



## **Peer Global File Service User Guide**

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.

Updated Thursday, May 13, 2021

# Table of Contents

<b>Peer Global File Service Help</b>	<b>1</b>
<b>Terminology</b>	<b>1</b>
<b>Installation and Configuration</b>	<b>7</b>
<b>Requirements and Prerequisites</b>	<b>7</b>
Dell EMC Prerequisites	8
NetApp Prerequisites	8
Nutanix Prerequisites	8
<b>Installing Peer Management Center</b>	<b>9</b>
Configuring and Managing the Web and API Services	14
Configuring the Web and API Services	14
Securing Access to the Web Client	16
<b>Installing Peer Agents</b>	<b>16</b>
<b>Updating Peer Management Center and Peer Agents</b>	<b>20</b>
Updating Peer Management Center	20
Updating Peer Agents	23
<b>Peer Management Center User Interface</b>	<b>24</b>
<b>Accessing the Web Client</b>	<b>27</b>
Peer Services Required for Web Client	29
<b>Views</b>	<b>30</b>
Agents View	32
Agents View Toolbar	34
Alerts View	34
Dashboard	36
Job Alerts View	37
Jobs View	38
Jobs View Toolbar	40
Runtime Views	41
Cloud Backup and Replication Job Runtime View	42
DFS-N Management Job Runtime View	43
File Collaboration Job Runtime View	43
Summary Tab	44
Session Tab	46
Event Log Tab	47
Quarantines Tab	48
Retries Tab	49
Alerts Tab	50
Participants Tab	51
Configuration Tab	53
File Replication Job Runtime View	53
File Synchronization Job Runtime View	54
Summary Views	55
Agent Summary View	56
Cloud Summary View	57
Collab, Sync, and Repl Summary View	58
Summary Tab	59
Reports Tab	62
Namespace Summary View	65
<b>Main Window Menus and Toolbar</b>	<b>66</b>

File Menu .....	67
Help Menu .....	68
Window Menu .....	70
Toolbar .....	71
<b>Tables .....</b>	<b>73</b>
<b>Basic Concepts .....</b>	<b>74</b>
<b>Email Alerts .....</b>	<b>74</b>
<b>File and Folder Filters .....</b>	<b>75</b>
Creating and Applying File Filters.....	76
Predefined File Filters.....	76
Updating Predefined File Filters.....	77
Defining Filter Patterns.....	78
Using Complex Regular Expressions in Filter Patterns .....	79
Using Wildcards in Filter Patterns .....	80
Automatically Excluded File Types.....	80
Excluding Temporary Files.....	81
Filtering on Last Modified Date.....	84
Filtering on File Size .....	86
Filtering Folders .....	88
Folder Filter Examples .....	89
File Filter Usage Notes.....	90
<b>List Filters .....</b>	<b>91</b>
Creating Complex Filter Expressions.....	92
Saving and Managing List Filters.....	93
Removing List Filters.....	93
<b>Logging and Alerts .....</b>	<b>93</b>
File Event Logs and Alerts .....	98
<b>Web Client Users .....</b>	<b>101</b>
Internal Users .....	101
Active Directory Users and Groups.....	102
Overview of Web Roles.....	103
Standard Web Roles .....	103
Standard Web Role Permissions .....	104
Custom Web Roles .....	107
Custom Web Role Permissions.....	107
<b>SNMP Notifications .....</b>	<b>109</b>
<b>Tags .....</b>	<b>110</b>
Creating Tags and Categories.....	111
Assigning Tags .....	111
Using Tags to Filter Resources.....	113
<b>Advanced Topics .....</b>	<b>114</b>
<b>Conflicts, Retries, and Quarantines .....</b>	<b>114</b>
<b>DFS Namespace Failover and Failback .....</b>	<b>116</b>
<b>File Metadata Synchronization .....</b>	<b>116</b>
<b>Managing Peer Agents .....</b>	<b>117</b>
Peer Agent Connection Statuses.....	120
Editing an Agent Configuration.....	121
Broker Configuration .....	123
General .....	124
Logging .....	125
Performance .....	126
VM Options .....	127
Viewing Agent Properties.....	127

Editing Agent Properties.....	129
Re-enabling a Disabled Agent Within a Job.....	131
Updating a Peer Agent.....	131
<b>PeerGFS API .....</b>	<b>132</b>
Accessing the PeerGFS API.....	132
Testing the PeerGFS API.....	133
Integrating Your Own Tools and Scripts with the PeerGFS API.....	133
API Quick Reference.....	134
API Categories .....	134
Status Codes .....	134
<b>Scheduled Replication .....</b>	<b>135</b>
<b>Smart Data Seeding .....</b>	<b>135</b>
<b>Storage Capacity .....</b>	<b>137</b>
<b>TLS Certificates .....</b>	<b>137</b>
Creating New Certificates.....	138
Using Existing Certificates.....	144
<b>Preferences .....</b>	<b>149</b>
<b>Configuring Preferences .....</b>	<b>151</b>
<b>Cloud Backup and Replication Job Preferences .....</b>	<b>152</b>
Cloud Backup and Replication.....	153
Database Connections.....	155
Destination Credentials.....	157
Email Alerts .....	159
File Retries and Source Snapshots.....	163
File and Folder Filters .....	164
Performance .....	167
Proxy Configuration.....	169
Replication and Retention Policies.....	171
SNMP Notifications .....	173
Scan Manager .....	176
<b>Collaboration, Replication, and Synchronization Job Preferences .....</b>	<b>178</b>
Collab, Sync, and Replication.....	178
DFS-N Management.....	180
Email Alerts .....	182
File Retries .....	185
File and Folder Filters .....	187
Locking .....	189
Performance .....	191
Real-time Event Detection.....	192
Revit Enhancements.....	193
SNMP Notifications .....	196
Scan Manager .....	199
Scheduled Replication.....	201
<b>DFS-N Management Job Preferences .....</b>	<b>206</b>
Email Alerts .....	207
SNMP Notifications .....	210
<b>Email Configuration .....</b>	<b>213</b>
<b>General Configuration .....</b>	<b>216</b>
General Configuration.....	217
Agent Connectivity.....	219
Broker Configuration.....	221
Email Alerts .....	222
Software Updates.....	225
Tags Configuration.....	226



Web and API Configuration .....	228
<b>Licensing .....</b>	<b>229</b>
<b>MED Configuration .....</b>	<b>232</b>
<b>NAS Configuration .....</b>	<b>238</b>
Dell EMC Configurations .....	238
Dell EMC Isilon Credentials .....	242
Dell EMC Isilon Advanced Options .....	243
Dell EMC Unity Credentials .....	246
Dell EMC Unity Advanced Options .....	247
Dell EMC VNX/Celerra Credentials .....	250
Dell EMC VNX/Celerra Advanced Options .....	251
NetApp 7-Mode Configurations .....	253
NetApp 7-Mode Advanced Options .....	257
NetApp cDOT Configurations .....	259
NetApp cDOT Advanced Options .....	263
Nutanix Files Configurations .....	266
Nutanix Files Advanced Options .....	269
<b>Real-time Event Detection Preferences .....</b>	<b>271</b>
<b>User Management .....</b>	<b>272</b>
Managing Web Client Users .....	274
Managing Internal Users .....	274
Managing Active Directory Users .....	278
Configuring Active Directory Authentication .....	281
Managing Web Roles .....	283
Creating a Custom Web Role .....	283
Editing and Deleting Web Roles .....	287
Assigning Tags to Web Roles .....	288
<b>Cloud Backup and Replication Jobs .....</b>	<b>288</b>
<b>Overview .....</b>	<b>288</b>
<b>Before You Create Your First Cloud Backup and Replication Job .....</b>	<b>289</b>
<b>Creating a Cloud Backup and Replication Job .....</b>	<b>289</b>
Step 1: Job Type and Name .....	290
Step 2: Source Storage Platform .....	292
Step 3: Management Agent .....	293
Step 4: Proxy Configuration .....	294
Step 5: Storage Information .....	300
NetApp ONTAP   Clustered Data ONTAP .....	301
NetApp Data ONTAP 7-Mode .....	303
Dell EMC Isilon .....	305
Dell EMC Unity .....	306
Dell EMC Celerra   VNX   VNX 2 .....	308
Nutanix Files .....	310
Step 6: Source Paths .....	312
Step 7: File and Folder Filters .....	313
Step 8: Destination .....	314
Step 9: Destination Credentials .....	316
Azure Blob Storage Credentials .....	316
Amazon S3 Credentials .....	318
NetApp StorageGRID Credentials .....	320
Nutanix Objects Credentials .....	321
Step 10: Container or Bucket Details .....	322
Azure Blob Storage Container Details .....	323
Amazon S3 Bucket Details .....	325
NetApp StorageGRID Bucket Details .....	327

Nutanix Objects Bucket Details.....	329
Step 11: Replication and Retention Policy .....	331
Step 12: Replication Schedule.....	332
Scheduled Scans .....	333
Batched Real-Time .....	335
Continuous Data Protection.....	336
Step 13: Retention.....	337
Step 14: Source Snapshots.....	338
Step 15: Miscellaneous Options.....	339
Step 16: Email Alerts .....	342
Step 17: SNMP Notifications.....	344
Step 18: Confirmation.....	346
<b>Running a Cloud Backup and Replication Job .....</b>	<b>348</b>
Starting a Cloud Backup and Replication Job.....	348
Stopping a Cloud Backup and Replication Job.....	350
<b>Monitoring Cloud Backup and Replication Jobs .....</b>	<b>351</b>
<b>Deleting a Cloud Backup and Replication Job .....</b>	<b>352</b>
<b>Recovering Data .....</b>	<b>353</b>
Search Options .....	356
Search by Name .....	356
Search by Snapshot .....	359
Search by Point in Time.....	360
Search by Latest Replication.....	362
Recovery Options .....	362
<b>DFS-N Management Jobs .....</b>	<b>366</b>
<b>Overview .....</b>	<b>367</b>
<b>Namespace Elements .....</b>	<b>367</b>
<b>Getting Started with DFS Namespaces .....</b>	<b>368</b>
<b>Creating a DFS-N Management Job .....</b>	<b>368</b>
Step 1: Job Type.....	369
Step 2: Management Agent.....	370
Step 3: Agent Verification.....	371
Step 4: Namespace Name.....	373
Step 5: Namespace Servers.....	374
Step 6: Namespace Settings.....	376
Step 7: Namespace Folders.....	378
Step 8: Email Alerts .....	382
Step 9: SNMP Notifications.....	384
Step 10: Review .....	385
Step 11: Results.....	386
<b>Importing an Existing Namespace .....</b>	<b>388</b>
<b>Running a DFS-N Management Job .....</b>	<b>396</b>
Starting a DFS-N Management Job.....	396
Stopping a DFS-N Management Job.....	397
<b>Managing DFS Namespaces .....</b>	<b>398</b>
Adding a Namespace Server.....	398
Adding a Namespace Folder.....	402
Adding a Namespace Folder Target.....	408
<b>Connecting DFS Namespaces with File Collaboration and File Synchronization Jobs .....</b>	<b>412</b>
Creating a File Collaboration or File Synchronization Job from a DFS Namespace Folder .....	413
Linking a Namespace Folder with an Existing File Collaboration or File Synchronization Job.....	423
<b>File Collaboration Jobs .....</b>	<b>431</b>

<b>Overview .....</b>	<b>431</b>
<b>Before You Create Your First File Collaboration Job .....</b>	<b>431</b>
<b>Creating a File Collaboration Job .....</b>	<b>432</b>
Step 1: Job Type and Name .....	432
Step 2: Participants .....	434
Participants .....	435
Storage Platform .....	435
Management Agent .....	436
Storage Information .....	437
NetApp ONTAP   Clustered Data ONTAP .....	438
NetApp Data ONTAP 7-Mode .....	440
Dell EMC Isilon .....	441
Dell EMC Unity .....	442
Dell EMC Celerra   VNX   VNX 2 .....	444
Nutanix Files .....	445
Path .....	447
Step 3: File Metadata .....	449
Step 4: Application Support .....	451
Step 5: Email Alerts .....	452
Step 6: Save Job .....	455
<b>Editing a File Collaboration Job .....</b>	<b>456</b>
Participants .....	458
Adding and Deleting Participants .....	459
Modifying Participant Attributes .....	461
Modifying Participant Detector Settings .....	463
General .....	466
File and Folder Filters .....	468
Scheduled Replication .....	469
Conflict Resolution .....	470
Delta Replication .....	472
File Metadata .....	475
File Locking .....	477
Application Support .....	478
Logging and Alerts .....	479
Target Protection .....	482
Email Alerts .....	484
SNMP Notifications .....	486
Tags .....	487
DFS-N .....	488
Editing Multiple Jobs .....	489
<b>Running and Managing a File Collaboration Job .....</b>	<b>491</b>
Overview .....	492
Job Initialization Process .....	492
Initial Synchronization Process .....	492
Starting a File Collaboration Job .....	493
Stopping a File Collaboration Job .....	495
Auto-Restarting a File Collaboration Job .....	495
Host Connectivity Issues .....	497
Removing a File from Quarantine .....	498
Manual Retries .....	499
<b>File Replication Jobs .....</b>	<b>500</b>
<b>Overview .....</b>	<b>500</b>
<b>Before You Create Your First File Replication Job .....</b>	<b>500</b>
<b>Creating a File Replication Job .....</b>	<b>501</b>

Step 1: Job Type and Name.....	501
Step 2: Storage Platform.....	503
Step 3: Source Agent.....	503
Step 4: Storage Information.....	504
NetApp ONTAP   Clustered Data ONTAP.....	505
NetApp Data ONTAP 7-Mode.....	507
Dell EMC Isilon .....	508
Dell EMC Unity .....	509
Dell EMC Celerra   VNX   VNX 2.....	511
Nutanix Files .....	512
Step 5: Source Path.....	513
Step 6: Destination Agent.....	515
Step 7: Destination Path.....	516
Step 8: File Metadata.....	517
Step 9: Email Alerts .....	519
Step 10: Save Job.....	521
<b>File Synchronization Jobs .....</b>	<b>522</b>
<b>Overview .....</b>	<b>522</b>
<b>Before You Create Your First File Synchronization Job .....</b>	<b>523</b>
<b>Creating a File Synchronization Job .....</b>	<b>523</b>
Step 1: Job Type and Name.....	523
Step 2: Participants .....	525
Participants .....	526
Storage Platform .....	526
Management Agent .....	527
Storage Information .....	528
NetApp ONTAP   Clustered Data ONTAP.....	529
NetApp Data ONTAP 7-Mode.....	531
Dell EMC Isilon .....	532
Dell EMC Unity .....	533
Dell EMC Celerra   VNX   VNX 2.....	535
Nutanix Files .....	536
Path .....	538
Step 3: File Metadata.....	540
Step 4: Email Alerts .....	542
Step 5: Save Job.....	544
<b>Editing a File Synchronization Job .....</b>	<b>545</b>
Participants .....	547
Adding and Deleting Participants .....	548
Modifying Participant Attributes .....	550
Modifying Participant Detector Settings .....	552
General .....	555
File and Folder Filters .....	557
Scheduled Replication.....	558
Conflict Resolution.....	559
Delta Replication .....	561
File Metadata .....	563
File Locking .....	566
Application Support.....	567
Logging and Alerts.....	568
Target Protection.....	571
Email Alerts .....	573
SNMP Notifications .....	575
Tags .....	576

DFS-N .....	576
Editing Multiple Jobs.....	577
<b>Running and Managing a File Synchronization Job .....</b>	<b>579</b>
Overview .....	579
Job Initialization Process.....	580
Initial Synchronization Process.....	580
Starting a File Synchronization Job.....	581
Stopping a File Synchronization Job.....	583
Auto-Restarting a File Synchronization Job.....	583
Host Connectivity Issues.....	584
Removing a File from Quarantine.....	585
Manual Retries .....	586
<b>PeerSync Management Jobs .....</b>	<b>587</b>
<b>Creating a PeerSync Management Job .....</b>	<b>587</b>
Before You Create Your First PeerSync Management Job.....	588
Email Alerts .....	588
Integrating Existing PeerSync Instances.....	591
Requirements .....	591
How To .....	591
Deploying New PeerSync Instances.....	592
Requirements .....	592
How To .....	592
Step 1: General Information.....	593
Step 2: PeerSync Profile.....	594
Step 3: Jobs Configuration List.....	596
Step 4: Installation Settings.....	597
Logging and Alerts.....	600
Email Alerts .....	601
<b>Running and Managing a PeerSync Management Job .....</b>	<b>602</b>
Starting and Stopping.....	603
PeerSync Management Summary .....	604
PeerSync Management Dashboard Summary View .....	607
Managing the PeerSync Profile.....	608
Updating a Profile Configuration.....	609
Importing an Existing Profile.....	610
Editing and Configuring Jobs .....	611
Editing Global Settings .....	614
Distributing a Profile .....	615
Managing the PeerSync Service.....	616
Runtime Job Views .....	617
Summary View .....	618
PeerSync Jobs Stats.....	620
Added Files .....	620
Updated Files .....	621
Deleted Files .....	622
Messages .....	623
Failed Events View .....	624
Monitoring Log View .....	624
Alerts View .....	625
Participants View .....	626
Configuration View .....	628
Upgrade/Reprocess Installation.....	629

**Index****631**

# Peer Global File Service Help

## Using This Help File

This help is designed to be used online. It is cross-linked so that you can find more relevant information to any subject from any location. If you prefer reading printed manuals, a PDF version of the entire help is available from our website. This may be useful as a reference, but you will probably find that the active hyperlinks, cross-references, and active index make the on-screen electronic version of this document much more useful.

## Trademark Information and Copyright

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.. Although we try to provide quality information, Peer Software makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Peer Software, Peer Management Center, and their respective logos are registered trademarks of Peer Software Inc. Microsoft, Azure, Windows, Windows Server, and their respective logos are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. NetApp, the NetApp logo, Data ONTAP, and FPolicy are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. "Amazon Web Services", "AWS", "Amazon S3", "Amazon Simple Storage Service", "Amazon SNS", "Amazon Simple Notification Service", and their respective graphics, logos, and service names are trademarks, registered trademarks or trade dress of Amazon Web Services LLC and/or its affiliates in the U.S. and/or other countries. Dell, EMC, Celerra, Isilon, VNX, Unity and other trademarks are trademarks of Dell Inc. or its subsidiaries. Nutanix is a trademark of Nutanix, Inc., registered in the United States and other countries. All other trademarks are the property of their respective companies. Peer Software Inc. vigorously protects and defends its trade name, trademarks, patents, designs, copyrights, and other intellectual property rights. Unless otherwise specified, no person has permission to copy, redistribute, reproduce, or republish in any form the information in this document.

Last updated: Thursday, May 13, 2021

Version: 4.6.0

## Terminology

### Introduction

Before getting started, it is important to have a good understanding of key concepts and terminology used throughout this help system.

## Terms

Term	Definition
<b>Active-Active</b>	Two or more file servers that hosts data sets that are in active use, as opposed to an active-passive environment where only one file server hosts active data. Made possible by real-time file synchronization to keep all file servers in sync.
<b>Agent</b>	See <i>Peer agent</i>
<b>Cloud Backup and Replication job</b>	A job type where a single participating host has a designated set of folders and files to be replicated to a cloud storage device.
<b>DFS (Distributed File System)</b>	A set of client and server services that allow an organization using Microsoft Windows servers to organize many distributed SMB file shares into a distributed file system.
<b>DFS namespace (DFS-N)</b>	A namespace that enables you to group shared folders located on different servers into one or more logically structured namespaces.
<b>DFS Namespaces</b>	A Windows Server feature that allows multiple SMB shares across different file servers (and even locations) to be combined into a single unified namespace. DFS Namespaces simplifies access to files, especially in large, distributed environments. When combined with Peer file synchronization technology, DFS Namespaces can provide redundancy to file shares across file servers and locations.
<b>DFS-N Management job</b>	A type of job that enables the creation and management of DFS namespaces.
<b>Event</b>	A single operation performed by a user on a file server.
<b>Failback</b>	The process of redirecting previously displaced users from a secondary file server back to the primary after a failure state has been resolved.



Term	Definition
<b>Failover</b>	The process of redirecting users from one file server to a secondary in the event of a failure.
<b>File access event</b>	An event that is triggered from the opening or closing of a file.
<b>File change event</b>	An event that causes a file to be changed in some way, for example, file modify, file delete, file rename, file attribute change.
<b>File Collaboration job</b>	A type of job that combines file synchronization with distributed file locking to prevent version conflicts across multiple active file servers.
<b>File Collaboration session</b>	A communication session made up of two or more hosts, each with a designated root of folders and files that are to be shared or collaborated on. A collaboration session coordinates the primary functions of file locking and synchronization.
<b>File filter</b>	A type of filter used to include or exclude specific files from replication and locking.
<b>File lock conflict</b>	A file collaboration condition that exists when two users open a file at the same time, and both hold exclusive locks on the file.
<b>File Replication job</b>	A type of job that involves real-time and/or scheduled copying of files and folders from one file server to another.
<b>File Synchronization job</b>	A type of job that involves multi-directional real-time replication so that two or more file servers are always up to date with each other.
<b>Filter</b>	Three types of filters: file, folder, and list.
<b>Filter expression</b>	See <i>list filter</i> .

Term	Definition
<b>Folder filter</b>	A type of filter used to include or exclude specific folders (and the files they contain) from replication and locking.
<b>Heartbeat</b>	A communication mechanism used between Peer Management Center and all connected Peer Agents to ensure that Peer Agents are alive and responsive. Heartbeats share information about the Peer Agent host server with Peer Management Center, aid in verifying when a Peer Agents is no longer available, and signal when a disconnected Peer Agent has reconnected. All heartbeat information is sent through the Peer Management Broker.
<b>Host (also host participant or participating host)</b>	A server that a Peer Agent is installed upon. When active in a job, it is called the host participant or participating host.
<b>Initialization process</b>	The steps executed whenever a job is started in Peer Management Center. The steps for an initialization process are different for each job type.
<b>Initial synchronization process</b>	The background process that occurs at the start of a file collaboration session, where the directory watch set is recursively scanned on all participating hosts, file conflict resolution is performed, and any files that require updating are synchronized with the most current copy of the file.
<b>List filter</b>	A type of filter used to show or hide information from various views in Peer Management Center.
<b>Management Agent</b>	A server running the Peer Agent. Can manage storage devices or a DFS namespace.
<b>Master host</b>	In file synchronization and collaboration, the master host will always win in a split-brain scenario.
<b>Malicious Event Detector (MED)</b>	Leverages the same real-time event detection that powers all job types to detect and alert administrators to malicious user and application behavior. For more information, see: <a href="https://kb.peersoftware.com/tb/introduction-to-peer-med">https://kb.peersoftware.com/tb/introduction-to-peer-med</a> .

Term	Definition
<b>Participant</b>	A participant consists of an Agent and the volume/share/folder to be replicated. The server that the Agent is installed upon is called the host participant or simply host. Applies to File Collaboration, File Replication, and File Synchronization jobs.
<b>Peer Agent (or Agent)</b>	A lightweight piece of software that is installed on Windows Servers to perform the storage and file management functions used by the entire Peer Global File Service solution suite. Typically installed on or alongside the file servers that will be managed by Peer Management Center.
<b>Peer Management Center (PMC)</b>	The focal component of Peer Global File Service. Responsible for configuration, management, and monitoring of Peer Agents and the various solutions configured in Peer Global File Service. Peer Management Center runs as three parts: a Windows Service that is always running, along with a rich client application and a web server component, both used for configuration and monitoring.
<b>Peer Management Broker</b>	The central messaging system of Peer Global File Service. The Peer Management Broker serves to connect Peer Management Center and Peer Agents, forming a Peer Management Center "network" that can be cast over local or wide-area networks via TCP/IP. One or more Peer Management Brokers are deployed in a Peer Management Center environment.
<b>Quarantined file</b>	A file that has been removed from a File Collaboration or File Synchronization job as a result of a lock or replication conflict that could not be automatically resolved. This file will not be deleted from any location but will be ignored while it remains in quarantine. An administrator or help desk user must manually remove files from quarantine.
<b>Quorum</b>	Requirement for a minimum of two participants must be available and connected. If that number dips to one or less, quorum will not be met. Applies to File Collaboration, File Replication, and File Synchronization jobs.
<b>Real-time event detection</b>	A key technology that backs all job types in Peer Management Center. Peer Management Center receives notifications as end users interact with the file servers that are being monitored. These notifications will usually result in replication or locking between file servers.
<b>Scan</b>	The initial process of comparing data sets on two or more file servers to ensure that they match. As differences are discovered, replication will

Term	Definition
	occur to bring each file server "in sync" with one another.
<b>Seeding target</b>	Smart data seeding helps to efficiently integrate a host that has been disconnected for a long period of time or a new host into a File Collaboration job. Such existing hosts or new hosts with pre-seeded data (using methods like shipping a drive or server) should be set as Seeding Targets within a collaboration job. When the scan starts, non-Seeding Targets will become the masters and bring the Seeding Targets up to date. Stale updates, deletes, and renames will NOT be brought back from the Seeding Targets. All local real-time activity will be quarantined. Once that initial scan is complete, the Seeding Targets will become full participants with real-time enabled. For more information on Smart Data Seeding and its potential options, see <a href="#">Smart Data Seeding</a> or contact support@peersoftware.com.
<b>SMB/CIFS</b>	Server Message Block or Common Internet File System, an application-layer protocol used for providing shared access to file data and other networked resources.
<b>Source host</b>	The file server hosting a file from which file access or change event originated.
<b>Target host</b>	One or more Management Agents of file servers where file access and change events will be propagated to.
<b>TLS</b>	Transport Layer Security, a successor to Secure Socket Layer (SSL) that secures network traffic between a client and server.
<b>UNC Path</b>	A UNC path can be used to access network resources and MUST be in the format specified by the Universal Naming Convention. A UNC path always starts with two backslash characters (\\).
<b>View</b>	Individual sections of Peer Management Center's user interface, each providing unique information and control.  Examples: Main view, Jobs view, Agent Summary view, Alerts view, Job Alerts view.
<b>Volume Shadow Copy</b>	Shadow Copy is a technology included in Microsoft Windows that allows taking manual or automatic snapshots of computer files or volumes, even

Term	Definition
<b>Service (VSS)</b>	when they are in use. It is implemented as a Windows service called the Volume Shadow Copy service.
<b>Watch set</b>	The root folder and all subfolders on a file server that are being scanned and/or monitored by a File Collaboration, File Replication, File Synchronization, or Cloud Backup and Replication job.

## Installation and Configuration

This topics in this section provide information about:

[Requirements and Prerequisites](#)

[Installing Peer Management Center](#)

[Installing Peer Agents](#)

[Updating Peer Management Center and Peer Agents](#)

[Configuring and Managing the Web and API Services](#)

For information about Peer Global File System licensing, see [Licensing](#).

## Requirements and Prerequisites

Before you get started, review the environmental requirements and platform prerequisites for using Peer Global File Service:

- [Peer Global File Service environmental requirements](#)
- [Dell EMC Prerequisites](#)
- [NetApp Prerequisites](#)
- [Nutanix Prerequisites](#)

### Dell EMC Prerequisites

In addition to the standard [Peer Global File Service environmental requirements](#), the following prerequisites must be met:

- [Dell EMC Isilon Prerequisites](#)
- [Dell EMC Unity Prerequisites](#)
- [Dell EMC Celerra | VNX | VNX 2 Prerequisites](#)

### CEE Server Configuration

See the following guides for steps on setting up a CEE Server on which the Peer Agent will be running:

- [Dell EMC Isilon Configuration Guide](#)
- [Dell EMC Unity Configuration Guide](#)
- [Dell EMC Celerra | VNX | VNX 2 Configuration Guide](#)

### NetApp Prerequisites

In addition to the standard [Peer Global File Service environmental requirements](#), the following prerequisites must be met:

- [NetApp Data ONTAP 7-Mode Prerequisites](#)
- [NetApp ONTAP | Clustered Data ONTAP Prerequisites](#)

### Nutanix Prerequisites

In addition to the standard [Peer Global File Service environmental requirements](#), the following prerequisites must be met:

- [Nutanix Files prerequisites](#)

## Installing Peer Management Center

### Overview

Peer Management Center (PMC) can be installed in numerous ways based on your needs and environment. Peer Management Center installation consists of two separate installers, both of which are available for download from the Peer Software website:

- **Peer Management Center installer:** This installer installs both Peer Management Center and [Peer Management Broker](#) on the same server. Peer Management Broker handles the communication between Peer Management Center and Peer Agents. See [Installing and Launching Peer Management Center](#) for installation instructions.
- **Peer Agent installer:** This installer contains the Peer Agent installation files. You must install an Agent on each server you plan to include in any of your jobs. See [Installing Peer Agents](#) for installation instructions.

Before installing Peer Management Center, see [Requirements and Prerequisites](#) to verify that your environment satisfies the requirements and prerequisites.

## Installing and Launching Peer Management Center

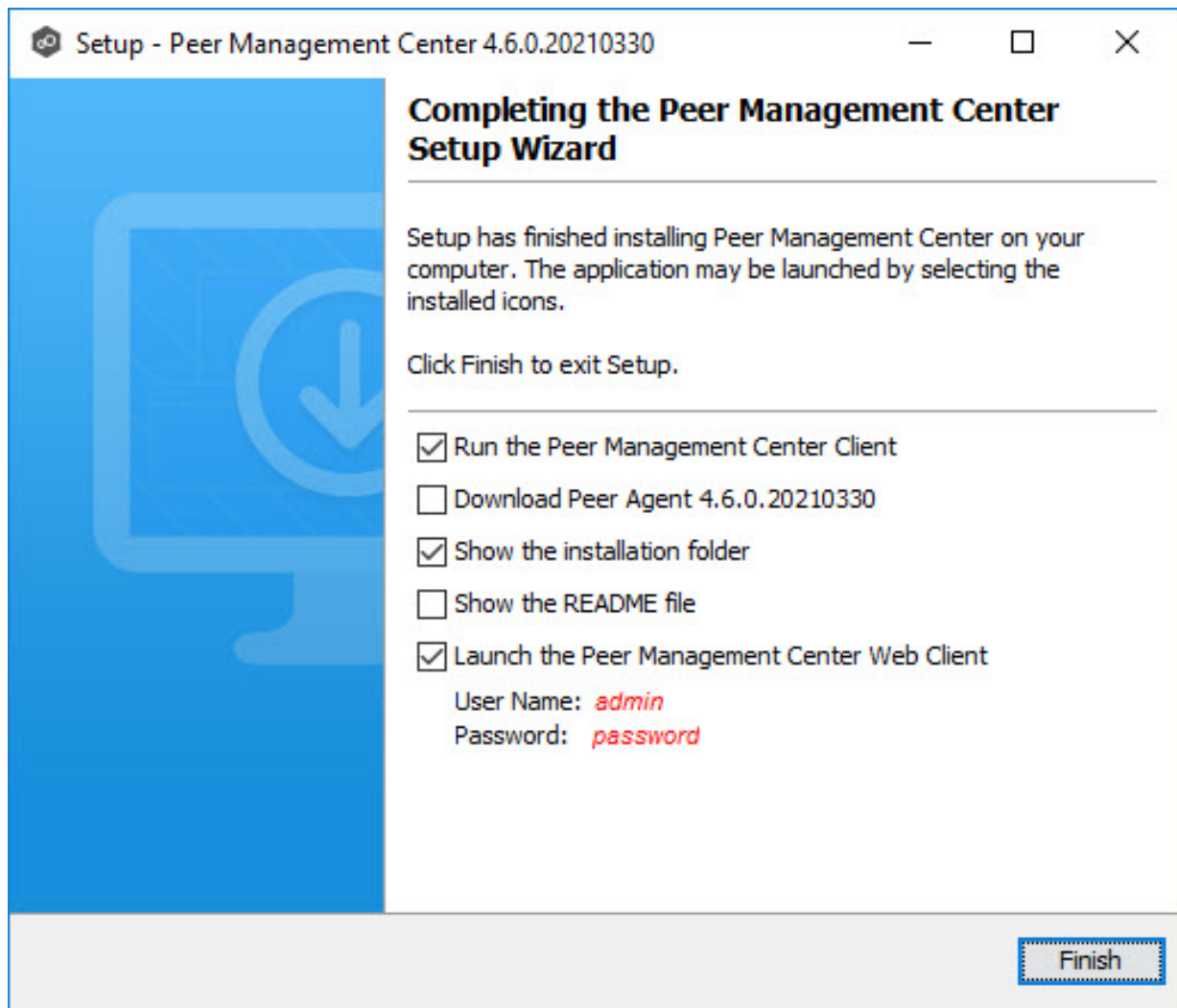
To install and launch Peer Management Center and Peer Management Broker:

1. Download the Peer Management Center installer (**PMC\_Installer\_win64.exe**) to the server you want to host Peer Management Center.
2. Run the installer and follow the installation wizard instructions.

During the installation, you will be prompted to configure access to the **Peer Management Center Web Service** and the **Peer Management API Service**. The web service allows users to access Peer Management Center via a web browser; the API service allows access to Peer Management Center through REST API calls. For detailed instructions on configuring access to these services, see [Configuring the Web and API Services](#).

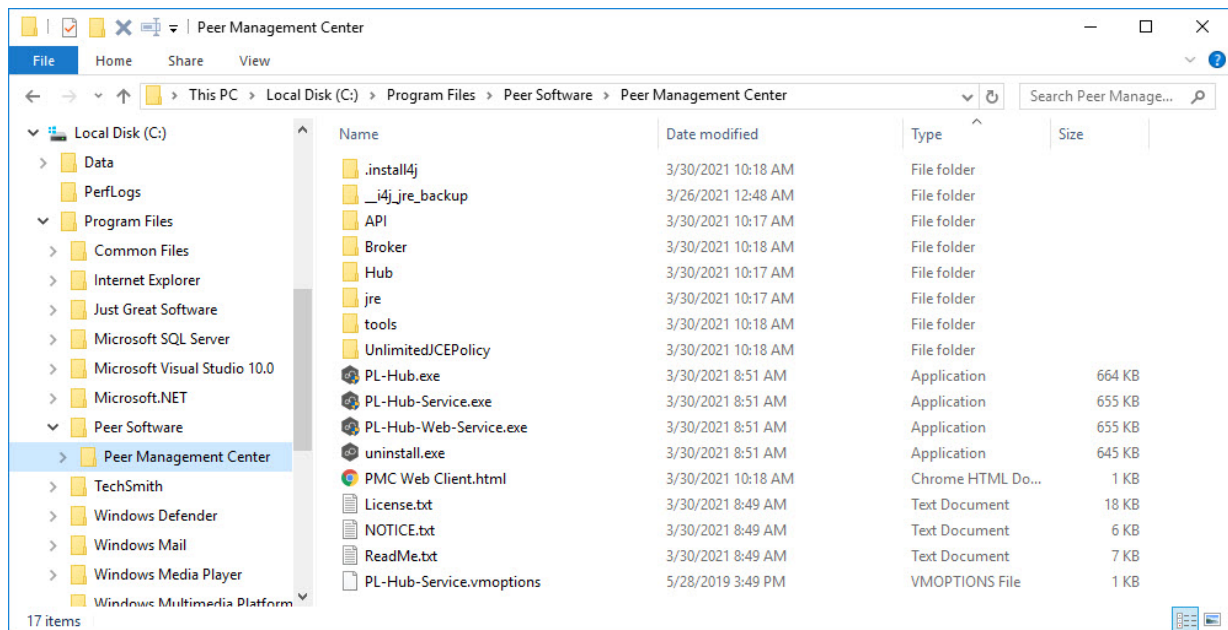
3. On the final page of the installation wizard, you have several options; we recommend that, at minimum, you select the first option.

If you enabled the Peer Management Web Service and selected the **Launch the Peer Management Center Web Client**, on the final page of the installation wizard, the default username and password for accessing the web client is displayed. After [logging in to the web client](#), you should [change the password](#) immediately.



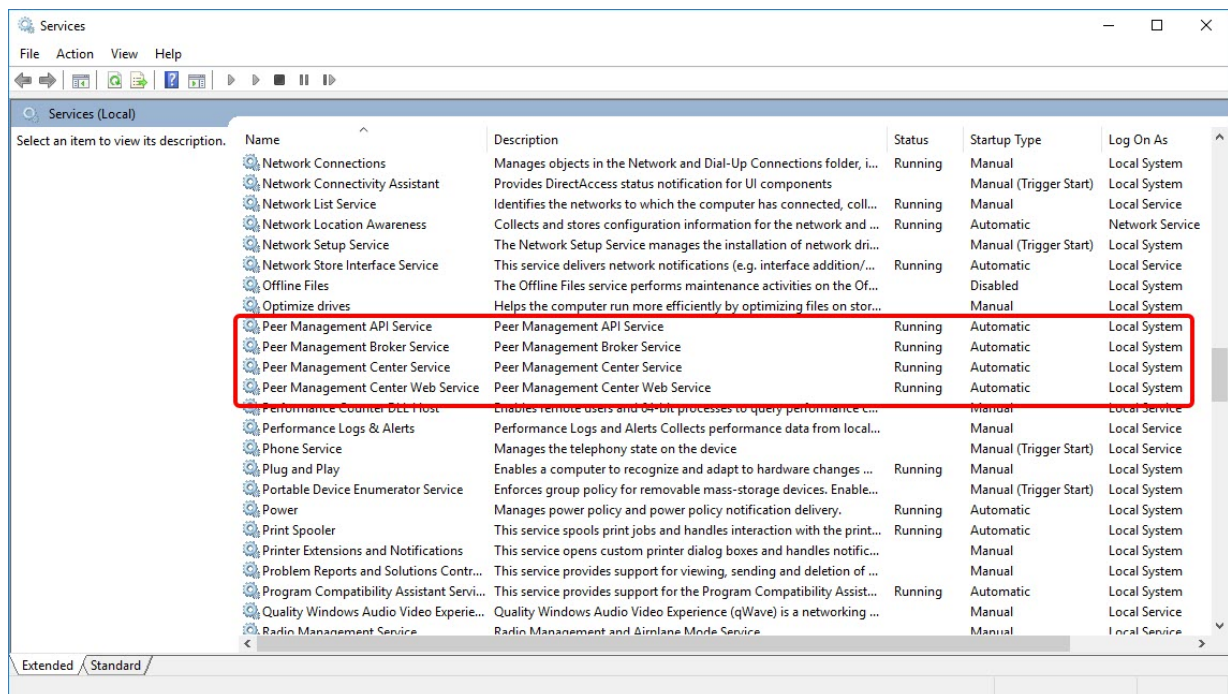
When the installation is complete, the Peer Management Center installation folder contains the following files and folders:





The **PL-Hub.exe** executable launches **Peer Management Center Client**, which is a Windows rich client application.

Four Windows services have been installed and are set to auto-start:

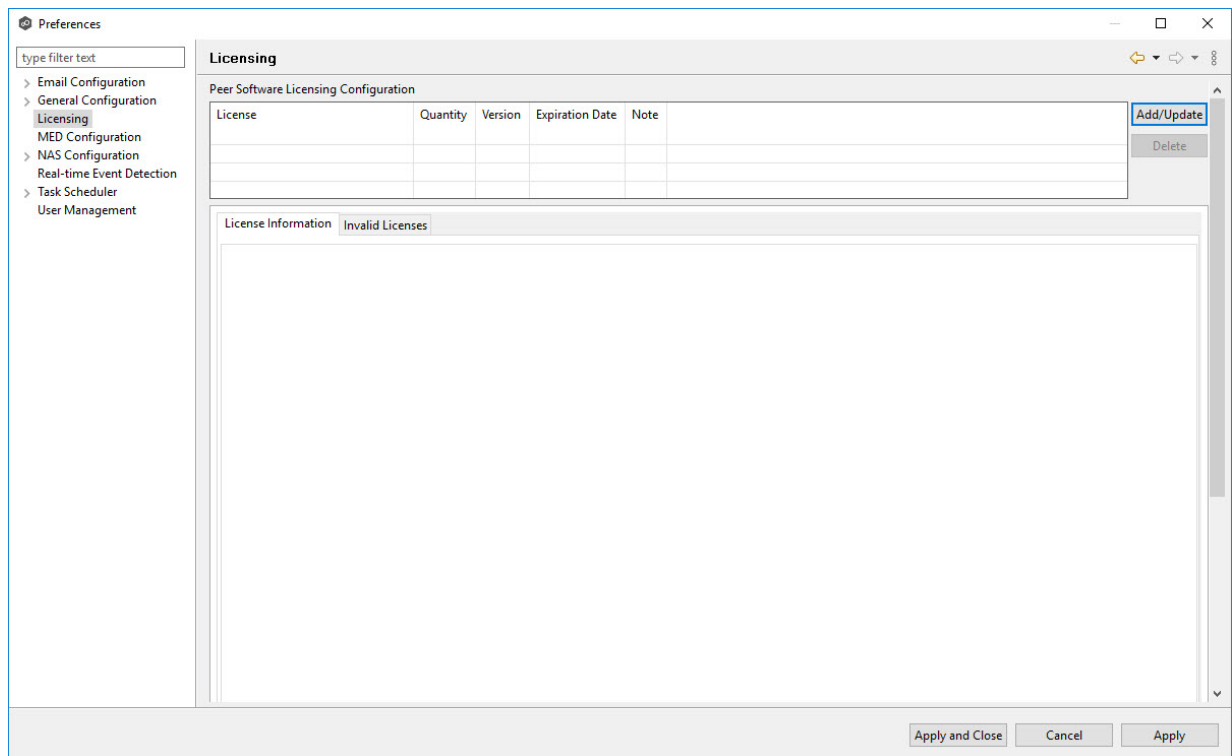


- If you didn't select the option to launch Peer Management Center Client on the last page of the installation wizard, launch it using one of the following methods:

- Select **Peer Management Center** from the Windows **Start** menu.
- Double-click the **PL-Hub.exe** executable in the Peer Management Center installation directory.

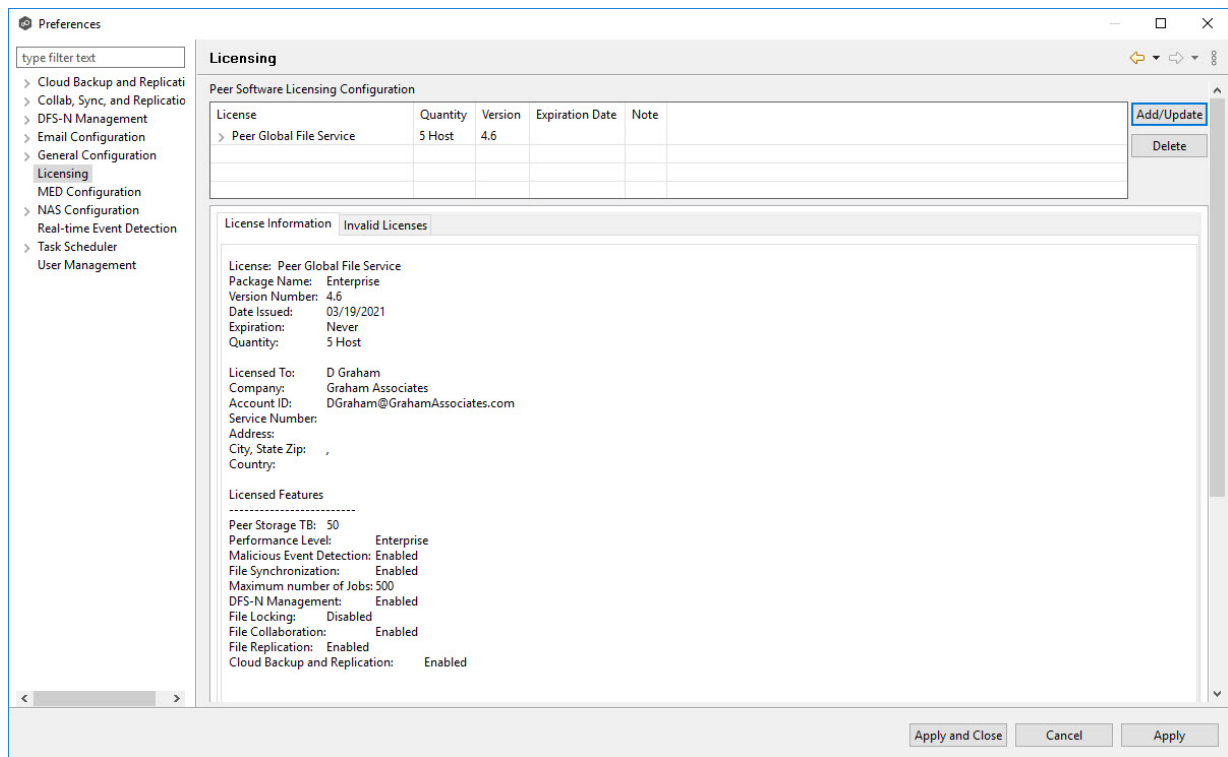
If both the **Peer Management Center Service** and the **Peer Management Broker Service** are up and running as background services, then Peer Management Center should successfully start. If not, open the Windows Service Panel (services.msc) and start both services.

5. When launching Peer Management Center Client for the first time, you are prompted to install your license. If you haven't already done so, copy the license to the desktop of the Peer Management Center server.

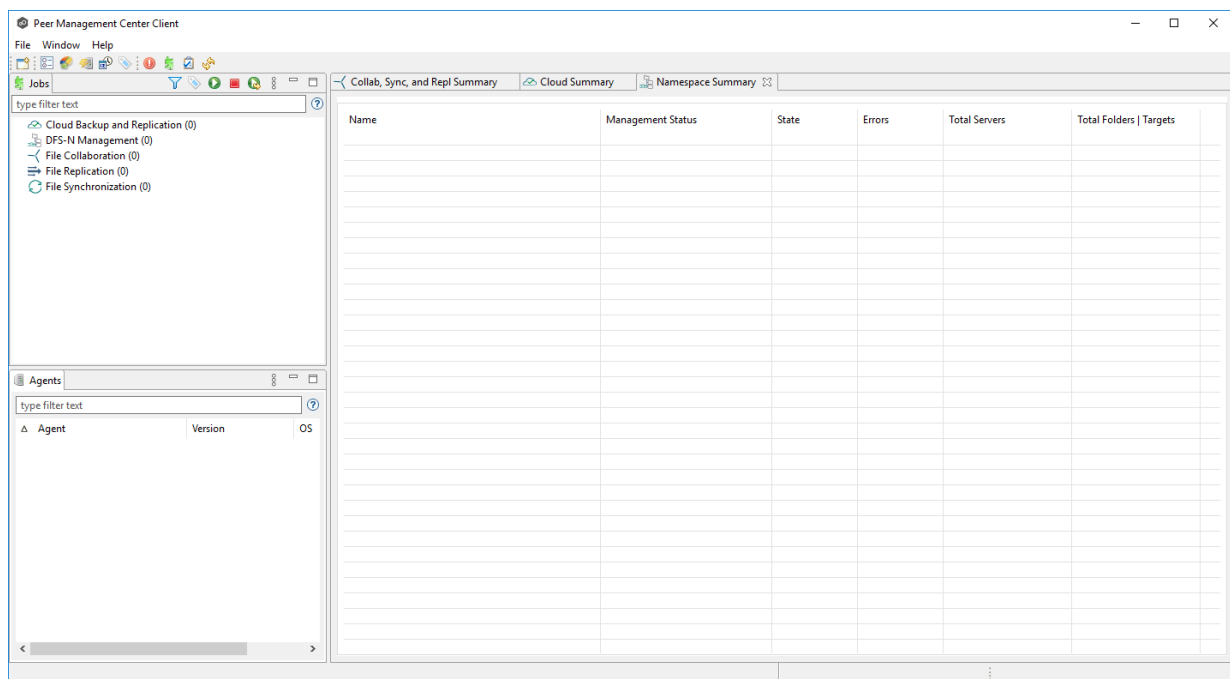


6. Click **Add/Update**.
7. Browse to where the License file is located and select the file.
8. Click **Open**.

The **License Information** tab displays your license information.



9. Click **Apply and Close**.



Now you are ready to [install the Peer Agents](#).

## Uninstalling Peer Management Center

Peer Management Center ships with an uninstaller for the environment it is running in. Please use the standard platform-specific method for removing programs/applications to uninstall Peer Management Center.

### Configuring and Managing the Web and API Services

As part of the [initial installation of Peer Management Center](#), you are prompted to configure access to the web and API services. The web service allows users to access Peer Management Center via a web browser; the API service allows access to Peer Management Center through REST API calls.

If you enable access to the web client, you will need to secure access to the web client and manage web client user accounts.

See the following topics for more information:

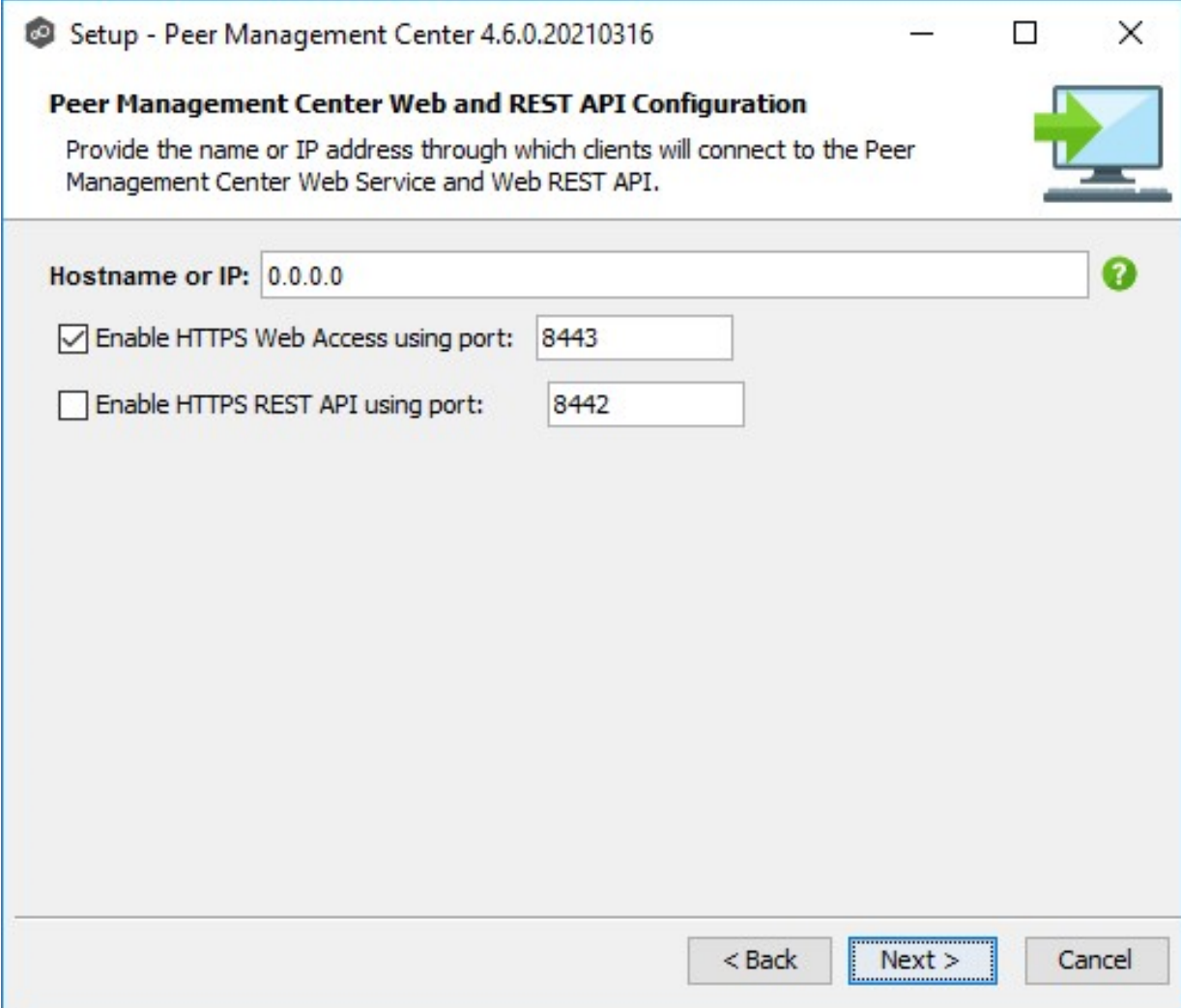
- [Configuring the Web and API Services](#)
- [Securing Access to the Web Client](#)
- [Accessing the Web Client](#)
- [Managing Web Client Users](#)

You can configure access to the web and API services during the [initial installation of Peer Management Center](#). If you do not enable access during the initial installation or want to modify settings at a later date, you can modify them through [Web and API Configuration](#) in [Preferences](#).

## Configuration Options

To configure the web and API services during the initial installation of Peer Management Center:

1. Enter the requested values when the configuration page appears in the installation wizard.



The screenshot shows a Windows-style window titled "Setup - Peer Management Center 4.6.0.20210316". The main heading is "Peer Management Center Web and REST API Configuration". Below the heading is a descriptive text: "Provide the name or IP address through which clients will connect to the Peer Management Center Web Service and Web REST API." To the right of the text is an icon of a computer monitor with a green arrow pointing towards it. The configuration area contains a text field labeled "Hostname or IP:" with the value "0.0.0.0" and a green question mark icon to its right. Below this are two checkboxes: "Enable HTTPS Web Access using port:" with a checked box and a text field containing "8443", and "Enable HTTPS REST API using port:" with an unchecked box and a text field containing "8442". At the bottom right are three buttons: "< Back", "Next >" (which is highlighted with a blue dashed border), and "Cancel".

Setup - Peer Management Center 4.6.0.20210316

### Peer Management Center Web and REST API Configuration

Provide the name or IP address through which clients will connect to the Peer Management Center Web Service and Web REST API.

Hostname or IP: 0.0.0.0 ?

☒ Enable HTTPS Web Access using port: 8443

☐ Enable HTTPS REST API using port: 8442

< Back Next > Cancel

**Hostname or IP**

Enter the hostname or IP address via which the services be can accessed:

- Enter **localhost** or **127.0.0.1** if you want the services to be accessible only to users of the local server via the loopback interface.
- Enter **0.0.0.0** to make the services accessible via all network interfaces.
- Enter a specific IP address to restrict access to a specific network interface.

**Enable HTTPS Web Access**

Select this to enable secure access to the web service, and then enter a port number.

<b>Enable HTTPS REST API</b>	Select this to enable secure access to the REST API service, and then enter a port number. The REST API port cannot be the same as the web service port.
------------------------------	--

2. Click **Next** to continue with the rest of the installation wizard.

Access to Peer Management Center's web client is through HTTPS, which ensures that all communication between the browser and the service hosting the web client is encrypted. However, you may want to take additional actions to secure access to Peer Management Center's web client:

- You can limit users' access to the web client when you configure the hostname or IP address for web access. For example, enter **localhost** or **127.0.0.1** if you want the web client to be accessible only to users of the local server via the loopback interface. See [Configuring the Web and API Services](#) for more details.
- While HTTPS access to the web client is secured out of the box with a built-in Transport Layer Security (TLS) certificate, this certificate can be swapped for a custom one. See [TLS Certificates](#) in [Advanced Topics](#) for information on using existing certificates and creating new certificates.
- The default password for the **admin** account should be changed immediately. See [Editing an Internal User](#) for information about changing the password.

## Installing Peer Agents

### Overview

You will need to install a Peer Agent on each server you plan to include in any of your jobs. After installing the Peer Agent software, you should verify that the **Peer Agent Service** is running and can successfully connect to the [Peer Management Broker](#).

### Installing a Peer Agent

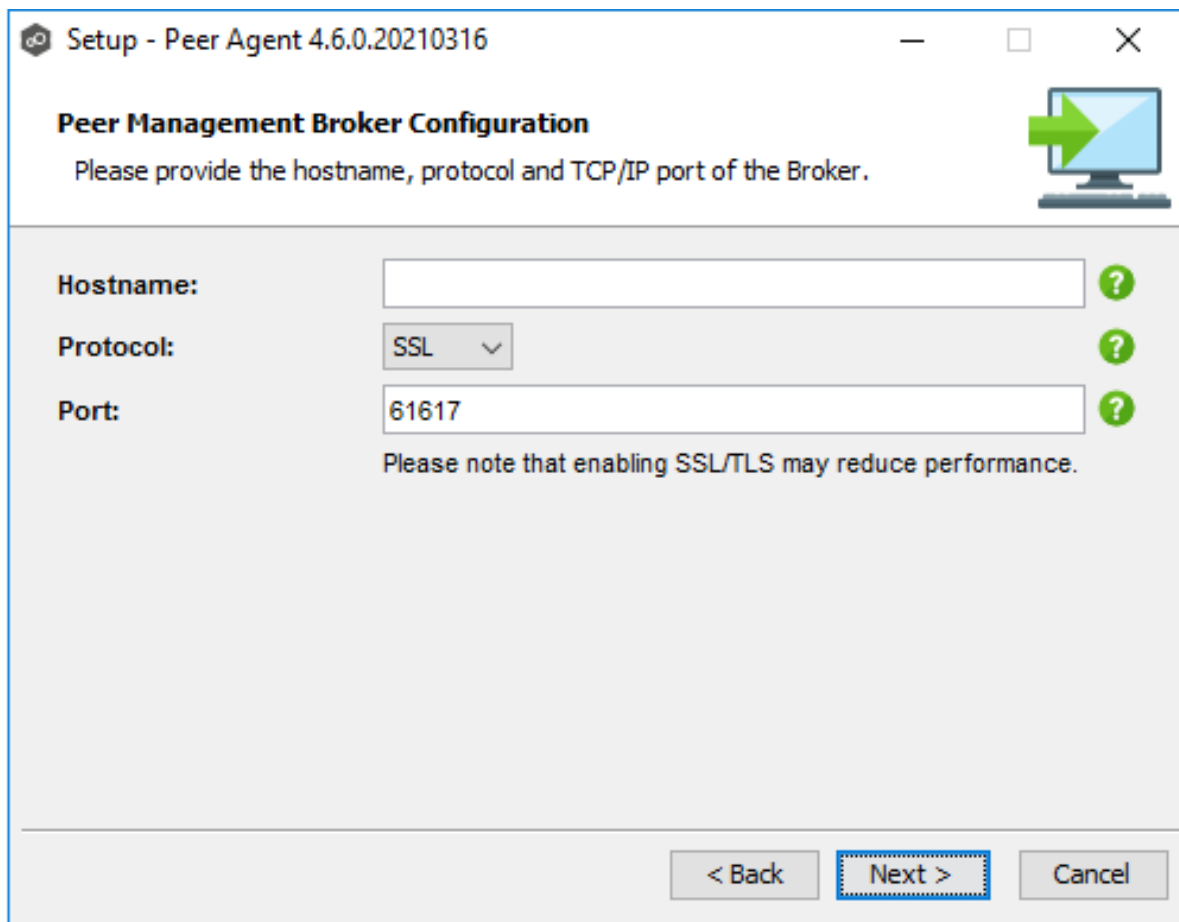
To install a Peer Agent and verify its connection to Peer Management Broker:

1. Download the Peer Agent installer (**P-Agent\_Installer\_win64.exe**) to the server you want to host the Agent.
2. Run the installer and follow the wizard instructions.

During installation, you will be prompted for:

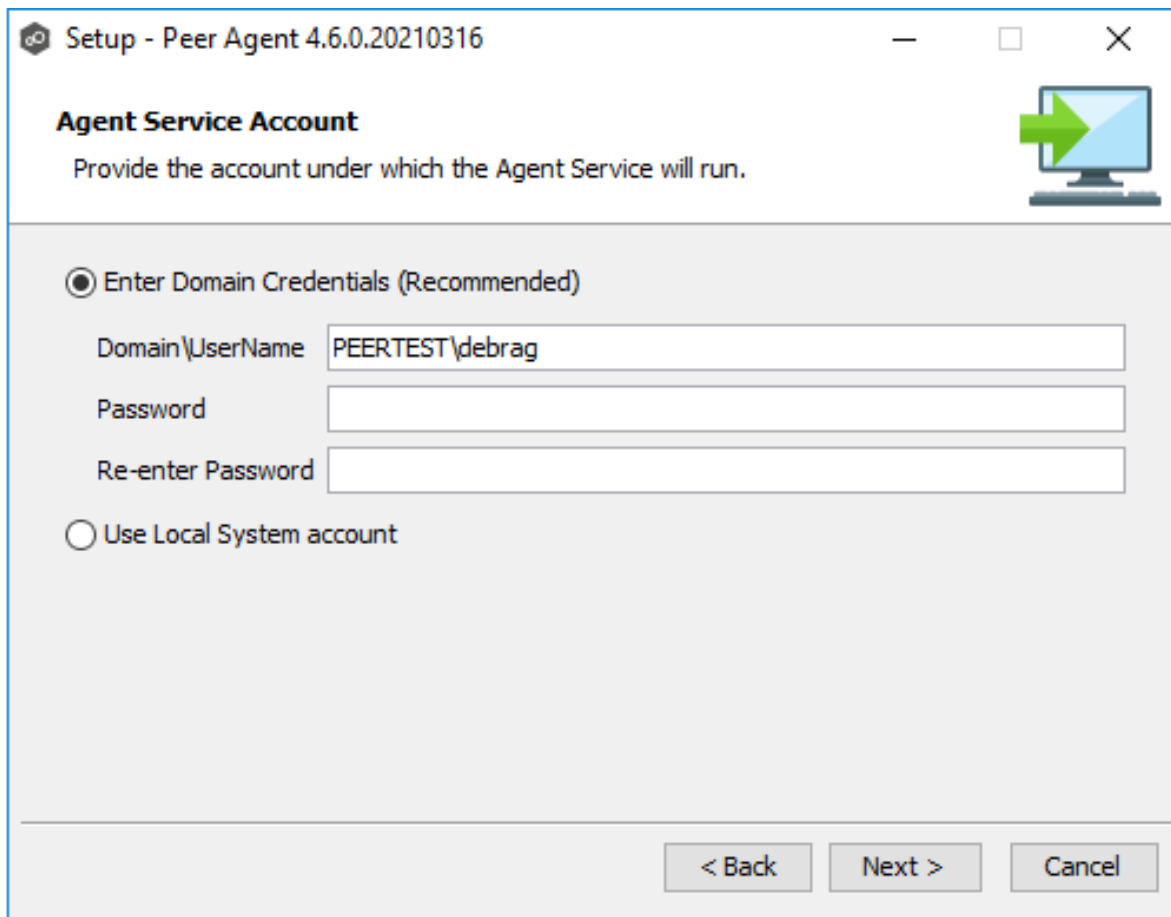
- The Peer Management Broker hostname (computer name, fully qualified domain name, or IP address) of the server where Peer Management Broker is running.
- The TCP/IP port number of the server where Peer Management Broker is running. The default port for TLS communication is 61617.

Enter the same values that you entered when [installing Peer Management Center and Peer Management Broker](#).



The screenshot shows a Windows installer window titled "Setup - Peer Agent 4.6.0.20210316". The main heading is "Peer Management Broker Configuration". Below the heading, it says "Please provide the hostname, protocol and TCP/IP port of the Broker." There is a green arrow icon pointing right. The form has three fields: "Hostname:" with an empty text box and a green question mark icon; "Protocol:" with a dropdown menu showing "SSL" and a green question mark icon; and "Port:" with a text box containing "61617" and a green question mark icon. Below these fields, a note states: "Please note that enabling SSL/TLS may reduce performance." At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

You will also need to provide the account credentials under which the Agent Service will run.



The screenshot shows a Windows-style window titled "Setup - Peer Agent 4.6.0.20210316". The window has standard minimize, maximize, and close buttons in the top right corner. The main content area is titled "Agent Service Account" and includes the instruction "Provide the account under which the Agent Service will run." To the right of this text is an icon of a computer monitor with a large green arrow pointing to the right. Below the instruction, there are two radio button options. The first option, "Enter Domain Credentials (Recommended)", is selected. It is followed by three text input fields: "Domain\UserName" containing "PEERTEST\debrag", "Password", and "Re-enter Password". The second option, "Use Local System account", is unselected. At the bottom right of the window, there are three buttons: "< Back", "Next >", and "Cancel".

Setup - Peer Agent 4.6.0.20210316

**Agent Service Account**  
Provide the account under which the Agent Service will run.

☒ Enter Domain Credentials (Recommended)

Domain\UserName: PEERTEST\debrag

Password:

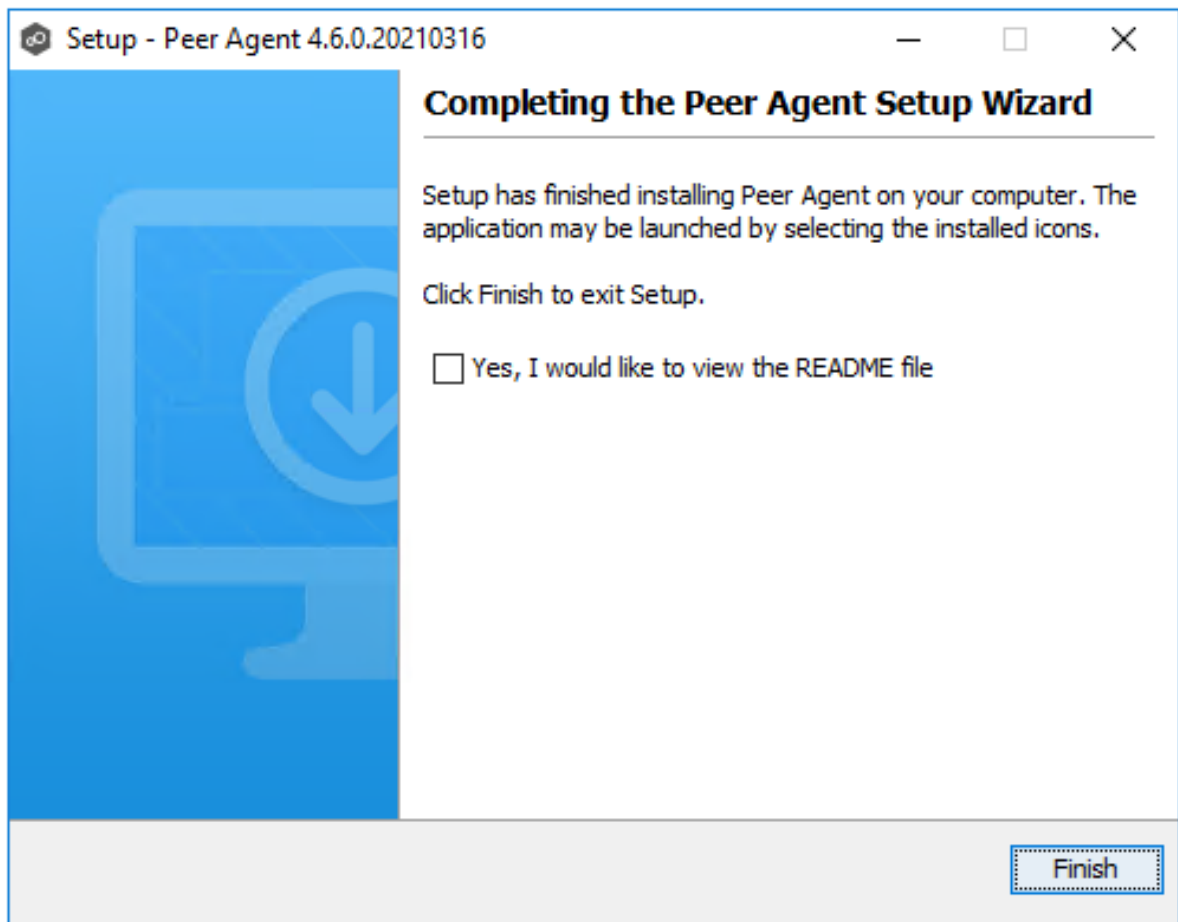
Re-enter Password:

☐ Use Local System account

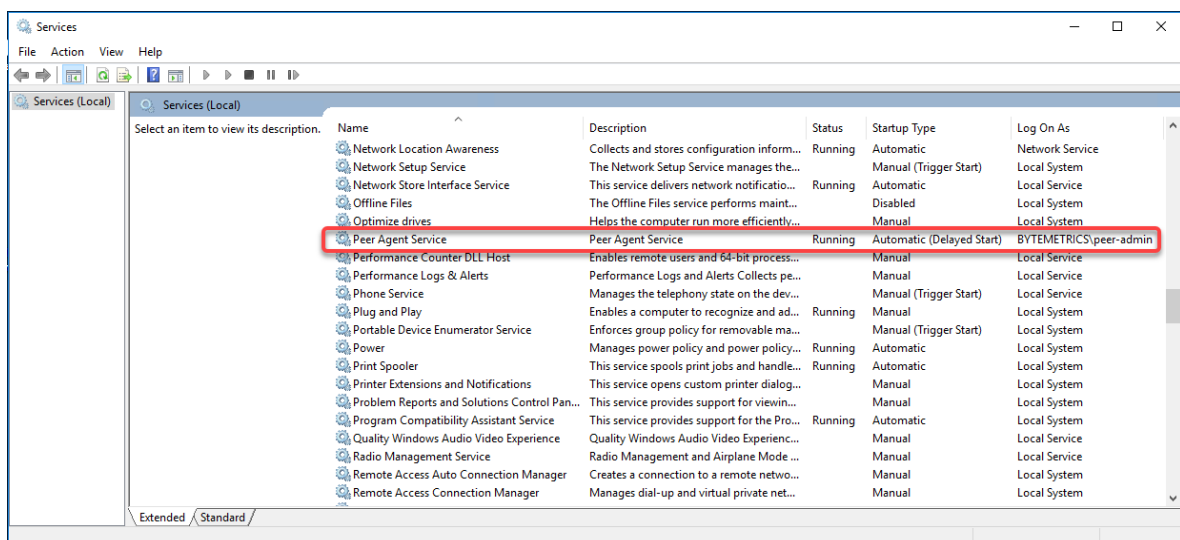
< Back   Next >   Cancel

- When the last page of the installation wizard appears, click **Finish**.





4. After the installation finishes, the Peer Agent is installed as a Windows service. You will need to verify that the **Peer Agent Service** is running, and that it was able to successfully connect to [Peer Management Broker](#). You can do this by opening the Windows Services Panel (services.msc) and verifying that the **Peer Agent Service** has started.



## Secure Encrypted TLS Connections

By default, the Peer Agent is installed with Transport Layer Security (TLS) encryption enabled, where the Peer Agent connects to Peer Management Broker through a secure, encrypted connection. If you are running Peer Management Center on a secure LAN or via a corporate VPN, you might want to disable TLS to boost performance. For more details on disabling or enabling encryption for the Peer Agent, see [Broker Configuration](#).

If AES-256 support is required, please contact [support@peersoftware.com](mailto:support@peersoftware.com) to obtain the necessary installers.

## Uninstalling a Peer Agent

Peer Agent ships with an uninstaller for the environment it is running in. Please use the standard platform-specific method for removing programs/applications to uninstall the Peer Agent.

## Updating Peer Management Center and Peer Agents

You can easily check for updates to the Peer Management Center software. Minor releases can be automatically downloaded and installed. Major releases require a new license key and must be requested from Peer Software Support.

For details about updating, see:

- [Updating Peer Management Center](#)
- [Updating Peer Agents](#)

### Updating Peer Management Center

#### Overview

There are two ways to check for software updates:

- You can manually check for software updates using the **Check for Updates** command on the **Help** menu. **Note:** This command is not available in the Peer Management Center Web Client.

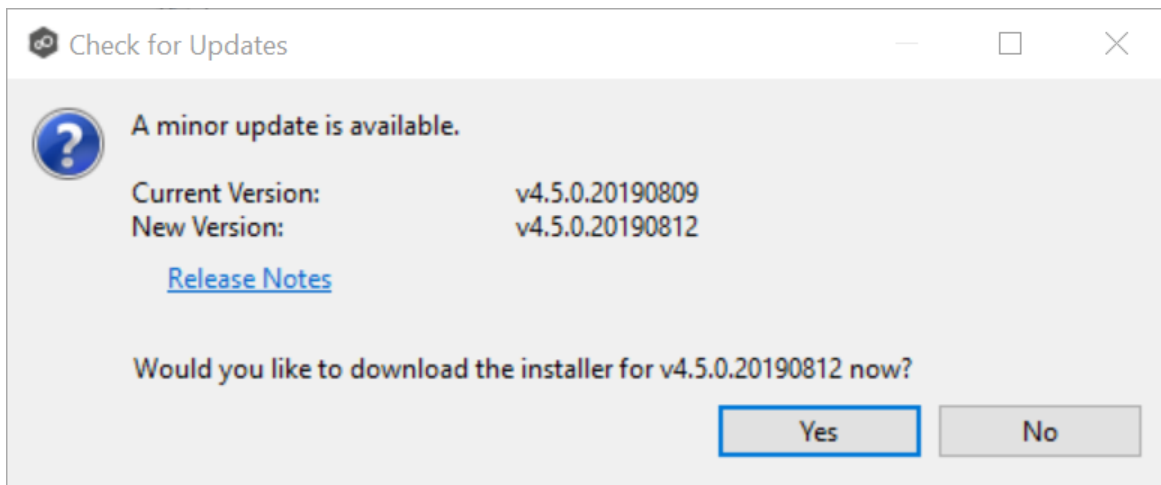
- You can also configure Peer Management Center to automatically check for updates and download the updates. For more information, see the [Software Updates](#) setting in [Preferences](#).

## Manually Checking for and Installing an Update

To manually check for an update:

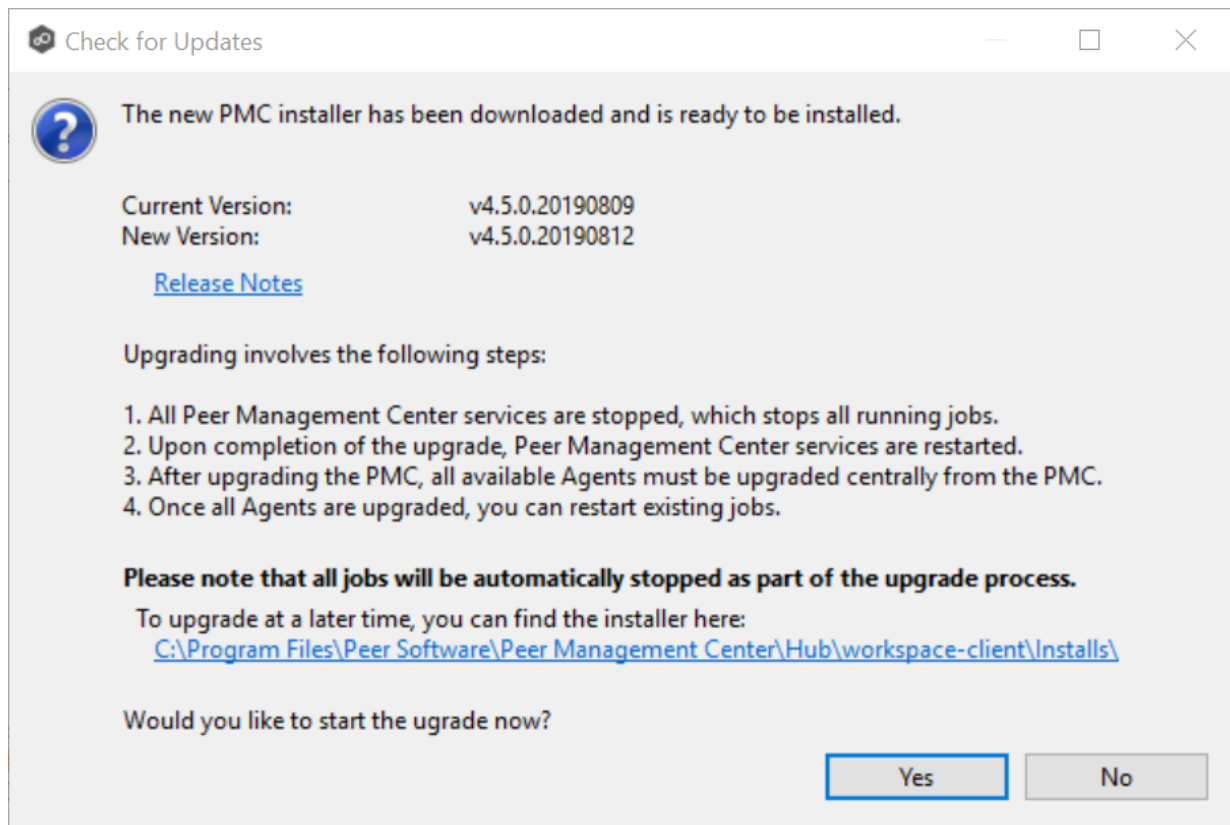
1. From the **Help** menu, select **Check for Updates**.

The **Check for Updates** dialog appears. If a minor update is available, the dialog identifies the new version (and your current version) and provides a link to the release notes. If a major update is available, the dialog presents a link to an announcement page on the Peer Software website.



2. Click **Yes** to download the Peer Management Center installer.

As the update is downloaded, a progress bar appears in the lower right corner of the Peer Management Center window. After the download is complete, the **Check for Updates** dialog displays information about the upgrade process.



3. Click **Yes** to install the upgrade; click **No** to install the update at a later time.

If you clicked **No**, you can install the update later by going to the folder shown in the dialog.

If you clicked **Yes**, the **Setup** wizard appears.

4. Follow the prompts in the **Setup** wizard to install the update.

When updating a Peer Management Center installation, you will not be prompted to specify web and API access. The settings entered previously will be used. If you wish to change those settings, you can do so by modifying them in [Web and API Configuration](#) in [Preferences](#).

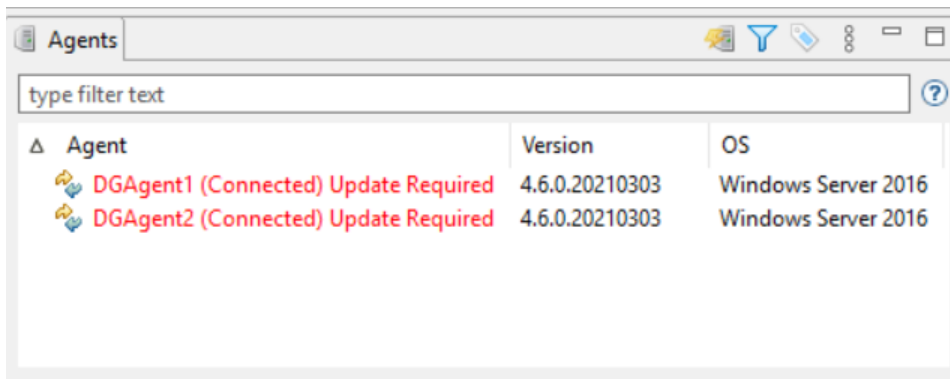
5. After the Peer Management Center upgrade is installed, update the Peer Agents. See [Updating Peer Agents](#) for details.

## Updating Peer Agents

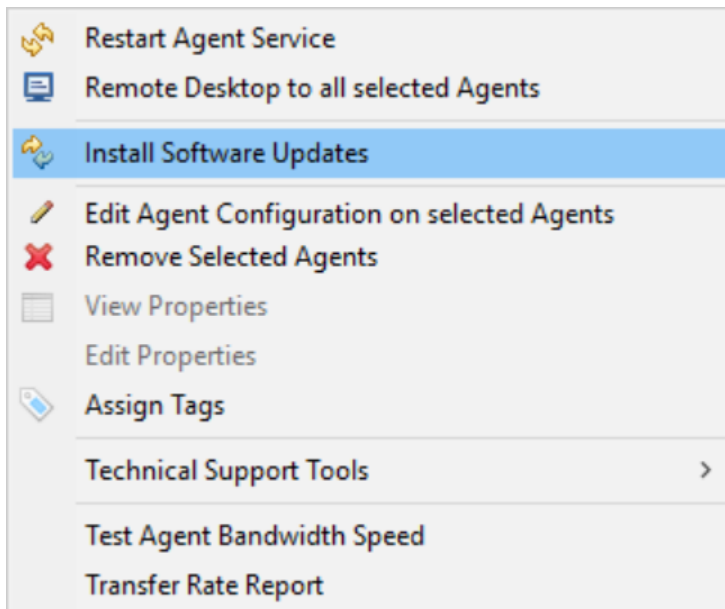
You can view the [status](#) of your Peer Agents in the [Agents](#) view. Whenever you [update Peer Management Center software](#), you need to update the Peer Agent software before you can start any jobs managed by that Agent. When **Update Required** appears next to an Agent's name, that indicates the software needs updating.

To update Peer Agents:

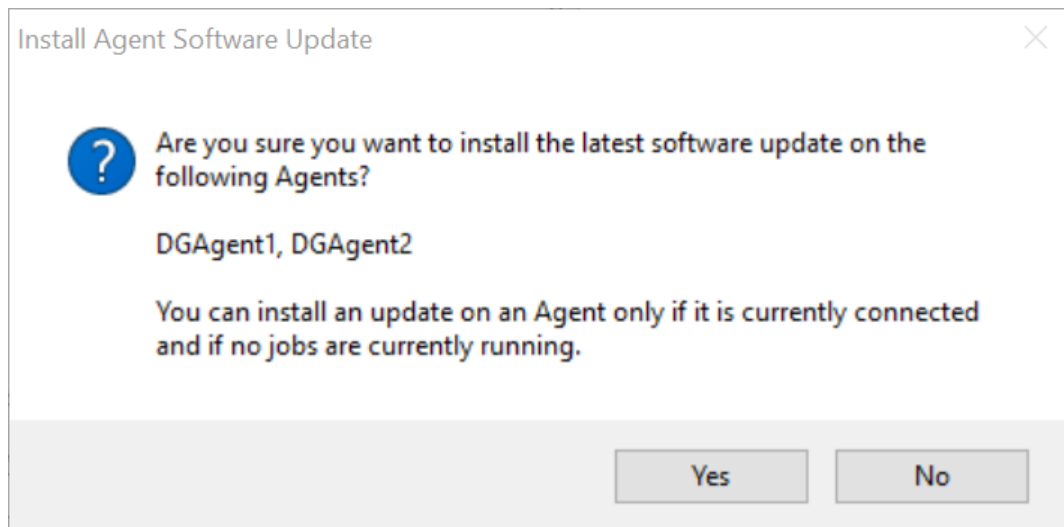
1. Select the Agents in the **Agents** view.



2. Right-click and select **Install Software Updates**.

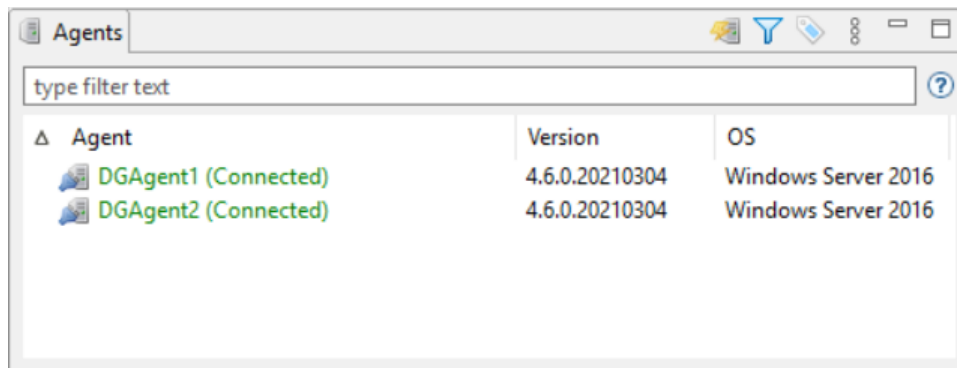


A confirmation dialog appears.



3. Click **Yes**.
4. Follow the prompts in the **Update Agent Software** dialog to complete the update.

After the Agents are updated, the Agents appear in green. The Agents automatically restart as part of the upgrade. Any jobs set to auto-start will restart once the Agents have reconnected.



## Peer Management Center User Interface

Peer Management Center is a management interface for configuring and deploying jobs, as well as view summary and runtime information for jobs. It offers two graphical user interface options:

- A **rich client** installed and run on the server running Peer Management Center.

- A **web client** that, when configured, can be [accessed](#) from remote systems via a web browser. You can manage and monitor jobs via the robust Peer Management Center web client. Unlike many other web management consoles, Peer Management Center's web client is very responsive and is built to mirror the functionality of the rich client (which is included with the Peer Management Center installer for use by system administrators). When properly configured, the web client allows for the management of Peer Management Center from remote clients without the need to directly log into the Peer Management Center server.

The interface can be divided into four quadrants: each quadrant displays information in panels called [views](#). A view can contain one or more tabs. See [Views](#) for more information about the views.

The screenshot displays the Peer Management Center Client interface, which is divided into four main quadrants:

- Jobs View:** Located on the left, it shows a tree view of jobs categorized by type (e.g., Cloud Backup and Replication, File Collaboration, File Replication, File Synchronization). It includes a filter bar and a list of jobs with their overall status (Running, Stopped, etc.).
- Summary and Runtime Views:** The central area, featuring a 'Runtime Summary' table with columns for Name, Overall Status, Job Type, Failed Hosts, Quaran..., Retries, Errors, Warnings, Open Files, Pending Bytes, Pending Events, Queued Items, Background..., Scan Status, Elapsed T..., and Session Structure. It also includes a summary bar at the bottom showing active jobs, failed participants, bytes pending, and other statistics.
- Alerts and Task History Views:** Located at the bottom right, it displays a table of alerts with columns for Received Date, Severity, Type, Name, Host, Message, and Exception. It includes a filter bar and a 'Clear Alerts' button.
- Agents View:** Located at the bottom left, it shows a list of agents with columns for Agent, Version, and Status. It includes a filter bar and a 'Task History' tab.

## Description of Quadrants

The quadrants are described in the following table.

Quadrant	Description
<b>Upper right</b>	Contains one view, the <a href="#">Jobs view</a> , which displays a list of all jobs, grouped by job type. The toolbar in this view allows you to start and stop jobs.
<b>Bottom right</b>	Contains one view, the <b>Agents</b> view. The <a href="#">Agents view</a> displays a list of known Peer Agents and connection status for each. Individual Peer Agents can be updated and restarted from this view as well by right-clicking on one or more items and selecting the appropriate item from the pop-up menu.
<b>Upper right</b>	Several types of views are displayed in this area, including: <ul style="list-style-type: none"> <li>• A <a href="#">dashboard</a> that provides metrics and key performance indicators.</li> <li>• <a href="#">Summaries of jobs by job type</a>.</li> <li>• An <a href="#">Agent Summary view</a>, which displays a list of all known <a href="#">Peer Agents</a> deployed and detailed status information that can be used to assess the health of the environment.</li> <li>• <a href="#">Runtime statistics for individual jobs</a>.</li> </ul>
<b>Lower left</b>	Contains a variety of views, including: <ul style="list-style-type: none"> <li>• The <a href="#">Alerts view</a>, which displays a list of Peer Management Center alerts that have occurred with detailed information about each alert. Alerts relating to Peer Agent connection status changes are reported here.</li> <li>• The <a href="#">Jobs Alerts view</a>, which displays a list of job-specific alerts that have occurred. Alerts relating to the <a href="#">automatic stopping and restarting</a> of jobs are displayed here.</li> </ul>

For information about other aspects of the user interface, see:

- [Accessing the Web Client](#)
- [Views](#)
- [Main Window Menus and Toolbar](#)
- [Tables](#)



## Accessing the Web Client

Once Peer Management Center has been installed, the Peer Management Center Web Client Service has been configured, and the [necessary Peer services](#) have been started, users can access the Peer Management Center web client in various ways:

- Log in directly through a web browser on the local Peer Management Center server.
- Remote access from another system on a network that can reach the Peer Management Center server.
- Start the Peer Management Center Client (rich client application) and select **Peer Management Center Web Client** from the **Help** menu.

## Logging into the Web Client

To access the Peer Management Center web client:

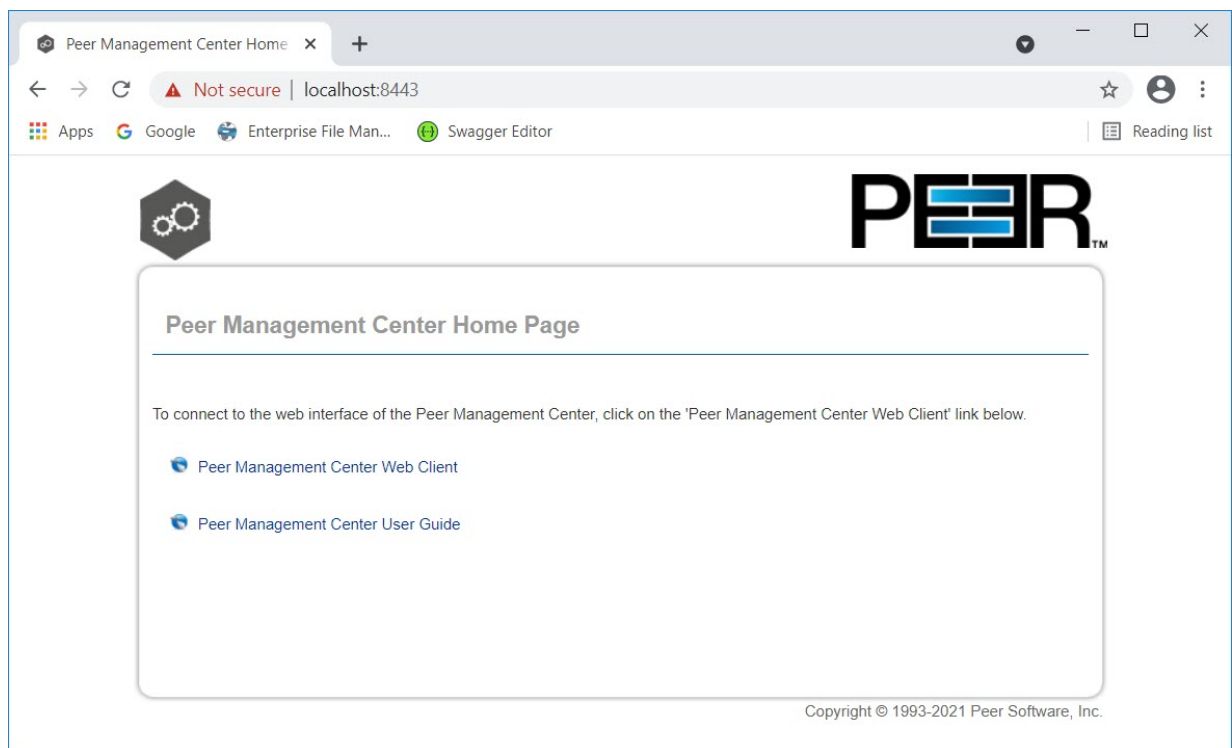
1. Open a web browser.
2. Enter one of the following URLs in the address field:

If this URL was entered in the Installation Wizard	Use this URL
A specific IP address	Enter <b>https://</b> followed by that IP address and <b>:8443</b> . You cannot use <b>localhost</b> even if you are directly logged into the Peer Management Center server.  For example: <b>https://10.0.0.1:8443</b>
<b>localhost</b> or <b>127.0.0.1</b>	Enter <b>https://localhost:8443</b> or <b>https://127.0.0.1:8443</b> .
<b>0.0.0.0</b>	Enter <b>https://</b> followed by the IP address of the Peer Management Center server and <b>:8443</b>  For example: <b>https://10.0.0.1:8443</b>

### Notes:

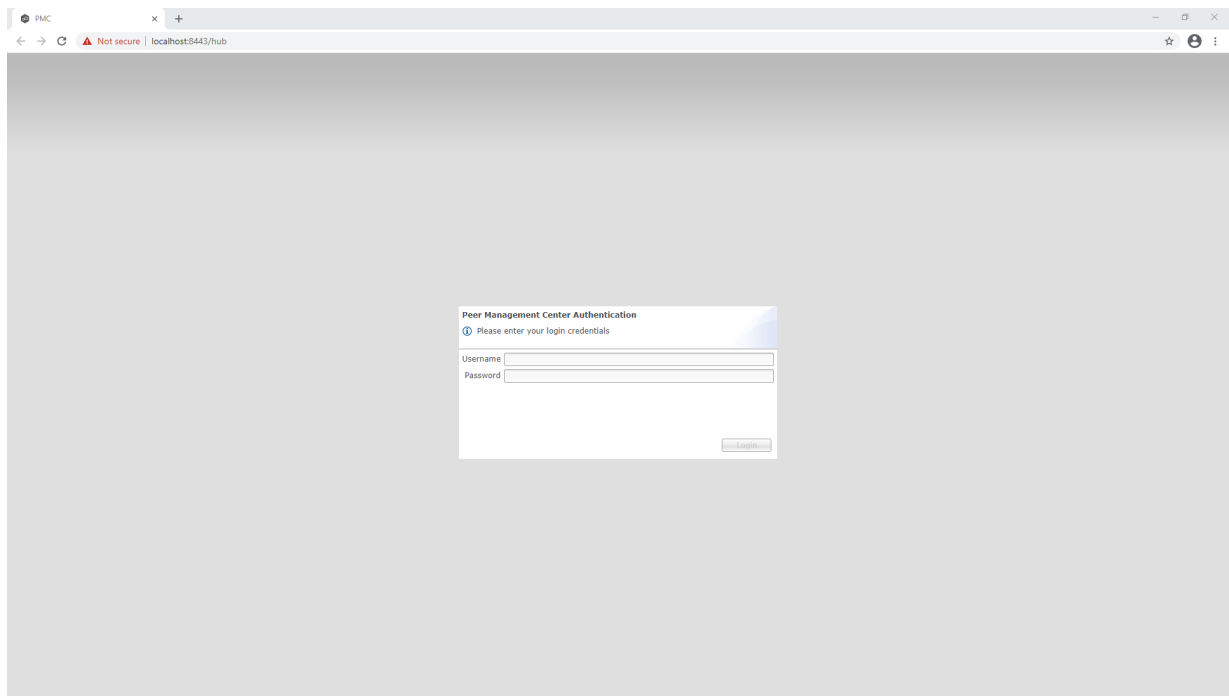
- The URL will depend on how [the web service was configured](#) during the installation process; you may need to contact the administrator who installed Peer Management Center to determine the correct URL.
- 8443 is the default HTTPS port and should be replaced with the port used in your environment if it is different.
- You can modify the web service configuration on the [General Configuration](#) page of [Preferences](#). For more information, see [Web and API Configuration](#).

After you enter the URL, the Peer Management Center Home Page appears.



3. Select the **Peer Management Center Web Client** link.

The login page is displayed.



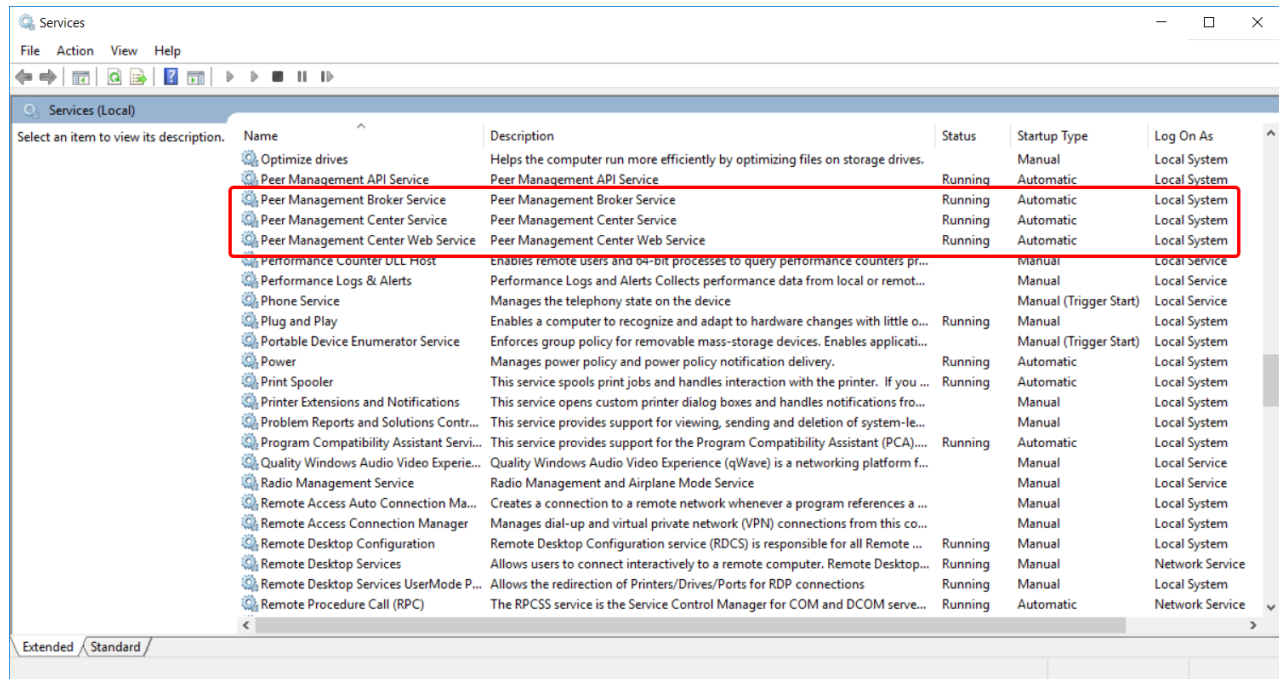
4. Enter a user name and password.

- The default user name is **admin**; the default password is **password**. For security reasons, we highly recommend that the user immediately changes the **admin** password. See [Editing an Internal User](#) for more information on changing account passwords.
- If logging in with an Active Directory account, enter the user name in this format: username@mydomain.local.

5. Click **Login**.

### Peer Services Required for Web Client

To use the Peer Management Center web client, the following Peer services must be running on the Peer Management Center server:



If a required service is not running, open the Windows Service Panel (services.msc) on the applicable PMC server and start the service.

## Views

The Peer Management Center interface can be divided into four quadrants; each quadrant displays information in panels called [views](#). A view can contain multiple tabs. There are various types of view. For example, some views display a combination of real-time file I/O activity, history, and configuration information for a specific job; others displays a summary of information about all jobs of a specific type.

The screenshot displays the Peer Management Center Client interface with four primary views highlighted by red boxes:

- Jobs View:** Located on the left, it shows a tree structure of jobs including Cloud Backup and Replication, DFS-N Management, File Collaboration, File Replication, File Synchronization, and File Watchers.
- Summary and Runtime Views:** The central pane shows a 'Runtime Summary' table with columns for Name, Overall Status, Job Type, Failed Hosts, Quarantined, Retries, Errors, Warnings, Open Files, Pending Bytes, Pending Events, Queued Items, Background, Scan Status, Elapsed Time, and Session Structure. It lists various jobs like FC-4, FC-2, FC-5, FS-1, FS-3, FS-4, FS-5, FR-1, FR-2, FR-3, FR-4, and FR-5.
- Agents View:** Located at the bottom left, it shows a list of agents including DGAgent1 and DGAgent2, along with their versions and connection status.
- Alerts and Task History Views:** The bottom right pane shows a table of alerts and task history with columns for Received Date, Severity, Type, Name, Host, Message, and Exception. It lists various events such as 'User Started Peerless - Restart Action', 'Host Reconnect startup error', and 'Host Failure'.

The primary views include:

- [Agents View](#)
- [Jobs View](#)
- [Dashboard](#)
- [Alerts View](#)
- [Job Alerts View](#)
- [Summary Views](#)
  - [Agent Summary View](#)
  - [Cloud Summary View](#)
  - [Collab, Sync, and Repl Summary View](#)
  - [Namespace Summary View](#)
- [Runtime Views](#)
  - [Cloud Backup and Replication Job Runtime View](#)

- [File Collaboration Job Runtime View](#)
- [File Replication Job Runtime View](#)
- [File Synchronization Job Runtime View](#)

## Displaying Views

You can open views in a variety of ways:

- Selecting a command from the Window menu
- Right-clicking on a item to display a context menu that
- Clicking the View button in a toolbar and selecting an option from the View menu/

## Resizing Views

You can resize views in a variety of ways:

- Drag the separator between views.
- Click the minimize or maximize button in the toolbar.
- Reset all views to the default size by selecting the **Reset Perspective** command on the **Window** menu.

### Agents View

The **Agents** view is displayed in the lower left quadrant of the Peer Management Center interface and lists all known Peer Agents installed in your environment and displays the current [connection status](#) for each. For more information, see [Agent Connection Statuses](#). This view is automatically displayed when Peer Management Center is started.

The screenshot shows the Peer Management Center Client interface. The main window displays a 'Runtime Summary' table with columns for Name, Overall Status, Job Type, Failed Hosts, Retries, Errors, Warnings, Open Files, Pending Bytes, Pending Events, Queued Items, Background..., Scan Status, Elapsed Time, and Session Structure. Below this is an 'Alerts' section showing a list of events with columns for Received Date, Severity, Type, Name, Host, Message, and Exception. A red box highlights the 'Agents' toolbar at the bottom left, which includes a 'Filter' field and a 'List Filters' button.

To filter a large list of Agents, use the **Filter** field located below the [Agents view toolbar](#). For more details on how to filter agents, see [List Filters](#).

## Updating Peer Agent Software

If the Peer Agent software running on a host is out of date, the host will be shown as having a pending update in this view. When right-clicking the Agent, the option to automatically update the Peer Agent software will also be available. You can update directly from the Peer Management Center; updating usually does not require any additional actions on the host server itself. See [Updating Peer Agents](#) for more information.

The following buttons are available on the toolbar in the Agents view:

Button	Description
<b>Show Agent Summary</b>	Opens the <a href="#">Agent Summary view</a> , which provides details for all known Agents and their status.
<b>Manage, Save and Load Filters</b>	Allows for the selection of predefined or user-defined filters and to save and manage filters. Default Agent filters include <b>Connected</b> and <b>Disconnected</b> .
<b>Assign Tags</b>	Opens the <b>Assign Tags</b> dialog where resources can be viewed and assigned to tags or categories. Tagging resources helps when managing large number of resources. New

### Alerts View

The **Alerts** view is displayed in the lower right quadrant of the Peer Management Center interface and displays various system alerts. The **Alerts** view is automatically displayed when a critical system alert (Error or Fatal) is received. You can also [set the Alerts view to be automatically displayed](#) when Peer Management Center is started.



The screenshot shows the Peer Management Center Client interface. The main window displays a table of alerts. The Alerts tab is selected, showing a list of alerts with columns: Received Date, Severity, Type, Name, Host, Message, and Exception. The alerts include information about agent connections, scheduled tasks, and heartbeats. The Alerts view is highlighted with a red border.

System alerts vary in their severity. The four categories of alerts are:

- Informational (containing Info, Debug, and Trace)
- Warning
- Error
- Fatal

An example of an Informational alert is when a [Peer Agent](#) connects to the [Peer Management Broker](#). If a Peer Agent's network connection is severed, then an Error alert will be logged. All alerts are also logged to the file **hub\_alert.log**, available under the **Hub\logs** subdirectory within the Peer Management Center installation directory.

You can filter alerts based on host name, severity level, or type, and you can sort alerts by clicking on a specific column header. You can also clear all alerts in the table by clicking the **Clear Alerts** link.

## Displaying the Alerts View

You can open the **Alerts** view at any time by clicking the **View Alerts** button located on the Peer Management Center toolbar or by selecting **View Alerts** from the **Show View** submenu of the **Window** menu. You can close the **Alerts** view at any time by clicking on the **X** (Close) button on the **Alerts** tab.

You can resize the Alerts view by dragging the separator between the upper view and the Alerts view, or you can double-click the **Alerts** tab to maximize the view. You can restore the view to its original, non-maximized size by double-clicking the **Alerts** tab again.

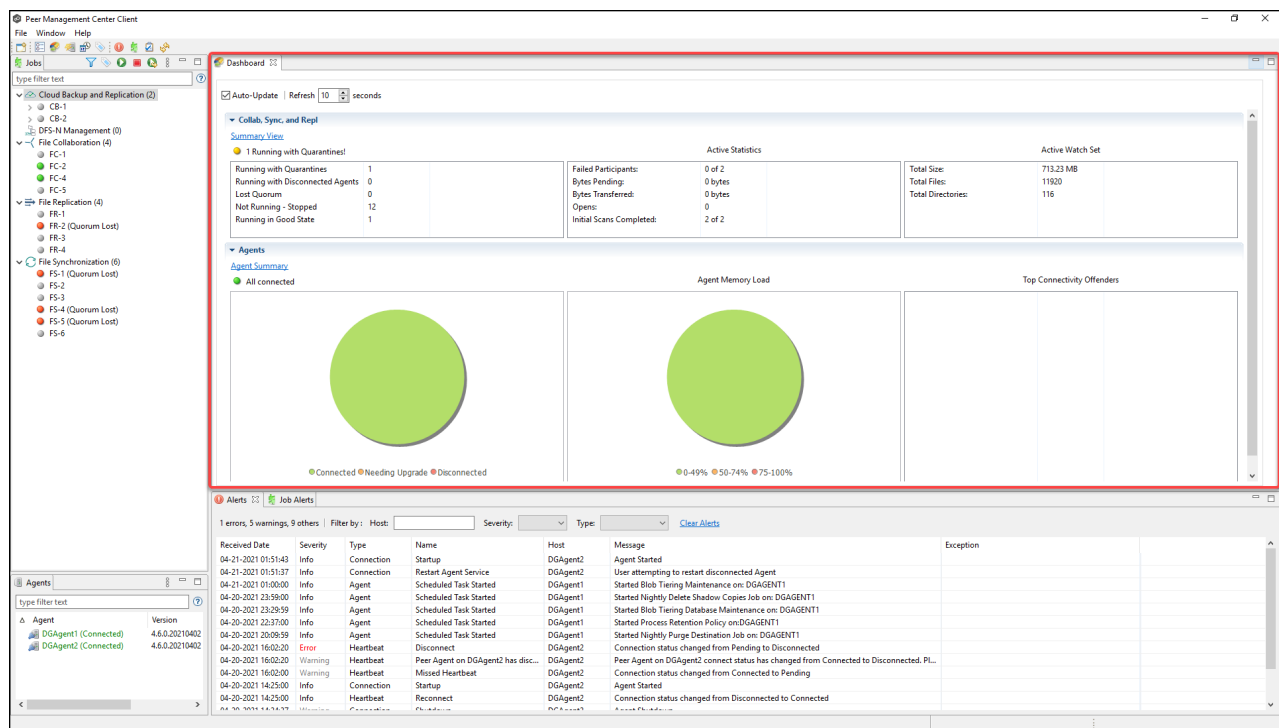
## Dashboard

The Dashboard is divided into two sections:

- **Collab, Sync, and Repl** - This top section displays a table of metrics and key performance indicators for all running File Collaboration, File Synchronization, and File Replication jobs. It also contains a link that opens the [Collab, Sync, and Repl Summary view](#). Entries in the table's first column can be double-clicked to display a filtered runtime view of the selected item for additional details.
- **Agents** - The bottom section displays information about Agents. It also contains a link that opens the [Agent Summary view](#).

Click the triangle to the left of the section name to collapse and expand the section.

For performance reasons, the Dashboard is not updated in real-time. However, you can set the table to be automatically updated every few seconds by selecting the **Auto-Update** checkbox, and choosing the update interval.



To display the Dashboard, use one of the following methods:

- Select **View Dashboard** from the **Window** menu.
- Click the **View Dashboard** icon in the main [Peer Management Center toolbar](#).
- Set the Dashboard to launch automatically at start. See [General Configuration](#).

### Job Alerts View

The **Alerts** view is displayed in the lower right quadrant of the Peer Management Center interface and displays various system alerts. The **Job Alerts** view is automatically displayed when a critical job-related (Error or Fatal) alert is received. .

There are four categories of alerts, distinguished by the severity of the alert:

- Informational (containing Info, Debug, and Trace information)
- Warning
- Error
- Fatal

An example of an Informational alert is when a job is started or stopped manually by the user. If a job loses one of its [participating hosts](#) and as a result, cannot keep a quorum and shuts down, then a Fatal alert will be logged. All alerts are also logged to the file **job\_alert.log**, available under the **Hub\logs** subdirectory within the Peer Management Center installation directory.

The screenshot displays the Peer Management Center Client interface. The top section shows the 'Jobs' view with a tree on the left and a table of job details. The bottom section shows the 'Job Alerts' view with a table of alerts.

**Jobs View Table:**

Name	Overall Status	Job Type	Failed Hosts	Quorum	Retries	Errors	Warnings	Open Files	Pending Bytes	Pending Events	Queued Items	Background	Scan Status	Elapsed T...	Session Structure
FC-4	Running	File Collaboration	0	0	0	0	1	0	0 bytes	0	0	0	Completed - 00:01:00	09:18:24	Size: 367.32 MB, ...
FR-4	Stopped	File Replication	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FC-2	Running	File Collaboration	0	0	0	0	3	0	0 bytes	0	0	0	Completed - 00:00:27	09:18:24	Size: 345.92 MB, ...
FC-5	Stopped	File Collaboration	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-1	Failed (Quorum Lost)	File Synchronization	DGAgent1	0	0	1	1	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-3	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FC-1	Stopped	File Collaboration	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FR-2	Failed (Quorum Lost)	File Replication	DGAgent2	0	0	1	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-4	Failed (Quorum Lost)	File Synchronization	DGAgent2	0	0	1	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-5	Failed (Quorum Lost)	File Synchronization	DGAgent1	0	0	1	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FR-1	Stopped	File Replication	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-6	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-2	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-3	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-5	Failed (Quorum Lost)	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-6	Failed (Quorum Lost)	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...

**Job Alerts View Table:**

Received Date	Severity	Type	Name	Host	Message	Exception
04-21-2021 02:49:01	Error	Configuration	FS-5	DGAgent2.DG...	Disabled auto restart because maximum # (15) of restart attempts was exceeded for host(s)...	
04-21-2021 02:47:59	Error	Start Job	FS-5	DGAgent1	Host Reconnect Startup Error. Operations=Install Watch Directories: ERROR Registering job...	
04-21-2021 02:47:01	Info	Auto Start Job	FS-5	DGAgent1	Auto starting job, DGAgent1 host is now available.	
04-21-2021 02:46:00	Error	Start Job	FS-5	DGAgent1	Host Reconnect Startup Error. Operations=Install Watch Directories: ERROR Registering job...	
04-21-2021 02:45:01	Info	Auto Start Job	FS-5	DGAgent1	Auto starting job, DGAgent1 host is now available.	
04-21-2021 02:44:01	Error	Configuration	FS-5	DGAgent2.DG...	Disabled auto restart because maximum # (15) of restart attempts was exceeded for host(s)...	
04-21-2021 02:44:00	Error	Start Job	FS-5	DGAgent1	Host Reconnect Startup Error. Operations=Install Watch Directories: ERROR Registering job...	
04-21-2021 02:43:01	Info	Auto Start Job	FS-5	DGAgent1	Auto starting job, DGAgent1 host is now available.	
04-21-2021 02:42:50	Error	Start Job	FS-5	DGAgent1	Host Reconnect Startup Error. Operations=Install Watch Directories: ERROR Registering job...	
04-21-2021 02:42:01	Info	Auto Start Job	FS-5	DGAgent1	Auto starting job, DGAgent1 host is now available.	
04-21-2021 02:41:58	Error	Start Job	FS-5	DGAgent1	Host Reconnect Startup Error. Operations=Install Watch Directories: ERROR Registering job...	
04-21-2021 02:41:01	Info	Auto Start Job	FS-5	DGAgent1	Auto starting job, DGAgent1 host is now available.	

You can filter alerts based on host name, job name, severity level, or type, and you can sort alerts by clicking on a specific column header. You can also clear all alerts in the table by clicking the **Clear Alerts** link.

## Displaying Job Alerts

You can open the Job Alerts view at any time by clicking the **View Job Alerts** button located on the Peer Management Center toolbar or by selecting the **Window** menu, then the **Show View** submenu, followed by the **View Job Alerts** menu item. You can close the view at any time by clicking on the **X** (Close) button on the Job Alerts tab.

You can resize the Job Alerts view by dragging the separator between the upper view and the Job Alerts view, or you can double click the **Job Alerts** tab to maximize the view. You can restore the view to its original, non-maximized size by double-clicking the **Job Alerts** tab again.

## Jobs View

The **Jobs** view is displayed in the upper left quadrant of the Peer Management Center interface and lists all the jobs, grouped by type. The number in the parentheses following the job type identifies the number of existing jobs of that type. This view is automatically displayed when Peer Management Center is started.

The screenshot displays the Peer Management Center Client interface. The top menu bar includes File, Window, and Help. The main window is divided into several sections:

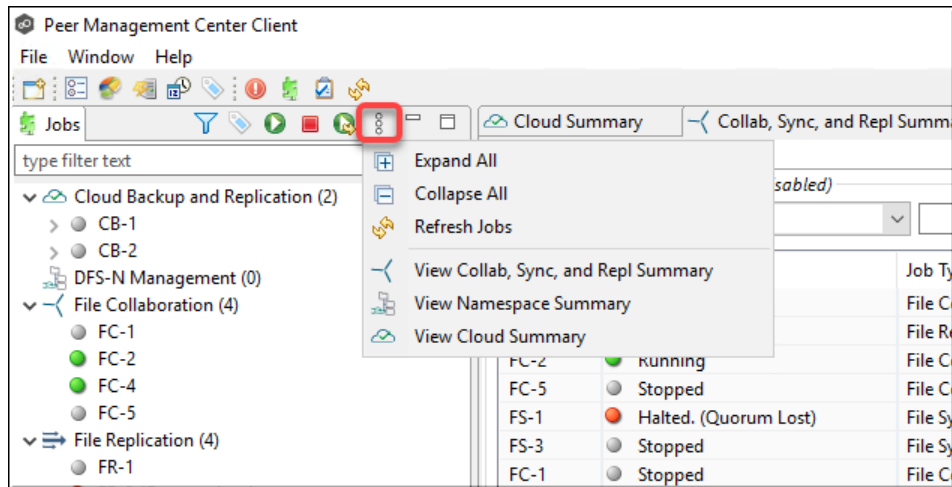
- Jobs View:** A tree view on the left shows a hierarchy of jobs: Cloud Backup and Replication (2), CB-1, CB-2, DFS-N Management (0), File Collaboration (4), FC-1, FC-2, FC-4, FC-5, File Replication (4), FR-1, FR-2, FR-3, FR-4, File Synchronization (6), FS-1, FS-2, FS-3, FS-4, FS-5 (Quorum Lost), and FS-6.
- Runtime Summary Table:** A large table with columns: Name, Overall Status, Job Type, Failed Hosts, Quarantined, Retries, Errors, Warnings, Open Files, Pending Bytes, Pending Events, Queued Items, Background..., Scan Status, Elapsed Time, and Session Structure. The table lists various jobs and their current status.
- Alerts and Agents:** A section at the bottom shows alerts (0 errors, 3 warnings, 2 others) and a list of agents (DGAgent1, DGAgent2) with their connection status and version.

You can easily display more information about a job or job type by double-clicking a job name or job type name:

- Double-clicking any job name in the list will display a [runtime view](#) of that job.
- Double-clicking any job type name in the list will display a [summary view](#) of that job type.

To filter a large list of jobs, use the **Filter** field located below the [Jobs view toolbar](#). For more details on how to filter jobs, see [List Filters](#).

You can expand all or collapse all jobs by clicking the **View** button in the [Jobs view toolbar](#) and selecting an option from the **View** menu:



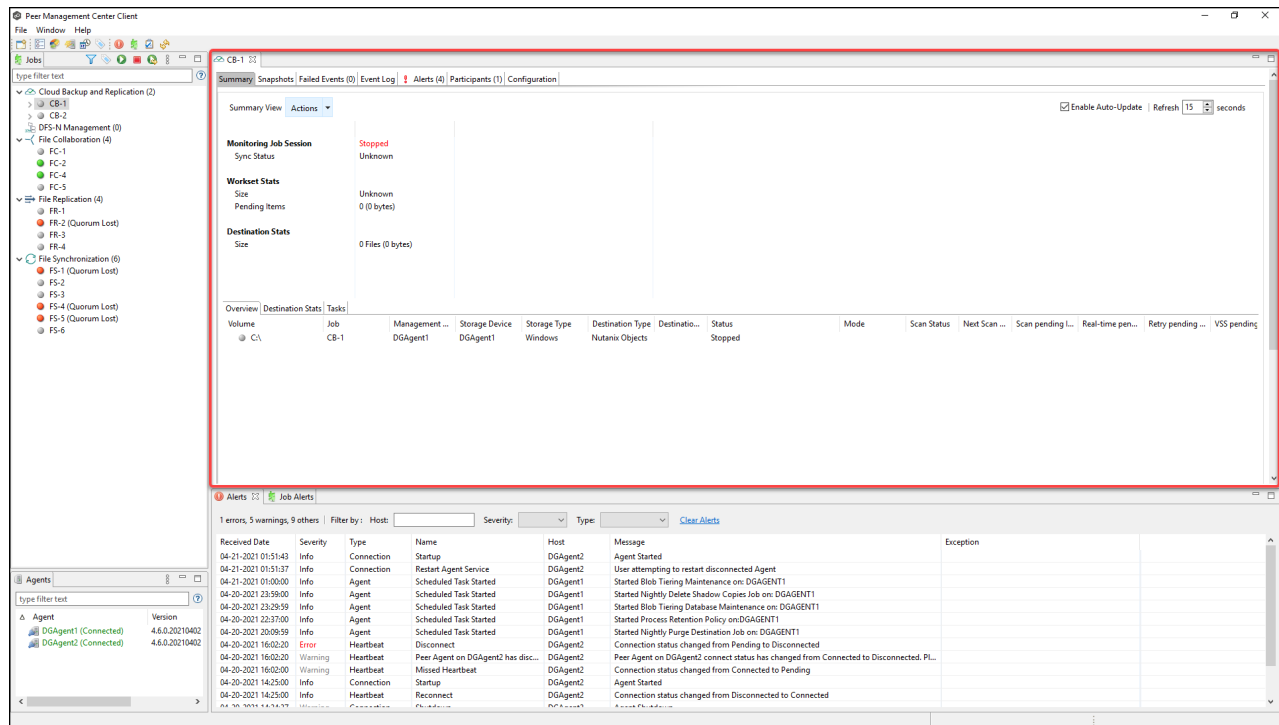
The following buttons are available on the toolbar within the **Jobs** view:

Button	Description
<b>Manage, Save and Load Filters</b>	Enables selection of predefined or user-defined filters and to save/manage filters. Default filters include Failed Jobs, Jobs with Backlog, and Running Scans.
<b>Assign Tags</b>	Opens the <a href="#">Assign Tags</a> dialog where resources can be viewed, tagged, and assigned to categories. Tagging resources helps when managing large number of resources.
<b>Start</b>	Starts one or more selected and currently stopped jobs.
<b>Stop</b>	Stops one or more selected and currently running jobs.
<b>Restart</b>	Restart one or more selected jobs.
<b>View</b>	Presents options for displaying views and collapsing and expanding jobs in the <b>Jobs</b> view.

## Runtime Views

The **runtime** views are displayed in the upper right quadrant of the Peer Management Center interface.

Each job has a **runtime view** that show a combination of real-time file I/O activity, history, and configuration information. The job name appears as the title of the view. A runtime view typically has several tabs. For example, in the following figure, the Cloud Backup and Replication job **CB-1** is displayed; this view contains six tabs.



The runtime views include:

- [Cloud Back and Replication job views](#)
- [File Collaboration job views](#)
- [File Replication job views](#)
- [File Synchronization job views](#)

To monitor a specific Cloud Backup and Replication job, open its runtime view.

Each Cloud Backup and Replication job has a runtime view that show a combination of real-time file I/O activity, history, and configuration. This runtime view has six tabs:

- **Summary** – Displays the status of the job, the number of and size of files uploaded in the last replication, and the size of replicated files.
- **Snapshots** – Displays a log of the snapshots taken since the job was created.
- **Failed Events** – Displays information about events that failed to successfully complete.
- **Event Log** – Displays a log of events that have occurred for the jobs – It displays the last 2500 actions that Cloud Backup and Replication has taken.
- **Alerts** – Displays a log of alerts that were issued for the job.
- **Participants** – Displays Agents that are participants in this Cloud Backup and Replication job (Currently a job can have only one participating agent.)
- **Configuration** – Displays a summary of the job configuration.

The screenshot displays the Peer Management Center Client interface. The left sidebar shows a tree view of the system hierarchy, including Cloud Backup and Replication jobs, File Collaboration, File Replication, and File Synchronization. The main window is titled 'Peer Management Center Client' and contains several tabs: Dashboard, Agent Summary, Cloud Summary, Collab, Sync, and Repl Summary, Namespace Summary, and a set of job-specific tabs (CB-1, FC-2, FR-2, FS-4). The 'Cloud Summary' tab is selected, showing a 'Summary View' for a job named 'CB-1'. The job status is 'Stopped', and the sync status is 'Unknown'. Below this, there are sections for 'Workset Stats' and 'Destination Stats'. At the bottom of the main window, there is an 'Alerts' section showing a list of 107 errors, 3 warnings, and 107 others. The alerts are filtered by host and severity, and a table lists the details of each alert, including the received date, severity, type, name, host, message, and exception.

Received Date	Severity	Type	Name	Host	Message	Exception
04-20-2021 14:45:46	Info	Start Job	FS-5		User Started Peerlet - Restart Action	
04-20-2021 14:45:43	Fatal	Error Running ...	CB-1		Uncaught Exception running job CB-1: java.lang.Exception: Reply not received from DGAg...	java.lang.Exception: Reply not received from DGAg...
04-20-2021 14:45:42	Info	Start Job	FS-4		User Started Peerlet - Restart Action	
04-20-2021 14:45:39	Info	Start Job	FS-1		User Started Peerlet - Restart Action	
04-20-2021 14:45:31	Info	Auto Start Job	FR-2	DGAgent2	Auto starting job, DGAgent2 host is now available.	
04-20-2021 14:45:06	Error	Host Failure	FS-5	DGAgent2	Host Reconnect Startup Error. Operations::StartSession Command : Host Reply Timeout (C...	
04-20-2021 14:45:06	Error	Host Failure	FS-1	DGAgent2	Host Reconnect Startup Error. Operations::StartSession Command : Host Reply Timeout (C...	
04-20-2021 14:45:06	Error	Host Failure	FS-4	DGAgent2	Host Reconnect Startup Error. Operations::StartSession Command : Host Reply Timeout (C...	
04-20-2021 14:44:36	Error	Host Failure	FR-2	DGAgent2	Host Reconnect Startup Error. Operations::StartSession Command : Host Reply Timeout (C...	
04-20-2021 14:44:01	Info	Auto Start Job	FS-1	DGAgent2	Auto starting job, DGAgent2 host is now available.	
04-20-2021 14:44:01	Info	Auto Start Job	FS-5	DGAgent2	Auto starting job, DGAgent2 host is now available.	
04-20-2021 14:44:01	Info	Auto Start Job	FS-4	DGAgent2	Auto starting job, DGAgent2 host is now available.	



To monitor a specific DFS-N Management job, open its runtime view.

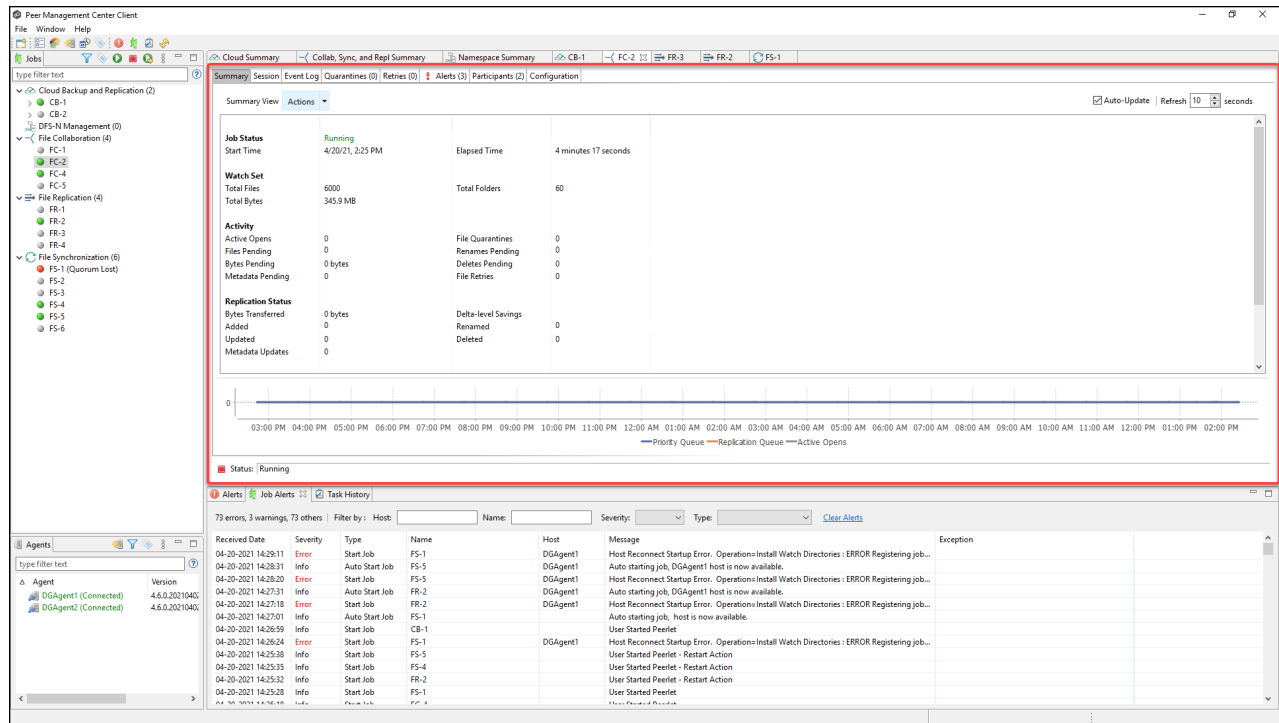
Each DFS-N Management job has a runtime view that show a combination of real-time file I/O activity, history, and configuration.

To monitor a specific File Collaboration job, open its runtime view.

Each File Collaboration job has a runtime view that show a combination of real-time file I/O activity, history, and configuration. This runtime view has eight tabs:

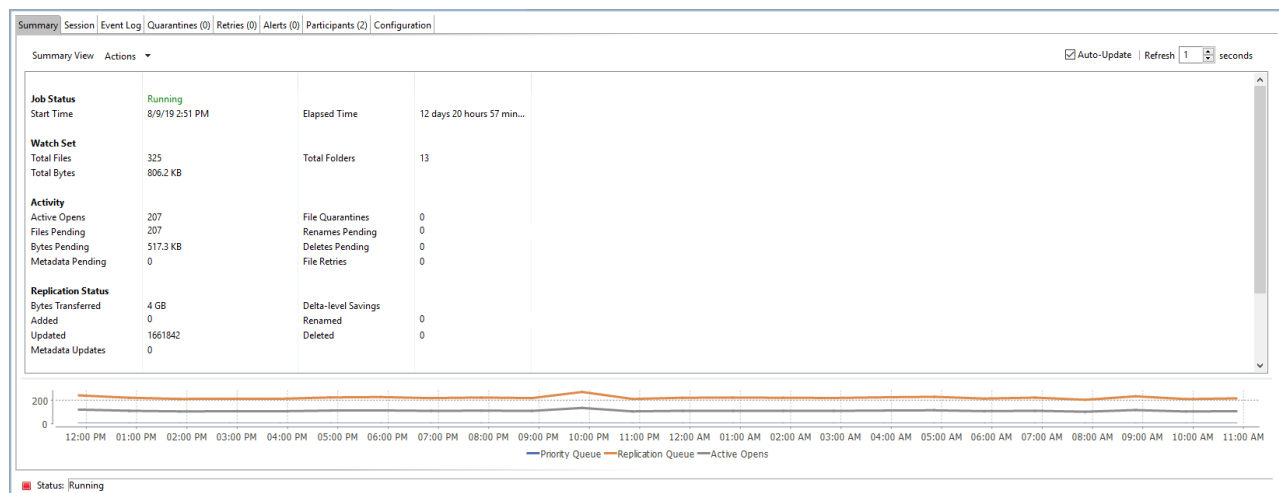
The view contains the following eight tabs:

- [Summary](#) - Displays overall statistics for the selected job.
- [Session](#) - Displays active open files and files that are currently in transit between [participating hosts](#).
- [Event Log](#) - Displays a list of all runtime activity that has occurred within the selected job.
- [Quarantines](#) - Displays a list of all files that are quarantined for the session or are in conflict between two or more participating hosts.
- [Retries](#) - Displays a list of files that are currently in the Retries list.
- [Alerts tab](#) - Displays a list of all job alerts specifically tied to the selected job.
- [Participants tab](#) - Displays a list of all hosts participating in the selected job.
- [Configuration tab](#) - Displays a summary of all configurable options for the selected job.



## Summary Tab

The **Summary** runtime tab allows you to view current and cumulative file collaboration and synchronization statistics, as well background synchronization status. For performance reasons, this tab is not updated in real-time. However, it can be set to automatically update every few seconds. Select the **Auto-Update** checkbox to enable this functionality; set the refresh interval (in seconds) in the **Refresh** checkbox. Each refresh cycle will update the totals across all active jobs listed at the bottom of the view.



Key statistics in this view are presented in the [Activity](#), [Replication Status](#), and [Background Scan](#) sections. Notice that this tab is scrollable.

## Activity

This section presents statistics on pending activity:

- **Files Pending** – Number of files pending synchronization, this includes queued initial scan items, bulk add files, single file adds and real-time modifies. This does not include Deletes, renames or security changes. Move your cursor over the field to see the breakdown from Adds, Updates, and Scan.
- **Bytes Pending** – Matches the Pending Bytes from the [Collab, Sync, and Repl Summary](#) view, which includes all Queued Transfers including scan works, as well as bulk adds. Note this does not track Files Pending exactly but does provide a good indication of the number of bytes currently still needing to be synchronized.
- **Metadata Pending** – Number of pending metadata changes from real-time and from initial and folder scans.
- **Renames Pending** – Total number of files and folders pending rename. Move your cursor over the field to see the breakdown for folders and files.
- **Deletes Pending** – Total number of files and folders pending delete.

## Replication Status

This section presents statistics on all completed synchronization from real-time and the initial scan:

- **Bytes Transferred** – Total number of bytes transferred for all real-time Add, Bulk Add, Modify, and Scan synchronization. This does not include bulk delete, security or renames.
- **Added** – Total number of files and folders added in real-time. Move your cursor over the field to see the breakdown for folders and files.
- **Updated** – Total number of files synchronized by initial scan or real-time.
- **Deleted** – Total number of files and folders deleted.
- **Renamed** – Total number of files and folders renamed. Move your cursor over the field to see the breakdown for folders and files.
- **File Metadata Updates** – Total number of real-time and scan metadata updates for folders and files.

This section presents pending and completed synchronization statistics from the initial full scan.

- ### Session Tab

[illegible]

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.

Component	Description
<b>Open Files table</b>	<p>A table showing all currently open files on the source host, any internal file locks being held by the running File Collaboration job on the target host(s), and file summary information. This table also shows all file transfers currently in progress along with file summary information, status, and overall progress. Clicking any column headers sorts by that column in ascending or descending order.</p> <p>All items listed in this table are grouped by file path. Each associated lock and/or transfer for each <a href="#">participating host</a> will be available as a hidden child item of a root row. The root row represents the file on the <a href="#">source host</a>. Pressing the + next to the root will show all associated file transfers and/or locks.</p>
<b>Session Status field</b>	<p>Field indicating the current status of the session. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Stopped:</b> Session is stopped.</li> <li>• <b>Starting:</b> Session is starting up.</li> <li>• <b>Collaborating:</b> Real-time event detection is enabled.</li> </ul>
<b>Filter by Host list</b>	A drop-down list of participating hosts to filter on. Selecting a specific host will filter the open files to show files on that host only.
<b>Filter By Combo list</b>	A drop-down list of additional filters that can be applied to the Open Files table, including filtering by user name (associated with the opening, adding, deleting, or modification of a file) and by file name.
<b>Actions menu</b>	<b>Refresh View:</b> Refreshes the entire Open Files table to show the latest list of file transfers and locks.

#### Event Log Tab

The **Event Log** tab allows you to view recent file event history for the currently running File Collaboration job based on your [Logging and Alerts](#) settings. You can specify the maximum number of events to store in the table by adjusting the Display Events spinner located in the top right corner of the panel. The maximum number of events that can be viewed is 3,000.

If you need to view more events or events from a prior session, then you can use the log files saved in the **Hub\logs** directory located in the installation directory. The event log files will start

with **fc\_event.log** and are written in a tab-delimited format. Microsoft Excel is a good tool to use to view and analyze a log file. See [Logging and Alerts](#) for more information about log files.

You can click any column header to sort by the column. For example, clicking the **File** column will sort by file name and you will be able to view all file events for that file in chronological order. Warnings are displayed in light gray, errors are displayed in red, and fatal errors are displayed in orange. Error records will also contain an error message in the **Message** column.

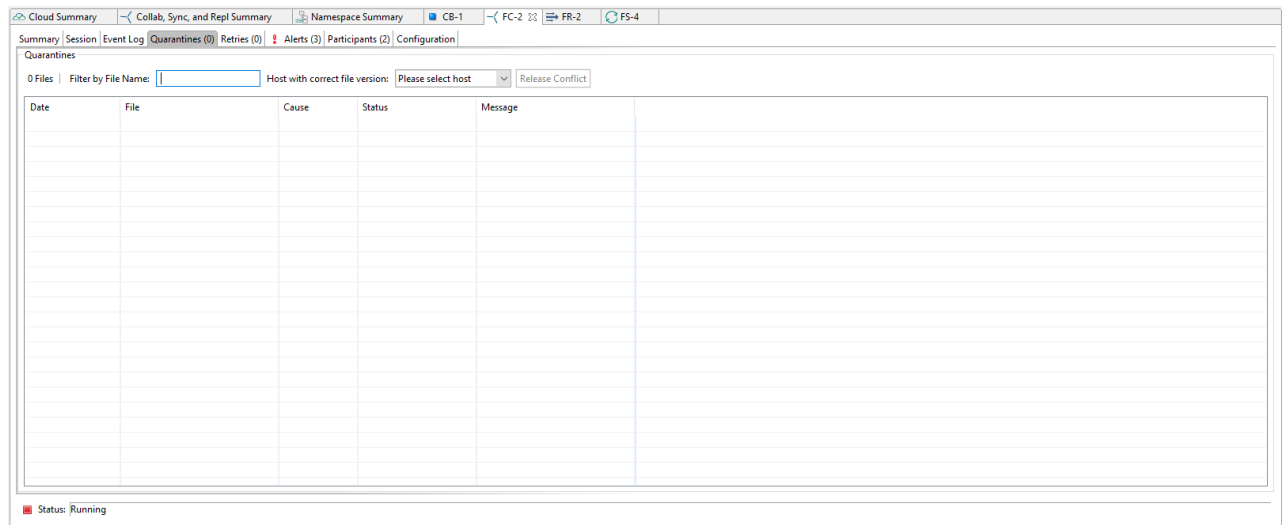
Date	Severity	Type	Host	Is Source	File	Comments	Message	Username	File Size	Modified Time
04-20-2021 14:26:23	INFO	Scan Complete		true			scan completed for path "\\", Scan Type: Full Directory, # Files=6,000, # Directories=59, Total Siz...			
04-20-2021 14:25:41	INFO	Scan Start		true			Scan Type: Full Directory			
04-20-2021 14:25:31	INFO	Watch Directory	DGAgent2	true						
04-20-2021 14:25:31	INFO	Watch Directory	DGAgent1	true						
04-20-2021 14:25:06	INFO	Install File Disposer	DGAgent2	true						
04-20-2021 14:25:06	INFO	Install File Disposer	DGAgent1	true						
04-20-2021 14:25:03	INFO	Collaboration Session Started	DGAgent2	true						
04-20-2021 14:25:03	INFO	Collaboration Session Started	DGAgent1	true						

The **Actions** menu provides the following options:

<b>Refr esh Vie w</b>	Refresh all information provided in the table. This can also be done from the right-click context menu of the table.
<b>Clea r Eve nts</b>	Remove all items from the table. This can also be done from the right-click context menu of the table.

### Quarantines Tab

The **Quarantines** tab displays a list of files (a) for which file conflicts could not be automatically resolved or (b) retries have failed after the maximum number of attempts. Files in this list will no longer be synchronized or protected with file locks until a winning file is picked through the PeerGFS user interface.

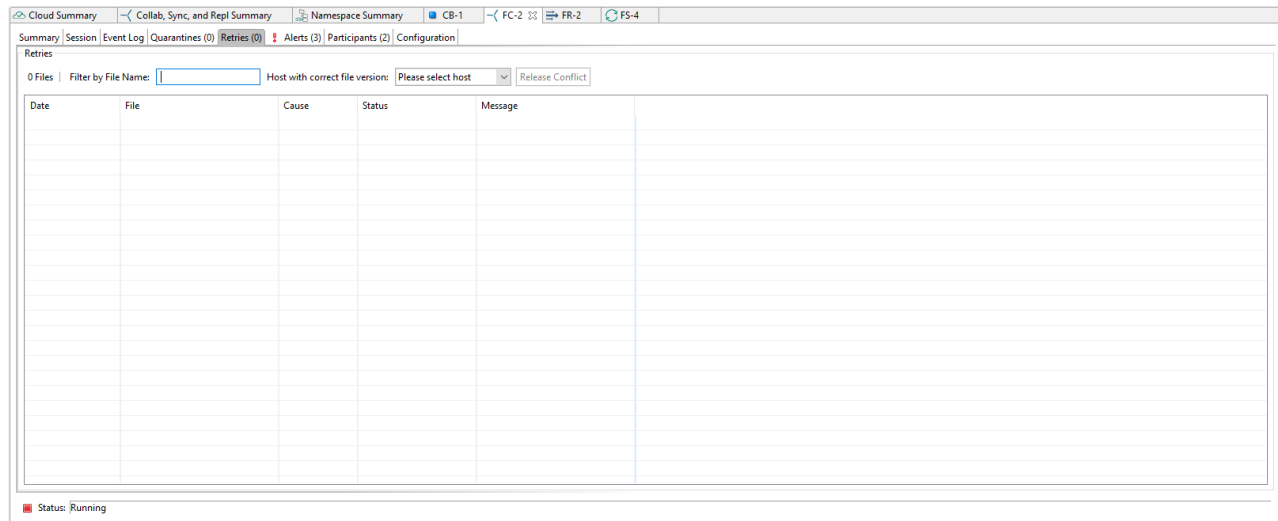


The context menu for the table contains the following actions:

<b>Refresh View</b>	Refresh all information provided in the table.
<b>Purge All Quarantines</b>	Clears all files from the quarantines list.
<b>Copy Details</b>	Copies the quarantine information for the selected file to your clipboard.

### Retries Tab

The **Retries** tab displays the files currently in the **Retries** list. Files are put into the retry list if certain errors are thrown when trying to synchronize a file between locations. Synchronization of a file in this list will be retried every minute for a maximum of 60 attempts. The frequency of attempts and the maximum number of attempts are configurable.



The context menu for the table contains the following actions:

<b>Refresh View</b>	Refresh all information provided in the table.
<b>Purge All Quarantines</b>	Clears all files from the <b>Quarantines</b> tab.
<b>Copy Details</b>	Copies the quarantine information for the selected file to your clipboard.

### Alerts Tab

The **Alerts** tab allows you to view any alerts relevant to the running File Collaboration job. Items shown here are based on the configured Alerts Severity setting on the Logging and Alerts configuration page. You can specify the maximum number of alerts to store in the table by adjusting the Display Alerts spinner located in the top right corner of the panel. The alerts are also written to a tab delimited file named **fc\_alert.log** within the subdirectory 'Hub/logs' within the installation directory of Peer Management Center. See the [Logging and Alerts](#) settings for more information about log files.

You can click on any column header to sort by that column. For example, clicking on the Severity column will sort by alert severity. Warnings are displayed in light gray, while errors and fatal alerts are displayed in red. In general, you should not see any alerts, but if an error or fatal alert occurs, it usually means something is wrong with the collaboration session. It may need to be restarted or



a configuration setting may need to be changed. You should consult the text in the message field for details on what occurred.

Received Date	Severity	Type	Host	Message
04-20-2021 14:26:20	WARNING	Application	DGAgent1	Recursive reparse point folder detected during scan, excluding folder path=C:\Users\Public\Documents\...
04-20-2021 14:26:20	WARNING	Application	DGAgent1	Recursive reparse point folder detected during scan, excluding folder path=C:\Users\Public\Documents\...
04-20-2021 14:26:20	WARNING	Application	DGAgent1	Recursive reparse point folder detected during scan, excluding folder path=C:\Users\Public\Documents\...
04-20-2021 14:24:41	ERROR	Application	DGAgent2	Agent service on host DGAgent2 was shutdown while job was running.
04-20-2021 13:58:33	WARNING	Application	DGAgent1	Recursive reparse point folder detected during scan, excluding folder path=C:\Users\Public\Documents\...
04-20-2021 13:58:33	WARNING	Application	DGAgent1	Recursive reparse point folder detected during scan, excluding folder path=C:\Users\Public\Documents\...
04-20-2021 13:58:33	WARNING	Application	DGAgent1	Recursive reparse point folder detected during scan, excluding folder path=C:\Users\Public\Documents\...
04-20-2021 13:56:17	WARNING	Application	DGAgent1	Unsupported Host Configuration: 8.3 short file name is enabled for Host DGAgent1
04-20-2021 13:52:37	ERROR	Application	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command: Host Reply Timeout (Connected)
04-20-2021 13:49:30	ERROR	Application	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command: Host Reply Timeout (Connected)

The context menu for the table contains the following actions:

<b>Refresh View</b>	Refresh all information provided in the table. This can also be done from the right-click context menu of the table.
<b>Clear Events</b>	Remove all items from the table. This can also be done from the right-click context menu of the table.

## Participants Tab

The **Participants** tab is divided into two sections:

- [Host Participants](#)
- [Host Participant State Change Log](#)

**Cloud Summary** | Collab, Sync, and Repl Summary | Namespace Summary | CB-1 | FC-2 | FR-2 | FS-4

---

Summary | Session | Event Log | Quarantines (0) | Retries (0) | Alerts (3) | **Participants (2)** | Configuration

### Host Participants

Host	Root Path	Status	State	Message
DGAgent1	C:\Users\Public	Participating	Active	
DGAgent2	\\AFS2\Share1	Participating	Active	

### Host Participant State Change Log

Filter by: Host:  Status:   
State:

Date	Host	Status	State	Message
04-20-2021 15:45:34	DGAgent1	Participating	Active	
04-20-2021 15:45:34	DGAgent2	Participating	Active	
04-20-2021 15:45:10	DGAgent2	Participating	Active	
04-20-2021 15:45:10	DGAgent1	Participating	Active	
04-20-2021 14:25:01	DGAgent1	Participating	Active	
04-20-2021 14:25:01	DGAgent2	Participating	Active	

Status: Running

## Host Participants

The **Host Participants** section contains a table that displays all the current [host participants](#) for the selected File Collaboration job. The **State** column displays activity status occurring on the hosts. If a host has become unavailable, an error message is displayed in red next to the failed host.

The following options are available in the right-click context menu for this section:

<b>Disable Host Participant</b>	Temporarily disables the selected participant from taking part in the File Collaboration job. You might want to do this if the host is experiencing temporary network outages.
<b>Cancel Auto Restart</b>	This menu item is only available if the global auto-restart functionality is enabled and the selected host has been removed from the File Collaboration job that is currently being viewed. The canceling of the auto-restart functionality for the host will only be in effect until the next time you start the File Collaboration job. If quorum has been lost for the job, canceling auto-restart on all unavailable hosts will prevent the job from automatically restarting. If quorum has not been lost, canceling auto-restart will simply prevent a host from automatically re-joining collaboration.

## Host Participant State Change Log

The **Host Participant State Change Log** section contains a table that displays the most recent host participant state changes, e.g., when a host was removed from collaboration session, or when a host came back online.

The **Host Participant State Change Log** is a log of all host participant status changes (e.g., Collaborating, Not Collaborating) and/or state changes (e.g., Active, Pending Restart) of a host participant. This table is limited to 250 rows and can be filtered by host, by status, and by state.

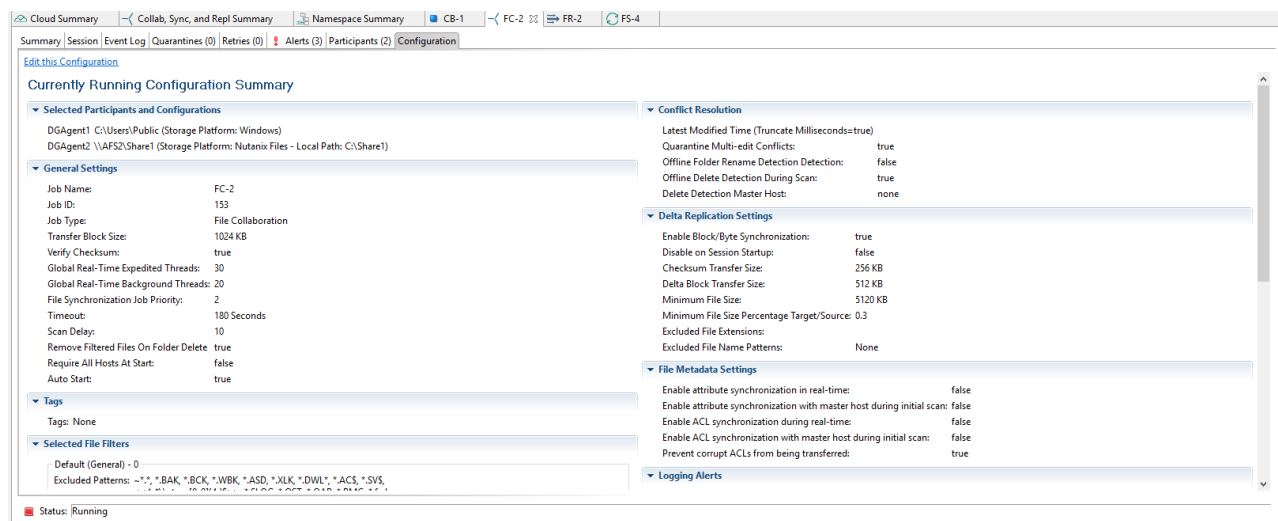
The following options are available in the right-click context menu for this section:

<b>Refresh View</b>	Refresh all information provided in the table.
<b>Clear Events</b>	Remove all items from the table.

### Configuration Tab

The **Configuration** tab displays a quick summary of all configurable items for the selected job.

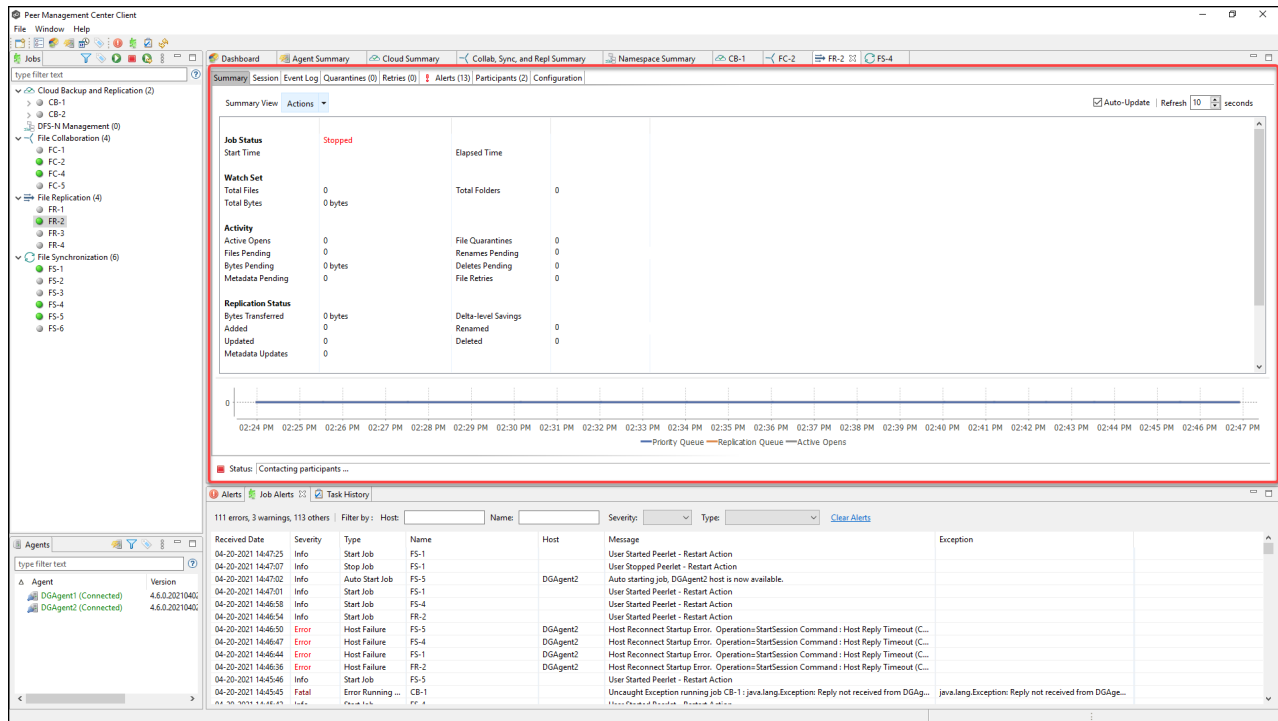
Each page of the File Collaboration Configuration edit wizard is represented in its own part of the view and can be collapsed if desired. Clicking **Edit this Configuration** opens the [File Collaboration Configuration edit wizard](#) where you can edit the current configuration.



To monitor a specific File Replication job, open its runtime view.

Each File Replication job has a runtime view that show a combination of real-time file I/O activity, history, and configuration. This runtime view has six tabs:

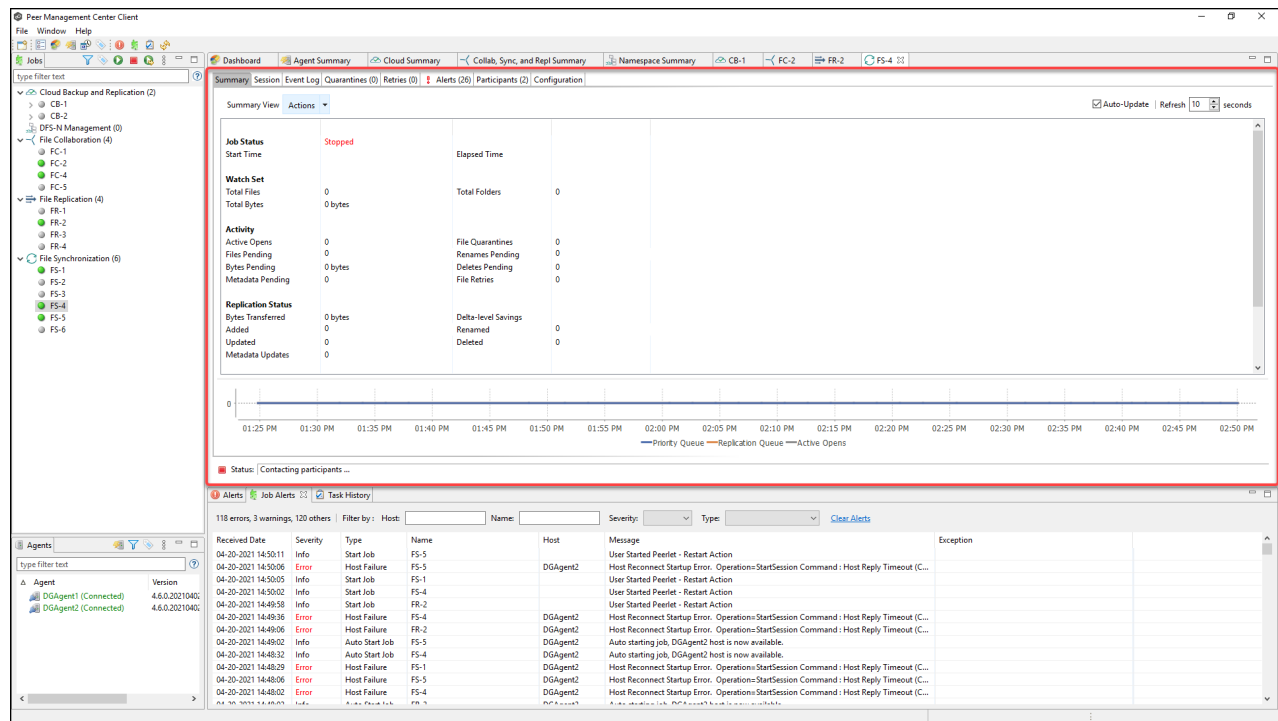
- Summary
- Session
- Event Log
- Quarantines
- Retries
- Alerts
- Participants
- Configuration



To monitor a specific File Synchronization job, open its runtime view.

Each File Synchronization job has a runtime view that show a combination of real-time file I/O activity, history, and configuration. This runtime view has six tabs:

- Summary
- Session
- Event Log
- Quarantines
- Retries
- Alerts
- Participants
- Configuration



## Summary Views

The **summary** views are displayed in the upper right quadrant of the Peer Management Center interface. You can use the summary views to monitor the overall health of your jobs and agents. You can [set summary views to be automatically displayed](#) when Peer Management Center is started.

A summary view typically has several tabs. For example, in the following figure, the summary view for File Collaboration, File Synchronization, and File Replication jobs is displayed; this view contains two tabs.

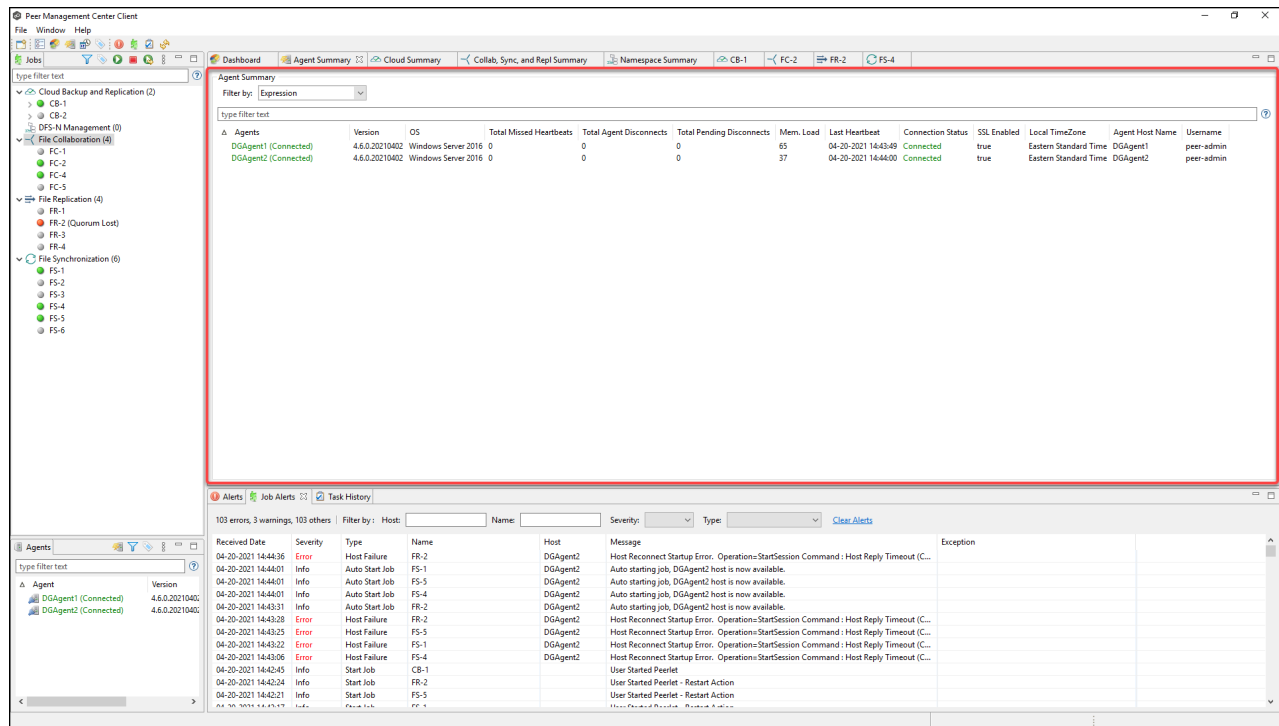
The screenshot displays the Peer Management Center Client interface. The main window is titled 'Collab, Sync, and Repl Summary'. It features a sidebar on the left with a tree view showing the hierarchy of jobs: Cloud Backup and Replication (2), DFS-N Management (0), File Collaboration (4), File Replication (4), File Synchronization (8), and Agents. The main area shows a table of job details with columns: Name, Overall Status, Job Type, Failed Hosts, Quorum, Retries, Errors, Warnings, Open Files, Pending Bytes, Pending Events, Queued Items, Background..., Scan Status, Elapsed Tl..., and Session Structure. The table lists various jobs such as FC-1, FC-2, FC-3, FC-4, FC-5, FR-1, FR-2, FR-3, FR-4, FS-1, FS-2, FS-3, FS-4, FS-5, and FS-6. Below the table, there is a summary bar showing 'Active Jobs -> Failed Participants: 2 of 2 | Bytes Pending: 0 bytes | Bytes Transferred: 0 bytes | Opens: 0 | Initial Scan Completed: 2 of 6 | Total Size: 713.23 MB | Total Files: 11920 | Total Directories: 116'. At the bottom, there is an 'Alerts' section with a table of alerts including Received Date, Severity, Type, Name, Host, Message, and Exception.

The summary views include:

- [Agent Summary view](#) - Displays summary information about the Agents.
- [Cloud Summary view](#) - Displays summary information about running Cloud Backup and Replication jobs.
- [Collab, Sync, and Repl Summary view](#) - Displays summary information about running File Collaboration, and File Replication jobs
- [Namespace Summary view](#) - Displays summary information about running DFS-N Management jobs.

The **Agent Summary** view displays a list of all known Agents deployed and their detailed status information, which can be used to assess the health of the environment. This summary view has a single tab.

The **Agent Summary** view is updated in real-time and can be filtered by using an expression or by built-in categories such as **Connected**, **Disconnected**, and **Needing Upgrade**.



To display the Agent Summary view, use one of the following methods:

- Select **Show Agent Summary** from the **Window** menu.
- Click the **Show Agent Summary** icon in the main [PMC toolbar](#) or in the [Agents view toolbar](#).

Use the **Cloud Summary** view to monitor the overall health of your Cloud Backup and Replication jobs. This view is the first place to check to see the status of your Cloud Backup and Replication jobs.

This view can be [set to be automatically displayed](#) when Peer Management Center is started and can be opened at any other time by double-clicking the job type name **Cloud Backup and Replication** in the [Jobs view](#) or by selecting **View Cloud Summary** from the toolbar in the **Jobs** view.

This view has four tabs:

- **Volume Summary** – Displays the volumes associated with jobs. The color of the icon next to a volume name quickly indicates the status of the job associated with that volume—a

green icon indicates an active job; a gray icon indicates an inactive job, and a red icon indicates a problem with a job.

- **Job Summary** – Displays the status of all Cloud Backup and Replication jobs.
- **Destination Statistics** – Displays the total number of files that have been replicated since the first run of the jobs and other statistics.
- **Tasks** – Displays a high-level view of activities such as snapshots, and recovery processes, and background events for all Cloud Backup and Replication jobs.

The screenshot shows the Peer Management Center Client interface. The main window displays the 'Job Summary' view, which lists various jobs and their statuses. The interface includes a sidebar on the left with a tree view of job categories, a top toolbar with tabs for Dashboard, Agent Summary, Cloud Summary, Collab, Sync, and Repl Summary, and Namespace Summary. The main pane shows a table of jobs with columns for Volume, Job, Management, Storage Device, Storage Type, Destination Type, Destination, Status, Mode, Scan Status, Host Scan, Scan pending, Real-time pen., Retry pending, and VSS pending. Below the table is an Alerts section showing a list of errors and warnings with columns for Received Date, Severity, Type, Name, Host, Message, and Exception.

Use the **Collab, Sync, and Repl Summary** view to monitor the overall health of your File Collaboration, File Replication, and File Synchronization jobs. This view is the first place to check to see the status of your File these job types.

This view can be [set to be automatically displayed](#) when when Peer Management Center is started and can be opened at any other time by double-clicking one of the job type names (**File Collaboration, File Replication, or File Synchronization**) in the [Jobs view](#) or by selecting **View Collab, Sync, and Repl Summary** from the **Jobs** view toolbar.

This view has two tabs:



- [Summary](#)
- [Reports](#)

The screenshot shows the Peer Management Center Client interface. The left sidebar contains navigation options: Cloud Backup and Replication (2), Cloud Management (0), File Collaboration (4), File Replication (4), and File Synchronization (8). The main window displays the 'Summary' tab, which shows a table of jobs. The table has columns for Name, Overall Status, Job Type, Failed Hosts, Quant, Retries, Errors, Warnings, Open Files, Pending Bytes, Pending Events, Queued Items, Background, Scan Status, Elapsed TL, and Session Structure. Below the table, there are sections for Alerts, Job Alerts, and Task History.

Name	Overall Status	Job Type	Failed Hosts	Quant	Retries	Errors	Warnings	Open Files	Pending Bytes	Pending Events	Queued Items	Background	Scan Status	Elapsed TL	Session Structure
FC-1	Stopped	File Collaboration	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FC-2	Running	File Collaboration	0	0	0	0	0	0	0 bytes	0	0	0	Completed - 00:00:41	00:19:27	Size: 345.92 MB, File...
FC-4	Running	File Collaboration	8	0	0	1	0	0	0 bytes	0	0	0	Scanning Directories -	00:19:09	Size: 42.3 MB, File...
FC-5	Stopped	File Collaboration	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FR-1	Stopped	File Replication	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FR-2	Contacting participants ...	File Replication	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:56	Size: 0 bytes, File...
FR-3	Stopped	File Replication	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FR-4	Stopped	File Replication	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-1	Contacting participants ...	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:26	Size: 0 bytes, File...
FS-2	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-3	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...
FS-4	Contacting participants ...	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:26	Size: 0 bytes, File...
FS-5	Contacting participants ...	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:26	Size: 0 bytes, File...
FS-6	Stopped	File Synchronization	0	0	0	0	0	0	0 bytes	0	0	0	Stopped	00:00:00	Size: 0 bytes, File...

Active Jobs -> Failed Participants: 0 of 2 | Bytes Pending: 0 bytes | Bytes Transferred: 0 bytes | Opens: 0 | Initial Scans Completed: 1 of 6 | Total Size: 388.22 MB | Total Files: 11328 | Total Directories: 116

Alerts | Job Alerts | Task History

103 errors, 3 warnings, 103 others | Filter by: Host | Name | Severity | Type | Clear Alerts

Received Date	Severity	Type	Name	Host	Message	Exception
04-20-2021 14:44:36	Error	Host Failure	FR-2	DGAgent2	Host Reconnect Startup Error. Operations=StartSession Command: Host Reply Timeout (C...	
04-20-2021 14:44:01	Info	Auto Start Job	FS-1	DGAgent2	Auto starting job, DGAgent2 host is now available.	
04-20-2021 14:44:01	Info	Auto Start Job	FS-5	DGAgent2	Auto starting job, DGAgent2 host is now available.	
04-20-2021 14:43:31	Info	Auto Start Job	FR-2	DGAgent2	Auto starting job, DGAgent2 host is now available.	
04-20-2021 14:43:28	Error	Host Failure	FR-2	DGAgent2	Host Reconnect Startup Error. Operations=StartSession Command: Host Reply Timeout (C...	
04-20-2021 14:43:25	Error	Host Failure	FS-5	DGAgent2	Host Reconnect Startup Error. Operations=StartSession Command: Host Reply Timeout (C...	
04-20-2021 14:43:22	Error	Host Failure	FS-1	DGAgent2	Host Reconnect Startup Error. Operations=StartSession Command: Host Reply Timeout (C...	
04-20-2021 14:43:06	Error	Host Failure	FS-4	DGAgent2	Host Reconnect Startup Error. Operations=StartSession Command: Host Reply Timeout (C...	
04-20-2021 14:42:45	Info	Start Job	CB-1	DGAgent2	User Started Peerlet	
04-20-2021 14:42:34	Info	Start Job	FR-2		User Started Peerlet - Restart Action	
04-20-2021 14:42:21	Info	Start Job	FS-5		User Started Peerlet - Restart Action	

## Summary Tab

The **Summary** tab aggregates critical status and statistical information from all File Collaboration, File Synchronization, and File Replication jobs in a single table. It presents overall job status, basic pending, and bytes transferred statistics. See the [Reports tab](#) for more detailed pending activity information.

Information in this view can be sorted and filtered. Operations such as starting, stopping, and editing multiple job at once are available, in addition to the ability to clear [job alerts](#) and purge [quarantines](#) from stopped jobs. Scroll the view horizontally to see all of its columns.

For performance reasons, this tab is not updated in real-time. However, it can be set to automatically update every few seconds. Select the **Auto-Update** checkbox to enable this functionality; set the refresh interval (in seconds) in the **Refresh** checkbox. Each refresh cycle will update the totals across all active jobs listed at the bottom of the view.

Name	Overall Status	Job Type	Failed Hosts	Quaran...	Retries	Errors	Warnin...	Open F...	Pending By...	Queued Ite...	Backgr...	Scan Status	Elapse...	Session Structure
FC-4	Running	File Collaboration		0	0	0	1	0	0 bytes	0	0	Completed ----	08:20:17	Size: 21.49 MB, Fil...
FC-3	Halted. (Quorum Lost)	File Collaboration	DGAgent2	0	0	1	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FR-4	Stopped	File Replication		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FC-2	Running	File Collaboration		0	0	0	4	0	0 bytes	0	0	Completed ----	08:20:16	Size: 345.92 MB, Fi
FC-5	Stopped	File Collaboration		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FS-1	Halted. (Quorum Lost)	File Synchronization	DGAgent2	0	0	1	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FS-3	Stopped	File Synchronization		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FC-1	Stopped	File Collaboration		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FR-2	Stopped	File Replication		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FS-4	Halted. (Quorum Lost)	File Synchronization	DGAgent2	0	0	1	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FS-5	Halted. (Quorum Lost)	File Synchronization	DGAgent2	0	0	1	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
North Am...	Stopped	File Locking		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:
FR-1	Stopped	File Replication		0	0	0	0	0	0 bytes	0	0	Stopped	00:00:00	Size: 0 bytes, Files:

Active Jobs -> Failed Participants: 1 of 2 | Bytes Pending: 0 bytes | Bytes Transferred: 0 bytes | Opens: 0 | Initial Scans Completed: 2 of 6 | Total Size: 367.4 MB | Total Files: 6018 | Total Directories: 69

You can change which items are displayed in the table by [filtering the list](#) or by its state (Running in Good State, Running with Quarantines, Not Running - Stopped, Running with Disconnected Agents, Lost Quorum), Job Name, Participant, Session Status) or by [tags](#). Select the desired filter or enter your own expression in the text field to the right of the **Filter by** drop-down list.

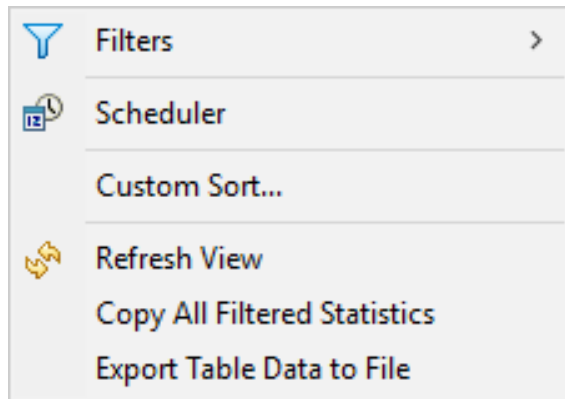
## Column Descriptions

Key columns in this view are:

- **Pending Bytes** – Presents the number of bytes pending synchronization which includes scan work, real-time, as well as bulk adds.
- **Pending Events** – (Hidden by default) Presents the number of total pending items in Fast Queue, Slow Queue and Bulk Adds. This does not include Renames, Deletes, and Bulk Security changes. This can contain multiple events for a single file because target locks are separate operations, (e.g., if you add one file, there will be two events for this in queue.) Scan synchronization is not included and metadata synchronization is not reflected here.
- **Queued Items** – Presents the number of items in just the Fast and Slow queue (does not include bulk adds).
- **Background Sync.** – Presents the number of initial and full scan items in queue.

Additional columns can be added to and removed from the table using the right-click context menu.

## Actions Menu



The **Actions** menu provides the following options:

Option	Description
<b>Filters</b>	Allows you to select predefined or user-defined filters and to save/manage <a href="#">list filters</a> . Default job filters include Failed Jobs, Jobs with Backlog, and Running Scans.
<b>Scheduler</b>	Opens the Task Scheduler.
<b>Custom Sort...</b>	Enables you to define multi-level sort criteria for the table. This is useful for keeping important items visible at the top. For example, you may choose to create a sort level where the Overall Status column is sorted in ascending order by default.
<b>Refresh View</b>	Refreshes all information displayed in the table.
<b>Copy All Filtered Statistics</b>	Copies detailed information to the system clipboard for all items current displayed in the table, taking any filters into account. This information can then be pasted into a text editor.
<b>Export Table Data to File</b>	Dumps the entire contents of the table to a text file that can be viewed in any text editor.

## Reports Tab

The **Reports** tab aggregates critical statistical information from all File Collaboration, File Synchronization, and File Replication jobs in a single table. The **Reports** tab is visible when the **Enable Advanced Reporting Tab** option on the [Collab, Sync, and Repl Summary](#) page in [Preferences](#) is selected.

The **Reports** tab is especially useful to view the number of files that are in the queue waiting to be synchronized (shown in the **File Sync Queue** column). Scroll the view horizontally to see all of its columns

For performance reasons, this tab is not updated in real-time. However, it can be set to automatically update every few seconds. Select the **Auto-Update** checkbox to enable this functionality; set the refresh interval (in seconds) in the **Refresh** checkbox. Each refresh cycle will update the totals across all active jobs listed at the bottom of the view.

Name	File Sync Queue	Real-Time Qu...	Queued Bytes	Mods	Adds	Metadata	Scan Queue	Deletes	Renames	Event Queue	Scheduled Replication Pending	Scheduled Replication Process
FC-4	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FC-3	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FR-4	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FC-2	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FC-5	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FS-1	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FS-3	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FC-1	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FR-2	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FS-4	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FS-5	0	0	0 bytes	0	0	0	0	0	0	0	0	0
North A...	0	0	0 bytes	0	0	0	0	0	0	0	0	0
FR-1	0	0	0 bytes	0	0	0	0	0	0	0	0	0

Global Event Processor Queue: 0 | Pending Scans: 0 | Running Scans: 0

Items in the table can be filtered by a [filter expression](#), job name, [Participant](#), Session Status, or by [tags](#). Select the desired filter or enter your own expression in the text field to the right of the **Filter** drop-down list. Check the **Auto-Hide** button to hide all jobs which have no pending activity.

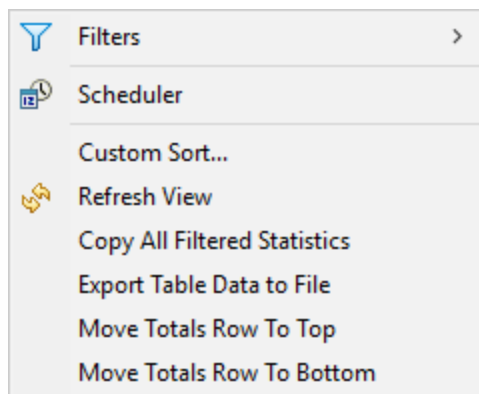
## Column Descriptions

Column	Description
<b>Name</b>	The name of the job.

Column	Description
<b>File Sync Queue</b>	The number of files that are in queue waiting to be processed. The number of threads available for this queue is set by the <b>Real-Time Background Threads</b> field in the <a href="#">Performance</a> preferences for Collaboration, Synchronization, and Replication jobs.
<b>Real-Time Queue</b>	The number of open/close events that are in queue waiting to be processed. The number of threads available to process this queue is set by the <b>Real-Time Expedited Threads</b> field in the <a href="#">Performance</a> preferences for Collaboration, Synchronization, and Replication jobs.
<b>Queued Bytes</b>	The number of bytes that are in queue waiting to be processed.
<b>Mods</b>	The number of file update events waiting to be processed for each job.
<b>Adds</b>	The number of file add events waiting to be processed for each job.
<b>Metadata</b>	The number of metadata updates waiting to be processed for each job.
<b>Background Transfers</b>	The number of files in the queue waiting to be synchronized as a result of a file system scan.
<b>Deletes</b>	The number of files deleted on a source host that are waiting to be processed.
<b>Renames</b>	The number of files renamed on a source host that are waiting to be processed.
<b>Event Queue</b>	The number of events that are queued up to run for each job.
<b>Slow Expedited Queue</b>	The number of events that are queued in the Slow Expedited Queue for each job.

Column	Description
<b>Fast Expedited Queue</b>	The number of events that are queued in the Fast Expedited Queue for each job.
<b>Scheduled Replication Pending</b>	The number of events that are queued awaiting replication at a scheduled time or interval.
<b>Scheduled Replication Processing</b>	The number of events that are queued awaiting scan to make sure source is correct version before releasing for replication at a scheduled time or interval.
<b>Scheduled Replication Transfers</b>	The number of events that are queued awaiting replication until a thread is available.

## Actions Menu

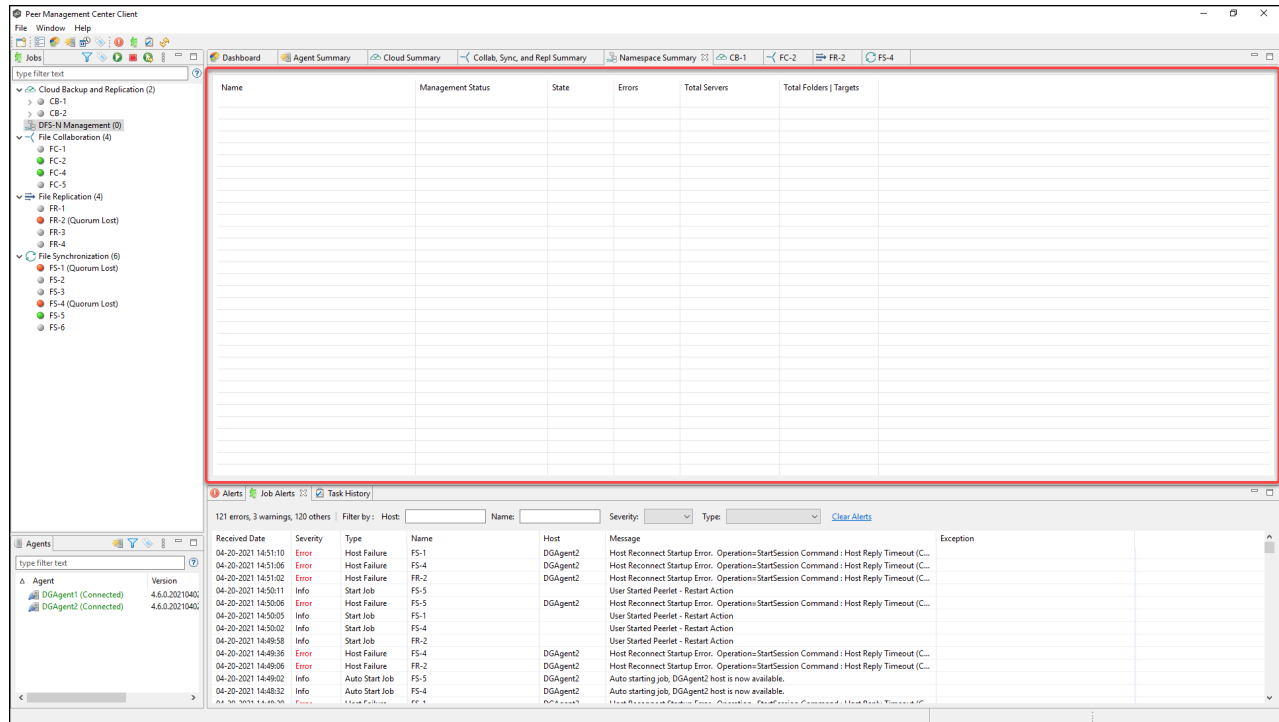


The **Actions** menu provides the following options:

Option	Description
<b>Filters</b>	Allows you to select predefined or user-defined filters and to save/manage <a href="#">list filters</a> . Default job filters include Failed Jobs, Jobs with Backlog, and Running Scans.
<b>Scheduler</b>	Opens the Task Scheduler.
<b>Custom Sort...</b>	Enables you to define multi-level sort criteria for the table. This is useful for keeping important items visible at the top. For example, you may choose to create a sort level where the Overall Status column is sorted in ascending order by default.
<b>Refresh View</b>	Refreshes all information displayed in the table.
<b>Copy All Filtered Statistics</b>	Copies detailed information to the system clipboard for all items current displayed in the table, taking any filters into account. This information can then be pasted into a text editor.
<b>Export Table Data to File</b>	Dumps the entire contents of the table to a file that can be viewed in any text editor.
<b>Move Totals Row To Top</b>	Moves the Totals row to the top of the table.
<b>Move Totals Row To Bottom</b>	Moves the Totals row to the bottom of the table.

Use the **Namespace** view to monitor the overall health of your DFS-N Management jobs. This view is the first place to check to see the status of your DFS-N Management jobs. This view has a single tab.

This view can be [set to be automatically displayed](#) when Peer Management Center is started and can be opened at any other time by double-clicking the job type name **DFS-N Management** in the [Jobs view](#) or by selecting **View Namespace Summary** from the toolbar in the **Jobs** view.

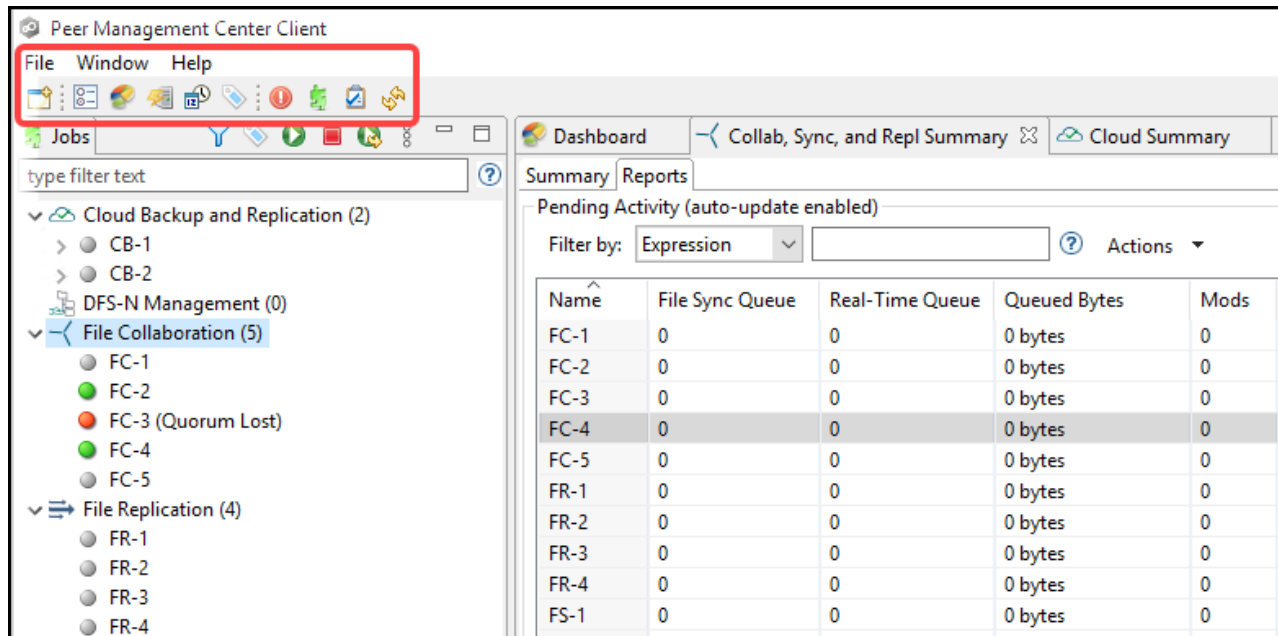


## Main Window Menus and Toolbar

The main window of Peer Management Center has three menus and a toolbar:

- [File](#)
- [Window](#)
- [Help](#)





## File Menu

The **File** menu in the Peer Management Center main window has the following commands:

Com man d	Description
<b>New Job</b>	Starts the Create New Job wizard.
<b>Close</b>	Closes the selected view.
<b>Close All</b>	Closes all views.
<b>Exit</b>	(Rich client only) Closes the Peer Management Center Client. Note that as long as the Peer Management Center Service remains running, all running jobs will continue to operate.

Command	Description
<b>Logout</b>	(Web client only) Logs the user out of the Peer Management Center Web client.

## Help Menu

The **Help** menu in the Peer Management Center main window has the following commands:

Command	Description
<b>User Guide</b>	Open the User Guide.
<b>Download Peer Agent Installer</b>	Opens the Peer Software website where you can download the Peer Agent installer compatible with this version of Peer Management Center.
<b>Peer Management Center Web Client</b>	Opens the Peer Management Center Web Client in a web browser.
<b>Peer Management Center API</b>	Opens the Peer Global File Service API in a web browser.
<b>Event Detection Analytics</b>	<p>Opens a submenu with the following options:</p> <ul style="list-style-type: none"> <li>• Run Event Detection Analytics for Hub Event Logs... - Runs event detections analytics immediately before the log files collected. PeerGFS can perform event detection analysis every night; however, this option allows you to receive the most up-to-date analytics.</li> <li>• Run Event Detection Analytics for a selected Hub Event Log File Directory...</li> </ul>

Command	Description
	<ul style="list-style-type: none"><li>• Run Even Detection Analytics for a selected Agent Outlog Log File Directory...</li></ul>
<b>Retrieve PMC/Agent Logs</b>	Collects and retrieve all useful log files for specified Peer Agents, Peer Management Center, and all jobs. This information is assembled into a single encrypted zip file that can optionally be uploaded to the Peer Software Technical Support. The collection and retrieval of the log and support files is performed in the background, which might take a while, depending on content size and network speed. Upon completion, you are notified and can view the zip file.
<b>Retrieve Broker Statistics</b>	Displays detailed statistical information about all messaging that has transpired for all connections (Peer Agents and Peer Management Center) to <a href="#">Peer Management Broker</a> .
<b>Thread Dump</b>	Gives options to generate a thread dump of the running Peer Management Center Client and Service, as well as the running Peer Management Broker service. Both can be used by Peer Software technical support to debug certain issues.
<b>Generate Memory Dump File</b>	Generates a memory dump of the running Peer Management Center Client and Service, which can be used by Peer Software Technical Support to debug certain issues.
<b>Compress DB on Restart</b>	(Rich client only) Compresses the database upon restart of the Peer Management Center Service. Select this option in cases where the database consumes a large amount of disk space.
<b>Check for Updates</b>	(Rich client only) Checks for updates to Peer Management Center. Minor releases can be automatically downloaded and installed. Major releases require a new license key and must be requested from Peer Software Technical Support.
<b>About Peer Management Center</b>	Displays version information and installation details.

## Window Menu

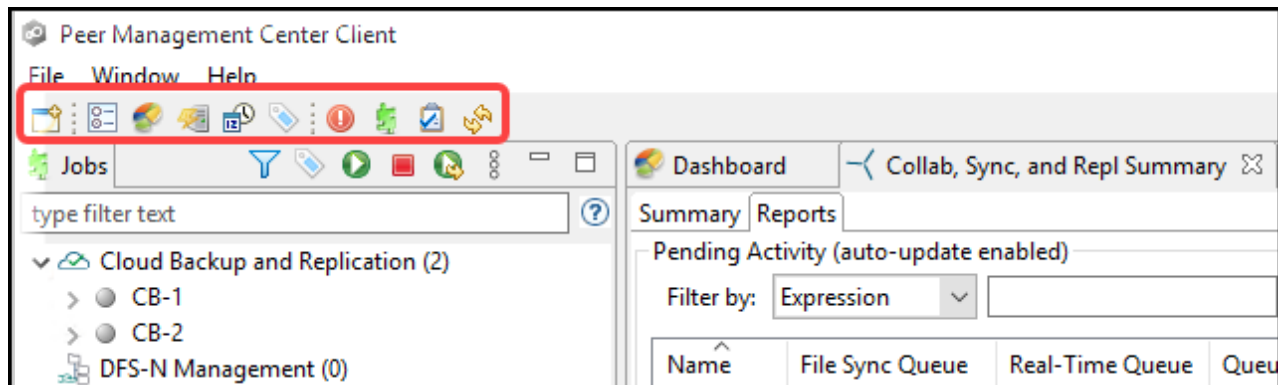
The **Window** menu in the Peer Management Center main window has the following commands:

Command	Description
<b>Reset Perspective</b>	Resets all current windows, views, and editors to their default size and layout.
<b>View Dashboard</b>	Displays the Dashboard, which displays metrics and key performance indicators from all running File Collaboration, File Replication, and File Synchronization jobs, and Peer Agents.
<b>Show Agent Summary</b>	Displays the <a href="#">Agent Summary</a> view, which displays a list of all known Peer Agents deployed and their detailed status information, which can be used to assess the health of the environment.
<b>Show Summary Views</b>	<p>Displays a submenu with the following options:</p> <ul style="list-style-type: none"> <li>• <b>Cloud Summary</b> - Displays the Summary view for Cloud Back and Replication jobs.</li> <li>• <b>Namespace Summary</b> - Displays the Summary view for DFS-N Management jobs.</li> <li>• <b>Collab, Sync, and Repl Summary</b> - Displays the Summary view for File Collaboration, File Replication, and File Synchronization jobs.</li> </ul>
<b>Show View</b>	<p>Displays a submenu with the following options:</p> <ul style="list-style-type: none"> <li>• <b>View Alerts</b> - Displays the <a href="#">Alerts view</a>, which displays Peer Management Center alerts such as Peer Agent connection status changes.</li> <li>• <b>View Job Alerts</b> - Displays the <a href="#">Job Alerts view</a>, which displays alerts such as job restarts.</li> <li>• <b>View Task History</b> - Displays the Task History view, which displays the status of tasks such as Daily Cleanup.</li> <li>• <b>View Progress</b> - Displays the Progress view, which displays information pertaining to any running background tasks within Peer Management Center.</li> </ul>

Command	Description
<b>Preferences</b>	Displays the <a href="#">Preferences</a> page, which enables the user to configure global settings for Peer Management Center, as well as settings for individual job types.
<b>Assign Tags</b>	Displays the <a href="#">Assign Tags</a> dialog where resources can be viewed, tagged, and assigned to categories. Tagging resources helps when managing large number of resources.
<b>Refresh</b>	Refreshes all open views and tabs.

## Toolbar

Use the toolbar in the main Peer Management Center window to quickly launch commonly performed actions.



The toolbar has the following buttons:

Button	Description
<b>New Job</b>	Opens the New Job wizard.
<b>Preferences</b>	Displays the <a href="#">Preferences</a> page, which enables the user to configure global settings for Peer Management Center, as well as settings for individual job types.
<b>View Dashboard</b>	Displays the Dashboard, which displays metrics and key performance indicators from all running File Collaboration, File Replication, and File Synchronization jobs, and Peer Agents.
<b>Show Agent Summary</b>	Displays the <a href="#">Agent Summary</a> view, which displays a list of all known Peer Agents deployed and their detailed status information, which can be used to assess the health of the environment.
<b>Task Scheduler</b>	Opens the Task Scheduler, which enables a user to schedule tasks that can be carried out by the Peer Management Center at scheduled times or intervals.
<b>Assign Tags</b>	Displays the <a href="#">Assign Tags</a> dialog where resources can be viewed, tagged, and assigned to categories. Tagging resources helps when managing large number of resources.
<b>View Alerts</b>	Displays the <a href="#">Alerts view</a> , which displays Peer Management Center alerts such as Peer Agent connection status changes.
<b>View Job Alerts</b>	Displays the <a href="#">Job Alerts view</a> , which displays job-related alerts such as job restarts.
<b>View Task History</b>	Displays the Task History view, which displays the status of tasks such as Daily Cleanup.
<b>Refresh</b>	Refreshes all current views and tabs.

## Tables

Tables are used throughout the Peer Management Center interface to present information. For example, the Job Alerts view contains a table displaying job-specific alerts:

Received Date	Severity	Type	Name	Host	Message
04-16-2021 15:37:23	Error	Configuration	FS-5	DGAgent2,DGAgent1	Disabled auto restart because maximum # (15) of restarts attempts was exceeded for host(s) DGAgent2,DGAgent1
04-16-2021 15:36:27	Error	Host Failure	FS-5	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)
04-16-2021 15:36:23	Error	Configuration	FS-1	DGAgent2,DGAgent1	Disabled auto restart because maximum # (15) of restarts attempts was exceeded for host(s) DGAgent2,DGAgent1
04-16-2021 15:35:27	Error	Host Failure	FS-1	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)
04-16-2021 15:35:23	Info	Auto Start Job	FS-5	DGAgent2	Auto starting job, DGAgent2 host is now available.
04-16-2021 15:34:27	Error	Host Failure	FS-5	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)
04-16-2021 15:34:23	Info	Auto Start Job	FS-1	DGAgent2	Auto starting job, DGAgent2 host is now available.
04-16-2021 15:33:47	Error	Host Failure	FS-1	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)
04-16-2021 15:33:23	Info	Auto Start Job	FS-5	DGAgent2	Auto starting job, DGAgent2 host is now available.
04-16-2021 15:32:53	Error	Configuration	FS-4	DGAgent2	Disabled auto restart because maximum # (15) of restarts attempts was exceeded for host(s) DGAgent2
04-16-2021 15:32:47	Error	Host Failure	FS-5	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)
04-16-2021 15:32:23	Info	Auto Start Job	FS-1	DGAgent2	Auto starting job, DGAgent2 host is now available.
04-16-2021 15:32:17	Error	Host Failure	FS-4	DGAgent2	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)

Most tables allow you to sort them by clicking on a column header.

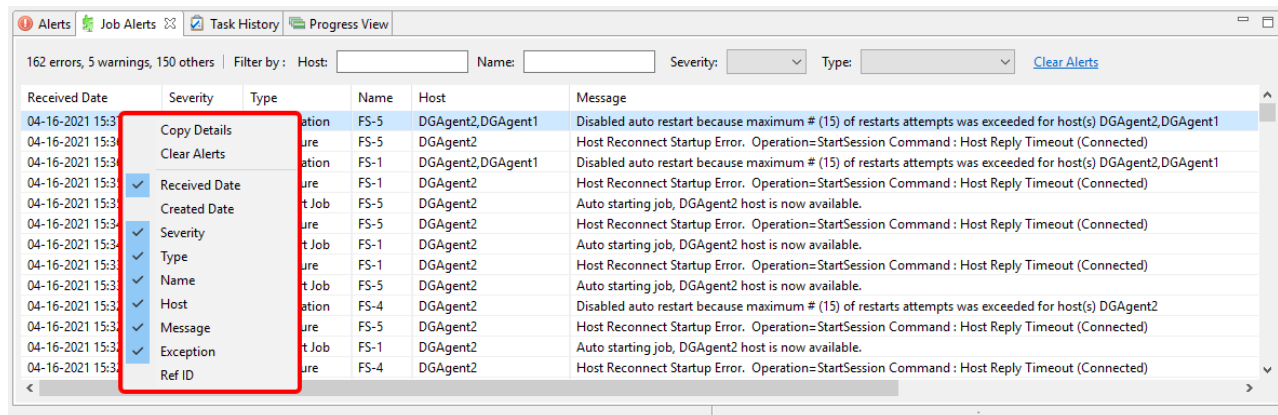
Most tables support double-clicking on any row to display a dialog containing details pertaining to that row. For example, clicking a row in the Job Alerts table displays detailed information for that particular alert:

**PMC Alert Details**

Received at	04-16-2021 15:36:27
Severity	Error
Category	Host Failure
Host Name	DGAgent2
Locally Generated at	04-16-2021 15:36:27
Name	FS-5
Message	Host Reconnect Startup Error. Operation=StartSession Command : Host Reply Timeout (Connected)
Ref ID	243

Click outside of popup to close

Right-clicking in a table displays a **context menu**. A context menu allow you to perform additional operations on the table. For example, you can choose which columns to hide and to display in the table. One very useful option available in many context menus is the ability to copy detailed information for one or more rows all at the same time. This information can then be pasted into any text editor.



## Basic Concepts

The topics in this section provide information on advanced functionality and configuration options available in Peer Management Center.

- [Email Alerts](#)
- [File and Folder Filters](#)
- [List Filters](#)
- [Logging](#)
- [SNMP Notifications](#)
- [Tags](#)

## Email Alerts

### Overview

An email alert notifies recipients when a certain type of event occurs, for example, file quarantined, session aborted, host failure, system alert. When an email alert is applied to a job, an alert is sent to all listed recipients whenever a selected event type is triggered by the job.

An email alert consists of a unique name, a selection of event types, and a list of email addresses. The available event types depend on the job type.



When you create a job, you can select an existing email alert to apply to the job or you can create a new alert and apply it to the job. Multiple email alerts can be applied to a job. You cannot modify an email alert while it is applied to a running job. You cannot delete an email alert while it is applied to any job. An alert can be applied to multiple jobs of the same type. Email alerts are defined in the [preferences](#) for a job type.

See [Email Configuration](#) for configuring an SMTP email connection. This must be configured before email alerts can be sent.

## Managing Email Alerts

You can create, edit, copy, and delete alerts.

To manage email alerts:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Select the job type from the navigation tree and expand it.
3. Select **Email Alerts** from the navigation tree.

The **Email Alerts** page lists existing email alerts for that job type.

## File and Folder Filters

### Overview

A file filter enables you to specify which files (and folders) should be included and/or excluded from a job's [watch set](#). Included files are subject to scan(s) and real-time event detection, while excluded files are not. Initially, all files are included and no files are excluded from a job, except for files matching the [predefined file filters](#) and [automatically excluded file types](#).

Filters can also operate on folders, allowing you to include and exclude folders from a job's watch set. For more information on folder filters, see [Folder Filters](#).

A file filter consists of a unique name and one or more [filter patterns](#). A filter can also be based on a file's [last modified time](#) and [file size](#). For more information on defining a filter pattern, see [Defining Filter Patterns](#). For more information on defining a filter pattern that can be used to filter folders, see [Filtering Folders](#).

## Types of File Filters

There are three types of file filters:

- **General** - Can be applied to any job type.
- **Synchronization Only** - Can be applied to File Collaboration jobs only. Select this filter type to exclude file types from being locked when a file open is detected on a participant in a File Collaboration job.
- **Locking Only** - Can be applied to File Collaboration jobs only. Select this filter type to exclude synchronization across the entire File Collaboration job so that only opens and closes are detected and acted on without any synchronization being performed.

For more information, see [Creating and Applying File Filters](#).

### Creating and Applying File Filters

You create a file filter in the **File and Folders** page of [Preferences](#) for a job type; the filter can then be applied to individual jobs of the same type. For example, a file filter created in [Cloud Backup and Replication Preferences](#) can be applied to any Cloud Backup and Replication job; a file filter created in [Collab, Sync, and Replication Preferences](#) can be applied to any File Collaboration, File Synchronization, or File Replication job. Multiple file filters can be applied to a single job.

In addition, there are also [predefined filters](#) that are applied to jobs; some of these predefined filters are automatically applied to certain job types.

For more information about creating a file filter, see:

- [Creating File Filters for a Cloud Backup and Replication Job](#)
- [Creating File Filters for File Collaboration, File Locking File Replication, and File Synchronization Jobs](#)

### Predefined File Filters

In addition to defining your own file filters, there are predefined file filters that can be applied to jobs. The predefined filters vary per job type.

File and Folder Filters					
Name	Type	Exclusions	Inclusions	Date Filter	Size Filter
Default	General	~*.*, *.BAK, *.BCK, *.WBK, *.ASD...	None Selected	Include all dates	None
File Collaboration Sync Only	Synchronization Only	None Selected	*.LOG, *.EXE, *.DLL, *.OTF,...	Include all dates	None
Invalid Characters	General	<<.*[. ]\$>>	None Selected	Include all dates	None
Locking Only	Locking Only	None Selected	\*	Include all dates	None
MacOS Exclusions	General	*\__MACOSX, *\TemporaryItem...	None Selected	Include all dates	None
PEER_Autodesk AutoCAD [General]	General	*.BAK, *.DWL	None Selected	Include all dates	None
Synchronizing Only	Synchronization Only	None Selected	\*	Include all dates	None
User Profile Exclusions	General	*\AppData\Roaming\Microsoft\...	None Selected	Include all dates	None

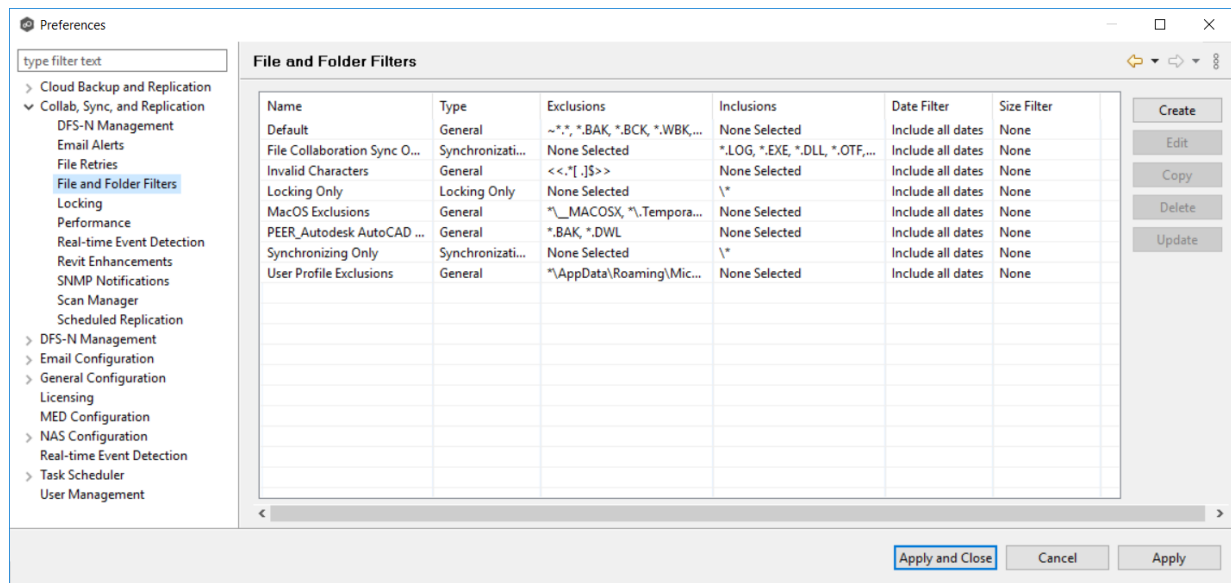
Two of the predefined filters, **Default** and **Invalid Characters**, are applied to all jobs by default. However, you can deselect a predefined filter for a specific job. Only the **Default** filter can be modified; none of the predefined file filters can be deleted.

In addition to these predefined filters, there are [file types that are automatically excluded](#) from a watch set for all job types.

To upgrade a predefined filter:

1. Select **Preferences** from the **Window** menu.
2. Expand **Cloud Backup and Replication** or **Collab, Sync, and Repl Summary** in the navigation tree, and then select **File and Folder Filters**.

Existing file filters are listed in the **File and Folder Filters** table.



3. Select the filter to upgrade, and then click **Upgrade**.

If an updated filter definition is available, a confirmation message lists the changes to the filter definition.

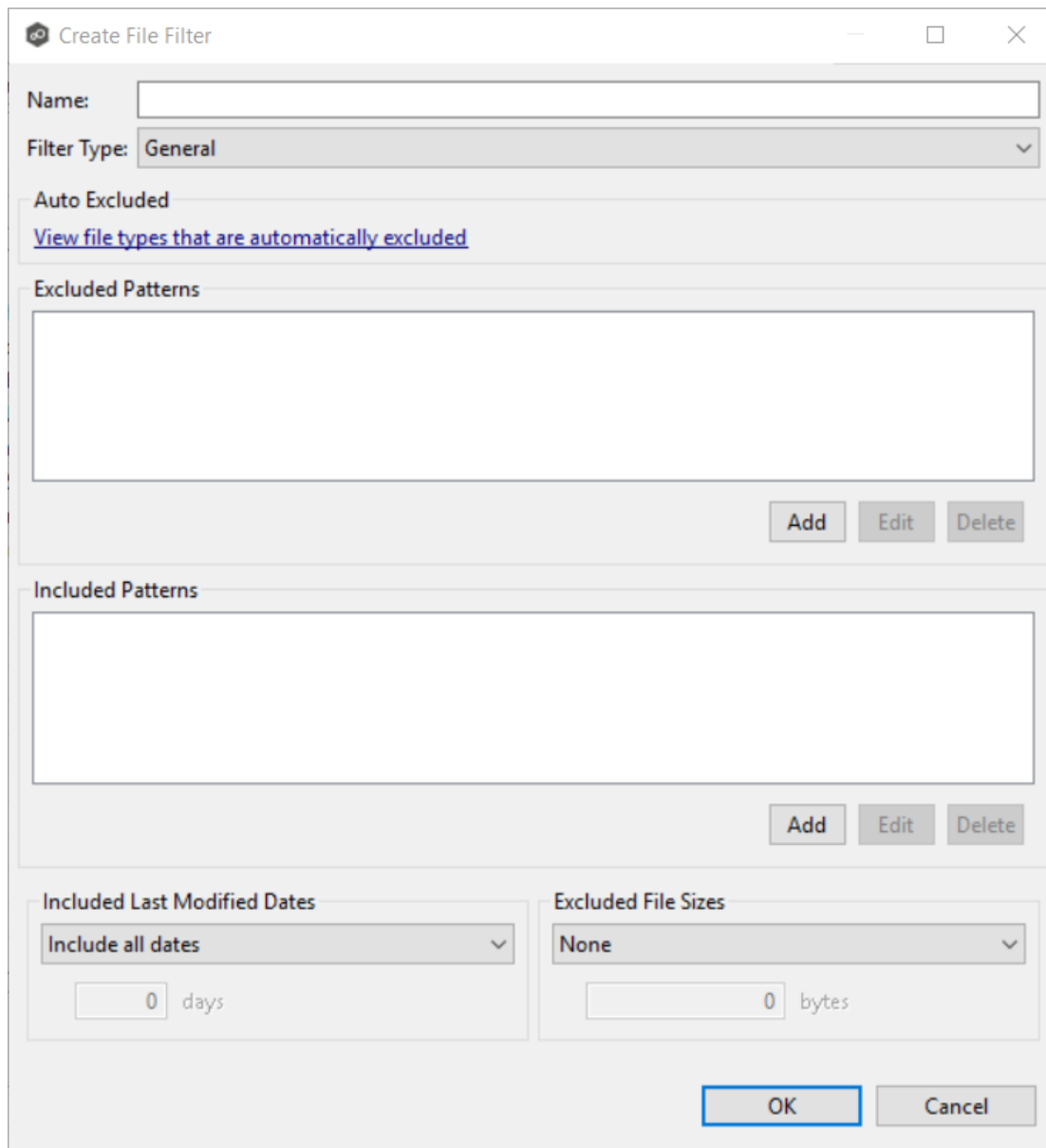
4. Click **OK** in the confirmation message.

The new file filter is listed in the **File Filters** table and can now be applied to jobs.

## Defining Filter Patterns

A **filter pattern** is a character string that defines a logical expression that is evaluated to determine which files and folders match the pattern. A file filter pattern can contain [complex regular expressions](#) and [wildcards](#). See [Folder Filters](#) for more information about what a folder filter pattern can contain.

Files and folders that match an **exclusion pattern** are excluded from the [watch set](#); files and folders that match an **inclusion pattern** are included the watch set. For example, in the following file filter definition, files with names ending in \*.dotx are excluded and files with names ending with \*.docx are included:



The "Create File Filter" dialog box is shown. It has a title bar with a close button. The "Name:" field is empty. The "Filter Type:" dropdown is set to "General". Below this is a section for "Auto Excluded" with a link "View file types that are automatically excluded". The "Excluded Patterns" section has a large text area and "Add", "Edit", and "Delete" buttons. The "Included Patterns" section also has a large text area and "Add", "Edit", and "Delete" buttons. At the bottom, there are two sections: "Included Last Modified Dates" with a dropdown set to "Include all dates" and a "0 days" input, and "Excluded File Sizes" with a dropdown set to "None" and a "0 bytes" input. "OK" and "Cancel" buttons are at the bottom right.

Create File Filter

Name:

Filter Type: General

Auto Excluded

[View file types that are automatically excluded](#)

Excluded Patterns

Add Edit Delete

Included Patterns

Add Edit Delete

Included Last Modified Dates

Include all dates

0 days

Excluded File Sizes

None

0 bytes

OK Cancel

You can use complex regular expressions in filter patterns. Use the following format for a regular expression:

<<regEx>>

For example, the following filter pattern contains a regular expression that finds AutoCAD temporary files (atmp files):

<<^.\*\\atmp[0-9]{4,}\$>>

Using the following regular expression in an exclusion pattern excludes any path containing a folder **XX** that also contains a child folder **YY**:

```
<<^.*\\XX\\YY(\\.*$|>)>>
```

The following files and folders **MATCH** the above expression:

```
\\projects\\xx\\yy
\\accounting\\projects\\xx\\yy\\file.txt
\\accounting\\projects\\xx\\yy\\zz\\file.txt
```

The following files and folders **DO NOT MATCH** the above expression:

```
\\projects\\accounting\\file.txt
\\projects\\xx\\y
\\projects\\xx\\yyy\\file.txt
\\accounting\\projects\\xx\\file.txt
\\accounting\\projects\\yy\\xx\\zz\\file.txt
```

For a good reference on regular expressions, see <http://www.regular-expressions.info/reference.html>

You can use the following wildcards in a file filter pattern to more easily cover well-known file extensions or names that follow established patterns.

<b>*</b>	Matches zero or more characters of any value
<b>?</b>	Matches one character of any value

The following examples show the use of a wildcard:

- \*.ext**      Filter files that end with the **.ext** extension
- ext\***      Filter files that begin with the string **ext**
- ext**        Filter files that contain the string **ext**

The following wildcard expressions are automatically applied as exclusion patterns and cannot be modified.

File Type	Exclusion Pattern
Temporary files generated by common applications	~\$*.* *.tmp *.\$\$\$ Any file without a file extension, e.g., abcdefg
Explorer System Files	desktop.ini, thumbs.db, and Windows shortcut file, e.g., *.lnk

You will generally want to exclude all temporary files created by the applications you use so they are not propagated to the target hosts. For example, if your [watch set](#) contains files created by AutoCAD applications, you should create a file filter to exclude the temporary files created by these applications.

Typically, AutoCAD files have the following extensions:

.AC\$

.SV\$

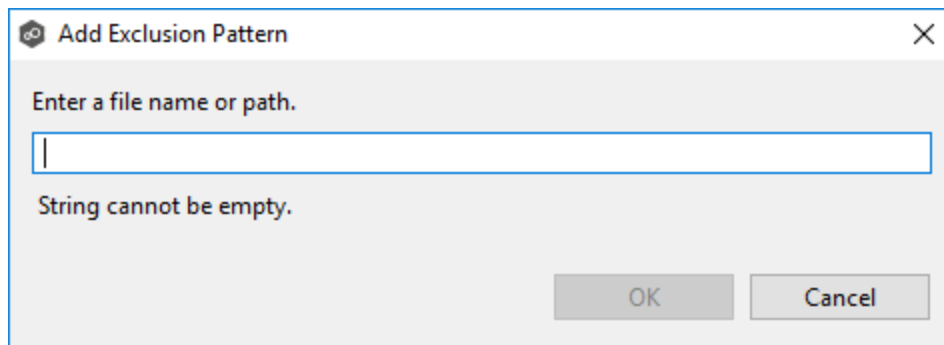
.DWL

.BAK

To create a file filter that excludes these temporary AutoCAD files, you would add these extensions (with [wildcards](#)) to the **Excluded Patterns** field:

1. Click the **Add** button under the **Excluded Patterns** field.

The **Add Exclusion Pattern** dialog appears.



2. Enter **\*.AC\$**, and then click **OK**.
3. Repeat Step 2 to add **\*.BAK**, **\*.DWL\*** and **\*.SV\$**.

The patterns are listed in the **Excluded Patterns** field.



Create File Filter

Name:

Filter Type:

Auto Excluded

[View file types that are automatically excluded](#)

Excluded Patterns

\*.AC\$  
\*.BAK  
\*.DWL\*  
\*.SV\$

Add Edit Delete

Included Patterns

Add Edit Delete

Included Last Modified Dates

days

Excluded File Sizes

bytes

OK Cancel

You have now created a file filter that excludes temporary AutoCAD files—all files ending in \*.AC\$, \*.BAK, \*.DWL\*, or \*.SV\$ will be excluded from any running job that uses this filter.

In addition to filtering on file names, file extensions, folder paths, or partial path wildcard pattern matching, you can filter based on a file's last modified date:

- Peer Management Center supports filtering on a file's last modified date but does not support filtering on a folder's last modified date.
- If you have a folder hierarchy that contains files that are all being filtered based on last modified date, then all folders will still be created during the initial scan process on all hosts.
- If a file is excluded from collaboration based on its last modified date, then the initial scanning process will not synchronize the file even if the file's last modified time and size do not match, or the file does not exist on all hosts. However, the file will be synchronized, if and when the file is modified in the future, and if a user deletes or renames the file on any host, the file will be deleted or renamed from all other hosts where the file exists.
- A file filter cannot combine filtering on last modified date with inclusion or exclusion patterns or [file size](#). The last modified date is the sole criteria used to identify matching files.

## Options for Included Last Modified Date Filter

**Create File Filter**

Name:

Filter Type: **General** ▼

Auto Excluded  
[View file types that are automatically excluded](#)

Excluded Patterns

Add Edit Delete

Included Patterns

Add Edit Delete

**Included Last Modified Dates**

Include older than ▼

days

**Excluded File Sizes**

None ▼

bytes

OK Cancel

<b>Include all dates</b>	This is the default option and will include all files regardless of last modified date.
<b>Include today and past</b>	Includes all files whose last modified date are more recent then the specified number days. For example, you can exclude all files that have not been modified within the last year (365 days).
<b>Include older than</b>	Includes all files whose last modified date are older than the specified number days.

In addition to filtering on file names, file extensions, folder paths, or partial path wildcard pattern matching, you can filter based on the size of an individual file, excluding files that are greater or less than a specified size:

- Peer Management Center does not support filtering on a folder's total size.
- If you have a folder hierarchy that contains files that are all being filtered based on size, then all folders will still be created during the initial scan process on all hosts.
- If a file is excluded from collaboration based on size, then the initial scanning process will not synchronize the file even if the file's last modified time and size do not match, or the file does not exist on all hosts. However, if a user deletes or renames the file on any host, the file will be deleted or renamed from all other hosts where the file exists.
- You cannot define a file filter that combines filtering on file size with inclusion or exclusion patterns or [last modified date](#). The file size is the sole criteria used to identify matching files.

## Options for Excluded File Sizes

Create File Filter

Name:

Filter Type: General ▾

Auto Excluded  
[View file types that are automatically excluded](#)

Excluded Patterns

Add Edit Delete

Included Patterns

Add Edit Delete

Included Last Modified Dates  
Include all dates ▾

days

Excluded File Sizes  
None ▾

bytes

OK Cancel

<b>None</b>	Default option. Select this option to include all files regardless of file size.
<b>Exclude files greater than or equal to</b>	Select this option to exclude all files whose size is greater than or equal to the specified number of bytes. For example, you can configure a job to exclude all files greater than 1 GB.
<b>Exclude files less than</b>	Select this option to exclude files whose size is less than the specified number of bytes.

## Filtering Folders

In addition to creating file filters, you can create folder filters. Folder filters allow you to include and exclude folders from a job's watch set. See [Folder Filter Examples](#) for examples of folder filters. Folder filters are created in the same way as file filters.

## Reduce the Number of Jobs Using Folder Filtering

For management purposes, we recommend keeping the total number of jobs as low as possible. Using folder filters, you can reduce the total number of jobs without sacrificing efficiency. This process involves analyzing all existing jobs, identifying all the folders and hosts that will be collaborating, and consolidating them into fewer jobs by watching a few root folders at a higher level. Filters will then be added to include or exclude only the folders of interest.

## Folder Filter Syntax

When defining a filter pattern to use on folders, use the following syntax:

**\Folder** or **\Folder\*** or **\Folder\\***

Presently, Peer Management Center supports included expressions for a full folder path only and does not support wildcard matching on parent paths. For example, the following expression is not valid:

**\Folder\*\Folder**

## Example of a Simple Folder Filter

The following example reduce the number of existing jobs from four to two:

		Server 1		Server 2	
		Drive D	Drive E	Drive D	Drive F
Old Jobs	Job 1	D:\General		D:\General	
	Job 2		E:\Common		F:\Common
	Job 3	D:\Projects		D:\Projects	
	Job 4		E:\Documents		F:\Documents

After consolidation:

				Filter Option 1	Filter Option 2
		Server 1	Server 2	INCLUDE	EXCLUDE
New Jobs	Job 1	D:\	D:\	\General\*	All other files
				\Projects\*	
	Job 2	E:\	F:\	\Common\*	All other files
				\Documents\*	

Jobs 1 and 3 were merged into a single job watching the root D drive on both servers while using Filter Option 1 or 2.

Jobs 2 and 4 were merged into a single job watching the root E drive on Server 1 and the root F drive on Server 2 while using Filter Option 1 or 2.

Please note the following regarding regular expressions:

- Peer Management Center does not support the ability to use regular expressions for multi-level folder inclusions such as \Level1\Level2\FolderName.
- Peer Management Center does not currently support the ability to filter on certain parts of a path, like \Folder\*\Folder and \Folder\*\.

## Additional Examples of Folder Filters

To exclude a specific folder from anywhere within the watch set:	*\FolderName *\FolderName\FolderName
To exclude a specific folder from the ROOT of the watch set:	\FolderName \FolderName\FolderName
To exclude folders that end with a specific name from anywhere within the watch set:	*FolderName\
To include a specific folder from the root of the watch set:	\FolderName \FolderName\FolderName

### File Filter Usage Notes

## Conflicting Patterns

Since inclusions and exclusions patterns are expressed separately, it is possible to submit conflicting patterns. The pattern evaluator addresses this by exiting when a file is determined to be excluded. Therefore, exclusions patterns override inclusion patterns.

## Rename Operations

Rename operations may subject files to an inclusion status change. Renaming a file out of the watch set will trigger a target deletion, while renaming into the watch set triggers a target addition. Renaming a file out of the [watch set](#) triggers a target addition.

## Folder Deletions

Folder deletions only affect included files, possibly leading to folder structure inconsistencies. When a session participant deletes a folder, the target outcome will vary depending on whether excluded files are present. Folder deletions are propagated in detail to the targets as to the exact files that have been affected.



## List Filters

Peer Management Center provides the ability to filter lists throughout the Peer Management Center interface. List filters can help you quickly find jobs, Agents, and sort through summary reports

To use a list filter, enter a filter expression in the filter expression box. The search results of your filter are displayed in the window below the expression.

You can save the list filters and reuse them. For more information, see [Saving and Managing List Filters](#). This is useful when you frequently use the same list filter or when you create complex list filters.

Use the **Ctrl + Space** keyboard shortcut to list all possible list filters and predefined labels, which can be selected to refine your search quickly.

## Basic Filter Expressions

The simplest filter expressions contain words you are looking for. For example, to find all items related to sales, simply type the word *sales* in the filter expression box. All items from the list that contain the word *sales* in their name, tag names, or tag categories will be displayed, and all other items will be hidden. The agent attribute fields (see **attr** below) are not included in generic searches.

If you want an exact word match or the words contain a space, enclose the terms in double quotes. For example, if you want to search for the words *North America*, the two words must be contained in double quotes. If you want to search for the word *agent* only without showing *USAgent* or *Agent2015* in results, the word *agent* must be contained in double quotes.

For information about creating more complex filter expressions using operators and labels, see [Creating Complex Filter Expressions](#).

## Predefined List Filters

- Default job filters include **Failed Jobs**, **Jobs with Backlog**, and **Running Scans**.
- Default Agent filters include **Connected** and **Disconnected** (e.g. filter:"Running Scans").

## Creating Complex Filter Expressions

You can create more sophisticated list filters by using operators and labels.

## Using Operators

Operators allow you to combine multiple simple expressions into a single compound expression. Supported operators are: **OR**, **AND**, and **NOT**. For example, typing **tag:Americas AND sales** in the Filter Expression will show only Agents with the word *Americas* in their tag(s) **AND** the word *sales* in their name, tags, or tag categories. Parentheses can be used to build more complex expressions by grouping simple expressions.

## Using Labels

Use predefined labels to specify in which field your filter word should appear. Use the following format to take advantage of labels in your filter expression:

**<label>:<search string>**.

List of possible labels include:

<b>name</b>	List only items that match the string (e.g. name:"Design Data")
<b>tag</b>	Show only items with the word specified in their tag(s) (e.g. tag:Americas)
<b>cat</b>	Search for items that have been assigned a specific category (e.g. search for Jobs that were categorized as Design - cat:Design)
<b>host</b>	Filter through Jobs and list only those that contain the host in the list of job participants (e.g. host:WIN12R2A)
<b>attr</b>	Search for the specified string in the following Agent fields: Connection Status, Operating System, JVM Architecture, and Agent Version (e.g. attr:x86)
<b>filter</b>	List items that have been assigned a default or user-created filter.

## Examples

Example 1: Show all Agents with the word *Sales* in their name, tag name, or tag category:

**Sales**

Example 2: Show all Agents with a tag that has *North America* in the tag name and *Location* in the tag category:

**cat:Location AND tag:"North America"**

Example 3: Show all Agents with the word *Sales* in their name, tag name, and tag category and with a tag that has *North America* in the tag name and *Location* in the tag category.

Sales AND (cat:Location AND tag:"North America")

## Saving and Managing List Filters

Throughout the Peer Management Center interface, you will have the opportunity to save your filter expression by clicking the **Manage, Save, and Load filters** button, usually located above the **Filter Expression** field or in the **Actions** drop-down menu. The **Manage, Save, and Load filters** button is available in the [Jobs view](#) panel, the [Agent Summary](#) view, the and the [Collaboration Summary](#) panel.

## Removing List Filters

To remove a list filter and show all items in the list, click the pencil icon to the right of the filter expression.

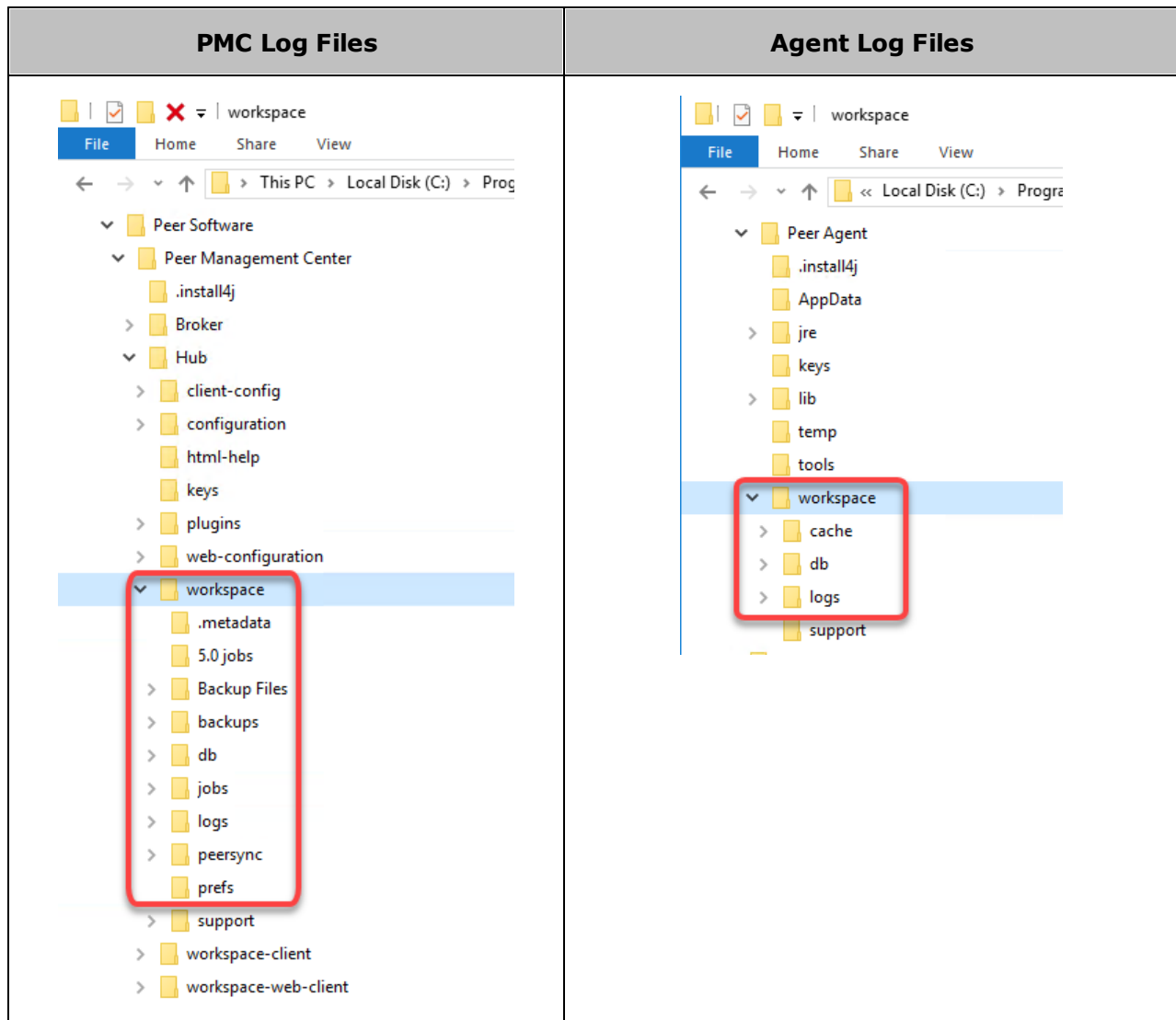
## Logging and Alerts

### Overview

PeerGFS performs an extensive amount of logging to track events and activities processed by PeerGFS. The results are stored in log files that are useful for troubleshooting and analytics. PeerGFS tracks and logs many types of information and activities, including file events, preferences, job-specific configuration files, and analytics files. See [File Event Logs and Alerts](#) for more information about job-related file event logging.

### Accessing Log Files

Many of the log files have an .log extension; these are text files that can be opened in a text editing application. Other log files are stored in other file formats such as .xml, .csv, and .prefs. Log files are stored in the **workspace** folder in the Peer Management Center and Agent installation directories:



If you want to review these files for troubleshooting or analytical purposes, you can retrieve them as a single, compressed file, which is then stored in the **support** folder in the Peer Management Center installation directory. The [retrieval process](#) compiles the various log files into a single zip file that is easy to review and send to others for review. When retrieving log files, you have various options, such as choosing which log files are included, whether to encrypt log files (which may contain sensitive information), and whether to have the zip file automatically sent to Peer Software Support.

## Retrieving Log Files

To retrieve log files:

1. Open Peer Management Center.
2. From the **Help** menu, choose **Retrieve PMC/Agent Logs**.

The **Retrieve PMC/Agent Log Files** dialog is displayed.

**Retrieve PMC/Agent Log Files**

**Log Collection Options**

Include logs newer than  days

☒ Run Event Detection Analytics before log file collection

☐ Collect only statistics files

**Agent Log Options**

☐ Do not include any agent log files

☒ Include all connected agent log files

☐ Include the log files from the connected agents selected below:

Name
<input type="checkbox"/> DGAgent1
<input type="checkbox"/> DGAgent2

[Select All](#) [Clear Selected](#)

**Encryption and Support Options**

☒ Encrypt log files

☒ Upload log files and telemetry to Peer Software Support

Log retrieval can take a while based on network speed and log file sizes.  
You will be notified when this operation completes.

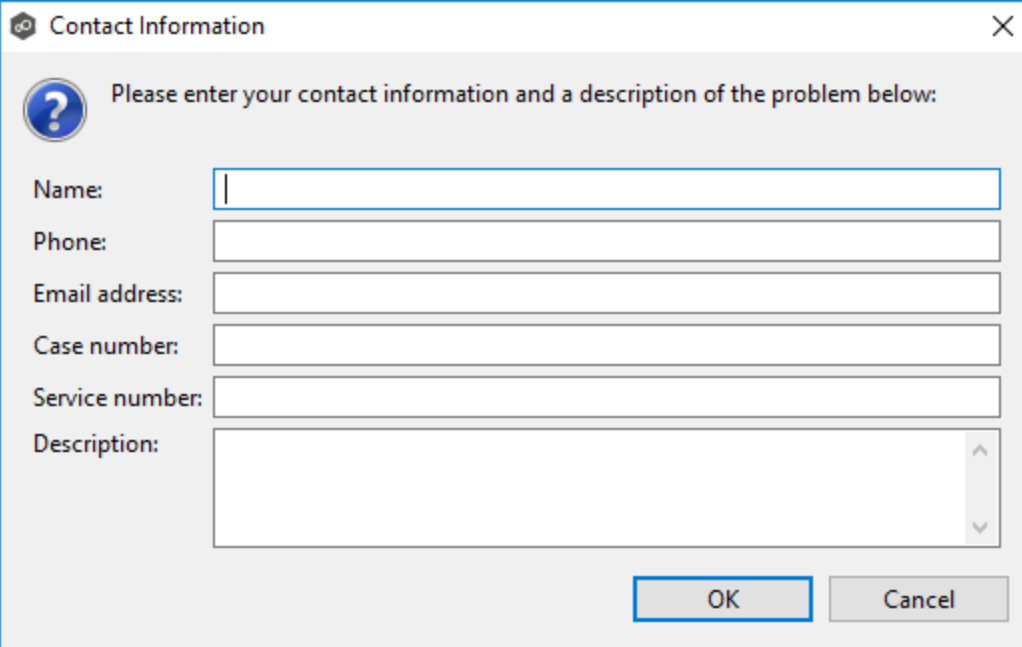
Are you sure you want to proceed with this operation?

3. Select the logging options.

There are three sets of options:

- [Log Collection Options](#)
- [Agent Log Options](#)
- [Encryption and Support Options](#)

4. Enter the your contact information and a description of the problem:

A dialog box titled "Contact Information" with a close button (X) in the top right corner. It contains a question mark icon and the text "Please enter your contact information and a description of the problem below:". Below this are six input fields: "Name:", "Phone:", "Email address:", "Case number:", "Service number:", and "Description:". The "Description:" field is a larger text area with a vertical scrollbar. At the bottom right are "OK" and "Cancel" buttons.

**Contact Information**

Please enter your contact information and a description of the problem below:

Name:

Phone:

Email address:

Case number:

Service number:

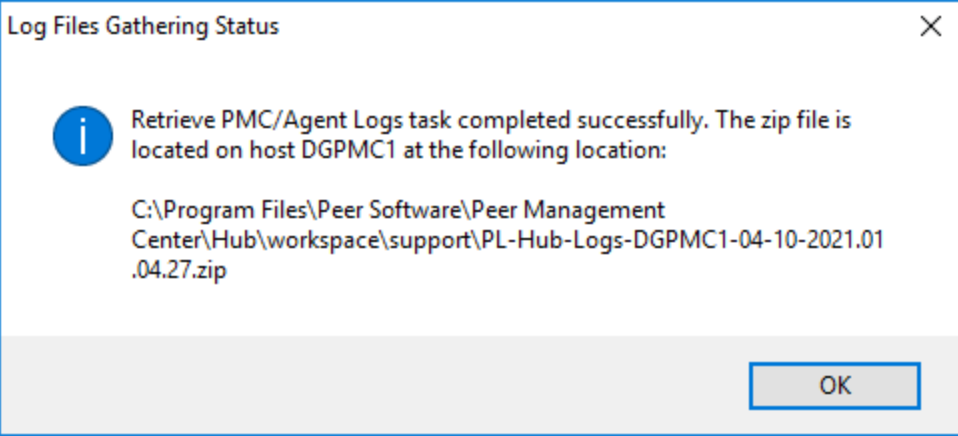
Description:

OK Cancel

This information will be sent to Peer Software Technical Support.

5. Click **Yes** to start the log retrieval process.

It may take some time for the log files to be collected and compiled into a single, compressed file. When the retrieval is finished, a message is displayed.

A dialog box titled "Log Files Gathering Status" with a close button (X) in the top right corner. It contains an information icon (i) and the text "Retrieve PMC/Agent Logs task completed successfully. The zip file is located on host DGPMC1 at the following location:". Below this is the file path: "C:\Program Files\Peer Software\Peer Management Center\Hub\workspace\support\PL-Hub-Logs-DGPMC1-04-10-2021.01.04.27.zip". At the bottom right is an "OK" button.

**Log Files Gathering Status**

Retrieve PMC/Agent Logs task completed successfully. The zip file is located on host DGPMC1 at the following location:

C:\Program Files\Peer Software\Peer Management Center\Hub\workspace\support\PL-Hub-Logs-DGPMC1-04-10-2021.01.04.27.zip

OK

6. Click **OK**.

The retrieved log file is stored as a zip file in the **workspace/support** subfolder in the Peer Management Center installation directory.

## Log Collection Options

<b>Include logs newer than X days</b>	Use this option to restrict the logs retrieved to a certain time period.
<b>Run Event Detection Analytics before log file collection</b>	Select this option to run event detections analytics immediately before the log files collected. PeerGFS can perform event detection analysis every night; however, this option allows you to receive the most up-to-date analytics.
<b>Collect only statistics files</b>	Select this option to retrieve log files that contain statistics only.

## Agent Log Options

<b>Do not include any agent log files</b>	Select this option if you do not want to retrieve log files for any agent.
<b>Include all connected agent log files</b>	Select this option if you want to retrieve log files for all connected agents.
<b>Include the log files from the connected agents selected below</b>	Select this option if you want to retrieve log files for selected connected agents.

## Encryption and Support Options

<b>Encrypt log files</b>	Select this option if you want to encrypt the log files in the zip file.
<b>Automatically upload log files and telemetry to Peer</b>	Select this option if you want to automatically upload the zip file containing the log files and telemetry information to Peer Software Support. No file data will be uploaded.

<b>Software Support</b>	
-------------------------	--

## File Event Logs and Alerts

### File Event Logging

PeerGFS records various types of file events for file collaboration, file replication, file synchronization, and file locking jobs. The events are written to the **fc\_event.log** file located in the **Hub\logs** subdirectory within the Peer Management Center installation directory. All log files are stored in a tab-delimited format that can easily be read by Microsoft Excel or other database applications. The events are also displayed in the **Event Log** tab located within the runtime summary view for the selected job.

### Logging Fields

Below is a list of logging fields and their descriptions:

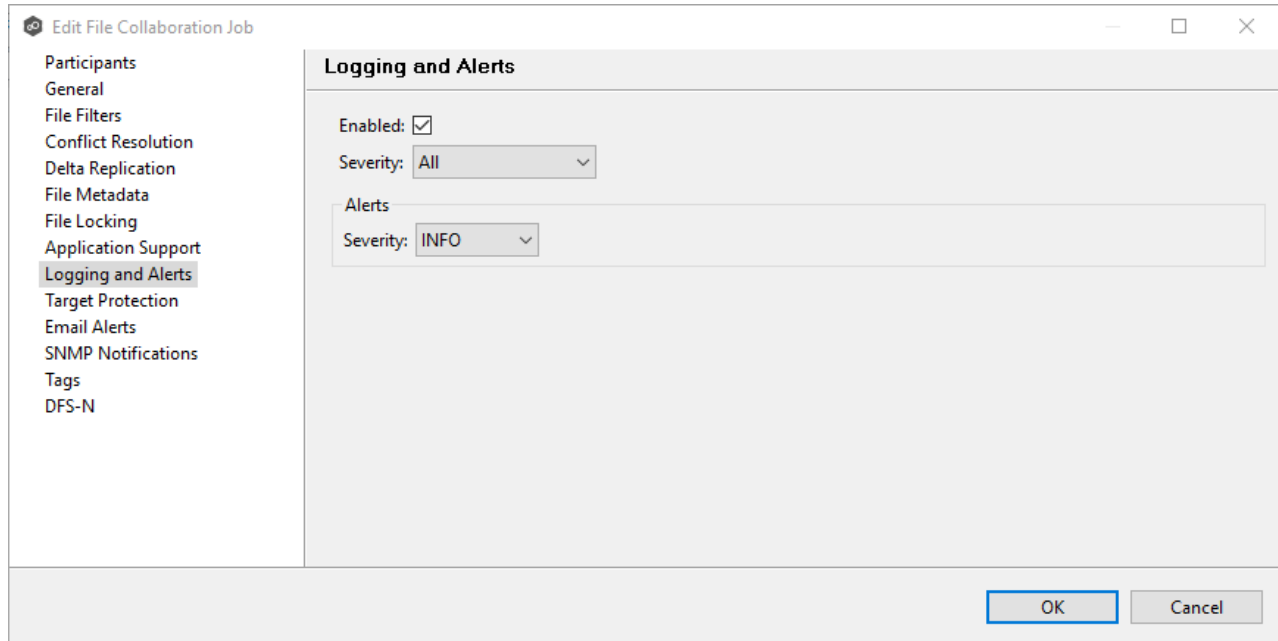
Field	Description
<b>Enabled</b>	Selecting this option will enable file event logging based on the other settings. Deselecting this option will completely disable all logging.
<b>Severity</b>	Determines what severity levels will be logged. There are two options: <ul style="list-style-type: none"><li>• All (Informational, Warnings, Error, Fatal)</li><li>• Errors &amp; Warnings (Warnings, Error, Fatal)</li></ul>
<b>Event Types</b>	If checked, the corresponding event type will be logged.
<b>File Open</b>	A file was opened by a remote application on a <a href="#">source host</a> .
<b>File Lock</b>	A file lock was acquired on a <a href="#">target host</a> when a file open is detected on another host.



Field	Description
<b>File Close</b>	A file was closed.
<b>File Add</b>	A file was added to the <a href="#">watch set</a> .
<b>File Modify</b>	A file was modified in the watch set.
<b>File Delete</b>	A file was deleted.
<b>File Rename</b>	A file was renamed.
<b>Attribute Change</b>	A file attribute was changed.
<b>Security (ACL) Change</b>	The security descriptor of a file or folder was changed.
<b>Directory Scan</b>	Indicates when a directory was scanned as a result of the <a href="#">initial synchronization process</a> .
<b>File ADS Transfer</b>	The Alternate Data Stream of a modified file was synced to target host(s).

## Configuring Job Logging and Alerts

You can configure the logging and alert settings for a job when you edit a job. By default, all file collaboration and synchronization activity is logged for all severity levels. You can enable or disable file event logging, as well as select the level of granularity.



The screenshot shows the 'Edit File Collaboration Job' window. On the left is a sidebar with the following menu items: Participants, General, File Filters, Conflict Resolution, Delta Replication, File Metadata, File Locking, Application Support, **Logging and Alerts** (highlighted), Target Protection, Email Alerts, SNMP Notifications, Tags, and DFS-N. The main panel is titled 'Logging and Alerts' and contains the following settings:

- Enabled:** A checkbox that is checked.
- Severity:** A dropdown menu currently set to 'All'.
- Alerts:** A section containing a dropdown menu currently set to 'INFO'.

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

## Log Entry Severity Levels

Level	Description
<b>Informational</b>	Informational log entry, e.g., a file was opened.
<b>Warning</b>	Some sort of warning occurred that did not produce an error but was unexpected or may need further investigation.
<b>Error</b>	An error occurred performing some type of file activity.
<b>Fatal</b>	A fatal error occurred that caused a host to be taken out of the session, a file to be quarantined, or a session to become invalid.

## Job Alerts

Various types of alerts will be logged to a log file and to the **Alerts** table located within the job's runtime summary view for the selected job. Each job will log to the **fc\_alert.log** file located in the **Hub\logs** subdirectory within the Peer Management Center installation directory.

The default log level is WARNING, which will show any warning or error alerts that occur during a running session. Depending on the severity of the alert, the job may need to be restarted.

## Web Client Users

Peer Management Center offers two [interfaces](#):

- A rich client interface: Rich client users have access to all Peer Management Center functionality.
- A web client interface: Web client users access to Peer Management Center functionality is controlled by their [web role](#).

Web client users can be divided into two categories based on how their access to the web client is authenticated:

- [Internal users](#)
- [Active Directory users and groups](#)

For information about managing web client users, see [Managing Web Client Users](#).

### Internal Users

An **internal user** is one whose access to the Peer Management Center web client is authenticated by an internal Peer Management Center database rather than through Active Directory.

For information about managing internal users, see [Managing Internal Users](#).

## Internal User and Web Roles

When you add internal users to Peer Management Center, you need to specify their access to Peer Management Center functionality by assigning them a [standard web role](#) or a [custom web role](#). A **web role** is a set of [permissions](#) that specifies the appropriate level of access to Peer Management Center functionality. For example, some users will need to the ability to create and

edit jobs, while other users may need only to view job summaries. Assign the most suitable role to each user, giving them the most appropriate level of control and not more.

For more information about web roles, see [Overview of Web Roles](#).

## Default Internal User: The admin User

There is a default internal user who has access to all Peer Management Center functionality available in the web client: the **admin** user. This user does not need to be created. This internal user has the following properties:

<b>Username</b>	admin
<b>Password</b>	password  This should be changed immediately upon first log-in.
<b>Web Role</b>	Administrator

Unlike other internal users, the admin user cannot be renamed or deleted, nor can its role be changed. However, for security reasons, [the password should be changed immediately](#).

## Active Directory Users and Groups

An Active Directory (AD) user or group is one whose access to Peer Management Center is authenticated through Active Directory. Adding an Active AD user or group authenticates and authorizes that user or group members to use Peer Management Center. The AD user or group must already exist in Active Directory prior to adding the user or group to Peer Management Center.

Active Directory users won't be able to access the web client until [Active Directory authentication is configured](#) in Peer Management Center.

For information about managing Active Directory users and groups, see [Managing Active Directory Users](#).

## Active Directory Users and Web Roles

When you add Active Directory users and groups to Peer Management Center, you need to specify their access to Peer Management Center functionality by assigning them a [standard web role](#) or a [custom web role](#). A **web role** is a set of [permissions](#) that specifies the appropriate level of access

to Peer Management Center functionality. For example, some users will need to the ability to create and edit jobs, while other users may need only to view job summaries. Assign the most suitable role to each user, giving them the most appropriate level of control and not more.

For more information about web roles, see [Overview of Web Roles](#).

## Overview of Web Roles

All users that access Peer Management Center through the web client must have an assigned **web role**. A web role is a set of [permissions](#) that specifies the appropriate level of access to Peer Management Center functionality. For example, some users will need to the ability to create and edit jobs, while other users may need only to view job summaries.

Web client users can have a [standard web role](#) or a [custom web role](#). In contrast, a user who accesses Peer Management Center through the rich client does not have a web role. All Peer Management Center functionality is accessible to a rich client user.

For more information about web roles, see [Managing Web Roles](#).

There are three standard web roles, each with a predefined set of permissions:

- **Administrator** - This role has complete access to all functionality found in the Peer Management Center's rich client.
- **Power User** - This role has view-only access to jobs and the **Agent Summary** view; this role cannot create, edit, or delete jobs, access settings in **Preferences**, or assign tags.
- **Help Desk** - This role has view-only access to jobs. Specifically, Help Desk users are limited to view-only access to the following:
  - The [Jobs view](#)
  - The [runtime views](#)
  - The Summary and Session tabs of each job.

In addition, Help Desk users have read-write access to the Quarantines tab of each job, with the ability to release conflicts for any running jobs.

Standard web roles cannot be modified or deleted, with one exception: tags can be assigned to standard roles. For a list of the permissions associated with standard web roles, see [Standard Web Role Permissions](#).

#### Standard Web Role Permissions

Each of the three standard web roles (Administrator, Power User, and Help Desk) has permission to access the resources shown in the following table.

Functionality	Administrator	Power User	Help Desk
<b>Advisory Alert View</b>	Edit	Edit	
<b>Broker Statistics Action</b>	Edit	Edit	
<b>Collaboration Summary View</b>	Edit	Edit	
<b>Configuration Interface</b>	Edit	Edit	
<b>Event Analyzer Configuration Interface</b>	Edit	Edit	
<b>Event Analyzer Log View</b>	Edit	Edit	View-only
<b>Event Analyzer Participant view</b>	Edit	Edit	
<b>Event Analyzer Runtime Summary Interface</b>	Edit	Edit	View-only
<b>Event Log View</b>	Edit	Edit	
<b>Expression List Dialog</b>	Edit	Edit	
<b>File Conflict View</b>	Edit	Edit	Edit
<b>File Sync Advisory Alert View</b>	Edit	Edit	

Functionality	Administrator	Power User	Help Desk
Folder Analyzer View	Edit	Edit	View-only
Job Alert View	Edit	Edit	
Job View	Edit	Edit	View-only
Log Dump Action	Edit	Edit	
Memory Dump Action	Edit	Edit	
New Job Action	Edit		
Participant View	Edit	Edit	
Permission Mode	Edit	Edit	
PMC Alert View	Edit	Edit	
PMC Download Agent	Edit	Edit	
PMC Refresh Perspective	Edit	Edit	
PMC View Progress	Edit	Edit	
Preferences	Edit		
Runtime Summary Interface	Edit	Edit	View-only
Session View	Edit	Edit	View-only
Status Agent Tree View	Edit	View-only	

Functionality	Administrator	Power User	Help Desk
Tag Resources Dialog	Edit		
Thread Dump Action	Edit	Edit	

## PeerSync Management Job Permissions

The following table outlines the permissions for PeerSync Management jobs.

Functionality	Administrator	Power User	Help Desk
PeerSync Summary View	Edit	Edit	Edit
PeerSync Job Stats View Part View	Edit	Edit	
PeerSync Configuration Interface	Edit	Edit	View-only
PeerSync Job Stats View	Edit	Edit	Edit
PeerSync Update Log View	Edit	Edit	Edit
PeerSync Add Log View	Edit	Edit	Edit
PeerSync File Conflict View	Edit	Edit	Edit
PeerSync Runtime Summary Interface	Edit	Edit	View-only
PeerSync Participant View	Edit	Edit	
PeerSync Advisory Alert View	Edit	Edit	



Functionality	Administrator	Power User	Help Desk
PeerSync Messages Log View	Edit	Edit	Edit
PeerSync Delete Log View	Edit	Edit	Edit
PeerSync Event Log View	Edit	Edit	

A custom web role allows you to customize and fine-tune the access that a user has to Peer Management Center resources. This is useful if you have multiple types or levels of users that need different types of access. For example, if you have multiple tiers of help desk staff, creating custom roles based on the standard Help Desk role allows you to provide them varying levels of access to Peer Management Center.

A custom role is based on one of the three [standard web roles](#) (Administrator, Power User, and Help Desk); the custom role starts with the same set of permissions as the role it is based on. However, during the process of creating the custom role, you modify the permissions associated with the new role.

For more information, see [Creating a Custom Web Role](#).

#### Custom Web Role Permissions

You can [create custom web roles](#) in User Management and specify the permissions you want associated with the role.

When creating a custom web role, you select the permissions for the web role in the **Permissions** table, which has three columns:

- **Category** - Identifies the general area of the user interface that the permission applies:
  - **Cloud Backup and Replication UI** - Applies to Cloud Backup and Replication jobs.
  - **Collab/Sync/Repl UI** - File Collaboration, File Synchronization, and File Replication jobs.

- **DFS-N UI** - Applies to DFS-N Management jobs.
- **PMC UI** - Applies to Agent Summary view, statistics, task scheduling and task history, logs, memory dumps ,and thread dumps.
- **Name** - Identifies the specific area of the user interface.
- **Access** - Identifies the level of access:
  - **Full access** - Has complete access.
  - **View-only access** - Can view but not create, edit, or delete.
  - **No access** - No access.

New Role

General  
Permissions  
Tags

Permissions

Category	Name	Access
Cloud Backup and Replication UI	Job View - Failed Events Tab	Full access
Cloud Backup and Replication UI	Runtime Summary View	Full access
Cloud Backup and Replication UI	Job View - Participants Tab	Full access
Cloud Backup and Replication UI	Job View - Event Log Tab	Full access
Cloud Backup and Replication UI	Job View - Alerts Tab	Full access
Cloud Backup and Replication UI	Job View - Summary Tab	Full access
Cloud Backup and Replication UI	Job View - Configuration Tab	Full access
Collab/Sync/Repl UI	Runtime Summary View	Full access
Collab/Sync/Repl UI	Job View - Session Tab	Full access
Collab/Sync/Repl UI	Job View - Summary Tab	Full access
Collab/Sync/Repl UI	Job View - Quarantines Tab	Full access
Collab/Sync/Repl UI	Job View - Configuration Tab	Full access
Collab/Sync/Repl UI	Job View - Event Log Tab	Full access
Collab/Sync/Repl UI	Job View - Participants Tab	Full access
Collab/Sync/Repl UI	Job View - Retries Tab	Full access
Collab/Sync/Repl UI	Job View - Alerts Tab	Full access
DFS-N UI	Job View - Namespace Tab	Full access
DFS-N UI	Runtime Summary View	Full access
DFS-N UI	Job View - Configuration Tab	Full access
DFS-N UI	Job View - Alerts Tab	Full access
DFS-N UI	Job View - Namespace Servers Tab	Full access
PMC UI	Assign Tags	Full access
PMC UI	Generate PMC Memory Dump	Full access
PMC UI	Show Agent Summary	Full access
PMC UI	Jobs View	Full access
PMC UI	Preferences	Full access
PMC UI	Retrieve Broker Statistics	Full access
PMC UI	View Alerts	Full access
PMC UI	New Job Wizard	Full access
PMC UI	Show Progress View	Full access
PMC UI	Task Scheduler and Task History	Full access
PMC UI	View Job Alerts	Full access
PMC UI	Retrieve PMC/Agent Logs	Full access
PMC UI	Generate PMC and Broker Thread...	Full access
PMC UI	Download Agent Installer	Full access

OK
Cancel

## SNMP Notifications

### Overview

Peer Management Center provides support for SNMP v1 messaging. A SNMP notification notifies recipients when a certain type of event occurs, for example, session abort, host failure, system alert.

When an SNMP notification is applied to a job, a SNMP trap is sent to the destination IP address or hostname whenever a selected notification type is triggered by the job.

An SMNP notification consists of a unique name, a selection of notification types, source IP address, along with a trap prefix and destination. The available notification types depend on the job type.

When you create a job, you can select an existing SNMP notification to apply to the job or you can create a new notification and apply it to the job. You cannot modify or delete a notification while it is applied to a job. An SMNP notification can be applied to multiple jobs of the same type. SNMP notifications are defined in the [preferences](#) for a job type. An SNMP notification can be applied to all job types except File Replication.

## Managing SMNP Notifications

To manage SMNP notifications:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Select the job type from the navigation tree and expand it.
3. Select **SMNP Notifications** from the navigation tree.

The **SMNP Notifications** page lists existing SMNP notifications for that job type. You can create, edit, copy, and delete notifications.

## Tags

Tags can be used to categorize resources and customize a user's workspace or perspective. Tagging helps when managing large number of resources.

You can assign tags to:

- Jobs
- Resources
- Web roles

- Agents

You can also assign resources to tags. See [Using Tags to Filter Resources](#).

## Creating Tags and Categories

Tags and categories are created in [Tags Configuration](#) in **Preferences**. The **Assign Tags** dialog also offers the option to create tags and categories.

## Assigning Tags

You can:

- Assign tags during job creation
- Assign tags while editing an existing job
- Assign tags to one or more resources
- Assign tags to web roles
- Assign resources to one or more tags

## Assigning Tags to Jobs

- During job creation - You can assign tags during the creation of a job from the [Tags](#) page of the job creation wizard.
- During job editing - You can assign tags to individual jobs by right-clicking on the job, selecting **Edit Job(s)**, and navigating to the **Tags** page of the job editing wizard.

## Assigning Tags to Resources

To assign tags to one or more resources:

1. Click the **Assign Tags** button from the main view, [Jobs view](#), or [Agent Summary view](#) toolbars.
2. In the **Assign Tags** dialog, click the **Tags** radio button.

3. Select the tag that needs to be assigned to one or more resources.
4. Click the **Edit** button.

The **Assign/Unassign resources** dialog appears.

5. In the **Unassigned Resources** table, select the resources to be assigned the selected tag, and then click the right-arrow button (Add One) to move it to the table on the right side.

**Tip:** To select multiple resources, press the Shift key on the keyboard when selecting resources.

6. Click **Save**.
7. Repeat the preceding steps for all the tags that need to be assigned to one or more resources.

## Assigning Tags to Web Roles

Web roles can be assigned tags that customize a user's Jobs view when they log in via the [web client](#). For example, in a very large deployment scenario, a user that is part of the Help Desk role can be assigned tags that limit their view to only jobs that are part of their region.

To assign tags to user roles:

1. Create tags and categories as outlined in Step 1 above.
2. Assign tags to one or more jobs as outlined in Step 2 above.
3. Go to [User Management](#) in the [Preferences](#) page.
4. Select the desired role to which you wish to assign specific job tags.
5. Click the **Edit** button.
6. In the **Tags** window, from the **Unassigned Tags** table on the left side, select the tags that need to be assigned the selected role, and then click the right-arrow button (Add one) to move it to the table on the right side (hold down the Shift key on the keyboard when selecting tags to select more than one).
7. Click **OK** to commit your changes and close the dialog, and then close the **Preferences** page.

The user will see only the jobs that were tagged in the user's role.

## Assigning Resources to One or More Tags

To assign resources to one or more tags:

1. Click the **Assign Tags** button from a summary view, [Jobs view](#), or [Agent Summary view](#) toolbar.
2. In the **Assign Tags** dialog, click the **Resources** radio button.
3. On the left-hand side, click inside the **Resource Name Filter** or **Type Filter** fields and press the CTRL + Space keys on the keyboard to list all possible filters and predefined labels, which can be selected to refine your search quickly.
4. Select the resource that needs to be assigned to one or more tags.
5. Click the **Edit** button to the right.
6. From the **Unassigned Tags** table on the left side, select the tags that need to be assigned the selected Resource, and then click the right-arrow button (Add one) to move it to the table on the right side (hold down the Shift key on the keyboard when selecting tags to select more than one).
7. Click the **Save** button to commit your changes, and then close the dialog.
8. Repeat the preceding steps for all the resources that need to be assigned to one or more tags.

### Using Tags to Filter Resources

You can use tags to filter resources:

- Filter jobs
- Filter agents

To filter resources using tags, use the tag label in any list filter field throughout the Peer Management Center interface.

### Filter Jobs

To filter through a large list of jobs, use the filter field located below the toolbar buttons in the **Jobs** view. For more details on how to filter through resources, see [List Filters](#).

Example:

Show all jobs with a tag that has "North America" in the tag name and "Location" in the tag category:

tag:"North America" AND cat:Location

## Filter Agents

To filter through a large list of Agents, use the **Filter** field located below the toolbar buttons in the [Agent Summary View](#) panel. For more details on how to filter through resources, see [Filter Expressions](#).

## Advanced Topics

This section discusses the following topics:

- [DFS Namespace Failover and Failback](#)
- [File Conflict Resolution](#)
- [File Metadata Synchronization](#)
- [Managing Peer Agents](#)
- [Smart Data Seeding](#)
- [TLS Certificates](#)

## Conflicts, Retries, and Quarantines

Making unstructured data active at multiple locations introduces the chance of users making conflicting changes to different copies of the same file. The real-time synchronization and locking engines built into Peer Global File Service are designed to prevent these conflicts by ensuring that only one user can modify a file at a time while also making sure that all locations always have the most up to date version of a file. There are scenarios, however, where the synchronization and locking engines may not be able to prevent version conflicts. Such scenarios include network outages and file system issues.

The conflict resolution engine in Peer Global File Service is designed to handle these circumstances with a three-tiered approach backed by a combination of scans and real-time activity:



- **File Conflicts** – The initial state of detection of a potential version conflict. Depending on user activity, these can often be resolved automatically.
- **File Retries** – If certain errors are thrown when trying to synchronize a file between locations, this file will be automatically put into a retry list. Synchronization of this file will be retried every minute for a maximum of 60 attempts. The frequency of attempts and the maximum number of attempts are configurable.
- **File Quarantines** – These are file conflicts that could not be automatically resolved, as well as file retries that have failed after the maximum number of attempts. Files in the quarantine list will no longer be synchronized or protected with file locks until a winning file is picked through the PeerGFS user interface.

File conflicts (and potentially quarantines) can occur for any of the following reasons:

- Two users open a file at the same time or in-and-around the same time.
- A file is open at the start of a job and has been modified on a host where the configured conflict resolution strategy selects a different host as the winner.
- Two or more users have the same file open on different hosts when a collaboration job is started.
- A file was modified on two or more hosts between job restarts or network outages.
- Peer Management Center is unable to obtain a lock on a target host file for various reasons.
- Peer Management Center may conflict a file when an unexpected error occurs, or a file is in an unexpected state.

File retries can occur for any of the following reasons:

- The transfer of a file between locations is interrupted for any reason.
- The renaming of a temp file after a successful file transfer is blocked for any reason.

An example of a file conflict versus a file quarantine is as follows:

Two users have the same file open at two different locations prior to a Peer Global File Service job being enabled. When starting the job, PeerGFS will track this file as a potential conflict. If only one or no users make a change to the file, this conflict will automatically be resolved. If both users make a change, the conflict will become a quarantine.

## DFS Namespace Failover and Failback

You can manage [DFS namespaces](#) through a dedicated job type in Peer Management Center, the [DFS-N Management job](#). Peer Management Center controls [failover](#) and [failback](#) by automatically disabling and enabling DFS namespace folder targets.

### Failover

Peer Management Center and Agents are constantly looking for connectivity issues and other failures across linked file servers, the Peer Agents themselves, and entire sites. If Peer Management Center detects a failure, it can be set to automatically disable a linked DFS namespace folder target from a namespace folder. This will prevent end users from accessing the associated folder target. If configured to do so, [DFS Namespaces](#) will automatically redirect clients to another available folder target.

### Failback

While DFS Namespaces itself can automate the disabling of folder targets, it does not automate the re-enabling of disabled targets. When configured to talk to DFS namespaces, Peer Management Center can automate this process. When Peer Management Center determines that a file server, Peer Agent, or entire site is back online, it automatically runs the following process to re-integrate that file server:

1. Kicks off a rescan to ensure the disconnected site or file server is brought back in sync with the others.
2. Re-enables the associated folder target once the re-scan is complete. Once this is done, DFS Namespaces begins to direct end users back to this file server.

## File Metadata Synchronization

### Overview

File metadata is additional information stored as part of a file. The primary component of file metadata is Security Descriptor Information, also known as access control levels (ACLs).

The Security Descriptor Information elements that can be synchronized are:

- **Owner:** NFTS Creator-Owner. By default, the owner is whomever created the object. The owner can modify permissions and give other users the right to take ownership.
- **DACL:** Discretionary Access Control List. It identifies the users and groups that are assigned or denied access permissions to a file or folder.

- **SACL:** System Access Control List. It enables administrators to log attempts to access a secured file or folder and is used for auditing.

## File Metadata Conflict Resolution

File metadata conflict resolution occurs only the first time a file is synchronized during the initial scan, and only when one or more security descriptors do not match the designated master host.

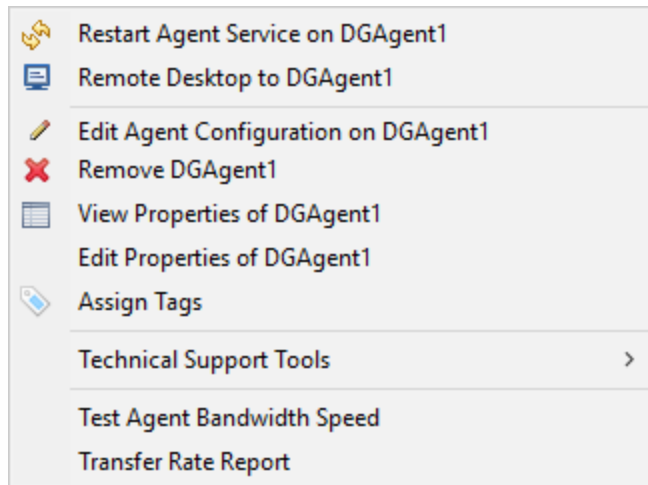
If the file does not exist on the designated master host, then no conflict resolution is performed. If a master host is not selected, then no file metadata synchronization is performed during the initial scan.

## ACL Requirements

- Enabling ACL synchronization requires that all participants be members of any referenced domains that are configured in the ACL(s) or as the owner of the file. Failure to do so may render the file unreadable on the offending target host.
- All Peer Agents must be run under a domain Administrator account and cannot be run under a local or System account.
- To ensure accurate and consistent ACL propagation, the security settings for the watch set must match EXACTLY across all the participants. The best and easiest way to ensure the security settings match is to compare the permissions in the Microsoft **Advanced Security Settings** dialog for the root folder being watched.

## Managing Peer Agents

The ability to remotely manage the configuration for connected [Peer Agents](#) is available from within Peer Management Center. Right-clicking one or more agent names in the **Agents** view displays the following context menu:




## Options

Option	Description
<b>Restart Agent Service</b>	<p>Restarts the Peer Agent Windows service running on the corresponding host if the selected Peer Agent is connected. If the Peer Agent is not connected to the Peer Management Broker, an attempt is made to restart the Peer Agent Windows service using the Windows <b>sc</b> command.</p> <p>Note that this works only if the user running the Peer Management Center can access the remote Peer Agent system and has the appropriate domain permissions to start and stop services on the remote Peer Agent system.</p>
<b>Remote Desktop to Agent</b>	Launches a Windows Remote Desktop connection to the selected Peer Agent.
<b>Edit Agent Configuration</b>	Displays a dialog through which the selected Peer Agent can be configured. Configurable options include Peer Management Center connectivity, Peer Agent logging, Peer Agent memory usage, among others. For more information, see <a href="#">Editing an Agent Configuration</a> .
<b>Remove Agent</b>	Remove the selected Peer Agent(s) from the <b>Agents</b> view, but if the Peer Agent is still running or connects again, then it will be added back to the list when the next heartbeat is received.

Option	Description
<b>View Properties of Agent</b>	Displays properties for the selected Peer Agent, for example, heartbeat information, host machine configuration, messaging statistics, performance statistics. See <a href="#">Viewing Agent Properties</a> for more details.
<b>Edit Properties of Agent</b>	Allows you to edit the connection type, preferred host, and RDP connection string.
<b>Assign Tags</b>	Displays a dialog where you can view and assign tags to resources.
<b>Technical Support Tools</b>	Displays a list of <a href="#">tools</a> that can be used to assist Peer Software Technical Support.
<b>Test Agent Bandwidth Speed</b>	Runs a bandwidth speed test to be performed in the background if the selected Peer Agent is connected. You are notified at completion with the results of the test.
<b>Transfer Rate Report (not available on Web Client)</b>	(Rich client only) Displays a time series performance chart of average transfer rate for the selected Peer Agent over the last 24 hours.

## Technical Support Tools

The options on the **Technical Support Tools** submenu are:

- Run Event Detection Analytics on DGAgent1
-  Retrieve Log Files from DGAgent1
- Open Log Folder for DGAgent1
- Generate Thread Dump File on DGAgent1
- Generate Memory Dump File on DGAgent1
- Memory Garbage Collection on DGAgent1

Command	Description
<b>Run Event Detection Analytics</b>	Runs the Event Detection Analytics tool for the selected job, which looks at real-time activity that has been occurring on that specific agent.
<b>Retrieve Log Files</b>	Retrieves log files for the selected Peer Agent. The log files contain information that the Peer Software Technical Support uses to assist in debugging issues. The log files are encrypted and are located in the support folder of the Peer Management Center installation directory. They can optionally be uploaded to the Technical Support team.
<b>Open Log Folder for Agent</b>	Opens the log folder.
<b>Generate Thread Dump File on Agent</b>	Generates a thread dump file for the selected Peer Agent, which can be used by Peer Software technical support to debug certain issues. The debug file is located in the Peer Agent installation directory.
<b>Generate Memory Dump File on Agent</b>	Generates a memory dump file for the selected Peer Agent, which can be used by Peer Software technical support to debug certain issues. The debug file is located in the Peer Agent installation directory.
<b>Memory Garbage Collection on Agent</b>	Forces a garbage collection operation to attempt to reclaim memory that is no longer used within the Peer Agent's JVM.

### Peer Agent Connection Statuses

A connection status indicates the state of the Peer Agent's connection to the Peer Management Broker. The Peer Management Broker serves to connect Peer Agents to Peer Management Center.

Peer Agent connection statuses are displayed in the **Agents** view in the Peer Management Management Center:

- The status of an Agent is displayed in parentheses after the Agent name.

- The color of an Agent is a visual aid that allows users to quickly identify the status.

Agent can have the following statuses:

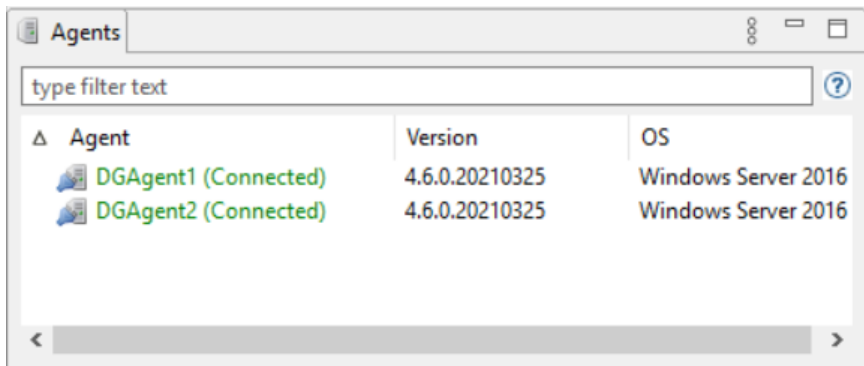
Status	Description
Connected	Indicates Peer Agent is currently connected to the <a href="#">Peer Management Broker</a> .
Disconnected	Indicates that Peer Agent has disconnected from the Peer Management Broker. This can be a result of stopping the Peer Agent, or if the network connection between the Peer Agent and the Peer Management Broker was severed.
Pending	This indicates that a <a href="#">heartbeat</a> for the Peer Agent was not received within the configured threshold and that the Peer Agent is in the process on being disconnected if a heartbeat is not received soon. This status can also occur if the Peer Agent does not respond to a pending ping.
Unknown	If no connection status is displayed, then either the Peer Agent was not running on that host when Peer Management Center was started, or the first heartbeat message has not been received from that host.

### Editing an Agent Configuration

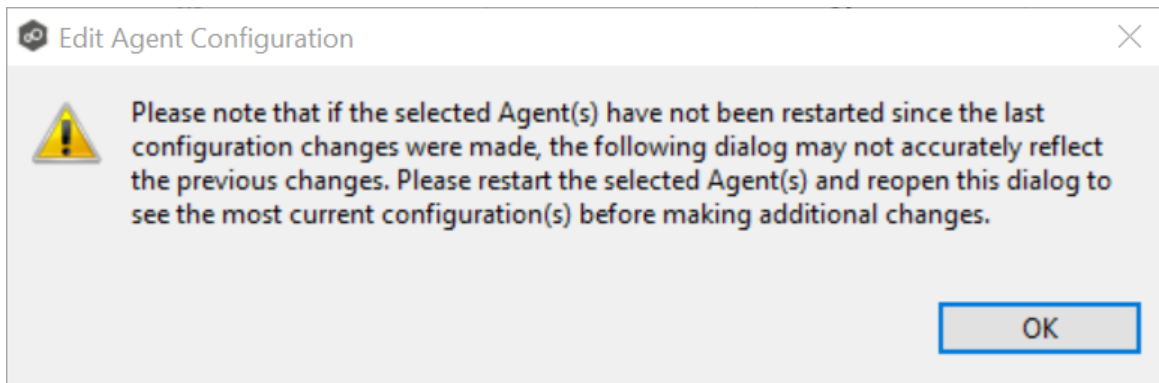
The ability to remotely manage the configuration of connected [Peer Agents](#) is available from within Peer Management Center.

To edit an Agent's configuration:

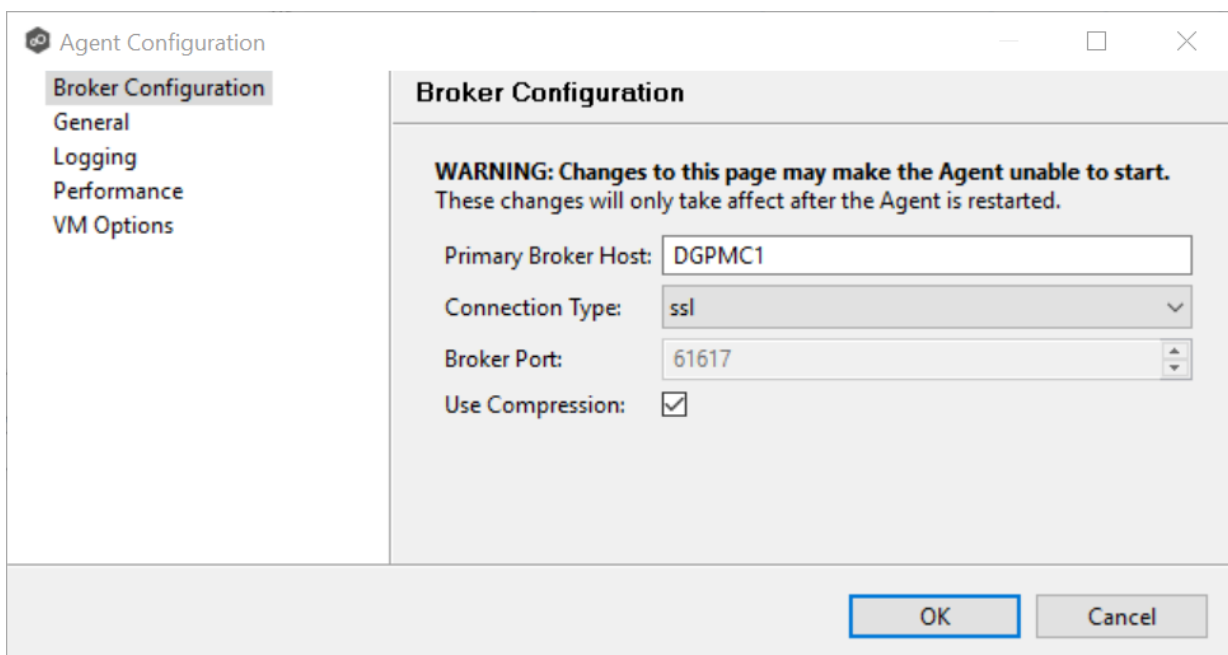
1. Right-click the connected Peer Agent in the **Agents** view:



2. Select **Edit Agent Configuration**.
3. Click **OK** in the dialog that appears:



The **Agent Configuration** page appears.





4. Select a tab to edit and make the desired changes:

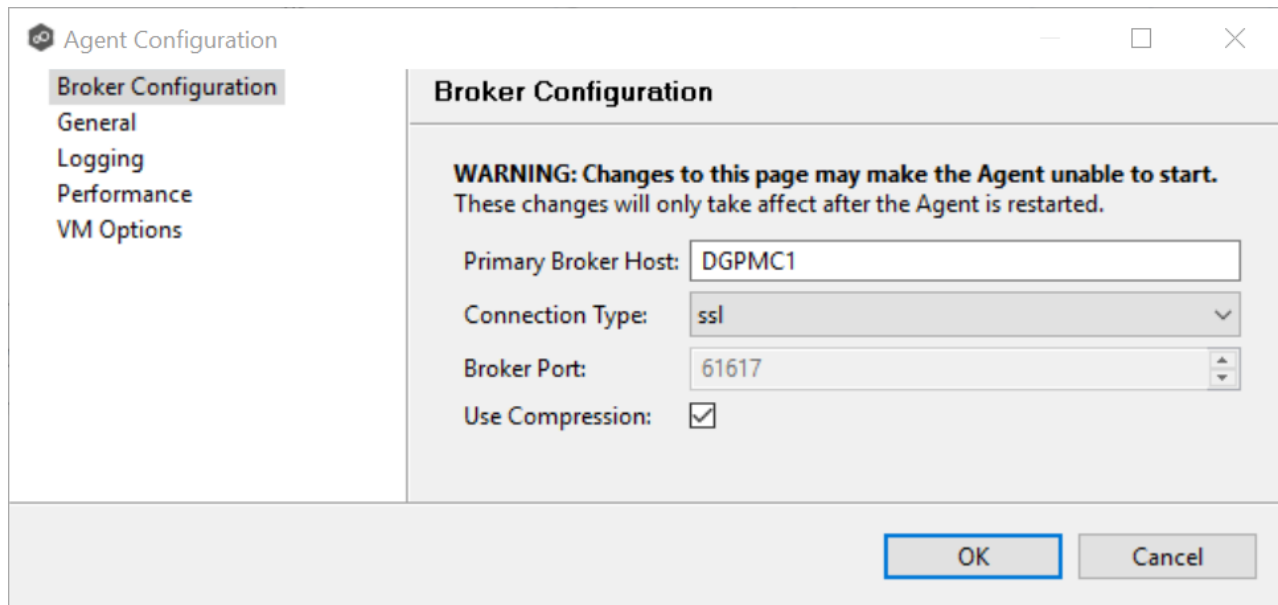
- [Broker Configuration](#)
- [General](#)
- [Logging](#)
- [VM Options](#)

5. Click **OK**.

For any configuration change to take effect, the selected Peer Agent must be restarted. If no jobs are running, you will have the option of restarting the Peer Agent at the close of the configuration dialog.

**Warning:** Changes to any of these options may result in problems when the Peer Agent restarts. Ensure all settings are correct before saving the dialog and restarting the selected Peer Agent.

The settings in **Broker Configuration** apply only to communication between the selected Peer Agent and Peer Management Broker and not to communication between Peer Management Center and Peer Management Broker.

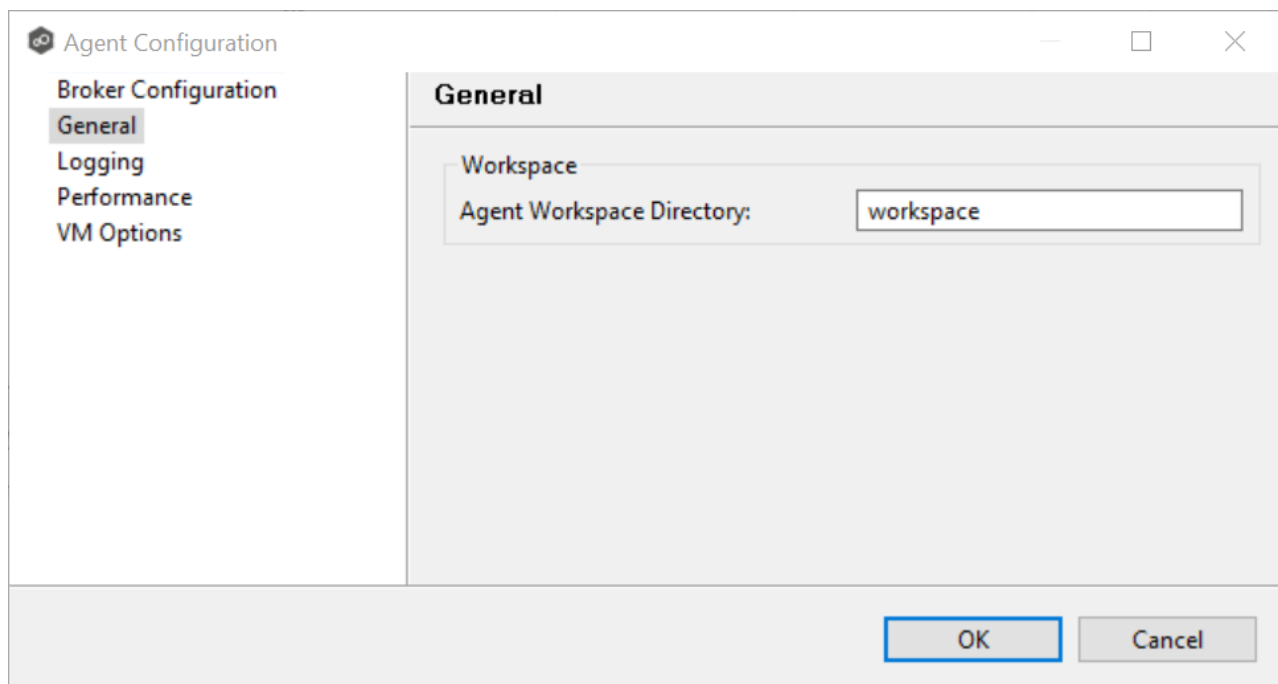


The screenshot shows the 'Agent Configuration' dialog box with the 'Broker Configuration' tab selected. The dialog has a sidebar on the left with tabs for 'Broker Configuration', 'General', 'Logging', 'Performance', and 'VM Options'. The main area displays the 'Broker Configuration' settings. A warning message at the top states: 'WARNING: Changes to this page may make the Agent unable to start. These changes will only take affect after the Agent is restarted.' Below the warning, there are four settings: 'Primary Broker Host' with a text input field containing 'DGPMC1', 'Connection Type' with a dropdown menu set to 'ssl', 'Broker Port' with a spinner box set to '61617', and 'Use Compression' with a checked checkbox. At the bottom right, there are 'OK' and 'Cancel' buttons.

Broker Configuration	
<b>WARNING: Changes to this page may make the Agent unable to start.</b> These changes will only take affect after the Agent is restarted.	
Primary Broker Host:	DGPMC1
Connection Type:	ssl
Broker Port:	61617
Use Compression:	<input checked="" type="checkbox"/>

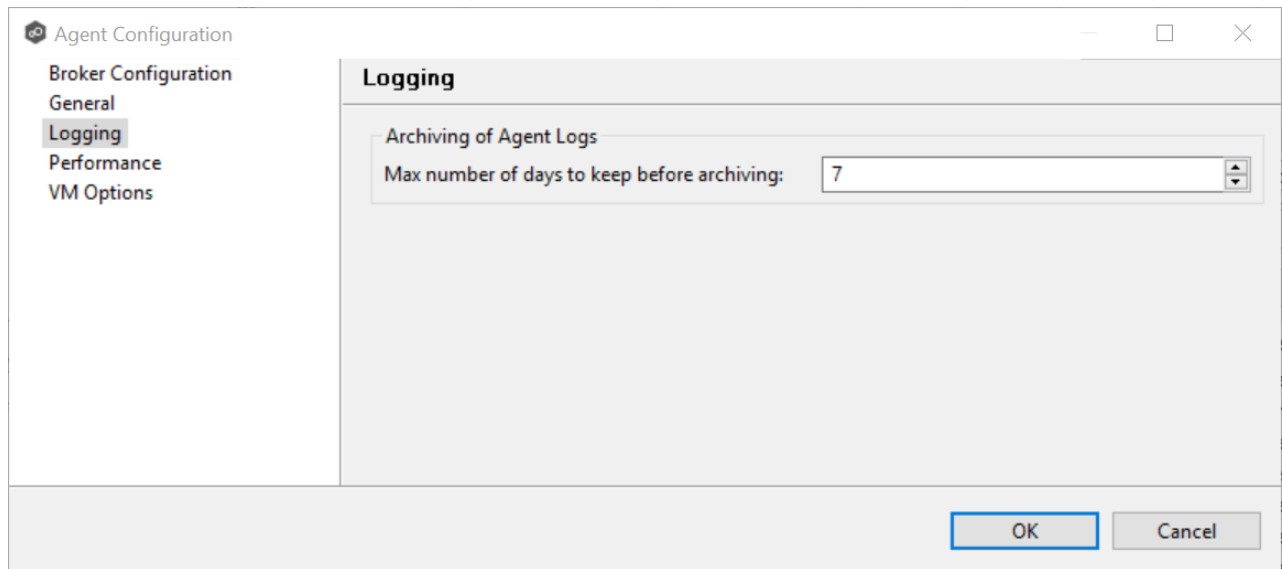
## Options

Option	Description
<b>Primary Broker Host</b>	The IP address or fully qualified host name of the server running Peer Management Center Broker.
<b>Connection Type</b>	The type of connection to use when communicating with Peer Management Center Broker. Types include SSL (encrypted) and TCP (not encrypted).
<b>Broker Port</b>	The port on which to communicate with Peer Management Center Broker.
<b>Use Compression</b>	When enabled, all communication between the selected Peer Agent and Peer Management Center Broker is compressed.

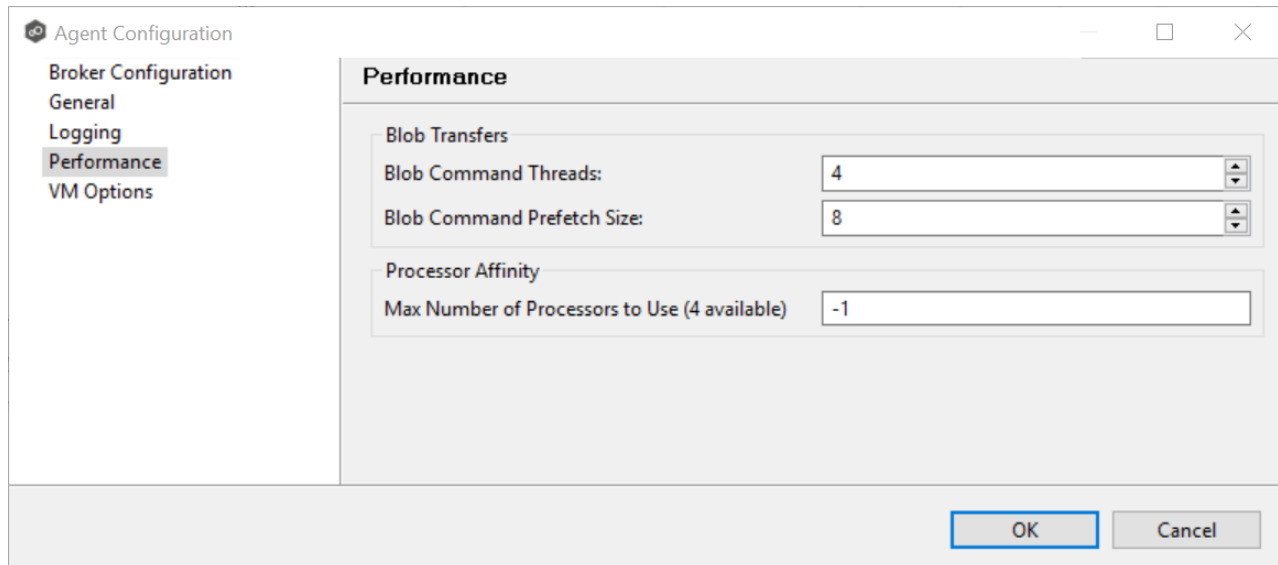


**Agent  
Workspace  
Directory**

The directory where log files and other application data is stored. This path is relative to the Peer Agent's installation directory. It can also be set to an explicit full path.

**Max number of  
days to keep  
before archiving**

Log files that are older than this date will automatically be zipped up and archived to reduce required space on disk.



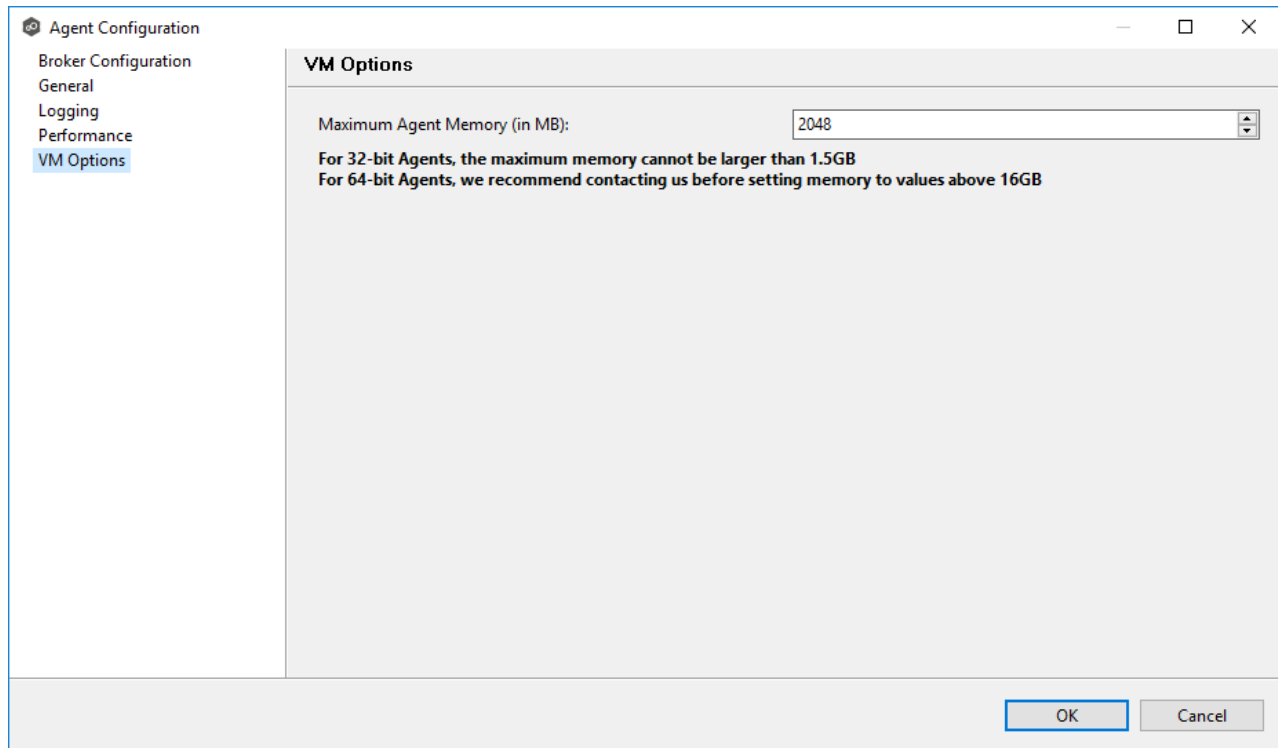
The image shows a screenshot of the 'Agent Configuration' window, specifically the 'Performance' tab. The window has a sidebar on the left with the following menu items: 'Broker Configuration', 'General', 'Logging', 'Performance' (which is highlighted), and 'VM Options'. The main area of the window is titled 'Performance' and contains three sections of settings:

- Blob Transfers**: This section contains two settings:
  - Blob Command Threads**: A numeric input field with the value '4'.
  - Blob Command Prefetch Size**: A numeric input field with the value '8'.
- Processor Affinity**: This section contains one setting:
  - Max Number of Processors to Use (4 available)**: A numeric input field with the value '-1'.

At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

Field	Description
<b>Blob Command Threads</b>	Enter the maximum number of threads to handle data transfer between each Agent and the Peer Management Center server. Increasing this typically improves replication performance but often increases memory consumption.
<b>Blob Command Prefetch Size</b>	Modify this setting only at the instruction of the Peer Software Technical Support Team.
<b>Max Number of Processors to Use (x available)</b>	Enter the maximum number of processors the Peer Agent service will be able to use. If set to -1, all processors will be available. The label for this setting displays how many total processors are available.

The option on the page allows you to tune the maximum amount of system memory that the Peer Agent service will use on the server where it is installed. We strongly recommend that this value be set to no lower than 1 GB.



## Viewing Agent Properties

To view the properties of an Agent:

1. Right-click the Agent in the **Agents** view.
2. Select **View Properties**.

The **View Agent Properties** dialog opens.

**View Agent Properties**

General | Heartbeat | Machine | Messaging | Performance | JVM Performance

Agent Host Name: DGWin16B

Connection Status: Connected

Custom Description: ☐

Description:

Discovery Time: 11-28-2018 14:35:17

Heartbeat Enabled: ☒

JVM Architecture: amd64

JVM Version: 1.8.0\_152-b16

Local Time: 02-12-2019 15:48:29 EST

Local TimeZone: Eastern Standard Time

SSL Enabled: ☒

Start Time: 02-11-2019 14:24:29

Username: administrator

Version: 4.3.0.20190208

OK Cancel

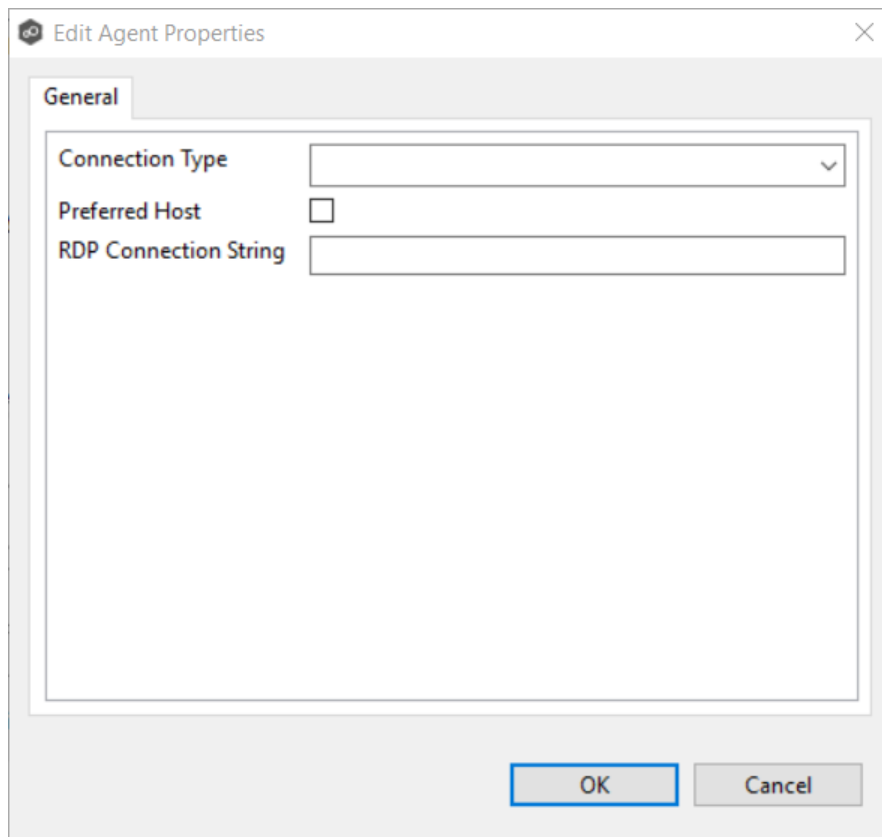
This dialog displays Peer Agent and host machine information across the following tabs:

Tab	Description
<b>General</b>	Displays general Peer Agent run-time information such as discovery time, local time, TLS use, Peer Agent start up time, Peer Agent version, and the user name Peer Agent service is running as.
<b>Heartbeat</b>	Displays heartbeat information and statistics such as heartbeat frequency, average heartbeat time, last heartbeat time, total Peer Agent disconnects, total missing heartbeats.
<b>Machine</b>	Displays machine information of the host that the Peer Agent is running on such as number of processors, computer name, domain name, IP address, installed memory, O/S.

Tab	Description
<b>Mess agin g</b>	Displays general Peer Management Center Broker messaging statistics for the selected host, such as total messages received, total messages sent, # errors.
<b>Perfo rman ce</b>	Displays general performance statistics for the underlying host machine such as available virtual memory, available physical memory, memory load.
<b>JVM Perfo rman ce</b>	Displays JVM performance statistics for the running Peer Agent application such as active number of threads, heap memory used, non-heap memory used.

### Editing Agent Properties

Selecting **Edit Properties** menu item for a selected agent will result in the opening of the following Peer Agent **Properties** dialog:



This dialog displays the following configurable Peer Agent and host machine options:

Option	Description
<b>Connection Type</b>	Allows for the selection of a connection type between the selected Peer Agent and the associated Peer Management Broker. When set, optimizations are made to the communication between the two parties based on the selected connection type.
<b>Preferred Host</b>	A best practice optimization for selecting which Peer Agent has the fastest connection to the Peer Management Broker (or in appropriate cases, for selecting which Peer Agent are on the same subnet as the Peer Management Broker).
<b>RDP Connection String</b>	The connection string to use when activating an <b>Remote Desktop Protocol (RDP)</b> session to this Peer Agent.



## Re-enabling a Disabled Agent Within a Job

Once disabled within a job, an Agent will not be involved in replication or locking. After the malicious activity that triggered MED is investigated and it is safe to re-enable the afflicted Agent, it will need to be re-enabled on a per job basis.

To review the status of an Agent within a job and to re-enable it, navigate to the **Participants** tab in the job's Runtime Summary view.

If an error is disabled because of a MED action, the message will be similar to the following:

The screenshot displays the 'Participants' tab in the Peer Management Center. A 'Participant Details' popup is open for the host 'DellT110a'. The popup shows the following information:

- Host Name:** DellT110a
- Directory:** \\svm9x-1\cifs1\Departments\Sales
- Status:** Disabled
- State:** Disabled
- Monitoring:** false
- Message:** Malicious Event Detection (MED) - Bait File Alert (Alert and Disable Host: Please check for unwanted activity before re-enabling) Alert Message info=BAIT FILE ALERT appld=113, appSessionId=144 path=See Message Field msg=TriggerAlertFileFound: Path=\\svm9x-1\cifs1\Departments\Sales\pc-med\_bin\Doc\_001-med.docx - EventName: RENAME details=|Participant Detected=DellT110a|Alert Message=TriggerAlertFileFound: Path=\\svm9x-1\cifs1\Departments\Sales\pc-med\_bin\Doc\_001-med.docx - EventName: RENAME|Time Detected=Mon Mar 12 19:36:14 EDT 2018|User Detected=MattM|IP Detected=ActiveCounterValue=|Process Detected=SMBVersion=31|Share Detected=cifs1|Job Session ID=3249149797
- Status Date:** 03-12-2018 19:36:18
- Message Date:** 03-12-2018 19:36:18

The background shows a table of participants and a 'Host Participant State Change Log'.

Date	Host	Status
03-12-2018 ...	DellT110a	Disabled
03-12-2018 ...	DellT3610b	Not Participi
03-12-2018 ...	DellT110a	Disabled
03-12-2018 ...	DellT110a	Not Participi
03-12-2018 ...	DellT3610b	Not Participi
03-12-2018 ...	DellT3610b	Particioatir

At the bottom, the status is shown as 'Halted. (Quorum Lost)'.

To re-enable the Agent, right-click it within this view, and select **Enable Host Participant**.

## Updating a Peer Agent

If the Peer Agent software running on a host is out of date, the host is shown as having a pending update in the [Agents view](#).

When right-clicking the host, the option to automatically update the Peer Agent software is also available. This process can be done from Peer Management Center and usually does not require any additional actions on the host server itself.

## PeerGFS API

The PeerGFS API is a RESTful API. It allows system administrators to monitor PeerGFS activity and developers to integrate PeerGFS functionality into their own application.

Currently, the API allows users to:

- Get information about running jobs, such as open files as well as files in the process of being synchronized; statistical info about watch set, queue sizes, replication metrics; scan status, alerts, and quarantined files.
- Start and stop jobs.
- View and restart agents.
- View scheduled tasks.
- Trigger log uploads.

Additional functionality, such as the ability to create and edit jobs, will be provided in future versions of the API.

## Accessing the PeerGFS API

Access to the PeerGFS API is available as a combination of two elements:

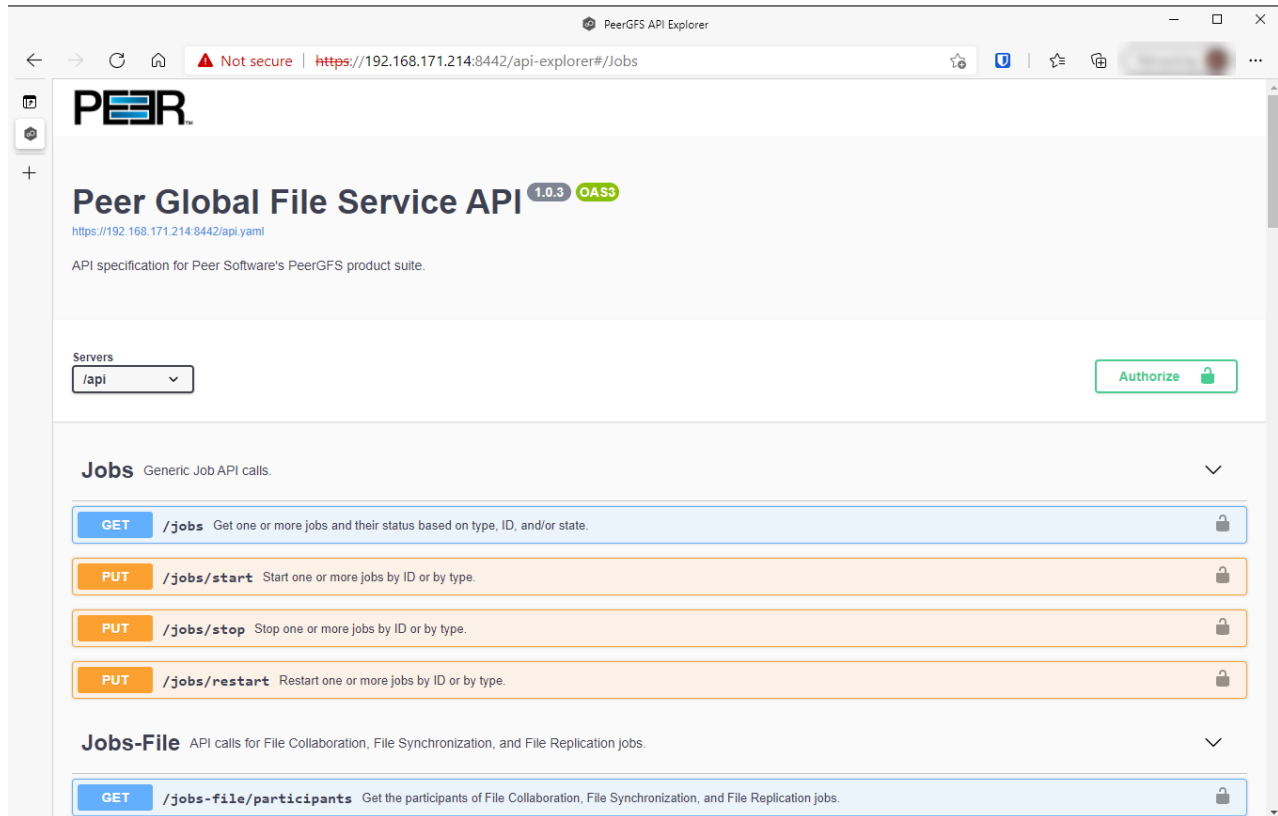
- A web URL hosted by the API service. This URL is defined as a combination of a PMC server name or IP and a port, as specified by the [Web and API Configuration](#) settings in [Preferences](#).
- Local (aka basic) authentication with a user name and password that is passed into a script or the API web interface. This user name and password is used to authenticate the user with the PeerGFS API service.

If you are authenticated, you are authorized to access the entire API. Role-based access will be added in future versions of the API.

## Testing the PeerGFS API

One way to test the PeerGFS API is to use the API web interface.

To access the web interface, open a browser, go to the API endpoint (e.g. `https://<PMC IP or name> or <8442>`), and try the API calls.



## Integrating Your Own Tools and Scripts with the PeerGFS API

The PeerGFS installation folder contains PowerShell and Bash toolkits in the **tools** subfolder of the PMC's installation folder. If you need a different language, contact Peer Technical Support for our latest YAML file.

If you would like to access the API through a client in a language other than PowerShell or BASH, you can use the Swagger Editor to convert our YAML file to the appropriate client code:

1. Save the PeerGFS YAML file to your desktop.
2. Open a web browser tab and point it to <https://editor.swagger.io/#/>.
3. Go to the **File** menu inside the web interface, and select **Import file**.

4. Select the PeerGFS YAML file on the desktop.

The manifest should appear on the left with the front-end mockup on the right.

5. Use the Swagger Editor to generate client code.

### API Quick Reference

The PeerGFS API REST specifications are documented using OpenAPI (also known as Swagger). This documentation is visible via the PMC API's web interface. To access the web interface, see [Testing the PeerGFS API](#).

Within the API web interface, you can also send test requests and view responses as well as see REST calls that can be made to the API service.

The PeerGFS is divided into four types of API calls:

- Jobs - Generic job-related calls
- Jobs-File - Job-specific calls
- Agents - Agent-related calls
- PMC - Calls related to alerts, tasks, and logs

The PeerGFS API has three status codes:

200 - Success

401 - Unauthorized

404 - Job(s) not found

## Scheduled Replication

Use a scheduled replication filter to identify files and folders that you don't want replicated in real-time--instead, they will be replicated at a scheduled time or interval. If a file or folder meets the filter criteria, instead of being processed in real-time, it will be placed in a queue for synchronization and processed as scheduled.

Schedule replication filters can be used with file collaboration, file replication, and file synchronization jobs. For information on defining a scheduled replication filter, see [Scheduled Replication](#) in [Preferences](#).

Note: When a scheduled replication filter is used in a file collaboration job, files that meet the filter criteria will not be locked.

## Smart Data Seeding

### Overview

Smart data seeding applies to File Collaboration, File Replication, and File Synchronization jobs.

Occasionally, a new host or a host which has been removed from the session for a long time, needs to be introduced into an existing collaboration. Smart Data Seeding supports integrating new hosts into a collaboration seamlessly. Conventional seeding methods take a long time over typically slow WAN connections and require a cut-over with a final scan to get the data synchronized. With Smart Data Seeding's default settings, real-time events are processed from the Smart Data Seeding hosts while the initial one-way background scan ensures the target(s) have all the files in place.

Smart Data Seeding provides the ability to set one or more participants in a Smart Data Seeding mode. Smart Data Seeding hosts are considered the hosts from where files will be copied to all the other participants in the session. When a host is in Smart Data Seeding mode, it follows the rules of the job's Smart Data Seeding Mode configuration (see below). Initial scans run in a one-way mode to avoid bringing back deleted files. It is not recommended to have active ([Active-Active](#)) users on the target hosts. Once the initial scan is completed, the Smart Data Seeding host(s) are set back to their default full collaboration mode with no user interaction or final scan.

To enable advanced settings in the Conflict Resolution window, add the following fc.ini option and restart Peer Management Center:

```
fc.scan.enable.preseeding.ui=true
```

### Smart Data Seeding Options

From the **Conflict Resolution** window, select from one of the following Smart Data Seeding modes:

Mode	Description
<b>PASSIVE (Default)</b>	<p>Initial scan will be one-way only with any host in Smart Data Seeding mode:</p> <ul style="list-style-type: none"> <li>• Real-time activity on Smart Data Seeding host is disabled.</li> <li>• Real-time events on that host will be quarantined.</li> <li>• Renamed files will be restored.</li> </ul>
<b>PASSIVE _WITH_R ESTORE</b>	<p>Initial scan will be one-way only with any host in Smart Data Seeding mode:</p> <ul style="list-style-type: none"> <li>• Real-time activity on Smart Data Seeding host is disabled.</li> <li>• Any activity on that host will be restored to its original state.</li> </ul>
<b>ACTIVE_ LIMITED</b>	<p>Initial scan will be one-way only with any host in Smart Data Seeding mode:</p> <ul style="list-style-type: none"> <li>• Real-time activity on Smart Data Seeding host is enabled in a limited mode (real-time file adds are processed).</li> <li>• Unsynchronized file updates will be quarantined.</li> <li>• Unsynchronized file renamed will be restored.</li> <li>• Unsynchronized file deletes will be restored.</li> </ul>
<b>ACTIVE_ FULL</b>	<p>Initial scan will be one-way only with any host in Smart Data Seeding mode except for updates (updates will be processed as Latest Modified wins):</p> <ul style="list-style-type: none"> <li>• Real-time activity on Smart Data Seeding host is enabled with latest modified file wins, regardless if latest file is on the Smart Data Seeding host.</li> </ul>
<b>REACTIV ATION</b>	<p>Initial Scan will be one-way only with any host in Smart Data Seeding mode:</p> <ul style="list-style-type: none"> <li>• Real-time activity on Smart Data Seeding host is enabled with Quarantine (Added and Updated Files will be quarantined during the scan).</li> </ul>

Mode	Description
	<ul style="list-style-type: none"><li>• Unsynchronized file updates will be quarantined during real-time.</li><li>• Unsynchronized file renames will be restored.</li><li>• Unsynchronized deletes will be restored.</li></ul>

The default setting is `ACTIVE_LIMITED`, which will initiate a one-way scan with any host in Smart Data Seeding mode. During the scan, new files will be deleted, newer files will be overwritten, and deleted files will be restored on the Target(s). During real-time activity, add events will be processed, but updates will be quarantined if the files are unsynchronized. Renames and deletes will be restored if the files are unsynchronized.

The `ACTIVE_LIMITED` setting is recommended in most cases in which a new host or a host which has been removed from the session for a long time needs to be introduced into an existing collaboration.

## Storage Capacity

The storage capacity available for your jobs is based on your Peer Global File Service [license](#). Automated alerts will notify you when you close to reaching your licensed storage capacity. If you exceed your licensed storage capacity, contact your Peer Software sales representative.

Total capacity consumed is defined by the total number of unique TBs under management across all participants rather than the total capacity used by all participants. In this unique TB model, a 1 TB file that is synchronized across 10 participants only counts as 1 TB and not 10 TBs. For example, if your licensed storage capacity is 100TB and you have a job with 5 participants totaling 20 unique TBs, you have used total of 20% of your storage capacity, not 100%.

## TLS Certificates

You can use custom or private Transport Layer Security (TLS) certificates to connect a Peer Agent to Peer Management Broker. The Keytool certificate management utility will be used to store the key and certificate into a keystore file, which protects the private keys with a password.

Note the paths in the following topics reference a default install directory for both Peer Management Center and Peer Agent.

For step-by-step instructions, see:

- [Creating New Certificates](#)
- [Using Existing Certificates](#)

For additional information, please contact Peer Software's support team via email: [support@peersoftware.com](mailto:support@peersoftware.com).

## Creating New Certificates

### Keytool Utility

Perform the necessary commands using the Keytool certificate management utility bundled with your Peer Management Center or Peer Agent installation. The location of the utility is:

- Peer Management Center system: PMC\_INSTALLATION\_FOLDER\jre\bin
- Peer Agent system: PEER\_AGENT\_INSTALLATION\_FOLDER\jre\bin

### Broker Keystore Generation

Step 1. Using the Keytool utility, create a certificate for Peer Management Center.

```
keytool -genkey -alias broker -keyalg RSA -keystore broker.ks -storepass  
plBroker4321 -validity 3000
```

<b>broker</b>	The alias of the new broker keystore containing the new certificate.
<b>broker.ks</b>	Destination broker keystore that will be created containing the new certificate.
<b>plBroker4321</b>	The password you assign to the new broker keystore.

**Note:** The broker.ks file will be created in the \jre\bin folder.

**Example:**



```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -genkey -alias
broker -keyalg RSA -keystore broker.ks -storepass plBroker4321 -validity 3000
What is your first and last name?
[Unknown]: Monika Cuellar
What is the name of your organizational unit?
[Unknown]: Peer Software, Inc.
What is the name of your organization?
[Unknown]: Peer Software, Inc.
What is the name of your City or Locality?
[Unknown]: Centreville
What is the name of your State or Province?
[Unknown]: VA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA, C=US
correct?
[no]: yes

Enter key password for <broker>
(RETURN if same as keystore password):

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

**Step 2:** Export the broker's certificate so it can be shared with clients.

```
keytool -export -alias broker -keystore broker.ks -file broker.cer
```

<b>broker</b>	The alias of the new broker keystore containing the new certificate.
<b>broker.ks</b>	Destination broker keystore that will be created containing the new certificate.
<b>broker.cer</b>	The name of the broker's certificate to be created.

**Note:** The broker.cer file will be created in the \jre\bin folder.

**Example:**

```

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -export -alias
broker -keystore broker.ks -file broker.cer
Enter keystore password: plBroker4321
Certificate stored in file <broker.cer>

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>

```

**Step 3:** Create a certificate/keystore for the client.

```
keytool -genkey -alias client -keyalg RSA -keystore client.ks -storepass
plClient4321 -validity 3000
```

<b>client</b>	The alias of the new client keystore containing the new certificate.
<b>client.ks</b>	Destination keystore for the client that will be created containing the new certificate.
<b>plClient4321</b>	The password you assign to the new client keystore.

**Note:** The client.ks file will be created in the \jre\bin folder.

**Example:**

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -genkey -alias
client -keyalg RSA -keystore client.ks -storepass plClient4321 -validity 3000
What is your first and last name?
[Unknown]: Monika Cuellar
What is the name of your organizational unit?
[Unknown]: Peer Software, Inc.
What is the name of your organization?
[Unknown]: Peer Software, Inc.
What is the name of your City or Locality?
[Unknown]: Centreville
What is the name of your State or Province?
[Unknown]: VA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville, ST=VA,
C=US
correct?
[no]: yes

Enter key password for <client>
(RETURN if same as keystore password):

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

**Step 4:** Create a truststore for the client and then import the broker's certificate. This establishes that the client "trusts" the broker.

```
keytool -import -alias broker -keystore client.ts -file broker.cer -
storepass plClient4321
```

<b>broker</b>	The alias of the broker keystore created in step 1.
<b>client.ts</b>	Destination truststore for the client that will be created containing the broker's certificate.

<b>broker.cer</b>	The broker's certificate created in step 2.
<b>plClient4321</b>	The password assigned to the client keystore in Step 3.

**Example:**

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -import -alias
broker -keystore client.ts -file broker.cer -storepass plClient4321
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA, C
=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA,
C=US
Serial number: 4fa7f34f
Valid from: Mon May 07 12:07:43 EDT 2012 until: Fri Jul 24 12:07:43 EDT 2020
Certificate fingerprints:
    MD5:  2C:18:DD:B5:CD:C5:3D:B2:9B:E3:93:50:D6:74:2B:64
    SHA1: 30:77:94:9B:34:63:6C:DE:2C:98:9C:00:C2:B9:F6:21:AE:22:D7:DE
Trust this certificate? [no]: yes
Certificate was added to keystore

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

**Optional:** List the certificates in the broker keystore.

```
keytool -list -v -keystore broker.ks -storepass plBroker4321
```

**Example:**

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -list -v -
keystore broker.ks -storepass plBroker4321

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: broker
Creation date: May 7, 2012
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA, C=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA, C=US
Serial number: 4fa7f34f
Valid from: Mon May 07 12:07:43 EDT 2012 until: Fri Jul 24 12:07:43 EDT 2020
Certificate fingerprints:
    MD5:  2C:18:DD:B5:CD:C5:3D:B2:9B:E3:93:50:D6:74:2B:64
    SHA1: 30:77:94:9B:34:63:6C:DE:2C:98:9C:00:C2:B9:F6:21:AE:22:D7:DE

*****
*****

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

## Verify Client Certificate

If you want to verify client certificates, you need to take a few extra steps.

**Step 1:** Export the client's certificate so it can be shared with broker.

```
keytool -export -alias client -keystore client.ks -file client.cer -
storepass plClient4321
```

**Note:** The client.cer file will be created in the \jre\bin folder.

**Example:**

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -export -alias
client -keystore client.ks -file client.cer -storepass plClient4321
Certificate stored in file <client.cer>

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

**Step 2:** Create a truststore for the broker, and import the client's certificate. This establishes that the broker "trusts" the client:

```
keytool -import -alias client -keystore broker.ts -file client.cer -
storepass plBroker4321
```

**Example:**

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -import -alias
client -keystore broker.tx -file client.cer -storepass plBroker4321
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA, C
=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=VA,
C=US
Serial number: 4fa7f982
Valid from: Mon May 07 12:34:10 EDT 2012 until: Fri Jul 24 12:34:10 EDT 2020
Certificate fingerprints:
    MD5: A7:D9:6E:78:8B:A9:AD:32:96:2D:51:6B:53:0B:E4:BD
    SHA1: 16:05:7C:C4:D5:AB:E7:D3:7D:5B:2E:02:B5:3B:69:54:D1:C3:53:52
Trust this certificate? [no]: yes
Certificate was added to keystore

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

**Optional:** List the certificates in the client keystore.

```
keytool -list -v -keystore client.ks -storepass plClient4321
```

**Example:**

```
C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>keytool -list -v -
keystore client.ks -storepass plClient4321

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: client
Creation date: May 7, 2012
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=NY,
C=US
Issuer: CN=Monika Cuellar, OU="Peer Software, Inc.", O="Peer Software, Inc.", L=Centreville,
ST=NY,
C=US
Serial number: 4fa80618
Valid from: Mon May 07 13:27:52 EDT 2012 until: Fri Jul 24 13:27:52 EDT 2020
Certificate fingerprints:
    MD5: 06:11:97:71:D6:23:91:63:2F:19:F4:05:EA:2F:9D:14
    SHA1: A7:26:80:9E:18:2B:46:8E:92:BB:AD:89:44:0A:8A:9C:8C:1F:62:38

*****
*****

C:\Program Files\Peer Software\File Collaboration Enterprise\jre\bin>
```

## Copy the Generated Keystore Files into Their Appropriate Location

**On the Peer Management Center system:** Copy the following files from the "C:\Program Files\Peer Software\Peer Management Hub\jre\bin" directory into the "C:\Program Files\Peer Software\Peer Management Hub\Broker\keys" directory on the Peer Management Center system. Overwrite the existing files.

broker.ks

broker.ts

**On the Peer Agent system:** Copy the following files from the "C:\Program Files\Peer Software\Peer Management Hub\jre\bin" directory into the "C:\Program Files\Peer Software\Peer Agent\keys" directory on the Peer Agent systems. Overwrite the existing files.

client.ks

client.ts

## Restart All Peer Management Center Services for the Changes to Take Effect

We recommend you create a folder outside the Peer Management Center/Peer Agent installation directories in which to store the keystore files. This will ensure that upgrades will not clear/overwrite these files. **The steps outlining this process will be posted shortly.**

### Using Existing Certificates

## Keytool Utility

Perform the necessary commands using the Keytool certificate management utility bundled with your Peer Management Center or Peer Agent installation. The location of the utility is:

- Peer Management Center system: PMC\_INSTALLATION\_FOLDER\jre\bin
- Peer Agent system: PEER\_AGENT\_INSTALLATION\_FOLDER\jre\bin

## Peer Management Broker and Peer Agent Keystore Generation

You will need to have two custom/private certificates. One for the Peer Management Broker and one for all the participating Peer Agents. You may select different algorithms and encryption key size (i.e., RSA, DSA with 1024 or 2048 key size).

**Step 1.** Using the Keytool utility, list the contents of the custom/private certificates. Perform these steps for both certificates (Peer Management Broker and Peer Agent. Make a note of the Alias of the certificate, if it exists.

```
keytool -list -v -keystore HubCert.pfx -storetype pkcs12
```

<b>HubCert.pfx</b>	Represents the custom/private certificate for Peer Management Center Broker.
<b>AgentCertificate.pfx</b>	Represents the custom/private certificate for the Peer Agents.

**Note:** The command will prompt you to enter the password you set on your custom certificate, if applicable.

**Step 2.** Add the custom/private Peer Management Center Broker certificate into the Peer Management Center Broker keystore.

```
keytool -importkeystore -deststorepass plBroker4321 -destkeypass  
plBroker4321 -destkeystore broker.ks -srckeystore HubCert.pfx -  
srcstoretype PKCS12 -srcstorepass PASSWORD -alias ALIAS -destalias broker
```

<b>plBroker4321</b>	The password you assign to the new Broker keystore.
<b>broker.ks</b>	Destination keystore that will be created containing the custom/private certificate.
<b>HubCert.pfx</b>	Custom/private certificate being imported into the new keystore.
<b>PASSWORD</b>	The password of the custom/private certificate, if it exists. If you omit the -srcstorepass command, you will be prompted for the certificate password if needed.
<b>ALIAS</b>	The Alias of the custom/private certificate you discovered in Step 1 above.

<b>broker</b>	The Alias of the new keystore containing the custom/private.
---------------	--

**Note:** The broker.cer and broker.ks files will be created in the \jre\bin folder where the keytool utility resides.

**Step 3.** Add the custom/private Peer Agent certificate into the Client keystore.

```
keytool -importkeystore -deststorepass plClient4321 -destkeypass
plClient4321 -destkeystore client.ks -srckeystore AgentCert.pfx -
srcstoretype PKCS12 -srcstorepass PASSWORD -alias ALIAS -destalias client
```

<b>plClient4321</b>	The password you assign to the new Broker keystore.
<b>client.ks</b>	Destination keystore that will be created containing the custom/private certificate.
<b>AgentCert.pfx</b>	Custom/private certificate being imported into the new keystore.
<b>PASSWORD</b>	The password of the custom/private certificate, if it exists. If you omit the -srcstorepass command, you will be prompted for the certificate password if needed.
<b>ALIAS</b>	The Alias of the custom/private certificate you discovered in Step 1 above.
<b>client</b>	The Alias of the new keystore containing the custom/private.

**Note:** The client.cer and client.ks files will be created in the \jre\bin folder where the keytool utility resides.

**Step 4.** Export the broker's certificate so it can be shared with clients.

```
keytool -export -alias broker -keystore broker.ks -file broker.cer
```



<b>broker</b>	The Alias of the broker keystore containing the custom/private certificate created in Step 2 above.
<b>broker.ks</b>	The keystore file created in Step 2 above containing the custom/private certificate for the Broker.
<b>broker.cer</b>	The certificate file created in Step 2 above.

The command will prompt you to enter the password for the broker keystore (e.g. plBroker4321).

**Step 5.** Export the client's certificate so it can be shared with broker.

```
keytool -export -alias client -keystore client.ks -file client.cer
```

<b>client</b>	The Alias of the client keystore containing the custom/private certificate created in Step 3 above.
<b>client.ks</b>	The keystore file created in Step 3 above containing the custom/private certificate for the Peer Agents.
<b>client.cer</b>	The certificate file created in Step 3 above.

The command will prompt you to enter the password for the client keystore (e.g., plClient4321).

**Step 6.** Create a truststore for the broker and import the client's certificate. This establishes that the broker "trusts" the client:

```
keytool -import -alias client -keystore broker.ts -file client.cer
```

<b>client</b>	The Alias of the client keystore containing the custom/private certificate created in Step 3 above.
<b>broker.</b>	The broker trust store to be created.

<b>ts</b>	
<b>client.cer</b>	The certificate file created in Step 3 above.

The command will prompt you to enter the password for the broker keystore (e.g., plBroker4321).

**Step 7.** Create a truststore for the client and import the broker's certificate. This establishes that the client "trusts" the broker.

```
keytool -import -alias broker -keystore client.ts -file broker.cer
```

<b>broker</b>	The Alias of the client keystore containing the custom/private certificate created in Step 3 above.
<b>client.ts</b>	The client truststore to be created.
<b>client.cer</b>	The certificate file created in Step 2 above.

The command will prompt you to enter the password for the client keystore (e.g., plClient4321).

## Copy the Generated Keystore Files into Their Appropriate Location

### On the Peer Management Center system:

Copy the following files from the **Peer Management Center\_INSTALLATION\_FOLDER\jre\bin** directory into **the Peer Management Center\_INSTALLATION\_FOLDER\Broker\keys** directory on the Peer Management Center system. Overwrite the existing files.

broker.ks

broker.ts

### On the Peer Agent system:

Copy the following files from **Peer Management Center\_INSTALLATION\_FOLDER\jre\bin** directory into the **PEER\_AGENT\_INSTALLATION\_FOLDER\keys** directory on the Peer Agent systems. Overwrite the existing files.

client.ks

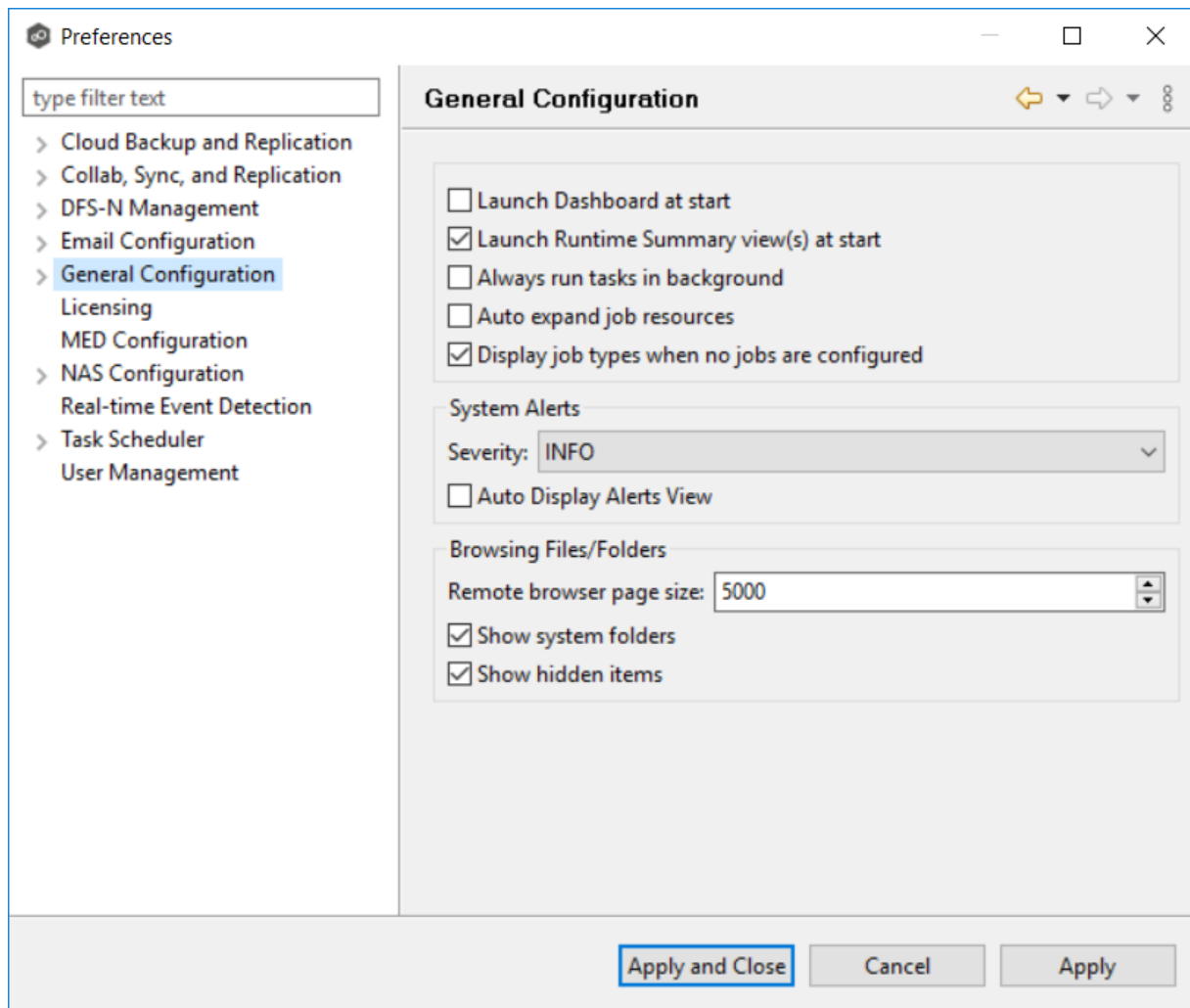
client.ts

## Restart All Peer Management Center Services for the Changes to Take Effect

We recommend you create a folder outside the Peer Management Center/Peer Agent installation directories in which to store the keystore files. This will ensure that upgrades will not clear/overwrite these files. The steps outlining this process will be posted shortly.

## Preferences

The **Preferences** dialog enables you to configure global settings, as well as settings specific to a job type. Before creating any jobs or configuring individual aspects of a job, Peer Software recommends first configuring a number of settings. Some settings are global and apply program-wide and/or to all job types; others are specific to a job type.



## Configuring Global Settings

Peer Software strongly recommends configuring the following settings before creating any jobs:

- [Email Configuration](#)
- Contacts and Distribution Lists
- System Alerts

Modify other global settings as needed. You may want to consult with Peer Software Technical Support when modifying the other global settings.

## Configuring Job Type Specific Settings

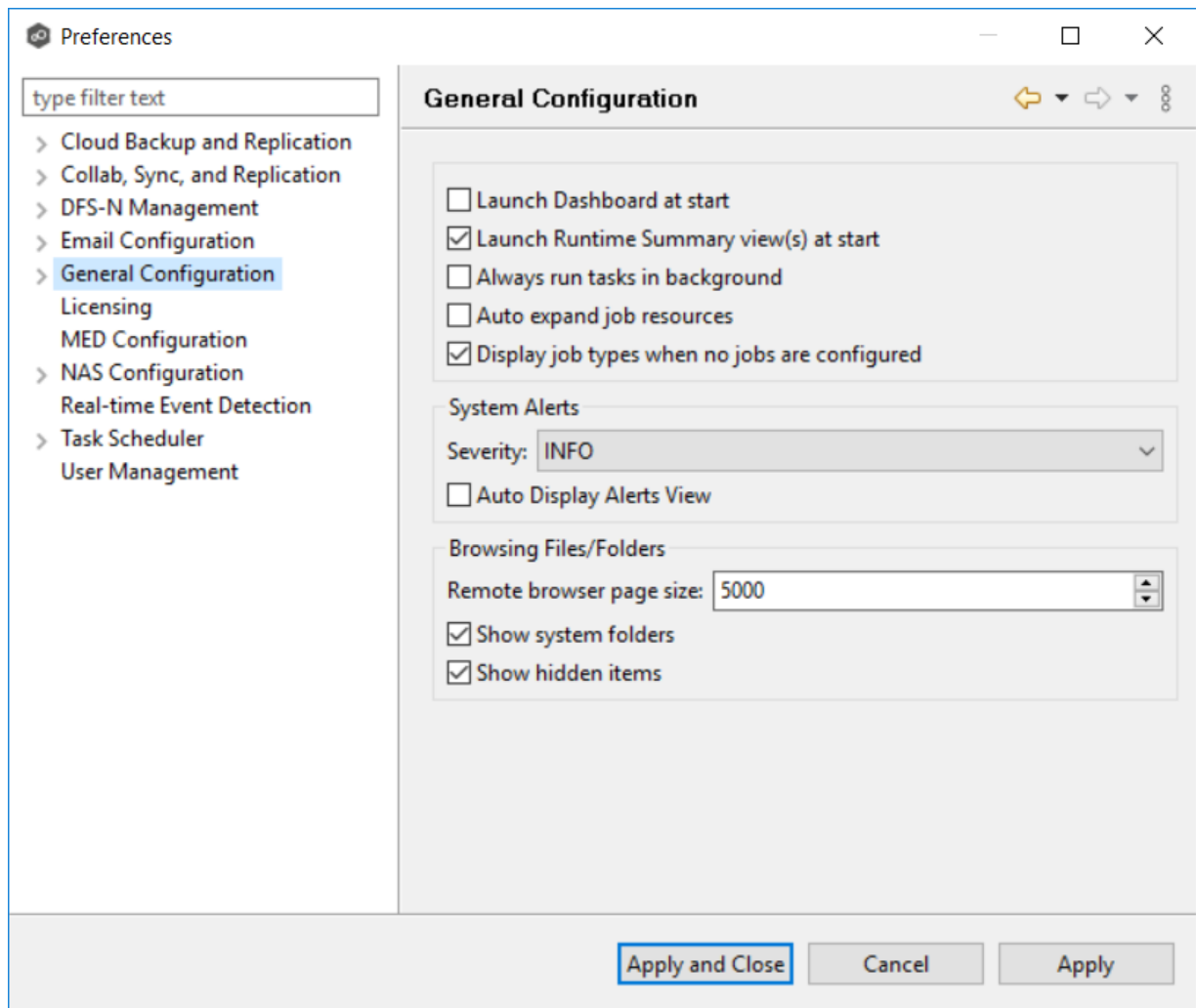
<b>Cloud Backup and Replication</b>	<ul style="list-style-type: none"><li>• <a href="#">Email Alerts</a></li><li>• <a href="#">File and Folder Filters</a></li><li>• <a href="#">Proxy Configuration</a>.</li></ul>
<b>File Collaboration, File Locking, File Replication, and File Synchronization</b>	<ul style="list-style-type: none"><li>• <a href="#">Email Alerts</a></li><li>• <a href="#">File and Folder Filters</a></li></ul>

## Configuring Preferences

To modify settings:

1. Click a category on the left to see its corresponding options appear on the right side of the dialog.

For example, click the **General Configuration** category to view and configure general program-wide settings.



2. Make as many changes as you like to the category settings, and then click:

- **Apply and Close** to save the new settings and return to the program.
- **Cancel** to close the dialog without saving your changes.
- **Apply** to save your changes and keep the **Preferences** dialog open.

## Cloud Backup and Replication Job Preferences

You can modify the following Cloud Backup and Replication settings:

- [Cloud Backup and Replication](#)

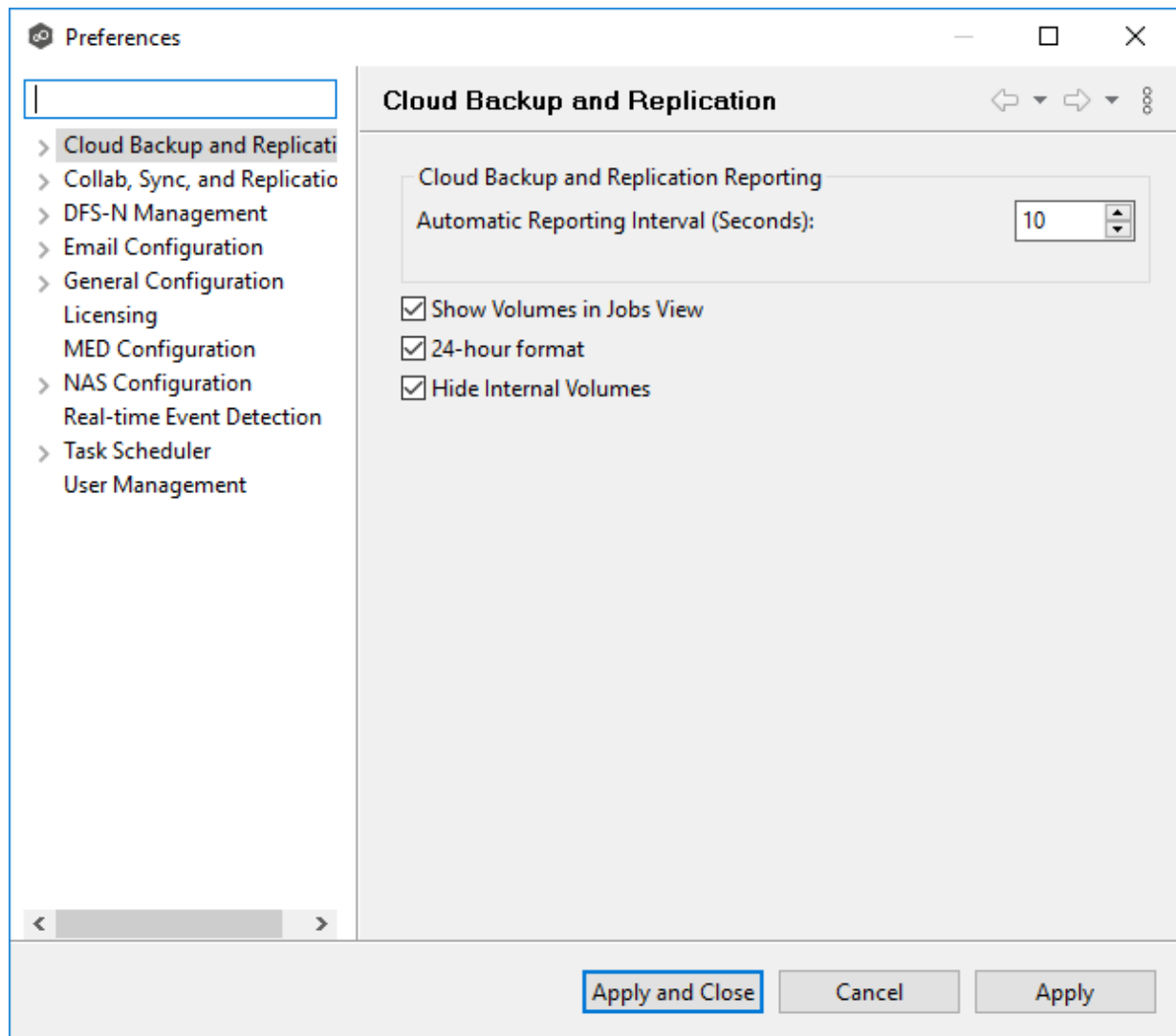
- [Database Connections](#)
- [Destination Credentials](#)
- [Email Alerts](#)
- [File and Folder Filters](#)
- [Performance](#)
- [Proxy Configuration](#)
- [File Retries and Source Snapshots](#)
- [Replication and Retention Policies](#)
- [SNMP Notifications](#)
- [Scan Manager](#)

## Cloud Backup and Replication

Cloud Backup and Replication settings control the overall performance of all Cloud Backup and Replication jobs.

To modify these settings:

1. Select **Preferences** from the **Window** menu.
2. Select **Cloud Backup and Replication** in the navigation tree.



3. Modify the settings as needed.

<b>Automatic Reporting Interval (Seconds)</b>	Each Peer Agent automatically reports its statistics to Peer Management Center at regular intervals. Select the number of seconds between these intervals. The default is 10 seconds.
<b>Show Volumes in Jobs View</b>	Select this checkbox if you want volumes to be displayed in the Jobs view.
<b>Use 24-hour format</b>	Select this checkbox if you want times to be displayed in a 24-hour format rather than a 12-hour format.





The **Create Database Connection** dialog appears.

**Create Database Connection**

Configure connection information for MS SQL Server.

\*Database Connection Name:

\*Management Agent:

\*DB Host Name:

Port:

Instance Name:

\*Database Name:

Authentication: ☒ Integrated ☐ Credentials

Username:

Password:

4. Enter the required values.

<b>Database Connection Name</b>	Enter a name for this database connection.
<b>Management Agent</b>	Select the Management Agent that will use this connection. The Agent must be the same one as managing the job.
<b>DB Host Name</b>	Enter the name of the SQL Server hosting the database. If the database is installed on the Agent server itself, enter the name of the Agent server.
<b>Port</b>	Optional. Enter the port to be used to communicate with the specified SQL Server. If not defined, the connection defaults to port 1433.

<b>Instance Name</b>	Optional. Enter the database instance name to use on the specified SQL Server. If no named instances are installed on the specified SQL Server, leave this blank.
<b>Database Name</b>	Enter the name of the database that Cloud Backup and Replication will create. The default name is "peercloud" but it can be changed to a name that follows your company's naming conventions.
<b>Authentication</b>	Select <b>Integrated</b> if the Agent service account is granted admin rights on the selected SQL instance. Otherwise, select <b>Credentials</b> to enter the user name and password of a database administrator.
<b>User Name</b>	Required when <b>Credentials</b> is selected for <b>Authentication</b> . Enter the user name of an account to be used to connect to the database. This can be a locally defined account such as "sa" or a domain account. The account must have adequate privileges to manage the database, such as database owner.
<b>Password</b>	Required when <b>Credentials</b> is selected for <b>Authentication</b> . Enter the password for account being used to connect to the database.

- Click **Validate** to test the connection, and then click **OK** in the confirmation message that appears.
- Click **OK** to close the dialog.

The new database connection is listed in the **Database Connections** table.

- Click **OK** or **Apply**.

### Destination Credentials

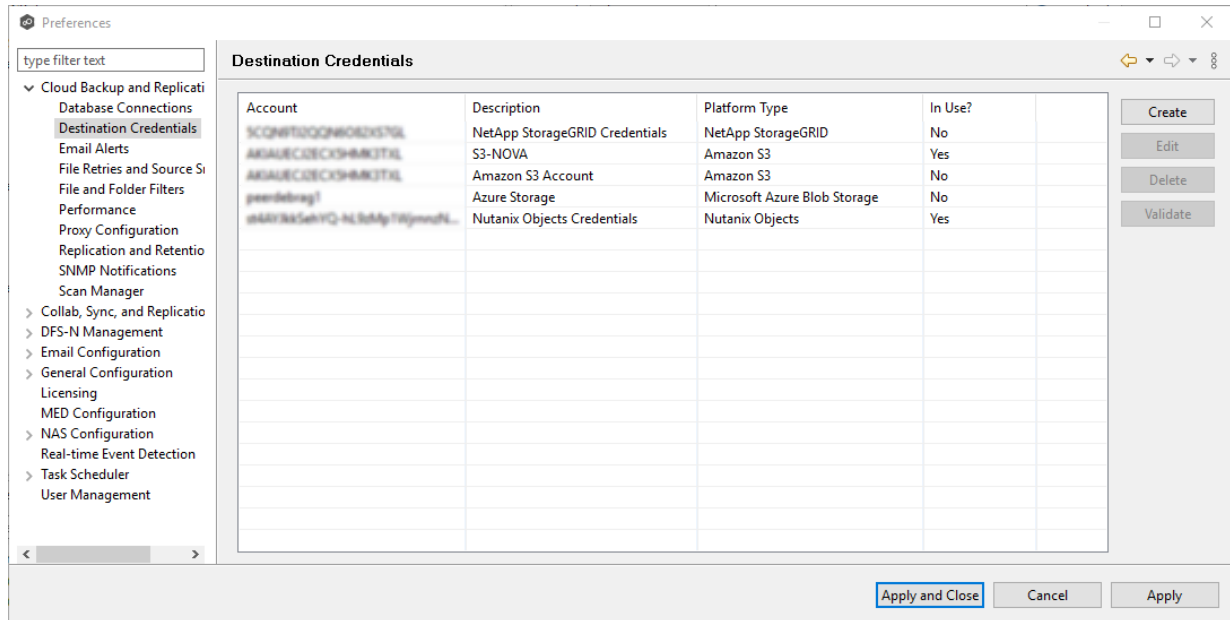
When you create a Cloud Backup and Replication job, you can select existing destination storage account credentials to apply to the job or you can create new credentials and apply them to the job. This [Preferences](#) page lists the existing credentials. From this page, you can view, create, edit, and delete credentials. However, you cannot edit or delete credentials while they are applied to a job.

To create new destination storage account credentials:

- Select **Preferences** from the **Window** menu.

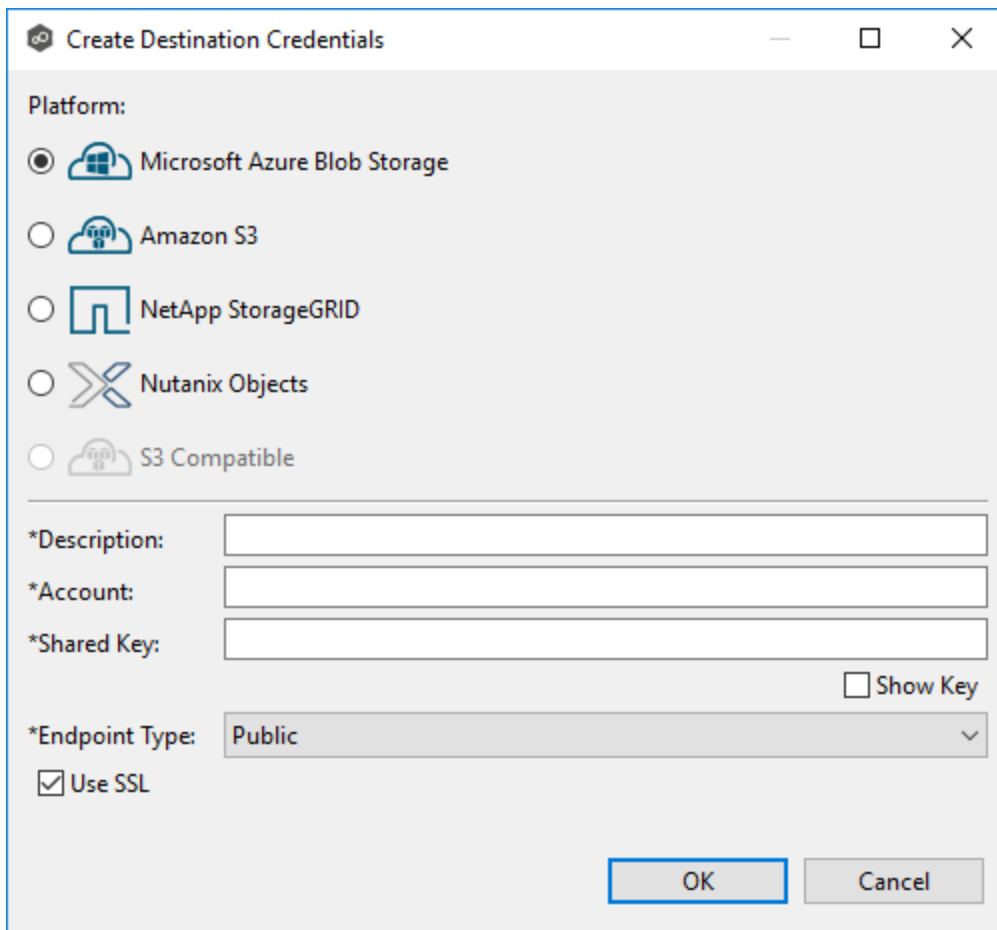
- Expand **Cloud Backup and Replication** in the navigation tree, and then select **Destination Credentials**.

The existing credentials are listed in the **Cloud Platform Credentials** table.



- Click the **Create** button.

The **Storage Account** dialog appears.



**Create Destination Credentials**

Platform:

- ☒ Microsoft Azure Blob Storage
- ☐ Amazon S3
- ☐ NetApp StorageGRID
- ☐ Nutanix Objects
- ☐ S3 Compatible

\*Description:

\*Account:

\*Shared Key:  ☐ Show Key

\*Endpoint Type:

☒ Use SSL

OK Cancel

4. Enter the required values. For information about the required values, see [Step 8: Destination Credentials](#) in the [Creating a Cloud Backup and Replication Job](#) section.
5. Click **OK** or **Apply**.

## Email Alerts

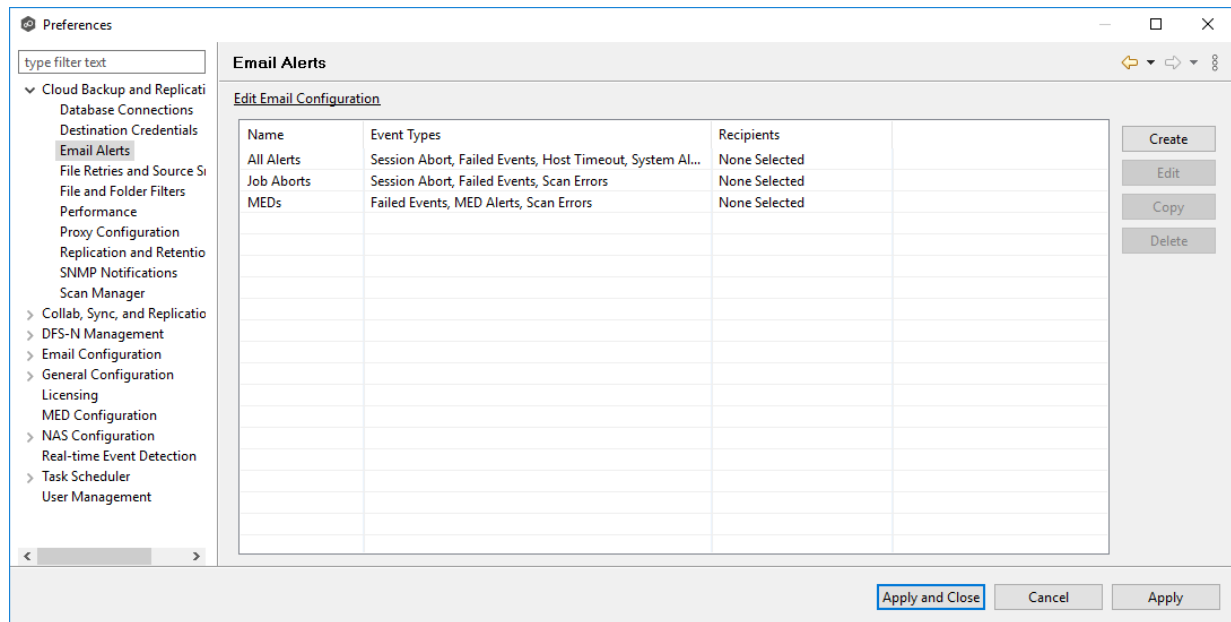
When you create a job, you can select existing email alerts to apply to the job or you can create new email alerts and apply them to the job. This [Preferences](#) page lists the existing email alerts. From this page, you can view, create, edit, and delete email alerts. However, you cannot edit or delete an email alert while it is applied to a job. See [Email Alerts](#) in the [Basic Concepts](#) section for more information about email alerts.

**Note:** An SMTP email connection must be configured before email alerts can be sent. See [Email Configuration](#) for information about configuring SMTP email settings.

To create an email alert:

1. Select **Preferences** from the **Window** menu.
2. Expand **Cloud Backup and Replication** in the navigation tree, and then select **Email Alerts**.

Any existing Cloud Backup and Replication email alerts are listed in the **Email Alerts** table.



3. Click the **Create** button.

The **Create Email Alert** dialog appears.

**Create Email Alert**

Name:

**Event Types**

☒ Session Abort ☒ Host Failure ☒ System Alerts ☒ MED Alerts

**Report Types**

☒ Scan ☐ Destination Snapshot

**Recipients**

Enter email, contact, or distribution list:

Recipients:

4. Enter a name for the alert.
5. Select the event types to be alerted.

The event type determines what will trigger the email alert to be sent.

Event Type	Description
Session Abort	Sends an alert when the Cloud Backup and Replication job stops unexpectedly.
Host Failure	Sends an alert when the Management Agent of a Cloud Backup and Replication job disconnects or stops responding.

Event Type	Description
System Alerts	Sends an alert when a system event such as low memory or low hub disk space occurs.
ME D Alerts	Sends an alert when a <a href="#">malicious event</a> is detected.

6. Select the report types to be sent.

Report Type	Description.
Scan	Sends scan statistics after a scan has completed.
Destination Snapshot	Sends the information about the snapshot after the snapshot is taken.

7. Enter alert recipients, and then click **Add to List**.

The recipients are listed in the **Recipients** field.

8. Click **OK** or **Apply**.

The new email alert is listed in the **Email Alerts** table and can now be applied to jobs.



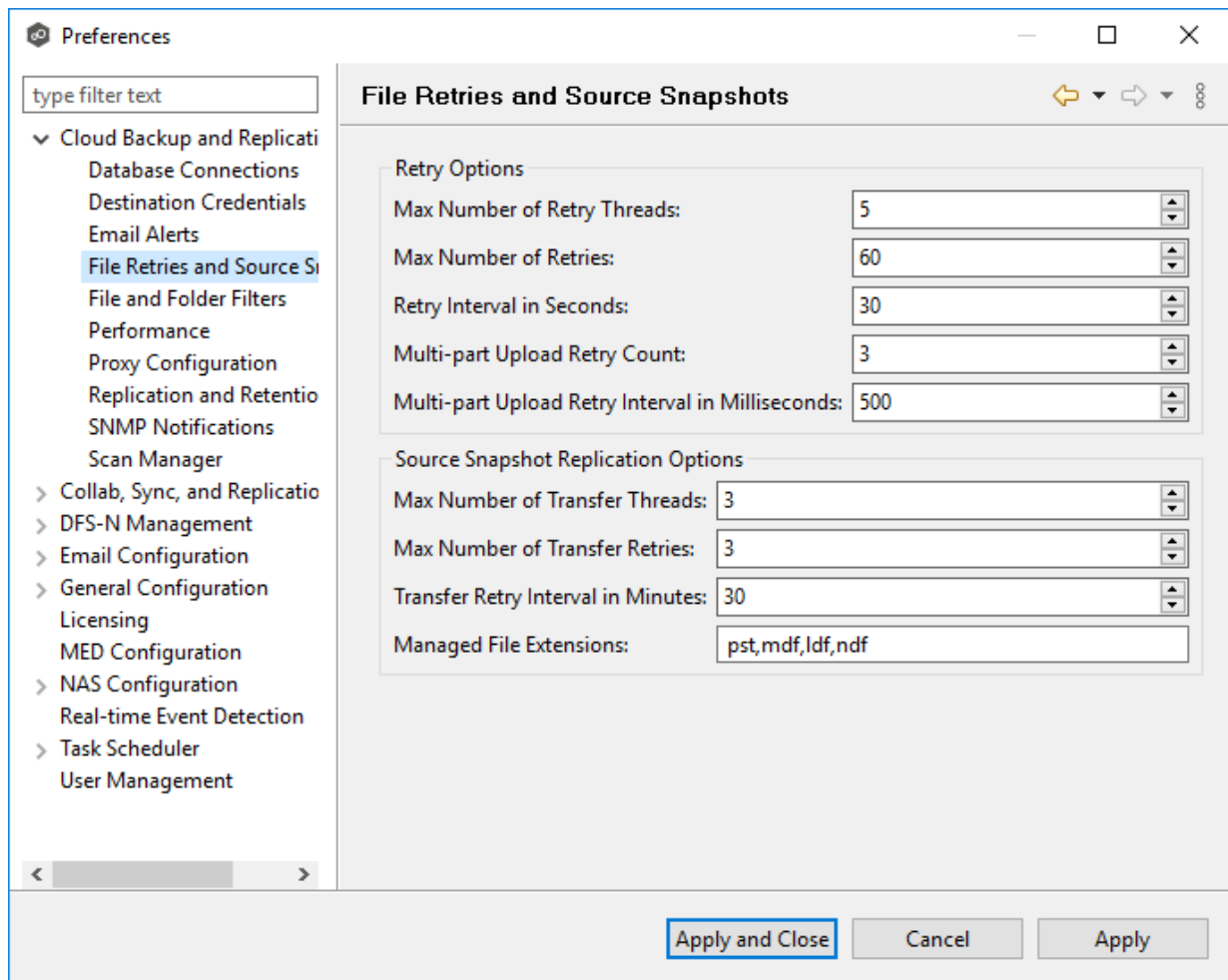
## File Retries and Source Snapshots

This page allows you to specify two sets of options:

- **File Retries** - Settings that are used when retry issues that arise while replicating a file or folder.
- **Source Snapshot Replication** - Settings that control how and when source snapshots are used.

To modify these options:

1. From the **Window** menu, select **Preferences**.
2. Expand **Cloud Backup and Replication** in the navigation tree, and then select **File Retries and Source Snapshots**.



3. Modify the **Retry Options** as needed:

<b>Max Number of Retry Threads</b>	Enter the maximum number of threads available for handling retries of failed file or folder transfers.
<b>Max Number of Retries</b>	Enter the maximum number of retries to perform on a file or folder that has failed to be replicated. If the number of retries is exceeded, the file or folder will be added to the Failed Events view and will need to be manually processed.
<b>Retry Interval in seconds</b>	Enter the number of seconds to wait in between retries of the failed replication of a file or folder.

4. Modify the **Source Snapshot Replication Options** as needed:

<b>Max Number of Transfer Threads</b>	Enter the maximum number of threads available for replicating files from a source snapshot.
<b>Max Number of Transfer Retries</b>	Enter the maximum number of retries to perform on a file or folder that has failed to be replicated from a source snapshot. If the number of retries is exceeded, the file or folder will be added to the Failed Events view and will need to be manually processed.
<b>Transfer Retry Interval in Minutes</b>	Enter the number of minutes to wait in between retries of the failed replication of a file or folder from a source snapshot.
<b>Managed File Extensions</b>	Enter the extensions for managed files that should be read from a source snapshot.

5. Click **OK** or **Apply**.

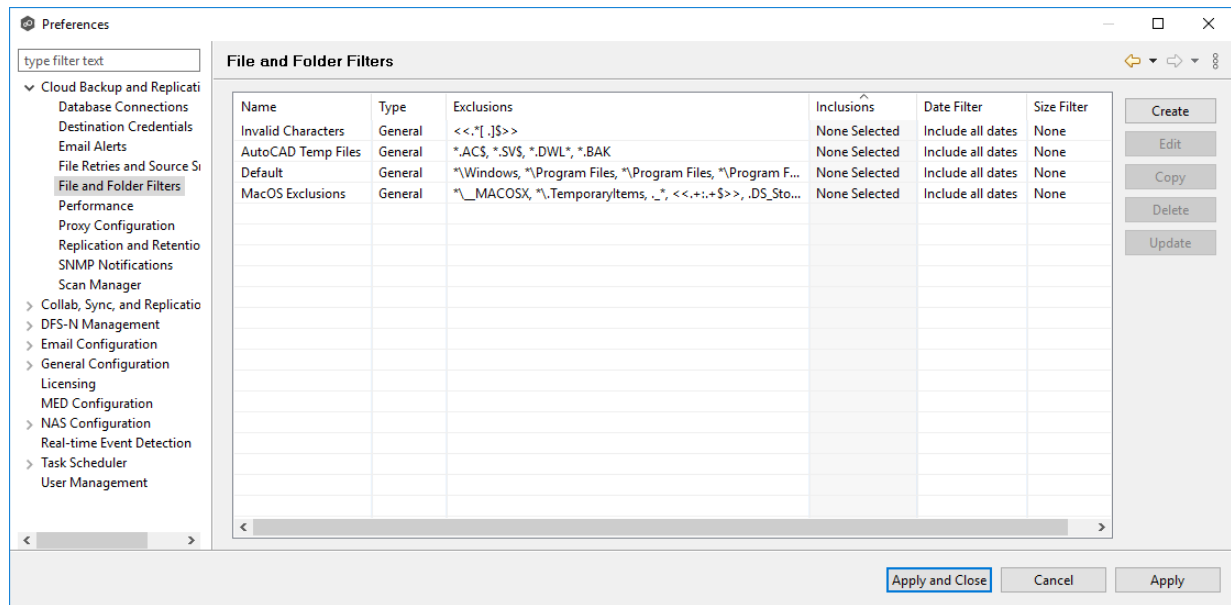
## File and Folder Filters

When you create a Cloud Backup and Replication job, you can select existing file filters to apply to the job or you can create new file filters and apply them to the job. This [Preferences](#) page lists the existing file filters. From this page, you can view, create, edit, and delete file filters. However, you cannot edit or delete a file filter while it is applied to a job. See [File and Folder Filters](#) in the [Basic Concepts](#) section for more information about file and folder filters.

To create a file filter:

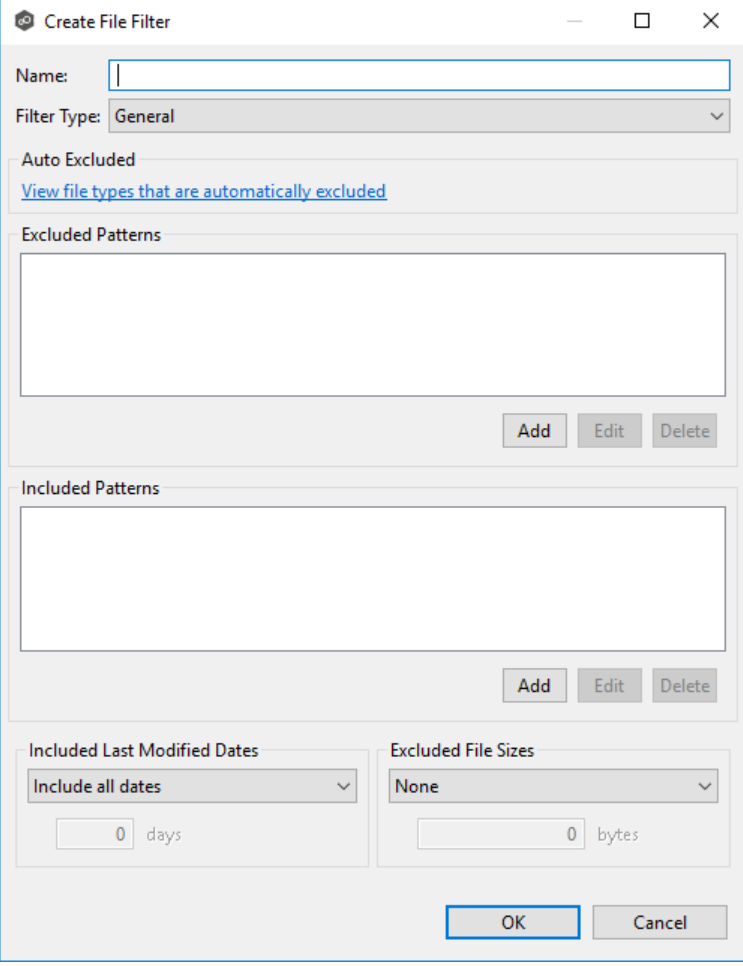
1. Select **Preferences** from the **Window** menu.
2. Expand **Cloud Backup and Replication** in the navigation tree, and then select **File and Folder Filters**.

Any existing Cloud Backup and Replication file filters are listed in the **File Filters** table.



3. Click the **Create** button.

The **Create File Filter** dialog appears.



The "Create File Filter" dialog box is shown. It has a title bar with a gear icon, the text "Create File Filter", and standard window controls. The "Name:" field is empty. The "Filter Type:" dropdown is set to "General". Below this is an "Auto Excluded" section with a link "View file types that are automatically excluded". There are two main sections: "Excluded Patterns" and "Included Patterns", each with a large text area and "Add", "Edit", and "Delete" buttons. At the bottom, there are two dropdowns: "Included Last Modified Dates" (set to "Include all dates") and "Excluded File Sizes" (set to "None"). Each dropdown has a numeric input field (set to "0") and a unit label ("days" or "bytes"). "OK" and "Cancel" buttons are at the bottom right.

4. Enter a unique name for the filter.
5. Select the [filter type](#).
6. (Optional) Click **Add** to enter a filter pattern for files that you want excluded from the job. Repeat to add more filter patterns.

See [Defining Filter Patterns](#) for information about filters patterns.

7. (Optional) Click **Add** to enter a filter pattern for files that you want included in the job. Repeat to add more filter patterns.
8. (Optional) Select a value for [Included Last Modified Dates](#).

Note: A filter cannot use **Included Last Modified Dates** in conjunction with any other excluded or included patterns.

9. (Optional) Select a value for [Excluded File Sizes](#).

Note: A filter cannot use **Excluded File Sizes** in conjunction with any other excluded or included patterns.

10. Click **OK** or **Apply**.

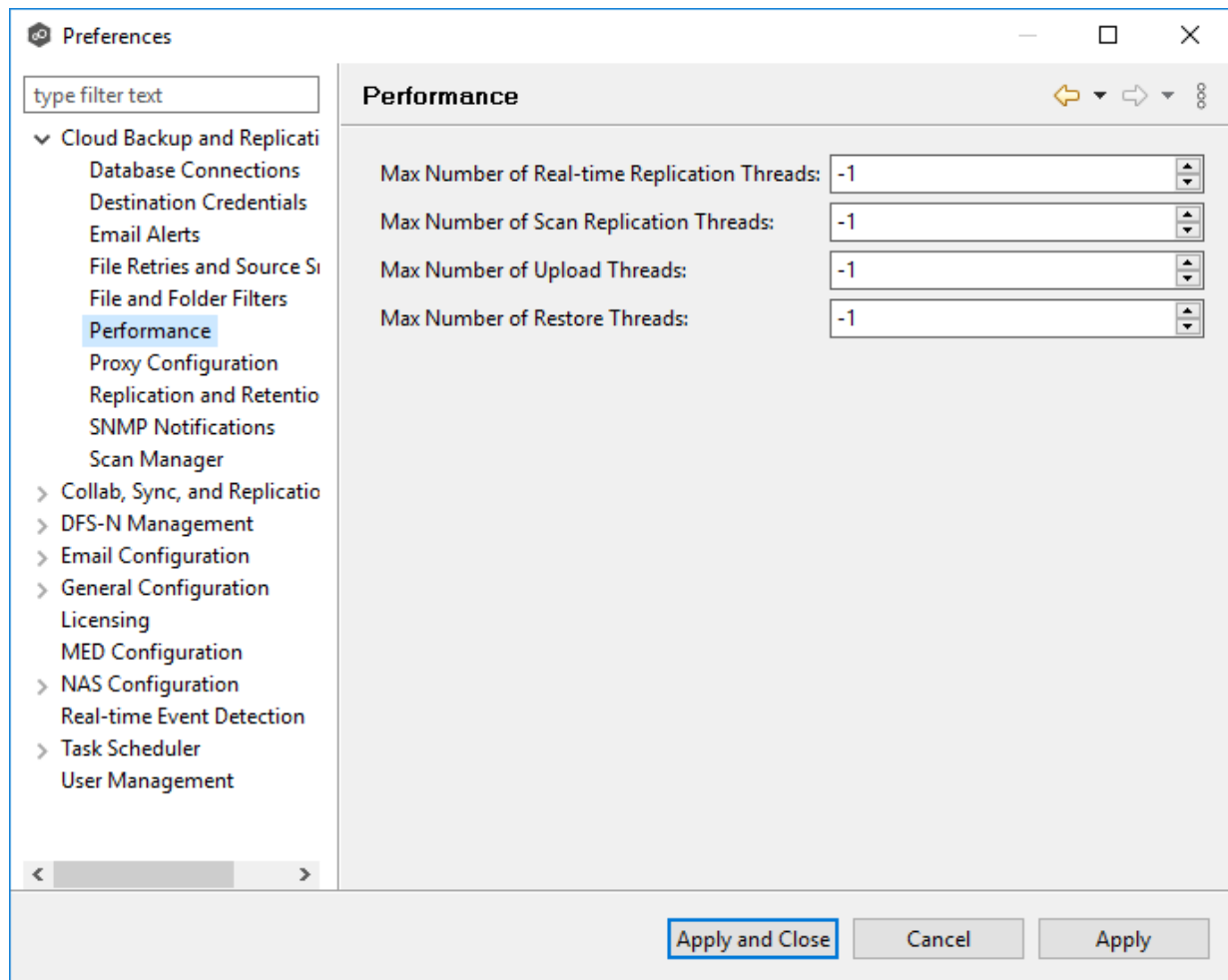
The new file filter is listed in the **File Filters** table and can now be applied to jobs.

## Performance

Performance settings allow you to adjust the performance of Cloud Backup and Replication jobs.

To modify the Cloud Backup and Replication performance settings:

1. Select **Preferences** from the **Window** menu.
2. Expand **Cloud Backup and Replication** in the navigation tree, and then select **Performance**.

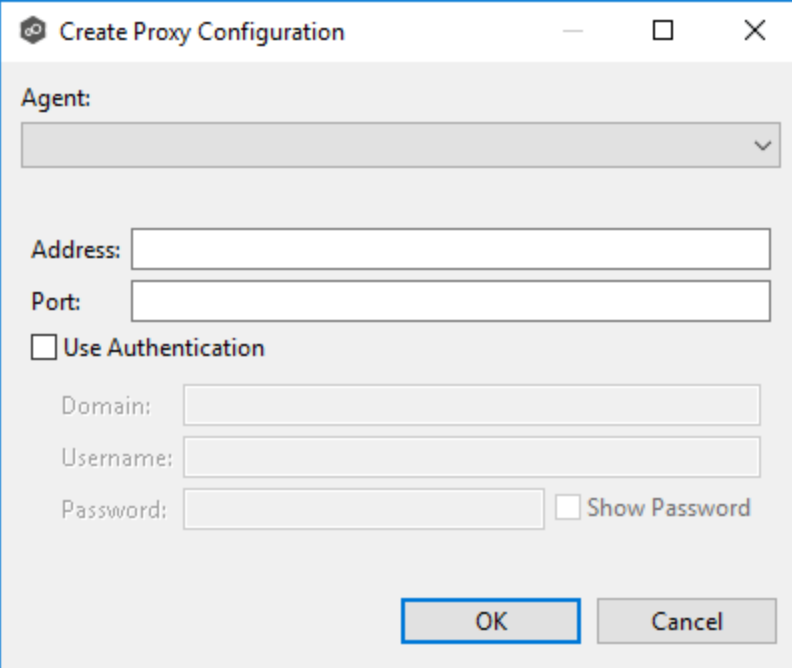


3. Modify the settings as needed:

<b>Max Number of Real-time Replication Threads</b>	Enter the maximum number of threads available for replicating files as they are updated in real-time on the source storage device.
<b>Max Number of Scan Replication Threads</b>	Enter the maximum number of threads available for replicating files during scheduled and on-demand scans of the source storage device.
<b>Max Number of Upload Threads</b>	Enter the maximum number of threads available for uploading files to the destination storage device.



The **Create Proxy Configuration** dialog appears.

The image shows a 'Create Proxy Configuration' dialog box. It has a title bar with a minimize button, a maximize button, and a close button. The dialog contains several fields: 'Agent:' with a dropdown menu, 'Address:' with a text box, 'Port:' with a text box, and a checkbox labeled 'Use Authentication'. Below the checkbox are three more text boxes: 'Domain:', 'Username:', and 'Password:'. To the right of the 'Password:' box is a checkbox labeled 'Show Password'. At the bottom right are two buttons: 'OK' and 'Cancel'.

5. Select the agent that manages your storage device.
6. Enter values for the following fields:

<b>Address</b>	Enter the IP address or fully qualified domain name of the proxy server.
<b>Port</b>	Enter the port number.
<b>User Authentication</b>	Select if your proxy server requires authentication. This option does not apply for proxy servers connecting to an Azure storage device

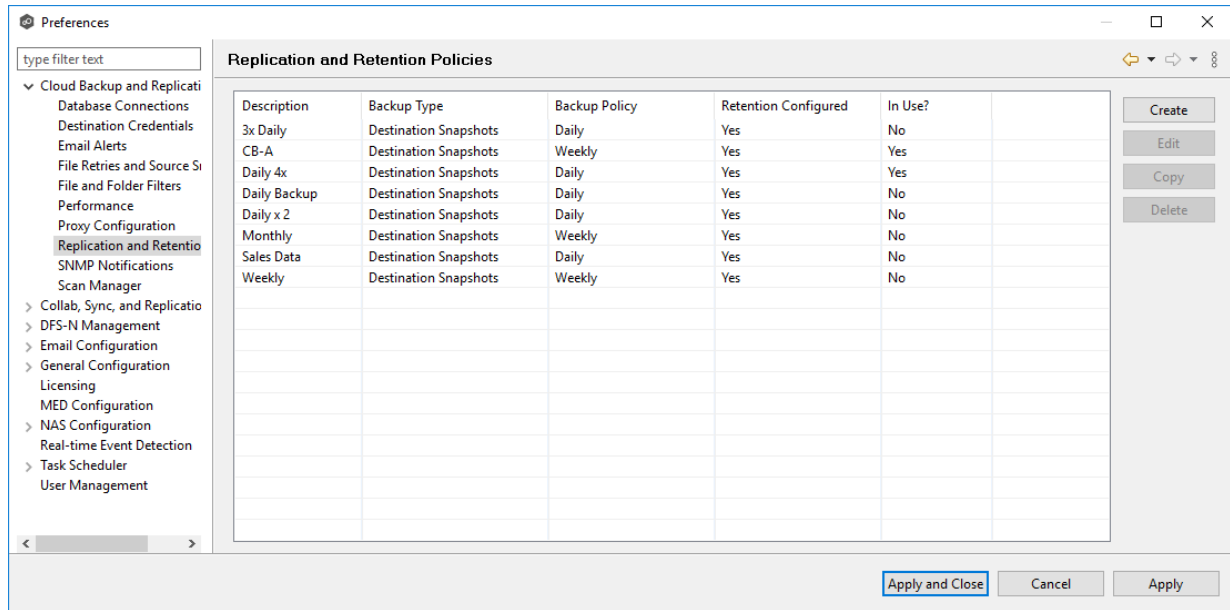
7. If your proxy server requires authentication, click the **User Authentication** checkbox and supply the necessary values:

<b>Domain</b>	Enter the domain name on the proxy server.
<b>Username</b>	Enter the user name for the proxy server.





- Expand **Cloud Backup and Replication** in the navigation tree, and then select **Replication and Retention Policies**.



- Click the **Create** button.

The **Replication and Retention Policy Wizard** opens.

Replication and Retention Policy Wizard

**Replication and Retention Policy**

You must enter a name for the policy.

Replication and Retention Policy  
Replication Schedule  
Retention  
Source Snapshots

\*Description:

☒ Enable Backup with Destination Snapshots

< Back   Next >   Cancel

4. Enter the required values, and then click **Finish**.

See [Step 10: Replication and Retention Policy](#) for assistance in completing the wizard.

## SNMP Notifications

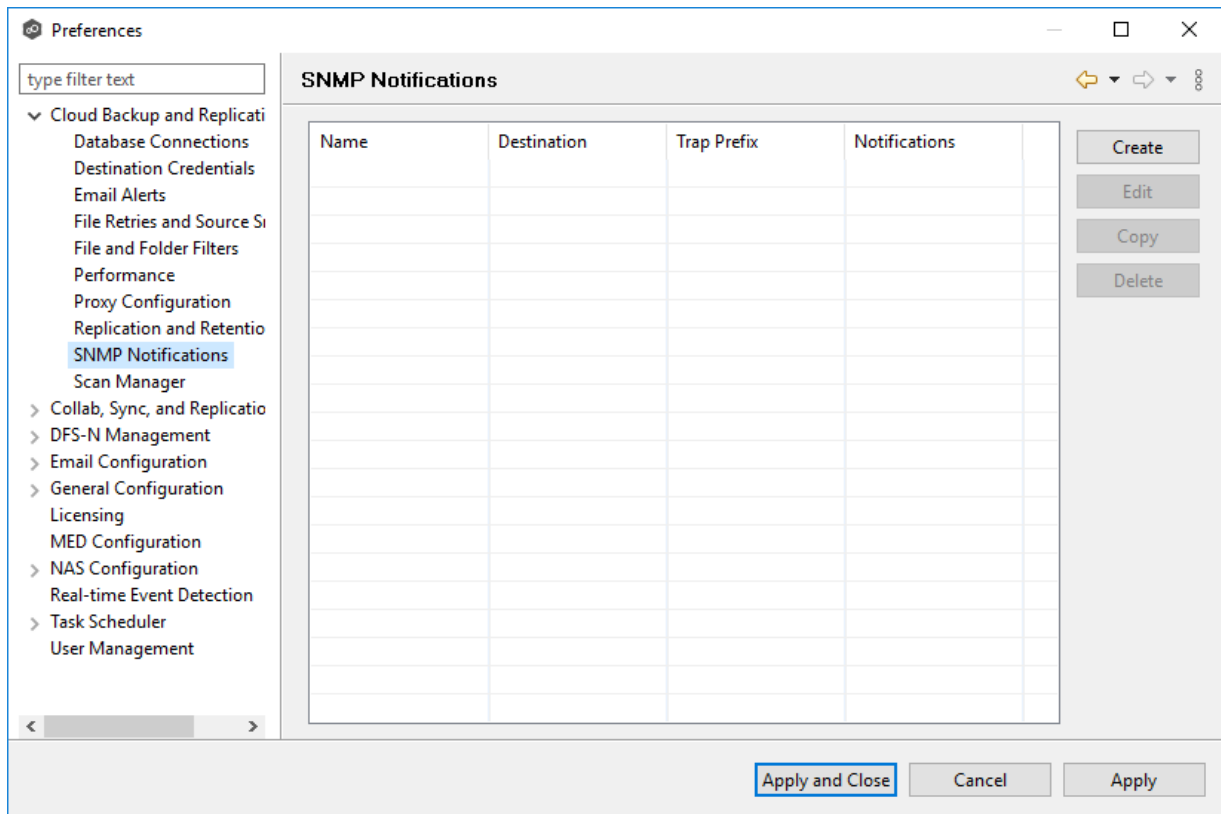
When you create a job, you can select an existing SNMP notification to apply to the job or you can create a new notification and apply it to the job. You cannot edit or delete an SNMP notification while it is applied to a job. See [SNMP Notifications](#) in the [Basic Concepts](#) section for more information about SNMP notifications.

To create an SNMP notification:

1. From the **Window** menu, select **Preferences**.

2. Expand **Cloud Backup and Replication** in the navigation tree, and then select **SNMP Notifications**.

The existing SNMP notifications are listed in the **SNMP Notifications** table.



3. Click the **Create** button.

The **Add SNMP Notification** dialog appears.

**Create SNMP Notification**

Name:

Source IP Address:

Destination:

Trap Prefix:

Notification Types

☒ Session Abort ☒ Host Failure ☒ System Alerts ☒ MED Alerts

4. In the **Source IP Address** field, select or manually enter the IP address over which the trap will be sent.
5. In the **Destination** field, enter the destination host name, IP address, or broadcast address.
6. For **Trap Prefix**, enter a prefix that will help to identify whether the message is coming from different instances of Peer Management Center or from different jobs.
7. For **Notification Types**, select the types of events that will trigger the generation of an SNMP trap:

<b>Session Abort</b>	Sends a notification when the Cloud Backup and Replication job stops unexpectedly.
<b>Host Failure</b>	Sends a notification when the Management Agent of a Cloud Backup and Replication job disconnects or stops responding.
<b>System Alerts</b>	Sends a notification when a system event such as low memory or low hub disk space occurs.
<b>MED Alert</b>	Sends a notification when a <a href="#">malicious event</a> is detected. For more information, see <a href="#">MED Configuration</a> .

<b>s</b>	
----------	--

8. Click **Test SNMP Settings**, and then click **OK** in the **Test Connection** dialog.
9. Click **OK** or **Apply**.

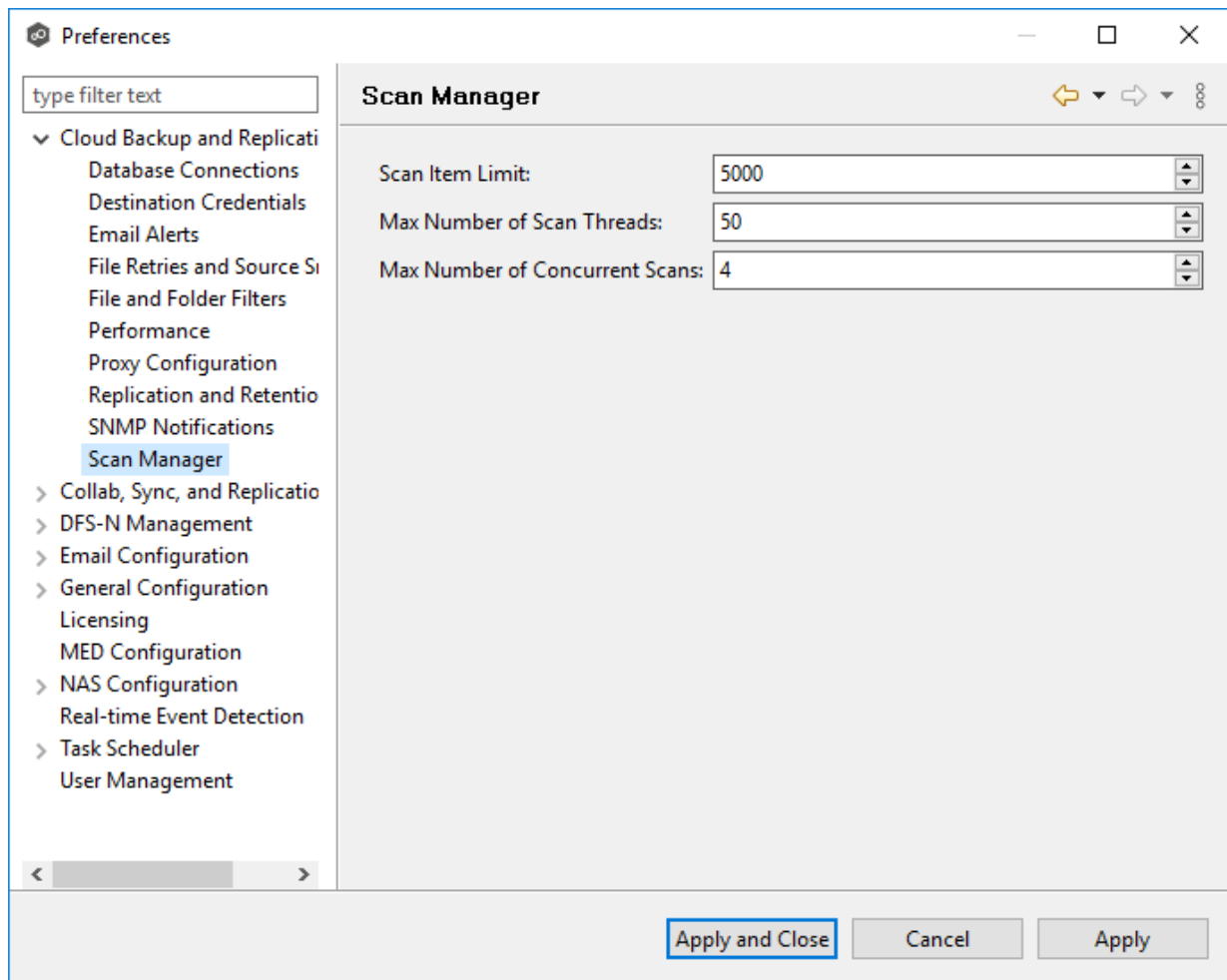
The new notification is listed in the **SNMP Notifications** table and can now be applied to jobs.

## Scan Manager

The Cloud Backup and Replication Scan Manager is responsible for handling all scheduled and on-demand scans of the source storage device.

To modify the Scan Manager settings for Cloud Backup and Replication jobs:

1. Select **Preferences** from the **Window** menu.
2. Expand **Cloud Backup and Replication** in the navigation tree, and then select **Scan Manager**.



3. Modify the settings as needed.

<b>Scan Item Limit</b>	Enter the maximum number of files and folders to obtain from a folder structure at a time during a scan.
<b>Max Number of Scan Threads</b>	Enter the maximum number of threads available for scanning files and folders. This number should be set to at least the maximum number of jobs running on any single Management Agent.
<b>Max Number of Concurrent Scans</b>	Enter the maximum number of scans that can run in parallel. If the number of active scan threads is greater than this number, scan threads will process on a rotating basis. Increasing this number can increase scan performance but will also increase system memory and CPU utilization.

4. Click **OK** or **Apply**.

## Collaboration, Replication, and Synchronization Job Preferences

You can modify the following settings for File Collaboration, File Synchronization, and File Replication jobs:

- [Collab Sync, and Replication](#)
- [DFS-N Management](#)
- [Email Alerts](#)
- [File and Folder Filters](#)
- [File Retries](#)
- [Locking](#)
- [Performance](#)
- [Real-time Event Detection](#)
- [Revit Enhancements](#)
- [SNMP Notifications](#)
- [Scan Manager](#)

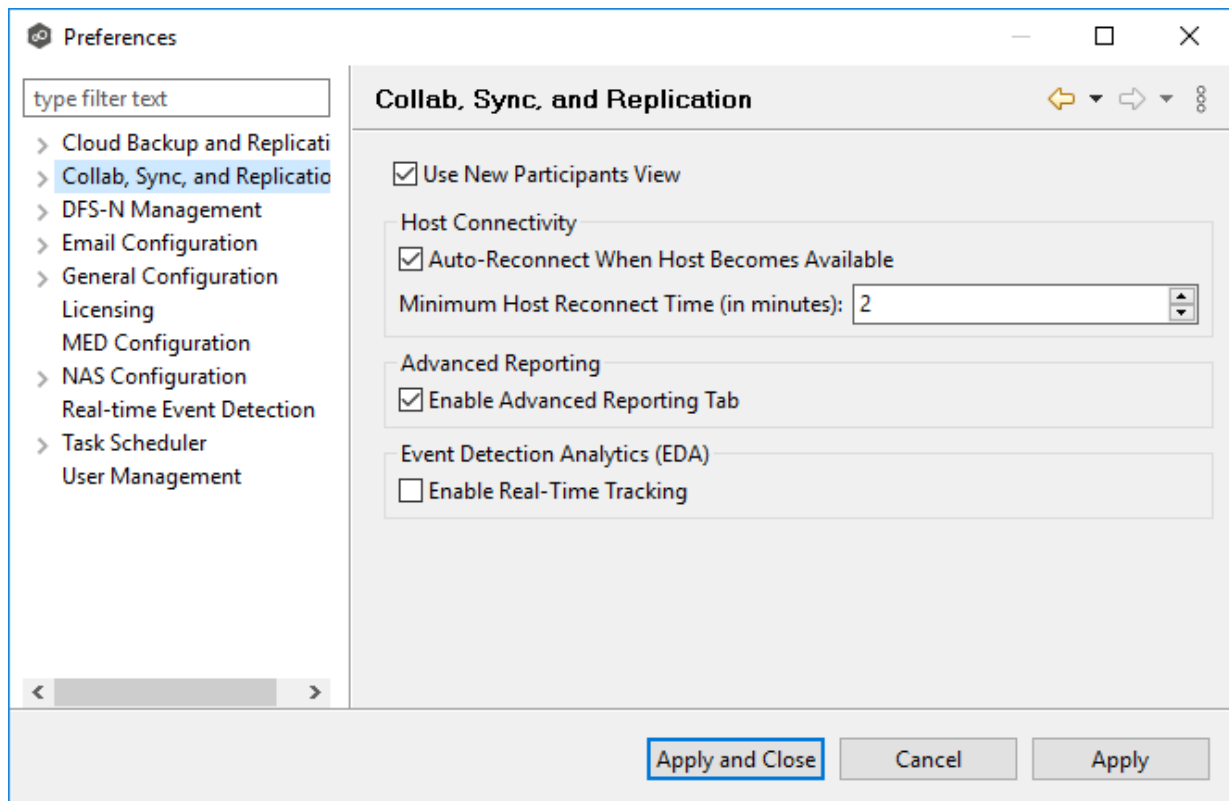
### Collab, Sync, and Replication

These settings control basic GUI and reconnect settings for all File Collaboration, File Synchronization, and File Replication jobs.

To modify these settings:

1. Select **Preferences** from the **Window** menu.
2. Select **Collab, Sync, and Replication** in the navigation tree.





3. Modify the settings as needed.

<b>Use New Participants View</b>	When creating a new job, use the new <b>Add New Participant</b> wizard instead of the legacy participant view. Highly recommended.
<b>Auto Reconnect when Host Becomes Available</b>	When an Agent reconnects to Peer Management Center after a failure, automatically re-enable it in any associated jobs. Highly recommended.
<b>Minimum Host Reconnect Time (in minutes)</b>	Enter the minimum number of minutes to wait after an Agent reconnects before re-enabling it in any associated jobs.
<b>Enable Advanced Reporting Tab</b>	Enables the <b>Reporting</b> sub-tab of the global <b>Collab, Sync, and Repl Summary</b> view.

4. (Optional) Click **Enable Real-Time Tracking** for **Event Detection Analytics** to track and report common activity processed by Peer Global File Service.

If enabled, every 24 hours, an Excel-based report will be written to disk that shows top folders, files, extensions, and users by total processed activity over the previous 24 hour window. These reports are stored under the installation folder of Peer Management Center and can be reviewed by Peer Software Support when uploading log files.

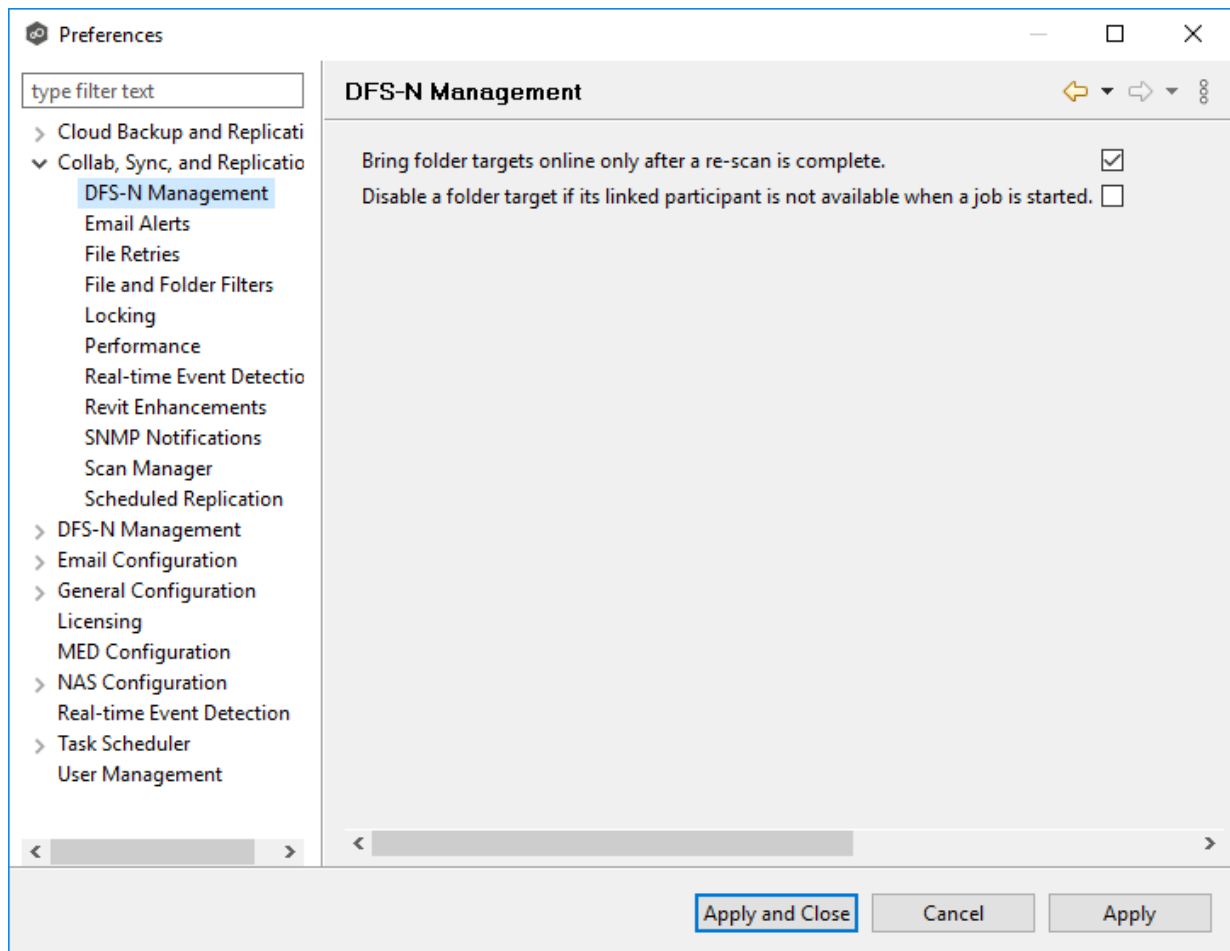
5. Click **Apply and Close** or **Apply**.

## DFS-N Management

These settings control the basic interoperability of all DFS-N Management jobs with File Collaboration and File Synchronization jobs.

To modify these settings:

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **DFS-N Management**.



3. Modify settings as needed.

<b>Bring folder targets online only after a re-scan is complete</b>	Re-enable a disabled folder target in a managed DFS namespace only when it has been rescanned and is back in sync after an outage. Highly recommended.
<b>Disable a folder target if its linked participant is not available when a job is started</b>	If a File Collaboration or File Synchronization job is started and a participant is not available, automatically disable its associated folder target in a managed DFS namespace.

4. Click **Apply and Close** or **Apply**.

## Email Alerts

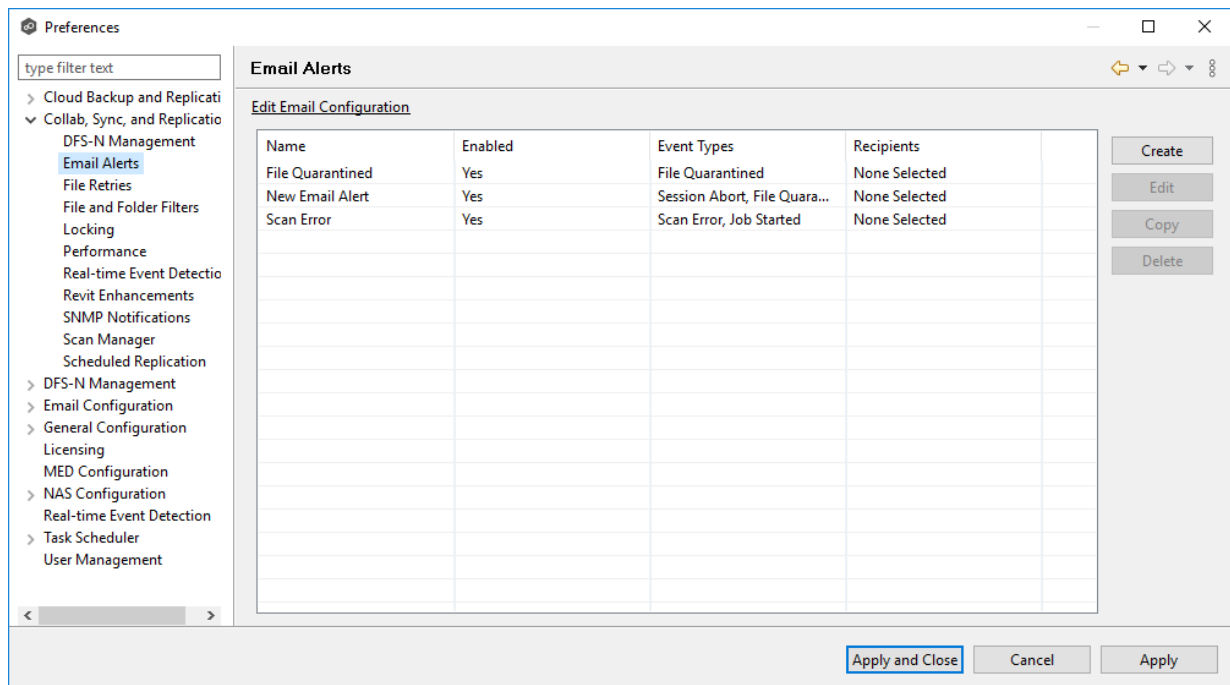
When you create a job, you can select existing email alerts to apply to the job or you can create new email alerts and apply them to the job. This [Preferences](#) page lists the existing email alerts. From this page, you can view, create, edit, and delete email alerts. However, you cannot edit or delete an email alert while it is applied to a job. See [Email Alerts](#) in the [Basic Concepts](#) section for more information about email alerts.

**Note:** An SMTP email connection must be configured before email alerts can be sent. See [Email Configuration](#) for information about configuring SMTP email settings.

To create an email alert:

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Email Alerts**.

Any existing email alerts are listed in the **Email Alerts** table.



3. Click **Create**.

The **Create Email Alert** dialog appears.

4. Enter a name for the alert.
5. Select the **Enable** checkbox if you want to enable the alert.

If you choose not to enable the alert, you can enable it later by editing the alert.

6. Select the event types to be alerted.

The event type determines what will trigger the email alert to be sent.

Event Type	Description
<b>Session Abort</b>	Sends an alert when a session is aborted because of lack of quorum due to one or more failed hosts.
<b>File Quarantined</b>	Sends an alert when a file is marked as quarantined because a file conflict was not able to be resolved.
<b>Host Failure</b>	Sends an alert when a host timeout occurs, and the host is taken out of session.

Event Type	Description
<b>Scan Error</b>	Sends an alert when an error occurs during the <a href="#">initial synchronization process</a> .
<b>MED Alerts</b>	Sends an alert when Peer MED detects potentially malicious activity. For more information, see <a href="#">MED Configuration</a> .
<b>Host Reconnect</b>	Sends an alert when the host is reconnected to the job and the job has resumed with the reconnected host.
<b>Health Check</b>	Sends an alert when Health Check finds an error. Checks to make sure that real-time information is being communicated.

7. If you want queue alerts sent, select **Enable Queue Alerts** and enter threshold values.

Option	Description
<b>Enable Queue Alerts</b>	Sends an email alert when the value in the <b>Queued Items</b> column for that job in the <b>Collab, Sync, and Repl Summary</b> view exceeds the <b>High Threshold</b> value. This column is the combination of the <b>Real-time</b> and <b>File Sync</b> queues as they are displayed in the user interface for the job. This counter is checked every 20 seconds and if it exceeds the <b>High Threshold</b> , an email alert is sent. Another alert will not be sent until the counter has dropped below the <b>Low Threshold</b> value and then exceeds the <b>High Threshold</b> value again.
<b>High Threshold</b>	The maximum value for the <b>Queued Items</b> value. When this value is exceeded, an alert is sent.
<b>Low Threshold</b>	Once an email has been sent, no additional emails will be sent until the <b>Low Threshold</b> value is met and then the <b>High Threshold</b> value is met again.

Option	Description
<b>Alert on Recovery</b>	Controls whether an email will be sent indicating that the counter has recovered to the <b>Low Threshold</b> value after an alert had been previously sent.

8. Select the **Scan** checkbox in the **Reports** section if you want scan statistics emailed to you after a scan has completed.
9. Select the **Quarantined Files** checkbox in the **Batch Email Alerts** section if you want email alerts about quarantined files sent to you in batches.
10. Enter alert recipients, and then click **Add to List**.

The recipients are listed in the **Recipients** field.

11. Click **Apply and Close** or **Apply**.

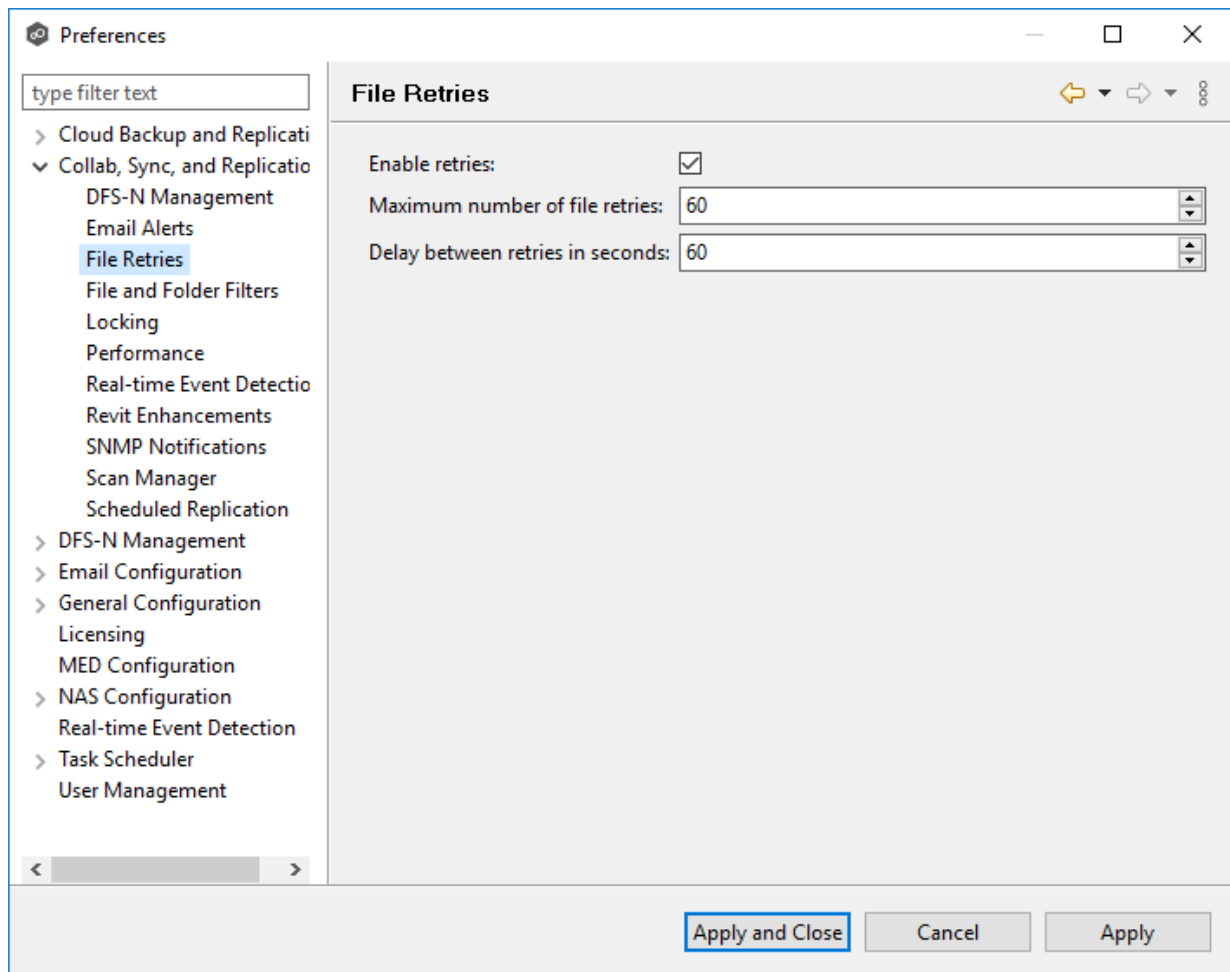
The new alert is listed in the **Email Alerts** table and can now be applied to jobs.

## File Retries

File retries settings enable you to configure the frequency of attempts and the maximum number of attempts. These settings apply to all File Collaboration, File Replication, and File Synchronization jobs. For more information about file retries, see [Conflicts, Retries, and Quarantines](#).

To modify the file retries settings:

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **File Retries**.



3. Modify the settings as needed.

<b>Enable retries</b>	Select this checkbox to enable the retry of failed file transfers. If this option is not enabled, files that would have been candidates for retries will be automatically quarantined.
<b>Maximum number of file retries</b>	Enter the maximum number of attempts to retry a failed file transfer before it is quarantined.
<b>Delay between retries in seconds</b>	Enter the number of seconds to wait between retries of a failed file transfer.

4. Click **Apply and Close** or **Apply**.



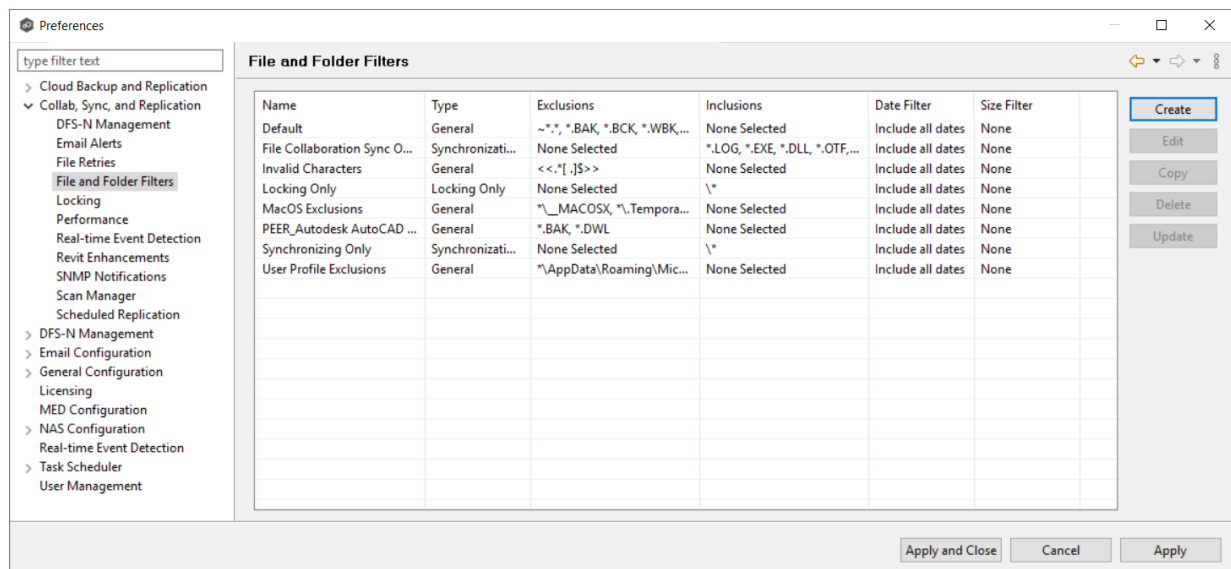
## File and Folder Filters

When you create a File Collaboration, File Synchronization, or File Replication job, you can select existing file and folder filters to apply to the job or you can create new file filters and apply them to the job. This [Preferences](#) page lists the existing file and folder filters. From this page, you can view, create, edit, and delete file filters. However, you cannot edit or delete a file filter while it is applied to a job. See [File and Folder Filters](#) in the [Basic Concepts](#) section for more information about file and folder filters.

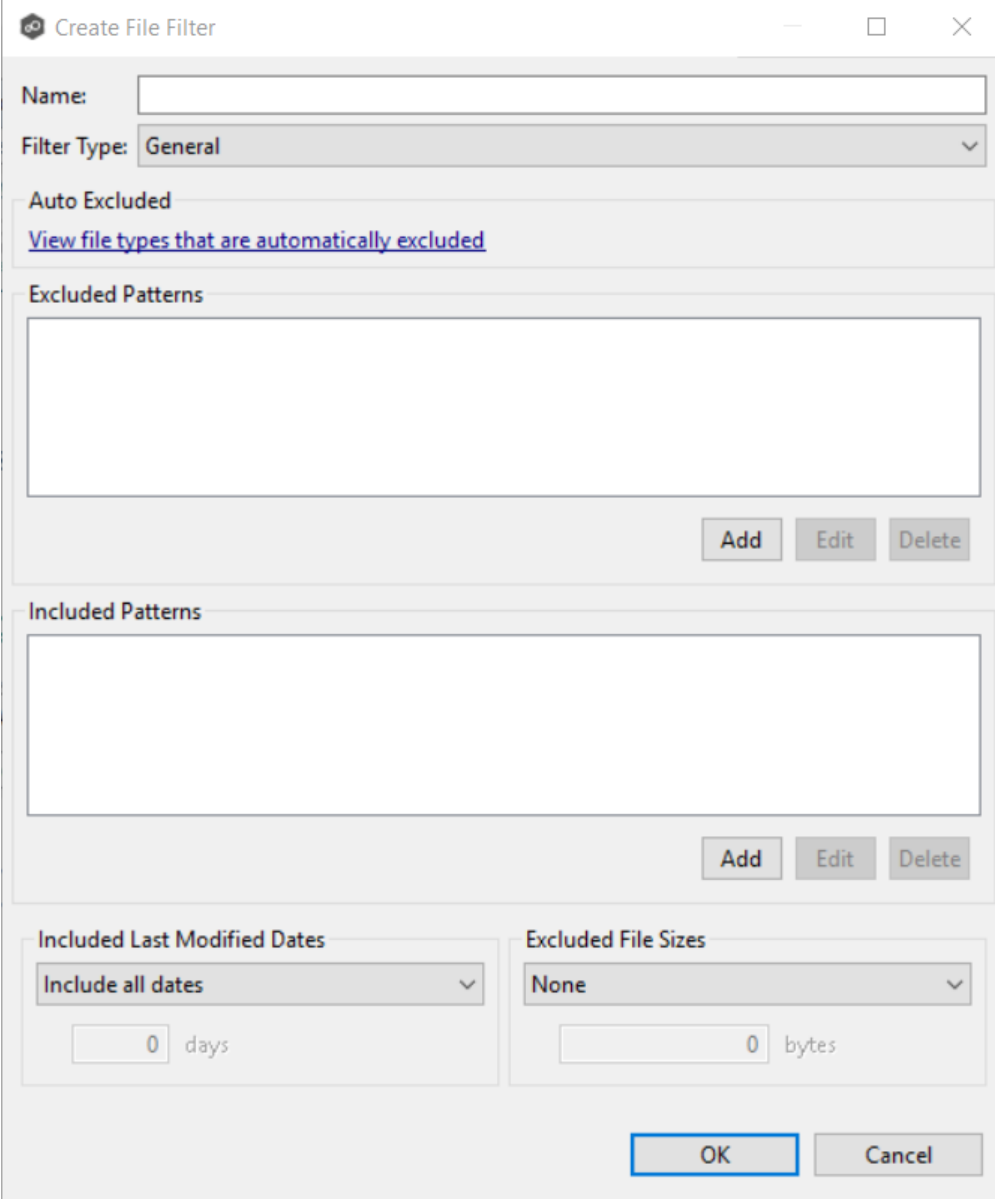
To create a file and folder filter:\Do

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **File and Folder Filters**.

Any existing file filters are listed in the **File and Folder Filters** table.



3. Click **Create**.



The "Create File Filter" dialog box is shown. It has a title bar with a logo, the text "Create File Filter", and standard window controls. The main area contains several sections: a "Name:" text input field; a "Filter Type:" dropdown menu currently set to "General"; an "Auto Excluded" section with a link "View file types that are automatically excluded"; an "Excluded Patterns" section with a large text area and "Add", "Edit", and "Delete" buttons; an "Included Patterns" section with a large text area and "Add", "Edit", and "Delete" buttons; an "Included Last Modified Dates" section with a dropdown set to "Include all dates" and a "0 days" input; and an "Excluded File Sizes" section with a dropdown set to "None" and a "0 bytes" input. At the bottom are "OK" and "Cancel" buttons.

Create File Filter

Name:

Filter Type: General

Auto Excluded

[View file types that are automatically excluded](#)

Excluded Patterns

Add Edit Delete

Included Patterns

Add Edit Delete

Included Last Modified Dates

Include all dates

0 days

Excluded File Sizes

None

0 bytes

OK Cancel

4. Enter a unique name for the filter.
5. Select the [filter type](#).
6. (Optional) Click **Add** to enter a filter pattern for files that you want excluded from the job. Repeat to add more filter patterns.

See [Defining Filter Patterns](#) for information about filter patterns.

7. (Optional) Click **Add** to enter a filter pattern for files that you want included in the job. Repeat to add more filter patterns.

8. (Optional) Select a value for [Included Last Modified Dates](#).

Note: A filter cannot use **Included Last Modified Dates** in conjunction with any other excluded or included patterns.

9. (Optional) Select a value for [Excluded File Sizes](#). Note: This cannot be combined with any other filter criteria

Note: A filter cannot use **Excluded File Sizes** in conjunction with any other excluded or included patterns.

10. Click **Apply and Close** or **Apply**.

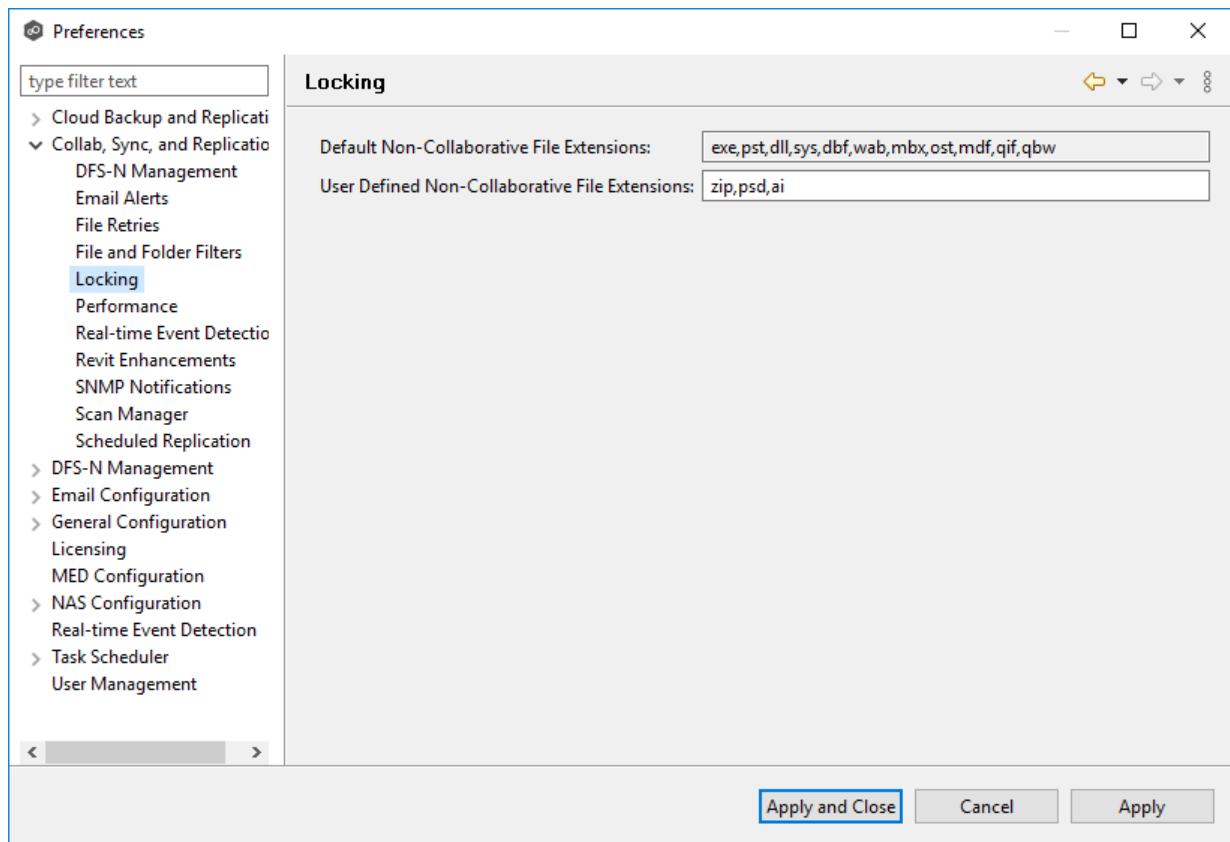
The new file filter is listed in the **File and Folders Filters** table and can now be applied to jobs.

## Locking

An option is available to mark certain file types as non-collaborative, changing the way locks on the specified file types are handled. These settings apply to all File Collaboration, File Synchronization, and File Replication jobs. These settings are critical for certain file types so that the job can correctly read these files, ensuring that managed file types are synchronized in a consistent and usable state.

To modify the locking settings:

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Locking**.



3. Modify the settings as needed.

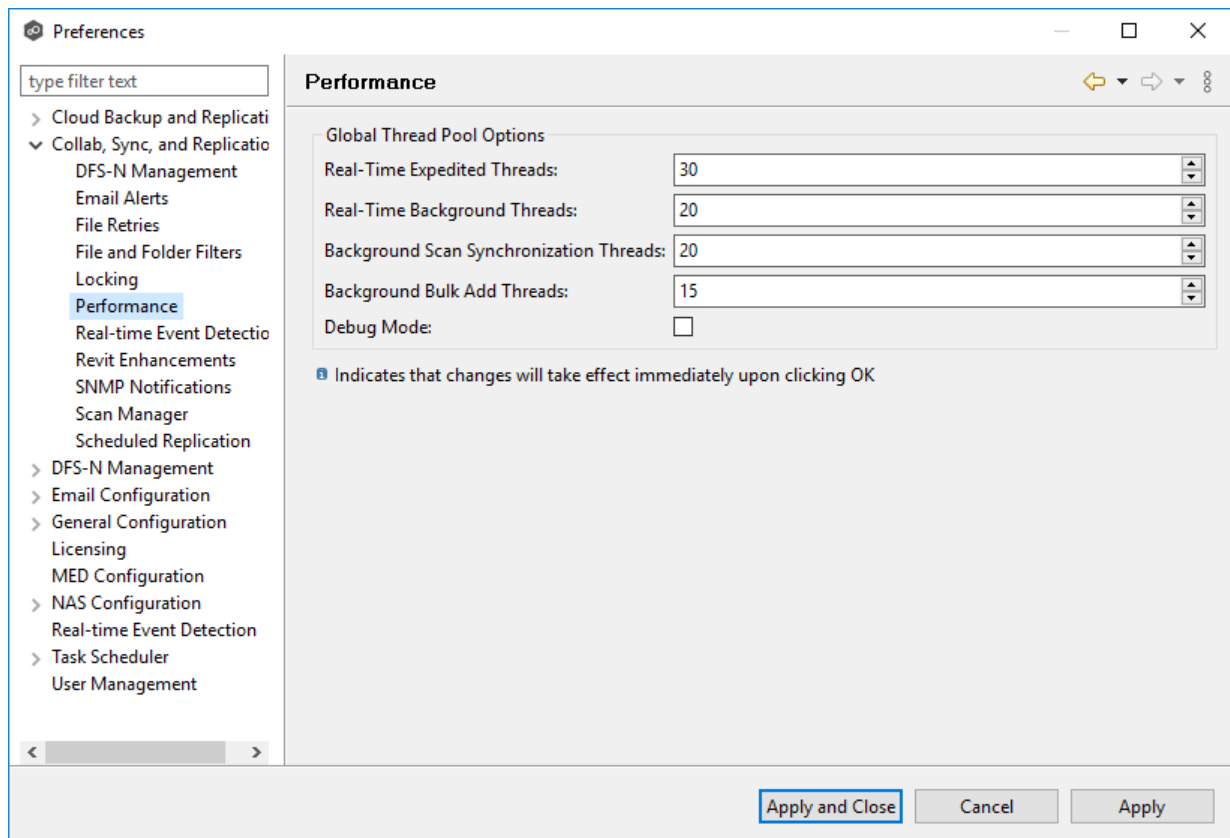
<b>Default Non-Collaborative File Extensions</b>	Non-editable. Displays the default, comma-separated list of file extensions of non-collaborative file types (e.g. database files). Write access to source files of these types is denied while the files are being synchronized.
<b>User Defined Non-Collaborative File Extensions</b>	Displays an editable, comma-separated list of file extensions of non-collaborative file types (e.g. database files). Write access to the source files of these types is denied while the files are being synchronized.

4. Click **Apply and Close** or **Apply**.

## Performance

To customize the performance settings of File Collaboration, File Synchronization, and File Replication jobs:

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Performance**.



3. Modify the settings as needed.

<b>Real-Time Expedited Threads</b>	Enter the maximum number of threads for controlling file locking and renames.
<b>Real-Time Background Threads</b>	Enter the maximum number of threads for controlling the replication of file content.

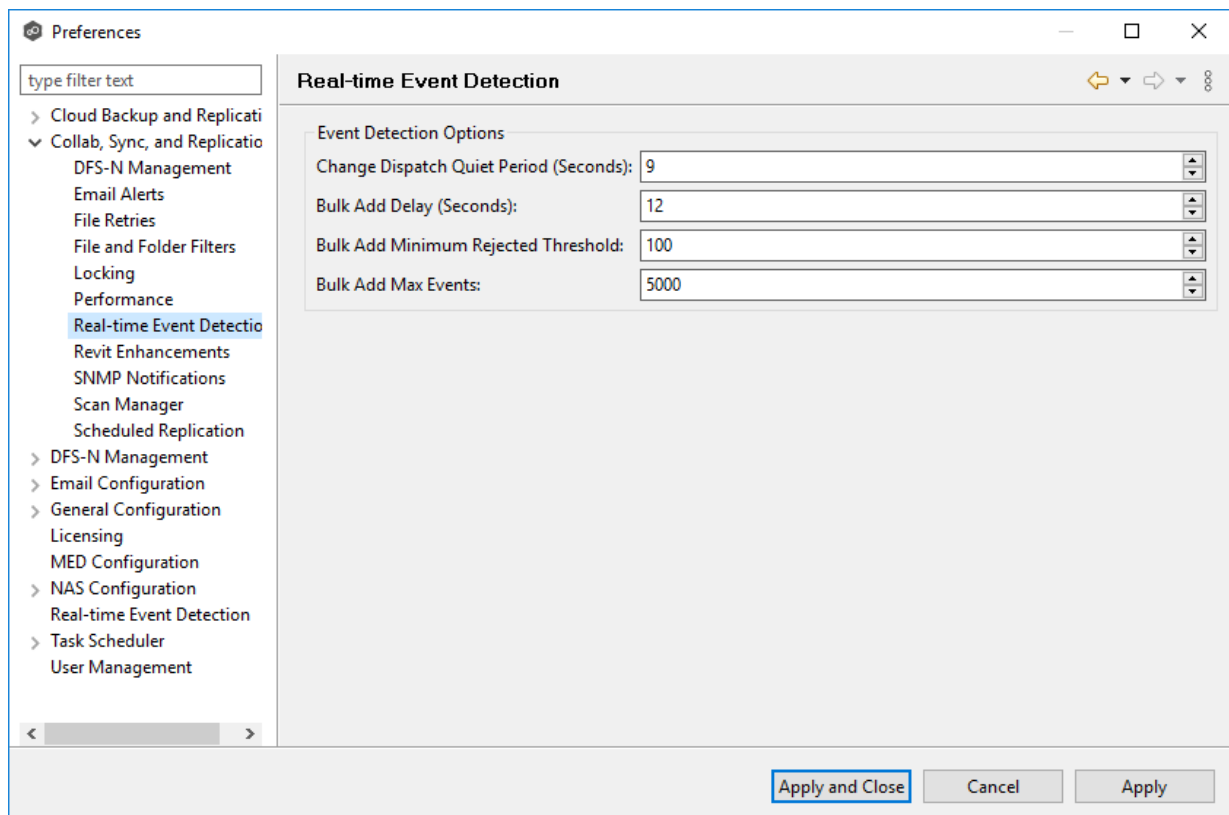
<b>Background Scan Synchronization Threads</b>	Enter the maximum number of threads for processing the differences found by background scans.
<b>Debug Mode</b>	Select to enable debug mode for the various types of threads.

- Click **Apply and Close** or **Apply**.

## Real-time Event Detection

To modify the File Collaboration real-time detection settings:

- Select **Preferences** from the **Window** menu.
- Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Real-time Event Detection**.



3. Modify the settings as needed.

<b>Change Dispatch Queue Period (Seconds)</b>	The number of seconds to wait before acting on a file modification, rename, or delete.
<b>Bulk Add Delay (Seconds)</b>	Controls when the bulk add logic is triggered. This is used to help de-prioritize mass copying or adding of files to a directory.
<b>Bulk Add Minimum Rejected Threshold</b>	The minimum number of file adds that must occur within the Bulk Add Delay for bulk add logic to be triggered.
<b>Bulk Add Max Events</b>	The maximum number of file adds to lump together in one batch.

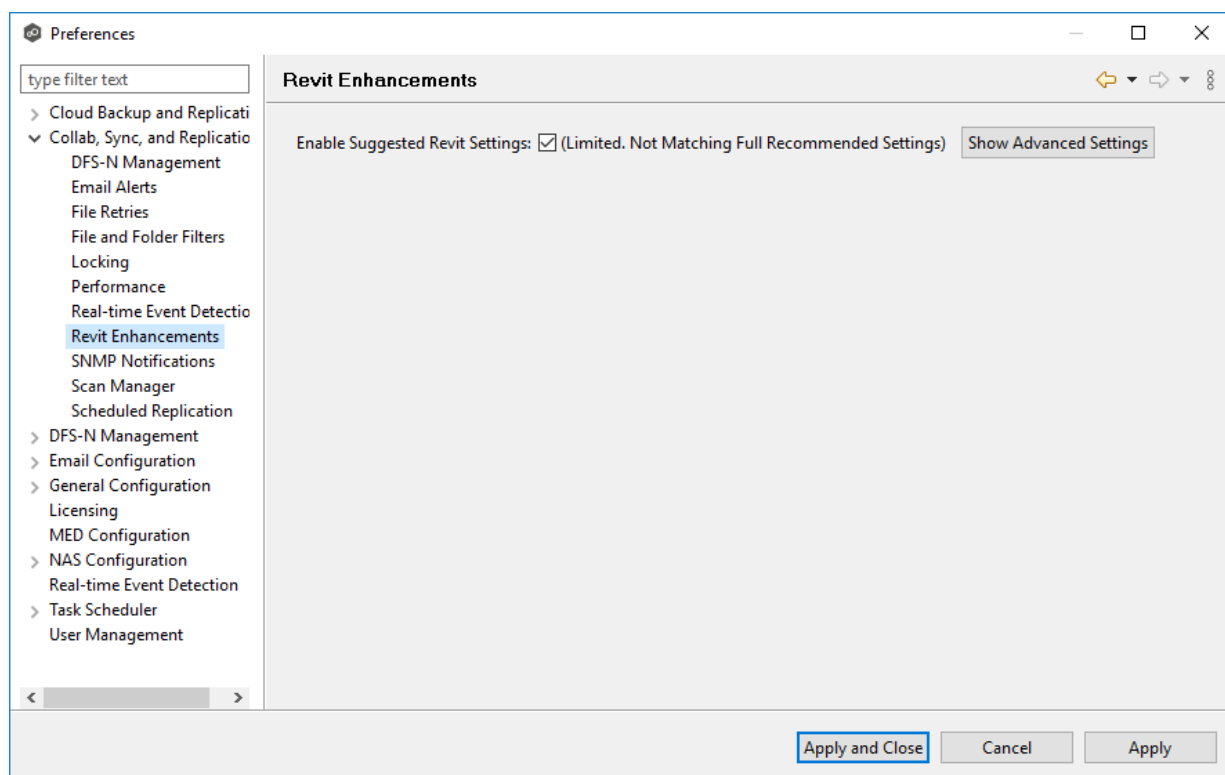
4. Click **Apply and Close** or **Apply**.

## Revit Enhancements

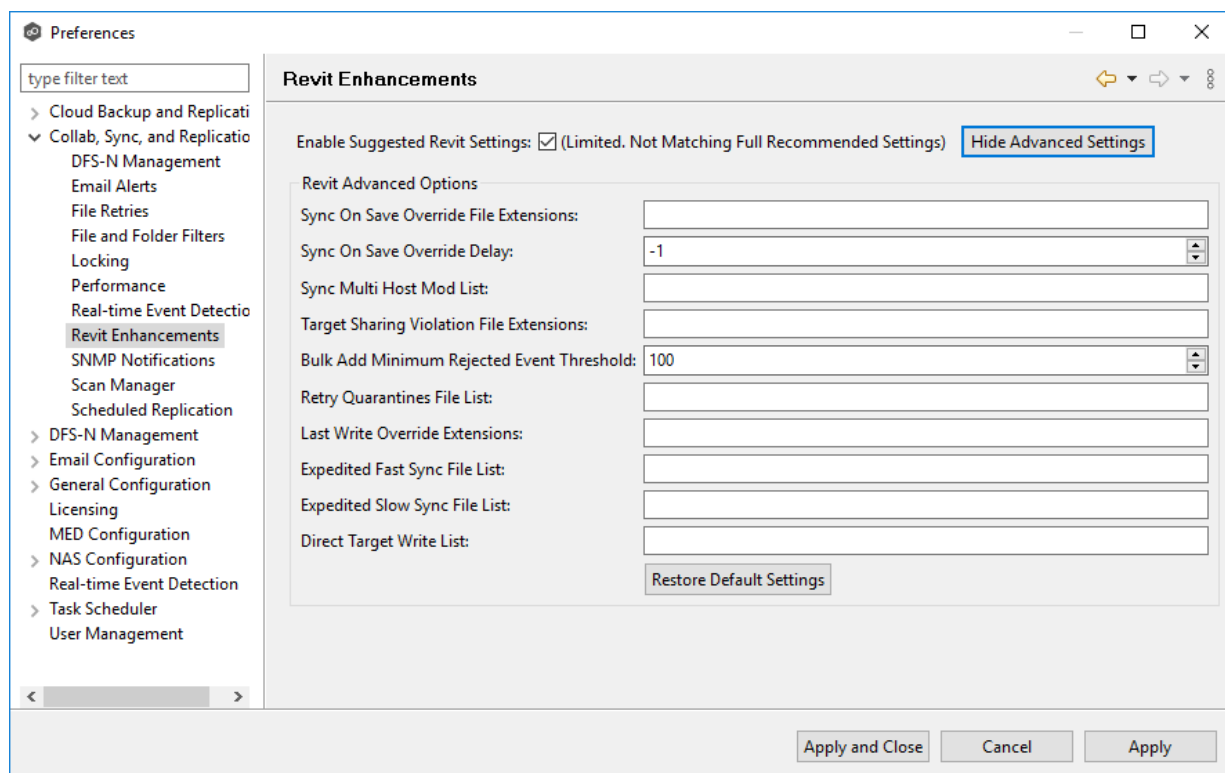
Revit Enhancements enable the Expedited Sync Queue for files specified in the Expedited Sync Queue File List.

To set advanced settings for Revit Enhancements:

1. Select **Preferences** from the Window menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Revit Enhancements**.



3. Click **Show Advanced Settings**.





## 4. Modify the settings as needed.

<b>Sync On Save Override File Extensions</b>	Extensions configured here will overwrite the <b>Sync. On Save</b> values configured in the interface for the job. In addition, these extensions use the delay value in <b>Sync On Save Override Delay</b> setting instead of the delay value configured in the interface. If no delay value is set, it will default to using a one second delay. Extensions configured in this list will still be processed via <b>Sync. On Save</b> even if they also exist in the user defined non-collaborative extension list (under the Window > Preferences menu option). Extensions in the normal <b>Sync. On Save</b> list that also exist in this list will not be processed.
<b>Sync On Save Override Delay</b>	The <b>Sync. On Save</b> delay value in seconds that applies only to the internal list of extensions listed in the <b>Sync On Save Override File Extension</b> field.
<b>Sync Multi Host Mod List</b>	Extensions configured here will not be quarantined if they are modified on two hosts simultaneously. The file with the latest modified time stamp will win.
<b>Target Sharing Violation File Extensions</b>	This is an option to retry setting the target lock when receiving error code 32 for the specified list of extensions. This may be useful for file types such as .one (OneNote), .rvt (Revit), and .dat (associated Revit files) that don't sustain a handle when the user has the file open.
<b>Bulk Context Minimum Rejected Event Threshold</b>	The number of bulk add files that can process immediately before batching the remainder of the files and process them in a single thread.
<b>Retry Quarantine File List</b>	Quarantined files that are in this list will be automatically removed and flagged as unsynchronized and will be retried every second after a delay period (delay is configured by <b>fc.retryQuarantinesDelay</b> ). Any change event that is detected for the files will trigger a scan of the files where the newest file will win. This list can contain file names (wperms.dat, eperms.dat, requests.dat, deltas.dat, users.dat) or extensions (*.dat,*.abc).
<b>Last Write Override Extensions</b>	Act on every write event performed on these extensions instead of waiting for the last write event prior to the closing of a file.

<b>Expedited Fast Sync File List</b>	Access events and transfer events will be expedited for the list of extension or files in this list.
<b>Expedited Slow Sync File List</b>	Access events received for files or extension in this list will be expedited. Transfers will go through a slow priority queue.
<b>Direct Target Write List</b>	List of files to be updated without the use of a temp file. This list can contain file names (wperms.dat, eperms.dat, requests.dat, deltas.dat, users.dat") or extensions.

5. Click **Apply and Close** or **Apply**.

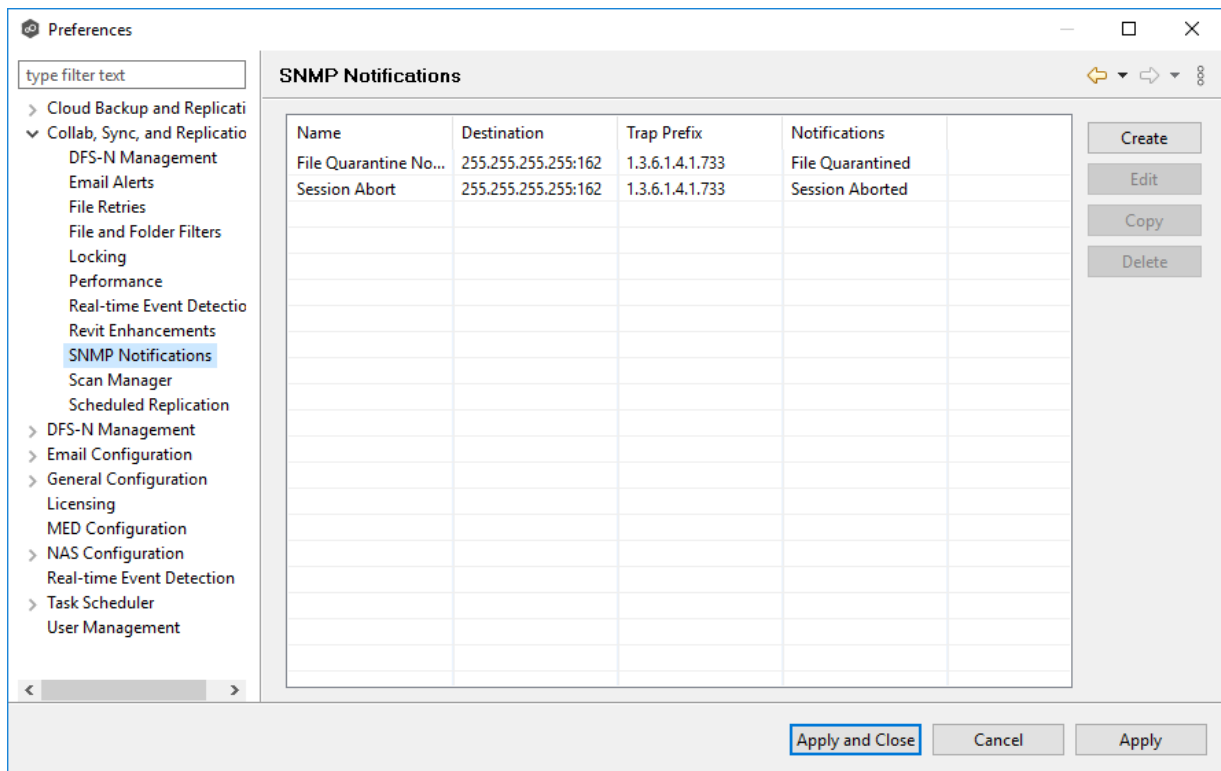
## SNMP Notifications

When you create a job, you can select an existing SNMP notification to apply to the job or you can create a new notification and apply it to the job. You cannot modify or delete an SNMP notification while it is applied to a job. See [SNMP Notifications](#) in the [Basic Concepts](#) section for more information about SNMP notifications.

To create an SNMP notification:

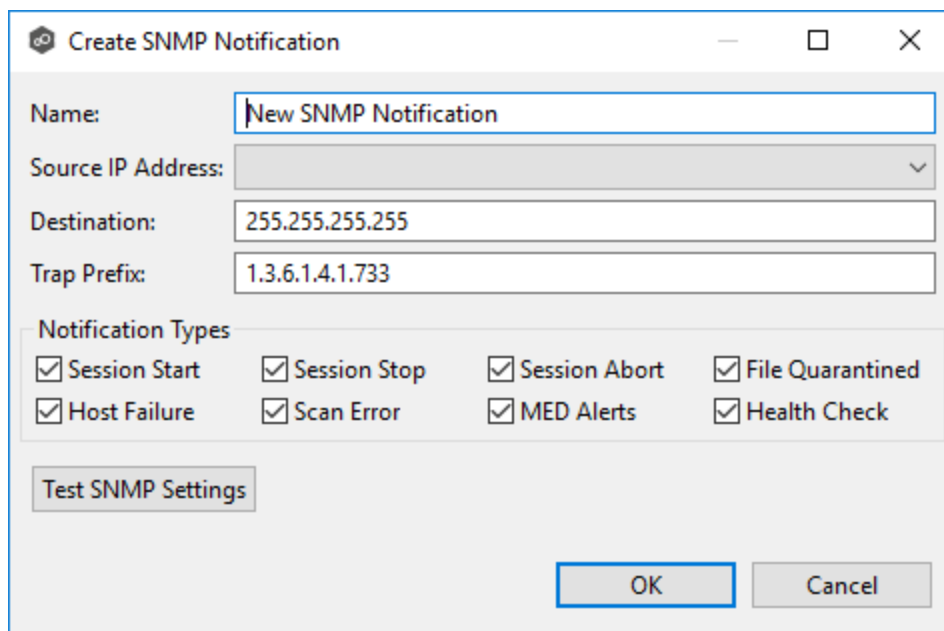
1. From the **Window** menu, select **Preferences**.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **SNMP Notifications**.

Any existing SNMP notifications are listed in the **SNMP Notifications** table.



3. Click the **Create** button.

The **Create SNMP Notification** dialog appears.



4. In the **Source IP Address** field, select or manually enter the IP address over which the trap will be sent.

5. In the **Destination** field, enter the destination host name, IP address, or broadcast address.
6. In the **Trap Prefix** field, enter a prefix that will help to identify whether the message is coming from different instances of Peer Management Center or from different jobs.
7. For **Notification Types**, select the types of events that will trigger the generation of an SNMP trap:

<b>Session Start</b>	Sends a notification when a session is started.
<b>Session Stop</b>	Sends a notification when a session is stopped.
<b>Session Abort</b>	Sends a notification when a session is aborted because of lack of quorum due to a failed host(s).
<b>File Quarantined</b>	Sends a notification when a file is marked as quarantined because a file conflict was not able to be resolved.
<b>Host Timeout</b>	Sends a notification when a host timeout occurs, and the host is taken out of session.
<b>Scan Error</b>	Sends a notification when an error occurs during the <a href="#">initial synchronization process</a> .
<b>MED Alerts</b>	Sends a notification when Peer MED detects potentially malicious activity. For more information, see <a href="#">MED Configuration</a> .
<b>Health Check</b>	Sends a notification when Health Check finds an error. Checks to make sure that real-time information is being communicated.

8. (Optional) Click **Test SNMP Settings**, and then click **OK** in the **Test Connection** dialog.
9. Click **Apply and Close** or **Apply**.

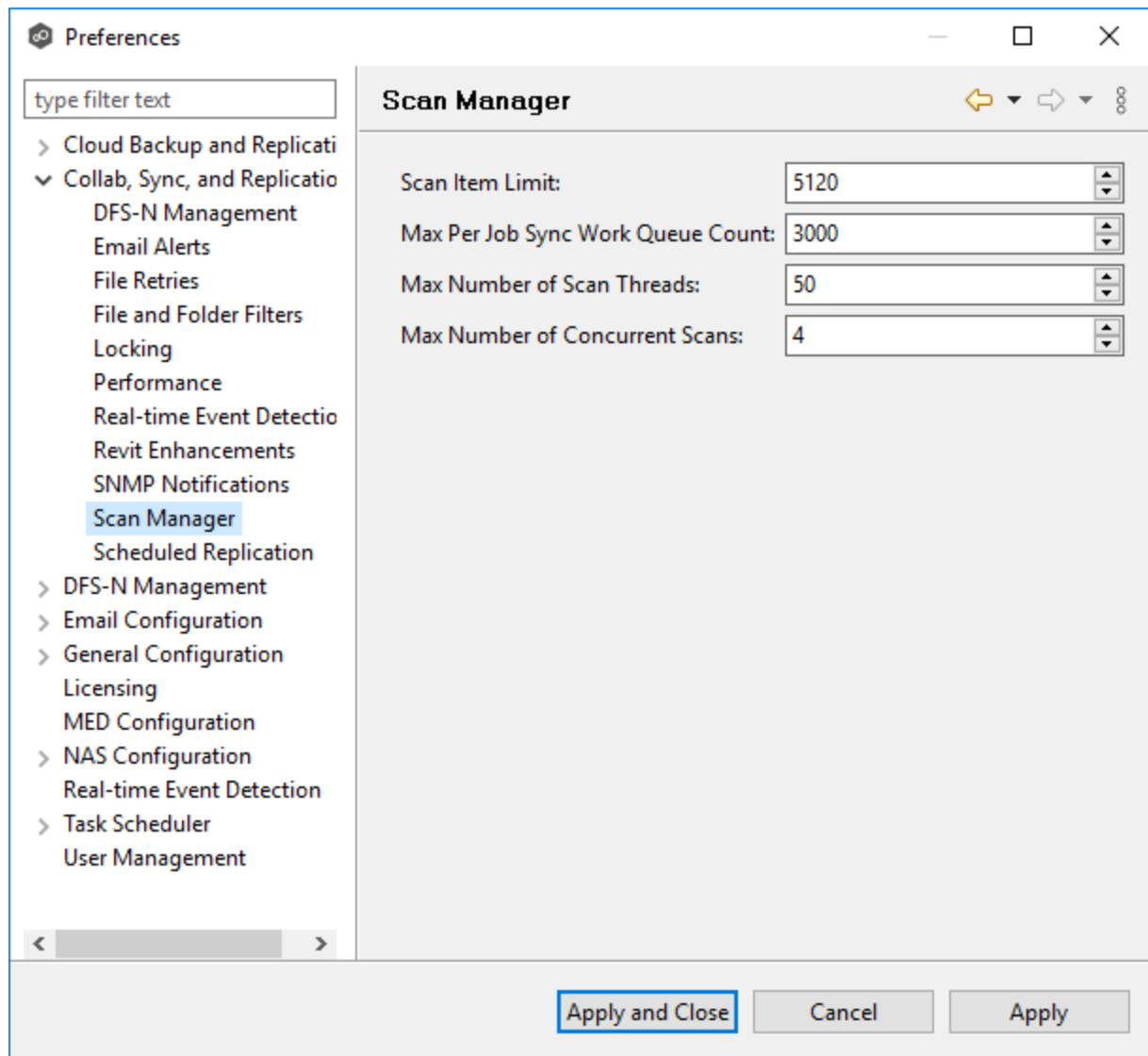
The new notification is listed in the **SNMP Notifications** table and can now be applied to jobs.

## Scan Manager

Several options are available to tune the way scans are performed for File Collaboration, File Synchronization, and File Replication jobs.

To modify the Scan Manager settings for File Collaboration, File Synchronization, and File Replication jobs:

1. From the **Window** menu, select **Preferences**.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Scan Manager**.



3. Modify the settings as needed.

<b>Scan Item Limit</b>	The maximum number of file and folder scan results that are returned in one scan iteration during a job's initial scan. This value is used to constrain the amount of memory used when performing initial scans with a large number of jobs.
<b>Max Sync Work Queue Count</b>	The per job maximum number of pending file synchronization tasks that are queued in memory before pausing the current scan. This value only has an effect on jobs with large numbers of files that must be synchronized during <a href="#">initial synchronization</a> .

<b>Max Number of Scan Threads</b>	The maximum number of threads that can be created to scan folders and files. This number should be set to at least the number of jobs that you are running.
<b>Max Number of Concurrent Scans</b>	The maximum number of scan threads that can be actively working at the same time. This differs from the Max Number of Scan Threads in that not all created scan threads can be simultaneously doing work. For example, if 20 scan threads are configured but only 10 can run concurrently, 10 of the 20 threads will be paused at any one time, waiting for a time slot to continue working. Each of the 20 scan threads will get a chance to work in a round-robin fashion.

4. Click **Apply and Close** or **Apply**.

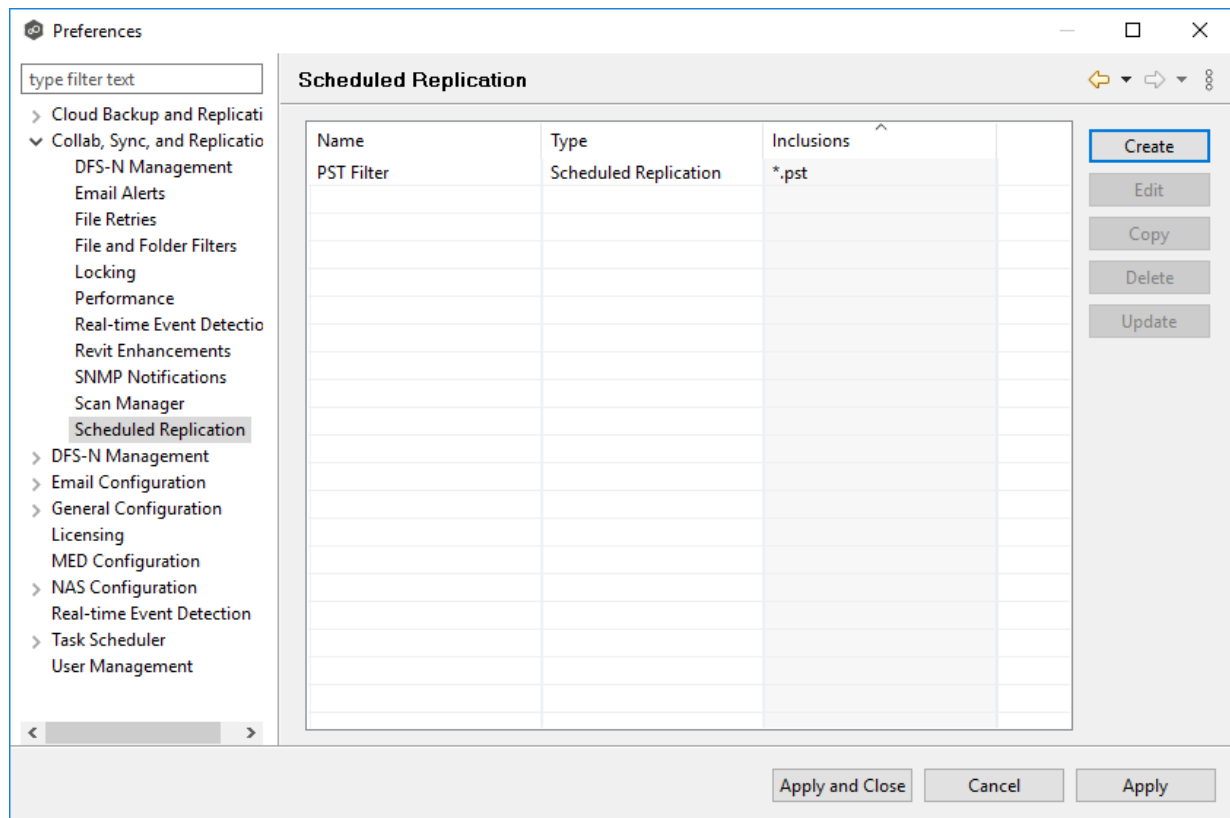
## Scheduled Replication

When you create a job, you can select existing scheduled replication filters to apply to the job or you can create new scheduled replication filters and apply them to the job. This [Preferences](#) page lists the existing scheduled replication filters. From this page, you can view, create, edit, and delete scheduled replication patterns. However, you cannot edit or delete an scheduled replication filter while it is applied to a job. See [Scheduled Replication](#) in the [Advanced Topics](#) section for more information about scheduled replication.

To create a scheduled replication filter:

1. Select **Preferences** from the **Window** menu.
2. Expand **Collab, Sync, and Replication** in the navigation tree, and then select **Scheduled Replication**.

Any existing scheduled replication filters are listed in the **Scheduled Replication** table.



3. Click **Create**.



**Create Scheduled Replication Filter**

Name:

Filter Type: Scheduled Replication

**Included Patterns**

Add Edit Delete

**Scheduling Options**

☒ Process every: 1 minute

☐ Process on a schedule

☐ Daily ☒ Weekly

Day(s):

☐ Sunday

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

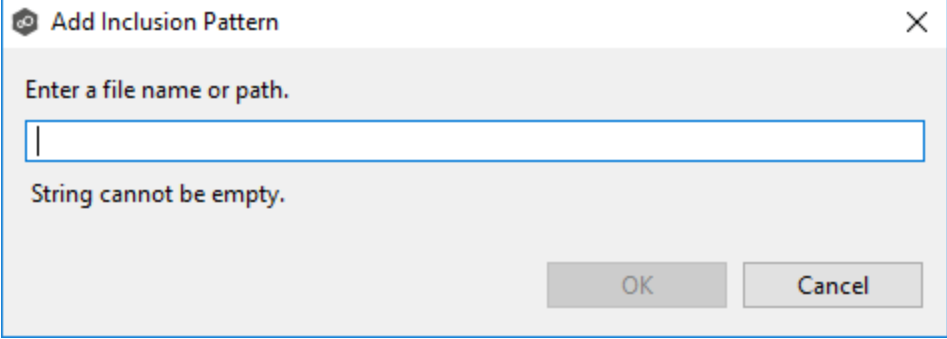
Time:

None

OK Cancel

4. Enter a unique name for the filter.
5. Click **Add** under **Included Patterns** to enter a filter pattern for files that you want to delay replication. Repeat to add more filter patterns.

A **filter pattern** is a character string that defines a logical expression that is evaluated to determine which files and folders match the pattern. A filter pattern can contain [complex regular expressions](#) and [wildcards](#).

A screenshot of a Windows-style dialog box titled "Add Inclusion Pattern" with a close button (X) in the top right corner. The dialog has a light gray background. Inside, the text "Enter a file name or path." is displayed above a text input field. The input field is currently empty, with a vertical cursor at the beginning. Below the input field, the text "String cannot be empty." is shown in a smaller font. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Add Inclusion Pattern

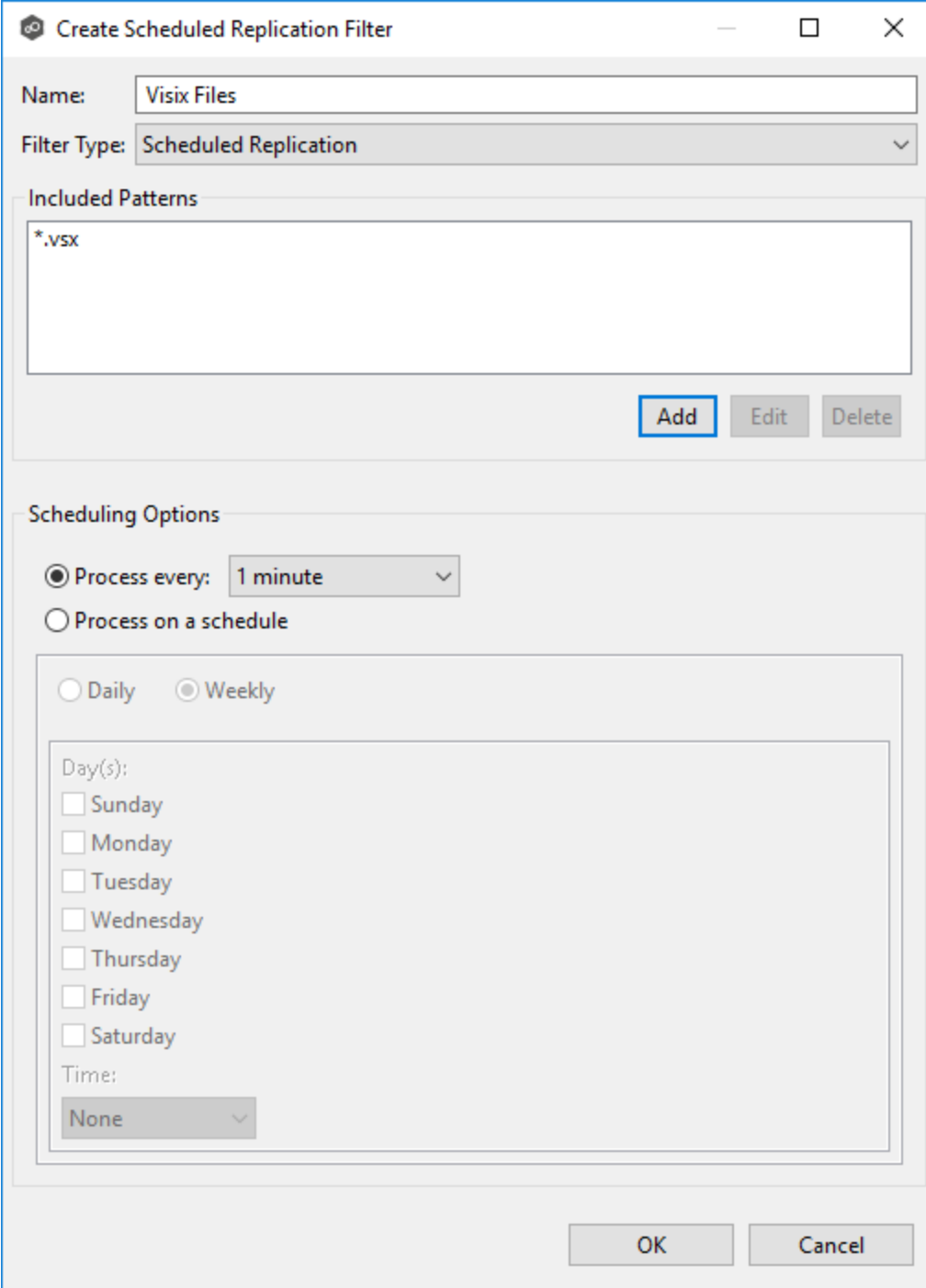
Enter a file name or path.

String cannot be empty.

OK Cancel

6. Click **OK**.

The pattern appears in the **Included Patterns** field.



The image shows a 'Create Scheduled Replication Filter' dialog box. It has a title bar with a logo, a minimize button, a maximize button, and a close button. The main area is divided into sections. The first section has a 'Name' field with 'Visix Files' and a 'Filter Type' dropdown set to 'Scheduled Replication'. Below this is an 'Included Patterns' section with a text area containing '\*.vsx' and buttons for 'Add', 'Edit', and 'Delete'. The second section is 'Scheduling Options', which has two radio buttons: 'Process every:' (selected) and 'Process on a schedule'. The 'Process every:' option has a dropdown set to '1 minute'. The 'Process on a schedule' option has sub-options for 'Daily' and 'Weekly' (selected). Below these are checkboxes for days of the week (Sunday through Saturday) and a 'Time' dropdown set to 'None'. At the bottom are 'OK' and 'Cancel' buttons.

Create Scheduled Replication Filter

Name: Visix Files

Filter Type: Scheduled Replication

Included Patterns

\*.vsx

Add Edit Delete

Scheduling Options

☒ Process every: 1 minute

☐ Process on a schedule

☐ Daily ☒ Weekly

Day(s):

☐ Sunday

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

Time:

None

OK Cancel

7. Select a scheduling option:

- **Interval** - Process at a specified interval.
- **Schedule** - Process at a scheduled time.

- After selecting a scheduling option, click **OK**.

The new filter is listed in the **Scheduled Replication** table and can now be applied to jobs.

- Click **Apply and Close** or **Apply**.

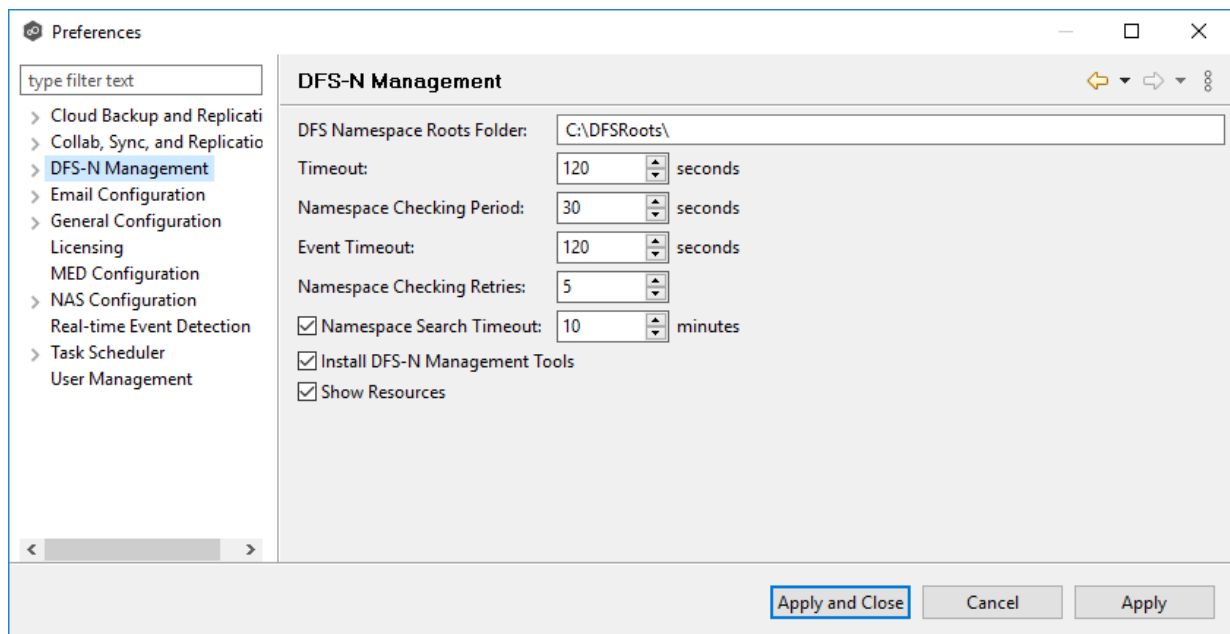
## DFS-N Management Job Preferences

To modify settings for [DFS-N Management jobs](#):

- Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

- Select **DFS-N Management** in the navigation tree.



- Modify settings as needed.

Setting	Description
<b>DFS Namespace</b>	Enter the path to the default local parent folder for namespaces on the namespace server.

Setting	Description
<b>Roots Folder</b>	
<b>Timeout</b>	Enter the number of seconds to wait for a response from any agent.
<b>Namespace Checking Period</b>	Enter the number of seconds to delay between checking namespace information calls. This check catches any changes made to a namespace using the Microsoft DFS Management tool. Selecting a low value will negatively affect performance but will reflect changes to the user interface more quickly.
<b>Event Timeout</b>	Enter the number of seconds to wait before marking an event containing DFS namespace information from the Agent has timed out.
<b>Namespace Checking Retries</b>	Enter the maximum number of times for checking namespace information if the namespace is not found. Once the maximum number is exceeded, the job is stopped.
<b>Namespace Search Timeout</b>	Enter the number of minutes before timing out after search.
<b>Install DFS-N Management Tools</b>	Select this option if you want Microsoft's DFS-N Management tools installed when creating or importing a namespace.
<b>Show Resources</b>	Select this option if you want to display individual namespace folders under each namespace in the <b>Jobs</b> view.

- Click **OK** or **Apply**.

## Email Alerts

When you create a job, you can select existing email alerts to apply to the job or you can create new email alerts and apply them to the job. This [Preferences](#) page lists the existing email alerts. From this page, you can view, create, edit, and delete email alerts. However, you cannot edit or

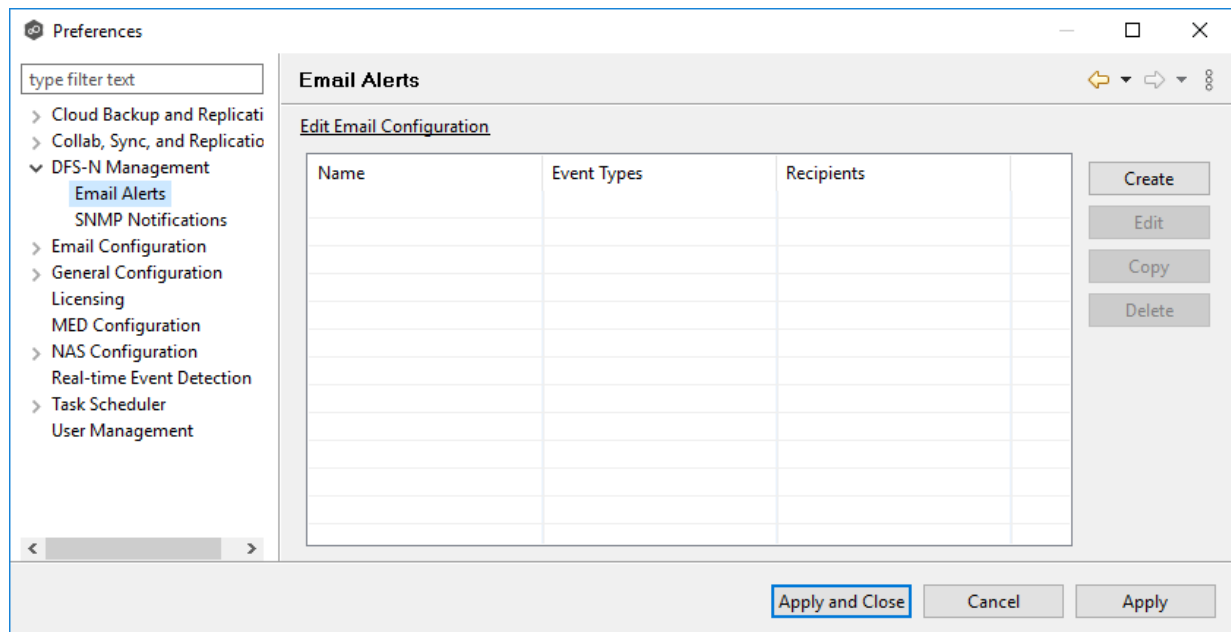
delete an email alert while it is applied to a job. See [Email Alerts](#) in the [Basic Concepts](#) section for more information about email alerts.

**Note:** An SMTP email connection must be configured before email alerts can be sent. See [Email Configuration](#) for information about configuring SMTP email settings.

To create an email alert:

1. Select **Preferences** from the **Window** menu.
2. Expand **DFS-N Management** in the navigation tree, and then select **Email Alerts**.

Any existing DFS-N Management email alerts are listed in the **Email Alerts** table.



3. Click the **Create** button.

The **Create Email Alert** dialog appears.

**Create Email Alert**

Name:

**Event Types**

☒ Session Abort
 ☒ Host Failure
 ☒ Host Reconnect
 ☒ Namespace Offline

☒ Namespace Not Found
 ☒ Folder Target Offline
 ☒ DFS Server Offline

**Recipients**

Enter email, contact, or distribution list:

Recipients:

4. Enter a name for the alert.
5. Select the event types to be alerted.

The event type determines what will trigger the email alert to be sent.

Event Type	Description
<b>Session Abort</b>	Sends an alert when the DFS-N Namespace job stops unexpectedly.
<b>Host Failure</b>	Sends an alert when the Management Agent of a DFS-N Namespace job disconnects or stops responding.
<b>Host Reconnect</b>	Sends an alert when a system event such as low memory or low hub disk space occurs.
<b>Namespace Offline</b>	Sends an alert when a namespace goes offline.

Event Type	Description
<b>Namespace Not Found</b>	Sends an alert when a namespace goes offline is not found.
<b>Folder Target Offline</b>	Sends an alert when a folder target goes offline.
<b>DFS Server Offline</b>	Sends an alert when a DFS server goes offline.

6. Enter alert recipients, and then click **Add to List**.

The recipients are listed in the **Recipients** field.

7. Click **OK** or **Apply**.

The new alert is listed in the **Email Alerts** table and can now be applied to jobs.

## SNMP Notifications

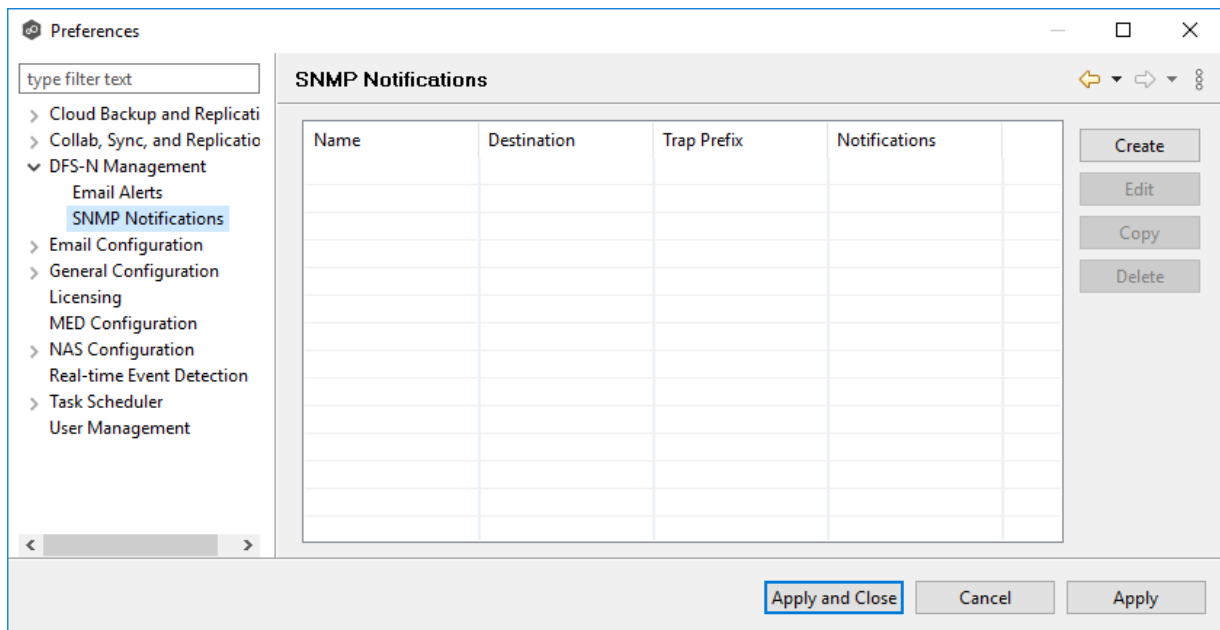
When you create a job, you can select an existing SNMP notification to apply to the job or you can create a new notification and apply it to the job. You cannot edit or delete an SNMP notification while it is applied to a job. See [SNMP Notifications](#) in the [Basic Concepts](#) section for more information about SNMP notifications.

To create an SNMP notification:

1. From the **Window** menu, select **Preferences**.
2. Expand **DFS-N Management** in the navigation tree, and then select **SNMP Notifications**.

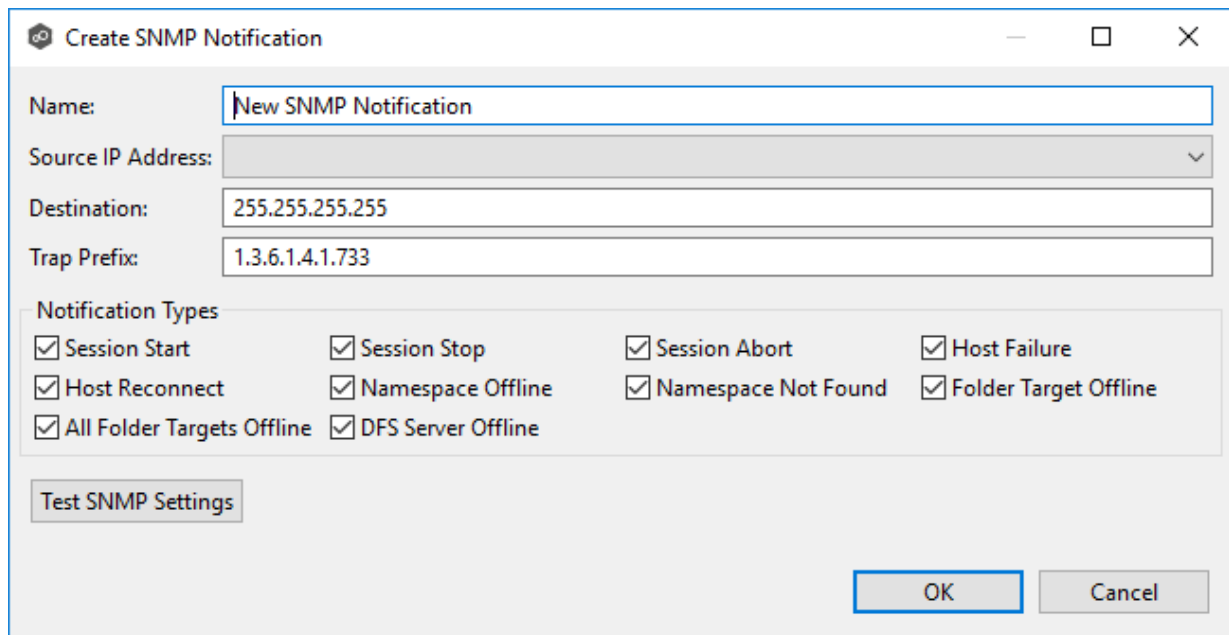
The existing SNMP notifications are listed in the **SNMP Notifications** table.





3. Click the **Create** button.

The **Add SNMP Notification** dialog appears.



4. In the **Source IP Address** field, select or manually enter the IP address over which the trap will be sent.
5. In the **Destination** field, enter the destination host name, IP address, or broadcast address.

6. In the **Trap Prefix** field, enter a prefix that will help to identify whether the message is coming from different instances of Peer Management Center or from different jobs.
7. For **Notification Types**, select the types of events that will trigger the generation of an SNMP trap:

Notification Type	Description
<b>Session Start</b>	Sends a notification when a session is started.
<b>Session Stop</b>	Sends a notification when a session is stopped.
<b>Session Abort</b>	Sends a notification when the DFS-N Namespace job stops unexpectedly.
<b>Host Failure</b>	Sends a notification a notification when the Management Agent of a DFS-N Namespace job disconnects or stops responding.
<b>Host Reconnect</b>	Sends an alert when a system event such as low memory or low hub disk space occurs.
<b>Namespace Offline</b>	Sends a notification when the namespace goes offline.
<b>Namespace Not Found</b>	Sends a notification when the namespace is not found.
<b>Folder Target Offline</b>	Sends a notification when a folder target goes offline.
<b>All Folder Targets Offline</b>	Sends a notification when all folder targets go offline.
<b>DFS Server</b>	Sends a notification when the DFS server goes offline.

Notification Type	Description
Offline	

- (Optional) Click **Test SNMP Settings**, and then click **OK** in the **Test Connection** dialog.
- Click **OK** or **Apply**.

The new notification is listed in the **SNMP Notifications** table and can now be applied to jobs.

## Email Configuration

Before Peer Management Center can send emails on behalf of any job, a few key SMTP email settings must be configured. In addition, you can define contacts and distribution lists.

To configure email settings:

- Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

- Select **Email Configuration** in the navigation tree.

The following is displayed:

The screenshot shows the 'Preferences' window with the 'Email Configuration' tab selected. The left sidebar lists various configuration categories, with 'Email Configuration' highlighted. The main area contains settings for SMTP email configuration and batch email alerts for quarantined files.

**Preferences**

type filter text

- > Cloud Backup and Replicati
- > Collab, Sync, and Replicatio
- > DFS-N Management
- > **Email Configuration**
- > General Configuration
- Licensing
- MED Configuration
- > NAS Configuration
- Real-time Event Detection
- > Task Scheduler
- User Management

**Email Configuration**

SMTP Email Configuration

\*SMTP Host: outlook.office365.com

\*SMTP Port: 587

Encryption: ☒

\*Encryption Type: TLS

\*Username: debrag@peersoftware.com

\*Password: ••••••••

\*Sender Email: debrag@peersoftware.com

Use Recommended Office 365 Settings: ☒

Test Email Settings

Batch Email Alerts for Quarantined Files

Batch Quiet Period (in seconds): 60

Maximum Number of Alerts: 1000

Apply and Close Cancel Apply

3. Enter values for the following fields:

<b>SMTP Host</b>	Enter the host name or IP address of the SMTP mail server through which Peer Management Center will send emails.
<b>SMTP Port</b>	Enter the TCP/IP connection port (default is 25 and 465 for encryption) on which the mail server is hosting the SMTP service. We recommend that you leave the default setting unless your email provider specifies otherwise.
<b>Encryption</b>	Select this checkbox if the SMTP mail server requires an encrypted connection.
<b>Encryption Type</b>	If encryption is enabled, an encryption method must be selected. TLS and SSL are the available options. If you do not know which one your mail server requires, try one, and then the other.
<b>Username</b>	Enter the user name to authenticate as on the SMTP mail server.
<b>Password</b>	Enter the password for the user specified above.
<b>Sender Email</b>	Enter the email address to appear in the <b>From</b> field of any sent emails. This email address sometimes needs to have a valid account on the SMTP mail server.
<b>Use Recommended Office 365 Settings</b>	Select this checkbox if you are connecting to an Office 365 SMTP server to use recommended settings for the connection. Follow Microsoft's <b>Direct Send</b> recommendations to set up email configuration with an Office 365 SMTP server.

4. (Recommended) Click **Test Email Settings**, enter an email address, and then click **OK**.

It is highly recommended that you test your SMTP settings before saving them. You will be prompted for an email address to send the test message to. Upon submission, Peer Management Center will attempt to send a test message using the specified settings.

5. Enter values for the fields in the **Batch Email Alerts for Quarantined Files** section:

<b>Batch Quiet Period (in seconds)</b>	Enter the number of seconds to wait before releasing a batch of alerts.
<b>Maximum Number of Alerts</b>	Enter the maximum number of alerts that should be sent in a single email.

6. Click **OK** or **Apply**.

## General Configuration

The **General Configuration** settings affect the overall operation of Peer Management Center, Peer Agents, the Peer Broker, and other general operations. They are not specific to jobs or job types.

You can modify the following settings:

[General Configuration](#)

[Agent Connectivity](#)

[Broker Configuration](#)

[Email Alerts](#)

[Software Updates](#)

[Tags Configuration](#)

[Web and API Configuration](#)

## General Configuration

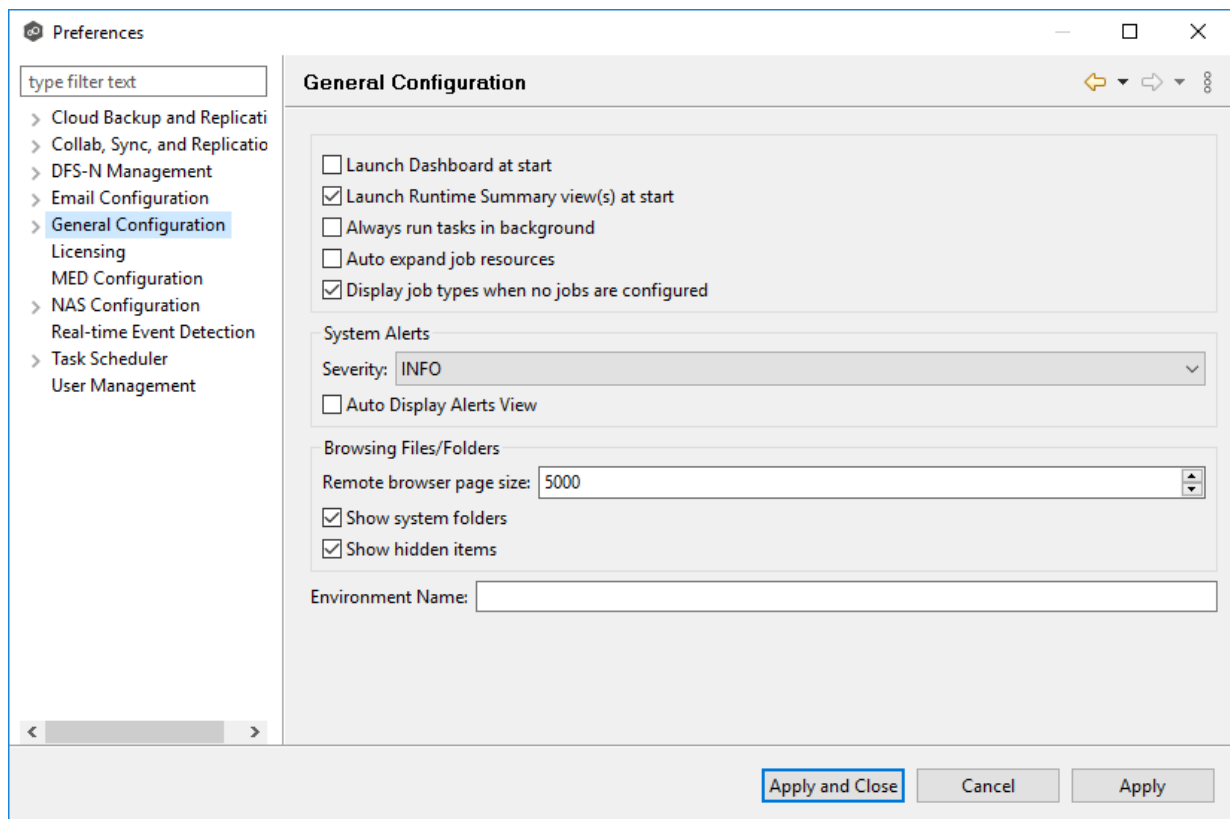
To modify General Configuration settings:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Select **General Configuration** in the navigation tree.

The first page of the General Configuration options is displayed.



3. Modify the first four settings as needed:

Setting	Description
<b>Launch Dashboard at start</b>	Select this option if you want the Dashboard to be automatically displayed when Peer Management Center is started.

Setting	Description
<b>Launch Runtime Summary view(s) at start</b>	Select this option if you want the <a href="#">Summary views</a> to be automatically displayed when Peer Management Center is started. Summary views will be displayed for all job types, even for job types without currently running jobs.
<b>Always run tasks in background</b>	Select this option to run tasks like log gathering and Agent updates in the background, preventing these tasks from blocking the use of the Peer Management Center client while they run.
<b>Auto expand job resources</b>	Select this option if you want all jobs with associated resources to start expanded in the <b>Jobs</b> view. Currently only available for Cloud Backup and Replication jobs and DFS-N Management jobs.
<b>Display job types when no jobs are configured</b>	Select this option if you want to display a job type in the <b>Jobs</b> view, even when no jobs of that type have been configured.

4. Select options for alerts regarding the operation of Peer Management Center in the [Alerts view](#):

Option	Description
<b>Severity</b>	Select one of these options: <ul style="list-style-type: none"> <li>• INFO</li> <li>• DEBUG</li> <li>• TRACE</li> </ul>
<b>Auto Display Alerts View</b>	Select this option if you want the alerts to be automatically displayed in the <a href="#">Alerts view</a> .

5. Select options for managing browsing files and folders on remote file systems in the **Browsing Files/Folders** section:



Option	Description
<b>Remote browser page size</b>	Enter the maximum page size for the remote file system browser. This browser is used for selecting paths during the creation of most new jobs.
<b>Show system folders</b>	Select this checkbox to show system folders in the remote file system browser.
<b>Show hidden folders</b>	Select this checkbox to show hidden folders in the remote file system browser.

6. (Optional) Enter the name of your PMC server or environment in the **Environment Name** field; if left blank, reports and dashboards will use the name of the PMC server.
7. Click **OK** or **Apply**.

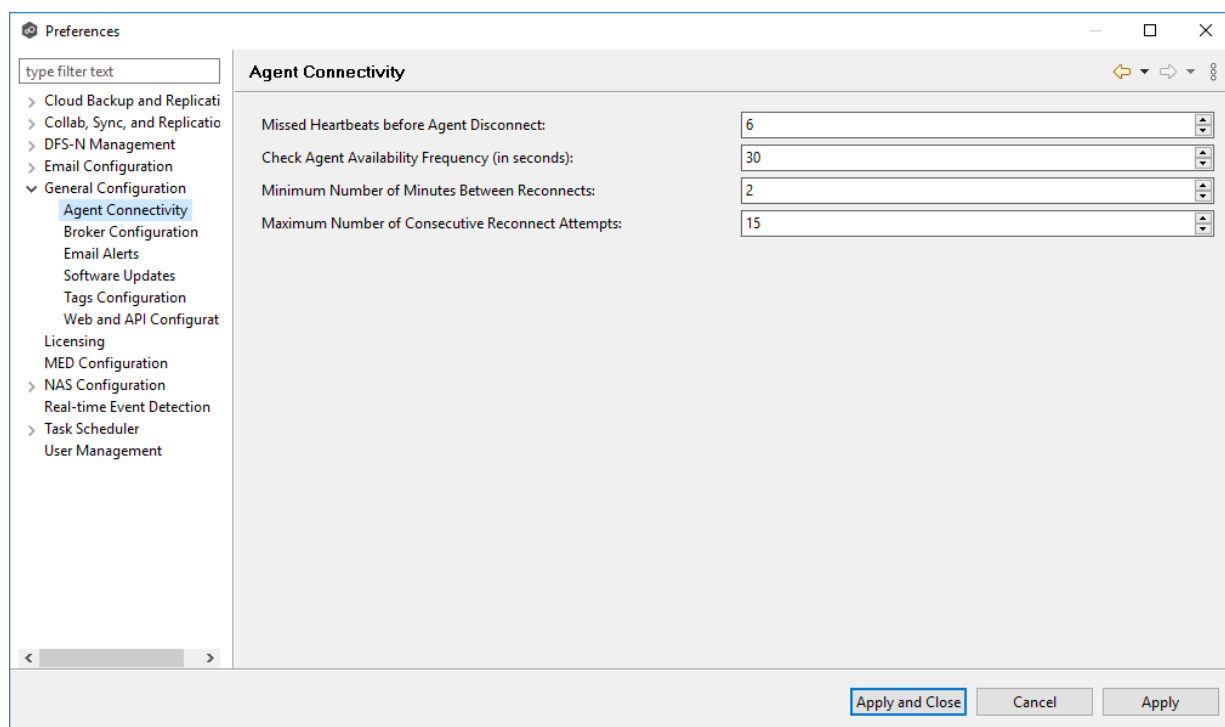
## Agent Connectivity

To modify Agent Connectivity settings:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Expand **General Configuration** in the navigation tree, and then select **Agent Connectivity**.



3. Modify the settings as needed:

<b>Missed Heartbeats before Agent Disconnect</b>	Enter the maximum number of heartbeats that can be missed on a host before Peer Management Center labels the Agent as disconnected. If a running job hits a timeout when communicating with a specific Agent, Peer Management Center will check this status to decide if the Agent should be dropped from the job.
<b>Check Agent Availability Frequency (in seconds)</b>	Enter the frequency (in seconds) that Peer Management Center should check whether an Agent is back online.
<b>Minimum Number of Minutes Between Reconnects</b>	Enter the minimum number of minutes that must elapse before Peer Management Center attempts to retry reconnecting to the Agent.
<b>Maximum Number of Consecutive Reconnect Attempts</b>	Enter the maximum number of attempts that Peer Management Center tries to reintegrate a previously connected agent into one or more jobs. Once the maximum number of attempts has been reached, you must manually reintegrate the Agent into affected jobs, typically by restarting the affected jobs.

4. Click **OK** or **Apply**.

## Broker Configuration

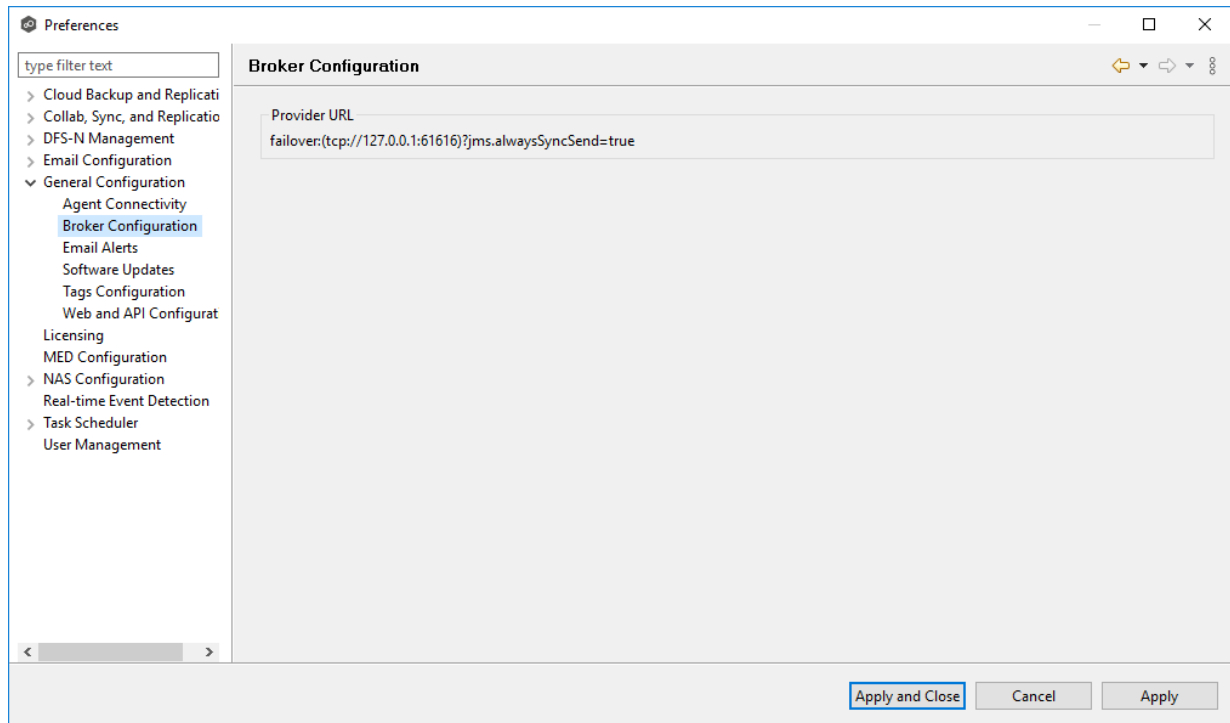
The **Broker Configuration** page displays a non-editable field that shows the URL used by the Peer Management Center service to connect to the Broker service.

To view the Broker Configuration URL:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Expand **General Configuration** in the navigation tree, and then select **Broker Configuration**.



3. Click **OK** or **Apply**.

## Email Alerts

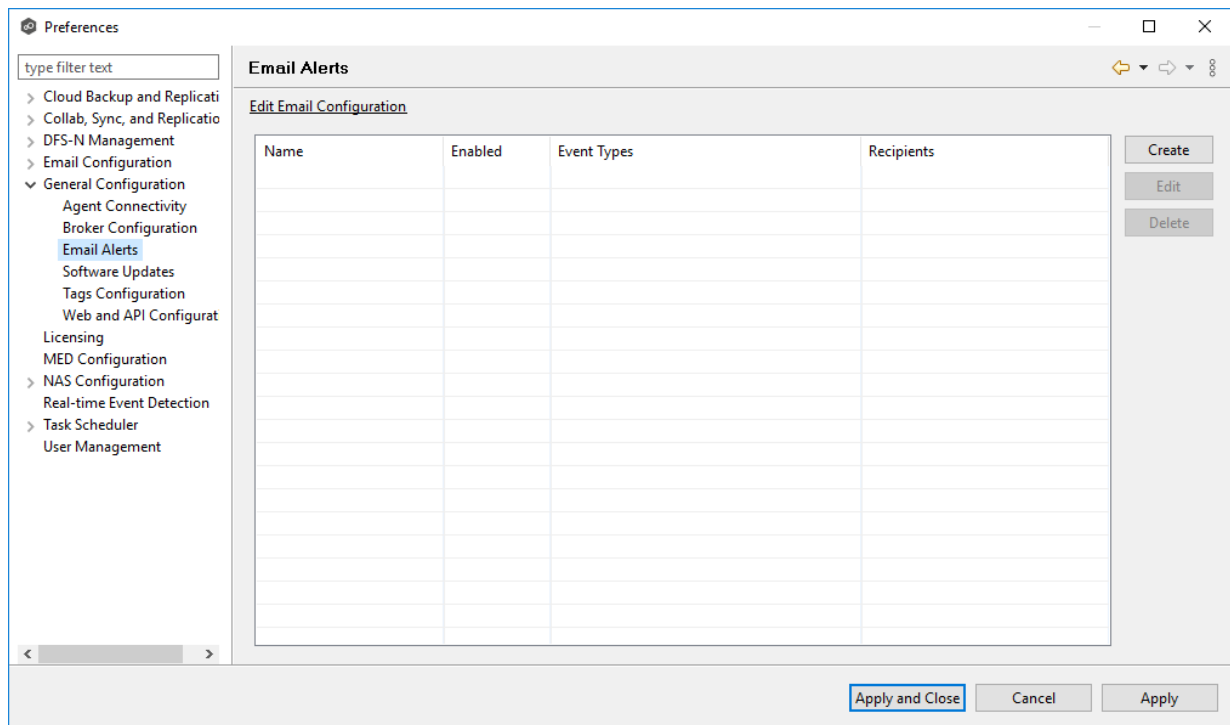
System email alerts notify recipients when certain types of system events occur, for example, low memory, low disk space, disconnected agents. This [Preferences](#) page lists the existing system email alerts. From this page, you can create, edit, and delete system email alerts. You can also disable and enable alerts. See [Email Alerts](#) in the [Basic Concepts](#) section for more information about email alerts.

**Note:** An SMTP email connection must be configured before email alerts can be sent. See [Email Configuration](#) for information about configuring SMTP email settings.

To create a system email alert:

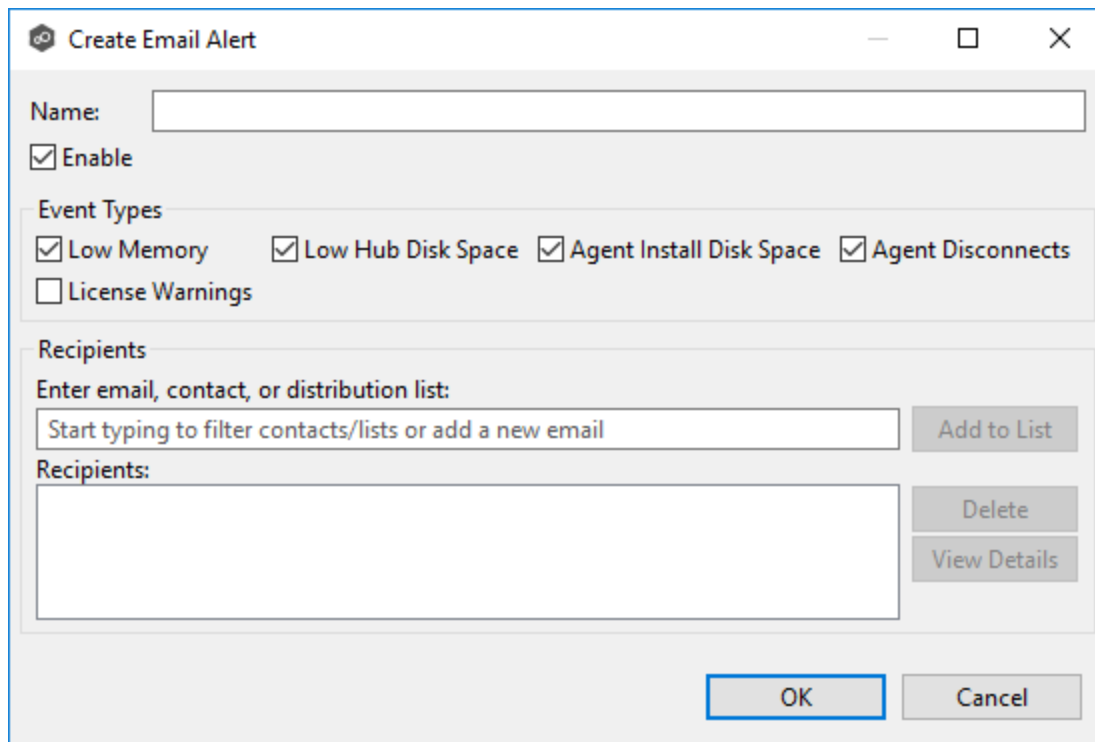
1. Select **Preferences** from the **Window** menu.
2. Expand **General Configuration** in the navigation tree, and then select **Email Alerts**.

Any existing system alerts are listed in the **Email Alerts** table.



3. Click **Create**.

The **Create Email Alert** dialog appears.



4. Enter a name for the alert.
5. Select the **Enable** checkbox if you want to enable the alert.

If you choose not to enable the alert, you can enable it later by editing the alert

6. Select the type of events for which you want alerts sent:

<b>Low Memory</b>	Sends an alert when Peer Management Center or connected Agent services are is low on memory.
<b>Low Hub Disk Space</b>	Sends an alert when the space on the disk where Peer Management Center software is installed running low.
<b>Agent Install Disk Space</b>	Sends an alert when the space on the disk where the Peer Agent software is installed is running low.
<b>Agent Disconnects</b>	Sends an alert whenever an Agent is disconnected.
<b>License Warnings</b>	Sends an alert when a license is about to expire or when a license violation is about to occur.

7. Enter alert recipients, and then click **Add to List**.
8. Click **OK** or **Apply**.

The new alert is listed in the **Email Alerts** table.

## Software Updates

You can configure Peer Management Center to automatically check for updates and download the updates. Peer Management Center checks for updates every evening at 11 p.m. local time. Only minor updates are automatically downloaded; if a major update is available, a notification appears. Major releases require a new license key and must be requested from Peer Software Support.

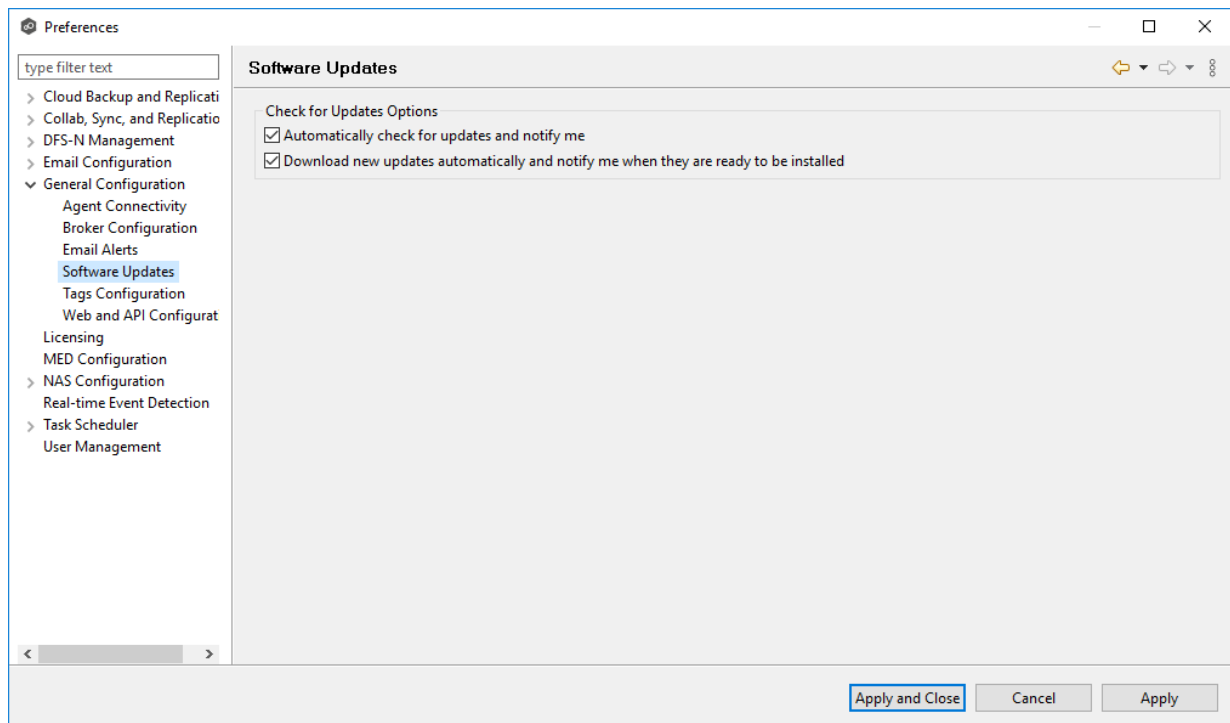
You can also manually check for updates. See [Updating Peer Management Center](#) for information about manually checking for updates.

To configure Peer Management Center to automatically check for updates:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Select **General Configuration** in the navigation tree, expand the node, and then select **Software Updates**.



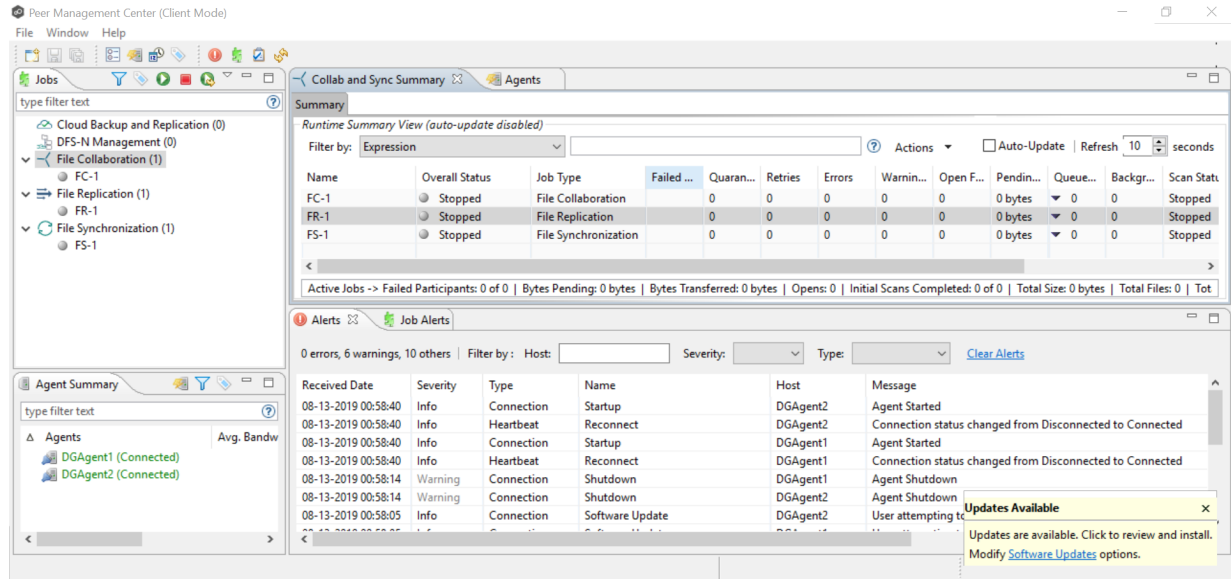
3. Select update options:

- **Automatically check for updates and notify me** - Select this option if you want to automatically check for updates.

- **Download new updates automatically and notify me when they are ready to be installed** - Select this option if you want to automatically check for and download available updates.

4. Click **OK** or **Apply**.

Whenever updates are available, a notification appears in the lower right corner of Peer Management Center.



5. Click the notification to review and proceed with the update. See [Updating Peer Management Center](#) for details.

## Tags Configuration

The **Tags Configuration** page in Preferences is the starting place for creating [tags](#) and categories that can later be assigned to resources. See [Assigning Tags](#) for more information about assigning to resources.

To create a tag:

1. Select **Preferences** from the **Window** menu.
2. Expand **General Configuration** in the navigation tree, and then select **Tags Configuration**.

Any existing tags are listed in the **Tags** table.





6. Click **OK**.

The tag appears in the **Tags** table.

7. Click **OK** or **Apply**.

## Web and API Configuration

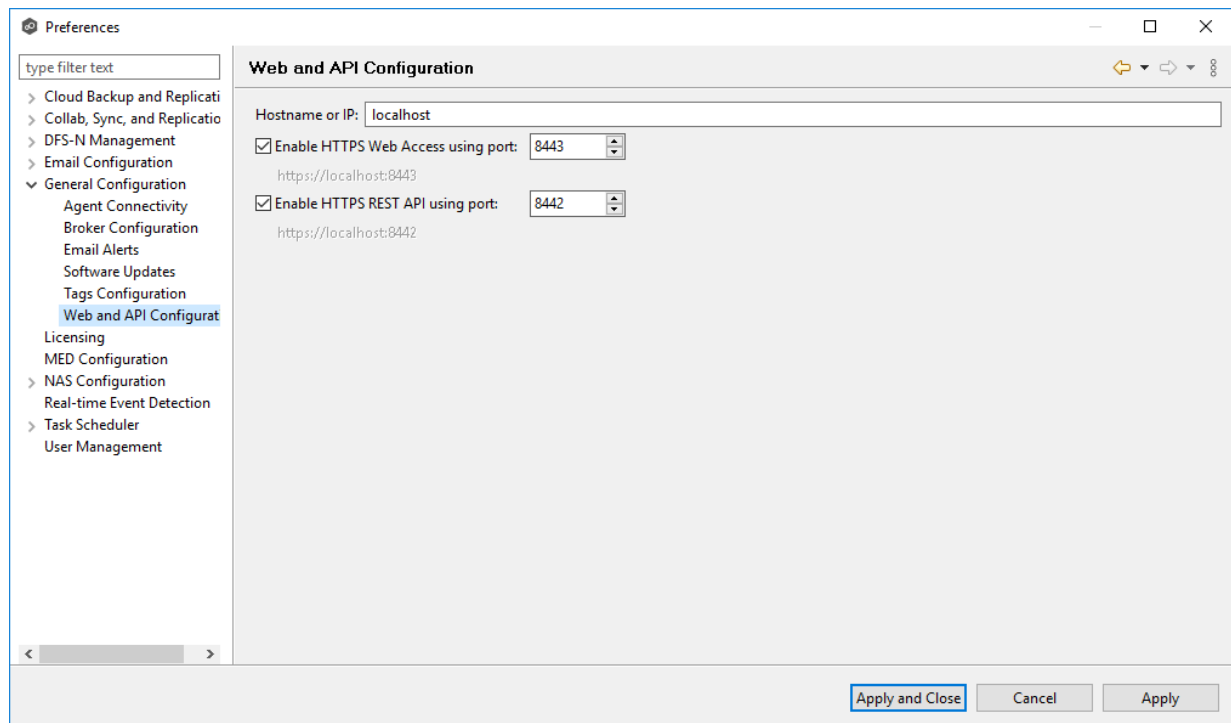
As part of the Peer Management Center installation process, you are prompted to [configure access to the web and API services](#). If you do not enable access during the initial installation or want to modify settings at a later date, you can modify them in [Web and API Configuration](#) in [Preferences](#).

To modify web and API settings:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Expand **General Configuration** in the navigation tree, and then select **Web and API Configuration**.



3. Modify the configuration options.

<b>Hostname or IP</b>	<p>Enter the hostname or IP address via which the services be can accessed:</p> <ul style="list-style-type: none"><li>• Enter <b>localhost</b> or <b>127.0.0.1</b> if you want the services to be accessible only to users of the local server via the loopback interface.</li><li>• Enter <b>0.0.0.0</b> to make the services accessible via all network interfaces.</li><li>• Enter a specific IP address to restrict access to a specific network interface.</li></ul>
<b>Enable HTTPS Web Access</b>	Select this checkbox to enable HTTP access to the web service using the specified port.
<b>Enable HTTPS REST API</b>	Select this checkbox to enable HTTPS access to the REST API service using the specified port.

4. Click **OK** or **Apply**.

## Licensing

Peer Global File System is licensed by the number of unique [participants](#) and by the number of terabytes in the [watch set](#).

## Installing or Upgrading a License File

After purchasing or requesting a trial download of Peer Management Center, you will receive a license file representing your purchase or trial.

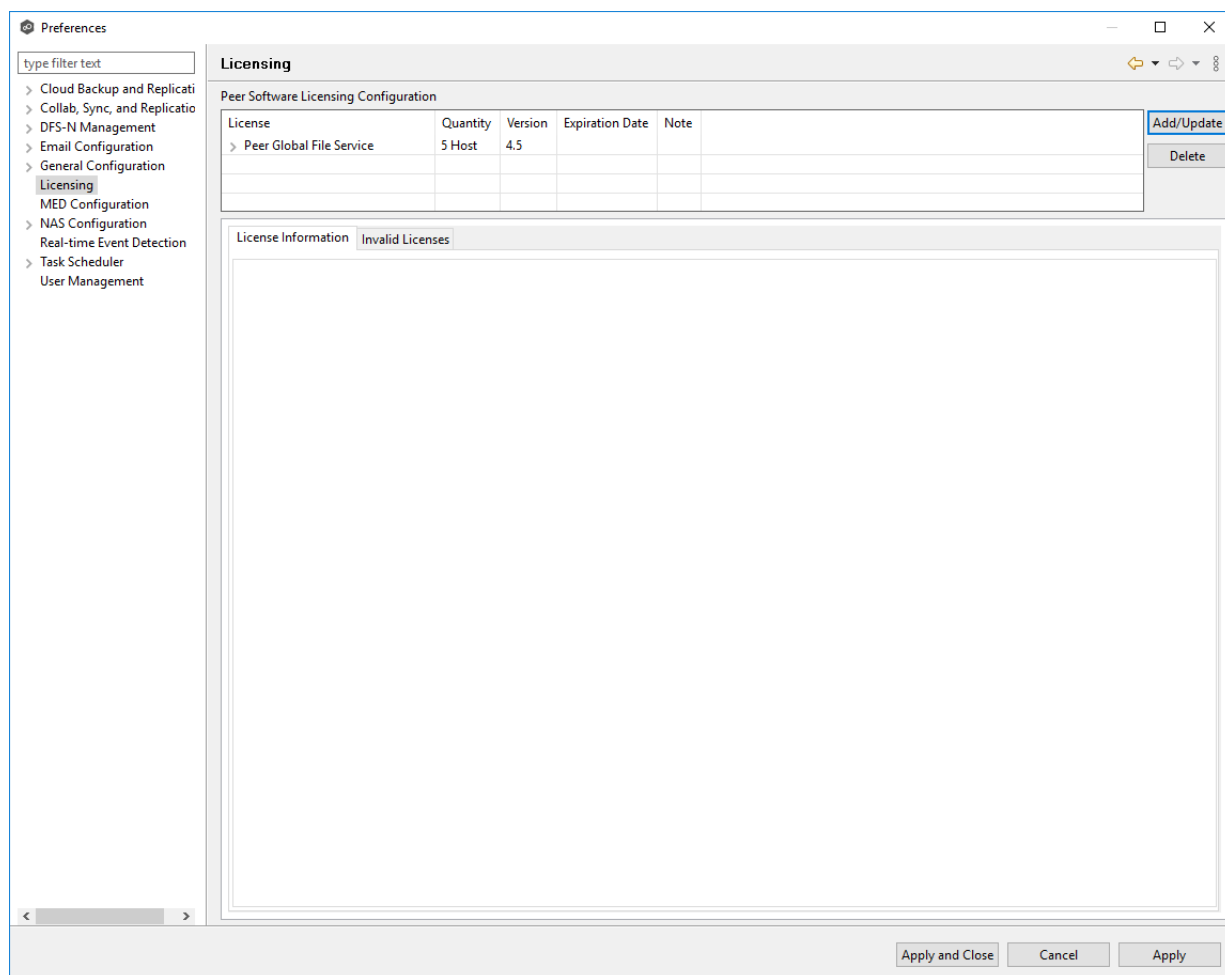
To install a new license file or upgrade an existing license:

1. From the **Window** menu, select **Preferences**.

The **Preferences** dialog appears.

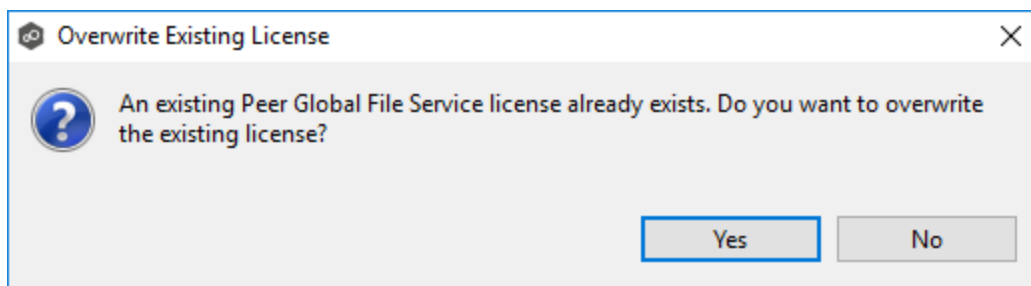
2. Select **Licensing** in the navigation tree.

Existing valid licenses are listed in the **Peer Software Licensing Configuration** table.



3. Click the **Add/Update** button to browse for a license file.
4. Select the license file, and then click **Open**.

If you are prompted with a message that an existing license already exists, click **Yes** to overwrite the existing license.

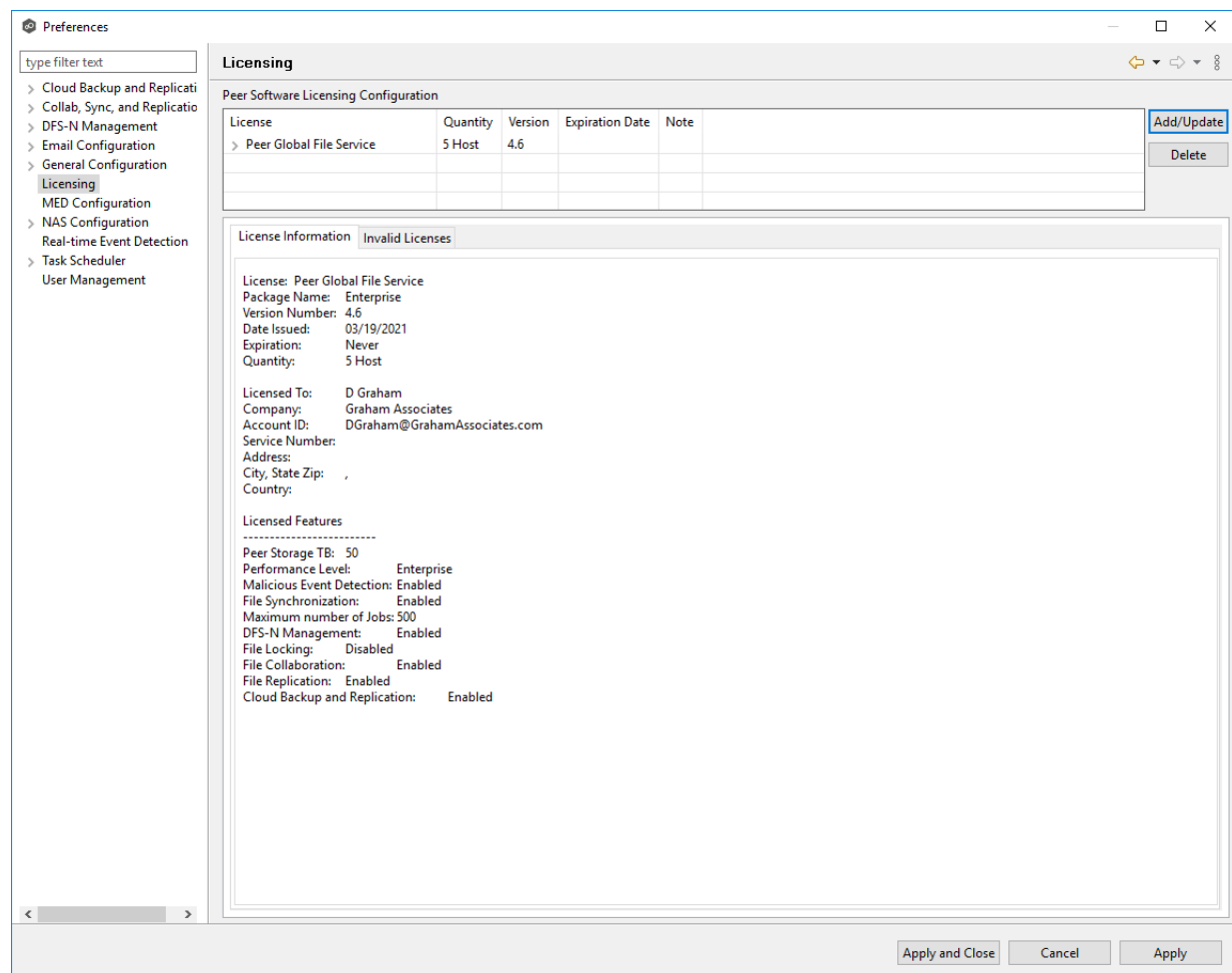


After successful installation of the license, it is listed in the table, along with the license quantity, version, and an expiration date (if applicable). You can now create, configure, and run jobs using the new license.

**Note:** You will need to restart existing jobs if any of the following applies:

- Software version is different (typically when upgrading to a new version).
- Software package level is different.
- New license is insufficient for the number of existing hosts.

5. Click the license in the table to view details about the license.



6. Click **OK** or **Apply**.

## Deleting a License File

To delete a license.

1. From the **Windows** menu, select **Preferences**.
2. Select **Licensing** in the navigation tree.
3. Select the license you want to delete.
4. Click the **Delete** button

Any job types enabled by that license will be hidden from Peer Management Center.

## MED Configuration

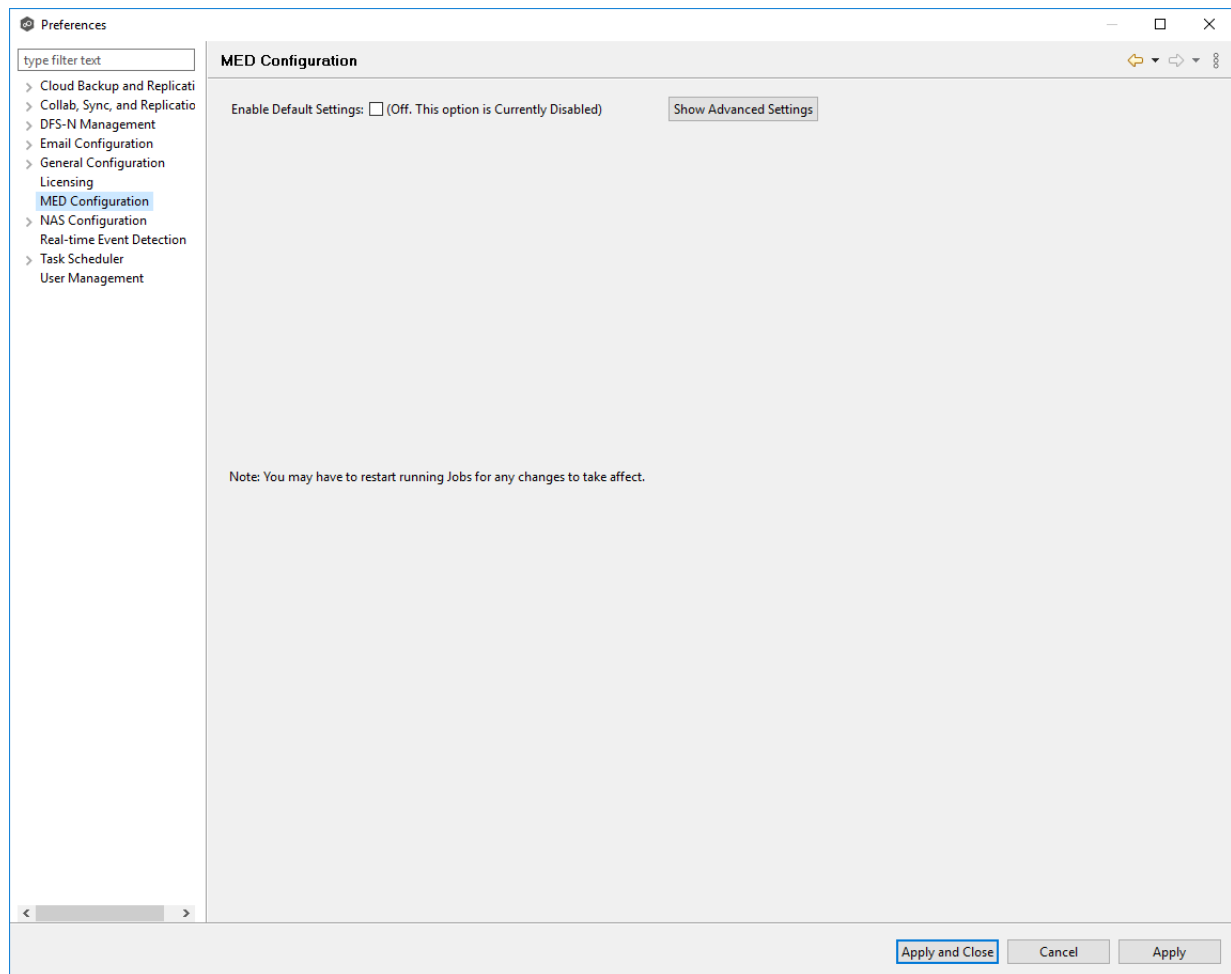
Peer's Malicious Event Detection (MED) real-time engine can spot unwanted activity being executed on storage platforms by ransomware, viruses, malware, hackers, or rogue users. MED technology provides alerting capabilities, as well as the ability to minimize the amount of encrypted or deleted content from being replicated to remote locations. Once MED is enabled and jobs are restarted, these capabilities apply to all jobs. For more information, see our knowledge base article [Introduction to Peer MED](#).

Peer MED deploys three different mechanisms for spotting malicious activity, each of which can be enabled and tuned independently. These settings are configured on a global level.

To view and modify these settings,

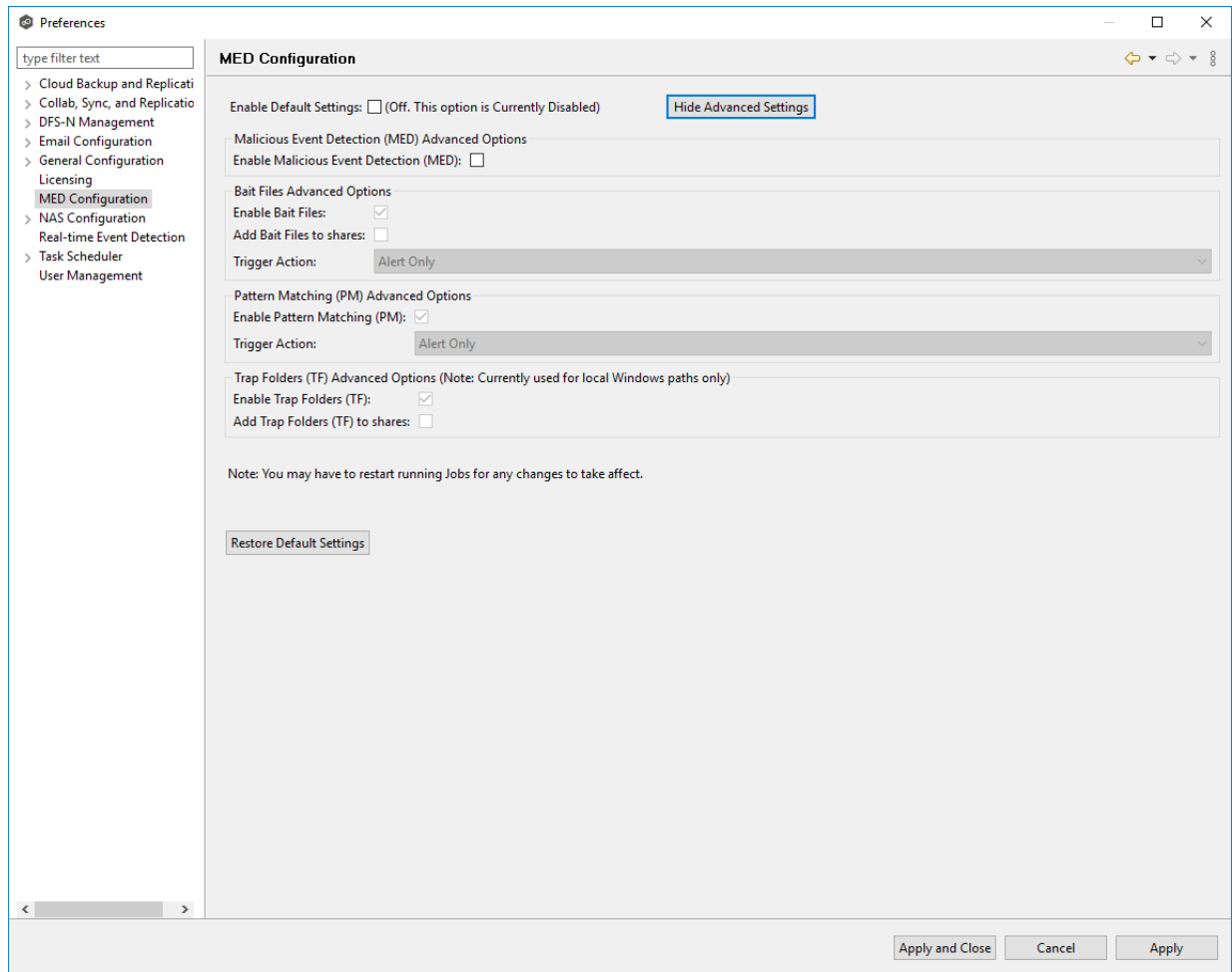
1. From the **Window** menu, select **Preferences**.
2. Select **MED Configuration** in the navigation tree.

The following page is displayed.



3. Select the **Enable Default Settings** or click **Show Advanced Settings**.

If you selected **Show Advanced Settings**, the following is displayed.



4. Modify the options as needed:

- [Primary MED Options](#)
- [Bait File Advanced Options](#)
- [Trap Folders Advanced Options](#)

5. Click **OK**.

## Primary MED Options

The main options are as follows:



Option	Description
<b>Enable Default Settings</b>	Enables/disables Peer MED using default settings. By default, all three MED mechanisms are enabled.
<b>Show/Hide Advanced Settings</b>	Shows/hides options for each of the three MED mechanisms.
<b>Enable Malicious Event Detection (MED)</b>	The master on/off switch for MED. If unchecked, all MED mechanisms will be disabled.
<b>Restore Default Settings</b>	Restores all defaults across the three MED mechanisms.

## Bait File Advanced Options

Bait files are files of common types, inserted into the file system in a way that hides them from users. Though hidden, these bait files are likely to be accessed by automated processes (like ransomware) or by mass deletions of entire folder structures. As soon as these files are touched, an action is triggered.

The options for bait files are:

Option	Description
<b>Enable Bait Files</b>	Enables/disables bait file creation and monitoring.
<b>Add Bait Files to shares</b>	At the start of each job, creates bait files under the root of each participant's configured watch directory. To see the watch directory for a job, review <a href="#">Host Participants and Directories</a> .
<b>Trigger Action</b>	Defines the action to take when MED detects malicious activity on a bait file. See <a href="#">Action Types</a> for more details on available actions.

## Action Types

For each MED mechanism, one of four actions can be configured on the detection of malicious activity. These actions are:

Action	Description
<b>Alert Only</b>	<p>Triggers an alert in Peer Management Center.</p> <p>If email alerts are configured for MED Alerts and enabled for a job, an email will also be sent. See <a href="#">Email Alerts</a> in the <a href="#">Basic Concepts</a> section for more information about email alerts.</p> <p>If SNMP traps are configured for MED Alerts and enabled for a job, an SNMP trap will also be sent. See <a href="#">SNMP Notifications</a> in the <a href="#">Basic Concepts</a> section for more information about SNMP notifications.</p>
<b>Alert and Disable Host</b>	<p>Triggers an alert while also removing the afflicted Agent from the job in which the malicious activity was detected. Once disabled, Agents will need to be manually re-enabled for collaboration to resume. See <a href="#">Re-enabling a Disabled Agent Within a Job</a> for details.</p>
<b>Alert and Stop Job</b>	<p>Triggers an alert while also stopping the job where the malicious activity was detected. Jobs will need to be restarted in order for collaboration to resume.</p>
<b>Alert, Disable Host and Stop Job</b>	<p>Triggers an alert, removes the afflicted Agent from the job where the malicious activity was detected, and stops the job. This option is the most aggressive and will require administrators to re-enable Agents as well as restart jobs. See <a href="#">Re-enabling a Disabled Agent Within a Job</a> for details.</p>

An example of an alert as displayed in Peer Management Center is as follows:

**Peerlet Advisory Alert Details**

Received Date:

03-12-2018 19:23:26

Severity:

FATAL

Category:

Event Detection

Host Name:

DelIT110a

Locally Created at:

03-12-2018 19:23:26

Message:

Malicious Event Detection (MED) - Bait File Alert (Alert Only: Please check for unwanted activity) Alert Message info=BAIT FILE ALERT appld=113, appSessionId=142 path= See Message Field msg=TriggerAlertFileFound: Path=\\svm9x-1\cifs1\Departments\Sales\pc-med\_bin\Doc\_000-med.docx - EventName: RENAME details=| Participant Detected=DelIT110a|Alert Message=TriggerAlertFileFound: Path=\\svm9x-1\cifs1\Departments\Sales\pc-med\_bin\Doc\_000-med.docx - EventName: RENAME|Time Detected=Mon Mar 12 19:23:26 EDT 2018|User Detected=MattM|IP Detected=Doc\_000-med.docx|Process Detected=SMBVersion=31|Share Detected=cifs1|Job Session ID=3248744344

Class Name:

WatchDirectoryOperations

App Session Key:

142

Error Code:

2520

Action:

Alert Only

Click outside of popup to close

## Trap Folders Advanced Options

On Windows file servers, Peer MED can be configured to create hidden, recursive folders that attempt to trap or slowdown ransomware as it enumerates a folder structure. As with the bait files, these folders cannot be seen by users but will be accessible by automated processes. If bait files (above) are enabled, a bait file will be placed within each trap folder, and an action will be triggered as soon as these files are touched.

Options for trap folders are:

Option	Description
<b>Enable Trap Folders</b>	Enables/disables the creation and monitoring of trap folders.

Option	Description
<b>Add Trap Folders to shares</b>	<p>At the start of each job, create trap folders under the root of each participant's configured watch directory. To see the watch directory for a job, review <a href="#">Host Participants and Directories</a>.</p> <p>Note: Trap Folders will only be used with participants that are Windows file servers. As such, these settings will not apply to any other enterprise NAS device.</p>

## NAS Configuration

This section contains information about configuring your NAS for use with Peer Global File System:

- [Dell EMC Configurations](#)
- [NetApp 7-Mode Configurations](#)
- [NetApp cDOT Configurations](#)
- [Nutanix Configurations](#)

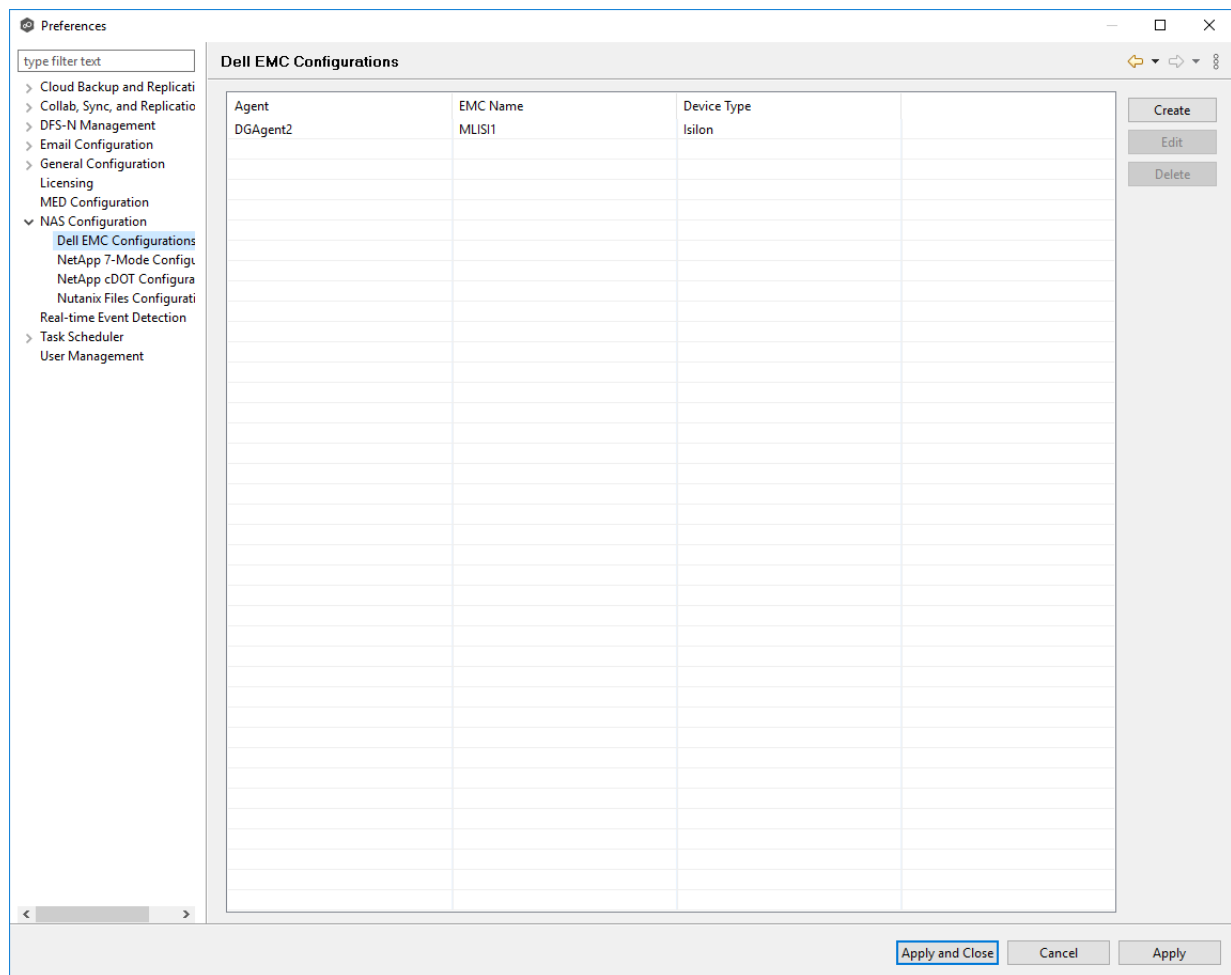
### Dell EMC Configurations

Peer Management Center supports the ability to include content from CIFS/SMB shares on one or more Dell EMC storage devices within most available job types. These Dell EMC devices can be running Isilon, Unity, or VNX. For detailed information about Dell EMC prerequisites, see [Dell EMC Prerequisites](#).

To create a new Dell EMC configuration:

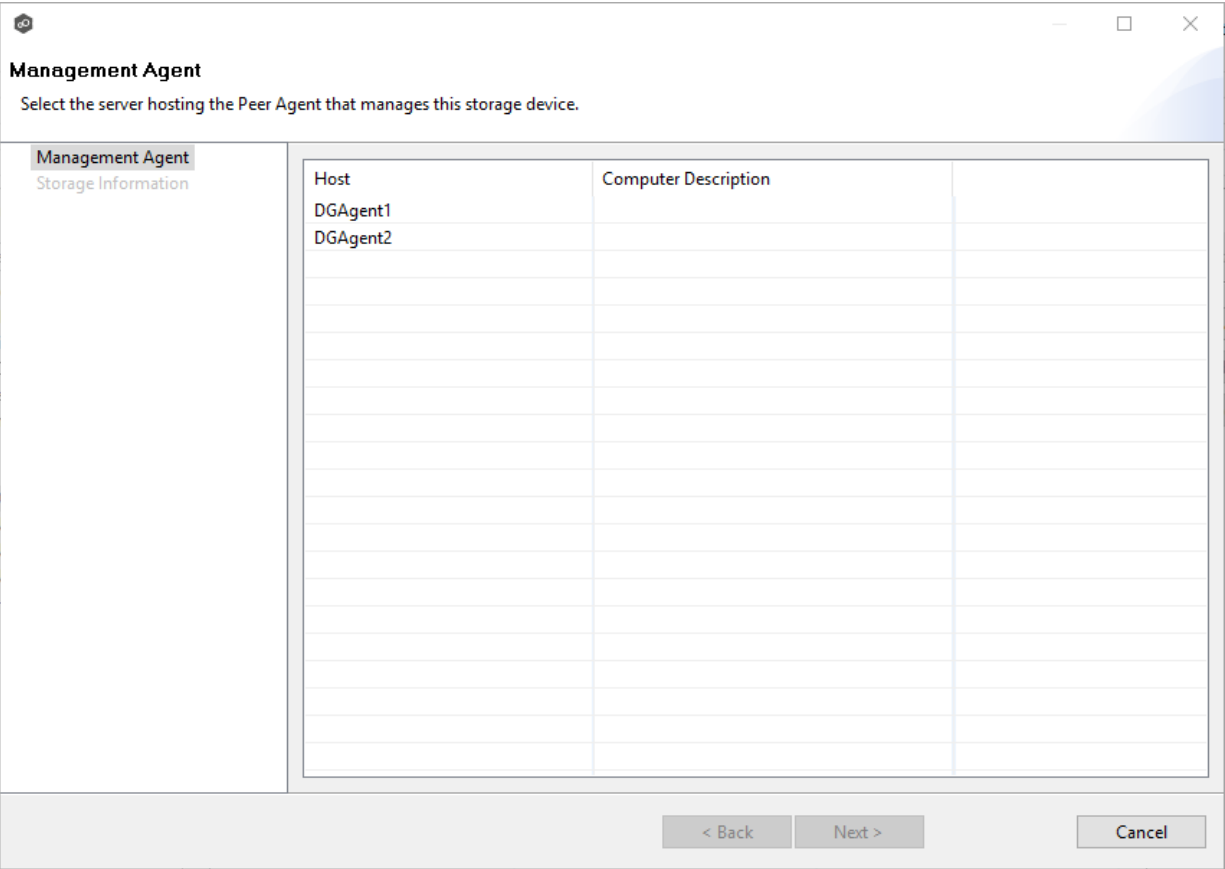
1. Select **Preferences** from the **Window** menu.  
  
The **Preferences** dialog appears.
2. Select **NAS Configuration** in the navigation tree.
3. Select **Dell EMC Configurations**.

The **Dell EMC Configurations** page is displayed. It lists existing configurations.



4. Click the **Create** button.

The **Management Agent** page appears.



5. Select a Management Agent, and then click **Next**.

The **Storage Information** page appears. The fields in the **Credentials** section vary, depending on the selected EMC platform type; VNX is selected by default.

**Storage Information**  
Enter the required information to connect to the storage

Management Agent  
Storage Information

**Credentials**

Device Type: VNX

\*CIFS Server Name:

\*Control Station Username:

\*Control Station Password:

\*Control Station IP:

Advanced

Validate You must enter the name.

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC VNX/Celerra environments.

< Back Next > Cancel

6. Select the device type, and then enter the required values in **Credentials**:

[Dell EMC Isilon Credentials](#)

[Dell EMC Unity Credentials](#)

[Dell EMC VNX Credentials](#)

7. (Optional) Click the **Advanced** button if you want to specify advanced options, and then enter the required values:

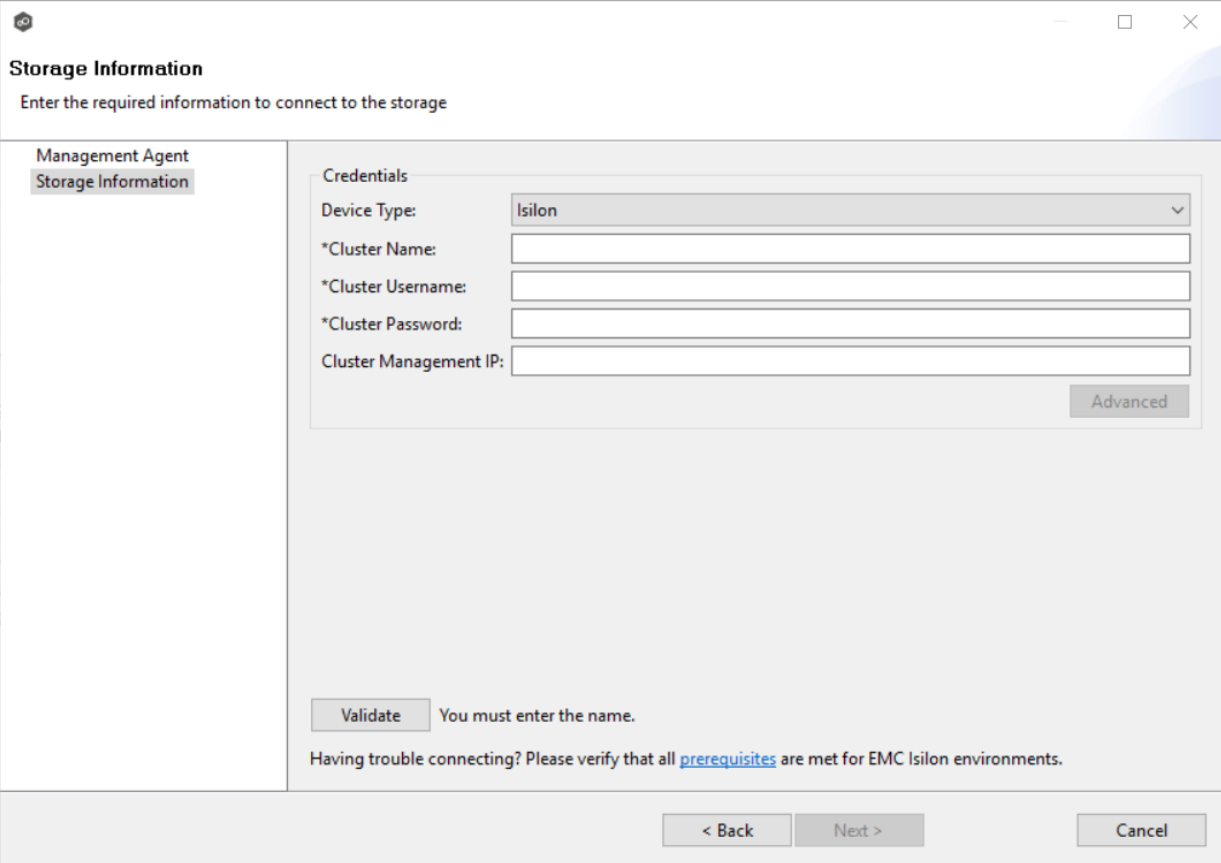
[Dell EMC Isilon Advanced Options](#)

[Dell EMC Unity Advanced Options](#)

[Dell EMC VNX Advanced Options](#)

8. Click **Validate**.
9. Click **Next**.
10. Click **OK**.

1. Enter the required values.



**Storage Information**  
Enter the required information to connect to the storage

Management Agent  
Storage Information

**Credentials**

Device Type: Isilon

\*Cluster Name:

\*Cluster Username:

\*Cluster Password:

Cluster Management IP:

Advanced

Validate You must enter the name.

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Isilon environments.

< Back Next > Cancel

<b>Cluster Name</b>	Enter the name of the EMC Isilon cluster hosting the data to be replicated.
<b>Cluster Username</b>	Enter the user name for the account managing the EMC Isilon cluster.
<b>Cluster Password</b>	Enter the password for account managing the EMC Isilon cluster.



<b>Cluster Management IP</b>	Enter the IP address of the system used to manage the EMC Isilon cluster. Required only if multiple Access Zones are in use on the cluster.
------------------------------	---

2. (Optional) Click [Advanced](#) and enter the required values.
3. Click **Validate**.
4. Click **Finish**.

#### Dell EMC Isilon Advanced Options

The options are divided into two groups:

- [EMC Isilon Options for this Job](#)
- [Advanced Settings](#)

EMC Isilon Options

EMC Isilon Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced Settings for Agent DGAgent1 and EMC Isilon:ADFADF

Filtered IP Addresses:

Nodes:

Audit Cluster Name:

Cluster IP:

Cluster Port:

\*Cluster Username:

\*Cluster Password:

Cluster Access Zone:

Validate Cluster: ☒

Update Isilon CEE Log Time: ☒

**NOTE: Any changes made to these Advanced EMC Settings will be used with every other session in which this CEE Event Server is connecting with an EMC storage device.**

OK Cancel

## EMC Isilon Options for this Job

The following configuration options are available for Dell EMC Isilon devices:

<b>Filter open/close events from these users</b>	A comma-separated list of user names to exclude from access event detection. For example, if "USER1" is excluded, any access event activity generated by USER1 will be ignored, e.g., file is opened and closed.
<b>Filter all events from these users</b>	A comma-separated list of user names to exclude from all event detection. For example, if "USER"1 is excluded, any activity generated by USER1 will be ignored, e.g., file is open and modified.

<b>Filter events from these IP Addresses</b>	A comma-separated list of IP addresses to exclude from all event detection. For example, if "192.168.0.100" is excluded, any activity generated by 192.168.0.100 will be ignored, e.g., file is open and modified.
<b>Access Event Suppression Time</b>	Represents the number of seconds that an open event will be delayed before being processed. Used to help reduce the amount of chatter generated by Windows clients when mousing over files in Windows Explorer. The default value is -1, which will be adjusted based on the selected NAS platform. A value of 0 will allow for dynamic changes to the amount of time that an open event will be delayed based on the load of the system.

## Advanced Settings

The following advanced settings are available for Dell EMC Isilon devices:

<b>Filtered IP Addresses</b>	Events generated from these IP addresses will be filtered. It is recommended that the IP address of the CEE Server is added to this list.
<b>Nodes</b>	Comma-delimited listed of additional node IP address to query for open files. These addresses must be accessible from the CEE Server where the Agent is running.
<b>Cluster IP</b>	The cluster IP address of the Isilon system.
<b>Audit Cluster Name</b>	The hostname that is set in the Isilon audit system configuration.
<b>Cluster Port</b>	The cluster port number of the Isilon system. Default value is 8080.
<b>Cluster UsernameT</b>	The user name used to sign into the Isilon cluster.
<b>Cluster Password</b>	The password used to sign into the Isilon cluster.
<b>Validate Cluster</b>	If enabled, the Isilon cluster will be validated both on registration and periodically by a maintenance thread.

**Update  
Isilon CEE  
Log Time**

If enabled, the audit log time on the Isilon cluster will be set to the start time of the first job to communicate with this Isilon cluster.

1. Enter the required values.

**Storage Information**  
Enter the required information to connect to the storage

Management Agent  
Storage Information

Credentials

Device Type: Unity

\*CIFS Server Name:

\*Unisphere Username:

\*Unisphere Password:

\*Unisphere Management IP:

Advanced

Validate You must enter the name.

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Unity environments.

< Back Next > Cancel

**CIFS  
Server  
Name**

Enter the name of the CIFS server hosting the data to be replicated.

**Unisphe  
re  
Userna  
me**

Enter the user name for the Unisphere account managing the Unity storage device.

<b>Unisphere Password</b>	Enter the password for the Unisphere account managing the Unity storage device.
<b>Unisphere Management IP</b>	Enter the IP address of the Unisphere system used to manage the Unity storage device. This should not point to the CIFS server.

2. (Optional) Click [Advanced](#) and enter the required values.
3. Click **Validate**.
4. Click **Finish**.

#### Dell EMC Unity Advanced Options

The options are divided into two groups:

- [EMC Unity Options for this Job](#)
- [Advanced Settings](#)

EMC Unity Options

EMC Unity Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced Settings for Agent DGAgent1 and EMC Unity:ADSADSFAP

Filtered IP Addresses:

\*Unisphere Management IP:

Unisphere Management Port:

\*Unisphere Username:

\*Unisphere Password:

Validate Unisphere: ☒

**NOTE: Any changes made to these Advanced EMC Settings will be used with every other session in which this CEE Event Server is connecting with an EMC storage device.**

OK Cancel

## EMC Unity Options for this Job

The following configuration options are available for EMC Unity devices:

<b>Filter open/close events from these users</b>	A comma-separated list of user names to exclude from access event detection. For example, if "USER1" is excluded, any access event activity generated by USER1 will be ignored, e.g., file is opened and closed.
<b>Filter all events from these users</b>	A comma-separated list of user names to exclude from all event detection. For example, if "USER"1 is excluded, any activity generated by USER1 will be ignored, e.g., file is open and modified.
<b>Filter events from these IP Addresses</b>	A comma-separated list of IP addresses to exclude from all event detection. For example, if "192.168.0.100" is excluded, any activity generated by 192.168.0.100 will be ignored, e.g., file is open and modified.

<b>Access Event Suppression Time</b>	Represents the number of seconds that an open event will be delayed before being processed. Used to help reduce the amount of chatter generated by Windows clients when mousing over files in Windows Explorer. The default value is -1, which will be adjusted based on the selected NAS platform. A value of 0 will allow for dynamic changes to the amount of time that an open event will be delayed based on the load of the system.
--------------------------------------	---

## Advanced Settings

The following advanced settings are available for Dell EMC Unity devices:

<b>Filtered IP Addresses</b>	Events generated from these IP addresses will be filtered. It is recommended that the IP address of the CEE Server is added to this list.
<b>Unisphere Management IP</b>	The Unisphere Management IP address of the Unity system. This address is used for making API calls to validate configuration.
<b>Unisphere Management Port</b>	The Unisphere Management port number of the Unity system. Default value is 443.
<b>Unisphere Username</b>	The user name used to sign into Unisphere.
<b>Unisphere Password</b>	The password used to sign into Unisphere.
<b>Validate Unisphere</b>	If enabled, Unisphere settings will be validated both on registration and periodically by a maintenance thread.

1. Enter the required values.

The screenshot shows a window titled "Storage Information" with a subtitle "Enter the required information to connect to the storage". On the left, there is a sidebar with two tabs: "Management Agent" and "Storage Information", with the latter being selected. The main area contains a "Credentials" section with the following fields: "Device Type" (a dropdown menu showing "VNX"), "\*CIFS Server Name:" (a text input field), "\*Control Station Username:" (a text input field), "\*Control Station Password:" (a text input field), and "\*Control Station IP:" (a text input field). An "Advanced" button is located to the right of the IP field. At the bottom of the main area, there is a "Validate" button and a message: "You must enter the name." Below this, a note states: "Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC VNX/Celerra environments." At the very bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

<b>CIFS Server Name</b>	Enter the name of the CIFS Server hosting the data to be replicated.
<b>Control Station Username</b>	Enter the user name for the Control Station account managing the VNX/Celerra storage device.
<b>Control Station Password</b>	Enter the password for the Control Station account managing the VNX/Celerra storage device.



<b>Control Station IP</b>	Enter the IP address of the Control Station system used to manage the VNX/Celerra storage device. This should not point to the CIFS Server.
---------------------------	---

2. (Optional) Click [Advanced](#) and enter the required values.
3. Click **Validate**.
4. Click **Finish**.

#### Dell EMC VNX/Celerra Advanced Options

The options are divided into two groups:

- [EMC VNX Options for this Job](#)
- [Advanced Settings](#)

EMC VNX Options

EMC VNX Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced Settings for Agent DGAgent1 and EMC VNX:ADFAF

Filtered IP Addresses:

\*Control Station IP:

Control Station Port:

\*Control Station Username:

\*Control Station Password:

Validate Control Station: ☒

**NOTE: Any changes made to these Advanced EMC Settings will be used with every other session in which this CEE Event Server is connecting with an EMC storage device.**

OK Cancel

## EMC VNX/Celerra Options for this Job

The following configuration options are available for Dell EMC VNX devices:

<b>Filter open/close events from these users</b>	A comma-separated list of user names to exclude from access event detection. For example, if "USER1" is excluded, any access event activity generated by USER1 will be ignored, e.g., file is opened and closed.
<b>Filter all events from these users</b>	A comma-separated list of user names to exclude from all event detection. For example, if "USER"1 is excluded, any activity generated by USER1 will be ignored, e.g., file is open and modified.
<b>Filter events from these IP Addresses</b>	A comma-separated list of IP addresses to exclude from all event detection. For example, if "192.168.0.100" is excluded, any activity generated by 192.168.0.100 will be ignored, e.g., file is open and modified.

<b>Access Event Suppression Time</b>	Represents the number of seconds that an open event will be delayed before being processed. Used to help reduce the amount of chatter generated by Windows clients when mousing over files in Windows Explorer. The default value is -1, which will be adjusted based on the selected NAS platform. A value of 0 will allow for dynamic changes to the amount of time that an open event will be delayed based on the load of the system.
--------------------------------------	---

## Advanced Settings

The following advanced settings are available for EMC VNX/Celerra devices:

<b>Filtered IP Addresses</b>	Events generated from these IP addresses will be filtered. It is recommended that the IP address of the CEE Server is added to this list.
<b>Control Station IP</b>	The Control Station IP address of the VNX/Celerra system.
<b>Control Station Port</b>	The Control Station Port number of the VNX/Celerra system. The default value is 443.
<b>Control Station Username</b>	The user name used to sign into the VNX/Celerra Control Station.
<b>Control Station Password</b>	The password used to sign into the VNX/Celerra Control Station.
<b>Validate Control Station</b>	If enabled, the VNX/Celerra Control Station will be validated both on registration and periodically by a maintenance thread.

### NetApp 7-Mode Configurations

Peer Management Center supports the ability to include content from CIFS/SMB shares on one or more NetApp storage devices within most available job types. These NetApp devices can be running Data ONTAP 7-Mode or clustered Data ONTAP. In order to work with NetApp devices, Peer Management Center leverages the FPolicy API built into the NetApp device. For detailed information about NetApp prerequisites and configuration, see [NetApp Prerequisites](#).

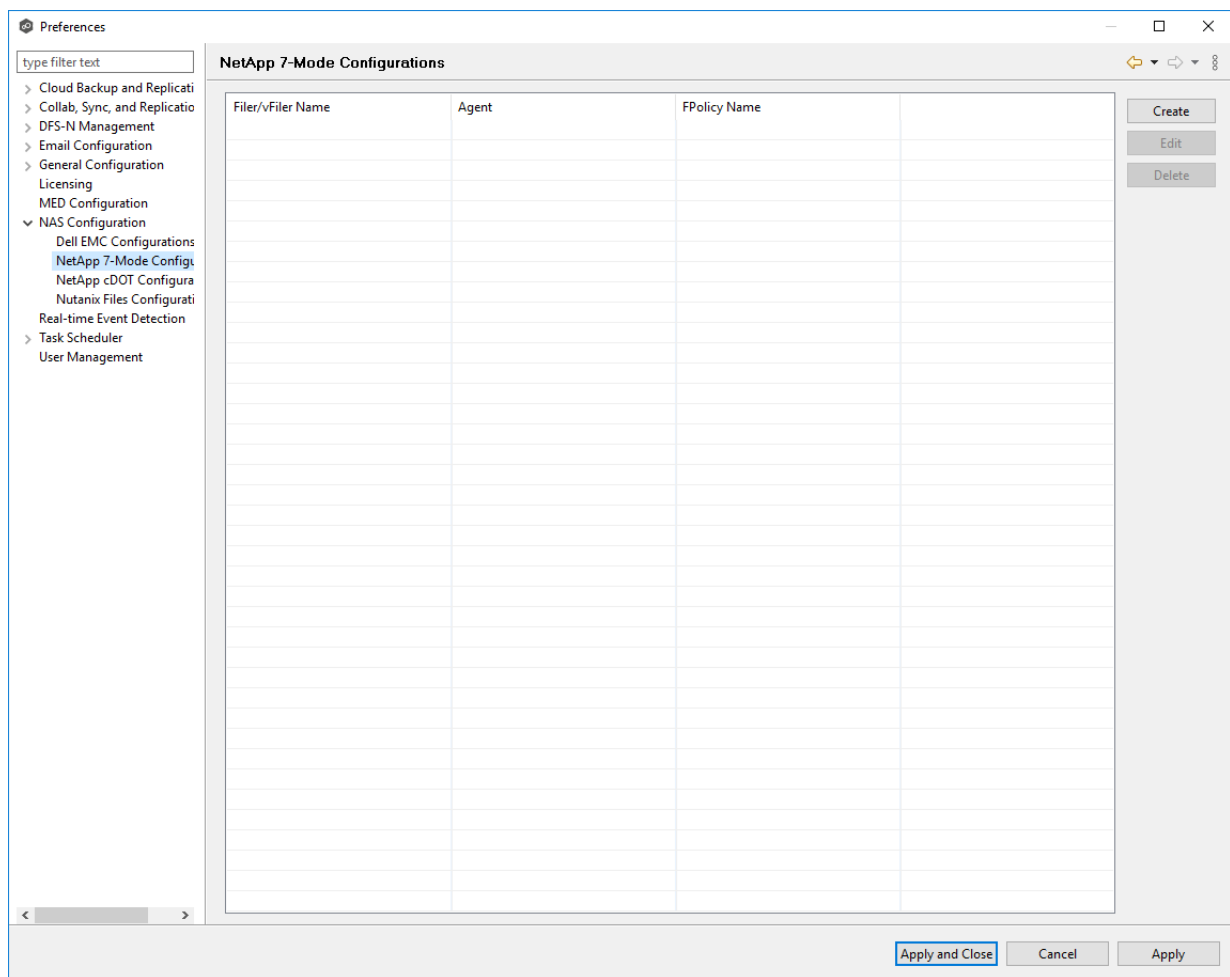
To create a new NetApp 7-Mode configuration:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

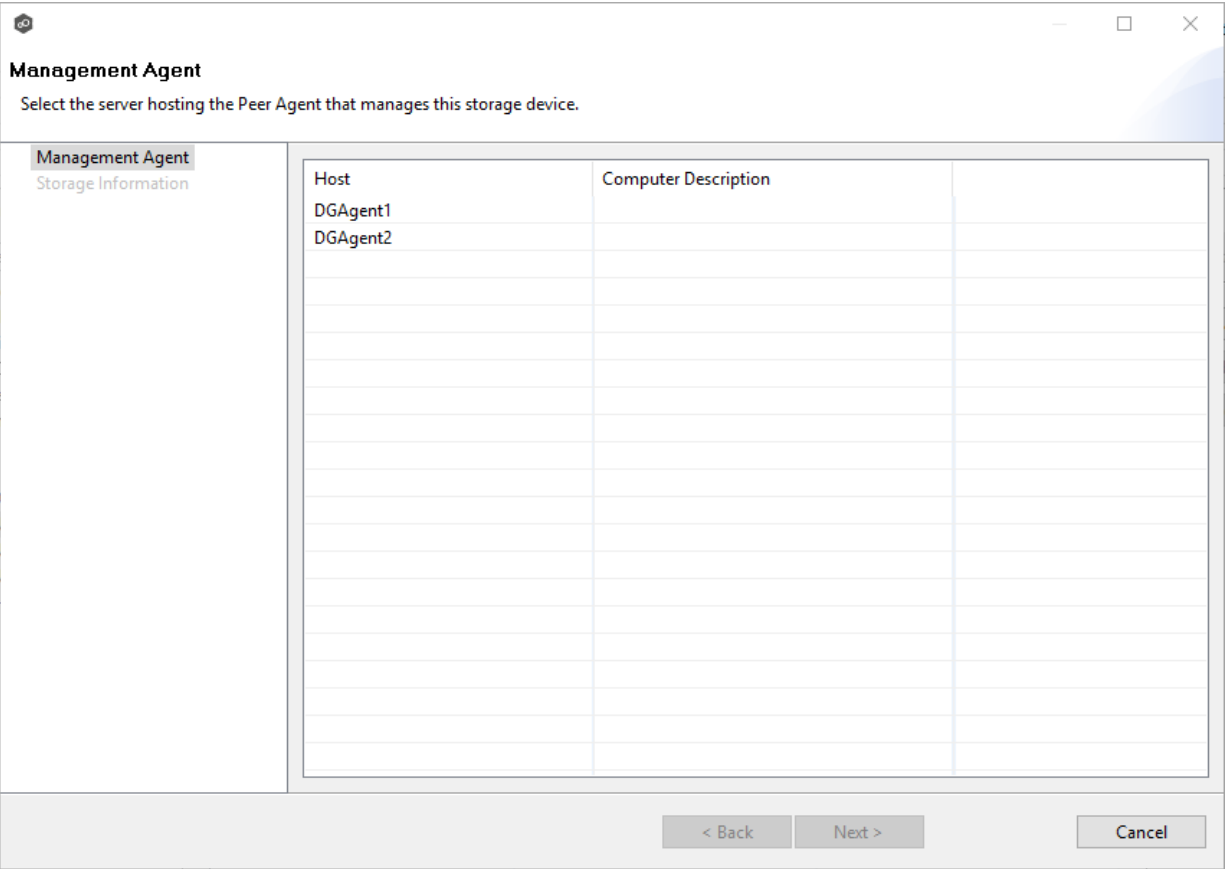
2. Select **NAS Configuration** in the navigation tree.
3. Select **NetApp 7-Mode Configurations**.

The **NetApp 7-Mode Configurations** page is displayed. It lists existing configurations.



4. Click the **Create** button.

The **Management Agent** page appears.



5. Select a Management Agent, and then click **Next**.

The **Storage Information** page appears.

**Storage Information**  
Enter the required information to connect to the storage

Management Agent  
Storage Information

**Credentials**  
\*Filer/vFiler Name:

Advanced

Validate You must enter the name.

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp 7-Mode environments.

< Back Next > Cancel

6. Enter the required values in **Credentials**.

<b>File r Na me</b>	Enter the name of the NetApp 7-Mode filer or vFiler hosting the data to be replicated.
---------------------------------	--

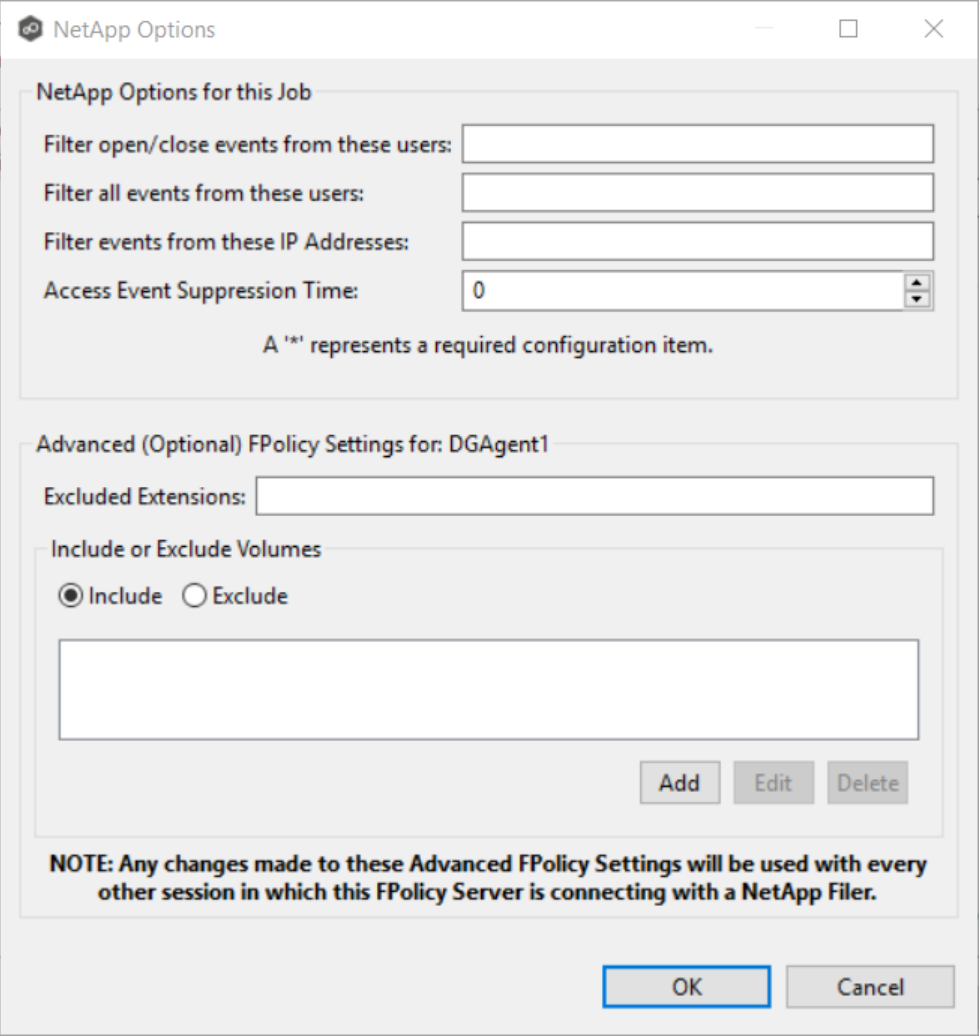
7. (Optional) Click the **Advanced** button if you want to specify advanced options, and then enter the required values:

[NetApp 7-Mode Advanced Options](#)

8. Click **Validate**.
9. Click **Next**.
10. Click **OK**.

The options are divided into two groups:

- [NetApp Options for this Job](#)
- [Advanced Settings](#)



The image shows a Windows-style dialog box titled "NetApp Options". It is divided into two main sections. The first section, "NetApp Options for this Job", contains four input fields: "Filter open/close events from these users:", "Filter all events from these users:", "Filter events from these IP Addresses:", and "Access Event Suppression Time:" (which has a numeric spinner set to 0). Below these fields is a note: "A '\*' represents a required configuration item." The second section, "Advanced (Optional) FPolicy Settings for: DGAgent1", contains an "Excluded Extensions:" input field, a section for "Include or Exclude Volumes" with radio buttons for "Include" (selected) and "Exclude", and a large empty text area for volume names. At the bottom of this section are "Add", "Edit", and "Delete" buttons. A note at the bottom of the dialog states: "NOTE: Any changes made to these Advanced FPolicy Settings will be used with every other session in which this FPolicy Server is connecting with a NetApp Filer." At the very bottom are "OK" and "Cancel" buttons.

## NetApp Options for this Job

The following configuration options are available for NetApp 7-Mode devices:

<b>Filter open/close</b>	A comma-separated list of user names to exclude from access event detection. For example, if "USER1" is excluded, any
--------------------------	---

<b>events from these users</b>	access event activity generated by USER1 will be ignored, e.g., file is opened and closed.
<b>Filter all events from these users</b>	A comma-separated list of user names to exclude from all event detection. For example, if "USER"1 is excluded, any activity generated by USER1 will be ignored, e.g., file is open and modified.
<b>Filter events from these IP Addresses</b>	A comma-separated list of IP addresses to exclude from all event detection. For example, if "192.168.0.100" is excluded, any activity generated by 192.168.0.100 will be ignored, e.g., file is open and modified.
<b>Access Event Suppression Time</b>	Represents the number of seconds that an open event will be delayed before being processed. Used to help reduce the amount of chatter generated by Windows clients when mousing over files in Windows Explorer. The default value is -1, which will be adjusted based on the selected NAS platform. A value of 0 will allow for dynamic changes to the amount of time that an open event will be delayed based on the load of the system.

## Advanced Settings

<b>Excluded Extensions</b>	<p>Extensions entered here are excluded from event detection on the NetApp Filer. Values are comma separated and must not contain any periods.</p> <p>FPolicy enables you to restrict a policy to a certain list of file extensions by excluding extensions that need to be screened.</p> <p>Note: The maximum length of a file name extension supported for screening is 260 characters. Screening by extensions is based only on the characters after the last period (.) in the file name. For example, for a file named fle1.txt.name.jpg, file access notification takes place only if a file policy is configured for the jpg extension.</p>
<b>Include or Exclude Volumes</b>	<p>List all volumes on the NetApp Filer to exclude or include based on selected choice.</p> <p>FPolicy enables you to restrict a policy to a certain list of volumes by including or excluding volumes that need to be screened.</p> <p>Using the include list, you can request notifications for the specified volume list. Using the exclude list, you can request</p>



notifications for all volumes except the specified volume list. However, by default, both the include and exclude list are empty.

You can use the question mark (?) or asterisk (\*) wildcard characters to specify the volume. The question mark (?) wildcard character stands for a single character. For example, entering vol? in a list of volumes that contain vol1, vol2, vol23, vol4, will result in only vol1 and vol2 being matched.

The asterisk (\*) wildcard character stands for any number of characters that contain the specified string. Entering \*test\* in a list of volumes to exclude from file screening excludes all volumes that contain the string such as test\_vol and vol\_test.

## NetApp cDOT Configurations

Peer Management Center supports the ability to include content from CIFS/SMB shares on one or more NetApp storage devices within most available job types. These NetApp devices can be running Data ONTAP 7-Mode or clustered Data ONTAP. In order to work with NetApp devices, Peer Management Center leverages the FPolicy API built into the NetApp device. For detailed information about NetApp prerequisites and configuration, see [NetApp Prerequisites](#).

To create a new NetApp cDOT configuration:

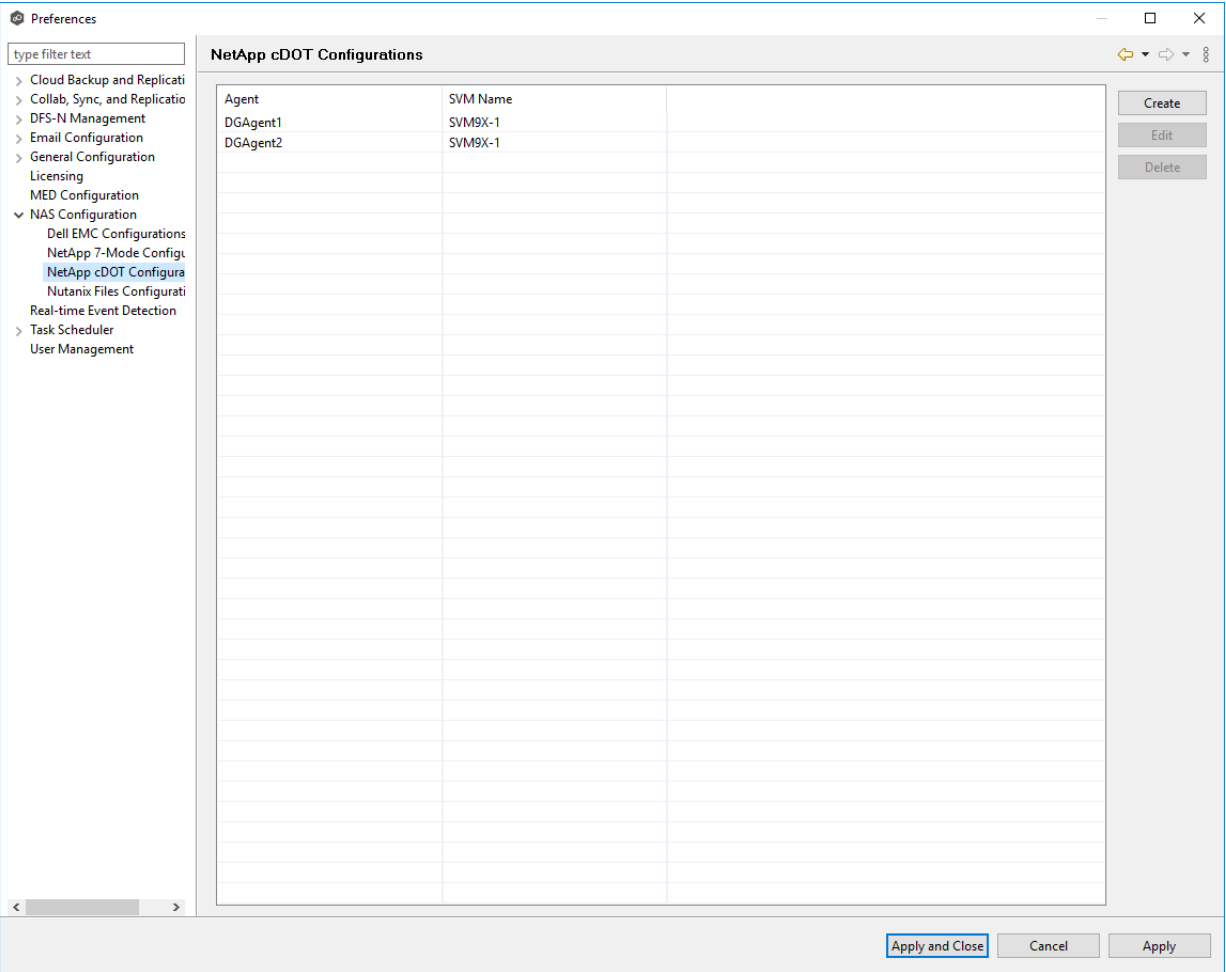
1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Select **NAS Configuration** in the navigation tree.

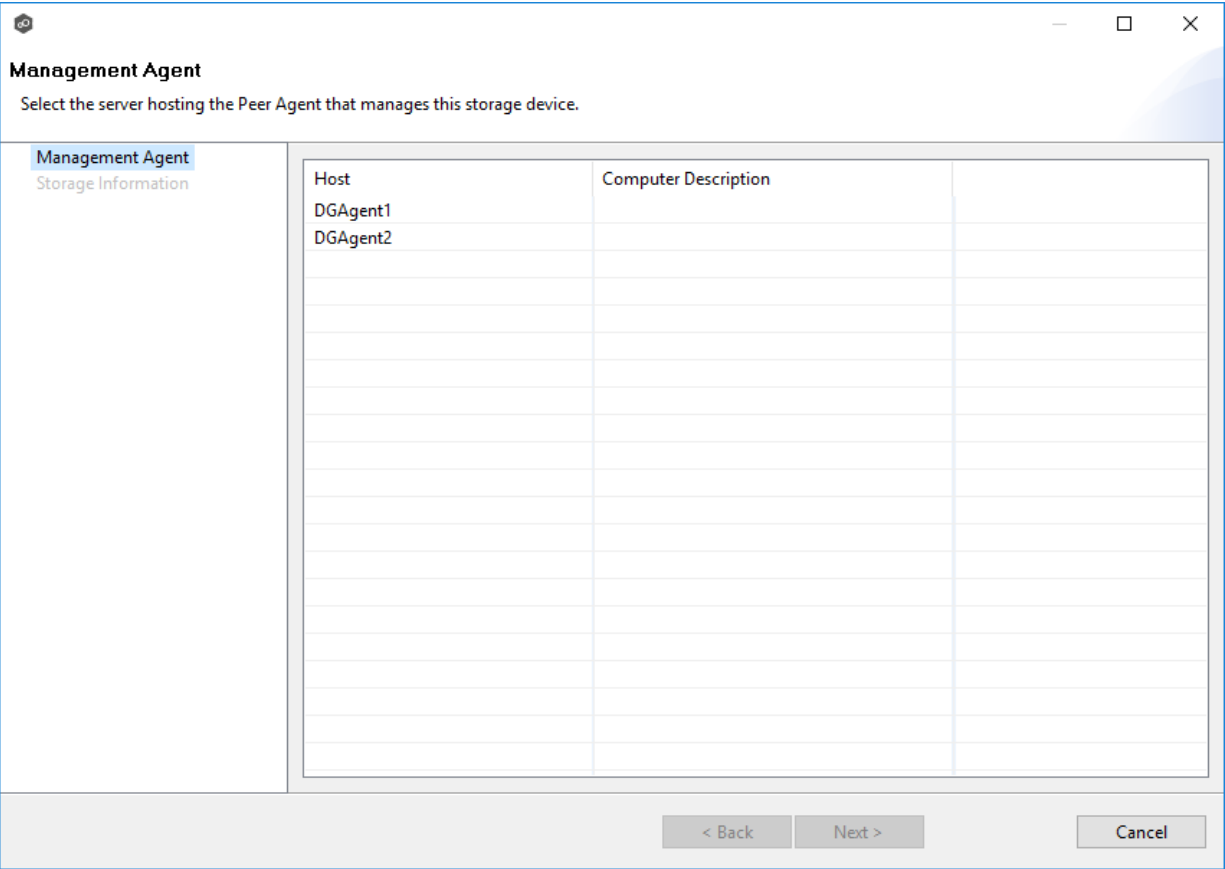
3. Select **NetApp cDot Configurations**.

The **NetApp cDOT Configurations** page is displayed. It lists existing configurations.



4. Click the **Create** button.

The **Management Agent** page appears.



5. Select a Management Agent, and then click **Next**.

The **Storage Information** page appears.

**Storage Information**  
Enter the required information to connect to the storage

Management Agent  
Storage Information

**Credentials**

\*SVM Name:

\*SVM User Name:

\*SVM Password:

SVM Management IP:

\*Peer Agent IP:

Advanced

Validate You must enter the name.

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp ONTAP/cDOT environments.

< Back Next > Cancel

6. Enter the required values in **Credentials**.

<b>SVM Name</b>	Enter the name of the Storage Virtual Machine hosting the data to be replicated.
<b>SVM Username</b>	Enter the user name for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Password</b>	Enter the password for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Management IP</b>	Enter the IP address used to access the management API of the NetApp Storage Virtual Machine. If the data LIFs (Logical Interfaces) corresponding to the SVM Name above already allow management access, this field is not required.

<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Storage Virtual Machine. The Storage Virtual Machine must be able to route traffic to this IP address. If the IP address you want does not appear, manually enter the address.
----------------------	---

7. (Optional) Click the **Advanced** button if you want to specify advanced options and enter the required values:

[NetApp cDOT Advanced Options](#)

8. Click **Validate**.
9. Click **Next**.
10. Click **OK**.

The options are divided into two groups:

- [NetApp Options for this Job](#)

- [Advanced Settings](#)

**NetApp Options**

**NetApp Options for this Job**

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

**Advanced FPolicy cDOT Settings for host: DGAgent1 and SVM: SFGSFGSFG**

\*SVM Username:

\*SVM Password:

SVM Management IP:

\*Agent IP for SVM Conn.:

Filtered Extensions:

Admin Share Override:

**NOTE: Any changes made to these Advanced FPolicy cDOT Settings will be used with every other session in which this FPolicy Server is connecting to the same Storage Virtual Machine.**

**OK** **Cancel**

## NetApp Options for this Job

The following configuration options are available for NetApp cDOT devices:

<b>Filter open/close events from these users</b>	A comma-separated list of user names to exclude from access event detection. For example, if "USER1" is excluded, any access event activity generated by USER1 will be ignored, e.g., file is opened and closed.
<b>Filter all events from these users</b>	A comma-separated list of user names to exclude from all event detection. For example, if "USER"1 is excluded, any activity generated by USER1 will be ignored, e.g., file is open and modified.
<b>Filter events from</b>	A comma-separated list of IP addresses to exclude from all event detection. For example, if "192.168.0.100" is excluded, any

<b>these IP Addresses</b>	activity generated by 192.168.0.100 will be ignored, e.g., file is open and modified.
<b>Access Event Suppression Time</b>	Represents the number of seconds that an open event will be delayed before being processed. Used to help reduce the amount of chatter generated by Windows clients when mousing over files in Windows Explorer. The default value is -1, which will be adjusted based on the selected NAS platform. A value of 0 will allow for dynamic changes to the amount of time that an open event will be delayed based on the load of the system.

## Advanced Settings

<b>SVM Username</b>	The account name of the VSAdmin or similar account on the SVM that has the appropriate access to ONTAPI.
<b>SVM Password</b>	The password of the VSAdmin or similar account on the SVM that has the appropriate access to ONTAPI. This value will be encrypted.
<b>SVM Management IP (optional)</b>	If the primary data LIF for the SVM (whose IP address is registered in DNS) does not support management calls, enter the management IP address of SVM.
<b>Agent IP for SVM Conn.</b>	The IP address over which this Peer Agent will connect to the configured SVM. This MUST be an IP address.
<b>Filtered Extensions</b>	A comma separated list of file extensions to exclude (without a leading asterisk (*)).
<b>Admin Share Override</b>	Enter the administrative-type share that you created on the cDOT SVM. To take advantage of performance improvements when using this option, the share must be created at the root of the SVM's namespace (/). Ideally it should be named to something similar to PMCShare\$ to prevent users from being able to see it.

## Nutanix Files Configurations

Peer Management Center supports the ability to include content from CIFS/SMB shares on one or more Nutanix Files (formerly Acropolis File Services or AFS) clusters within most available job types. For detailed information about Nutanix prerequisites, see [Nutanix Prerequisites](#).

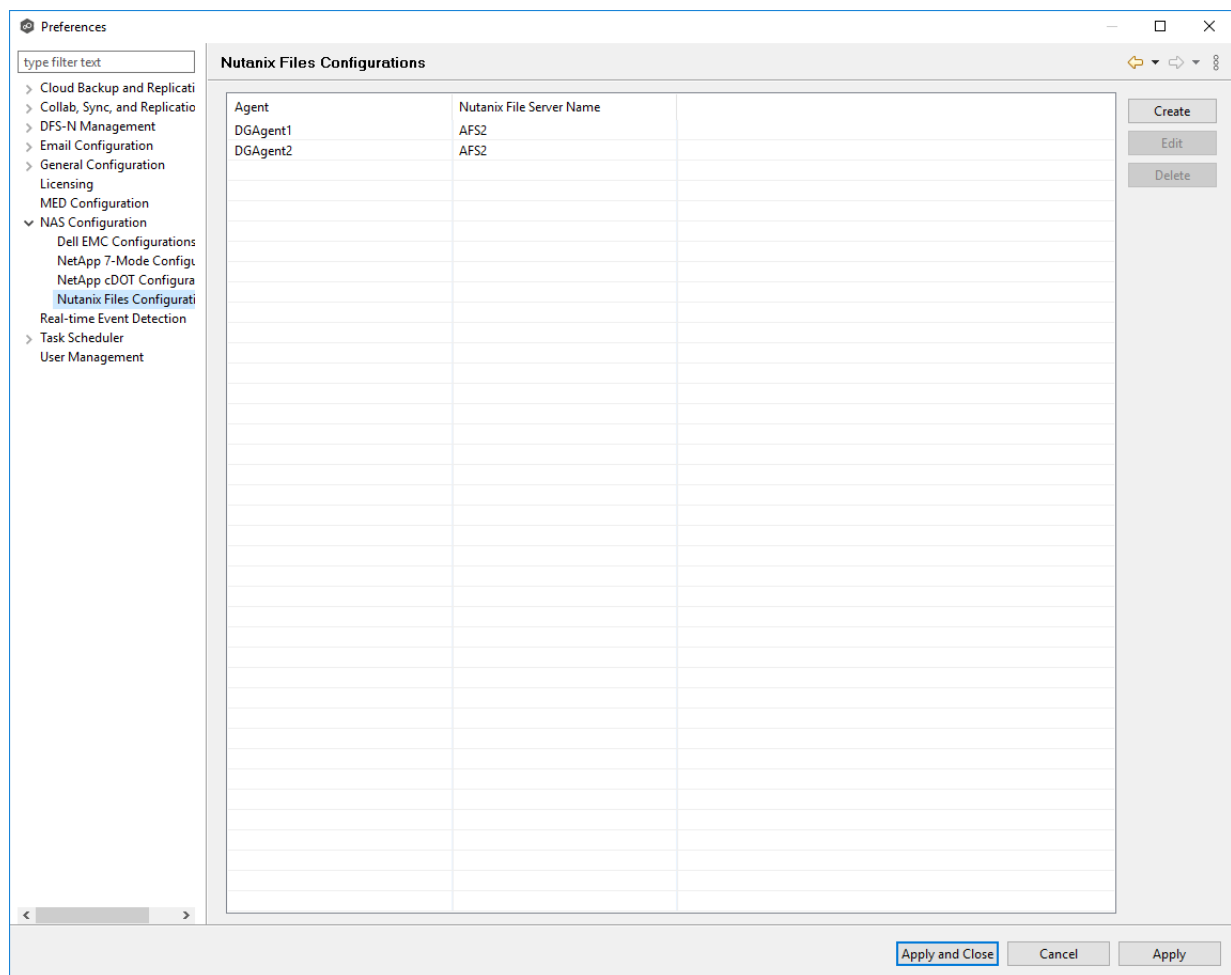
To create a new Nutanix configuration:

1. Select **Preferences** from the **Window** menu.

The **Preferences** dialog appears.

2. Select **NAS Configuration** in the navigation tree.
3. Select **Nutanix Configurations**.

The **Nutanix Files Configurations** page is displayed. It lists existing configurations.



4. Click the **Create** button.



The **Management Agent** page appears.

[illegible]

5. Select a Management Agent, and then click **Next**.

The **Storage Information** page appears.

**Storage Information**  
Enter the required information to connect to the storage

Management Agent  
Storage Information

**Credentials**

\*Nutanix File Server Name:

\*Username:

\*Password:

\*Peer Agent IP:

Advanced

Validate You must enter the name.

Having trouble connecting? Please verify that all [prerequisites](#) are met for Nutanix Files environments.

< Back Next > Cancel

6. Enter the required values in **Credentials**.

<b>Nutanix File Server Name</b>	Enter the name of the Nutanix Files cluster hosting the data to be replicated.
<b>Username</b>	Enter the user name for the account managing the Nutanix Files cluster via its management APIs.
<b>Password</b>	Enter the password for the account managing the Nutanix Files cluster via its management APIs.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Nutanix Files cluster. The Files cluster must be able to route traffic to this IP address. If the IP address you want does not appear, manually enter the address. This should not point to the Files cluster itself.

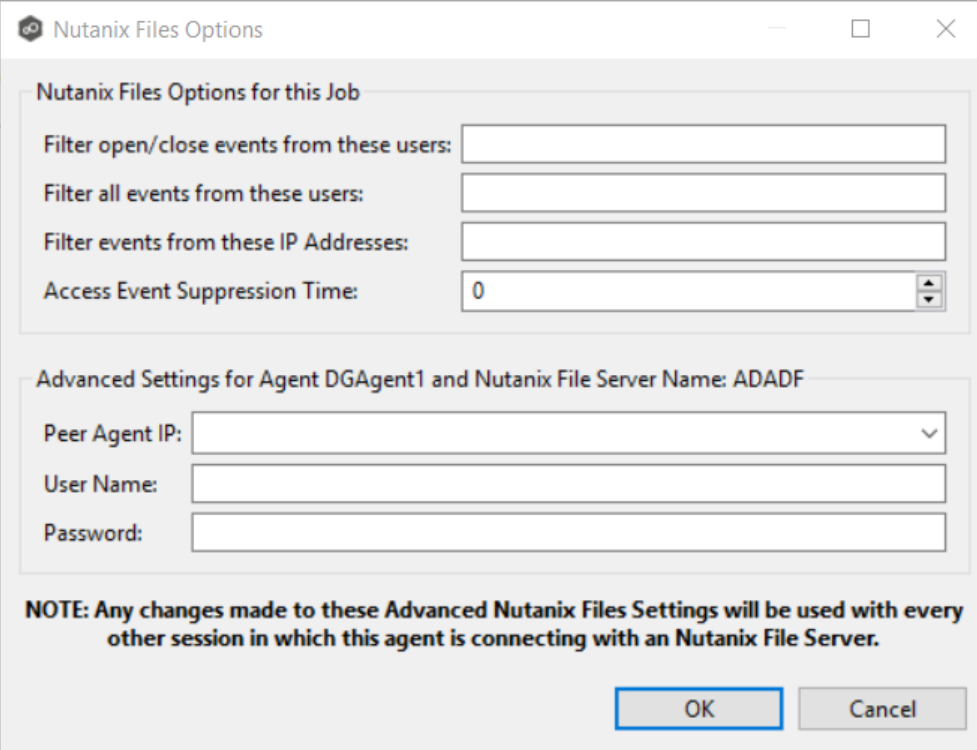
7. (Optional) Click the **Advanced** button if you want to specify advanced options, and then enter the required values:

[Nutanix Files Advanced Options](#)

8. Click **Validate**.
9. Click **Next**.
10. Click **OK**.

The options are divided into two groups:

- [Nutanix Files Options for this Job](#)
- [Advanced Settings](#)



The image shows a Windows-style dialog box titled "Nutanix Files Options". It contains two main sections. The first section, "Nutanix Files Options for this Job", has four input fields: "Filter open/close events from these users:", "Filter all events from these users:", "Filter events from these IP Addresses:", and "Access Event Suppression Time:" (which is a numeric spinner set to 0). The second section, "Advanced Settings for Agent DGAgent1 and Nutanix File Server Name: ADADF", has three input fields: "Peer Agent IP:" (a dropdown menu), "User Name:", and "Password:". At the bottom, there is a note: "NOTE: Any changes made to these Advanced Nutanix Files Settings will be used with every other session in which this agent is connecting with an Nutanix File Server." and two buttons: "OK" and "Cancel".

Nutanix Files Options

Nutanix Files Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced Settings for Agent DGAgent1 and Nutanix File Server Name: ADADF

Peer Agent IP:

User Name:

Password:

**NOTE: Any changes made to these Advanced Nutanix Files Settings will be used with every other session in which this agent is connecting with an Nutanix File Server.**

OK Cancel

## Nutanix Files Options for this Job

The following configuration options are available for Nutanix Files devices:

<b>Filter open/close events from these users</b>	A comma-separated list of user names to exclude from access event detection. For example, if "USER1" is excluded, any access event activity generated by USER1 will be ignored, e.g., file is opened and closed.
<b>Filter all events from these users</b>	A comma-separated list of user names to exclude from all event detection. For example, if "USER"1 is excluded, any activity generated by USER1 will be ignored, e.g., file is open and modified.
<b>Filter events from these IP Addresses</b>	A comma-separated list of IP addresses to exclude from all event detection. For example, if "192.168.0.100" is excluded, any activity generated by 192.168.0.100 will be ignored, e.g., file is open and modified.
<b>Access Event Suppression Time</b>	Represents the number of seconds that an open event will be delayed before being processed. Used to help reduce the amount of chatter generated by Windows clients when mousing over files in Windows Explorer. The default value is -1, which will be adjusted based on the selected NAS platform. A value of 0 will allow for dynamic changes to the amount of time that an open event will be delayed based on the load of the system.

## Advanced Settings

The following advanced settings are available for Nutanix Files devices:

<b>Peer Agent IP</b>	The IP address over which the configured Files cluster will send activity to this Peer Agent. This must be an IP address.
<b>User Name</b>	User name used to access the APIs on the Files cluster.
<b>Password</b>	Password used to access the APIs on the Files cluster.

## Real-time Event Detection Preferences

Several options are available to tune the way real-time event detection occurs. These options apply to all job types, except for DFS-N Management and PeerSync Management.

**Note:** There are also real-time event detection settings applicable to most job types in Peer Management Center. See [Real-time Event Detection](#) in the [File Collab, Sync, and Repl, and Locking Preferences](#) topic for more information.

To view and modify real-time event detection settings for all job types:

1. From the **Window** menu, select **Preferences**.
2. Select **Real-time Detection** in the navigation tree.

The following page is displayed.

3. Modify values as needed:

Option	Description
<b>Max Path Length</b>	The maximum length in characters of a file or folder path that can be detected and worked with. In rare cases, this can be increased to 2048 or even 4096 but doing so will impact memory usage of the Peer Agents.

Option	Description
<b>Event Buffer Size</b>	The buffer size used by the Peer Agents to communicate with various Windows and enterprise NAS platform APIs.
<b>Access Polling Delay (Seconds)</b>	Controls how often a Peer Agent will poll a Windows File Server for its open files list.
<b>Debug Mode</b>	Turns on debug logging for real-time detection. This logs additional information that is often useful in troubleshooting issues but can increase overhead.
<b>Advanced Job Configuration Options</b>	When selected, enables advanced job-level options tied to real-time event detection.
<b>Raw Event Logging</b>	When selected, turns on raw logging. This logs every single event that we receive from a storage platform, even ones that we may be able to consolidate and coalesce. This additional information is often useful in troubleshooting issues but will increase overhead.
<b>Advanced Configuration</b>	A list of strings to enable advanced real-time detection options not found in the GUI. This should only be used when instructed by Peer Software support.

4. Click **OK** or **Apply**.

## User Management

Peer Management Center has both a rich client interface and a web client interface. The **User Management** page allows you to manage users of the web client interface. From this page, you can [manage web client users](#), [manage web roles](#), and [configure Active Directory authentication](#).

**Note:** The User Management page can be accessed by any rich client user but only by web client users that have an **Administrator** role.

To access the User Management page:

1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.

The **User Management** page is displayed:

The screenshot shows the 'User Management' window within the 'Preferences' application. The window has a title bar with standard OS controls. On the left is a navigation pane with a search box labeled 'type filter text' and a list of categories: Cloud Backup and Replicati, Collab, Sync, and Replicatio, DFS-N Management, Email Configuration, General Configuration, Licensing, MED Configuration, NAS Configuration, Real-time Event Detection, Task Scheduler, and User Management (which is highlighted). The main area is titled 'User Management' and contains several sections: 'Roles' with a list box containing 'Power User', 'Administrator', and 'Help Desk', and 'Create', 'Edit', 'Delete' buttons; 'Internal Users' with a list box containing 'admin' and 'Create', 'Edit', 'Delete' buttons; 'Active Directory Authentication' with fields for 'URL:' and 'LDAP Admin User:', an 'Add/Update LDAP Admin User' button, and a 'Test' button; 'Active Directory Users' with an empty list box and 'Add', 'Edit', 'Delete' buttons; and 'Active Directory Groups' with an empty list box and 'Add', 'Edit', 'Delete' buttons. At the bottom right are 'Apply and Close', 'Cancel', and 'Apply' buttons.

3. From this page, you can add, edit, and remove [web roles](#), [internal users](#), [active directory users and groups](#), and [configure Active Directory authentication](#).

## Managing Web Client Users

**Web client users** are users that access Peer Management Center through the web client.

Web users can be divided into two types based on how their access to the web client is authenticated:

- [Internal users](#) - Users whose access to the web client is authenticated through the internal PMC database.
- [Active Directory \(AD\) users and groups](#) - Users whose access to the web client is authenticated through Active Directory.

You add, modify, and delete web users through the [User Management](#) page in [Preferences](#). The **User Management** page is also where you specify the Active Directory account that will be used when Peer Management Center queries Active Directory for authentication.

Management of web users can be performed through the rich client or through the web client by a user with an **Administrator** role. For more information, see:

- [Managing Internal Users](#)
- [Managing Active Directory Users and Groups](#)
- [Configuring Active Directory Authentication](#)

Managing [internal users](#) involves:

- [Creating internal users](#)
- [Editing internal users](#)
- [Deleting internal users](#)

## Creating an Internal User

To add an internal user, follow these steps:

1. From the **Window** menu, select **Preferences**.

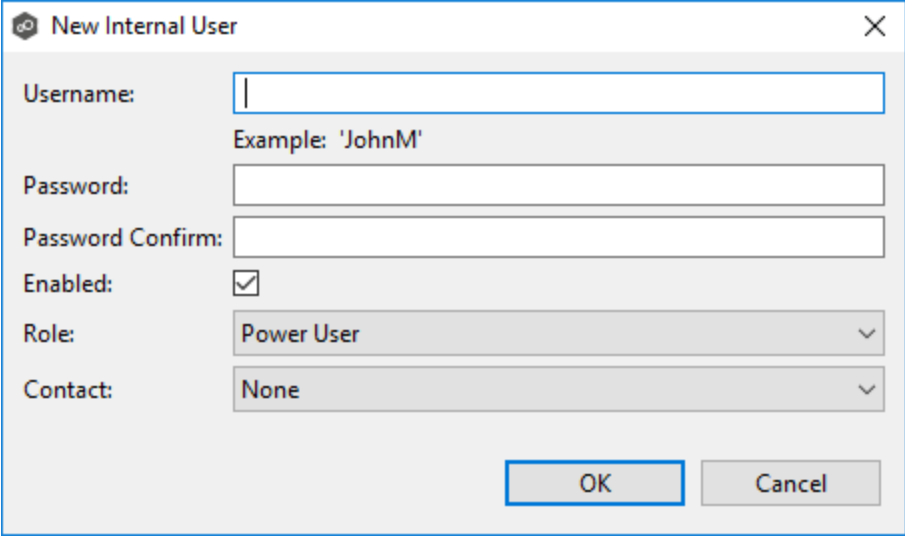


2. Select **User Management** from the navigation tree.

The screenshot shows the 'User Management' window within a 'Preferences' application. On the left is a navigation tree with a search bar labeled 'type filter text'. The tree includes categories like 'Cloud Backup and Replicati', 'Collab, Sync, and Replicatio', 'DFS-N Management', 'Email Configuration', 'General Configuration', 'Licensing', 'MED Configuration', 'NAS Configuration', 'Real-time Event Detection', 'Task Scheduler', and 'User Management' (which is highlighted). The main area is titled 'User Management' and contains several sections: 'Roles' with a list box containing 'Power User', 'Administrator', and 'Help Desk', and buttons 'Create', 'Edit', and 'Delete'; 'Internal Users' with a list box containing 'admin' and buttons 'Create', 'Edit', and 'Delete'; 'Active Directory Authentication' with fields for 'URL:' and 'LDAP Admin User:', an 'Add/Update LDAP Admin User' button, and a 'Test' button; 'Active Directory Users' with an empty list box and 'Add', 'Edit', and 'Delete' buttons; and 'Active Directory Groups' with an empty list box and 'Add', 'Edit', and 'Delete' buttons. At the bottom are 'Apply and Close', 'Cancel', and 'Apply' buttons.

3. Select the **Create** button for Internal Users.

The **New Internal User** dialog appears.



The screenshot shows a 'New Internal User' dialog box. It has a title bar with a gear icon and a close button. The fields are: Username (text input), Password (text input), Password Confirm (text input), Enabled (checkbox, checked), Role (dropdown menu, 'Power User'), and Contact (dropdown menu, 'None'). At the bottom right are 'OK' and 'Cancel' buttons. An example 'Example: 'JohnM'' is shown below the Username field.

4. Enter the following information.

- **Username:** The username can contain letters, numbers, and spaces; it cannot contain special characters. The minimum number of characters is 6; the maximum number of characters is 20.
- **Password:** The minimum number of characters is 6; the maximum number of characters is 20. The password cannot be the same as the username.
- **Password Confirm:** Re-enter the password you entered.
- **Enabled:** Select this checkbox if you want to enable this user to access Peer Management Center. You can enable or disable the user at a later date by [editing the user](#).
- **Role:** Select the [web role](#) you want to assign to the user. It can be a standard role or a custom role. For more details on the available roles, see [Web Roles](#)
- **Contact:** Select the user's email address from the drop-down list.. If the user's email address does not appear in the list, you can add it to **Contacts** in the [Email Configuration](#) in [Preferences](#).

5. Click **OK**.

The new user appears in the list of internal users on the User Management page.

6. Click **Apply and Close** or **Apply**.

## Editing an Internal User

Once an internal user has been created, its user name, password, email address, and web role can all be changed.

**Note:** The [default admin user](#) cannot be renamed, nor can its role be changed. However, you should change the default password for the default admin user.

To edit an internal user from Peer Management Center:

1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.
3. Select the user from the list of internal users.
4. Click **Edit**.
5. Make the changes in the **Edit User Information** dialog.
6. Click **OK**.
7. Click **Apply and Close** or **Apply**.

## Deleting an Internal User

Once the account of an internal user is deleted, that user can no longer access Peer Management Center through the web client.

**Note:** The [default admin user](#) user cannot be deleted.

To delete an Active Directory user or group from Peer Management Center:

1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.
3. Select the user from the list of internal users.
4. Click **Delete**.
5. Click **OK** in the **Remove User** dialog.
6. Click **Apply and Close** or **Apply**.

Managing Active Directory users involves:

- [Adding an Active Directory User or Group](#)
- [Editing an Active Directory User or Group](#)
- [Deleting an Active Directory User or Group](#)

## Adding an Active Directory User or Group

To add Active Directory users and groups to Peer Management Center, follow these steps:

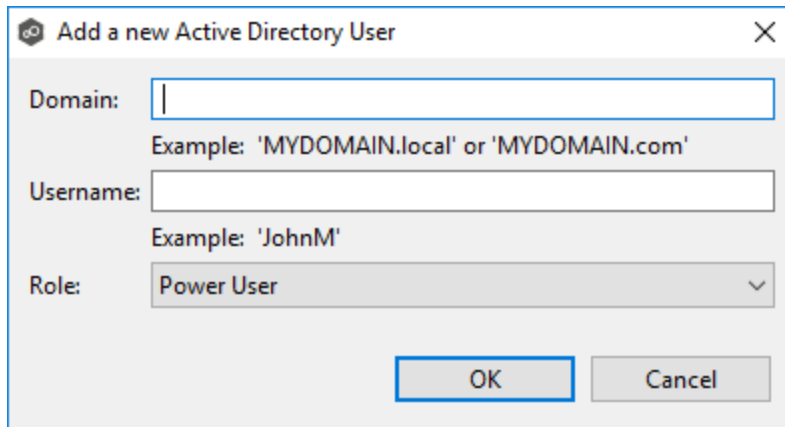
1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.

The screenshot shows the 'Preferences' window with the 'User Management' section selected in the left sidebar. The main area is titled 'User Management' and contains several sections:

- Roles:** A list box containing 'Power User', 'Administrator', and 'Help Desk'. Below the list are 'Create', 'Edit', and 'Delete' buttons.
- Internal Users:** A list box containing 'admin'. Below the list are 'Create', 'Edit', and 'Delete' buttons.
- Active Directory Authentication:** Fields for 'URL:' and 'LDAP Admin User:'. Below these are 'Add/Update LDAP Admin User' and 'Test' buttons.
- Active Directory Users:** An empty list box. Below it are 'Add', 'Edit', and 'Delete' buttons.
- Active Directory Groups:** An empty list box. Below it are 'Add', 'Edit', and 'Delete' buttons.

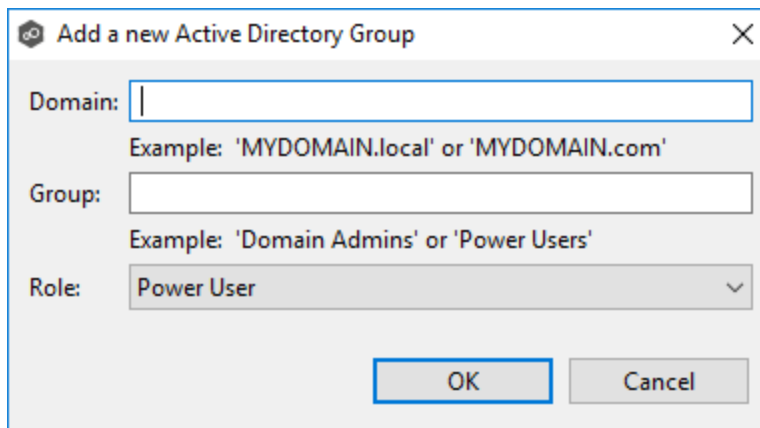
At the bottom of the window are 'Apply and Close', 'Cancel', and 'Apply' buttons.

3. Add an Active Directory user or group by clicking the appropriate **Add** button.
4. Enter the information required in the dialog that appears:
  - For an individual user, enter the domain name, user name, and select a role.



The dialog box is titled "Add a new Active Directory User" and has a close button (X) in the top right corner. It contains three input fields: "Domain:" with a text box and an example "Example: 'MYDOMAIN.local' or 'MYDOMAIN.com'", "Username:" with a text box and an example "Example: 'JohnM'", and "Role:" with a dropdown menu showing "Power User". At the bottom right are "OK" and "Cancel" buttons.

- For a user group, enter the domain name, group name, and select a role.



The dialog box is titled "Add a new Active Directory Group" and has a close button (X) in the top right corner. It contains three input fields: "Domain:" with a text box and an example "Example: 'MYDOMAIN.local' or 'MYDOMAIN.com'", "Group:" with a text box and an example "Example: 'Domain Admins' or 'Power Users'", and "Role:" with a dropdown menu showing "Power User". At the bottom right are "OK" and "Cancel" buttons.

Directory users and groups are saved in the following format: username@mydomain.local

5. Click **OK**.

The added user or group appears in the list of Active Directory users or groups.

6. Click **OK**.

## Editing an Active Directory User or Group

To edit an Active Directory user or group:

1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.
3. Select the AD user or group from the list of AD users or groups.

4. Click **Edit**.
5. Make the changes.
6. Click **OK**.

## Deleting an Active Directory User or Group

If you delete an Active Directory user or group from Peer Management Center, that user or group will no longer have access to Peer Management Center through the web client. However, deleting the AD user or group from Peer Management Center does not delete that user or group from the Active Directory.

To delete an Active Directory user or group from Peer Management Center:

1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.
3. Select the AD user or group from the list of AD users or groups.
4. Click **Delete**.
5. Confirm that you want to delete the user or group.
6. Click **OK**.

To configure Active Directory authentication, you need:

- The URL of the LDAP server
- The LDAP administrator credentials

Active Directory users won't be able to access Peer Management Center until the authentication is configured.

To configure Active Directory authentication:

1. From the **Window** menu, select **Preferences**.
2. Select **User Management** from the navigation tree.

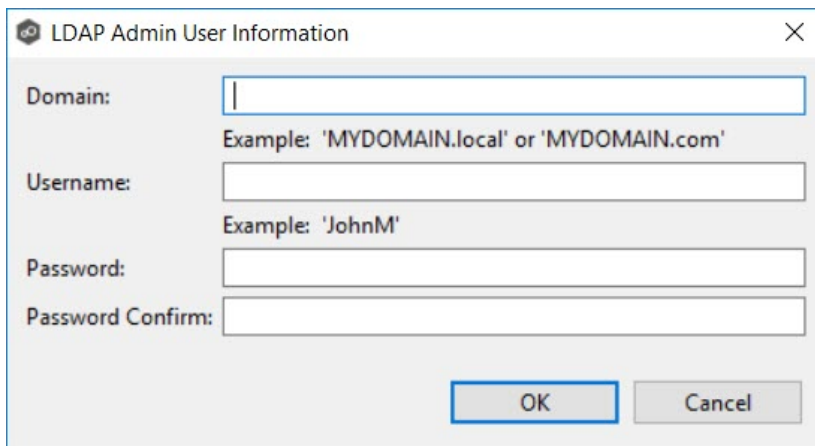
The screenshot shows the 'Preferences' window with the 'User Management' section selected in the left sidebar. The main area is titled 'User Management' and contains several sections:

- Roles:** A list box containing 'Power User', 'Administrator', and 'Help Desk'. Below it are 'Create', 'Edit', and 'Delete' buttons.
- Internal Users:** A list box containing 'admin'. Below it are 'Create', 'Edit', and 'Delete' buttons.
- Active Directory Authentication:** A section with a 'URL:' label and an empty text field. Below it is an 'LDAP Admin User:' label and an empty text field. To the right of the 'LDAP Admin User' field is a 'Test' button. Below these fields is an 'Add/Update LDAP Admin User' button.
- Active Directory Users:** An empty list box. Below it are 'Add', 'Edit', and 'Delete' buttons.
- Active Directory Groups:** An empty list box. Below it are 'Add', 'Edit', and 'Delete' buttons.

At the bottom of the window are three buttons: 'Apply and Close', 'Cancel', and 'Apply'.

3. In the **URL** field in the **Active Directory Authentication** section, enter the URL of the LDAP server on the network using one of the following formats:
  - ldap://MYDOMAIN.LOCAL
  - ldaps://MYDOMAIN.LOCAL
4. Click **Add/Update LDAP Admin User**.



A screenshot of a Windows-style dialog box titled "LDAP Admin User Information". It contains four text input fields: "Domain:", "Username:", "Password:", and "Password Confirm:". Below the "Domain:" field is a small text example: "Example: 'MYDOMAIN.local' or 'MYDOMAIN.com'". Below the "Username:" field is a small text example: "Example: 'JohnM'". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

5. Enter the domain name, user name, and password.
6. Confirm the password.
7. Click **OK**.

The LDAP user's information appears below the **Add/Update LDAP Admin User** button.

8. Click **Test** to verify the connection to the LDAP server.
9. Click **OK**.

## Managing Web Roles

Managing web roles involves:

- [Creating custom web roles](#)
- [Editing and deleting web roles](#)
- [Assigning tags to web roles](#)

To create a custom role:

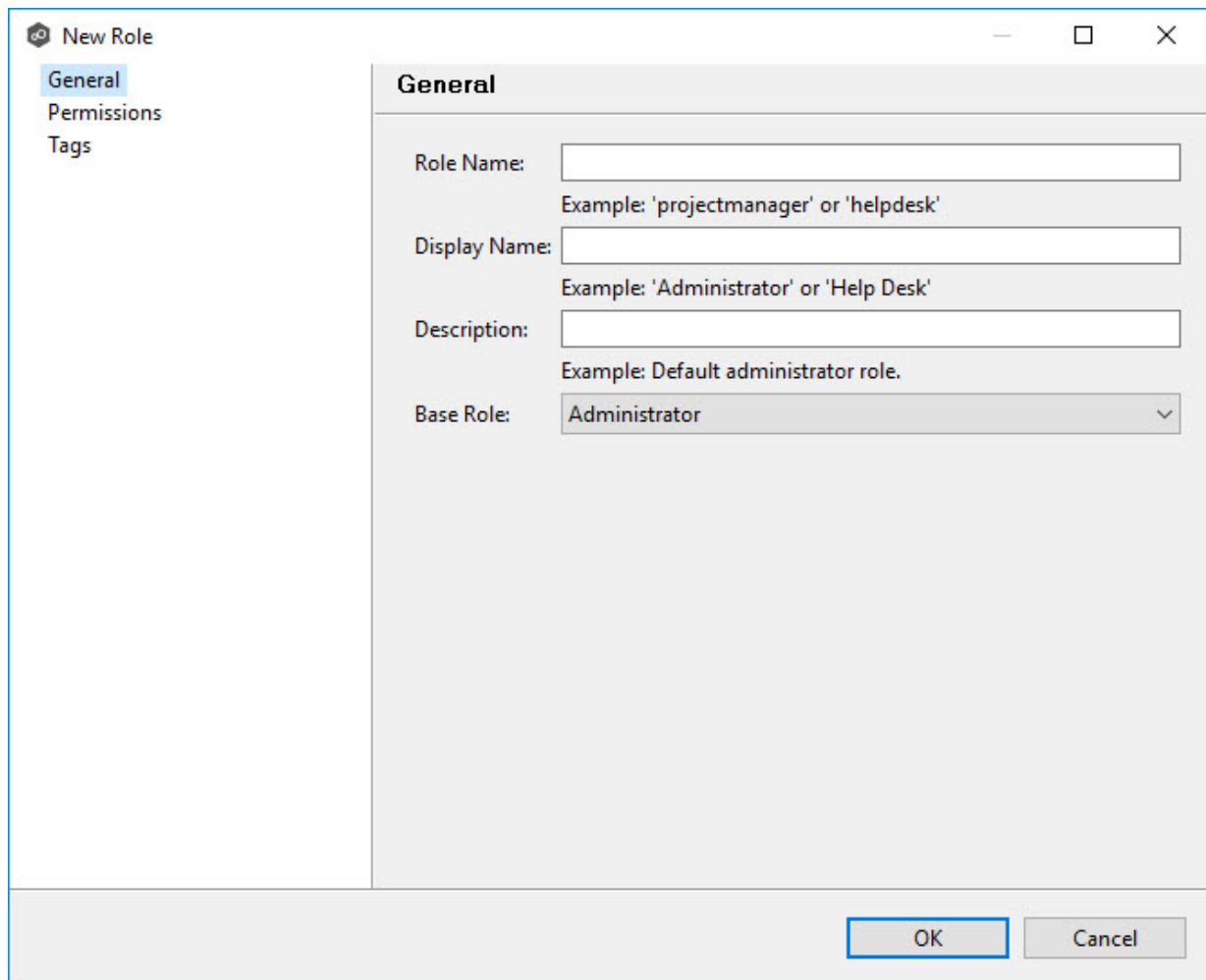
1. From the **Window** menu, select **Preferences**.

2. Select **User Management** from the navigation tree.

The screenshot shows the 'User Management' window within a 'Preferences' application. On the left is a navigation tree with a search bar labeled 'type filter text'. The tree includes categories like 'Cloud Backup and Replicati', 'Collab, Sync, and Replicatio', 'DFS-N Management', 'Email Configuration', 'General Configuration', 'Licensing', 'MED Configuration', 'NAS Configuration', 'Real-time Event Detection', 'Task Scheduler', and 'User Management', which is currently selected. The main area of the window is titled 'User Management' and contains several sections: 'Roles' with a list box containing 'Power User', 'Administrator', and 'Help Desk', and 'Create', 'Edit', and 'Delete' buttons; 'Internal Users' with a list box containing 'admin' and the same three buttons; 'Active Directory Authentication' with fields for 'URL:' and 'LDAP Admin User:', an 'Add/Update LDAP Admin User' button, and a 'Test' button; 'Active Directory Users' with an empty list box and 'Add', 'Edit', and 'Delete' buttons; and 'Active Directory Groups' with an empty list box and 'Add', 'Edit', and 'Delete' buttons. At the bottom of the window are 'Apply and Close', 'Cancel', and 'Apply' buttons.

3. Click the **Create** button in the **Roles** section.

The **General** tab of **New Role** dialog is displayed.



The screenshot shows a 'New Role' dialog box with a sidebar on the left containing 'General', 'Permissions', and 'Tags'. The 'General' tab is selected. The main area is titled 'General' and contains four fields: 'Role Name' with an example of 'projectmanager' or 'helpdesk', 'Display Name' with an example of 'Administrator' or 'Help Desk', 'Description' with an example of 'Default administrator role.', and 'Base Role' which is a dropdown menu currently set to 'Administrator'. At the bottom right are 'OK' and 'Cancel' buttons.

4. Enter the following information:

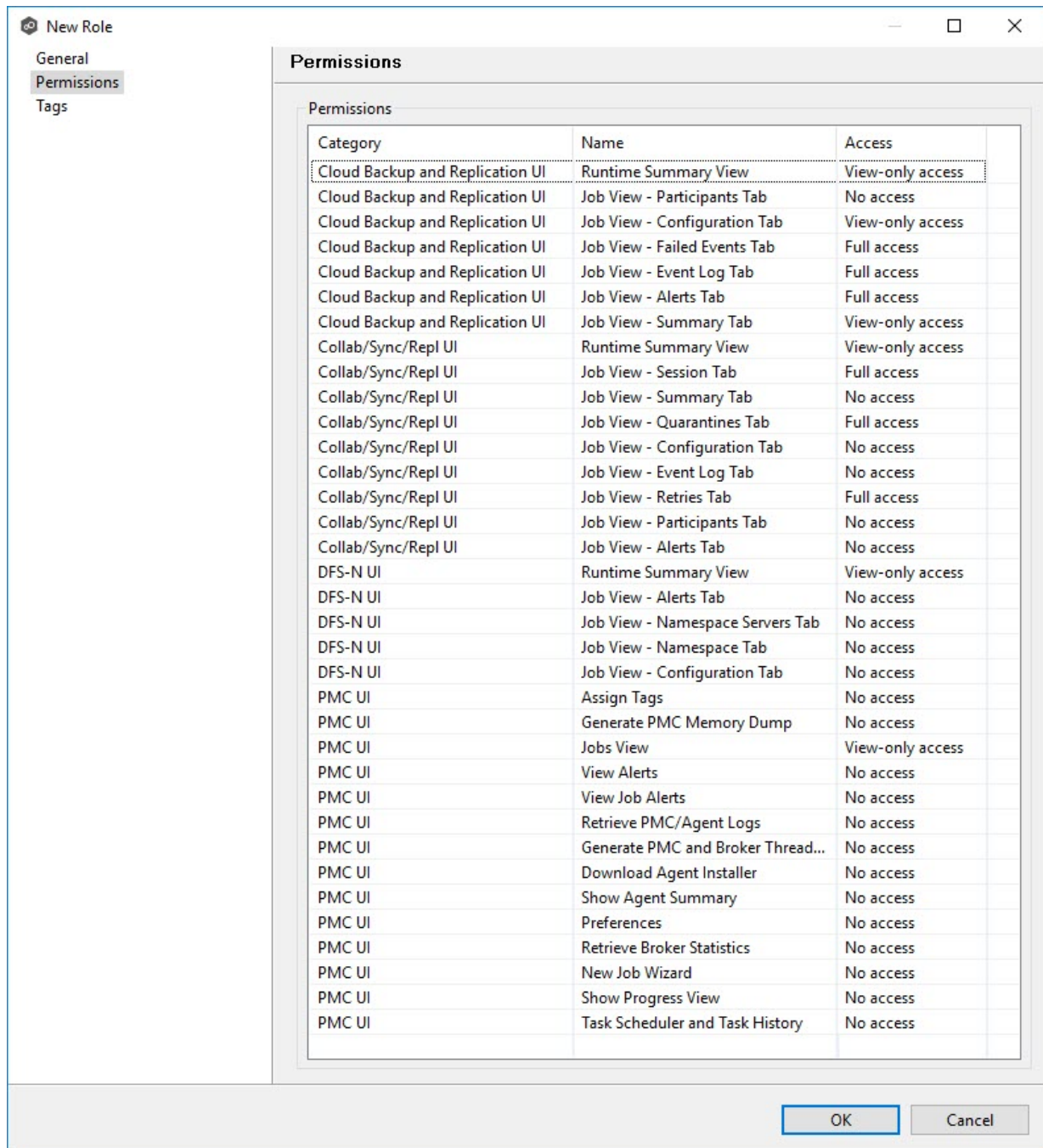
- **Role Name:** A Role Name can contain only letters and numbers; it cannot contain any spaces or special characters. The maximum number of characters is 20. The Role Name is used in the internal Peer Management Center database.
- **Display Name:** The Display Name can contain spaces and special characters, in addition to letter and numbers. The Display Name is displayed in the PMC user interface and reports.
- **Description:** (Optional) Use the Description to provide a brief summary of the intended use of the role.

5. Select a [standard web role](#) on which to base the custom role.

6. Select the **Permissions** tab.

The **Permissions** tab displays a table of [the permissions that are available to be modified for the new role](#). The **Access** column displays the current level of access that the role has

to the resource. There are three levels of access: **Full access**, **View-only access**, and **No access**.



**New Role**

General  
Permissions  
Tags

**Permissions**

Category	Name	Access
Cloud Backup and Replication UI	Runtime Summary View	View-only access
Cloud Backup and Replication UI	Job View - Participants Tab	No access
Cloud Backup and Replication UI	Job View - Configuration Tab	View-only access
Cloud Backup and Replication UI	Job View - Failed Events Tab	Full access
Cloud Backup and Replication UI	Job View - Event Log Tab	Full access
Cloud Backup and Replication UI	Job View - Alerts Tab	Full access
Cloud Backup and Replication UI	Job View - Summary Tab	View-only access
Collab/Sync/Repl UI	Runtime Summary View	View-only access
Collab/Sync/Repl UI	Job View - Session Tab	Full access
Collab/Sync/Repl UI	Job View - Summary Tab	No access
Collab/Sync/Repl UI	Job View - Quarantines Tab	Full access
Collab/Sync/Repl UI	Job View - Configuration Tab	No access
Collab/Sync/Repl UI	Job View - Event Log Tab	No access
Collab/Sync/Repl UI	Job View - Retries Tab	Full access
Collab/Sync/Repl UI	Job View - Participants Tab	No access
Collab/Sync/Repl UI	Job View - Alerts Tab	No access
DFS-N UI	Runtime Summary View	View-only access
DFS-N UI	Job View - Alerts Tab	No access
DFS-N UI	Job View - Namespace Servers Tab	No access
DFS-N UI	Job View - Namespace Tab	No access
DFS-N UI	Job View - Configuration Tab	No access
PMC UI	Assign Tags	No access
PMC UI	Generate PMC Memory Dump	No access
PMC UI	Jobs View	View-only access
PMC UI	View Alerts	No access
PMC UI	View Job Alerts	No access
PMC UI	Retrieve PMC/Agent Logs	No access
PMC UI	Generate PMC and Broker Thread...	No access
PMC UI	Download Agent Installer	No access
PMC UI	Show Agent Summary	No access
PMC UI	Preferences	No access
PMC UI	Retrieve Broker Statistics	No access
PMC UI	New Job Wizard	No access
PMC UI	Show Progress View	No access
PMC UI	Task Scheduler and Task History	No access

OK Cancel

- For each permission that you want to modify, click in the **Access** column and select the access level that you want for the new role.
- (Optional) Click **Tags** to assign tags to the role.

[illegible]

See [Assigning Tags](#) for more information.

9. Click **OK**.

The new role appears in the **Roles** section.

## Editing a Web Role

You can edit a custom web role, changing its Role Name and Display Name, its base role, associated permissions, and tags assigned to the role.

Editing of a standard role is much more restricted. It is limited to modifying the tags assigned to the role. You cannot edit its names or associated permissions.

To edit a web role, select the role in the **Roles** section in the **User Management** page, and then click **Edit**.

## Deleting a Web Role

You cannot delete a standard web role.

To delete a custom web role, select the role in the **Roles** section in the **User Management** page, and then click **Delete**.

For information about assigning a tag to a web role, see [Assigning Tags](#).

## Cloud Backup and Replication Jobs

This section provides information about creating, running, and managing a Cloud Backup and Replication job:

- [Overview](#)
- [Before You Create Your First Cloud Backup and Replication Job](#)
- [Creating a Cloud Backup and Replication Job](#)
- [Running a Cloud Backup and Replication Job](#)
- [Monitoring Your Cloud Backup and Replication Jobs](#)
- [Deleting a Cloud Backup and Replication Job](#)
- [Recovering Data from the Cloud](#)

### Overview

Cloud Backup and Replication brings file to object replication into Peer Software's capabilities for enterprise NAS environments. Leveraging the same real-time engine that powers Peer Software's

multi-site, multi-vendor replication, Cloud Backup and Replication efficiently pushes data into Microsoft Azure or Amazon S3 storage in an open format that is immediately consumable by other applications and services.

Use cases for Cloud Backup and Replication include: (1) pushing exact replicas of on-premises data sets into object storage for use with burstable compute and cloud-borne services and (2) tape replacement-style backup to object with point-in-time recovery capability.

## Before You Create Your First Cloud Backup and Replication Job

We strongly recommend that you configure the [Cloud Backup and Replication settings](#) (including [proxy configurations](#)), as well as other global settings such as SMTP configuration, email alerts, and before configuring your first Cloud Backup and Replication job. See [Preferences](#) for details on what and how to configure these settings.

In addition, we recommend that you set up your destination storage account before creating the job.

## Creating a Cloud Backup and Replication Job

The **Create Job Wizard** walks you through the process of creating a Cloud Backup and Replication job. The process consists of the following steps:

[Step 1: Job Type and Name](#)

[Step 2: Source Storage Platform](#)

[Step 3: Management Agent](#)

[Step 4: Proxy Configuration](#)

[Step 5: Storage Information](#)

[Step 6: Source Paths](#)

[Step 7: File Filters](#)

[Step 8: Destination](#)

[Step 9: Destination Credentials](#)

[Step 10: Container or Bucket Details](#)

[Step 11: Replication and Retention Policy](#)

[Step 12: Replication Schedule](#)

[Step 13: Retention](#)

[Step 14: Source Snapshots](#)

[Step 15: Miscellaneous Options](#)

[Step 16: Email Alerts](#)

[Step 17: SNMP Notifications](#)

[Step 18: Confirmation](#)

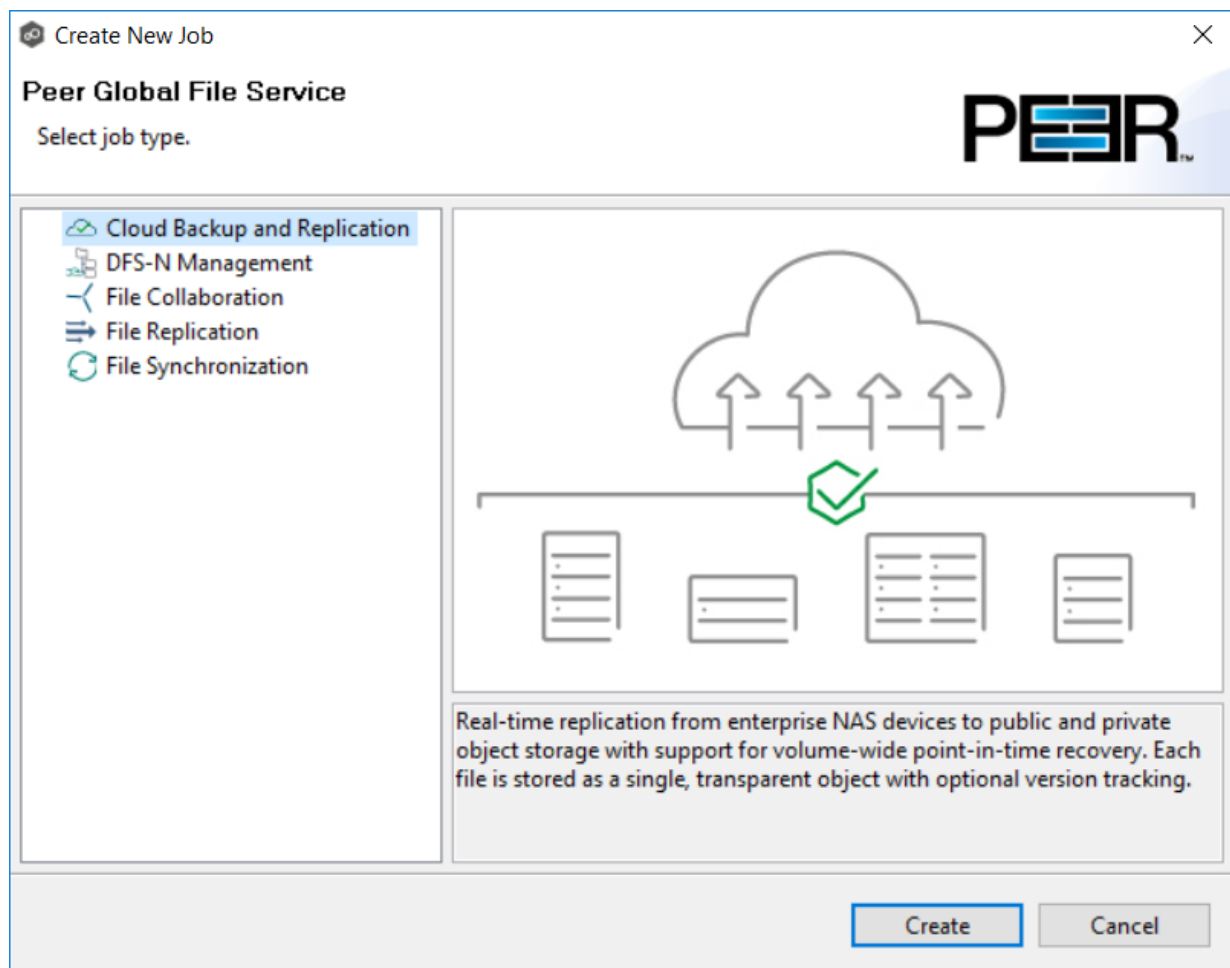
### Step 1: Job Type and Name

1. Open Peer Management Center.
2. From the **File** menu, select **New Job** (or click the **New Job** button on the toolbar).

The **Create New Job** wizard displays a list of job types you can create.

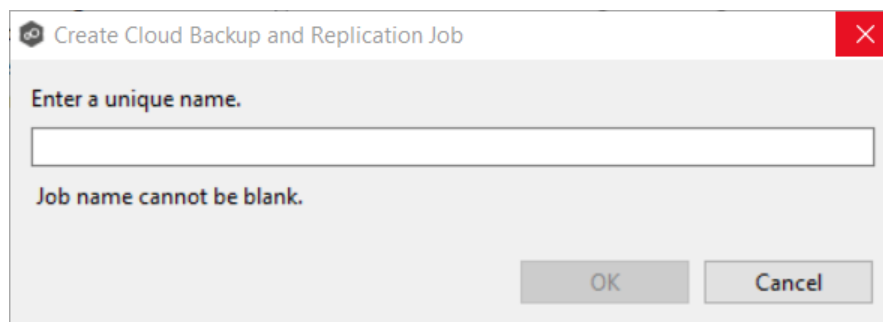
3. Click **Cloud Backup and Replication**, and then click **Create**.





4. Enter a name for the job in the dialog that appears.

The job name must be unique.



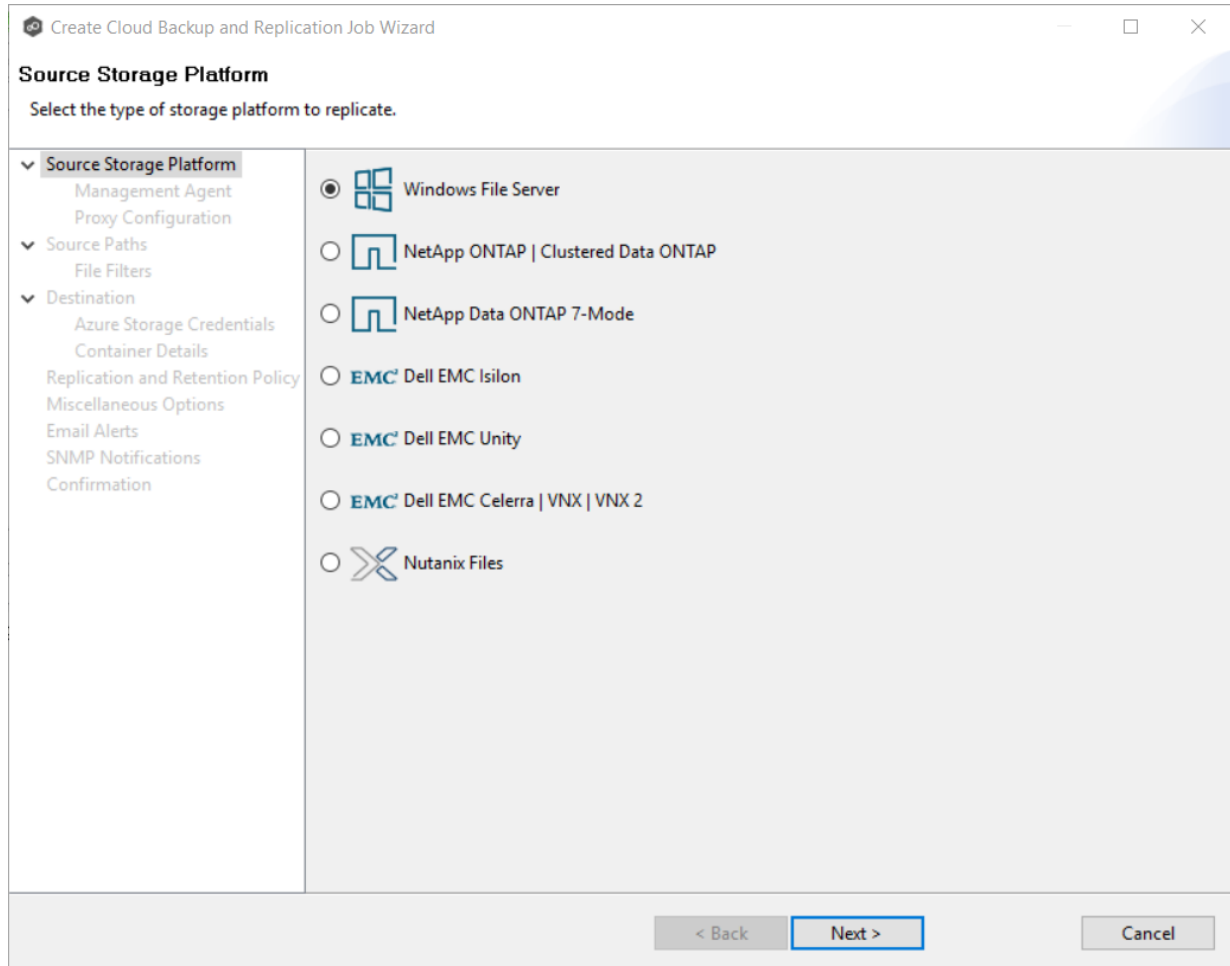
5. Click **OK**.

The [Source Storage Platform](#) page appears.

## Step 2: Source Storage Platform

The **Source Storage Platform** page lists the types of source storage platforms that Cloud Backup and Replication supports. The source storage device hosts the data you want to replicate.

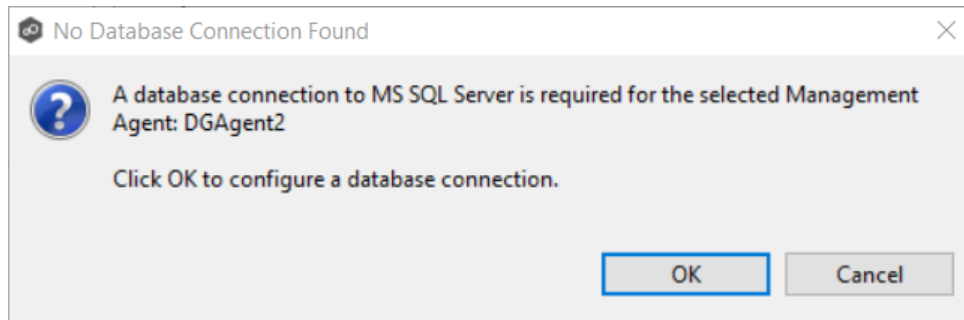
1. Select the type of storage platform you want to replicate.



2. Click **Next**.

The [Management Agent](#) page appears.





Click **OK** and then configure the database connection for the selected Management Agent. See [Database Connections](#) for instructions about creating a database connection.

2. Click **Next**.

The [Proxy Configuration](#) page appears.

#### Step 4: Proxy Configuration

If you do not need a proxy server to connect to outside networks, skip this step and proceed to [Step 5](#).

If you do need a proxy server to connect to outside networks, you have three options:

- Create a new proxy configuration.
- Use the existing proxy configuration. If there is an existing proxy configuration, details about the configuration will be displayed on the page.

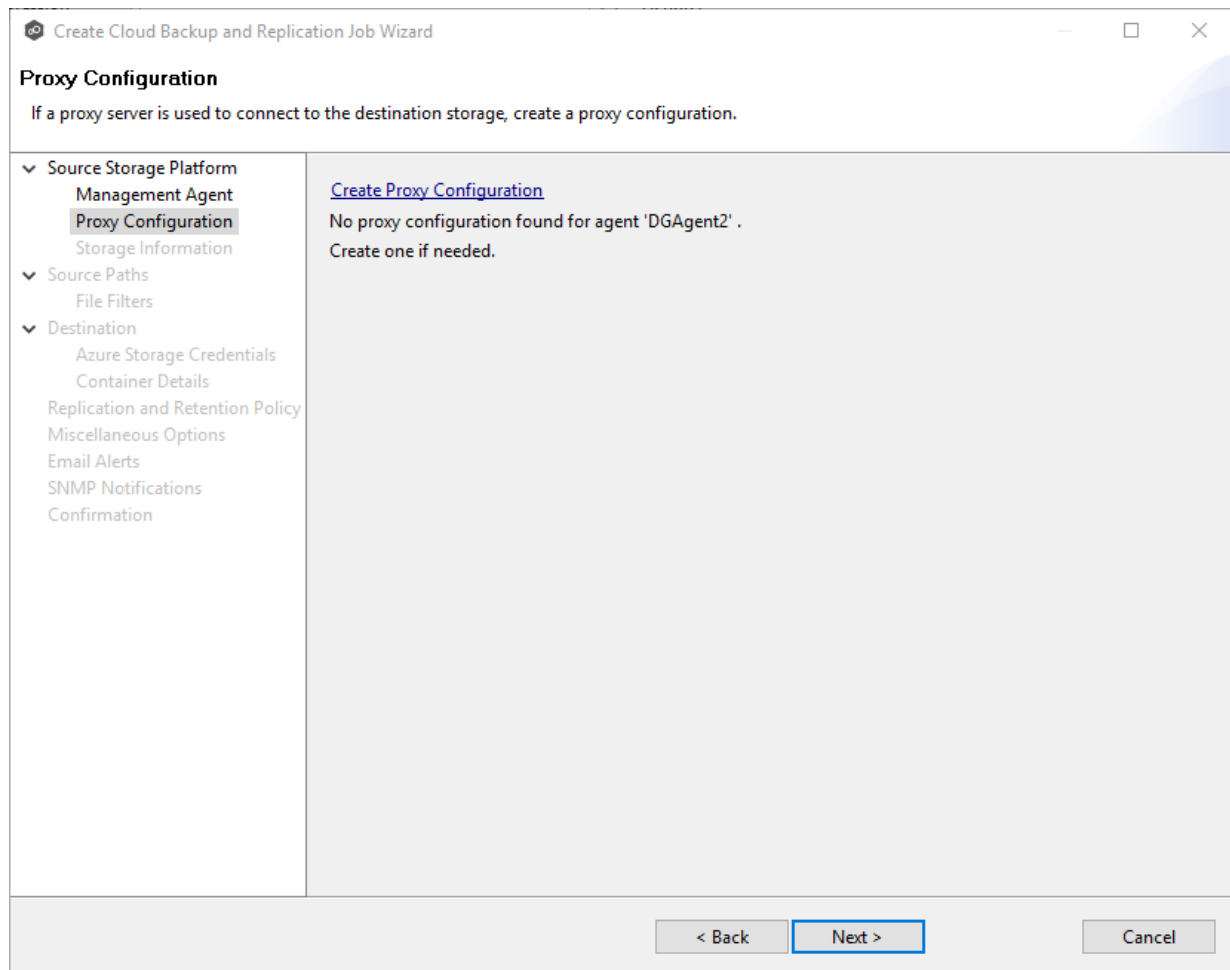
You may have created one in advance through [Cloud Back and Replication Preferences](#) or when you created another Cloud Backup and Replication job. Once a proxy configuration is created for a source storage platform, that proxy configuration is used for all Cloud Backup and Replication jobs using that agent.

- Edit an existing proxy configuration. Click the **Edit Proxy Configuration** link to edit the existing proxy.

If you edit the proxy configuration, it affects other jobs using the same agent. Editing an existing proxy configuration has the potential to create problems with the other jobs.

If there is not an existing proxy configuration for the selected management agent, follow these steps to create a new proxy configuration:

1. Click **Create Proxy Configuration**.



The **Proxy Configuration** page is displayed. Existing proxies are listed in the Proxy Configuration table.



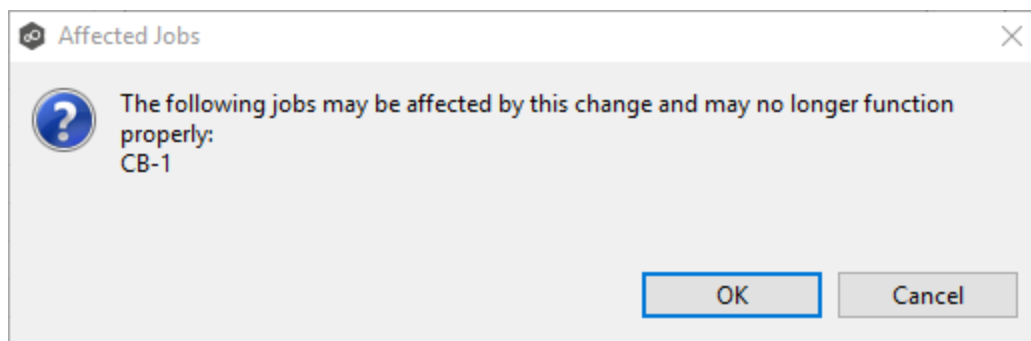
<b>Address</b>	Enter the IP address or fully qualified domain name of the proxy server.
<b>Port</b>	Enter the port number.
<b>User Authentication</b>	Select this checkbox if the proxy server requires authentication.

4. If your proxy server requires authentication, click the **User Authentication** checkbox and supply the necessary values.

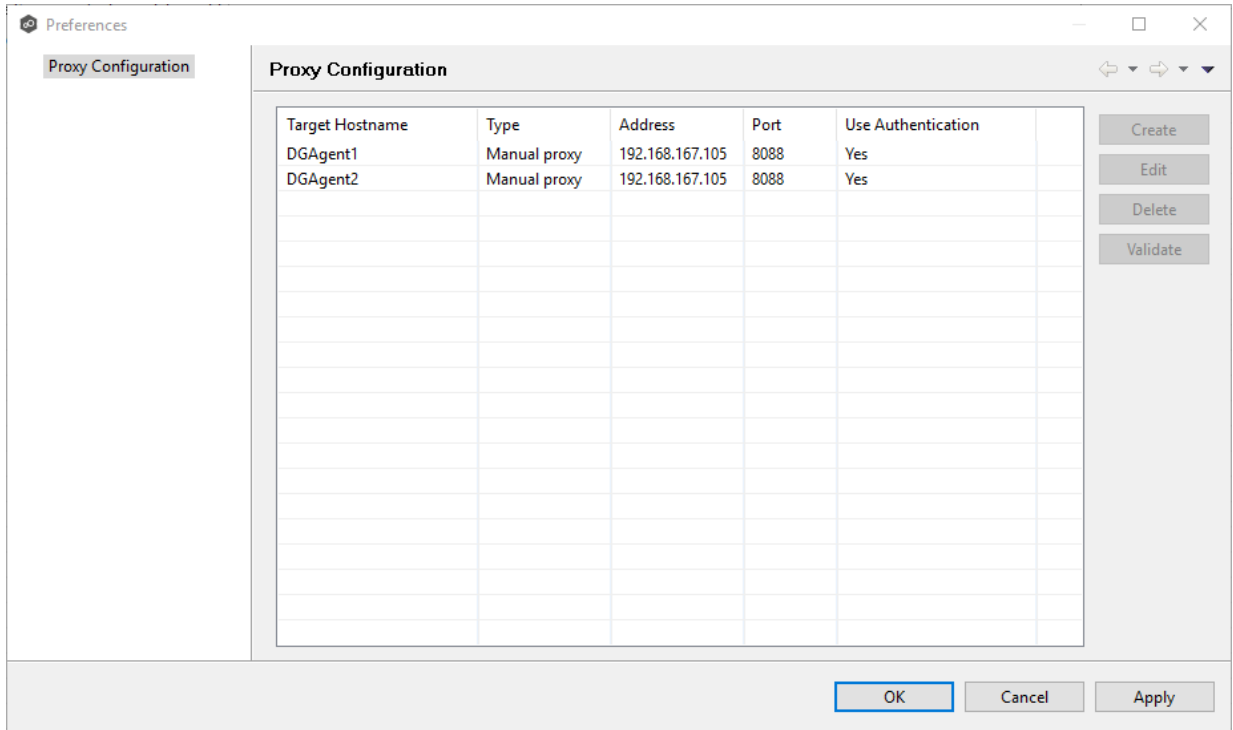
<b>Domain</b>	Enter the domain name on the proxy server.
<b>Username</b>	Enter the user name for the proxy server.
<b>Password</b>	Enter the password for the proxy server.

5. Click **OK**.

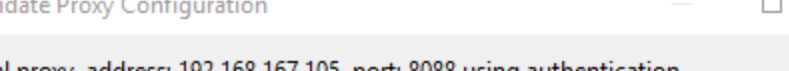
If you already have jobs managed by this agent, a message appears and identifies those jobs. They will now use the proxy as well.



After you click OK, the **Proxy Configuration** page is redisplayed. The proxy you just created now appears in the table.



- The **Validate Proxy Configuration** dialog appears.

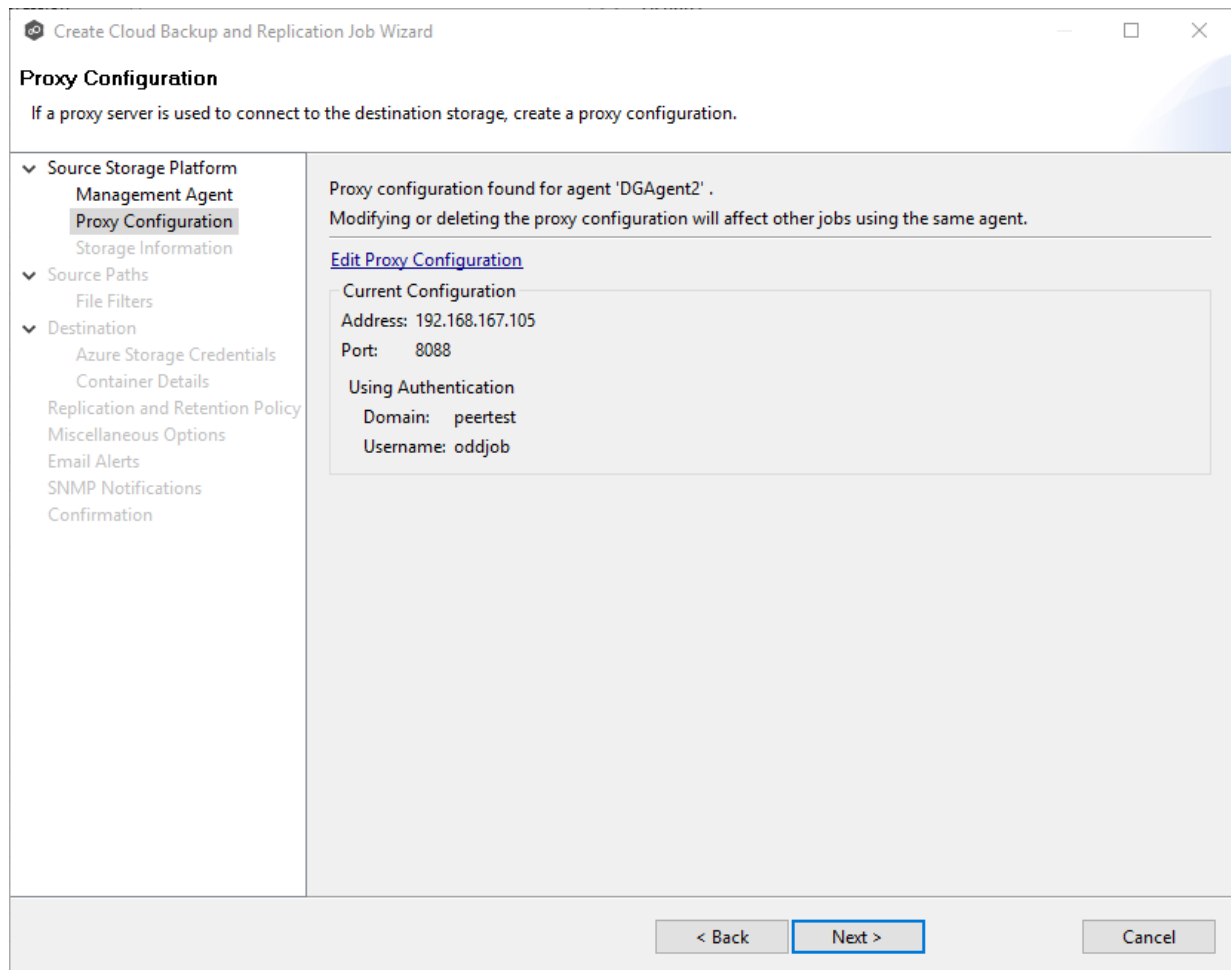
- 
- Validate Proxy Configuration
- Manual proxy, address: 192.168.167.105, port: 8088 using authentication.  
Agent: DGAgent2
- Storage Account:
- Close

8. Click **OK** in the **Validation Result** dialog.

- Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.







11. Click **Next**.

The [Storage Information](#) page appears.

### Step 5: Storage Information

The **Storage Information** page requests the credentials necessary to connect to the storage device you want to replicate.

**Note:** If you selected **Windows File Server** in [Step 2](#), this page doesn't appear; skip to [Step 5: Source Paths](#).

1. Select **New Credentials** to enter a new set of credentials for the source storage platform or select **Existing Credentials**.

2. If you selected **Existing Credentials**, select a credential from the drop-down list, and then click **Next** to continue with [Step 5: Source Paths](#).

If you selected **New Credentials**, enter the credentials for connecting to the source storage device. The information you are prompted to enter varies, depending on the type of storage platform:

[NetApp ONTAP | Clustered Data ONTAP](#)

[NetApp Data ONTAP 7-Mode](#)

[Dell EMC Isilon](#)

[Dell EMC Unity](#)

[Dell EMC Celerra | VNX | VNX 2](#)

[Nutanix Files](#)

3. Click **Validate** to test the credentials, and then click **OK** in the confirmation message that appears.
4. Click **Next**.

The [Source Paths](#) page appears.

1. Enter the credentials to connect to the Storage Virtual Machine hosting the data to be replicated or select existing credentials.

Create Cloud Backup and Replication Job Wizard

### Storage Information

Enter the information required to connect to the source storage platform.

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information**
- Source Paths
  - File Filters
- Destination
  - Azure Storage Credentials
  - Container Details
  - Replication and Retention Policy
  - Miscellaneous Options
  - Email Alerts
  - SNMP Notifications
  - Confirmation

**Credentials**

☒ New Credentials

\*SVM Name:

\*SVM User Name:

\*SVM Password:

SVM Management IP:

\*Peer Agent IP:

☐ Existing Credentials

SVM9X-1, user:vsadmin

**Access Path**

Access Path:

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp ONTAP/cDOT environments.

< Back   Next >   Cancel

<b>SVM Name</b>	Enter the name of the Storage Virtual Machine hosting the data to be replicated.
<b>SVM Username</b>	Enter the user name for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Password</b>	Enter the password for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Management IP</b>	Enter the IP address used to access the management API of the NetApp Storage Virtual Machine. If the data LIFs (Logical Interfaces) corresponding to the SVM Name above already allow management access, this field is not required.

<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Storage Virtual Machine. The Storage Virtual Machine must be able to route traffic to this IP address. If the IP address you want does not appear, manually enter the address.
<b>Access Path</b>	Use only when experiencing access issues. Contact Peer Software support for more information.

2. Click **Validate**.
3. Click **Next**.

The [Source Paths](#) page is displayed.

1. Enter the credentials to connect to the NetApp 7-Mode filer or vFiler hosting the data to be replicated or select existing credentials.

Create Cloud Backup and Replication Job Wizard

### Storage Information

Enter the information required to connect to the source storage platform.

Source Storage Platform

- Management Agent
- Proxy Configuration
- Storage Information**

Source Paths

- File Filters

Destination

- Azure Storage Credentials
- Container Details
- Replication and Retention Policy
- Miscellaneous Options
- Email Alerts
- SNMP Notifications
- Confirmation

**Credentials**

☒ New Credentials

\*Filer Name:

☐ Existing Credentials

Access Path:

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp 7-Mode environments.

< Back   Next >   Cancel

<b>File r Na me</b>	Enter the name of the NetApp 7-Mode filer or vFiler hosting the data to be replicated.
<b>Acc ess Pat h</b>	Use only when experiencing access issues. Contact Peer Software support for more information.

- Click **Validate**.
- Click **Next**.

The [Source Paths](#) page is displayed.

1. Enter the credentials to connect to the EMC Isilon cluster hosting the data to be replicated or select existing credentials.

**Storage Information**  
Enter the information required to connect to the source storage platform.

**Source Storage Platform**  
Management Agent  
Proxy Configuration  
**Storage Information**  
Source Paths  
File Filters  
Destination  
Azure Storage Credentials  
Container Details  
Replication and Retention Policy  
Miscellaneous Options  
Email Alerts  
SNMP Notifications  
Confirmation

**Credentials**  
☒ New Credentials  
☐ Existing Credentials

\*Cluster Name:   
\*Cluster Username:   
\*Cluster Password:   
Cluster Management IP:  **Advanced**

Access Path  
Access Path:  **Browse**

**Validate**

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Isilon environments.

< Back   Next >   Cancel

<b>Cluster Name</b>	Enter the name of the EMC Isilon cluster hosting the data to be replicated.
<b>Cluster Username</b>	Enter the user name for the account managing the EMC Isilon cluster.
<b>Cluster Password</b>	Enter the password for account managing the EMC Isilon cluster.

<b>Cluster Management IP</b>	Enter the IP address of the system used to manage the EMC Isilon cluster. Required only if multiple Access Zones are in use on the cluster.
<b>Access Path</b>	Use only when experiencing access issues. Contact Peer Software support for more information.

2. Click **Validate**.
3. Click **Next**.

The [Source Paths](#) page is displayed.

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.



Create Cloud Backup and Replication Job Wizard

### Storage Information

Enter the information required to connect to the source storage platform.

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information**
- Source Paths
  - File Filters
- Destination
  - Azure Storage Credentials
  - Container Details
  - Replication and Retention Policy
  - Miscellaneous Options
  - Email Alerts
  - SNMP Notifications
  - Confirmation

**Credentials**

☒ New Credentials

\*CIFS Server Name:

\*Unisphere Username:

\*Unisphere Password:

\*Unisphere Management IP:

☐ Existing Credentials

**Access Path**

Access Path:

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Unity environments.

< Back   Next >   Cancel

<b>CIFS Server Name</b>	Enter the name of the CIFS server hosting the data to be replicated.
<b>Unisphere Username</b>	Enter the user name for the Unisphere account managing the Unity storage device.
<b>Unisphere Password</b>	Enter the password for the Unisphere account managing the Unity storage device.
<b>Unisphere</b>	Enter the IP address of the Unisphere system used to manage the Unity storage device. This should not point to the CIFS server.

<b>Management IP</b>	
<b>Access Path</b>	Use only when experiencing access issues. Contact Peer Software support for more information.

2. Click **Validate**.
3. Click **Next**.

The [Source Paths](#) page is displayed.

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.

Create Cloud Backup and Replication Job Wizard

### Storage Information

Enter the information required to connect to the source storage platform.

Source Storage Platform

- Management Agent
- Proxy Configuration
- Storage Information**

Source Paths

- File Filters

Destination

- Azure Storage Credentials
- Container Details
- Replication and Retention Policy
- Miscellaneous Options
- Email Alerts
- SNMP Notifications
- Confirmation

**Credentials**

☒ New Credentials

\*CIFS Server Name:

\*Control Station Username:

\*Control Station Password:

\*Control Station IP:

☐ Existing Credentials

**Access Path**

Access Path:

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC VNX/Celerra environments.

< Back   Next >   Cancel

<b>CIFS Server Name</b>	Enter the name of the CIFS Server hosting the data to be replicated.
<b>Control Station Username</b>	Enter the user name for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station Password</b>	Enter the password for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station</b>	Enter the IP address of the Control Station system used to manage the Celerra/VNX storage device. This should not point to the CIFS Server.

<b>IP</b>	
<b>Access Path</b>	Use only when experiencing access issues. Contact Peer Software support for more information.

2. Click **Validate**.

3. Click **Next**.

The [Source Paths](#) page is displayed.

1. Enter the credentials to connect to the Nutanix Files cluster hosting the data to be replicated or select existing credentials.

Create Cloud Backup and Replication Job Wizard

### Storage Information

Enter the information required to connect to the source storage platform.

Source Storage Platform

- Management Agent
- Proxy Configuration
- Storage Information**

Source Paths

- File Filters

Destination

- Azure Storage Credentials
- Container Details
- Replication and Retention Policy
- Miscellaneous Options
- Email Alerts
- SNMP Notifications
- Confirmation

**Credentials**

☒ New Credentials

\*Nutanix File Server Name:

\*Username:

\*Password:

\*Peer Agent IP:

☐ Existing Credentials

AFS2, user:admin

Having trouble connecting? Please verify that all [prerequisites](#) are met for Nutanix Files environments.

< Back   Next >   Cancel

<b>Nutanix File Server Name</b>	Enter the name of the Nutanix Files cluster hosting the data to be replicated.
<b>Username</b>	Enter the user name for the account managing the Nutanix Files cluster via its management APIs.
<b>Password</b>	Enter the password for the account managing the Nutanix Files cluster via its management APIs.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Nutanix Files cluster. The Files server must be able to route traffic to this IP address. If the IP address you want does not appear, manually enter the address. This should not point to the Files cluster itself.

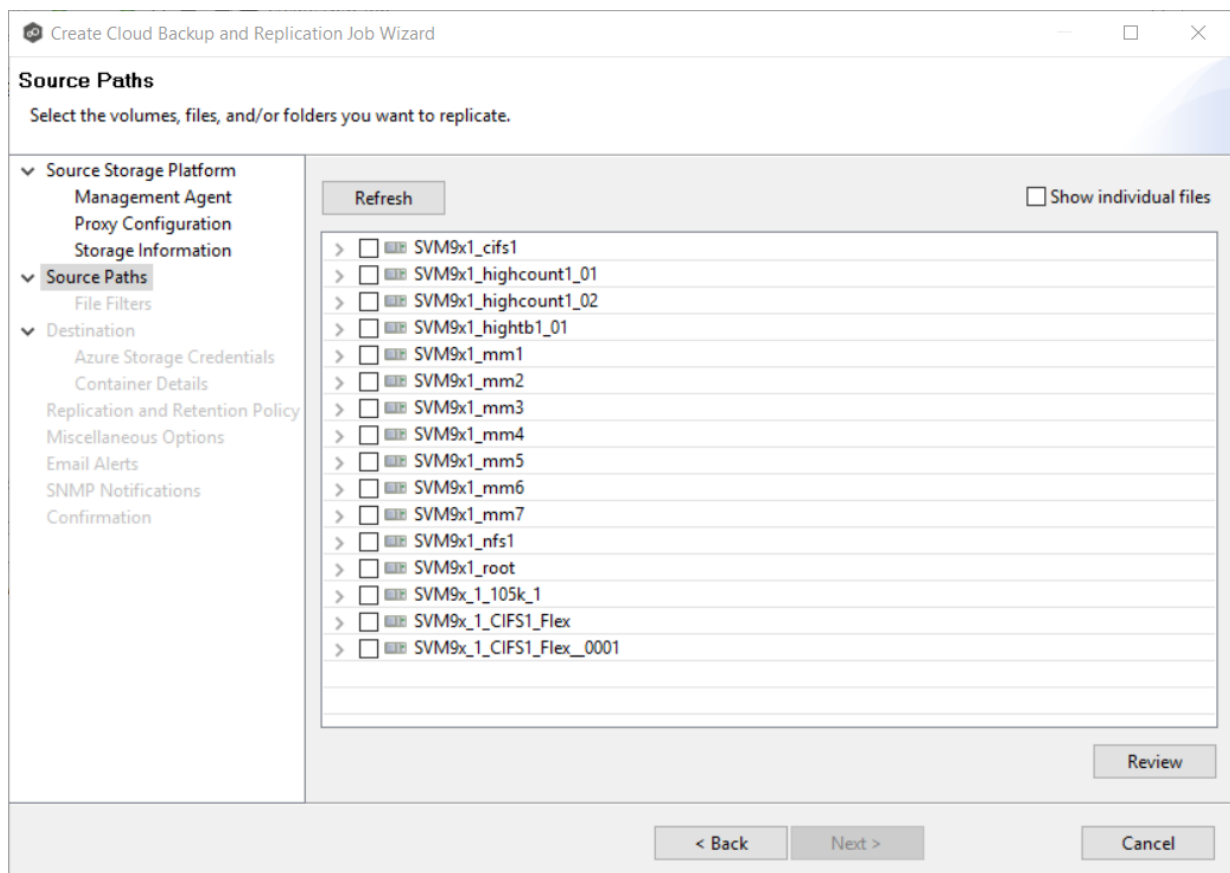
2. Click **Validate**.
3. Click **Next**.

The [Source Paths](#) page is displayed.

## Step 6: Source Paths

The **Source Paths** page displays a list of available volumes to replicate. You can choose to replicate an entire volume or selectively replicate files and folders. The files/folders/volumes selected for replication are referred to as the [watch set](#).

1. Select the paths to the files/folders/volumes you want to replicate.



To replicate:

<b>The entire volume (all files and folders, including subfolders and their files)</b>	Select the volume checkbox.
<b>All files at the root level of the volume (but no folders)</b>	Expand the volume, scroll to the bottom of the expanded list, and select <b>All Files</b> .
<b>A specific folder and its content (including subfolders and their files)</b>	Expand the volume, find the desired folder, and select its checkbox.
<b>All files within a specific folder (but not the folder)</b>	Expand the folder and select <b>All Files</b> .
<b>Specific files and folders</b>	Select the <b>Show individual files</b> checkbox, expand the folders, and select the files and folders you want to replicate.

2. (Optional) Click the **Review** button to see your selections.
3. Click **Next**.

The [File and Folder Filters](#) page appears.

## Step 7: File and Folder Filters

The **File and Folder Filters** page displays a list of [file and folder filters](#). A file or folder filter enables you to exclude and/or include files and folders from the job based on file type, extension, name, or directory path. Any file or folder that matches the filter is excluded or included from replication, depending on the filter's definition. By default, all files and folders selected in the **Source Paths** page will be replicated.

1. Select the file and folder filters you want to apply to the job.

If you want to create a new file or folder filter or modify an existing one, click **Edit File Filters**. See [File and Folder Filters](#) in the [Preferences](#) section for information about creating or modifying a file filter.

[illegible]

2. Select the **Include Files Without Extensions** checkbox if you want to replicate files that do not have extensions.

**Note:** Files without extensions are ignored during replication unless you select this checkbox.

3. Click **Next**.

The [Destination](#) page appears.

## Step 8: Destination

The **Destination** page displays a list of the available storage platforms to which Cloud Backup and Replication can replicate. Currently, the following platforms are supported:

- Microsoft Azure

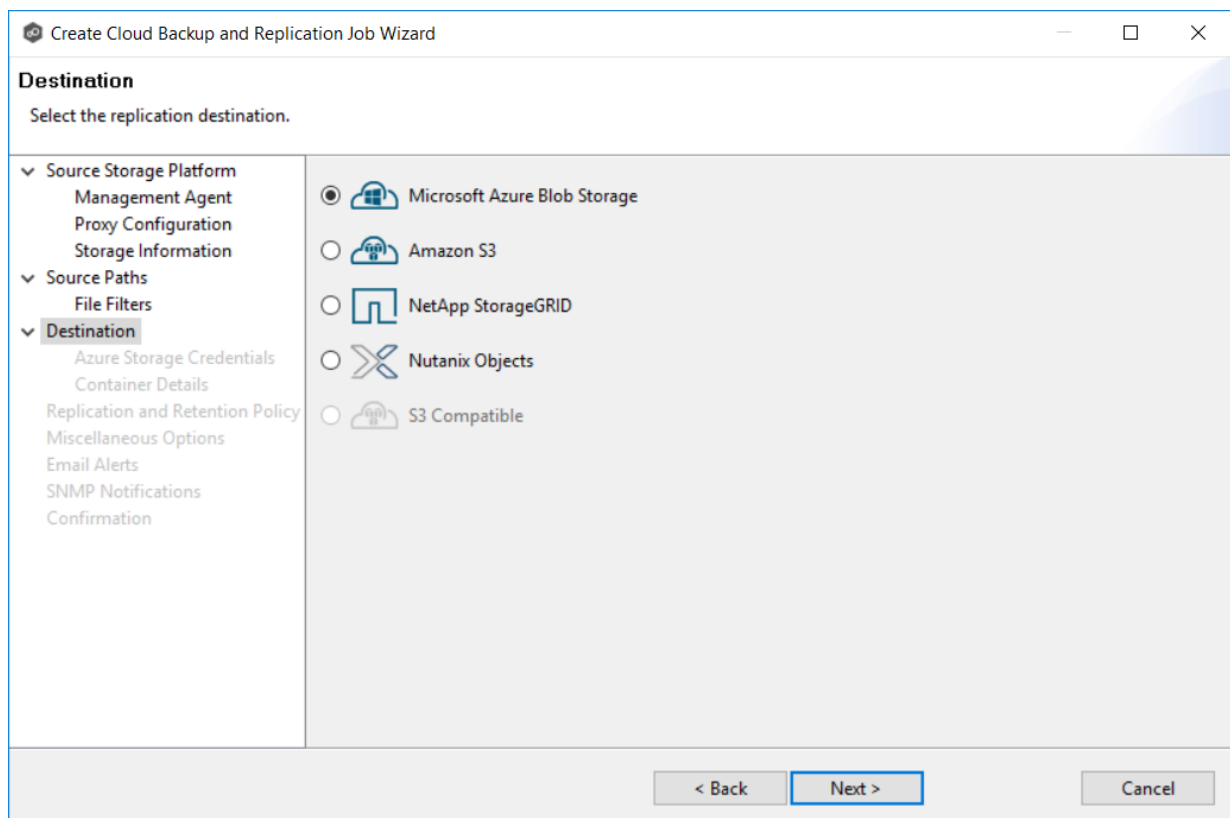


- Amazon S3
- NetApp StorageGRID
- Nutanix Objects

In addition, some S3-compatible platforms are also supported. Contact your Peer Software Sales representative to see if the S3 compatible platform you want to use is supported.

**Important:** You should create the storage account before creating the Cloud Backup and Replication job.

1. Select the type of destination storage platform.



2. Click **Next**.

The [Destination Credentials](#) page appears.

**Step 9: Destination Credentials**

The **Credentials** page requests the credentials necessary to connect to the destination storage account.

1. Select **New Credentials** to enter a new set of credentials for the destination storage device or select **Existing Credentials**.
2. If you selected **Existing Credentials**, select a credential from the drop-down list.

If you selected **New Credentials**, enter the credentials for connecting to the destination storage account. The information you are prompted to enter varies, depending on the type of storage platform:

[Azure Blob Storage Credentials](#)

[Amazon S3 Credentials](#)

[NetApp StorageGRID](#)

[Nutanix Objects](#)

3. Click **Next**.

The **Details** page for the selected destination storage account.

1. Enter the credentials to connect to a Microsoft Azure storage account. General Purpose and Blob storage accounts are supported.

Create Cloud Backup and Replication Job Wizard

### Azure Storage Credentials

Enter new credentials or select existing credentials.

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information
- Source Paths
  - File Filters
- Destination
  - Azure Storage Credentials**
  - Container Details
  - Replication and Retention Policy
  - Miscellaneous Options
  - Email Alerts
  - SNMP Notifications
  - Confirmation

**Credentials**

☒ New Credentials

\*Description:

\*Account:

\*Shared Key:  ☐ Show Key

\*Endpoint Type:

☒ Use SSL

☐ Existing Credentials

< Back   **Next >**   Cancel

<b>Description</b>	Enter a name for the credentials.
<b>Account</b>	Enter the name of the Azure storage account, which can be found in the Azure Portal.
<b>Shared Key</b>	Enter one of the shared keys for the Azure Storage account. The shared keys can be found in the Azure Portal.
<b>Endpoint Type</b>	Select the type of data center endpoint. The options are: <b>Public</b> , <b>Germany</b> , <b>China</b> , <b>US Government</b> , and <b>Custom</b> .
<b>Endpoint</b>	If you selected <b>Custom</b> for <b>Endpoint Type</b> , the <b>Endpoint</b> field appears. Enter the IP address of the endpoint.
<b>Use SSL</b>	Select this if you want to use the SSL (Secure Sockets Layer) protocol to communicate with the destination rather than the standard (non-encrypted) HTTP protocol.

- Click **Validate** to test the connection.

If you are using a proxy in your environment and you get an error while trying to validate, you may want to check the [proxy configuration](#) in [Preferences](#).

- Click **Next**.

The [Container Details](#) page appears.

- Enter the credentials to connect to an Amazon S3 storage account.

**Desc  
ription**

Enter a name for the credentials.

<b>Access Key</b>	Enter one of the shared keys of the Amazon S3 Storage account, which can be found in the Amazon AWS portal.
<b>Secret Key</b>	Enter the secret key of the Amazon S3 Storage account, which can be found in Amazon AWS portal.
<b>Use SSL</b>	Select this if you want to use the SSL (Secure Sockets Layer) protocol to communicate with the destination rather than the standard (non-encrypted) HTTP protocol.

2. Click **Validate** to test the connection.

If you are using a proxy in your environment and you get an error while trying to validate, you may want to check the [proxy configuration](#) in [Preferences](#).

3. Click **Next**.

The [Bucket Details](#) page appears.

1. Enter the credentials to connect to a NetApp StorageGRID storage account.

**Create Cloud Backup and Replication Job Wizard**

**NetApp StorageGRID Credentials**  
Enter new credentials or select existing credentials.

☒ **New Credentials**  
 \*Description:   
 \*Access Key:   
 \*Secret Key:  ☐ Show Key  
 \*Service Point:   
☒ Use SSL  
☐ **Existing Credentials**

Validate

< Back **Next >** Cancel

<b>Description</b>	Enter a name for the credentials.
<b>Access Key</b>	Enter one of the shared keys of the NetApp StorageGRID account, which can be found in the Tenant Manager.
<b>Secret Key</b>	Enter the secret key of the NetApp StorageGRID account, which can be found in the Tenant Manager.
<b>Service</b>	Enter the IP or name of the object store.

Poin t	
<b>Use SSL</b>	Select this if you want to use the SSL (Secure Sockets Layer) protocol to communicate with the destination rather than the standard (non-encrypted) HTTP protocol.

- Click **Validate** to test the connection.
- Click **Next**.

The [Container Details](#) page appears.

- Enter the credentials to connect to a Nutanix Objects storage account.

Create Cloud Backup and Replication Job Wizard

**Nutanix Objects Credentials**  
Enter new credentials or select existing credentials.

Source Storage Platform  
Management Agent  
Proxy Configuration  
Storage Information

Source Paths  
File Filters

Destination  
**Nutanix Objects Credentials**  
Bucket Details  
Replication and Retention Policy  
Miscellaneous Options  
Email Alerts  
SNMP Notifications  
Confirmation

**Credentials**  
☒ New Credentials  
\*Description:   
\*Access Key:   
\*Secret Key:  ☐ Show Key  
\*Service Point:   
☒ Use SSL  
☐ Existing Credentials  
Nutanix Objects Credentials

Validate

< Back Next > Cancel

<b>Description</b>	Enter a name for the credentials.
<b>Access Key</b>	Enter one of the shared keys of the Nutanix Objects account, which can be found in Prism Central.
<b>Secret Key</b>	Enter the secret key of the Nutanix Objects account, which can be found in Prism Central.
<b>Service Point</b>	Enter the IP or name of the object store.
<b>Use SSL</b>	Select this if you want to use the SSL (Secure Sockets Layer) protocol to communicate with the destination rather than the standard (non-encrypted) HTTP protocol.

2. Click **Validate** to test the connection.
3. Click **Next**.

The [Container Details](#) page appears.

#### Step 10: Container or Bucket Details

The **Container Details** or **Bucket Details** page allow you to create a new storage container or bucket or choose an existing one.

1. Select **New Container/New Bucket** to create a new storage container/bucket; otherwise, select **Existing Container/Existing Bucket** to choose an existing one.
2. If you selected **Existing Container** or **Existing Bucket**, select a container or bucket from the drop-down list.

If you selected **New Container** or **New Bucket**, enter the requested information. The information you are prompted to enter varies, depending on the type of storage platform:

[Azure Blob Storage Container Details](#)



[Amazon S3 Bucket Details](#)

[NetApp StorageGRID Bucket Details](#)

[Nutanix Objects Bucket Details](#)

3. Click **Next**.

The [Replication and Retention Policy](#) page appears.

1. Select **New Container** to create a new container or select **Existing Container**.

Choose **Existing Container** if:

- You (or someone else) already created a container you want to use.
- You want to use a container that was created outside Peer Management Center.
- You don't have the permissions required to create a new container and want to use one that someone else will create.

Create Cloud Backup and Replication Job Wizard

**Container Details**  
Create a new container or select an existing one.

Source Storage Platform  
Management Agent  
Proxy Configuration  
Storage Information

Source Paths  
File Filters

Destination  
Azure Storage Credentials  
**Container Details**  
Replication and Retention Policy  
Miscellaneous Options  
Email Alerts  
SNMP Notifications  
Confirmation

☒ New Container

\*Name:  
dgagent2-mykirzevab

☒ Automatically name

☐ Existing Container

< Back   Next >   Cancel

2. If you selected **Existing Container**, select a container from the drop-down list. If the container does not appear in the list because the person who has the permissions to create a container has not yet created the bucket, click the **Reload** button after the container is created. The container will appear in the updated list.

If you selected **New Container**, you have two options. By default, the **Automatically name** checkbox is selected. You can deselect the checkbox and enter a name for the container; the container name must conform to the following naming rules:

- A container name must be unique.
- A container name must be a valid DNS name.
- A container name must start with a letter or number, and can contain only letters, numbers, and the dash (-) character.
- Every dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in container names.

- All letters in a container name must be lowercase.
- A container name must be from 3 through 63 characters long.

For more information about container names, see [Naming and referencing containers, blobs, and metadata](#).

3. Click **Next**.

The [Replication and Retention Policy](#) page appears.

1. Select **New Bucket** to create a new bucket or select **Existing Bucket**.

Choose **Existing Bucket** if:

- You (or someone else) already created a bucket you want to use.
- You want to use a bucket that was created outside Peer Management Center.
- You don't have the permissions required to create new buckets and want to use one that someone else will create.

Create Cloud Backup and Replication Job Wizard

### Bucket Details

Create a new bucket or select an existing one.

Source Storage Platform  
Management Agent  
Proxy Configuration  
Storage Information

Source Paths  
File Filters

Destination  
Amazon S3 Credentials  
**Bucket Details**  
Replication and Retention Policy  
Miscellaneous Options  
Email Alerts  
SNMP Notifications  
Confirmation

☒ New Bucket

\*Name:  
dgagent2-qczkmxosg

☒ Automatically name

\*Region:  
US East (N. Virginia)

☐ Existing Bucket

< Back   Next >   Cancel

2. If you selected **Existing Bucket**, select a bucket from the drop-down list. If the bucket does not appear in the list because the person who has the permissions to create a bucket has not yet created the bucket, click **Reload** after the bucket is created. The bucket will appear in the updated list.

If you selected **New Bucket**, you have two options. By default, the **Automatically name** checkbox is selected. You can deselect the checkbox and enter a name for the bucket; the bucket name must conform to the following naming rules:

- A bucket name must be unique across all existing bucket names in Amazon S3 (that is, across all AWS customers). For more information, see [Bucket Restrictions and Limitations](#).
- Bucket names must comply with DNS naming conventions. For information about legacy non-DNS-compliant bucket names, see [Bucket Restrictions and Limitations](#).
- A bucket name must start with a lowercase letter or number.
- A bucket name must not contain uppercase characters or underscores.
- A bucket name must be from 3 through 63 characters long.

- A bucket name must be a series of one or more labels. Adjacent labels are separated by a single period (.). Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number.
- A bucket name must not be formatted as an IP address (for example, 192.168.5.4).
- When you use virtual hosted-style buckets with Secure Sockets Layer (SSL), the SSL wildcard certificate only matches buckets that don't contain periods. To work around this, use HTTP or write your own certificate verification logic. We recommend that you do not use periods (".") in bucket names when using virtual hosted-style buckets.
- Choose a bucket name that reflects the objects in the bucket because the bucket name is visible in the URL that points to the objects that you're going to put in your bucket. After you create the bucket, you cannot change the name, so choose wisely.

For information about naming buckets, see [Rules for Bucket Naming](#) in the Amazon Simple Storage Service Developer Guide.

3. Select the region where you want the bucket to reside.

**Important:** After you have created a bucket, you cannot change its region.

4. Click **Next**.

The [Replication and Retention Policy](#) page appears.

1. Select **New Bucket** to create a new bucket or select **Existing Bucket**.

Choose **Existing Bucket** if:

- You (or someone else) already created a bucket you want to use.
- You want to use a bucket that was created outside Peer Management Center.
- You don't have the permissions required to create new buckets and want to use one that someone else will create.

Create Cloud Backup and Replication Job Wizard

### Bucket Details

Create a new bucket or select an existing one.

Source Storage Platform

- Management Agent
- Proxy Configuration
- Storage Information

Source Paths

- File Filters

Destination

- NetApp StorageGRID Credential
- Bucket Details**
- Replication and Retention Policy
- Miscellaneous Options
- Email Alerts
- SNMP Notifications
- Confirmation

New Bucket

\*Name:

dgagent2-yvgjhyrdsb

☒ Automatically name

Existing Bucket

< Back Next > Cancel

1. If you selected **Existing Bucket**, select a bucket from the drop-down list. If the bucket does not appear in the list because the person who has the permissions to create a bucket has not yet created the bucket, click **Reload** after the bucket is created. The bucket will appear in the updated list

If you selected **New Bucket**, you have two options. By default, the **Automatically name** checkbox is selected. You can deselect the checkbox and enter a name for the bucket; the bucket name must comply with the following rules:

- Must be unique across each StorageGRID Webscale system (not just unique within the tenant account).
- Must be DNS compliant.
- Must contain between 3 and 63 characters.
- Can be a series of one or more labels, with adjacent labels separated by a period. Each label must start and end with a lowercase letter or a number and can only use lowercase letters, numbers, and hyphens.

- Must not look like a text-formatted IP address.
- Should not use periods in virtual hosted-style requests because periods will cause problems with server wildcard certificate verification.

For information about naming buckets, see [Rules for Bucket Naming](#) in the Amazon Simple Storage Service Developer Guide.

2. Click **Next**.

The [Replication and Retention Policy](#) page appears.

1. Select **New Bucket** to create a new bucket or select **Existing Bucket**.

Choose **Existing Bucket** if:

- You (or someone else) already created a bucket you want to use.
- You want to use a bucket that was created outside Peer Management Center.
- You don't have the permissions required to create new buckets and want to use one that someone else will create.

2. If you selected **Existing Bucket**, select a bucket from the drop-down list. If the bucket does not appear in the list because the person who has the permissions to create a bucket has not yet created the bucket, click **Reload** after the bucket is created. The bucket will appear in the updated list

If you selected **New Bucket**, you have two options. By default, the **Automatically name** checkbox is selected. You can deselect the checkbox and enter a name for the bucket; the bucket name must comply with the following rules:

- Must start with a number or a letter.
- Must be 3 - 255 characters long.
- Can contain lowercase letters, numbers, underscores (\_), and dashes (-).
- There may be additional restrictions on bucket names in some AWS regions. We recommend that you create bucket names that are DNS-compliant, if you want to access objects using URL. For more information, see [Amazon Simple Storage Service Console user's guide](#).



3. Click **Next**.

The [Replication and Retention Policy](#) page appears.

### Step 11: Replication and Retention Policy

Each Cloud Backup and Replication job must have a Replication and Retention policy. A Replication and Retention policy specifies:

- How often you want to scan the storage device for replication or if you want to replicate in real-time.
- Whether you want to take snapshots of the data. A **snapshot** captures the state of a file system at a point in time. There are two types of snapshots:
  - A **destination snapshot** captures an image of the data on the destination storage device immediately after replication. Destination snapshots are useful for recovering data from different period of times. Destination snapshots track versions of changed files and file system structure that can be used for data recovery. For more information about recovering data, see [Recovering Data](#).
  - A **source snapshot** captures an image of the data on the source storage device immediately before replication. Sources snapshots are useful for replicating open and locked files, which otherwise may not be able to be replicated. A source snapshot also ensures that the replicated data is coming from a static version of the source file system. For details about using source snapshots, see [Step 13: Source Snapshots](#).
- How long you want to retain destination snapshots.

The **Replication and Retention Policy** page enables you to create a new Replication and Retention policy or choose an existing policy.

1. Select **New Policy** or **Existing Policy**.

2. If you selected **Existing Policy**, select a policy from the drop-down list, and then click **Next**. Continue with [Step 14. Miscellaneous Options](#).

If you selected **New Policy**, enter a name for the policy in the **Name** field.

3. Select **Enable Backup with Destination Snapshots** if you want to replicate what is on premises to the [destination storage device](#), while taking [destination snapshots](#) at specified points in times.
4. Click **Next**.

The [Replication Schedule](#) page appears.

## Step 12: Replication Schedule

The **Replication Schedule** page enables you to select the frequency of the replication and when snapshots should be taken. Replication can be performed on a scheduled, batched real-time, or a continuous real-time basis.

1. Select the frequency of the replication:

- [Scheduled Scans](#) – Select this option if you want to replicate files on a scheduled basis. A scan of changes to the file system occurs on a scheduled basis, either daily or weekly, and replication of changes occurs as the scan progresses.
- [Batched Real-time](#) – Select this option if you want to continuously monitor changes to the file system but replicate changes on scheduled basis. Changes are monitored in real-time and only the latest version of changed file is replicated at scheduled times. An initial scan can be performed to establish a baseline.
- [Continuous Data Protection](#) – Select this option if you want continuously monitor changes and replicate changes in real-time. Whenever a file changes, the change is replicated in real-time.

2. Click **Next**.

The [Retention](#) page appears.

If you selected **Scheduled Scans** for the replication frequency:

1. Select the **Scan at Start** checkbox if you want a baseline replication to be performed.
2. Select **Daily** or **Weekly** for the frequency of the scans:
  - Select **Daily** if you want replications performed every day. You can schedule one to four scans per day
  - Select **Weekly** if you want to select specific days for replication. You can select one scan per day.
3. Select the day(s) and time(s) when you want the replication performed:
  - If you selected **Daily**, select the times you want the scans performed. Then, if you selected **Enable Backup with Destination Snapshots** in [Step 10](#), choose when snapshots are taken (you must take at least one snapshot). If you did not select the backup option, the **Take Destination Snapshot** options will not appear.

Create Cloud Backup and Replication Job Wizard

### Replication Schedule

✖ You must select at least one replication time.

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information
- Source Paths
  - File Filters
- Destination
  - Amazon S3 Credentials
  - Bucket Details
- Replication and Retention Policy
  - Replication Schedule**
  - Retention
  - Source Snapshots
  - Miscellaneous Options
  - Email Alerts
  - SNMP Notifications
  - Confirmation

☒ Scheduled Scans

☒ Daily ☐ Weekly

Times (up to 4)

None	<input type="checkbox"/> Take Destination Snapshot
None	<input type="checkbox"/> Take Destination Snapshot
None	<input type="checkbox"/> Take Destination Snapshot
None	<input type="checkbox"/> Take Destination Snapshot

☐ Scan at Start

☐ Batched Real-time

☐ Continuous Data Protection

< Back    Next >    Cancel

- If you selected **Weekly**, select the day(s) and time you want the replication performed. Then, if you selected **Enable Backup with Destination Snapshots** in Step 10, choose when snapshots are taken. You must take at least one snapshot. If you did not select the backup option, the **Destination Snapshot** option will not appear.

Create Cloud Backup and Replication Job Wizard

### Replication Schedule

You must select at least one day.

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information
- Source Paths
  - File Filters
- Destination
  - Amazon S3 Credentials
  - Bucket Details
- Replication and Retention Policy
  - Replication Schedule**
  - Retention
  - Source Snapshots
  - Miscellaneous Options
  - Email Alerts
  - SNMP Notifications
  - Confirmation

☒ Scheduled Scans

☐ Daily ☒ Weekly

Day(s):

- ☐ Sunday
- ☐ Monday
- ☐ Tuesday
- ☐ Wednesday
- ☐ Thursday
- ☐ Friday
- ☐ Saturday

Time:  ☒ Take Destination Snapshot

☐ Scan at Start

☐ Batched Real-time

☐ Continuous Data Protection

< Back Next > Cancel

4. Click **Next**.

The [Retention](#) page appears.

If you selected **Batched Real-time** for the replication frequency:

1. Select **Scan at Start** if you want a baseline replication to be performed.
2. Select the frequency of the replications; you can schedule one to four replications per day.
3. If you selected **Enable Backup with Destination Snapshots** in [Step 10](#), choose when destination snapshots are taken (you must take at least one snapshot). The destination snapshot will be taken after the files have been replicated. If you did not select the backup option, the **Take Destination Snapshot** option will not appear.

4. Click **Next**.

The [Retention](#) page appears.

If you selected **Continuous Data Protection** for the replication frequency:

1. Enter a value for **Processing Delay** if you want the replication to occur after a slight delay. A delay is useful to ensure that when a file or folder is created and quickly renamed, only the latest copy of the file or folder is replicated. This reduces WAN usage.
2. If you selected **Enable Backup with Destination Snapshots** in [Step 10](#), choose when snapshots are taken (you must take at least one snapshot). If you did not select the backup option, the **Take Destination Snapshot at** options will not appear.

Create Cloud Backup and Replication Job Wizard

### Replication Schedule

✖ You must select at least one destination snapshot trigger time.

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information
- Source Paths
  - File Filters
- Destination
  - Amazon S3 Credentials
  - Bucket Details
- Replication and Retention Policy
  - Replication Schedule**
  - Retention
  - Source Snapshots
  - Miscellaneous Options
  - Email Alerts
  - SNMP Notifications
  - Confirmation

☐ Scheduled Scans

☐ Batched Real-time

☒ Continuous Data Protection

Processing Delay: 5 minutes

Take Destination Snapshot at:

None

None

None

None

< Back   Next >   Cancel

3. Click **Next**.

The [Retention](#) page appears.

### Step 13: Retention

The **Retention** page enables you to define how long you want to retain destination snapshots. You have the option to retain destination snapshots on a daily, weekly, monthly, and yearly basis. If you did not select the **Enable Backup with Destination Snapshots** in Step 10, the **Retention** page will not appear.

1. Select the **Purge all versions between snapshots** checkbox if you do not want to indefinitely retain all versions.
2. Select the retention options. The options vary according to the replication schedule you selected.

**Retention**  
Select retention options.

- ☒ Purge all versions between snapshots
- ☒ Keep daily destination snapshots taken
  - at: 05:00, 15:00, 20:00
  - for: 30 day(s)
- ☒ Keep weekly destination snapshots taken
  - at: 05:00
  - on: Monday
  - for: 52 week(s)
- ☒ Keep monthly destination snapshots taken
  - at: 15:00
  - on: ☒ First ☐ Last
  - Tuesday
  - for: 60 month(s)
- ☒ Keep yearly destination snapshots taken
  - at: 20:00
  - on: January
  - ☒ First ☐ Last
  - Wednesday
  - for: 10 year(s)

< Back   Next >   Cancel

3. Click **Next**.

The [Source Snapshots](#) page appears.

#### Step 14. Source Snapshots

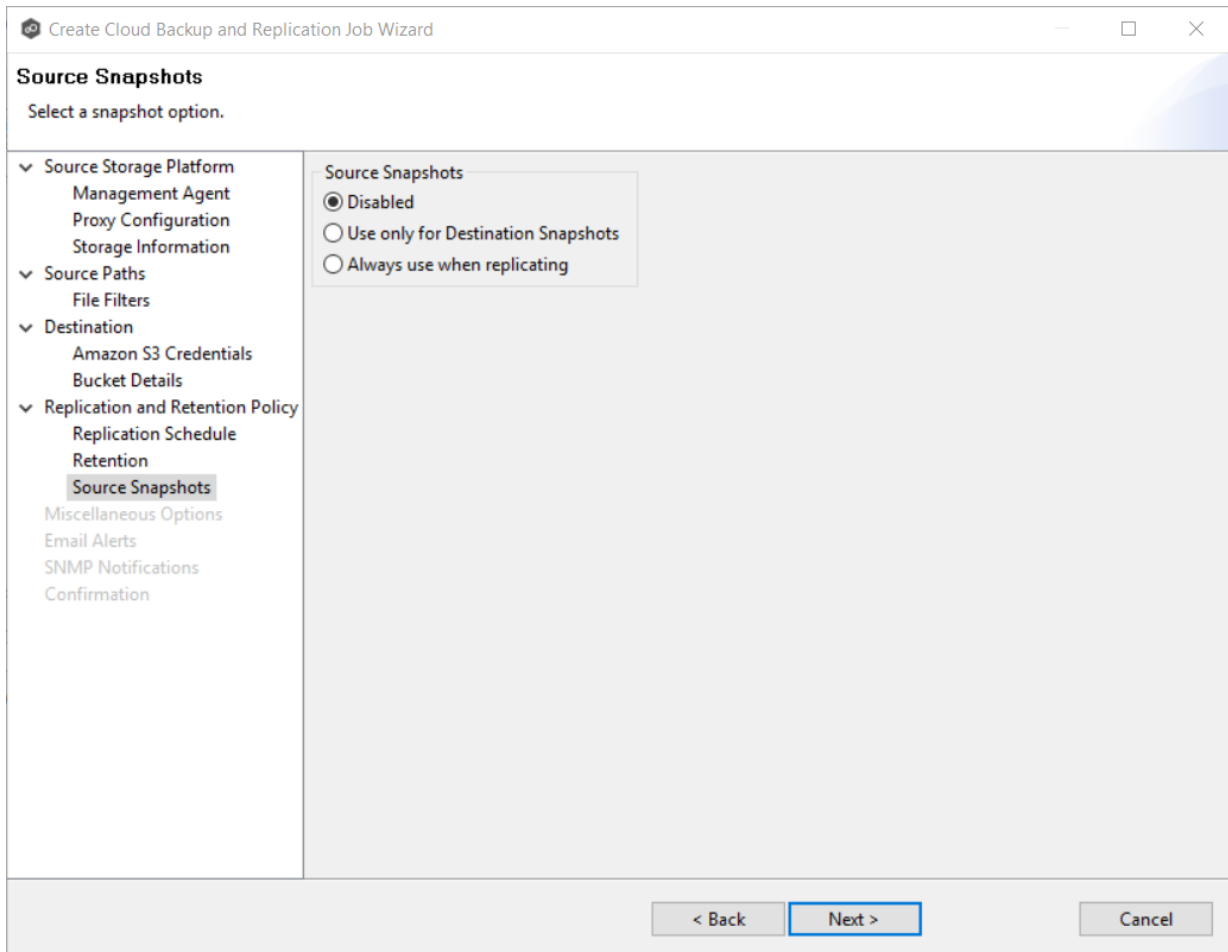
The **Source Snapshots** page enables you to choose whether to take snapshots of the source storage before the items are replicated. A [source snapshot](#) is a read-only point-in-time version of the volume. A source snapshot allows the creation of consistent backups of a volume, ensuring that the contents do not change and are not locked while the backup is being made. It can be used to provide a consistent state of a managed file, e.g. pst files, and help with errors accessing files that are currently open.

1. Select a source snapshot option:

- Select the **Disabled** option if you do not want to take source snapshots.



- Select the **Use only for Destination Snapshots** option when you want the source snapshot to be stored on the destination storage as the destination snapshot rather than an actual destination snapshot. To use this option, you must have selected the **Enable Backup with Destination Snapshot** in Step 10.
- Select **Always use when replicating** when you want to replicate always using source snapshots.



2. Click **Next**.

The [Miscellaneous Options](#) page appears.

### Step 15: Miscellaneous Options

The **Miscellaneous Options** page displays various options; the options available depend on the destination storage platform selected.

1. Select the options to apply to this job.

Option	Description
<b>NTFS Permissions</b>	<p>If you want NTFS permissions metadata included in the replication, select the elements to include:</p> <ul style="list-style-type: none"> <li>• <b>Owner</b> – The NTFS Creator-Owner who owns the object (which is, by default, whomever created it).</li> <li>• <b>DACL</b> – A Discretionary Access Control List identifies the users and groups that are assigned or denied access permissions on a file or folder.</li> <li>• <b>SACL</b> - A System Access Control List enables administrators to log attempts to access a secured file or folder. It is used for auditing.</li> </ul> <p>See <a href="#">File Metadata Synchronization</a> for more information about NTFS permissions metadata.</p>

Option	Description
<b>Storage Tier/Class</b>	<p>Only available with Azure Blob Storage with either a General Purpose v2 (GPv2) account or Blob Storage Account.</p> <p>Select a storage tier. If you do not select a tier, it will default to the tier you configured on your Azure Storage account.</p> <p>Azure Storage offers three storage tiers for blob object storage so that you can store your data most cost-effectively depending on how you use it:</p> <ul style="list-style-type: none"> <li>• <b>Azure Hot Storage Tier</b> is optimized for storing data that is accessed frequently.</li> <li>• <b>Azure Cool Storage Tier</b> is optimized for storing data that is infrequently accessed and stored for at least 30 days.</li> <li>• <b>Azure Archive Storage Tier</b> is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours). The archive storage tier is only available at the blob level and not at the storage account level.</li> </ul> <p>To read data in archive storage, Cloud Backup and Replication must first change the tier of the blob to hot or cool. This process is known as rehydration and can take up to 15 hours to complete.</p> <p><b>Rehydrated data</b> remains in hot or cool storage for a specified number of days before Cloud Backup and Replication automatically returns it to archive storage.</p>
<b>Rehydrated Data Availability (Days)</b>	<p>Only available with Azure Blob Storage with either a General Purpose v2 (GPv2) account or Blob Storage Account.</p> <p>Rehydrated data is automatically returned to archive storage after a specified period. Enter the number of days for rehydrated data to remain in hot or cool storage before returning to archive storage. The default is seven days.</p>

2. Click **Next**.

The [Email Alerts](#) page appears.

## Step 16: Email Alerts

This step is optional.

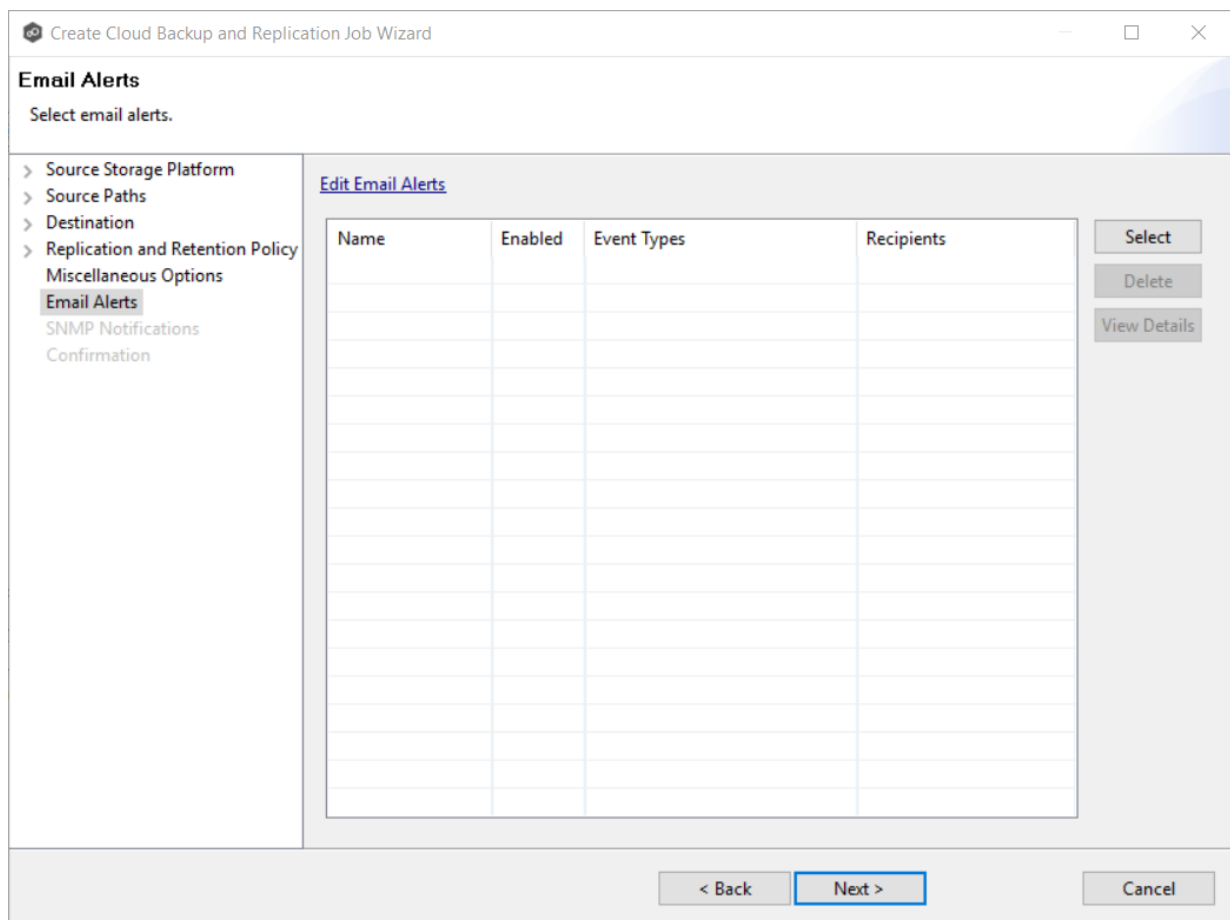
An [email alert](#) notifies recipients when a certain type of event occurs, for example, session abort, host failure, system alert. The **Email Alerts** page displays a list of email alerts that have been applied to the job. When you first create a job, this list is empty. Email alerts are defined in [Preferences](#) and can then be applied to multiple jobs of the same type.

Peer Software recommends that you create email alerts in advance. However, from this wizard page, you can select existing alerts to apply to the job or create new alerts to apply.

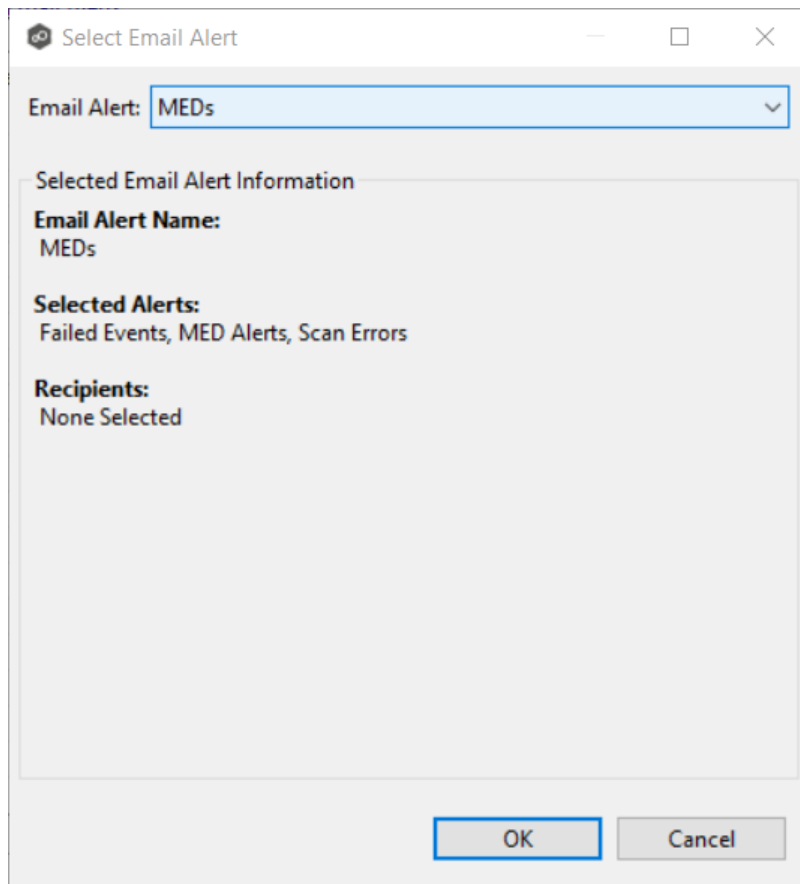
To create a new alert, see [Email Alerts](#) in the [Preferences](#) section.

To apply an existing email alert to the job:

1. Click the **Select** button.

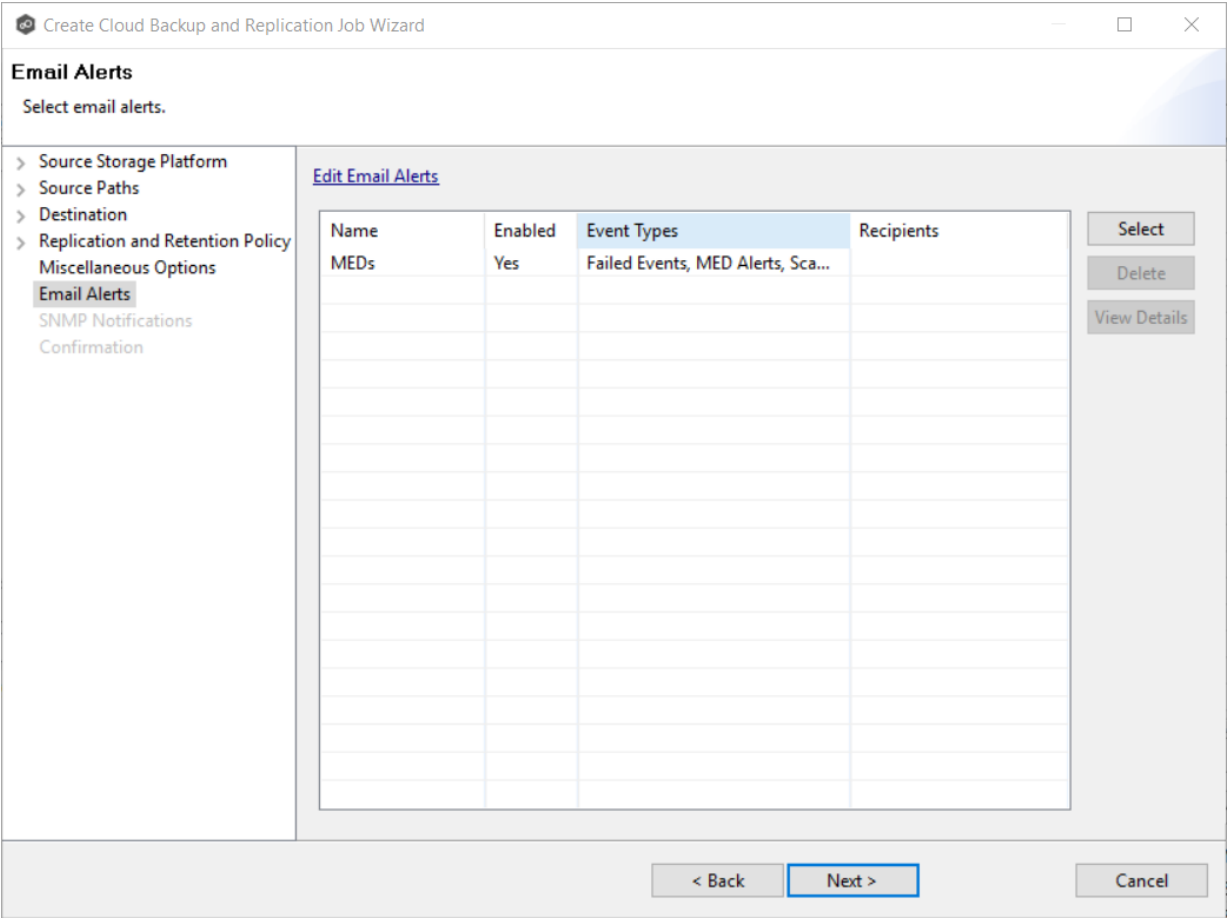


The **Select Email Alert** dialog appears.



2. Select an alert from the **Email Alert** drop-down list, and then click **OK**.

The alert is listed in the **Email Alerts** page.



3. (Optional) Repeat steps 1-3 to apply additional alerts.
4. Click **Next**.

The [SNMP Notifications](#) page appears.

## Step 17: SNMP Notifications

This step is optional.

An [SNMP notification](#) notifies recipients when certain type of event occurs, for example, session abort, host failure, system alert. The **SNMP Notifications** page displays a list of notifications that have been applied to the job. When you first create a job, this list is empty. Like email alerts and file filters, an SNMP notification is defined in [Preferences](#) and can then be applied to multiple jobs of the same type.

Peer Software recommends that you create SNMP notifications in advance. However, from this wizard page, you can select an existing SNMP notification to apply to the job or create new SNMP notifications.

To apply an existing SNMP notification to the job or disable notifications:

1. Select an SNMP notification from the drop-down list.

To disable, select **None - Disabled**.

Create Cloud Backup and Replication Job Wizard

### SNMP Notifications

- Source Storage Platform
  - Management Agent
  - Proxy Configuration
  - Storage Information
- Source Paths
  - File Filters
- Destination
  - Amazon S3 Credentials
  - Bucket Details
- Replication and Retention Policy
  - Replication Schedule
  - Retention
  - Source Snapshots
- Miscellaneous Options
- Email Alerts
- SNMP Notifications**
- Confirmation

[Edit SNMP Notifications](#)

SNMP Notification: **None - Disabled**

Selected SNMP Notification Information

**No SNMP Notification Selected**  
SNMP notifications disabled for this job

< Back   Next >   Cancel

2. Click **Next**.

The [Confirmation](#) page appears.

**Step 18: Confirmation**

The **Confirmation** page displays the job configuration.

1. Review the job configuration.
2. If you need to modify the job configuration after reviewing it, click **Back** until you reach the appropriate page and make your changes.

**Note:** You cannot change the job name.



Create Cloud Backup and Replication Job Wizard

**Confirmation**  
Review your job configuration.

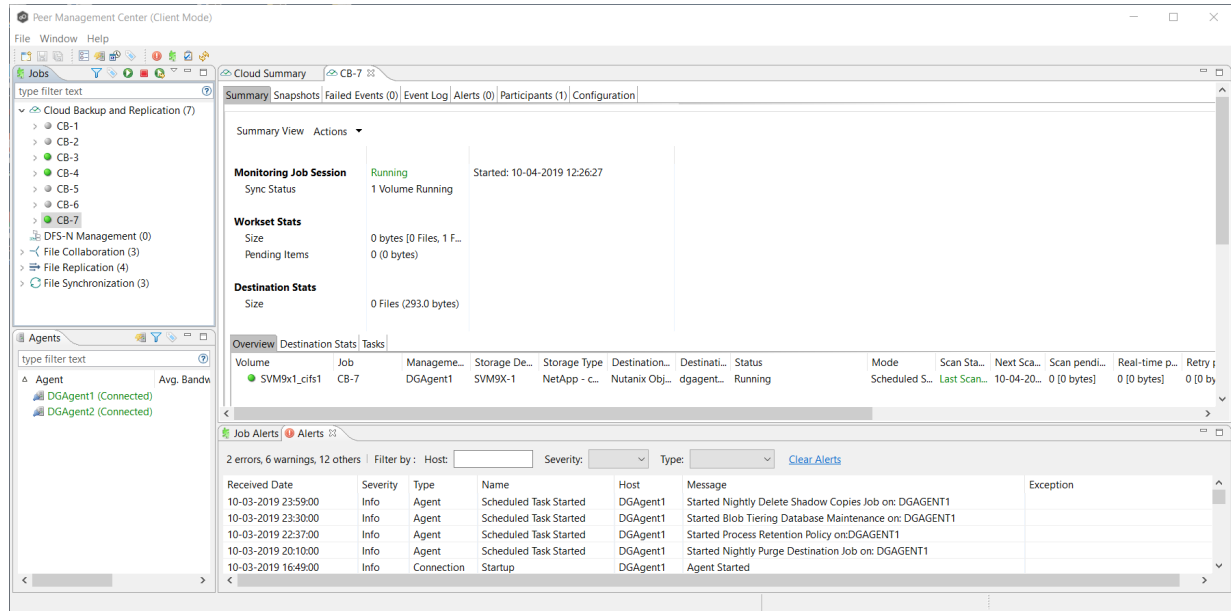
<ul style="list-style-type: none"> <li>Source Storage Platform             <ul style="list-style-type: none"> <li>Management Agent</li> <li>Proxy Configuration</li> <li>Storage Information</li> </ul> </li> <li>Source Paths             <ul style="list-style-type: none"> <li>File Filters</li> </ul> </li> <li>Destination             <ul style="list-style-type: none"> <li>NetApp StorageGRID Credential</li> <li>Bucket Details</li> <li>Replication and Retention Policy</li> <li>Miscellaneous Options</li> <li>Email Alerts</li> <li>SNMP Notifications</li> <li><b>Confirmation</b></li> </ul> </li> </ul>	<p><b>Source Storage:</b> NetApp ONTAP   Clustered Data ONTAP</p> <p><b>Management Agent:</b> DGAgent2</p> <p><b>Source Paths:</b> One or more specific paths</p> <p><b>Source Items:</b>  <b>Volume:</b> SVM9x1_mm1  <b>Destination:</b> -1  <b>Item(s) to Include:</b>          ..\</p> <p><b>Destination:</b> NetApp StorageGRID</p> <p><b>Replication and Retention Policy:</b> 3x Daily  <b>Replication Schedule:</b> Destination Snapshots</p> <p>Replicate every day</p> <p><b>Times:</b>          - 05:00 (Take destination snapshot)          - 15:00 (Take destination snapshot)          - 20:00 (Take destination snapshot)</p> <p><b>Retention Configuration (3x Daily):</b>          Purge all versions between destination snapshots: true</p> <p><b>Daily Retention</b>          Keep destination snapshots taken at:          - 05:00          - 15:00          - 20:00          For: 30 day(s)</p> <p><b>Weekly Retention</b>          Keep destination snapshots taken on:          - Monday          Taken at: 05:00          For: 52 weeks(s)</p> <p><b>Monthly Retention</b>          Keep destination snapshots taken on:          First          Tuesday          Taken at: 15:00          For: 60 month(s)</p> <p><b>Yearly Retention</b>          Keep destination snapshots taken on:          First          - Wednesday          in month(s):          - January          Taken at: 20:00          For: 10 year(s)</p> <p><b>Source Snapshots:</b>          Disabled</p> <p><input type="checkbox"/> Start job after creation</p>
---	--

< Back   Next >   **Finish**   Cancel

3. Select the **Start job after creation** checkbox if you want the job to start immediately after clicking **Finish**.

#### 4. Click **Finish**.

The **Summary** tab in the **Cloud Backup and Replication Job** runtime view is displayed.



## Running a Cloud Backup and Replication Job

This section describes:

- [Starting a Cloud Backup and Replication Job](#)
- [Stopping a Cloud Backup and Replication Job](#)

### Starting a Cloud Backup and Replication Job

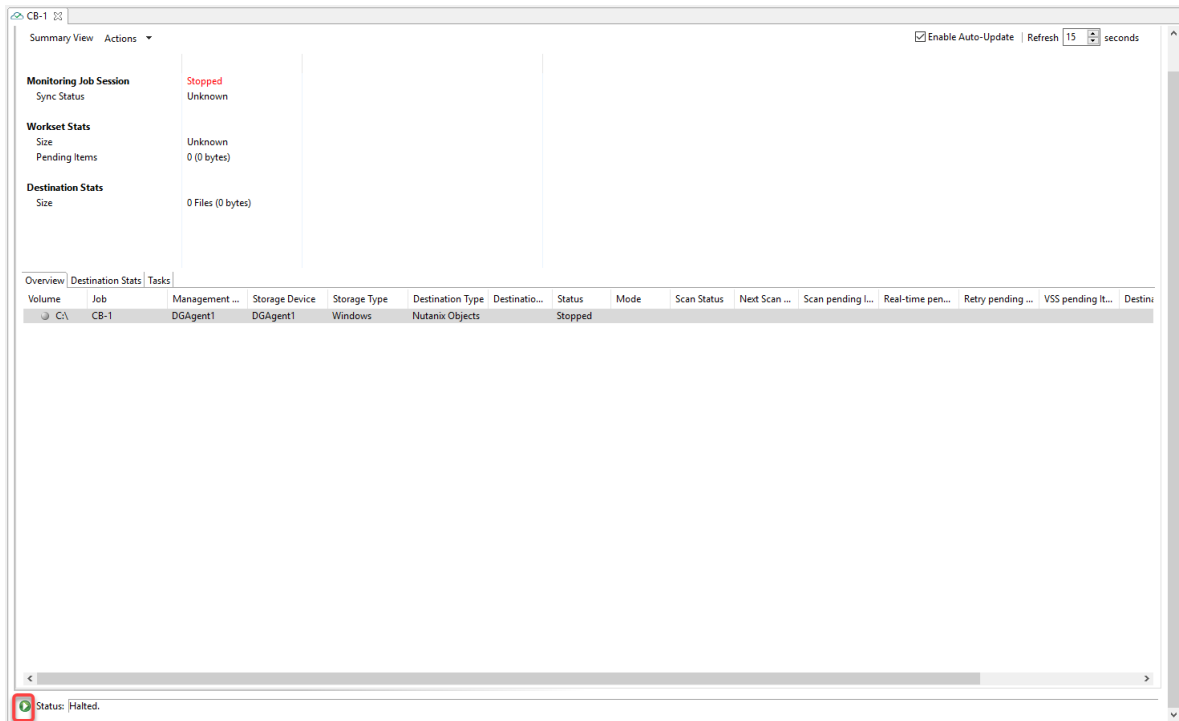
When running a Cloud Backup and Replication job for the first time, you must manually start it. After the initial run, a job will automatically start, even when the Peer Management Center server is rebooted.

**Note:** You cannot run two jobs concurrently on the same volume if the [watch sets](#) contain an overlapping set of files and folders.

To manually start a job:

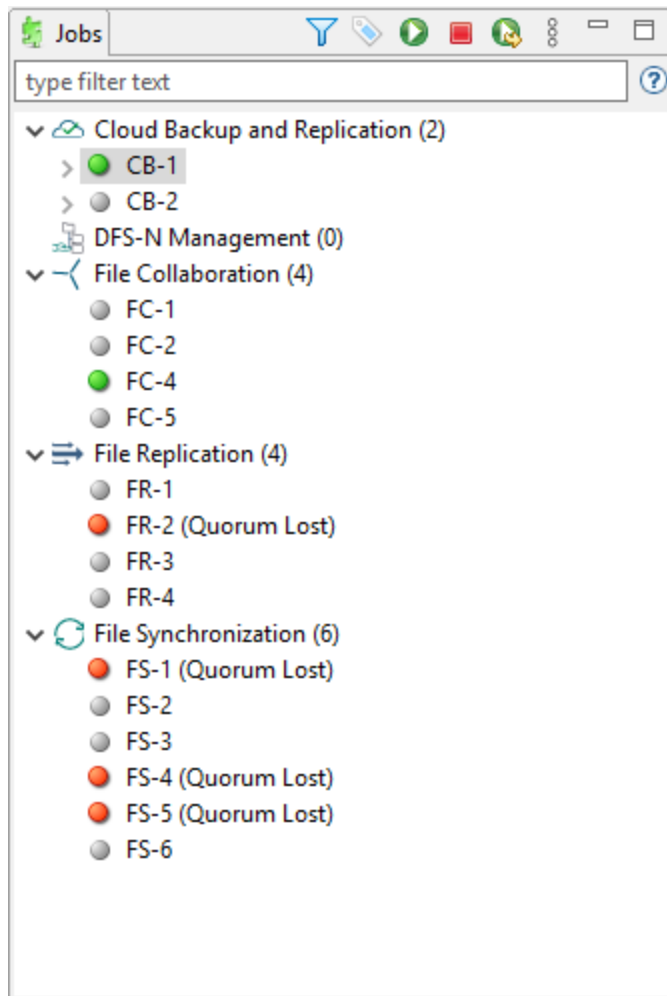
1. Choose one of these options:

- Right-click the job name in the **Jobs** view.
- Open a job and then click the **Start/Stop** button to the left of the **Status** field in the bottom left corner of the job's view (shown below).



2. Click **Yes** in the confirmation dialog.

After the job initialization has completed, the job will run. Once the job starts, the icon next to the job name in the **Jobs** view changes from gray to green.



### Stopping a Cloud Backup and Replication Job

You can stop a Cloud Backup and Replication job at any time.

To stop a Cloud Backup and Replication job:

1. Right-click the job name in the **Jobs** view or in the **Cloud Backup and Replication Job Summary** view, and then choose **Stop** from the pop-up menu.

Or, open the job and then click the **Start/Stop** button to the left of the **Status** field in the bottom left corner of the job's runtime view (shown below)

2. Click **Yes** in the confirmation dialog.

The icon next to the job name in the **Jobs** view changes from green to red.

## Monitoring Cloud Backup and Replication Jobs

Monitoring your Cloud Backup and Replication jobs is an important aspect of successfully replicating to the cloud. Monitoring involves checking the execution of a running job, checking the status of a job, reviewing performance statistics, making sure snapshots are created correctly, identifying problems such as a server outage, seeing how much data has been uploaded, and so forth. Cloud Backup and Replication provides several views to help you monitor the health and performance of your Cloud Backup and Replication jobs.

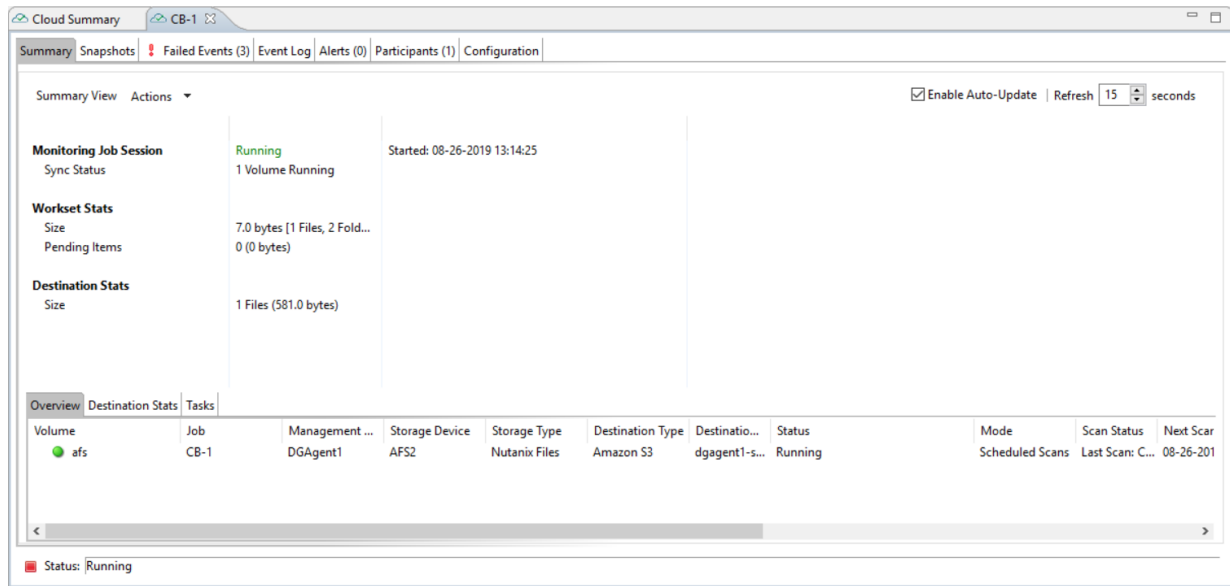
Many of the views are customizable tables. You can sort the columns in the view, filter by columns, add and subtract columns from the default display, and so forth.

To display a view:

- Double-click **Cloud Backup and Replication** in the **Jobs** view to display the summary view for all Cloud Backup and Replication jobs. The **Volume Summary** tab of the **Cloud Summary** view is displayed.

Volume	Job	Management ...	Storage Device	Storage Type	Destination Type	Destinatio...	Status	Mode	Scan Status	Next Scan
afs	CB-2	DGAgent1	AFS2	Nutanix Files	Amazon S3	dgagent1-c...	Running	Scheduled Scans	Last Scan: C...	08-26-2015
afs	CB-1	DGAgent1	AFS2	Nutanix Files	Amazon S3	dgagent1-s...	Running	Scheduled Scans	Last Scan: C...	08-26-2015

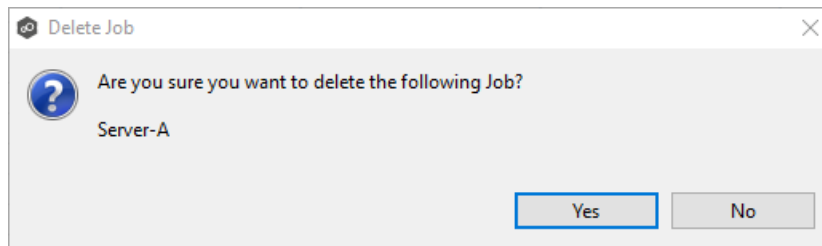
- Double-click the name of a Cloud Backup and Replication job in the **Jobs** view to display the runtime view associated with that job. The **Summary** tab of the runtime view is displayed.



## Deleting a Cloud Backup and Replication Job

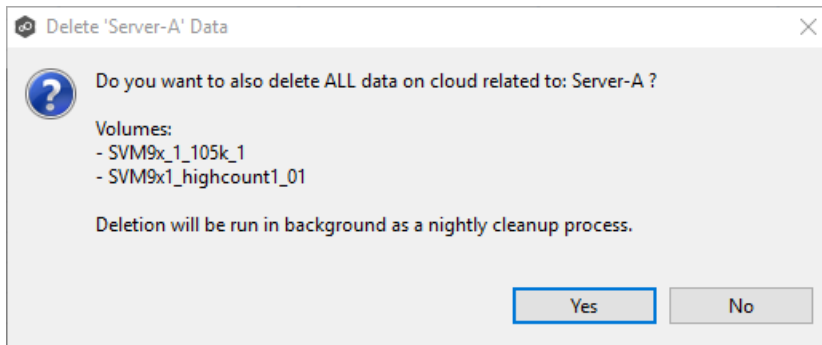
To delete a Cloud Backup and Replication job:

1. Right-click on the job name in the **Jobs** view, and then choose **Delete** from the menu. A confirmation dialog appears.



2. Click **OK** in the confirmation dialog.

Another dialog appears, prompting you to choose whether to delete data associated with the job.



3. Click **Yes** or **No**.

If you click **Yes**, the data associated with this job will be deleted as part of a nightly clean-up process in addition to the job itself. If you click **No**, the data will not be deleted but the job will be deleted.

## Recovering Data

When you need to recover data from the cloud to on-premises, you can use the **Data Recovery** wizard. To restore data, you must have an existing Cloud Backup and Replication job that has been replicating that data.

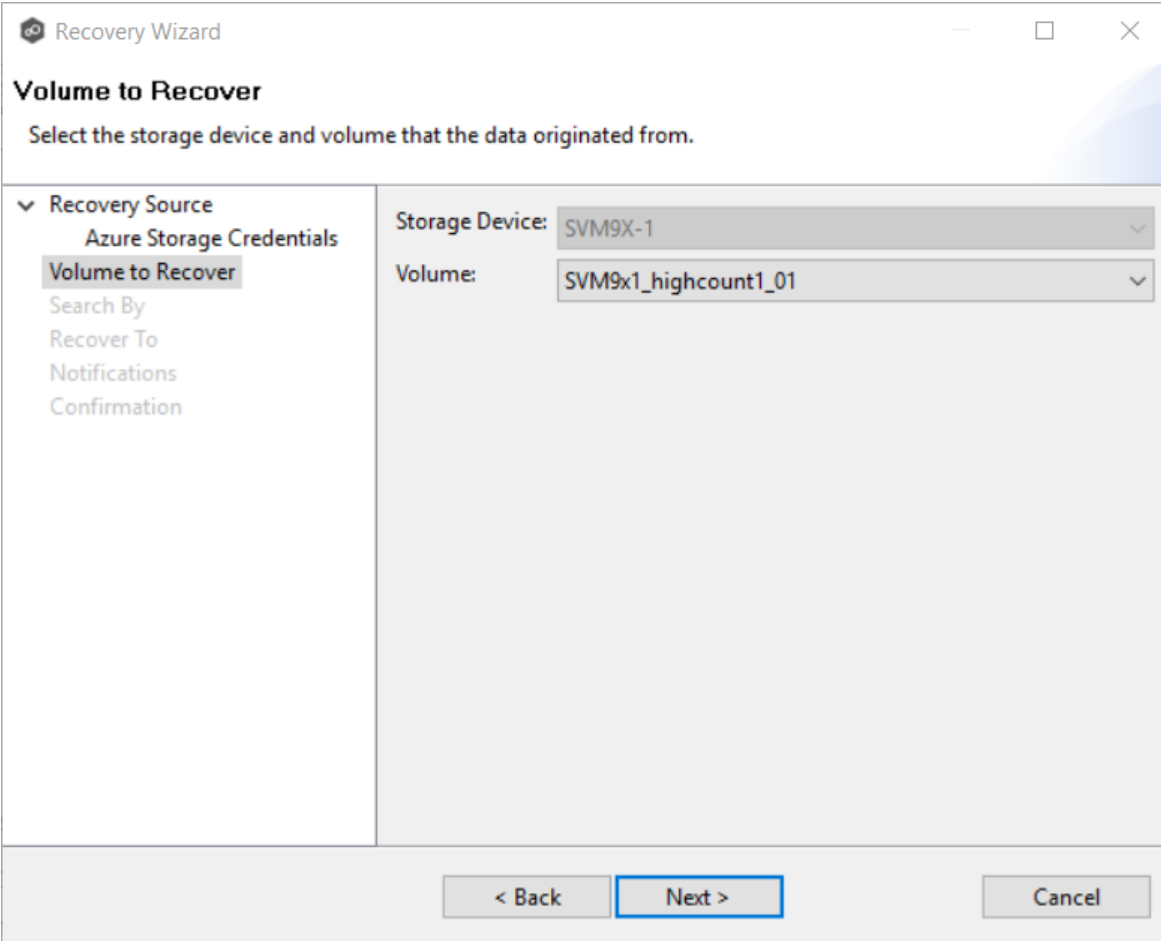
**Note:** You can recover data from a running job. However, if you plan to restore the data to the original location, you should stop the job first.

To recover data:

1. Open Peer Management Center.
2. In the **Jobs** view, identify the Cloud Backup and Replication job that replicated the data you want to restore.
3. Right-click the job name, and then select **Recover Volume/File(s)** from the menu.

The **Recovery Wizard** opens and displays the **Volume to Recover** page. The **Storage Device** field on the page is a read-only field that displays the name of the source storage device.

4. Select the volume that was the source of the replicated data from the **Volume** drop-down list.



The screenshot shows a window titled "Recovery Wizard" with standard Windows window controls (minimize, maximize, close). The main heading is "Volume to Recover" with the instruction "Select the storage device and volume that the data originated from." On the left is a sidebar with a tree view containing: "Recovery Source" (expanded), "Azure Storage Credentials", "Volume to Recover" (selected and highlighted), "Search By", "Recover To", "Notifications", and "Confirmation". The main area contains two dropdown menus: "Storage Device:" with the value "SVM9X-1" and "Volume:" with the value "SVM9x1\_highcount1\_01". At the bottom are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

5. Click **Next**.

The **Search By** page is displayed.



Recovery Wizard

**Search By**  
Select a search option.

▼ Recovery Source  
    Azure Storage Credentials  
    Volume to Recover  
    **Search By**  
    Recover To  
    Notifications  
    Confirmation

☐ Name  
☐ Snapshot  
☐ Point in Time  
☐ Latest Replication

< Back    Next >    Cancel

6. Select one of the search options.

- [Name](#)
- [Snapshot](#)
- [Point in Time](#)
- [Latest Replication](#)

7. Click **Next** and continue with [Recovery Options](#).

The search pages vary according to the search option you selected.

## Search Options

1. The search options are:

- Name
- Snapshot
- Point in Time
- Latest Replication

Use the **Search by Name** option if you know any part of the name of a file or folder but don't know which folder contained it on the original volume on premises.

To search by name:

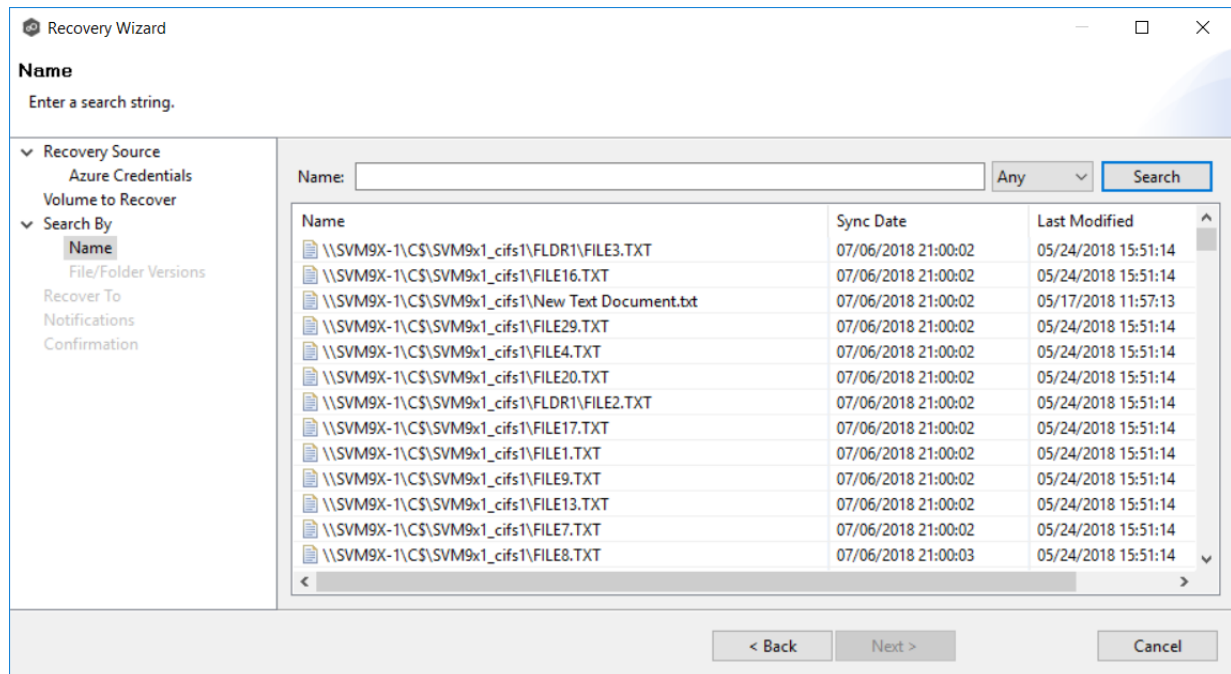
1. Enter a search string in the **Name** field.

The search string can be a full or partial name and can include wildcards. If you do not enter a search string, all files and folders will be listed in the search results.

[illegible]

2. Select **File** or **Folder** from the **Any** drop-down list; if you want to search for both files and folders, select **Any**.
3. Click **Search**.

A list of matching files and/or folders appears. The **Sync Date** column shows the date the file was replicated; the **Last Modified Date** column shows the last known date and time that the file was changed on premises.



4. Select the file or folder to recover.
5. Click **Next**.

The **File/Folder Versions** page appears. Your options will vary, depending on whether you are recovering a file or folder.

6. If you selected a file to recover, all available versions of that file are presented below the calendar. Select the time of the desired version and then click elsewhere in the page.

Recovery Wizard

**File/Folder Versions**

Select a version to recover.

Recovery Source

- Azure Credentials
- Volume to Recover

Search By

- Name
- File/Folder Versions**

Recover To

- Notifications
- Confirmation

**Selected Sync Item(s):**

\\SVM9X-1\CS\SVM9x1\_cifs1\FLDR1\FILE2.TXT

Calendar: Jul, 2018

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Select Time

**Oldest Available:**  
07/06/2018 21:00:03

**Newest Available:**  
07/06/2018 21:00:03

< Back   Next >   Cancel

If you selected a folder to recover, you have two options. You can recover the contents of the folder based on a snapshot that was previously taken, or you can recover the contents of the folder as it existed at a specific point in time. Select one of the options, select a time, and then click elsewhere in the page.

Recovery Wizard

**File/Folder Versions**

Select a version to recover.

Recovery Source

- Azure Credentials
- Volume to Recover

Search By

- Name
- File/Folder Versions**

Recover To

- Notifications
- Confirmation

**Selected Sync Item(s):**

\\SVM9X-1\CS\SVM9x1\_cifs1\22mil\FLDR2L1

☒ Snapshots   ☐ Date and Time

Calendar: Jul, 2018

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Select Time

**Oldest Available:**  
07/07/2018 00:30:01

**Newest Available:**  
07/10/2018 07:30:01

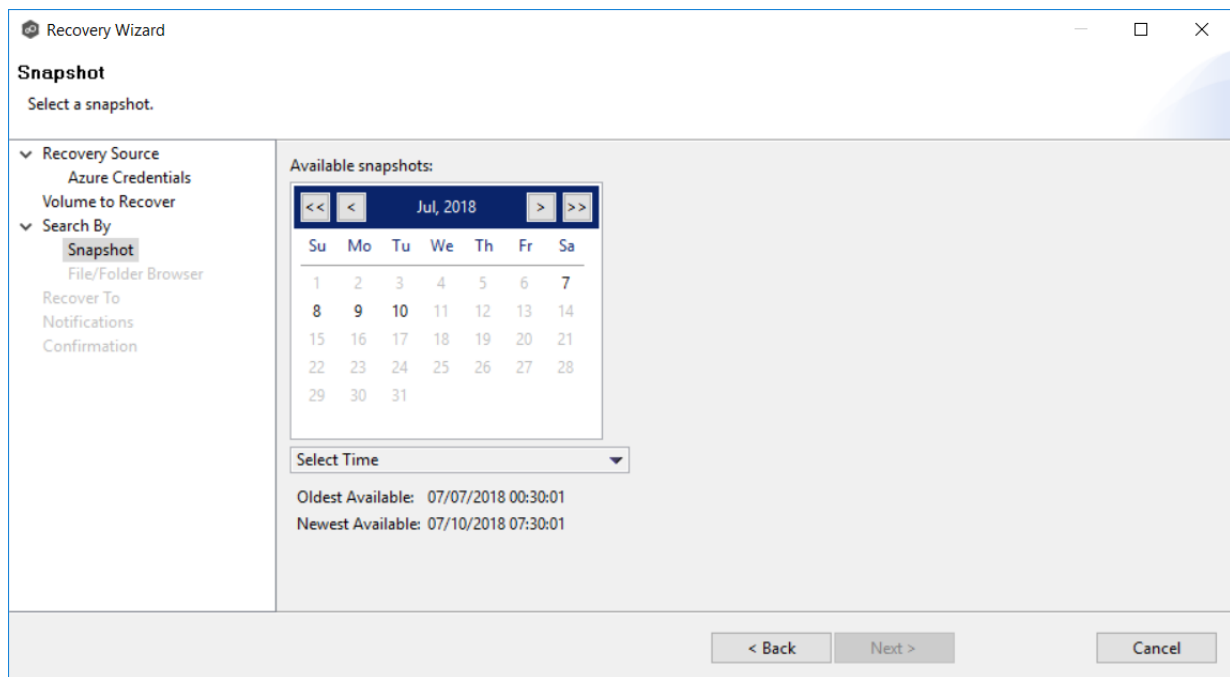
< Back   Next >   Cancel

- Click **Next** and continue with [Recovery Options](#).

Use the **Search by Snapshot** option if you want to recover data by browsing a previously taken destination snapshot. All available snapshots will be represented in the calendar widget below.

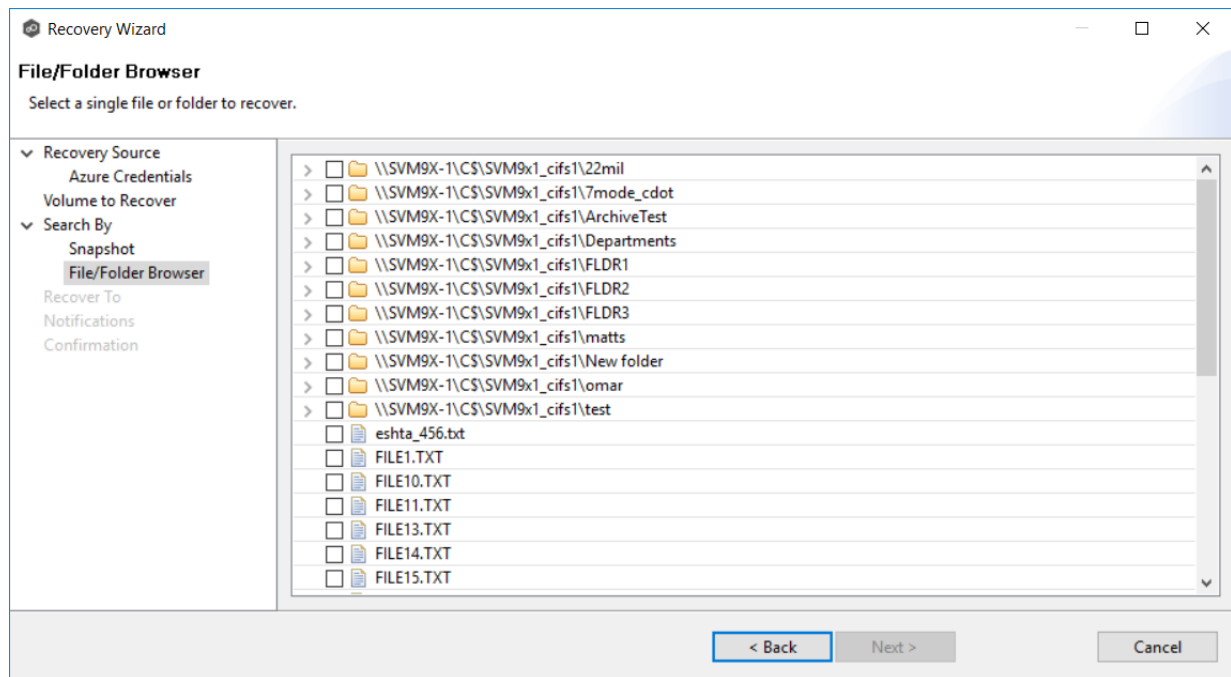
To search by snapshot:

1. Select the date of the snapshot.



2. Select the time of the snapshot, and then click elsewhere in the page.
3. Click **Next**.

The **File/Folder Browser** page appears.

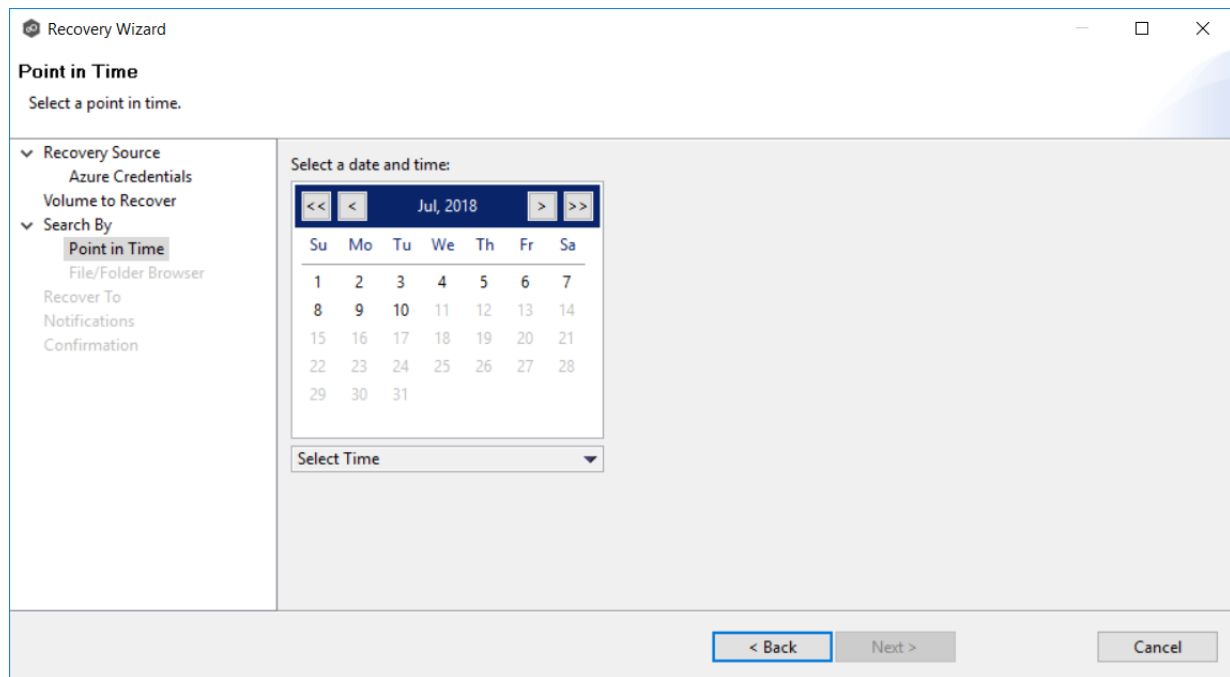


4. Select the file or folder to restore. If no snapshots are available, click **Back** and select a different search option.
5. Click **Next** and continue with [Recovery Options](#).

Use the **Search by Point in Time** option if you want to restore a data from a specific point in time. This option does not require that a snapshot was taken and is very useful if you selected [Continuous Data Protection](#), where replication is performed on an on-going basis

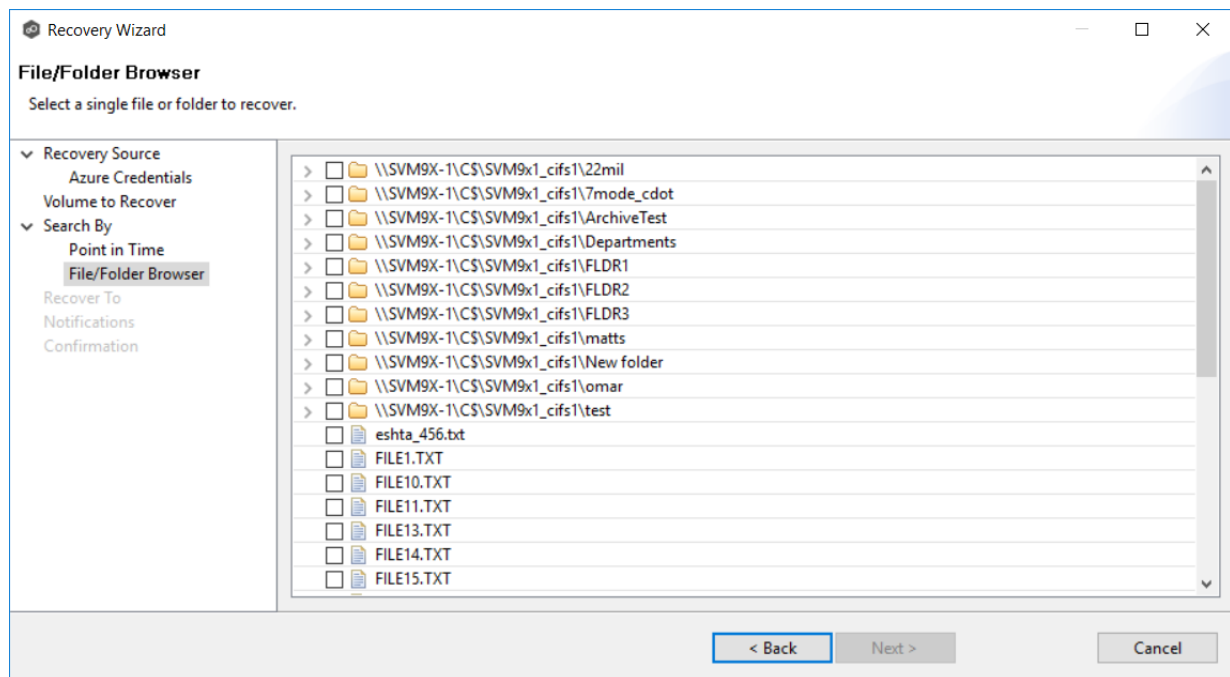
To search by a point in time:

1. Select a date.



2. Select a date and time, and then click elsewhere in the page.
3. Click **Next**.

The **File/Folder Browser** page appears.



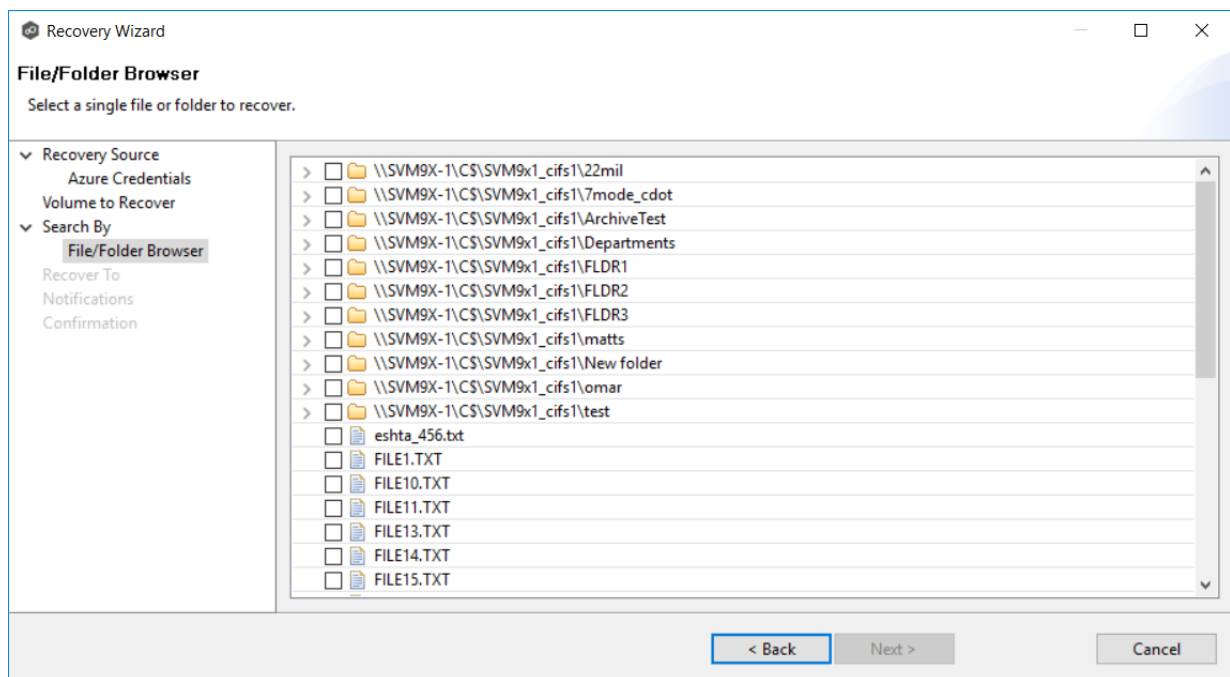
4. Select the file or folder to restore.

5. Click **Next** and continue with [Recovery Options](#).

Use the **Search by Latest Replication** option if you want to restore from the latest replication. For example, you may want to restore data from the last time that replication occurred rather than a snapshot or a point in time. This option is very useful if you selected [Continuous Data Protection](#), where replication is performed on an on-going basis.

To search by latest replication:

1. Select the file or folder to restore.



2. Click **Next** and continue with [Recovery Options](#).

## Recovery Options

After you select the data to recover, the **Recover To** page appears.

1. Select the recovery location. You have two options:



- **Another Location** - Enter the UNC path to a location on another storage device.
- **Original Location** - Browse to a location on the device hosting the management agent. However, we recommend not restoring directly to the original location, especially if the job is currently running. If the version that is restored is older than the latest version in the destination storage, the restored version will not be backed up until the next scan.

2. Select the recovery options for when the file to recover already exists in the recovery location:

Recovery Option	Select this option if you want to:
<b>Recover with unique name</b>	Ensure that the existing file is not overwritten with the cloud version.
<b>Overwrite if sizes or timestamps don't match</b>	Overwrite the existing file with the cloud version if the sizes or timestamps the existing file do not match the cloud version.
<b>Overwrite if cloud version is newer</b>	Overwrite the existing file if the cloud version has a more recent modification date.

<b>Overwrite always</b>	Always overwrite the existing file with the cloud version.
<b>Skip</b>	Skip recovering a file if the file already exists.

3. Select the recovery metadata options:

<b>Metadata Option</b>	<b>Select this option if you want to:</b>
<b>Recover Last Modified Time</b>	Set the last modification time of a recovered file to match the last modification time stored at upload rather than the time at which it was recovered.
<b>Recover Create Time</b>	Set the creation time of a recovered file to match the creation time stored at upload rather than the time at which it was recovered.
<b>Recover NTFS Permissions</b>	Set the NTFS permissions of any recovered files and folders to match the original permissions when those files and folders were uploaded.
<b>Recover</b>	Set the attributes of any recovered files and folders to match the original attributes when those files and folders were uploaded.

4. (Optional) Click the **Review** button to see your selections.
5. Click **Next**.

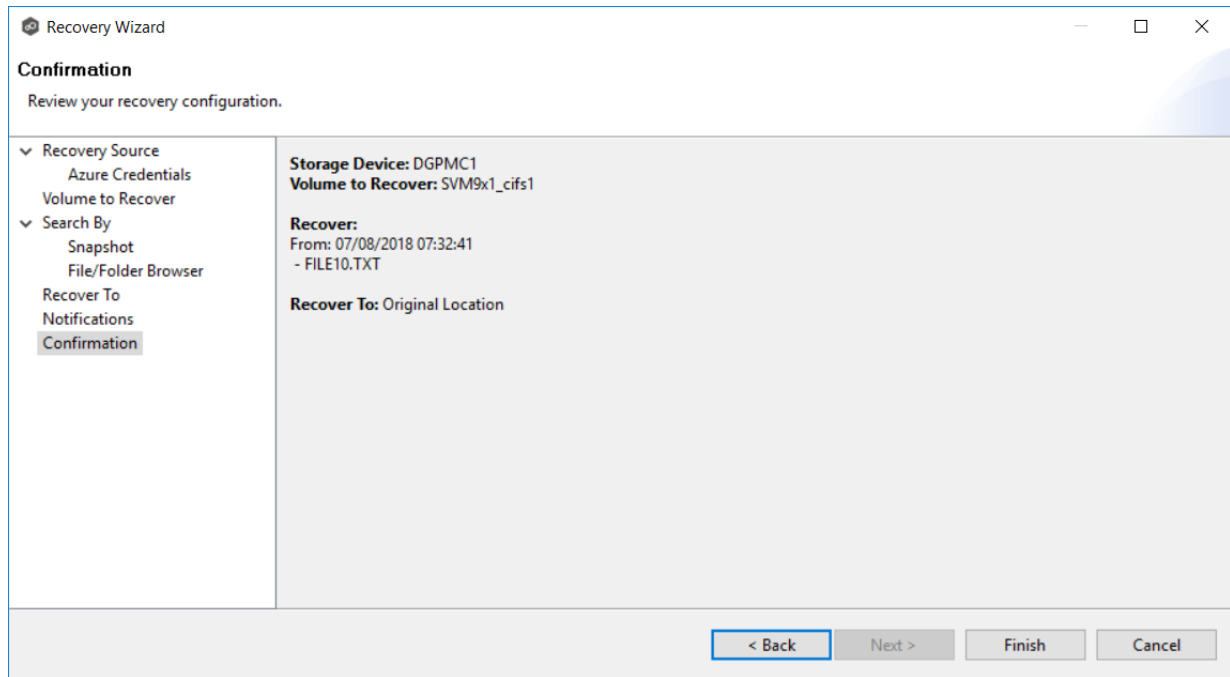
The **Notifications** page appears.

The screenshot shows the 'Recovery Wizard' window with the 'Notifications' step selected in the left sidebar. The main area is titled 'Notifications' with the instruction 'Select email notifications.' Below this, there's a section 'Edit Email Alerts' containing a checkbox for 'Send email notification when complete' and a sub-checkbox for 'Only on failure'. A text input field is labeled 'Enter recipient name, email or distribution list to add:' with a placeholder 'Start typing to filter contacts/lists or add a new email'. To the right of this field are 'Add to List', 'Remove', and 'View Details' buttons. Below the input field is a large empty box labeled 'Recipients:'. At the bottom of the window are '< Back', 'Next >', and 'Cancel' buttons.

6. (Optional) Select the **Send email notification when complete** checkbox if you want notifications sent when the recovery process is complete. Select **Only on failure** if you want notifications sent only if the recovery does not successfully complete.
7. If sending notifications, enter recipients and add them to the list.
8. Click **Next**.

The **Confirmation** page is displayed.

9. Review your recovery settings.



10. Click **Finish**.

## DFS-N Management Jobs

This section provides information about creating, editing, running, and managing a DFS-N Management job:

- [Overview](#)
- [Namespace Elements](#)
- [Getting Started with DFS Namespaces](#)
- [Creating a DFS-N Management Job](#)
- [Running a DFS-N Management Job](#)
- [Managing DFS Namespaces](#)
  - [Adding an Existing Namespace](#)
  - [Adding a Namespace Server](#)

- [Adding a Namespace Folder](#)
- [Adding a Namespace Folder Target](#)
- [Connecting DFS Namespaces with File Collaboration and File Synchronization Jobs](#)

## Overview

The purpose of creating a DFS Namespace Management job is to allow you to manage various activities related to [DFS namespaces](#), such as creating a namespace, creating namespace folders, and adding folder targets. A DFS namespace enables you to group shared folders located on different servers into one or more logically structured namespaces. DFS namespace activities can be performed using a Microsoft tool; however, the benefits of creating and configuring namespace within Peer Management Center are:

- **Ease of managing a namespace** - You can [create](#) and [manage](#) a namespace within the same interface that manages our synchronization and collaboration technologies. This removes the need to use two different tools to manage the key elements of multi-site and multi-vendor file services.
- **Integration with Synchronization and Collaboration** - [When combined with PMC's file synchronization technology](#), DFS namespaces can provide redundancy to file shares across file servers and locations.
- **Automating failover and fallback** - If a file server goes offline, Peer Management Center will disable the associated folder target in DFS namespace. This automatically redirects users to another available file server. When the original file server comes back, Peer Management Center will automatically make sure it is brought back in sync, and then enable the associated folder target so users can once again connect to it. See [DFS Namespace Failover and Fallback](#) in [Advanced Topics](#) for more information.

## Namespace Elements

The elements that make up a DFS namespace are:

- **Namespace server** - A namespace server hosts a namespace. The namespace server can be a member server or a domain controller.
- **Namespace root** - The namespace root is the starting point of the namespace. For example, if you have a namespace path of `\\Domain.local\MyNamespace`, the root is

**MyNamespace.** This is a domain-integrated namespace, meaning that its metadata is stored in Active Directory Domain Services.

- **Folder** (also referred to as **namespace folders**)- Folders with **folder targets** provide users with actual content. When users browse a folder that has folder targets in the namespace, the client computer receives a referral that transparently redirects the client computer to one of the folder targets.
- **Folder targets** - A folder target is the UNC path of a shared folder or another namespace that is associated with a folder in a namespace. The folder target is where data and content are stored. For example, if a user navigates to `\Domain.local\MyNamespace\MyFolder`, they are transparently redirected to `\\NYC-FS.Domain.local\MyFolder` or `\\LA-FS.Domain.local\MyFolder`, depending on which site the user is currently accessing.

## Getting Started with DFS Namespaces

If you need to create a namespace, begin by [creating a DFS-N Management job](#). You may want to [configure your DFS preferences](#) before you create the job.

If you already have a namespace that you want to import, see [Adding an Existing Namespace](#).

See [Managing DFS Namespaces](#) for information about adding namespace servers, namespace folders, or folder targets to a DFS namespace.

Once you have configured your namespace, you can [link it to a File Collaboration or File Synchronization job](#).

## Creating a DFS-N Management Job

The **Create Job** Wizard walks you through the process of creating a DFS-N Management job. The process consists of the following steps:

[Step 1: Job Type](#)

[Step 2: Management Agent](#)

[Step 3: Agent Verification](#)

[Step 4: Namespace Name](#)

[Step 5: Namespace Servers](#)

[Step 6: Namespace Settings](#)

[Step 7: Namespace Folders](#)

[Step 8: Email Alerts](#)

[Step 9: SNMP Notifications](#)

[Step 10: Review](#)

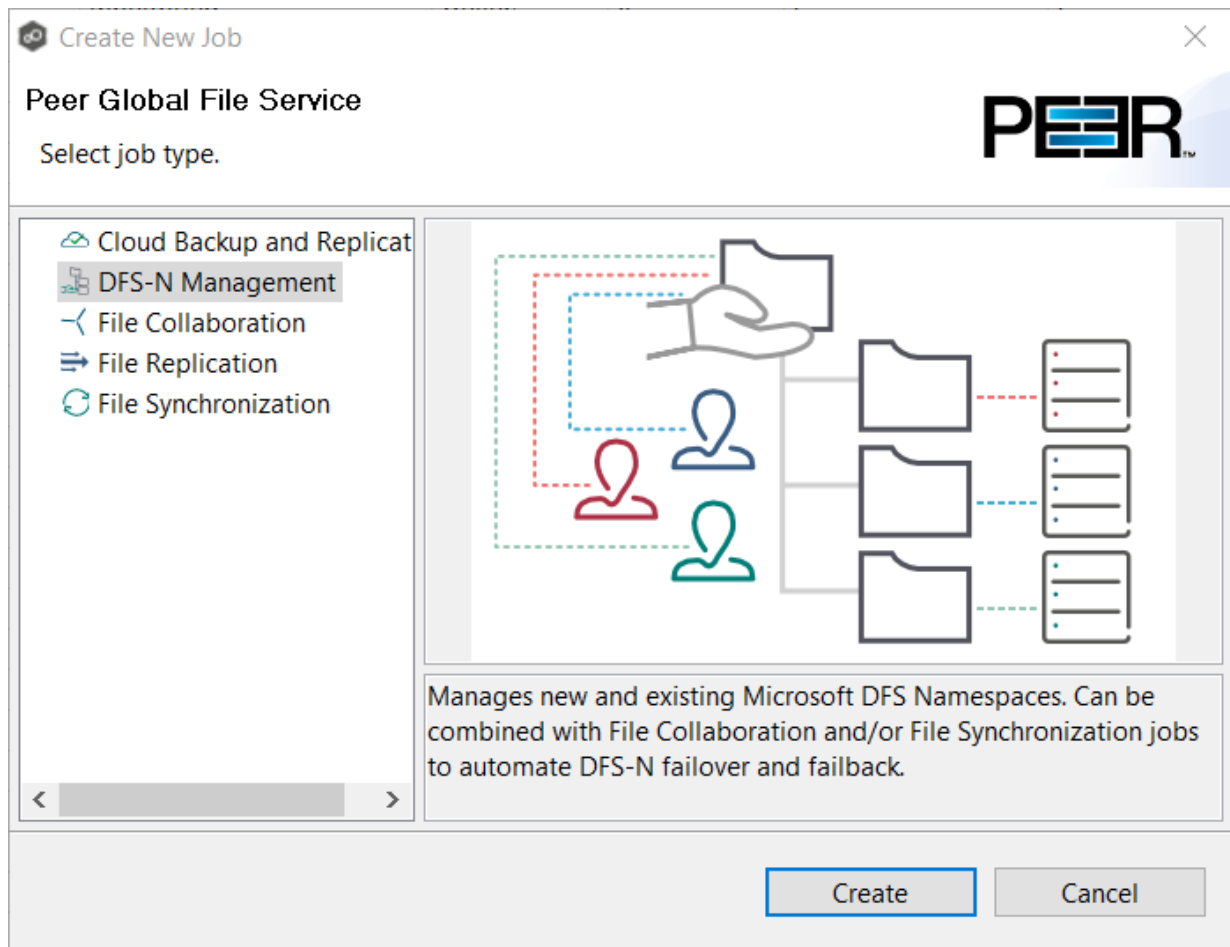
[Step 11: Results](#)

### Step 1: Job Type

1. Open Peer Management Center.
2. From the **File** menu, select **New Job** (or click the **New Job** button on the toolbar).

The **Create New Job** wizard displays a list of job types you can create.

3. Click **DFS-N Management**, and then click **Create**.



The [Management Agent](#) page appears.

## Step 2: Management Agent

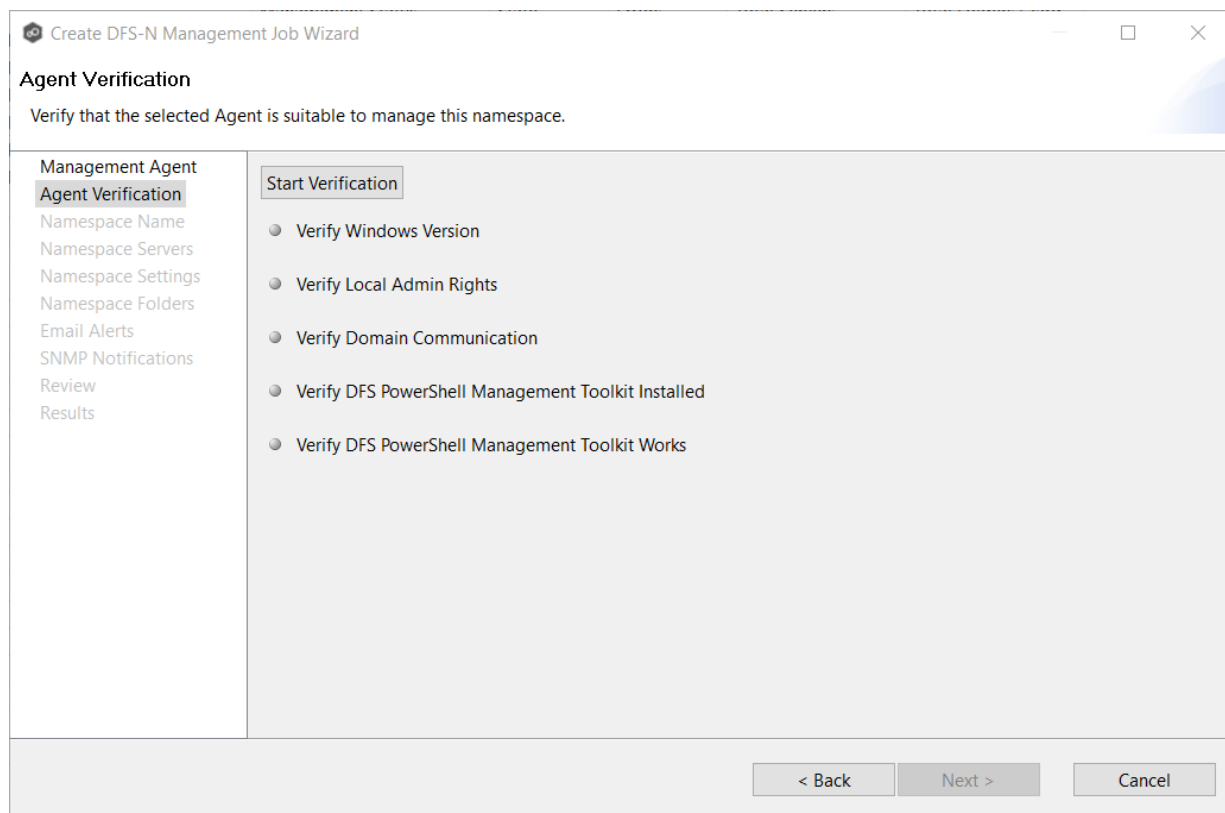
The **Management Agent** page presents a list of servers that have a Peer Agent installed.

1. Select an Agent that is in the domain of the DFS namespace or where you want to create the new DFS namespace.

**Note:** If you select an Agent that has **No** in the **DFS Mgmt. Enabled** column, the Microsoft DFS PowerShell Management toolkit will be installed in the next step.

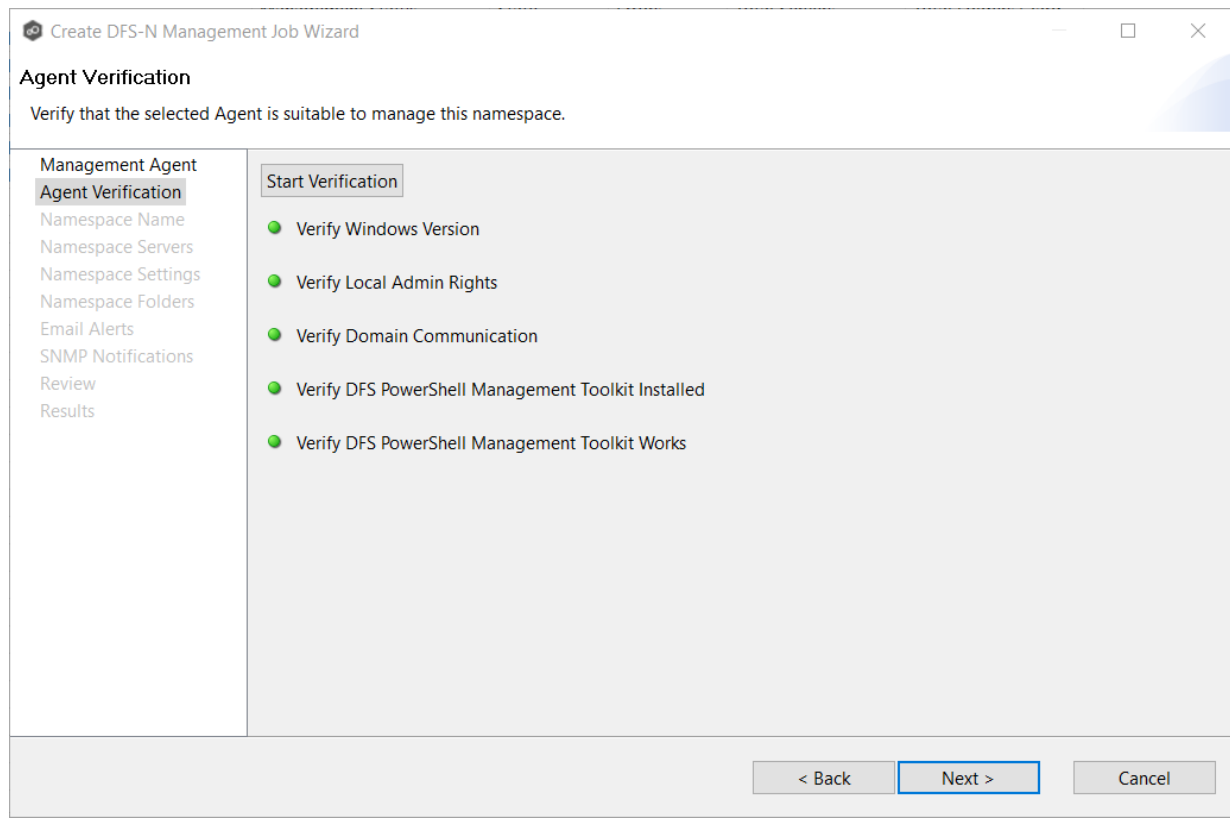






2. If the DFS PowerShell Management toolkit is not installed, click the **Install** button that appears next to **Verify DFS PowerShell Management Toolkit Installed**.

After the toolkit is installed, the verification continues. A green dot signifies that the verification of that element was successful.



3. After the verification has successfully completed, click **Next**.

The [Namespace Name](#) page appears.

#### Step 4: Namespace Name

The name of the namespace will also be the name of the DFS-N Management job.

1. Enter the name of the namespace.

Create DFS-N Management Job Wizard

**Namespace Name**  
Enter a name of the new namespace.

Management Agent  
Agent Verification  
**Namespace Name**  
Namespace Servers  
Namespace Settings  
Namespace Folders  
Email Alerts  
SNMP Notifications  
Review  
Results

This name will appear after the server or domain name in the namespace path, such as \\Server\\Name or \\Domain\\Name.

Namespace Name:

< Back   Next >   Cancel

2. Click **Next**.

The [Namespace Servers](#) page appears.

### Step 5: Namespace Servers

A server that you want to host a namespace is called a namespace server. It does not have to host the data. However, a namespace server must be running the Microsoft DFS Namespace Service. In most cases, a namespace server should be a domain controller.

1. Enter the fully qualified path of a file server in the **Server Name** field, and then click **Add**.

Create DFS-N Management Job Wizard

**Namespace Servers**

Select one or more servers to host this namespace. The servers you select will be known as namespace servers.

Management Agent  
Agent Verification  
Namespace Name  
**Namespace Servers**  
Namespace Settings  
Namespace Folders  
Email Alerts  
SNMP Notifications  
Review  
Results

Enter the fully qualified domain name of a server running the DFS namespace service.

Server Name:

< Back   Next >   Cancel

The server path is listed in the area below.

Create DFS-N Management Job Wizard

**Namespace Servers**

Select one or more servers to host this namespace. The servers you select will be known as namespace servers.

Management Agent  
Agent Verification  
Namespace Name  
**Namespace Servers**  
Namespace Settings  
Namespace Folders  
Email Alerts  
SNMP Notifications  
Review  
Results

Enter the fully qualified domain name of a server running the DFS namespace service.

Server Name:

DGWin16B.peertest.local

< Back   **Next >**   Cancel

2. Add additional servers if desired.

3. Click **Next**.

The [Namespace Settings](#) page appears.

### Step 6: Namespace Settings

The **Namespace Settings** page displays the namespace servers selected for the job. You can modify a server's local path and access permissions.

To edit a server's settings:

1. In the **DFS Root Share Path** column for the server, modify the path.



[illegible]

4. Click **Next**.

The [Namespace Folders](#) page appears.

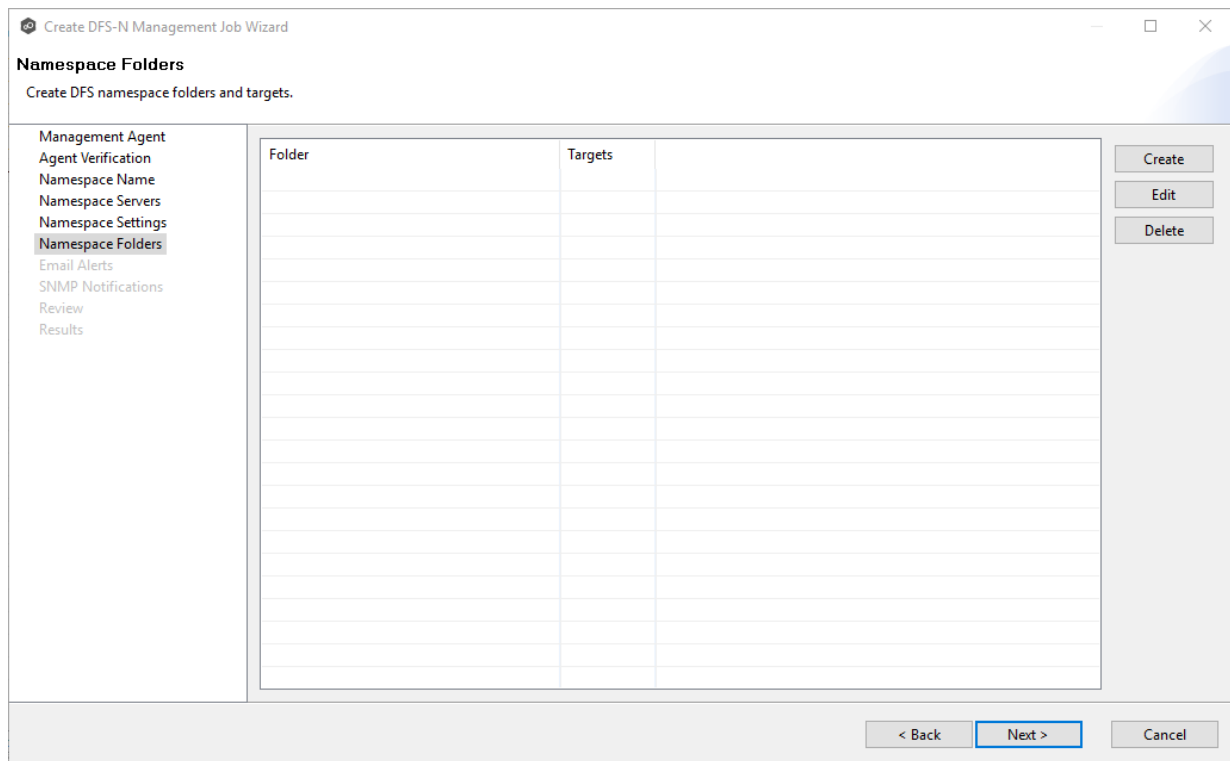
## Step 7: Namespace Folders

A namespace folder contains folder targets, which provide users with actual content. A folder target is the [Universal Naming Convention \(UNC\) path](#) of a shared folder or another namespace that is associated with a folder in a namespace. The folder target is where data and content are stored. Adding multiple folder targets increases the availability of the folder in the namespace.

The **Namespace Folders** page lists existing namespace folders and folder targets.

1. Click the **Create** button.

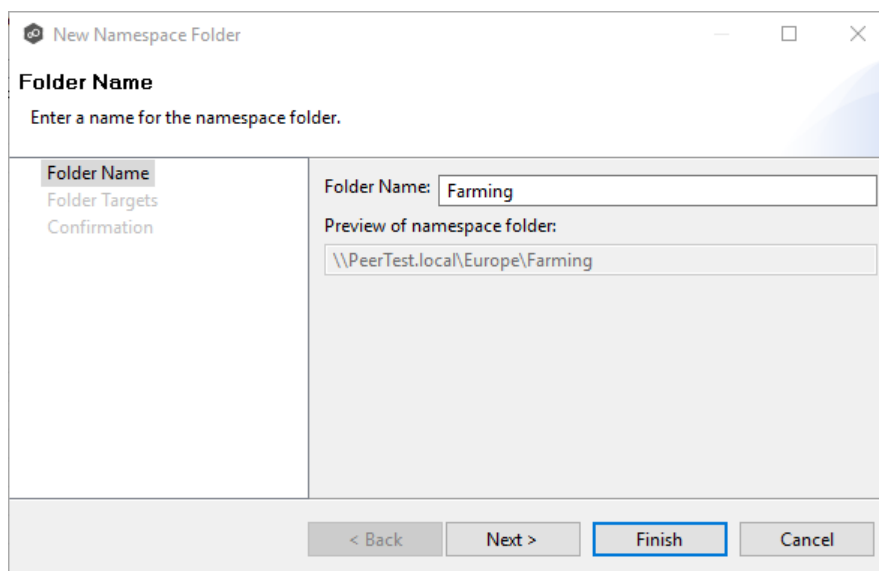




The **Folder Name** dialog appears.

2. Enter a name for the namespace folder in the **Folder Name** field.

After you enter the folder name, a preview of the folder and path name appears below the **Folder Name** field.



- (Optional) To add folder targets for the namespace folder, click **Next**. You can add folder targets now or later when editing the job.

The **Folder Targets** dialog appears.

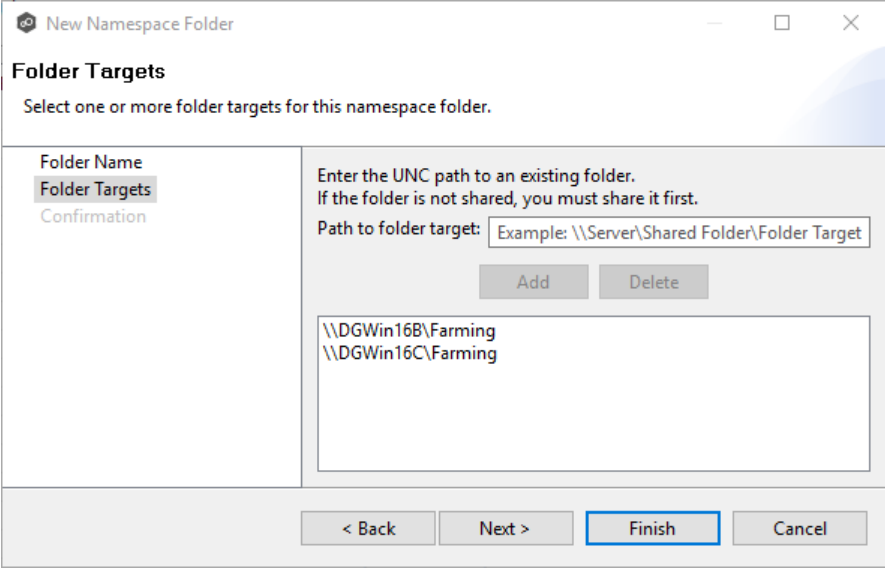
The screenshot shows the 'New Namespace Folder' dialog box with the 'Folder Targets' tab selected. The dialog has a title bar with a gear icon and the text 'New Namespace Folder'. Below the title bar, the tab is labeled 'Folder Targets' and the instruction 'Select one or more folder targets for this namespace folder.' is displayed. On the left, there is a sidebar with three options: 'Folder Name', 'Folder Targets' (which is highlighted), and 'Confirmation'. The main area on the right contains the text 'Enter the UNC path to an existing folder. If the folder is not shared, you must share it first.' followed by a text input field labeled 'Path to folder target:' with the example text '\\Server\Shared Folder\Folder Target'. Below the input field are 'Add' and 'Delete' buttons. At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Finish' (which is highlighted with a blue border), and 'Cancel'.

- Enter the UNC path to a shared folder, and then click **Add**.

The folder target path is listed in the field below.

This screenshot shows the same 'New Namespace Folder' dialog box, but now the 'Path to folder target:' input field contains the text '\\DGWin16B\Farming'. The 'Add' button is still visible below the input field. The 'Finish' button remains highlighted at the bottom of the dialog.

5. (Optional) Add additional folder targets.



The 'New Namespace Folder' dialog box is shown with the 'Folder Targets' tab selected. The dialog has a title bar with a gear icon and standard window controls. Below the title bar, the 'Folder Targets' tab is active, showing a list of folder targets. The 'Folder Name' tab is also visible. The 'Folder Targets' list contains two entries: '\\DGWin16B\Farming' and '\\DGWin16C\Farming'. The 'Path to folder target' text box contains the example '\\Server\Shared Folder\Folder Target'. The 'Add' and 'Delete' buttons are visible. The 'Finish' button is highlighted with a blue border.

**New Namespace Folder**

**Folder Targets**

Select one or more folder targets for this namespace folder.

Folder Name  
Folder Targets  
Confirmation

Enter the UNC path to an existing folder.  
If the folder is not shared, you must share it first.

Path to folder target: Example: \\Server\Shared Folder\Folder Target

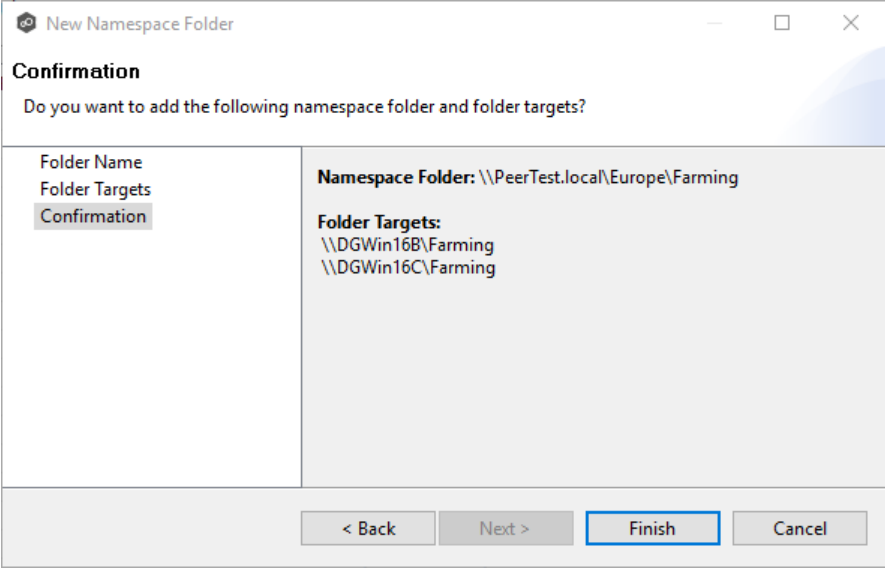
Add Delete

\\DGWin16B\Farming  
\\DGWin16C\Farming

< Back Next > Finish Cancel

6. Click **Next**.

The **Confirmation** dialog appears.



The 'New Namespace Folder' dialog box is shown with the 'Confirmation' tab selected. The dialog has a title bar with a gear icon and standard window controls. Below the title bar, the 'Confirmation' tab is active, showing a confirmation message. The 'Folder Name' tab is also visible. The 'Confirmation' message asks 'Do you want to add the following namespace folder and folder targets?'. The 'Namespace Folder' is '\\PeerTest.local\Europe\Farming'. The 'Folder Targets' are '\\DGWin16B\Farming' and '\\DGWin16C\Farming'. The 'Finish' button is highlighted with a blue border.

**New Namespace Folder**

**Confirmation**

Do you want to add the following namespace folder and folder targets?

Folder Name  
Folder Targets  
Confirmation

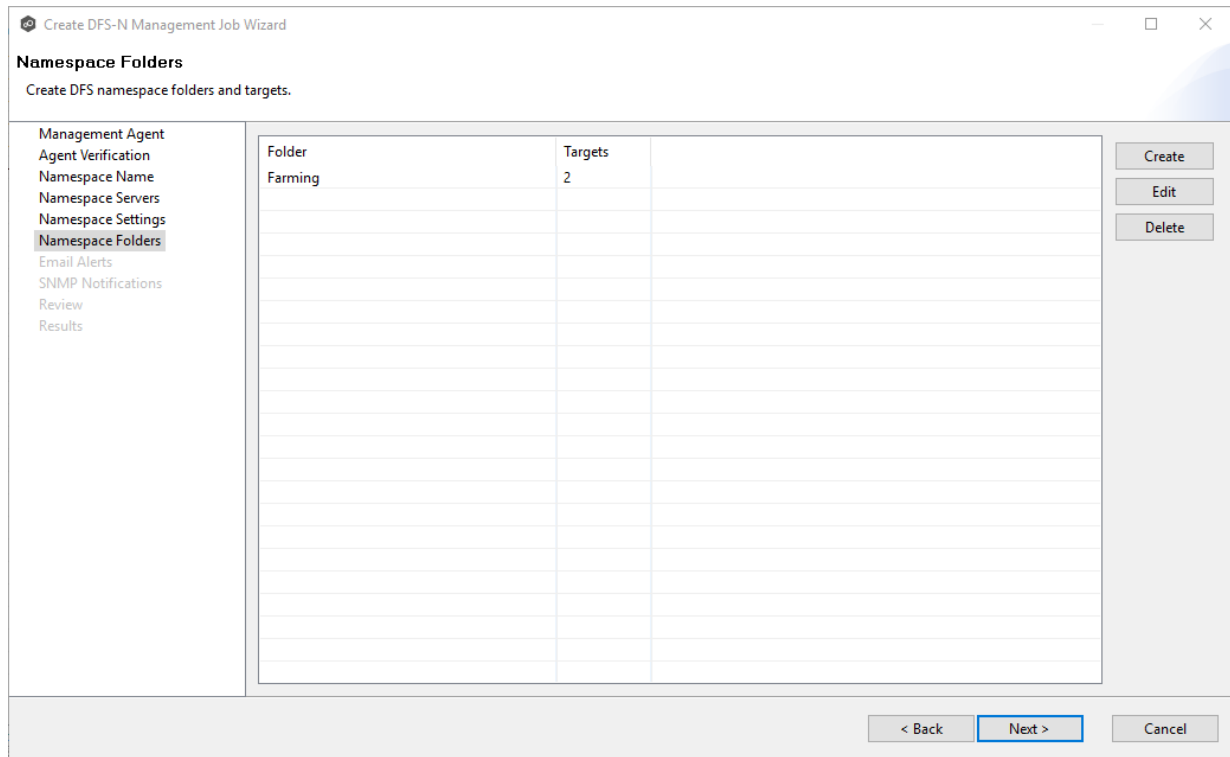
**Namespace Folder:** \\PeerTest.local\Europe\Farming

**Folder Targets:**  
\\DGWin16B\Farming  
\\DGWin16C\Farming

< Back Next > Finish Cancel

7. Review the folders and folder targets, and then click **Back** to add more folder and folder targets; otherwise, click **Finish**.

The **Namespace Folders** page reappears; it lists the folder you added and the number of its targets.



8. Click **Next**.

The [Email Alerts](#) page appears.

## Step 8: Email Alerts

This step is optional.

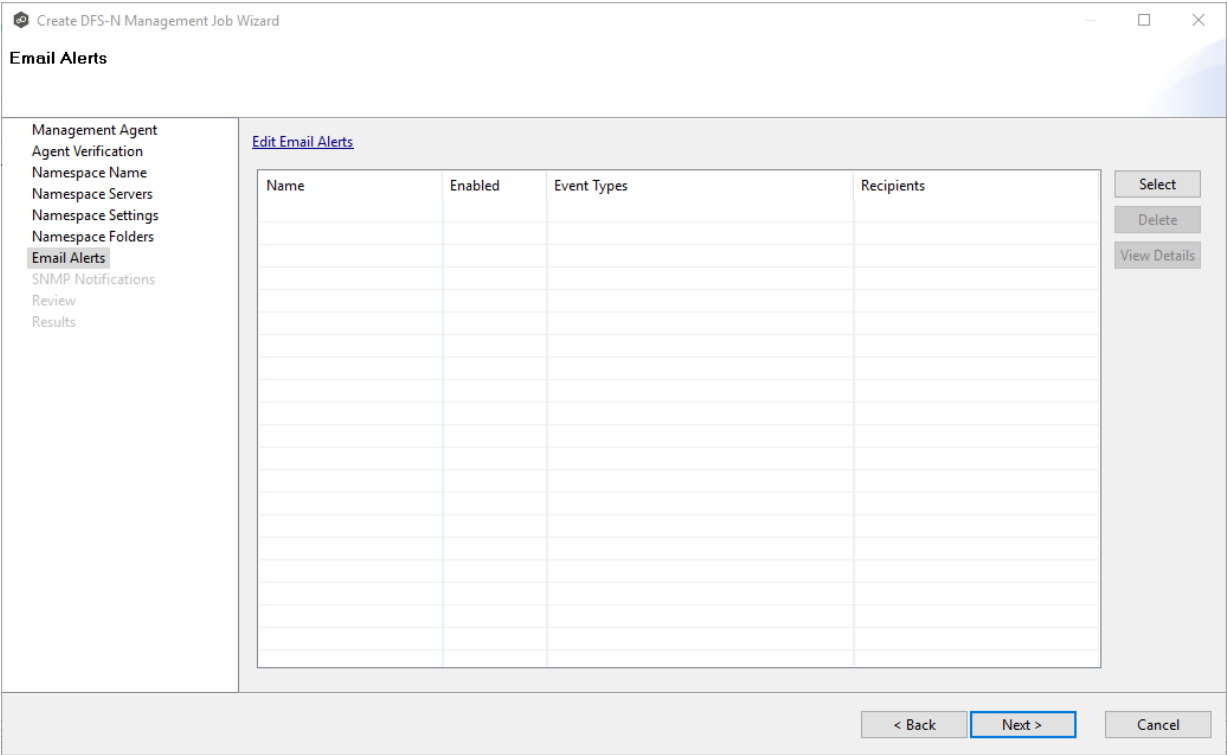
An [email alert](#) notifies recipients when a certain type of event occurs, for example, session abort, host failure, system alert. The **Email Alerts** page displays a list of email alerts that have been applied to the job. When you first create a job, this list is empty. Email alerts are defined in [Preferences](#) and can then be applied to multiple jobs of the same type.

Peer Software recommends that you create email alerts in advance. However, from this wizard page, you can select existing alerts to apply to the job or create new alerts to apply.

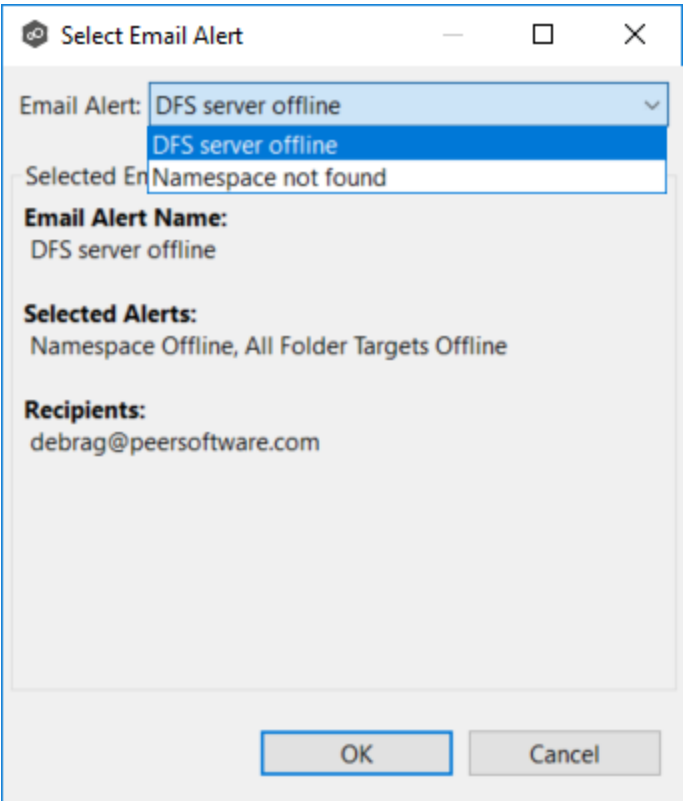
To create a new alert, see [Email Alerts](#) in the [Preferences](#) section.

To apply an existing email alert to the job:

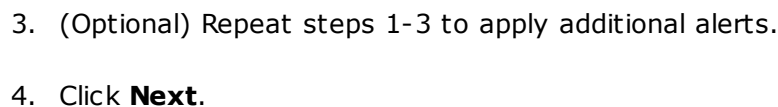
1. Click the **Select** button.



The **Select Email Alert** dialog appears.



- The alert is listed in the **Email Alerts** page.



The [SNMP Notifications](#) page appears.

## Step 9: SNMP Notifications

This step is optional.

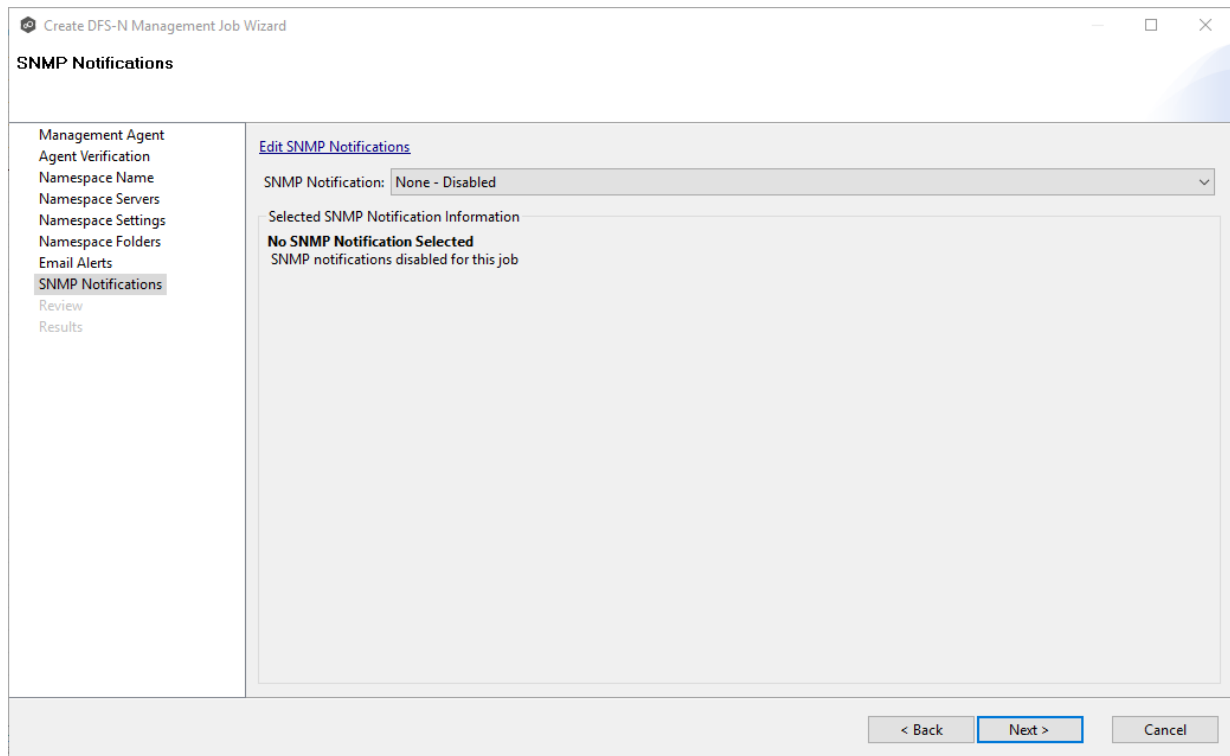
An [SNMP notification](#) notifies recipients when certain type of event occurs, for example, session abort, host failure, system alert. The **SNMP Notifications** page displays a list of notifications that have been applied to the job. When you first create a job, this list is empty. Like email alerts and file filters, an SNMP notification is defined in [Preferences](#) and can then be applied to multiple jobs of the same type.

Peer Software recommends that you create SNMP notifications in advance. However, from this wizard page, you can select an existing SNMP notification to apply to the job or create new SNMP notifications.

To apply an existing SNMP notification to the job or disable notifications:

1. Select an SNMP notification from the drop-down list.

To disable, select **None - Disabled**.



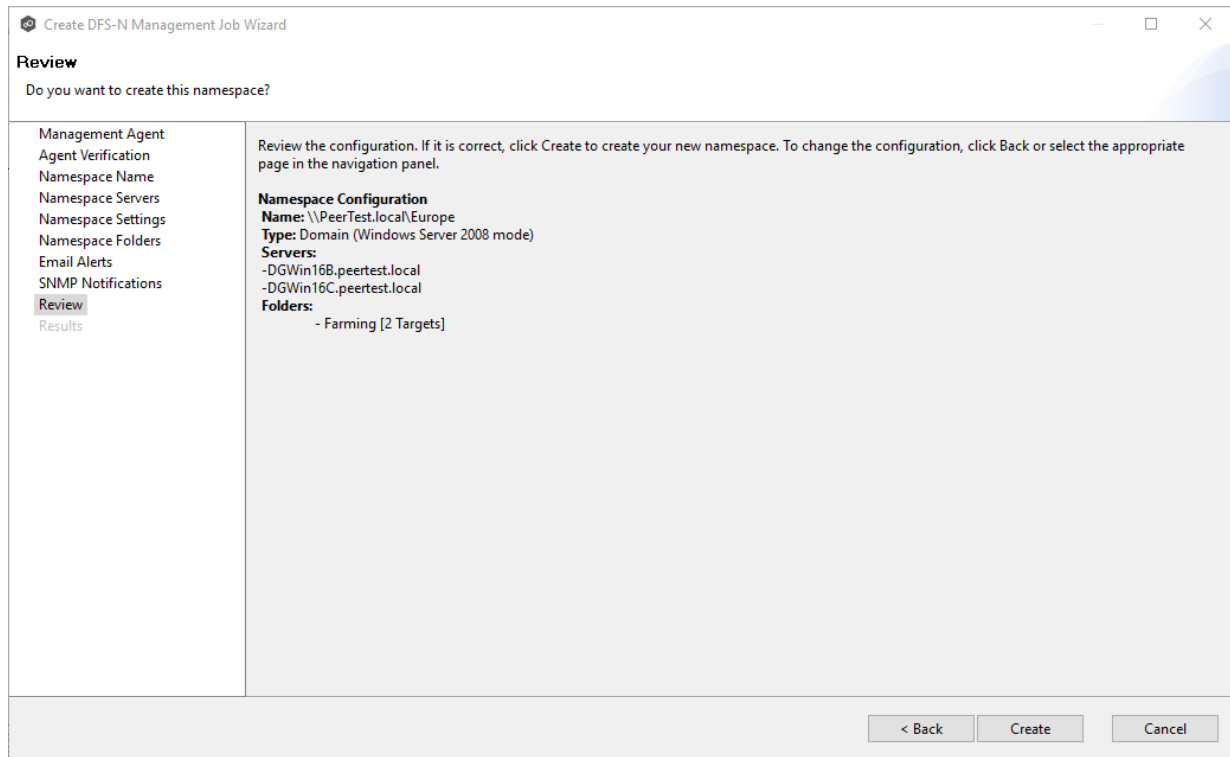
2. Click **Next**.

The [Review](#) page appears.

## Step 10: Review

The **Review** page allows you to review the configuration before it is actually created.

1. Review the namespace configuration.



2. Click **Create** if the configuration is correct; otherwise, click **Back** and correct the configuration.

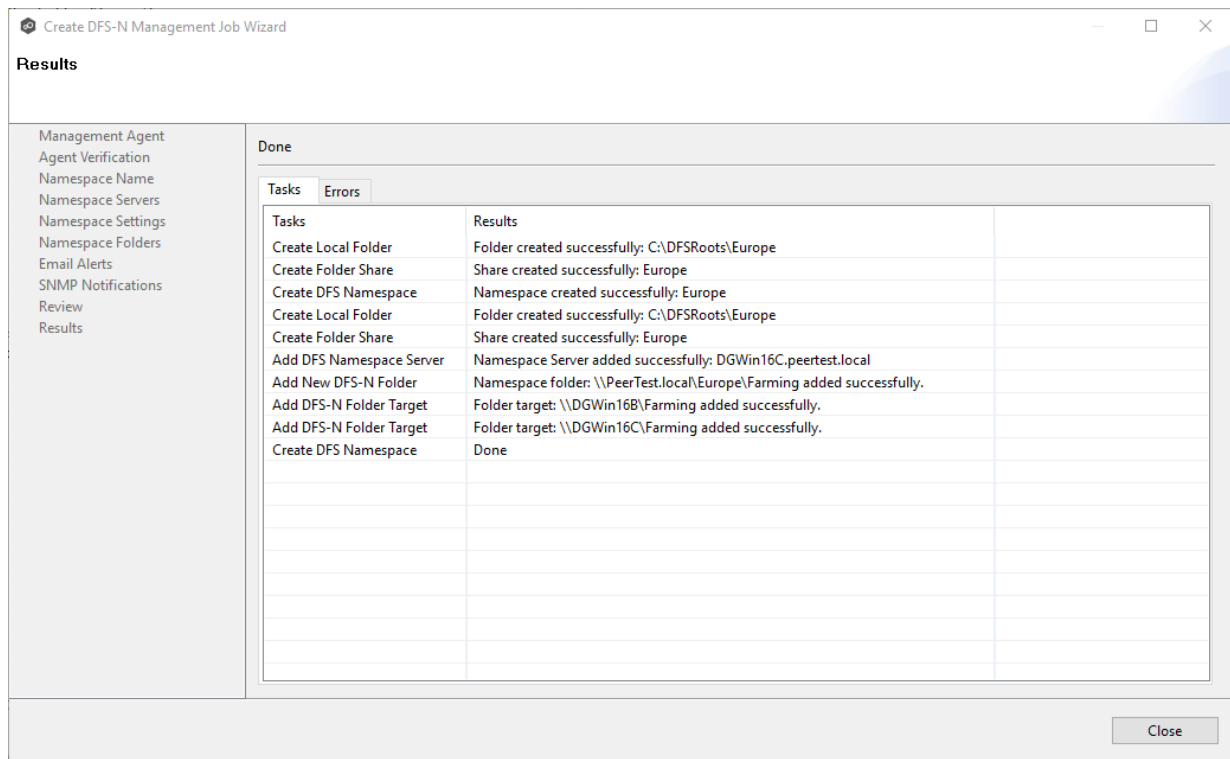
After you click **Create**, the [Results](#) page appears.

## Step 11: Results

The **Results** page has two tabs: **Tasks** and **Errors**.

1. Review the results in the **Tasks** and **Errors** tabs.

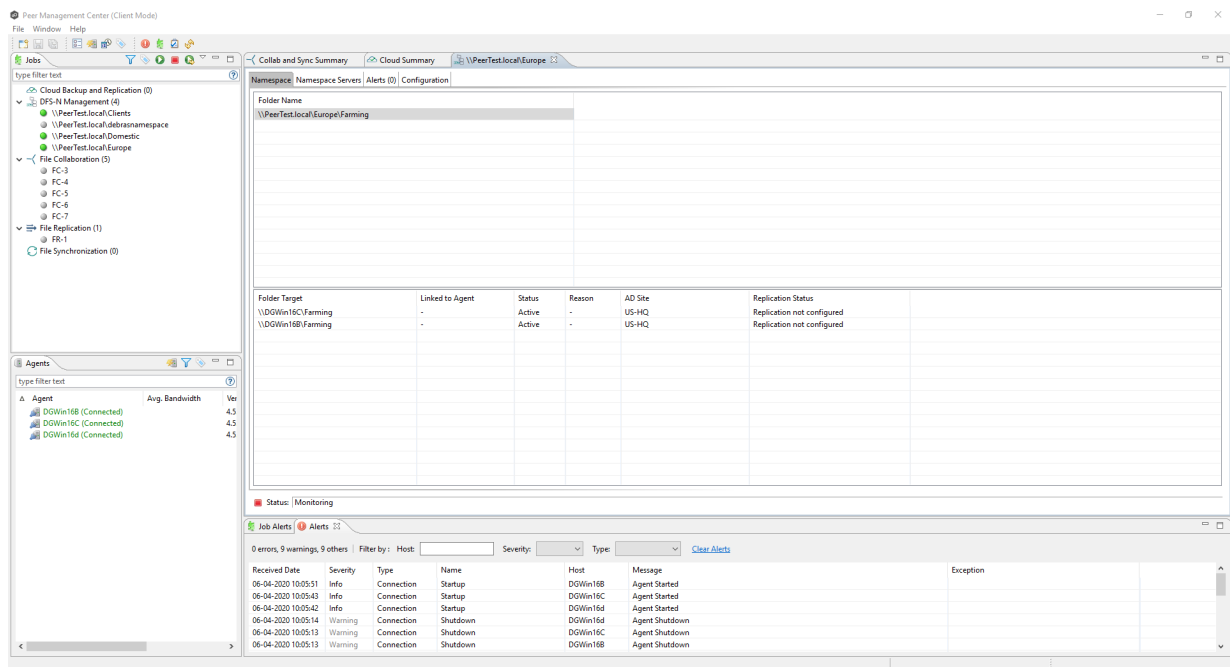




- Click **Close**.

The job automatically starts and the runtime summary view for the new job is displayed.

- Select the job in the Namespace tab to view the folder targets.



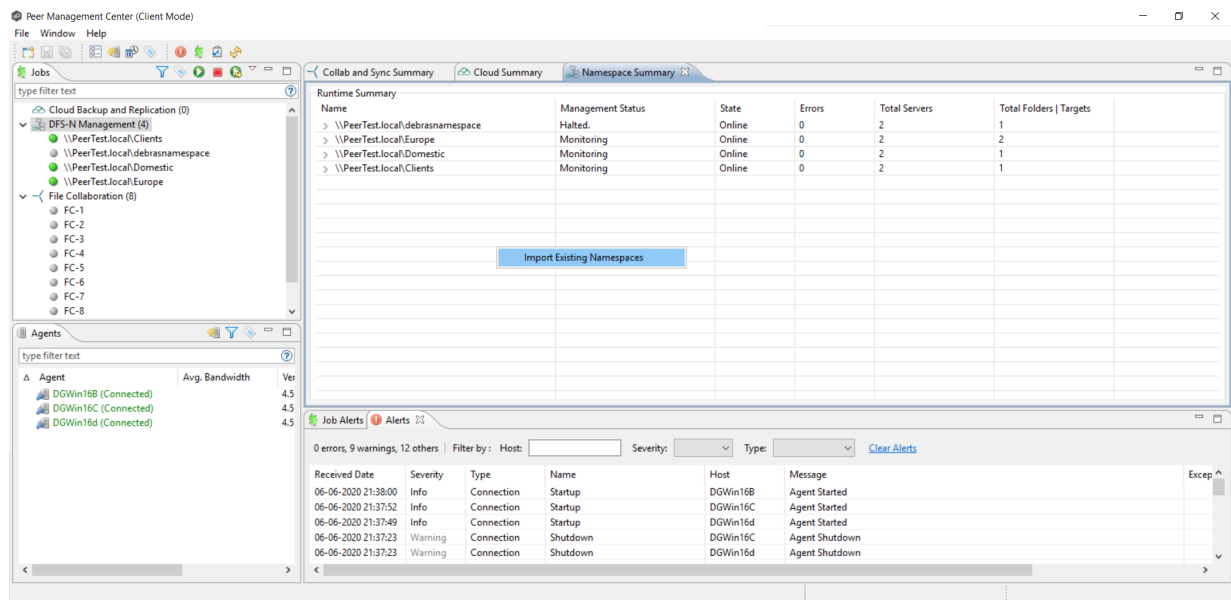
## Importing an Existing Namespace

If you have an existing namespace that you want to use in a File Collaboration or File Synchronization job, you can import the namespace. Importing the namespace creates a new DFS-N Management job with the same name as the imported namespace.

You can then either [link the namespace to an existing File Collaboration or File Synchronization job](#) or [create a new File Collaboration or File Synchronization job](#) that uses the namespace.

To import an existing namespace:

1. Right-click anywhere in the **Runtime Summary** tab of the **Namespace Summary** view, and then select **Import Existing Namespaces** (or right-click the DFS-N Management job type in the **Jobs** view).

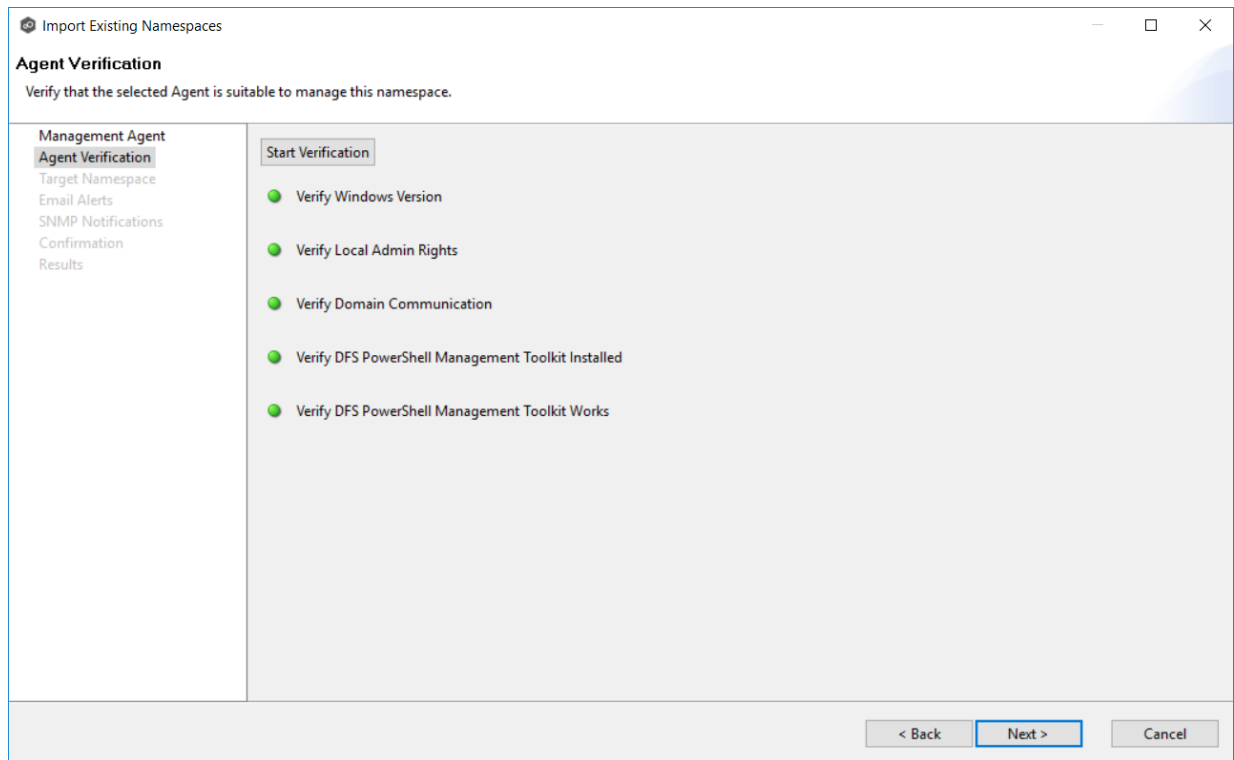


The **Add Existing Namespace** wizard appears.

2. Select a management agent.



After the toolkit is installed, the verification continues. A green dot signifies that the verification of that element was successful.



5. After the verification has successfully completed, click **Next**.

The **Target Namespace** page appears. You have two options for selecting the namespace to import: either by entering its name or by selecting it from a list of namespaces.

Import Existing Namespaces

**Target Namespace**

Management Agent  
Agent Verification  
**Target Namespace**  
Email Alerts  
SNMP Notifications  
Confirmation  
Results

☒ Select By Name  
\*Namespace Name: \\PeerTest.local\\

☐ List All Namespaces

< Back   Next >   Cancel

6. If you choose **Select By Name**, enter the namespace name and then click **Validate**. After the namespace is validated, continue with Step 8.

If you choose **List All Namespaces**, click **Next**.

The **Existing Namespace** page appears. It displays a table listing the existing namespaces

**Note:** It may take a few minutes for existing namespaces to appear in the table.

7. Select one or more existing namespaces from the table, and then click **Next**.

Import Existing Namespaces

Existing Namespaces

Management Agent  
Agent Verification  
Target Namespace  
Existing Namespaces  
Email Alerts  
SNMP Notifications  
Confirmation  
Results

Refresh

Available namespaces: 58

Namespace	State	Description
<input type="checkbox"/> Atlas Shared D...	Online	
<input type="checkbox"/> BlueDFS	Online	
<input type="checkbox"/> CAD Projects - ...	Online	
<input type="checkbox"/> Cheri	Online	
<input type="checkbox"/> Colors	Online	
<input type="checkbox"/> Debra01	Online	
<input type="checkbox"/> Debra02	Online	
<input type="checkbox"/> DFS-N_DE	Online	
<input type="checkbox"/> DFSDemoTest1	Online	
<input type="checkbox"/> DfsNamespace...	Not Found	
<input type="checkbox"/> DFSR_Germany	Online	
<input type="checkbox"/> DG	Online	
<input type="checkbox"/> DGNamespace	Online	
<input type="checkbox"/> Family_DFS	Online	
<input type="checkbox"/> Fine Arts	Online	
<input type="checkbox"/> Food	Online	
<input type="checkbox"/> FullCycle	Online	
<input type="checkbox"/> Kim	Online	
<input type="checkbox"/> LLCY	Online	
<input type="checkbox"/> marcus-test	Not Found	

< Back

Next >

Cancel

The **Email Alerts** page appears.

[illegible]

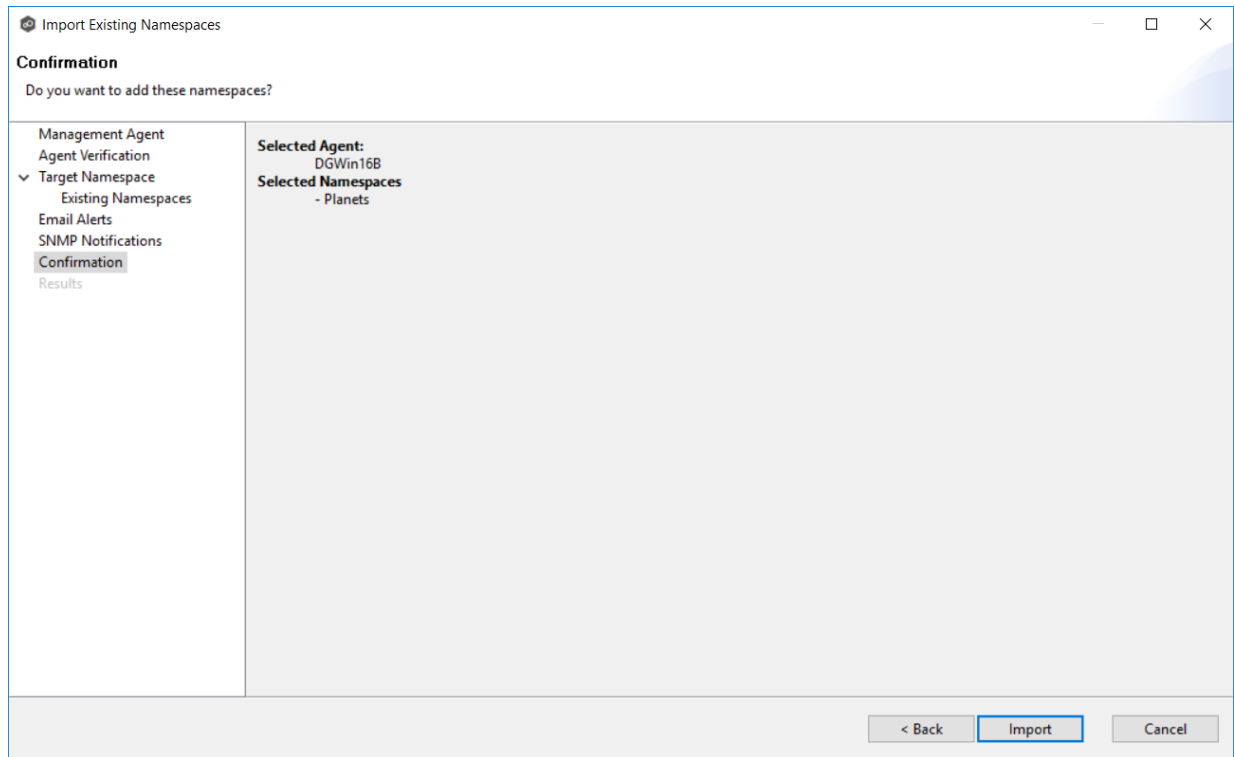
8. (Optional) Select or create email alerts to apply to the job, and then click **Next**.

The **SNMP Notifications** page appears.

The screenshot shows a window titled "Import Existing Namespaces" with a sidebar on the left and a main content area on the right. The sidebar contains a tree view with the following items: "Management Agent", "Agent Verification", "Target Namespace" (expanded), "Existing Namespaces", "Email Alerts", "SNMP Notifications" (selected), "Confirmation", and "Results". The main content area is titled "SNMP Notifications" and contains a link "Edit SNMP Notifications". Below the link is a dropdown menu labeled "SNMP Notification:" with the value "None - Disabled". Underneath is a section titled "Selected SNMP Notification Information" which contains the text "No SNMP Notification Selected" and "SNMP notifications disabled for this job". At the bottom of the window are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

9. (Optional) Select or create an SNMP notification to apply to the job, and then click **Next**.

The **Confirmation** page appears.



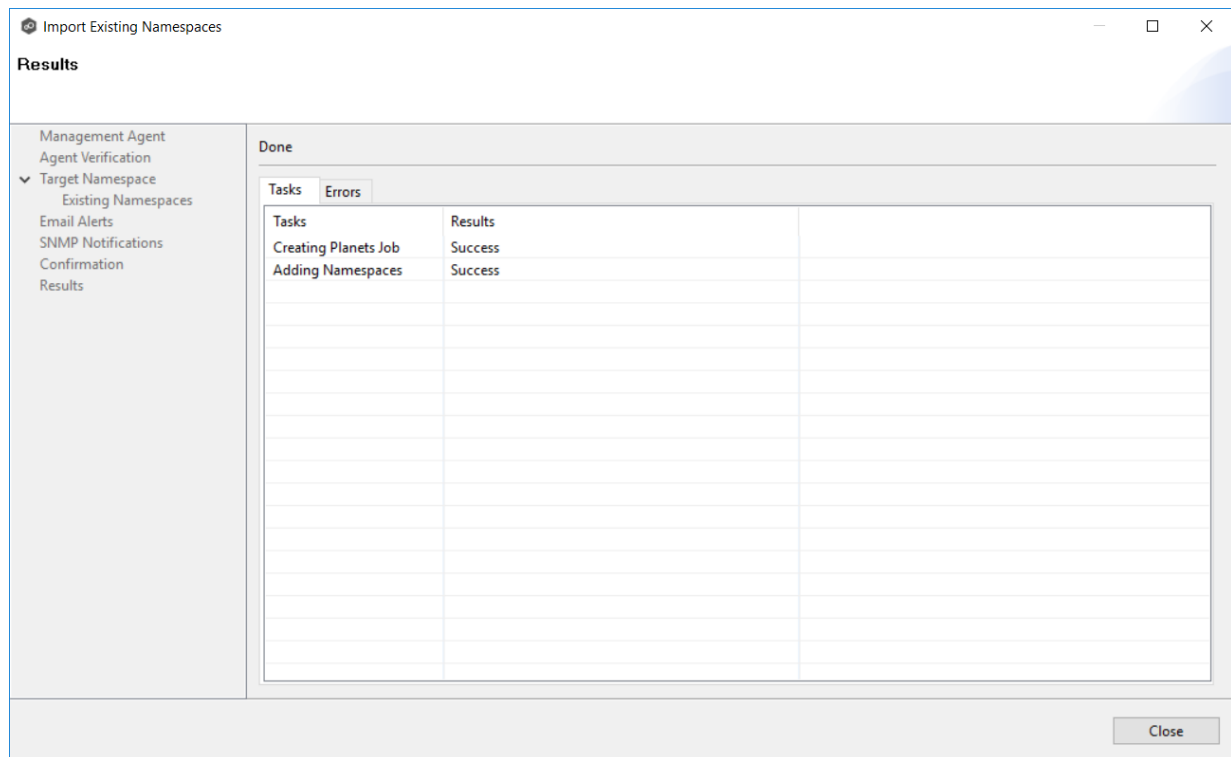
10. Review the configuration.

11. If you need to modify the job configuration after reviewing it, click **Back** until you reach the appropriate page and make your changes.

12. Once you are satisfied with the job configuration, click **Import**.

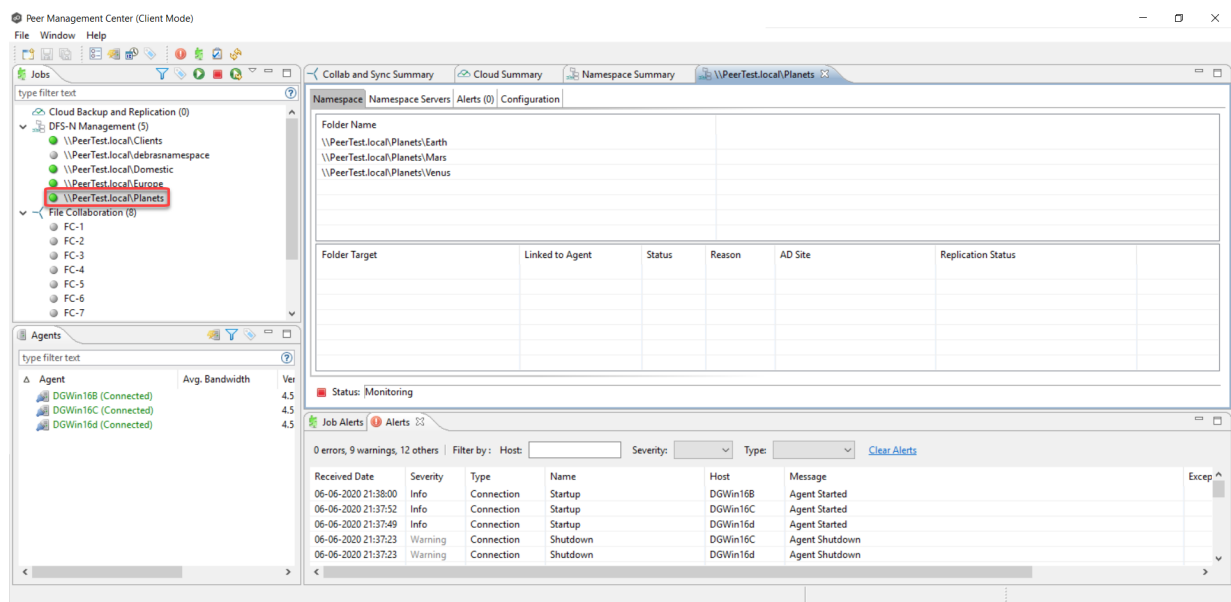
The **Results** page appears.





13. Review the results, and then click **Close**.

A DFS-N Namespace job is created for each namespace you added. The new job(s) are displayed in the **Jobs** view and tab(s) for the jobs appear in the runtime summaries view. The jobs automatically start running. The namespaces can now be [linked to File Collaboration and File Synchronization jobs](#).



## Running a DFS-N Management Job

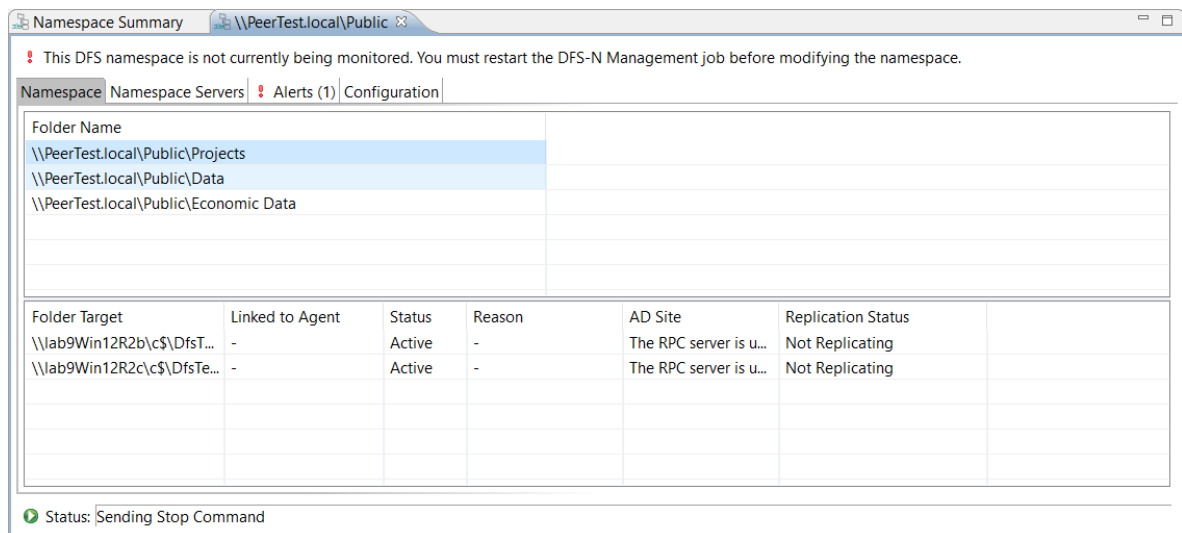
This section describes:

- [Starting a DFS-N Management Job](#)
- [Stopping a DFS-N Management Job](#)

### Starting a DFS-N Management Job

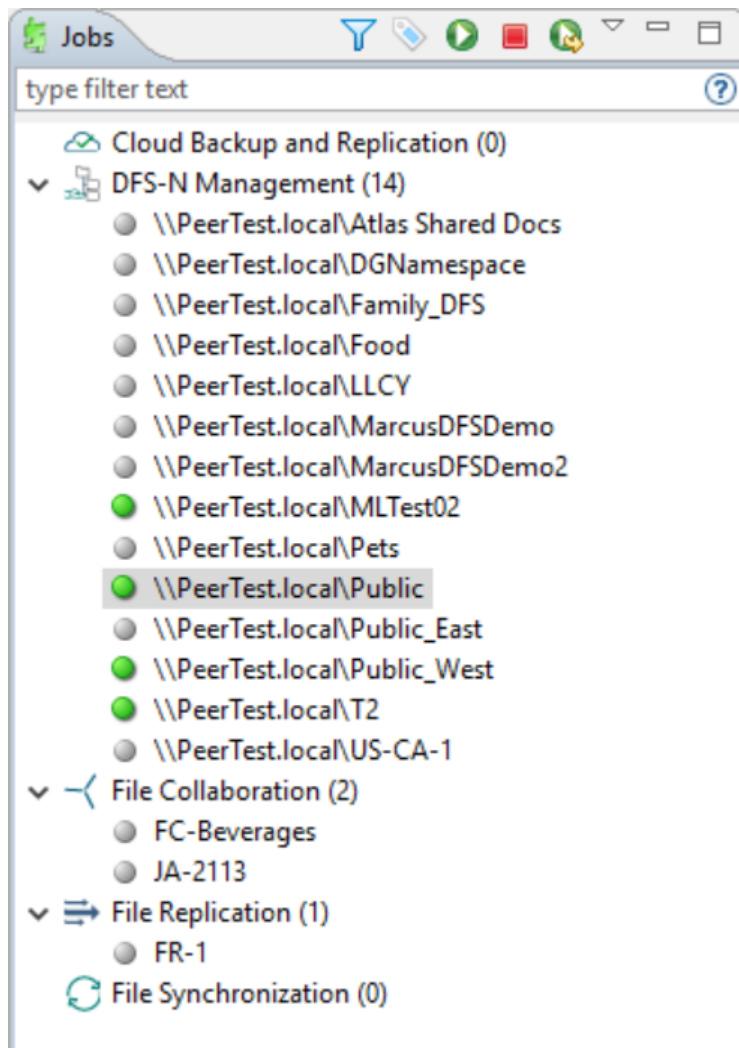
To manually start a DFS-N Management job:

1. Choose one of these options:
  - Right-click the job name in the **Jobs** view.
  - Open the job and then click the **Start/Stop** button in the bottom left corner of the job's **Namespace** tab in the run-time view (shown below).



2. Click **Yes** in the confirmation dialog.

After the job initialization has completed, the job will run. Once the job starts, the icon next to the job name in the **Jobs** view changes from gray to green.



### Stopping a DFS-N Management Job

You can stop a DFS-N Management job at any time. Note that you cannot edit a DFS-N Management job while it is stopped.

To stop a DFS-N Management job:

1. Right-click the job name in the **Jobs** view, and then choose **Stop** from the context menu.

Or, open the job and click the **Start/Stop** button in the bottom left corner of the job's **Namespace** tab in the runtime view.

2. Click **Yes** in the confirmation dialog.

The icon next to the job name in the **Jobs** view changes from green to red.

## Managing DFS Namespaces

This section describes:

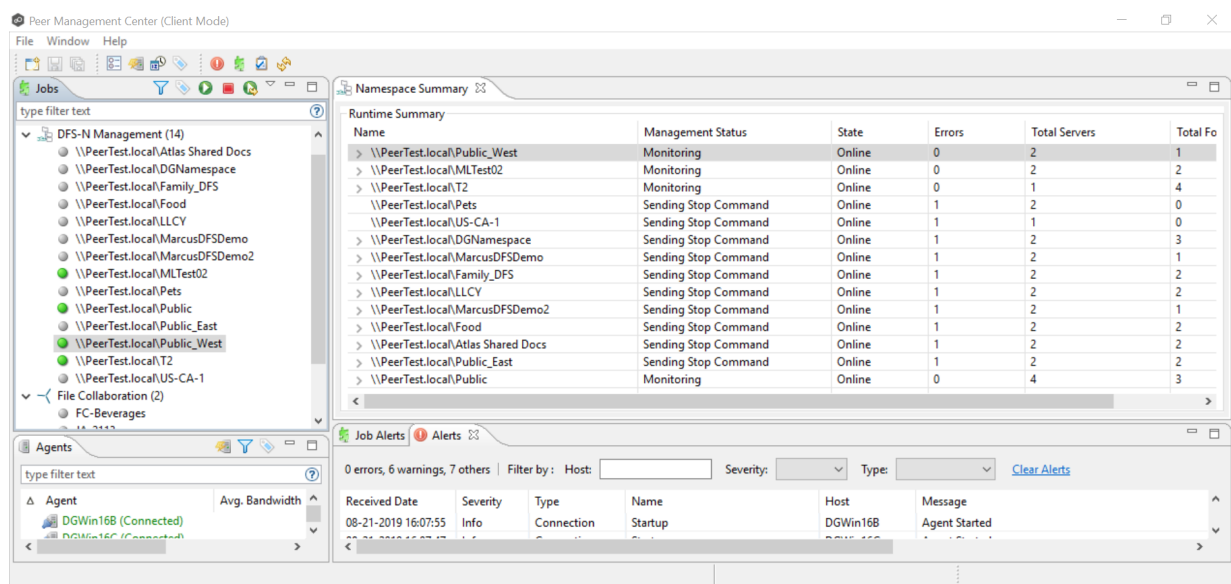
- [Adding an Existing Namespace](#)
- [Adding a Namespace Server](#)
- [Adding a Namespace Folder](#)
- [Adding a Namespace Folder Target](#)

### Adding a Namespace Server

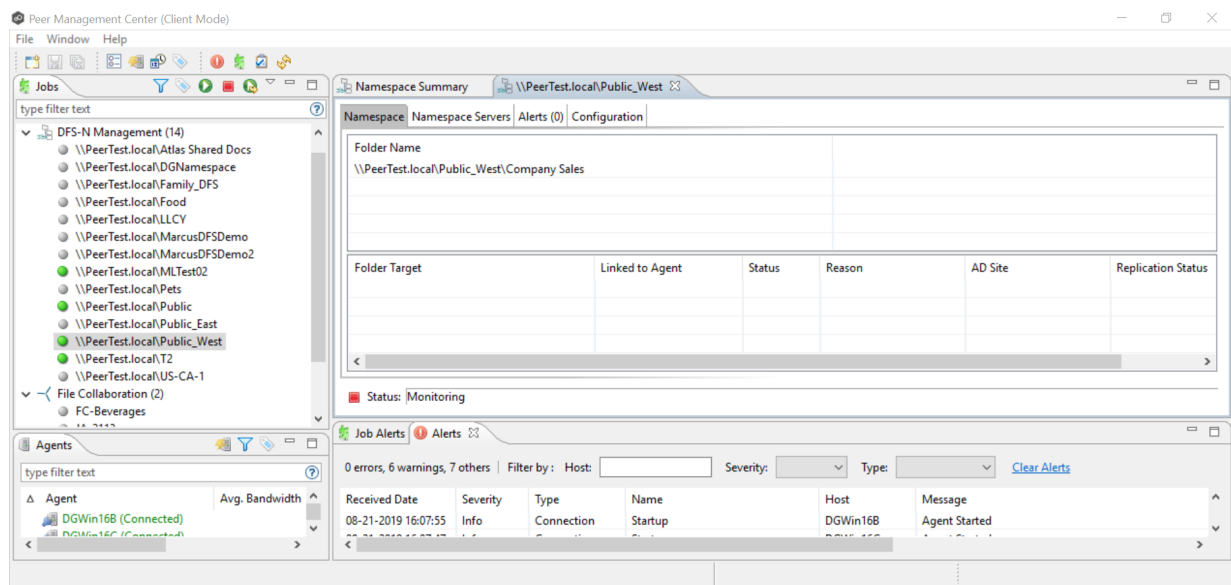
You can add a namespace server to a namespace.

To add a namespace server to a namespace:

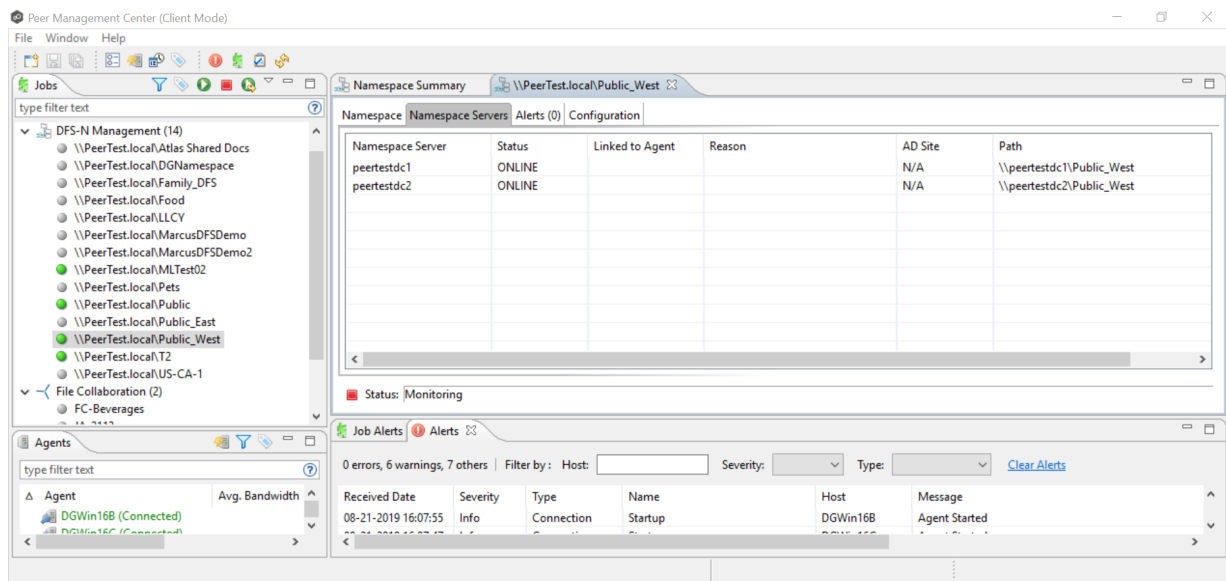
1. Double-click the job name in the **Jobs** view or the **Namespace Summary** view to open the runtime summary view for the job.



The runtime summary view for the job is displayed.



- Click the **Namespace Servers** tab.



- Right-click anywhere in the **Namespace Servers** tab, and then select **Add Servers**.

Namespace Namespace Servers Alerts (0) Configuration					
Namespace Server	Status	Linked to Agent	Reason	AD Site	Path
peertestdc1	ONLINE			N/A	\\peertestdc1\Public_West
peertestdc2	ONLINE			N/A	\\peertestdc2\Public_West
<div> Enable/Disable Server  Delete Server  Open in Explorer  Add Servers </div>					

< >

Status: Monitoring

The **Add DFS Namespace Server** wizard appears.

4. Enter the fully qualified path of a file server in the **Server Name** field, and then click **Add**.

Add DFS Namespace Server

## Namespace Servers

Select one or more servers to be added. The servers you select will be known as namespace servers.

Namespace Servers

Namespace Settings

Confirmation

Results

Enter the fully qualified domain name of a server running the DFS Namespace Service.

Server Name:

Browse

AddDelete

< BackNext >Cancel

The server path is listed in the area below.

5. Add additional servers if desired.
6. Click **Next**.

The **Namespace Settings** page is displayed.

The screenshot shows the 'Add DFS Namespace Server' wizard at the 'Namespace Settings' step. The left sidebar has 'Namespace Settings' selected. The main area contains instructions and a table for configuring the shared folder.

**Namespace Settings**  
Modify the settings of the shared folder.

If necessary, the wizard will create a shared folder on the namespace server.  
Modify the settings of the DFS root share for each namespace server, including its local path and permissions.

Shared Folder:  
Public\_West

Server Name	DFS Root Share Path	Permissions
peertestdc1.peert...	C:\DFSRoots\Public_West	Everyone Full Access

< Back   Next >   Cancel

7. (Optional) Edit the namespace server settings: **DFS Root Share Path** and **Permissions**.

8. Click **Next**.

The **Confirm** page is displayed.

The screenshot shows the 'Add DFS Namespace Server' wizard at the 'Confirmation' step. The left sidebar has 'Confirmation' selected. The main area displays the namespace and the servers to be added.

**Confirmation**  
Do you want to add the following DFS namespace servers?

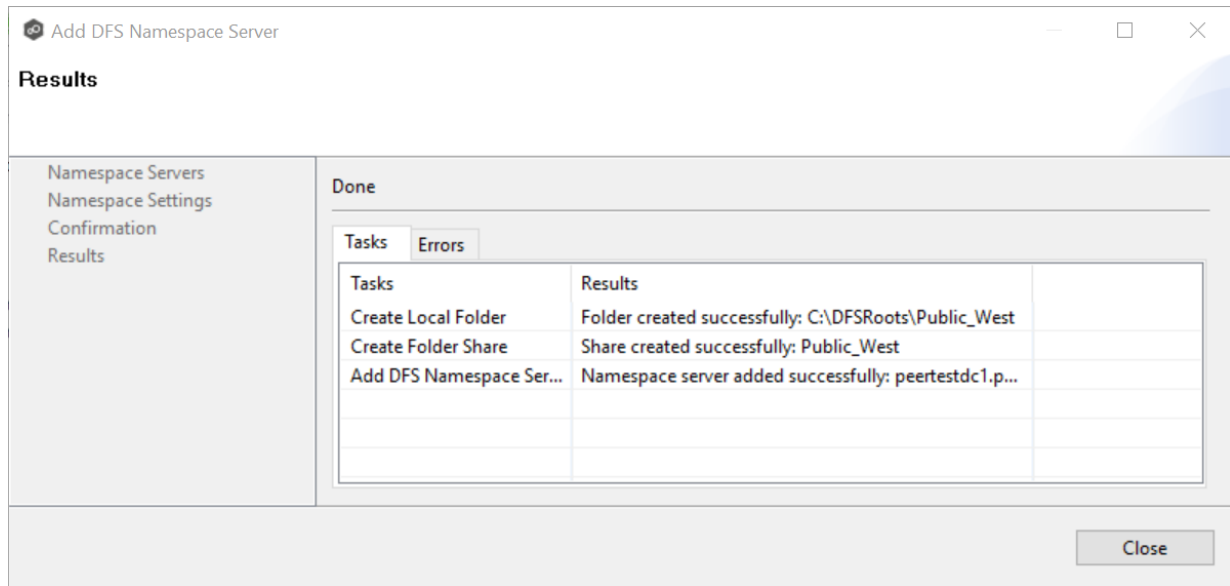
Namespace: Public\_West  
Adding Servers:  
- peertestdc1.peertest.local

< Back   Add   Cancel

9. Review the namespace server configuration.

10. Click **Add** if the configuration is correct; otherwise, click **Back** and correct the configuration.

The **Results** page is displayed.



11. Click **OK**.

The newly added server is listed in the **Namespace Servers** tab.

### Adding a Namespace Folder

You can add a namespace folder to a namespace. When adding a namespace folder, you can also add folder targets to the new namespace folder; you can also [add folder targets](#) later if you wish.

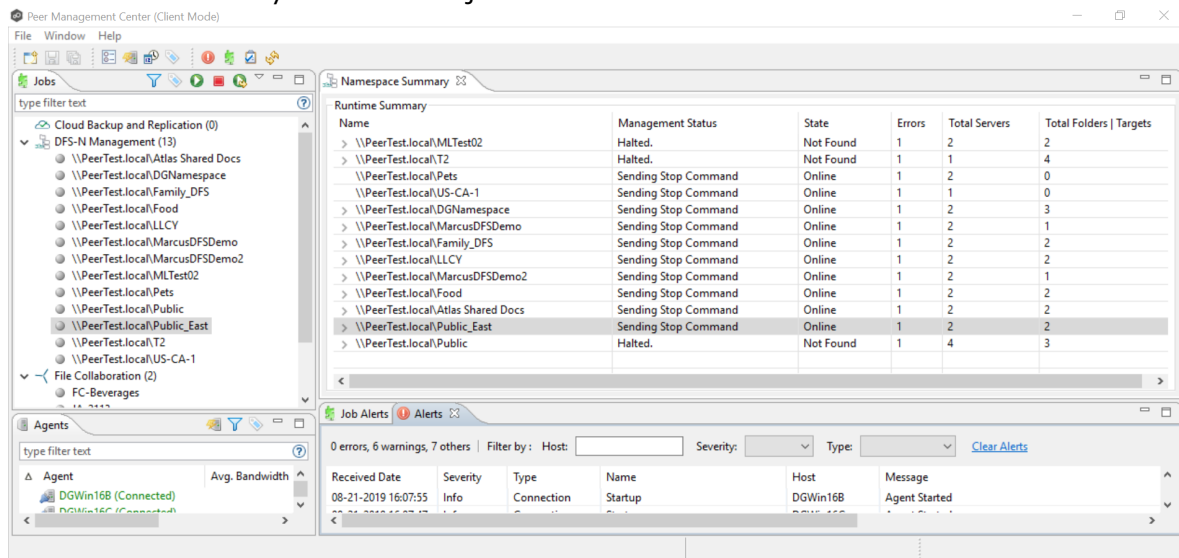
**Note:** A DFS-N Namespace job must be running before you can edit it.

The job must be running.

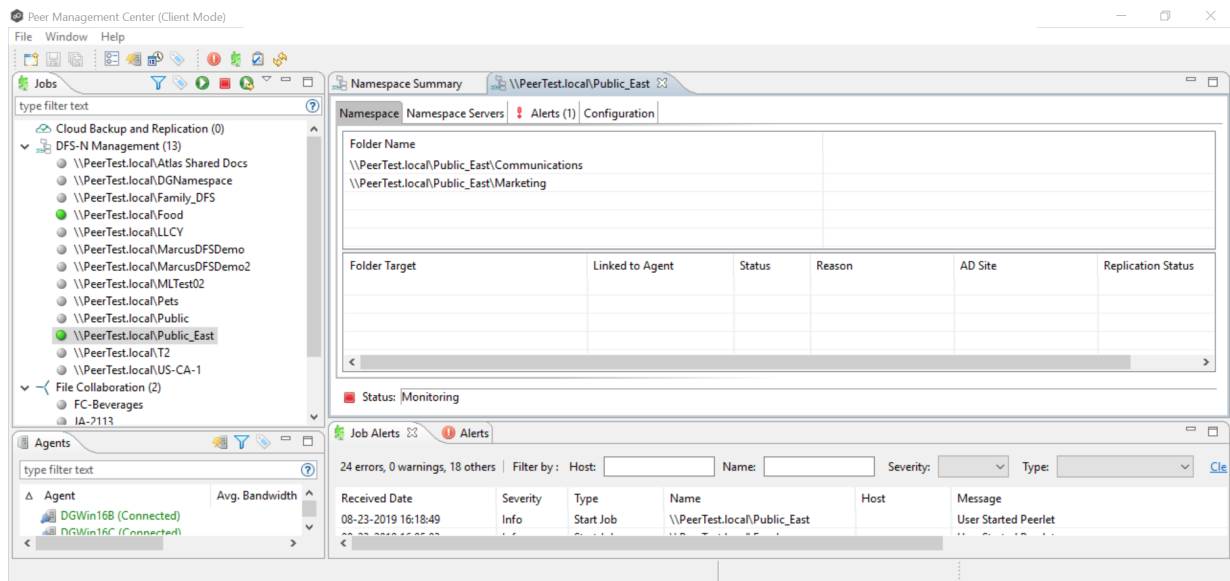
To add a namespace folder to a namespace:



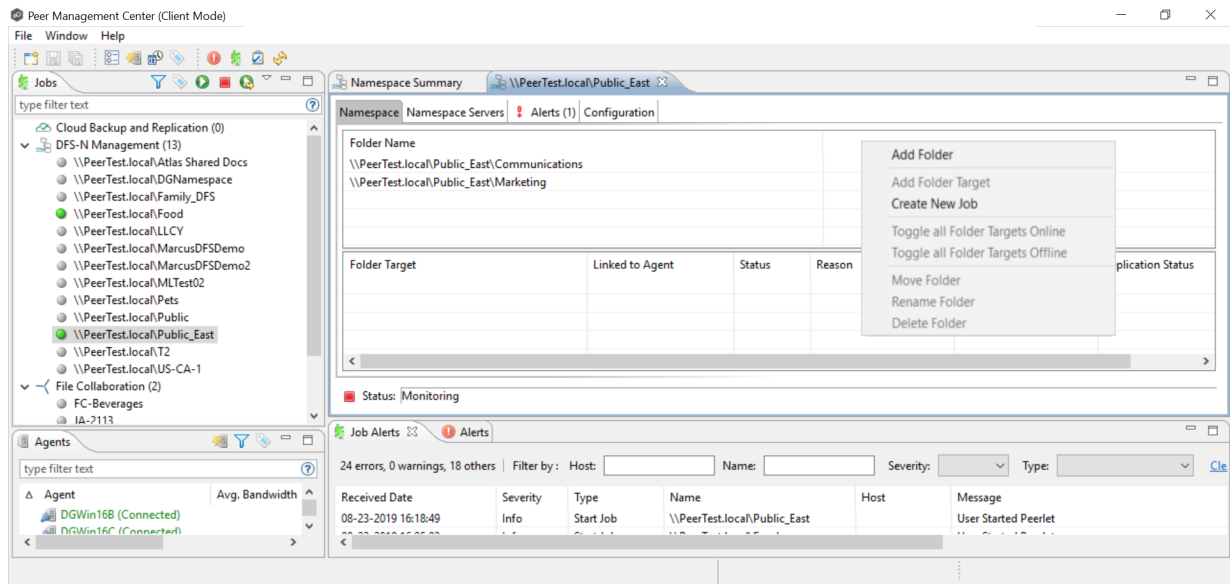
1. Double-click the job name in the **Jobs** view or the **Namespace Summary** view to open the runtime summary view for the job.



The runtime summary view for the job is displayed.

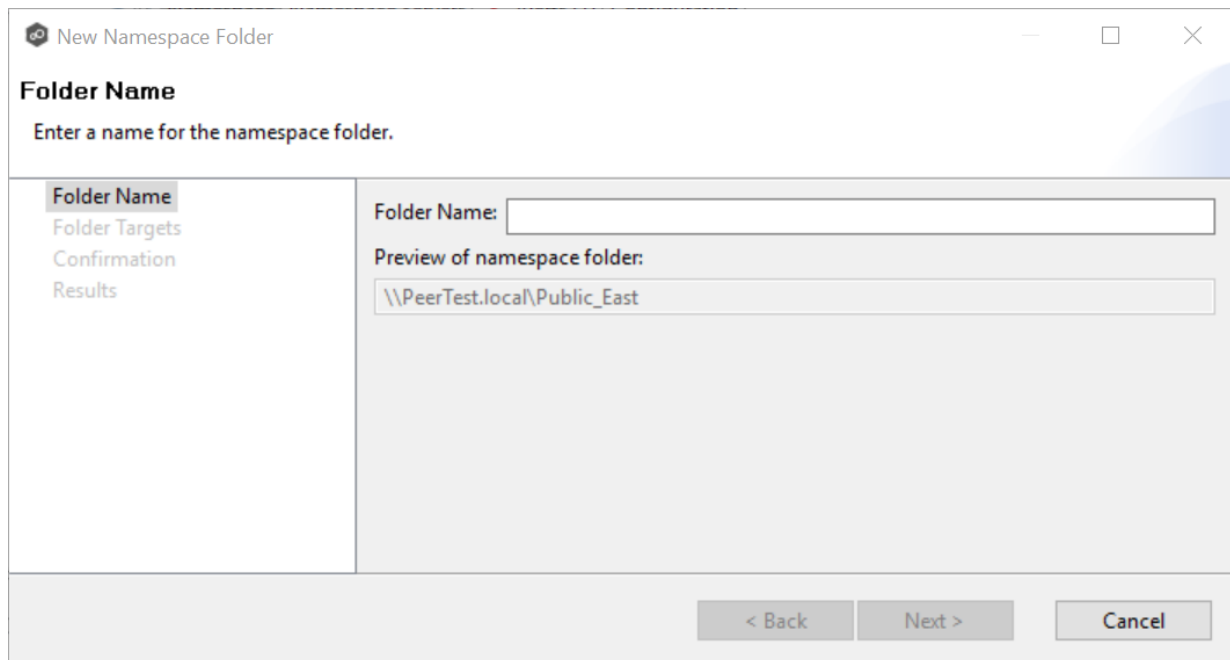


2. Right-click anywhere in the **Namespace** tab, and then select **Add Folder**.

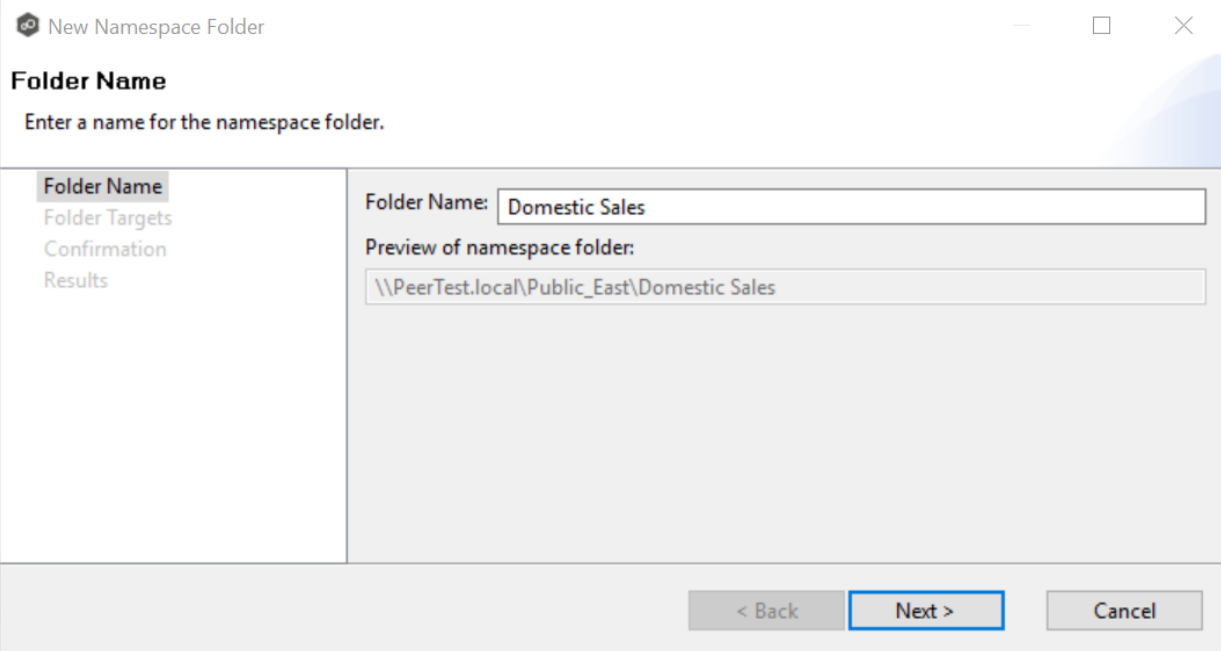


The **New Namespace Folder** wizard appears.

- Enter a name for the namespace folder in the **Folder Name** field.



After you enter the folder name, a preview of the folder and path name appears below the **Folder Name** field.

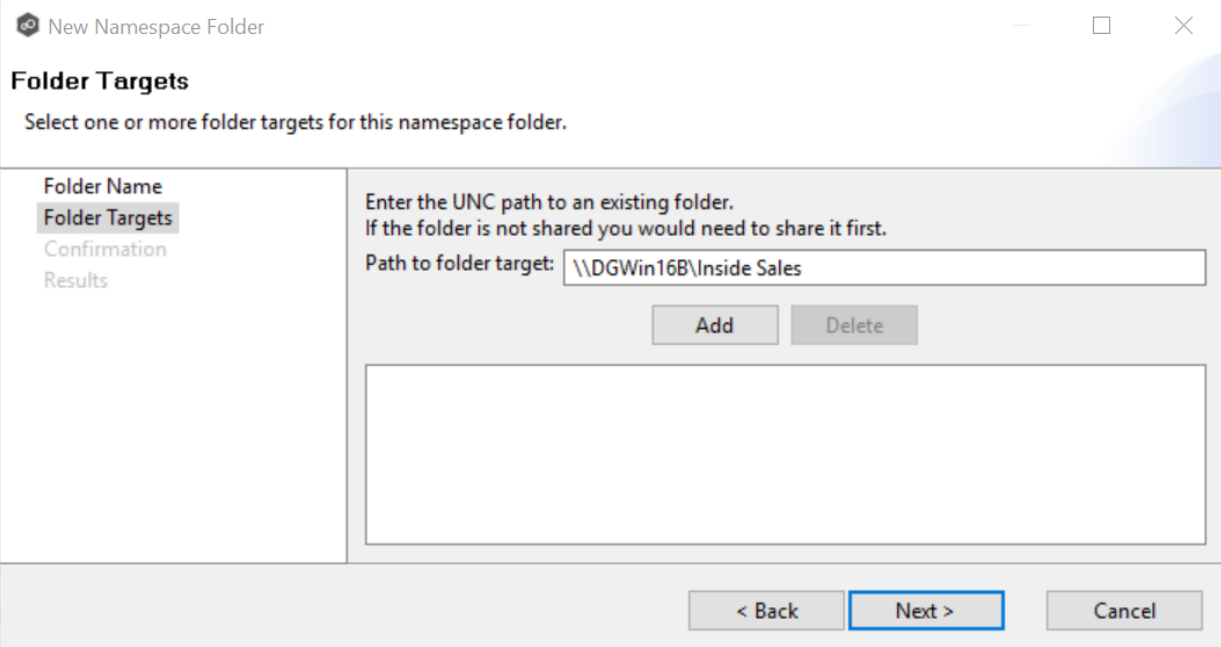


The dialog box is titled "New Namespace Folder". It has a sidebar on the left with four items: "Folder Name" (selected), "Folder Targets", "Confirmation", and "Results". The main area is titled "Folder Name" and contains the instruction "Enter a name for the namespace folder." Below this, there is a text input field labeled "Folder Name:" with the value "Domestic Sales". Underneath is a "Preview of namespace folder:" section with a text box showing the path "\\PeerTest.local\\Public\_East\\Domestic Sales". At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

- Click **Next**.

The **Folder Targets** page is displayed. It is optional to add folder targets for the namespace folder at this point. You can add them later if you wish. If you choose to add the folder targets now, they must already exist and be shared.

- (Optional) Enter the UNC path to the shared folder you want to be a folder target, and then click **Add**. (Click **Next** if you do not want to add folder targets at this point.)



The dialog box is titled "New Namespace Folder". It has a sidebar on the left with four items: "Folder Name", "Folder Targets" (selected), "Confirmation", and "Results". The main area is titled "Folder Targets" and contains the instruction "Select one or more folder targets for this namespace folder." Below this, there is a text input field labeled "Path to folder target:" with the value "\\DGWin16B\\Inside Sales". Above this field is the instruction "Enter the UNC path to an existing folder. If the folder is not shared you would need to share it first." Below the input field are two buttons: "Add" and "Delete". At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

The folder target path is listed in the field below.

The screenshot shows the 'New Namespace Folder' dialog box with the 'Folder Targets' tab selected. The dialog has a title bar with a minimize button, a maximize button (disabled), and a close button. Below the title bar, the text 'New Namespace Folder' is displayed. The main area is titled 'Folder Targets' and contains the instruction 'Select one or more folder targets for this namespace folder.' On the left, there is a sidebar with four tabs: 'Folder Name', 'Folder Targets' (selected), 'Confirmation', and 'Results'. The main content area on the right has the following text: 'Enter the UNC path to an existing folder. If the folder is not shared you would need to share it first.' Below this is a text input field labeled 'Path to folder target:' with the example text '\\Server\Shared Folder\Folder Target'. To the right of the input field are 'Add' and 'Delete' buttons. Below the input field is a list box containing the path '\\DGWin16B\Inside Sales'. At the bottom of the dialog are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

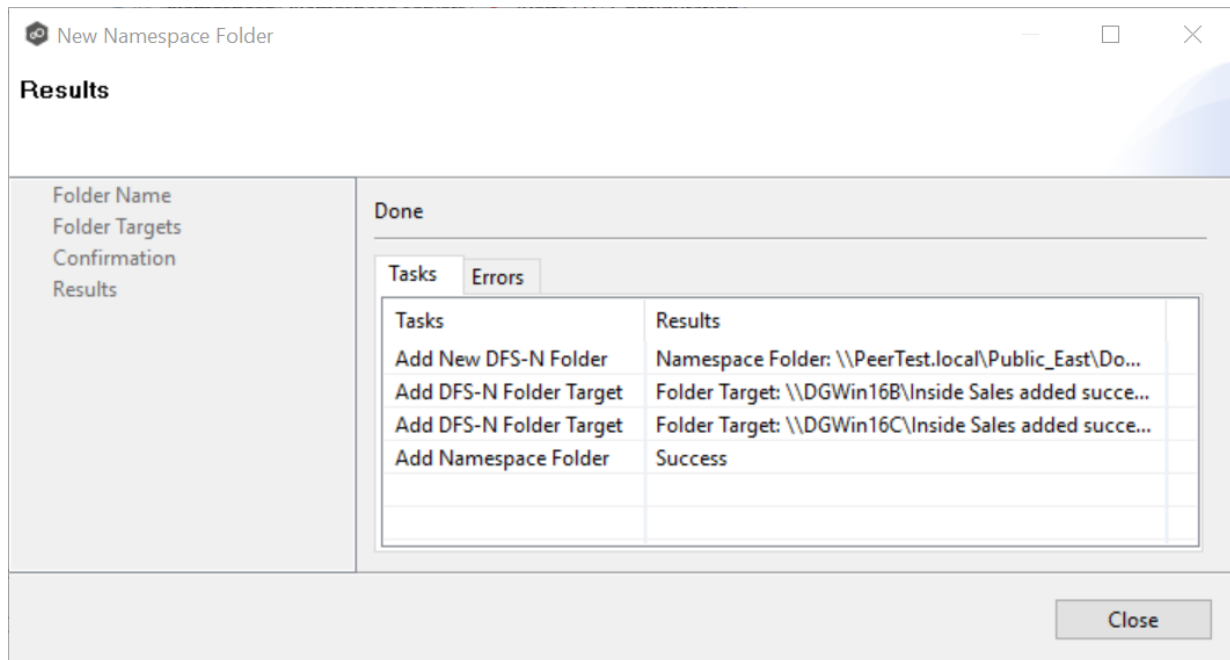
6. Add additional folder targets if desired.
7. Click **Next**.

The **Confirmation** page is displayed.

The screenshot shows the 'New Namespace Folder' dialog box with the 'Confirmation' tab selected. The dialog has the same title bar as the previous screenshot. Below the title bar, the text 'New Namespace Folder' is displayed. The main area is titled 'Confirmation' and contains the question 'Do you want to add the following namespace folder and folder targets?'. On the left, there is a sidebar with four tabs: 'Folder Name', 'Folder Targets', 'Confirmation' (selected), and 'Results'. The main content area on the right displays the following information: 'Namespace Folder: \\PeerTest.local\Public\_East\Domestic Sales' and 'Folder Targets: \\DGWin16B\Inside Sales' and '\\DGWin16C\Inside Sales'. At the bottom of the dialog are three buttons: '< Back', 'Add', and 'Cancel'.

8. Review the folders and folder targets.
9. Click **Add** if the configuration is correct; otherwise, click **Back** and correct the configuration.

The **Results** page is displayed.

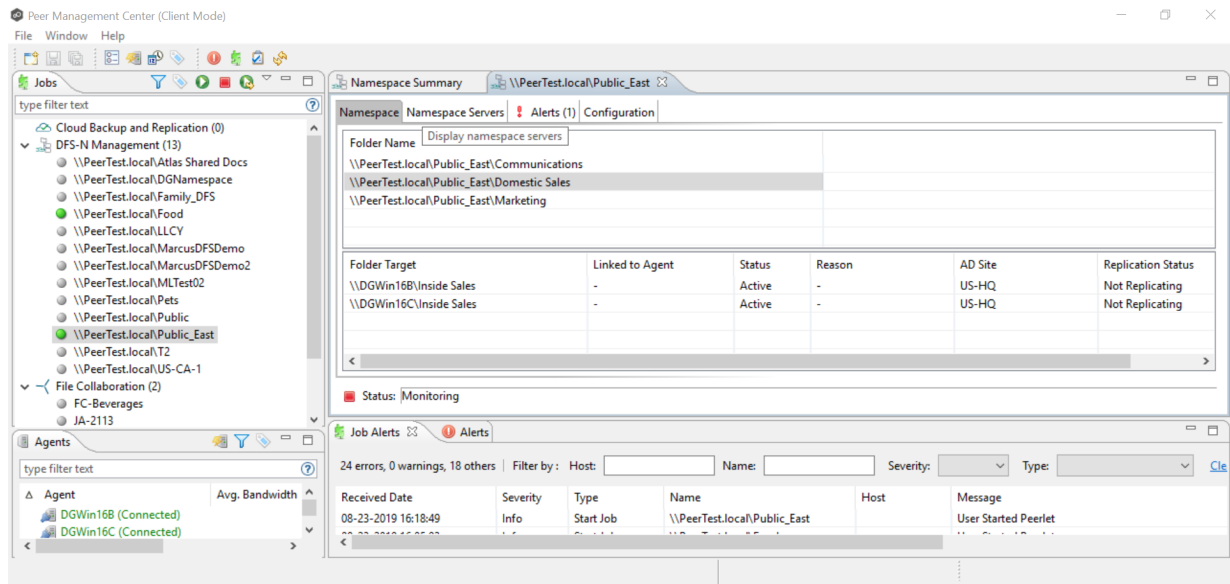


10. Click **Close**.

The runtime summary view for the job is displayed.

11. Click the job you just modified.

The newly added folder and folder targets are listed in the **Namespace** tab. (You may have to scroll to view the **Folder Target** section of the tab.)



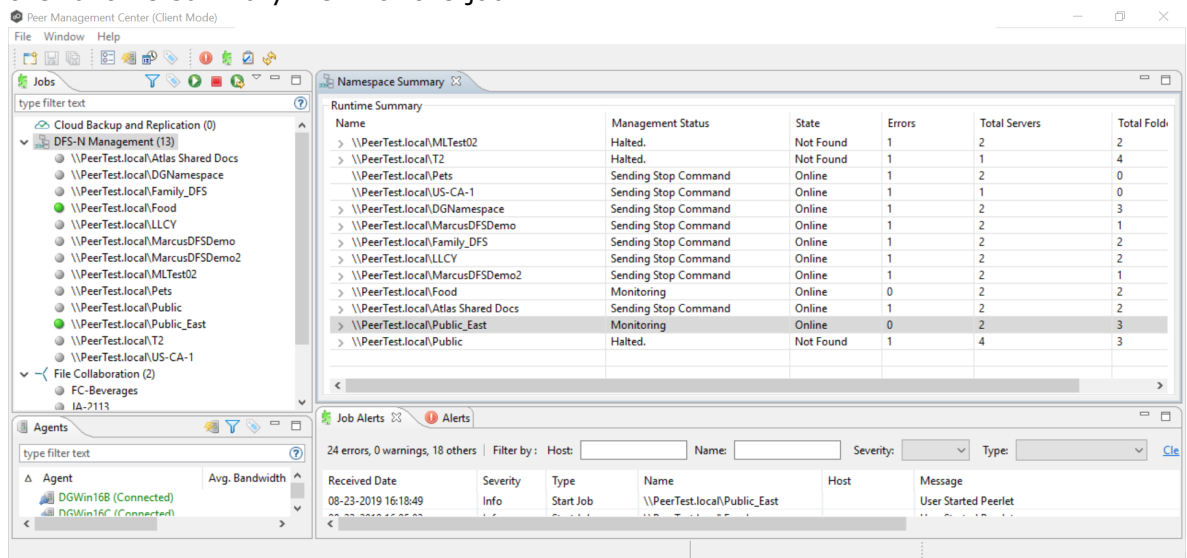
## Adding a Namespace Folder Target

You can add a folder target to a namespace.

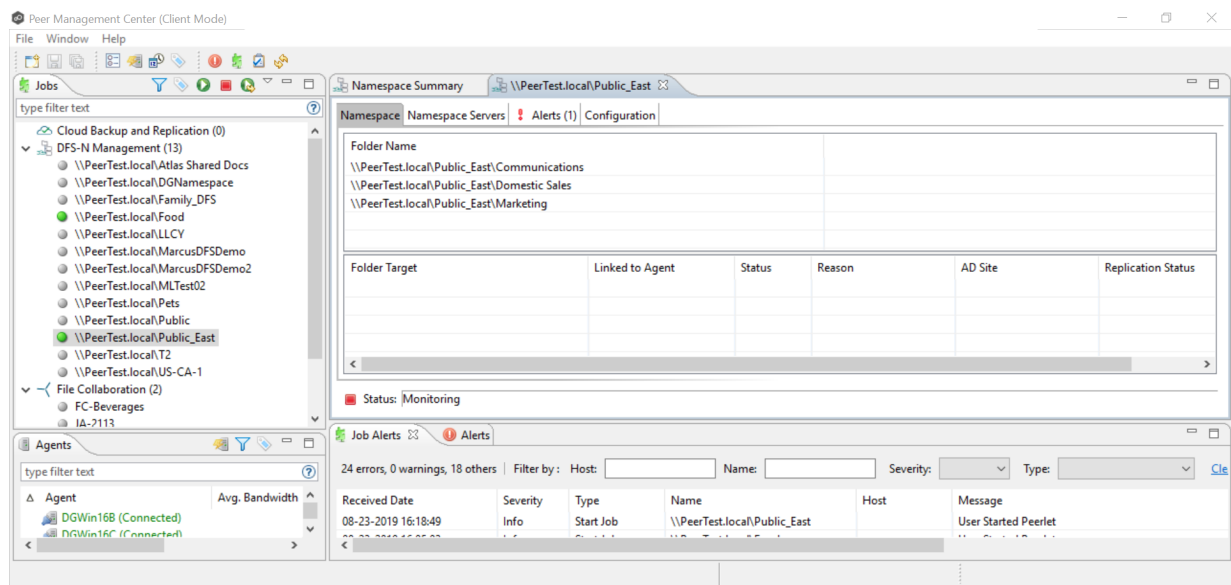
**Note:** A DFS-N Namespace job must be running before you can edit it.

To add a folder target to a namespace:

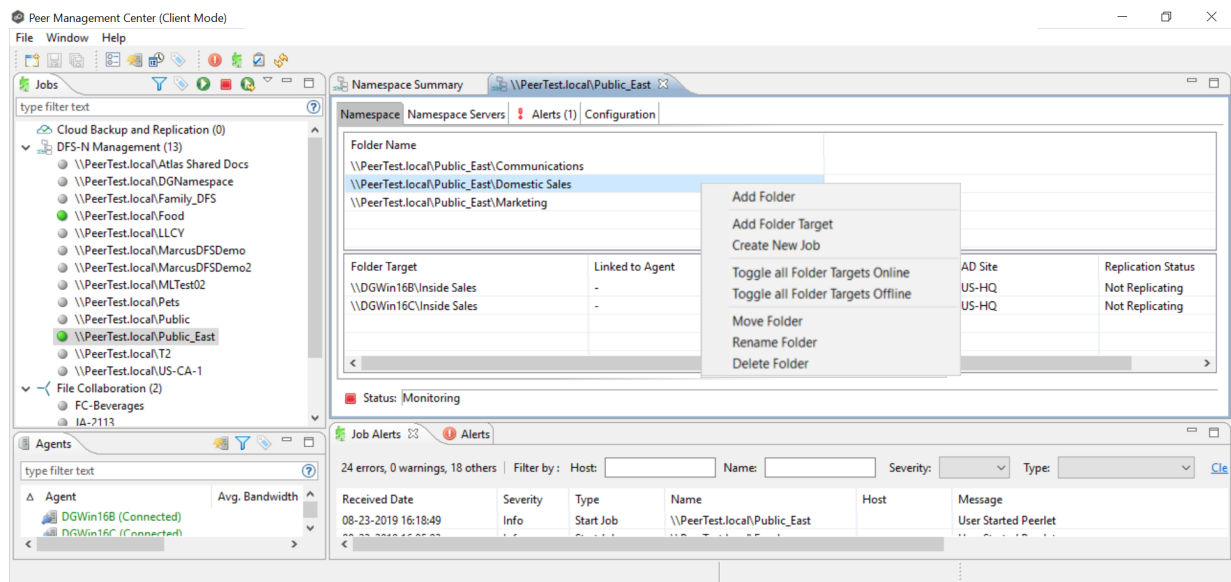
1. Double-click the job name in the **Jobs** view or the **Namespace Summary** view to open the runtime summary view for the job.



The runtime summary view for the job is displayed.

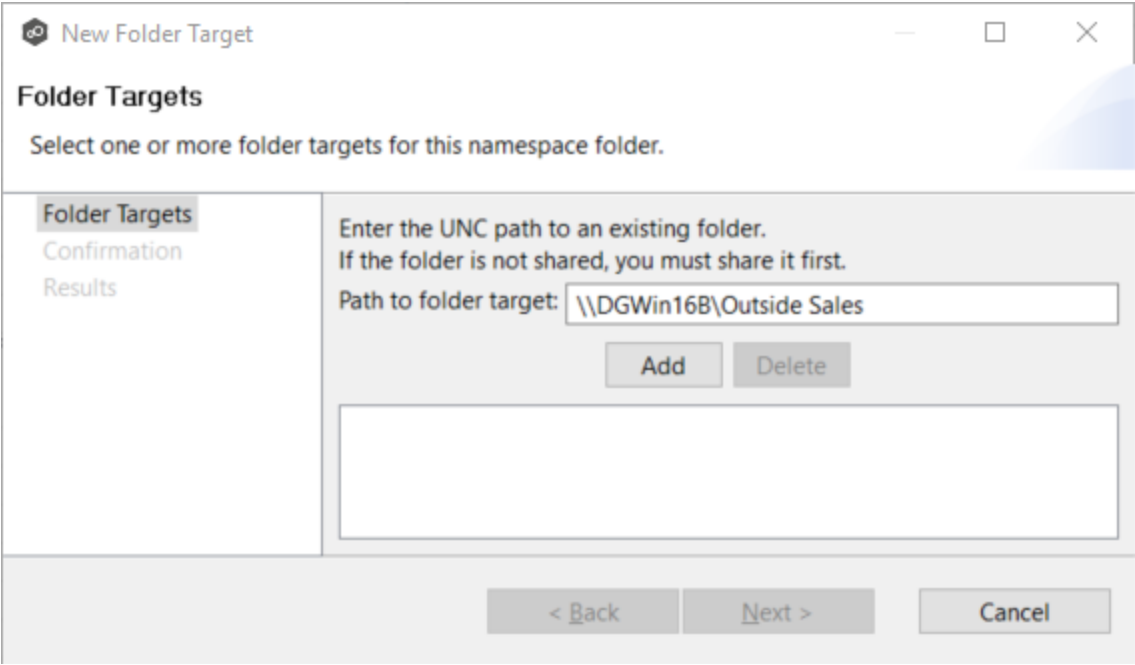


2. Right-click the folder you want to add a folder target to, and then select **Add Folder Target**.



The **New Folder Target** wizard appears.

3. Enter the UNC path to a shared folder, and then click **Add**.



The dialog box is titled "New Folder Target" and has a "Folder Targets" tab selected. It contains a list of folder targets on the left and a text input field on the right. The text input field contains the path "\\DGWin16B\\Outside Sales". Below the text input field are "Add" and "Delete" buttons. At the bottom of the dialog are "< Back", "Next >", and "Cancel" buttons.

New Folder Target

Folder Targets

Select one or more folder targets for this namespace folder.

Folder Targets

Confirmation

Results

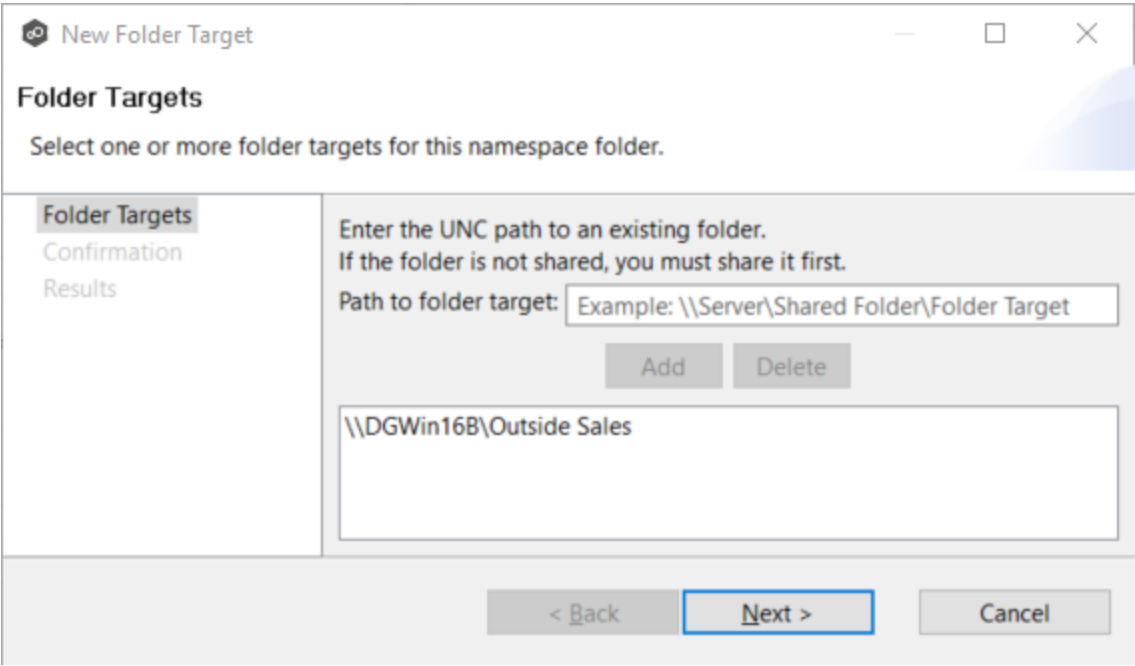
Enter the UNC path to an existing folder.  
If the folder is not shared, you must share it first.

Path to folder target: \\DGWin16B\\Outside Sales

Add Delete

< Back Next > Cancel

The folder target path is listed in the field below.



The dialog box is titled "New Folder Target" and has a "Folder Targets" tab selected. It contains a list of folder targets on the left and a text input field on the right. The text input field contains the path "\\DGWin16B\\Outside Sales". Below the text input field are "Add" and "Delete" buttons. At the bottom of the dialog are "< Back", "Next >", and "Cancel" buttons.

New Folder Target

Folder Targets

Select one or more folder targets for this namespace folder.

Folder Targets

Confirmation

Results

Enter the UNC path to an existing folder.  
If the folder is not shared, you must share it first.

Path to folder target: Example: \\Server\\Shared Folder\\Folder Target

Add Delete

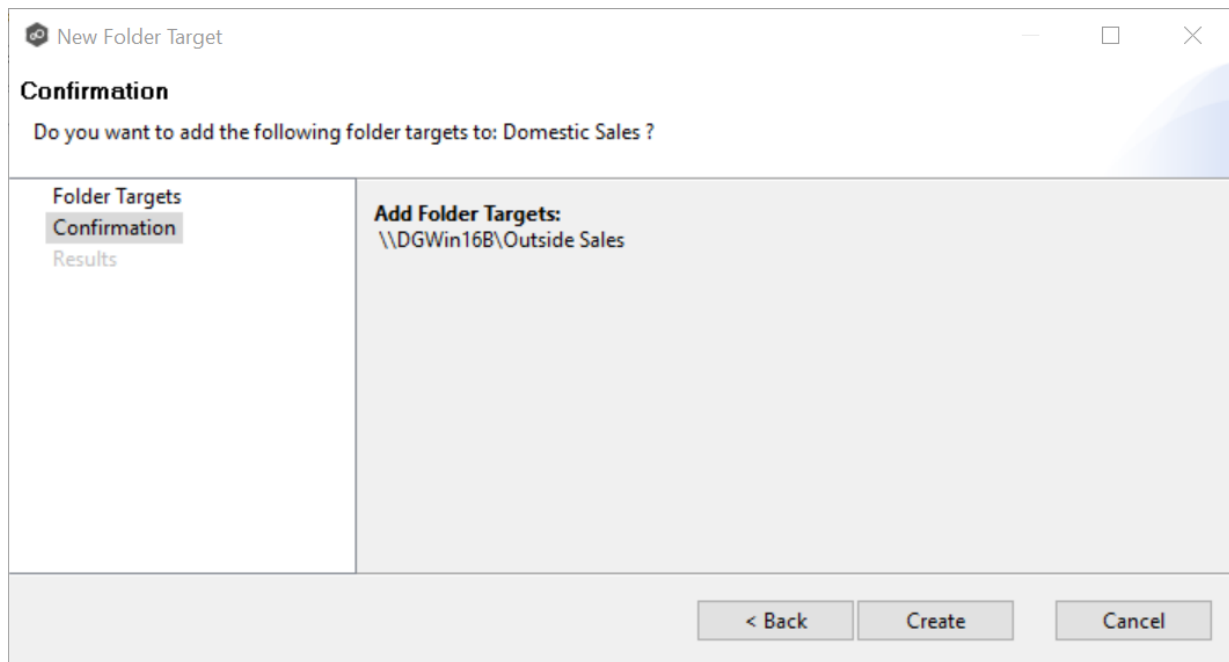
\\DGWin16B\\Outside Sales

< Back Next > Cancel

4. (Optional) Add additional folder targets.
5. Click **Next**.

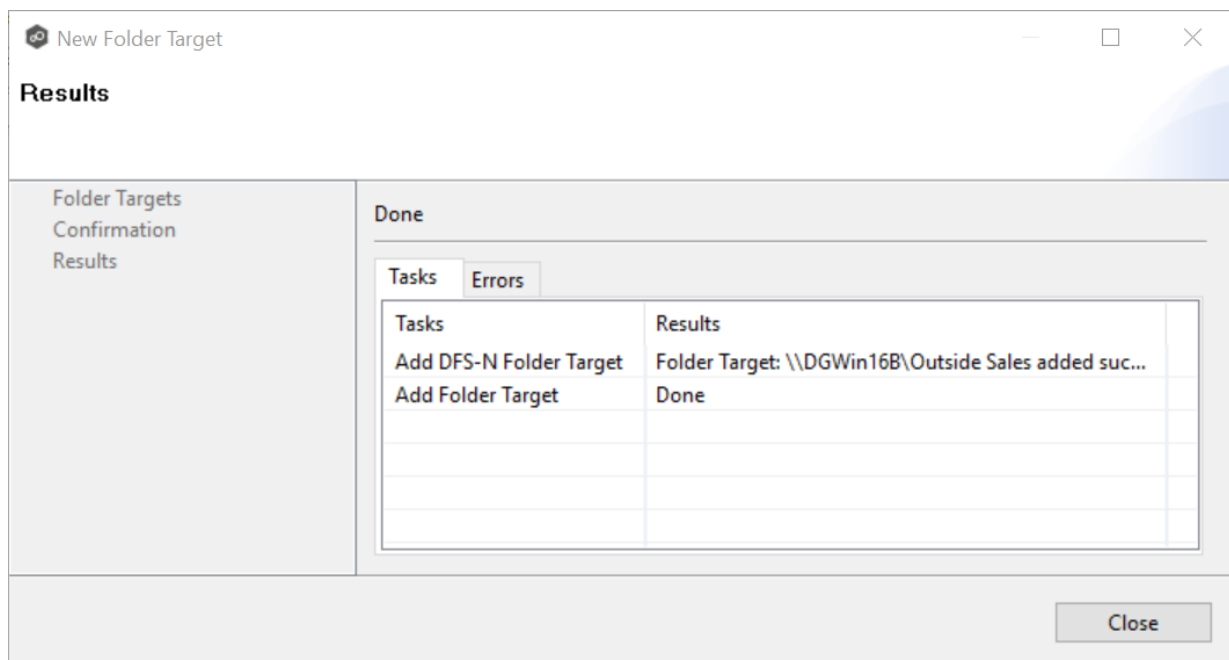
The **Confirmation** page is displayed.





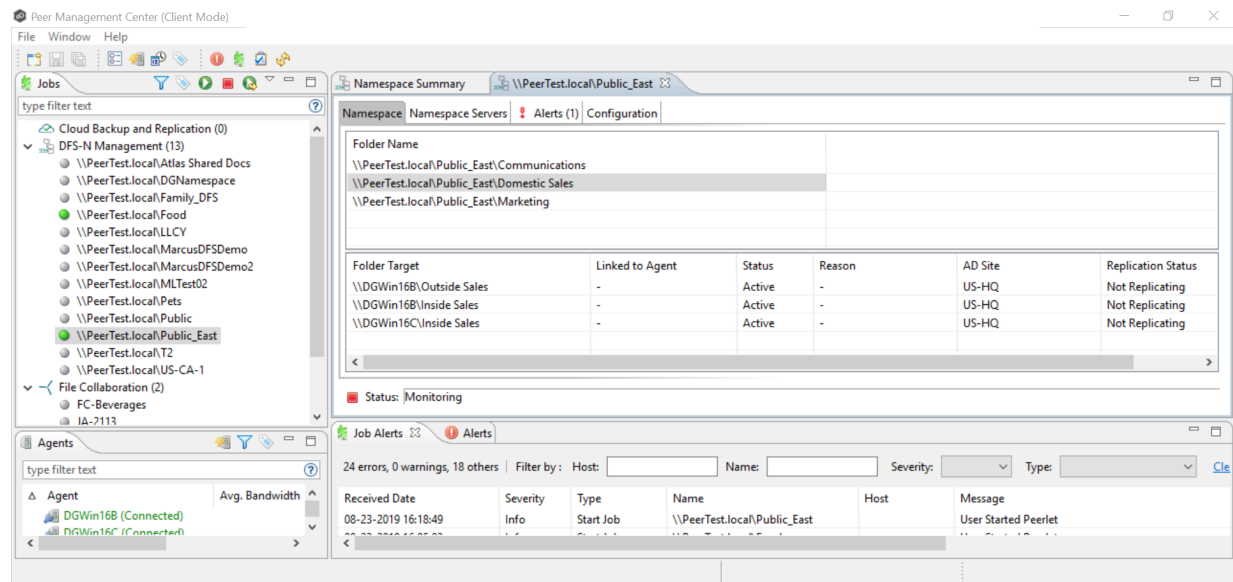
6. Review the folder targets.
7. Click **Create** if the configuration is correct; otherwise, click **Back** and correct the configuration.

The **Results** page is displayed.



8. Click **Close**.

The newly added folder targets are listed in the Folder Target section of the job's **Namespace** tab.



## Connecting DFS Namespaces with File Collaboration and File Synchronization Jobs

In order to allow the PeerGFS synchronization engine to automate the state of folder targets, a File Collaboration or File Synchronization job must be linked to a job that manages the appropriate DFS namespace.

The two ways to create this link are:

- If the File Collaboration or File Synchronization job does not yet exist, create one from the DFS namespace folder. See [Create a File Collaboration or Synchronization Job from a DFS Namespace Folder](#) for step-by-step instructions.
- If the File Collaboration or File Synchronization job already exists, edit the job and use the [File Collaboration DFS-N settings page](#) or [File Synchronization DFS-N settings page](#) to link the collaboration or synchronization to the DFS-N Management job. See [Linking a Namespace with an Existing File Collaboration or Synchronization Job](#) for step-by-step instructions.

**Note:** Currently, only File Collaboration and File Synchronization jobs can be linked to a DFS-N Management job.

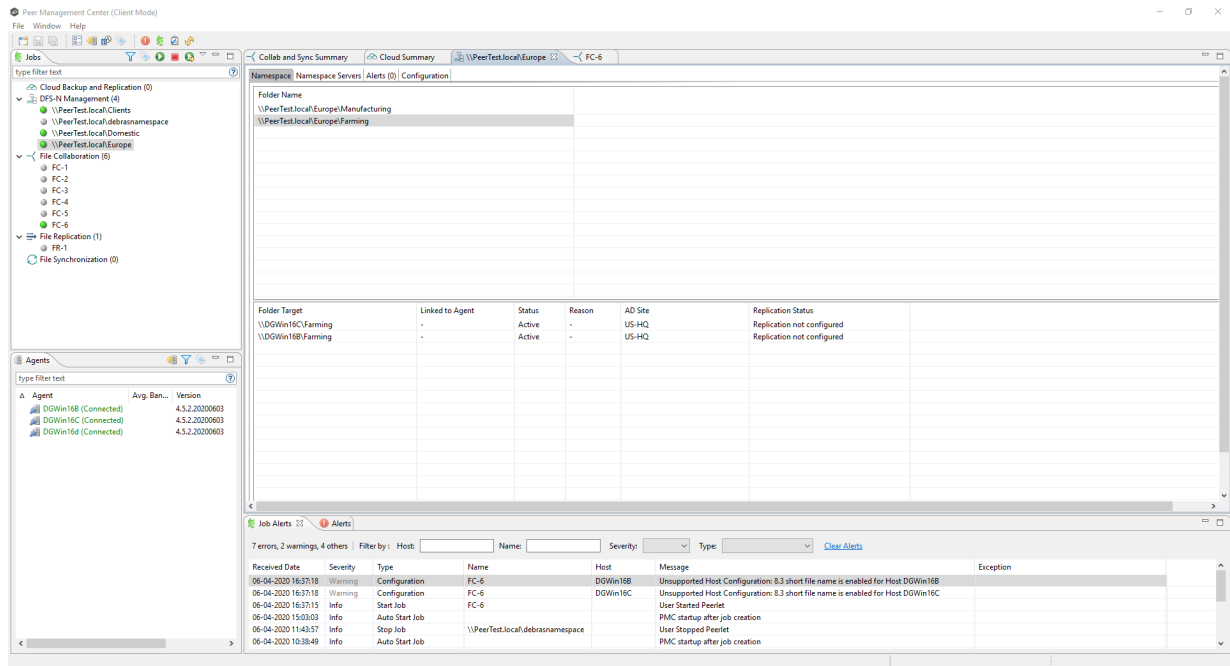
## Creating a File Collaboration or File Synchronization Job from a DFS Namespace Folder

You can create a File Collaboration or File Synchronization job from a DFS namespace folder. These steps require that:

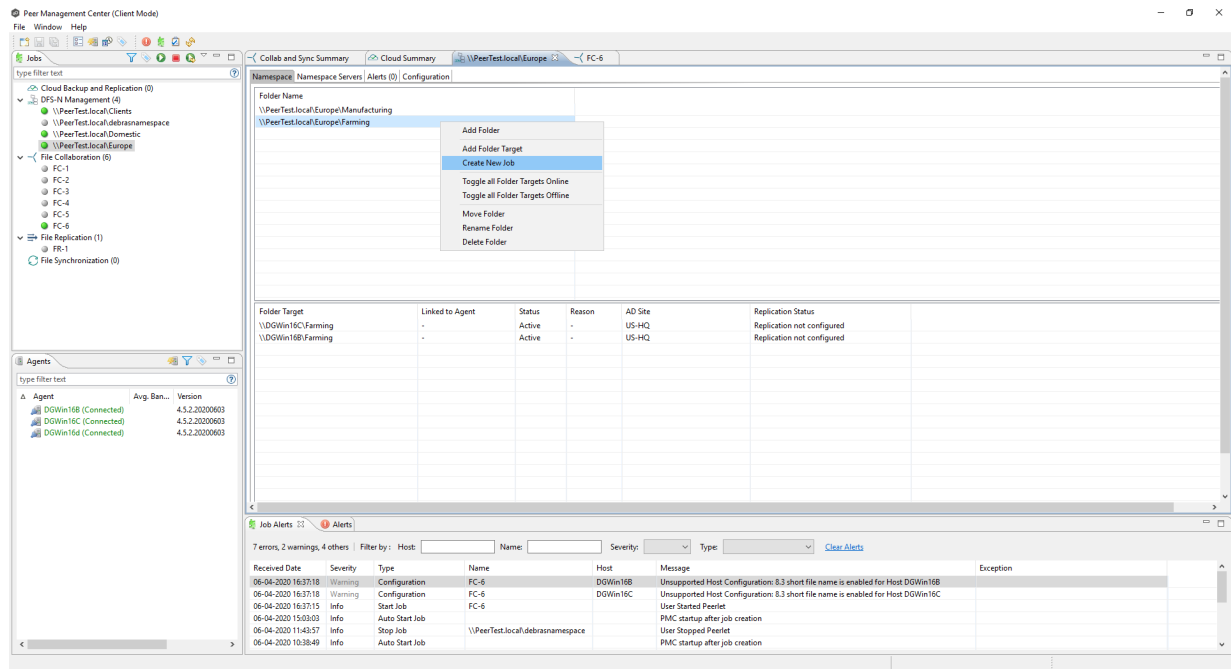
- The DFS namespace has been already created and is being managed by Peer Management Center.
- The namespace folder has at least two folder targets.

To create a File Collaboration or File Synchronization job from a namespace folder:

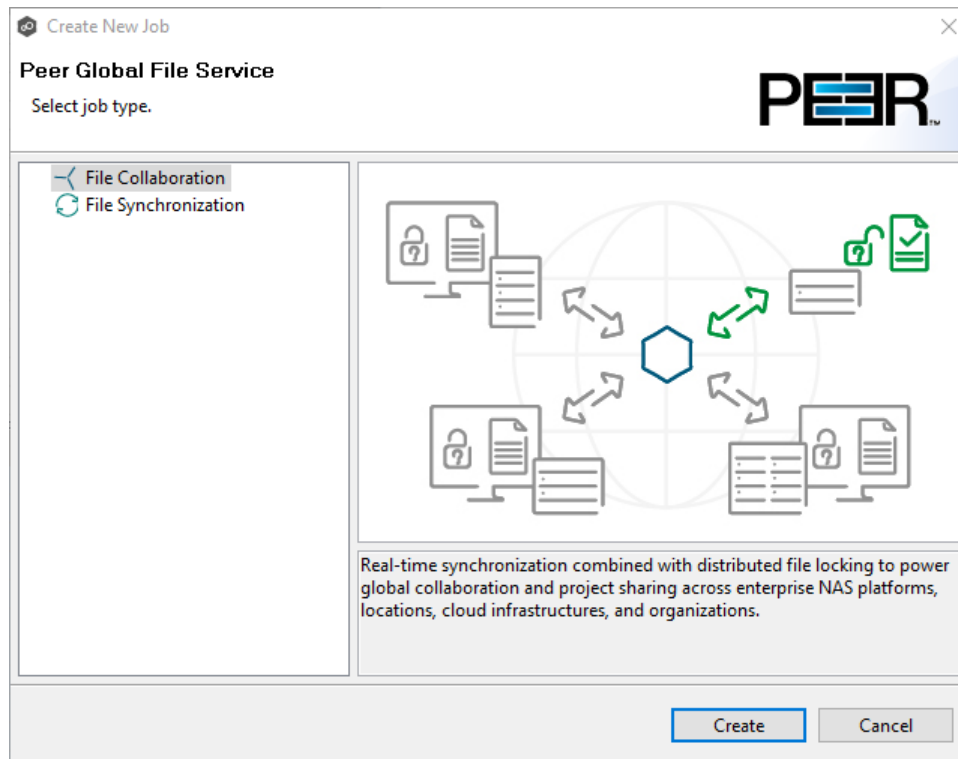
1. From the **Jobs** view, open the DFS-N Management job managing the namespace.
2. Open the **Namespace** tab if it is not already displayed.



3. In the **Namespace** tab, right-click the desired namespace folder and select **Create New Job**.



The **Create New Job** wizard displays a list of job types you can create: File Collaboration and File Synchronization. All other job types are not supported for use with DFS namespace management.



4. Select a job type and click **Create**:

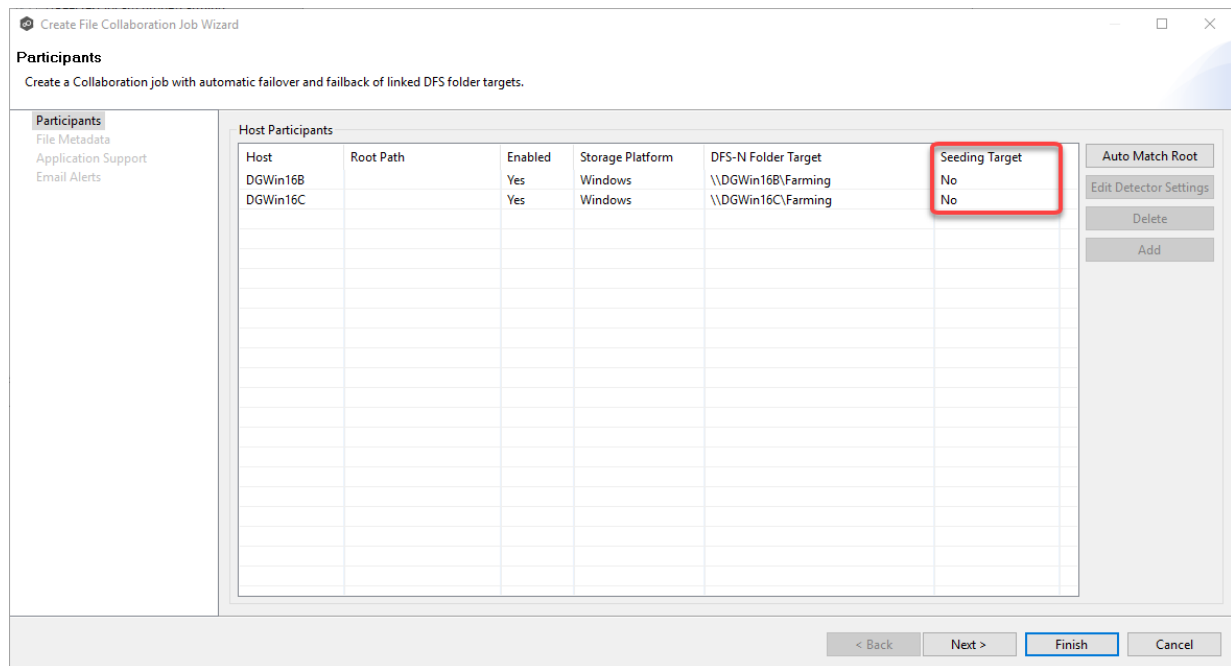
- The job name must be unique.

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.

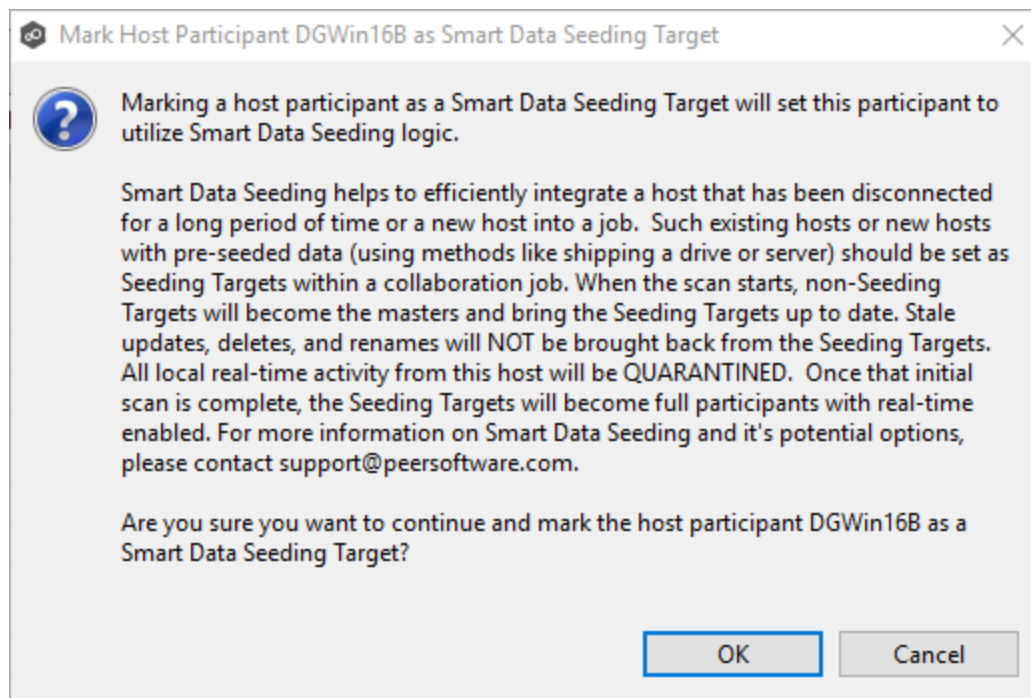
7. If the **Storage Platform** column is blank, select the platform from the drop-down list.

- If you selected a platform other than Windows, click the **Edit Detector Settings** button and enter the required settings for your selected platform.
- If the **DFS Folder Target** column is blank, manually enter the folder targets in the **DFS Folder Target** column or click in the column and select one from the drop-down list.





If you select **Yes**, a message describing seeding behavior is displayed. Multiple participants in a File Collaboration or File Synchronization job can be set as smart data seeding targets; however, at least one participant should not be set as a smart data seeding target. This participant will be acting as the "master" source for the smart data seeding targets. For more information about smart data seeding, see [Smart Data Seeding](#) or contact [support@peersoftware.com](mailto:support@peersoftware.com).





13. Click **Auto Match Root** to automatically match a participant with the appropriate namespace folder target.

After clicking **Auto Match Root**, the root path will appear in the **Root Path** column. If this is the first collaboration or file synchronization job created with these Agents, you may need to populate the **Root Path** column manually:

- If using a Windows file server, the root path should be the local path on that file server that corresponds to the share path of the folder target.
- If using a non-Windows NAS device, this path should match the namespace folder target.

**Create File Collaboration Job Wizard**

**Participants**  
Create a Collaboration job with automatic failover and failback of linked DFS folder targets.

**Participants**  
File Metadata  
Application Support  
Email Alerts

Host	Root Path	Enabled	Storage Platform	DFS-N Folder Target	Seeding Target
DGWin16B	C:\Farming	Yes	Windows	\\DGWin16B\Farming	Yes
DGWin16C	C:\Farming	Yes	Windows	\\DGWin16C\Farming	No

Auto Match Root  
Edit Detector Settings  
Delete  
Add

< Back   Next >   Finish   Cancel

14. Once all participants are added and associated with folder targets, click **Next**.
15. (Optional) In the **File Metadata** page, [enable file metadata replication](#), and then click **Next**.

**Create File Collaboration Job Wizard**

**File Metadata**  
Configure the replication of NTFS security permissions.

**Participants**  
**File Metadata**  
 Application Support  
 Email Alerts

**Synchronize Security Descriptors (ACLs)**  
☐ Enable synchronizing NTFS security descriptors (ACLs) in real-time  
☐ Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan

**Synchronize Security Descriptor Options**  
☒ Owner  
☒ DACL: Discretionary Access Control List  
☐ SACL: System Access Control List

**Metadata Conflict Resolution**  
 Select Master Host for initial scan:

< Back   Next >   **Finish**   Cancel

16. (Optional) In the **Application Support** page, [select the applications you want optimized](#), and then click **Next**.

**Create File Collaboration Job Wizard**

**Application Support**  
Select the applications that will be used with the data that is managed by this job.

**Participants**  
 File Metadata  
**Application Support**  
 Email Alerts

Select below to optimize this job for any of the following file types:

**Adobe Products**  
☐ Adobe Illustrator   ☐ Adobe Photoshop  
☐ Adobe InDesign

**Autodesk Products**  
☐ Autodesk AutoCAD   ☐ Autodesk Revit  
☐ Autodesk Civil 3D   ☐ Autodesk Sheet Set Manager (for AutoCAD or Civil 3D)  
☐ Autodesk Inventor

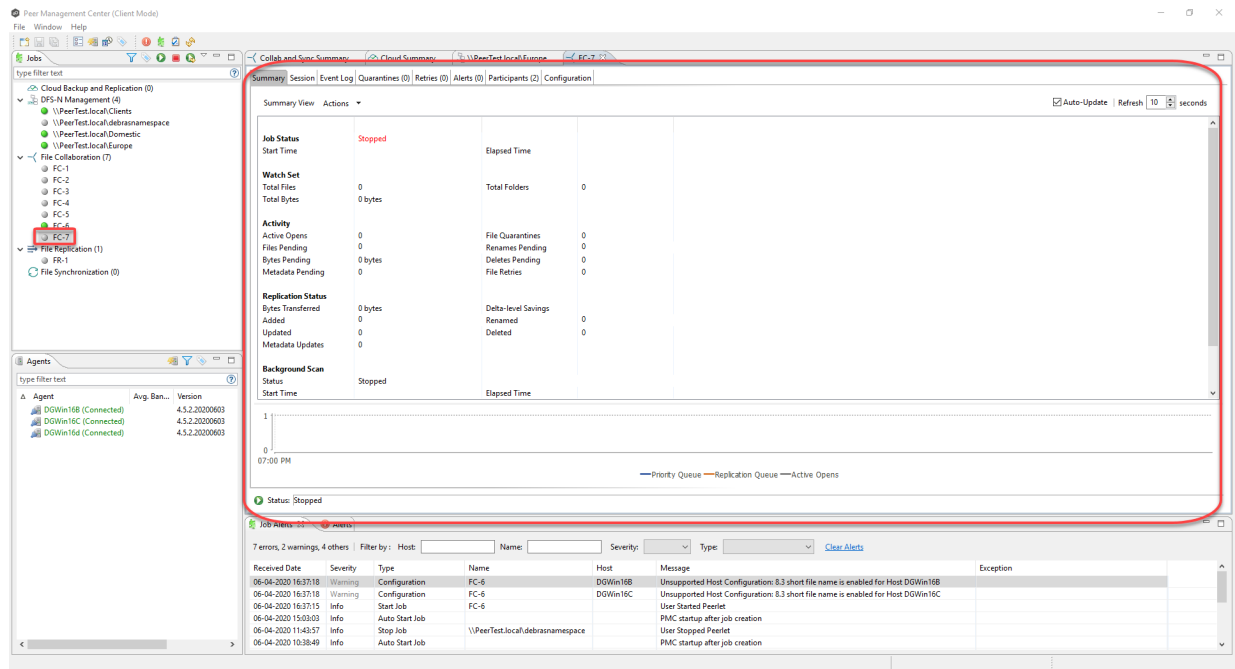
**Other**  
☐ ArcGIS   ☐ Microsystems Allegro  
☐ Dassault Systems CATIA   ☐ Newforma Project Center  
☐ Microsoft Office   ☐ Rhinoceros Rhino3D

< Back   Next >   **Finish**   Cancel

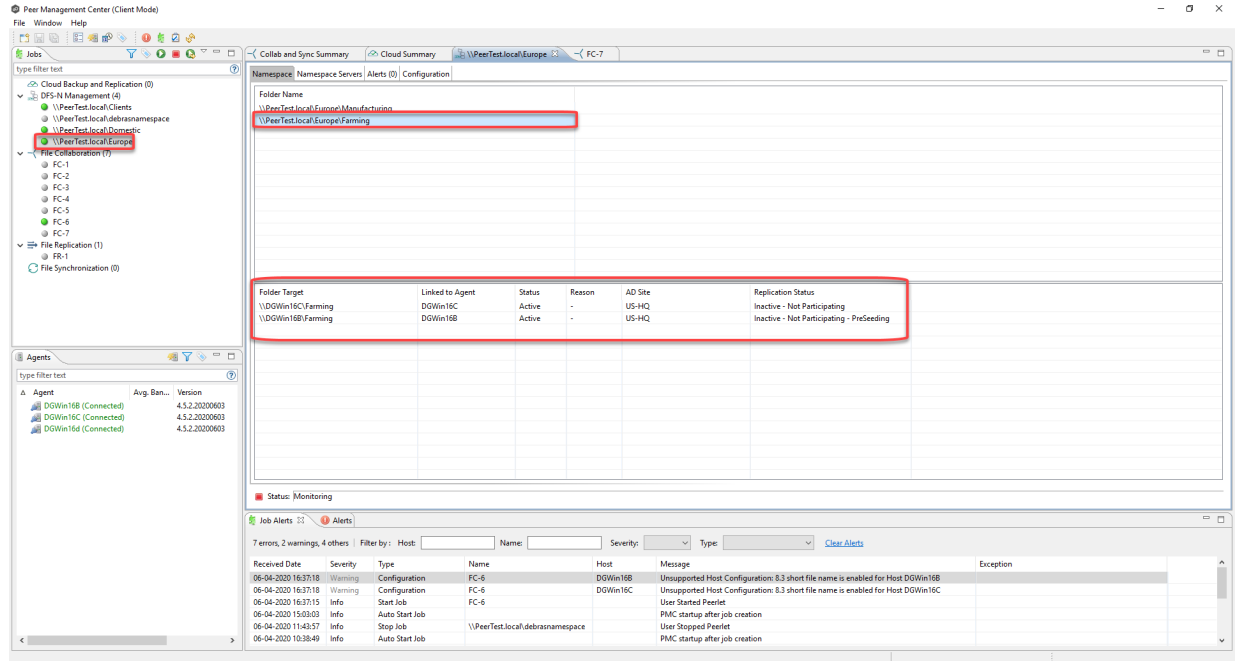
17. (Optional) In the **Email Alerts** page, [select the emails alerts](#) to apply to the job.

18. Click **Finish** to complete the creation of this job.

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.



If you open the linked DFS-N Management job, and click the namespace folder in the Namespace tab, you can view the folder targets in the view below.



## Linking a Namespace Folder with an Existing File Collaboration or File Synchronization Job

You can link a DFS namespace with an existing File Collaboration or File Synchronization job. These steps require that the DFS namespace has been already created and is being managed by a DFS-N Management job. If your desired namespace does not exist, you need to either [create](#) it (via the [Create DFS-N Management Job wizard](#)) or you can [import an existing namespace](#) into Peer Management Center.

To link a namespace folder with an existing File Collaboration or File Synchronization job:

1. Select the File Collaboration or File Synchronization job in the **Jobs** view.
2. Right-click and select **Edit Job**.

The **Edit Job** wizard appears.

The screenshot shows the 'Edit File Collaboration Job' wizard with the 'Participants' tab selected. The left navigation pane lists various settings: Participants, General, File Filters, Conflict Resolution, Delta Replication, File Metadata, File Locking, Application Support, Logging and Alerts, Target Protection, Email Alerts, SNMP Notifications, Tags, and DFS-N. The main area is divided into 'Available' and 'Selected' sections. The 'Available' section has a table with columns 'Host' and 'Computer Description', containing one entry: DGWin16d. Below this table are buttons for 'Add', 'Edit Detector Settings', and 'Delete'. The 'Selected' section has a table with columns: Host, Computer Description, Directory, Enabled, Storage Platform, and Seeding Target. It contains two entries: DGWin16B and DGWin16C, both pointing to 'C:\Terra Firma' with 'Enabled' set to 'Yes' and 'Storage Platform' set to 'Windows'. At the bottom right are 'OK' and 'Cancel' buttons.

Host	Computer Description
DGWin16d	

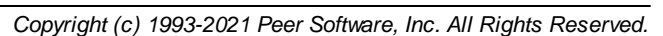
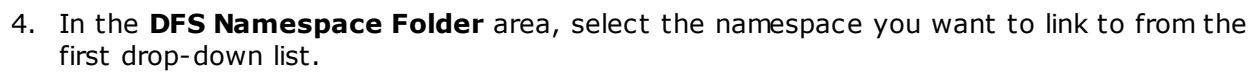
Add Edit Detector Settings Delete

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGWin16B		C:\Terra Firma	Yes	Windows	No
DGWin16C		C:\Terra Firma	Yes	Windows	No

OK Cancel

3. Select **DFS-N** in the navigation tree.

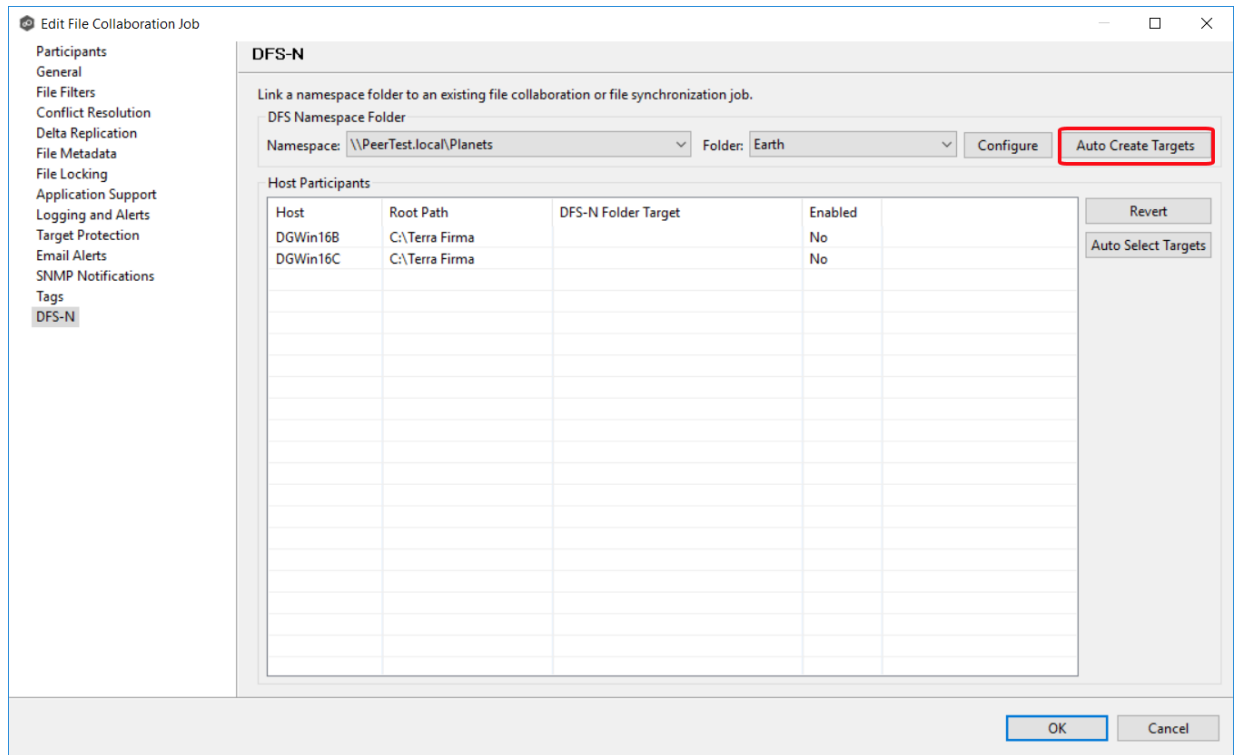
The DFS-N page is displayed.



5. Select the namespace folder from **Folder**.

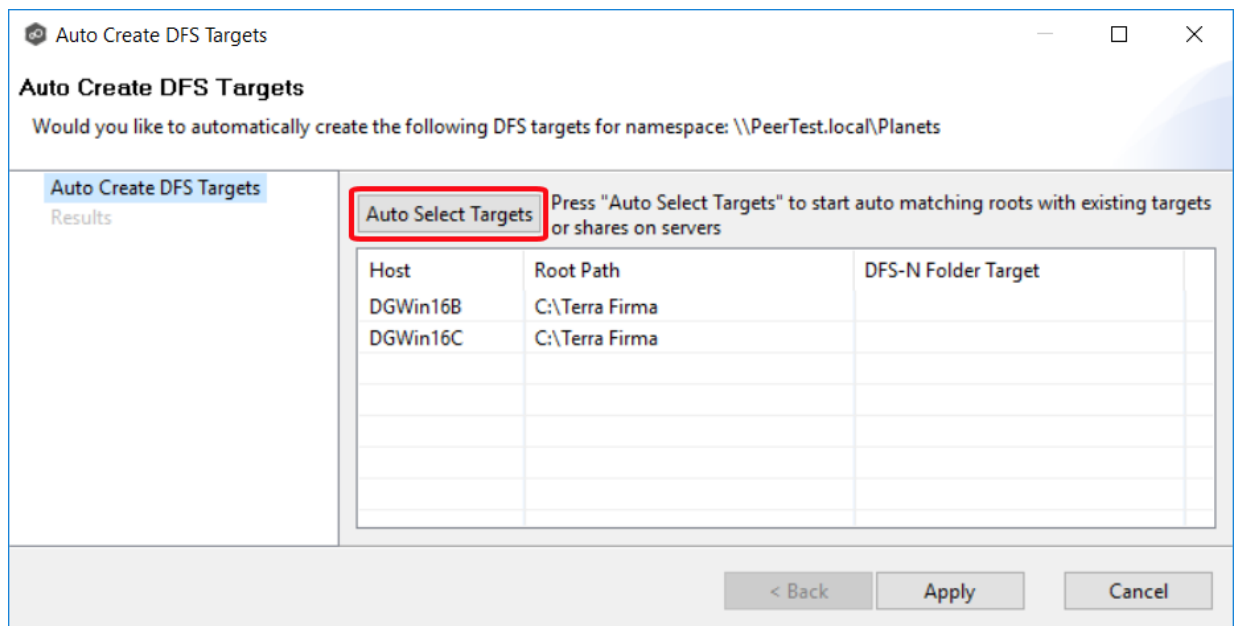
[illegible]

6. If your selected folder does not have the appropriate folder targets, click the **Auto Create Targets** button.



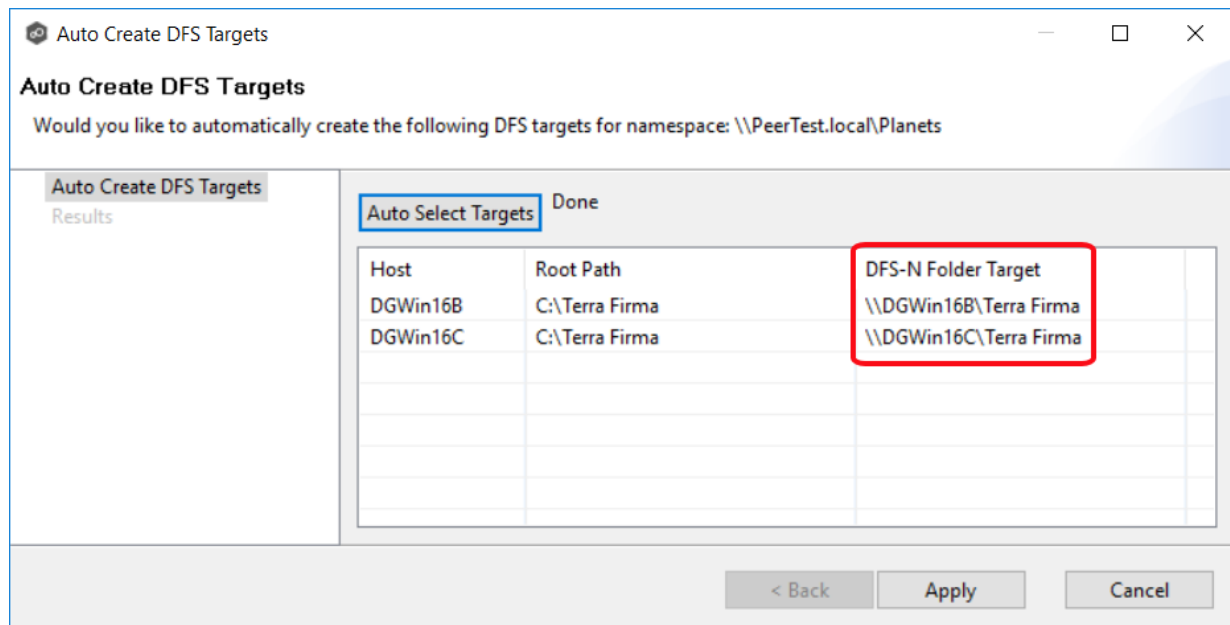
The wizard that appears will use the paths configured in your File Collaboration or File Synchronization job and try to automatically create folder targets for you.

7. Click **Auto Select Targets**.



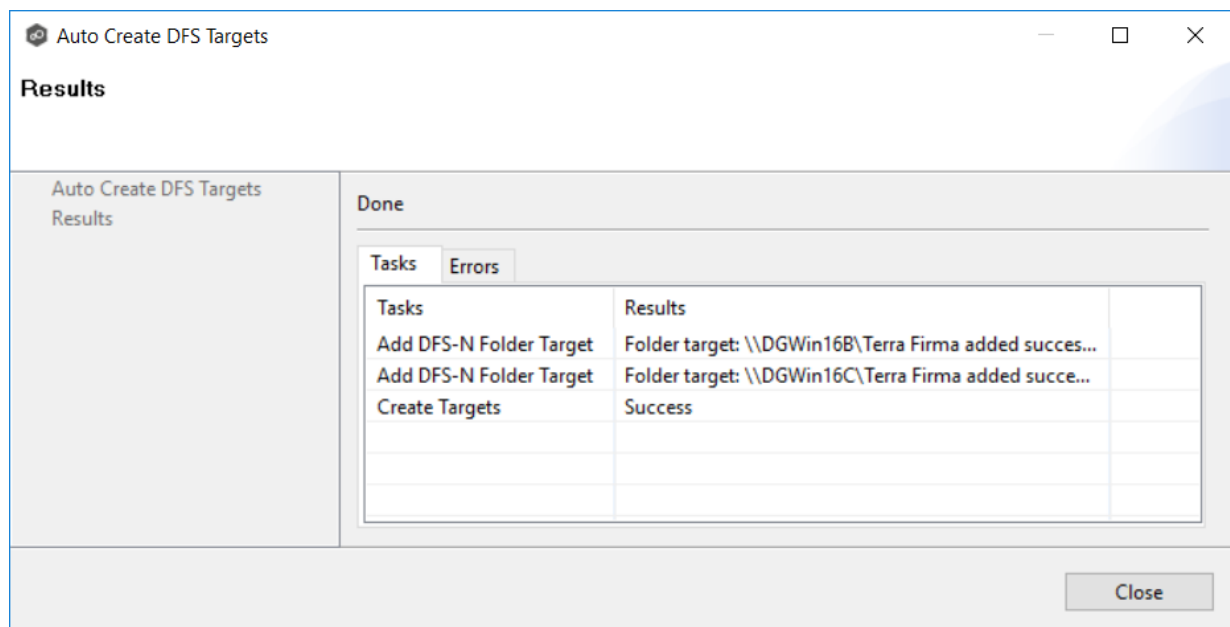
The matched folder targets are listed in the table.





- Click **Apply**.

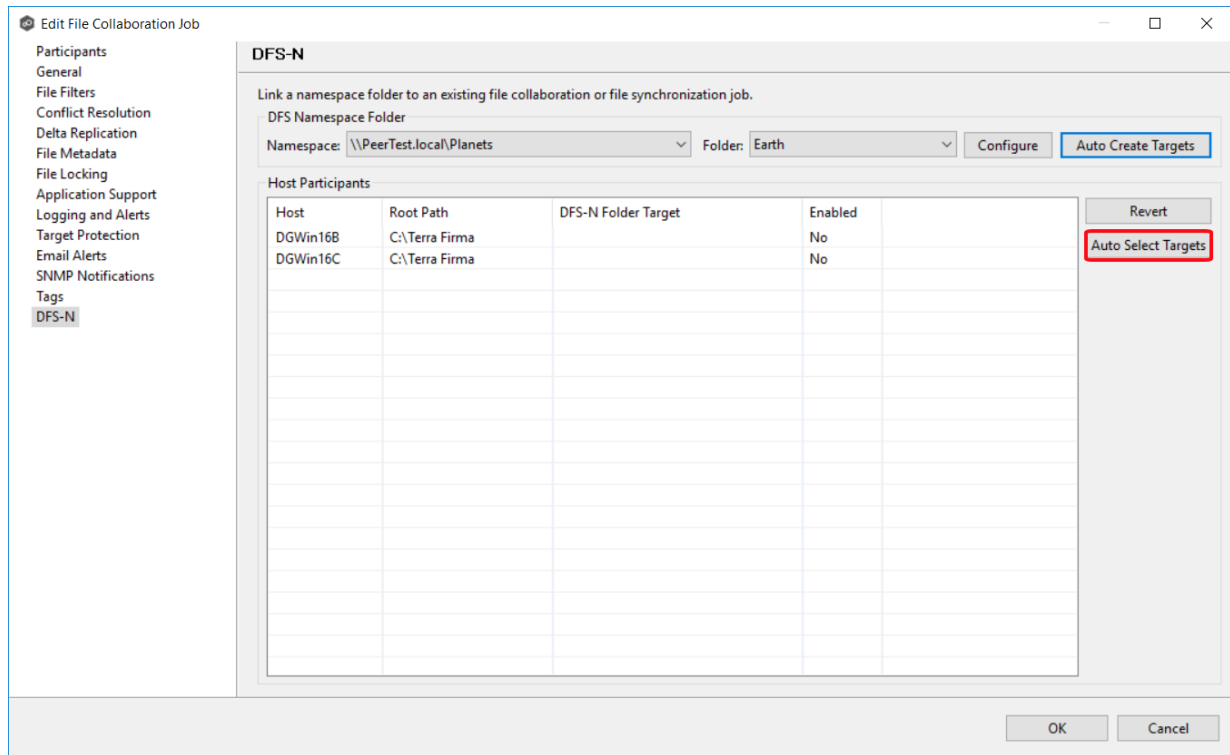
The **Results** page appears.



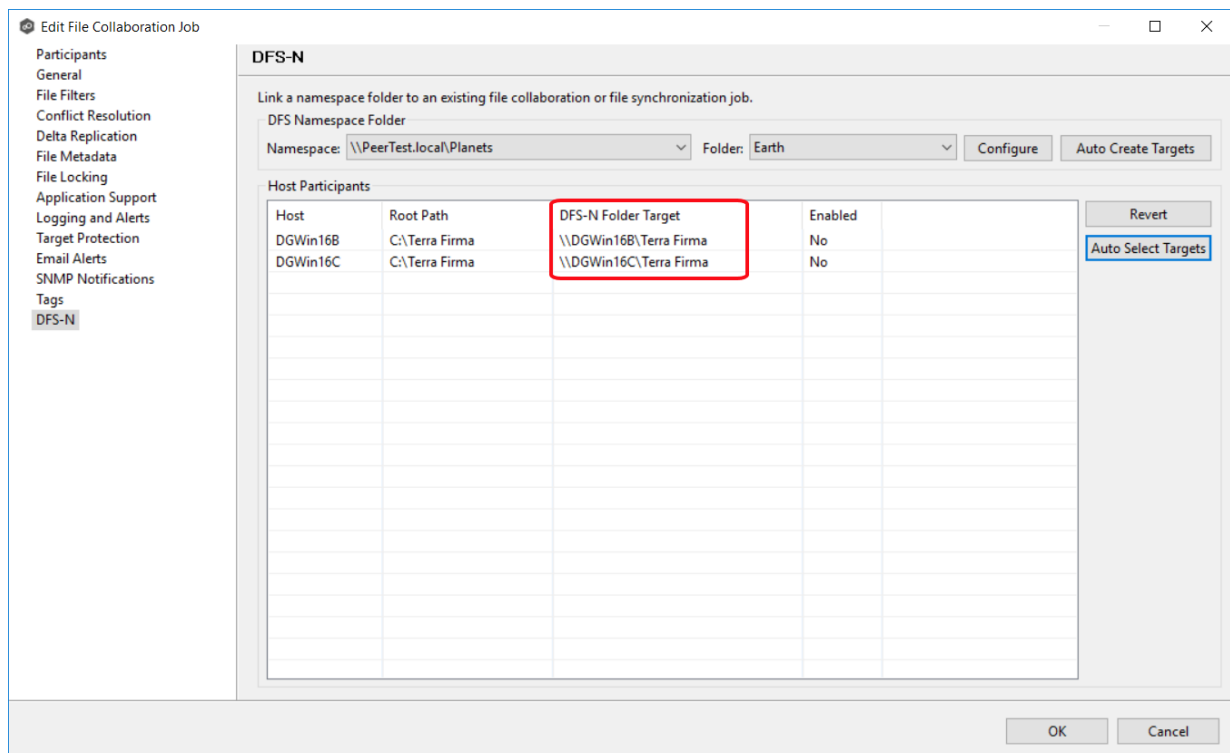
- Click **Close**.

Once you've selected a namespace and a folder, you need to assign a target to each participant in the collaboration or synchronization job.

- Click **Auto Select Targets**.



In most scenarios, clicking the **Auto Select Targets** button will be able to automatically link a folder target with the appropriate participant.



11. If **No** appears in the **Enabled** column, select **Yes** from the drop-down list.

The screenshot shows the "Edit File Collaboration Job" window. On the left is a sidebar menu with options like Participants, General, File Filters, Conflict Resolution, Delta Replication, File Metadata, File Locking, Application Support, Logging and Alerts, Target Protection, Email Alerts, SNMP Notifications, Tags, and DFS-N. The main area is titled "DFS-N" and contains instructions to link a namespace folder to an existing file collaboration or synchronization job.

Below the instructions, there are two dropdown menus: "Namespace:" set to "\\PeerTest.local\Planets" and "Folder:" set to "Earth". To their right are "Configure" and "Auto Create Targets" buttons.

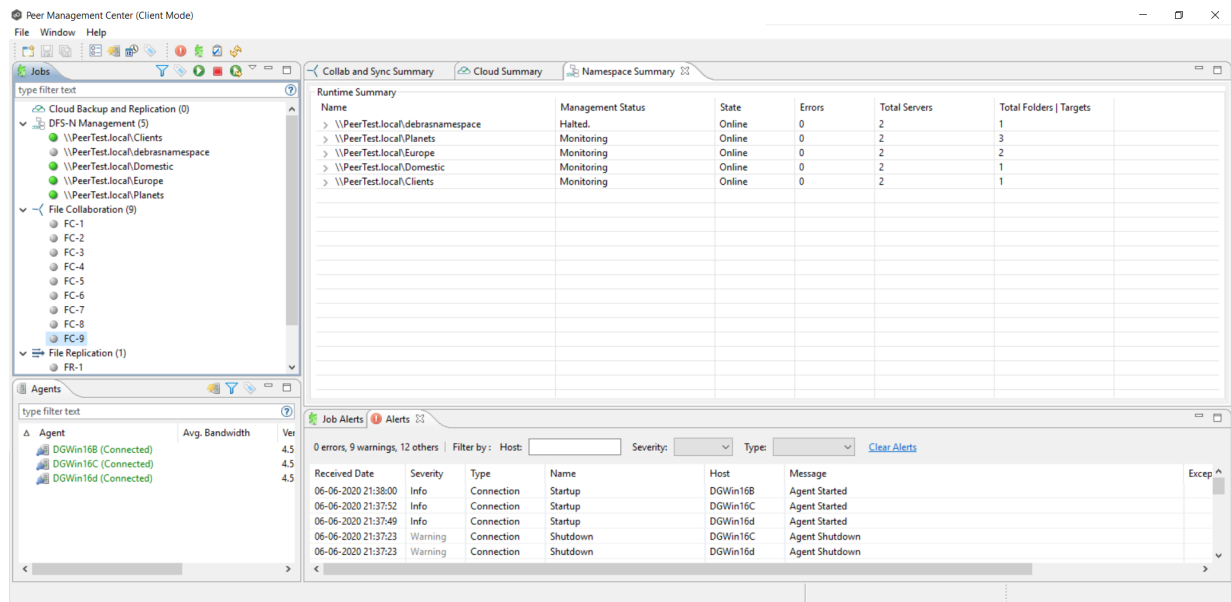
A section labeled "Host Participants" features a table with four columns: Host, Root Path, DFS-N Folder Target, and Enabled. Two rows are visible:

Host	Root Path	DFS-N Folder Target	Enabled
DGWin16B	C:\Terra Firma	\\DGWin16B\Terra Firma	Yes
DGWin16C	C:\Terra Firma	\\DGWin16C\Terra Firma	Yes

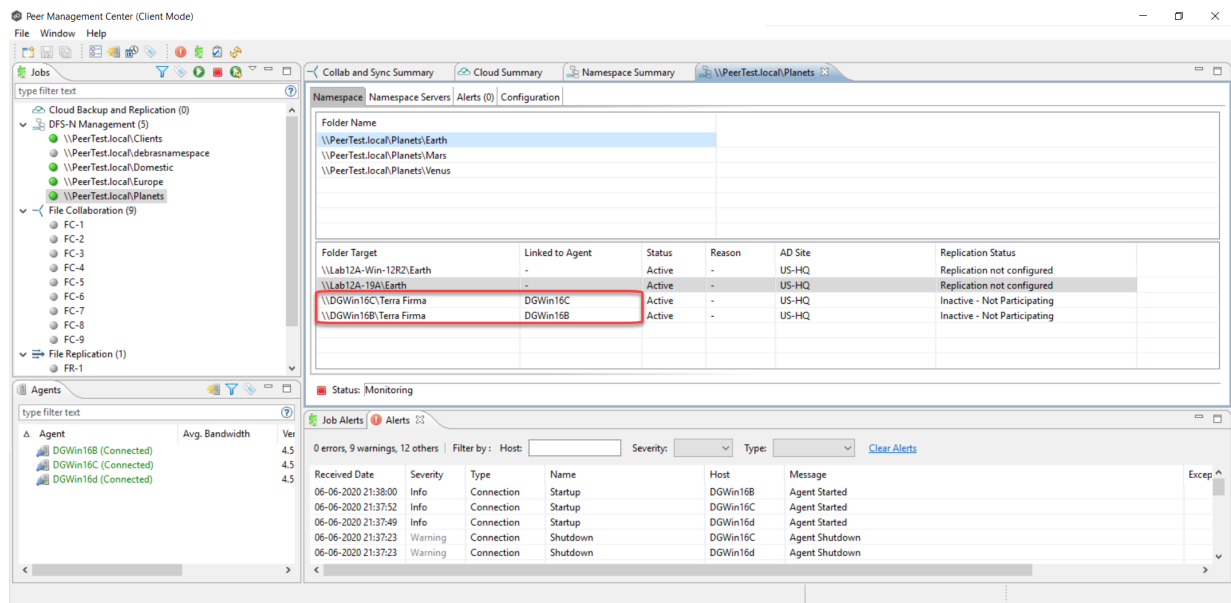
To the right of the table are "Revert" and "Auto Select Targets" buttons. At the bottom right of the window are "OK" and "Cancel" buttons.

12. Once all participants are linked to the appropriate folder targets, click **OK** to save your changes.

From this point forward, if this collaboration or synchronization job is running along with its paired DFS-N Management job, Peer Management Center will automatically [failover and failback](#) folder targets.



13. To confirm that the namespace is linked to the file collaboration or file synchronization job, open the namespace job, select the folder name, and confirm that the appropriate folder targets are linked to Agents.



## File Collaboration Jobs

This section provides information about creating, editing, running, and managing a File Collaboration job:

- [Overview](#)
- [Before You Create Your First File Collaboration Job](#)
- [Creating a File Collaboration Job](#)
- [Editing a File Collaboration Job](#)
- [Running and Managing a File Collaboration Job](#)
- [Runtime Job Views](#)

### Overview

A File Collaboration job provides distributed teams a fast and efficient way to collaborate with shared project files. Unlike other file collaboration solutions that centralize files into a single data repository that cause slow file access across a WAN, a File Collaboration job replicates shared project files to each office site in a distributed environment so that end users are guaranteed high-speed LAN access to shared files no matter their file size. Version conflicts are prevented through integrated distributed file locking.

By keeping hot data local, File Collaboration maximizes end user productivity. Because files are close to the users, their applications, and their compute resources, the actual performance is as fast as possible from a physical view. At the same time File Collaboration ensures version conflicts are eliminated with file locking.

### Before You Create Your First File Collaboration Job

We strongly recommend that you configure the File Collaboration settings (e.g. SMTP notifications), as well as other [global settings](#) such as SMTP email settings, email alerts, and file filters before configuring your first File Collaboration job. See [Preferences](#) for details on these settings.

## Creating a File Collaboration Job

The Create Job wizard walks you through the process of creating a File Collaboration job. The process consists of the following steps:

[Step 1: Job Type and Name](#)

[Step 2: Participants](#)

[Step 3: File Metadata](#)

[Step 4: Application Support](#)

[Step 5: Email Alerts](#)

[Step 6: Save Job](#)

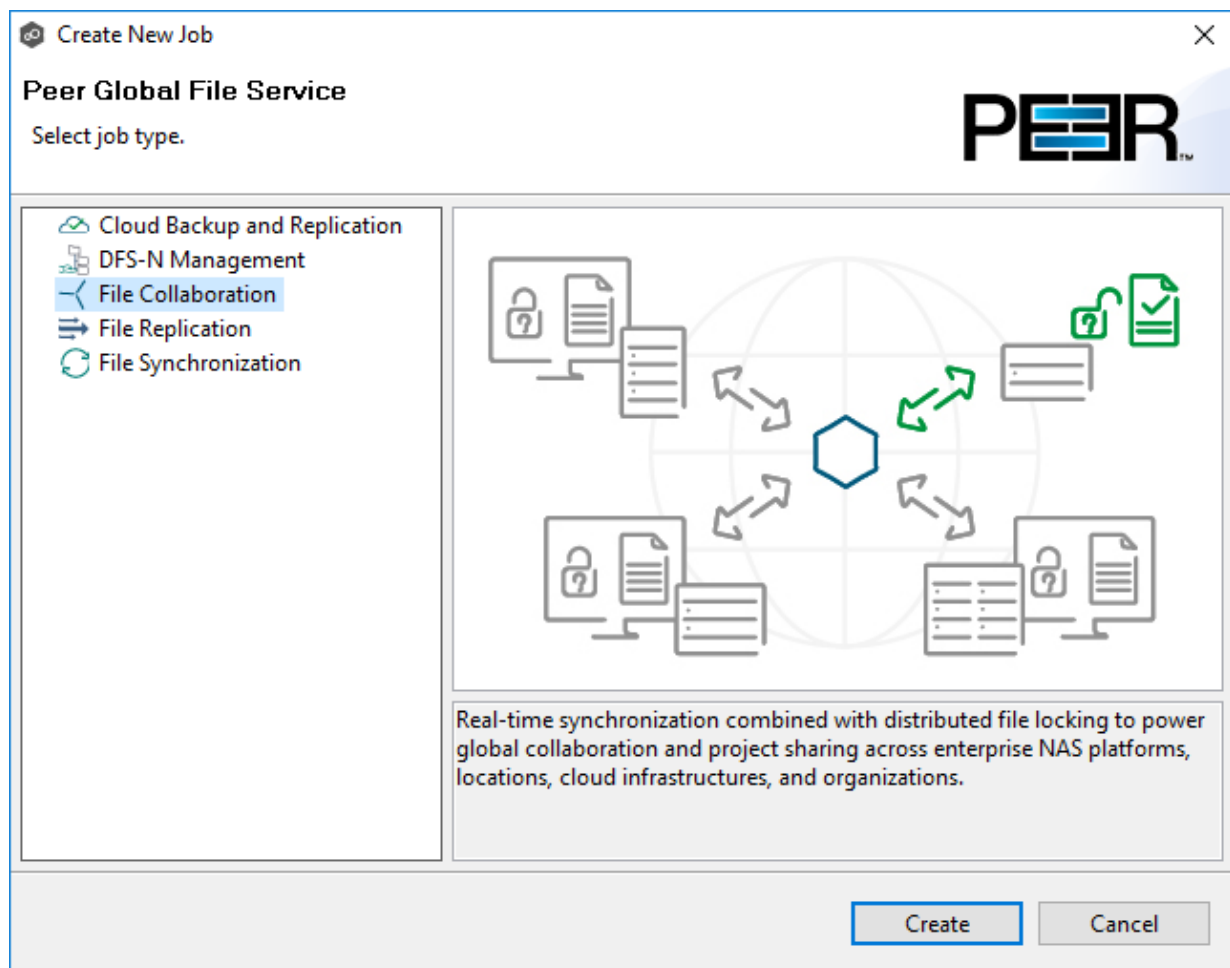
Additional configuration options, such as applying [file filters](#) and specifying [delta level replication](#), are available when [editing a File Collaboration job](#).

### Step 1: Job Type and Name

1. Open Peer Management Center.
2. From the **File** menu, select **New Job** (or click the **New Job** button on the toolbar).

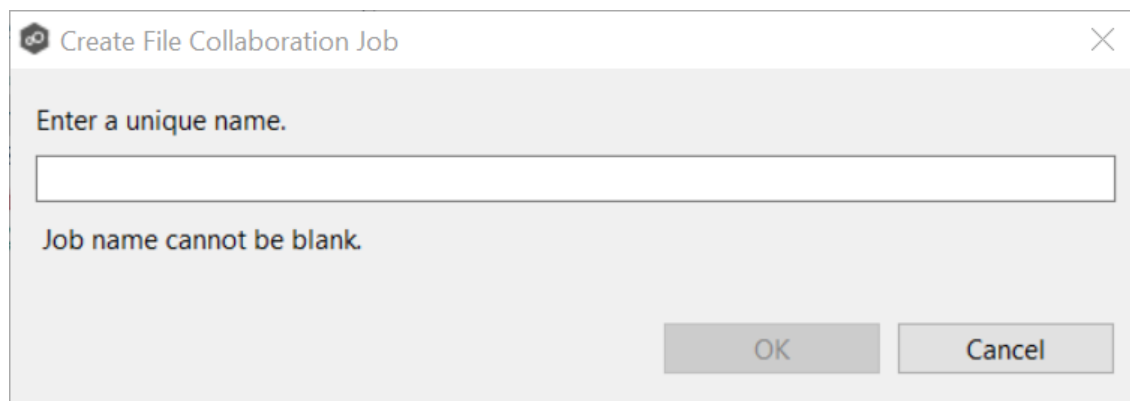
The **Create New Job** wizard displays a list of job types you can create.

3. Click **File Collaboration**, and then click **Create**.



4. Enter a name for the job.

The job name must be unique.



5. Click **OK**.

The [Participants](#) page appears.

## Step 2: Participants

A File Collaboration job must have two or more participants. A [participant](#) consists of an Agent and the volume/share/folder to be replicated. The server that the Agent is installed upon is called the [host](#) (or [host participant](#)). A File Collaboration job replicates the files of participants in real-time.

1. Complete the five substeps:

[Participants](#)

[Storage Platform](#)

[Management Agent](#)

[Storage Information](#)

[Path](#)

After you add a participant, it appears in the **Participants** table.

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\SVM9X-1\kent...	Yes	NetApp cDOT	No
DGAgent2		\\AFS2\Share2\...	Yes	Nutanix Files	No

2. Repeat the five substeps for each participant you want to add to the job.
3. Once you have added all the participants, click **Next** to specify [file metadata](#) for the job. (Don't click **Finish**.)



To begin the process of adding a participant:

- Create File Collaboration Job Wizard

Participants

Add two or more participants to this File Collaboration job.

Participants

File Metadata

Application Support

Email Alerts

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target	

Add

Edit

Delete

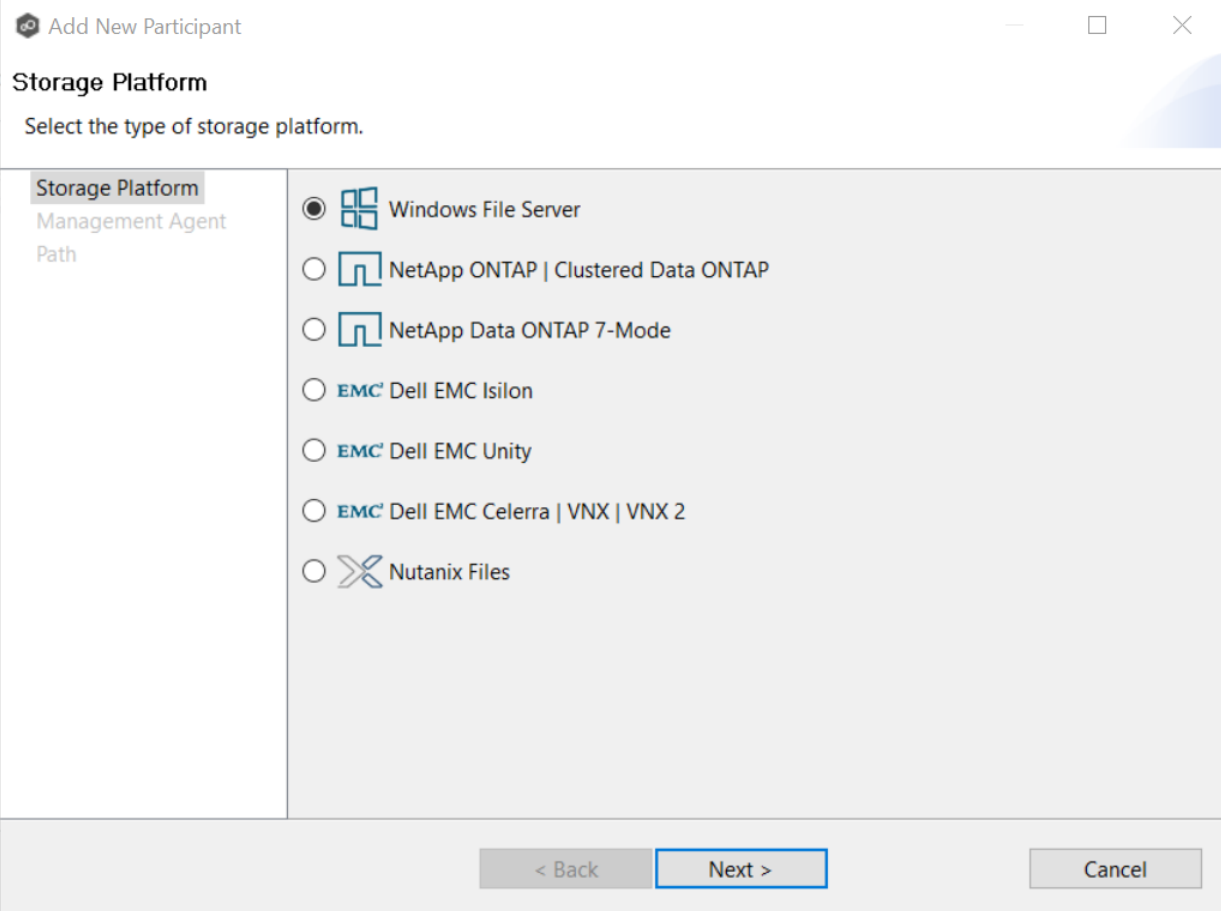
< Back

Next >

Cancel

The **Storage Platform** page lists the types of storage platforms that File Collaboration supports. A storage device hosts data you want to collaborate on. It is often referred to as the [host or host participant](#).

- Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.



The screenshot shows a window titled "Add New Participant" with a close button in the top right corner. Below the title bar, the text "Storage Platform" is displayed, followed by the instruction "Select the type of storage platform." The main area of the window is divided into two sections. On the left, there is a sidebar with the following labels: "Storage Platform" (highlighted), "Management Agent", and "Path". On the right, there is a list of storage platform options, each with a radio button and an icon:

- ☒ Windows File Server (icon: four squares in a 2x2 grid)
- ☐ NetApp ONTAP | Clustered Data ONTAP (icon: stylized 'N' shape)
- ☐ NetApp Data ONTAP 7-Mode (icon: stylized 'N' shape)
- ☐ EMC Dell EMC Isilon (icon: stylized 'E' shape)
- ☐ EMC Dell EMC Unity (icon: stylized 'E' shape)
- ☐ EMC Dell EMC Celerra | VNX | VNX 2 (icon: stylized 'E' shape)
- ☐ Nutanix Files (icon: stylized 'X' shape)

At the bottom of the window, there are three buttons: "< Back" (disabled), "Next >" (active/highlighted), and "Cancel" (disabled).

2. Click **Next**.

The [Management Agent](#) page is displayed.

The **Management Agent** page lists available [Agents](#). You can have more than one Agent managing a storage device—however, the Agents must be managing different volumes/shares/folders on the storage device. For your File Collaboration job, you should select the [Management Agent](#) that manages the volumes/shares/folders you want to replicate in this job.

1. Select the Agent that manages the host.

[illegible]

**Tip:** If the Agent you want is not listed, try restarting the Peer Agent Windows Service on that host. If it successfully connects to the Peer Management Broker, then the list is updated with that Agent.

2. Click **Next**.

The [Storage Information](#) page is displayed if you selected any storage platform other than Windows. If you selected Windows, skip to the [Path](#) page.

If you selected any storage platform type other than Windows File Server in [Storage Platform](#) page, the **Storage Information** page appears. It requests the credentials necessary to connect to the storage device you want to replicate. If you selected Windows Files Server in the previous wizard page, skip to [Step 3: File Metadata](#).

1. Select **New Credentials** or **Existing Credentials**.
2. If you selected **Existing Credentials**, select a credential from the drop-down list, and then click **Next** to continue to the [Path](#) page.

If you selected **New Credentials**, enter the credentials for connecting to the storage device. The information you are prompted to enter varies, depending on the type of storage platform:

[NetApp ONTAP | Clustered Data ONTAP](#)

[NetApp Data ONTAP 7-Mode](#)

[Dell EMC Isilon](#)

[Dell EMC Unity](#)

[Dell EMC Celerra | VNX | VNX 2](#)

[Nutanix Files](#)

3. Click **Validate** to test the credentials.

After the credentials are validated, a success message appears.

4. Click **Next**.

The [Path](#) page is displayed.

#### NetApp ONTAP | Clustered Data ONTAP

1. Enter the credentials to connect to the Storage Virtual Machine hosting the data to be replicated or select existing credentials.

Add New Participant

**Storage Information**  
Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

**Credentials**  
☒ New Credentials

\*SVM Name:   
\*SVM User Name:   
\*SVM Password:   
SVM Management IP:   
\*Peer Agent IP:

☐ Existing Credentials  
SVM9X-1, user:vsadmin

Validate

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp ONTAP/cDOT environments.

Advanced

< Back
Next >
Cancel

<b>SVM Name</b>	Enter the name of the Storage Virtual Machine hosting the data to be replicated.
<b>SVM Username</b>	Enter the user name for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Password</b>	Enter the password for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Management IP</b>	Enter the IP address used to access the management API of the NetApp Storage Virtual Machine. If the data LIFs (Logical Interfaces) corresponding to the SVM Name above already allow management access, this field is not required.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Storage Virtual Machine. The Storage Virtual Machine must be able to route

traffic to this IP address. If the IP address you want does not appear, manually enter the address.

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

### NetApp Data ONTAP 7-Mode

1. Enter the credentials to connect to the NetApp 7-Mode filer or vFiler hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Add New Participant" with standard window controls (minimize, maximize, close). The "Storage Information" tab is selected in the left-hand navigation pane, which also lists "Storage Platform", "Management Agent", and "Path". The main content area of the dialog has the heading "Storage Information" and the instruction "Enter the information required to connect to the storage device." Below this, there are two radio button options under the "Credentials" section: "New Credentials" (which is selected) and "Existing Credentials". The "New Credentials" option includes a text field labeled "\*Filer Name:" and an "Advanced" button to its right. Below the "Existing Credentials" option is a dropdown menu. At the bottom left of the main content area is a "Validate" button. At the very bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel". A footer note at the bottom of the main content area reads: "Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp 7-Mode environments."

<b>Filer Name</b>	Enter the name of the NetApp 7-Mode filer or vFiler hosting the data to be replicated.
-------------------	--

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Dell EMC Isilon

1. Enter the credentials to connect the EMC Isilon cluster hosting the data to be replicated or select existing credentials.

**Add New Participant**

**Storage Information**  
Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

**Credentials**  
☒ New Credentials  
\*Cluster Name:   
\*Cluster Username:   
\*Cluster Password:   
Cluster Management IP:   
Nodes:

☐ Existing Credentials

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Isilon environments.

<b>Cluster Name</b>	Enter the name of the EMC Isilon cluster hosting the data to be replicated.
<b>Cluster Username</b>	Enter the user name for the account managing the EMC Isilon cluster.
<b>Cluster Password</b>	Enter the password for account managing the EMC Isilon cluster.
<b>Cluster Management IP</b>	Enter the IP address of the system used to manage the EMC Isilon cluster. Required only if multiple Access Zones are in use on the cluster.
<b>Nodes</b>	Enter one IP from each node in the Isilon cluster that the Agent can access to perform open file lookups. Use commas to separate nodes.

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Dell EMC Unity

1. Enter the credentials to connect to the NAS Server hosting the data to be replicated or select existing credentials.



Add New Participant

Storage Platform Management Agent

Storage Information

Path

Credentials

☒ New Credentials

\*CIFS Server Name:

\*Unisphere Username:

\*Unisphere Password:

\*Unisphere Management IP:

Advanced

☐ Existing Credentials

Validate

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Unity environments.

< Back

Next >

Cancel

<b>CIFS Server Name</b>	Enter the name of the NAS server hosting the data to be replicated.
<b>Unisphere Username</b>	Enter the user name for the Unisphere account managing the Unity storage device.
<b>Unisphere Password</b>	Enter the password for the Unisphere account managing the Unity storage device.
<b>Unisphere Management IP</b>	Enter the IP address of the Unisphere system used to manage the Unity storage device. This should not point to the NAS server.

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Dell EMC Celerra | VNX | VNX 2

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.

**Add New Participant**

**Storage Information**  
Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

**Credentials**

☒ New Credentials

\*CIFS Server Name:

\*Control Station Username:

\*Control Station Password:

\*Control Station IP:

☐ Existing Credentials

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC VNX/Celerra environments.

#### CIFS Server Name

Enter the name of the CIFS Server hosting the data to be replicated.

<b>Control Station Username</b>	Enter the user name for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station Password</b>	Enter the password for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station IP</b>	Enter the IP address of the Control Station system used to manage the Celerra/VNX storage device. This should not point to the CIFS Server.

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Nutanix Files

1. Enter the credentials to connect to the Nutanix Files cluster hosting the data to be replicated or select existing credentials.

Add New Participant

**Storage Information**  
Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

**Credentials**  
☒ New Credentials

\*Nutanix File Server Name:   
\*Username:   
\*Password:   
\*Peer Agent IP:

☐ Existing Credentials  
AFS2, user:admin

Validate

Having trouble connecting? Please verify that all [prerequisites](#) are met for Nutanix Files environments.

Advanced

< Back
Next >
Cancel

<b>Nutanix File Server Name</b>	Enter the name of the Nutanix Files cluster hosting the data to be replicated.
<b>Username</b>	Enter the user name for the account managing the Nutanix Files cluster via its management APIs.
<b>Password</b>	Enter the password for the account managing the Nutanix Files cluster via its management APIs.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Nutanix Files cluster. The Files cluster must be able to route traffic to this IP address. If the IP address you want does not appear, manually enter the address. This should not point to the Files cluster itself.

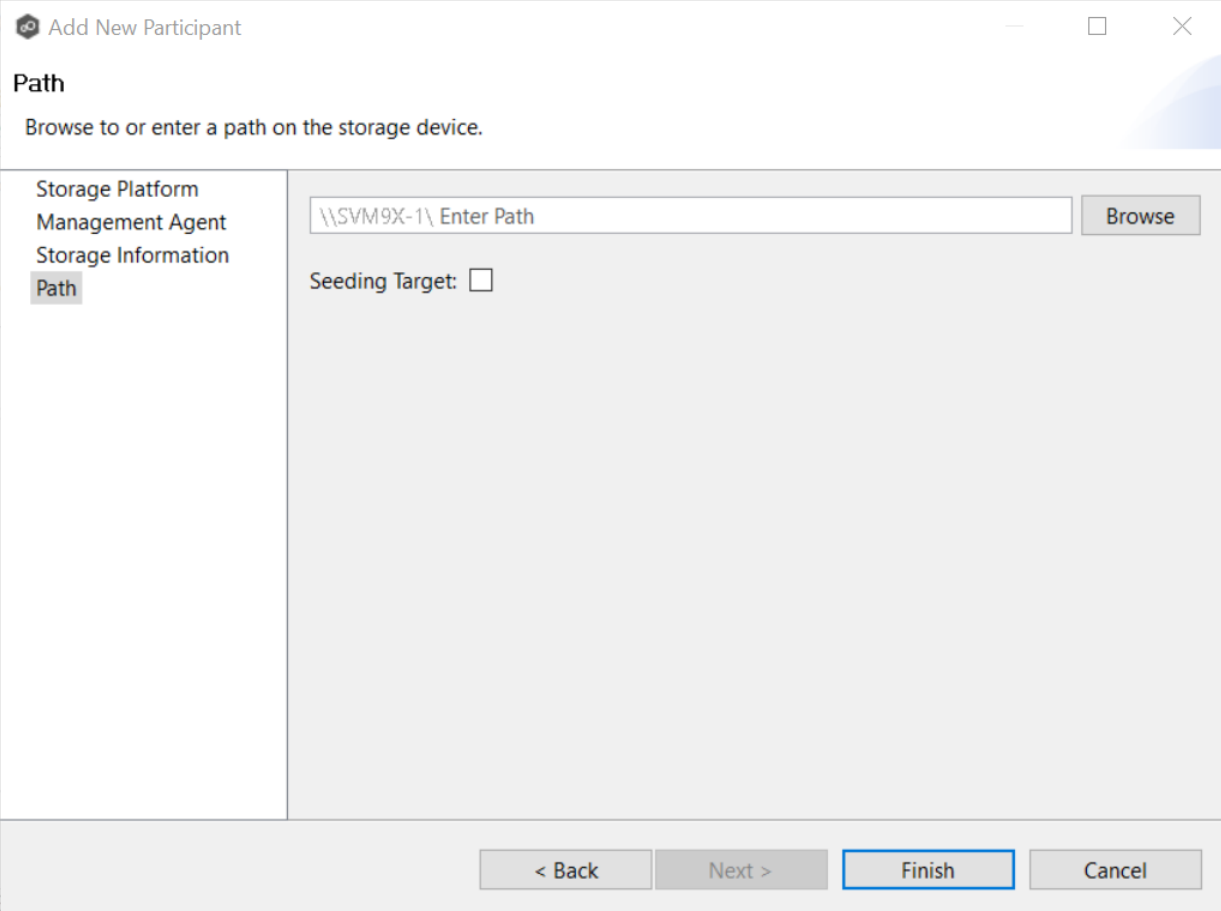
2. Click **Validate**.

3. Click **Next**.

The [Path](#) page is displayed.

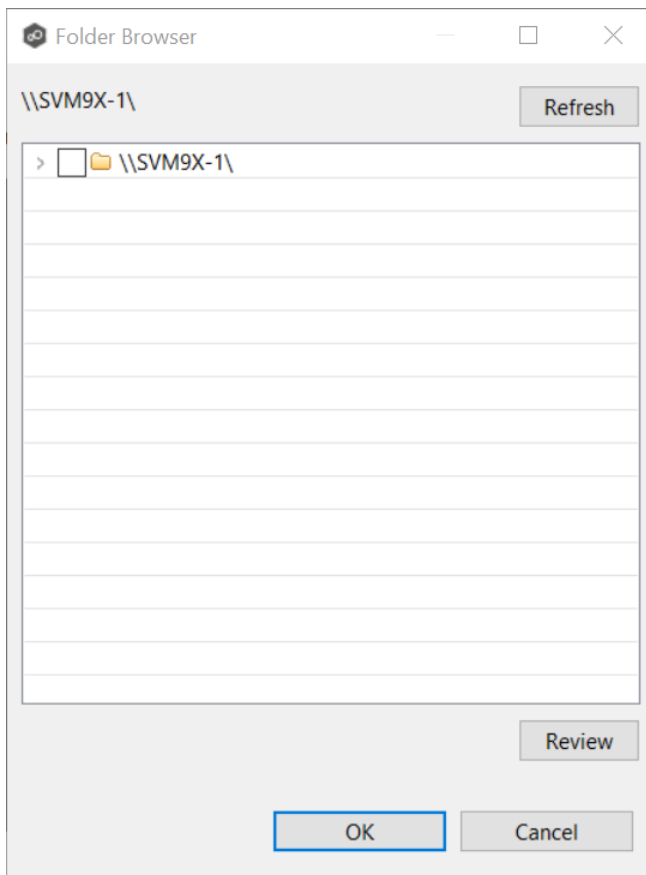
The **Path** page is where you specify the path to the volume/share/folder you want to replicate. This volume/share/folder is referred to as the [watch set](#). The watch set can contain a single volume/share/folder. If you want to replicate multiple volumes/shares/folders, you need to create a separate job for each one.

1. Browse to or enter the path to the watch set.



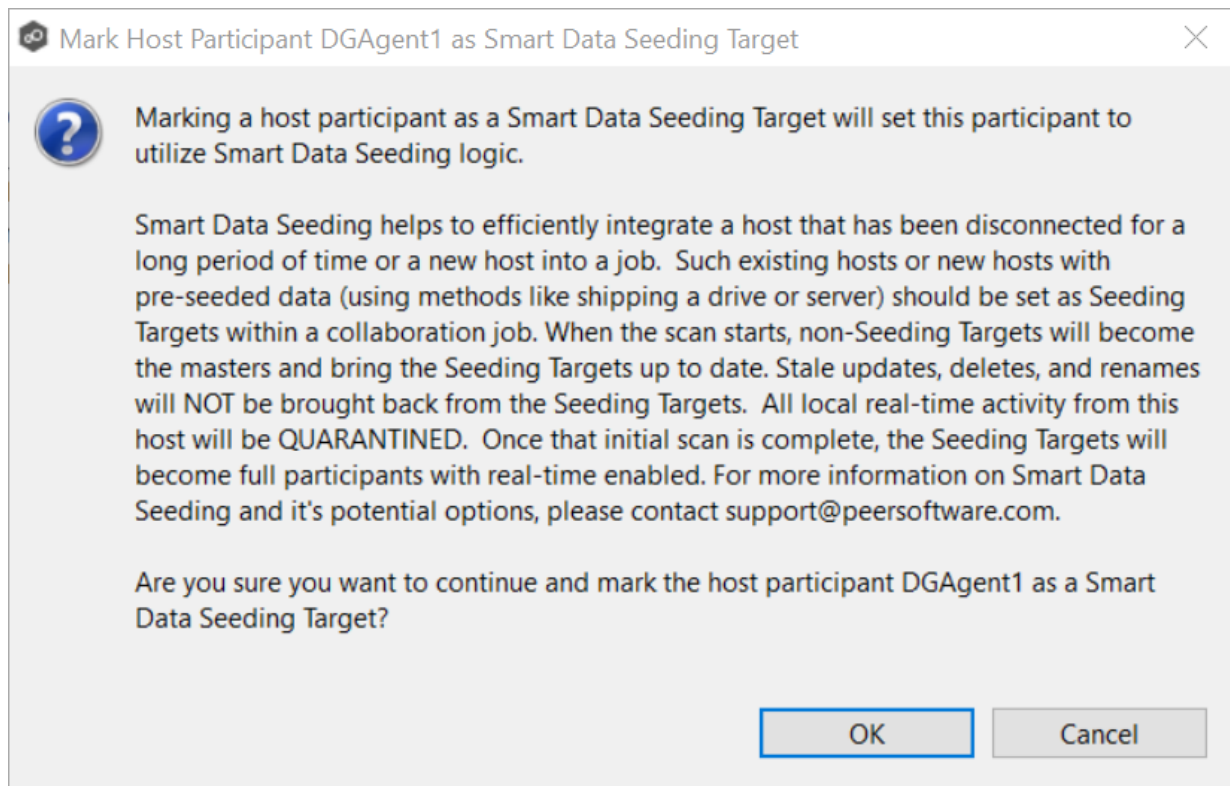
The screenshot shows a window titled "Add New Participant" with standard Windows window controls (minimize, maximize, close). The window has a sidebar on the left with the following items: "Storage Platform", "Management Agent", "Storage Information", and "Path" (which is highlighted). The main area of the window is titled "Path" and contains the instruction "Browse to or enter a path on the storage device." Below this instruction, there is a text input field containing the placeholder text "\\SVM9X-1\ Enter Path". To the right of the input field is a "Browse" button. Below the input field, there is a "Seeding Target:" label followed by an unchecked checkbox. At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish" (which is highlighted with a blue border), and "Cancel".

If you selected **Browse**, the **Folder Browser** dialog appears:



- a. Expand the folder tree.
  - b. Select the appropriate volume/share/folder.
  - c. (Optional) Click the **Review** button to see your selection.
  - d. Click **OK**.
2. (Optional) Select the **Seeding Target** checkbox, and then click **OK** in the dialog that appears.

If you select this option, a message describing seeding behavior is displayed. Multiple participants in a File Collaboration job can be set as smart data seeding targets; however, at least one participant should not be set as a smart data seeding target. This participant will be acting as the "master" source for the smart data seeding targets. For more information about smart data seeding, see [Smart Data Seeding](#) or contact [support@peersoftware.com](mailto:support@peersoftware.com).



3. Click **Finish** to complete the wizard for this participant.
4. Return to [Step 2: Participants](#) to add more participants, if applicable. A File Collaboration job must have at least two participants. If you have added all the participants, continue with [Step 3: File Metadata](#).

### Step 3: File Metadata

This step is optional.

The **File Metadata** page allows you to specify whether you want to synchronize NTFS security permissions metadata and the types of metadata. It also allows you to specify which volume/share/folder's metadata should be used if there is a conflict during the initial synchronization. The volume/share/folder used if there is a conflict is referred to as the [master host](#).

For more information on synchronizing NTFS metadata, see [File Metadata Synchronization](#) in the [Advanced Topics](#) section.

To enable file metadata synchronization:

1. Select when you want the metadata synchronized (you can select one or both options):
  - **Enable synchronizing NTFS security descriptors (ACLs) in real-time** - Select this option if you want the metadata synchronized in real-time. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be synchronized to all participants as they occur.
  - **Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan** - Select this option if you want the metadata synchronized during the initial scan. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be synchronized during the initial scan.

Create File Collaboration Job Wizard

**File Metadata**

Configure the replication of NTFS security permissions.

**Participants**

- File Metadata
- Application Support
- Email Alerts

**Synchronize Security Descriptors (ACLs)**

- ☐ Enable synchronizing NTFS security descriptors (ACLs) in real-time
- ☐ Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan

**Synchronize Security Descriptor Options**

- ☒ Owner
- ☒ DACL: Discretionary Access Control List
- ☐ SACL: System Access Control List

**Metadata Conflict Resolution**

Select Master Host for initial scan:

< Back    Next >    **Finish**    Cancel

2. Click **OK** in the message that appears after selecting a metadata option.
3. If you selected either of the first two options in the **Synchronize Security Descriptor Options** section, select the security descriptor components (Owner, DACL, and SACL) to be synchronized.
4. If you selected the option for metadata synchronization during the initial scan, select the host to be used as the [master host](#) in case of metadata conflict.

If a master host is not selected, then no metadata synchronization will be performed during the initial scan. If one or more security descriptors do not match across participants during the initial scan, [conflict resolution](#) will use permissions from the designated master host as the winner. If the file does not exist on the designated master host, a winner will be randomly picked from the other participants.



5. Click **Next**.

The [Application Support](#) page is displayed.

#### Step 4: Application Support

This step is optional.

A File Collaboration job can be automatically optimized to work with specific applications. Optimization is performed automatically for all watch sets of all participants in the job.

The **Application Support** page lists the file types for which Peer Software has known best practices, which include filtering recommendations, the prioritization of certain file types, and the enabling or disabling of file locking. However, if an application is not listed, this does not mean that the application is not supported.

For details about how an application is optimized, contact [support@peersoftware.com](mailto:support@peersoftware.com).

1. Select the applications that have files in the job's watch set.

2. Click **Next**.

The [Email Alerts](#) page is displayed.

### Step 5: Email Alerts

This step is optional.

An email alert notifies recipients when a certain type of event occurs, for example, session abort, host failure, system alert. The **Email Alerts** page displays a list of email alerts that have been applied to the job. When you first create a job, this list is empty. Email alerts are defined in [Preferences](#) and can then be applied to multiple jobs of the same type.

Peer Software recommends that you create email alerts in advance. However, from this wizard page, you can select existing alerts to apply to the job or create new alerts to apply.

To create a new alert, see [Email Alerts](#) in the [Preferences](#) section.

To apply an existing email alert to the job.

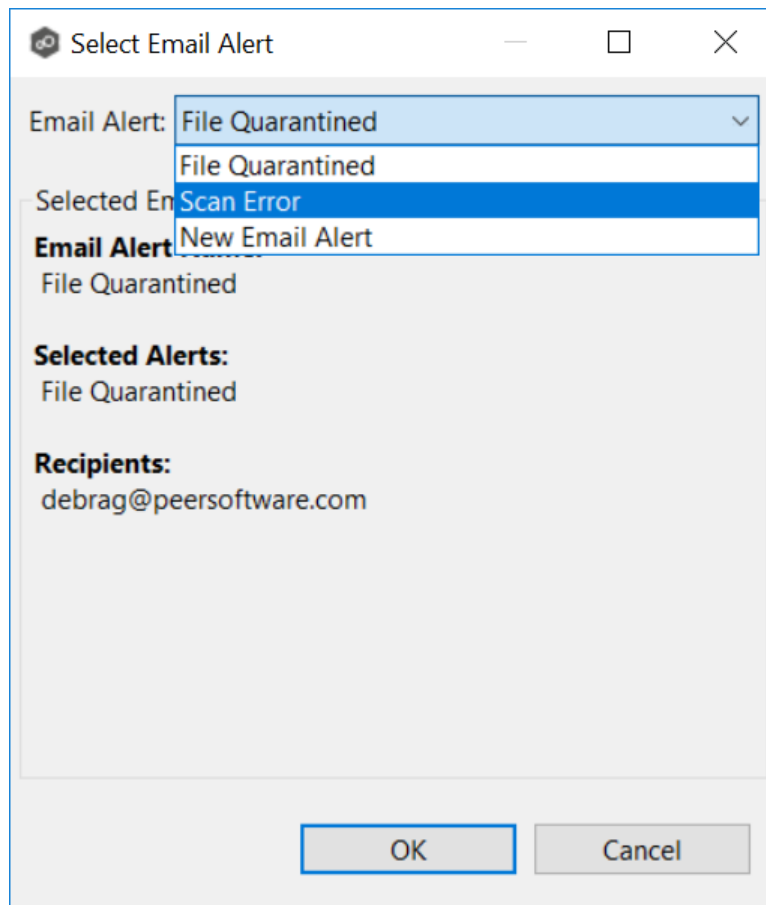
1. Click the **Select** button.

The screenshot shows a window titled "Create File Collaboration Job Wizard". Inside, the "Email Alerts" step is active, with the instruction "Select email alerts." A left sidebar contains a list of steps: "Participants", "File Metadata", "Application Support", and "Email Alerts" (which is highlighted). Above a table is a link "Edit Email Alerts". The table has four columns: "Name", "Enabled", "Event Types", and "Recipients". To the right of the table are three buttons: "Select", "Delete", and "View Detail". At the bottom of the window are four navigation buttons: "< Back", "Next >", "Finish" (which is highlighted with a blue border), and "Cancel".

Name	Enabled	Event Types	Recipients

The **Select Email Alert** dialog appears.

2. Select an alert from the **Email Alert** drop-down list.



3. Click **OK**.

The alert is listed in the **Email Alerts** page.

Create File Collaboration Job Wizard

Email Alerts

Select email alerts.

Participants  
File Metadata  
Application Support  
Email Alerts

[Edit Email Alerts](#)

Name	Enabled	Event Types	Recipients
Scan Error	Yes	Scan Error, Job Started	debrag@peersoftware.com

Select  
Delete  
View Detail

< Back   Next >   **Finish**   Cancel

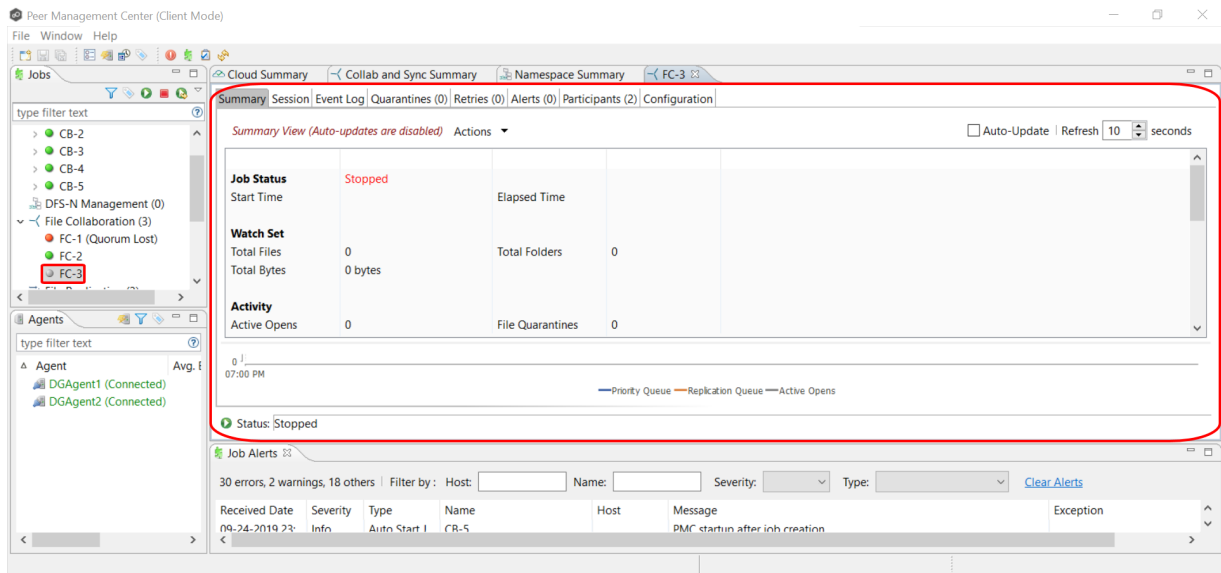
4. (Optional) Repeat steps 1-3 to apply additional alerts.
5. Continue to [Step 6: Save Job](#).

## Step 6: Save Job

Now that you have completed the first five steps of the wizard, you are ready to save the job configuration.

1. If you are satisfied with your job configuration, click **Finish** to save your job. Otherwise, click the **Back** button and make any necessary changes.

Congratulations! You have created a File Collaboration job. It is now listed in the **Jobs** view under **File Collaboration** and a view of the job appears in the **Runtime Summaries** area. You can start the job from either place. See [Running and Managing a File Collaboration job](#) for more information.



## Editing a File Collaboration Job

You can edit a File Collaboration job while it is running; however, any changes will not take effect until the job is restarted.

## Overview

When you create a File Collaboration job, the **Create Job** wizard guides you through the process, presenting the most common options for configuration. When editing a job, you have access to all options, allowing you to fine-tune the job configuration. Options not included in the initial job creation include:

- [Delta Replication](#)
- [DFS-N](#)
- [File Filters](#)
- [File Locking](#)
- [General](#)
- [Logging and Alerts](#)
- [Scheduled Replication](#)

- [SNMP Notifications](#)
- [Target Protection](#)
- [Tags](#)

You can edit multiple File Collaboration jobs simultaneously. For information about simultaneously editing multiple jobs, see [Editing Multiple Jobs](#).

## Editing a Job

To edit a File Collaboration job:

1. Select the job in the **Jobs** view.
2. Right-click and select **Edit Job**.

The **Edit File Collaboration** dialog appears.

**Edit File Collaboration Job**

**Participants**

General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
Delta Replication  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Available**

Host	Computer Description

Add Edit Detector Settings Delete

**Selected**

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		C:\Users\Public	Yes	Windows	No
DGAgent2		\\AFS2\Share1	Yes	Nutanix Files	No

OK Cancel

3. Select a configuration item in the navigation tree and make the desired changes:
  - [Participants](#)
  - [General](#)

- [File Filters](#)
- [Conflict Resolution](#)
- [Delta Replication](#)
- [File Metadata](#)
- [File Locking](#)
- [Application Support](#)
- [Logging and Alerts](#)
- [Target Protection](#)
- [Email Alerts](#)
- [SNMP Notifications](#)
- [Tags](#)
- [DFS-N](#)

4. Click **OK** when finished.

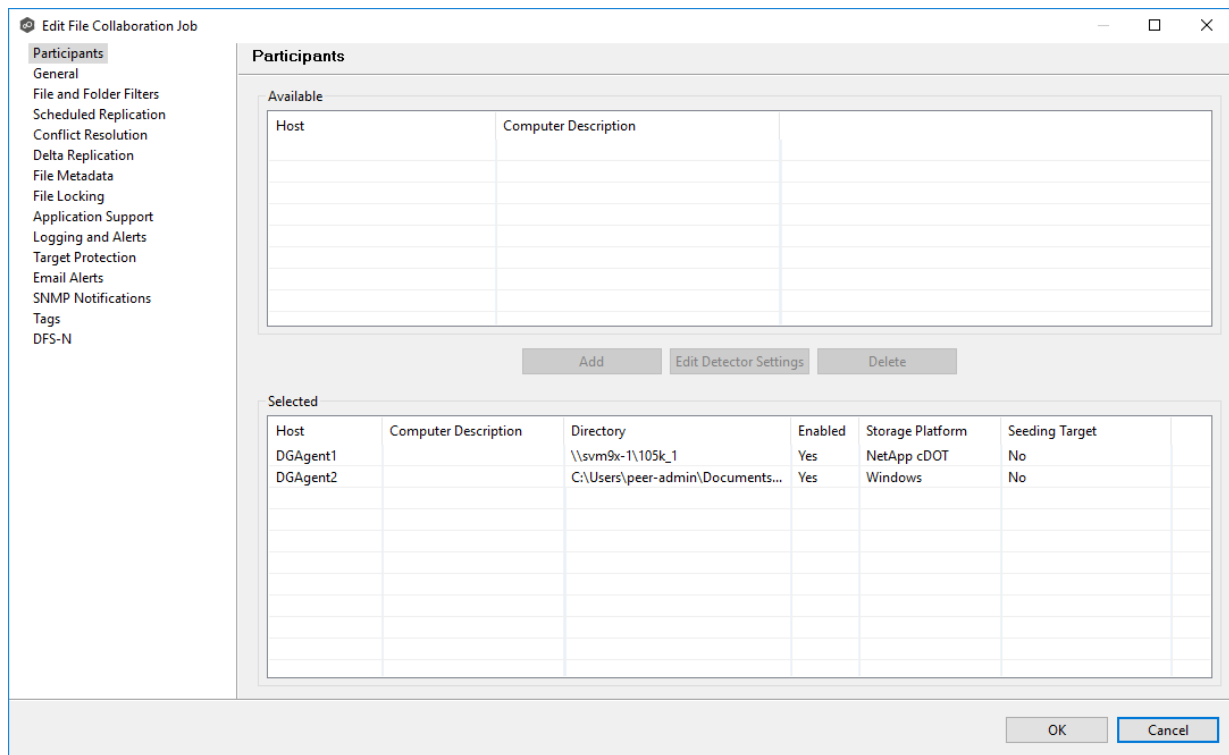
## Participants

The **Participants** page in the **Edit File Collaboration Configuration** dialog allows you to:

- [Add and delete participants from a job.](#)
- [Modify a participant's attributes.](#)
- [Modify a participant's detector settings.](#)

The **Participants** page in the **Edit File Collaboration Job** dialog has two tables: **Available** and **Selected**. The **Available** table lists the available hosts and the **Selected** table lists hosts that have already been added to the job. The **Computer Description** field displays the name of the server that the Peer Agent is running on.





This topic describes [adding](#) and [deleting](#) participants in a File Collaboration job.

## Adding a Participant to a Job

To add a participant to the job:

1. Click the participant in the **Available** table.

To be available, a host must have Peer Agent installed and successfully connect to the Peer Management Broker. If a particular host is not displayed in the list, try restarting the Peer Agent Windows Service on that host, and if it successfully connects to Peer Management Center Broker, then the list will be updated with the computer name of that host.

Edit File Collaboration Job

**Participants**

General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
Delta Replication  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Participants**

Available

Host	Computer Description
DGAgent3	

Add Edit Detector Settings Delete

Selected

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\svm9x-1\105k_1	Yes	NetApp cDOT	No
DGAgent2		C:\Users\peer-admin\Documents...	Yes	Windows	No

OK Cancel

2. Click the **Add** button.

The participant is moved to the **Selected** table.

Edit File Collaboration Job

**Participants**

General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
Delta Replication  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Participants**

Available

Host	Computer Description

Add Edit Detector Settings Delete

Selected

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\svm9x-1\105k_1	Yes	NetApp cDOT	No
DGAgent2		C:\Users\peer-admin\Documents...	Yes	Windows	No
DGAgent3		\\AFS2\Share3	Yes	Nutanix Files	No

OK Cancel

3. (Optional) Enter the computer's name in the **Computer Description** column.
4. Enter the path to the folder to be watched in the **Directory** column.
5. (Optional) Modify whether the participant is a [seeding target](#).
6. (Optional) Modify the participant's [detector settings](#).
7. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Deleting a Participant from a job

To delete a participant from a job:

1. Click the participant in the **Selected** table.
2. Click the **Delete** button.

The participant is moved to the **Available** table.

**Note:** A File Collaboration job must have at least two participants, so if after deleting a participant, there is only a single participant, you must add another participant to the job.

3. Click **OK** to close the Edit wizard or select another configuration item to modify.

You can modify the following attributes of a participant in a File Collaboration job:

- **Directory** - Specifies the watch set that has been selected for replication.
- **Enabled** - Determines whether the participant is enabled.
- **Storage Platform** - Identifies the type of storage platform that the agent will manage. If the storage device that the agent is managing has changed to a different storage platform, then you need to select the new platform.
- **Seeding Target** - Determines whether the participant host is used as a [data seeding target](#). For more information on smart data seeding, see [Smart Data Seeding](#) in [Advanced Topics](#) or contact [support@peersoftware.com](mailto:support@peersoftware.com).

To change the attributes of a participant:

1. Select the participant from the **Host** column in the **Selected** table.

**Participants**

**Available**

Host	Computer Description

Add Edit Detector Settings Delete

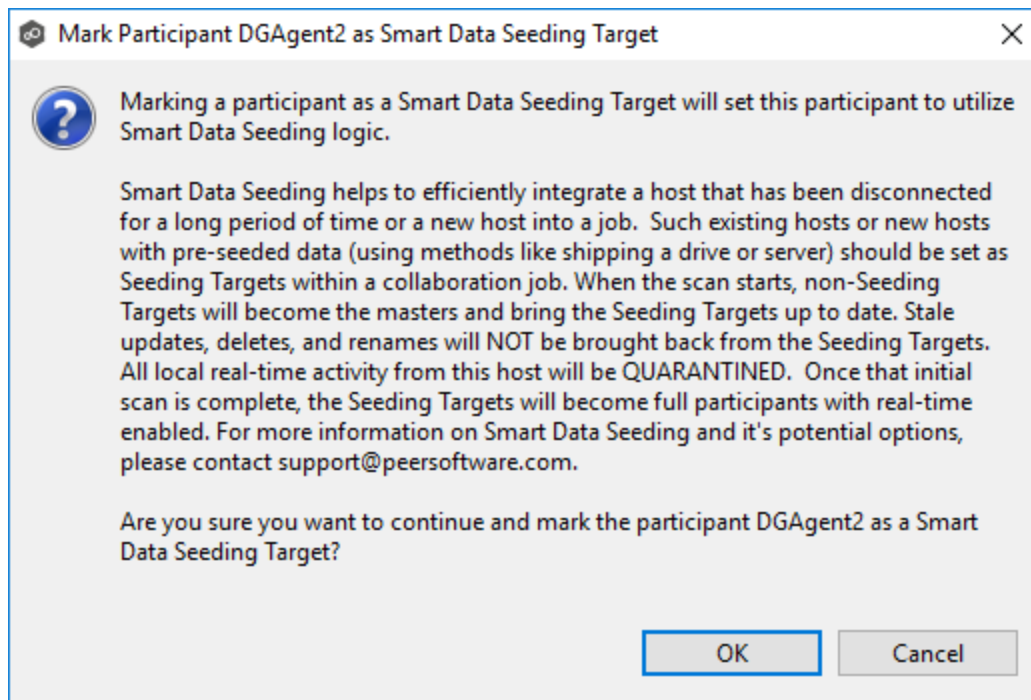
**Selected**

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\svm9x-1\105k_1	Yes	NetApp cDOT	No
DGAgent2		C:\Users\peer-admin\Documents...	Yes	Windows	No

OK Cancel

2. To change the directory that is replicated, enter a new directory path in the **Directory** column.
3. To enable or disable the agent, select a value in the **Enabled** column.
4. To change whether the agent is a seeding host, select **Yes** or **No** in the **Seeding Target** column.

If you selected **Yes**, review the information in the message dialog that appears and then click **OK**.

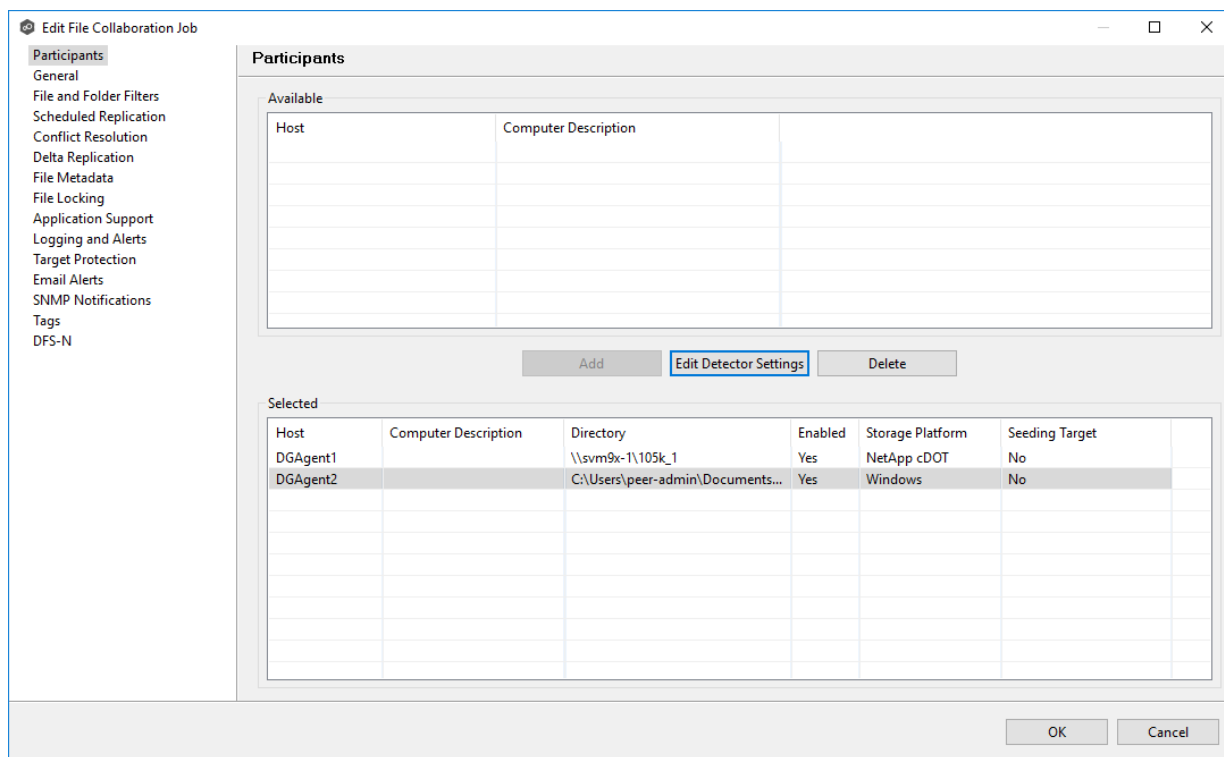


5. Click **OK** to close the Edit wizard or select another configuration item to modify.

In addition to [global real-time detection options](#) that apply to all jobs, you can set additional detection-related options for a specific File Collaboration job. For example, you can exclude real-time events by certain users. This is helpful if you are trying to prevent events generated from backup and/or archival tools from triggering activity.

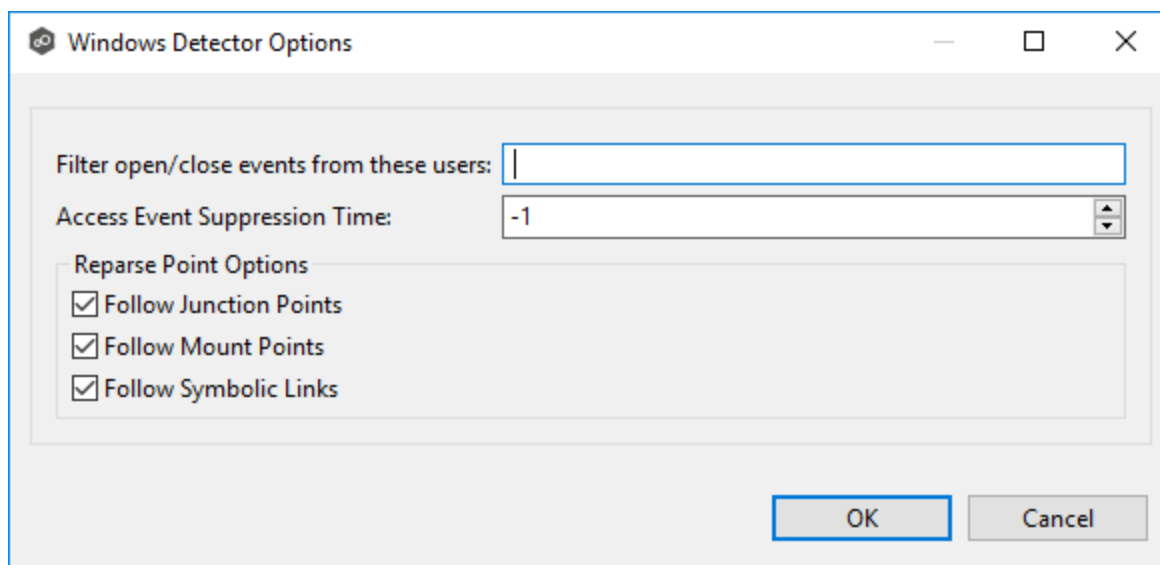
To modify the detector settings for a host:

1. Select the host in the **Selected** table.



2. Click **Edit Detector Settings**.

The information you are prompted to enter varies, depending on the type of storage platform. Windows, NetApp, and Nutanix examples are shown below.



**NetApp Options**

NetApp Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced FPolicy cDOT Settings for host: DGAgent2 and SVM: SVM9x-1

\*SVM Username:

\*SVM Password:

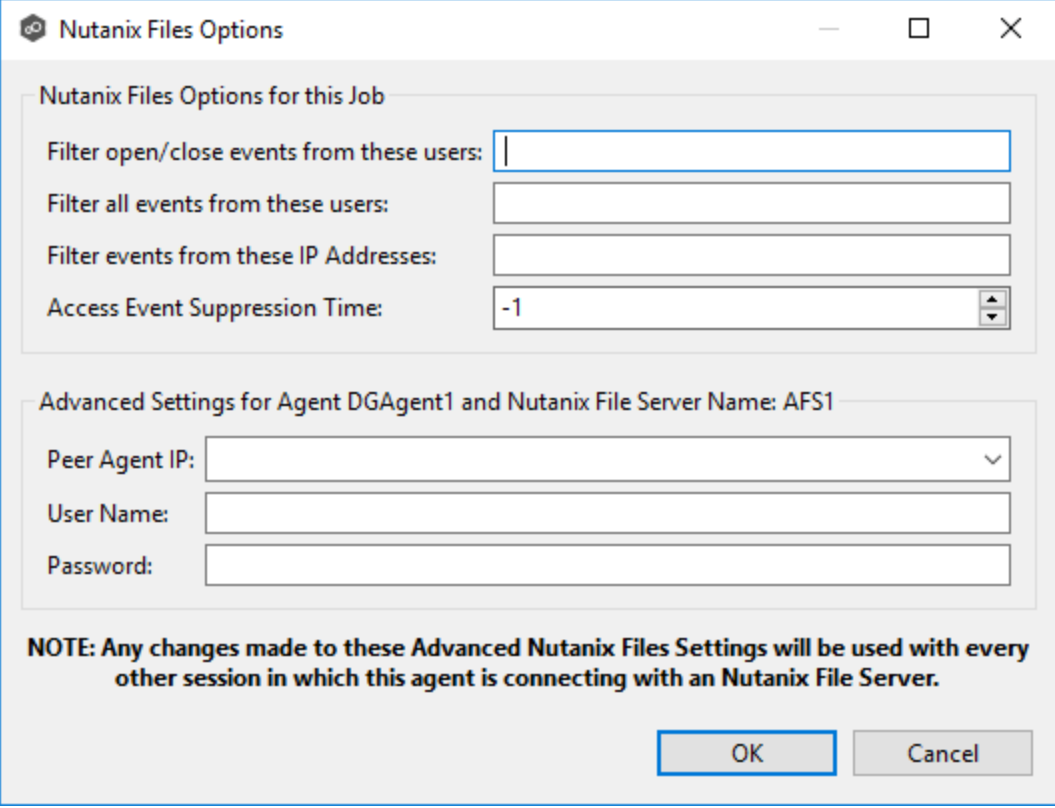
SVM Management IP:

\*Agent IP for SVM Conn.:

Filtered Extensions:

Admin Share Override:

**NOTE: Any changes made to these Advanced FPolicy cDOT Settings will be used with every other session in which this FPolicy Server is connecting to the same Storage Virtual Machine.**



The image shows a Windows-style dialog box titled "Nutanix Files Options". It contains two main sections. The first section, "Nutanix Files Options for this Job", has four input fields: "Filter open/close events from these users:" (empty), "Filter all events from these users:" (empty), "Filter events from these IP Addresses:" (empty), and "Access Event Suppression Time:" (set to -1). The second section, "Advanced Settings for Agent DGAgent1 and Nutanix File Server Name: AFS1", has three input fields: "Peer Agent IP:" (empty), "User Name:" (empty), and "Password:" (empty). At the bottom, there is a note: "NOTE: Any changes made to these Advanced Nutanix Files Settings will be used with every other session in which this agent is connecting with an Nutanix File Server." and two buttons: "OK" and "Cancel".

Nutanix Files Options

Nutanix Files Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced Settings for Agent DGAgent1 and Nutanix File Server Name: AFS1

Peer Agent IP:

User Name:

Password:

**NOTE: Any changes made to these Advanced Nutanix Files Settings will be used with every other session in which this agent is connecting with an Nutanix File Server.**

OK Cancel

3. Modify the values as needed.
4. Click **OK**.

## General

The **General** page in the **Edit File Collaboration Job** dialog presents miscellaneous settings pertaining to a File Collaboration job. You may want to consult with Peer Software's Technical Support team before modifying these values.

To modify these settings:

1. Enter the values recommended by Peer Software Support.



The screenshot shows a window titled "Edit File Collaboration Job" with a sidebar on the left and a main configuration area on the right. The sidebar lists various options: Participants, General (selected), File and Folder Filters, Scheduled Replication, Conflict Resolution, Delta Replication, File Metadata, File Locking, Application Support, Logging and Alerts, Target Protection, Email Alerts, SNMP Notifications, Tags, and DFS-N. The main area is titled "General" and contains the following fields and checkboxes:

- Job ID: 153
- Job Type: File Collaboration
- Job Name: FC-2
- Transfer Block Size (KB): 1024
- File Synchronization Job Priority: 2
- Timeout (Seconds): 180
- First Scan Mode: FOLDER\_BY\_FOLDER
- Remove Filtered Files On Folder Delete: ☒
- Require All Hosts At Start: ☐
- Auto Start: ☒

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

Option	Description
<b>Job ID</b>	Unique, system-generated job identifier that cannot be edited.
<b>Job Type</b>	Identifies the job type. This cannot be modified.
<b>Job Name</b>	Name of this File Collaboration job. This name must be unique.
<b>Transfer Block Size (KB)</b>	The block size in Kilobytes used to transfer files to hosts. Larger sizes will yield faster transfers on fast networks but will consume more memory in the <a href="#">Peer Management Broker</a> and <a href="#">Peer Agents</a> .
<b>File Synchronization Job Priority</b>	Use this to increase or decrease a job's file synchronization priority relative to other configured job priorities. Jobs are serviced in a round-robin fashion, and this number determines the maximum number of synchronization tasks that will be executed sequentially before yielding to another job.

Option	Description
<b>Timeout (Seconds)</b>	Number of seconds to wait for a response from any host before performing retry logic.
<b>First Scan Mode</b>	Determines which scan type will be used when the job is first started. For environments where most data is NOT seeded, the FOLDER_BY_FOLDER method will be best. For environments where most data IS seeded, the BULK_CHECKSUM method will result in a faster first scan.
<b>Remove Filtered Files On Folder Delete</b>	If selected, then all child files on target hosts will be deleted when its parent folder is deleted on another source host. Otherwise, filtered files will be left intact on targets when a parent folder is deleted on another source host.
<b>Require All Hosts At Start</b>	If selected, requires all <a href="#">participating hosts</a> to be online and available at the start of the File Collaboration job in order for the job to successfully start.
<b>Auto Start</b>	If selected, then this file collaboration session will automatically be started when the Peer Management Center Service is started.

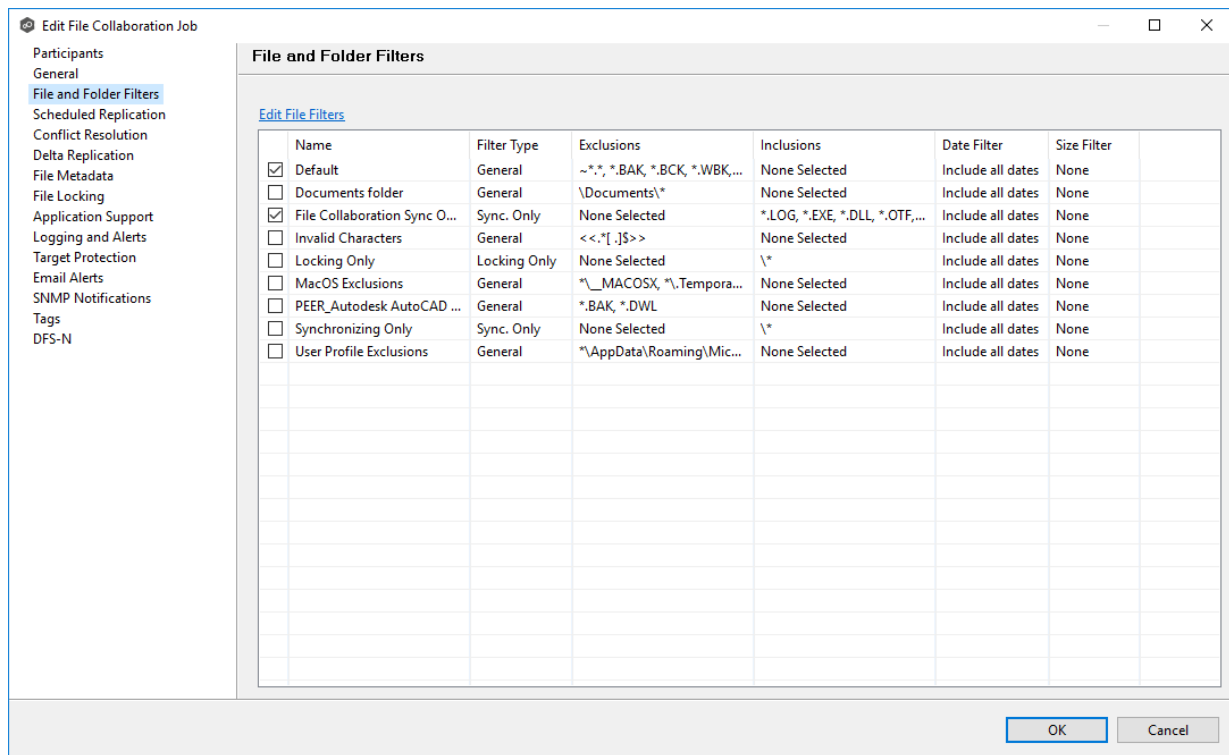
2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## File and Folder Filters

The **File and Folder Filters** page in the **Edit File Collaboration Job** dialog displays a list of [file and folder filters](#). A file or folder filter enables you to exclude and/or include files and folders from the job based on file type, extension, name, or directory path. Any file or folder that matches the filter is excluded or included from replication, depending on the filter's definition. By default, all files and folders selected in the **Source Paths** page will be replicated.

1. Select the file and folder filters you want to apply to the job.

If you want to create a new file or folder filter or modify an existing one, click **Edit File Filters**. See [File and Folder Filters](#) in the [Preferences](#) section for information about creating or modifying a file filter.



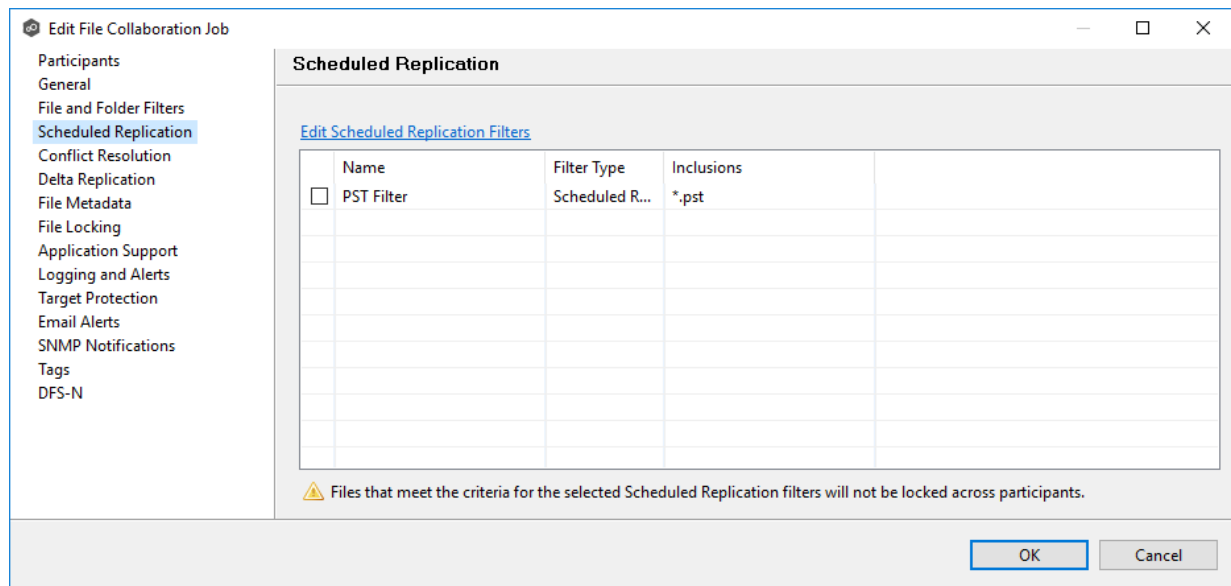
2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Scheduled Replication

The **Scheduled Replication** page in the **Edit File Collaboration Job** dialog displays a list of [scheduled replication filters](#). A scheduled replication filter enables you to identify files and folders that you don't want replicated in real-time.

1. Select the scheduled replication filters you want to apply to the job.

If you want to create a new filter or modify an existing one, click **Edit Scheduled Replication Filters**. See [Scheduled Replication](#) in the [Preferences](#) section for information about creating or modifying a scheduled replication filter.



2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Conflict Resolution

By default, any file conflicts that are encountered during the [initial synchronization process](#) are automatically resolved by Peer Management Center. Peer Management Center resolves the conflict by selecting the file with the most recent modification time. Conflicts that cannot be automatically be resolved result in the files being quarantined. The **Conflict Resolution** page in the **Edit File Collaboration Job** allows you to select options for resolving file conflicts and quarantines.

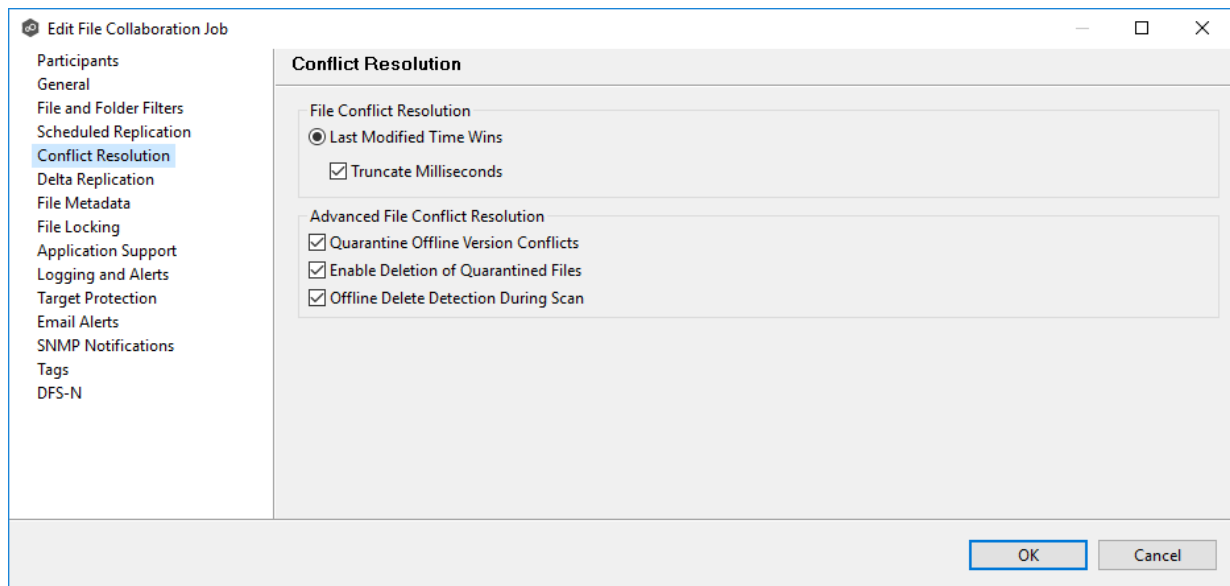
However, if you want to resolve the conflicts yourself, you can contact Peer Software to enable manual resolution. With manual resolution, you can select the host with the correct version of the file.

For more information about the cause of file conflicts, see [Conflicts, Retries, and Quarantines](#).

To modify conflict resolution settings for the File Collaboration job:

1. In the **File Conflict Resolution** section, select the **Truncate Milliseconds** option if you want the millisecond value truncated from each time stamp when comparing the time stamps of a file on two or more hosts.

As some storage platforms and applications track milliseconds slightly differently, selecting this option will prevent subtle millisecond differences from causing an otherwise in-sync file to be replicated or quarantined.



2. Select the **Advanced File Conflict Resolution** options you want applied:

Option	Description
<b>Quarantine Offline Version Conflicts</b>	Select this option if you want Peer Management Center to quarantine a file that was updated in two or more locations while the collaboration session was not running. If it is not selected, the file with the most recent last modified time will be replicated to all other participants.
<b>Enable Deletion of Quarantined Files</b>	Select this option if you want Peer Management Center to process a delete event for a quarantined file. If it is not selected, the quarantined file is not deleted and remains quarantined.
<b>Offline Delete Detection During Scan</b>	Select this option (and enable <a href="#">target protection</a> ), if you want any files or folders that were deleted while the job was stopped to be deleted from all participants when the job is restarted. If it is not selected, then the deleted file or folder is restored from a participant with the file or folder to any participant where it no longer exists.

3. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Delta Replication

The **Delta Replication** page in the **Edit File Collaboration Job** dialog allows you to specify the delta-replication options to use for the selected File Collaboration job. Delta-level replication is a byte replication technology that enables block/byte level synchronization for a File Collaboration job. Through this feature, Peer Management Center is able to transmit only the bytes/blocks of a file that have changed instead of transferring the entire file. This results in much lower network bandwidth utilization, which can be an enormous benefit if you are transferring files across a slow WAN or VPN, as well as across a high-volume LAN.

Delta-level replication is enabled on a per File Collaboration job basis and generally affects all files in the [watch set](#). You will only benefit from delta-level replication for files that do not change much between file modifications, which includes most document editing programs.

**Edit File Collaboration Job**

Participants  
General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
**Delta Replication**  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

### Delta Replication

Enable Delta-level Replication: ☒

Checksum Transfer Size (KB): 256

Delta Block Transfer Size (KB): 512

Minimum File Size (KB): 5120

Minimum File Size Percentage Target/Source: 0.30

**Excluded File Extensions**

- zip
- jpg
- jpeg
- png
- gif
- tiff
- tif
- Z
- tgz
- gz
- gzip
- rar
- 7z
- bz
- bz2
- bzip2
- mp3
- mp4
- m4v
- ogg
- avi
- wav
- vob
- aac
- aif
- aifc
- aiffasf
- asx
- wax
- wma
- wmd
- wmv
- wvx
- wmp
- wmx
- mpeg
- mpg
- m1v
- mp2
- mpa
- mpe
- mp2v
- mpv2
- m4p
- mov

**Excluded File Name Patterns**

OK Cancel

To modify delta-level replication options:

1. Modify the following the fields as necessary.

Field	Description
<b>Enable Delta-Level Replication</b>	Select to enable delta encoded file transfers which only sends the file blocks that are different between source and target(s). If this is disabled, the standard file copy method will be used to synchronize files.
<b>Checksum Transfer Size (KB)</b>	Enter the block in kilobytes used to transfer checksums from target to source at one time. Larger sizes will result in faster checksum transfer, but will consume more memory on the Peer Agents
<b>Delta Block Transfer Size (KB)</b>	Enter the block size in kilobytes used to transfer delta encoded data from source to target at one time. Larger sizes will result in faster overall file transfers but will consume more memory on the Peer Agents.
<b>Minimum File Size (KB)</b>	Enter the minimum size of files in kilobytes to perform delta encoding for. If a file is less than this size, then delta encoding will not be performed.
<b>Minimum File Size Percentage Target/Source</b>	Enter the minimum allowed file size difference between source and target, as a percentage, to perform delta encoding. If the target file size is less than this percentage of the source file size, then delta encoding will not be performed.
<b>Excluded File Extensions</b>	Enter a comma-separated list of file extension patterns to be excluded from delta encoding, e.g., zip, jpg, png. In general, compressed files should be excluded from delta encoding and the most popular compressed file formats are excluded by default.
<b>Excluded File Name Patterns</b>	Enter a list of file name patterns to be excluded from delta encoding. If a file name matches any pattern in this list, then it will be excluded from delta encoding transfers and a regular file transfer will be performed. See <a href="#">File and Folder Filters</a> for more information on specifying wildcard expressions.

- Click **OK** to close the Edit wizard or select another configuration item to modify.



## File Metadata

The **File Metadata** page in the **Edit File Collaboration Job** dialog allows you to modify your file metadata synchronization settings and provides some additional options not available when creating the job. See [File Metadata Synchronization](#) in [Advanced Topics](#) for more information about file metadata replication.

To enable file metadata synchronization:

1. Select when you want the metadata synchronized (you can select one or both options):
  - **Enable synchronizing NTFS security descriptors (ACLs) in real-time** - Select this option if you want the metadata replicated in real-time. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be transferred to the target host file(s) as they occur.
  - **Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan** - Select this option if you want the metadata replicated during the initial scan. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be synchronized during the initial scan.

The screenshot shows the 'Edit File Collaboration Job' dialog box with the 'File Metadata' tab selected. The left sidebar lists various settings categories, with 'File Metadata' highlighted. The main panel contains several sections of options:

- Synchronize Security Descriptors (ACLs)**:
  - ☐ Enable synchronizing NTFS security descriptors (ACLs) in real-time
  - ☐ Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan
  - ☒ Enable prevention of corrupt or blank Owner or DACLs on source or master host from being applied to any target host
- Synchronize Security Descriptor Options**:
  - ☐ Owner
  - ☒ DACL: Discretionary Access Control List
  - ☐ SACL: System Access Control List
- Metadata Conflict Resolution**:
  - Select a Master Host for initial scan:
  - ☐ Enable enhanced metadata conflict resolution
- File Reparse Point Synchronization**:
  - Reparse Tag Name (numerical value only):
  - Reparse Master Host:
- Alternate Data Streams Transfer**:
  - ☐ Enable transfer of file Alternate Data Streams (ADS)

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

2. Click **OK** in the message that appears after selecting a metadata option.
3. If you selected either of the first two options in the **Synchronize Security Descriptor Options** section, select the security descriptor components (Owner, DACL, and SACL) to be synchronized.

4. If you selected the option for metadata synchronization during the initial scan, select the host to be used as the [master host](#) in case of file metadata conflict.

If a master host is not selected, then no metadata synchronization will be performed during the initial scan. If one or more security descriptors do not match across participants during the initial scan, [conflict resolution](#) will use permissions from the designated master host as the winner. If the file does not exist on the designated master host, a winner will be randomly picked from the other participants.

5. (Optional) Click the **Enable enhanced metadata conflict resolution** checkbox.

If enabled, this option ensures that when a metadata conflict occurs and a file or folder is written to a target, the Peer Agent service account is not assigned as the owner of that file or folder. If the Peer Agent service account is the owner, the user may not have permission to access the file or folder.

Note: The Peer Agent service account cannot be a local or system administrator. As described in [Peer Global File Service - Environmental Requirements](#), the Peer agent service account should be an actual user.

6. (Optional) Enter values for one or both file reparse point data synchronization options:

- **Reparse Tag Name** - Enter a single numerical value. Must be either blank (if blank, reparse synchronization will be disabled) or greater than or equal to 0. The default for Symantec Enterprise Vault is 16. A value of 0 enables reparse point synchronization for all reparse file types. If you are unsure as to what value to use, then contact Peer Software technical support, or you can use a value of 0 if you are sure that you are only utilizing one vendor's reparse point functionality.
- **Reparse Master Host** - Select a master host. If a master host is selected, then when the last modified times and file sizes match on all hosts, but the file reparse attribute differs (e.g. archived/offline versus unarchived on file server), then the file reparse data will be synchronized to match the file located on the master host. For Enterprise Vault, this should be the server where you run the archiving task on. If the value is left blank, then no reparse data synchronization will be performed, and the files will be left in their current state.

Note: Use this option only if you are utilizing archiving or hierarchical storage solutions that make use of NTFS file reparse points to access data in a remote location, such as Symantec's Enterprise Vault. Enabling this option allows synchronization of a file's reparse data, and not the actual offline content, to target hosts, and prevents the offline file from being recalled from the remote storage device.

7. (Optional) Select the **Enable transfer of file Alternate Data Stream (ADS)** checkbox.

If enabled, Alternate Data Streams (ADS) of updated files will be transferred to the corresponding files on target participants as a post process of the normal file synchronization.

Known limitation: ADS information is transferred only when a modification on the actual file itself is detected. ADS will not be compared between participants. The updated file's ADS will be applied to the corresponding files on target participants.

- Click **OK** to close the Edit wizard or select another configuration item to modify.

## File Locking

The **File Locking** page in the **Edit File Collaboration Job** dialog presents options pertaining to how source and target files are locked by Peer Management Center.

To modify file locking options:

The screenshot shows the 'Edit File Collaboration Job' dialog box with the 'File Locking' tab selected. The left sidebar lists various configuration categories, with 'File Locking' highlighted. The main area contains three sections: 'Locking Options', 'Source Snapshot Synchronization', and 'Sync. On Save'. Each section has a title bar and a group of settings.

Section	Setting	Value
Locking Options	Exclusive Target Lock:	<input type="checkbox"/>
	Include MS Office User Lock Information:	<input checked="" type="checkbox"/>
	Include AutoCAD User Lock Information:	<input type="checkbox"/>
Source Snapshot Synchronization	Enable Source Snapshot Copy Sync.:	<input type="checkbox"/>
	Snapshot Copy Max File Size (MB):	512
	Snapshot Copy File Extensions:	mdb,accdb,zip,psd,ai,indd
Sync. On Save	Enable Sync. On Save:	<input type="checkbox"/>
	Included File Extensions:	xls,xlsx,doc,docx,dwg
	Synchronization Delay (Seconds):	20

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

Modify these fields as needed:

<b>Exclusive Target Lock</b>	If enabled, then whenever possible, an exclusive lock will be obtained on target file handles, which will prevent users from opening the file (even in read-only mode) while a user has the file opened on the source host. When this option is disabled, then users will be allowed to open files for read-only if the application allows for this.
------------------------------	--

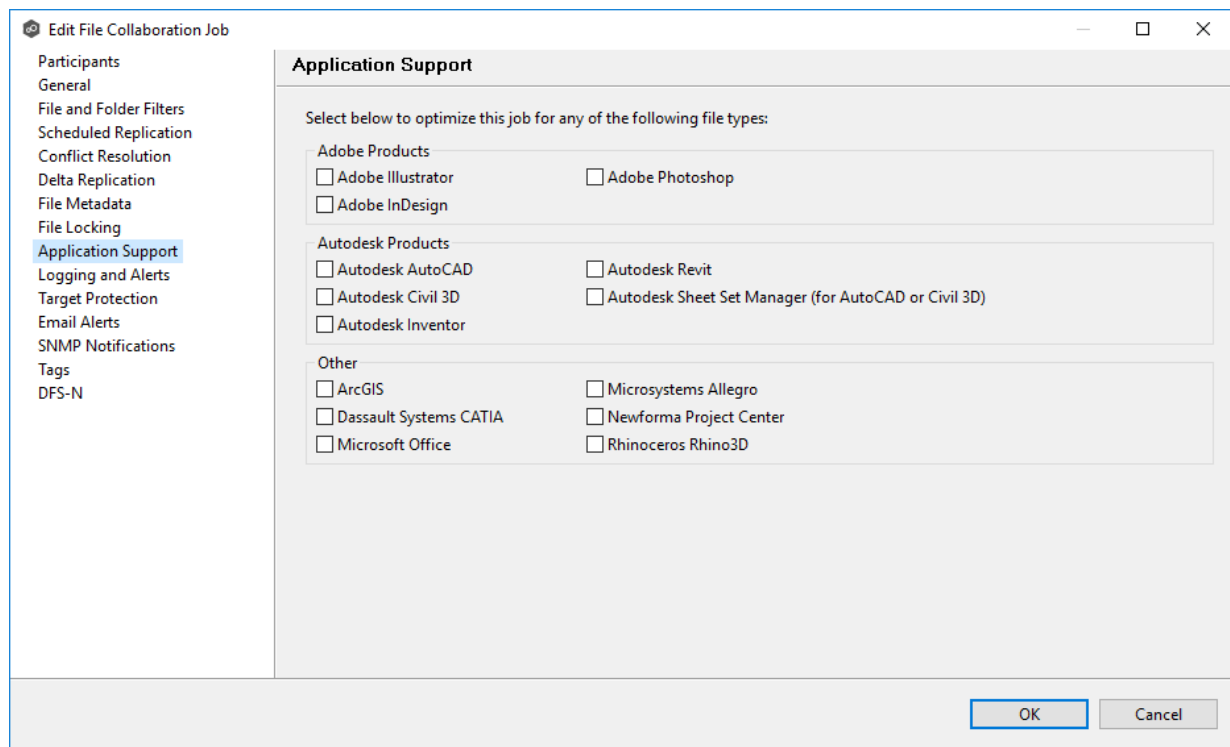
<b>Include MS Office User Lock Information</b>	If enabled, user lock information (if available) will be propagated to target locks for supported Microsoft Office files (e.g., Word, Excel, and PowerPoint).
<b>Include AutoCad User Lock Information</b>	If enabled, user lock information (if available) will be propagated to target locks for supported AutoCAD files.
<b>Enable Source Snapshot Copy Sync.</b>	If enabled, a snapshot copy of the source file will be created for files that meet the snapshot configuration criteria below, and this copy will be used for synchronization purposes. In addition, no file handle will be held on the source file except while making a copy of the file.
<b>Snapshot Copy Max File Size (MB)</b>	The maximum file size for which source snapshot synchronization will be utilized.
<b>Snapshot Copy File Extensions</b>	A comma-separated list of file extensions for which source snapshot synchronization will be utilized.
<b>Enable Sync. On Save</b>	If enabled, this feature will allow supported file types to be synchronized after a user saves a file, rather than waiting for the file to close.
<b>Included File Extensions</b>	A comma separated list of file extensions for which to enable the Sync. On Save feature.
<b>Synchronization Delay (Seconds)</b>	The number of seconds to wait after a file has been saved before initiating a synchronization of the file.

## Application Support

When you create a File Collaboration job, you have the option of [selecting applications that are automatically optimized](#). When editing the job, you can modify your selections in the **File Locking** page in the **Edit File Collaboration Job** dialog.

To modify which applications are optimized:

1. Select the applications to be optimized.



2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Logging and Alerts

### Overview of File Event Logging

Various types of file collaboration events can be written to a log file and to the [Event Log](#) tab located within the File Collaboration runtime view for the selected File Collaboration job. Each job will log to the **fc\_event.log** file located in the **Hub\logs** subdirectory within the Peer Management Center installation directory. All log files are stored in a tab-delimited format that can easily be read by Microsoft Excel or other database applications.

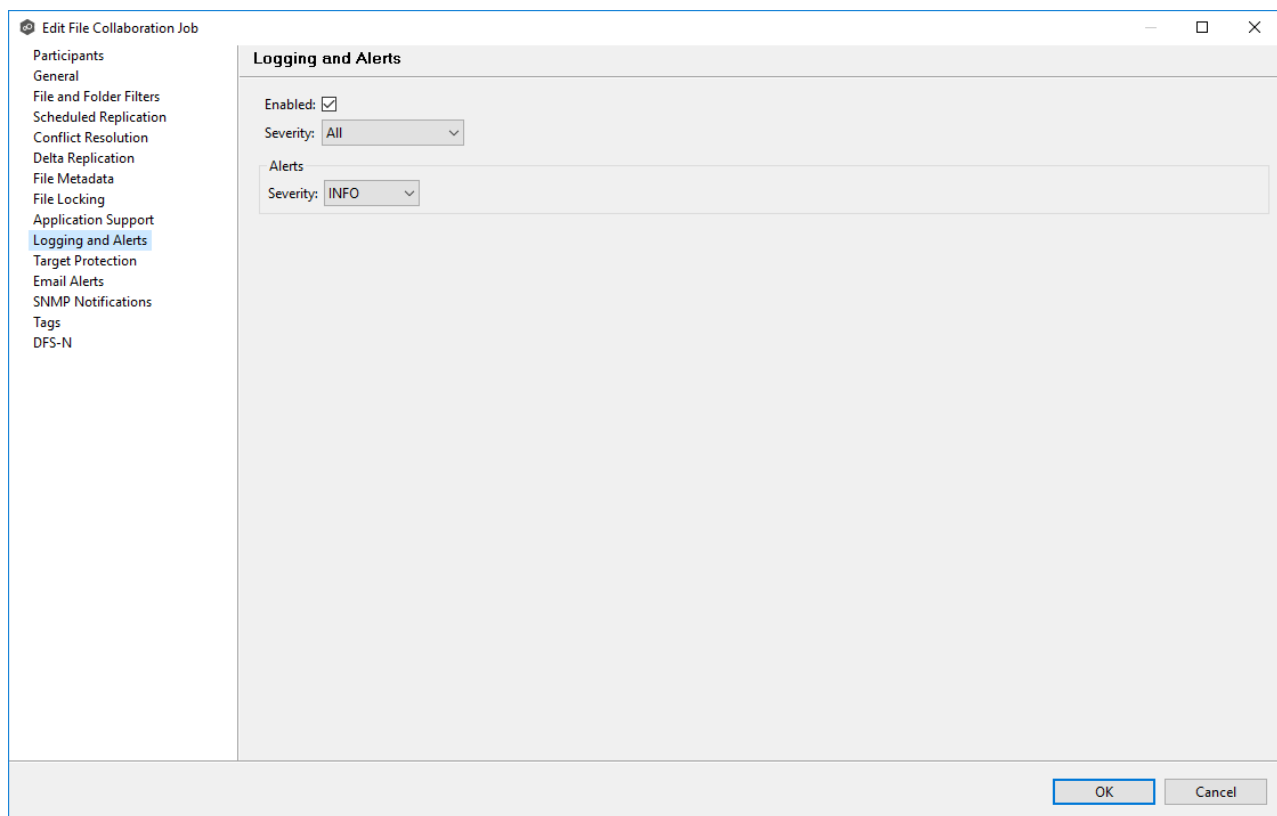
### Log Entry Severity Levels

<b>Informational</b>	Informational log entry, e.g., a file was opened.
----------------------	---

<b>Warning</b>	Some sort of warning occurred that did not produce an error but was unexpected or may need further investigation.
<b>Error</b>	An error occurred performing some type of file activity.
<b>Fatal</b>	A fatal error occurred that caused a host to be taken out of the session, a file to be quarantined, or a session to become invalid.

## Configuration

By default, all file collaboration activity is logged for all severity levels. You can enable or disable file event logging as well as select the level of granularity.



## Logging Fields

Below is a list of logging fields and their descriptions:

Field	Description
<b>Enabled</b>	Selecting this option will enable file event logging based on the other settings. Deselecting this option will completely disable all logging.
<b>Severity</b>	Determines what severity levels will be logged. There are two options: <ul style="list-style-type: none"><li>• All (Informational, Warnings, Error, Fatal)</li><li>• Errors &amp; Warnings (Warnings, Error, Fatal)</li></ul>
<b>Event Types</b>	If checked, the corresponding event type will be logged.
<b>File Open</b>	A file was opened by a remote application on a <a href="#">source host</a> .
<b>File Lock</b>	A file lock was acquired on a <a href="#">target host</a> by the File Collaboration job.
<b>File Close</b>	A file was closed.
<b>File Add</b>	A file was added to the <a href="#">watch set</a> .
<b>File Modify</b>	A file was modified in the watch set.
<b>File Delete</b>	A file was deleted.
<b>File Rename</b>	A file was renamed.
<b>Attribute Change</b>	A file attribute was changed.

Field	Description
<b>Security (ACL) Change</b>	The security descriptor of a file or folder was changed.
<b>Directory Scan</b>	Indicates when a directory was scanned as a result of the <a href="#">initial synchronization process</a> .
<b>File ADS Transfer</b>	The Alternate Data Stream of a modified file was synced to target host(s).

## Alerts

Various types of alerts can be logged to a log file and to the [Alerts](#) table located within the [File Collaboration runtime view](#) for the selected job. Each File Collaboration job will log to the **fc\_alert.log** file located in the **Hub\logs** subdirectory within the Peer Management Center installation directory. All log files are stored in a tab-delimited format that can easily be read by Microsoft Excel or other database applications.

The default log level is WARNING, which will show any warning or error alerts that occur during a running session. Depending on the severity of the alert, the session may need to be restarted.

### Target Protection

Target protection is used to protect files on [target hosts](#) by saving a backup copy before a file is either deleted or overwritten on the target host. If enabled, then whenever a file is deleted or modified on the source host but before the changes are propagated to the targets, a copy of the existing file on the target is moved to the Peer Management Center trash bin.

The trash bin is located in a hidden folder named **.pc-trash\_bin** found in the root directory of the [watch set](#) of the target host. A backup file is placed in the same directory hierarchy location as the source folder in the watch set within the recycle bin folder. If you need to restore a previous version of a file, you can copy the file from the trash bin into the corresponding location in the watch set and the changes will be propagated to all other collaboration hosts.

You can configure target protection in the **Target Protection** page in the **Edit File Collaboration Job** dialog.



**Edit File Collaboration Job**

- Participants
- General
- File and Folder Filters
- Scheduled Replication
- Conflict Resolution
- Delta Replication
- File Metadata
- File Locking
- Application Support
- Logging and Alerts
- Target Protection**
- Email Alerts
- SNMP Notifications
- Tags
- DFS-N

### Target Protection

Enabled: ☒

# of Backup Files to Keep:

# of Days to Keep:

Trash Bin:

OK Cancel

Modify the fields as needed:

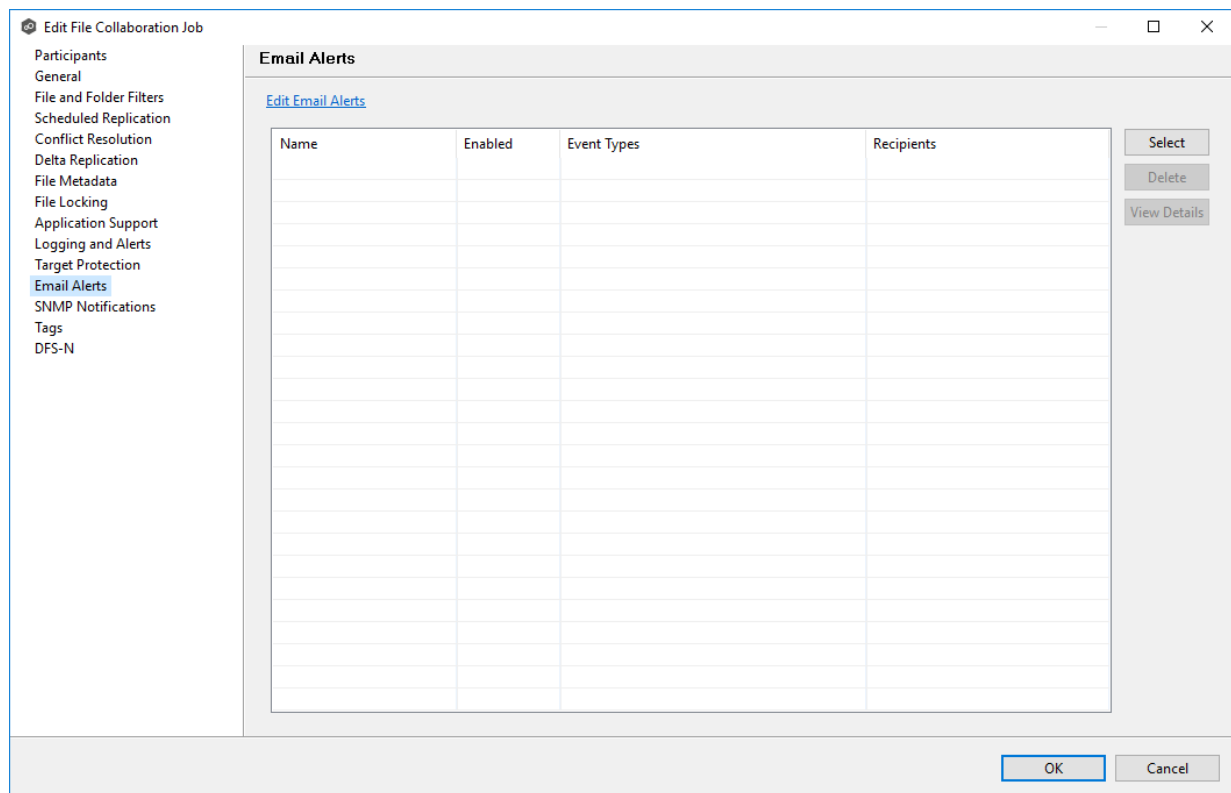
Field	Description
<b>Enabled</b>	Enables target protection.
<b># of Backup Files to Keep</b>	The maximum number of backup copies of an individual file to keep in the trash bin before purging the oldest copy.
<b># of Days to Keep</b>	The number of days to keep a backup archive copy around before deleting from disk. A value of 0 will disable purging any files from archive.
<b>Trash Bin</b>	The trash bin folder name located in the root directory of the watch set. This is a hidden folder and the name cannot be changed by the end-user.

## Email Alerts

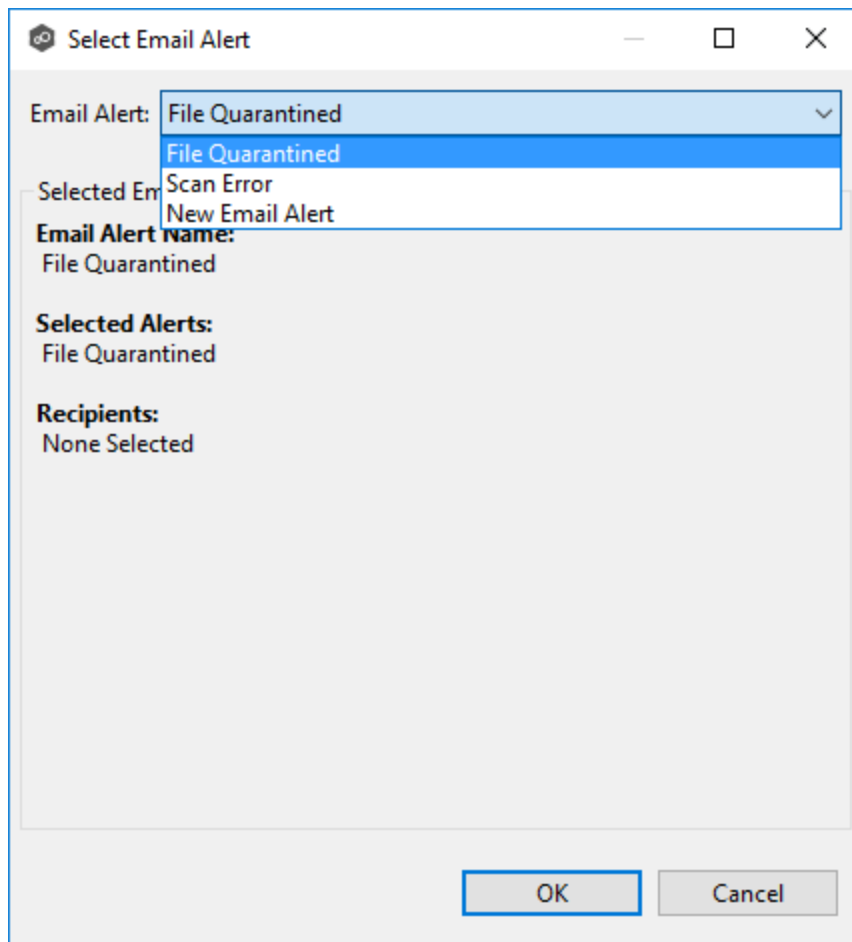
The **Email Alerts** page in the **Edit File Collaboration Job** dialog allows you to select which email alerts to apply to a File Collaboration job. Email alerts are defined in the [Preferences](#) dialog, and can then be applied to individual jobs. See [Email Alerts](#) in the **Preferences** section for information about creating an email alert for a File Collaboration job.

To apply email alerts to a File Collaboration job while editing the job:

1. Click the **Select** button.



The **Select Email Alert** dialog opens.



2. Select the email alert from the drop-down list, and then click **OK**.

The newly added email alert appears in the **Email Alerts** table.

[illegible]

3. Repeat to add additional alerts to the job.
4. Click **OK** to close the Edit wizard or select another configuration item to modify.

## SNMP Notifications

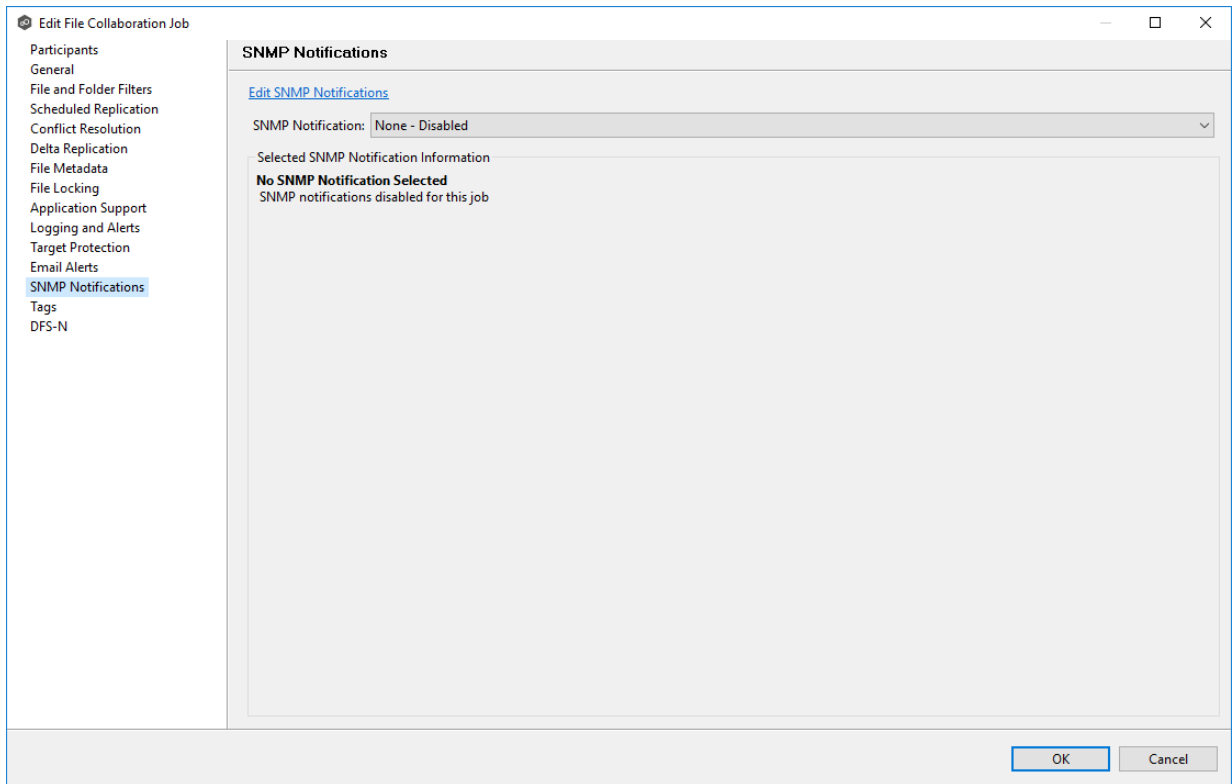
The **SNMP Notifications** page in the **Edit File Collaboration Job** dialog allows you to apply SNMP notifications to a File Collaboration job.

SNMP notifications, like email alerts and file filters, are configured at a global level in the [Preferences](#) dialog, then applied to individual jobs. For more information about SNMP Notifications, see [SNMP Notifications](#) in the **Preferences** section.

To enable or disable SNMP notifications for a File Collaboration job:

1. To enable, select an SNMP notification from the drop-down list.

To disable, select **None - Disabled**.



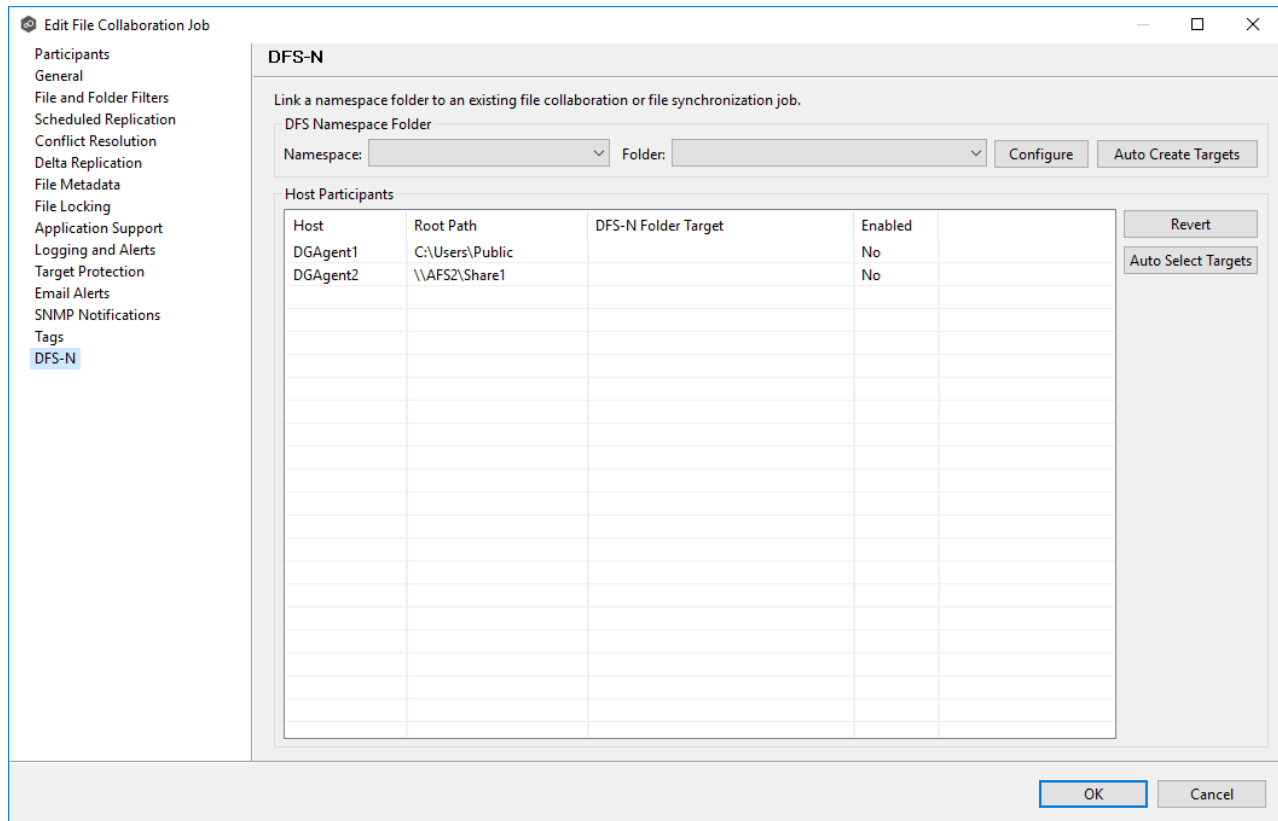
2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Tags

The **Tags** page in the **Edit File Collaboration Job** dialog allows you to assign existing tags and categories to the selected job. This page is not available in [Multi-Job Editing](#) mode. For more information about tags, see [Tags](#) in the [Basic Concepts](#) section.



Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.



## Editing Multiple Jobs

Peer Management Center supports multi-job editing, allowing you to quickly and effectively manipulate multiple File Collaboration jobs simultaneously. For example, you can use this feature to change a single configuration item such as **Auto Start** for any number of already configured jobs in one operation instead of having to change the item individually for each.

While this feature does cover most of the options available on a per-job basis, certain options are unavailable in multi-job edit mode, specifically ones tied to [participants](#). Configuration of participants must be performed on a per job basis.

To edit multiple jobs simultaneously:

1. Open Peer Management Center.
2. Select the jobs you want to edit in the **Jobs** view.
3. Right-click and select **Edit Jobs**.

For the most part, the original configuration dialog remains the same with a few minor differences depending on similarities between the selected File Collaboration jobs. A sample dialog is as follows:

**Edit File Collaboration Jobs - Multiple Selected**

**General**

File Filters  
Delta Replication  
File Metadata  
File Locking  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications

**General**

Job ID: MULTIPLE SELECTED

Job Type: MULTIPLE SELECTED

Transfer Block Size (KB): 1024

File Synchronization Job Priority: 2

Timeout (Seconds): 180

First Scan Mode: FOLDER\_BY\_FOLDER

Remove Filtered Files On Folder Delete: ☒

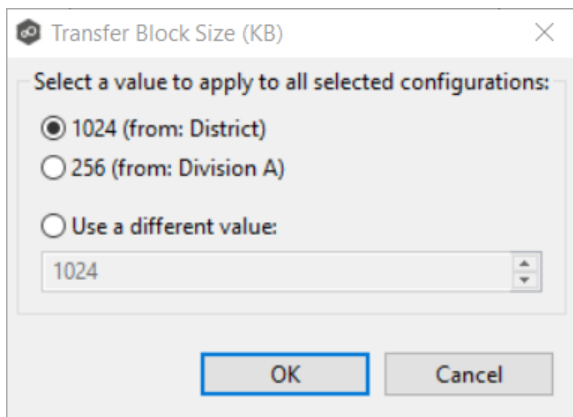
Require All Hosts At Start: ☐

Auto Start: ☒

OK Cancel

In this dialog, any discrepancies between multiple selected jobs will generally be illustrated by a read-only text field with the caption **Multiple Values - Click to Edit**. Clicking this field will bring up a dialog similar to the following:





This dialog gives you the option of choosing a value that is already used by one or more selected File Collaboration jobs, in addition to the ability to use your own value. Notice that variances in the look and feel of this pop-up dialog above depend on the type of information it is trying to represent (for example, text vs. a checkbox vs. a list of items).

Upon clicking **OK**, the read-only text field you originally clicked will be updated to reflect the new value. Any fields that have changed will be marked by a small caution sign. On saving in this multi-job edit dialog, the changed values will be applied to all selected jobs.

**Note:** Read all information on each configuration page carefully when using the multi-job edit dialog. A few pages operate in a slightly different manner than mentioned above. All the necessary information is provided at the top of these pages in bold text.

## Running and Managing a File Collaboration Job

The topics in this section provide some basic information about starting, stopping, and managing File Collaboration jobs:

- [Overview](#)
- [Starting a File Collaboration Job](#)
- [Stopping a File Collaboration Job](#)
- [Auto-Restarting a File Collaboration Job](#)
- [Host Connectivity Issues](#)
- [Removing a File from Quarantine](#)
- [Manual Retries](#)

## Overview

This topic describes:

- The [initialization process](#) for a File Collaboration job: What occurs the first time you run a File Collaboration job.
- The [initial synchronization process](#): How files are synchronized the first time you run a File Collaboration job.

The initialization process for a File Collaboration job consists of the following steps:

1. All participating hosts are contacted to make sure they are online and properly configured.
2. [Real-time event detection](#) is initialized on all participating hosts where file locks and changes will be propagated in real-time to all participating hosts. You can view real-time activity and history via the various [Runtime Job views](#) for the open job.
3. The [initial synchronization process](#) is started; all the configured root folders on the participating hosts are scanned in the background, and a listing of all folders and files are sent back to the running job.
4. The background directory scan results are analyzed, and directory structures compared to see which files are missing from which hosts. In addition, file conflict resolution is performed to decide which copy to use as the master for any detected file conflicts based on the [File Conflict Resolution](#) settings.
5. After the analysis is performed, all files that need to be synchronized are copied to the pertinent host(s).

Before you start a File Collaboration job for the first time, you need to decide how you would like the [initial synchronization](#) to be performed.

During the initial synchronization process:

- The watch set is recursively scanned on all participating hosts.
- File conflict resolution is performed.
- Any files that require updating are synchronized with the most current copy of the file.

The two primary options are:

- Have the File Collaboration job perform the initial synchronization based on the [Conflict Resolution](#) settings.
- [Pre-seed](#) all [participating hosts](#) with the correct folder and file hierarchy for the configured root folders before starting the session.

If you have a large data set, we strongly recommend that you perform the initial synchronization manually by copying the data from a host with the most current copy to all other participating hosts. This needs to be done only once--before the first time that you run the File Collaboration job.

If you choose the first option, click the **Start** button to begin [collaboration session initialization](#). Otherwise, pre-seed each participating host with the necessary data, then click the **Start** button.

### Starting a File Collaboration Job

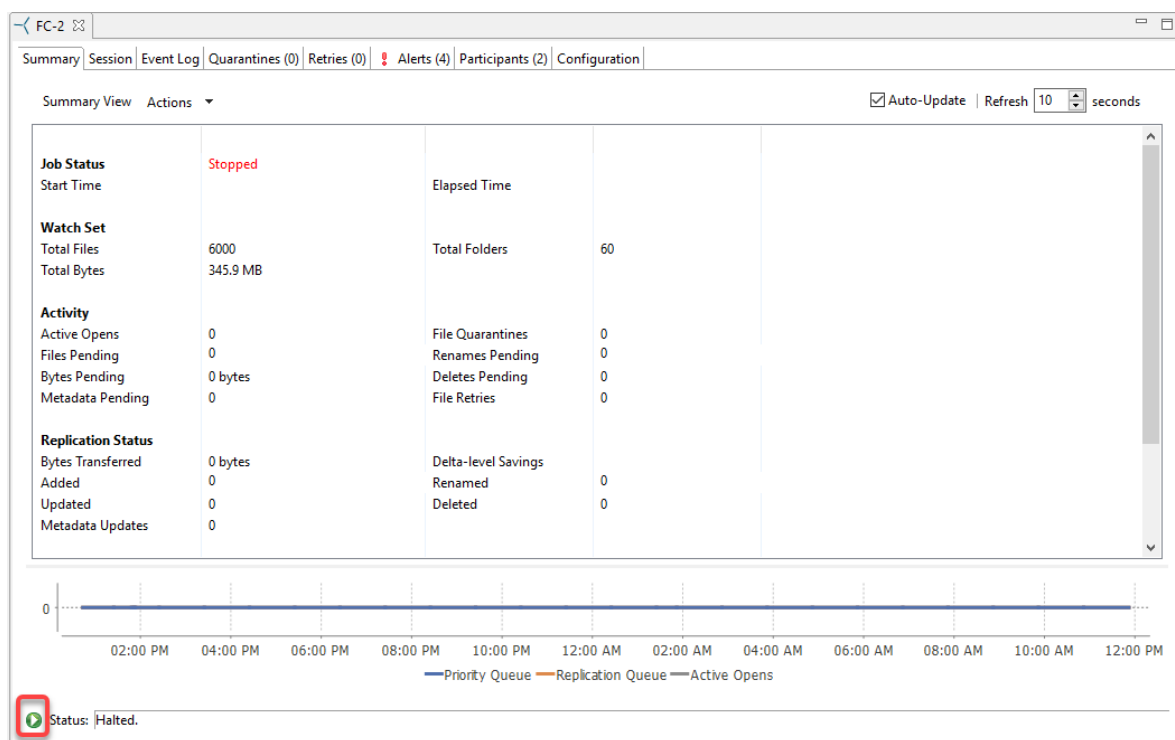
Before starting a File Collaboration job for the first time, make sure that you have decided how you want the [initial synchronization](#) to be performed.

When running a File Collaboration job for the first time, you must manually start it. After the initial run, a job will automatically start, even when the Peer Management Center server is rebooted.

**Note:** You cannot run two jobs concurrently on the same volume if the [watch sets](#) contain an overlapping set of files and folders.

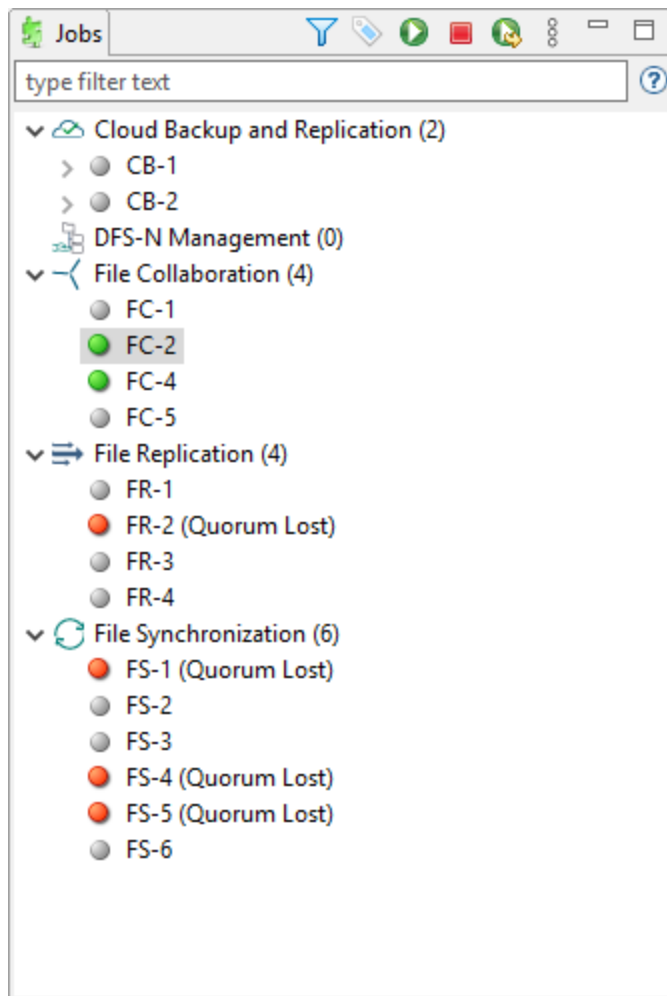
To manually start a job:

1. Choose one of three options:
  - Right-click the job name in the **Jobs** view.
  - Right-click the job name in the **Summary** tab of the **Collab, Sync, and Repl Summary** summary view, and then choose **Start** from the context menu.
  - Open a job and then click the **Start/Stop** button to the left of the **Status** field in the bottom left corner of the job's runtime view (shown below).



2. Click **Yes** in the confirmation dialog.

After the job initialization has completed, the job will run. Once the job starts, the icon next to the job name in the **Jobs** view changes from gray to green.



### Stopping a File Collaboration Job

You can stop a File Collaboration job at any time by selecting the job in the **Jobs** view and clicking the **Stop** button. Doing this shuts down the real-time file event detection and close all running operations (e.g., file transfers).

### Auto-Restarting a File Collaboration Job

Peer Management Center includes support for automatically restarting File Collaboration jobs that include [participating hosts](#) that have been disconnected, have reconnected, and are once again available.

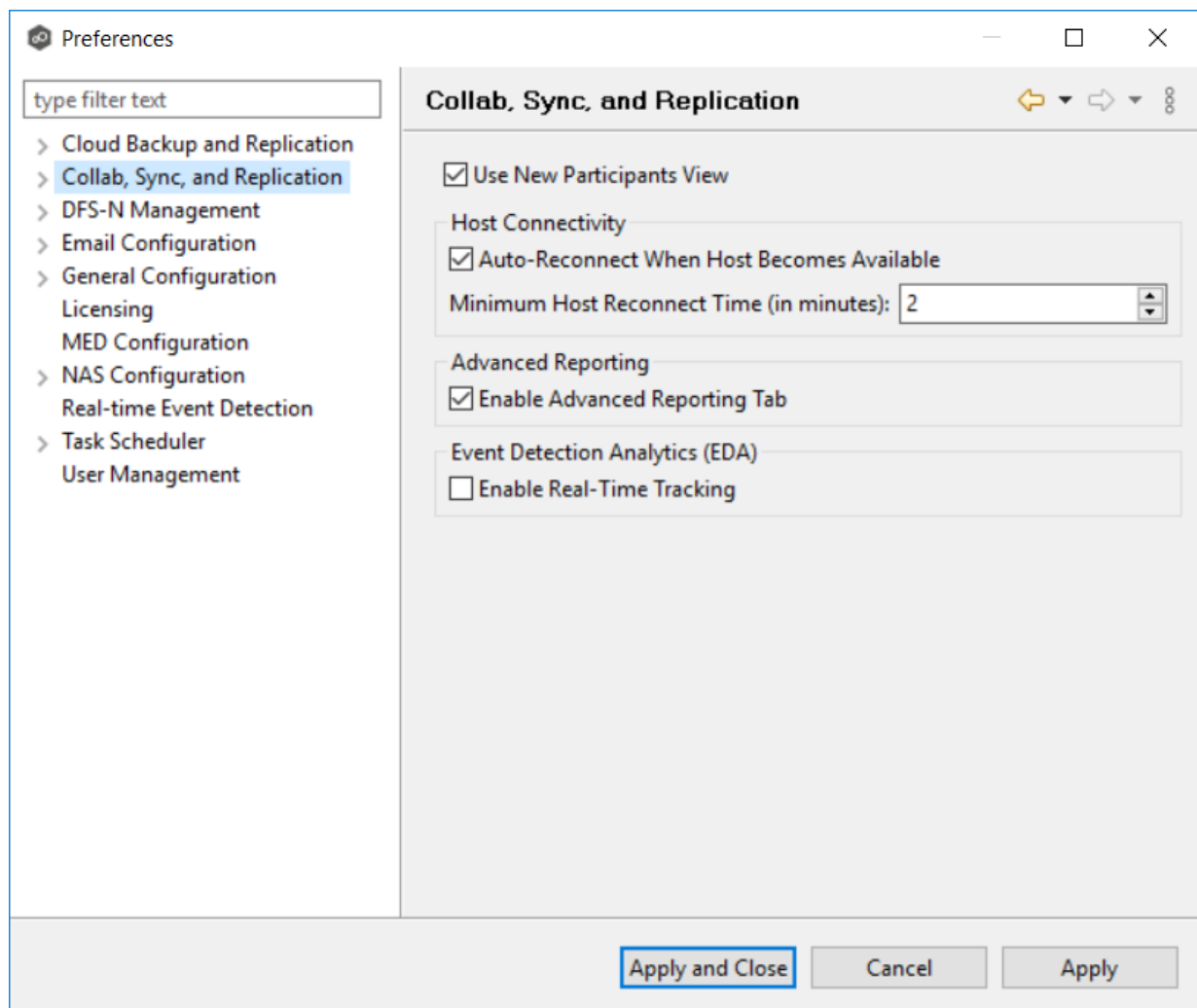
After a host becomes unavailable and the [quorum](#) is lost on a running File Collaboration job, the job automatically stops running and enters a pending state, waiting for one or more hosts to become available again so that the quorum can be met. Once the quorum is met, the pending job will automatically be restarted, beginning with a scan of all root folders.

In a job where a host becomes unavailable but quorum is not lost, the remaining hosts will continue collaborating. If the unavailable host becomes available once again, it is brought back into the running job and a background scan begins on all participating hosts, similar in fashion to the initial background scan at the start of a job.

You can enable all File Collaboration jobs to auto-restart. You can also disable auto-restart File Collaboration jobs on a per-job and per-host instance. For more information on disabling auto-restart at the job level, see [Participants Tab](#).

To enable all File Collaboration jobs to auto-restart:

1. Select **Preferences** from the **Window** menu.
2. Select **Collab, Sync, and Repl Summary** in the navigation tree.



3. Select the **Auto Reconnect when Host Becomes Available** checkbox.
4. Enter the minimum number of minutes to wait after an Agent reconnects before re-enabling it in any associated jobs in the **Minimum Host Reconnect Time** field.
5. Click **OK**.

### Host Connectivity Issues

Peer Management Center is designed to be run in an environment where all [participating hosts](#) are highly available and on highly available networks. The two primary connectivity issues result from:

- [Unavailable Hosts](#)

- [Quorum Not Met](#)

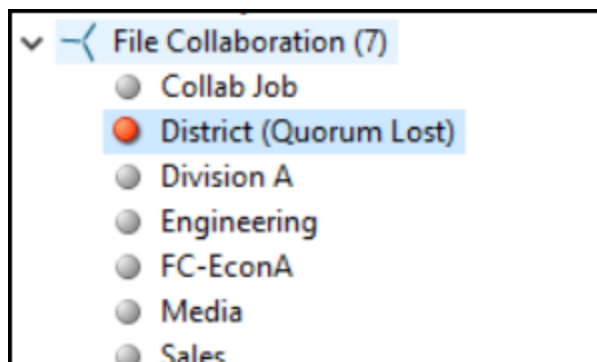
## Unavailable Hosts

If a host becomes unavailable while a File Collaboration job is running and is unreachable within the configured timeout period (specified in the job's [General settings](#)), it may be removed from collaboration. If no response is received while performing a file collaboration operation within the timeout period, Peer Management Center pings the host; if still no response, the host is taken out of the running session, a FATAL event is logged, and the [Participants tab](#) for the job is updated to indicate that the host has failed. In addition, if [email alerts](#) and/or [SNMP notifications](#) are configured and enabled for **Host Timeouts**, then the appropriate message(s) are sent.

If [auto-restart](#) not enabled, you must stop and start the File Collaboration job to bring any failed hosts back into the session. As a result, all root folders on all hosts will need to be scanned again to detect any inconsistencies. Therefore, if you are operating over a WAN with low bandwidth, you will want to set the timeout to a higher value on each related job.

## Quorum Not Met

For a File Collaboration job to run correctly, a quorum of available hosts must be met. When a quorum is lost, a message appears after the job name in the **Jobs** view.



Quorum is currently set to at least two hosts, and if quorum is not met, then the collaboration session is automatically terminated. If [email alerts](#) and/or [SNMP notifications](#) are configured and enabled for **Session Aborts**, then the appropriate message(s) are sent.

## Removing a File from Quarantine

Quarantines are a key feature of Peer Global File Service, used for resolving version conflicts. For more detailed information on how quarantines work, see [Conflicts, Retries, and Quarantines](#) in the [Advanced Topics](#) section.



You must explicitly remove a file from quarantine in order to have it participate in the collaboration session once again.

You may also choose to perform no action, in which case, the file is removed from the **Quarantines** table but none of the file versions are modified; therefore if the files are not currently in-sync, then the next time the file is modified, changes will be propagated to the other hosts. If an error occurs while removing the quarantine, then the **Status** field in the **Quarantines** table is updated to reflect the error.

To remove a file (or multiple files) from quarantine:

1. Open the job.
2. Open the [Quarantines tab](#) in the **Runtime Summaries** view.
3. Select the file(s) in the **Quarantines** table.
4. Select the host with the correct version.
5. Click the **Release Conflict** button.

After doing this, all hosts are checked to make sure the file is not currently locked by anyone. If no locks are found, then locks are obtained on all versions of the file and the targets that are out-of-date are synchronized with the selected source host.

## Manual Retries

Retries are a key feature of Peer Global File Service, used for automatically handling errors in the collaboration environment that would have otherwise led to a quarantine. For more detailed information on how retries work, see [Conflicts, Retries, and Quarantines](#) in the [Advanced Topics](#) section.

When a file is put in the retry list, it will be automatically retried based on the settings defined in [File Retries](#) in [Preferences](#). If need be, you can also manually force the retry of a file. This can be done from the Retries list of a specific File Collaboration job.

You may also chose to perform no action, in which case, the file is removed from the Retries list but none of the file versions are modified; therefore if the files are not currently in-sync, then the next time the file is modified, changes will be propagated to the other hosts. If an error occurs while forcing the retry, then the **Status** field in the **Retries** table is updated to reflect the error.

To manually force the retry of a file (or multiple files):

1. Select the file(s) in the **Retries** list.

2. Select the host with the correct version.
3. Click the **Release Conflict** button.

After doing this, all hosts are checked to make sure the file is not currently locked by anyone. If no locks are found, then locks are obtained on all versions of the file and the targets that are out-of-date are synchronized with the selected source host.

## File Replication Jobs

This section provides information about creating a File Replication job.

- [Overview](#)
- [Before You Create Your First File Replication Job](#)
- [Creating a File Replication Job](#)

### Overview

A File Replication job is designed to push files one way from a single file server (known as the source) to another single file server (known as the destination or target). This job type requires two Agents, although only the Agent at the source location will register with its local storage platform for real-time activity. The destination Agent will simply act as a relay to the destination file server.

### Before You Create Your First File Replication Job

We strongly recommend that you configure global settings such as SMTP configuration and email alerts before configuring your first File Replication job. See [Preferences](#) for details on what and how to configure these settings.

## Creating a File Replication Job

The **Create Job Wizard** walks you through the process of creating a File Replication job:

[Step 1: Job Type and Name](#)

[Step 2: Source Platform](#)

[Step 3: Source Agent](#)

[Step 4: Storage Information](#)

[Step 5: Source Path](#)

[Step 6: Destination Agent](#)

[Step 7: Destination Path](#)

[Step 8: File Metadata](#)

[Step 9: Email Alerts](#)

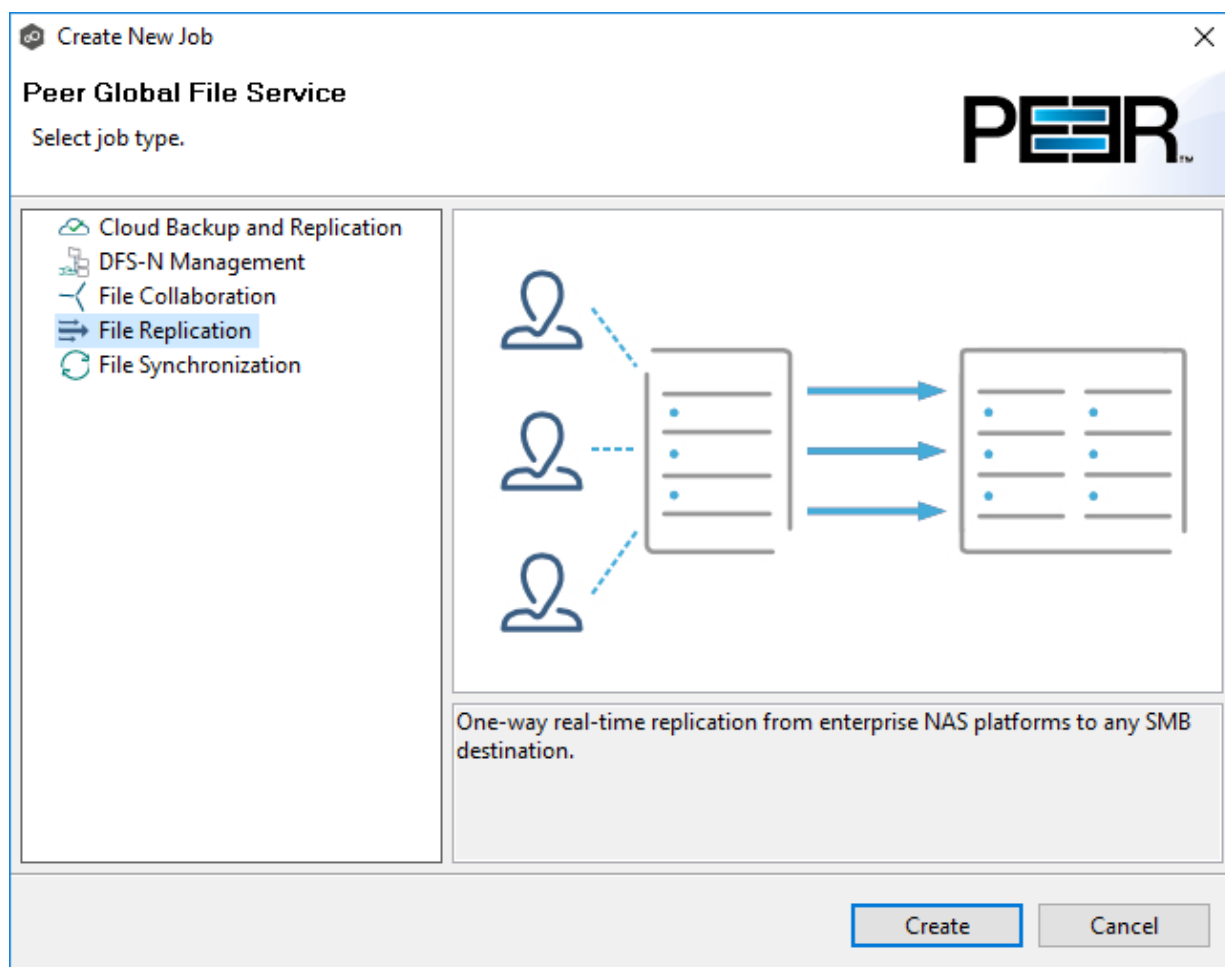
[Step 10: Save Job](#)

### Step 1: Job Type and Name

1. Open Peer Management Center.
2. From the **File** menu, select **New Job** (or click the **New Job** button on the toolbar).

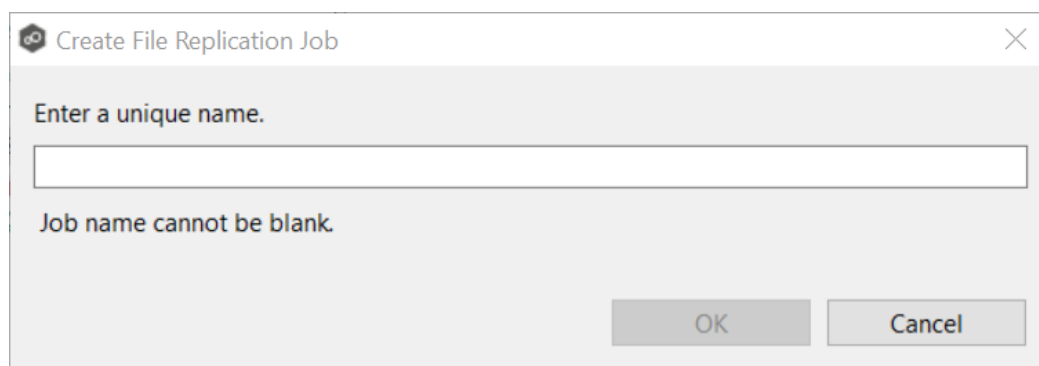
The **Create New Job** wizard displays a list of job types you can create.

3. Click **File Replication**, and then click **Create**.



4. Enter a name for the job in the dialog that appears.

The job name must be unique.



5. Click **OK**.

The [Storage Platform](#) page is displayed.

## Step 2: Storage Platform

The **Storage Platform** page lists the types of source storage platforms that File Replication supports. The source storage device hosts the data you want to replicate.

1. Select the type of storage platform you want to replicate.

Create File Replication Job Wizard

**Storage Platform**

Select the type of storage platform.

**Storage Platform**

Source Agent

Source Path

Destination Agent

Destination Path

File Metadata

Email Alerts

☒ Windows File Server

☐ NetApp ONTAP | Clustered Data ONTAP

☐ NetApp Data ONTAP 7-Mode

☐ EMC Dell EMC Isilon

☐ EMC Dell EMC Unity

☐ EMC Dell EMC Celerra | VNX | VNX 2

☐ Nutanix Files

< Back   Next >   Cancel

2. Click **Next**.

The [Source Agent](#) page is displayed.

## Step 3: Source Agent

The **Source Agent** page lists available Agents. You can have more than one Agent managing a storage device—however, the Agents must be managing different volumes/shares/folders. You should select the Agent that manages the volumes/shares/folders you want to replicate in this job.

1. Select the Source Agent for the volume/share/folder you want replicated.

Create File Replication Job Wizard

Source Agent

Select the server hosting the Peer Agent that manages the source.

Storage Platform

Source Agent

Storage Information

Source Path

Destination Agent

Destination Path

File Metadata

Email Alerts

Host	Computer Description
DGAgent1	
DGAgent2	

< Back

Next >

Cancel

2. Click **Next**.

The [Storage Information](#) page is displayed if you selected any storage platform other than Windows. If you selected Windows, skip to the [Source Path](#) page.

### Step 4: Storage Information

If you selected any storage platform other than Windows File Server in [Step 2](#), the **Storage Information** page appears. It requests the credentials necessary to connect to the storage device you want to replicate.

If you selected **Windows File Server**, skip to [Step 5: Source Paths](#).

1. Select **New Credentials** or **Existing Credentials**.
2. If you selected **Existing Credentials**, select a credential from the drop-down list, and then click **Next**. Continue with [Step 5. Source Paths](#).

If you selected **New Credentials**, enter the credentials for connecting to the storage platform. The information you are prompted to enter varies, depending on the type of storage platform:

[NetApp ONTAP | Clustered Data ONTAP](#)

[NetApp Data ONTAP 7-Mode](#)

[Dell EMC Isilon](#)

[Dell EMC Unity](#)

[Dell EMC Celerra | VNX | VNX 2](#)

[Nutanix Files](#)

3. Click **Validate** to test the credentials, and then click **OK** in the confirmation message that appears.
4. Click **Next**.

The [Source Path](#) page is displayed.

1. Enter the credentials to connect to the Storage Virtual Machine hosting the data to be replicated or select existing credentials.

Create File Replication Job Wizard

### Storage Information

Enter the information required to connect to the storage device.

Storage Platform  
Source Agent  
**Storage Information**  
Source Path  
Destination Agent  
Destination Path  
File Metadata  
Email Alerts

**Credentials**

☒ New Credentials

\*SVM Name:

\*SVM User Name:

\*SVM Password:

SVM Management IP:

\*Peer Agent IP:

☐ Existing Credentials

SVM9X-1, user:vsadmin

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp ONTAP/cDOT environments.

<b>SVM Name</b>	Enter the name of the Storage Virtual Machine hosting the data to be replicated.
<b>SVM Username</b>	Enter the user name for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Password</b>	Enter the password for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Management IP</b>	Enter the IP address used to access the management API of the NetApp Storage Virtual Machine. If the data LIFs (Logical Interfaces) corresponding to the SVM Name above already allow management access, this field is not required.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Storage Virtual Machine. The Storage Virtual Machine must be able to route traffic to this IP address. The Storage Virtual Machine must be able to



route traffic to this IP address. If the IP address you want does not appear, manually enter the address.

2. Click **Validate**.
3. Click **Next**.

The [Source Path](#) page is displayed.

1. Enter the credentials to connect to the NetApp 7-Mode filer or vFiler hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Create File Replication Job Wizard" with standard window controls. The "Storage Information" step is active, with a sidebar on the left listing steps: Storage Platform, Source Agent, Storage Information (highlighted), Source Path, Destination Agent, Destination Path, File Metadata, and Email Alerts. The main area contains the instruction "Enter the information required to connect to the storage device." and a "Credentials" section. Under "Credentials", the "New Credentials" radio button is selected. Below it is a text field labeled "\*Filer Name:" and an "Advanced" button. The "Existing Credentials" radio button is unselected, with a dropdown menu below it. A "Validate" button is at the bottom left of the main area. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel". A note at the bottom of the main area reads: "Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp 7-Mode environments."

<b>Filer Name</b>	Enter the name of the NetApp 7-Mode filer or vFiler hosting the data to be replicated.
-------------------	--

2. Click **Validate**.
3. Click **Next**.

The [Source Path](#) page is displayed.

1. Enter the credentials to connect to the EMC Isilon cluster hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Create File Replication Job Wizard" with standard window controls. The "Storage Information" step is active, with a sidebar on the left listing steps: Storage Platform, Source Agent, Storage Information (highlighted), Source Path, Destination Agent, Destination Path, File Metadata, and Email Alerts. The main area contains the instruction "Enter the information required to connect to the storage device." Below this, there are two sections for "Credentials". The "New Credentials" section is selected with a radio button and includes fields for \*Cluster Name, \*Cluster Username, \*Cluster Password, Cluster Management IP, and Nodes. An "Advanced" button is to the right of the Nodes field. The "Existing Credentials" section is unselected and shows a dropdown menu. A "Validate" button is located below the credentials sections. At the bottom of the window, there are navigation buttons: "< Back", "Next >", and "Cancel". A note at the bottom states: "Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Isilon environments."

<b>Cluster Name</b>	Enter the name of the EMC Isilon cluster hosting the data to be replicated.
---------------------	---

<b>Cluster Username</b>	Enter the user name for the account managing the EMC Isilon cluster.
<b>Cluster Password</b>	Enter the password for account managing the EMC Isilon cluster.
<b>Cluster Management IP</b>	Enter the IP address of the system used to manage the EMC Isilon cluster. Required only if multiple Access Zones are in use on the cluster.
<b>Nodes</b>	For each node in the Isilon cluster, enter an IP address that can be reached by the Agent. Separate multiple values with a comma.

2. Click **Validate**.
3. Click **Next**.

The [Source Path](#) page is displayed.

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.

Create File Replication Job Wizard

### Storage Information

Enter the information required to connect to the storage device.

Storage Platform  
Source Agent  
**Storage Information**  
Source Path  
Destination Agent  
Destination Path  
File Metadata  
Email Alerts

**Credentials**

☒ New Credentials

\*CIFS Server Name:

\*Unisphere Username:

\*Unisphere Password:

\*Unisphere Management IP:

☐ Existing Credentials

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Unity environments.

<b>CIFS Server Name</b>	Enter the name of the CIFS server hosting the data to be replicated.
<b>Unisphere Username</b>	Enter the user name for the Unisphere account managing the Unity storage device.
<b>Unisphere Password</b>	Enter the password for the Unisphere account managing the Unity storage device.
<b>Unisphere Management IP</b>	Enter the IP address of the Unisphere system used to manage the Unity storage device. This should not point to the NAS server.

- Click **Validate**.
- Click **Next**.

The [Source Path](#) page is displayed.

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Create File Replication Job Wizard" with standard window controls (minimize, maximize, close). The "Storage Information" step is active, with a sub-header "Enter the information required to connect to the storage device." A left-hand navigation pane lists steps: "Storage Platform", "Source Agent", "Storage Information" (highlighted), "Source Path", "Destination Agent", "Destination Path", "File Metadata", and "Email Alerts". The main area is titled "Credentials" and has two radio button options: "New Credentials" (selected) and "Existing Credentials". Under "New Credentials", there are four text input fields labeled "\*CIFS Server Name:", "\*Control Station Username:", "\*Control Station Password:", and "\*Control Station IP:". An "Advanced" button is to the right of the IP field. Below the "Existing Credentials" option is a dropdown menu. A "Validate" button is at the bottom left of the main area. A note at the bottom states: "Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC VNX/Celerra environments." At the very bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

<b>CIFS Server Name</b>	Enter the name of the CIFS Server hosting the data to be replicated.
<b>Control Station Username</b>	Enter the user name for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station Password</b>	Enter the password for the Control Station account managing the Celerra/VNX storage device.

<b>Control Station IP</b>	Enter the IP address of the Control Station system used to manage the Celerra/VNX storage device. This should not point to the CIFS Server.
---------------------------	---

2. Click **Validate**.
3. Click **Next**.

The [Source Path](#) page is displayed.

1. Enter the credentials to connect to the Nutanix Files cluster hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Create File Replication Job Wizard" with a sidebar on the left containing the following items: Storage Platform, Source Agent, Storage Information (highlighted), Source Path, Destination Agent, Destination Path, File Metadata, and Email Alerts. The main area is titled "Storage Information" with the instruction "Enter the information required to connect to the storage device." It features a "Credentials" section with two radio buttons: "New Credentials" (selected) and "Existing Credentials". Under "New Credentials", there are input fields for "\*Nutanix File Server Name:", "\*Username:", "\*Password:", and "\*Peer Agent IP:" (a dropdown menu). An "Advanced" button is to the right of the "\*Peer Agent IP:" field. Under "Existing Credentials", there is a dropdown menu showing "AFS2, user:admin". A "Validate" button is at the bottom left of the main area. Below the "Validate" button is a note: "Having trouble connecting? Please verify that all [prerequisites](#) are met for Nutanix Files environments." At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

<b>Nutanix File</b>	Enter the name of the Nutanix Files cluster hosting the data to be replicated.
---------------------	--

<b>Server Name</b>	
<b>Username</b>	Enter the user name for the account managing the Nutanix Files cluster via its management APIs.
<b>Password</b>	Enter the password for the account managing the Nutanix Files cluster via its management APIs.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Nutanix Files cluster. The Files cluster must be able to route traffic to this IP address. If the IP address you want does not appear, manually enter the address. This should not point to the Files cluster itself.

2. Click **Validate**.
3. Click **Next**.

The [Source Path](#) page is displayed.

#### Step 5: Source Path

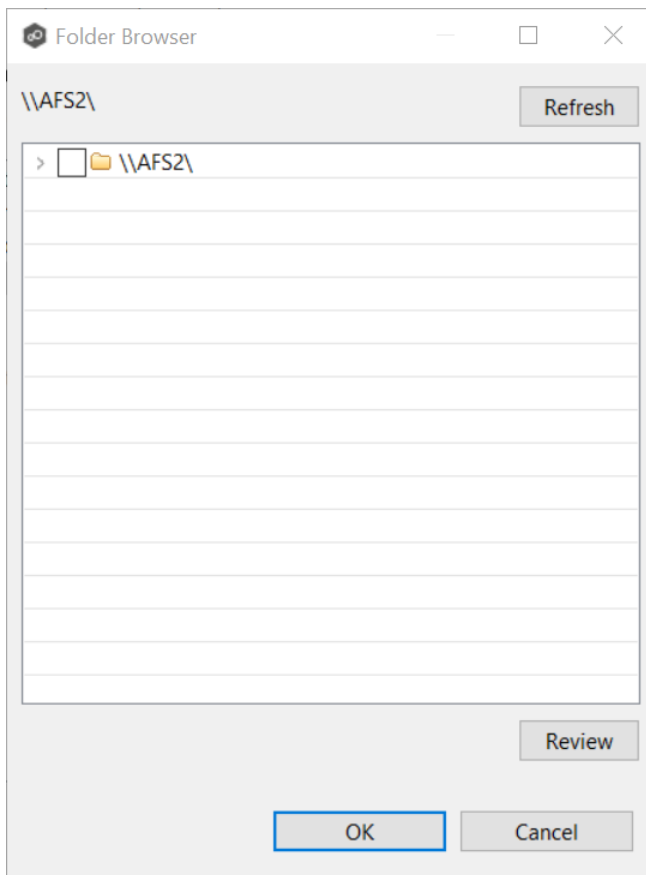
The **Source Path** page is where you specify the path to the volume/share/folder you want to replicate. This volume/share/folder is referred to as the [watch set](#). The watch set can contain a single volume/share/folder. If you want to replicate multiple volumes/shares/folders, you need to create a separate job for each one.

1. Browse to or enter the path to the watch set.

The screenshot shows a window titled "Create File Replication Job Wizard" with standard Windows window controls (minimize, maximize, close). The main heading is "Source Path", followed by the instruction "Browse to or enter a path on the storage device." On the left is a vertical list of steps: "Storage Platform", "Source Agent", "Storage Information", "Source Path" (which is highlighted with a grey background), "Destination Agent", "Destination Path", "File Metadata", and "Email Alerts". The main area of the wizard contains a text input field with the placeholder text "\\AFS2\ Enter Path" and a "Browse" button to its right. At the bottom of the wizard are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

If you selected **Browse**, the **Folder Browser** dialog appears:





- a. Expand the folder tree.
  - b. Select the appropriate volume/share/folder.
  - c. (Optional) Click the **Review** button to see your selection.
  - d. Click **OK**.
2. Click **Next**.

The [Destination Agent](#) page is displayed.

#### Step 6: Destination Agent

The **Destination Agent** page lists available Agents, not including the Agent used as the Source Agent. This Destination Agent will be responsible for writing files and metadata to the destination storage device. No credentials are required for this Agent as it will not be monitoring anything in real-time.

- [illegible]

2. Click **Next**.

The [Destination Path](#) page is displayed.

The **Destination Path** page is where you specify the volume/share/folder that you want to replicate to. If the destination storage device is a Windows file server, this path should be a local path such as D:\Data. This path can also be the UNC path to any SMB-capable file server.

- Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.

- If you enter the start of a UNC path and click **Browse**, the **Folder Browser** dialog will attempt to present a list of the available shares on the file server specified in the path.

The screenshot shows a window titled "Create File Replication Job Wizard". The "Destination Path" step is selected in the left-hand navigation pane, which also lists "Storage Platform", "Source Agent", "Storage Information", "Source Path", "Destination Agent", "File Metadata", and "Email Alerts". The main area of the wizard has the heading "Destination Path" and the instruction "Browse to or enter a path on the storage device." Below this is a large text input field labeled "Enter Path" and a "Browse" button to its right. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

2. Click **Next**.

The [File Metadata](#) page is displayed.

## Step 8: File Metadata

This step is optional.

The **File Metadata** page allows you to specify whether you want to replicate NTFS security permissions metadata and the types of metadata to synchronize. It also allows you to specify which volume/share/folder's metadata should be used if there is a conflict during the [initial](#) synchronization. The volume/share/folder used if there is a conflict is referred to as the [master host](#).

For more information on synchronizing NTFS metadata, see [File Metadata Synchronization](#) in the [Advanced Topics](#) section.

To enable file metadata synchronization:

1. Select when you want the metadata replicated (you can select one or both options):

- **Enable synchronizing NTFS security descriptors (ACLs) in real-time** - Select this option if you want the metadata synchronized in real-time. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be transferred to the target host file(s) as they occur.
- **Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan** - Select this option if you want the metadata replicated during the initial scan. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be synchronized during the initial scan.

Create File Replication Job Wizard

**File Metadata**  
Configure the replication of NTFS security permissions.

Storage Platform  
Source Agent  
Storage Information  
Source Path  
Destination Agent  
Destination Path  
**File Metadata**  
Email Alerts

**Synchronize Security Descriptors (ACLs)**  
☐ Enable synchronizing NTFS security descriptors (ACLs) in real-time  
☐ Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan

**Synchronize Security Descriptor Options**  
☒ Owner  
☒ DACL: Discretionary Access Control List  
☐ SACL: System Access Control List

**Metadata Conflict Resolution**  
Select Master Host for initial scan:

< Back   Next >   **Finish**   Cancel

2. Click **OK** in the message that appears after selecting a metadata option.
3. If you selected either of the first two options in the **Synchronize Security Descriptor Options** section, select the security descriptor components (Owner, DACL, and SACL) to be synchronized.
4. If you selected the option for metadata synchronization during the initial scan, select the host to be used as the [master host](#) in case of file metadata conflict.

If a master host is not selected, then no metadata synchronization will be performed during the initial scan. If one or more security descriptors do not match across participants during the initial scan, [conflict resolution](#) will use permissions from the designated master host as the winner. If the file does not exist on the designated master host, a winner will be randomly picked from the other participants.

- The [Email Alerts](#) page is displayed.

This step is optional.

Peer Software recommends that you create email alerts in advance. However, from this wizard page, you can select existing alerts to apply to the job or create new alerts to apply.

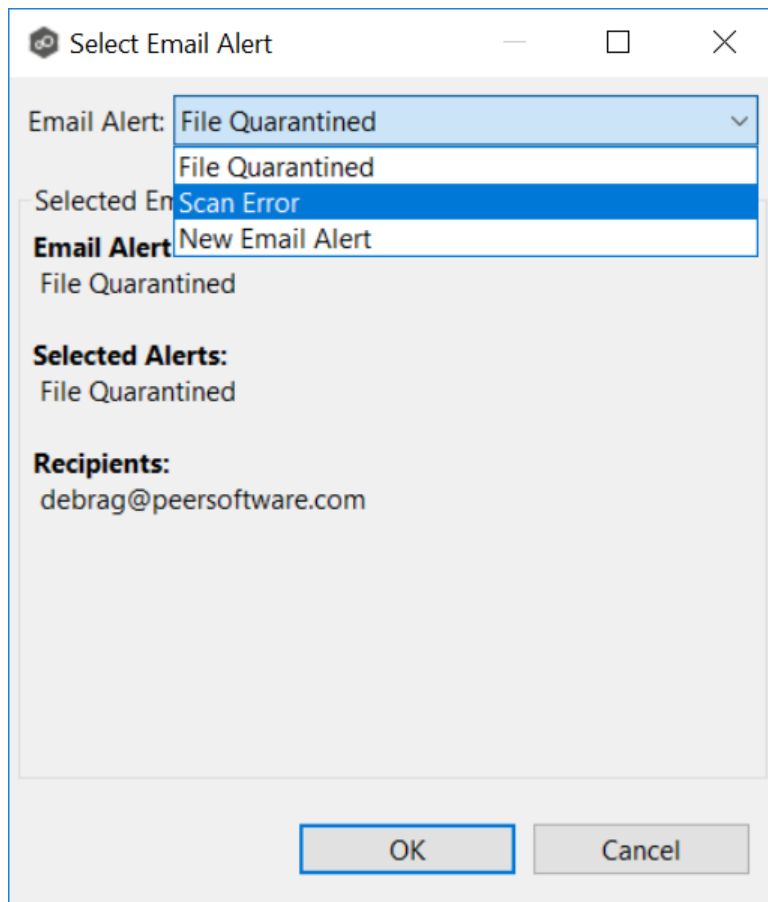
To apply an existing email alert to the job.

1. Click the **Select** button.

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.

The **Select Email Alert** dialog appears.

2. Select an alert from the **Email Alert** drop-down list.



3. Click **OK**.

The alert is listed on the **Email Alerts** page.

Create File Replication Job Wizard

Email Alerts

Select email alerts.

Storage Platform

Source Agent

Storage Information

Source Path

Destination Agent

Destination Path

File Metadata

Email Alerts

Edit Email Alerts

Name	Enabled	Event Types	Recipients
File Quarantined	Yes	File Quarantined	debrag@peersoftware.c...

Select

Delete

Show Detail

< Back

Next >

Finish

Cancel

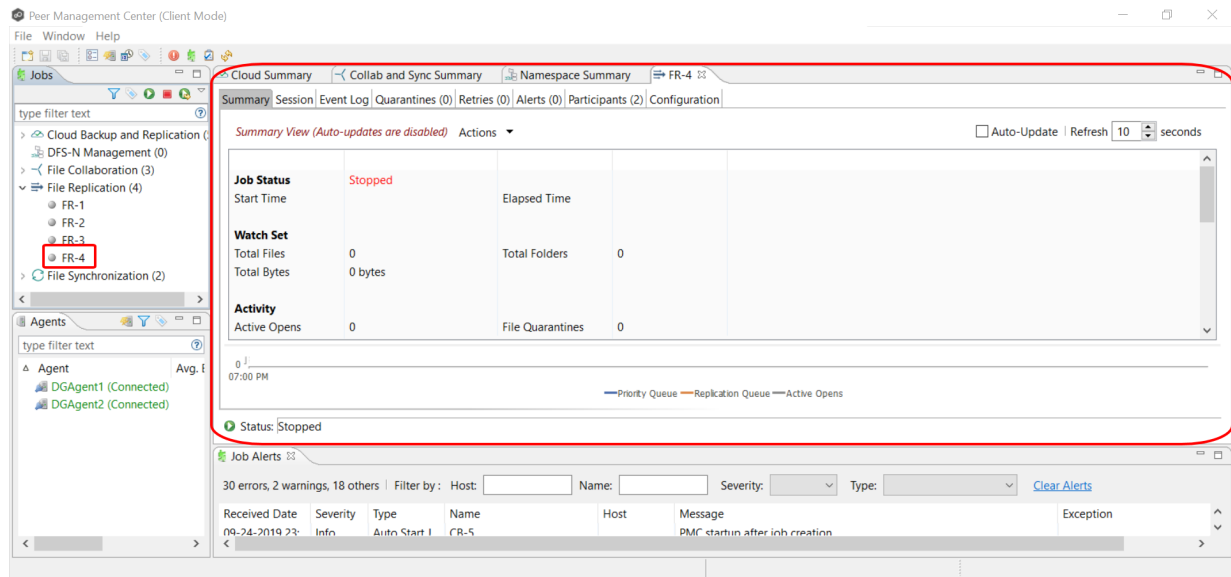
4. (Optional) Repeat steps 1-3 to apply additional alerts.
5. Continue to [Step 10: Save Job](#).

## Step 10: Save Job

Now that you have completed the first nine steps of the wizard, you are ready to save the job configuration.

1. If you are satisfied with your job configuration, click **Finish** to save your job. Otherwise, click the **Back** button and make any necessary changes.

Congratulations! You have created a File Replication job. It is now listed in the **Jobs** view under **File Replication** and a job run-time view appears in the **Runtime Summaries** area. You can start the job from either place.



## File Synchronization Jobs

This section provides information about creating a File Synchronization job:

- [Overview](#)
- [Before You Create Your First File Synchronization Job](#)
- [Creating a File Synchronization Job](#)
- [Editing a File Synchronization Job](#)
- [Running and Managing a File Synchronization Job](#)

## Overview

A File Synchronization job provides real-time, multi-directional synchronization between various storage platforms and across locations. It is designed to handle non-collaborative workloads where files still need to be kept in-sync at multiple locations in real-time without locking. This job type is specifically optimized for use with user home directories and profiles.



## Before You Create Your First File Synchronization Job

We strongly recommend that you configure global settings such as SMTP configuration and email alerts before configuring your first File Synchronization job. See [Preferences](#) for details on what and how to configure these settings.

## Creating a File Synchronization Job

The **Create Job Wizard** walks you through the process of creating a File Synchronization job:

[Step 1: Job Type and Name](#)

[Step 2: Participants](#)

[Step 3: File Metadata](#)

[Step 4: Email Alerts](#)

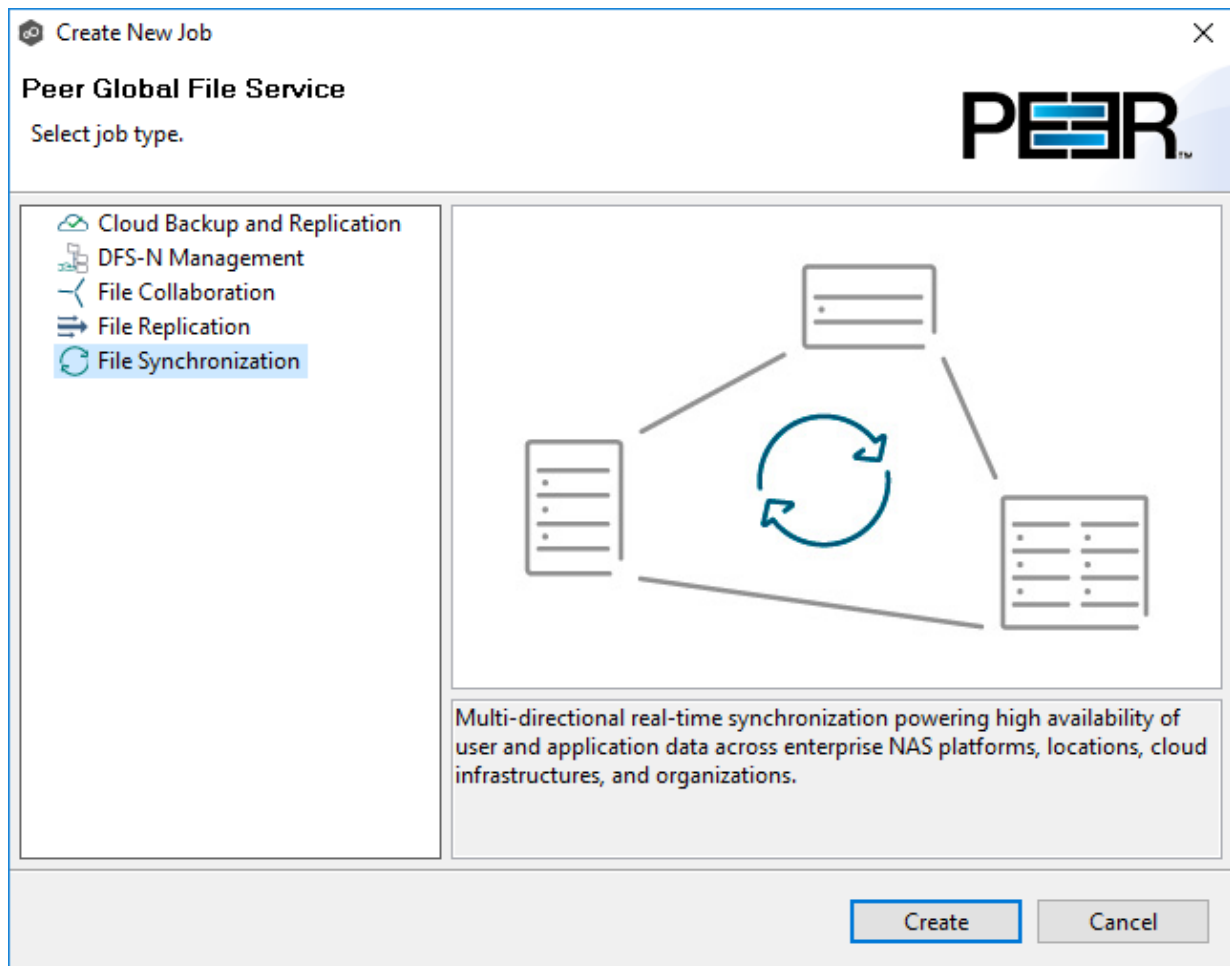
[Step 5: Save Job](#)

### Step 1: Job Type and Name

1. Open Peer Management Center.
2. From the **File** menu, select **New Job** (or click the **New Job** button on the toolbar).

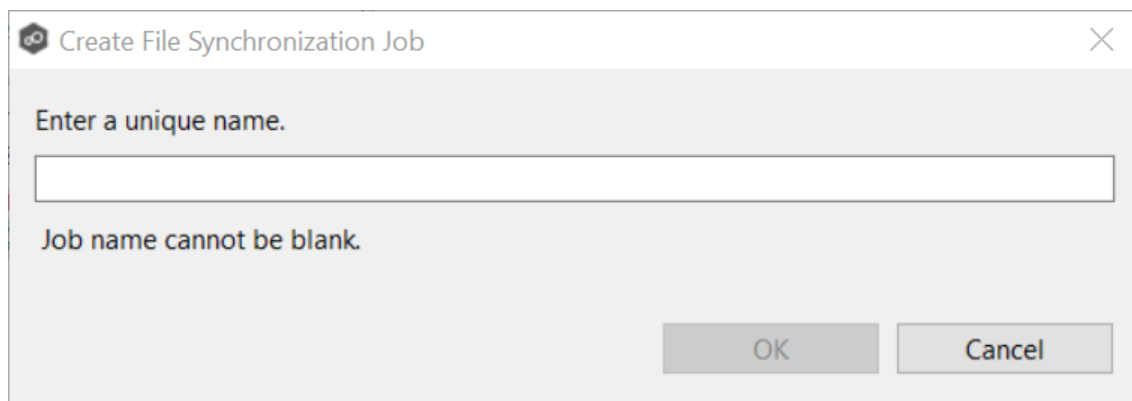
The **Create New Job** wizard displays a list of job types you can create.

3. Click **File Synchronization**, and then click **Create**.



4. Enter a name for the job in the dialog that appears.

The job name must be unique.



5. Click **OK**.

The [Participants](#) page is displayed.

## Step 2: Participants

A File Synchronization job must have two or more participants. A [participant](#) consists of an Agent and the volume/share/folder to be replicated. The server that the Agent is installed upon is called the [host](#) (or [host participant](#)). A File Synchronization job synchronizes the files of participants in real-time.

1. Complete the five substeps:

[Participants](#)

[Storage Platform](#)

[Management Agent](#)

[Storage Information](#)

[Path](#)

After you add a participant, it appears in the **Participants** table.

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\AFS1\Share1\Mar...	Yes	Nutanix Files	No
DGAgent2		C:\Users\Public\Do...	Yes	Windows	No

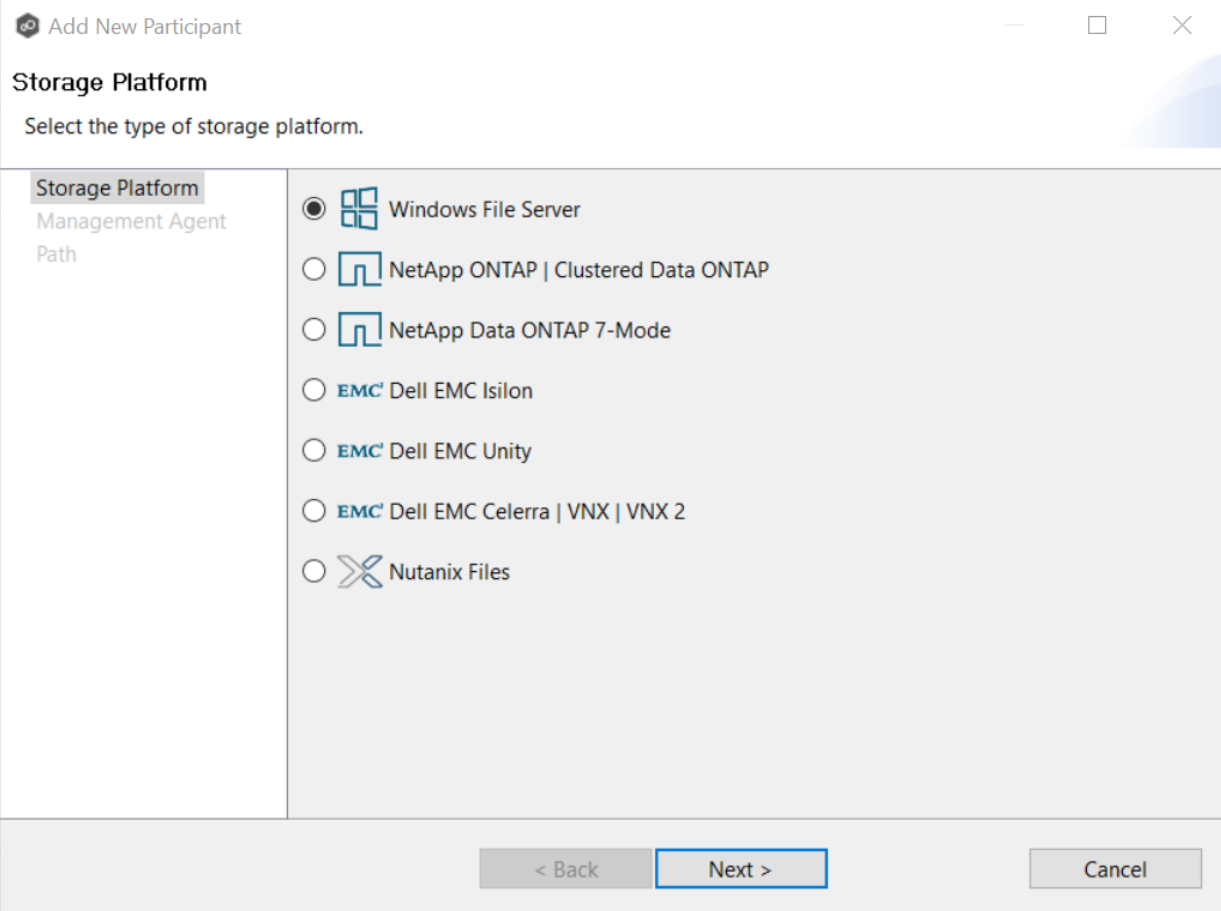
2. Repeat the five substeps for each participant you want to add to the job.
3. Once you have added all the participants, click **Next** to specify [file metadata](#) for the job. (Don't click **Finish**.)

To begin the process of adding a participant:

- [illegible]

The **Storage Platform** page lists the types of storage platforms that File Synchronization supports. A storage device hosts data you want to synchronize. It is often referred to as the [host or host participant](#).

- Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.



The screenshot shows a window titled "Add New Participant" with a close button in the top right corner. Below the title bar, the text "Storage Platform" is displayed, followed by the instruction "Select the type of storage platform." The main area of the window is divided into two sections. On the left, there is a sidebar with the heading "Storage Platform" and two sub-items, "Management Agent" and "Path". The right section contains a list of storage platform options, each with a radio button and an icon: "Windows File Server" (selected), "NetApp ONTAP | Clustered Data ONTAP", "NetApp Data ONTAP 7-Mode", "EMC Dell EMC Isilon", "EMC Dell EMC Unity", "EMC Dell EMC Celerra | VNX | VNX 2", and "Nutanix Files". At the bottom of the window, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

2. Click **Next**.

The [Management Agent](#) page is displayed.

The **Management Agent** page lists available [Agents](#). You can have more than one Agent managing a storage device—however, the Agents must be managing different volumes/shares/folders on the storage device. For your File Synchronization job, you should select the [Management Agent](#) that manages the volumes/shares/folders you want to replicate in this job.

1. Select the Agent that manages the host.

Add New Participant

Management Agent

Select the server hosting the Peer Agent that manages this storage device.

Storage Platform  
Management Agent  
Storage Information  
Path

Host	Computer Description
DGAgent1	
DGAgent2	

< BackNext >Cancel

**Tip:** If the Agent you want is not listed, try restarting the Peer Agent Windows Service on that host. If it successfully connects to the [Peer Management Broker](#), then the list is updated with that Agent.

2. Click **Next**.

The [Storage Information](#) page is displayed if you selected any storage platform other than Windows. If you selected Windows, skip to the [Path](#) page.

If you selected any storage platform type other than Windows File Server in the [Storage Platform](#) page, the **Storage Information** page appears. It requests the credentials necessary to connect to the storage device you want to replicate. If you selected Windows Files Server in the previous wizard page, skip to [Step 3: File Metadata](#).

1. Select **New Credentials** or **Existing Credentials**.

2. If you selected **Existing Credentials**, select a credential from the drop-down list, and then click **Next** to continue to the [Path](#) page.

If you selected **New Credentials**, enter the credentials for connecting to the storage device. The information you are prompted to enter varies, depending on the type of storage platform:

[NetApp ONTAP | Clustered Data ONTAP](#)

[NetApp Data ONTAP 7-Mode](#)

[Dell EMC Isilon](#)

[Dell EMC Unity](#)

[Dell EMC Celerra | VNX | VNX 2](#)

[Nutanix Files](#)

3. Click **Validate** to test the credentials.

After the credentials are validated, a success message appears.

4. Click **Next**.

The [Path](#) page is displayed.

#### NetApp ONTAP | Clustered Data ONTAP

1. Enter the credentials to connect to the Storage Virtual Machine hosting the data to be replicated or select existing credentials.

Add New Participant

Storage Information

Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

Credentials

☒ New Credentials

\*SVM Name:

\*SVM User Name:

\*SVM Password:

SVM Management IP:

\*Peer Agent IP:

Advanced

☐ Existing Credentials

SVM9X-1, user:vsadmin

Validate

Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp ONTAP/cDOT environments.

< Back
Next >
Cancel

<b>SVM Name</b>	Enter the name of the Storage Virtual Machine hosting the data to be replicated.
<b>SVM Username</b>	Enter the user name for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Password</b>	Enter the password for the account managing the Storage Virtual Machine. This must not be a cluster management account.
<b>SVM Management IP</b>	Enter the IP address used to access the management API of the NetApp Storage Virtual Machine. If the data LIFs (Logical Interfaces) corresponding to the SVM Name above already allow management access, this field is not required.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Storage Virtual Machine. The Storage Virtual Machine must be able to route traffic to this IP address. If the IP address you want does not appear, you can manually enter the address.



<b>Override Access Path</b>	Used only when experiencing access issues. Contact Peer Software support for more information.
-----------------------------	--

- Click **Validate**.
- Click **Next**.

The [Path](#) page is displayed.

### NetApp Data ONTAP 7-Mode

- Enter the credentials to connect to the NetApp 7-Mode filer or vFiler hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Add New Participant" with standard window controls (minimize, maximize, close). The "Storage Information" tab is selected in the left-hand navigation pane, which also lists "Storage Platform", "Management Agent", and "Path". The main content area of the "Storage Information" tab contains the instruction "Enter the information required to connect to the storage device." Below this, there are two radio button options under the heading "Credentials": "New Credentials" (which is selected) and "Existing Credentials". The "New Credentials" option includes a text field labeled "\*Filer Name:" and an "Advanced" button to its right. Below the "Existing Credentials" option is a list box. At the bottom of the main content area is a "Validate" button. Below the "Validate" button is a note: "Having trouble connecting? Please verify that all [prerequisites](#) are met for NetApp 7-Mode environments." At the very bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

<b>File r Na me</b>	Enter the name of the NetApp 7-Mode filer or vFiler hosting the data to be replicated.
---------------------------------	--

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Dell EMC Isilon

1. Enter the credentials to connect the EMC Isilon cluster hosting the data to be replicated or select existing credentials.

The screenshot shows a window titled "Add New Participant" with standard window controls (minimize, maximize, close). The "Storage Information" tab is selected, with a sub-header "Enter the information required to connect to the storage device." On the left is a sidebar with links: "Storage Platform", "Management Agent", "Storage Information" (highlighted), and "Path". The main area contains a "Credentials" section with two radio buttons: "New Credentials" (selected) and "Existing Credentials". Under "New Credentials", there are five text input fields labeled: "\*Cluster Name:", "\*Cluster Username:", "\*Cluster Password:", "Cluster Management IP:", and "Nodes:". An "Advanced" button is to the right of the "Nodes" field. Below the radio buttons is a dropdown menu. At the bottom left is a "Validate" button. At the bottom right is a note: "Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Isilon environments." The footer contains three buttons: "< Back", "Next >", and "Cancel".

<b>Cluster Name</b>	Enter the name of the EMC Isilon cluster hosting the data to be replicated.
<b>Cluster Username</b>	Enter the user name for the account managing the EMC Isilon cluster.
<b>Cluster Password</b>	Enter the password for account managing the EMC Isilon cluster.
<b>Cluster Management IP</b>	Enter the IP address of the system used to manage the EMC Isilon cluster. Required only if multiple Access Zones are in use on the cluster.
<b>Nodes</b>	Enter one IP from each node that the Agent can access to perform open file lookups. Use commas to separate nodes.

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Dell EMC Unity

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.

Add New Participant

Storage Information

Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
Storage Information  
Path

Credentials

☒ New Credentials

\* CIFS Server Name:

\* Unisphere Username:

\* Unisphere Password:

\* Unisphere Management IP:

Advanced

☐ Existing Credentials

Validate

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC Unity environments.

< Back
Next >
Cancel

<b>CIFS Server Name</b>	Enter the name of the CIFS server hosting the data to be replicated.
<b>Unisphere Username</b>	Enter the user name for the Unisphere account managing the Unity storage device.
<b>Unisphere Password</b>	Enter the password for the Unisphere account managing the Unity storage device.
<b>Unisphere Management IP</b>	Enter the IP address of the Unisphere system used to manage the Unity storage device. This should not point to the CIFS server.

<b>Override Access Path</b>	Used only when experiencing access issues. Contact Peer Software support for more information.
-----------------------------	--

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Dell EMC Celerra | VNX | VNX 2

1. Enter the credentials to connect to the CIFS Server hosting the data to be replicated or select existing credentials.

**Add New Participant**

**Storage Information**  
Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

**Credentials**

☒ New Credentials

\*CIFS Server Name:

\*Control Station Username:

\*Control Station Password:

\*Control Station IP:

☐ Existing Credentials

Having trouble connecting? Please verify that all [prerequisites](#) are met for EMC VNX/Celerra environments.

<b>CIFS Server Name</b>	Enter the name of the CIFS Server hosting the data to be replicated.
<b>Control Station Username</b>	Enter the user name for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station Password</b>	Enter the password for the Control Station account managing the Celerra/VNX storage device.
<b>Control Station IP</b>	Enter the IP address of the Control Station system used to manage the Celerra/VNX storage device. This should not point to the CIFS Server.

2. Click **Validate**.
3. Click **Next**.

The [Path](#) page is displayed.

#### Nutanix Files

1. Enter the credentials to connect to the Nutanix Files cluster hosting the data to be replicated or select existing credentials.

**Add New Participant**

**Storage Information**  
Enter the information required to connect to the storage device.

Storage Platform  
Management Agent  
**Storage Information**  
Path

**Credentials**  
☒ New Credentials  
\*Nutanix File Server Name:   
\*Username:   
\*Password:   
\*Peer Agent IP:   
  
☐ Existing Credentials  
AFS2, user:admin

Having trouble connecting? Please verify that all [prerequisites](#) are met for Nutanix Files environments.

<b>Nutanix File Server Name</b>	Enter the name of the Nutanix Files cluster hosting the data to be replicated.
<b>Username</b>	Enter the user name for the account managing the Nutanix Files cluster via its management APIs.
<b>Password</b>	Enter the password for the account managing the Nutanix Files cluster via its management APIs.
<b>Peer Agent IP</b>	Select the IP address of the server hosting the Agent that manages the Nutanix Files cluster. If the IP address you want does not appear, you can manually enter the address. This should not point to the Files cluster itself.

2. Click **Validate**.

3. Click **Next**.

The [Path](#) page is displayed.

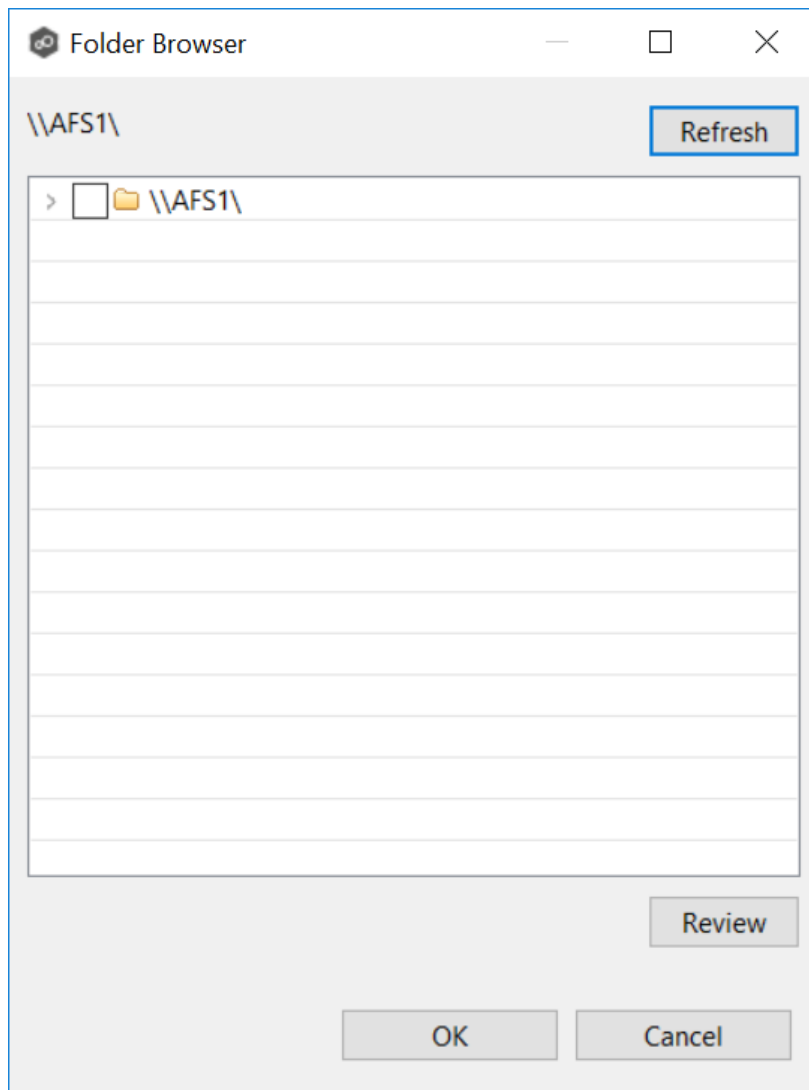
The **Path** page is where you specify the path to the volume/share/folder you want to replicate. This volume/share/folder is referred to as the [watch set](#). The watch set can contain a single volume/share/folder. If you want to replicate multiple volumes/shares/folders, you need to create a separate job for each one.

1. Browse to or enter the path to the watch set.

The screenshot shows a window titled "Add New Participant" with a close button. Inside, the "Path" page is active, with the instruction "Browse to or enter a path on the storage device." On the left, a sidebar lists "Storage Platform", "Management Agent", "Storage Information", and "Path" (which is selected). The main area contains a text input field with the placeholder text "\\AFS1\ Enter Path" and a "Browse" button to its right. Below the input field is a "Seeding Target:" label followed by an unchecked checkbox. At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish" (which is highlighted with a blue border), and "Cancel".

If you selected **Browse**, the **Folder Browser** dialog appears:

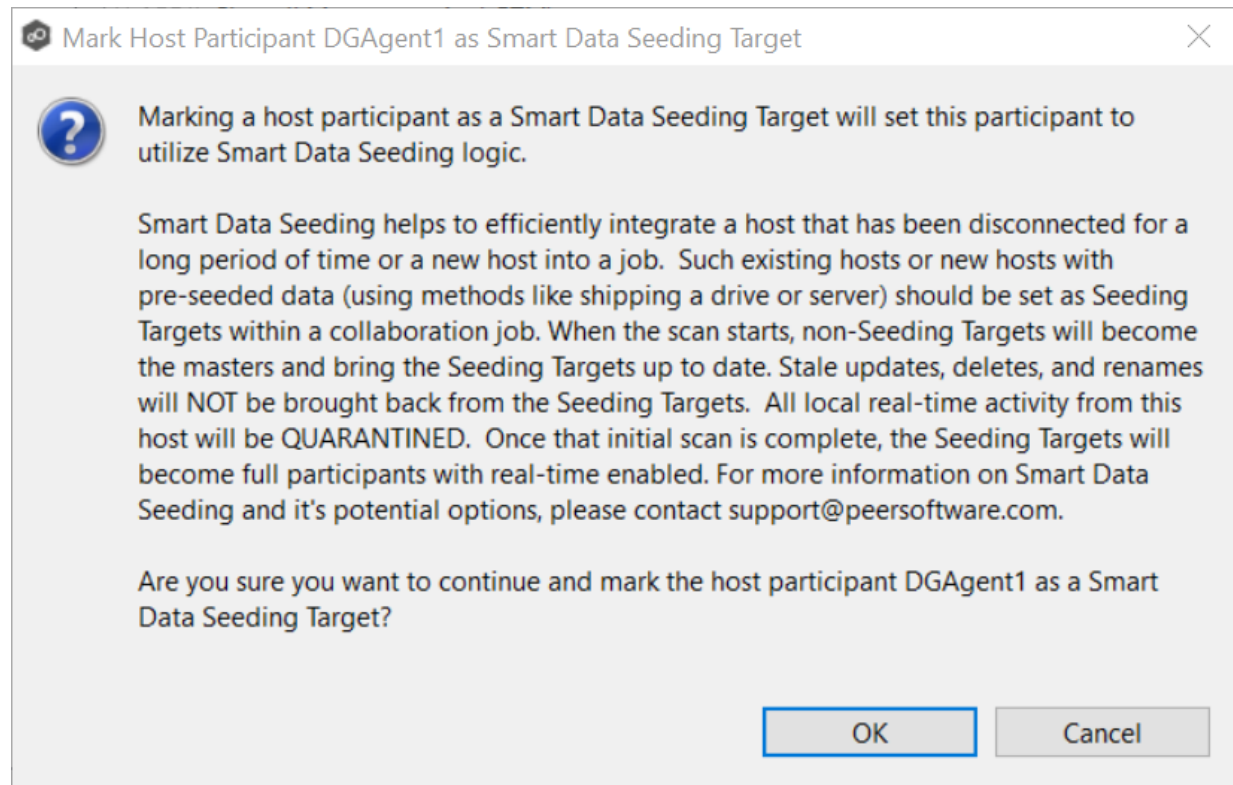




- a. Expand the folder tree.
  - b. Select the appropriate volume/share/folder.
  - c. (Optional) Click the **Review** button to see your selection.
  - d. Click **OK**.
2. (Optional) Select the **Seeding Target** checkbox, and then click **OK** in the dialog that appears.

If you select this option, a message describing seeding behavior is displayed. Multiple participants in a File Synchronization job can be set as smart data seeding targets; however, at least one participant should not be set as a smart data seeding target. This participant will be acting as the "master" source for the smart data seeding targets. For

more information about smart data seeding, see [Smart Data Seeding](#) or contact [support@peersoftware.com](mailto:support@peersoftware.com).



3. Click **Finish** to complete the wizard for this participant.
4. Return to [Step 2: Participants](#) to add more participants, if applicable. A File Synchronization job must have at least two participants. If you have added all the participants, continue with [Step 3: File Metadata](#).

### Step 3: File Metadata

This step is optional.

The **File Metadata** page allows you to specify whether you want to synchronize NTFS security permissions metadata and the types of metadata. It also allows you to specify which volume/share/folder's metadata should be used if there is a conflict during the initial synchronization. The volume/share/folder used if there is a conflict is referred to as the [master host](#).

For more information on synchronizing NTFS metadata, see [File Metadata Synchronization](#) in the [Advanced Topics](#) section.

To enable file metadata synchronization:

1. Select when you want the metadata synchronized (you can select one or both options):
  - **Enable synchronizing NTFS security descriptors (ACLs) in real-time** - Select this option if you want the metadata synchronized in real-time. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be transferred to the target host file(s) as they occur.
  - **Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan** - Select this option if you want the metadata replicated during the initial scan. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be synchronized during the initial scan.

Create File Synchronization Job Wizard

**File Metadata**  
Configure the replication of NTFS security permissions.

Participants  
File Metadata  
Email Alerts

Synchronize Security Descriptors (ACLs)

- ☐ Enable synchronizing NTFS security descriptors (ACLs) in real-time
- ☐ Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan

Synchronize Security Descriptor Options

- ☒ Owner
- ☒ DACL: Discretionary Access Control List
- ☐ SACL: System Access Control List

Metadata Conflict Resolution

Select Master Host for initial scan:

< Back Next > Finish Cancel

2. Click **OK** in the message that appears after selecting a metadata option.
3. If you selected either of the first two options in the **Synchronize Security Descriptor Options** section, select the security descriptor components (Owner, DACL, and SACL) to be synchronized.
4. If you selected the option for metadata synchronization during the initial scan, select the host to be used as the [master host](#) in case of file metadata conflict.

If a master host is not selected, then no metadata synchronization will be performed during the initial scan. If one or more security descriptors do not match across participants during the initial scan, [conflict resolution](#) will use permissions from the designated master host as

5. Click **Next**.

### Step 4: Email Alerts

An email alert notifies recipients when a certain type of event occurs, for example, session abort, host failure, or system alert. The **Email Alerts** page displays a list of email alerts that have been applied to the job. When you first create a job, this list is empty. Email alerts are defined in [Preferences](#) and can then be applied to multiple jobs of the same type.

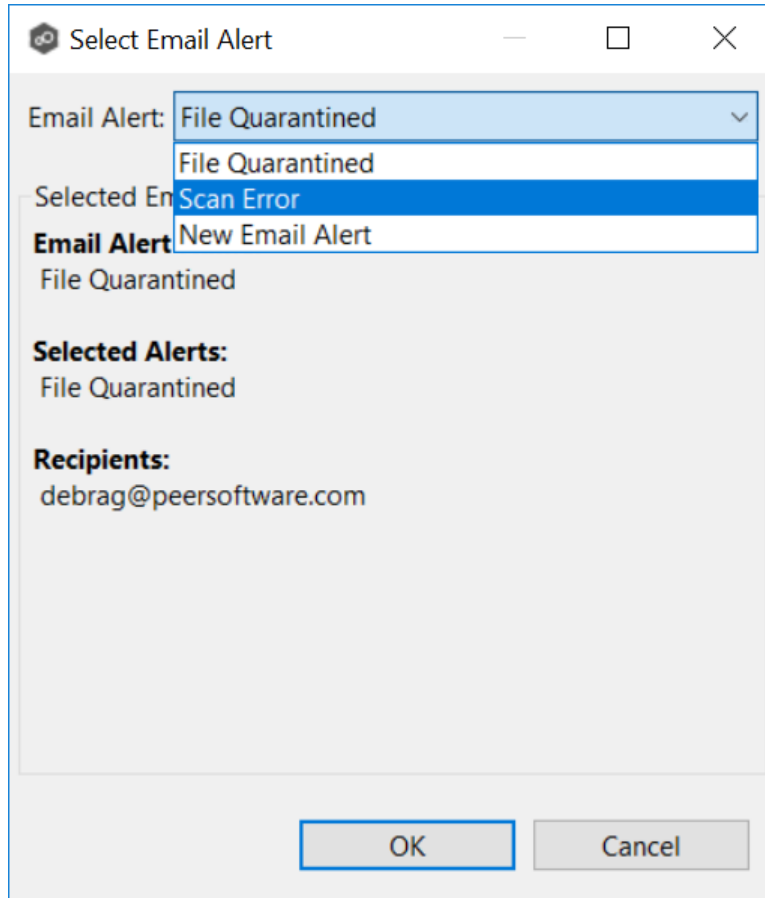
To create a new alert, see [Email Alerts](#) in the [Preferences](#) section.

1. Click the **Select** button.

Copyright (c) 1993-2021 Peer Software, Inc. All Rights Reserved.

The **Select Email Alert** dialog appears.

2. Select an alert from the **Email Alert** drop-down list.



3. Click **OK**.

The alert is listed on the **Email Alerts** page.

New File Synchronization Job

Email Alerts

Select email alerts.

Participants  
File Metadata  
**Email Alerts**

Edit Email Alerts

Name	Enabled	Event Types	Recipients
Scan Error	Yes	Scan Error, Job Started	debag@peersoftware.com

Select

Delete

View Details

< Back

Next >

Finish

Cancel

4. (Optional) Repeat steps 1-3 to apply additional alerts.
5. Continue to [Step 5: Save Job](#).

## Step 5: Save Job

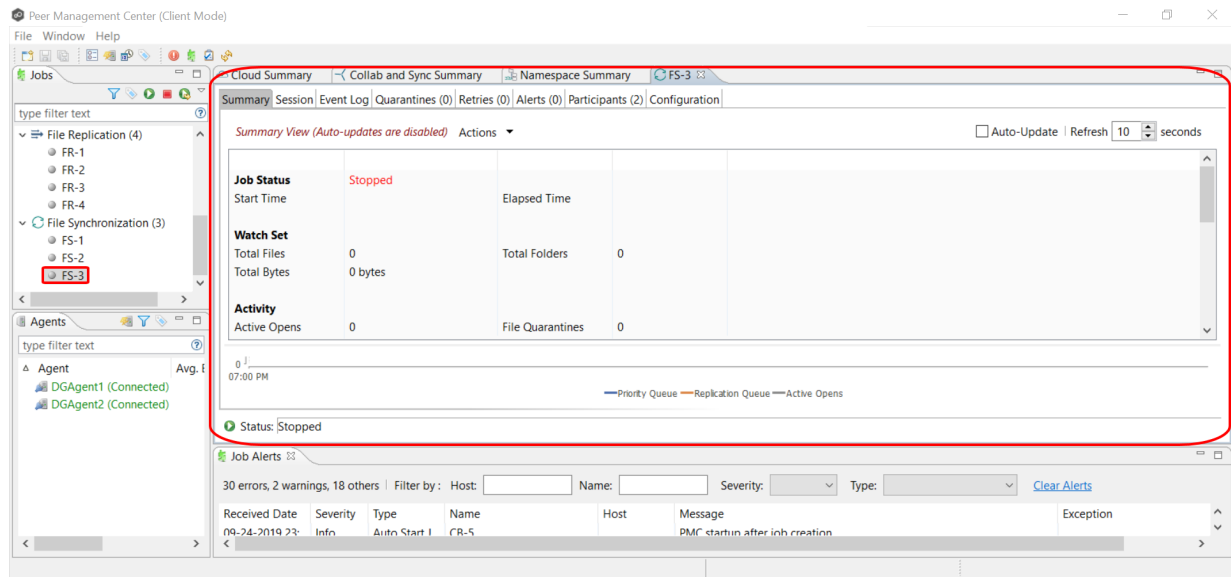
Now that you have completed the first four steps of the wizard, you are ready to save the job configuration.

1. If you are satisfied with your job configuration, click **Finish** to save your job. Otherwise, click the **Back** button and make any necessary changes.

Congratulations! You have created a File Synchronization job. It is now listed in the **Jobs** view under **File Synchronization**.

2. Click the **Summaries** tab to view the summary information about the job.

See [Starting a File Synchronization Job](#) for information about starting the job.



## Editing a File Synchronization Job

You can edit a File Synchronization job while it is running; however, any changes will not take effect until the job is restarted.

### Overview

When you create a File Synchronization job, the **Create Job** wizard guides you through the process, presenting the most common options for configuration. When editing a job, you have access to all options, allowing you to fine-tune the job configuration. Options not included in the initial job creation include:

- [Application Support](#)
- [Conflict Resolution](#)
- [Delta Replication](#)
- [DFS-N](#)
- [File and Folder Filters](#)
- [File Locking](#)
- [General](#)

- [Logging and Alerts](#)
- [Scheduled Replication](#)
- [SNMP Notifications](#)
- [Target Protection](#)
- [Tags](#)

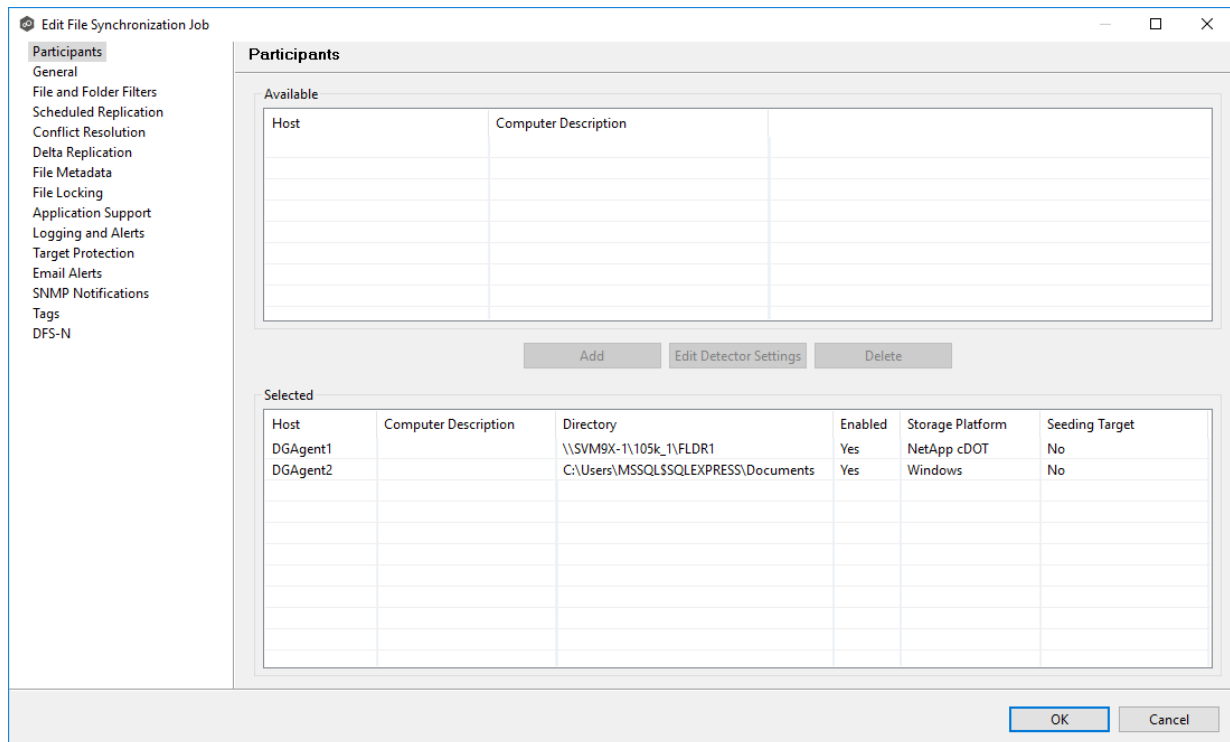
You can edit multiple File Synchronization jobs simultaneously. For information about simultaneously editing multiple jobs, see [Editing Multiple Jobs](#).

## Editing a Job

To edit a File Synchronization job:

1. Select the job in the **Jobs** view.
2. Right-click and select **Edit Job**.

The **Edit File Synchronization Configuration** dialog appears.



3. Select a configuration item in the navigation tree and make the desired changes:



- [Participants](#)
- [General](#)
- [File and Folder Filters](#)
- [Scheduled Replication](#)
- [File Conflict Resolution](#)
- [Delta Replication](#)
- [File Metadata](#)
- [File Locking](#)
- [Logging and Alerts](#)
- [Application Support](#)
- [Target Protection](#)
- [Email Alerts](#)
- [SNMP Notifications](#)
- [Tags](#)
- [DFS-N](#)

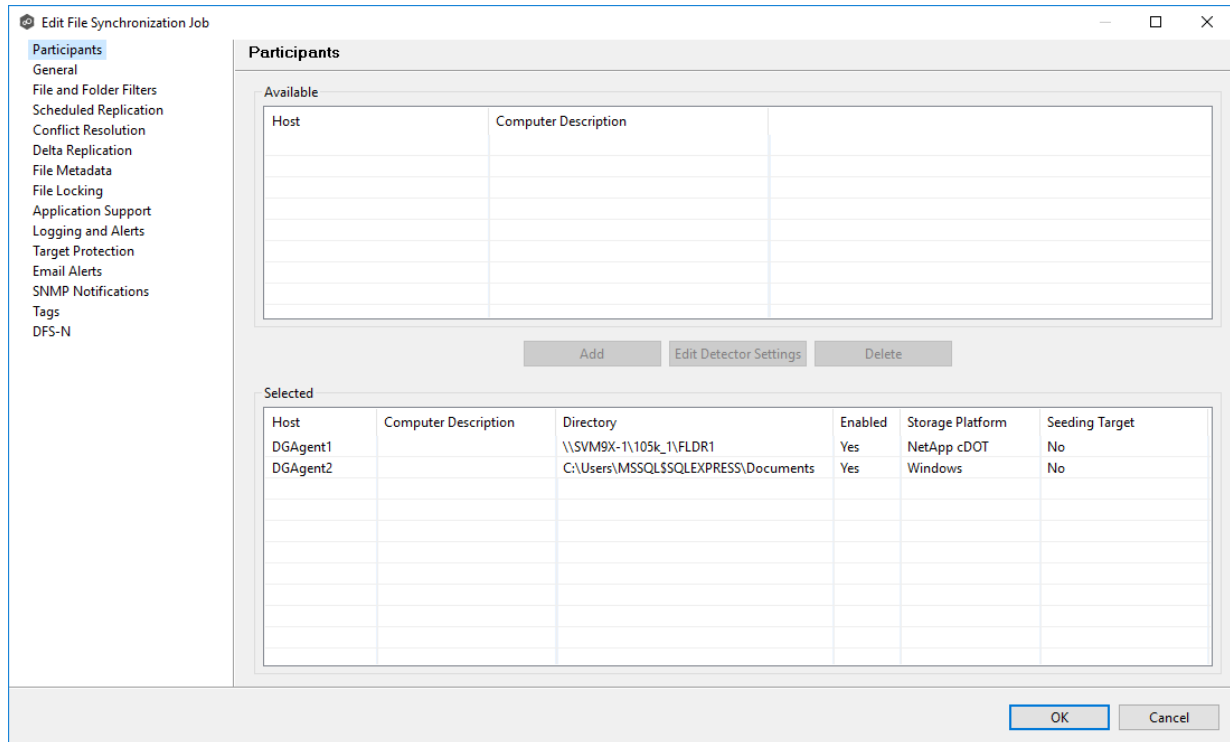
4. Click **OK** when finished.

## Participants

The **Participants** page in the **Edit File Synchronization Job** dialog allows you to:

- [Add and remove participants from a job.](#)
- [Modify a participant's attributes.](#)
- [Modify a participant's detector settings.](#)

The **Participants** page in the **Edit File Synchronization Jobs** dialog has two tables: the **Available** table and the **Selected** table. The **Available** table lists the available hosts and the **Selected** table lists hosts that have already been added to the job. The **Computer Description** field displays the name of the server that the Peer Agent is running on.



This topic describes [adding](#) and [deleting](#) participants in a File Synchronization job.

## Adding a Participant to a Job

To add a participant to a job:

1. Click the participant in the **Available** table.

To be available, a host must have Peer Agent installed and successfully connect to the Peer Management Broker. If a particular host is not displayed in the list, try restarting the Peer Agent Windows Service on that host, and if it successfully connects to Peer Management Center Broker, then the list will be updated with the computer name of that host.

Edit File Synchronization Job

**Participants**

General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
Delta Replication  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Participants**

Available

Host	Computer Description
DGAgent3	

Add Edit Detector Settings Delete

**Selected**

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\SVM9X-1\105k_1\FLDR1	Yes	NetApp cDOT	No
DGAgent2		C:\Users\MSSQL\$SQLEXPRESS\Documents	Yes	Windows	No

OK Cancel

- Click the **Add** button.

The participant is moved to the **Selected** table.

Edit File Synchronization Job

**Participants**

General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
Delta Replication  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Participants**

Available

Host	Computer Description

Add Edit Detector Settings Delete

**Selected**

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\SVM9X-1\105k_1\FLDR1	Yes	NetApp cDOT	No
DGAgent2		C:\Users\MSSQL\$SQLEXPRESS\Documents	Yes	Windows	No
DGAgent3		\\AFS2\Share3	Yes	Nutanix Files	No

OK Cancel

3. (Optional) Enter the computer's name in the **Computer Description** column.
4. Enter the path to the folder to be watched in the **Directory** column.
5. (Optional) Modify whether the participant is a [seeding target](#).
6. (Optional) Modify the participant's [detector settings](#).
7. Click **OK** or select another item to modify.

## Deleting a Participant from a Job

To delete a participant from a job:

1. Click the participant in the **Selected** table.
2. Click the **Delete** button.

The participant is moved to the **Available** table.

**Note:** A File Synchronization job must have at least two participants, so if after deleting a participant, there is only a single participant, you must add another participant to the job.

3. Click **OK** or select another item to modify.

You can modify the following attributes of a participant in a File Synchronization job:

- **Directory** - Specifies the watch set that has been selected for replication.
- **Enabled** - Determines whether the participant is enabled.
- **Storage Platform** - Identifies the type of storage platform that the agent will manage. If the storage device that the agent is managing has changed to a different storage platform, then you need to select the new platform.
- **Seeding Target** - Determines whether the participant host is used as a [data seeding target](#). For more information on smart data seeding, see [Smart Data Seeding](#) in [Advanced Topics](#) or contact [support@peersoftware.com](mailto:support@peersoftware.com).

To change the attributes of a participant:

1. Select the participant from the **Host** column in the **Selected** table.

**Participants**

**Available**

Host	Computer Description

Add Edit Detector Settings Delete

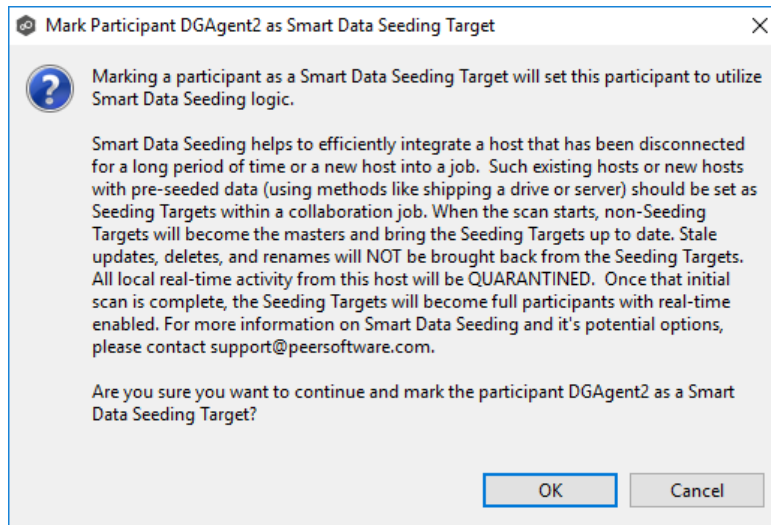
**Selected**

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\AFS2\Share3	Yes	Nutanix Files	No
DGAgent2		\\SVM9x-1	Yes	NetApp cDOT	No

OK Cancel

2. To change the directory that is replicated, enter a new directory path in the **Directory** column.
3. To enable or disable the agent, select a value in the **Enabled** column.
4. To change whether the agent is a seeding host, select **Yes** or **No** in the **Seeding Target** column.

If you selected **Yes**, review the information in the message dialog that appears and then click **OK**.



5. Click **OK** to close the Edit wizard or select another configuration item to modify.

In addition to [global real-time detection options](#) that apply to all jobs, you can set additional detection-related options for a specific File Synchronization job. For example, you can exclude real-time events by certain users. This is helpful if you are trying to prevent events generated from backup and/or archival tools from triggering activity.

To modify the detector settings for a host:

1. Select the host in the **Selected** table.

**Edit File Synchronization Job**

**Participants**

Available

Host	Computer Description

Add Edit Detector Settings Delete

Selected

Host	Computer Description	Directory	Enabled	Storage Platform	Seeding Target
DGAgent1		\\AFS2\Share3	Yes	Nutanix Files	No
DGAgent2		\\SVM9x-1	Yes	NetApp cDOT	Yes

OK Cancel

2. Click **Edit Detector Settings**.

The information you are prompted to enter varies, depending on the type of storage platform. Windows, NetApp, and Nutanix examples are shown below.

**Windows Detector Options**

Filter open/close events from these users:

Access Event Suppression Time:

**Reparse Point Options**

☒ Follow Junction Points

☒ Follow Mount Points

☒ Follow Symbolic Links

OK Cancel

**NetApp Options**

NetApp Options for this Job

Filter open/close events from these users:

Filter all events from these users:

Filter events from these IP Addresses:

Access Event Suppression Time:

Advanced FPolicy cDOT Settings for host: DGAgent2 and SVM: SVM9x-1

\*SVM Username:

\*SVM Password:

SVM Management IP:

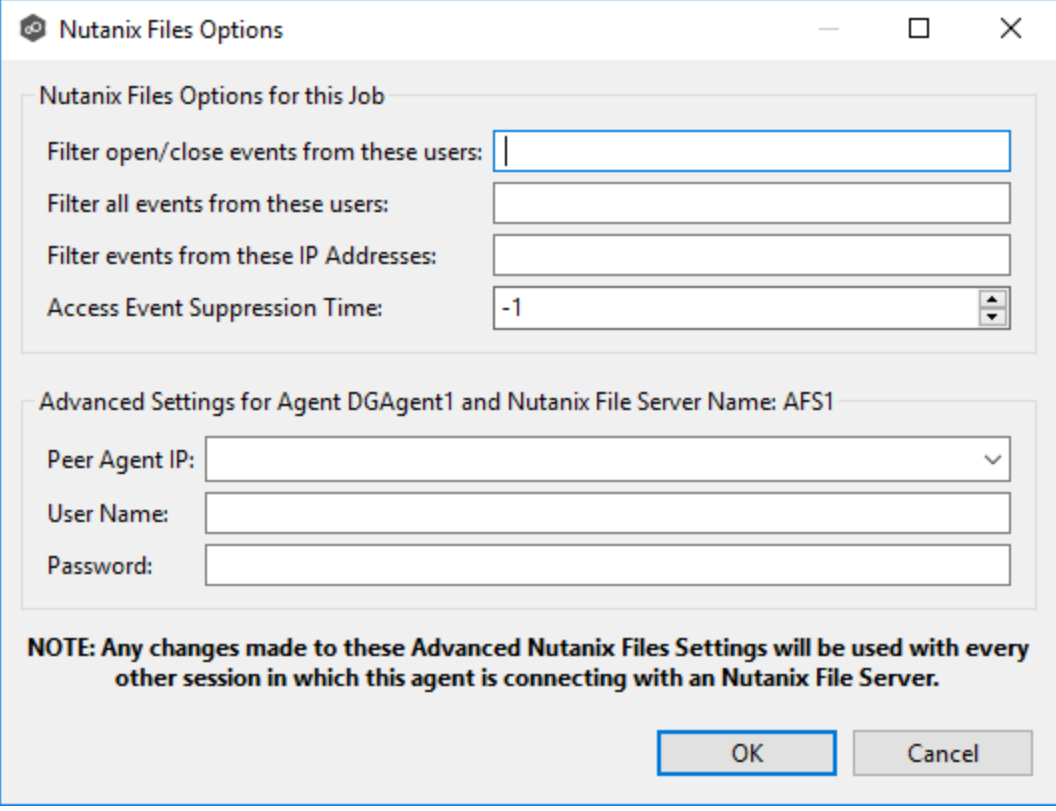
\*Agent IP for SVM Conn.:

Filtered Extensions:

Admin Share Override:

**NOTE: Any changes made to these Advanced FPolicy cDOT Settings will be used with every other session in which this FPolicy Server is connecting to the same Storage Virtual Machine.**





The image shows a Windows-style dialog box titled "Nutanix Files Options". It has a standard title bar with minimize, maximize, and close buttons. The dialog is divided into two main sections. The first section, "Nutanix Files Options for this Job", contains four input fields: "Filter open/close events from these users:" (with a text input), "Filter all events from these users:" (with a text input), "Filter events from these IP Addresses:" (with a text input), and "Access Event Suppression Time:" (with a spinner box set to -1). The second section, "Advanced Settings for Agent DGAgent1 and Nutanix File Server Name: AFS1", contains three input fields: "Peer Agent IP:" (with a dropdown arrow), "User Name:" (with a text input), and "Password:" (with a text input). At the bottom of the dialog, there is a bold note: "NOTE: Any changes made to these Advanced Nutanix Files Settings will be used with every other session in which this agent is connecting with an Nutanix File Server." Below the note are two buttons: "OK" and "Cancel".

3. Modify the values as needed.
4. Click **OK**.

## General

The **General** page in the **Edit File Synchronization Job** dialog presents miscellaneous settings pertaining to a File Synchronization job. You may want to consult with Peer Software's Technical Support team before modifying these values.

To modify these settings:

1. Enter the values recommended by Peer Software Support.

**Edit File Synchronization Job**

**General**

Job ID: 168

Job Type: File Synchronization

Job Name: FS-2

Transfer Block Size (KB): 1024

File Synchronization Job Priority: 2

Timeout (Seconds): 180

First Scan Mode: FOLDER\_BY\_FOLDER

Remove Filtered Files On Folder Delete: ☒

Require All Hosts At Start: ☐

Auto Start: ☒

OK Cancel

Option	Description
<b>Job ID</b>	Unique, system-generated job identifier that cannot be edited.
<b>Job Type</b>	Identifies the job type. This cannot be modified.
<b>Job Name</b>	Name of this File Synchronization job. This name must be unique.
<b>Transfer Block Size (KB)</b>	The block size in Kilobytes used to transfer files to hosts. Larger sizes will yield faster transfers on fast networks but will consume more memory in the <a href="#">Peer Management Broker</a> and <a href="#">Peer Agents</a> .
<b>File Synchronization Job Priority</b>	Use this to increase or decrease a job's file synchronization priority relative to other configured job priorities. Jobs are serviced in a round-robin fashion, and this number determines the maximum number of synchronization tasks that will be executed sequentially before yielding to another job.
<b>Timeout (Seconds)</b>	Number of seconds to wait for a response from any host before performing retry logic.

Option	Description
<b>First Scan Mode</b>	Determines which scan type will be used when the job is first started. For environments where most data is NOT seeded, the FOLDER_BY_FOLDER method will be best. For environments where most data IS seeded, the BULK_CHECKSUM method will result in a faster first scan.
<b>Remove Filtered Files On Folder Delete</b>	If selected, then all child files on target hosts will be deleted when its parent folder is deleted on another source host. Otherwise, filtered files will be left intact on targets when a parent folder is deleted on another source host.
<b>Require All Hosts At Start</b>	If selected, requires all <a href="#">participating hosts</a> to be online and available at the start of the File Synchronization job in order for the job to successfully start.
<b>Auto Start</b>	If selected, then this file synchronization session will automatically be started when the Peer Management Center Service is started.

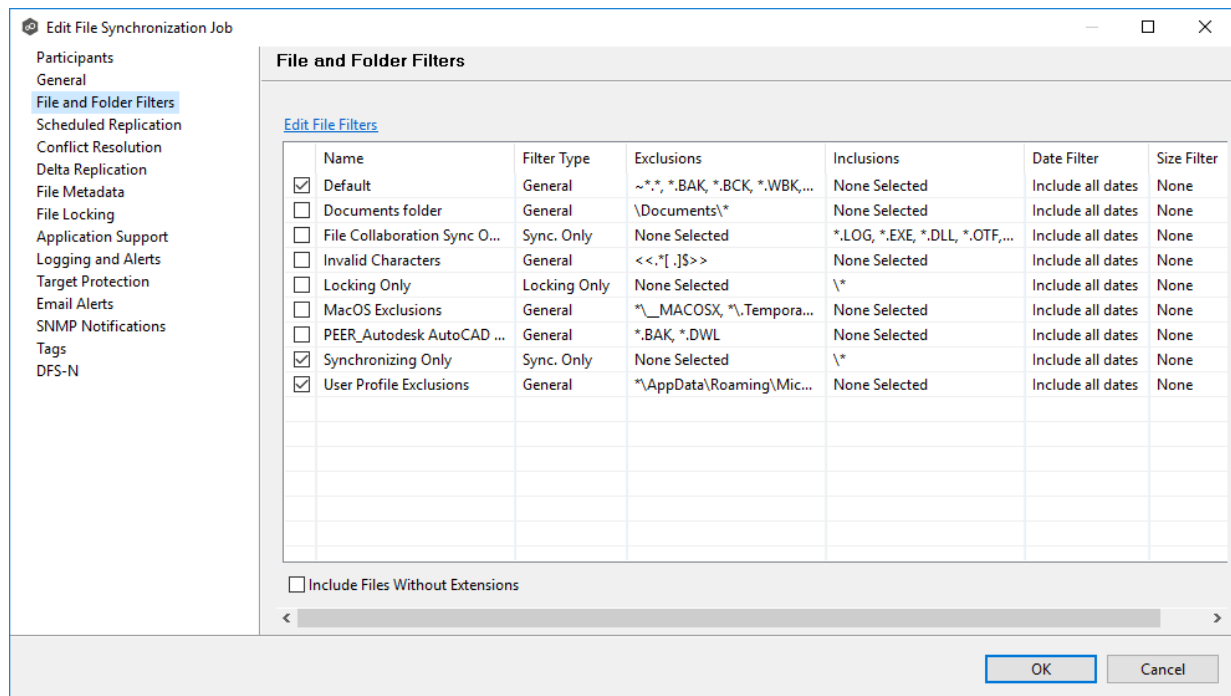
2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## File and Folder Filters

The **File and Folder Filters** page in the **Edit File Synchronization Job** dialog displays a list of [file and folder filters](#). A file or folder filter enables you to exclude and/or include files and folders from the job based on file type, extension, name, or directory path. Any file or folder that matches the filter is excluded or included from replication, depending on the filter's definition. By default, all files and folders selected in the **Source Paths** page will be replicated.

1. Select the file and folder filters you want to apply to the job.

If you want to create a new file or folder filter or modify an existing one, click **Edit File Filters**. See [File Filters](#) in the [Preferences](#) section for information about creating or modifying a file filter.



2. Select the **Include Files Without Extensions** checkbox if you want to replicate file that do not have extensions.

**Note:** Files without extensions are ignored during replication unless you select this checkbox.

3. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Scheduled Replication

The **Scheduled Replication** page in the **Edit File Synchronization Job** dialog displays a list of [scheduled replication filters](#). A scheduled replication filter enables you to identify files and folders that you don't want replicated in real-time.

1. Select the scheduled replication filters you want to apply to the job.

If you want to create a new filter or modify an existing one, click **Edit Scheduled Replication Filters**. See [Scheduled Replication](#) in the [Preferences](#) section for information about creating or modifying a scheduled replication filter.

[illegible]

2. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Conflict Resolution

By default, any file conflicts that are encountered during the [initial synchronization process](#) are automatically resolved by Peer Management Center. Peer Management Center resolves the conflict by selecting the file with the most recent modification time. Conflicts that cannot be automatically be resolved result in the files being quarantined. The **Conflict Resolution** page in the **Edit File Synchronization Job** allows you to select options for resolving file conflicts and quarantines.

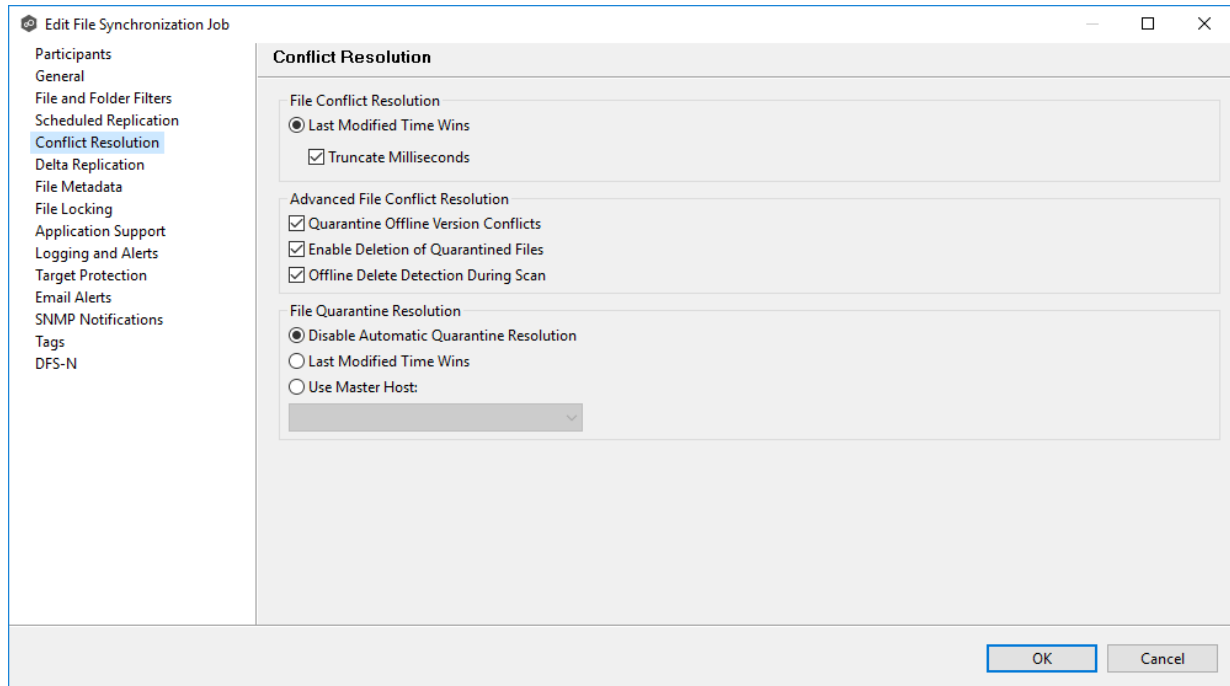
However, if you want to resolve the conflicts yourself, you can contact Peer Software to enable manual resolution. With manual resolution, you can select the host with the correct version of the file.

For more information about the cause of file conflicts, see [Conflicts, Retries, and Quarantines](#).

To modify conflict resolution settings for the File Synchronization job:

1. In the **File Conflict Resolution** section, select the **Truncate Milliseconds** option if you want the millisecond value truncated from each time stamp when comparing the time stamps of a file on two or more hosts.

As some storage platforms and applications track milliseconds slightly differently, selecting this option will prevent subtle millisecond differences from causing an otherwise in-sync file to be replicated or quarantined.



2. Select the **Advanced File Conflict Resolution** options you want applied:

<b>Quarantine Offline Version Conflicts</b>	Select this option if you want Peer Management Center to quarantine a file that was updated in two or more locations while the collaboration session was not running. If it is not selected, the file with the most recent last modified time will be replicated to all other participants.
<b>Enable Deletion of Quarantined Files</b>	Select this option if you want Peer Management Center to process a delete event for a quarantined file. If it is not selected, the quarantined file is not deleted and remains quarantined.
<b>Offline Delete Detection During Scan</b>	Select this option (and enabled <a href="#">target protection</a> ), if you want any files or folders that were deleted while the job was stopped to be deleted from all participants when the job is restarted. If it is not selected, then the deleted file or folder is restored from a participant with the file or folder to any participant where it no longer exists.

3. Select an option for automatically resolving quarantines (this option is intended to be used in environments where a single file server is active for a job):

<b>Disable Automatic Resolution of Quarantines</b>	Select this option if you want to manually resolve quarantines. For more information, see <a href="#">Removing a File from Quarantine</a> .
<b>Last Modified Time</b>	Select this option if you want quarantines automatically resolved by selecting the file with the latest modification time.
<b>Use Master Host</b>	Select this option if you want quarantines automatically resolved by selecting the file on the Master Host.

4. Click **OK** to close the Edit wizard or select another configuration item to modify.

## Delta Replication

The **Delta Replication** page in the **Edit File Synchronization Job** dialog allows you to specify the delta-replication options to use for the selected File Synchronization job. Delta-level replication is a byte replication technology that enables block/byte level synchronization for a File Synchronization job. Through this feature, Peer Management Center is able to transmit only the bytes/blocks of a file that have changed instead of transferring the entire file. This results in much lower network bandwidth utilization, which can be an enormous benefit if you are transferring files across a slow WAN or VPN, as well as across a high-volume LAN.

Delta-level replication is enabled on a per File Synchronization job basis and generally affects all files in the [watch set](#). You will only benefit from delta-level replication for files that do not change much between file modifications, which includes most document editing programs.

**Edit File Synchronization Job**

Participants  
General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
**Delta Replication**  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
Target Protection  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Delta Replication**

Enable Delta-level Replication: ☒

Checksum Transfer Size (KB): 256

Delta Block Transfer Size (KB): 512

Minimum File Size (KB): 5120

Minimum File Size Percentage Target/Source: 0.30

**Excluded File Extensions**

- zip
- jpg
- jpeg
- png
- gif
- tiff
- tif
- Z
- tgz
- gz
- gzip
- rar
- 7z
- bz
- bz2
- bzip2
- mp3
- mp4
- m4v
- ogg
- avi
- wav
- vob
- aac
- aif
- aifc
- aiffast
- asx
- wax
- wma
- wmd
- wmv
- wvx
- wmp
- wmx
- mpeg
- mpg
- m1v
- mp2
- mpa
- mpe
- mp2v
- mpv2
- m4p
- mov

**Excluded File Name Patterns**

OK Cancel

To modify delta-level replication options:

1. Modify the following the fields as necessary.

**Enable Delta-Level**

Select to enable delta encoded file transfers which only sends the file blocks that are different between source and



<b>Replication</b>	target(s). If this is disabled, the standard file copy method will be used to synchronize files.
<b>Checksum Transfer Size (KB)</b>	Enter the block in kilobytes used to transfer checksums from target to source at one time. Larger sizes will result in faster checksum transfer, but will consume more memory on the Peer Agents
<b>Delta Block Transfer Size (KB)</b>	Enter the block size in kilobytes used to transfer delta encoded data from source to target at one time. Larger sizes will result in faster overall file transfers but will consume more memory on the Peer Agents.
<b>Minimum File Size (KB)</b>	Enter the minimum size of files in kilobytes to perform delta encoding for. If a file is less than this size, then delta encoding will not be performed.
<b>Minimum File Size Percentage Target/Source</b>	Enter the minimum allowed file size difference between source and target, as a percentage, to perform delta encoding. If the target file size is less than this percentage of the source file size, then delta encoding will not be performed.
<b>Excluded File Extensions</b>	Enter a comma-separated list of file extension patterns to be excluded from delta encoding, e.g., zip, jpg, png. In general, compressed files should be excluded from delta encoding and the most popular compressed file formats are excluded by default.
<b>Excluded File Name Patterns</b>	Enter a list of file name patterns to be excluded from delta encoding. If a file name matches any pattern in this list, then it will be excluded from delta encoding transfers and a regular file transfer will be performed. See <a href="#">File and Folder Filters</a> for more information on specifying wildcard expressions.

- Click **OK** to close the Edit wizard or select another configuration item to modify.

## File Metadata

The **File Metadata** page in the **Edit File Synchronization Job** dialog allows you to modify your file metadata synchronization settings and provides some additional options not available when

creating the job. See [File Metadata Synchronization](#) in [Advanced Topics](#) for more information about file metadata replication.

To enable file metadata synchronization:

1. Select when you want the metadata synchronized (you can select one or both options):
  - **Enable synchronizing NTFS security descriptors (ACLs) in real-time** - Select this option if you want the metadata replicated in real-time. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be transferred to the target host file(s) as they occur.
  - **Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan** - Select this option if you want the metadata replicated during the initial scan. If enabled, changes to the selected security descriptor components (Owner, DACL, and SACL) will be synchronized during the initial scan.

The screenshot shows the 'Edit File Synchronization Job' window with the 'File Metadata' tab selected. The left sidebar lists various configuration categories, with 'File Metadata' highlighted. The main panel contains the following settings:

- Synchronize Security Descriptors (ACLs)**
  - ☒ Enable synchronizing NTFS security descriptors (ACLs) in real-time
  - ☒ Enable synchronizing NTFS security descriptors (ACLs) with master host during initial scan
  - ☐ Enable prevention of corrupt or blank Owner or DACLs on source or master host from being applied to any target host
- Synchronize Security Descriptor Options**
  - ☒ Owner
  - ☐ DACL: Discretionary Access Control List
  - ☐ SACL: System Access Control List
- Metadata Conflict Resolution**
  - Select a Master Host for initial scan:
  - ☒ Enable enhanced metadata conflict resolution
- File Reparse Point Synchronization**
  - Reparse Tag Name (numerical value only):
  - Reparse Master Host:
- Alternate Data Streams Transfer**
  - ☐ Enable transfer of file Alternate Data Streams (ADS)

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

2. Click **OK** in the message that appears after selecting a metadata option.
3. If you selected either of the first two options in the **Synchronize Security Descriptor Options** section, select the security descriptor components (Owner, DACL, and SACL) to be synchronized.

Note: To synchronize SACLs or Owner, the user that a [Peer Agent](#) service is run under on each [participating host](#) must have permission to read and write Owner and SACLs.

4. If you selected the option for metadata synchronization during the initial scan, select the host to be used as the [master host](#) in case of file metadata conflict.

If a master host is not selected, then no metadata synchronization will be performed during the initial scan. If one or more security descriptors do not match across participants during the initial scan, [conflict resolution](#) will use permissions from the designated master host as the winner. If the file does not exist on the designated master host, a winner will be randomly picked from the other participants.

5. (Optional) Click the **Enable enhanced metadata conflict resolution** checkbox.

If enabled, this option ensures that when a metadata conflict occurs and a file or folder is written to a target, the Peer Agent service account is not assigned as the owner of that file or folder. If the Peer Agent service account is the owner, the user may not have permission to access the file or folder.

Note: The Peer Agent service account cannot be a local or system administrator. As described in [Peer Global File Service - Environmental Requirements](#), the Peer agent service account should be an actual user.

6. (Optional) Enter values for one or both file reparse point data synchronization options:

- **Reparse Tag Name** - Enter a single numerical value. Must be either blank (if blank, reparse synchronization will be disabled) or greater than or equal to 0. The default for Symantec Enterprise Vault is 16. A value of 0 enables reparse point synchronization for all reparse file types. If you are unsure as to what value to use, then contact Peer Software technical support, or you can use a value of 0 if you are sure that you are only utilizing one vendor's reparse point functionality.
- **Reparse Master Host** - Select a master host. If a master host is selected, then when the last modified times and file sizes match on all hosts, but the file reparse attribute differs (e.g. archived/offline versus unarchived on file server), then the file reparse data will be synchronized to match the file located on the master host. For Enterprise Vault, this should be the server where you run the archiving task on. If the value is left blank, then no reparse data synchronization will be performed, and the files will be left in their current state.

Note: Use this option only if you are utilizing archiving or hierarchical storage solutions that make use of NTFS file reparse points to access data in a remote location, such as Symantec's Enterprise Vault. Enabling this option allows synchronization of a file's reparse data, and not the actual offline content, to target hosts, and prevents the offline file from being recalled from the remote storage device.

7. (Optional) Select the **Enable transfer of file Alternate Data Stream (ADS)** checkbox.

If enabled, Alternate Data Streams (ADS) of updated files will be transferred to the corresponding files on target participants as a post process of the normal file synchronization.

**Known limitation:** ADS information is transferred only when a modification on the actual file itself is detected. ADS will not be compared between participants. The updated file's ADS will be applied to the corresponding files on target participants.

- Click **OK** to close the Edit wizard or select another configuration item to modify.

## File Locking

The **File Locking** page in the **Edit File Synchronization Job** dialog presents options for managing how source and target files are locked by Peer Management Center.

To modify file locking options:

- Modify the fields in Source Snapshot Synchronization section as needed:

The screenshot shows the 'Edit File Synchronization Job' dialog with the 'File Locking' tab selected. The left sidebar lists various configuration sections, with 'File Locking' highlighted. The main area contains two sections: 'Source Snapshot Synchronization' and 'Sync. On Save'.

**Source Snapshot Synchronization**

- Enable Source Snapshot Copy Sync.:** ☐
- Snapshot Copy Max File Size (MB):** 512
- Snapshot Copy File Extensions:** mdb,accdb,zip,psd,ai,indd
- Use Storage Snapshots:** ☐

**Sync. On Save**

- Enable Sync. On Save:** ☐
- Included File Extensions:** xls,xlsx,doc,docx,dwg
- Synchronization Delay (Seconds):** 20

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

<b>Enable Source Snapshot Sync.</b>	If enabled, a snapshot copy of the source file is created for files that meet the snapshot configuration criteria below, and this copy is used for synchronization purposes. In addition, no file handle is held on the source file except while making a copy of the file.
<b>Snapshot Copy Max File Size (MB)</b>	The maximum file size for which source snapshot synchronization is utilized.
<b>Snapshot Copy File</b>	A comma-separated list of file extensions for which source snapshot synchronization is utilized.

<b>Extensions</b>	
<b>Use Storage Snapshots</b>	If enabled, a storage volume snapshot is created and used for synchronization purposes. As a result, no file handle is held on the source file. The snapshot is created using either VSS or storage-platform specific snapshot technologies. This option is in addition to the <b>Enable Source Snapshot Sync.</b> option above and will only apply to files with pst, mdf, ldf, and ndf extensions.

2. Modify the fields in the **Sync. on Save** section as needed.

<b>Enable Sync. On Save</b>	If enabled, this feature allows supported file types to be synchronized after a user saves a file, rather than waiting for the file to close.
<b>Included File Extensions</b>	A comma separated list of file extensions for which to enable the Sync. On Save feature.
<b>Synchronization Delay (Seconds)</b>	The number of seconds to wait after a file has been saved before initiating a synchronization of the file.

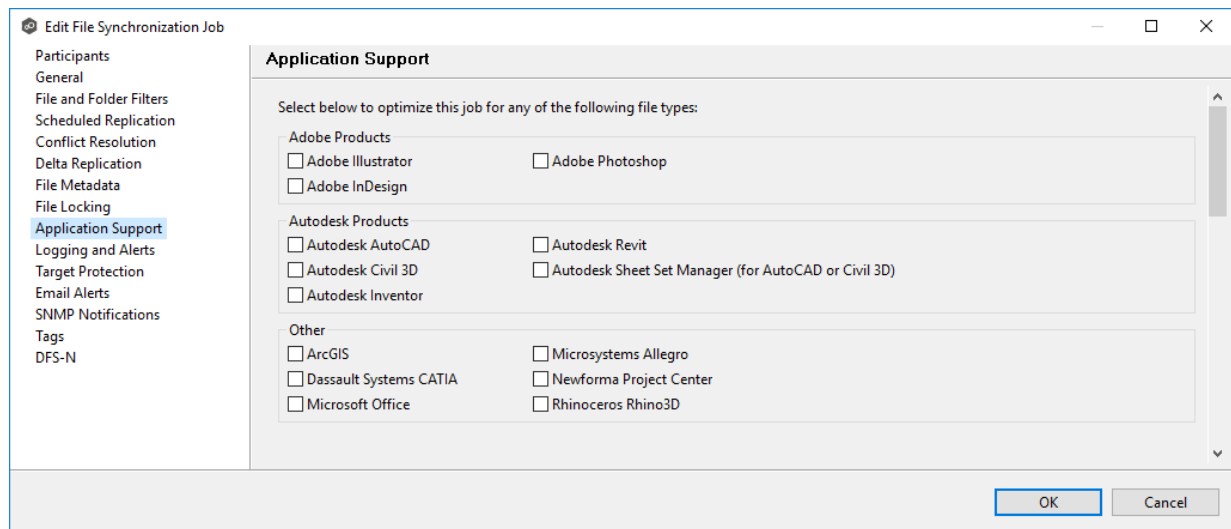
3. Click **OK**.

## Application Support

When you create a File Synchronization job, you have the option of [selecting applications that are automatically optimized](#). You can modify your selections when editing the job.

To modify which applications are optimized:

1. Select the applications to be optimized.



- Click **OK** to close the Edit wizard or select another configuration item to modify.

## Logging and Alerts

### Overview of File Event Logging

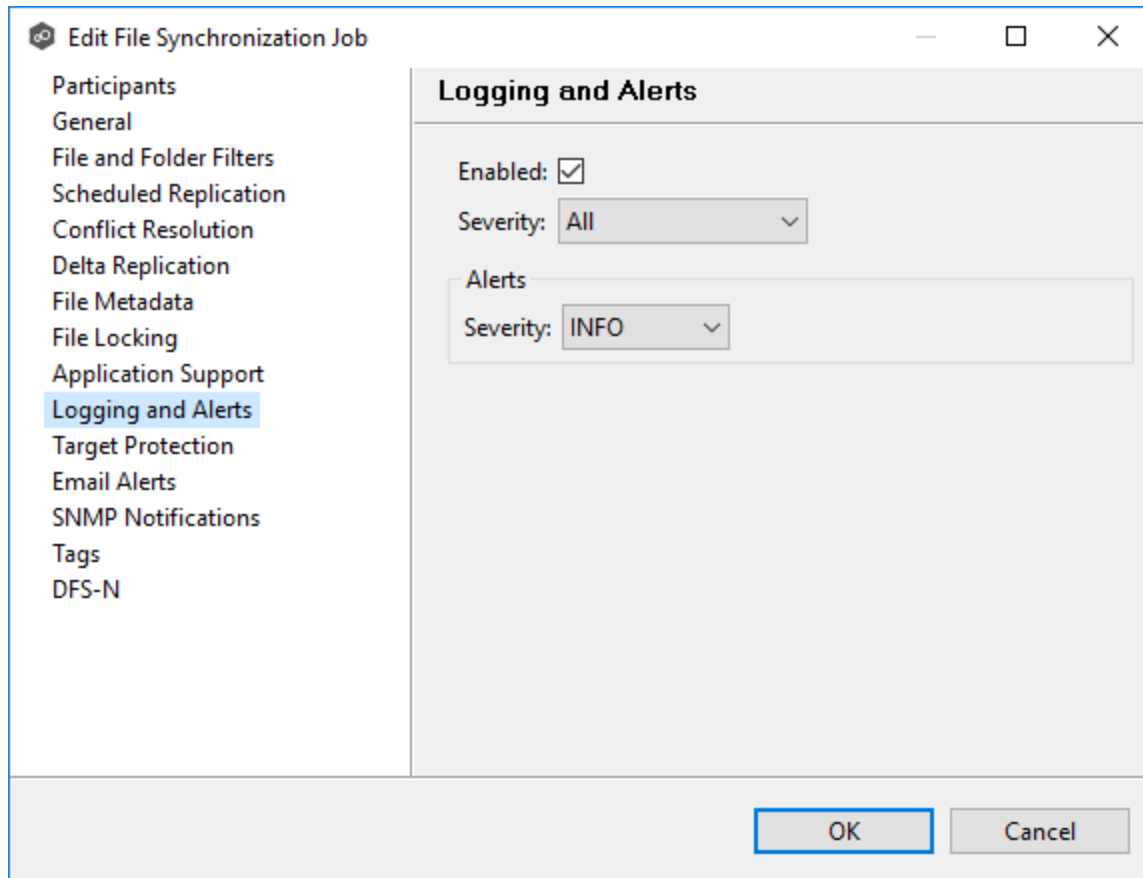
Various types of file synchronization events can be written to a log file and to the Event Log tab located within the File Synchronization runtime view for the selected File Synchronization job. Each job will log to the **fc\_event.log** file located in the **Hub\logs** subdirectory within the Peer Management Center installation directory. All log files are stored in a tab-delimited format that can easily be read by Microsoft Excel or other database applications.

### Log Entry Severity Levels

<b>Informational</b>	Informational log entry, e.g., a file was opened.
<b>Warning</b>	Some sort of warning occurred that did not produce an error but was unexpected or may need further investigation.
<b>Error</b>	An error occurred performing some type of file activity.
<b>Fatal</b>	A fatal error occurred that caused a host to be taken out of the session, a file to be quarantined, or a session to become invalid.

## Configuration

By default, all file synchronization activity is logged for all severity levels. You can enable or disable file event logging as well as select the level of granularity.



## Logging Fields

Below is a list of logging fields and their descriptions:

Field	Description
Enabled	Selecting this option will enable file event logging based on the other settings. Deselecting this option will completely disable all logging.
Severity	Determines what severity levels will be logged. There are two options: <ul style="list-style-type: none"><li>• All (Informational, Warnings, Error, Fatal)</li><li>• Errors &amp; Warnings (Warnings, Error, Fatal)</li></ul>

Field	Description
<b>Event Types</b>	If checked, the corresponding event type will be logged.
<b>File Open</b>	A file was opened by a remote application on a <a href="#">source host</a> .
<b>File Lock</b>	A file lock was acquired on a <a href="#">target host</a> during synchronization of a file.
<b>File Close</b>	A file was closed.
<b>File Add</b>	A file was added to the <a href="#">watch set</a> .
<b>File Modify</b>	A file was modified in the watch set.
<b>File Delete</b>	A file was deleted.
<b>File Rename</b>	A file was renamed.
<b>Attribute Change</b>	A file attribute was changed.
<b>Security (ACL) Change</b>	The security descriptor of a file or folder was changed.
<b>Directory Scan</b>	Indicates when a directory was scanned as a result of the <a href="#">initial synchronization process</a> .
<b>File ADS Transfer</b>	The Alternate Data Stream of a modified file was synced to target host(s).



## Alerts

Various types of alerts can be logged to a log file and to the **Alerts** table located within the [File Synchronization runtime](#) view for the selected job. Each File Synchronization job will log to the **fc\_alert.log** file located in the **Hub\logs** subdirectory within the Peer Management Center installation directory. All log files are stored in a tab-delimited format that can easily be read by Microsoft Excel or other database applications.

The default log level is WARNING, which will show any warning or error alerts that occur during a running session. Depending on the severity of the alert, the job may need to be restarted.

## Target Protection

Target protection is used to protect files on [target hosts](#) by saving a backup copy before a file is either deleted or overwritten on the target host. If enabled, then whenever a file is deleted or modified on the source host but before the changes are propagated to the targets, a copy of the existing file on the target is moved to the Peer Management Center trash bin.

The trash bin is located in a hidden folder named **.pc-trash\_bin** found in the root directory of the [watch set](#) of the target host. A backup file is placed in the same directory hierarchy location as the source folder in the watch set within the recycle bin folder. If you need to restore a previous version of a file, you can copy the file from the trash bin into the corresponding location in the watch set and the changes will be propagated to all other collaboration hosts.

Target protection configuration is available by selecting **Target Protection** from the tree node within the Edit File Synchronization Configuration dialog.

**Edit File Synchronization Job**

Participants  
General  
File and Folder Filters  
Scheduled Replication  
Conflict Resolution  
Delta Replication  
File Metadata  
File Locking  
Application Support  
Logging and Alerts  
**Target Protection**  
Email Alerts  
SNMP Notifications  
Tags  
DFS-N

**Target Protection**

Enabled: ☒

# of Backup Files to Keep:

# of Days to Keep:

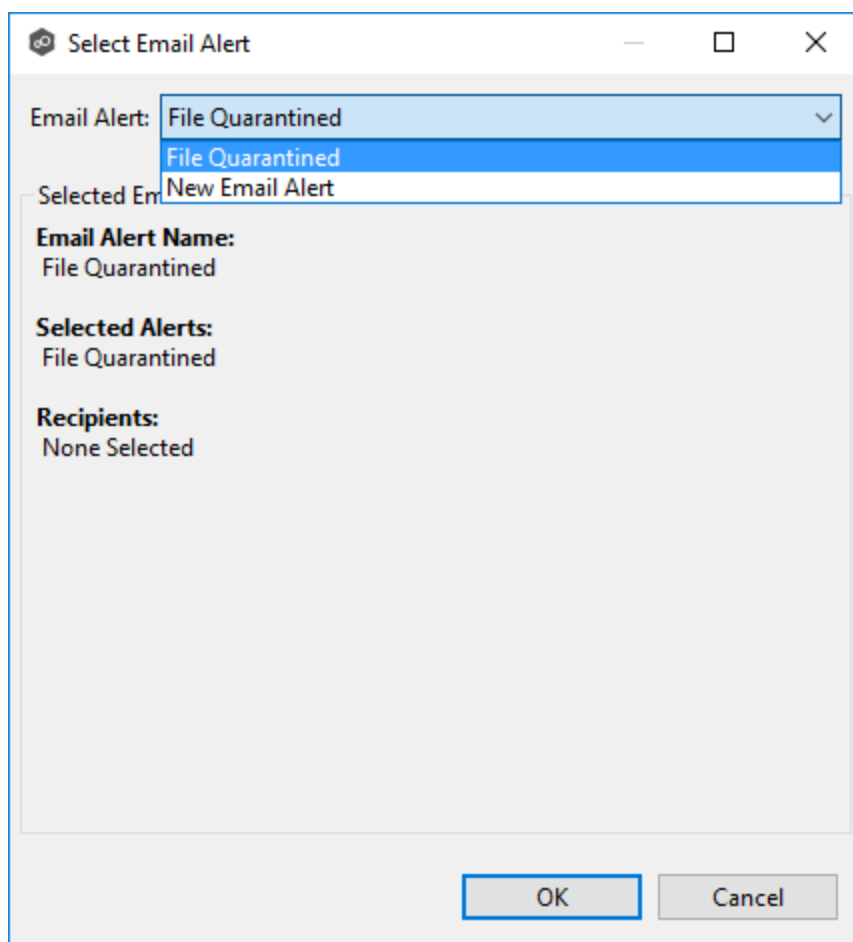
Trash Bin:

OK Cancel

Modify the fields as needed:

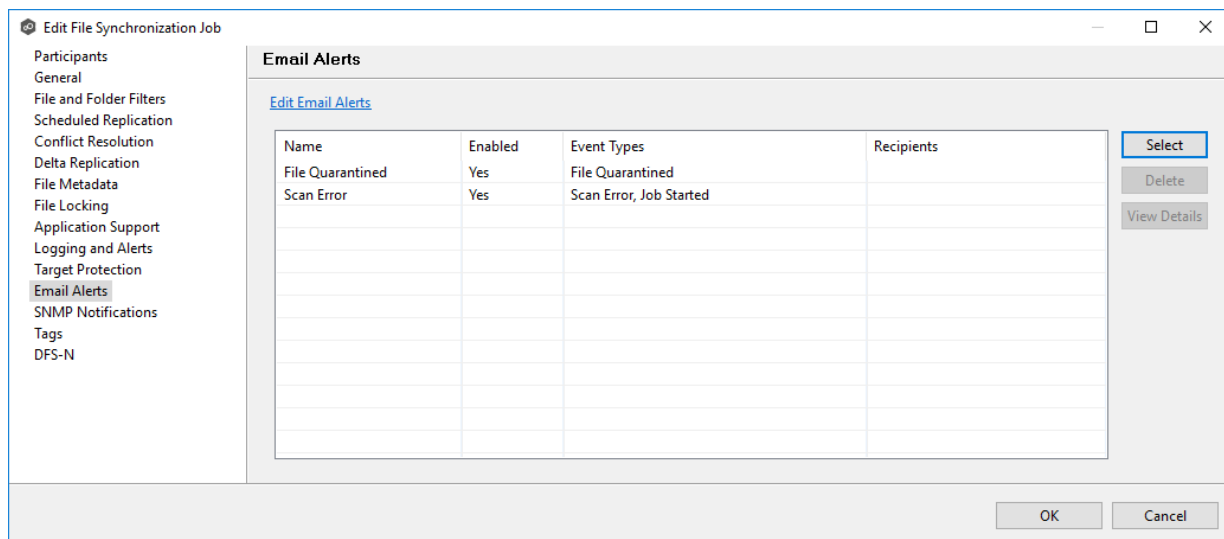
Field	Description
<b>Enabled</b>	Enables target protection.
<b># of Backup Files to Keep</b>	The maximum number of backup copies of an individual file to keep in the trash bin before purging the oldest copy.
<b># of Days to Keep</b>	The number of days to keep a backup archive copy around before deleting from disk. A value of 0 will disable purging any files from archive.
<b>Trash Bin</b>	The trash bin folder name located in the root directory of the watch set. This is a hidden folder and the name cannot be changed by the end user.





2. Select the email alert from the drop-down list, and then click **OK**.

The newly added email alert appears in the **Email Alerts** table.



3. Repeat to add additional alerts to the job.
4. Click **OK** to close the Edit wizard or select another configuration item to modify.

## SNMP Notifications

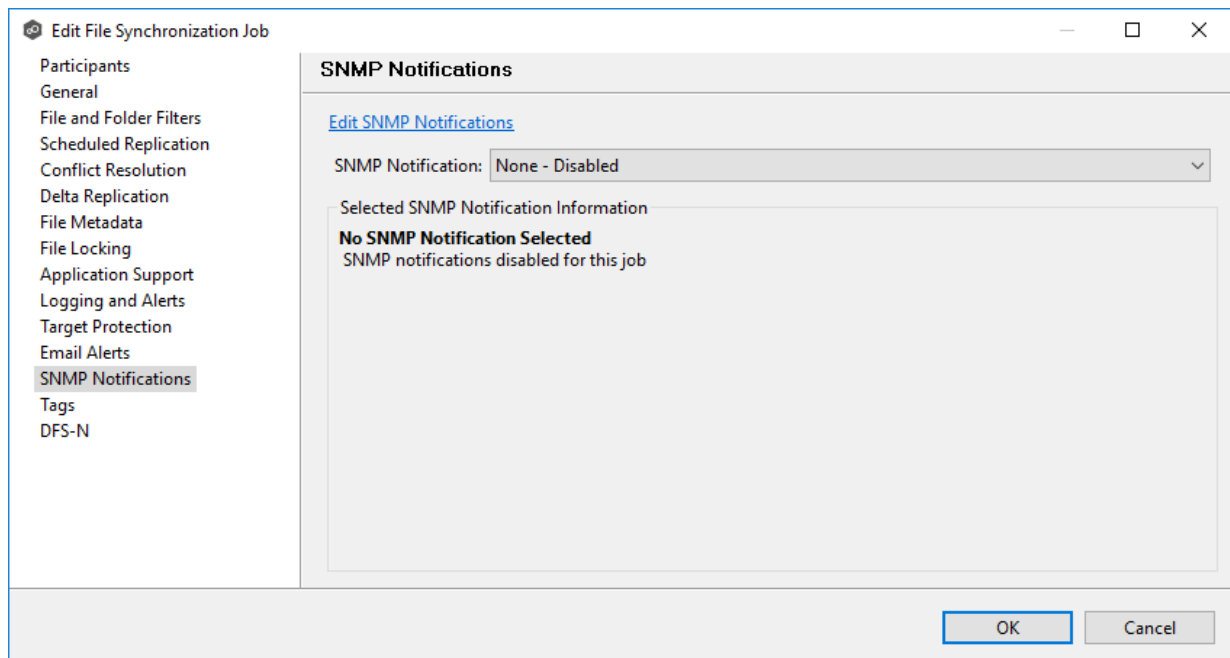
The **SNMP Notifications** page in the **Edit File Synchronization Job** dialog allows you to select which SNMP notification to apply to a File Synchronization job.

SNMP notifications, like email alerts and file filters, are configured at a global level in the [Preferences](#) dialog, then applied to individual jobs. For more information about SNMP Notifications, see [SNMP Notifications](#) in the **Preferences** section.

To enable or disable SNMP notifications for a File Synchronization job:

1. To enable, select an SNMP notification from the drop-down list.

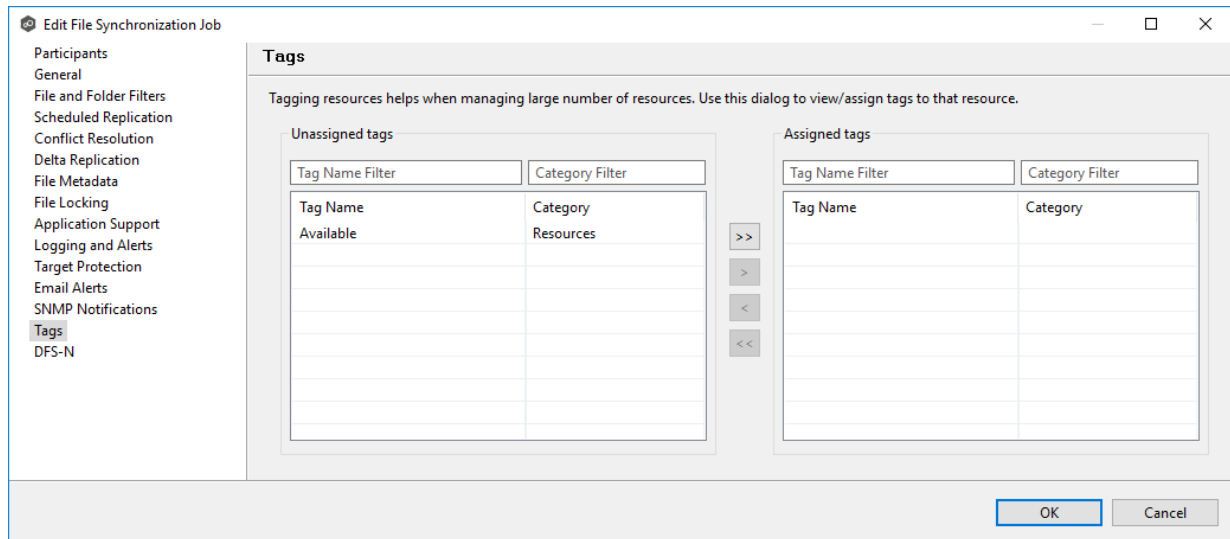
To disable, select **None - Disabled**.



2. Click **OK** to close the Edit wizard or select another configuration item to modify.

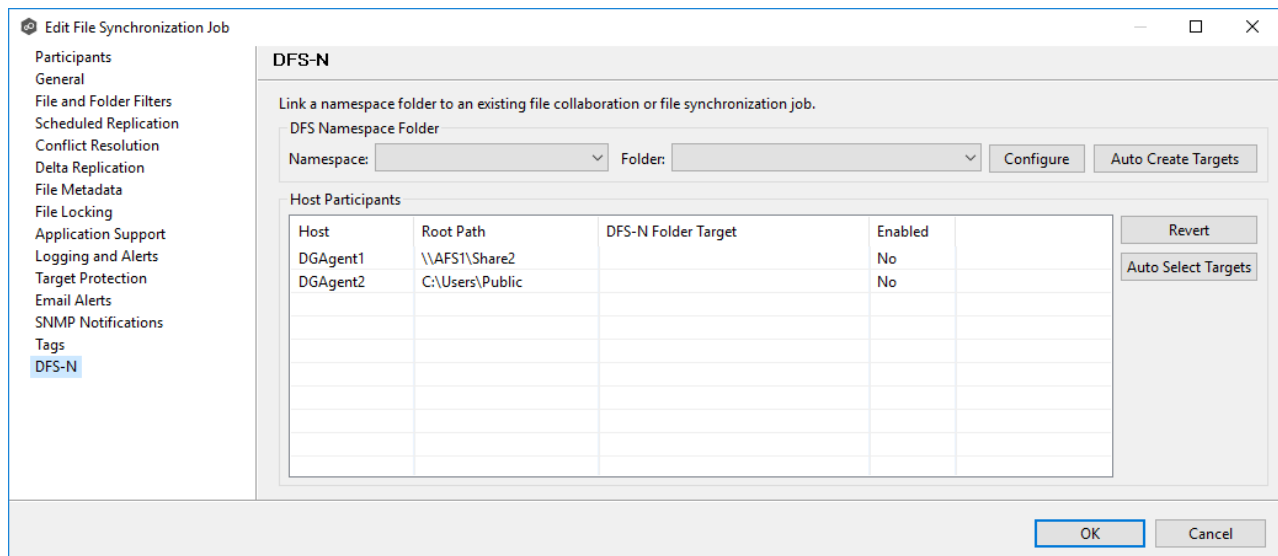
## Tags

The **Tags** page in the **Edit File Synchronization Jobs** dialog allows you to assign existing tags and categories to the selected job. This page is not available in [Multi-Job Editing](#) mode. For more information about tags, see [Tags](#) in the [Basic Concepts](#) section.



## DFS-N

The **DFS-N** page in the **Edit File Synchronization Job** dialog presents options for linking a DFS namespace folder to this job. See [Link a Namespace Folder with an Existing File Collaboration or Synchronization Job](#) for more information.



## Editing Multiple Jobs

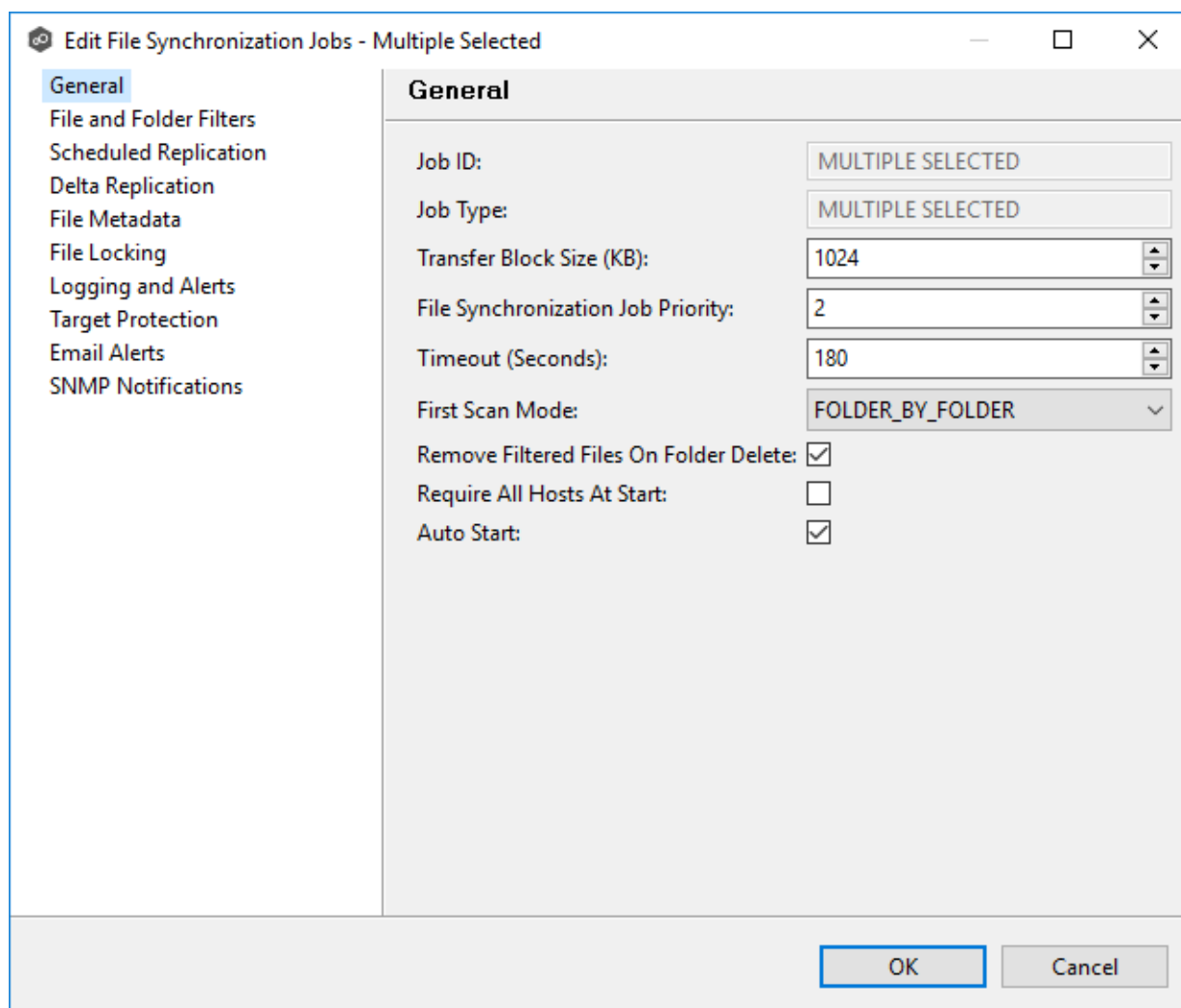
Peer Management Center supports multi-job editing, allowing you to quickly and effectively manipulate multiple File Synchronization jobs simultaneously. For example, you can use this feature to change a single configuration item such as **Auto Start** for any number of already configured jobs in one operation instead of having to change the item individually for each.

While this feature does cover most of the options available on a per-job basis, certain options are unavailable in multi-job edit mode, specifically ones tied to [participants](#). Configuration of participants must be performed on a per job basis.

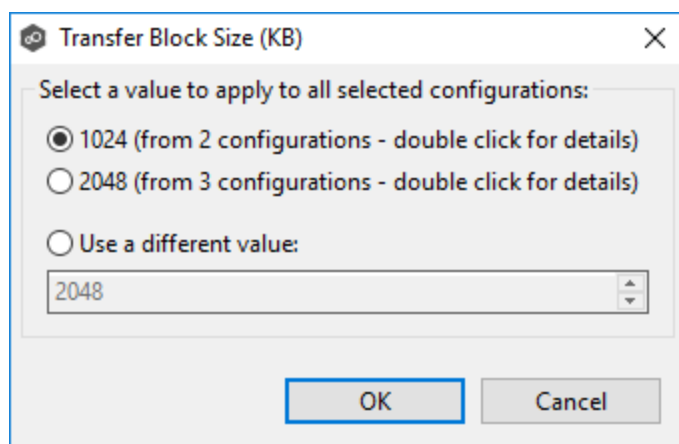
To edit multiple jobs simultaneously:

1. Open Peer Management Center.
2. Select the jobs you want to edit in the **Jobs** view.
3. Right-click and select **Edit Jobs**.

For the most part, the original configuration dialog remains the same with a few minor differences depending on similarities between the selected File Synchronization jobs. A sample dialog is as follows:



In this dialog, any discrepancies between multiple selected jobs will generally be illustrated by a read-only text field with the caption **Multiple Values - Click to Edit**. Clicking this field will bring up a dialog similar to the following:





This dialog gives you the option of choosing a value that is already used by one or more selected File Synchronization jobs, in addition to the ability to use your own value. Notice that variances in the look and feel of this pop-up dialog above depend on the type of information it is trying to represent (for example, text vs. a checkbox vs. a list of items).

Upon clicking OK, the read-only text field you originally clicked will be updated to reflect the new value. Any fields that have changed will be marked by a small caution sign. On saving in this multi-job edit dialog, the changed values will be applied to all selected jobs.

**Note:** Read all information on each configuration page carefully when using the multi-job edit dialog. A few pages operate in a slightly different manner than mentioned above. All of the necessary information is provided at the top of these pages in bold text.

## Running and Managing a File Synchronization Job

The topics in this section provide some basic information about starting, stopping, and managing File Synchronization jobs:

- [Overview](#)
- [Starting a File Synchronization Job](#)
- [Starting a File Synchronization Job](#)
- [Auto-Restarting a File Synchronization Job](#)
- [Host Connectivity Issues](#)
- [Removing a File from Quarantine](#)
- [Manual Retries](#)

### Overview

This topic describes:

- The [initialization process](#) for a File Synchronization job: What occurs the first time you run a File Synchronization job.
- The [initial synchronization process](#): How files are synchronized the first time you run a File Synchronization job.

The initialization process for a File Synchronization job consists of the following steps:

1. All participating hosts are contacted to make sure they are online and properly configured.
2. [Real-time event detection](#) is initialized on all participating hosts where file locks and changes will be propagated in real-time to all participating hosts. You can view real-time activity and history via the various Runtime views for the open job.
3. The [initial synchronization process](#) is started; all of the configured root folders on the participating hosts are scanned in the background, and a listing of all folders and files are sent back to the running job.
4. The background directory scan results are analyzed and directory structures compared to see which files are missing from which hosts. In addition, file conflict resolution is performed to decide which copy to use as the master for any detected file conflicts based on the [File Conflict Resolution](#) settings.
5. After the analysis is performed, all files that need to be synchronized are copied to the pertinent host(s).

Before you start a File Synchronization job for the first time, you need to decide how you would like the [initial synchronization](#) to be performed. During the initial synchronization process:

- The watch set is recursively scanned on all participating hosts.
- File conflict resolution is performed.
- Any files that require updating are synchronized with the most current copy of the file.

The two primary options are:

- Have the File Synchronization job perform the initial synchronization based on the [Conflict Resolution](#) settings.
- [Pre-seed](#) all [participating hosts](#) with the correct folder and file hierarchy for the configured root folders before starting the session.

If you have a large data set, we strongly recommend that you perform the initial synchronization manually by copying the data from a host with the most current copy to all other participating hosts. This needs to be done only once--before the first time that you run the File Synchronization job.

If you choose the first option, click the **Start** button to begin [synchronization session initialization](#). Otherwise, pre-seed each participating host with the necessary data, then click the **Start** button.

### Starting a File Synchronization Job

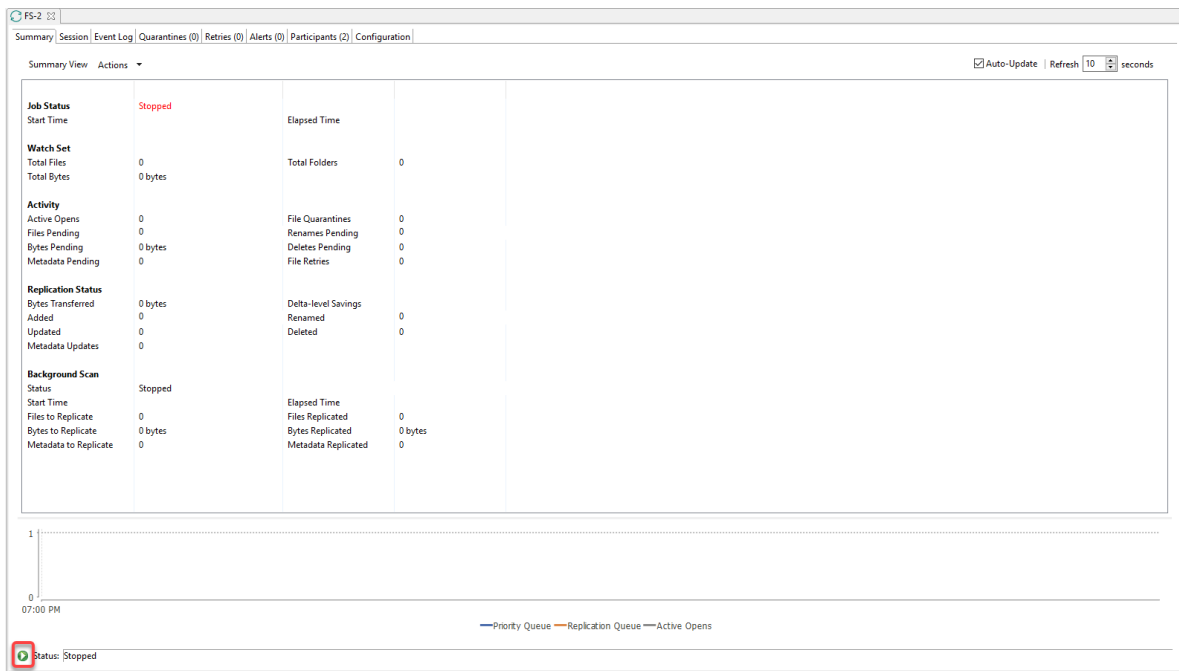
Before starting a File Synchronization job for the first time, make sure that you have decided how you want the [initial synchronization](#) to be performed.

When running a File Synchronization job for the first time, you must manually start it. After the initial run, a job will automatically start, even when the Peer Management Center server is rebooted.

**Note:** You cannot run two jobs concurrently on the same volume if the [watch sets](#) contain an overlapping set of files and folders.

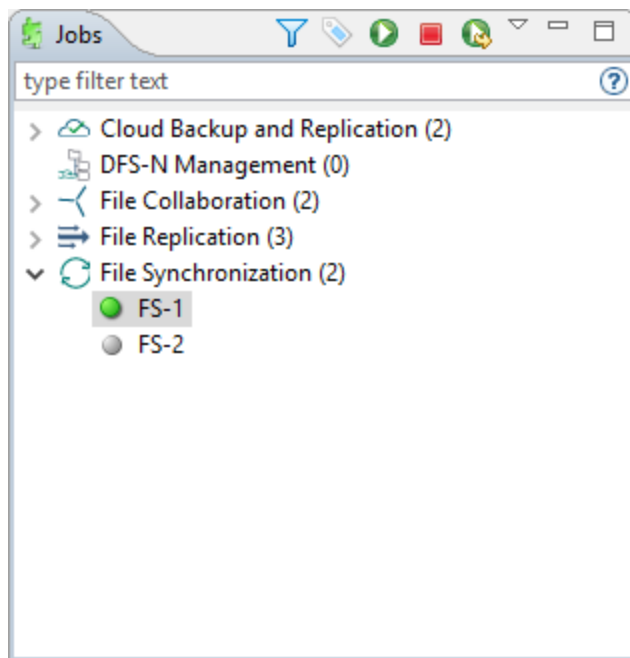
To manually start a job:

1. Choose one of three options:
  - Right-click the job name in the **Jobs** view.
  - Right-click the job name in the **Summary** tab of the **Collab, Sync, and Repl Summary** summary view, and then choose **Start** from the pop-up menu.
  - Open a job and then click the **Start/Stop** button to the left of the **Status** field in the bottom left corner of the job's runtime view (shown below).



2. Click **Yes** in the confirmation dialog.

After the job initialization has completed, the job will run. Once the job starts, the icon next to the job name in the **Jobs** view changes from gray to green.



## Stopping a File Synchronization Job

You can stop a File Synchronization job at any time by clicking the **Stop** button on the **Jobs** view toolbar. Doing this shuts down the real-time file event detection and close all running operations (e.g., file transfers).

## Auto-Restarting a File Synchronization Job

Peer Management Center includes support for automatically restarting File Synchronization jobs that include [participating hosts](#) that have been disconnected, have reconnected, and are once again available.

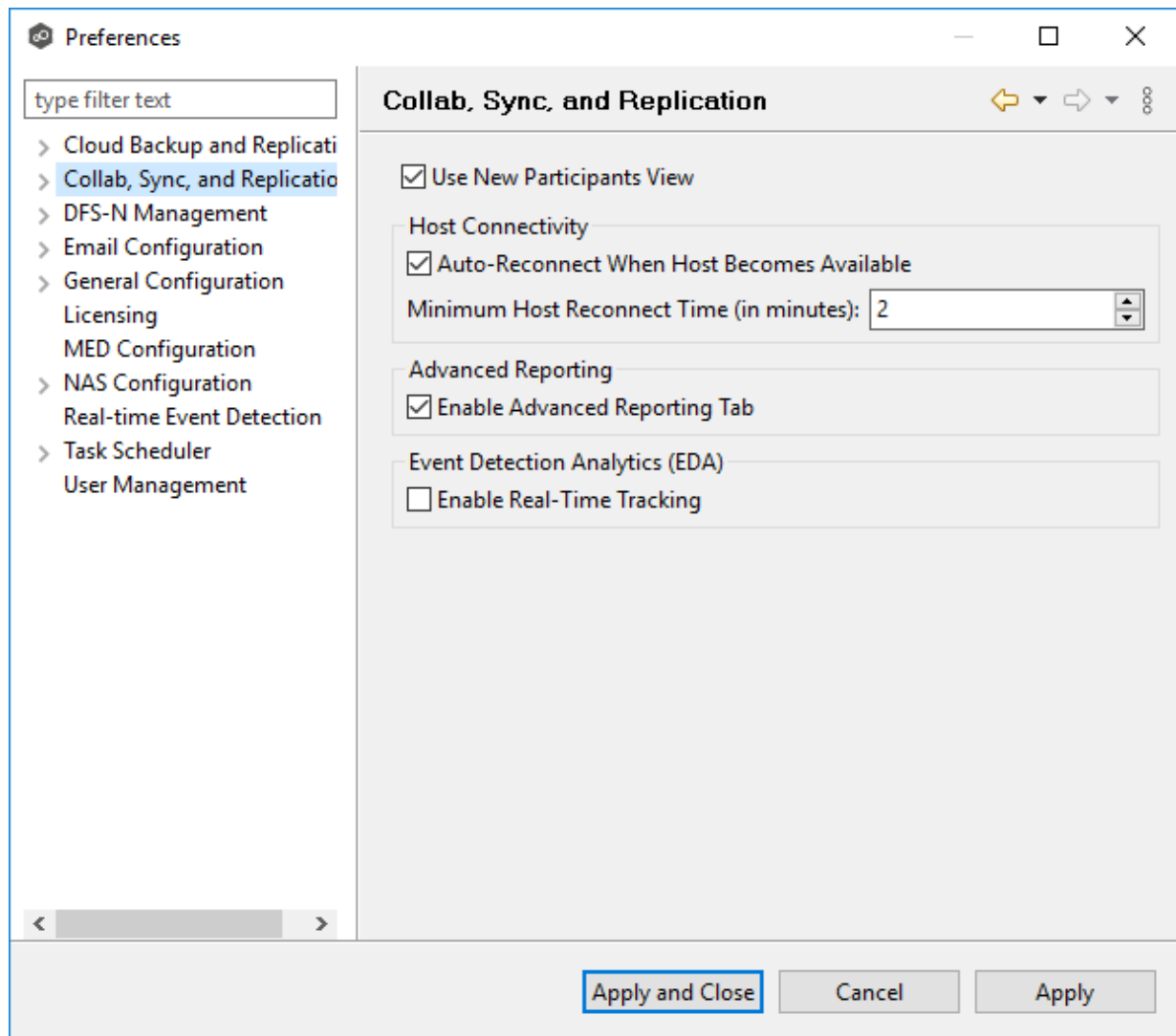
After a host becomes unavailable and the [quorum](#) is lost on a running File Synchronization job, the job automatically stops running and enters a pending state, waiting for one or more hosts to become available again so that the quorum can be met. Once the quorum is met, the pending job will automatically be restarted, beginning with a scan of all root folders.

In a job where a host becomes unavailable but quorum is not lost, the remaining hosts will continue synchronizing. If the unavailable host becomes available once again, it is brought back into the running job and a background scan begins on all participating hosts, similar in fashion to the initial background scan at the start of a job.

You can enable all File Synchronization jobs to auto-restart. You can also disable auto-restart File Synchronization jobs on a per-job and host instance.

To enable all File Synchronization jobs to auto-restart:

1. Select **Preferences** from the **Window** menu.
2. Select **Collab, Sync, and Repl Summary** in the navigation tree.



3. Select the **Auto Reconnect when Host Becomes Available** checkbox.
4. Enter the minimum number of minutes to wait after an Agent reconnects before re-enabling it in any associated jobs in the **Minimum Host Reconnect Time** field.
5. Click **OK**.

### Host Connectivity Issues

Peer Management Center is designed to be run in an environment where all [participating hosts](#) are highly available and on highly available networks. The two primary connectivity issues result from:

- [Unavailable Hosts](#)
- [Quorum Not Met](#)

## Unavailable Hosts

If a host becomes unavailable while a File Synchronization job is running, and is unreachable within the configured timeout period (specified in the job's [General settings](#)), it may be removed from synchronization. If no response is received while performing a file synchronization operation within the timeout period, Peer Management Center pings the host; if still no response, the host is taken out of the running session, a FATAL event is logged, and the **Participants** tab for the job is updated to indicate that the host has failed. In addition, if [email alerts](#) and/or [SNMP notifications](#) are configured and enabled for **Host Timeouts**, then the appropriate message(s) are sent.

If [auto-restart](#) not enabled, you must stop and start the File Synchronization job to bring any failed hosts back into the session. As a result, all root folders on all hosts will need to be scanned again to detect any inconsistencies. Therefore, if you are operating over a WAN with low bandwidth you will want to set the timeout to a higher value on each related job.

## Quorum Not Met

For a File Synchronization job to run correctly, a quorum of available hosts must be met. Quorum is currently set to at least 2 hosts, and if quorum is not met, then the synchronization session is automatically be terminated. If [email alerts](#) and/or [SNMP notifications](#) are configured and enabled for **Session Aborts**, then the appropriate message(s) are sent.

## Removing a File from Quarantine

Quarantines are a key feature of Peer Global File Service, used for resolving version conflicts. For more detailed information on how quarantines work, see [Conflicts, Retries, and Quarantines](#) in the [Advanced Topics](#) section.

You must explicitly remove a file from quarantine in order to have it participate in the synchronization session once again.

You may also choose to perform no action, in which case, the file is removed from the **Quarantines** table but none of the file versions are modified; therefore if the files are not currently in-sync, then the next time the file is modified, changes will be propagated to the other hosts. If an error occurs while removing the quarantine, then the **Status** field in the **Quarantines** table is updated to reflect the error.

To remove a file (or multiple files) from quarantine:

1. Open the job.

2. Open the **Quarantines** tab.
3. Select the file(s) in the Quarantines table.
4. Select the host with the correct version.
5. Click the **Release Conflict** button.

After doing this, all hosts are checked to make sure the file is not currently locked by anyone. If no locks are found, then locks are obtained on all versions of the file and the targets that are out-of-date are synchronized with the selected source host.

### Manual Retries

Retries are a key feature of Peer Global File Service, used for automatically handling errors in the collaboration environment that would have otherwise led to a quarantine. For more detailed information on how retries work, see [Conflicts, Retries, and Quarantines](#) in the [Advanced Topics](#) section.

When a file is put in the retry list, it will be automatically retried based on the settings defined in [File Retries](#) in [Preferences](#). If need be, you can also manually force the retry of a file. This can be done from the Retries list of a specific File Synchronization job.

You may also chose to perform no action, in which case, the file is removed from the Retries list but none of the file versions are modified; therefore if the files are not currently in-sync, then the next time the file is modified, changes will be propagated to the other hosts. If an error occurs while forcing the retry, then the **Status** field in the **Retries** table is updated to reflect the error.

To manually force the retry of a file (or multiple files):

1. Select the file(s) in the **Retries** list.
2. Select the host with the correct version.
3. Click the **Release Conflict** button.

After doing this, all hosts are checked to make sure the file is not currently locked by anyone. If no locks are found, then locks are obtained on all versions of the file and the targets that are out-of-date are synchronized with the selected source host.



## PeerSync Management Jobs

This section provides information about creating, editing, running, and managing a PeerSync Management job:

- [Creating a PeerSync Management Job](#)
- [Running and Managing a PeerSync Management Job](#)

### Creating a PeerSync Management Job

The topics in this section provide some basic information about creating and editing PeerSync Management jobs.

### Integrating Existing PeerSync Instances

To integrate existing PeerSync instances in Peer Management Center, follow the [step-by-step](#) instructions.

### Creating and Deploying New PeerSync Instances

To create a new job and deploy the PeerSync installation to one or more hosts, click the **Create New** button in toolbar of Peer Management Center or select **New** from the **File** menu. A list of all installed job types will be displayed. Select the PeerSync Management option to open the PeerSync Management Configuration dialog. Go to the [Step-by-Step](#) instructions for more information.

When configuring Alerts, you will want to configure global settings like SMTP configuration, which is specific to Peer Management Center. Details on what and how to configure these global options can be found in the [Before You Create Your First PeerSync Management Job](#) section.

To edit the PeerSync Management configuration, right-click on the job in the Jobs view and select **Edit Job(s)**. Within the **Edit PeerSync Management Job** dialog, select the **Associated Profile** node from the left. For step-by-step instructions, see [Running and Managing PeerSync Management Jobs](#).

- [Integrating Existing PeerSync Instances](#)
- [Deploying New PeerSync Instances](#)

## Before You Create Your First PeerSync Management Job

Before creating your first PeerSync Management job, we highly recommend preconfiguring a number of global options that can be applied to all PeerSync Management jobs.

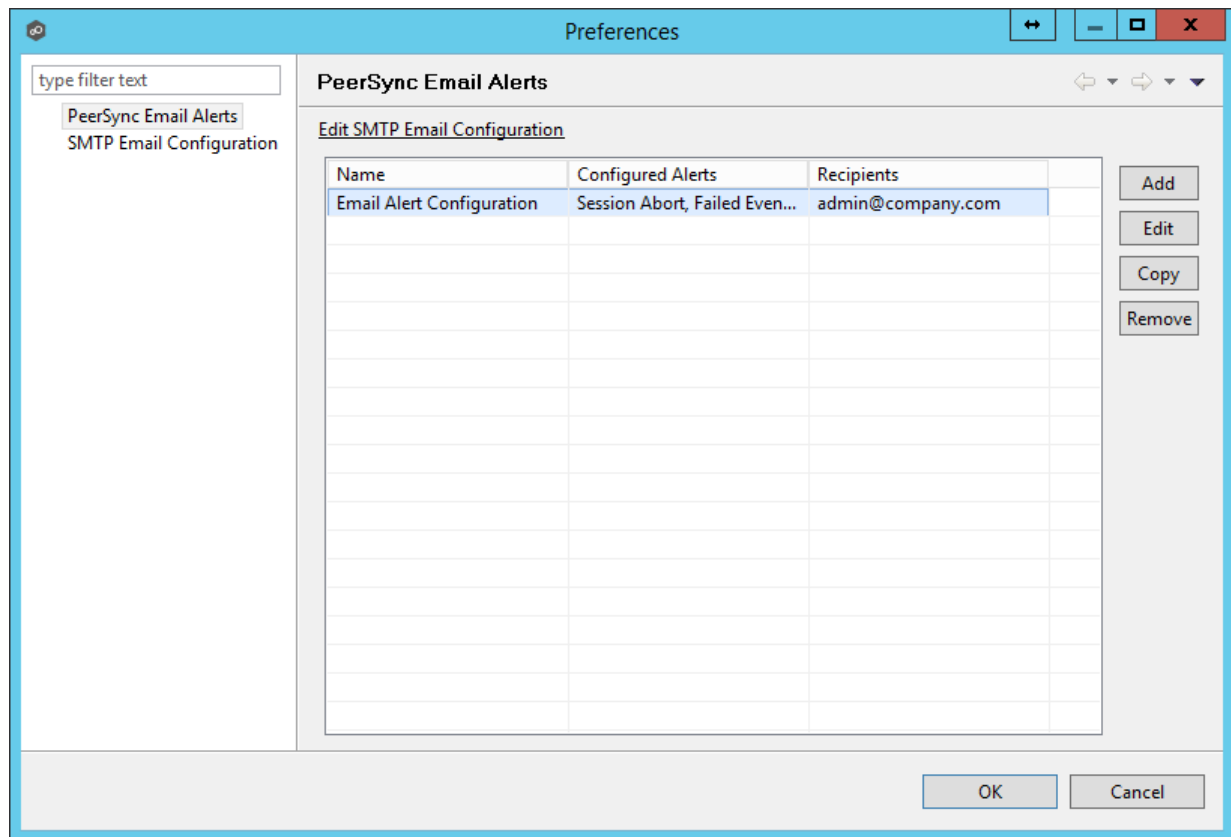
The following configuration items are not always required, but highly recommended:

- [Email Configuration](#)
- [Email Alerts](#)

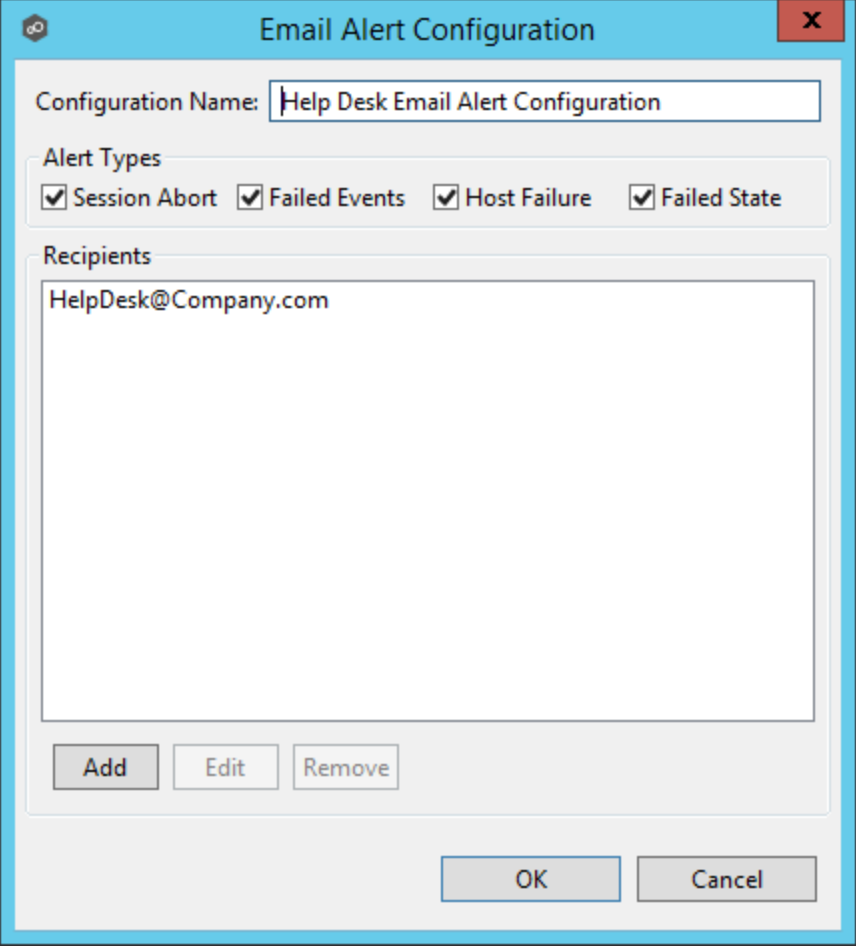
## Overview

The Peer Management Center supports the concept of email alerts, where a single alert (consisting of a unique name, a selection of event types along with a list of email addresses) can be applied to multiple file synchronization jobs without requiring repeat entry for each job. When an email alert is applied to a job, an email is sent to all listed recipients anytime a selected event type is triggered by that job.

To manage email alerts, right-click any file synchronization job from the Jobs view and select the **Email Alerts** node from the **Monitoring** node. Click **Edit PeerSync Email Alerts**. The following screen represents the list of defined email alerts, along with buttons to add new ones and edit, copy, and remove existing ones.



Upon adding or editing an email alert, the following dialog is displayed:

The image shows a Windows-style dialog box titled "Email Alert Configuration". At the top, there is a text field for "Configuration Name" containing the text "Help Desk Email Alert Configuration". Below this is a section titled "Alert Types" containing four checked checkboxes: "Session Abort", "Failed Events", "Host Failure", and "Failed State". Underneath is a section titled "Recipients" with a text area containing the email address "HelpDesk@Company.com". At the bottom of the "Recipients" section are three buttons: "Add", "Edit", and "Remove". At the very bottom of the dialog are "OK" and "Cancel" buttons.

Email Alert Configuration

Configuration Name: Help Desk Email Alert Configuration

Alert Types

☒ Session Abort ☒ Failed Events ☒ Host Failure ☒ Failed State

Recipients

HelpDesk@Company.com

Add Edit Remove

OK Cancel

Within this dialog, you can select specific event triggers on which an email will be generated and configure the list of email recipients of the alert(s). Event types are defined below.

## Event Types

<b>Session Abort</b>	Enables sending an alert when a session is aborted because of lack of quorum due to one or more failed host agents.
<b>Failed Events</b>	Enables sending an alert when a failed event is received from the PeerSync machine.
<b>Host Failure</b>	Enables sending an alert when a host agent timeout occurs or a PeerSync service timeout occurs.

<b>Failed State</b>	Enables sending an alert when the state of the File Synchronization machine changes from Active to "Failed State" indicating that either a failed scan or failed event was detected in the latest set of synchronization stats.
---------------------	---

## Integrating Existing PeerSync Instances

The topics in this section provide some basic information on how to integrate existing PeerSync instances within the Peer Management Center.

- [Requirements](#)
  - [How to Integrate Existing PeerSync Instances](#)
- 
- PeerSync must be installed as a Service and running version 9.3.0 or newer.
  - Peer Agent must be installed on the PeerSync machine and connected to the Peer Management Center.
- 
1. Open the profile on the PeerSync machine with the PeerSync Profiler.
  2. Add the argument /LZTAI in Options/Command section.
  3. Save the profile.
  4. Restart the PeerSync Service.
  5. Install the Peer Agent.
  6. Start the Peer Agent.

Once the Peer Agent is started and connected to the Peer Management Center, PeerSync will be auto detected and a Peer Management Center file synchronization job will be generated with the name of the machine.

Optionally you can edit the job and add [email alerts](#) and save and restart the File Synchronization job for changes to take effect.

### Deploying New PeerSync Instances

The topics in this section provide basic information on how to integrate existing PeerSync instances within the Peer Management Center:

- [Requirements](#)
- [How To](#)

- Peer Agent must be installed on the machine where PeerSync will be deployed to.
- It is recommended to run the Agent under a domain admin account or account with enough rights to modify registry and service configuration.

The topics in this section provide step-by-step instructions on how to create and deploy new PeerSync instances through Peer Management Center.

- [Step 1: General Information](#)
- [Step 2: PeerSync Profile](#)
- [Step 3: Jobs Configuration List](#)
- [Step 4: Installation Settings](#)

### Step 1: General Information

Create a new PeerSync Management job by clicking the **Create New** button in the toolbar of the Peer Management Center, or by selecting the **New** from the **File** menu. A list of all available job types will be displayed. Selecting the **PeerSync Management** option will open the PeerSync Management **Configuration** dialog.

The first page of configuration will be for general information such as Host Participants and Job name tag.

File Synchronization Configuration

1 of 4 - General Information

Generic information on this PeerSync configuration

Name: [COMPUTERNAME] - EMEA\_Region

Job Name Tag

Available

Host	Computer Description
Win12x64a	

Add Remove

Selected

Host	Computer Description

< Back Next > Finish Cancel

1. The job name will default to the computer name of the host participant. If you wish to group your computers, you can optionally add a name tag in the text box next to the job name (e.g., East Coast, EMEA, Region2). This will help in filtering machines by their given tag.

2. A list of all available hosts that have not yet been configured with a PeerSync installation, will appear in the **Available** table on the top of the page. Available hosts are any host with a Peer Agent installed that has successfully connected to the configured Peer Management Center Broker. The name that will be displayed is the computer name of the server that the Peer Agent is running on. If a particular host is not displayed in the list, then try restarting the Peer Agent Windows Service on that host, and if it successfully connects to Peer Management Center Broker, then the list will be updated with the computer name of that host.

**Note: Computer Description** is defined through Windows on a per-computer basis.

3. Select one or more hosts from the **Available** table and click the **Add** button to add the hosts to the **Selected** table. These are the hosts you wish to deploy the PeerSync configuration and installation to.

#### Step 2: PeerSync Profile

In the second page, choose a preconfigured profile from the available templates, or browse to load a PeerSync profile you may have configured through the PeerSync Profiler and saved as a .snc file on this system.

You may also choose to start from scratch by choosing **Other** from the drop-down menu.

Enter or update the **Profile Description** and **Performance Options**.



File Synchronization Configuration

**2 of 4 - PeerSync profile**

Profile Configuration

Pre-Defined Profile

Profile Description

Performance Options

Maximum number of Job Threads

Maximum number of Copy Threads

< Back   Next >   Finish   Cancel

<b>Profile Description</b>	A textual description of the current profile.
<b>Maximum number of Job Threads</b>	Maximum number of job scans that can run parallel to one another.
<b>Maximum number of Copy Threads</b>	Maximum number of events that can be processed parallel to one another.

In this page, modify the loaded PeerSync jobs and/or add new jobs by clicking on the **Add** or **Edit** button to the right of the view.

[illegible]

For more information, see [Edit/Configure Jobs](#).

Step 4: Installation Settings

In the last page of the PeerSync Management Configuration wizard, enter the installation settings for this PeerSync instance.

File Synchronization Configuration

4 of 4 - Installation Settings

Remote Installation Settings

Pre-Defined Settings

EastCoast

Name

EMEA

Installation Path

%ProgramFiles%\Peer Software\PeerSync

Existing Exe

peersync93-9\_3\_1\_1007.exe

Browse

Imported Exe Version: v9.3.1.1007 [C:\Program Files (x86)\Peer Software\Peer Management Hub\Hub\workspace\peersync\templates\exes\peersync93-9\_3\_1\_1007

License

User Name

Peer Software

Company

Peer Software

Options

Password

Service

Logon User

bytemetrics\adminidanielad

Password

.....

< Back

Next >

Finish

Cancel

<b>Pre-Defined Settings</b>	<p>A list of previously used Installation Settings with the Name given at the time of use.</p> <p>Note: If the installation settings have the same path, service user name, license password, and installation exe, a new Installation record will not be created, regardless if a new name has been given to the Installation Settings.</p>
-----------------------------	--

<b>Installation Path</b>	Path where PeerSync will be installed. When using the %ProgramFiles% variable, PeerSync will install in the x86 Program Files directory for 64-bit systems, otherwise it will install in the Program Files base directory.
<b>Existing Exe</b>	A list of PeerSync executables available in the template folder or used in a past installation. This is the PeerSync executable that will be used to install PeerSync.
<b>License User Name</b>	License information provided by Peer Software. Cut and paste the User Name section in this field.
<b>License Company</b>	License information provided by Peer Software. Cut and paste the Company section in this field.
<b>License Options</b>	License information provided by Peer Software. Cut and paste the Options section in this field.
<b>License Password</b>	License information provided by Peer Software. Cut and paste the Password section in this field.
<b>Service Logon User*</b>	<p>This is the Service account User Id used to run the PeerSync Service (DOMAIN\USER).</p> <p>Note: This account must be valid on all included participants for this File Synchronization Configuration.</p>
<b>Service Password</b>	PeerSync Windows Service account Password.

**\*Note:** When using a service account that has not been granted to run as a service on the machine, PeerSync will fail to start return the following Global Alert to the Peer Management Center. This will indicate that PeerSync could not start and you will have to log on to that machine and confirm the credentials to grant access to that account to run as a service.

**Hub Alert Details**

Received at: 09-30-2015 13:08:52

Severity: Warning

Category: Global Resource

Host Name: Peer Management Center

Locally Generated at: 09-30-2015 13:08:52

Name: Process PeerSyncEvent

Message: pe..... Last Event=PeerSyncEvent [host=Win12x64a, eventType=SERVICE\_CMD, description=The service did not start due to a logon failure., exception=null, errorCode=0, coordinationId=null, eventId=66, properties = {}] : The service did not start due to a logon failure.

Click outside of popup to close

Once the Configuration Settings have completed, click **Finish** and the installation configuration will be sent to the selected Participants.

A File Synchronization job will be auto created for each Participant and set to be in a Pending Installation state. Once the installation completes and PeerSync reports to the Peer Management Center, the state will change to Running/Active.

**Synchronization Summary**

Runtime Summary View (auto-update enabled)

Filter by: [ ] Actions [ ] ☒ Enable Auto

Name	Overall Status	Backup Status	Failed Scans	Failed Events	Messages	Pending Events	Pending Retries	Checked	Updated
Composite4a[East_Coast]	PeerSync Service Not Avail...	N/A							
DDWin12R2a[EastCoast]	Running	Normal	0	0	0	No Pending Items	0	5738	5389
DDWin12R2b[WestCoast]	Running - Failed State	Target Folders ...	1	3	8	No Pending Items	0	258	0
VMSRV2008X32[Asia]	Stopped [Pending Installat...	N/A							
Win12x64a[EMEA_Region]	Running	Normal	0	0	0	No Pending Items	0	26880	0

**Install PeerSync**

Scheduling PeerSync Operation Task

☐ Always run in background

Run in Background Cancel Details >>

## Logging and Alerts

Use the following dialog to enable or disable logging and alerts, including specifying event types to log.

**File Synchronization Configuration [DDWin12R2b]**

**Monitoring**

- Logging and Alerts**
- Email Alerts

**Associated Profile**

- Jobs
- Global Settings
- Associated Installation

**Logging and Alerts**

Enabled: ☒

Severity: All

**Event Types**

☐ Stats Update
 ☒ Profile Update
 ☒ Profile Distribution

☒ PeerSync Service Start
 ☒ PeerSync Service Stop
 ☒ Failed Events Reprocess

☒ Restart Detected

**Alerts**

Severity: WARNING

OK Cancel

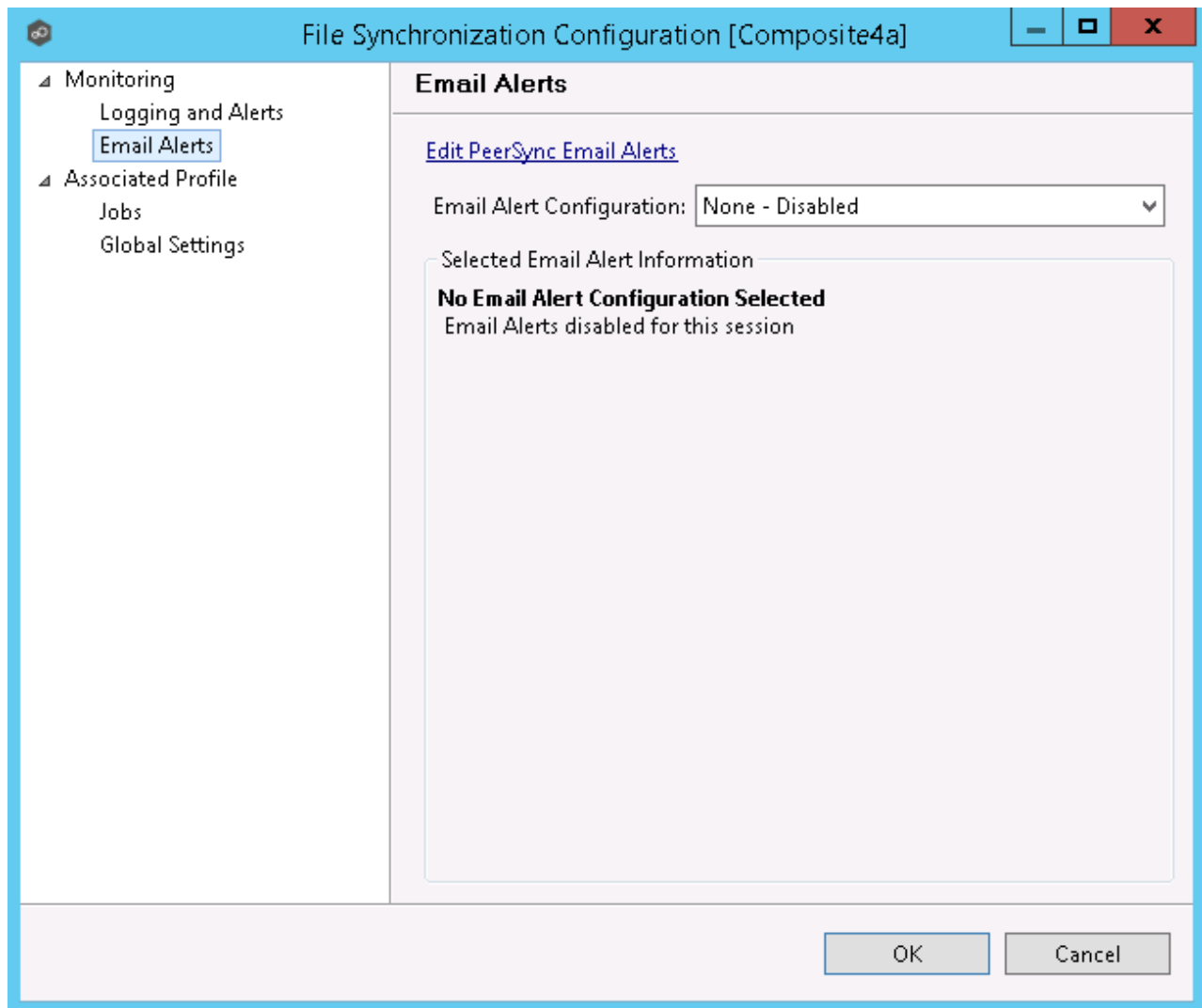
<b>Stats Update</b>	Log when PeerSync Stats are received (This could generate large amount of Log Entries).
<b>Profile Update</b>	Log whenever the PeerSync Profile configuration is updated.
<b>Profile Distribution</b>	Log when the PeerSync Profile is distributed to one or more hosts.

<b>PeerSync Service Start</b>	Log when a user initiates a PeerSync Service Start.
<b>PeerSync Service Stop</b>	Log when a user initiates a PeerSync Service Stop.
<b>Failed Events Reprocess</b>	Log when a user initiates a Failed Event Reprocess.
<b>Restart Detected</b>	Log when Peer Management Center detects that the PeerSync service has been restarted by comparing known Session Id with received one.

## Email Alerts

Email alerts configuration is available by selecting **Email Alerts** from the tree node within the PeerSync Management Configuration dialog.

Email alerts are configured at a global level, then applied to individual jobs. The following screen shows how this is accomplished.



To enable email alerts for this job, select an email alert from the drop-down list. To disable, select **None - Disabled**.

## Running and Managing a PeerSync Management Job

This section includes topics for managing your PeerSync Management Jobs.

- [Starting and Stopping](#)
- [Synchronization Summary View](#)
- [Synchronization Dashboard Summary View](#)



- [PeerSync Profile Management](#)
- [PeerSync Service Management](#)
- [Runtime Job Views](#)
- [Upgrade/Reprocess Installation](#)

## Starting and Stopping

### Starting a PeerSync Management Job

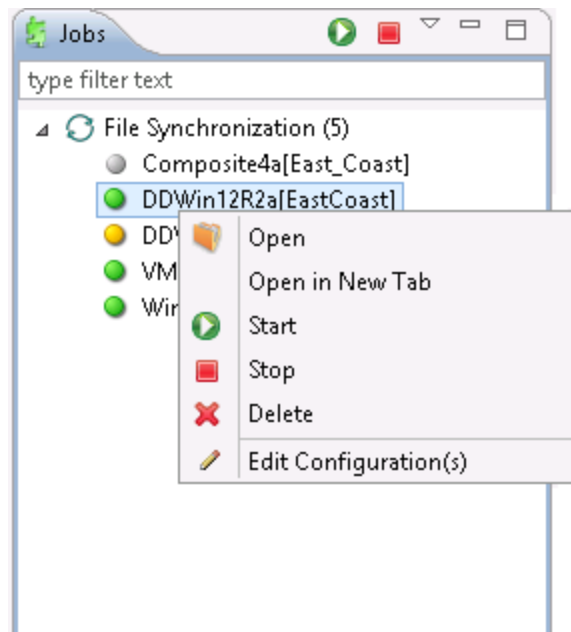
A PeerSync Management job is auto-started as soon as the Agent connects to the Peer Management Center; normally you will not need to manually start the job.

Click the **Start** button to begin the session.

### Stopping a PeerSync Management Job

You can stop a PeerSync Management job at any time by pressing the **Stop** button. Doing this will shut down the monitoring of the specific PeerSync host(s).

**Note:** If the job is stopped and the participating host is still running an instance of the PeerSync software, the job will auto start the next time that host agent is restarted or a Reconnect is detected.



### PeerSync Management Summary

The **Synchronization Summary** view aggregates critical status and statistical information from all configured PeerSync Management jobs in a single table view. It is automatically displayed when the Peer Management Center client is started and can be opened at any other time by double-clicking on the **PeerSync Management** parent tree node in the Job's View or by clicking the **View Runtime Summary** icon in the toolbar of the Jobs view.

Information in this view can be sorted and filtered. Operations such as starting, stopping, and editing multiple jobs at once are available, in addition to the ability to clear Monitoring Alerts, Start PeerSync, Stop PeerSync, Reprocess Failed Events, Request Support Info File and Reprocess/Upgrade Installation.

The screenshot shows a window titled "Synchronization Summary" with a sub-header "Runtime Summary View (auto-update enabled)". Below the header, there is a "Filter by:" dropdown, an "Actions" dropdown, and a checkbox for "Enable Auto-Update" which is checked. To the right of the checkbox is a "Refresh" button and a numeric input set to "10" with "seconds" next to it. The main area contains a table with the following data:

Name	Overall Status	Backup Status	Failed Scans	Failed Events	Messages	Pending Events	Pending Retries	Checked
Composite4a	Running - Failed State	Target Folder i...	1	0	0	No Pending It...	0	0
DDWin12R2a[East...	PeerSync Service No...	Normal	0	0	0	No Pending It...	0	484
DDWin12R2b[Wes...	Running	Normal	0	0	2	No Pending It...	0	2895

Unlike other views within the Peer Management Center, the **Synchronization Summary** view is not updated in real-time. This is done for performance reasons. Instead, the table can be set to automatically update itself every few seconds. Clicking **Enable Auto-Update** enables this functionality, while the refresh interval (in seconds) can be set right beside the checkbox. Additional columns can be added to and removed from the table from the right-click context menu.

Double-clicking any item in the table will automatically open the selected PeerSync Management job in a tab within the **Runtime Summary** view, allowing you to drill down and view specific information about that single job. Items in the summary table can be filtered by job name, overall status, activity state and host participant name.

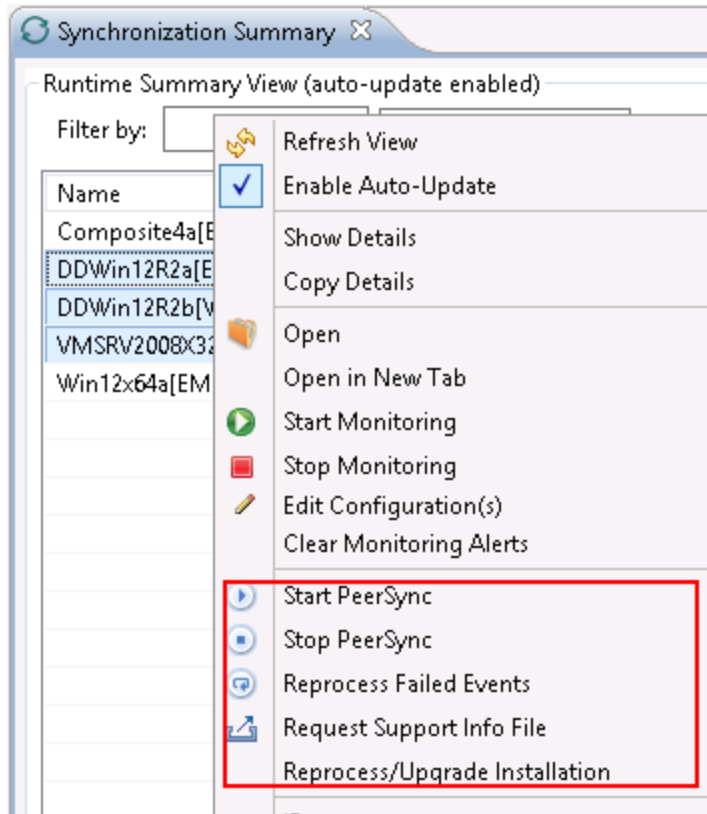
Selecting one or more items in the table, then right-clicking will bring up a context menu of available actions that can be performed on the selected jobs. The actions that are unique to this table are as follows:

<b>Clear Monitoring Alerts</b>	Clears all monitoring alerts for the selected jobs. This can be performed while a job is running.
--------------------------------	---

**PeerSync multi-job global actions:**

**Clear Monitoring Alerts**

Clears all monitoring alerts for the selected jobs. This can be performed while a job is running.



<b>Start PeerSync</b>	Send a Start command to the PeerSync service instance running on the selected jobs' participant. This can be performed while the associated File Synchronization Job is running.
<b>Stop PeerSync</b>	Send a Stop command to the PeerSync service instance running on the selected jobs' participant. This can be performed while the associated File Synchronization Job is running.
<b>Reprocess Failed Events</b>	Send a Reprocess Failed Events command to the PeerSync instance running on the selected jobs' participant. This can be performed while the associated File Synchronization Job is running.
<b>Request Support Info File</b>	Send a request to collect the Support info File from the PeerSync instance running on the selected jobs' participant. This can be performed while the associated File Synchronization Job is running.

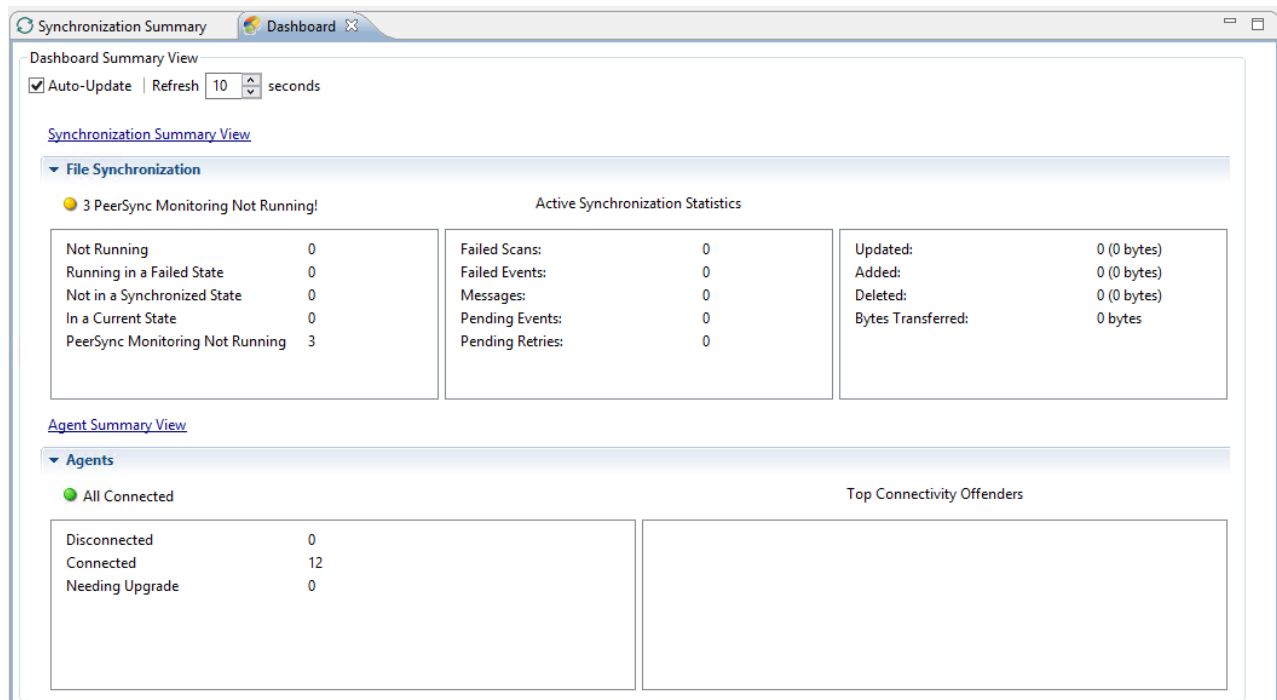
<b>Clear Monitoring Alerts</b>	Clears all monitoring alerts for the selected jobs. This can be performed while a job is running.
<b>Reprocess/Upgrade Installation</b>	Deploy an upgrade or reprocess an existing installation for the selected File Synchronization Job(s). <a href="#">Upgrade/Reprocess Installation</a>

Clicking the **Actions** table menu provides the following options:

<b>Refresh View</b>	Refresh all information provided in the table.
<b>Copy All Filtered Statistics</b>	Copy detailed information to the system clipboard for all items current displayed in the table, taking any filters into account. This information can then be pasted into a text editor.
<b>Export Entire Table to File</b>	Dump the entire contents of the table to a text file that can be viewed in any text editor.

### PeerSync Management Dashboard Summary View

The **PeerSync Management Dashboard Summary** view is a view that displays metrics and key performance indicators from all running PeerSync Management jobs. It is automatically displayed when the Peer Management Center client is started and can be opened at any other time by selecting **View Dashboard** from the **Window** menu or by clicking the **View Dashboard** icon in the Peer Management Center toolbar.



The Dashboard is not updated in real-time. This is done for performance reasons. Instead, the table can be set to automatically update itself every few seconds. Enabling the **Auto-Update** option will enable this functionality, while the **Refresh** interval (in seconds) can be set right beside the checkbox.

Entries in the first column of the **PeerSync Management Job** and **Agents** categories can be double-clicked, which will take the user to a filtered Runtime view of the selected item for additional details.

## Managing the PeerSync Profile

The topics in this section provide some basic information about PeerSync Profile Management:

- [Updating the Profile Configuration](#)
- [Importing an Existing Profile](#)
- [Distributing a Profile](#)

This topic provides information on how to update a PeerSync profile from the Peer Management Center.

If using the Peer Management Center to manage the PeerSync instances, we recommend making changes through the Peer Management Center. If changes are made directly on the PeerSync machine, they should be [imported](#) in the Peer Management Center job manually to keep the Peer Management Center PeerSync Configuration in sync.

## How to Update a PeerSync Profile through Peer Management Center

- From the **PeerSync Management Summary** runtime view (double-click the **PeerSync Management jobs** node from the left), right-click the machine you wish to modify the profile for and choose **Edit Configuration(s)**. Alternatively, you can right-click the machine job from the left menu under the **PeerSync Management** node and choose **Edit Configuration(s)**.
- You can update the Profile by importing an updated Profile through the **Import** button in the **Associated Profile** page, or manually update the configuration through **Jobs and/or Global Settings** section.
- If you wish to update the profile outside of the Peer Management Center, export the existing configuration using the **Export** button in **Associated Profile** page. Make your changes through the PeerSync Profiler and import the updated Profile back into Peer Management Center through the **Import** button.
- After having made your entire configuration changes either through Peer Management Center or by [importing](#) the updated Profile, choose **OK** and close the **Edit Configuration** dialog.

Your configuration changes will not reach the PeerSync machine until they are [distributed](#). The updated profile will become active on the machine after the PeerSync service has been restarted.

- [Import Existing Profile](#)
- [Edit/Configure Jobs](#)
- [Edit Global Settings](#)
- [Distribute Profile](#)

### Importing an Existing Profile

In the **Associated Profile** section of the **PeerSync Management Configuration** dialog, you can update the configured profile with one you have saved and configured outside of the Peer Management Center.

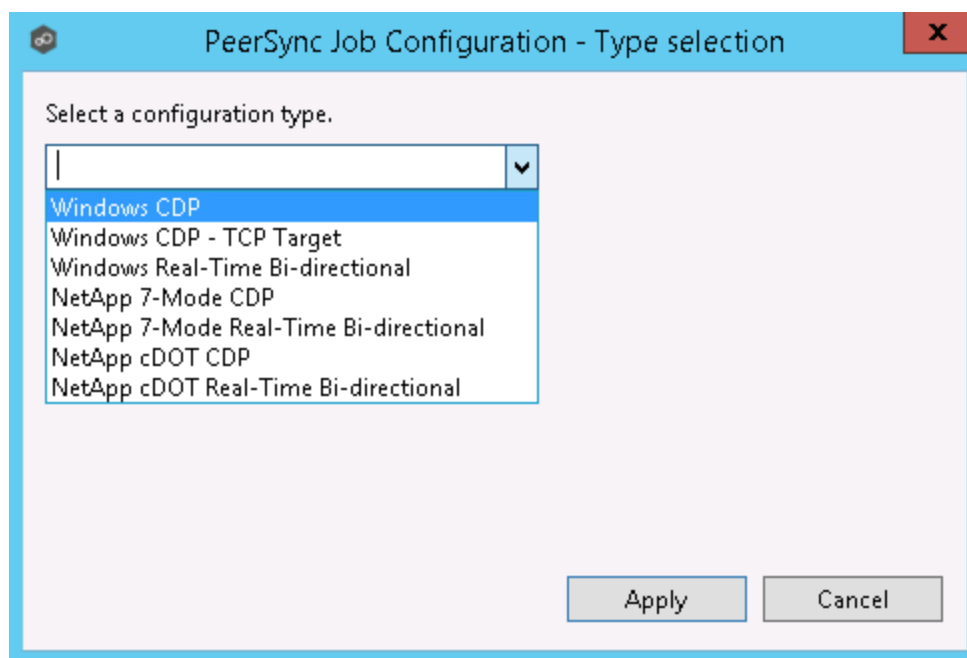
**Note:** If making changes outside of the Peer Management Center, we recommend exporting the profile from the Peer Management Center (by clicking the **Export** button), making necessary changes outside of the Peer Management Center, and finally importing the profile back into the Peer Management Center.

Click the **Import** button on the right of the dialog to import the profile. To propagate this new updated profile, close the **PeerSync Management** dialog, reopen it and distribute to the PeerSync host through the [Distribute](#) button.

The screenshot shows a window titled "File Synchronization Configuration [DDWin12R2a]". On the left is a sidebar with a tree view containing: Monitoring, Logging and Alerts, Email Alerts, Associated Profile (selected), Jobs, Global Settings, and Associated Installation. The main area is titled "Associated Profile" and contains four input fields: "Description:" with the value "Backup", "File Name:" with "DDWin12R2a.snc", "Last Updated On:" with "Aug 24, 2015 10:47:38 PM", and "Current State:" with "Active". To the right of these fields are three buttons: "Export", "Import", and "Distribute". Below the input fields, it states "Total number of jobs configured in this profile is 1". At the bottom right of the dialog are "OK" and "Cancel" buttons.



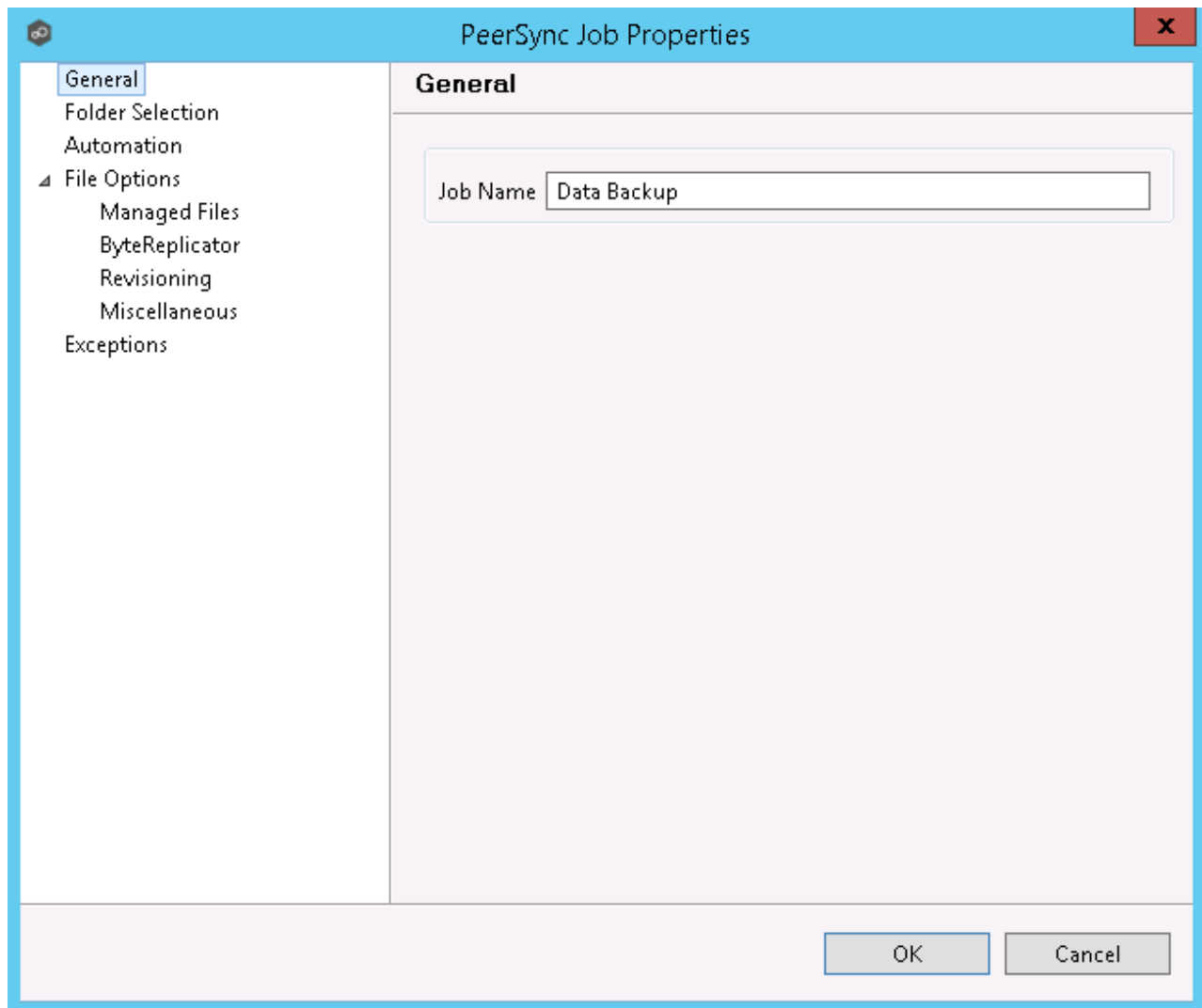




Once a job type has been selected, click **Apply** and complete the PeerSync Job Configuration wizard to complete the job configuration and add the job to the profile.

## Edit Existing Job

To edit an existing job, select the job in the **Jobs** view, and then click the **Edit** button on the right. The **PeerSync Job Properties** dialog will open with all available settings grouped by category in the navigation tree.



## Enable/Disable Job

To enable or disable a job, click the checkbox to the left of the job name in the **Jobs** view.

To save these changes, click **OK** on the bottom right of the **PeerSync Management Configuration** dialog.

## Copy Job

You can copy an existing job by selecting the job from the **Jobs** view and clicking the **Copy** button on the right. The **PeerSync Job Properties** dialog will open, allowing you to make changes to the copied job.

**Note:** You must make at least one change to the job settings. If the job settings remain identical, it will not be saved after the **OK** button is clicked.

## Remove Job

To remove jobs from the PeerSync Configuration, select one job from the **Jobs** view, click the **Remove** button on the right. Repeat this for any additional jobs you wish to remove.

### Editing Global Settings

In the **Global Settings** of the **PeerSync Management Configuration** dialog, you can make changes to settings that apply to all PeerSync Jobs within the profile.

The screenshot shows the 'File Synchronization Configuration [DDWin12R2a]' dialog box. The 'Global Settings' tab is selected in the left sidebar. The main content area is divided into three sections:

- Recovery Options:**
  - Retry open/inaccessible files: ☒ 1 times
  - Retry Failed Connection every: ☒ 1 minutes
- Performance Options:**
  - Maximum number of Job Threads: 5
  - Maximum number of File Threads: 10
  - Use Enhanced Event Processing: ☒
- Reconnect Options:**
  - Reconnect Options: Run a Scan on reconnect
  - Application Priority Selection: Normal

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

<b>Recovery Options</b>	These changes will update how we retry failed or inaccessible files as well as the interval in which we retry Failed Connections.
<b>Performance Options</b>	These settings allow you to change the maximum number of job scans that can run parallel to one another and the maximum number of events that can be processed parallel to one another.
<b>Reconnect Options</b>	This setting allows you to choose how PeerSync handles a re-established connection. Options are to Run a Scan on Reconnect or Store missed events and process on reconnect.

<b>Application Priority Selection</b>	This setting enables to select the priority level you want PeerSync to have.
---------------------------------------	--

### Distributing a Profile

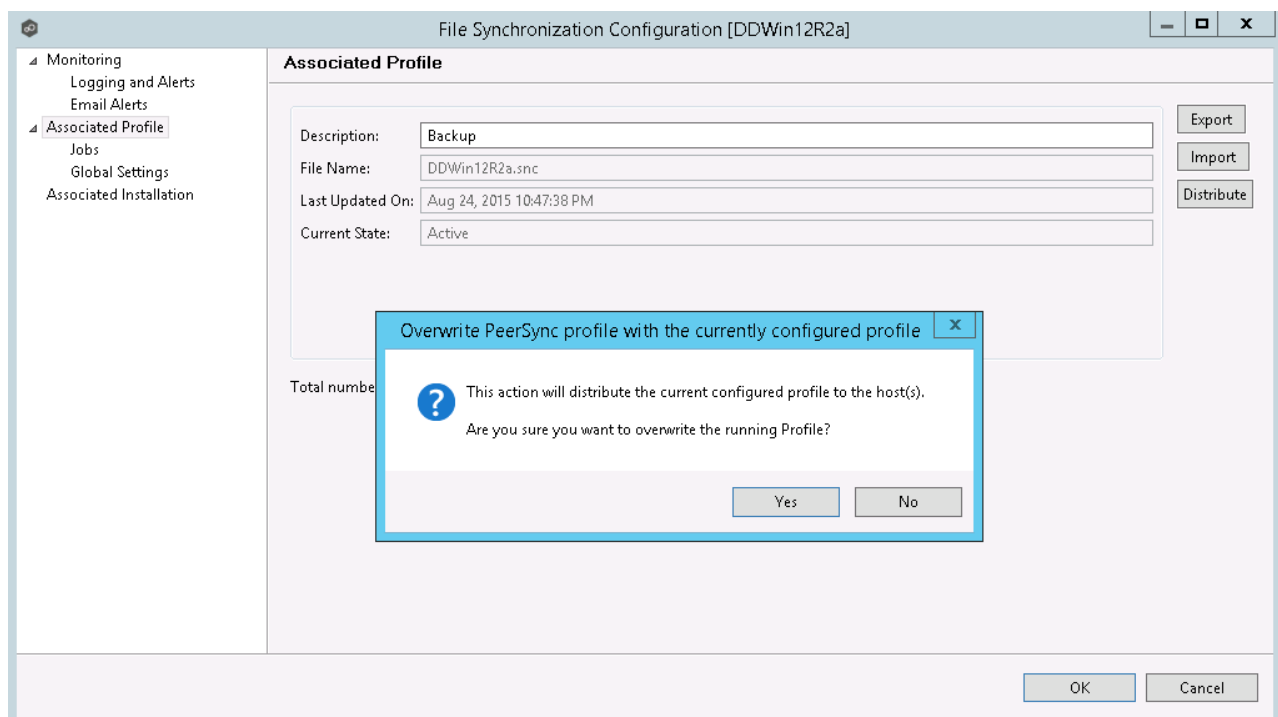
This topic covers information on how to distribute changes to the PeerSync profile from the Peer Management Center

To distribute the PeerSync profile changes, right-click the PeerSync Management job from the **Jobs** view, and then click **Edit Configuration**.

In the **PeerSync Management Configuration** screen, click the **Associated Profile** node, and then click the **Distribute** button.

In the event that one or more of your jobs are configured to use a ByteReplicator Relay Server (usually used in NetApp source environments), the Distribute Profile process will also distribute your relay Server configurations by compiling all unique target Hosts and relay servers into a `%profilename%.pls` file. This file will be distributed to the PeerSync machine alongside the profile.

**Note:** This action will distribute the profile to the machine and attempt to stop and start PeerSync Service to commit those changes. If you do not wish to restart the PeerSync service, wait to distribute the profile until you are ready to have the service restart.



## Managing the PeerSync Service

The following PeerSync service management actions are available from the [Synchronization Summary view](#) and the [Summary view](#) for a specific PeerSync Management job.

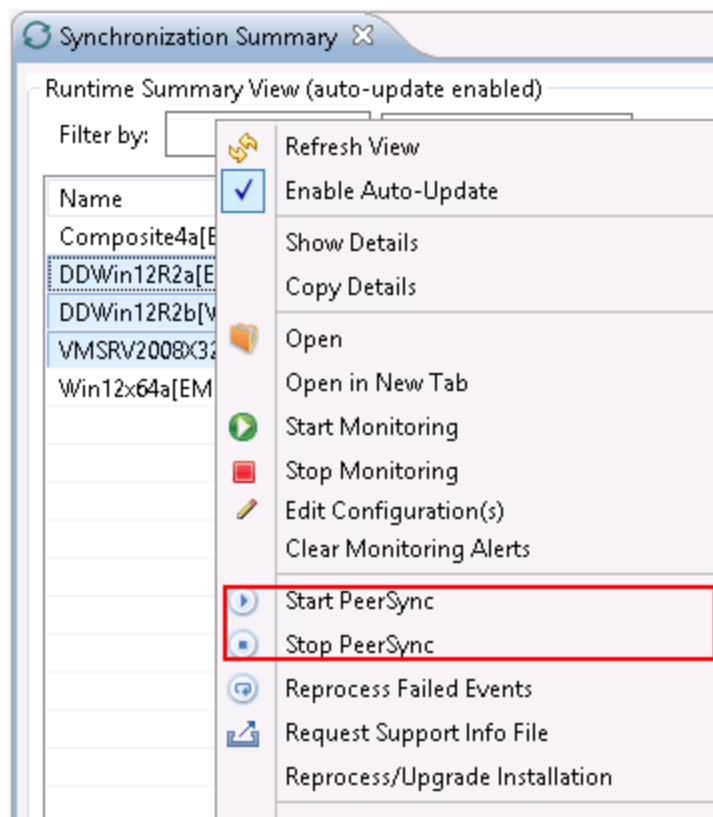
## Starting the PeerSync Service

To start the PeerSync service associated with any PeerSync Management job, right-click the view and choose **Start PeerSync**.

## Stopping the PeerSync Service

To stop the PeerSync service associated with any PeerSync Management job, right-click the view and choose **Stop PeerSync**.

**Note:** The associated PeerSync Management job must be running in order to successfully perform this action.



For information on the additional PeerSync multi-job global actions, see [Synchronization Summary View](#).

### Runtime Job Views

Double-clicking on the PeerSync Management job from the [Synchronization Summary view](#) will open the job-specific runtime views.

- [Summary View](#)
- [Failed Events View](#)
- [Monitoring Log View](#)
- [Alerts View](#)
- [Participants View](#)
- [Configuration View](#)

Summary
Failed Events (2)
Monitoring Log
Alerts (16)
Participants (1)
Configuration

Summary View
Actions

<b>Monitoring Peerlet Session</b>		Failed	Started: 9/30/15 12:23 PM	
Stats Timestamp	9/30/2015 1:56:51 PM			
Stats State	Failed			
<b>PeerSync Running Info</b>			Started: 9/30/2015 12:09:46 PM	
Mode	Automatic and Real-Ti...			
Status	Target Folders are Not A...			
<b>PeerSync Real Time Stats</b>				
Real Time Events	128			
Real Time Events Peak	53.318 events/minute			
Real Time Events In Process	0			
Real Time Events Average	1.195 events/minute			

Overview
PeerSync Jobs Stats
Added
Updated
Deleted
Messages

<b>PeerSync Overall Status</b>					
Checked	260	Updated	0	Current Event Status	Real-time Monitoring (Failed Scans: 1) (Failed Events...
Excluded	0	Added	0	Pending Event Status	No Pending Items
Messages	11	Deleted	0	Bytes Transferred	0 bytes
Elapsed Time: 01:47:08 Xfer Rate: N/A					

When double-clicking a PeerSync Management job, the default selected tab will be the **Summary** tab. This view will show information received by the PeerSync machine on the status of the PeerSync Management job.

Information found in this view is global to the PeerSync profile. To see PeerSync job-specific statistics, click the [PeerSync Jobs Stats](#) tab.

Information on this view is received whenever the information changes on the PeerSync machine, normally every 1 minute or so. To auto-refresh this view with the latest data, click **Enable Auto-Update** on the top right of the view, and choose a Refresh cycle. The cycle is the not the cycle



for receiving the information, just to refresh the view with the latest information received by PeerSync.

Summary
Failed Events (2)
Monitoring Log
Alerts (16)
Participants (1)
Configuration

Summary View
Actions

**Monitoring Peerlet Session** Failed Started: 9/30/15 12:23 PM  
Stats Timestamp 9/30/2015 1:56:51 PM  
Stats State Failed

**PeerSync Running Info** Started: 9/30/2015 12:09:46 PM  
Mode Automatic and Real-Ti...  
Status Target Folders are Not A...

**PeerSync Real Time Stats**  
Real Time Events 128  
Real Time Events Peak 53.318 events/minute  
Real Time Events In Process 0  
Real Time Events Average 1.195 events/minute

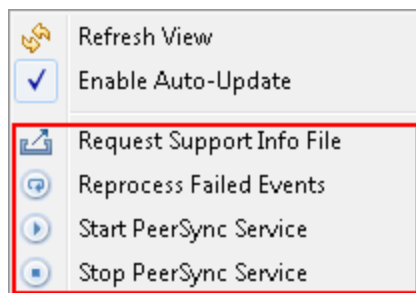
Overview
PeerSync Jobs Stats
Added
Updated
Deleted
Messages

**PeerSync Overall Status**

Checked	260	Updated	0	Current Event Status	<span>Real-time Monitoring (Failed Scans: 1) (Failed Events...</span>
Excluded	0	Added	0	Pending Event Status	No Pending Items
Messages	11	Deleted	0	Bytes Transferred	0 bytes

Elapsed Time: 01:47:08 Xfer Rate: N/A

On this page, you can right-click to display the PeerSync **Actions** menu:



On the bottom half of the page, you will find a set of tabs showing more granular information regarding this PeerSync session.

- [PeerSync Jobs Stats](#)
- [Added Files](#)
- [Updated Files](#)
- [Deleted Files](#)
- [Messages](#)

### PeerSync Jobs Stats

When clicking the **PeerSync Jobs Stats** view, a request goes out to the PeerSync machine to request job-specific statistics and return them to the Peer Management Center to be displayed. These statistics can be requested only if PeerSync is running on that machine and only if the PeerSync Management job is started on the Peer Management Center.

When the statistics are received, the view is updated with the job-specific statistics and the caption on the top of the view will show the date and time the list was last updated.

By right-clicking on the info table, you can choose to hide or show columns.

Overview	PeerSync Jobs Stats	Added	Updated	Deleted	Messages
----------	---------------------	-------	---------	---------	----------

Jobs Stats (List Updated on 09-30-2015 13:55:40)											
3 jobs		Filter by:									
Job Na...	Source	Target	Last Scan (Status: Durati...	Xfer Rate	Event Averages	Upda...	Added	Delet...	Mess...	Fail...	Status
● Data ...	c:\source\	c:\target\	9/30/2015 12:09:47 PM (...)	N/A	0.00 per min (0...	0 (0 ...	0 (0 ...	0 (0 ...	0	0	Normal
● Data2...	c:\source2\	c:\target2\	9/30/2015 12:09:47 PM (...)	N/A	0.00 per min (0...	0 (0 ...	0 (0 ...	0 (0 ...	0	0	Normal
● Data ...	c:\source3\	\\backupserve...	N/A	N/A	0.00 per min (0...	0 (0 ...	0 (0 ...	0 (0 ...	11	3	Target Not Available (Scan on Re...
All Jobs	-----	-----	N/A	N/A	0.00 per min (0...	0 (0 ...	0 (0 ...	0 (0 ...	11	3	Target Folders are Not Available f...

### Added Files

When clicking the **Added** tab, a request goes out to the PeerSync machine to request a list of latest added files and return it to the Peer Management Center to be displayed. This list can be requested only if PeerSync is running on that machine and only if the PeerSync Management job is started on the Peer Management Center.

When the list is received, the view is updated with the latest added events processed by PeerSync, and the caption on the top of the view will show the date and time the list was last updated.

By right-clicking on the info table, you can choose to hide or show columns.

This information in this table can be filtered by Path or by Job Name.

Overview

PeerSync Jobs Stats

Added

Updated

Deleted

Messages

Added Log

0 errors, 0 warnings, 100 others

Filter by:

Date	Type	Path	Comments	Message	Job Name	File Size	Modified Time
09-15-2015 17:0...	Event	c:\target\FILE42.TXT	Added [Attrib...		Data Backup	2.3 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE44.TXT	Added [Attrib...		Data Backup	1.9 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE43.TXT	Added [Attrib...		Data Backup	4.0 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE45.TXT	Added [Attrib...		Data Backup	4.0 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE47.TXT	Added [Attrib...		Data Backup	1.7 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE46.TXT	Added [Attrib...		Data Backup	1.6 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE48.TXT	Added [Attrib...		Data Backup	3.2 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE41.TXT	Added [Attrib...		Data Backup	3.3 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE50.TXT	Added [Attrib...		Data Backup	1.4 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE49.TXT	Added [Attrib...		Data Backup	2.7 KB	09-15-2015 17:01:27
09-15-2015 17:0...	Event	c:\target\FILE27.TXT	Added [Attrib...		Data Backup	2.1 KB	09-15-2015 17:01:26
09-15-2015 17:0...	Event	c:\target\FILE28.TXT	Added [Attrib...		Data Backup	3.9 KB	09-15-2015 17:01:26
09-15-2015 17:0...	Event	c:\target\FILE29.TXT	Added [Attrib...		Data Backup	2.6 KB	09-15-2015 17:01:26
09-15-2015 17:0...	Event	c:\target\FILE30.TXT	Added [Attrib...		Data Backup	3.9 KB	09-15-2015 17:01:26
09-15-2015 17:0...	Event	c:\target\FILE31.TXT	Added [Attrib...		Data Backup	2.8 KB	09-15-2015 17:01:26
09-15-2015 17:0...	Event	c:\target\FILE32.TXT	Added [Attrib...		Data Backup	1.9 KB	09-15-2015 17:01:26
09-15-2015 17:0...	Event	c:\target\FILE33.TXT	Added [Attrib...		Data Backup	1.9 KB	09-15-2015 17:01:26

### Updated Files

When clicking the **Updated** tab, a request goes out to the PeerSync machine to request a list of latest updated files and return it to the Peer Management Center to be displayed. This list can be requested only if PeerSync is running on that machine and only if the PeerSync Management job is started on the Peer Management Center.

When the list is received, the view is updated with the latest updated events processed by PeerSync, and the caption on the top of the view will show the date and time the list was last updated.

By right-clicking on the info table, you can choose to hide or show columns.

This information on this table can be filtered by Path or by Job Name.

Overview

PeerSync Jobs Stats

Added

Updated

Deleted

Messages

Updated Log

0 errors, 0 warnings, 100 others

Filter by:

Date	Type	Path	Comments	Message	Job Name	File Size	Modified Time
09-15-2015 17:0...	Event	c:\target\FLDR3\FILE33....	Updated [Attri...		Data Backup	2.5 KB	09-15-2015 17:03:50
09-15-2015 17:0...	Event	c:\target\FLDR3\FILE35....	Updated [Attri...		Data Backup	1.9 KB	09-15-2015 17:03:50
09-15-2015 17:0...	Event	c:\target\FLDR3\FILE37....	Updated [Attri...		Data Backup	3.8 KB	09-15-2015 17:03:50
09-15-2015 17:0...	Event	c:\target\FLDR3\FILE36....	Updated [Attri...		Data Backup	1.7 KB	09-15-2015 17:03:50
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE13....	Updated [Attri...		Data Backup	3.6 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE16....	Updated [Attri...		Data Backup	1.6 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE12....	Updated [Attri...		Data Backup	1.3 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE14....	Updated [Attri...		Data Backup	2.9 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE15....	Updated [Attri...		Data Backup	2.1 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE10....	Updated [Attri...		Data Backup	3.0 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE11....	Updated [Attri...		Data Backup	1.4 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE17....	Updated [Attri...		Data Backup	2.3 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE18....	Updated [Attri...		Data Backup	1.0 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE19....	Updated [Attri...		Data Backup	2.3 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE23....	Updated [Attri...		Data Backup	1.9 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE21....	Updated [Attri...		Data Backup	1.3 KB	09-15-2015 17:03:48
09-15-2015 17:0...	Event	c:\target\FLDR2\FILE20....	Updated [Attri...		Data Backup	3.0 KB	09-15-2015 17:03:48

### Deleted Files

When clicking on the **Deleted** tab, a request goes out to the PeerSync machine to request a list of latest deleted files and return it to the Peer Management Center to be displayed. This list can be requested only if PeerSync is running on that machine and only if the PeerSync Management job is started on the Peer Management Center.

When the list is received, the view is updated with the latest deleted events processed by PeerSync, and the caption on the top of the view will show the date and time the list was last updated.

By right-clicking on the info table, you can choose to hide or show columns.

This information on this table can be filtered by Path or by Job Name.

Overview | PeerSync Jobs Stats | Added | Updated | Deleted | Messages

Deleted Log (List Updated on 10-05-2015 11:57:51)

0 errors, 0 warnings, 10 others | Filter by:

Date	Type	Path	Comments	Message	Job Name	File Size	Modified Time
10-05-2015 11:5...	Data Bac...	c:\target\FLDR3	Scan		Session	0 bytes	10-05-2015 11:57:49
10-05-2015 11:5...	Data Bac...	c:\target\FILE6.TXT	Scan		Session	1.2 KB	10-05-2015 11:57:49
10-05-2015 11:5...	Data Bac...	c:\target\FILE4.TXT	Scan		Session	1.3 KB	10-05-2015 11:57:49
10-05-2015 11:5...	Data Bac...	c:\target\FILE8.TXT	Scan		Session	1.5 KB	10-05-2015 11:57:49
10-05-2015 11:5...	Data Bac...	c:\target\FILE2.TXT	Scan		Session	3.1 KB	10-05-2015 11:57:49
10-05-2015 11:5...	Data Bac...	c:\target\FILE5.TXT	Scan		Session	0 bytes	10-05-2015 11:57:48
10-05-2015 11:5...	Data Bac...	c:\target\FILE7.TXT	Scan		Session	2.1 KB	10-05-2015 11:57:48
10-05-2015 11:5...	Data Bac...	c:\target\FILE9.TXT	Scan		Session	2.2 KB	10-05-2015 11:57:48
10-05-2015 11:5...	Data Bac...	c:\target\FILE1.TXT	Scan		Session	1.3 KB	10-05-2015 11:57:48
10-05-2015 11:5...	Data Bac...	c:\target\FILE3.TXT	Scan		Session	1.4 KB	10-05-2015 11:57:48

## Messages

When clicking on the **Messages** tab, a request goes out to the PeerSync machine to request a list of messages/errors logged and return it to the Peer Management Center to be displayed. This list can be requested only if PeerSync is running on that machine and only if the File Synchronization job is started on the Peer Management Center.

When the info list is received the view is updated with the messages logged by PeerSync, and the caption on the top of the view will show the date and time the list was last updated.

By right-clicking on the info table, you can choose to hide or show columns.

This information on this table can be filtered by Path, Job Name, or Message.

Overview	PeerSync Jobs Stats	Added	Updated	Deleted	Messages
Message Log ( List Updated on 09-30-2015 13:53:45)					
0 errors, 0 warnings, 13 others    Filter by: <input type="text"/> <input type="text"/>					
Date	Path	Message	Job Name		
09-30-2015 13:2...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 13:2...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 13:2...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:2...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:1...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:1...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:1...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:1...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:1...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:1...	\\backupserver\da...	Failed Event - Add...	Data 3 Backup		
09-30-2015 12:0...	\\backupserver\da...	Connection Failure	Data 3 Backup		
09-30-2015 12:0...	\\backupserver\da...	Cannot create/got...	Data 3 Backup		

The **Failed Events** view allows you to see all those events that have failed to be processed by PeerSync. The list is populated when the PeerSync Management job starts, as well as in real-time as new failures occur. The information can be filtered by File Name.

Summary	Failed Events (2)	Monitoring Log	Alerts (16)	Participants (1)	Configuration
Failed Events					
2 Files   Filter by File Name: <input type="text"/>					
Date	File	Cause	Status	Message	
09-30-2015 13:20:48	\\backupserver\data3\FLDR3\FILE...	ADDFILE	Failed Event	Connection Failure (Target Not A...	
09-30-2015 13:20:48	\\backupserver\data3\FILE4 - Co...	ADDFILE	Failed Event	Connection Failure (Target Not A...	

You can right-click the info table and choose to **Reprocess Failed Events**. This action will send a request to PeerSync to retry all the failed events in the list.

The **Monitoring Log** view allows you to view recent event history for the currently running PeerSync Management job based on your [Logging and Alerts](#) settings. You can specify the maximum number of events to store in the table by adjusting the **Display Events** spinner located in the top right corner of the panel. The maximum number of events that can be viewed is 3,000.

If you need to view more events or events from a prior session, then you can use the log files saved in the **Hub\logs** directory located in the installation directory. The event log files will start with **fs\_event.log** and are written in a tab-delimited format. Microsoft Excel is a good tool to use to view and analyze a log file. See [Logging and Alerts](#) for more information about log files.

You can click on any column header to sort by the column. Warnings are displayed in light gray; errors are displayed in red; fatal errors are displayed in orange. Error records will also contain an error message in the **Message** column.

To change what is being logged, update the selected Event Types in the [Logging and Alerts](#) settings.

Summary Failed Events (2) **Monitoring Log** Alerts (16) Participants (1) Configuration

Event Log (Auto-Update Disabled)

0 errors, 0 warnings, 4 others | Filter by Severity:  Filter by:   Actions ▾

Date	Severity	Type	Host	Is Source	File	Comments	Message
09-30-2015 13:2...	INFO	Failed Events Reprocess	DDWin12R2b	true			Failed Event Repro...
09-30-2015 13:2...	INFO	Failed Events Reprocess	DDWin12R2b	true			Failed Event Repro...
09-30-2015 12:2...	INFO	Watch Directory		true			
09-30-2015 12:2...	INFO	Session Started		true			

Clicking the **Actions** table menu provides the following options:

<b>Ref res h Vie w</b>	Refresh all information provided in the table.
<b>Cle ar Ev ent s</b>	Remove all items from the table.

The **Alerts** view allows you to view any alerts relevant to the running PeerSync Management job. Items shown here are based on the configured Alerts Severity setting on the Logging and Alerts configuration page. You can specify the maximum number of alerts to store in the table by adjusting the Display Alerts spinner located in the top right corner of the panel.

The alerts are also written to a tab-delimited file named **fs\_alert.log** within the subdirectory **Hub/logs** within the installation directory of the Peer Management Center. See the [Logging and Alerts](#) settings for more information about log files.

You can click on any column header to sort by that column. For example, clicking on the **Severity** column will sort by alert severity. Warnings are displayed in light gray; errors and fatal alerts are displayed in red. A common error may be the PeerSync service is not running, which will trigger a PeerSync Quorum lost alert.

Summary	Failed Events (2)	Monitoring Log	Alerts (16)	Participants (1)	Configuration
Alert Log					
16 errors, 0 warnings, 0 others   Filter by Severity: <input type="text"/>					
Received Date	Severity	Type	Host	Message	
09-30-2015 12:09:30	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 12:09:30	ERROR	Application	DDWin12R2b	Service Not Running	
09-30-2015 12:09:30	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 12:09:30	ERROR	Application	DDWin12R2b	Service Not Running	
09-30-2015 12:07:30	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 12:07:30	ERROR	Application	DDWin12R2b	Service Not Running	
09-30-2015 12:07:30	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 12:07:30	ERROR	Application	DDWin12R2b	Service Not Running	
09-30-2015 11:53:59	FATAL	Application		Quorum lost for job DDWin12R2b[WestCoast]. Sessi...	
09-30-2015 11:53:59	ERROR	Application	DDWin12R2b	Agent on host DDWin12R2b was restarted while job ...	
09-30-2015 11:52:41	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 11:52:41	ERROR	Application	DDWin12R2b	Service Not Running	
09-30-2015 11:51:11	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 11:51:11	ERROR	Application	DDWin12R2b	Service Not Running	
09-30-2015 11:50:54	FATAL	Application		PeerSync Quorum lost for job DDWin12R2b[WestCo...	
09-30-2015 11:50:54	ERROR	Application	DDWin12R2b	Service Not Running	

The following right-click menu items are unique to this table:

<b>Refresh View</b>	Refresh all information provided in the table. This can also be done from the right-click context menu of the table.
<b>Clear Events</b>	Remove all items from the table. This can also be done from the right-click context menu of the table.

The **Participants** view shows the currently configured host participant for the selected PeerSync Management job and contains a column used to display activity status occurring on the hosts. If a host has become unavailable or the PeerSync service stopped, an error message will be displayed in red next to the failed host.



Summary Failed Events (2) Monitoring Log Alerts (16) **Participants (1)** Configuration

Host Participants

Host	Root Path	Status	State	Message
DDWin12R...	C:\Program Files (x86)\P...	Participating	Active	

Host Participant State Change Log

Filter by: Host:  Status:  State:

Date	Host	Status	State	Message
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Not Participating	Inactive	Job Stopped
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Not Participating	Inactive	Job Stopped
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Not Participating	Inactive	Job Stopped
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Host Resource Av...	Active	PeerSync Service is running
09-30-2015 ...	DDWin12R...	Host Resource Av...	Active	PeerSync Service Available
09-30-2015 ...	DDWin12R...	Host Resource Un...	Inactive	PeerSync Service Not Running
09-30-2015 ...	DDWin12R...	Host Resource Av...	Active	PeerSync Service is running
09-30-2015 ...	DDWin12R...	Host Resource Av...	Active	PeerSync Service Available
09-30-2015 ...	DDWin12R...	Host Resource Un...	Inactive	PeerSync Service Not Running
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Not Participating	Inactive	Job Stopped
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Participating	Active	
09-30-2015 ...	DDWin12R...	Host Unavailable	Inactive	Agent on host DDWin12R2b was restarted while jo

The **Participants** view also contains a table that displays the most recent host participant state changes, for example, when a host was removed from synchronization session, when a host came back online, or when the PeerSync service was stopped or started. This functionality is broken down into two parts: right-click context menu items and the **Host Participant State Change Log** view.

The **Host Participant State Change Log** is a log of all host participant status changes (e.g., Collaborating, Not Collaborating) and/or state changes (e.g., Active, Pending Restart) of a host participant. This table is currently limited to 250 rows and can be filtered by host, by status, and by state.

The following items are available in the right-click context menu for this table:

<b>Refresh View</b>	Refresh all information provided in the table.
<b>Clear Events</b>	Remove all items from the table.

The **Configuration** view displays a quick summary of all configurable items for the selected PeerSync Management job. Each page of the **File Synchronization Configuration** dialog is represented in its own part of the view and can be collapsed if desired.

Clicking **Edit this Configuration** will immediately bring you to the **PeerSync Management Configuration** dialog where you can edit the current monitoring configuration or the associated PeerSync profile.

Summary | Failed Events (2) | Monitoring Log | Alerts (16) | Participants (1) | **Configuration**

[Edit this Configuration](#)

### Configuration Summary

▼ General Settings

Host Name: DDWin12R2b  
Session Name: DDWin12R2b[WestCoast]  
Session ID: 101  
Alert Severity: WARNING

▼ Configured PeerSync Jobs

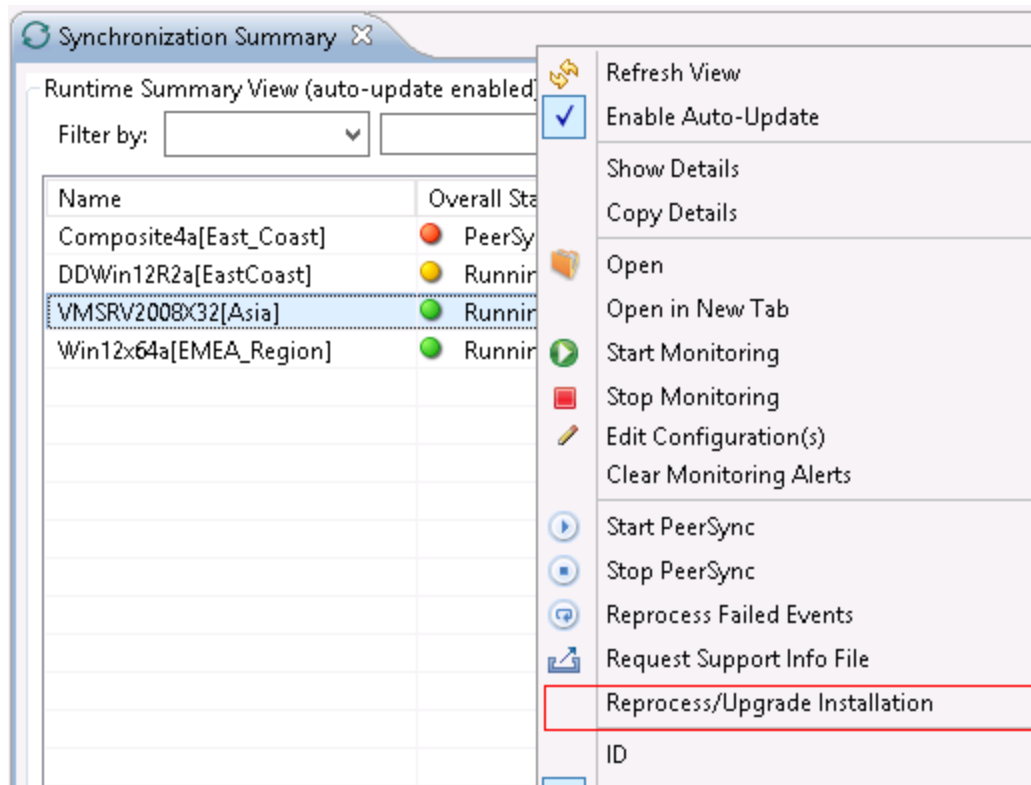
Filter by:   ☒ Include Disabled Jobs

Name	#	Source	Target	Type	
<input checked="" type="checkbox"/> Data 3 Backup	3	c:\source3	\\backupserver\data3	Real Time Backup	
<input checked="" type="checkbox"/> Data Backup	1	c:\source	c:\target	Real Time Backup	
<input checked="" type="checkbox"/> Data2 Backup	2	c:\source2	c:\target2	Real Time Backup	

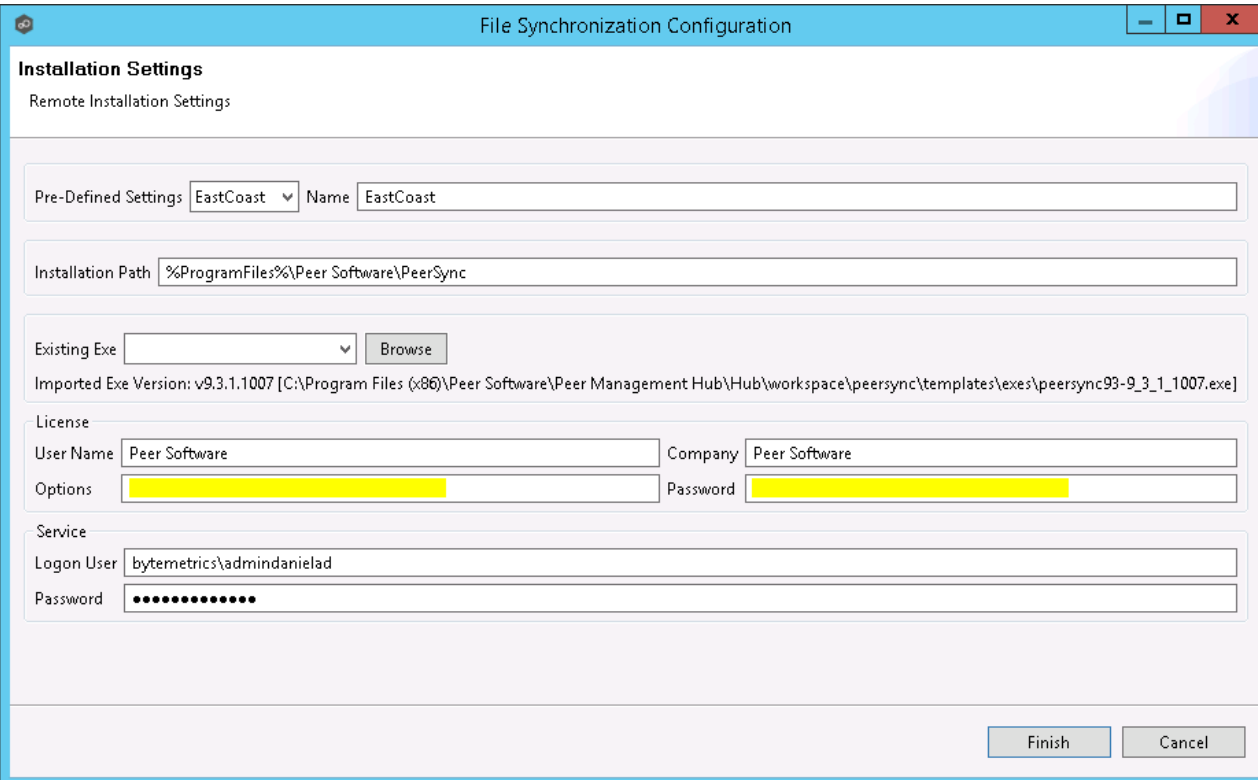
► Monitoring Settings

## Upgrade/Reprocess Installation

From the [Synchronization Summary view](#), you can click on one or more PeerSync Management jobs and choose **Reprocess/Upgrade Installation**. This option sends a request to the selected PeerSync instances to install/upgrade given the configured settings.



The installation settings should be common for ALL the PeerSync Management PeerSync instances in order to successfully install PeerSync.



The image shows a Windows-style dialog box titled "File Synchronization Configuration". Inside, there is a section titled "Installation Settings" with a sub-label "Remote Installation Settings". The dialog contains several input fields and buttons. At the top, "Pre-Defined Settings" is set to "EastCoast" and "Name" is "EastCoast". Below this is the "Installation Path" field with the value "%ProgramFiles%\Peer Software\PeerSync". The "Existing Exe" field has a dropdown arrow and a "Browse" button. Below that, it says "Imported Exe Version: v9.3.1.1007 [C:\Program Files (x86)\Peer Software\Peer Management Hub\Hub\workspace\peersync\templates\exes\peersync93-9\_3\_1\_1007.exe]". The "License" section includes "User Name" (Peer Software), "Company" (Peer Software), "Options" (a yellowed-out field), and "Password" (a yellowed-out field). The "Service" section includes "Logon User" (bytemetrics\adminidanielad) and "Password" (a field with 10 dots). At the bottom right are "Finish" and "Cancel" buttons.

**File Synchronization Configuration**

**Installation Settings**  
Remote Installation Settings

Pre-Defined Settings: EastCoast Name: EastCoast

Installation Path: %ProgramFiles%\Peer Software\PeerSync

Existing Exe: [Dropdown] Browse

Imported Exe Version: v9.3.1.1007 [C:\Program Files (x86)\Peer Software\Peer Management Hub\Hub\workspace\peersync\templates\exes\peersync93-9\_3\_1\_1007.exe]

**License**

User Name: Peer Software Company: Peer Software

Options: [Redacted] Password: [Redacted]

**Service**

Logon User: bytemetrics\adminidanielad

Password: [Redacted]

Finish Cancel

See [Installation Settings](#) for information on the settings on this page.

# Index

## - A -

- Access, PeerGFS API 132
- Active Directory authentication 281
- Active Directory groups 278
- Active Directory users 278
- Advanced configuration options, Dell EMC Isilon 243, 247, 251
- Advanced configuration options, NetApp 7-Mode 257
- Advanced configuration options, NetApp cDOT 263
- Advanced configuration options, Nutanix Files 269
- Agent availability 219
- Agent configuration 121
- Agent connectivity, preferences 219
- Agent performance 126
- Agent properties, editing 129
- Agent properties, viewing 127
- Agent Summary view 56
- Agent, disabled 131
- Agent, disconnected 219
- Agent, general configuration 124
- Agent, installation 16
- Agent, re-enabling 131
- Agent, updating 23, 131
- Agent, VM options 127
- Agents view 32
- Alerts 93
- Alerts view 34
- Amazon S3 318, 325
- API 132
- API access 132
- API categories 134
- API integration 133
- API reference 134
- API status codes 134
- Application support, File Collaboration job 451, 478
- Application support, File Synchronization job 567
- Auto match root 413
- Auto-restarting, File Collaboration job 495
- Auto-restarting, File Synchronization job 583
- Azure Blob Storage 316
- Azure Storage 323

## - B -

- Bash 133
- Basic concepts 74
- Batched emails 182
- Batched real-time 335
- Broker configuration 123
- Broker configuration, preferences 221
- Broker statistics 66, 67, 68, 70
- Browsing files and folders 217
- Bucket 322
- Bucket details, Amazon S3 325
- Bucket details, NetApp StorageGRID 327
- Bucket details, Nutanix Objects 329

## - C -

- CDP 336
- Cloud Backup and Replication job, creating 289
- Cloud Backup and Replication job, proxy configuration 294
- Cloud Backup and Replication jobs 288
- Cloud Backup and Replication jobs, overview 288
- Cloud Backup and Replication jobs, preferences 152
- Collab and Sync Summary view, Reports tab 62
- Collab and Sync Summary view, Summary tab 59
- Complex regular expressions 79
- Concepts 74
- Configuration 7
- Configuration, Agent 121, 124
- Configuration, broker 123
- Configuration, Preferences 151
- Conflict resolution, File Collaboration job 470
- Conflict resolution, File Synchronization job 559
- Conflict resolution, metadata 475, 563
- Conflicts 114
- Connection statuses 120
- Container 322
- Container details, Azure Storage 323
- Continuous data protection 336
- Create File Collaboration job 413
- Create File Synchronization job 413
- Credentials 157
- Credentials, Dell EMC Isilon 242, 246
- Credentials, Dell EMC VNX/Celerra 250
- Credentials, NetApp 7-Mode 253

Credentials, NetApp cDOT 259  
 Credentials, Nutanix Files 266

## - D -

Dashboard view 36  
 Data recovery 353  
 database compression 66, 67, 68, 70  
 Database connections 155  
 delayed replication 135  
 Dell EMC configuration 238  
 Delta-level replication 339  
 Delta-level replication, File Collaboration job 472  
 Delta-level replication, File Synchronization job 561  
 Destination snapshot report 159  
 Destination Credentials 316, 318, 320, 321  
 Destination storage credentials 157  
 Detector settings 413, 463, 552  
 DFS 116  
 DFS namespace 413  
 DFS namespace folder, adding 402  
 DFS namespace server, adding 398  
 DFS Namespace, elements 367  
 DFS namespaces 368  
 DFS namespaces, connecting to jobs 412  
 DFS namespaces, managing 398  
 DFS-N Management job, creating 368  
 DFS-N Management job, folder targets 378  
 DFS-N Management job, importing existing namespace 388  
 DFS-N Management job, Management Agent 370  
 DFS-N Management job, namespace folders 378  
 DFS-N Management job, namespace name 373  
 DFS-N Management job, namespace servers 374  
 DFS-N Management job, namespace settings 376  
 DFS-N Management job, running 396  
 DFS-N Management job, starting 396  
 DFS-N Management job, stopping 397  
 DFS-N Management job, verifying Agent 371  
 DFS-N Management jobs 366  
 DFS-N Management jobs, preferences 206  
 DFS-N, File Collaboration job 488  
 DFS-N, File Synchronization job 576  
 Disabled agent 131  
 Disconnected agent 219

## - E -

Editing multile File Collaboration jobs 489, 577  
 Email alerts, Cloud Backup and Replication job 342  
 Email alerts, concepts 74  
 Email alerts, DFS-N Management job 382  
 Email alerts, File Collaboration job 452, 484  
 Email alerts, File Replication job 519  
 Email alerts, File Synchronization job 542, 573  
 Email Alerts, preferences 159, 182, 222  
 EMC Isilon environment prerequisites 7  
 EMC VNX/Celerra environment prerequisites 7  
 Enhanced metadata conflict resolution 475, 563  
 Environmental requirements 7  
 Event detection 271  
 event detection analytics 66, 67, 68, 70  
 Expedited Sync Queue 193

## - F -

File and folder filters, preferences 164, 187  
 File Collaboration job, application support 451, 478  
 File Collaboration job, auto-restarting 495  
 File Collaboration job, conflict resolution 470  
 File Collaboration job, creating 432  
 File Collaboration job, delta-level replication 472  
 File Collaboration job, DFS-N 488  
 File Collaboration job, editing 456  
 File Collaboration job, email alerts 452, 484  
 File Collaboration job, file filters 468  
 File Collaboration job, file locking 477, 566  
 File Collaboration job, file metadata 449, 475  
 File Collaboration job, General 466  
 File Collaboration job, host connectivity issues 497  
 File Collaboration job, logging and alerts 479  
 File Collaboration job, Management Agent 436  
 File Collaboration job, modifying participant attributes 461  
 File Collaboration job, modifying participant detector settings 463  
 File Collaboration job, participants 434, 435, 458  
 File Collaboration job, running 491, 492  
 File Collaboration job, runtime view 43  
 File Collaboration job, runtime view, Alerts tab 50  
 File Collaboration job, runtime view, Configuration tab 53

- File Collaboration job, runtime view, Event Log tab 47
  - File Collaboration job, runtime view, Participants tab 51
  - File Collaboration job, runtime view, Quarantines tab 48
  - File Collaboration job, runtime view, Retries tab 49
  - File Collaboration job, runtime view, Session tab 46
  - File Collaboration job, runtime view, Summary tab 44
  - File Collaboration job, SNMP notifications 486
  - File Collaboration job, starting 493
  - File Collaboration job, stopping 495
  - File Collaboration job, tags 487
  - File Collaboration job, target protection 482
  - File Collaboration jobs 431
  - File Collaboration jobs, editing multiple 489, 577
  - File Collaboration jobs, overview 431
  - File Collaboration jobs, preferences 178
  - File conflicts 114
  - File event logs 98
  - File events 98
  - File filters 75
  - File filters, Cloud Backup and Replication job 313
  - File filters, creating 76
  - File filters, File Collaboration job 468
  - File filters, File Synchronization job 557
  - File filters, predefined 76
  - File filters, usage notes 90
  - File locking 189
  - File locking, File Collaboration job 477, 566
  - File menu 66, 67, 68, 70
  - File metadata 116, 339
  - File metadata, File Collaboration job 449, 475
  - File metadata, File Synchronization job 540, 563
  - File quarantine 114
  - File Replication job, email alerts 519
  - File Replication job, runtime view 53
  - File Replication jobs 500
  - File Replication jobs, preferences 178
  - File retries 114, 185
  - File Retries and Source Snapshots, preferences 163
  - File Synchronization job, application support 567
  - File Synchronization job, auto-restarting 583
  - File Synchronization job, conflict resolution 559
  - File Synchronization job, creating 523
  - File Synchronization job, delta-level replication 561
  - File Synchronization job, DFS-N 576
  - File Synchronization job, editing 545
  - File Synchronization job, email alerts 542, 573
  - File Synchronization job, file filters 557
  - File Synchronization job, file metadata 540, 563
  - File Synchronization job, General 555
  - File Synchronization job, host connectivity issues 584
  - File Synchronization job, logging and alerts 568
  - File Synchronization job, Management Agent 527
  - File Synchronization job, modifying participant attributes 550
  - File Synchronization job, modifying participant detector settings 552
  - File Synchronization job, participants 525, 526, 547
  - File Synchronization job, running 579
  - File Synchronization job, runtime view 54
  - File Synchronization job, SNMP notifications 575
  - File Synchronization job, starting 581
  - File Synchronization job, stopping 583
  - File Synchronization job, tags 576
  - File Synchronization job, target protection 571
  - File Synchronization jobs 522
  - File Synchronization jobs, preferences 178
  - Files and folders, browsing 217
  - Filter expressions 92
  - Filter patterns 78
  - Filter patterns, complex regular expressions 79
  - Filter patterns, excluding temporary files 81
  - Filter patterns, using wildcards 80
  - filter, scheduled replication 135
  - Filtering by date 84
  - Filtering by file size 86
  - Filtering folders 88
  - Filters, file 90
  - Filters, folders 88
  - Filters, list 91
  - Folder filters 75
  - Folder filters, creating 76
  - Folder target, adding 408
  - Folders, filtering 88
- G -**
- General Configuration, preferences 216, 217
  - General, File Collaboration job 466
  - General, File Synchronization job 555

## - H -

Heartbeats 219  
 Help menu 66, 67, 68, 70  
 Hidden items 217

## - I -

Importing existing namespace 388  
 Initial synchronization process 492, 580  
 Initialization process 492, 580  
 Installation 7  
 Installation, Peer Agent 16  
 Internal users 101, 102, 272, 274  
 Isilon credentials 242, 246  
 Isilon, advanced configuration options 243, 247, 251

## - J -

Job alerts 98  
 Job Alerts view 37  
 Job initialization process 492, 580  
 Job logs 98  
 Job, manual retries 499, 586  
 Jobs view 38  
 Jobs, Cloud Backup and Replication 288  
 Jobs, DFS-N Management 366  
 Jobs, File Collaboration 431  
 Jobs, File Replication 500  
 Jobs, File Synchronization 522  
 Jobs, PeerSync Management 587

## - K -

Keytool certificate management utility 137

## - L -

Last modified date 84  
 LDAP administrator 281  
 LDAP settings 272  
 License 137  
 License file 229  
 Licensed storage capacity 137  
 Licensing 229

Link namespace to job 412, 423  
 Link to DFS Namespace job 413  
 List filter expressions 92  
 List filters, concepts 91  
 List filters, examples 92  
 List filters, managing 93  
 List filters, removing 93  
 Locking 189  
 Logging 93, 125  
 Logging and alerts, File Collaboration job 479  
 Logging and alerts, File Synchronization job 568  
 Logging, jobs 98

## - M -

Malicious Event Detection 232  
 Management Agent 293  
 Management Agent, DFS-N Management job 370  
 Management Agent, File Collaboration job 436  
 Management Agent, File Synchronization job 527  
 MED configuration, preferences 232  
 memory dump file 66, 67, 68, 70  
 Menus 66, 67, 68, 70  
 Metadata 116  
 Metadata conflict resolution 475, 563  
 Miscellaneous options 339

## - N -

Namespace elements 367  
 Namespace failback 116  
 Namespace failover 116  
 Namespace folder 413  
 Namespace folder target, adding 408  
 Namespace folder, adding 402  
 Namespace folder, linking with job 423  
 Namespace server, adding 398  
 Namespace, linked to job 412  
 Namespaces 368  
 NAS configuration, NetApp 7-Mode 253  
 NAS configuration, Dell EMC 238  
 NAS configuration, NetApp cDOT 259  
 NAS configuration, Nutanix Files 266  
 NAS configuration, preferences 238  
 NetApp 7-Mode configuration 253  
 NetApp 7-Mode credentials 253  
 NetApp 7-Mode environment prerequisites 7



NetApp 7-Mode, advanced configuration options 267  
 NetApp cDOT configuration 259  
 NetApp cDOT credentials 259  
 NetApp cDOT, advanced configuration options 263  
 NetApp cDOT/ONTAP9+ environment prerequisites 7  
 NetAPP prerequisites 8  
 NetApp StorageGRID 320, 327  
 NTFS permissions 339, 449, 475, 540, 563  
 Nutanix Files configuration 266  
 Nutanix Files credentials 266  
 Nutanix Files, advanced configuration options 269  
 Nutanix Objects 321, 329  
 Nutanix prerequisites 8

## - P -

Participant detector settings 463, 552  
 Participant, modifying attributes 461, 550  
 Participants, adding to File Collaboration job 459  
 Participants, adding to File Synchronization job 548  
 Participants, File Collaboration job 434, 435, 458, 463  
 Participants, File Synchronization job 525, 526, 547, 552  
 Participants, removing from File Collaboration job 459  
 Participants, removing from File Synchronization job 548  
 Peer Agent, installation 16  
 Peer Agent, updating 23  
 Peer Agents, managing 117  
 Peer Global File Service license 229  
 Peer Global File Service license 137  
 Peer Management Broker 458, 547  
 Peer Management Center, updating 20  
 PeerGFS API 132  
 PeerGFS license 137, 229  
 PeerGFS preferences 149  
 PeerSync Management jobs 587  
 Performance, Agent 126  
 Performance, preferences 167, 191  
 PMC user interface 24  
 PMC user interface, views 30  
 PMC, updating 20  
 PMC/Agent logs 66, 67, 68, 70  
 Powershell 133  
 Predefined file filters 76

Preferences 149  
 Preferences, Agent connectivity 219  
 Preferences, Broker configuration 221  
 Preferences, Cloud Backup and Replication 152  
 Preferences, configuring 151  
 Preferences, database connections 155  
 Preferences, Email Alerts 159, 182, 222  
 Preferences, file and folder filters 164, 187  
 Preferences, File Collaboration jobs 178  
 Preferences, File Replication jobs 178  
 Preferences, File Retries and Source Snapshots 163  
 Preferences, File Synchronization jobs 178  
 Preferences, General Configuration 216, 217  
 Preferences, MED configuration 232  
 Preferences, NAS configuration 238  
 Preferences, performance 167, 191  
 Preferences, real-time event detection 192, 193  
 Preferences, Replication and Retention Policies 171  
 Preferences, Scan Manager 176, 199  
 Preferences, SNMP Notifications 173, 196  
 Preferences, Software updates 225  
 Preferences, Tags 226  
 Prerequisites, NetAPP 8  
 Prerequisites, Nutanix 8  
 Pre-Seeding 135  
 Properties, Agent 127, 129  
 proxy configuration 294

## - Q -

Quarantined file 498, 585  
 Quarantined files 182  
 Quarantines 114

## - R -

Real-time event detection 192, 271  
 Real-time event detection, preferences 192, 193  
 real-time replication 135  
 Reconnect attempts 219  
 Recovering data 353  
 Re-enable agent 131  
 Rehydrated data 339  
 Removing file from quarantine 498, 585  
 Replication and Retention Policies, preferences 171  
 Replication and Retention policy 331

Replication schedule 332, 333, 335, 336  
 Reports tab, Collab and Sync Summary view 62  
 Reports, destination snapshot 159  
 Reports, scan 159  
 Requirements, environment 7  
 Retention 337  
 Retries 114  
 Retrying a job 499, 586  
 REVIT 193  
 Roles 272  
 Root path 413  
 Runtime views 41

## - S -

Scan Manager, preferences 176, 199  
 Scan report 159  
 scheduled replication 135  
 scheduled replication filter 135  
 Scheduled scans 333  
 Security 137  
 Seeding Target 458, 547  
 Smart Data Seeding 135  
 Snapshots, source 338  
 SNMP notifications, Cloud Backup and Replication job 344  
 SNMP notifications, DFS-N Management job 384  
 SNMP notifications, File Collaboration job 486  
 SNMP notifications, File Synchronization job 575  
 SNMP notifications, overview 109  
 SNMP Notifications, preferences 173, 196  
 Software updates, preferences 225  
 Source paths 312  
 Source snapshots 338  
 Source storage platform 292  
 Starting, DFS-N Management job 396  
 Starting, File Collaboration job 493  
 Starting, File Synchronization job 581  
 status codes, API 134  
 Stopping, DFS-N Management job 397  
 Stopping, File Collaboration job 495  
 Stopping, File Synchronization job 583  
 Storage capacity 137  
 storage information 300  
 Storage platform credentials 157  
 Storage tiering options 339  
 Summary tab, Collab and Sync Summary view 59  
 Summary views 55

System alerts 217, 222  
 System folders 217

## - T -

Tables 73  
 Tag categories 111  
 Tags overview 110  
 Tags, assigning 111  
 Tags, File Collaboration job 487  
 Tags, File Synchronization job 576  
 Tags, filtering resources 113  
 Tags, preferences 226  
 Target protection, File Collaboration job 482  
 Target protection, File Synchronization job 571  
 Temporary files 81  
 Terminology 1  
 Testing API access 133  
 thread dump file 66, 67, 68, 70  
 TLS Certificates 137  
 TLS Certificates, existing 144  
 TLS Certificates, new 138  
 Toolbar 71

## - U -

Updating software 225  
 Updating, Agent 131  
 Updating, Peer Agent 23  
 Updating, PMC 20  
 Upgrade 229  
 User interface 24  
 User management 272  
 Users, internal 101, 102, 274

## - V -

View, Agents 32  
 View, Alerts 34  
 View, Job Alerts 37  
 View, Jobs 38  
 Views 30  
 Views, Agent Summary 56  
 Views, dashboard 36  
 Views, runtime 41  
 Views, summary 55  
 VM options 127

---

VNX/Celerra credentials 250

## - W -

Web client users 101  
Web client, accessing 27, 29  
Web client, configuration 14  
Web client, securing access 16  
Web client, setting up 14  
Web roles 103  
Wildcards, filter patterns 80  
Window menu 66, 67, 68, 70

## - Y -

YAML file 133