

Administration Guide

Version 24.3

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 © 2024 Condrey Corporation. All Rights Reserved.

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

Condrey Corporation
122 North Laurens St.
Greenville, SC 29601
U.S.A.

<https://condreycorp.com/>

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 to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth 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 of these elements must fully adhere to and support the appropriate APIs, standards, and protocols 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

Administration Guide	1
Version 24.3	1
Legal Notices	3
Third-Party Systems	5
Contents	7
About This Guide	13
1 - Overview	15
1.1 - Introduction	15
1.2 - How File Reporter Works	15
1.3 - Core Components	16
1.3.1 - Web Application	16
1.3.2 - Engine	16
1.3.3 - Database	16
1.4 - File System Scanning	17
1.4.1 - Scan Processor	17
1.4.2 - AgentFS	17
1.4.3 - Scans	17
1.5 - File Content Scanning	18
1.5.1 - ManagerFC	18
1.5.2 - AgentFC	18
1.5.3 - Scans	18
1.6 - Microsoft 365 Cloud Scanning	18
1.7 - Reporting	19
1.7.1 - Built-in Reports	19
1.7.2 - Custom Query Reports	20
1.8 - Client Tools	21
1.8.1 - Data Analytics	22
2 - Web Application	25

2.1 - Supported Browsers	25
2.2 - Logging In	25
2.3 - Overview	27
2.3.1 - Notifications	27
2.3.2 - Web Client Options	28
2.3.3 - System Information	29
3 - Setup Procedures	31
3.1 - Storage Resources	31
3.2 - Assigning Proxy Targets	33
3.3 - Configuring Notifications	34
3.4 - Integrating with File Dynamics	35
4 - File System Scans	37
4.1 - Overview	37
4.1.1 - Scan Retention	38
4.2 - Scan Targets	38
4.2.1 - Adding a Scan Target	38
4.2.2 - Removing a Scan Target	40
4.3 - Scan Policies	40
4.3.1 - Creating a Scan Policy	40
4.3.2 - Editing a Scan Policy	44
4.3.3 - Deleting a Scan Policy	44
4.4 - Scan Scheduling	44
4.4.1 - Setting a Scan Schedule	44
4.4.2 - Editing a Scan Schedule	46
4.4.3 - Clearing a Scan Schedule	46
4.4.4 - Conducting an Immediate Scan	46
4.5 - Baseline Scans	47
4.5.1 - Establishing a Baseline Scan	47
4.5.2 - Clearing a Baseline Scan	47
4.6 - Scans in Progress	47

4.7 - Scan Data	48
4.7.1 - Viewing Scan Data	48
4.7.2 - Deleting Scan Data	48
4.8 - Scan History	49
4.9 - Retrying Failed Scans	50
4.10 - Troubleshooting	50
5 - Active Directory Identity Scans	51
5.1 - Overview	51
5.1.1 - Scope	51
5.1.2 - Collected Data	51
5.2 - Performing Scans	51
5.2.1 - Scheduling Identity Scans	51
5.2.2 - Performing an Immediate Scan	51
5.3 - Viewing Collected Identities	52
5.4 - Extending Custom Query Reports	52
6 - File Content Scanning	53
6.1 - File Content Classifications	53
6.1.1 - Creating a New Classification	53
6.1.2 - Editing a Classification	54
6.2 - File Content Categories	54
6.2.1 - Creating a New Category	54
6.2.2 - Editing a Category	54
6.3 - File Content Search Patterns	55
6.3.1 - Creating a New Search Pattern	55
6.3.2 - Editing a Search Pattern	57
6.4 - File Content Jobs	57
6.4.1 - Creating a New Job Definition	57
6.4.2 - Editing a Job Definition	61
6.5 - Managing File Content Scans	61
6.5.1 - Verify AgentFC Registrations	61

6.5.2 - Start a File Content Scan Job	62
6.5.3 - Viewing Jobs in Progress	62
6.5.4 - Viewing Scanned Data Matches	63
6.5.5 - Download Search Results	63
7 - Microsoft 365 Scans	65
7.1 - Tenants	65
7.2 - Drives and Document Libraries	66
8 - Reporting	67
8.1 - Built-in Reports	67
8.2 - Custom Query Reports	67
8.3 - Report Definitions	67
8.3.1 - Creating a Report Definition	67
8.3.2 - Deleting a Report Definition	68
8.3.3 - Copying a Report Definition	69
8.4 - Preview Reports	70
8.5 - Stored Reports	72
8.5.1 - Generating Stored Reports	72
8.5.2 - Stored Reports Path	74
8.5.3 - Stored Reports Lifespan	75
8.6 - Report Scheduling	75
8.6.1 - Setting a Report Schedule	75
8.6.2 - Editing a Report Schedule	77
8.6.3 - Clearing a Report Schedule	77
8.7 - Reports in Progress	77
8.7.1 - View Reports In Progress	77
8.7.2 - Cancel a Report in Progress	78
8.8 - Troubleshooting Reports	78
9 - Built-in Reports	79
9.1 - Overview	79
9.2 - Built-in Report Types	79

9.3 - Branding and Style	80
9.3.1 - Cover Sheet Logo	80
9.3.2 - Report Data Font	82
9.4 - File Management Policy Reports	83
9.5 - Built-in Report Filtering	84
Filters Tab	84
9.6 - Directory Reports	86
9.6.1 - Summary Report	86
9.6.2 - Directory Quota Report	90
9.6.3 - Storage Cost Report	91
9.6.4 - Comparison Report	92
9.7 - File Data Reports	94
9.7.1 - Filename Extension Report	94
9.7.2 - Detailed Filename Extension Report	95
9.7.3 - Owner Report	96
9.7.4 - Detailed Owner Report	97
9.7.5 - Duplicate File Report	98
9.7.6 - Detailed Duplicate File Report	100
9.7.7 - Date-Age Report	101
9.7.8 - Detailed Date-Age Report	103
9.8 - Permissions Reports	104
9.8.1 - Assigned NTFS Permissions Report	104
9.8.2 - Permissions by Path Report	105
9.8.3 - Permissions by Identity Report	106
9.9 - Historic Comparison Reports	107
9.9.1 - Historic File System Comparison Report	108
9.9.2 - Historic NTFS Permissions Comparison Report	110
9.10 - Trending Report	111
Generating a Volume Free Space Report	111
9.11 - Folder Summary Reports	112

10 - Custom Query Reports	115
A.1 - Security Settings	119
A.1.1 - Windows Firewall Settings	119
A.1.2 - Windows LSA User Rights	119
A.1.3 - Proxy Rights Group	120
A.1.4 - Windows File Server Cluster	120
B.1 - Log File Locations	123
C.1 - AgentFS Scan Capabilities	125
C.1.1 - Server Platform and NAS Device Support	125
C.1.2 - File System Feature Support	125
C.1.3 - Security Scans	127
C.1.4 - Other Microsoft Supported Features	127
C.1.5 - Current Limitations	128
C.1.6 - AgentFS Scan Capabilities	128
D.1 - NAS Device Considerations	133
D.1.1 - NetApp Filer	133
D.1.2 - PowerScale OneFS	133
D.1.3 - Other NAS Devices	133
E.1 - Resetting the Proxy User Password	135

About This Guide

This guide provides the concepts and procedures for administering File Reporter 24.3 to network administrators who manage network storage resources.

1 - Overview

The following section covers File Reporter, the supported databases, the Engine and Agents, and explains how reports and analytics information are generated.

1.1 - Introduction

File Reporter inventories Microsoft network file systems and Microsoft 365 cloud storage to provide detailed file storage intelligence that helps you secure and optimize your systems for efficiency and compliance.

Engineered for enterprise system reporting, File Reporter gathers data about the millions of files and folders scattered across your network storage devices and cloud storage—including OneDrive for Business, SharePoint Online, and Teams.

Flexible reporting, filtering, and querying options present the exact findings to demonstrate compliance or enable you to take corrective action.

File Reporter identifies currently-stored files, including:

- File size
- Whether the files contain personal or other sensitive information
- When users last accessed or modified the files
- The locations of duplicate files
- And more

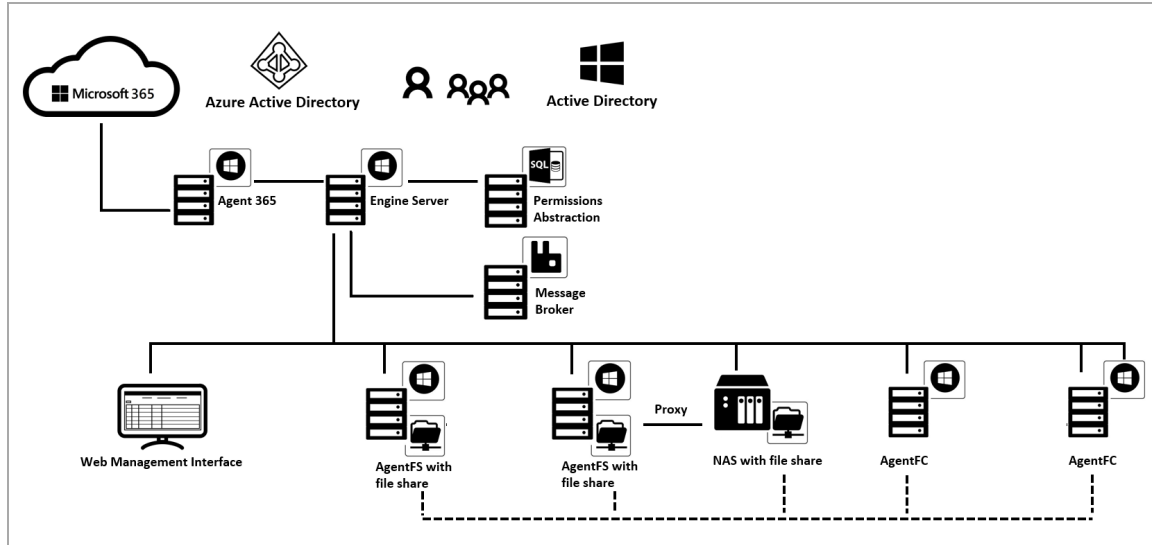
File Reporter can also help you calculate individual or department-wide storage costs, and can even identify access rights to folders and the files contained within.

1.2 - How File Reporter Works

File Reporter examines, analyzes, and reports on the metadata contained within your Windows file systems and Microsoft 365 cloud shares, including file contents, permissions and sharing links associated with these files, folders, and shares.

File Reporter disperses the work among a Web Application, Engine, scan agents, message broker, and database service.

1 - Overview



1.3 - Core Components

1.3.1 - Web Application

The Web Application runs on top of Microsoft Internet Information Services (IIS) and is responsible for all administrative interaction, including:

- Managing scan policies and report definitions.
- Generating preview reports.
- Accessing stored reports.
- Performing all other management functions.

1.3.2 - Engine

The Engine runs File Reporter from a Windows Server host and is responsible for:

- Scheduling scans conducted by the Agents.
- Compiling scans for inclusion in a report.
- Running scheduled reports.
- Managing scan delegations to Agents.
- Sending notifications that File Reporter has completed a scan or generated a report.

1.3.3 - Database

The database stores information needed for generating reports, including:

- Cached Active Directory objects
- Scans

- Identity system information (e.g., the names of Active Directory domains and forests)
- Scheduled scans and reports
- Notification information
- Report definitions
- Scan history
- Scan policies
- Free space on shares

1.4 - File System Scanning

The following components are associated with file system scanning.

1.4.1 - Scan Processor

This component processes file system scan files and updates file system scan information in the database.

1.4.2 - AgentFS

This program runs on Microsoft Windows Server hosts. It examines and reports on NTFS file systems hosted through shares, and collects and scans data related to file system metadata and permissions — See [AgentFS Scan Capabilities \(page 128\)](#) for more information.



IMPORTANT: Install an Agent on every server with a share you want to report on for optimal results. Agents cannot be installed on NAS devices or clustered storage. To report on these types of devices, Agents can be set up as proxy agents.

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

1.4.3 - Scans

File Reporter uses AgentFS to scan storage resources such as Microsoft network shares or Network-Attached Storage (NAS) devices.

File system scans index data specific to a storage resource and generates storage reports, enabling authorized users to review data with the analytics tools.

File system scans include comprehensive information on:

- The file types stored by users.
- When the files were created.
- When the files were last modified.

1 - Overview

- Permission data on the folders in which the files reside.
- And much more.

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

You can conduct scans at any time, but scheduling a time after normal business hours will minimize the effect on network performance.



NOTE: See [Scan Scheduling \(page 44\)](#) for the procedures to perform a scan.

1.5 - File Content Scanning

The following components are associated with file content scanning.

1.5.1 - ManagerFC

The ManagerFC service executes and manages file scan jobs. When processing a scan job, Manager FC:

- Enumerates files in target paths.
- Submits files to scan queues in the message broker, based on filter criteria.
- Processes the scan results and updates the resulting data to the database and scan result files.

1.5.2 - AgentFC

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

1.5.3 - Scans

File Reporter performs, classifies, and categorizes file content scans through AgentFC and ManagerFC. A content scan can identify files containing specified patterns (e.g., US Social Security numbers or credit card numbers).

1.6 - Microsoft 365 Cloud Scanning

File Reporter extends the ability to report on the files stored on your enterprise storage devices—including access permissions—with new reporting features on files and associated permissions located in Microsoft 365 cloud repositories for OneDrive for Business, as well as document libraries for SharePoint Online and Teams.

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

Reporting on Microsoft 365 requires you to develop custom queries and report layouts yourself, or use a report template from <https://filequerycookbook.com>.

See Microsoft 365 Reports in the *File Reporter 24.3 Custom Query Guide* for instructions on creating a Custom Query report from a predefined template.

1.7 - Reporting

When File Reporter performs a scan, you can generate a report through either Built-in Reports or Custom Queries.

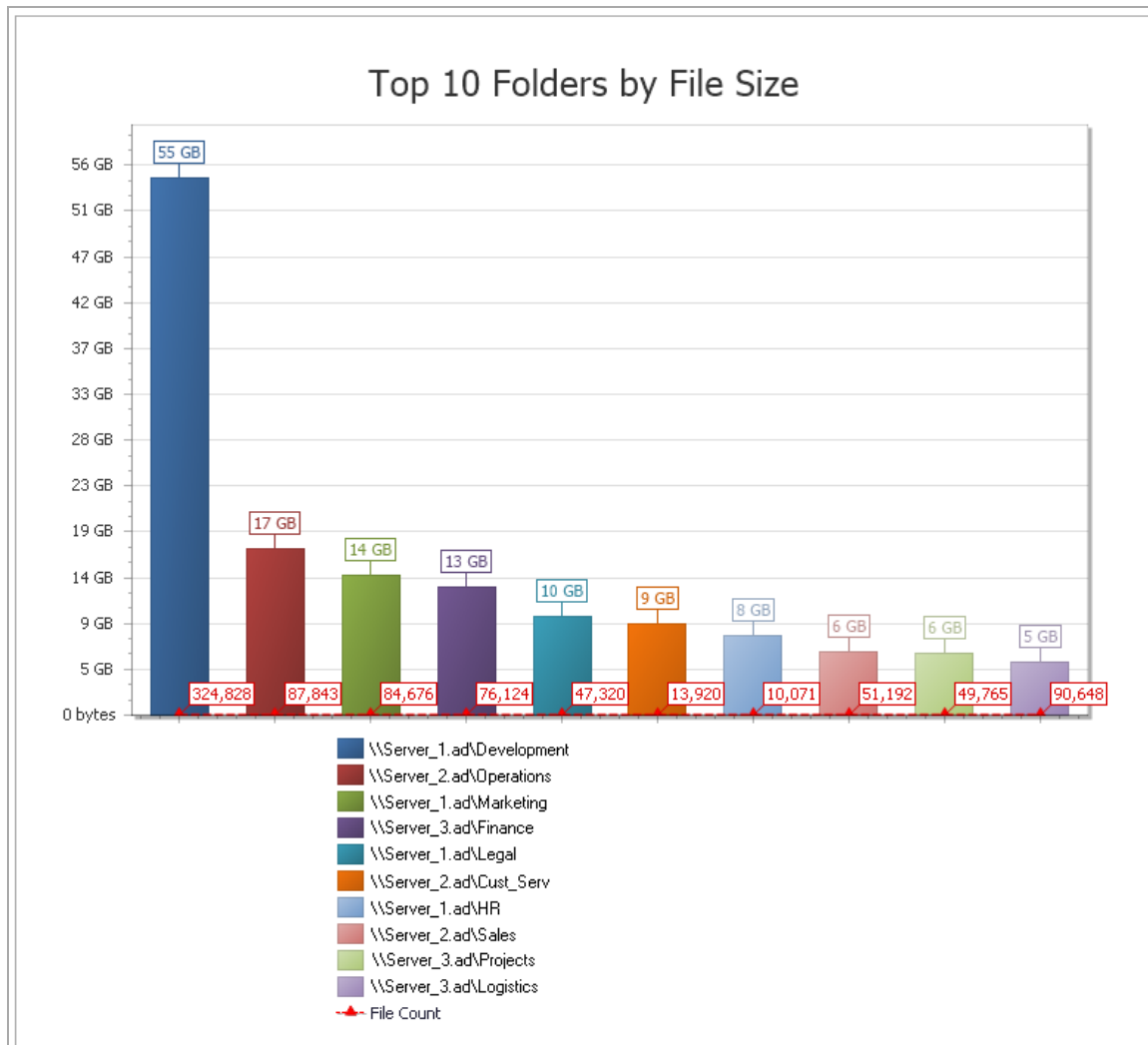
1.7.1 - Built-in Reports

Select the report type from the menu to generate a Built-in Report. The Engine takes the applicable scans specified in the report type, and consolidates and indexes them into a single report.

File System Reports	Security Reports	Trending Reports
Folder Summary	Assigned NTFS Permissions	Volume Free Space
Detail Reports	Permissions by Path	
File Extension	Permissions by Identity	
Duplicate Files	Historic NTFS Permissions	
Date-Age		
Owner		
Storage Cost		
Comparison		
Directory Quota		
Historic File System Comparison		

1 - Overview

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.



1.7.2 - Custom Query Reports

These reports allow administrators to generate precise report data that may not be available through one of the Built-in Report types.

Custom Query report data can be further customized for layout and presentation using the Report Designer (which requires a Windows workstation).

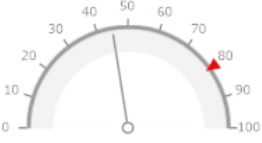
File Content and Microsoft 365 reports are delivered as Custom Query reports.

Membership List:
 NVB\Tatkins NVB\Tsanchez

\\nvb-main.nvb.local\Shares\Forms

Access Based Enumeration Enabled

Total Quota **3 GB**
 Remaining Quota **1.65 GB**



Percent Quota Used

NVB\Managers Member Count: 2

Assigned Permissions **FMELRW**

Membership List:
 NVB\JLarkins NVB\Jsmith

NVB\NVB-Users Member Count: 10

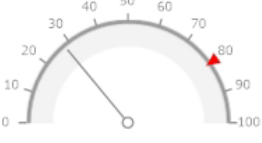
Assigned Permissions **ELR**

Membership List:
 NVB\Flincoln NVB\DThompson
 NVB\Blee NVB\BClarke
 NVB\Tatkins NVB\Tsanchez
 NVB\JLarkins NVB\Jsmith
 NVB\Gstinson NVB\Glopez

\\nvb-main.nvb.local\Shares\Home

Access Based Enumeration Enabled

Total Quota **12 GB**
 Remaining Quota **8.62 GB**



Percent Quota Used

NVB\NVB-Users Member Count: 10

Assigned Permissions **ELR**

Membership List:
 NVB\Flincoln NVB\DThompson
 NVB\Blee NVB\BClarke

3/4

1.8 - Client Tools

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

21

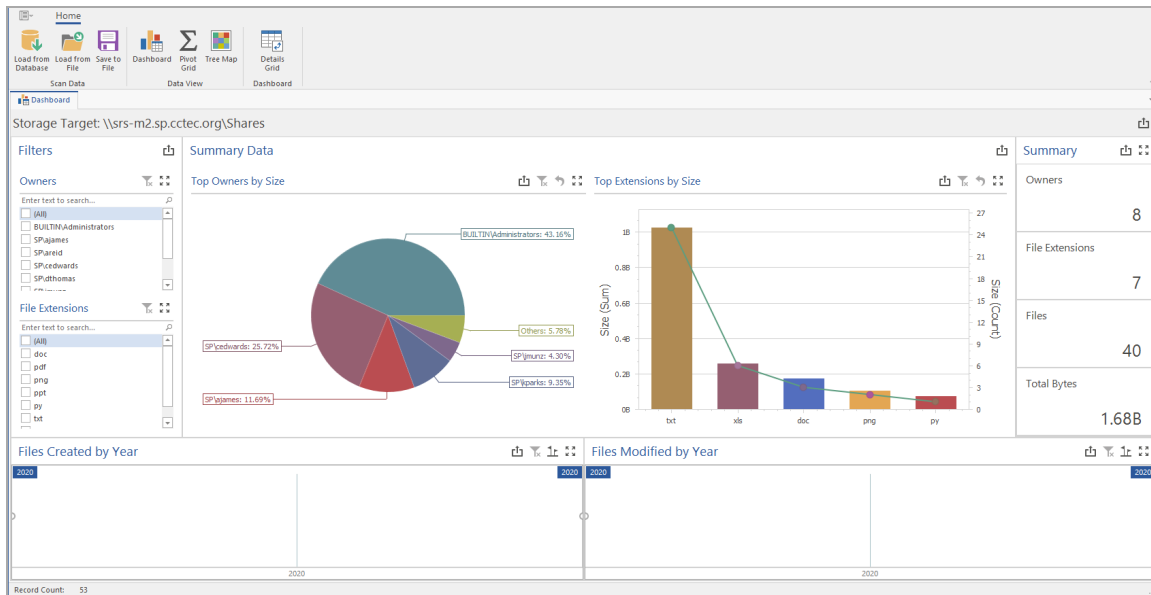
1 - Overview

1.8.1 - Data Analytics

In addition to extensive reporting options, File Reporter can graphically analyze file system data using a variety of analytics tools.

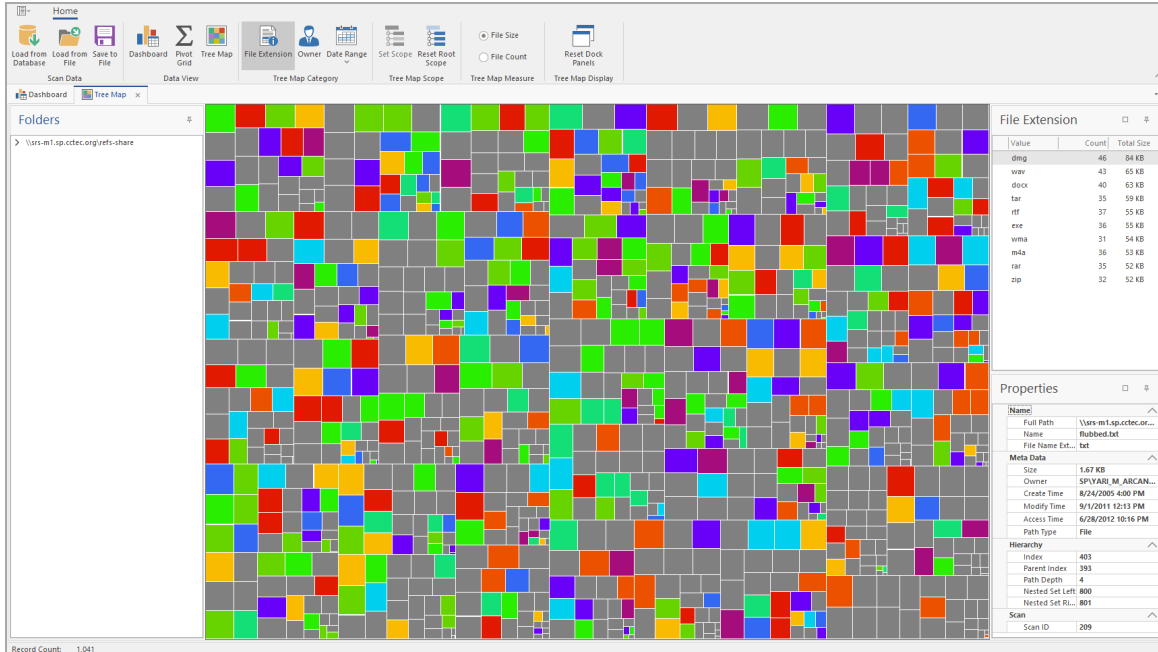
Dashboard

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



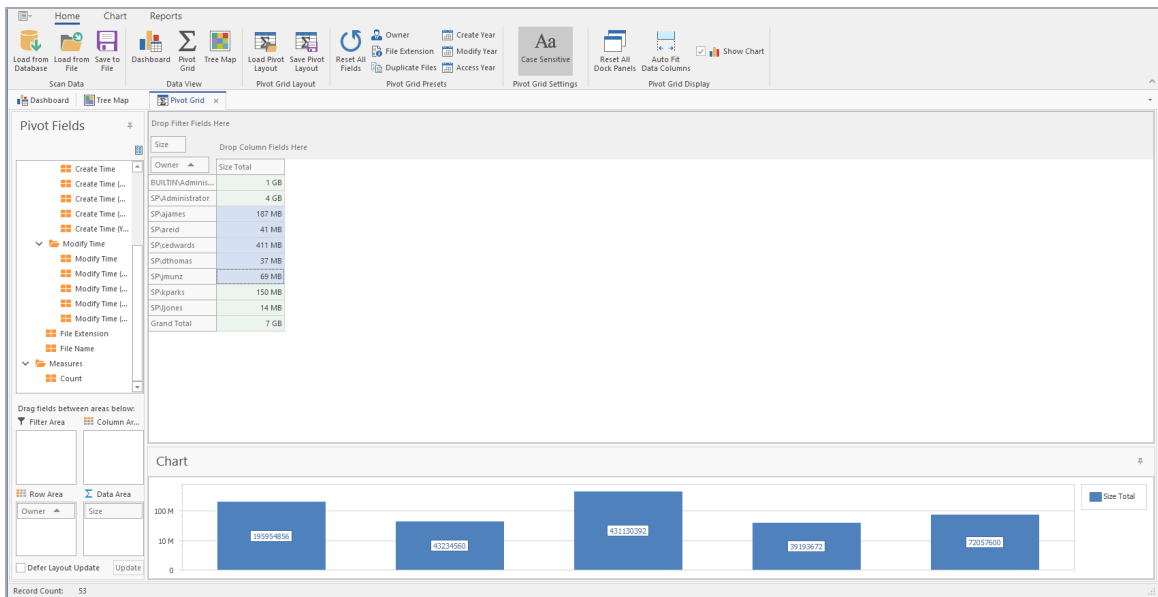
Tree Map

The Tree Map lets you view graphical representations of hierarchical file system data and gain insight quickly.



Pivot Grid

The Pivot Grid lets you visually analyze data according to combinations of variables.



Report Viewer

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

1 - Overview

Print Preview

Open Save Print Quick Print Find Bookmarks

First Page Previous Page Next Page Last Page

Many Pages Zoom Out Zoom Zoom In

Page Color Watermark Export To

Document Print Navigation Zoom Page Background Exp...

Document Map

- Owner
 - Parameters
 - Top Ten Owners by File Size
 - Report Data

Owner Report

CCTEC

Report Date: 11/30/2020 8:54:32 PM
Generated by: File Reporter

File Reporter Page 1 of 5

2 - Web Application

The following procedures enable the use of File Reporter's web browser-based administrative interface and options.

2.1 - Supported Browsers

File Reporter is managed through a browser-based interface, using one of the following supported browsers::

Windows	Linux	Mac OS X
Firefox	Firefox	Firefox
Chrome		Chrome
Edge		

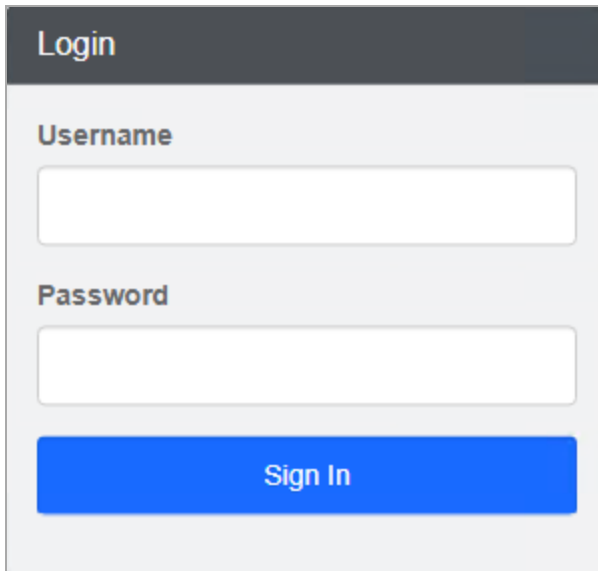
2.2 - Logging In

1. Enter `https://File Reporter_web_server_dns_name` in the browser's address bar to open the login window.



NOTE: In the above file path, "dns_name" is the DNS name you created when installing File Reporter. You must enter the DNS name. You cannot log in with an IP address.

2 - Web Application



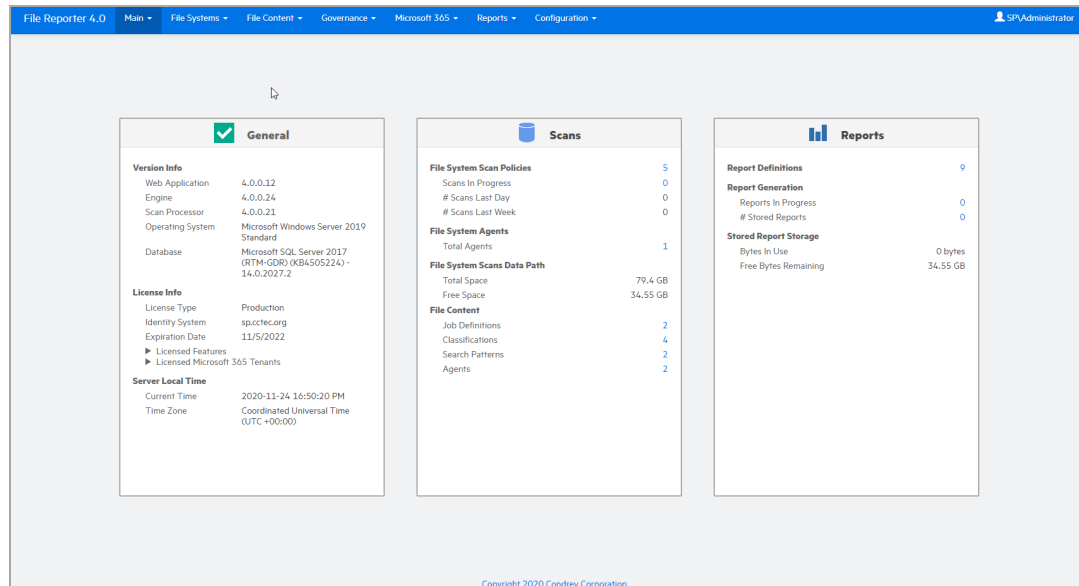
2. Enter the username and password of a member of the SrsAdmins group you created and click *Log In* to open the File Reporter Home page.



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

- *domain\SAMAccountName* (AD\User1)
- UPN (user1@sp.cctec.org)
- LDAP (CN=user1,OU=home,DC=sp,DC=cctec,DC=org)

There may be partial case sensitivity with LDAP, especially with regard to the domain (DC=) components.



2.3 - Overview

All tasks are performed by selecting an option from one of the menus at the top of the File Reporter Home page.

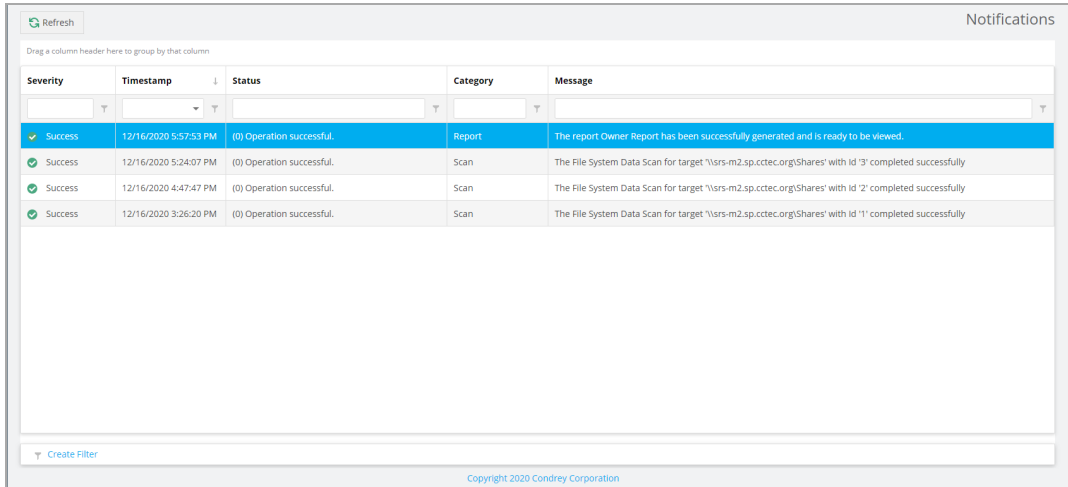
- *Main* provides access to notifications and system information.
- *File Systems* lets you set up and view the progress of file system scans.
- *File Content* lets you set up and conduct file content scans.
- *Governance* lets you conduct access reviews on unstructured data through OpenText Identity Governance.
- *Microsoft 365* launches scans of OneDrive for Business, and document libraries for SharePoint Online and Teams.
- *Reports* lets you generate and access reports.
- *Configuration* lets you establish and modify configuration settings within File Reporter.

2.3.1 - Notifications

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

2 - Web Application

1. Select *Notifications* from the *Main* menu.



The screenshot shows a web application window titled "Notifications". At the top left is a "Refresh" button. Below it is a header row with columns: "Severity", "Timestamp", "Status", "Category", and "Message". Each column has a dropdown arrow. Below the header is a table with four rows of notification data. The first row is highlighted in blue. At the bottom left is a "Create Filter" button. At the bottom center is the text "Copyright 2020 Condrey Corporation".

Severity	Timestamp	Status	Category	Message
Success	12/16/2020 5:57:53 PM	(0) Operation successful.	Report	The report Owner Report has been successfully generated and is ready to be viewed.
Success	12/16/2020 5:24:07 PM	(0) Operation successful.	Scan	The File System Data Scan for target '\\srs-m2.sp.cctec.org\Shares' with id '3' completed successfully
Success	12/16/2020 4:47:47 PM	(0) Operation successful.	Scan	The File System Data Scan for target '\\srs-m2.sp.cctec.org\Shares' with id '2' completed successfully
Success	12/16/2020 3:26:20 PM	(0) Operation successful.	Scan	The File System Data Scan for target '\\srs-m2.sp.cctec.org\Shares' with id '1' completed successfully

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

2. (Optional) Display columns in the order you want by dragging them to the desired location.
3. (Optional) List the most recent notification by clicking the column heading twice.
4. (Optional) Filter the notifications to display only the information you want:
 - a. Click the "pin" icon in the desired column heading (e.g., *Message*).
 - b. Select the desired filter option (e.g., *Contains*).
 - c. Enter the distinguishing word or letter for the filter (e.g., *Permissions*) in the field to the left of the "pin" icon.

The page is updated according to the filtering parameters.

2.3.2 - Web Client Options

Users are logged out of the administrative interface after 20 minutes of inactivity. You can use the *Web Application* option in the *Configuration* menu to adjust this setting and specify the number of items displayed per page.

1. Select *Web Application* from the *Configuration* menu.

The screenshot shows the 'Web Config' interface. It has two main sections: 'Display Options' and 'Session Options'. In 'Display Options', the 'Grid Page Size' is set to 50 rows. In 'Session Options', the 'Authentication Timeout' is set to 1440 minutes and the 'Report Page Execution Timeout' is set to 900 seconds. There is an 'Apply' button at the bottom left and a copyright notice at the bottom center.

2. Specify the number of entries to display in the *Grid Page Size* field.
3. Specify the minutes of inactivity before login is required again in the *Authentication Timeout* field.
4. Click *Apply*.
5. When notified that the Web interface configuration is saved, click *OK*

2.3.3 - System Information

When you work with a Support representative to diagnose the source of a problem, you may be asked to access the System Info page by selecting *System Configuration* in the *Main* menu.

The screenshot shows the 'System Info' page. It is divided into two main panels. The left panel, 'Database Statistics', shows details for a Microsoft SQL Server 2019 instance, including version string, total size, host address, name, and schema version. It also lists 'Scans' and 'Identity System Data'. The right panel, 'Referenced Web Application Assemblies', contains a table with columns for Name, Version, and Processor Architecture.

Name	Version	Processor Architecture
Condrey.Product	2.0.7.0	None
Condrey.Srs.Core	4.0.8.0	None
Condrey.Srs.Core.Database	4.0.0.2	None
Condrey.Srs.CoreExt	4.0.0.6	None
Condrey.Srs.Product	4.0.12.0	None

3 - Setup Procedures

A few tasks must be performed before you can begin scanning storage resources and generating reports.

3.1 - Storage Resources

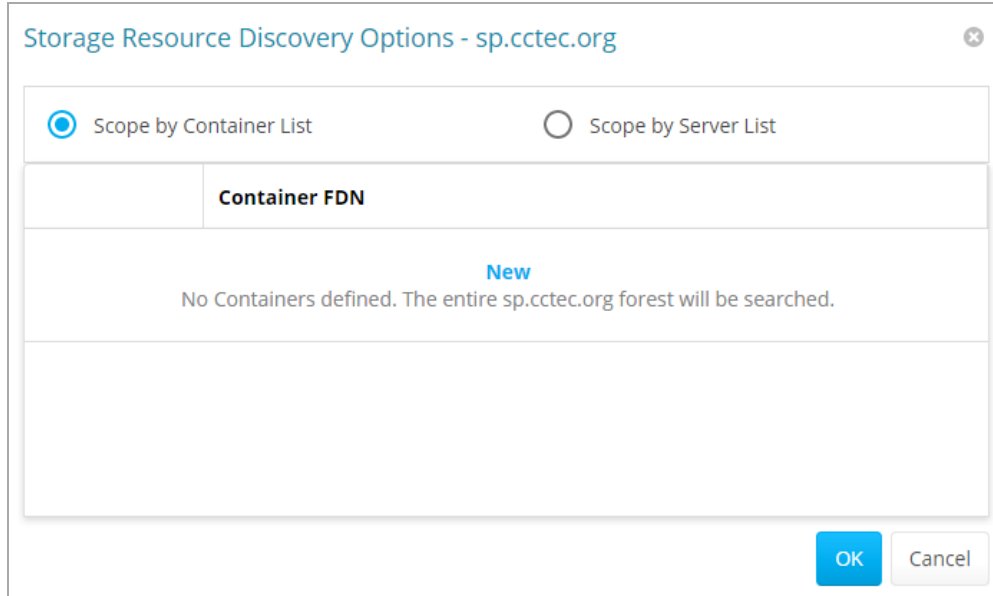
When Active Directory is enabled, the associated storage resources become available for scanning and reporting. File Reporter cannot see a Windows network disk drive that is not shared.

1. Select *Storage Resources* in the *Configuration* menu to display all the servers in the Active Directory forest.

Resource	Operating System	File System	Last Update	Last Update Attempt	Last Status
<input type="checkbox"/> dc.sp.cctec.org	Windows Server 2019 Standard		12/16/2020 3:24:57 PM	12/16/2020 3:24:57 PM	✓
<input checked="" type="checkbox"/> srs-m1.sp.cctec.org	Windows Server 2019 Standard	Never	Never	Never	⚠ The specified name could not be resolved by the network client.
<input type="checkbox"/> srs-m2.sp.cctec.org	Windows Server 2019 Standard		12/16/2020 3:24:57 PM	12/16/2020 3:24:57 PM	✓
<input type="checkbox"/> srs-m3.sp.cctec.org	Windows Server 2019 Standard	Never	Never	Never	⚠ The specified name could not be resolved by the network client.
<input type="checkbox"/> w2k8r2.sp.cctec.org	Windows Server 2008 R2 Standard	Never	Never	Never	⚠ The specified name could not be resolved by the network client.

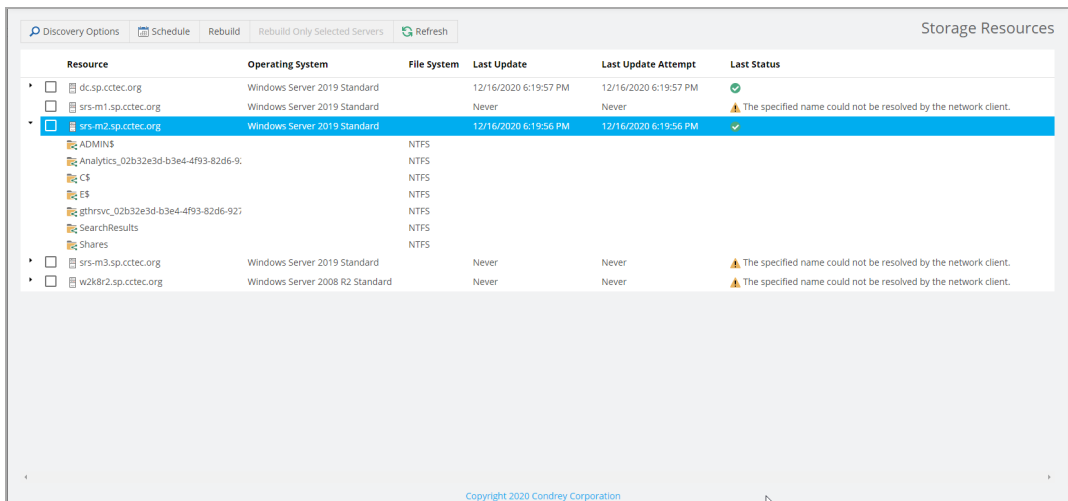
2. Click each button to view the options.
 - **Discovery Options:** Rebuilding storage resources can take many hours for large organizations with Active Directory forests spanning multiple locations. Instead of rebuilding everything, select this option to specify only the containers or servers to include for rebuilding.
 - 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 search are listed, click *OK*.

3 - Setup Procedures



- **Schedule:** File Reporter rebuilds Active Directory's storage resources each day at midnight by default. You can change this setting to weekly or monthly by clicking this option and modifying the settings in the dialog box.
- **Rebuild:** Click this button to rebuild Active Directory's storage resources automatically.
- **Rebuild Only Selected Servers:** Click this option to rebuild specific servers.
- **Refresh:** Reload and update the resource list.

3. Click the drop-down arrow (▾) for each server to browse its storage resources.

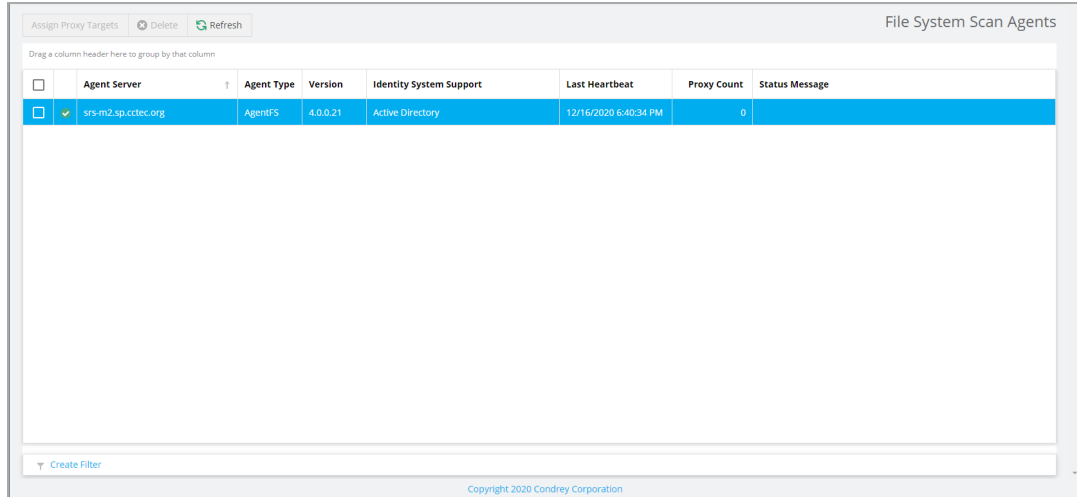


3.2 - Assigning Proxy Targets

An Agent cannot be deployed on a NAS device or storage cluster, and only one Agent type (AgentFS, AgentFC, or Agent365) can be hosted on a server.

If your organization does not want to deploy an Agent on every server, you can set a deployed Agent on another server to function as a proxy agent.

1. Select *Scan Agents* in the *File Systems* menu to open a list of all Agents.



The screenshot shows a web interface titled "File System Scan Agents". At the top, there are buttons for "Assign Proxy Targets", "Delete", and "Refresh". Below the buttons is a table with the following columns: "Agent Server", "Agent Type", "Version", "Identity System Support", "Last Heartbeat", "Proxy Count", and "Status Message". The first row of the table is highlighted in blue and contains the following data: "srs-m2.sp.cctec.org", "AgentFS", "4.0.0.21", "Active Directory", "12/16/2020 6:40:34 PM", "0", and an empty status message. Below the table is a "Create Filter" button and a copyright notice "Copyright 2020 Condrey Corporation".

<input type="checkbox"/>	Agent Server	Agent Type	Version	Identity System Support	Last Heartbeat	Proxy Count	Status Message
<input checked="" type="checkbox"/>	srs-m2.sp.cctec.org	AgentFS	4.0.0.21	Active Directory	12/16/2020 6:40:34 PM	0	

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

3 - Setup Procedures

Assign Proxy Targets for **srs-m1.sp.cctec.org**

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

OK Cancel

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

3.3 - Configuring Notifications

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

1. Select *Notifications* in the *Configuration* menu.

Notification Configuration

Notification Settings

Only notify me about events of at least this severity level: Success

Days to display notifications in the dashboard: 30

Enable Mail Notifications

Mail Settings

Mail Server: IP Address or Hostname

Port: 25

Connection Type: TLS

From Email Address: noreply@cctec.org

Use Authentication

Username: malluser

Password:

Minutes to buffer multiple notifications for a single email: 1

Save Changes

Copyright 2020 Condrey Corporation

- **Only notify me about events of at least this severity level:** Specify the severity level of events that are recorded and displayed on the Notifications page and through email notifications.
 - 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.
 - To avoid receiving emails for every successful event, modify this setting to a more restrictive level.
 - When severity level changes, previously-recorded notifications continue to be displayed on the Notifications page (e.g., if you change the setting from *Success* to *Warning*, then only warning and error events are recorded; the notification records for prior success and info events remain displayed, however, until you filter them out).
 - **Days to display notifications in the dashboard:** Indicates the number of days an event remains listed on the Notifications page.
 - **Enable Mail Notifications:** Click to activate the fields in the *Mail Settings* section of the window. Email notifications are sent to all members of the SrsAdmins group. File Reporter finds each member's email address from Active Directory.
 - **Mail Server:** Specify the IP address or hostname of the mail server to use for sending 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 email address to use in the *From* field of the email notifications when sent.
 - **Use Authentication:** Select if your mail server requires authentication.
 - **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, for example, then File Reporter consolidates all events that take place over a 5-minute period and emails you a single notification.
2. When your notification parameters are set, click *Save Changes*.

3.4 - Integrating with File Dynamics

If you deploy OpenText File Dynamics, you can use it to report on File Dynamics policies. You must first specify the server address and port number of the server hosting the File Dynamics Engine.

3 - Setup Procedures



IMPORTANT: File Reporter 24.3 integrates with File Dynamics 6.6 and above.

1. Select *File Management* in the *Configuration* menu.

Refresh File Management Integration

Engine Communication

Server Address

Port 3009

Save Changes

Copyright 2020 Condrey Corporation

2. Specify the IP address or DNS name of the server hosting the File Dynamics Engine.
3. Specify the port number the Engine uses (default: 3009).
4. Click *Save Changes*.

4 - File System Scans

The following procedures cover how to scan your Microsoft network file systems.

4.1 - Overview

Through AgentFS, File Reporter scans a file system's storage resource (e.g., a Microsoft network share) at a given moment.

File system scans index the data specific to a storage resource, in order to generate storage reports or analytics views. Scans include comprehensive information on:

- The file types stored by users.
- When the files were created.
- When the files were last modified
- The permission data on the folders in which these files reside.
- And much more.

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

File system scans can be performed at any time, but scheduling a time after normal business hours minimizes the effect on network performance.

Consider several factors when deciding how often to conduct a file system scan:

- Daily scanning provides the most up-to-date information, but scanning is not throttled and may 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 lightest total load on individual servers and the network, but the scans are not the most current.
- Another strategy is to scan frequently-changing shares more often, and scan static shares less often.
- The primary purpose of the reporting should be considered when deciding the frequency of scanning. Reporting on storage trending generally requires less frequent scans, but reporting intended to solve immediate problems (e.g., "Who filled up this volume?") requires more frequent scans.
- When information is needed immediately, you can trigger a scan manually.
- If you are unsure of the optimal scanning frequency, start with weekly scanning and then adjust the interval based on your particular needs.

4 - File System Scans

4.1.1 - Scan Retention

File Reporter only retains the most current file system scan and permissions scan of a storage resource by default. If you want to generate Historic Comparison reports to compare two scans of the same storage resource over two points in time, however, you must specify that scans be retained—either manually or automatically, depending on the retained scan type.

Manual Retention

You can set a file system or permissions scan to be retained indefinitely as a “Baseline scan” by specifying it manually on the Scan Data page —see [Establishing a Baseline Scan \(page 47\)](#) for details and procedures.

Automatic Retention

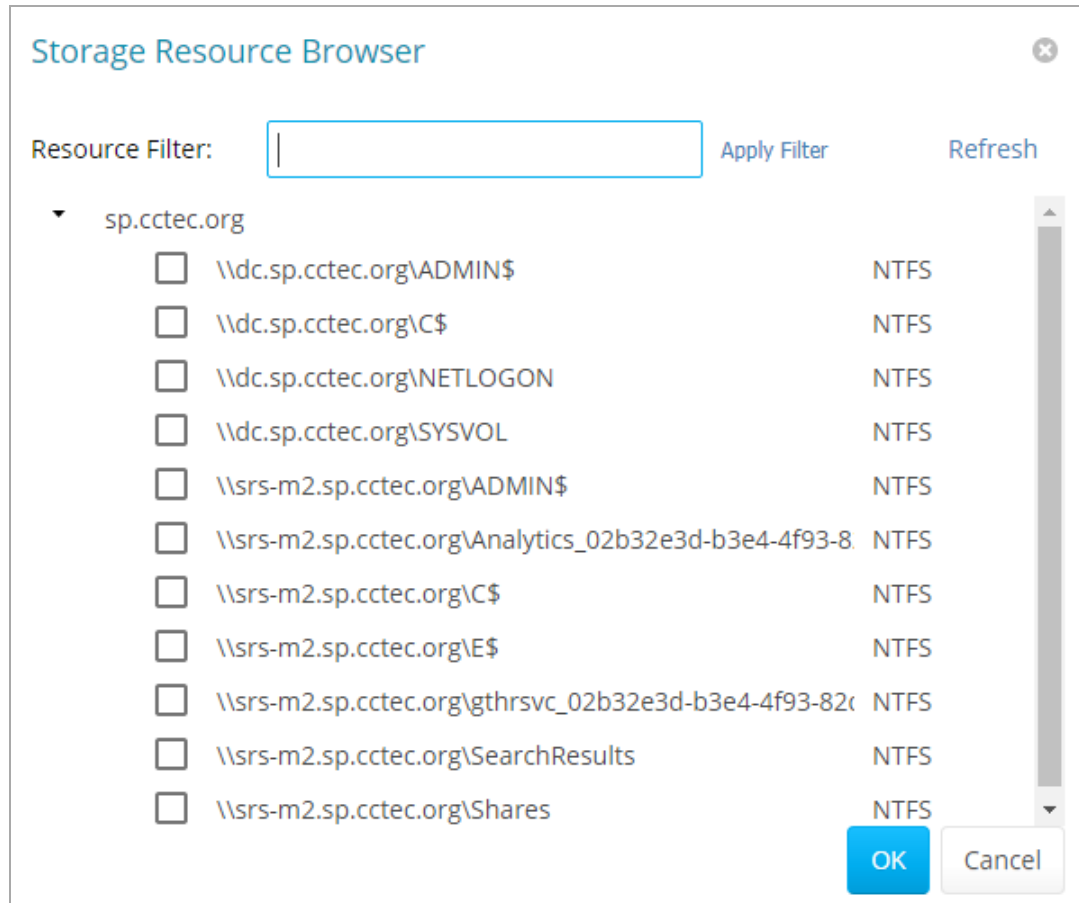
Within the scan policy, you can specify that the last file system scan or permissions scan be retained whenever you conduct a new file system scan or permissions scan. The retained version is known as a “Previous scan” —see [Creating a Scan Policy \(page 40\)](#) for details and procedures.

4.2 - Scan Targets

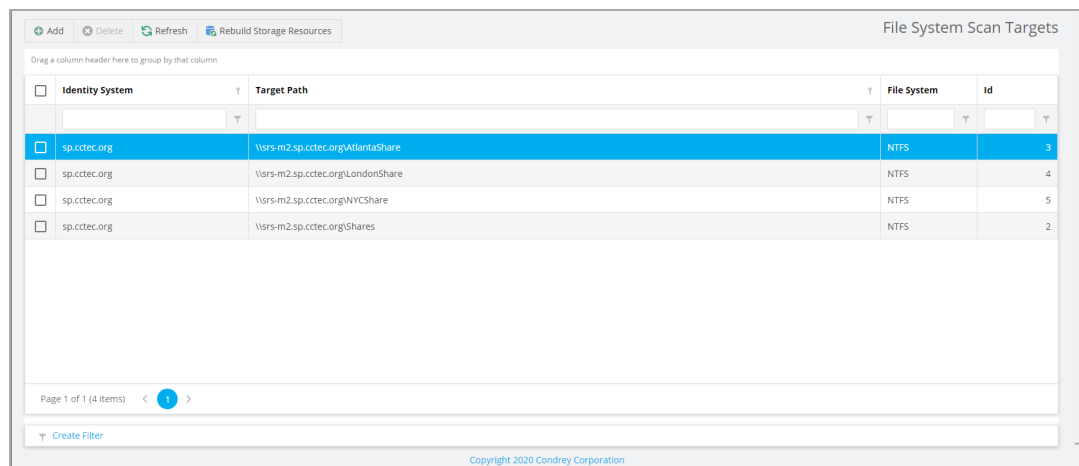
4.2.1 - Adding a Scan Target

A share must be specified as a scan target before it can be scanned.

1. Select *Scan Targets* in the *File Systems* menu.
2. Click *Add*.
3. Click the drop-down arrow (▶) to view the shares of the listed servers.



4. Select each share you want File Reporter to add as a scan target and click *OK*.



4 - File System Scans

4.2.2 - Removing a Scan Target

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

4.3 - Scan Policies

4.3.1 - Creating a Scan Policy

A scan policy establishes the following parameters:

- Type of scan (File System, Permissions, or Volume Free Space)
- Scan target(s)
- Scan retry settings
- Scan schedule



IMPORTANT: The scan policy requires a unique name. If you attempt to use an existing name, File Reporter generates an error.

1. Select *Scan Policies* in the *File Systems* menu.
2. Click *Add*.

The screenshot shows a dialog box titled "New Scan Policy". It has a close button in the top right corner. The "Policy Name" field is empty. The "Policy Type" section has three radio buttons: "File System", "Permissions", and "Volume Free Space". The "OK" button is highlighted in blue, and the "Cancel" button is greyed out.

3. Enter a name for the scan policy in the *Policy Name* field.

4. Select the type of scan to conduct in the *Policy Type* field.
 - **File System:** Scans the files stored currently on the network share to identify the size of the files, when they were last accessed, the locations of duplicate versions, etc.
 - **Permissions:** Scans the permissions of the folders stored on the shares.
 - **Volume Free Space:** Scans the availability of free space on the shares.
5. Click *OK* to open the Scan Policy Editor.

Scan Policy Editor ✕

Name:*

Description:

Retry Count: ⬆️ ⬇️ ⬆️

Retry Interval: ⬆️ ⬇️ ⬆️ ▾

Directory Quotas: Scan Directory Quotas

Previous Scans: Save Previous Scan

Content Hash: Generate file content hashes

All Files
 Files updated since last scan

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

	Target Path

6. **Name:** Displays the name of the scan policy you established.

7. **Description:** Enter a description of the scan policy.

- **Retry Count:** Specify the number of times File Reporter will attempt to scan the storage resource targets listed in the scan policy in response to a failure.
- **Retry Interval:** Specify the length of time that passes after a failure before File Reporter retries a scan of the storage resource targets listed in the scan policy.
- **Directory Quotas:** A scan does not include home folder quota information by default, because gathering this information on Windows shares can extend the scan time significantly. Leave this check box unselected unless you plan to generate a Directory Quota report. This option applies only to File System scans.
- **Previous Scans:** Check this box to keep the Previous scan generated through this policy whenever a new scan is performed.

When a new scan is complete, the results become the Current scan and the prior version becomes the Previous scan. If an earlier Previous scan exists, it is deleted. If you later uncheck the box in preparation for a new scan, the existing Previous scan will not be removed until a new scan is processed.

You can use the Previous scan to generate an *Historic Comparison* report with either a Baseline scan or a Current scan —see [Historic Comparison Reports \(page 107\)](#) for details.



NOTE: To maintain a scan indefinitely, specify it as a Baseline scan — see [Establishing a Baseline Scan \(page 47\)](#) for more information.

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

File Reporter has a Duplicate File report option as part of its Built-in Reports, but those reports are based solely on metadata comparisons. Generating a Duplicate File report through content comparisons is more accurate —see Content Hash Duplicate File Reports in the *File Reporter 24.3 Custom Query Guide* for details on generating duplicate file reports through content-based hashes.

- **All Files:** Check this box to create a new individual hash for each file in the specified target path.
- **Files updated since last scan:** Check this box to create an individual hash for each file that does not already have a previously-created hash, or for files that

were updated since the hash was created.



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

- **Add:** Click this option to specify storage resource scan targets for the scan policy in the dialog box that opens.



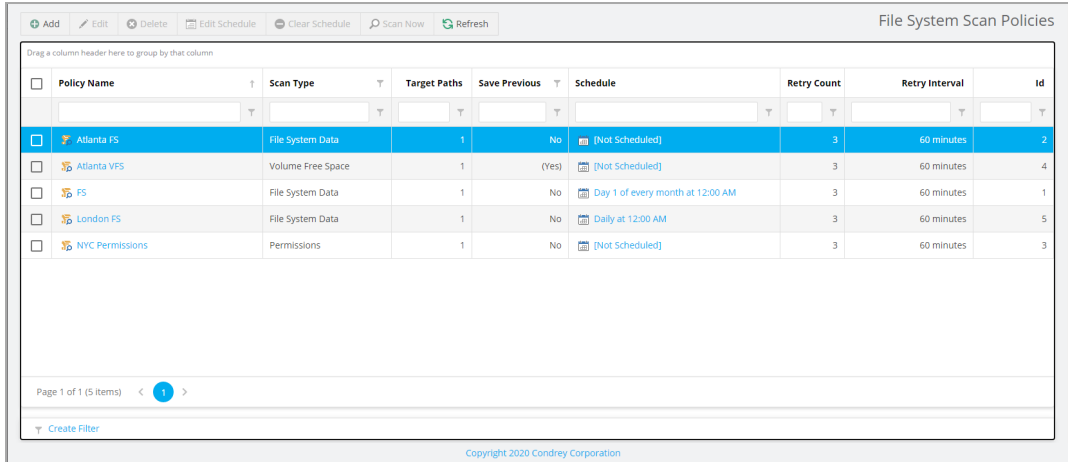
IMPORTANT: After adding a target to a scan policy, the same target cannot be added to another scan policy of the same type.

Scan Target Browser ✕

	Identity System	Target Path
	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	sp.cctec.org	\\srs-m2.sp.cctec.org\AtlantaShare
<input type="checkbox"/>	sp.cctec.org	\\srs-m2.sp.cctec.org\LondonShare
<input type="checkbox"/>	sp.cctec.org	\\srs-m2.sp.cctec.org\NYCShare
<input type="checkbox"/>	sp.cctec.org	\\srs-m2.sp.cctec.org\Shares

8. Click *OK* to save the scan policy, which is now displayed on the Scan Policies page.

4 - File System Scans



The screenshot shows the 'File System Scan Policies' interface. At the top, there are buttons for 'Add', 'Edit', 'Delete', 'Edit Schedule', 'Clear Schedule', 'Scan Now', and 'Refresh'. Below the buttons is a table with the following columns: Policy Name, Scan Type, Target Paths, Save Previous, Schedule, Retry Count, Retry Interval, and Id. The table contains five rows of scan policies. The first row, 'Atlanta FS', is highlighted in blue. Below the table is a pagination control showing 'Page 1 of 1 (5 items)' and a 'Create Filter' button. At the bottom of the interface, there is a copyright notice: 'Copyright 2020 Condrey Corporation'.

Policy Name	Scan Type	Target Paths	Save Previous	Schedule	Retry Count	Retry Interval	Id
<input checked="" type="checkbox"/> Atlanta FS	File System Data	1	No	(Not Scheduled)	3	60 minutes	2
<input type="checkbox"/> Atlanta VFS	Volume Free Space	1	(Yes)	(Not Scheduled)	3	60 minutes	4
<input type="checkbox"/> FS	File System Data	1	No	Day 1 of every month at 12:00 AM	3	60 minutes	1
<input type="checkbox"/> London FS	File System Data	1	No	Daily at 12:00 AM	3	60 minutes	5
<input type="checkbox"/> NYC Permissions	Permissions	1	No	(Not Scheduled)	3	60 minutes	3

The scan policy still needs to be scheduled —see [Scan Scheduling \(page 44\)](#) for details and procedures.

4.3.2 - Editing a Scan Policy

1. Select *Scan Policies* in the *File Systems* menu.
2. Check the box for the scan policy you want to edit.
3. Click *Edit*.
4. Change the desired settings.
5. Click *OK*.

4.3.3 - Deleting a Scan Policy

1. Select *Scan Policies* in the *File Systems* menu.
2. Check the box for the scan policy you want to delete.
3. Read the warning and click *Yes*.

4.4 - Scan Scheduling

4.4.1 - Setting a Scan Schedule

1. Select *Scan Policies* in the *File Systems* menu.
2. Check the box for the scan policy you want to schedule.
3. Click *Edit Schedule*.

Schedule for Atlanta Users FS ✕

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 you want the scan to begin.



NOTE: The time you select is based on the time zone in which the Engine is located, not the time zone of the Agent that conducts the scan.

- **Engine Local Start Date:** Specify the date on which you want the scan schedule to take effect.



NOTE: Entering a start date does not mean that the scan takes place on that date, it means the schedule *starts* on that date. Thus, if the Engine Local Start Date is set for a Monday but Schedule Recurrence is set for Weekly on Sunday, then the scan itself does not take place until the Sunday following the scheduled Engine Local Start Date.

- **Schedule Recurrence:** Set the frequency of scheduled scans.
 - **Once:** Select to scan the storage resources specified in the scan policy one time only.
 - **Daily:** Select to scan the storage resources specified in the scan policy at a designated time each day.
 - **Weekly:** Select a specific day on which to scan the storage resources specified in the scan policy each week.
 - **Monthly:** Select a specific day on which to scan the storage resources specified in the scan policy each month.

4. When finished specifying the scheduling parameters, click *OK*.

4.4.2 - Editing a Scan Schedule

1. Select *Scan Policies* in the *File Systems* menu.
2. Check the box for the scan policy you want to reschedule.
3. Click *Edit Schedule*.
4. Make the desired changes to the schedule.
5. Click *OK*.

4.4.3 - Clearing a Scan Schedule

1. Select *Scan Policies* in the *File Systems* menu.
2. Check the box for the scan policy you want to unschedule.
3. Click *Clear Schedule*.
4. When the confirmation prompt appears, click *Yes*.

4.4.4 - Conducting an Immediate Scan

1. Select *Scan Policies* in the *File Systems* menu.
2. Check the box for the scan policy you want to execute.
3. Click *Scan Now*.
4. When the confirmation prompt appears, click *Yes*.

4.5 - Baseline Scans

4.5.1 - Establishing a Baseline Scan

A Baseline scan is a scan you save as a reference to compare with another scan of the same Scan Target, such as when you generate an Historical Comparison report. Unlike a Previous scan, which is replaced when a new Current scan is created, a Baseline scan is retained indefinitely until you delete it. You can save 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 new Baseline overrides any established Baseline scan of the same scan type for the same scan target.

1. Select *Scan Data* in the *File Systems* menu.
2. Check the box of the scan you want to set as a Baseline scan.
3. Click *Set Baseline*.
4. When the confirmation dialog box appears, click *Yes*.

4.5.2 - Clearing a Baseline Scan

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

1. Select *Scan Data* in the *File Systems* menu.
2. Uncheck the box of the scan you want to clear as a Baseline scan.
3. Click *Clear Baseline*.
4. When the confirmation dialog box appears, click *Yes*.

4.6 - Scans in Progress

You can view the details of scans in progress.

1. Select *Scans in Progress* in the *File Systems* menu.

4 - File System Scans

File System Scans in Progress

Drag a column header here to group by that column

<input type="checkbox"/>	Scan ID	Scan Target	Scan Policy	Scan Type	Agent	Start Time	Status	Try Count	Next Retry Time	Last Error
<input type="checkbox"/>	9	\\srs-m2.sp.cctec.org\NYCShare	NYC Permissions	Permissions	SRS-M2	12/17/2020 9:04:06 PM	Scan In Progress	0		(0) Operation successful.
<input type="checkbox"/>	8	\\srs-m2.sp.cctec.org\LondonSF	London FS	File System Data	SRS-M2	12/17/2020 9:04:06 PM	Scan In Progress	0		(0) Operation successful.
<input type="checkbox"/>	7	\\srs-m2.sp.cctec.org\Shares	FS	File System Data	SRS-M2	12/17/2020 9:04:06 PM	Scan In Progress	0		(0) Operation successful.
<input type="checkbox"/>	6	\\srs-m2.sp.cctec.org\AtlantaSh	Atlanta VFS	Volume Free Space		12/17/2020 9:04:06 PM	Waiting for Retry	1	12/17/2020 10:04:00 PM	(-1) An unspecified error has occurred.
<input type="checkbox"/>	5	\\srs-m2.sp.cctec.org\AtlantaSh	Atlanta FS	File System Data	SRS-M2	12/17/2020 9:04:06 PM	Scan In Progress	0		(0) Operation successful.

Page 1 of 1 (5 items) < 1 >

Create Filter

Copyright 2020 Condrey Corporation

2. Click *Refresh* to remove completed scan listings, which are then listed in the Scan Data and Scan History pages.
3. You can view the details of completed scans on the Scan History page.

4.7 - Scan Data

4.7.1 - Viewing Scan Data

You can view a limited set of details for the currently-available scans for each scan target on the Scan Data page.

1. Select *Scan Data* in the *File Systems* menu.

File System Scan Data

Delete Set Baseline Clear Baseline Refresh

Drag a column header here to group by that column

<input type="checkbox"/>	Scan ID	Scan Target	Scan Type	State	Baseline	Triggered Scan Time	Policy	Agent	Status
<input type="checkbox"/>	10	\\srs-m2.sp.cctec.org\LondonShare	File System Data	Current	False	12/18/2020 2:13:21 PM	London FS	SRS-M2	(0) Operation successful.
<input type="checkbox"/>	7	\\srs-m2.sp.cctec.org\Shares	File System Data	Current	False	12/17/2020 9:04:06 PM	FS	SRS-M2	(0) Operation successful.
<input type="checkbox"/>	9	\\srs-m2.sp.cctec.org\NYCShare	Permissions	Current	False	12/17/2020 9:04:06 PM	NYC Permissions	SRS-M2	(0) Operation successful.
<input type="checkbox"/>	5	\\srs-m2.sp.cctec.org\AtlantaShare	File System Data	Current	False	12/17/2020 9:04:06 PM	Atlanta FS	SRS-M2	(0) Operation successful.
<input type="checkbox"/>	1	\\srs-m2.sp.cctec.org\Shares	File System Data	Retained	True	12/16/2020 3:26:12 PM	FS	SRS-M2	(0) Operation successful.

Page 1 of 1 (5 items) < 1 >

[State] is any of ('Current', 'Previous', 'Retained') Clear

Copyright 2020 Condrey Corporation

4.7.2 - Deleting Scan Data

To delete specific scan data:

1. Select *Scan Data* in the *File Systems* menu.
2. Check the boxes of the scans you want to delete.
3. Click Delete in the menu at the top of the page to open a confirmation dialog box.
4. (Optional) Check the box for *Delete Immediately* to perform the data cleanup right away, rather than wait for the next scheduled cleanup interval.



IMPORTANT: The Delete Scans operation marks selected scans for cleanup on the next maintenance interval by default. Scheduled cleanup is performed by the Engine, which is the recommended option. Deleting scans with the *Delete Immediately* option is performed by the Web Application directly and may result in timeout errors if the operation takes too long, especially with large scan sets.

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

4.8 - Scan History

You can view a complete history of all scans, along with details of the scan and basic information about the storage resource at the time of the scan, including file and folder count.

1. Select *Scan History* in the *File Systems* menu.

Scan Id	Start Time	Scan Target	Scan Policy	Scan Type	Agent	Scan Duration	Database Duration	File Count	Folder Count	Status
10	12/18/2020 2:13:21 PM	\\srs-m2.sp.cctec.org\LondonShare	London FS	File System Data	SRS-M2	00.00:00:00.000	00.00:00:00.140	0	1	(0) - Success
6	12/17/2020 9:04:06 PM	\\srs-m2.sp.cctec.org\AtlantaShare	Atlanta VFS	Volume Free Space	SRS-M2	00.00:00:01.517	00.00:00:00.033	0	0	(0) - Success
8	12/17/2020 9:04:06 PM	\\srs-m2.sp.cctec.org\LondonShare	London FS	File System Data	SRS-M2	00.00:00:00.000	00.00:00:00.106	0	1	(0) - Success
7	12/17/2020 9:04:06 PM	\\srs-m2.sp.cctec.org\Shares	FS	File System Data	SRS-M2	00.00:00:00.000	00.00:00:01.123	40	13	(0) - Success
9	12/17/2020 9:04:06 PM	\\srs-m2.sp.cctec.org\NYCShare	NYC Permissions	Permissions	SRS-M2	00.00:00:00.000	00.00:00:00.203	0	1	(0) - Success
5	12/17/2020 9:04:06 PM	\\srs-m2.sp.cctec.org\AtlantaShare	Atlanta FS	File System Data	SRS-M2	00.00:00:00.000	00.00:00:00.190	0	1	(0) - Success

Page 1 of 1 (10 items) < 1 >

Create Filter

Copyright 2020 Condrey Corporation

2. Click a column to list the data in ascending or descending order.

Because the Scan History page logs each successful scan, the most efficient way to locate a scan is to use a filter.

4.9 - Retrying Failed Scans

In the Scan Policy Editor dialog box, *Retry Count* is set to three and *Retry Interval* is set to 60 minutes by default, meaning File Reporter retries the scan every 60 minutes, but only up to three times. You can adjust each of these settings.

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

While a failed scan remains listed on the Scans in Progress page, you can retry the scan manually from this page:

1. Check the box of the failed scan you want to retry.
2. Click *Retry*.

4.10 - Troubleshooting

1. Verify that the Agent service is running properly on its host machine.
2. Verify that the host machine on which the Agent is installed has enough free disk space to store a temporary copy of the scan in both 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 is established.
4. If the proxy agent is not scanning, assign the storage resource from a different proxy agent and try scanning again.
5. Verify that the proxy rights group has been assigned to the `Builtin\Administrators` group on the server on which the scan is conducted.
6. Verify that the Windows Firewall is configured to permit network traffic to flow between the Engine and the Agent —see [Windows Firewall Settings \(page 119\)](#) for more information.

5 - Active Directory Identity Scans

File Reporter 24.3 performs an extended collection of identities (security principals) in your Active Directory forest. The data collected is available for Custom Query reports or direct review via the *Identities* page, or for use with other customer-defined processes that query the database directly.

5.1 - Overview

5.1.1 - Scope

Active Directory's Identity Scan feature scans for all identities across all domains in the associated Active Directory forest. An "identity" is classified as any object in Active Directory with a valid Security Identifier (objectSid) attribute.

5.1.2 - Collected Data

The collected data includes a pre-defined set of single-value attributes that enrich the basic identity metadata for users, groups, and other security principals found in Active Directory — see `ad.ds_objects` in the *File Reporter 24.3 Custom Query Guide* for a list of current attributes.



NOTE: Multi-value attributes are not supported currently, except for the *objectClass* attribute, for which only the primary structural class value is collected. Support for multi-value attributes such as group members, direct reports, and SID history is slated for a future release.

5.2 - Performing Scans

5.2.1 - Scheduling Identity Scans

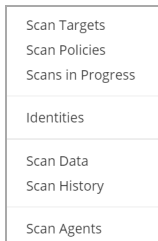
Active Directory Identity Scans run once per day at midnight. Support for custom schedules is slated for a future release.

5.2.2 - Performing an Immediate Scan

To perform an immediate scan of Active Directory identity objects in the File Reporter Web Application.

5 - Active Directory Identity Scans

1. Select *Identities* in the *File Systems* menu.

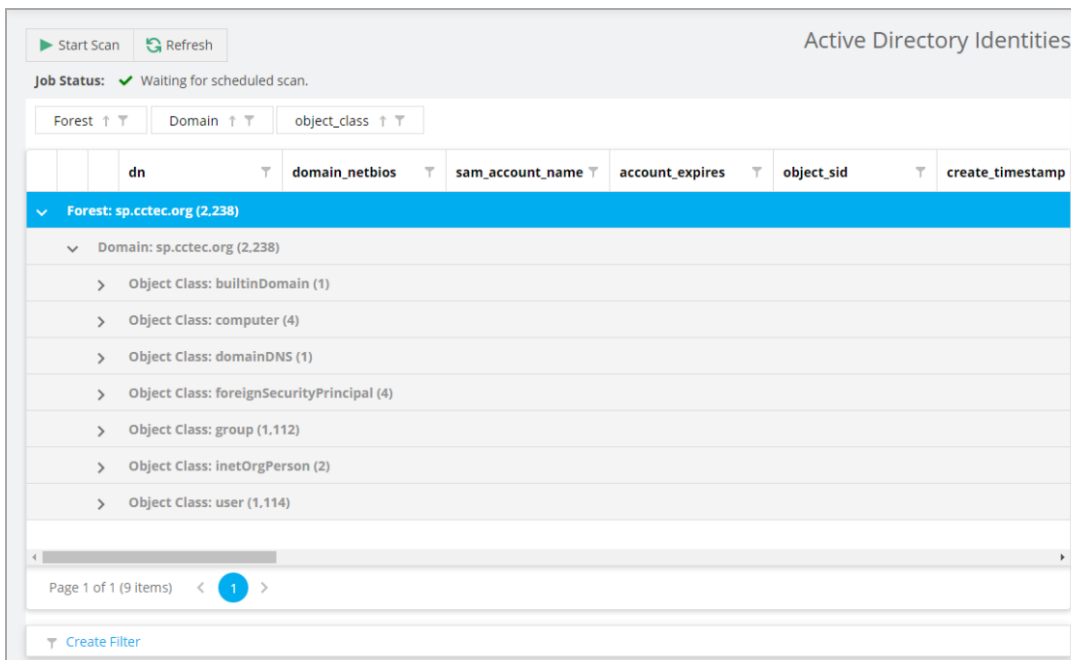


2. Click *Start Scan*.

5.3 - Viewing Collected Identities

In the File Reporter Web Application:

1. Select *Identities* in the *File Systems* menu.
2. Collected identities are grouped by domain and object type, by default.



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

5.4 - Extending Custom Query Reports

See Active Directory Identity Enrichment in the *File Reporter 24.3 Custom Query Guide* for an example of creating a Custom Query report with extended identity information.

6 - File Content Scanning

In addition to generating reports on the file system, permissions, and trends, File Reporter enables you to analyze your files based on content. Analyzing content allows you to locate files containing confidential, sensitive, and personal information that should be given restricted access, moved to a more secure location, or deleted.

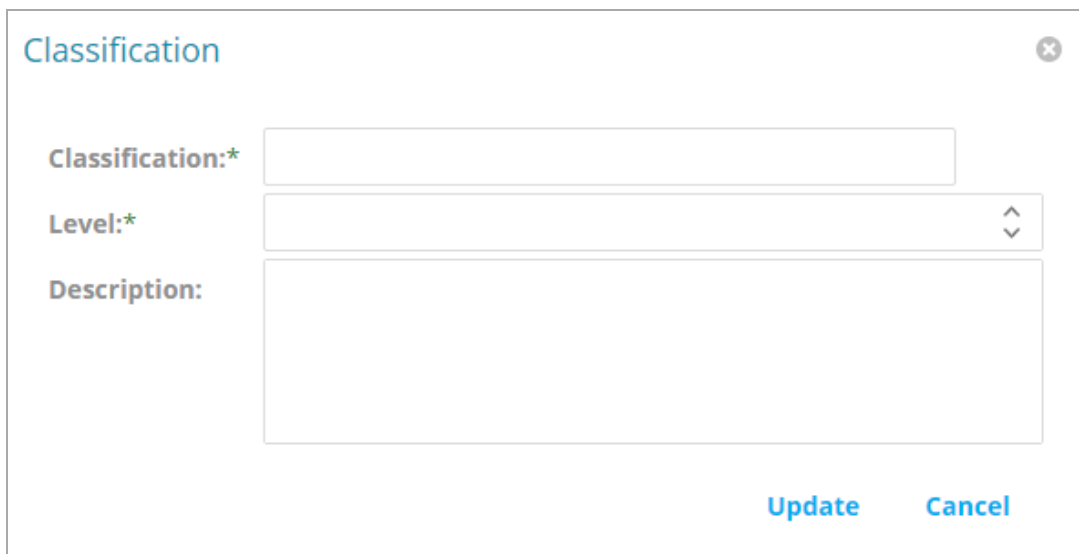
All File Content procedures are performed through the *File Content* menu options.

6.1 - File Content Classifications

File Reporter requires file content classifications as search parameters. File Reporter includes three classifications and severity levels which you can modify by editing the settings, or you can create your own classifications.

6.1.1 - Creating a New Classification

1. Select *Classifications* in the *File Content* menu.
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 double arrow icon), and "Description:" (a text area). At the bottom right of the dialog are two buttons: "Update" and "Cancel".

3. Enter a name in the *Classification* field (e.g., "Private").
4. Specify a severity level for the new classification in the *Level* field (e.g., "400").
5. Enter a description for the new classification in the *Description* field (e.g., "High-risk, private information not intended for public disclosure.")
6. Click *Update*.

6 - File Content Scanning

6.1.2 - Editing a Classification

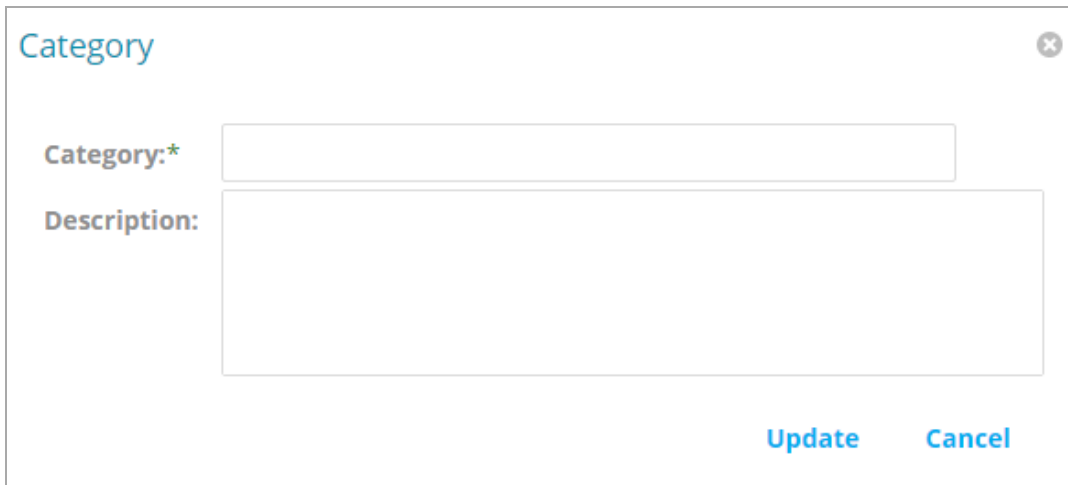
1. Select *Classifications* in the *File Content* menu.
2. Select the classification you want to edit.
3. Click *Edit*.
4. Edit the fields.
5. Click *Update*.

6.2 - File Content Categories

Categories provide an additional method of refining your search parameters. File Reporter includes three standard categories, but you can modify this list by creating your own classifications.

6.2.1 - Creating a New Category

1. Select *Categories* in the *File Content* menu.
2. Click *Add*.



The image shows a dialog box titled "Category" with a close button in the top right corner. Inside the dialog, there are two input fields. The first is labeled "Category:*" and the second is labeled "Description:". At the bottom right of the dialog, there are two buttons: "Update" and "Cancel".

3. Enter a name in the *Category* field (e.g., "National ID").
4. Enter a description for the new category in the *Description* field (e.g., "US Social Security Numbers").
5. Click *Update*.

6.2.2 - Editing a Category

1. Select *Categories* in the *File Content* menu.
2. Select the category you want to edit.

3. Click *Edit*.
4. Edit the fields.
5. Click *Update*.

6.3 - File Content Search Patterns

Search patterns specify the conditions for content scanning, and establish how to classify and categorize the results.

To conduct content scans, File Reporter uses regular expression (regex) search strings, which describe and define a search pattern. Regex search strings are ideal for locating files containing specified patterns (e.g., Social Security numbers, credit card numbers, etc.) or other user-defined patterns.

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

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



NOTE: This version of File Reporter makes use of the C# (.NET) regular expression variant for cases in which different regex engines or languages are mentioned.

6.3.1 - Creating a New Search Pattern

1. Select *Search Patterns* in the *File Content* menu.
2. Click *Add*.

6 - File Content Scanning

The image shows a 'Search Pattern' dialog box with the following fields and controls:

- Name:***: A text input field.
- Classification:***: A dropdown menu.
- Category:***: A dropdown menu.
- Match Confidence:***: A dropdown menu.
- Regex Options:**: A dropdown menu.
- Search String:***: A large text area for entering the search string.
- Description:**: A text input field.
- Update** and **Cancel**: Buttons at the bottom right.

3. Enter a descriptive name for the search pattern in the *Name* field (e.g., "Social Security US - High"). Names are restricted to the following characters: A-Z, a-z, 0-9, space, - (hyphen), and _ (underscore).
4. Select a *Classification* from the drop-down menu.
5. Select a *Category* from the drop-down menu.
6. Select *Match Confidence* from the drop-down menu to indicate your confidence in the search results: *Low*, *Medium*, or *High*, based on the accuracy of the search string (e.g., a search of all Social Security numbers might have Low confidence of a match, while a search for a particular Social Security number specified in the search string would have High match confidence).
7. Select any applicable options in the *Regex Options* drop-down menu. Refer to the following documentation for an explanation of these options:
<https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-options>.
8. Enter or paste the *Search String* in the text field.
9. Enter a *Description* of the search pattern in the text field.

Search Pattern ✕

Name:*

Classification:*

Category:*

Match Confidence:*

Regex Options:

Search String:*

Description:

[Update](#) [Cancel](#)

10. Click *Update*.

6.3.2 - Editing a Search Pattern

1. Select *Search Patterns* in the *File Content* menu.
2. Select the search pattern you want to edit.
3. Click *Edit*.
4. Edit the fields.
5. Click *Update*.

6.4 - File Content Jobs

A job definition specifies:

- The file system paths where the content scan will take place;
- The search patterns that will be applied;
- The filters for the search; and
- The location where the content scan results will be stored.

6.4.1 - Creating a New Job Definition

1. Select *Job Definitions* in the *File Content* menu.
2. Click *Add*.

6 - File Content Scanning

Job Definition

Name:* Result Type:*

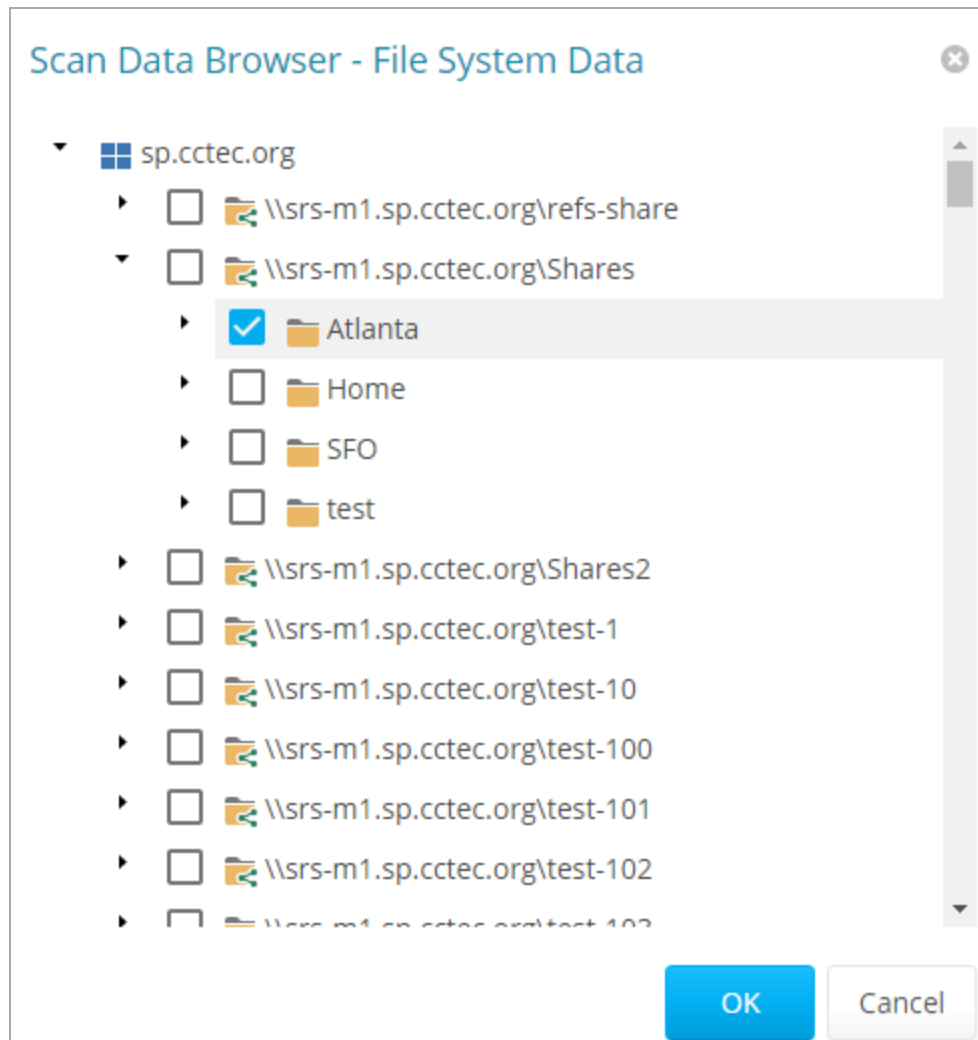
TARGET PATHS **SEARCH PATTERNS** **FILTERS**

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

	Target
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares

[Update](#) [Cancel](#)

3. Enter a descriptive *Name* for the job definition in the text field.
4. Select one of the following options in the *Result Type* menu:
 - **Database:** Save the results of the content scan to the database, where you can use the Report Designer to generate a report. Having the scan in the database also enables you to search and report using the established classifications and categories.
 - **File:** Save 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. Click *Add* in the *Target Paths* tab.



6. Select the target path(s) containing the file content you want to scan.



IMPORTANT: A file path only appears in the Scan Data Browser - File System Data dialog after undergoing a file system scan. If the path you want does not appear in the dialog, you must first conduct a file system scan on it.

7. Click *OK*.
8. Click the *Search Patterns* tab.
9. Click *Add*.

6 - File Content Scanning

<input type="checkbox"/>	Name ↑ ▾	Category ▾	Classification ▾
	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Amanda Cox	General	Sensitive
<input type="checkbox"/>	Social Security US	PII	Sensitive

10. Specify your search patterns in the Search Pattern Browser and click *OK*.
11. Click the *Filters* tab.
12. Specify the *Maximum File Size* to exclude from the content scan (e.g., for large files such as ISO files). If you do not specify a setting, then all files in the file path will be scanned.
13. Specify the file types you want scanned in the *File Extensions* field. If you do not specify any file extensions, then all file types 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:

```
txt
pdf
doc
xlsx
```

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

[Update](#) [Cancel](#)

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

6.4.2 - Editing a Job Definition

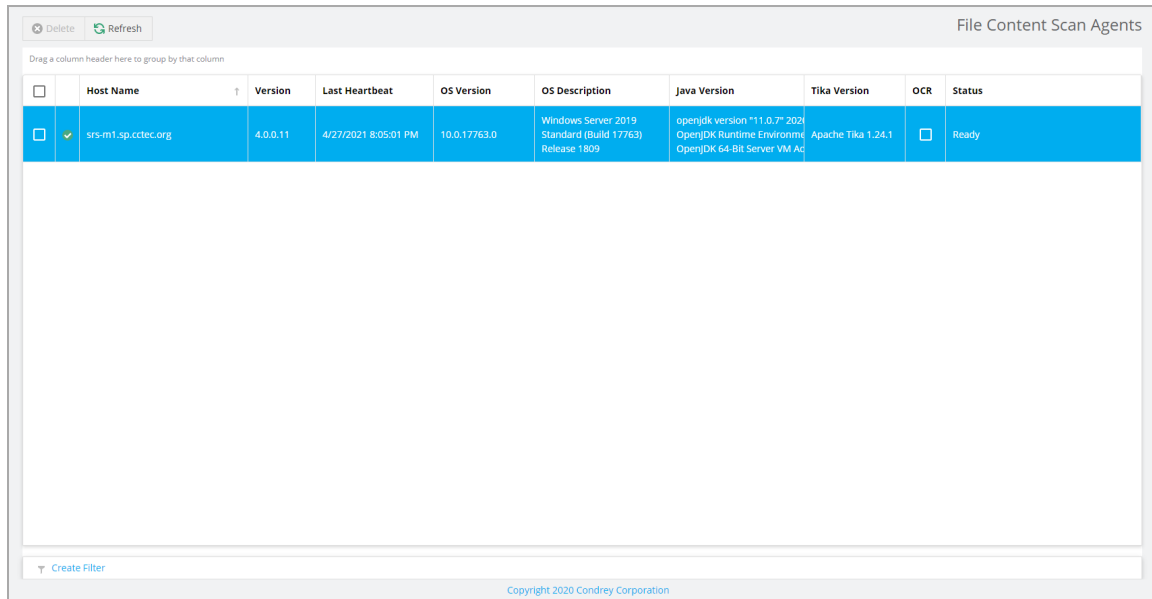
1. Select *Job Definitions* in the *File Content* menu.
2. Select the job definition you want to edit.
3. Click *Edit*.
4. Edit the fields.
5. Click *Update*.

6.5 - Managing File Content Scans

6.5.1 - Verify AgentFC Registrations

1. Select *Agents* in the *File Content* menu to view the version, last heartbeat, and other details for each deployed AgentFC.

6 - File Content Scanning



The screenshot shows a web interface titled "File Content Scan Agents". At the top left, there are "Delete" and "Refresh" buttons. Below the title bar, there is a text prompt: "Drag a column header here to group by that column". The main area contains a table with the following columns: Host Name, Version, Last Heartbeat, OS Version, OS Description, Java Version, Tika Version, OCR, and Status. A single row is visible, representing an agent with the following details:

	Host Name	Version	Last Heartbeat	OS Version	OS Description	Java Version	Tika Version	OCR	Status
<input checked="" type="checkbox"/>	srs-m1.sp.cctec.org	4.0.0.11	4/27/2021 8:05:01 PM	10.0.17763.0	Windows Server 2019 Standard (Build 17763) Release 1809	openjdk version "11.0.7" 2020-09-14 OpenJDK Runtime Environment OpenJDK 64-Bit Server VM Ad	Apache Tika 1.24.1	<input type="checkbox"/>	Ready

At the bottom left of the table area, there is a "Create Filter" button. At the bottom center, there is a copyright notice: "Copyright 2020 Condrey Corporation".

This window enables you to verify the consistency of AgentFC deployments and configuration parameters.

6.5.2 - Start a File Content Scan Job

To start a File Content scan job:

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

6.5.3 - Viewing Jobs in Progress

1. Select *Jobs in Progress* in the *File Content* menu to view the status of the file content scanning process.

File Content Jobs in Progress

Cancel Refresh

Drag a column header here to group by that column

Job ID	Job Definition	Files Submitted	Files Processed	Status Code	Status Message
2	amanda cox	5,926	14 (0%)	Processing	Processing

Page 1 of 1 (1 Items)

Copyright 2020 Condrey Corporation

6.5.4 - Viewing Scanned Data Matches

1. Select *Scan Data* in the *File Content* menu to view the set of matched results data.

File Content Scan Data

Refresh

Job

Full Path	Scan Time	Classification	Category	Matched Search Pattern	Confidence
Job: amanda cox - 2 (4 entries - Processing)					
\\srs-m1.sp.cctec.org\Shares\FQ\Employee\acox\finding names.txt	4/27/2021 8:04:38 PM	Sensitive	General	Amanda Cox (2 matches)	Low
\\srs-m1.sp.cctec.org\Shares\Atlanta\Employee\anance\New Text Document.txt	4/27/2021 8:04:37 PM	Sensitive	General	Amanda Cox (2 matches)	Low
\\srs-m1.sp.cctec.org\Shares\Atlanta\Employee\acox\New Text Document.txt	4/27/2021 8:04:15 PM	Sensitive	General	Amanda Cox (2 matches)	Low
\\srs-m1.sp.cctec.org\Shares\Atlanta\Employee\acox\finding names.txt	4/27/2021 8:03:52 PM	Sensitive	General	Amanda Cox (2 matches)	Low
Job: amanda cox - 1 (11 entries - Completed)					
\\srs-m1.sp.cctec.org\Shares\test\Microsoft Visual Studio 14.0\Common7\IDE\ItemTemplates\VisualBasic\Windows Forms\1033>LoginForm\LoginForm.resx	11/10/2020 7:58:53 PM	Sensitive	General	Amanda Cox (5 matches)	Low
\\srs-m1.sp.cctec.org\Shares\test\Microsoft Visual Studio 14.0\Common7\IDE\ItemTemplates\VisualBasic\Windows Forms\1033\Explorer\explorer.resx	11/10/2020 7:58:53 PM	Sensitive	General	Amanda Cox (2 matches)	Low
\\srs-m1.sp.cctec.org\Shares\test\Microsoft SQL Server Management Studio 18\Common7\IDE\Extensions\Platform\Debugger\WebViews\BptDiagnosticComm\4.0.0.0.debug.js	11/10/2020 7:58:23 PM	Sensitive	General	Amanda Cox (1 match)	Low
\\srs-m1.sp.cctec.org\Shares\test\Microsoft SQL Server Management Studio 18\Common7\IDE\Mashup\ODBC Drivers\Simba Spark ODBC Driver\cacerts.pem	11/10/2020 7:55:31 PM	Sensitive	General	Amanda Cox (4 matches)	Low
\\srs-m1.sp.cctec.org\Shares\test\Microsoft SQL Server Management Studio 18\Common7\ServiceHub\Services\Typescript\Linting\Service\typescript\linting.all.js	11/10/2020 7:49:56 PM	Sensitive	General	Amanda Cox (1 match)	Low
\\srs-m1.sp.cctec.org\Shares\test\Microsoft Visual Studio 14.0\Common7\IDE\1033\UpgradeReportL.xslit	11/10/2020 7:47:09 PM	Sensitive	General	Amanda Cox (1 match)	Low
\\srs-m1.sp.cctec.org\Shares\test\Microsoft SQL Server Management Studio					

Page 1 of 1 (17 Items)

Copyright 2020 Condrey Corporation

6.5.5 - Download Search Results

You can download the file content scan file for job definitions with *Result Type* set to *File* from the Search Results page.

File Reporter outputs the file as a CSV file, which you can import into the OpenText File Dynamics Data Owner Client for remediation.

6 - File Content Scanning

File Content Search Results

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"/>	amanda.cox-1.csv	Completed	3 KB	11/10/2020 7:58:53 PM

Page 1 of 1 (1 Items) < 1 >

Copyright 2020 Condrey Corporation

7 - Microsoft 365 Scans

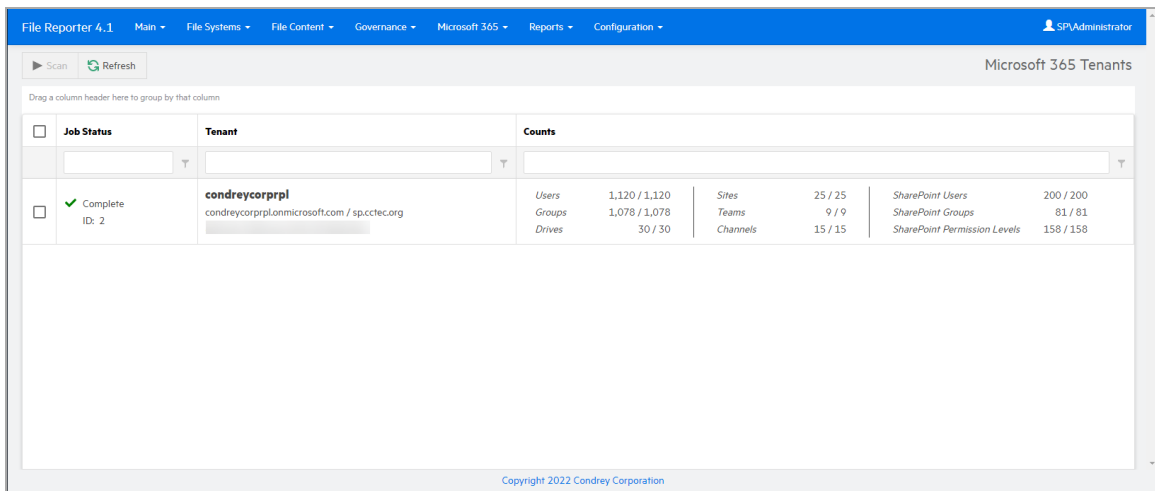
Scanning your Microsoft 365 tenant identifies all users and groups from Azure AD and SharePoint Site Collections, including associated drives, SharePoint sites, Teams and Team Channels, and document libraries.

Each drive and document library scan includes details of the file system structure, individual files, and file and folder permissions.

7.1 - Tenants

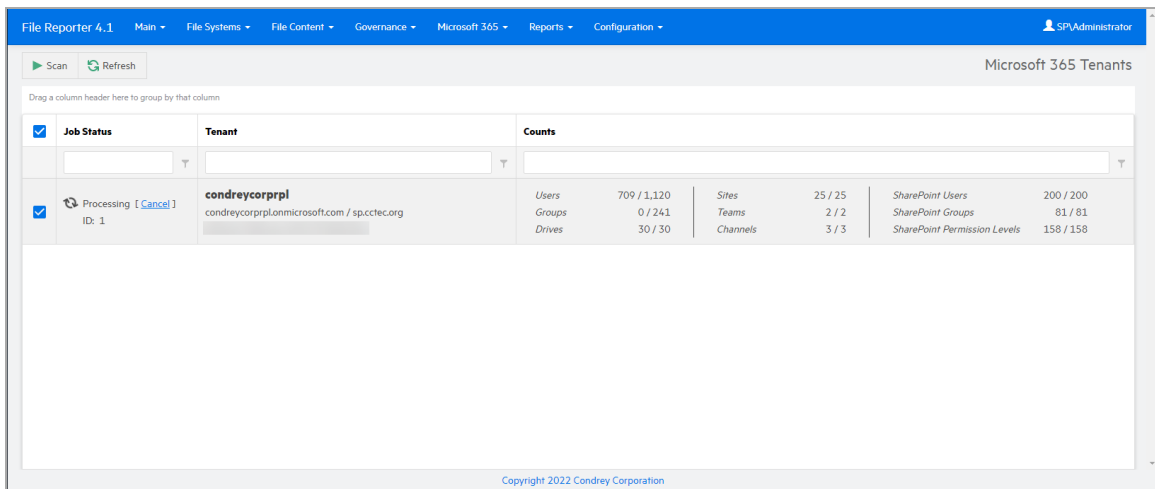
To scan the Microsoft 365 Tenant:

1. Select *Tenant* in the *Microsoft 365* menu.



Job Status	Tenant	Counts																		
<input checked="" type="checkbox"/> Complete ID: 2	condreycorprpl condreycorprpl.onmicrosoft.com / sp.cctec.org	<table border="1"> <tr> <td>Users</td> <td>1,120 / 1,120</td> <td>Sites</td> <td>25 / 25</td> <td>SharePoint Users</td> <td>200 / 200</td> </tr> <tr> <td>Groups</td> <td>1,078 / 1,078</td> <td>Teams</td> <td>9 / 9</td> <td>SharePoint Groups</td> <td>81 / 81</td> </tr> <tr> <td>Drives</td> <td>30 / 30</td> <td>Channels</td> <td>15 / 15</td> <td>SharePoint Permission Levels</td> <td>158 / 158</td> </tr> </table>	Users	1,120 / 1,120	Sites	25 / 25	SharePoint Users	200 / 200	Groups	1,078 / 1,078	Teams	9 / 9	SharePoint Groups	81 / 81	Drives	30 / 30	Channels	15 / 15	SharePoint Permission Levels	158 / 158
Users	1,120 / 1,120	Sites	25 / 25	SharePoint Users	200 / 200															
Groups	1,078 / 1,078	Teams	9 / 9	SharePoint Groups	81 / 81															
Drives	30 / 30	Channels	15 / 15	SharePoint Permission Levels	158 / 158															

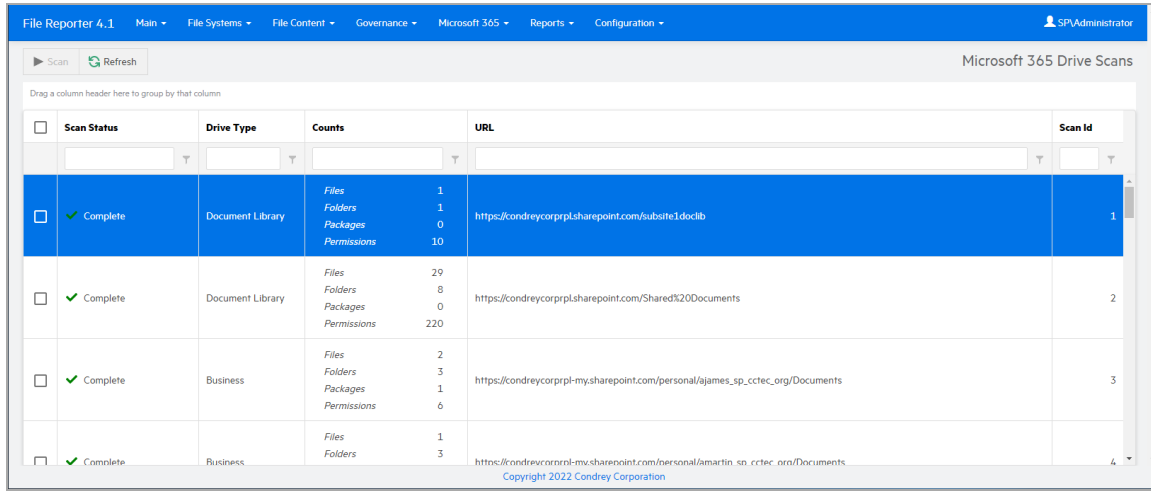
2. Check the box associated with the listed tenant, then click *Scan*. The progress of the scan is displayed in the *Counts* column.



Job Status	Tenant	Counts																		
<input checked="" type="checkbox"/> Processing [Cancel] ID: 1	condreycorprpl condreycorprpl.onmicrosoft.com / sp.cctec.org	<table border="1"> <tr> <td>Users</td> <td>709 / 1,120</td> <td>Sites</td> <td>25 / 25</td> <td>SharePoint Users</td> <td>200 / 200</td> </tr> <tr> <td>Groups</td> <td>0 / 241</td> <td>Teams</td> <td>2 / 2</td> <td>SharePoint Groups</td> <td>81 / 81</td> </tr> <tr> <td>Drives</td> <td>30 / 30</td> <td>Channels</td> <td>3 / 3</td> <td>SharePoint Permission Levels</td> <td>158 / 158</td> </tr> </table>	Users	709 / 1,120	Sites	25 / 25	SharePoint Users	200 / 200	Groups	0 / 241	Teams	2 / 2	SharePoint Groups	81 / 81	Drives	30 / 30	Channels	3 / 3	SharePoint Permission Levels	158 / 158
Users	709 / 1,120	Sites	25 / 25	SharePoint Users	200 / 200															
Groups	0 / 241	Teams	2 / 2	SharePoint Groups	81 / 81															
Drives	30 / 30	Channels	3 / 3	SharePoint Permission Levels	158 / 158															

7 - Microsoft 365 Scans

3. Select *Drives* in the *Microsoft 365* menu to monitor the progress of the scan in the various drives.



Scan Status	Drive Type	Counts	URL	Scan Id
<input checked="" type="checkbox"/> Complete	Document Library	Files: 1 Folders: 1 Packages: 0 Permissions: 10	https://condreycorprpl.sharepoint.com/subsite1doclib	1
<input checked="" type="checkbox"/> Complete	Document Library	Files: 29 Folders: 8 Packages: 0 Permissions: 220	https://condreycorprpl.sharepoint.com/Shared%20Documents	2
<input checked="" type="checkbox"/> Complete	Business	Files: 2 Folders: 3 Packages: 1 Permissions: 6	https://condreycorprpl-my.sharepoint.com/personal/ajames_sp_cctec_org/Documents	3
<input checked="" type="checkbox"/> Complete	Business	Files: 1 Folders: 3	https://condreycorprpl-my.sharepoint.com/personal/amartin_sn_cctec_org/Documents	4

Copyright 2022 Condrey Corporation

When the Job Status column indicates the scan is complete, you can generate a Microsoft 365 report —see *Microsoft 365 Reports* in the *File Reporter 2024.1 Custom Query Guide* for details.

7.2 - Drives and Document Libraries

For instances in which changes are made to a select number of libraries after the initial tenant scan, you can select the specific drives to scan rather than rescanning the entire tenant.



NOTE: Significant changes—such as the addition of a new team and consequently the creation of a new drive—require a tenant scan for the drive to be scanned.

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

8 - Reporting

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

8.1 - Built-in Reports

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

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



NOTE: See [Built-in Reports \(page 79\)](#) for more details.

8.2 - Custom Query Reports

For cases in which customized file system reporting is required, or for repository types without available Built-in Reports—such as Microsoft 365—Custom Query reporting provides an advanced interface for querying collected scan data and laying out report data results.

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



NOTE: See [Custom Query Reports \(page 115\)](#) for more details.

8.3 - Report Definitions

8.3.1 - Creating a Report Definition

To create a report definition:

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add* in the toolbar.

8 - Reporting

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

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

Permissions

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

Historic Comparison

- File System Comparison
- NTFS Permissions Comparison

Trending

- Volume Free Space

Custom Query

- Custom Query Report

OK Cancel

3. Enter a *Name* for the report in the text field.
4. (Optional) Select *Unformatted* to create a report that is delimited text only, with no report layout assigned.
5. Click a radio button to select a report type.



NOTE: If you're familiar with writing SQL queries, a Custom Query report definition may provide better control and performance than a comparable unformatted report definition.

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

Depending on the report definition type, set any remaining report definition parameters, or for Custom Query reports, write the necessary SQL query and report definition layout —See [Built-in Reports \(page 79\)](#) and [Custom Query Reports \(page 115\)](#) for details.

8.3.2 - Deleting a Report Definition

To delete a report definition:

1. Select *Report Definitions* in the *Reports* menu.
2. Select a report definition you want to delete from the list.
3. Click *Delete* in the toolbar.
4. Click *Yes* in the confirmation dialog to confirm deletion of the report definition.



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

8.3.3 - Copying a Report Definition

You can copy an existing report definition to save time in creating a new report definition and its associated properties. When you copy a Built-in Report, the following properties are included:

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

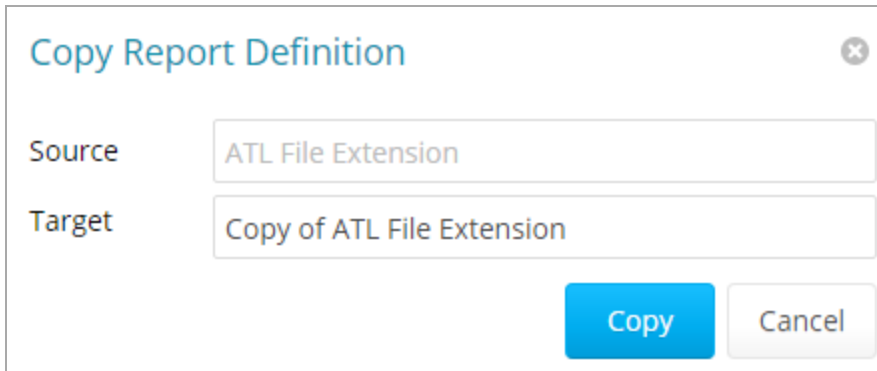
When you copy a Custom Query report, the following properties are included:

- SQL Query
- Report Layout



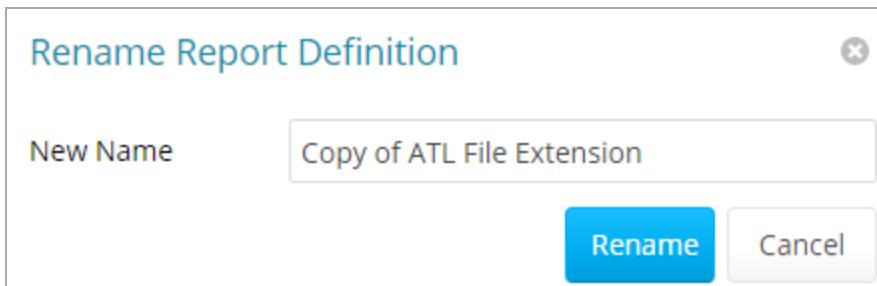
NOTE: Copying a report definition does not copy the content in the Description field or the report schedule.

1. Select *Report Definitions* in the *Reports* menu.
2. Select a report definition you want to copy from the list.
3. Click *Copy* in the toolbar.



The dialog box is titled "Copy Report Definition" and has a close button in the top right corner. It contains two text input fields: "Source" with the value "ATL File Extension" and "Target" with the value "Copy of ATL File Extension". At the bottom right, there are two buttons: a blue "Copy" button and a grey "Cancel" button.

4. Click *Copy* to add the new report definition to the list, under *Copy of* preceding the name of the original report definition.
5. Select the copy of the report definition.
6. Select *Rename* in the toolbar.



The dialog box is titled "Rename Report Definition" and has a close button in the top right corner. It contains one text input field labeled "New Name" with the value "Copy of ATL File Extension". At the bottom right, there are two buttons: a blue "Rename" button and a grey "Cancel" button.

7. Enter a *New Name* for the new report definition in the text field, then click *Rename*.
8. Select *Edit Schedule* in the *Schedule* menu.
9. Set the scheduling parameters for the new report definition, then click *OK*.
10. Click *Edit* in the toolbar.
11. Enter a new *Description* in the text field.
12. Click *Save*.

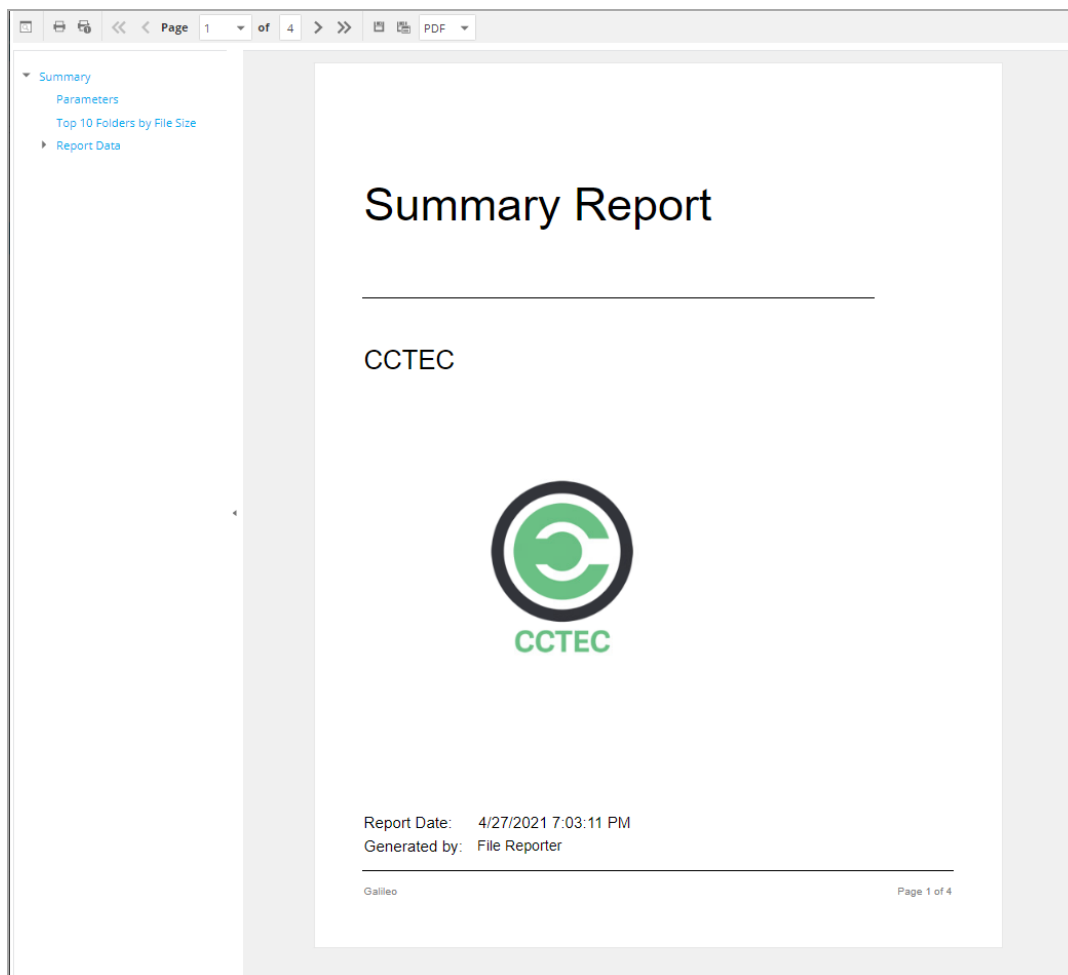
8.4 - Preview Reports

A Preview report is generated from scan data in the database, and temporarily cached in the Web Application's data folder. When you close a Preview report, you can't 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. Select the report definition you want in the Report Definitions window.
2. Select *Generate Preview* in the *Generate* menu.

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



All reports have a similar structure: a title page, the report parameters, and a Top Ten summary for some report types, followed by a comprehensive breakdown of the data.

- **Display the Search Window:** Click to conduct a search within the Preview Report.
- **Print the Report:** Click to print the entire Preview report.
- **Print the Current Page:** Click to print the currently-displayed page.
- **First Page:** Click to go to the first page of the Preview report.
- **Previous Page:** Click to go to the page preceding the current page.
- **Page:** Go to the page number you select in the drop-down menu.

8 - Reporting

- **Next Page:** Click to go to the page following the current page.
- **Last Page:** Click to go to the last page of the Preview report.
- **Export a Report and Save It to the Disk:** Click to export the Preview report as the file type listed in the drop-down menu, and then view or save it in the new format.
- **Export a Report and Show It in a New Window:** Click to export the Preview report as the file type listed in the drop-down menu.
- **File Type:** Select the file type format for exporting the report in the drop-down menu.
- **Document Navigation:** Click an item in the list of report contents to go to that section of the Preview report.

4. Export, save, or print the Preview report.

8.5 - Stored Reports

8.5.1 - Generating Stored Reports

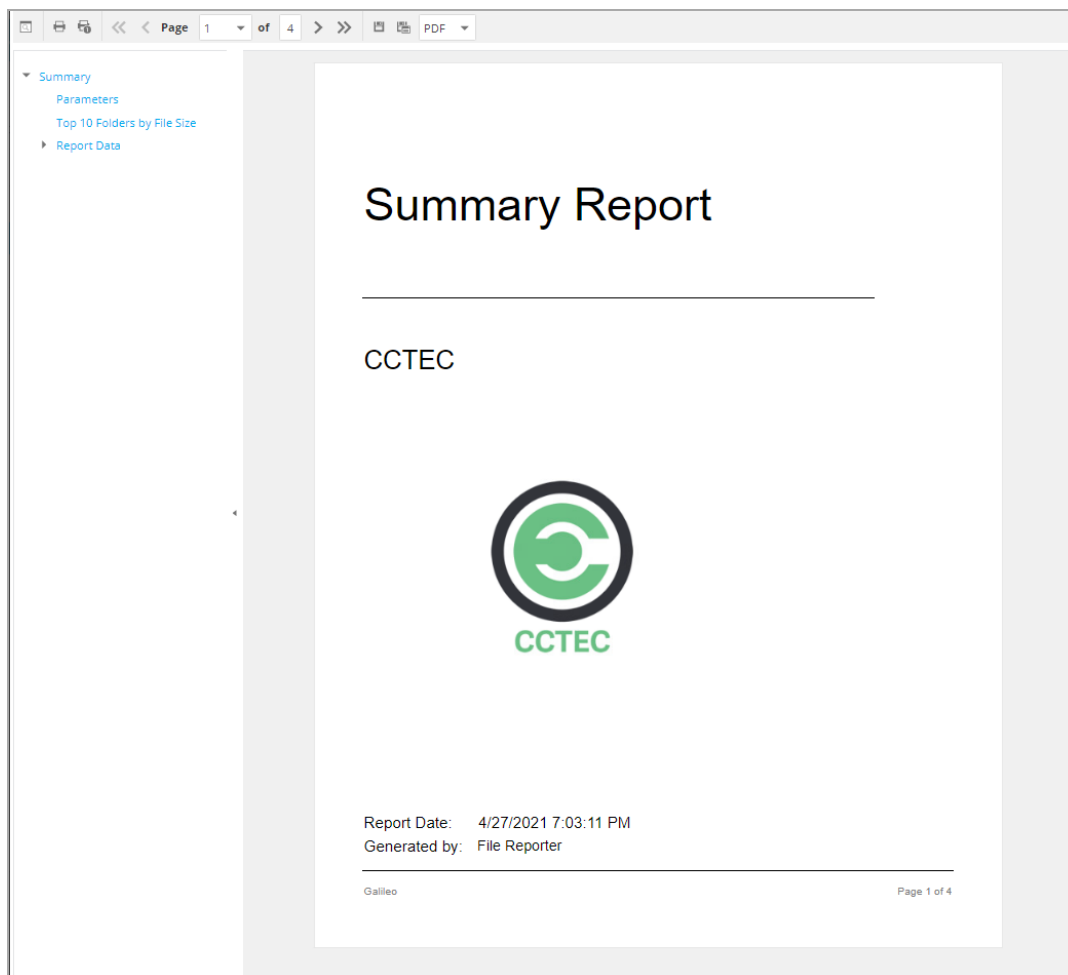
A Stored report is saved and accessible for a set number of days after it is generated. You can save the report locally to keep it indefinitely.

1. Select *Generate Stored Report* in the *Generate* menu of the Report Definitions window.
2. Select *Stored Reports* in the *Reports* menu.

	Name	Size	Report Type	Report Time	Expiration Date	Id
<input type="checkbox"/>	ATL Summary	35.61 KB	Summary	4/27/2021 7:06:07 PM	5/27/2021 12:00:00 AM	3
<input type="checkbox"/>	Owner	35.98 KB	Owner	4/27/2021 6:36:02 PM	5/27/2021 12:00:00 AM	2
<input type="checkbox"/>	refs summary	11.92 KB	Summary	10/22/2020 12:28:30 PM	11/21/2020 12:00:00 AM	1

3. Click the report you want to view.

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



All reports have a similar structure: a title page, the report parameters, a Top Ten summary for some report types, followed by a comprehensive breakdown of the data.

- **Display the Search Window:** Click to conduct a search within the Preview report.
- **Print the Report:** Click to print the entire Preview report.
- **Print the Current Page:** Click to print the currently-displayed page.
- **First Page:** Click to go to the first page of the Preview report.
- **Previous Page:** Click to go to the page preceding the current page.
- **Page:** Go to the page number you select in the drop-down menu.
- **Next Page:** Click to go to the page following the current page.

8 - Reporting

- **Last Page:** Click to go to the last page of the Preview report.
- **Export a Report and Save It to the Disk:** Click to export the Preview report as the file type listed in the drop-down menu, and then view or save it in the new format.
- **Export a Report and Show It in a New Window:** Click to export the Preview report as the file type listed in the drop-down menu.
- **File Type:** Select the file type format for exporting the report in the drop-down menu.
- **Document Navigation:** Click an item in the list of report contents to go to that section of the Preview report.

5. Save or print the Stored report.

8.5.2 - Stored Reports Path

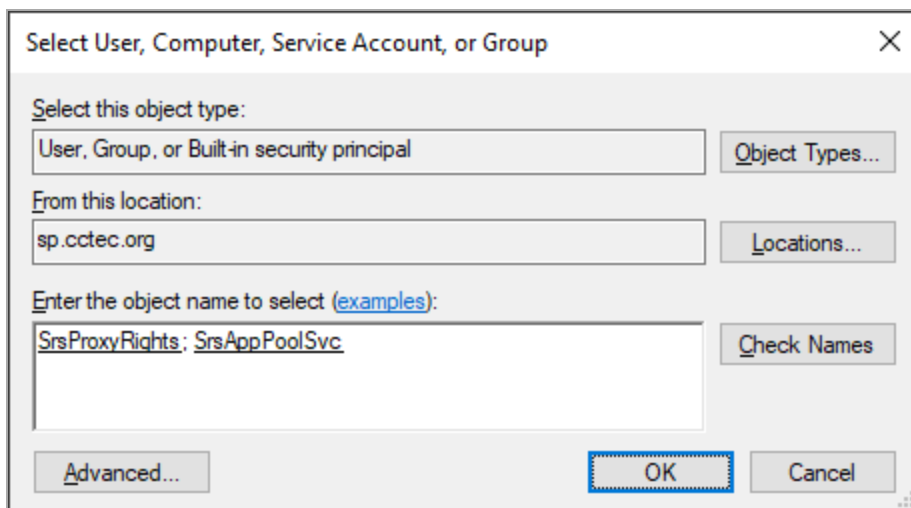
The default path for Stored reports is established during the installation of the Engine. You can change the file path so long as the new path is on the same server hosting both the Engine and Web Application.

The Web Application and the Engine need access to the report files, so the service accounts for which they run processes must have both Read and Write access to the specified path.

For the Engine, this service account is the Windows Proxy Account. For the Web Application, the service account is the associated IIS AppPool Identity, which is created by Windows and tied to the Application Pool when the Web service is configured.

If you create a new folder for Stored Reports, you must assign Read and Write access to that folder for the associated Windows server/proxy account and the AppPool Identity.

You can't browse for the AppPool Identity, so you must use the name of the AppPool itself:



1. Select *Stored Reports* in the *Configuration* menu.
2. Specify a new path in the *Stored Reports Folder* field.
3. Click *Save Changes*.



IMPORTANT: File Reporter does not move previously-generated reports to the new location when reconfiguring the Stored reports path—you must move these yourself.

8.5.3 - Stored Reports Lifespan

Stored reports are available for access for 30 days by default. You can adjust this setting if desired:

1. Select *Stored Reports* in the *Configuration* menu.
2. Adjust the setting in the *Default Expiration* field.
3. Click *Save Changes*.



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

8.6 - Report Scheduling

8.6.1 - Setting a Report Schedule

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

1. Select *Report Definitions* in the *Reports* menu.
2. Check the box for the report definition you want to schedule.
3. Select *Edit Schedule* in the *Schedule* menu.

Schedule for ATL Duplicate File

SCHEDULE START

Engine Local Time:* 12:00 AM

Engine Local Start Date:* 4/27/2021

SCHEDULE RECURRENCE

Once

Daily

Weekly Tuesday

Monthly

Day 1 of every month

The First Sunday of every month

OK Cancel

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



NOTE: The selected time is based on the time zone in which the Engine is located, not the time zone of the workstation you use to access the Web Application.

- **Engine Local Start Date:** Specify the date on which you want the report schedule to take effect.



NOTE: Entering a start date does not mean the report generates on that date, it means the schedule starts on that date. If the *Engine Local Start Date* is set for a Monday but *Schedule Recurrence* is set for Weekly on Sunday, then the report itself does not generate until the Sunday following the scheduled *Engine Local Start Date*.

- **Schedule Recurrence:** Set the frequency of generated reports.
 - **Once:** Select to generate the report one time only.
 - **Daily:** Select to generate the report at a designated time each day.
 - **Weekly:** Select and specify a day on which to generate the report each week.
 - **Monthly:** Select and specify a day on which 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.

8.6.2 - Editing a Report Schedule

1. Select *Report Definitions* in the *Reports* menu.
2. Check the box for the report definition you want to reschedule.
3. Select *Edit Schedule* in the *Schedule* menu.
4. Make the schedule changes you want.
5. Click *OK*.

8.6.3 - Clearing a Report Schedule

1. Select *Report Definitions* in the *Reports* menu
2. Check the box for the report definition with the schedule you want to remove.
3. Select *Clear Schedule* in the *Schedule* menu.
4. When the confirmation screen appears, click *Yes*. The status of the report definition appears in the *Schedule* column as *Not Scheduled*.

8.7 - Reports in Progress

8.7.1 - View Reports In Progress

To view the progress of large reports:

8 - Reporting

1. Select *Reports in Progress* in the *Reports* menu.
2. Click *Refresh*. The report generation is complete when the report disappears from the list.

8.7.2 - Cancel a Report in Progress

To cancel a report in progress:

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

8.8 - Troubleshooting Reports

If there is potential for a reporting problem, File Reporter provides notifications to help resolve the issue. Other helpful tips:

1. Verify that a scan exists for the storage resources on which you want to report.
2. If your Built-in Reports include too much data to be useful, narrow the scope of the report by using filters or reducing the number of report target paths —see [*Built-in Report Filtering \(page 84\)*](#) for details.

9 - Built-in Reports

File Reporter enables you to generate reports applicable to your Microsoft network, including Built-in Reports and Custom Query reports.

9.1 - Overview

After scanning your storage resources, File Reporter has the content necessary to generate reports. The type of report you can generate depends on the type of scan you conducted (e.g., to create an Assigned NTFS Permissions report, you must first conduct a Permissions scan on a Windows share).

Every report is created by first creating report definitions, which specify the report name, type, target path to the scans, and more.



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

File Reporter has built-in aggregate reporting capabilities, meaning you can specify multiple target paths in the same report. Additionally, File Reporter has built-in scoping, which allows you to browse through the file path or Active Directory, and specify the level where you want to start reporting data. Finally, Boolean filtering is available for all file data reports. See [Built-in Report Filtering \(page 84\)](#) for more information.

Once the report definition is created and saved, you can generate the report immediately or schedule it to be generated.

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

You can generate detailed reports from certain built-in report types (e.g., a File Extension report can generate a detailed report that includes the specific details of all *.mov files).

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

9.2 - Built-in Report Types

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

- Directory Data
- Permissions
- File Data

9 - Built-in Reports

- Historic Comparison
- Trending

Each classification includes one or more report types (e.g., the Permissions category can generate three different reports).

9.3 - Branding and Style

9.3.1 - Cover Sheet Logo


All generated Built-in Reports include a cover sheet with a default graphic, which you can replace with your organization's logo.

1. Select *Report Definitions* in the *Reports* menu.
2. Select *Report Branding* in the *Report Branding and Styling* menu.

Report Branding ✕

Company Name:

Company Logo:



Images must meet the following criteria:

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


[Reset](#)

3. Enter the name of your organization in the *Company Name* field. This is the name that appears on the front cover of the report.
4. Click *Browse* to locate the new logo file that will replace the default logo.

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)

5. Click **Save**.

9.3.2 - Report Data Font

Due to the limitations of font encoding in PDF files, you may need to specify an alternate report data font. This is likeliest in locations with multi-byte characters or characters outside the Latin-1 set of characters supported by the default font.

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 may contain characters that span multiple locales, or that include both multi-byte and Latin-1 characters, for example, then choose an appropriate Unicode Font that

can accurately display most characters from the Unicode set and not just for a specific locale.

Two Unicode fonts known for having good character coverage and glyph presentation are MS Arial Unicode (a sans-serif font) and CODE2000 (a serif font) —see http://en.wikipedia.org/wiki/Unicode_font for more information on these fonts and on Unicode fonts in general.



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 Arial font by default. To change the report data font:

1. Select *Report Definitions* in the *Reports* menu.
2. Select *Report Data Font* in the *Report Branding and Styling* menu.
3. Select the font you want to use for the report from the *Report Data Font Name* drop-down menu.
4. Click *Save*.

9.4 - File Management Policy Reports

For most Built-in Reports, you specify a file path for the report through the *Target Paths* tab. If File Dynamics manages your organization's user and collaborative storage, then File Reporter can report on the storage according to the target paths of the File Dynamics policies, rather than through a specific file path.



IMPORTANT: File Reporter 24.3 only supports File Dynamics 6.6 or later.

The advantage to specifying a File Dynamics policy rather than a file path is that a policy can include many different target paths.

In a large organization that utilizes File Dynamics' load balancing capabilities, for example, 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. If you list each of the target paths in a single policy through the *File Management Policies* tab, however, you only need to add the single policy.

Another important advantage is that File Reporter reads the associated policy target paths each time a report is generated so that it dynamically responds to changes in assigned target paths for File Dynamics policies —see [Integrating with File Dynamics \(page 35\)](#) for details.

You can specify policies for most of File Reporter's built-in reports except for Comparison reports, Permissions by Identity reports, and Volume Free Space reports.

9.5 - Built-in Report Filtering

You can 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, including:

- 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

Filters Tab

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

The screenshot shows the 'Report Definition Editor - Atlanta Users Owner Report' window. The 'Name' field contains 'Atlanta Users Owner Report'. The 'Unformatted' checkbox is unchecked. The 'Type' is 'Owner Report'. The 'Description' field contains 'Report Definition created on 12/7/2020 7:46:06 PM by SP\Administrator'. The 'FILTERS' tab is selected, showing a filter expression 'And' with a dropdown arrow. Below the expression, there are labels for 'EXPRESSION' and 'RELATIVE DATE'. At the bottom right, there are 'Save' and 'Cancel' buttons.

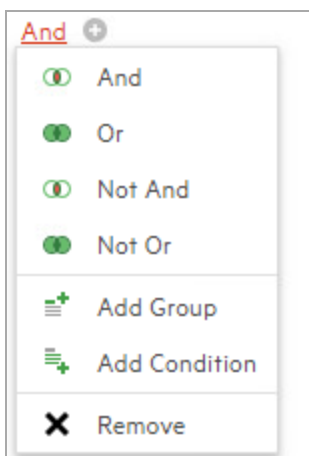
Set filter parameters using the Boolean operators available through the *And* drop-down menu and add the search parameters with the + button. Alternatively, you can set date filters using the *Relative Date* filter parameters on the right-hand portion of the window.

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

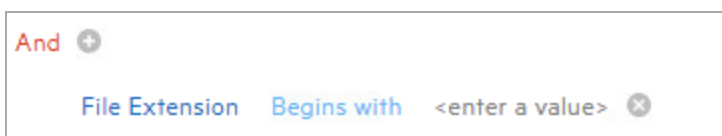
Filter Expression Builder

Use the *And* drop-down menu to:

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



Create parameters for a search condition using the + button next to the *And* drop-down menu.



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

Relative Date Filter Settings

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

9 - Built-in Reports

EXPRESSION						
<input checked="" type="checkbox"/>	Create Date	Since	0	Days	ago	
<input checked="" type="checkbox"/>	Modify Date	Since	0	Days	ago	
<input checked="" type="checkbox"/>	Access Date	Since	0	Days	ago	



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

9.6 - Directory Reports

Reports in this classification include Summary, Directory Quota, Storage Cost, and Comparison reports. Before generating any type of Directory Data report, you must first conduct a File System scan on the desired shares.

9.6.1 - Summary Report

Generate a report that summarizes the contents of folders according to a specified level in the file system.

1. Select *Report Definitions* in the *Reports* menu.
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 NTFS Permissions
- Permissions by Path
- Permissions by Identity

Historic Comparison

- File System Comparison
- NTFS Permissions Comparison

Trending

- Volume Free Space

Custom Query

- Custom Query Report

3. Enter a descriptive *Name* for the report definition in the text field (e.g., User Volume Summary report). The name can contain up to 64 alphanumeric characters.
4. Select the *Summary* option and click *OK*.

9 - Built-in Reports

Report Definition Editor - ATL Summary

Name:* Report Path Depth

Type: Summary Report Initial Chart Path Depth

Description: Report Definition created on 4/27/2021 6:58:47 PM by SPVAdministrator

TARGET PATHS FILE MANAGEMENT POLICIES

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

Save Cancel

5. Specify the depth of reporting in the *Report Path Depth* field.

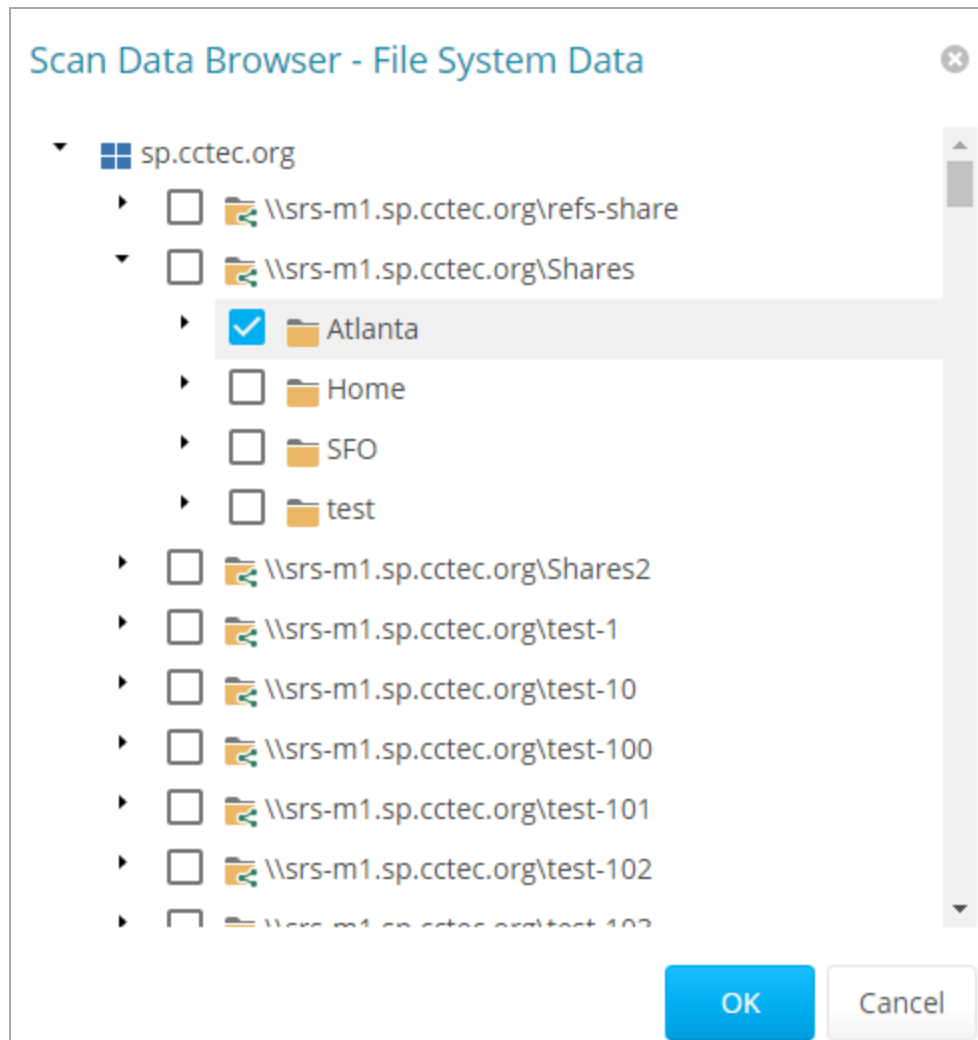
For example, if you select 3 for a Summary report on a server named srs-m1sp, the report would list the file contents of all file paths in the specified shares up to three levels deep in the file structure, as follows:

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

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

This is important so that when the *Report Path Depth* is greater than zero, the top-level folders will be included conditionally. The *Chart Path Depth* parameter cannot be greater than the currently-specified *Report Path Depth*.

7. Click *Add* in the *Target Paths* tab.



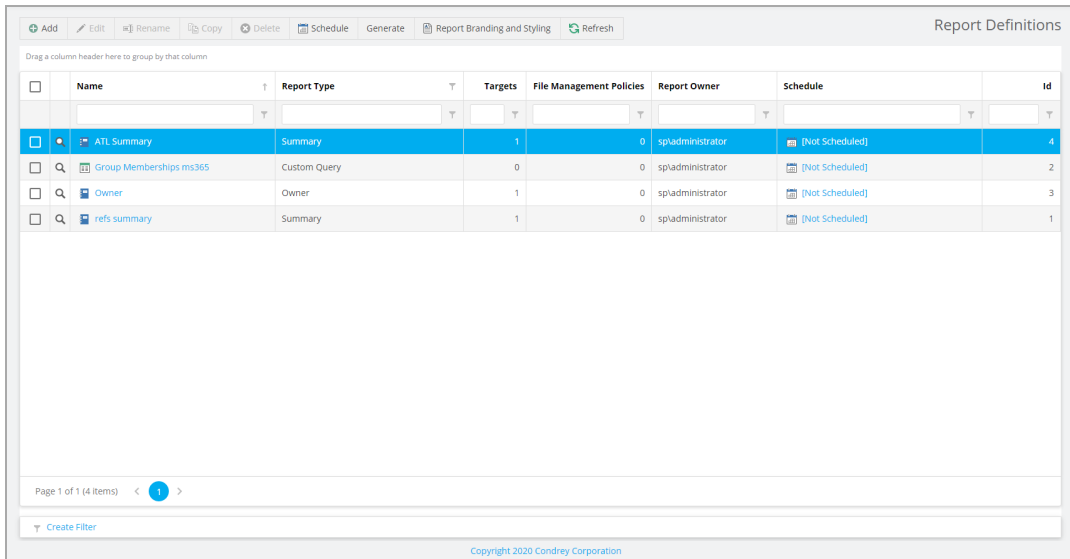
8. Click the drop-down arrow (▶) to browse and select the file paths to include in the report, then click *OK*.



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

9. Click *Save* to add the report definition to the list.

9 - Built-in Reports



The screenshot shows the 'Report Definitions' window with a table of report definitions. The table has columns for Name, Report Type, Targets, File Management Policies, Report Owner, Schedule, and Id. The first row is highlighted in blue.

<input type="checkbox"/>	Name	Report Type	Targets	File Management Policies	Report Owner	Schedule	Id
<input checked="" type="checkbox"/>	ATL Summary	Summary	1	0	spladministrator	[Not Scheduled]	4
<input type="checkbox"/>	Group Memberships ms365	Custom Query	0	0	spladministrator	[Not Scheduled]	2
<input type="checkbox"/>	Owner	Owner	1	0	spladministrator	[Not Scheduled]	3
<input type="checkbox"/>	refs summary	Summary	1	0	spladministrator	[Not Scheduled]	1

Page 1 of 1 (4 items) < 1 >

Create Filter

Copyright 2020 Condrey Corporation

10. Do one of the following:

- Generate the report in Preview mode by following the procedures under [Preview Reports \(page 70\)](#)
- Generate the report in Stored mode by following the procedures under [Stored Reports \(page 72\)](#)

9.6.2 - Directory Quota Report

Generate a report that specifies folders with assigned quota, the amount of quota assigned, and the amount of quota consumed.



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

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Directory Quota* option and click *OK*.

Report Definition Editor - ATL Users Directory Quota

Name:*

Unformatted:

Type: Directory Quota Report

Description: Report Definition created on 4/27/2021 7:10:27 PM by SP\Administrator

TARGET PATHS FILE MANAGEMENT POLICIES

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

5. Click *Add* in the *Target Paths* tab.
6. Select the file paths to include in the report and click *OK*.
7. Click *Save*.
8. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.6.3 - Storage Cost Report

Generate a report that indicates storage costs, according to prices established in the *Cost per Unit* setting of the Report Definition editor, to review the network storage practices of users and groups.



NOTE: The monetary symbol displayed in the report is determined by the local Engine/Web server's Windows locale and region settings (e.g., if the Windows server is set up using a US locale and region, it will display a \$ next to cost entries in the report).

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.

9 - Built-in Reports

3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Storage Cost* option and click *OK*.

The screenshot shows the 'Report Definition Editor - ATL Storage Cost' dialog box. It has a title bar with a close button. The main area contains several fields: 'Name:*' with the value 'ATL Storage Cost', 'Unit:' with a dropdown menu set to 'GB', 'Unformatted:' with an unchecked checkbox, 'Type:' with the value 'Storage Cost Report', and 'Cost per Unit:*' with a spinner box set to '1.0'. A 'Description:' field contains the text 'Report Definition created on 4/27/2021 7:11:35 PM by SPAdministrator'. Below these fields are two tabs: 'TARGET PATHS' (selected) and 'FILE MANAGEMENT POLICIES'. Under the 'TARGET PATHS' tab, there are 'Add' and 'Remove' buttons above a table. The table has a header row with 'Target Path' and one data row with a checkbox and the path '\\srs-m1.sp.cctec.org\Shares\Atlanta'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

5. Establish a cost by selecting the storage unit value in the *Unit* drop-down menu.
6. Indicate the cost of the selected storage unit in the *Cost per Unit* field.
7. Click *Add* in the *Target Paths* tab.
8. Select the file paths to include in the report and click *OK*.
9. Click *Save*.
10. Generate the report as either a *Preview* report or as a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.6.4 - Comparison Report

Generate a report that specifies the differences between two selected folders on the network, which is useful in verifying that servers are hosting the same version of library files, documents, etc.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.

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

Report Definition Editor - ATL Comparison

Name:* ATL SFO Comparison Results: Show unique paths from both targets

Unformatted:

Type: Comparison Report

Description: Report Definition created on 4/27/2021 7:12:15 PM by SPAdministrator

TARGET PATHS

Add Remove

	Target Path	Index
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta	1
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\SFO	2

Save Cancel

5. Select an option from the *Comparison Results* drop-down menu.
 - **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. Click *Add* in the *Target Paths* tab.
7. Select two shares or folders you want to compare and click *OK*.
8. Click *Save*.
9. Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.7 - File Data Reports

Generate detailed reports on a variety of file data, including Filename Extension, Owner, Duplicate File, and Date Age. Before generating any type of File Data report, you must first conduct a File System scan on the desired shares.

9.7.1 - Filename Extension Report

Generate a report that groups data according to the filename extension. This report helps you locate the file types you don't want stored on your network drives (e.g., find stored .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 an extension.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Filename Extension* option and click OK.

Report Definition Editor - ATL File Extension

Name:*

Unformatted:

Type: Filename Extension Report

Description:

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

5. Click *Add* in the *Target Paths* tab.
6. Specify the file paths to include in the report and click *OK*.
7. (Optional) Click the *Filters* tab to set the filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
8. Click *Save*.
9. Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.
10. (Optional) Click a file extension name in the report to generate a detailed report on an individual file extension.

9.7.2 - Detailed Filename Extension Report

Filter a Filename Extension report to include only the files with the extension types you want to view.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.

9 - Built-in Reports

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

The screenshot shows a dialog box titled "Report Definition Editor - ATL File Extension Detail". It contains the following fields and sections:

- Name:** ATL File Extension Detail
- Unformatted:**
- Type:** Filename Extension Detail Report
- Description:** Report Definition created on 4/27/2021 7:17:00 PM by SPAdministrator
- Filename Extensions (no leading dot), one per line:** pdf, doc, txt, png, jpeg
- TARGET PATHS** (selected tab):
 - Buttons: Add, Remove
 - Table with one row: \\srs-m1.sp.cctec.org\Shares\Atlanta
- FILE MANAGEMENT POLICIES** (disabled tab)
- FILTERS** (disabled tab)
- Buttons: Save, Cancel

5. Specify the filename extensions to include in the report by listing each on an individual line in the *Filename Extension* field. Do not precede the filename extension with a period (e.g., mov, jpeg, tmp).
6. Click *Add* in the *Target Paths* tab.
7. Specify the file paths to include in the report and click *OK*.
8. (Optional) Click the *Filters* tab to set the filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
9. Click *Save*.
10. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.7.3 - Owner Report

Generate a report that groups data according to file owners to determine the amount of storage each owner uses, what data is being stored, and whether the data is justified for storage.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Owner* option and click *OK*.

Report Definition Editor - ATL Owner

Name:*

Unformatted:

Type: Owner Report

Description: Report Definition created on 4/27/2021 7:18:06 PM by SPAdministrator

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

Save Cancel

5. Click *Add* in the *Target Paths* tab.
6. Specify the file paths to include in the report and click *OK*.
7. (Optional) Click the *Filters* tab to set the filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
8. Click *Save*.
9. Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.
10. (Optional) Click an individual owner's name to generate a detailed report on them.

9.7.4 - Detailed Owner Report

Filter an Owner report to specify only the users you want to view.

9 - Built-in Reports

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Owner Detail* option and click *OK*.

Report Definition Editor - ATL Owner Detail

Name:* ATL Owner Detail See Owners tab below for selected identities.

Unformatted:

Type: Owner Detail Report

Description: Report Definition created on 4/27/2021 7:18:57 PM by SPAdministrator

OWNERS TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

#	Identity System	Owner
<input type="checkbox"/>	sp.cctec.org	SPVAARO_C_EMFIN695
<input type="checkbox"/>	sp.cctec.org	SPVADRI_Z_BUGOS942
<input type="checkbox"/>	sp.cctec.org	SPVANET_U_HUGIL883
<input type="checkbox"/>	sp.cctec.org	SPVANIT_Y_CROUT029
<input type="checkbox"/>	sp.cctec.org	SPVANJA_G_NOETH789
<input type="checkbox"/>	sp.cctec.org	SPVANJA_G_NOETH789

Page 1 of 1 (9 items) < 1 >

Save Cancel

5. Click *Add* in the *Owners* tab.
6. Check the box to specify each owner to include in the report and click *OK*.
7. Click *Add* in the *Target Paths* tab
8. Check the box to specify each file path to include in the report and click *OK*.
9. (Optional) Click the *Filters* tab to set filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
10. Click *Save*.
11. Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.7.5 - Duplicate File Report

Generate a report that locates duplicate versions of stored files in order to delete them as part of best network storage practices.



NOTE: This Duplicate File report option compares filenames and other metadata. File Reporter offers a more advanced Duplicate File report generated through content hash comparisons —see Content Hash Duplicate File Reports for more details.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Duplicate File* option and click *OK*.

Report Definition Editor - ATL Duplicate File

Name:* Match Size

Unformatted: Match Name

Type: Duplicate File Report Match Create Time

Description: Report Definition created on 4/27/2021 7:20:33 PM by SPAdministrator Match Modify Time

Minimum Duplicates

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

5. Check the relevant boxes and enter the *Minimum Duplicates* limit to specify the reporting parameters. The more check boxes you select, the more likely it is that File Reporter can identify definitive duplicate files.
 - **Match Size:** Reported files must have duplicate file sizes. This option cannot be deselected.
 - **Match Name:** Reported files must have duplicate names with other files.

9 - Built-in Reports

- **Match Create Time:** Reported files must have duplicate file creation times with other files.
 - **Match Modify Time:** Reported files must have duplicate file modification times with other files.
 - **Minimum Duplicates:** Specifies the minimum number of duplicate files to include in the report, according to the parameters selected above.
6. Check the box to specify each file path to include in the report and click *OK*.
 7. (Optional) Click the *Filters* tab to set filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
 8. Click *Save*.
 9. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.
 10. (Optional) Click a specific duplicate file name in the report to generate a detailed report on it.

9.7.6 - Detailed Duplicate File Report

Filter a Duplicate File report to specify only the exact filename(s) to search for, along with exact create and modify times.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Duplicate File Detail* option and click *OK*.

Report Definition Editor - ATL Duplicate File Detail

Name:*

Unformatted:

Type: Duplicate File Detail Report

Description: Report Definition created on 4/27/2021 7:21:12 PM by SP\Administrator

Duplicate Criteria

Name

Size bytes

Create Time

Modify Time

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

- In the *Duplicate Criteria* section, check the relevant boxes and enter the desired parameters to specify the file name, file size, and the dates and times that the file was created or modified.



IMPORTANT: When specifying Create or Modify times, enter the exact time 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 instead —see [Built-in Report Filtering \(page 84\)](#) for details.

- Check the box to specify each file path to included in the report and click *OK*.
- (Optional) Click the *Filters* tab to set the filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
- Click *Save*.
- Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.7.7 - Date-Age Report

Generate a report that groups file count data according to when files were created, last accessed, or last modified to determine which files may be eligible to delete, archive, or move those files to less expensive storage as part of best network storage practices.

9 - Built-in Reports

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Date-Age* option and click *OK*.

The screenshot shows the 'Report Definition Editor - ATL Date-Age' dialog box. It contains the following fields and options:

- Name:** ATL Date-Age
- Date Type:** Create Time
- Unformatted:**
- Type:** Date-Age Report
- Detail Level:** Year
- Description:** Report Definition created on 4/27/2021 7:22:59 PM by SP\Administrator

Below these fields are three tabs: **TARGET PATHS** (selected), **FILE MANAGEMENT POLICIES**, and **FILTERS**. Under the 'TARGET PATHS' tab, there are 'Add' and 'Remove' buttons and a table with one row:

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

5. Select one of the following options in the *Date Type* drop-down menu:
 - **Create Time** reports when files were created.
 - **Modify Time** reports when files were last modified.
 - **Access Time** reports when files were last accessed.
6. Select one of the following options in the *Detail Level* drop-down menu:
 - **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. Check the box to specify each file path to include in the report and click *OK*.
8. (Optional) Click the *Filters* tab to set filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
9. Click *Save*.
10. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.
11. (Optional) Click a specific year, month, or date to generate a detailed report. Unlike the standard Date-Age report that lists the data by file count, the generated detailed report lists individual files.

9.7.8 - Detailed Date-Age Report

Filter a Date-Age report to specify the exact create, modify, or access date parameters.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Date-Age Detail* option and click *OK*.

Report Definition Editor - ATL Date-Age Detail ✕

<p>Name:* <input style="width: 90%;" type="text" value="ATL Date-Age Detail"/></p> <p>Unformatted: <input type="checkbox"/></p> <p>Type: Date-Age Detail Report</p> <p>Description: <input style="width: 90%;" type="text" value="Report Definition created on 4/27/2021 7:23:37 PM by SP\Administrator"/></p>	<p>Date Type: <input style="width: 90%;" type="text" value="Create Time"/></p> <p>Detail Level: <input style="width: 90%;" type="text" value="Year"/></p> <p>Selected Dates: <input style="width: 90%;" type="text" value="2020
2019
2018"/></p> <p style="font-size: small;">Enter one or more dates with the format yyyy-mm-dd, one per line.</p>
--	--

TARGET PATHS FILE MANAGEMENT POLICIES FILTERS

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

5. Select one of the following options in the *Date Type* drop-down menu:

9 - Built-in Reports

- **Create Time** reports when files were created.
 - **Modify Time** reports when files were last modified.
 - **Access Time** reports when files were last accessed.
6. Select one of the following options in the *Detail Level* drop-down menu:
 - **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. Specify the dates to include in the *Selected Dates* field. The report will only indicate the files created, last modified, or last accessed on those dates.
 8. Check the box to specify each file path to include in the report and click *OK*.
 9. (Optional) Click the *Filters* tab to set filters for the report —see [Built-in Report Filtering \(page 84\)](#) for details.
 10. Click *Save*.
 11. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.8 - Permissions Reports

Generate detailed reports on a variety of permissions data, including Assigned NTFS Permissions, Permissions by Path, and Permissions by Identity. Before generating any type of Permissions report, you must first conduct a Permissions scan on the desired volumes or shares.

9.8.1 - Assigned NTFS Permissions Report

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

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Assigned NTFS Permissions* option and click *OK*.

Report Definition Editor - ATL NTFS Permissions

Name:* ATL NTFS Permissions Limit Path Depth 0

Unformatted: Include Inherited ACEs

Type: Assigned NTFS Permissions Report

Description: Report Definition created on 4/27/2021 7:14:00 PM by SPAdministrator

TARGET PATHS FILE MANAGEMENT POLICIES

Add Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

Save Cancel

5. (Conditional) To limit the scope of the report to a set depth in the file structure, check the *Limit Path Depth* box and specify the depth level (e.g., 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 Access Control Entries (ACEs), uncheck the *Include Inherited ACEs* box.
7. Click *Add* in the *Target Paths* tab.
8. Check the box to specify each file path to include in the report and click *OK*.
9. Click *Save*.
10. Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.8.2 - Permissions by Path Report

Generate a report that indicates the effective permissions to the Microsoft file system according to the paths you specify.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.

9 - Built-in Reports

3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Permissions by Path* option and click *OK*.

The screenshot shows a dialog box titled "Report Definition Editor - ATL Path Permissions". It contains the following fields and options:

- Name:** A text field containing "ATL Path Permissions".
- Unformatted:** A checkbox that is currently unchecked.
- Type:** A dropdown menu set to "Permissions by Path Report".
- Description:** A text area containing "Report Definition created on 4/27/2021 7:14:36 PM by SPAdministrator".

Below these fields are two tabs: "TARGET PATHS" (which is selected) and "FILE MANAGEMENT POLICIES". Under the "TARGET PATHS" tab, there are "Add" and "Remove" buttons. A table with the following content is visible:

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

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

5. Click *Add* in the *Target Paths* tab.
6. Check the box to specify each file path to include in the report and click *OK*.
7. Click *Save*.
8. Generate the report as either a *Preview* report or a *Stored* report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.8.3 - Permissions by Identity Report

Generate a report that indicates the effective permissions to the Microsoft file system, according to the identities you specify.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Permissions by Identity* option and click *OK*.

Report Definition Editor - ATL Identity Permissions

Name:*

Unformatted:

Type: Permissions by Identity Report

Description:

IDENTITIES

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

	Identity System	Name
<input type="checkbox"/>	sp.cctec.org	SP\AARO_C_EMFIN695
<input type="checkbox"/>	sp.cctec.org	SP\ABIB_V_SONNE757
<input type="checkbox"/>	sp.cctec.org	SP\ADEN__BOHNE231
<input type="checkbox"/>	sp.cctec.org	SP\ADOL_V_BEISH699
<input type="checkbox"/>	sp.cctec.org	SP\ADRI_Z_BUGOS942

5. Click *Add* in the *Identities* tab.
6. Check the box to specify each identity to include 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 —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.9 - Historic Comparison Reports

Generate a report that specifies the differences between two similar scan types of the same target system (e.g., using a Previous Permissions scan and a Current Permissions scan of the same Windows share, you can identify the changes in the share's permissions that occurred between the two scans).

Historic Comparison reports can compare the following:

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

9 - Built-in Reports

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

9.9.1 - Historic File System Comparison Report

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Under *Historic Comparison*, select the *File System Comparison* option, then click *OK*.

Report Definition Editor - ATL Historic FS Comparison

Name:* ATL Historic FS Comparison

Unformatted:

Type: Historic File System Comparison Report

Description: Report Definition created on 4/27/2021 7:24:47 PM by SP\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
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

Save Cancel

5. (Conditional) To limit the scope of the report to a set depth in the file structure, check the *Limit Path Depth* box and specify the depth level (e.g., 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. Select one of the following options from the *Scans to Compare* drop-down menu:
 - **Current and Previous** compares the Current scan of the storage resource to its Previous scan.

- **Current and Baseline** compares the Current scan of the storage resource to its Baseline scan.
- **Previous and Baseline** compares the Previous scan of the storage resource to its Baseline scan.



NOTE: All options appear whether you have the designated scans or not. If you have not created a designated scan yet, then File Reporter will generate an empty report.

7. Specify which metadata categories to include in the report by checking or unchecking the boxes in the *Query Filters* section:
 - **Added Entries** lists files or folders that have been added since the older scan.
 - **Removed Entries** lists files or folders that have been removed since the older scan.
 - **Modified Entries** lists files or folders that have been modified since the older scan.
 - **Files** lists files.
 - **Folders** lists folders.
8. Specify which of the attributes modified between scans to include in the report in the *Include entries modified by:* section under *Query Filters*.
9. Specify which metadata categories to display in the *Detail Display Options* section of the report by checking or unchecking the boxes in the *Detail Data* section.
 - **Added Entries**
 - **Removed Entries**
 - **Modified Entries**



NOTE: These categories pertain only to the Detail Data section of the report, not the Summary Data section. If a box is checked, the report will display the category, even if there is no data to list.

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

9 - Built-in Reports

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

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

11. Check the box to specify each file path to include in the report and click *OK*.
12. Click *Save* to close the Report Definition Editor.
13. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.9.2 - Historic NTFS Permissions Comparison Report

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.
4. Select the *Historic NTFS Permissions* option, then click *OK*.

The screenshot shows the 'Report Definition Editor - ATL Historic NTFS Comparison' dialog box. It contains the following fields and options:

- Name:** ATL Historic NTFS Comparison
- Unformatted:**
- Type:** Historic NTFS Permissions Comparison Report
- Description:** Report Definition created on 4/27/2021 7:25:49 PM by SP\Administrator
- Limit Path Depth:** Limit Path Depth (100)
- Scans to Compare:** Current and Previous
- Include Inherited ACEs:**
- Include Removed Paths:**

TARGET PATHS

Buttons: Add, Remove

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares\Atlanta

Buttons: Save, Cancel

5. (Conditional) To limit the scope of the report to a set depth in the file structure, check the *Limit Path Depth* box and specify the depth level (e.g., 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. Select one of the following options from the *Scans to Compare* drop-down menu:
 - **Current and Previous** compares the Current scan of the storage resource to its Previous scan.
 - **Current and Baseline** compares the Current scan of the storage resource to its Baseline scan.
 - **Previous and Baseline** compares the Previous scan of the storage resource to its Baseline scan.



NOTE: All options appear whether you have the designated scans or not. If you have not created a designated scan yet, then File Reporter will generate an empty report.

7. (Conditional) If you want the report to include inherited permissions as well as direct permissions, check the *Include Inherited ACEs* 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, uncheck the *Include Removed Paths* box.
9. Check the box to specify each file path to include in the report and click *OK*.
10. Click *Save* to close the Report Definition Editor.
11. Generate the report as either a Preview report or a Stored report —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.10 - Trending Report

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

Generating a Volume Free Space Report

This report lets you view available Windows share disk space over a set amount of time. For best results, you should schedule regular Volume Free Space scans on specific shares to give File Reporter the data it needs to graph the pattern of free space on the share.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive *Name* for the report definition in the text field.

9 - Built-in Reports

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

The screenshot shows a window titled "Report Definition Editor - ATL Volume Free Space Report". It contains the following fields and controls:

- Name:** ATL Volume Free Space Report
- Last number of days to include:** 365 (with up and down arrows)
- Unformatted:**
- Type:** Volume Free Space Trending Report
- Description:** Report Definition created on 4/27/2021 7:26:31 PM by SPAdministrator

Below these fields is a section titled "TARGET PATHS" with "Add" and "Remove" links. A table lists target paths:

	Target Path
<input type="checkbox"/>	\\srs-m1.sp.cctec.org\Shares

At the bottom right of the window are "Save" and "Cancel" buttons.

5. Specify the *Last number of days to include* in the report (e.g., enter 30 if you want the report to graph the previous month). The lowest number you can specify is 7.
6. Check the box to specify each share to include in the report and click *OK*.
7. Click *Save*.
8. Generate the report as either a *Preview report* or a *Stored report* —see [Preview Reports \(page 70\)](#) and [Stored Reports \(page 72\)](#) for details.

9.11 - Folder Summary Reports

Generate a report that provides a visual folder structure according to the latest scanned file system data. Folder Summary reports also provide extensive summary information for the folders and files.

1. Select *Folder Summary* in the *Reports* menu.

Export Pdf Refresh Folder Summary

Path	Scan Start Time	File Size	File Count	Folder Count	Folder Quota	% of Parent Folder Size	% of Total Size
sp.cctec.org							
\rsrs-m1.sp.cctec.org\trefs-share	11/10/2020 7:36:20 PM						
\rsrs-m1.sp.cctec.org\Shares	4/27/2021 7:40:32 PM						
\		2 GB	45	1,105	100	100	
Atlanta		1 GB	29	30	67	67	
Employees		1 GB	27	17	100	67	
Files...		223 bytes	1		0	0	
atcox		591 MB	15	1	50	33	
Files...		591 MB	10		100	33	
old		7 KB	5	0	0	0	
anance		591 MB	11	0	50	33	
Files...		591 MB	11		100	33	
areid		0 bytes	0	0	0	0	
blawson		0 bytes	0	0	0	0	
bnabors		0 bytes	0	0	0	0	
cedwards		0 bytes	0	0	0	0	
dadams		0 bytes	0	0	0	0	
dbetts		0 bytes	0	0	0	0	
dthomas		0 bytes	0	0	0	0	
jmcicord		0 bytes	0	0	0	0	
jmunz		0 bytes	0	0	0	0	
jsmilley		0 bytes	0	0	0	0	
kparkes		0 bytes	0	0	0	0	
lhanson		0 bytes	0	0	0	0	
ljones		0 bytes	0	0	0	0	
pdavis		0 bytes	0	0	0	0	
Groups		919 KB	2	11	0	0	
Home		0 bytes	0	6	0	0	

Copyright 2020 Condrey Corporation

2. Print, save, or export the data as a PDF or XLS file.

10 - Custom Query Reports

File Reporter enables you to generate reports from SQL queries that you enter, and create optional report layouts for displaying the resulting data. These queries allow you to collect specific details in reports that are not available through the Built-in Report types in File Reporter.

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



NOTE: Refer to the *File Reporter 24.3 Custom Query Guide* for details and examples of the supported database functions, tables, and views you can generate using Custom Query reports.

You enter SQL queries through report editors available from File Reporter's browser-based administrative interface and the Report Designer client tool.



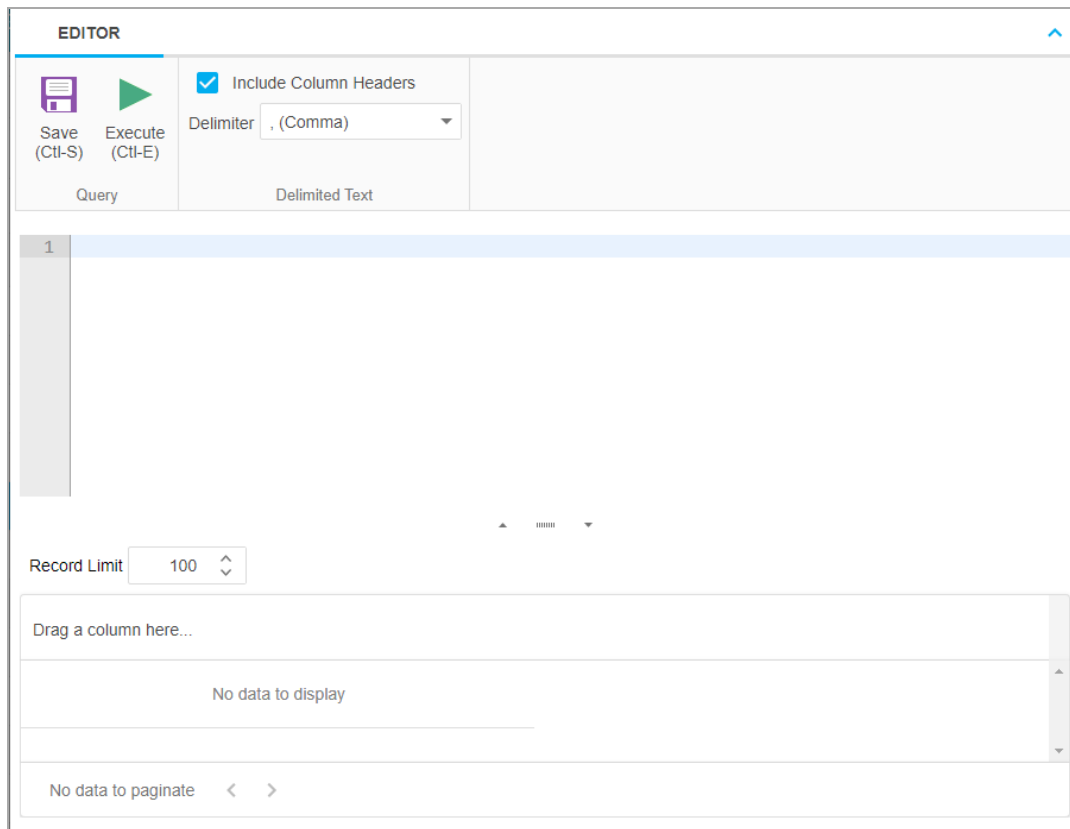
NOTE: See *Designing a Custom Query Report* in the *File Reporter 24.3 Client Tools Guide* for details on using the report editor in the Report Designer.



IMPORTANT: Use the File Query Cookbook to obtain SQL queries and sample report layouts. The SQL queries and report layouts can both be customized as needed. You can access the File Query Cookbook directly through the Report Designer interface or at <https://filequerycookbook.com>.

1. Select *Report Definitions* in the *Reports* menu.
2. Click *Add*.
3. Enter a descriptive name *Name* for the report definition in the text field.
4. Select *Custom Query Report*.
5. Click *OK*.

10 - Custom Query Reports



6. Enter the SQL query according to the information you want to include in the report.
 - Click Execute as you update the query to see a preview in the bottom portion of the editor that shows how the report will appear.
 - The *Row Limit* setting does not limit the size of the report. Instead, it limits how much can be previewed.

EDITOR

Save (Ctl-S) Execute (Ctl-E) Include Column Headers Delimiter: , (Comma)

Query Delimited Text

```

29         ELSE 'Other Files'
30     END AS category
31 FROM srs.current_fs_scandata AS sd
32 WHERE (sd.fullpath LIKE '\\srs-m1.sp.cctec.org\Shares\%' ESCAPE '#') AND
33       (sd.path_type = 1)),
34 y(category, filename_extension, extension_size, extension_count) AS (SELECT x.category,
35 x.filename_extension,
36 Sum(x.size) AS extension_size,
37 Count(x.filename_extension) AS extension_count
38 FROM x
39 GROUP BY x.category
40

```

Record Limit: 100

#	category	filename_exte	extension_siz	extension_co	cat_size	cat_size_strir	ext_size_strir	cat_ext_coun	c
1	Database Files	accdb	20	1	20	20 bytes	20 bytes	1	
2	Executables	exe	1239905456	14	1239905456	1.15 GB	1.15 GB	1	
3	Other Files	lic	11873	8	12096	11.81 KB	11.59 KB	2	
4	Log Files	log	941143	1	941143	919.08 KB	919.08 KB	1	

Page 1 of 1 (6 items) < 1 >

7. When you are satisfied with the report and the previewed results, click *Save*.
8. Close the Custom Query Report Editor.
9. Select *Report Definitions* in the *Reports* menu.
10. Select the Custom Query report you just saved and generate the report as either a *Preview Report* or a *Stored Report* —see *Preview Reports (page 70)* and *Stored Reports (page 72)* in the *File Reporter24.3 Administration Guide* for details.

A.1 - Security Settings

A.1.1 - Windows Firewall Settings

Exceptions must be added to the firewall rules for your particular host system.

The following exceptions are required to perform File Reporter tasks.



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

- The Engine must be permitted to make outbound connections.
- The Engine must be able to listen on port 3035 (which is the default setting during installation and configuration).
- AgentFS must be permitted to make outbound connections.
- AgentFS must be able to listen on TCP port 3037 (which is the default setting during installation and configuration).
- The Web Application hosted on IIS must be allowed to listen on TCP ports 80 and 443.
- You must enable the Remote File Server Resource Manager Management - FSRM Service (RPC-In) firewall rule on each server that hosts storage for which you want to collect quota via proxy.
- If File Content Analysis is enabled:
 - ManagerFC, AgentFC, and RabbitMQ must be permitted to make outbound connections.
 - RabbitMQ must be able to listen on TCP port 15671 for the management interface (which is the default setting during RabbitMQ configuration with TLS).
 - RabbitMQ must be able to listen on TCP port 5671 (which is the default setting during RabbitMQ configuration with TLS).

A.1.2 - Windows LSA User Rights

Windows Local Security Authority (LSA) User Rights and Privileges are assigned to accounts or groups, and they determine how those accounts or group members may access the system. You can modify User Rights through the Local Security Policy:

1. Select *Local Security Policy* in the *Administrative Tools* menu.
2. Select *Local Policies* in the *Security Settings* menu.
3. Select *User Rights Assignments* and verify that the File Reporter proxy rights group has the following assignments:

- Access this computer from the network.
- Back up files and directories.
- Bypass traverse checking.
- Create a token object.
- Create symbolic links.
- Impersonate a client after authentication.
- Log on as a batch job.
- Manage auditing and security log.



IMPORTANT: Absence or removal of these privileges may prevent the Engine and Agent components from functioning properly. In some cases, Group Policy Object (GPO) settings may remove or override the necessary Local Security Policy settings and revoke the membership of the File Reporter proxy object from one or more required LSA privileges.

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

A.1.3 - Proxy Rights Group

Whenever any of File Reporter's components are installed on a server in a domain, the Proxy Rights Security group is granted membership in that server's built-in Administrators security group by default. This grants File Reporter certain necessary permissions in addition to the LSA privileges required for successful scanning of file system metadata.

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

Additionally, the other servers in the domain that do not host components, but *do* host storage to be scanned, must have the necessary rights and privileges, along with certain file share and NTFS permissions. The easiest way to grant these rights and privileges is through Group Policy objects in Active Directory.

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

A.1.4 - Windows File Server Cluster

File Reporter supports Windows File Server clusters via proxy agents. Configuring a cluster to be scanned through a proxy agent is similar to configuring an individual server to be scanned by a proxy agent.

To support proxy-based scanning, the File Reporter Proxy Rights group must be granted membership in the built-in Administrators group and granted all the required LSA user rights on each cluster node.

When this is done, the required folder share permissions and NTFS permissions must be granted to the Proxy Rights group for all shares and NTFS volumes that will be scanned by File Reporter.

B.1 - Log File Locations

When troubleshooting File Reporter, you may need to refer to component log files. The following table identifies the locations for each log file.

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

C.1 - AgentFS Scan Capabilities

C.1.1 - Server Platform and NAS Device Support

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

Server Platform	Scan Type
Windows Server 2022	Local Scan Proxy Scan
Windows Server 2019	
Windows Server 2016	
Windows Server 2012 R2	Proxy scan only

Older systems such as Windows Server 2008 or 2012 may work but are not supported as scan target hosts.

The following Network-Attached Storage (NAS) devices are supported as hosts for scan targets.

NAS Device	Scan Type
NetApp Filer with OnTAP 9.x PowerScale (formerly Isilon) OneFS 9.x	Proxy scan only



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



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

C.1.2 - File System Feature Support

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

Feature	NTFS	ReFS
File Name / Extension	✓	✓
File Size	✓	✓
File Sparse Size	✓	✓
File Compressed Size	✓	✗
File Size on Disk ¹	✓	✓
Create Time	✓	✓
Modify Time	✓	✓
Access Time	✓	✓
Directory Quota ²	✓	✗
Owner	✓	✓
Encrypting File System (EFS)	✗	✗

1. File size-on-disk calculations default to an assumed 4 KB block size for cases in which AgentFS can't retrieve the actual allocation size.
2. Directory Quotas are only available on Windows 2008 R2 and later servers, and only if the File Server Resource Manager (FSRM) role is installed.

C.1.3 - Security Scans

Windows Component	Supported	Notes
Share Permissions	✓	
Security Descriptors	✓	Includes the DACLs, owner, and all ACE and security descriptor flags. Only security descriptors for folders are currently collected, however. 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 processed currently.
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 preserved currently .
Primary Groups	✓	
Local Security Authority (LSA) Privileges	✗	LSA privileges are not collected currently.

C.1.4 - Other Microsoft Supported Features

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

C.1.5 - Current Limitations

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

C.1.6 - AgentFS Scan Capabilities

Server Platform and NAS Device Support

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

Server Platform	Scan Type
Windows Server 2022	Local Scan Proxy Scan
Windows Server 2019	
Windows Server 2016	
Windows Server 2012 R2	Proxy scan only

Older systems such as Windows Server 2008 or 2012 may work but are not supported as scan target hosts.

The following Network-Attached Storage (NAS) devices are supported as hosts for scan targets.

NAS Device	Scan Type
NetApp Filer with OnTAP 9.x	Proxy scan only
PowerScale (formerly Isilon) OneFS 9.x	



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



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

File System Feature Support

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

Feature	NTFS	ReFS
File Name / Extension	✓	✓
File Size	✓	✓
File Sparse Size	✓	✓
File Compressed Size	✓	✗
File Size on Disk ¹	✓	✓
Create Time	✓	✓
Modify Time	✓	✓
Access Time	✓	✓
Directory Quota ²	✓	✗
Owner	✓	✓
Encrypting File System (EFS)	✗	✗

1. File size-on-disk calculations default to an assumed 4 KB block size for cases in which AgentFS can't retrieve the actual allocation size.
2. Directory Quotas are only available on Windows 2008 R2 and later servers, and only if the File Server Resource Manager (FSRM) role is installed.

Security Scans

Windows Component	Supported	Notes
Share Permissions	✓	
Security Descriptors	✓	Includes the DACLs, owner, and all ACE and security descriptor flags. Only security descriptors for folders are currently collected, however. 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 processed currently.
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 preserved currently .
Primary Groups	✓	
Local Security Authority (LSA) Privileges	✗	LSA privileges are not collected currently.

Other Microsoft Supported Features

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

Current Limitations

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

D.1 - NAS Device Considerations

D.1.1 - NetApp Filer

Configuration for a NetApp Filer device is 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 membership in the NAS device's built-in Administrators group to the Proxy Rights group.
3. Grant the folder the share permissions required to access the storage to the Proxy Rights group.

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

D.1.2 - PowerScale OneFS

Perform the following steps to integrate a PowerScale OneFS device (formerly EMC Isilon). You can use these same steps to determine 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 steps necessary to give the proxy rights group access to the desired shares and folders on the NAS device.

D.1.3 - Other NAS Devices

Perform the following steps to determine 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 steps necessary to give the Proxy Rights group access to the desired shares and folders on the NAS device.

E.1 - Resetting the Proxy User Password

If the proxy user password is not working, you can reset it through the Engine Configuration Utility.

The proxy user password is reset as part of the configuration process.