabilities," on page 159.</a>	Updated supported scan target hosts, scan target NAS hosts, and file system metadata support.

### F.3 July 19, 2016

Updates were made to the following sections:

Location	Update Description
<a href="#">Chapter 9, "Using the Report Viewer," on page 117.</a>	New section.
<a href="#">Chapter 10, "Using the Client Tools," on page 121.</a>	New section.

Location	Update Description
Chapter 11, "Using Report Designer," on page 131.	New section.
Appendix D, "Agent Scan Capabilities," on page 159.	Updated this section.

## F.4 August 5, 2015

Updates were made to the following sections:

Location	Update Description
Section D.7, "Current Limitations," on page 162.	Removed information on support for NetWare Traditional file system support.
Appendix E, "Glossary," on page 165.	Removed information on support for NetWare Traditional file system support.

## F.5 April 27, 2015

Updates were made to the following sections:

Location	Update Description
Section 5.1.1, "Scan Retention," on page 42.	New section.
Section 5.4, "Creating Scan Policies," on page 44.	Information on Previous scans.
Section 5.5, "Establishing a Baseline Scan," on page 49.	New section.
Section 5.6, "Clearing a Baseline Scan," on page 50.	New section.
Section 6.8, "Historic Comparison Reports," on page 86.	New section.
Section 6.16, "Copying a Report Definition," on page 98.	New section.
Appendix E, "Glossary," on page 165.	New entries.

## F.6 October 7, 2014

Updates were made to the following sections:

Location	Update Description
"Custom Query Reports" on page 20.	New section.
Section 5.14, "Retrying Failed Scans," on page 53.	New section.
Section 6.10, "Custom Query Reports," on page 92.	New section.
Chapter 10, "Using the Client Tools," on page 121.	New section.

## F.7 February 18, 2014

Updates were made to the following sections:

Location	Update Description
Various.	Updated references to database references to include information specific to Microsoft SQL Server 2012.
<a href="#">Section 8.3, "Considerations for Reporting on NAS Devices," on page 113.</a>	Updated this section to include new procedures for EMC Isilon and other NAS devices.
<a href="#">Section 6.3, "Changing the Report Data Font," on page 59.</a>	Expanded this section.
<a href="#">Appendix D, "Agent Scan Capabilities," on page 159.</a>	New section.

## F.8 November 26, 2013

Updates were made to the following sections:

Location	Update Description
<a href="#">Section 6.3, "Changing the Report Data Font," on page 59.</a>	New section.

## F.9 April 25, 2013

Updates were made to the following sections:

Location	Update Description
<a href="#">Section 3.3.2, "Configuring the Web Interface," on page 28.</a>	New procedures.
<a href="#">Appendix A, "Filtering," on page 147.</a>	New section.
<a href="#">Appendix B, "Security Settings," on page 153.</a>	New section.
<a href="#">Appendix C, "Log File Locations," on page 157.</a>	New section.

## F.10 February 13, 2013

Updates were made to the following sections:

Location	Update Description
<a href="#">Section 3.1, "Supported Browsers," on page 25.</a>	Removed Internet Explorer 8 from the list of supported browsers.
<a href="#">Section 5.4, "Creating Scan Policies," on page 44.</a>	Specified that a target path cannot be included in more than one scan policy of the same type.

---

Location	Update Description
<a href="#">Section 6.7.1, "Generating a Filename Extension Report," on page 77.</a>	Inserted a note on the maximum length of file extensions.

---