

# Acronis

[acronis.com](https://acronis.com)

# Acronis Files Connect 11.4

# Table of contents

- Introduction** ..... 6
  - About Acronis Files Connect ..... 6
- QuickStart guide** ..... 7
  - Acronis Files Connect System requirements ..... 7
    - Operating System Requirements ..... 7
    - Hardware Requirements ..... 7
  - Installing Acronis Files Connect ..... 8
  - First run / Installing your license ..... 8
  - Configuring your first shared volume ..... 8
  - Volume services ..... 10
  - Configuring your first shared print queue ..... 11
  - The Acronis Files Connect Mac client app ..... 12
    - Installation ..... 14
    - Use ..... 15
    - Multi-selection ..... 16
    - Search ..... 16
    - Mounting Shares and Finder integration ..... 18
    - Bookmarks and Recent Files ..... 18
    - Removing the Acronis Files Connect Mac client app ..... 18
  - Connecting from the Mac Finder ..... 18
  - Connecting from a mobile client ..... 19
  - Additional resources ..... 19
    - Network Reshares ..... 19
    - Network Spotlight Search ..... 19
    - Filename Policies ..... 19
    - DFS Support ..... 20
- Installing Acronis Files Connect** ..... 21
  - Getting started ..... 21
    - System requirements ..... 21
    - Getting help ..... 22
  - Installing Acronis Files Connect ..... 23
    - Before you begin ..... 23
    - Installing Acronis Files Connect ..... 24
  - Administering Acronis Files Connect on a Cluster ..... 25
  - Configuring the Acronis Files Connect server for Acronis Files Connect Mac client app ..... 26

Adding additional servers to the Primary Server .....	27
<b>Launching Acronis Files Connect for the first time .....</b>	<b>28</b>
Automatically importing SMB shares .....	28
SMB Shares .....	29
Importing SMB shares after first launch .....	29
Naming conventions for SMB volumes .....	29
Using Kerberos .....	30
Troubleshooting Kerberos .....	30
<b>Setting up Acronis Files Connect Clustering .....</b>	<b>31</b>
Cluster worksheet .....	34
Installing Acronis Files Connect on a Cluster .....	35
Installation procedure .....	36
Installing Acronis Files Connect .....	37
Creating an Acronis Files Connect Service .....	38
Configuring Acronis Files Connect services .....	39
Adding an Acronis Files Connect Service to a Cluster .....	39
Setting Cluster resource dependencies .....	48
Bringing the new service online .....	48
<b>Upgrading Acronis Files Connect .....</b>	<b>49</b>
Upgrading to a new version of Acronis Files Connect .....	49
Upgrading to a new version of Acronis Files Connect on a Microsoft Failover Cluster .....	49
<b>Configuring Acronis Files Connect .....</b>	<b>51</b>
Acronis Files Connect File server .....	51
Starting and stopping the Acronis Files Connect File Server .....	51
Configuring the Acronis Files Connect server .....	51
Configuring network reshare support .....	72
Administering Acronis Files Connect remotely .....	82
Configuring client computers to print to Acronis Files Connect .....	83
Adding a printer from a Web Page .....	83
Mac users configuration for DFS support .....	84
Acronis Files Connect Mac client app .....	84
Adding a License Serial Number .....	85
You need to enter a new license serial number when: .....	85
To add a license serial number .....	85
<b>Searching with Acronis Files Connect .....</b>	<b>87</b>
Enumeration search .....	87
Catalog search .....	87

Spotlight search .....	87
To enable Spotlight Search for all volumes: .....	87
To enable Spotlight Search for individual volumes: .....	87
Storing search index files .....	88
<b>Using Acronis Files Connect .....</b>	<b>89</b>
Using the Acronis Files Connect File server .....	89
Creating Volumes for Use with Acronis Files Connect .....	89
Acronis Files Connect Users .....	101
Connecting Mac users .....	102
Viewing files opened with Acronis Files Connect .....	103
Using the log .....	104
Keeping track of activities with the operation log .....	104
Using the Print log .....	105
Using the Acronis Files Connect Print server .....	106
How the Print server works .....	107
Setting up print queues .....	107
Setting up processing methods .....	109
Controlling the processing of jobs .....	111
Publishing a print queue .....	113
<b>Backup and recovery .....</b>	<b>114</b>
Backup .....	114
Recovery .....	114
<b>Appendices .....</b>	<b>116</b>
Appendix A: Using the Registry keys .....	116
Reconnecting a dropped session .....	116
Sending password expiration notifications during session .....	116
Scheduling re-indexing with EZIPUTIL .....	117
Adding print log entries to text files .....	117
Customizing Acronis Files Connect Print Processing Log columns .....	117
Columns .....	118
Appendix B: Monitoring Acronis Files Connect .....	118
Counters for Acronis Files Connect File server .....	119
Counters for Acronis Files Connect File server users .....	120
Counters for Acronis Files Connect File server volumes .....	120
Counters for Acronis Files Connect Printing .....	120
Counters for Acronis Files Connect Print queues .....	120
<b>Supplemental material .....</b>	<b>122</b>

TCP/IP ports .....	122
Acronis Files Connect uses the following TCP/IP ports .....	122
Additional AFP port notes .....	122
Acronis Files Connect compatibility information .....	122
Support for Microsoft Networking Domains .....	122
Windows Registry Keys .....	123
General parameter registry keys – non-refreshable .....	123
General parameter registry keys – refreshable .....	132
Debug logging registry keys – refreshable .....	145
Debug logging registry keys – non-refreshable .....	148
Print parameter registry keys – refreshable .....	148
Print parameter registry keys – non-refreshable .....	150
Filename policy registry keys – Refreshable .....	150
HTTP discovery registry keys – refreshable .....	153
Spotlight registry keys – Refreshable .....	154
Acronis Files Connect Streams .....	157
EZIPUTIL command line tool .....	158
Network Reshare and Kerberos authentication under the local SYSTEM account .....	167
Configuring Network Reshare .....	167
Enabling Kerberos authentication .....	168
<b>Known issues .....</b>	<b>169</b>
<b>What's new .....</b>	<b>171</b>

# Introduction

This guide provides the documentation of Acronis Files Connect installation, configuration, and features.

## About Acronis Files Connect

With Acronis Files Connect, Windows® computers can provide Apple Filing Protocol (AFP) file sharing and IP-printing to Macintosh® computers. Acronis Files Connect is optimized to provide the fastest file and print services available, resolve common Mac/Window file sharing issues, and provide support for Apple technologies such as Network Spotlight full-content search and Time Machine backup.

Acronis Files Connect includes the following services:

- Acronis Files Connect File Server
- Acronis Files Connect Print Server

With Acronis Files Connect, Mac users can connect to and mount directories on a Windows file server just as native AFP volumes. With the Acronis Files Connect Print Server installed, Mac users can create desktop printers that deliver print jobs to printers via the server automatically. Acronis Files Connect's integration into the existing network is seamless – Mac users continue using the same tools and applications for accessing servers and printers that they always have.

# QuickStart guide

## Acronis Files Connect System requirements

Verify that your server meets the requirements for Acronis Files Connect. It is recommended that you quit any running programs, including the **Services** control panel, before starting the installation.

The following are the minimum system requirements for the Acronis Files Connect File & Print Server on Windows Server and Windows Workstation platforms and for connecting from Mac machines. For optimal results, your Windows Server machine should be running the latest service pack from Microsoft®. Adding additional RAM to your server machine will greatly enhance Acronis Files Connect performance. The recommended system requirements for a particular implementation or application can vary, so please **contact Acronis Technical Support** if you have questions or need assistance.

## Operating System Requirements

### Windows Server Platforms

- 2022 Standard & Datacenter
- 2019 Standard & Datacenter
- 2016 Standard & Datacenter & Essentials
- Windows Storage Server 2016
- Windows Powered NAS

### Windows Workstation Platforms:

- Windows 10

### Mac users:

- macOS 10.10.5

Find more details about newer macOS versions in the Acronis Files Connect [Release notes](#).

## Hardware Requirements

### Minimal configuration

- Local shares – Core class CPU with 2 or more cores, 4 GB of RAM
- Network Reshare – Core 'i' class CPU with 4 or more cores, 8 GB of RAM, dual non-bonded Gigabit Ethernet NICs

---

### Note

You may need substantially more resources depending on the number of volumes and users and other applications running on the server.

---

# Installing Acronis Files Connect

## First run / Installing your license

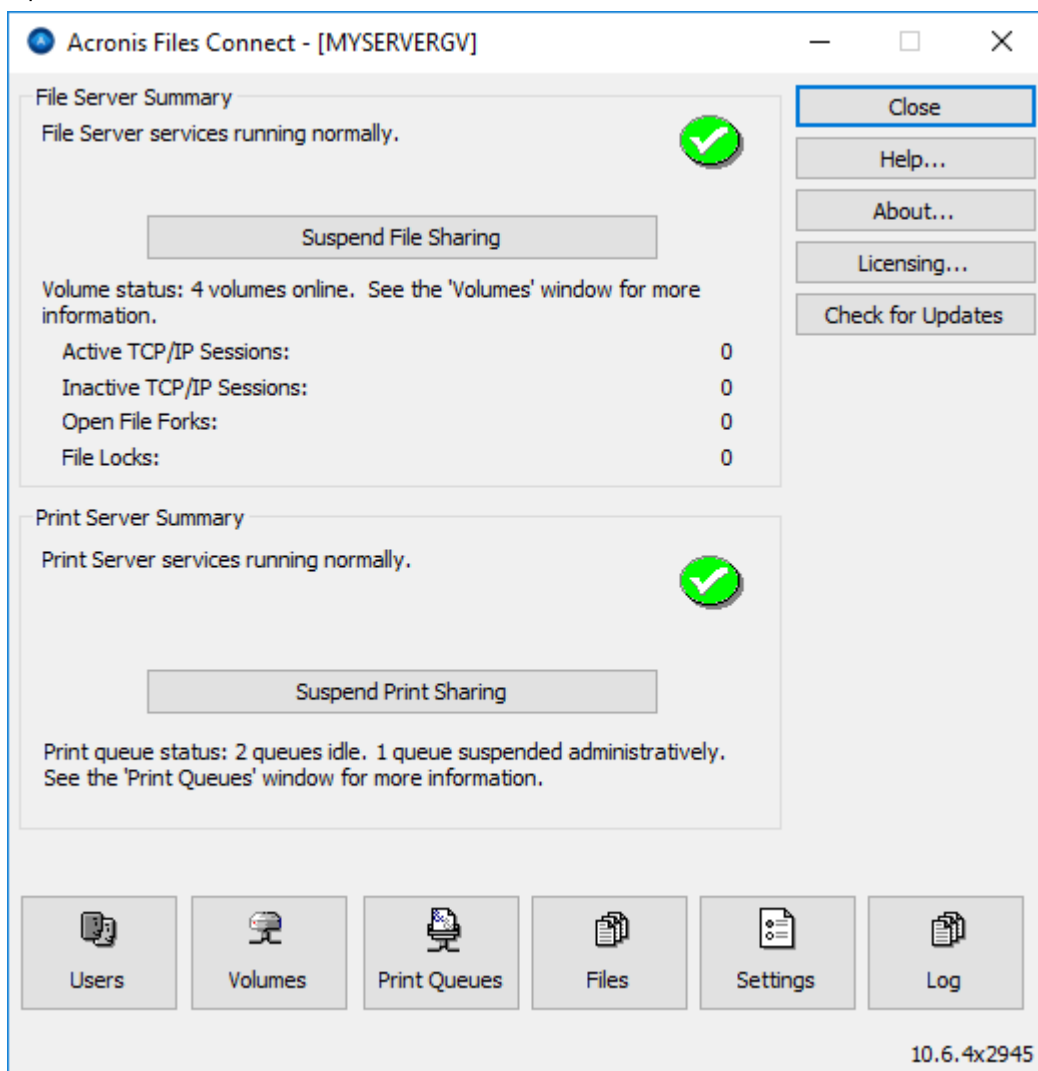
When you start the Acronis Files Connect for the first time, you can choose to enable the **Print Server** or not.

New Acronis Files Connect installations default to **Trial** mode. If you have an Acronis Files Connect license, enter your license serial number. For more information on how to do it, refer to [Adding a License Serial Number](#)

If you upgraded a previous version of Acronis Files Connect, it will continue to use your existing license serial number.

## Configuring your first shared volume

1. Open the **Acronis Files Connect Administrator**.

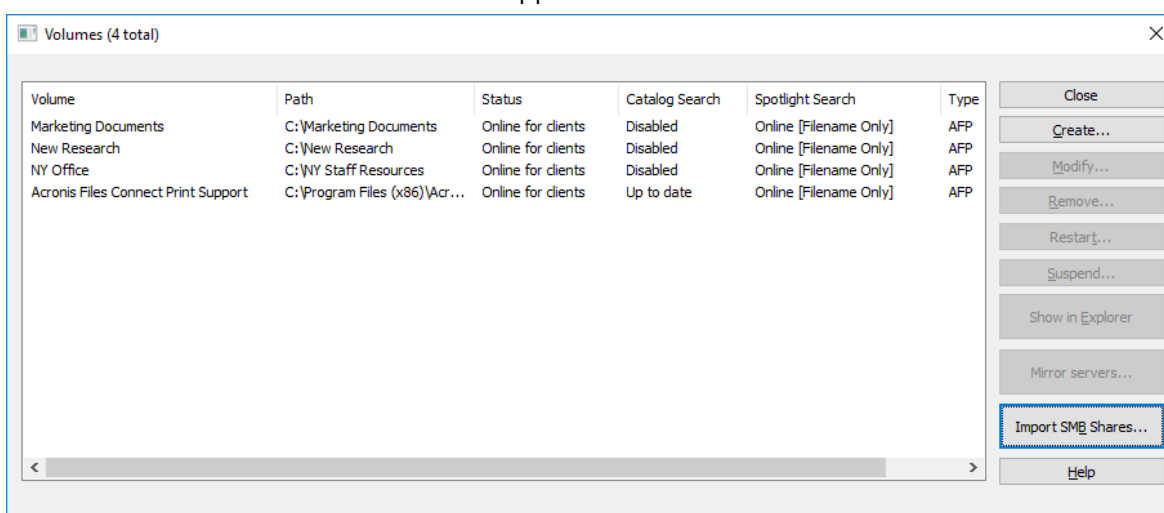


- **Suspend File Sharing** – Disconnects all clients and prevents new connections to the server.
- **Suspend Print Sharing** – Disconnects all the printers and prevents new connections to them.
- **Users** – Displays a list of the connected users.
- **Volumes** – Creates or configures shared volumes.
- **Print Queues** – Creates or administers **Print Queues**.
- **Files** – Displays files currently open by Mac users.
- **Settings** – Edits Acronis Files Connect settings.
- **Log** – Shows Acronis Files Connect related events from the Windows Event Viewer.

### Note

The first time the Acronis Files Connect Administrator is opened, it will prompt you to create shared volumes or import your existing SMB shares to Acronis Files Connect. This can also be done any time from within the **Volumes** window.

2. Click **Volumes**. The Volumes window will appear.



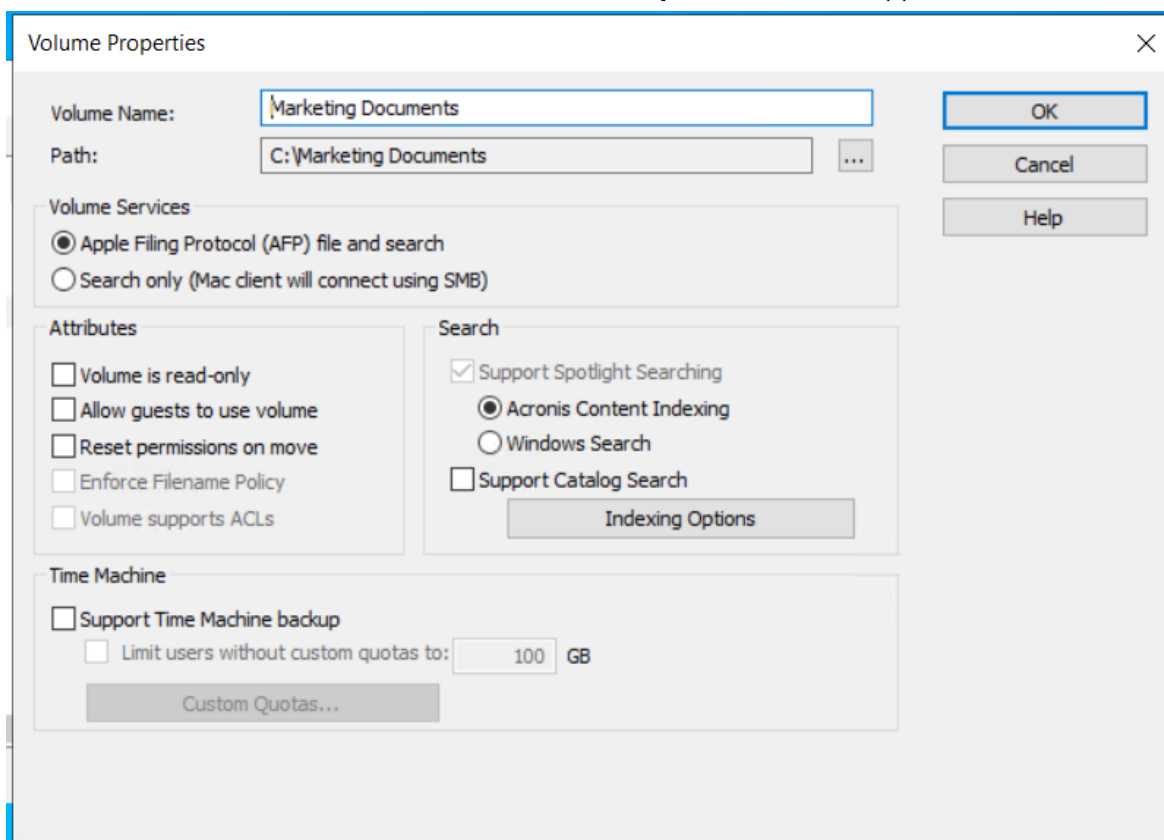
- **Create** – Creates a volume.
- **Modify** – Opens the Volume Properties window.
- **Remove** – Removes the selected volume.
- **Restart** – Restarts the volume.
- **Suspend** – Takes a volume temporarily offline so that clients cannot connect to it.

### Note

Suspended volumes will be resumed every time the Acronis Files Connect service is restarted.

- **Show in Explorer** – Shows the volume's parent folder in Windows File Explorer.
- **Mirror servers** – Mirrors one or multiple file servers so that all SMB shares on them are automatically added as AFP file share volumes in Acronis Files Connect. See more about [Mirroring SMB file servers](#).
- **Import SMB Shares** – Reshares all folders shared with Windows file sharing (SMB) with Acronis Files Connect as well.

3. Click **Create** to create a new volume. The **Volume Properties** windows appears.



- **Volume Name** – Choose a name for the volume.
- **Path** – Browse for the folder that you want to share.

## Volume services

- **Apple Filing Protocol (AFP) file and search** – This is the default setting and creates a volume accessible by AFP. The volume will be accessible and searchable from the Acronis Files Connect Mac client app and the Mac Finder. When opening files and browsing these volumes, the Mac will connect using AFP in either case.
- **Search only (Mac client app will connect using SMB)** – With this option, the volume will be displayed in the Acronis Files Connect Mac client app and will be searchable, but it will not be shared as an AFP volume. Macs connecting to the Acronis Files Connect server using AFP will not see this volume. Macs will automatically connect to 'Search only' volumes and files found in Acronis Files Connect Mac client app search results using SMB. This connection uses preexisting Windows or NAS SMB file server shared volumes.

---

### Note

Acronis Files Connect Search only volumes are not supported on Microsoft Failover Clusters.

---

- **Volume is read-only** – Prevents writing to the volume.
- **Allow guests to use volume** – When checked, a Mac user can log into the file server without supplying a name and password.

- **Reset permissions on move** – Resets the permissions on moved files and folders to inherit from the destination folder.
  - **Enforce Filename Policy** – Enforces the filename policies that are defined in the global settings.
  - **Volume supports ACLs** – ACL support allows Mac machines to use Windows Access Control Lists.
  - **Support Spotlight Searching** – Enables Spotlight searching of file attributes and content.
    - **Windows Search** – When checked, this volume will use Windows Search as the default search engine for this volume.
    - **Acronis Content Indexing** – When checked, this volume will use Acronis Content Indexing as the default search engine for this volume.
  - **Support Catalog Search** – Selecting this check box enables Catalog searching for this volume.
  - **Indexing Options** – Configures all [Indexing options](#).
  - **Support Time Machine backup** – Advertises the volume to Time Machine clients.
4. Browse for the folder you want to share.

---

#### Note

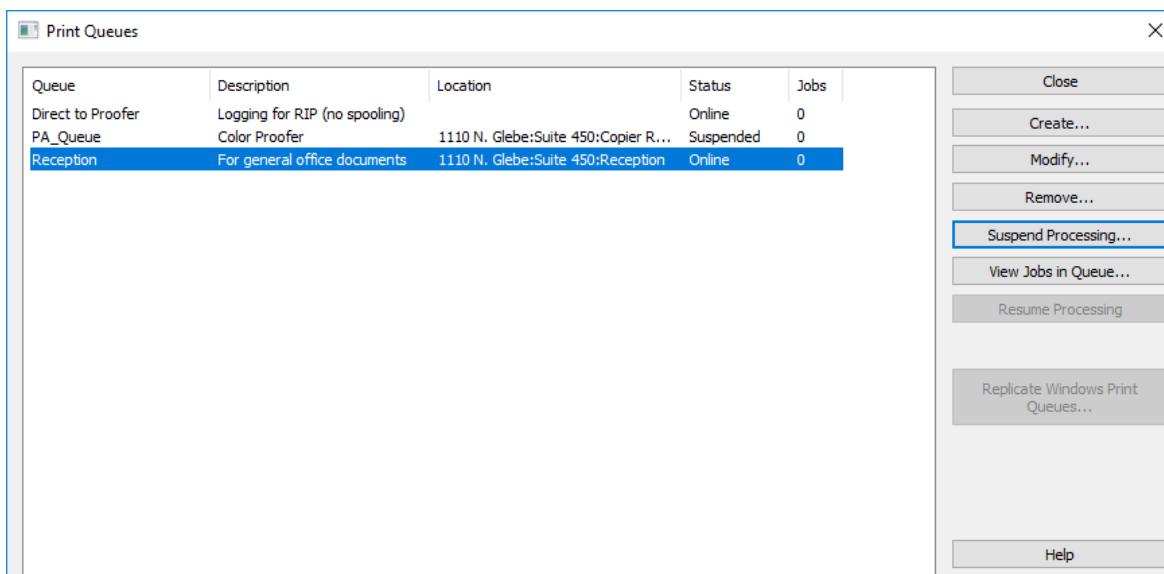
Removable devices (Flash drives, USB drives, etc.) are not supported as volumes.

---

5. Click **OK** to share the volume with Acronis Files Connect.

## Configuring your first shared print queue

1. In the **Acronis Files Connect Administrator**, click **Print Queues**.



- **Create** – Creates print queues. Opens a window with a list of the pending jobs that allows you to start, stop, or reorder the print jobs.
- **Suspend Processing** – When a queue is suspended jobs are accepted by the server however they are not sent to the printer until processing is resumed.

- **View Jobs in Queue** – Opens a window with a list of the pending jobs that allows you to start, stop, or reorder the print jobs.
- **Replicate Windows Print Queues** – Takes the existing Windows print queues and republishes them as Acronis Files Connect queues.

2. Click **Create** to create a new print queue.

- **Name** – The name that appears in the **Printer & Scanner** window of Mac computers.
- **Publish queue** – Defines if the print queue should be discoverable by clients.
- **Processing** – Specifies where Acronis Files Connect will send the jobs after they are received.
- **File** – Specifies the PPD to be used by clients when printing to this queue.

3. Enter a **Name** for the print queue.

4. Select a **Processing** method and enter the information required for the selected processing method.

5. Click **OK**.

## The Acronis Files Connect Mac client app

Introduced in Acronis Files Connect 10.5, the Acronis Files Connect Mac client app is by far the easiest way to connect to network resources.

---

### Note

The Acronis Files Connect Mac client app can only be run on Mac OS X 10.10 or later.

---

There are two ways to download the Acronis Files Connect Mac client app:

- By opening the Web Service address of your Acronis Files Connect deployment with the proper port. For example, `https://myserver.mycompany.com:8085`

---

### Note

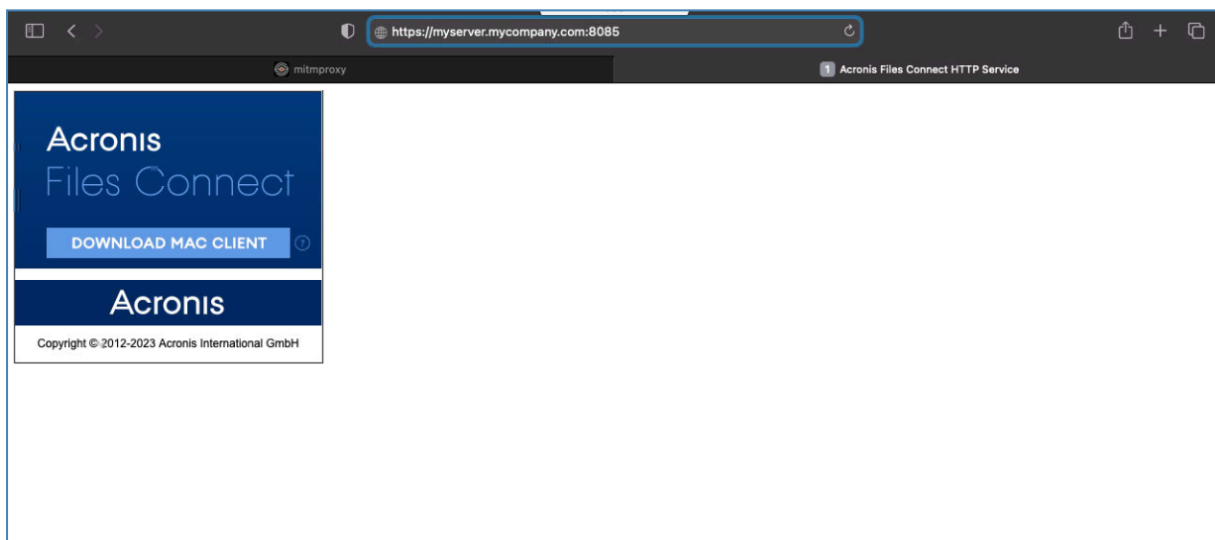
When connecting to the server, you may see the message *This connection is not private*. This is expected behavior if the Acronis Files Connect Web Service App/HTTPS Port has not been configured with a public trusted certificate. *See more about [Ports and certificates](#).*

Alternatively, for Safari, you may wish to adjust your Certificate Trust Settings to trust the default self-signed certificate used by Acronis Files Connect. To update them, click on *Show details* and then *Visit this website*. Then click on *Visit website* and enter your password to complete the process.

Other web browsers may require different steps.

---

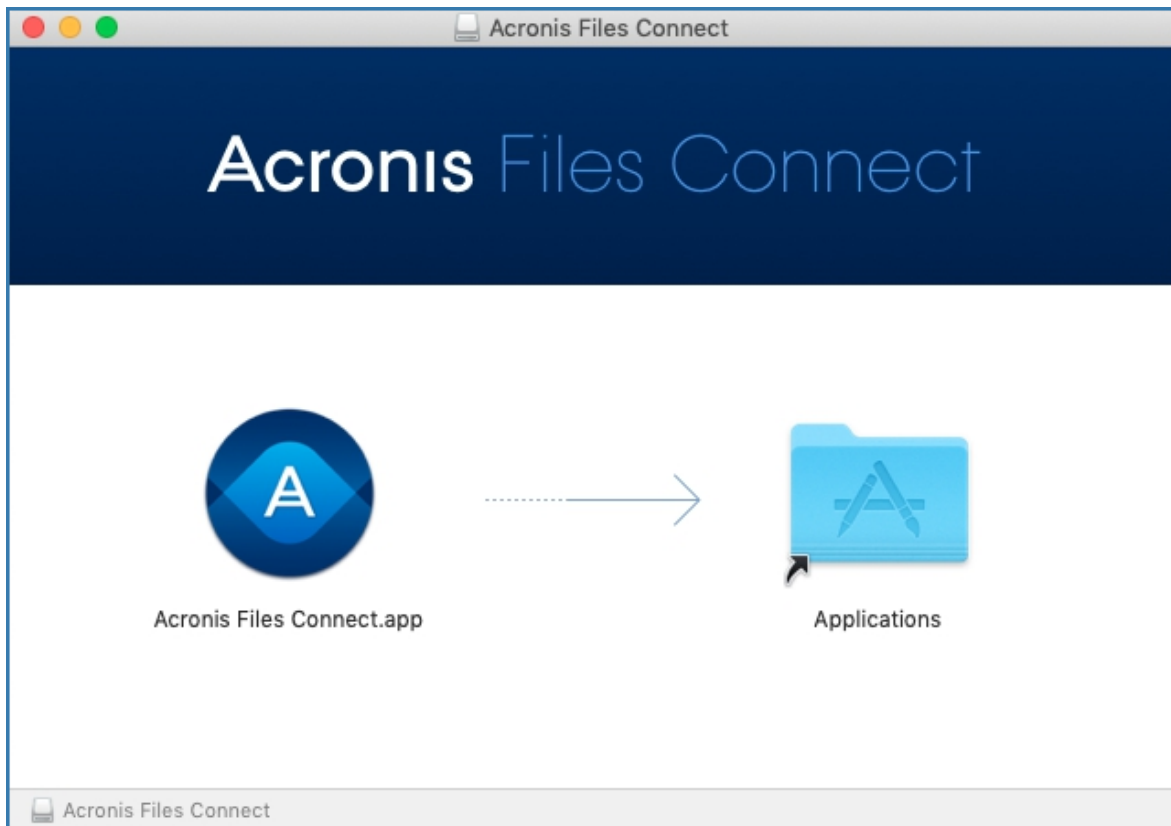
Once you have opened the address of Acronis Files Connect in a browser, you will see a button to download the Acronis Files Connect Mac client app.



- Users that have access to the **Acronis Mac Resources** (Acronis Files Connect AFP) volume, can also download the Acronis Files Connect Mac client app from there.

## Installation

1. Download the Acronis Files Connect application and install it.



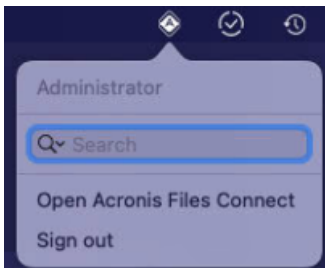
2. In your Menu Bar you will see the Acronis Files Connect icon.
3. The Acronis Files Connect options menu is opened by default. Select **Preferences**.

---

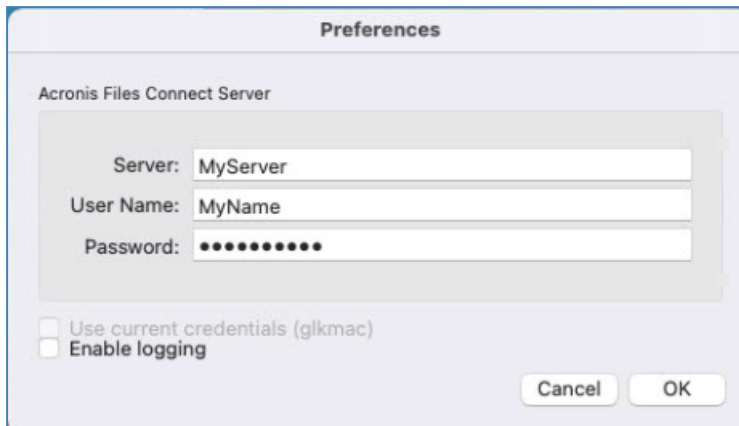
### Note

If it isn't open, you can click on the app menu to open it.

---



4. In the **Server** field, enter the FQDN or short name of your Acronis Files Connect server. For example, `myserver.mycompany.com` OR `myserver`.  
If you have multiple servers, using the address of the primary gives you access to all servers and volumes.



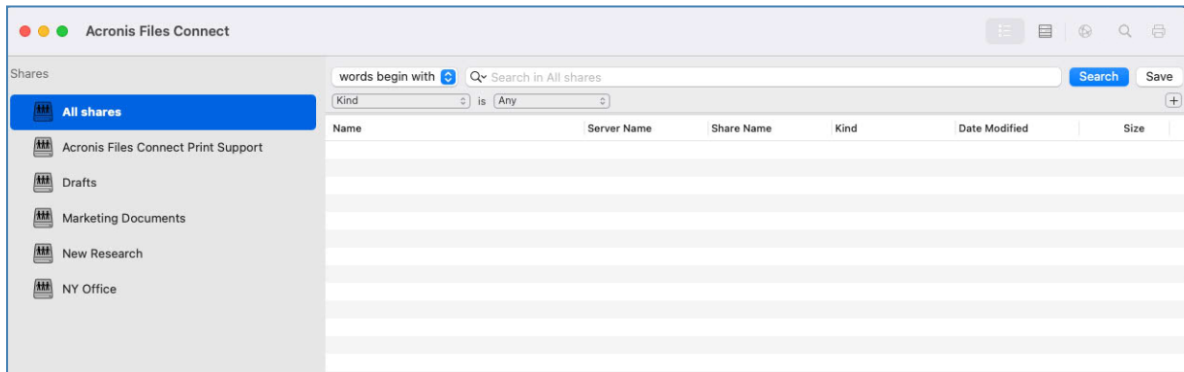
5. Enter your credentials which will be used to connect to Acronis Files Connect's resources. These are most likely your Active Directory username and password.
6. Alternatively, if your computer is bound to the company domain and you are logged in to the computer with the account you wish to use, you can select **Use current credentials (yourusername)**.

## Use

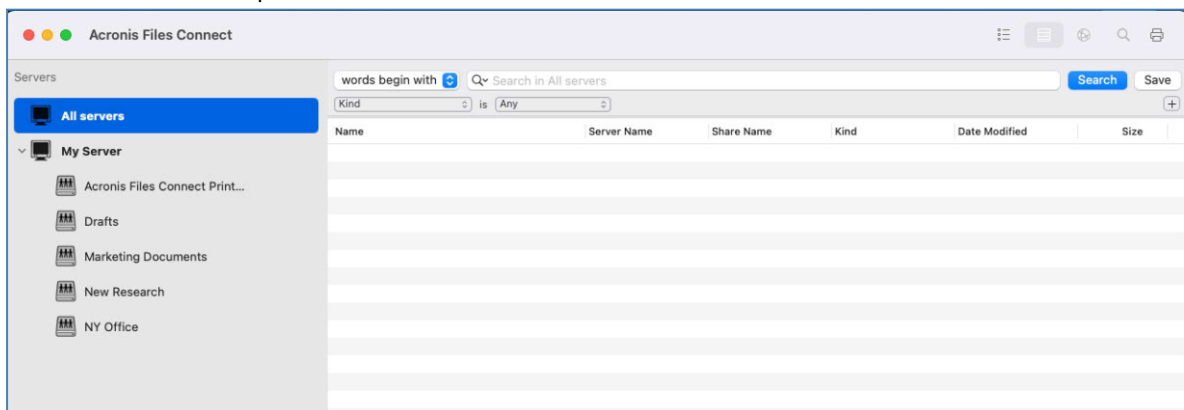
Once connected, you can navigate the available resources via the four tabs in the upper left corner.

They allow you to view the available resources, as follows:

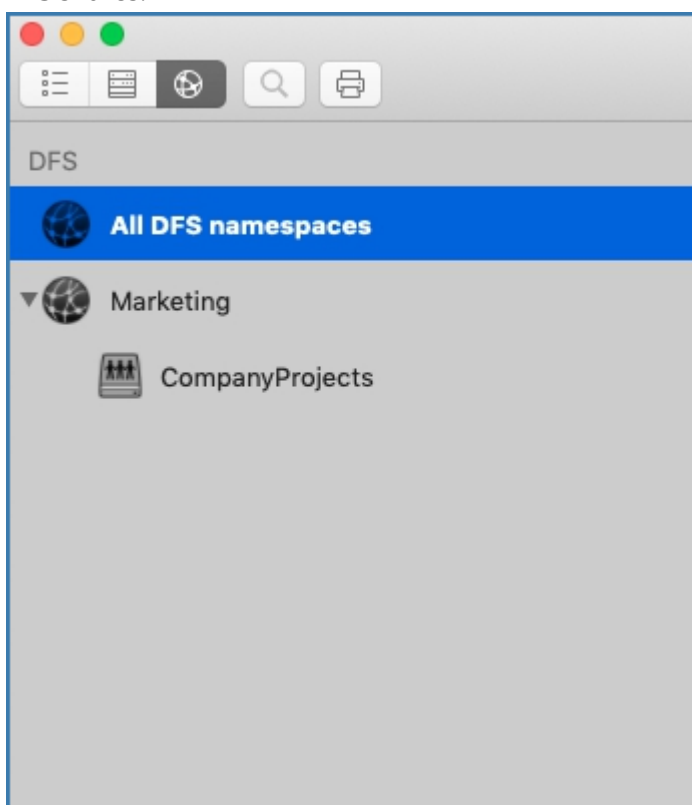
- Only shares:



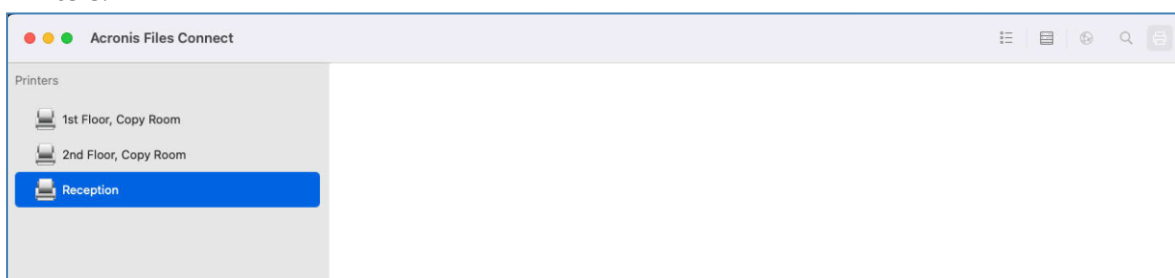
- Servers and their respective shares:



- DFS shares:



- Printers:



- To refresh the list of shares and printers, click on **View** in the menu bar and select **Refresh**. You can also use **Command + R**.

## Multi-selection

You can multi-select items by using **Command + Click** or **Shift + Click** on them. This works for files and folders and also works for **Shares** and **Servers** when you want to search in a couple of specific shares instead of **All Shares**.

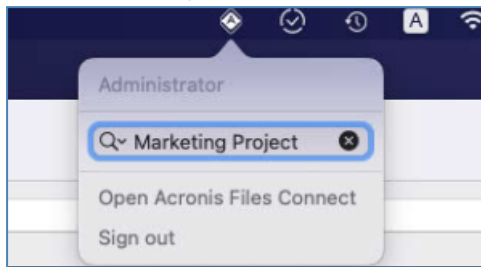
## Search

You can search for files by many parameters like file type, creation date, filename, file content and more. The search is performed only for the selected share(s)/server(s).

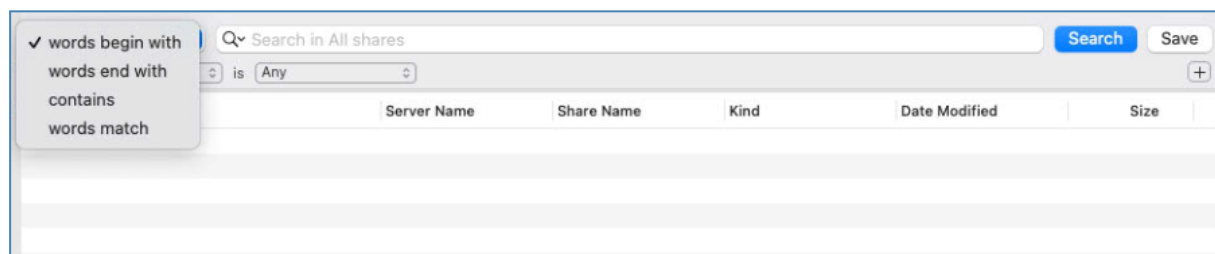
1. The quickest way to search is by clicking on the Acronis Files Connect icon in the Menu Bar and using the search field. By default, this will search in all available shares unless you have already

used the app to search in specific shares. Your last search will become the new default.

- You can also click on the magnifying glass icon and select the search parameters from a list of recent search queries.



- The default filter is by **name** and **content** if content search is enabled for the volumes being searched.
2. Alternatively, you can use the search bar in the app itself. Here you can also configure the search parameters. For example, searching for files that **begin with X**, and their file **Kind** is **Executable**.



## Search Filters

- **Words begin with** matches any word, within a string, beginning with the pattern you have entered. For example, "**alpha delta tango**" would match "**Words begin with del**".
- **Words end with** matches any word, within a string, ending with the pattern. For example, "**alpha delta tango**" would match "**Words end with Ita**".
- **Contains** matches any substring, within a string, wherever it is. For example, "**alpha delta tango**" would match "**Contains ang**".
- **Words match** only searches for exact matches within the string. For example, "**alpha delta tango**" would match "**Words match alpha delta tango**".

---

### Note

Only whitespace is treated as a word separator. The strings **alpha\_delta\_tango** and **alphaDeltaTango** are considered one word and would not match a **Words begin with del** search.

---

### Note

Whatever parameter you choose for the main search filter, will become the new default until you change it. This does not include the additional filters you add like **Kind**, **Any**, etc.

---

## Recent Searches

- For quicker and easier access to the files you search for often, you can pick one of the 10 most recent searches. This list is accessible from the magnifying glass icon both in the Menu Bar and in the app itself.

## Mounting Shares and Finder integration

- Double-clicking on a share or a found file automatically mounts the share and opens the file. To unmount such a share, click on the icon that appears next to its name.
- You can right-click on a file and select '**Show in Finder**', which opens the Finder directly to the file's location. This also works for multiple selected files.

## Bookmarks and Recent Files

- Right-clicking on a file or a number of selected files allows you to create bookmarks for the selected items. Afterwards, these bookmarks can be accessed from the Acronis Files Connect Menu Bar > **Bookmarks**.
- A list of the 20 most recent files you have opened is accessible in the Acronis Files Connect Menu Bar > **History**.

## Removing the Acronis Files Connect Mac client app

1. Open the **Applications** folder and move Acronis Files Connect to **Trash**.
2. In **Terminal**, write:  

```
defaults remove com.acronis.AcronisFilesConnect
```
3. In ~/Library/Application Support/Acronis/, delete the Acronis Files Connect folder.

## Connecting from the Mac Finder

1. From the Finder, click the **Go** menu, and then click **Connect to Server**.
2. Type **afp://** and then the name of the server. For example, **afp://server.mycompany.com**.
3. Select the volume you want to mount.

**Ensure that you connect with afp://. If you connect with smb://, you will be using the Windows SMB protocol and won't get the benefits of Acronis Files Connect.**

---

### Note

AFP volume names are case-sensitive. When you specify a volume to connect to, the case will need to match the volume name configured in the **Acronis Files Connect Administrator > Volumes** panel. Connecting to the server without specifying a volume will present a list of available volumes.

---

### Note

You may also be able to see the server by clicking the **Browse** button.

---

---

**Note**

If you cannot connect using the name of the server, try with the IP address. For example, `afp://10.1.5.27`

---

## Connecting from a mobile client

You can allow mobile clients to connect to your Volumes. To enable the mobile access feature, open the Acronis Files Connect Administrator > **Settings** > **Mobile Access**, and then select the check box.

For more information on mobile access feature, refer to [Setting Mobile Access](#) and [Using Mobile Access](#).

## Additional resources

### Network Reshares

With the introduction of 'Network Reshare', Acronis Files Connect now includes the ability to create file share volumes that point to folders located on other servers and NAS devices on your network. Mac users continue to connect to Acronis Files Connect using the standard AFP file sharing protocol, while Acronis Files Connect utilizes the SMB/CIFS file sharing protocol to access files that are requested by Mac users from remote servers and NAS systems. By doing so, Mac users retain all the benefits of AFP file sharing while gaining access to resources that have traditionally only been available through SMB/Windows file sharing.

For in-depth information on the configuration and usage of Network Reshares, refer to [Configuring Network Reshare](#).

### Network Spotlight Search

Spotlight search allows files to be found by searching on content, in addition to file names and file attributes. When enabled, Spotlight search replaces both enumeration and catalog search and provides results when searching at both the root of a volume and within subfolders.

You can do Spotlight searches through the Acronis Files Connect Mac client app. See [more details on how to use it](#). For in-depth information on how to configure and use Spotlight Search, refer to [Spotlight Search](#) and [Support Spotlight Search](#).

### Filename Policies

Since Acronis Files Connect provides seamless communication between Windows file servers and Mac users, you can configure policies on valid file names and file types.

Acronis Files Connect could detect and reject the Mac users' attempts to save (create, rename, move) files with characters that are "illegal" in Microsoft File Explorer or other applications that don't support the Unicode file system APIs.

You have to configure what is allowed or deemed "illegal". The list could include:

- Characters that cannot be displayed on Windows
- Trailing spaces
- Unicode characters not available in the default Windows font
- Any given character
- File names longer than "x" characters
- Specific file extensions

Filename Policies do not affect existing files on the server or files that are copied via Windows file sharing.

For in-depth information on the configuration and usage of filename policies, refer to [Setting Filename Policy](#).

## DFS Support

Acronis Files Connect can be configured to make a Microsoft Distributed File System (DFS) available to Mac users. In addition to the server-side configuration, installation of the Acronis Files Connect Mac client app is necessary for each Mac that requires access to DFS.

Find [more information](#) about the prescribed client-side configuration.

For more information on how to configure and use Distributed File System with Acronis Files Connect, refer to [DFS](#).

---

### Note

DFS support requires two additional settings. In the Acronis Files Connect Administrator, select **Settings > Security** tab. Enter your **Directory Services** credentials and enable **Support UNIX Permissions and ACLs**.

---

# Installing Acronis Files Connect

## Getting started

Acronis Files Connect is optimized to provide the fastest file and print services available.

Acronis Files Connect includes the following services:

- Acronis Files Connect File Server
- Acronis Files Connect Print Server

With Acronis Files Connect, Mac users can connect to and mount directories on a Windows file server. With the Acronis Files Connect Print Server installed, Mac users can create desktop printers that deliver print jobs to printers via the server automatically. Acronis Files Connect's integration into the existing network is seamless – Mac users continue using the same tools and applications for accessing the server and printers that they always have, but the server delivers much higher performance.

## System requirements

Verify that your server meets the requirements for Acronis Files Connect. It is recommended that you quit any running programs, including the **Services** control panel, before starting the installation.

The following are the minimum system requirements for the Acronis Files Connect File & Print Server on Windows Server and Windows Workstation platforms and for connecting from Mac machines. For optimal results, your Windows Server machine should be running the latest service pack from Microsoft®. Adding additional RAM to your server machine will greatly enhance Acronis Files Connect performance. The recommended system requirements for a particular implementation or application can vary, so please **contact Acronis Technical Support** if you have questions or need assistance.

## Operating System Requirements

### Windows Server Platforms

- 2022 Standard & Datacenter
- 2019 Standard & Datacenter
- 2016 Standard & Datacenter & Essentials
- Windows Storage Server 2016
- Windows Powered NAS

### Windows Workstation Platforms:

- Windows 10

### Mac users:

- macOS 10.10.5  
Find more details about newer macOS versions in the Acronis Files Connect [Release notes](#).

## Hardware Requirements

### Minimal configuration

- Local shares – Core class CPU with 2 or more cores, 4 GB of RAM
- Network Reshare – Core 'i' class CPU with 4 or more cores, 8 GB of RAM, dual non-bonded Gigabit Ethernet NICs

---

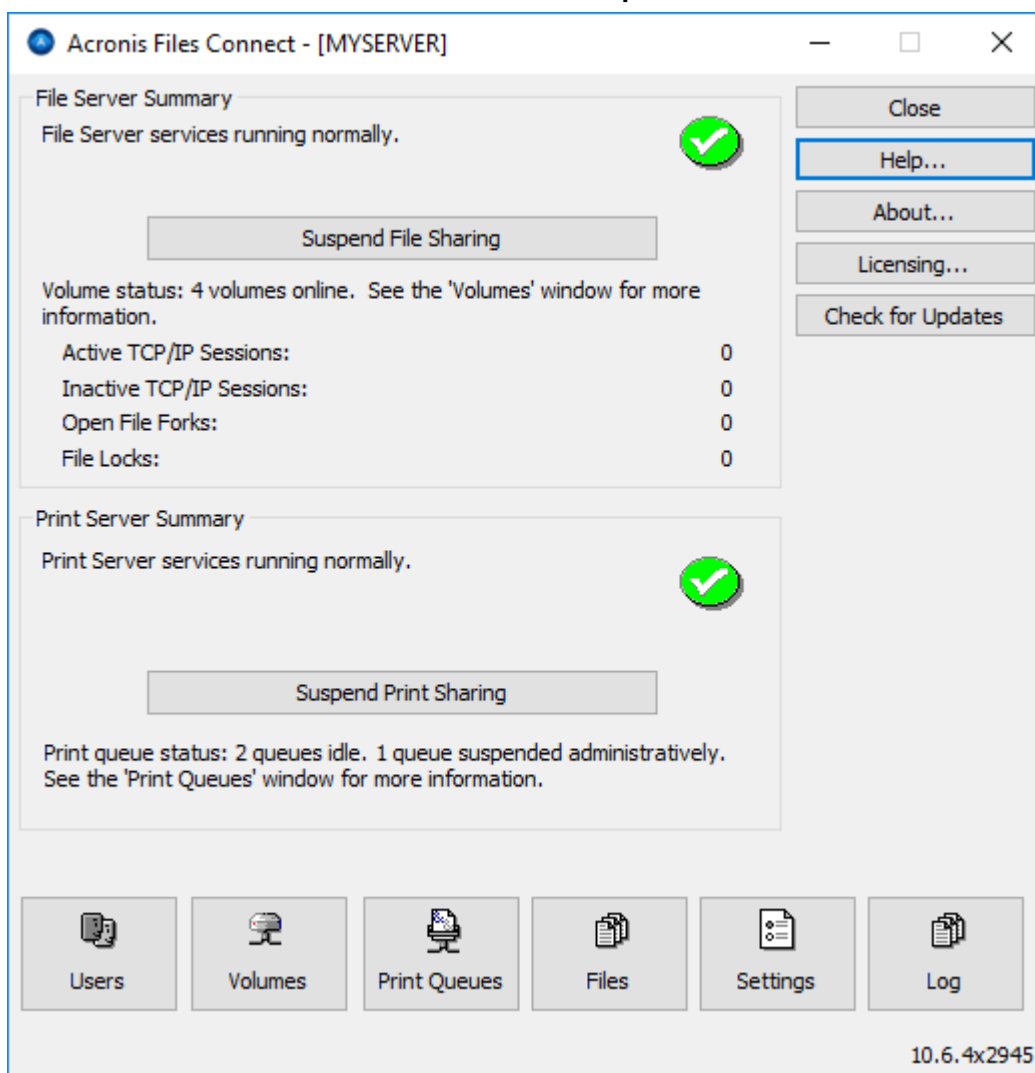
### Note

You may need substantially more resources depending on the number of volumes and users and other applications running on the server.

---

## Getting help

1. In **Acronis Files Connect Administrator**, click **Help**.



2. Find more information at [Acronis website](#).

3. Check the most up-to-date release at [Acronis Files Connect Latest Releases page](#).
4. Search the [Acronis Support Portal](#).

The price of Acronis Files Connect includes one year of free technical support and updates. After that, you can purchase extended support.

For technical support services, please submit a support request at <https://support.acronis.com/mobility>. Please have your Acronis Files Connect serial number ready for verification. For more details, refer to [Acronis Files Connect Mobility: Support & Maintenance Guide](#).

## Installing Acronis Files Connect

The primary component of Acronis Files Connect is a Windows Service that provides file and print sharing to Mac users. Acronis Files Connect also includes a GUI Administrator where you can configure shared volumes and other settings, and a Gateway service which enables mobile users to connect to your Volumes. The number of clients who can connect using Acronis Files Connect depends on your license and its client count. You can upgrade your client count as needed. Acronis Files Connect counts multiple connections from one user account on one IP address as one user for licensing purposes.

### Before you begin

This topic gives you the information you need before installing Acronis Files Connect.

***Installing Acronis Files Connect on a Domain Controller is not recommended as it can cause issues with Kerberos.***

### Required Windows File Permissions for Shared Volumes

Acronis Files Connect relies on the SYSTEM account on the Windows server to perform many of its core functions. For this reason, any folder hierarchy that is shared as a volume with Acronis Files Connect requires that the SYSTEM account has **Full Control** access to the entire folder hierarchy. These permissions are set by default for the Windows OS partition, but any additional disks or partitions containing Acronis Files Connect volumes must also have SYSTEM = 'Full Control' set to allow Acronis Files Connect to function properly. Make sure to verify that all the volumes you share have this permission set. See also the [Acronis Files Connect: File System Best Practices](#), especially the PDF document attached to this article.

### Sharing the Root of a Drive

Although Acronis Files Connect supports sharing out the root of the drive, Windows treats permissions at the root of the file system differently from other folder permissions. We recommend that you do not share out drive letters directly. Instead, you should create a sub-folder for your shared volume.

## Installing Acronis Files Connect

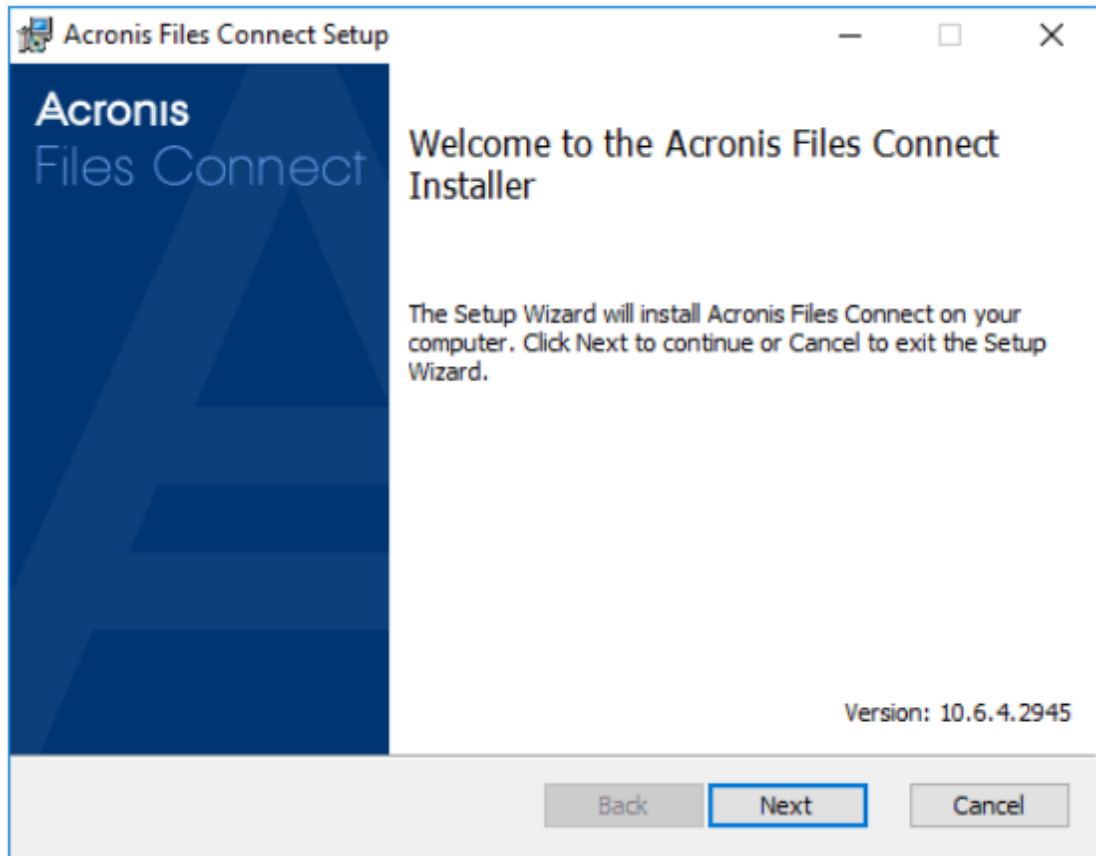
1. Run the **Acronis Files Connect Installer**.

---

### Note

To install Acronis Files Connect you must log in to Windows with Administrator privileges.

---



2. Click **Next** to begin the installation.
3. Accept the Software License Agreement and click **Next**.
4. Click **Next** to accept the default Destination Folder.
5. Click **Install** to begin installation.

---

### Note

If you have a previous version of Acronis Files Connect installed, it will be upgraded to the new version. Any existing settings will be retained.

---

6. Click **Finish** to close the completed installer and automatically launch the **Acronis Files Connect Administrator**.

---

## Note

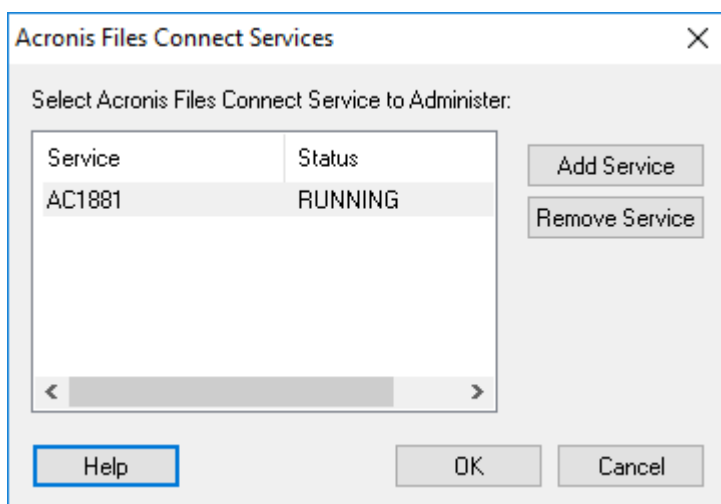
For re-installations, the Acronis Files Connect installer stops the Acronis Files Connect Service to perform the install. However, in some cases the installation fails because the Acronis Files Connect Service cannot be stopped. These cases include possible service errors, conflicts with other running processes, or installing while the Services Control Panel is open. If you experience installation failures, you can stop the Service manually from the Services Control Panel and proceed with the install.

---

## Administering Acronis Files Connect on a Cluster

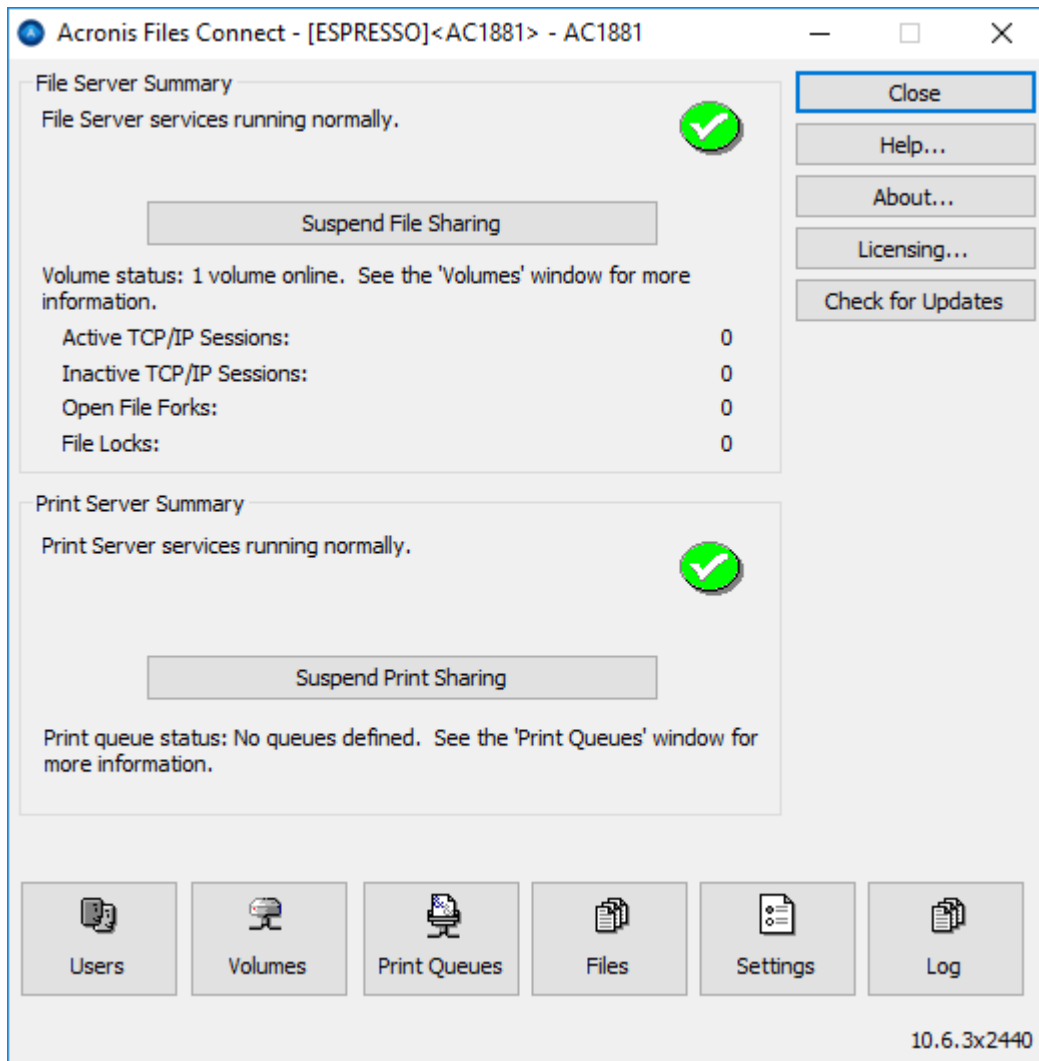
In a clustered environment, the Acronis Files Connect Administrator behaves differently than it does in a non-clustered environment. You should always execute administration tasks on the node currently running the Acronis Files Connect Virtual Server you want to administer. Starting the service from the Acronis Files Connect Administrator or the Services control panel is disabled for clustered configurations. Clustered services should be started ONLY from the Microsoft Cluster Administrator. If the service is started by some other means (an application or the Services control panel) the Cluster Administrator will not know the service is running and, if required, cannot manage a failover.

**Administer services only from the node they are running on.** Then, you can create volumes that point to a specific folder. On a cluster, a node can only access the disks in its cluster group. In order to select a folder with the **Browse for folder** dialog you must run the Acronis Files Connect Administrator on the node where the Physical Disks are located. Using the Acronis Files Connect Administrator, you can create a volume on another node; however, you will need to enter the path manually.



- 1.
2. When the Acronis Files Connect Administrator is started, you will be prompted to select the Acronis Files Connect service that you want to administer.
3. Select an Acronis Files Connect Service and click OK.
4. Once you have chosen a service, the Administrator launches and connects to that service. The Administrator title bar tells you which server it is connected to in the format '(Network Name –

Service Name)'.



If the connection to the server is broken (that Cluster Group is failed over) the administrator cannot reconnect to that service since it is on another node. However, you can now administer it on the node to which it has been moved. If it fails back to the original node, you can reconnect to it.

## Configuring the Acronis Files Connect server for Acronis Files Connect Mac client app

Acronis Files Connect supports the Acronis Files Connect Mac client app with no additional configuration.

On the **Service Discovery** tab of the Administrator, you can change the settings related to the Web Service, which control how users get and connect to the Acronis Files Connect server.

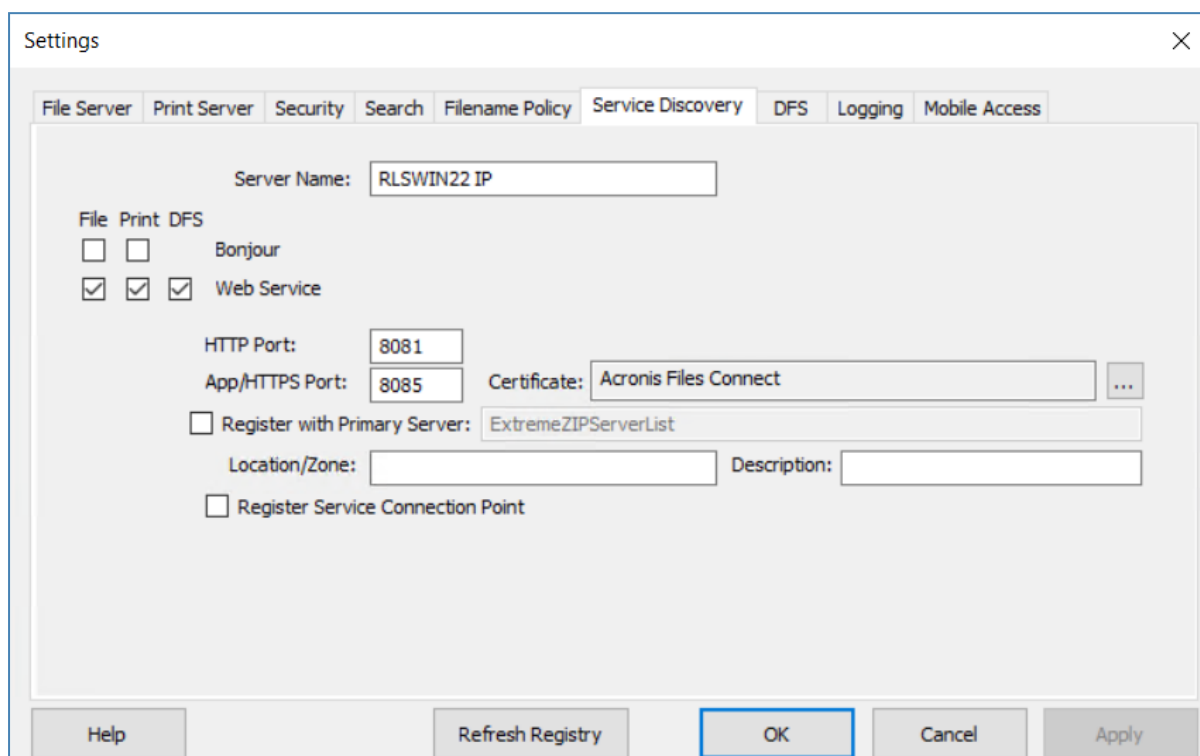
Acronis Files Connect servers are configured to be their own primary server unless specifically set to be Secondary (by enabling **Register with Primary Server**).

---

**Note**

On the Primary server this checkbox should be **Disabled**.

---



If you would like, you can also assign a server to a specific location. A location is composed of locations, separated by colons that contain the hierarchy of zones/locations.

An example of a single-level zone is GLIHQ and a multi-level location might be Virginia:Arlington:1st Floor. In addition to the location property of a print queue or file server, an administrator can also assign them descriptions.

---

**Note**

Locations and descriptions are optional.

---

If only some of the servers do not have a location, they will be displayed at the end of the list, below the locations.

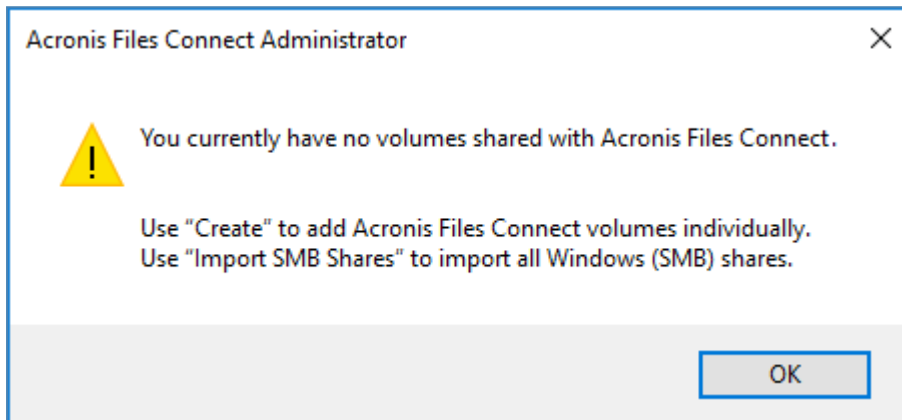
## Adding additional servers to the Primary Server

If you have multiple Acronis Files Connect servers, designate one server to be the Primary server that the Acronis Files Connect Mac client app will contact to discover the other Acronis Files Connect servers on the network.

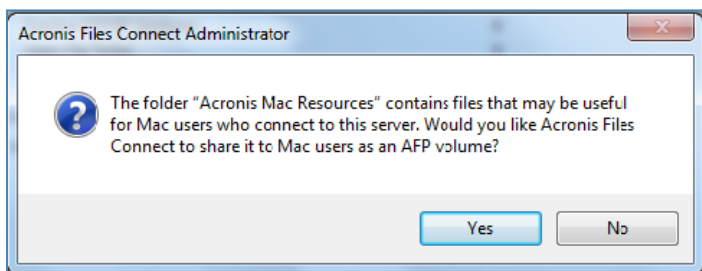
All Secondary servers will be automatically registered with the Primary server by enabling the **Register with Primary Server** setting on the Secondaries and entering the address of the Primary server.

# Launching Acronis Files Connect for the first time

When you launch the Acronis Files Connect Administrator for the first time with no configured volumes (shares), Acronis Files Connect prompts you to create new volumes or import existing volumes. Acronis Files Connect can import existing volumes on your server that are shared using Windows file sharing (SMB).



You will be asked whether to share the **Acronis Mac Resources** volume.



If you are upgrading from a previous version, Acronis Files Connect checks for volumes shared with previous versions of Acronis Files Connect and automatically creates these Acronis Files Connect volumes.

## Automatically importing SMB shares

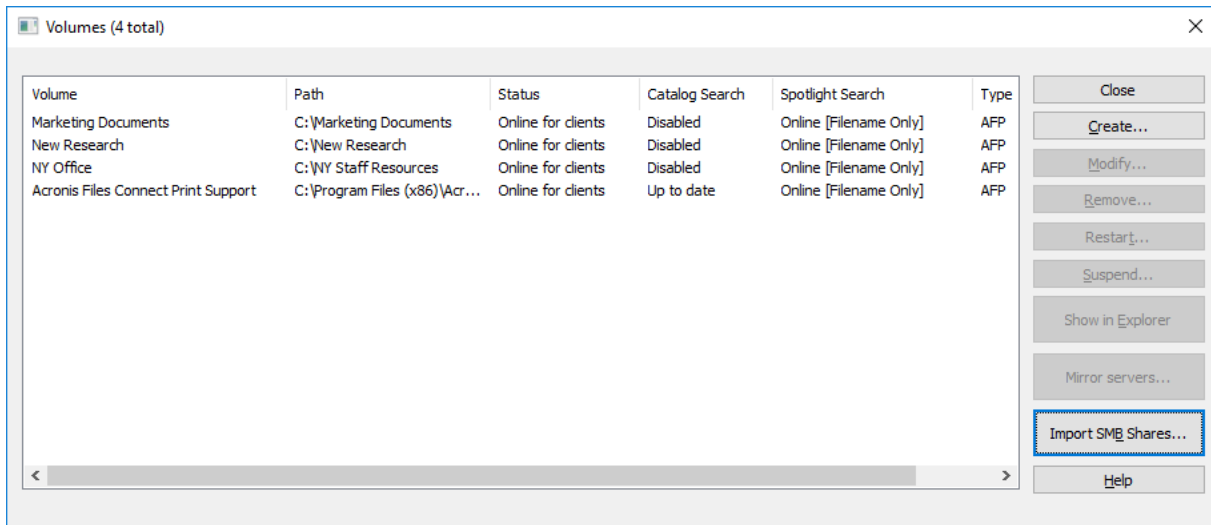
---

### Note

**All shares will be imported as "AFP" shares.**

---

## SMB Shares



Each time the Acronis Files Connect Administrator is launched, Acronis Files Connect checks for any SMB shares that are not being shared as Acronis Files Connect volumes. If any such volumes exist, the **Import SMB Shares** button within the **Volumes** dialog becomes active. If you choose to import such shares, Acronis Files Connect creates new AFP volumes for them.

Acronis Files Connect does not replicate hidden shares (for example, C\$).

---

### Note

SMB shares will not be migrated on a Windows Cluster Server installation of Acronis Files Connect.

---

## Importing SMB shares after first launch

The prompt for SMB importing, that is described above, is only performed once—the first time you launch the Acronis Files Connect Administrator. After that, use the **Import SMB Shares** button in the **Volumes** window of the Acronis Files Connect Administrator to bring shares over as Acronis Files Connect volumes. See [Creating volumes](#) for information about migrating volumes.

## Naming conventions for SMB volumes

Imported SMB volumes must adhere to the standards of Acronis Files Connect volume names. With Acronis Files Connect 8.0.4 or later, a name can have up to 127 characters for UTF16 and 190 for UTF8. If any migrated or replicated shares have names that are too long, the names are truncated. In the event that a migrated or replicated share has a name matching a current Acronis Files Connect volume, Acronis Files Connect appends a number to its volume name, for example 'Volume (2)'. The volume name may be truncated in order to have room to append the number.

## Using Kerberos

The Massachusetts Institute of Technology created Kerberos to address security issues as username/password exchange, network security, client computer security, and login persistence. Kerberos is a protocol that provides secure network authentication and support for 'single sign-on' to network resources. With single sign-on support, a user logs in one time to a network domain (also called a realm) and, after he or she is authenticated, gains access to resources on other computers without resubmitting user name and password. Kerberos works on the premise that only the client and the authenticating server share a piece of secret information and it provides a way to confirm that the shared information is accurate throughout the user's session. When a user on a client computer enters username and password and submits that information to a server to log in, Kerberos first authenticates the user and then issues a ticket that uniquely identifies the client for that session. This ticket is used for future access to other applications and shared volumes during the user's session. Kerberos provides encrypted key exchange to ensure security on both internal networks (behind firewalls) and insecure networks such as the internet. Once a user is authenticated, all further communication is encrypted for privacy and security.

Acronis Files Connect supports the Kerberos extensions in the AFP protocol and works directly with Active Directory. It is registered as a Kerberos service provider and can authenticate Mac tickets. Since the tickets themselves are a standard format within Kerberos, Acronis Files Connect takes tickets from a Mac and passes them to Microsoft Windows Active Directory for authentication and then grants access to Windows server resources if Active Directory confirms that the client has a valid ticket.

## Troubleshooting Kerberos

If you are having trouble getting Kerberos to work with Acronis Files Connect, use the following troubleshooting steps:

- To verify that a client computer has communicated successfully with the Kerberos ticket authority and has received a ticket for Acronis Files Connect, run the Kerberos application located in `/System/Library/CoreServices`. The active Kerberos tickets are listed in `Kerberos.app`. In addition, the Kerberos application can be used to destroy existing tickets before their normal expiration time.
- To verify that a client computer is bound to the Active Directory Domain correctly and is running the right version of Kerberos modules, try connecting to the server from the Mac over **SMB** instead of **AFP** by typing `smb://SERVER_NAME` into the Server Address field in the **Connect To Server** dialog. If you are required to log in then you will know that there is a general problem with Kerberos.

# Setting up Acronis Files Connect Clustering

Clustering ensures fast failover and quick restart of the services provided by a failed server node. You set up an Acronis Files Connect cluster using Microsoft Cluster Servers (MSCS)—specially linked servers running the Microsoft Cluster Service. If one server fails or is taken offline, the other server or servers in the cluster immediately take over the failed server's operations. The applications running on the cluster are always available. The resources running on multiple servers appear to the connected clients as a single system, referred to as Acronis Files Connect virtual server. When a successful failover occurs because of a problem, the connected users sometimes cannot tell that the service was interrupted. Acronis Files Connect is a cluster-aware application that you can use on active/active clustered configurations. Multiple instances of Acronis Files Connect can run on a single server node. Each instance has its own IP address and can be assigned its own shared volume. The configuration of multiple virtual servers provides server consolidation and load management benefits. Running multiple instances of Acronis Files Connect on a server node provides high reliability because each instance runs in isolation from the others. For help in configuring a cluster, see the following Cluster Worksheet. Acronis Files Connect supports the following services in clustered configurations:

- active-active clustering
- multiple virtual servers per node in a cluster
- improved reliability and availability
- eight node clusters
- possible server consolidation

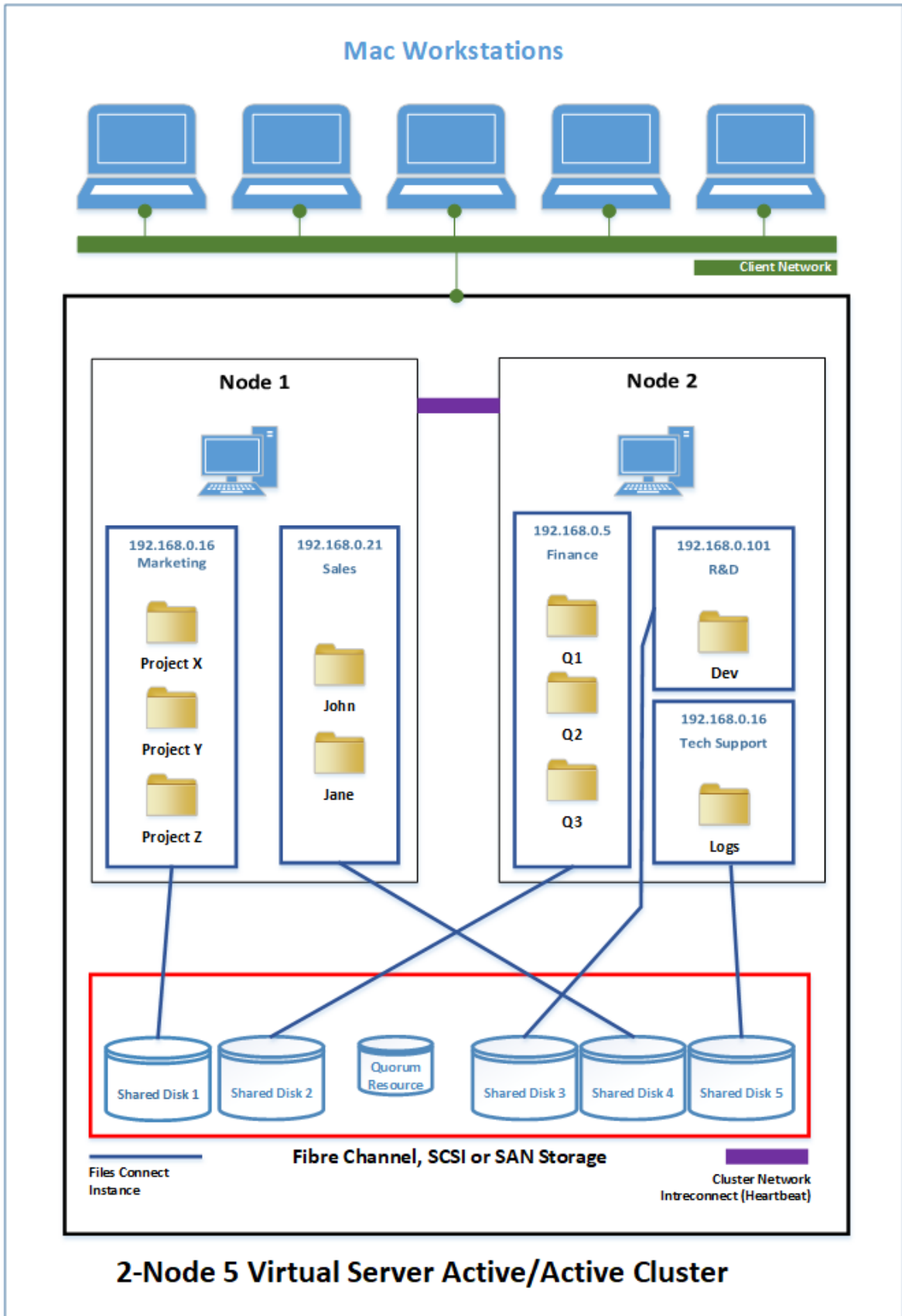
When you are running Acronis Files Connect in a clustered environment, the Acronis Files Connect Administrator window shows the following in the title bar:

- the name of the server in upper case characters
- the name of the service in upper or lower case as you typed it when you set up the service.

MSCS uses the following terms to describe the component parts of a cluster configuration. Do not confuse these terms as you proceed with installing Acronis Files Connect.

- **Node** – A single member server in a cluster.
- **Resource** – A hardware or software component that runs in a cluster, such as a disk, an IP address, a network name, or an instance of the Acronis Files Connect service.  
**Group** – A combination of resources that are managed as a unit of failover. Groups are also known as resource groups or failover groups. A typical Acronis Files Connect failover group consists of a disk, an IP address, a network name, and an instance of Acronis Files Connect.
- **Dependency** – A service or other resource that must be available first in order for the dependant service to start.
- **Failover** – The process of moving resources or resource groups from one server to another. Failover can occur when one server experiences a failure of some sort or when you, the administrator, initiate the failover. This term is equivalent to the Microsoft Cluster Administrator action of moving a Cluster Group to another node.

- **Quorum Resource** – A disk resource containing the failover information that is shared between nodes in a cluster.
- **Heartbeat** – The communication between Cluster nodes tells the other nodes that the service is still running.
- **Virtual Server** – A virtual server is a combination of configuration information and cluster resources, such as an IP address, network name and an application resource. An Acronis Files Connect Virtual Server (EVS) is defined by its unique IP address.
- **Active/Active** – This term describes a configuration in which multiple nodes are Acronis Files Connect file servers running in production.
- **Active/Passive** – This term describes a configuration in which one node is active in production and another node sits idle until a failover occurs.
- **Shared Storage** – This term refers to the external SCSI or fibre channel storage system. Shared storage is a requirement for multi-node clusters. Although this storage is shared, only one node can access an external storage resource at any given time.



---

**Note**

Each server has its own IP address. You can configure multiple shares for each virtual server.

---

**Note**

Acronis Files Connect Search only volumes are not supported on Microsoft Failover Clusters.

---

## Cluster worksheet

For each Acronis Files Connect service running on your cluster you will need the following:

1. A name for the unique Acronis Files Connect service (the first instance is created by default and is named ExtremeZ-IP)
2. A unique IP address and optionally a network name
3. Shared physical storage
4. A cluster group in which to put the new Acronis Files Connect service

To simplify this process we have provided a worksheet to prepare for your installation. Duplicate the worksheet for each additional Acronis Files Connect virtual server you would like to create.

Information needed to install the software Acronis Files Connect Serial Number:

For each virtual server you want to set up, you will need to have unique values for all the sections below.

Information needed to create a new service:

- **Unique service name**
- **Information needed to set up a new cluster group**
- **Cluster Group name**
- **Network name (DNS/Netbios name)**
- **Unique service name (created above)**
- **Volumes to be shared**
- **Drive**
- **Letter Volume Name**
- **Is the volume shared with Windows?**

INFORMATION NEEDED TO INSTALL THE SOFTWARE	
Acronis Files Connect Serial Number	

For each virtual server that you want to set up, you will need to have unique values for all sections below

INFORMATION NEEDED TO CREATE A NEW SERVICE	
Unique service name	



- An IP address and network name for each Acronis Files Connect virtual server you want to create; create a DNS entry for each IP address.

---

**Note**

If folders shared over SMB (for Windows clients) reside on the same physical disk as Acronis Files Connect shares, we recommend configuring DFS (Distributed File System) so that your Windows users can use one IP address or host name to access your shared volumes.

---

## Installation procedure

Installation consists of the following four primary parts, detailed in the subsequent sections. Complete these steps on each node of the cluster.

### 1. Software installation

You need the installer and the serial number provided by Acronis to install the Acronis Files Connect on each node of the cluster.

Follow the instructions:

- "Installing Acronis Files Connect" (p. 37)

### 2. Service configuration

Use the Acronis Files Connect Administrator application to configure the necessary Acronis Files Connect service(s) on each node of the cluster.

Follow the instructions:

- "Creating an Acronis Files Connect Service" (p. 38)

### 3. Cluster configuration

Use the Failover Cluster Management application to configure the Microsoft clustering service.

Follow these instructions:

- "Creating a Cluster Group in old versions of Windows" (p. 40)
- "Creating a Cluster Group by adding a Windows Role" (p. 44)

### 4. Feature setup

Use the Acronis Files Connect Administrator application again to configure shared folders and other features of the Acronis Files Connect service.

Follow the instructions:

- "Setting Cluster resource dependencies" (p. 48)
- "Bringing the new service online" (p. 48)

---

**Note**

Leaving the Acronis Files Connect Administrator application running may negatively impact the stability of the service. Make sure you open the application, perform the necessary tasks, and then close the application.

---

## Installing Acronis Files Connect

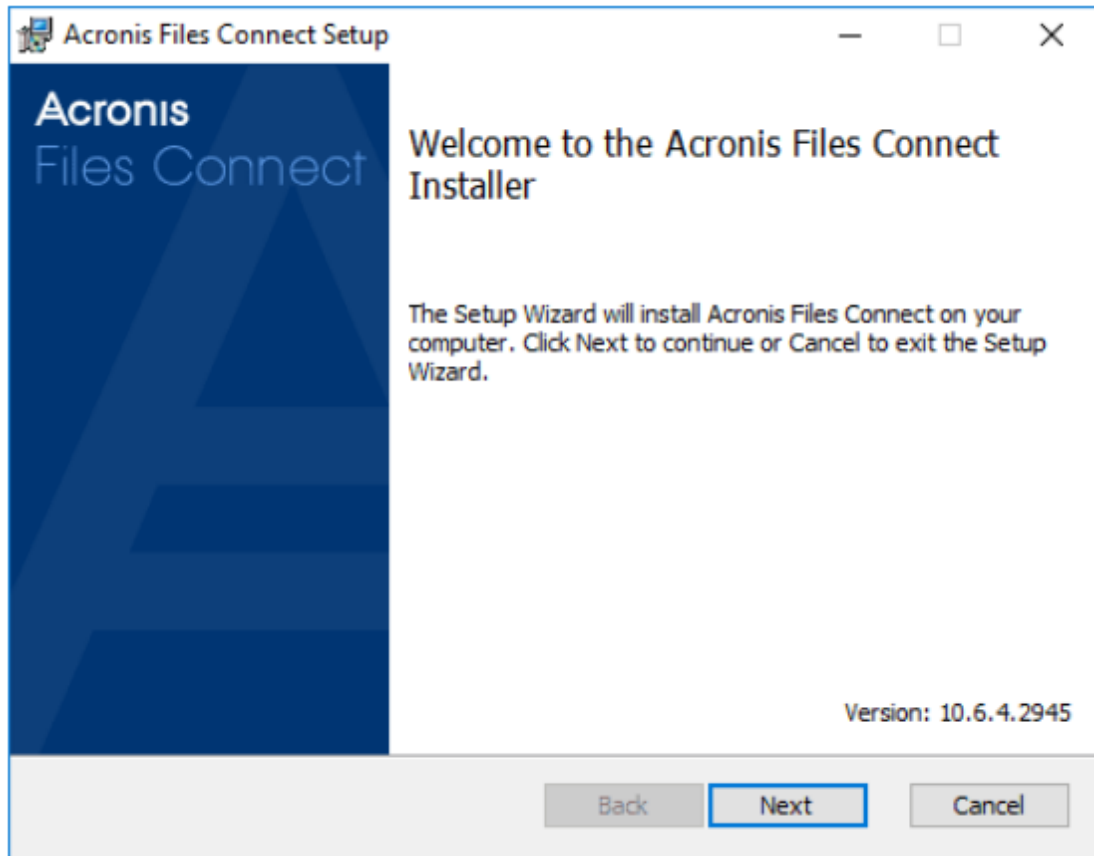
1. Run the **Acronis Files Connect Installer**.

---

### Note

To install Acronis Files Connect you must log in to Windows with Administrator privileges.

---



2. Click **Next** to begin the installation.
3. Accept the Software License Agreement and click **Next**.
4. Click **Next** to accept the default Destination Folder.
5. Click **Install** to begin installation.

---

### Note

If you have a previous version of Acronis Files Connect installed, it will be upgraded to the new version. Any existing settings will be retained.

---

6. Click **Finish** to close the completed installer and automatically launch the **Acronis Files Connect Administrator**.

---

**Note**

For re-installations, the Acronis Files Connect installer stops the Acronis Files Connect Service to perform the install. However, in some cases the installation fails because the Acronis Files Connect Service cannot be stopped. These cases include possible service errors, conflicts with other running processes, or installing while the Services Control Panel is open. If you experience installation failures, you can stop the Service manually from the Services Control Panel and proceed with the install.

---

## Creating an Acronis Files Connect Service

Each Acronis Files Connect virtual server you want to use requires an Acronis Files Connect service instance. Each of these Acronis Files Connect services requires a unique Service Name. When Acronis Files Connect is installed on a cluster enabled server, no services are created by default. In this step, you will create a new Acronis Files Connect service for each virtual server, on each node you want the service to run on.

### Create an Acronis Files Connect Service

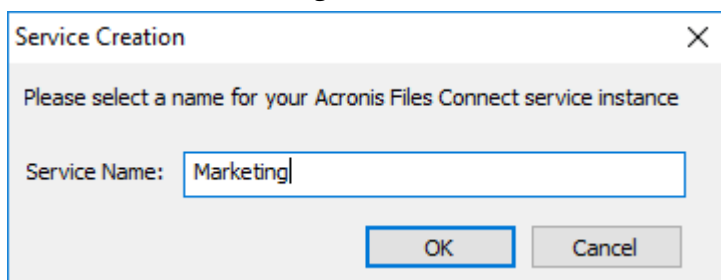
---

**Note**

Prior to adding an Acronis Files Connect Service, you need to first check in the registry if such services already exist at **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services**. If those services are there, remove them before adding the new one.

---

1. After completing the Acronis Files Connect installation process, or on a cluster server with an existing Acronis Files Connect installation, run the **Acronis Files Connect Administrator** application.
2. If Acronis Files Connect is being installed for the first time and no services exist, you will be prompted to create a service. Enter a name for the service and press OK. In this example, our service name is 'Marketing'.



3. Write down the exact service name you enter as you will need it when configuring Microsoft clustering in the next section. The service name will also be displayed in the title bar when you start the Acronis Files Connect Administrator.

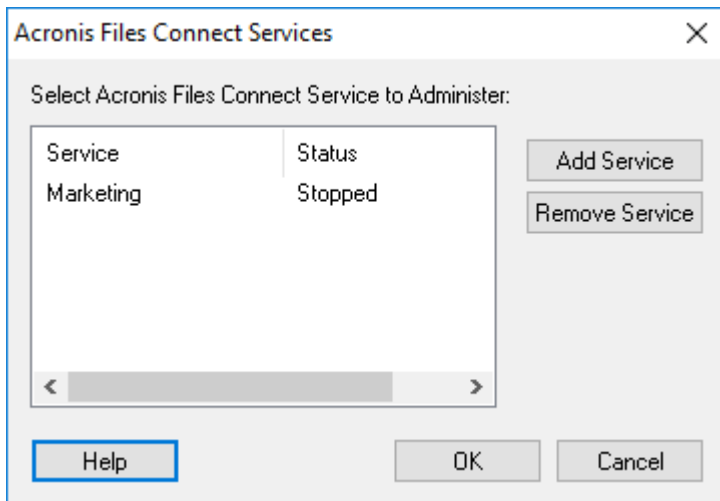
---

**Note**

The Acronis Files Connect service name must be identical on all nodes expected to host the Failover cluster role to which the Acronis Files Connect service is added. Variations in service names across nodes can lead to failures when attempting to transfer the role during a failover.

---

4. After the service is created, it will appear in the Acronis Files Connect Services window. Acronis Files Connect Services will be shown each time the Acronis Files Connect Administrator is launched. It is used to select the service you would like to administer, as well as to add or remove additional services.



5. You will need to perform these steps on each cluster node that these Acronis Files Connect services will run on.

## Configuring Acronis Files Connect services

To operate, Acronis Files Connect requires the following four components:

- **IP Address**
- **Network Name**
- **Acronis Files Connect Service**

Place each set of components in its own cluster group or Acronis Files Connect Virtual Server (EVS). The number of EVSs created is based on the number of physical disks that need to be shared out with Acronis Files Connect. For example, if the volumes are on three physical disks, create three EVSs. This configuration has the most flexibility; however, in some cases you may not want to use up multiple IP addresses. Then you can have multiple physical disks shared out by one EVS. The [Cluster Worksheet](#) can help you set up a plan for your cluster.

## Adding an Acronis Files Connect Service to a Cluster

You can configure the cluster for Acronis Files Connect in a number of ways:

- If you already have set up a Cluster Group, simply add Acronis Files Connect as a generic service to your Cluster Group.
- If you do not have any existing cluster group, follow the steps in the sections below, which take you through the process of using the Cluster Application Wizard® to configure the cluster group.
- Or use an alternative method that is familiar to you.

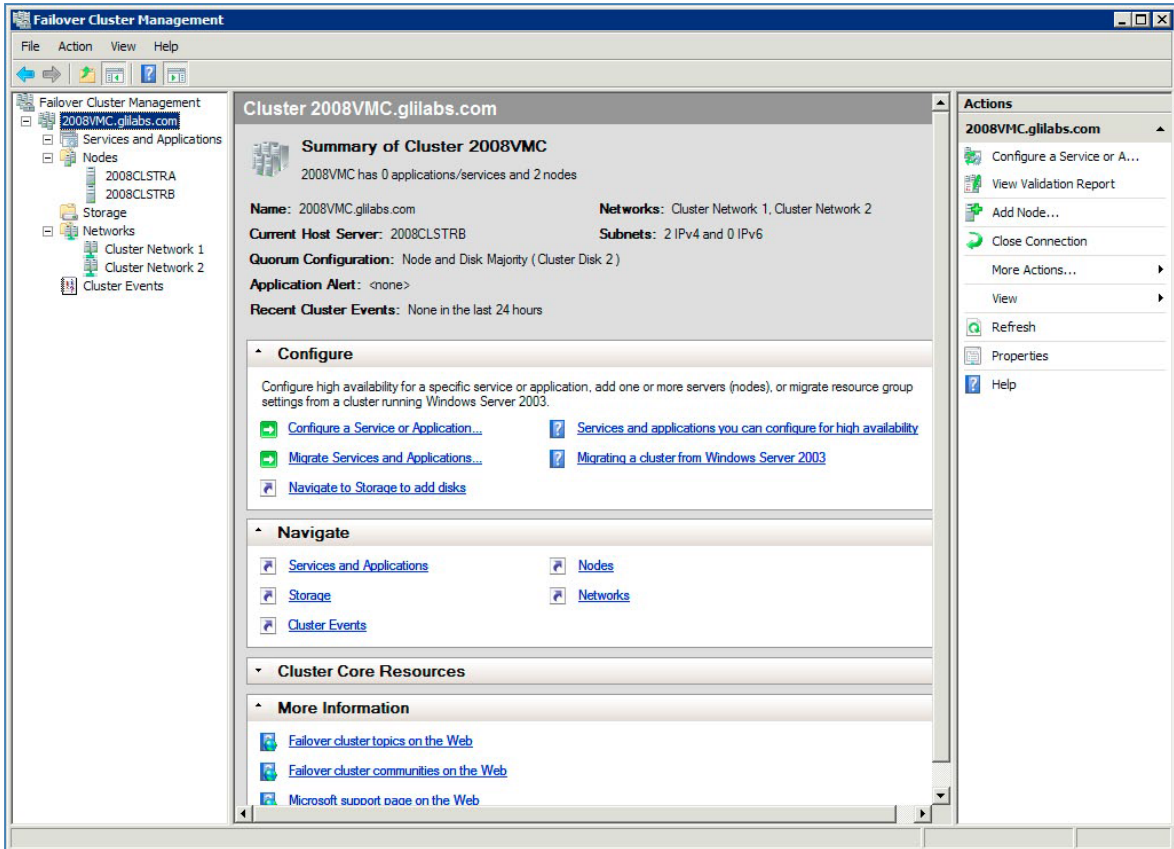
If folders shared over SMB for Windows clients reside on the same physical disk as your Acronis Files Connect volumes, you can add the Acronis Files Connect service to an existing group. In addition, when using an active/active configuration with Windows SMB shares, you may want to install and configure Windows DFS (Distributed File System). DFS makes it easier for connected users to find shared folders on the network without having to learn multiple IPs or DNS names. For more information, see Microsoft's DFS documentation. Although the Acronis Files Connect client does not support DFS, Acronis Files Connect has the ability to make DFS volumes available to Mac users.

## Creating a Cluster Group in old versions of Windows

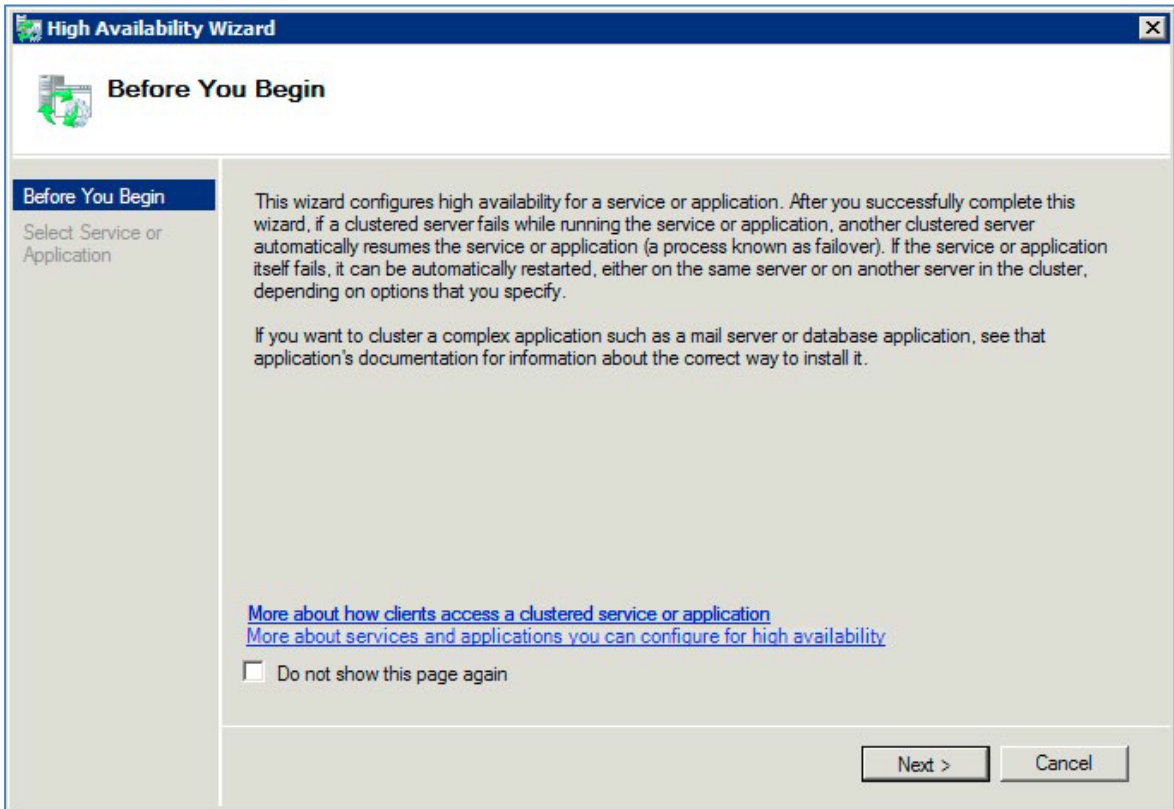
This is the recommended method for creating a new cluster group that includes a Acronis Files Connect service. If you already have a cluster group configured and would like to add Acronis Files Connect to it, right click the cluster group and select **Add Resource - Generic Service**. Then follow the steps below to select the desired Acronis Files Connect service. This will bypass the cluster group network and storage configuration steps.

### **To create a cluster group, do the following:**

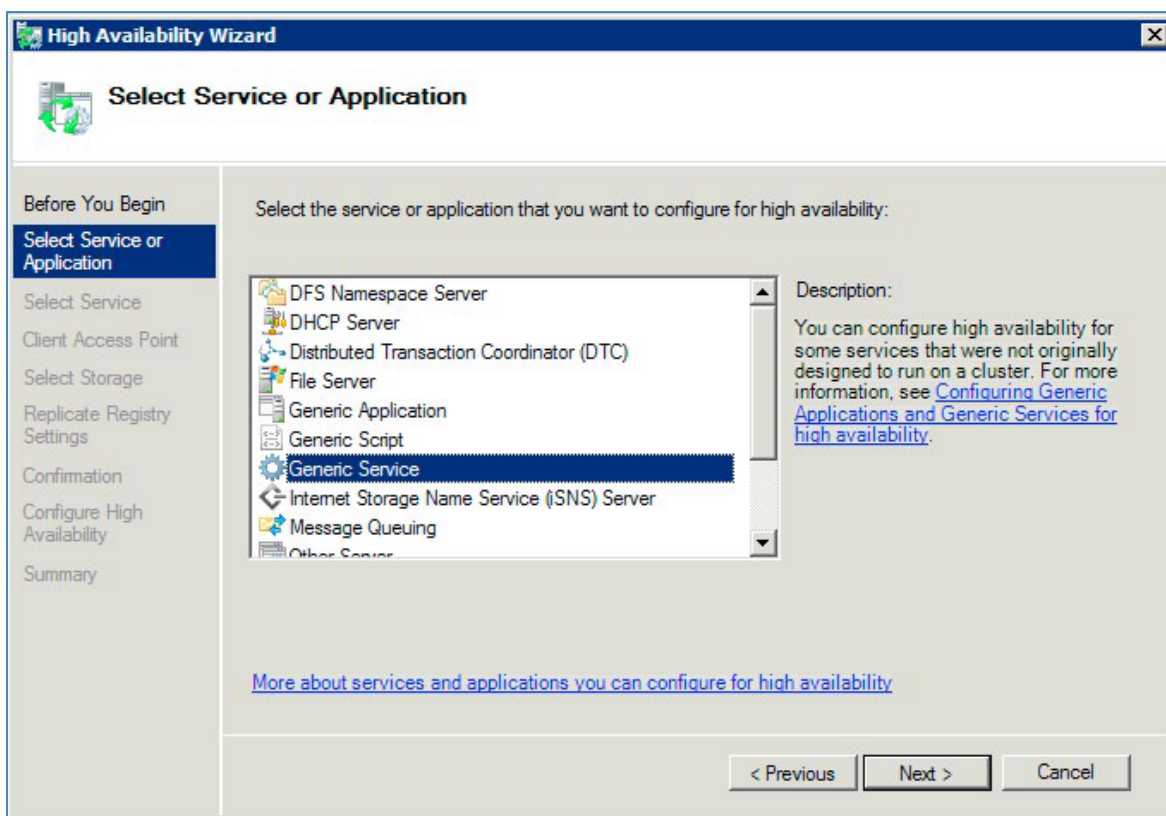
1. Open **Failover Cluster Management** in **Administrative Tools** and select your cluster on the left pane.



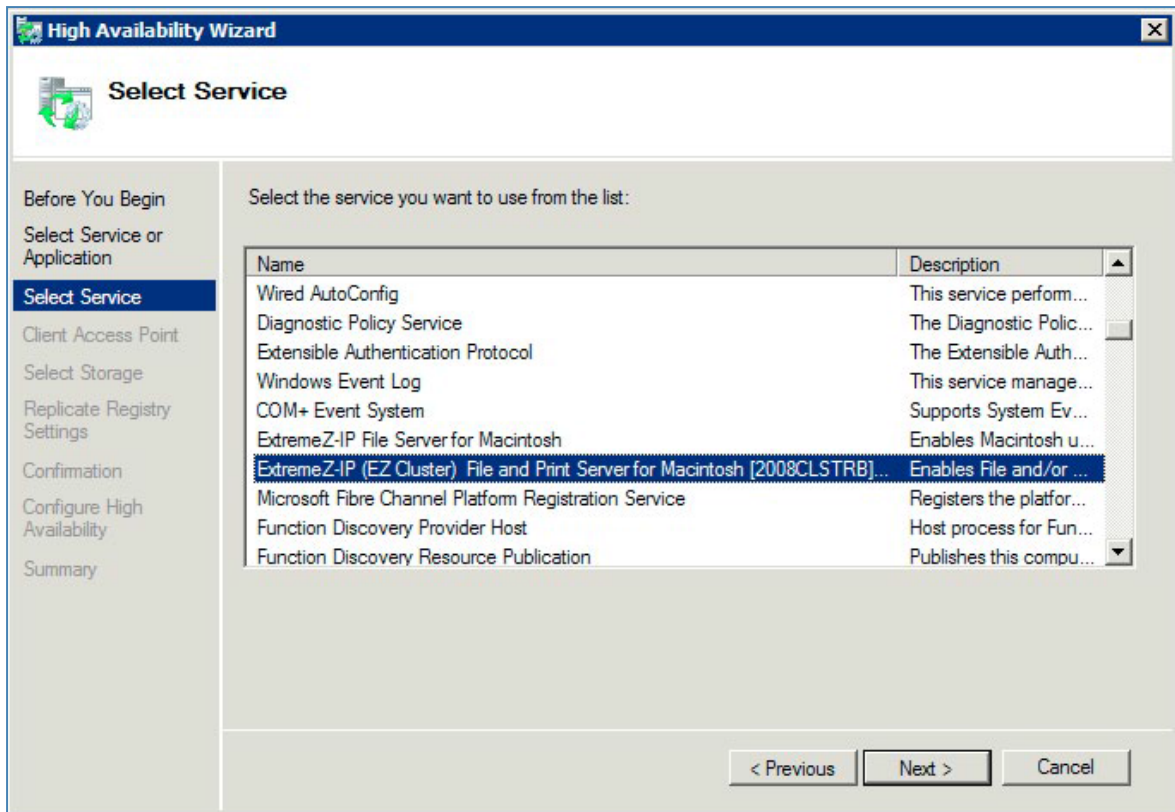
- Right click on the cluster name and select Configure a Service or Application. This will launch the High Availability Wizard. Click **Next**.



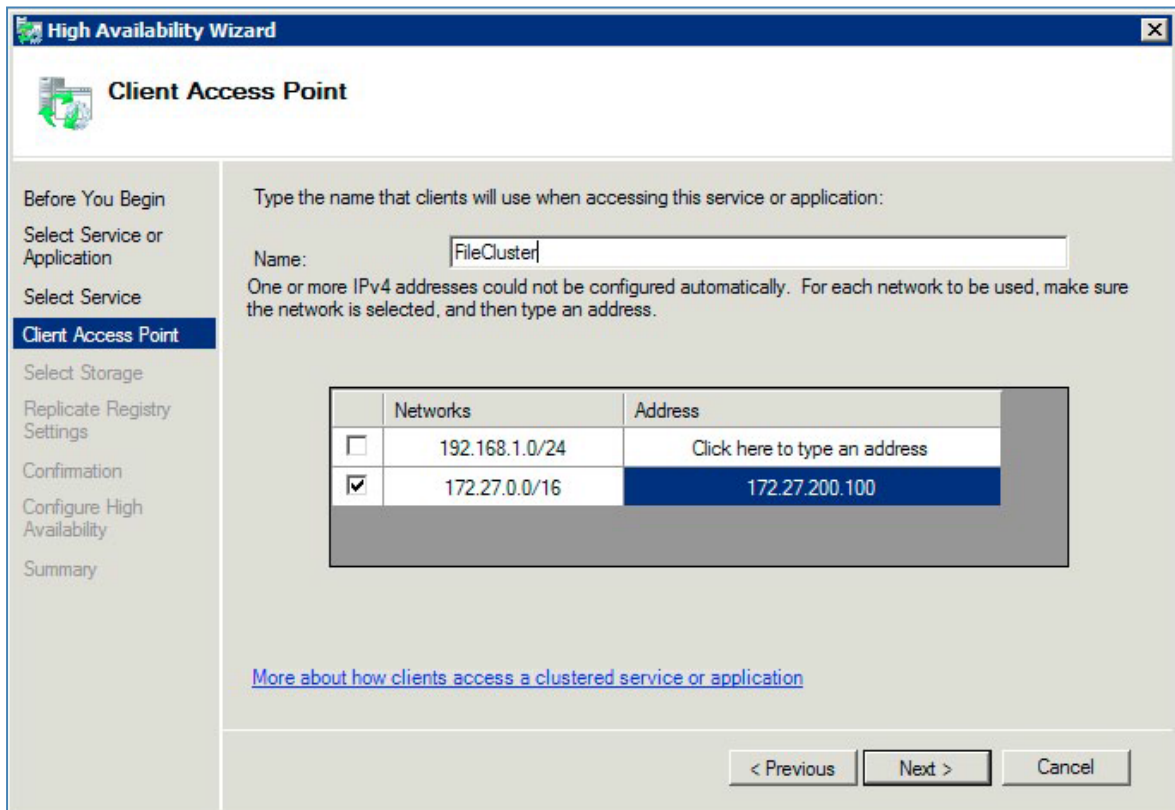
3. Select **Generic Service** and click **Next**.



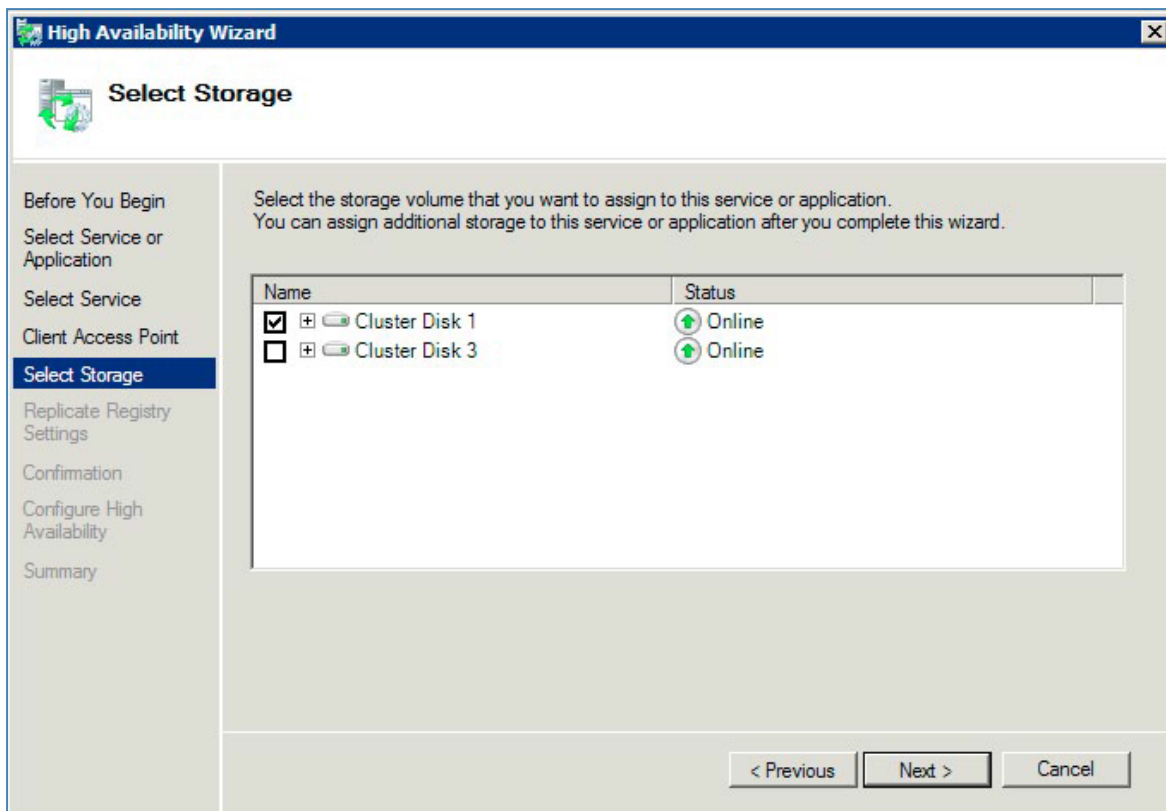
4. You must now select the service to add. You may see multiple entries for Acronis Files Connect in the list. Each entry will display the Acronis Files Connect service name as defined when the service was created. See the clustering section for more information. Select the entry that includes the specific Acronis Files Connect service name you would like to configure and click Next.



5. Enter the network service name for your cluster group. This will define the DNS name that clients will use to connect to this cluster group. Select the Networks that this cluster group will use and define an IP address for the cluster group on each selected network.



6. Select the volume(s) you would like to make available to this cluster group and click Next. These should be the volumes that contain the directories to be shared with Acronis Files Connect.



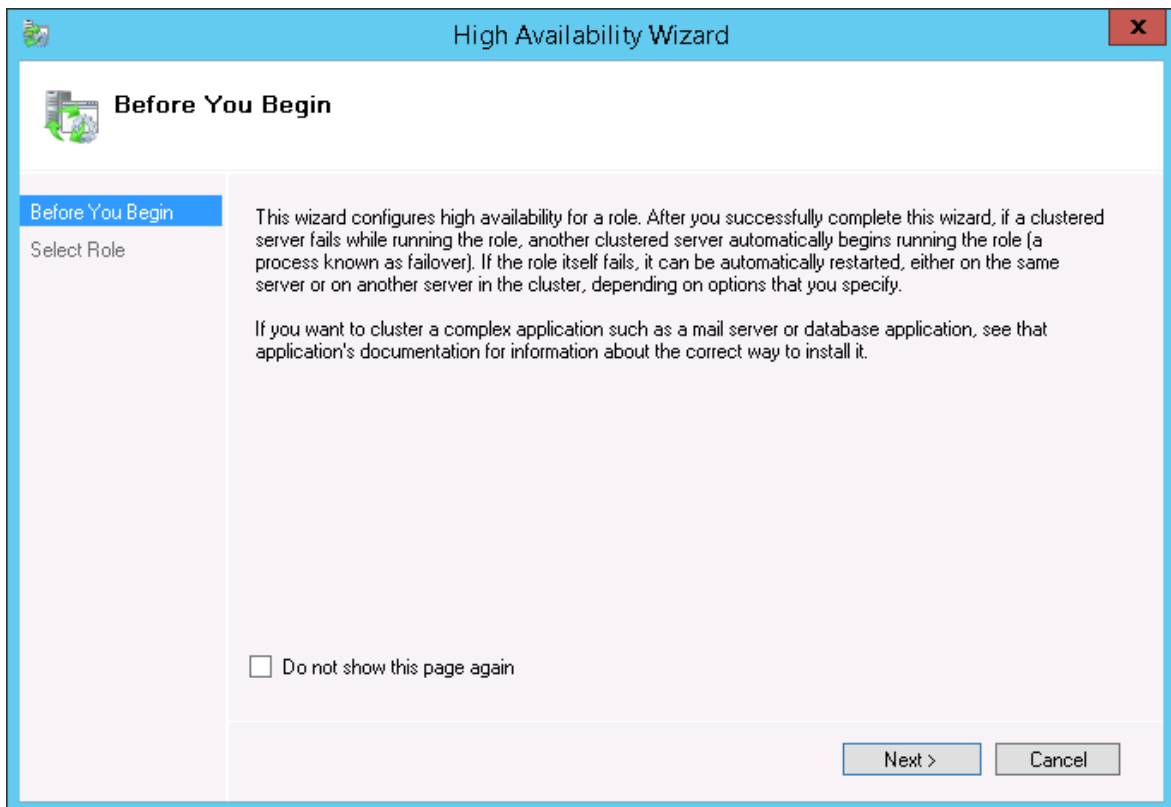
7. Click **Next** on the **Replicate Registry Settings** step. No changes are necessary.
8. Click **Next** on the **Confirmation** step.

## Creating a Cluster Group by adding a Windows Role

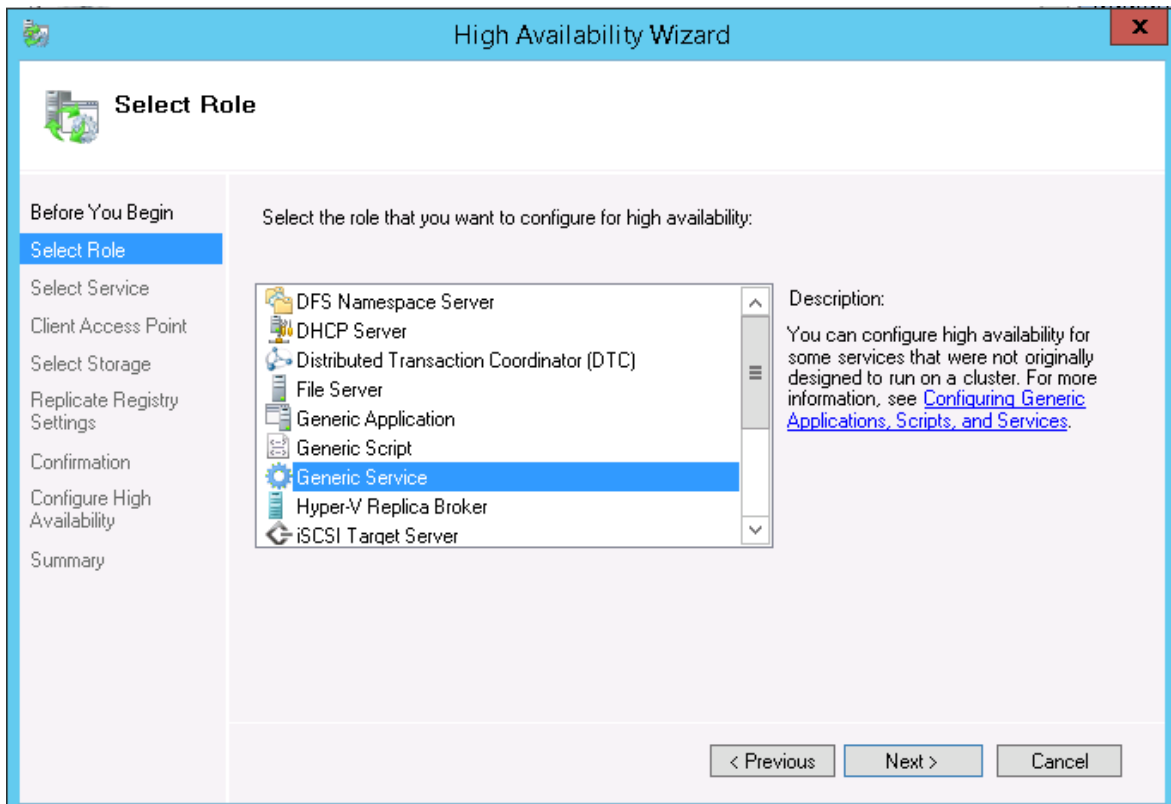
This is the recommended method for creating a new cluster group that includes an Acronis Files Connect service. If you already have a role configured and would like to add Acronis Files Connect to that role, right click on the role and select **Add Resource -> Generic Service**. Then follow the steps below to select the desired Acronis Files Connect service. This will bypass the role network and storage configuration steps.

### To create a role, do the following:

1. Open **Failover Cluster Management** in **Administrative Tools** and select your cluster on the left pane.
2. Right click on **Roles** and select **Configure a Role**. This will launch the High Availability Wizard. Click **Next**.

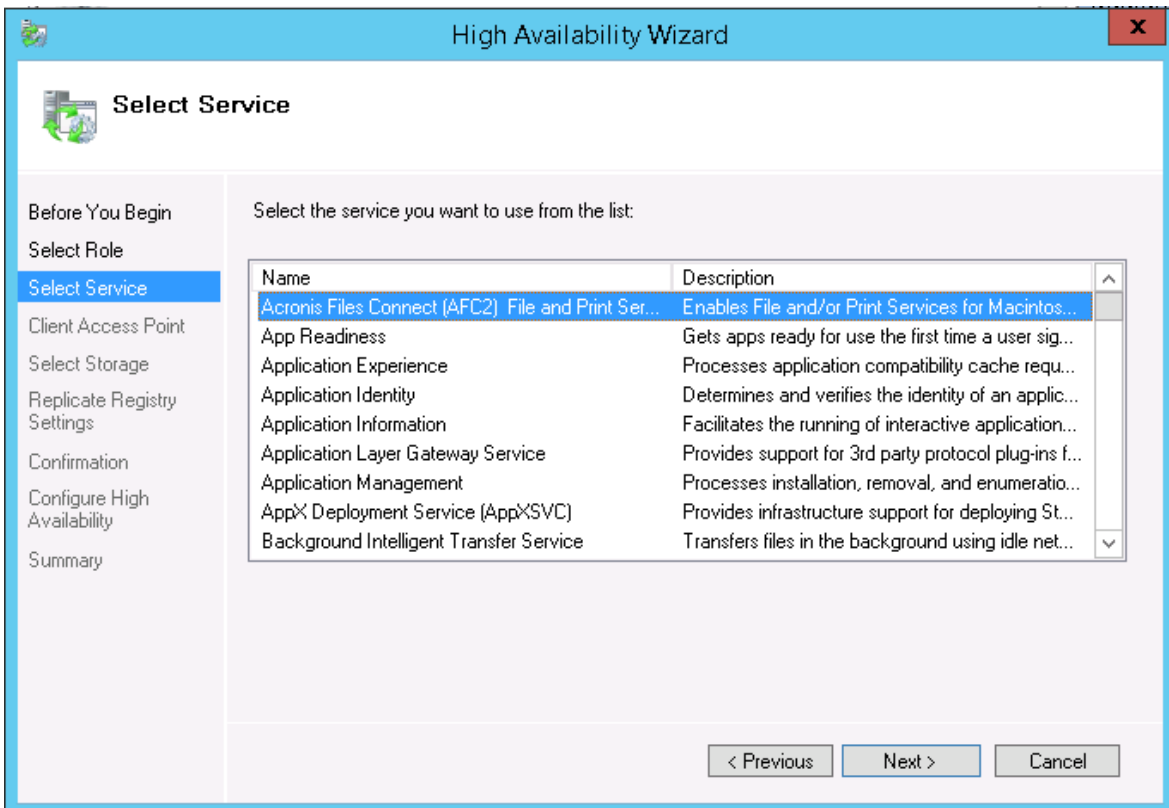


3. Select **Generic Service** and click **Next**.

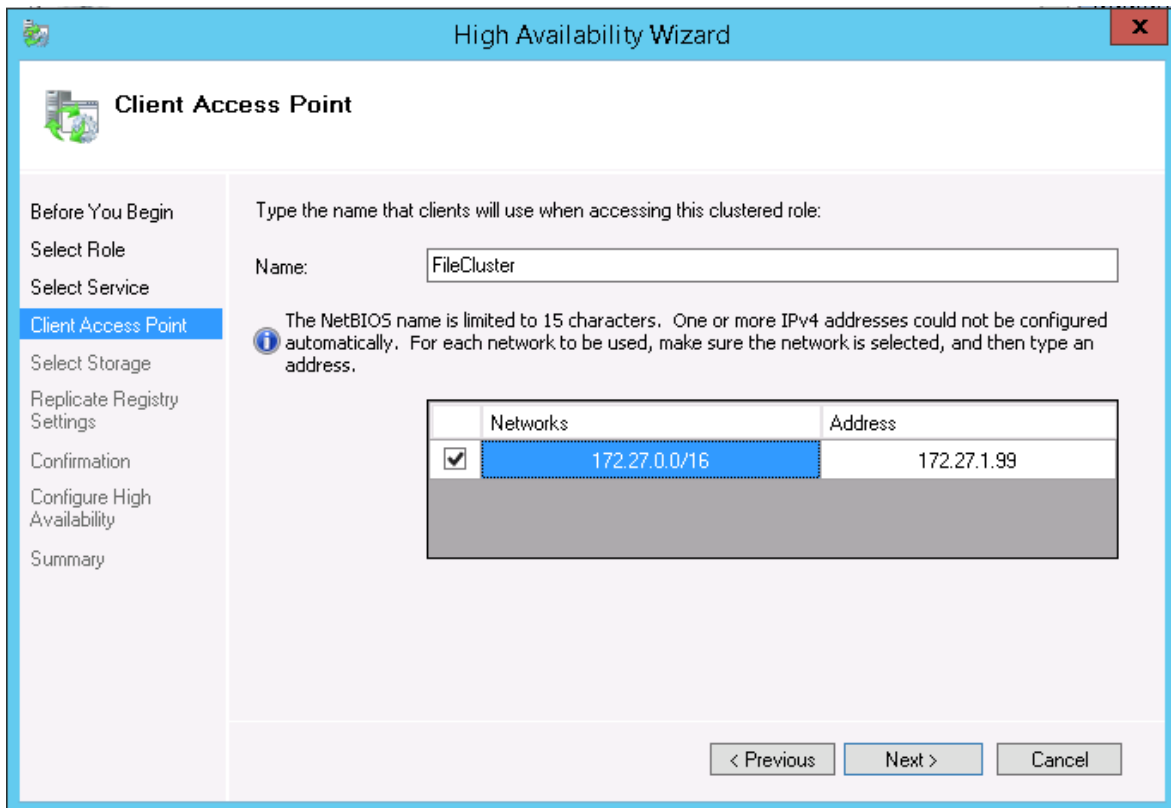


4. You must now select the service to add. You may see multiple entries for Acronis Files Connect in the list. Each entry will display the Acronis Files Connect service name as defined when the

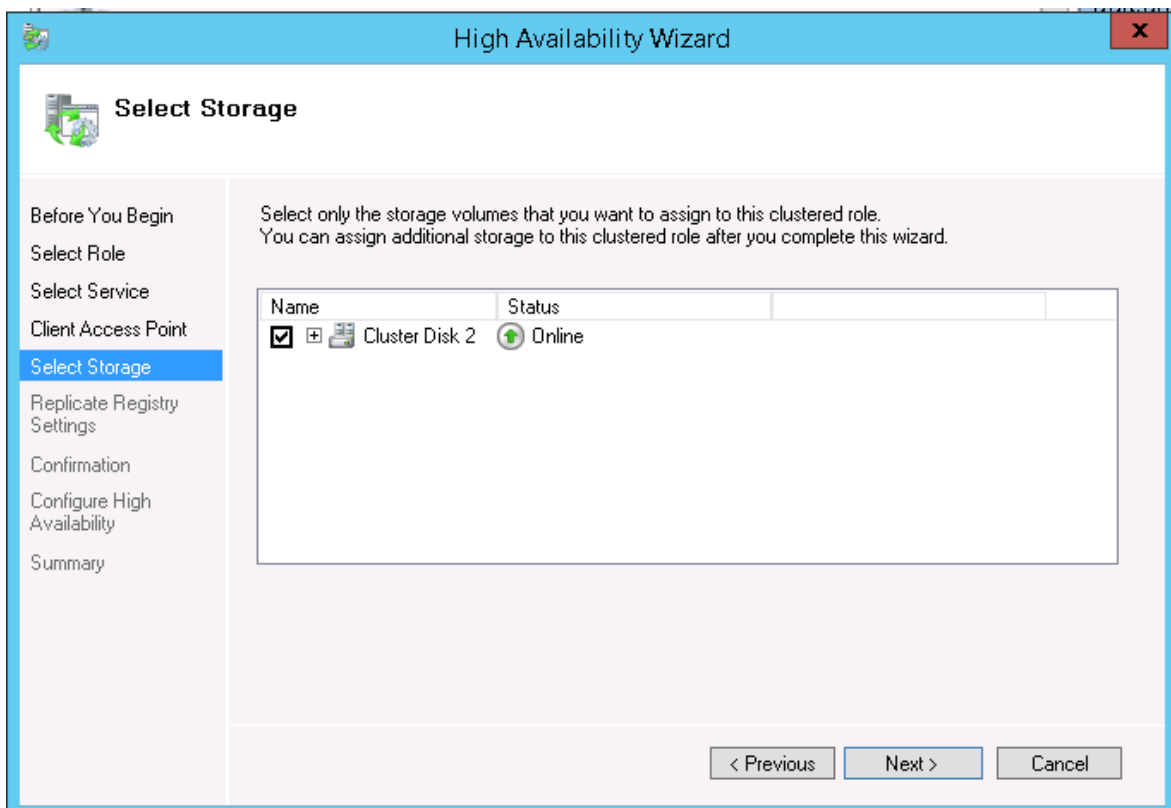
service was created. See the clustering section for more information. Select the entry that includes the specific Acronis Files Connect service name you would like to configure and click Next.



5. Enter the network service name for your cluster group. This will define the DNS name that clients will use to connect to this cluster group. Select the Networks that this cluster group will use and define an IP address for the cluster group on each selected network.



6. Select the volume(s) you would like to make available to this cluster group and click Next. These should be the volumes that contain the directories to be shared with Acronis Files Connect.



7. Click **Next** on the **Replicate Registry Settings** step. No changes are necessary.

8. Click **Next** on the **Confirmation** step.

## Setting Cluster resource dependencies

To ensure that cluster services start-up in correct order, you must set resource dependencies for the **IP Address**, **Network Name**, and the **Physical Disk**.

**To set resource dependencies for the IP Address, Network Name, and the Cluster Disk, do the following:**

1. From **Failover Cluster Management**, under the **Resources** tab for the role, right click on the **Acronis Files Connect File and Print Server** resource.
2. Click **Properties**.
3. Select the **Dependencies** tab.
4. Add the **IP Address**, **Network Name**, and the **Cluster Disk** as dependencies.
5. Click **OK**.

---

### Note

Since the Acronis Files Connect resource is created under the High Availability Wizard, all the nodes in the cluster are owners for the resource. If you do not want this configuration, you can change it before you bring the service online. To change the owners for the resource, click the **Advanced Policies** tab and modify the **Possible Owners** accordingly.

---

## Bringing the new service online

At completion of this configuration, the Acronis Files Connect resource may be offline. You can now bring the new resource online.

**To bring the Acronis Files Connect resource online, do the following:**

1. Right click the **Acronis Files Connect File and Print Server** resource.
2. Select **Bring online**.

# Upgrading Acronis Files Connect

Upgrading to a new version of Acronis Files Connect is an easy and straightforward process. The Acronis Files Connect installer automatically detects the existing version and upgrades it to the newer one – you do not have to uninstall the previous version in order to install the new one.

---

## Note

You may receive an inadvertent error message indicating that the service could not be stopped or that a file could not be removed. If you receive these errors, the best strategy is to manually stop the Acronis Files Connect service first, then re-run the installer.

---

**Review the [Backup and Recovery guidelines](#) and perform a backup of your deployment before proceeding.**

## Upgrading to a new version of Acronis Files Connect

---

### Note

In-place upgrades of operating systems are not supported. Please contact [Acronis Mobility Technical Support](#) if you have any questions.

---

### Note

Upgrades from ExtremeZ-IP to Acronis Files Connect require no special configurations. Start the Acronis Files Connect installer and proceed with the steps below.

1. Start the Acronis Files Connect installer.
2. Press **Next**.
3. Accept the license agreement and press **Next**.
4. Press **Install**.
5. When the installation procedure completes, press **Finish**.

---

### Note

If you are using Acronis Content Indexing, when dtSearch is updated in a release, you should rebuild the search indexes to get the full benefit. See more details in the Acronis Files Connect [Release notes](#).

## Upgrading to a new version of Acronis Files Connect on a Microsoft Failover Cluster

Upgrading Acronis Files Connect on a cluster requires that you upgrade your inactive nodes one by one, and finally failing-over the rest, so they can be upgraded as well.

1. Verify your clustered configuration has no issues. This is done by right-click on your cluster in Microsoft Failover Cluster Manager and selecting **Validate Cluster**. Follow the wizard until

everything is verified and there are no errors. If errors are found, they must be fixed before proceeding with the upgrade.

2. Select one of your inactive clustered instances.
3. Start the Acronis Files Connect installer.
4. Press **Next**.
5. Accept the license agreement and press **Next**.
6. Press **Install**.
7. When the installation procedure completes, press **Finish**.
8. Repeat the above procedures until all **inactive** instances are upgraded.
9. Failover the **active** instance(s) to any of the upgraded instances. Once the active instance has become inactive, upgrade it as described above.
10. Confirm that Acronis Files Connect works correctly.

---

**Note**

For upgrades, the Acronis Files Connect installer stops the Acronis Files Connect Service to perform the install. However, in some cases the installation fails because the Acronis Files Connect Service cannot be stopped. These cases include possible service errors, conflicts with other running processes, or installing while the Services Control Panel is open. If you experience installation failures, you can stop the Service manually from the Services Control Panel and proceed with the install.

---

# Configuring Acronis Files Connect

## Acronis Files Connect File server

### Starting and stopping the Acronis Files Connect File Server

To start the Acronis Files Connect File Server, log into Windows with Administrator privileges and launch the Acronis Files Connect Administrator. If you have not already started the Acronis Files Connect service, the Acronis Files Connect Administrator asks if you want to start the service. In addition, you can start and stop the service from the Service Control Panel on a standalone server or the Cluster Administrator on a cluster server.

### Configuring the Acronis Files Connect server

This section gives an overview of configuring the Acronis Files Connect service. Use the Acronis Files Connect Administrator to view, disconnect, and send messages to connected users, create shared volumes, and adjust specific machine settings. You can configure the local computer or remote computers on which Acronis Files Connect is installed as long as you have Administrative privileges.

To configure Acronis Files Connect on the computer you are using, from the Windows **Start menu**, go to **Programs/Acronis Files Connect** and select **Acronis Files Connect Administrator**.

---

#### Note

You can also configure Acronis Files Connect at the command line using the EZIPUTIL.EXE. For more information, refer to [EZIPUTIL command line tool](#).

---

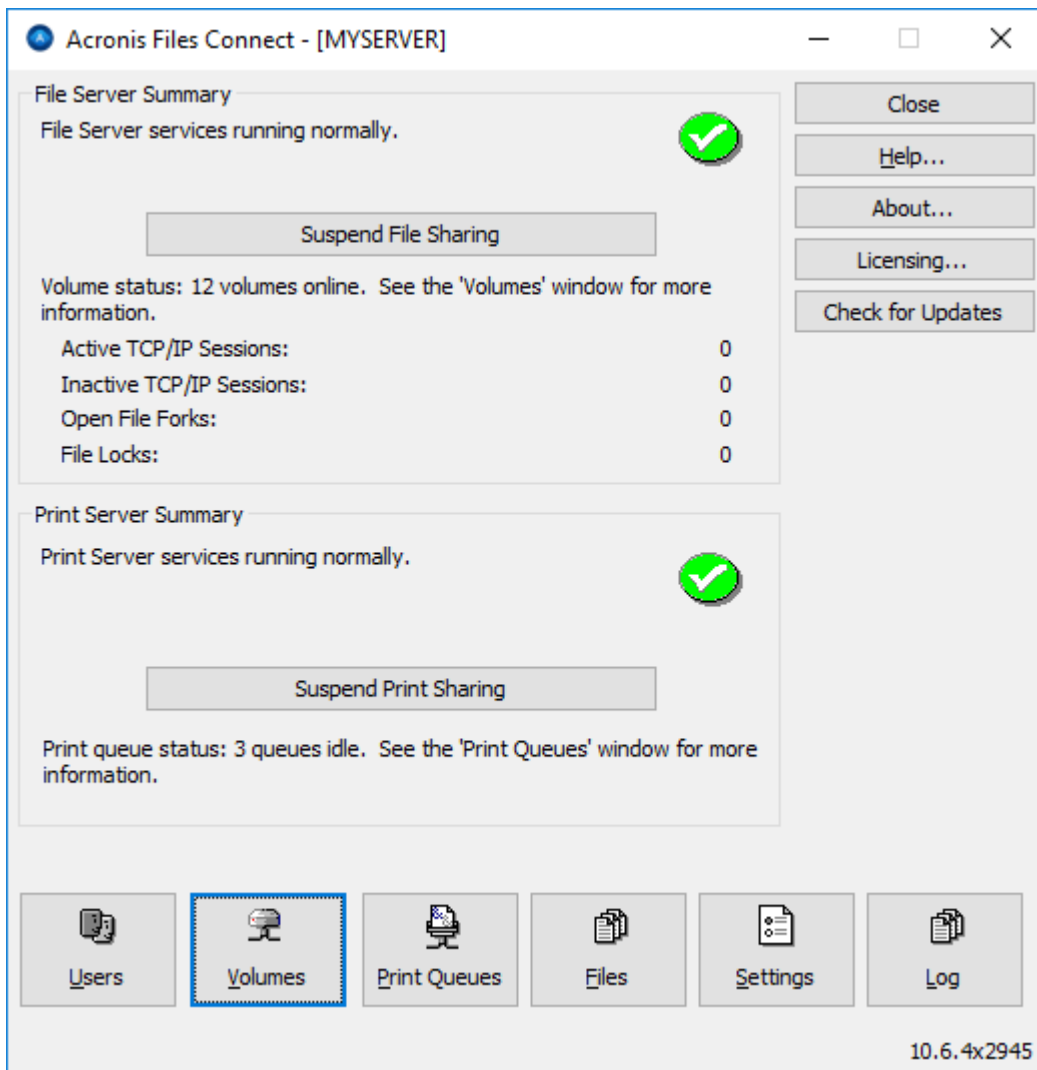
### Setting up Acronis Files Connect

Before using Acronis Files Connect, review the default settings; you can make changes at this time or later.

The **Settings** dialog box has the following tabs: **File Server**, **Print Server**, **Security**, **Search**, **Filename Policy**, **Service Discovery**, **DFS**, **Logging** and **Mobile Access**.

#### To change settings, do the following:

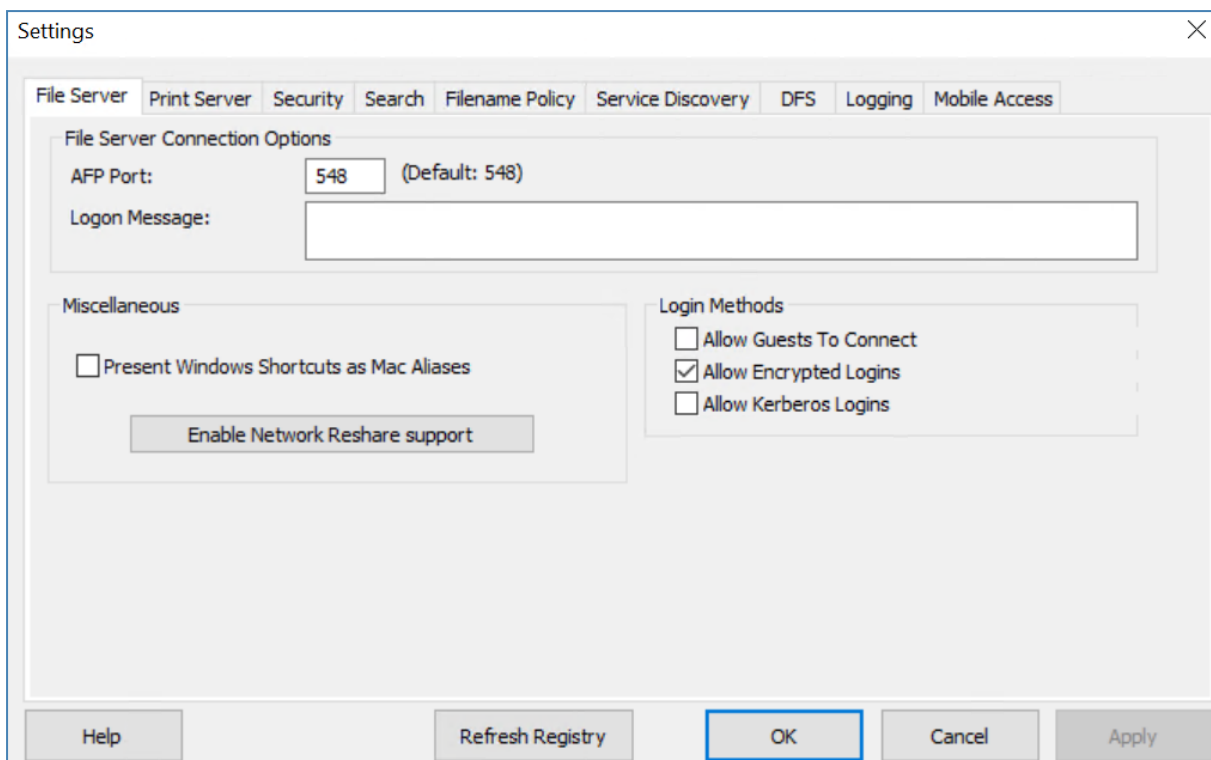
1. Access the **Acronis Files Connect Administrator** window.
2. Click **Settings**.
3. Choose the settings appropriate for your use, then click **OK** to return to the **Acronis Files Connect Administrator** window.



- **Suspend File Sharing** – Start/Suspend File Sharing Services.
- **Log** – View a log of Acronis Files Connect's activity.
- **Users** – View the users who are connected; disconnect users; send messages.
- **Volumes** – Set up volumes you want to share.
- **Files** – View files opened by Mac users. Displays the active TCP/IP sessions, open file forks and file locks.
- **Licensing** – Add serial numbers.
- **Check for Updates** – Check our web site for updates.

## Setting File server options

Use the **File Server Settings** tab to change the way Acronis Files Connect interacts with Mac users when it offers file sharing services.



## AFP Port

If required for your connection, make changes to the **AFP port**. Although rarely necessary, you can type a new port number for the TCP/IP port the file server uses; the default is 548.

---

### Note

If Mac machines cannot connect to your server, Acronis Files Connect may be running on a port other than the default. In this case, Acronis Files Connect displays a message on the Acronis Files Connect Administrator window warning you that you have picked a non-default port.

---

## Logon messages

The logon message is shown on the Mac users' computers after they successfully log in. Leave the message blank if you do not want clients to receive a message when they log in. To increase the maximum number of characters in this message, use the registry key **LoginMsgW**. For more information on this key, refer to [General Parameter Registry Keys – Refreshable](#). You can use as many as 500 characters.

---

### Note

OS X 10.9 or later does not support sending messages.

---

## Present Windows shortcuts as Mac aliases

This allows Acronis Files Connect to represent Windows shortcuts (.lnk files stored on AFP shares) as symbolic links (similar to Mac aliases), so that Mac users could use them.

### Prerequisites for this feature:

- The Mac users must have access to the Acronis Files Connect's AFP share containing the target.
- The shortcut file's extension must be .lnk
- Both the link and the target must be within the same Acronis Files Connect AFP volume.

---

**Note**

Shortcuts whose targets are not within a volume shared by Acronis Files Connect will not resolve. A WARNING entry will be written to the log.

---

**Note**

Large amount of unresolvable shortcuts within a volume can lead to performance issues.

---

## Enable Network Reshare support

Network Reshare allows Acronis Files Connect AFP file volumes to give access to folders located on other servers and NAS devices on your network. Mac machines continue to connect to Acronis Files Connect using the standard AFP file sharing protocol, while Acronis Files Connect utilizes the SMB/CIFS file sharing protocol to access files that are requested by Mac users from remote servers and NAS systems. By doing so, Mac users retain all the benefits of AFP file sharing while gaining access to resources that have traditionally only been available through SMB/Windows file sharing. For more information on Network Reshares, see this section: [Configuring Network Reshare support](#).

## Allow guests to connect

If you choose to allow guests to connect, a Mac user can log into the file server without supplying a name and password. Permission to connect does not give Macintosh machines access to your entire computer. You designate which volumes on your computer you want to share with Mac users. See [Creating a Volume](#). The user's privileges during that session are limited to the permissions normally given to the **Everyone** group under Windows.

---

**Note**

You must configure Windows so that guests can access the server. Find more information at [Acronis Files Connect: enabling guest access in Windows](#).

---

## Allow encrypted logins

If you select this option, Mac users can encrypt their passwords before sending them across the network. With encryption, users have greater security and can use longer passwords.

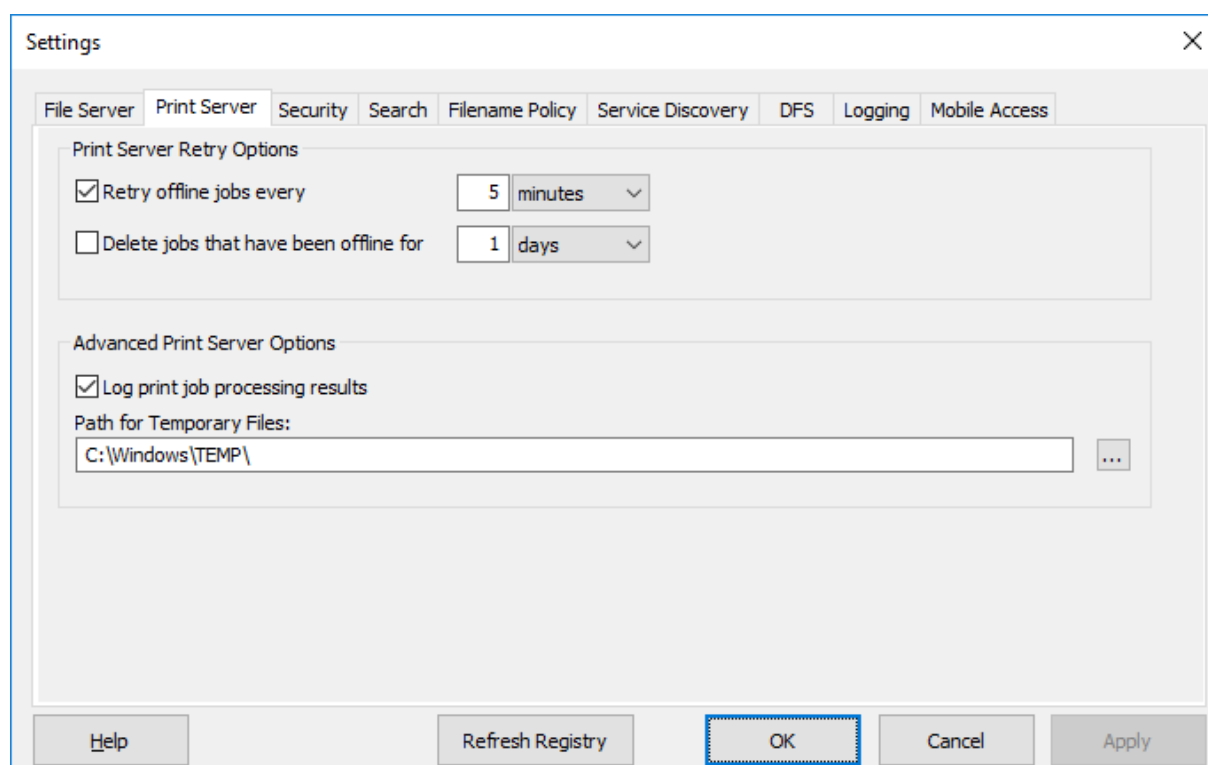
## Allow Kerberos logins

This option provides support for "single sign-on" to network resources. For more information, refer to [Using Kerberos](#).

## Setting Print server options

To make changes to Print Server Settings, click **Settings** on the Acronis Files Connect **Administrator** window, then click the **Print Server** tab. Changes you make to print server settings take effect

immediately after you click the **Apply** or **OK** button.



- **Retry offline jobs every** – Change wait time for retrying jobs.
- **Delete jobs that have been offline for** – Delete offline jobs.
- **Log print job processing results** – Control whether or not the server logs print job processing results.

### Automatic retry of print jobs

When a job fails for any reason - LPR error code, TCP connection terminated, error from Windows print queue - the job status is set to Offline and it is sent to the end of the queue. Use the **Print Server** tab to configure the interval that will elapse before the server retries printing the job.

By default, Acronis Files Connect automatically retries offline jobs every five minutes until the job prints successfully. To disable this feature, uncheck the **Retry offline jobs every . . .** box. You can enter only one auto-retry interval, which applies to all offline jobs.

### Deleting offline jobs

Acronis Files Connect can also automatically delete jobs that have been offline for a specified period of time. This functionality is disabled by default, and, when enabled, the default setting is one day. To enable this feature, check the **Delete jobs that have been offline for . . .** box.

## Note

In order to make sure that jobs aren't automatically deleted because of a queue-wide problem, such as a network problem, or printer turned off, Acronis Files Connect will not automatically delete a job after the configured period of time unless at least two other jobs have been successfully printed since the job went offline.

For the purposes of our performance counters, any queue that has more than one offline job and has not successfully processed a job since the last job went offline is considered an offline queue. So a single offline job does not make a queue offline—it could just be a bad job, but having multiple offline jobs without any recent successful jobs would suggest that a queue-wide problem exists. A queue that is offline does not differ from an online queue in terms of its processing; how it is reported in performance counters is the only difference.

## Advanced Print server options

If you want each print job to be logged in the Windows Event Log, check the Log print job processing results box. You can enter a location for storing temporary files; as a default, Acronis Files Connect uses the default temporary directory.

## Setting Security options

On the **Security Settings** tab, select the appropriate check box to change permissions and other options. Enter information for **Directory Services** in the appropriate text boxes.

The screenshot shows the 'Settings' dialog box with the 'Security' tab selected. The dialog has several tabs: File Server, Print Server, Security, Search, Filename Policy, Service Discovery, DFS, Logging, and Mobile Access. The 'Security' tab is active and contains two main sections: 'Permissions' and 'Directory Services'.  
**Permissions:**  
-  Allow Mac clients to change permissions  
-  Reset permissions on move (global)  
-  Support UNIX permissions and ACLs  
-  Support ACLs on all volumes (global)  
- Show only accessible:  
-  Folders  Files  
**Other Options:**  
-  Allow remote administration of server  
-  Allow workstations to save password (OS 9 only)  
-  Notify Mac clients of password expiration in 14 days  
-  Enable IPv6  
**Directory Services:**  
- Required to verify Active Directory domain account credentials when enabling the 'Support UNIX permissions and ACLs' option or 'DFS'.  
- Use  Global Catalog  SSL  
- Account: [text box]  
- Password: [text box]  
- Domain: [text box]  
- Additional directory search criteria: [text box]  
- Validate Account button  
At the bottom of the dialog are buttons for Help, Refresh Registry, OK (highlighted with a red dashed border), Cancel, and Apply.

## Allow Mac users to change permissions

If you select this option, Mac users will be able to change file and folder permissions. With this option disabled, they will be prevented from changing permissions the Windows Administrator has set on the server. Many Mac applications set unexpected permissions without user intervention. For increased reliability, it is recommended that Mac users are not allowed to modify permissions unless this capability is required for a particular workflow.

## Reset permissions on move

If you would like files and folders to always inherit permissions from their parent folder after they have been moved, select this check box.

---

### Note

If the directory that is moved contains a large number of sub-folders, resetting the permissions can take awhile.

---

## Support UNIX permissions and ACLs

---

### Note

Since this feature is not required for ordinary workflows other than DFS support and can create issues with routine file operations if not properly configured, make sure to clarify with [Acronis Technical Support](#) if your workflow needs this before enabling.

---

UNIX permissions and Access Control Lists (ACLs) require the Acronis Files Connect service to have access to the list of users in Active Directory in order to resolve SID, UUID, UID, and name mappings. For UNIX permissions, the Acronis Files Connect Mac client app requests a name mapping for UID. However, for the 'ls' command the Mac uses AD and does the name mapping internally. Therefore, the Mac machine does not make a name request to Acronis Files Connect. If the UID Acronis Files Connect provides does not match the user's UID obtained from Active Directory, then the Mac will not allow the user to change UNIX permissions at all. In addition, the client will not be able to determine the user's group membership or whether the user is the owner.

To verify your account, enter the requested information in the **Directory Services** text fields. This account will be used to search Active Directory to resolve account IDs. By default, Acronis Files Connect will search within your entire Active Directory forest to validate security credentials. If you would like Acronis Files Connect to only search the **Domain** specified, uncheck the **Use Global Catalog** option. Add additional search criteria, if necessary, and click **Validate Account**. If the credentials are invalid, the service will not be able to access Active Directory and UNIX permissions will be disabled. Acronis Files Connect DFS support requires this option to be enabled and valid Directory Service credentials to be entered.

## Support ACLs on all volumes (global)

To support ACLs on all volumes, check this box.

## Show only accessible: folders, files

If you check the Folders option, users will see only folders that they can access. If you check the **Files** option, users will only see files that they can access.

## Allow remote administration of server

This option lets Windows users, who have Administrative privileges, use the Remote Administration features of Acronis Files Connect to configure the server remotely; see [Administering Acronis Files Connect Remotely](#).

## Notify Mac users of password expiration

You can request from Active Directory users to change their sign-on password after a specified period of time. With this textbox, you can notify Mac users that their old passwords are about to expire and ask them to create new ones.

## Enable IPv6

If you would like to use IPv6, select the **Enable IPv6** check box. On some versions of Windows you will need to install IPv6 manually before services such as Acronis Files Connect will be able to use it.

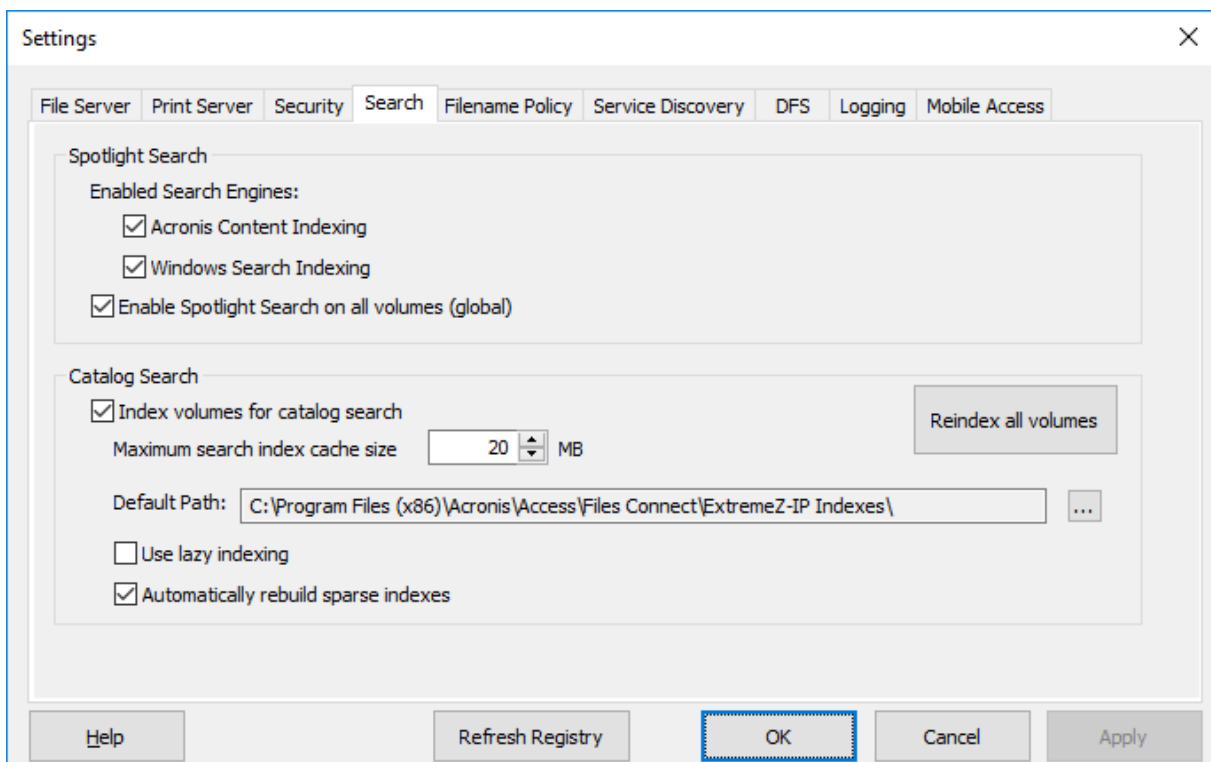
## Verify Directory services

UNIX permissions and ACLs require access to Active Directory in order to resolve SID, UUID, UID, and name mappings. For UNIX permissions, Finder requests a name mapping for UID. However, for ones, the Mac uses AD and does the name mapping internally. Therefore, the Mac does not make a name request to Acronis Files Connect. If the UID Acronis Files Connect provides does not match the user's UID obtained from Active Directory, then the software will not allow the user to change UNIX permissions at all. In addition, the client will not be able to determine the user's group membership or if the user is the owner.

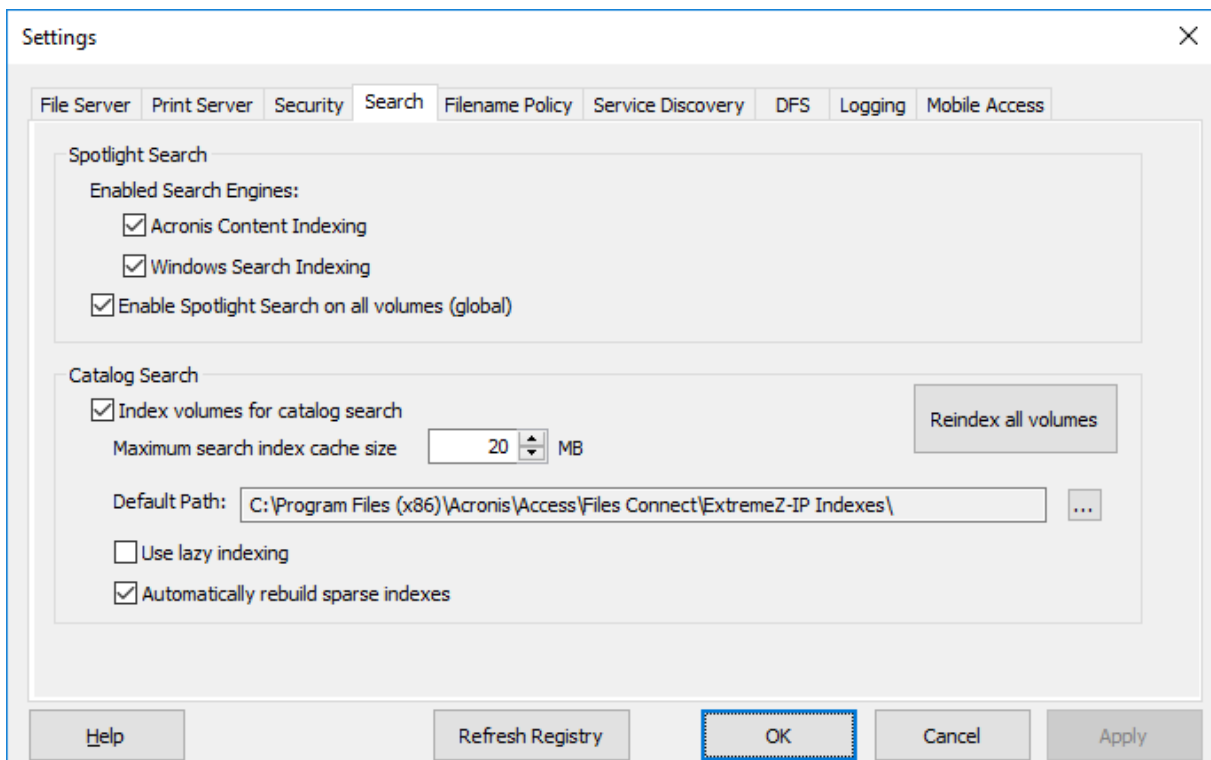
To verify your account, enter the requested information in the **Directory Services** text fields. Add additional search criteria, if necessary, and click **Validate Account**. The **SSL** option can be selected to enable secure SSL communication with Active Directory. If the account is not valid, you may not be able to access Active Directory and UNIX permissions support will not be enabled. In addition, DFS support will not function.

## Setting Search options

To set search options, check the appropriate boxes and enter the relevant information.



## Spotlight search



## Acronis Content Indexing

Acronis Content Indexing is the default and provides Network Spotlight support for reshare volumes on non-Windows machines (for example, Network-attached storages (NAS) and for StorNext

volumes. It also indexes more files than Windows Search and indexes more of the file, making it easier to search.

Selecting this check box will allow indexing using Acronis Content Indexing.

Acronis Content Indexing will skip the indexing of archive stub files, so you can now use this indexing on volumes that are being archived with an Hierarchical storage management (HSM) system.

As of Acronis Files Connect 10.5 the local shares and network reshares are continuously monitored for changes and the index is updated immediately.

---

### Note

You can enable or disable Spotlight searching on a per volume basis in the individual volume's **Volume Properties** dialog. For more information, please see [Volume Properties](#) article. You can enable this setting when you create a new volume, or later. Enabling it takes effect for all new sessions using the volume.

---

### Windows Search indexing

Windows Search comes built into every modern Windows operating systems (see below for exceptions). Using Windows Search ensures that the index is automatically kept up to date by updating the index for every change. The main disadvantages of Windows Search are that it does not support resharing volumes on non-Windows machines and that it has issues when working with more than a couple of million indexed files.

Selecting this check box will allow indexing using the built-in Windows Search. In addition to enabling this setting, Spotlight Search requires that the Microsoft Windows Search application is installed on the Acronis Files Connect server and is configured to index any volume where Spotlight Search is enabled.

***As of Acronis Files Connect 10.5, Windows Search supports searching by Windows or Mac file tags, but requires an add-on to be installed. To install it, do the following:***

1. Open Command Prompt as administrator, and navigate to the AppleTagAddOn folder, which you can find in the Acronis Files Connect installation folder.

For example, `cd C:\Program Files (x86)\Acronis\Access\Files Connect\AppleTagAddOn`

---

### Note

By default, AppleTagAddOn is located in `C:\Program Files (x86)\Acronis\Access\Files Connect`. Your path may be different if you upgraded from an older version or performed a custom install. To identify the path to the program executable folder, you can check the Acronis Files Connect entry in Windows Services.

---

2. At the Command Prompt, run the `regHandler.bat` file that is stored in the AppleTagAddOn folder.
3. Confirm that a dialog message says: "DllRegisterServer in AppleTagAddOn.dll succeeded."
4. It is recommended to restart the machine running Windows Search.
5. Rebuild the index for the desired volumes. To do so:

- In the Acronis Files Connect Administrator, select **Volumes**
- Right-click the desired volume and press the **Indexing option** button
- In the dialog box that opens, press **Reindex**

Alternatively, you can use the built-in Windows feature **Indexing Options**.

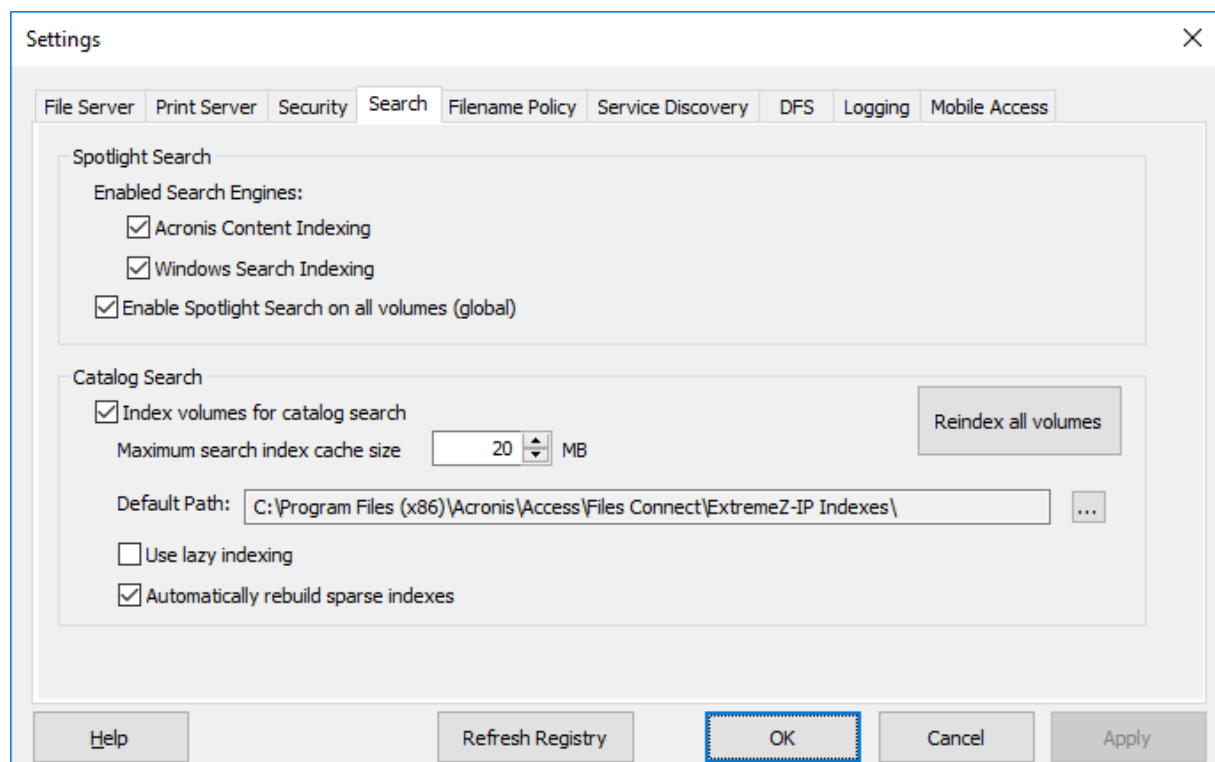
### Note

You can enable or disable Spotlight searching on a per volume basis in the individual volume's **Volume Properties** dialog. For more information, please see [Volume Properties](#) article. You can enable this setting when you create a new volume, or later. Enabling it takes effect for all new sessions using the volume.

### Enable Spotlight Search on all volumes (global)

To support [Spotlight Search](#) on all volumes, select this box. After it has been enabled, the Acronis Content Indexing process will begin immediately for all volumes except volumes already configured to use Windows Search.

### Catalog search



### Index volumes for catalog search

By default, indexed searching is enabled on all existing and newly created volumes. You can disable or enable indexed searching on a per volume basis in the individual volume's **Volume Properties** dialog in **Acronis Files Connect Administrator** see [View the Volumes Window](#). You can set this property at initial volume creation time or after the volume has been created. In order for changes

to this setting to take effect, you must stop and restart the Acronis Files Connect File Services for Macintosh service.

### Maximum search index cache size

This cache is set to a maximum size of 20 MB by default. We do not recommend changing this cache size. An index file containing 250,000 files is only about 8 MB in size. Leaving the cache limit at the default setting gives sufficient performance in almost all cases. If the index files on disk are larger than search index cache size, the file will be read from disk when the client does a search; however in many cases the file will be in the Windows file system cache so performance impact is minimal. When the server is running with limited physical memory, the cache size can be reduced to as little as 8 MB.

### Default path

By default on a standalone server, Acronis Files Connect stores index files in the Acronis Files Connect Indexes directory in the Acronis Files Connect application folder. If you would like to locate the index files in a different location, click **Browse** to select a new folder.

---

#### Note

If you modify the default path while Acronis Files Connect is running, all index files for volumes without individual custom paths are created in the new location.

---

Administrators can also specify custom index file paths for individual volumes; this setting overrides the global default path setting.

---

#### Note

In a clustered environment we recommend that you set the Default Path to be a location on the shared disk.

---

### Use lazy indexing

By default, indexed searching uses any available system resource to keep its indexes current and cooperates with other system processes. It should not affect overall system performance adversely. However, when a server is under high load or is running many different services simultaneously, you can limit the system resources that search indexing consumes by selecting the **Use lazy indexing** check box. This setting takes effect immediately.

### Automatically rebuild sparse index

In order to optimize runtime performance, the Acronis Files Connect index file entries for files that have been deleted or moved from a volume are not physically removed from the index file at the time the actual file is deleted. The indexed search service ignores these deleted entries to keep search results accurate. However, the index file grows over time and, as the file gets larger, slows search performance to a small extent. The rate at which the index file grows is dependent on the number of files being added, moved, and deleted on the file server. In order to keep Acronis Files Connect search performing at optimal levels, volumes' indexes are routinely re-indexed and

compacted. The interval at which this occurs is determined by the ratio of deleted (stale) records to valid entries in the index. By default, the Acronis Files Connect search service re-indexes an individual volume when approximately one-third of that volume's index file records are deleted, stale records.

Maintenance occurs on a per volume basis and only on volumes requiring re-indexing. While re-indexing, the volume's existing search index is kept up to date and used to provide one hundred percent accurate search results. Re-indexing should not have any detrimental effect on other server processes while it is running. While Acronis Files Connect is re-indexing an individual volume, a status of 'Reindexing' shows in the **Volumes** dialog of the Acronis Files Connect Administrator. If you prefer, you can schedule re-indexing on a set schedule during off-hours. You can use an EZIPUTIL command, described on the [Appendices](#) page used in a batch file or script and triggered by a scheduling service of your choice. If you choose this method of scheduled re-indexing, disable automatic re-indexing by clearing the **Automatic rebuild of sparse indexes** check box.

## Setting Filename policy

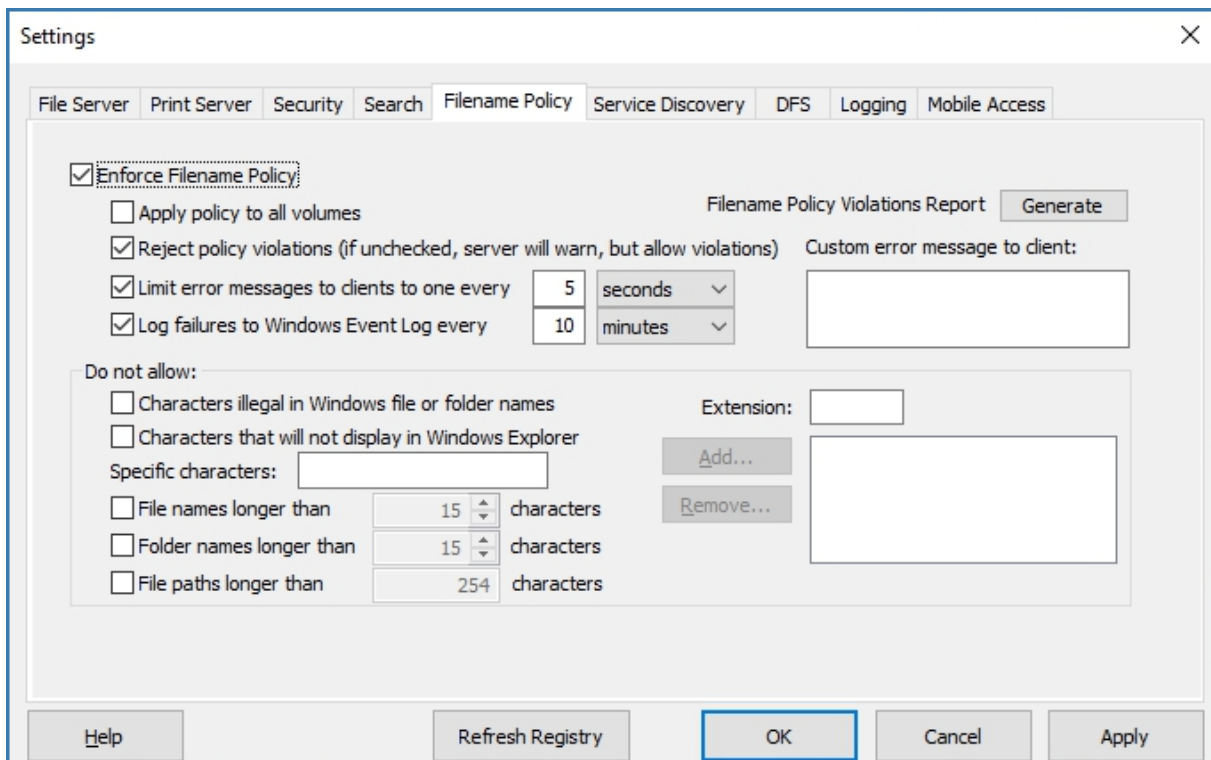
Since Acronis Files Connect provides seamless communication between Windows file servers and Mac users, you can configure policies on valid file names and file types.

Acronis Files Connect could detect and reject the Mac users' attempts to save (create, rename, move) files with characters that are "illegal" in Microsoft File Explorer or other applications that don't support the Unicode file system APIs.

You have to configure what is allowed or deemed "illegal". The list could include:

- Characters that cannot be displayed on Windows
- Trailing spaces
- Unicode characters not available in the default Windows font
- Any given character
- File names longer than "x" characters
- Specific file extensions

Filename Policies do not affect existing files on the server or files that are copied via Windows file sharing



## Enforce Filename Policy

Checking this setting will allow you to enforce filename policies set in Acronis Files Connect.

## Filename policy violations report

A report listing all existing files and folders that violate the presently configured filename policy can be created by clicking the **Generate** button. A confirmation dialog box will appear and allow you to access the folder containing the report's output. This folder will contain a Report Summary text file and individual, comma-separated summary files for each Acronis Files Connect volume on the server. These CSV files can be viewed in a spreadsheet application or a text editor.

From version 10.6.3 on, the Filename Policy Violations Report feature requires that the [Spotlight search feature](#) is enabled. No violations will be reported for volumes without enabled Spotlight search.

By default, the Filename Policy Violations Report displays up to 20,000 violations per volume. This could be modified by changing the setting in [MaxViolationsReported](#) Windows registry key.

## Apply policy to all volumes

You can enforce filename policies for all Acronis Files Connect AFP volumes or for individual ones. Selecting **Apply policy to all volumes** checkbox enables this feature across all Acronis Files Connect AFP volumes and overrides individual volume policy settings.

## Limit error messages to clients to one every

---

### Note

OS X 10.9 and later does not support displaying messages sent from the server.

---

Checking this setting limits the number of error messages to one for each client at the specified time interval. You can set the time interval.

## Log failures to Windows Event Log every

If you check this setting, the server will log errors to the Windows Application Event Log at the specified time interval.

## Custom error message to client

---

### Note

OS X 10.9 and later does not support displaying messages sent from the server.

---

You can specify a custom message that will be appended to the standard filename policy error messages. For example: "This action violates company policy regarding filenames." would lead to the following message being sent to the user: "File 'foo.mp3' cannot be created because the 'mp3' extension is not allowed. This action violates company policy regarding filenames."

## Do not allow

In this section, set characters, filenames, and extensions that your Mac users will not be able to save to your file server.

- **Characters illegal in Windows file or folder names** – If you check this setting, users cannot save files with names that include characters illegal in Windows. The characters are / ? < > \ : \* | and trailing spaces and trailing periods.
- **Characters Not Displayable in Windows Explorer** – If you check this setting, users cannot save files with names that include characters that cannot be displayed in the font used by Windows Explorer (the default is Tahoma).
- **Custom error message** – Custom message that will be added to the built-in description for each error.
- **Specific Characters** – You can specify additional characters that you do not want users to include in filenames. Type the characters in this field without separators.
- **File names over** – You can limit file names to a specified number of characters.
- **Folder names over** – You can limit folder names to a specified number of characters.
- **File Paths longer than** – You can limit the path length to a specified number of characters.

---

**Note**

The limit will be the entire Windows file path as it resides on the server. The file paths may appear shorter to the Mac users.

---

- **Extension** – You can restrict users from saving specific file extensions, such as mp3, mov and wav, by typing in the extension without the (.) dot precursor and clicking **Add**. To remove extensions from the list, highlight the extension and click **Remove**.

## Service discovery

Mac users can discover an Acronis Files Connect server via a number of different protocols, depending on the operating system that is being used and how the administrator configures the server.

The screenshot shows the 'Settings' dialog box with the 'Service Discovery' tab selected. The 'Server Name' field contains 'RLSWIN22 IP'. Under the 'File Print DFS' section, 'Bonjour' is unchecked and 'Web Service' is checked. The 'HTTP Port' is set to 8081 and the 'App/HTTPS Port' is set to 8085. The 'Certificate' field is set to 'Acronis Files Connect'. The 'Register with Primary Server' checkbox is unchecked, and the 'Location/Zone' field contains 'ExtremeZIPServerList'. The 'Description' field is empty. The 'Register Service Connection Point' checkbox is also unchecked. At the bottom, there are buttons for 'Help', 'Refresh Registry', 'OK', 'Cancel', and 'Apply'.

Select the network protocols you want the server to use to register with — Bonjour, HTTP — by selecting the appropriate checkboxes.

---

**Note**

The protocols available for discovering file, print, and DFS resources can be configured independently.

---

## Server name

The Server name appears in the login window whenever a Mac user connects to the server. This name also appears in the macOS **Connect to Server** dialog and on earlier Mac OS systems in the

**Chooser** and the **Network Browser** when Mac users browse the network. You may change the name; use uppercase and lowercase text.

## Bonjour

Acronis Files Connect is compatible with Apple Bonjour. For more information, refer to [Acronis Files Connect and Apple Bonjour](#).

## Web service

The Acronis Files Connect Mac client app uses the web service's address in order to function.

This client is the new app for Acronis Files Connect that makes it easy for users to connect to all the necessary resources and also has a powerful search engine.

## Port

Enter the port used for client-server communication between the server and the Acronis Files Connect Mac client app.

On Acronis Files Connect 10.5 and newer, you can also select a certificate to be used for the newly added HTTPS port.

---

### Note

Even if you turn off HTTP, Acronis Files Connect still uses this port to support the legacy Acronis Files Connect Print Components. Only the new features are disabled.

---

## Register with Primary Server

This setting should be enabled only on **Secondary** servers in order to register them with the Primary server.

By selecting the **Register with Primary server** checkbox, you are turning this server into a **Secondary** to the server whose address you enter. The Primary server will have its table of servers automatically populated for every Secondary server that is registered this way.

---

### Note

Your registration will be successful only if both the Primary and Secondary servers are part of the same Active Directory domain.

---

The Acronis Files Connect Mac client app supports connecting to a single Primary server to discover the other Acronis Files Connect servers on the network.

## Location

This field specifies the location of the server. The location is also the default location of print queues on the server, but you can assign a different location on a queue by queue basis. If you want to have a hierarchy of locations, such as 1100 N. Glebe RD, Arlington, Virginia, enter the locations separated by colons ('Virginia:Arlington:1100 N. Glebe RD').

## Description

The optional description for the server.

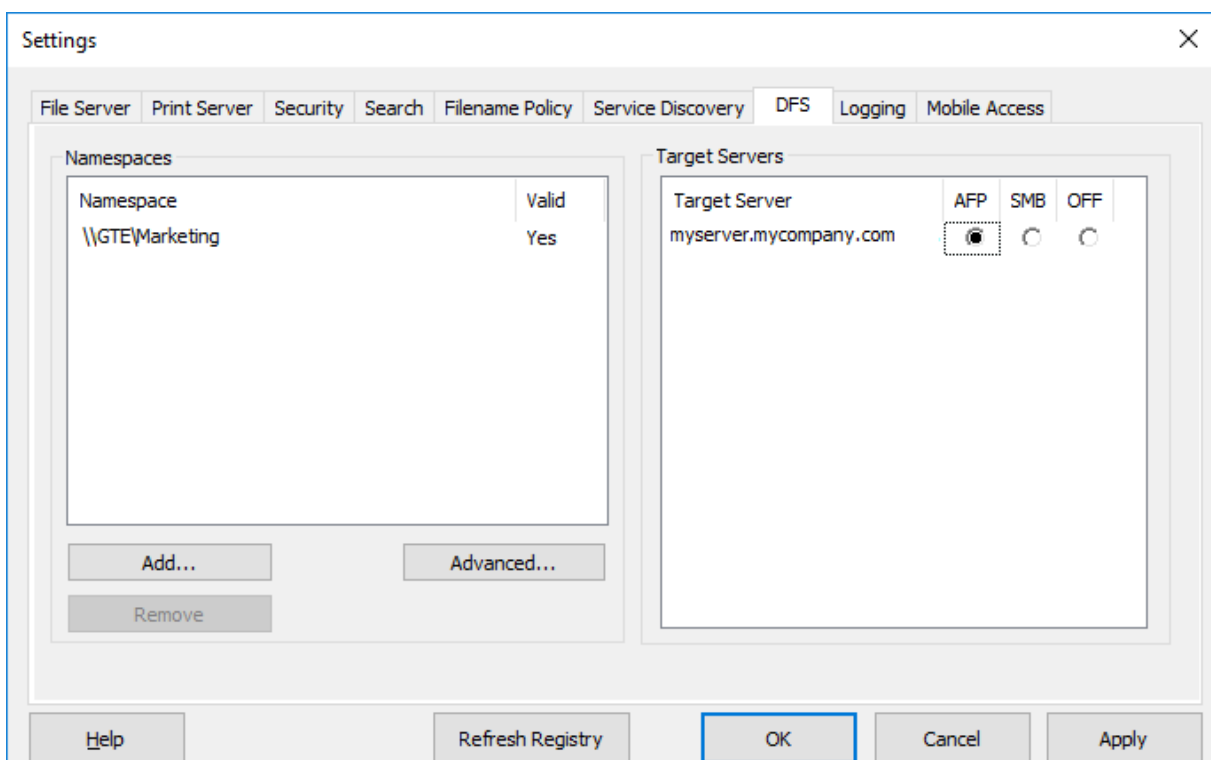
## Register Service Connection Point

This option allows Acronis Files Connect to publish its existence using a Microsoft Service Connection Point (SCP). This technology is used to locate and contact other Acronis Files Connect servers in your Active Directory.

## DFS

Acronis Files Connect can be configured to make a Microsoft Distributed File System (DFS) available to Mac users. In addition to the server-side configuration, you will need to install and configure the Acronis Files Connect [Mac client app](#).

DFS support also requires two settings on the **Security** tab of the **Settings** dialog. Valid **Directory Services** credentials must be entered and **Support UNIX Permissions and ACLs** must be enabled for DFS to function.



## Namespaces

### Note

You can add a namespace only if this namespace is visible on the server on which Acronis Files Connect is installed. This server must have **DFS Namespaces** role enabled.

To add a namespace, click the **Add** button. You will be prompted to enter the path of your DFS namespace. Acronis Files Connect will attempt to verify that the DFS namespace entered is valid. If it is not valid, you will be prompted to correct the DFS namespace path.

Acronis Files Connect will automatically create a DFS virtual root volume in the 'Acronis Files Connect DFS Volumes' folder, located in the Acronis Files Connect program directory. This volume will contain links to target servers in the DFS namespace and will be added as a shared volume with a volume name matching your DFS domain or host server name. The location where DFS virtual root volumes are created can be modified by selecting **Advanced** on the **DFS** settings tab.

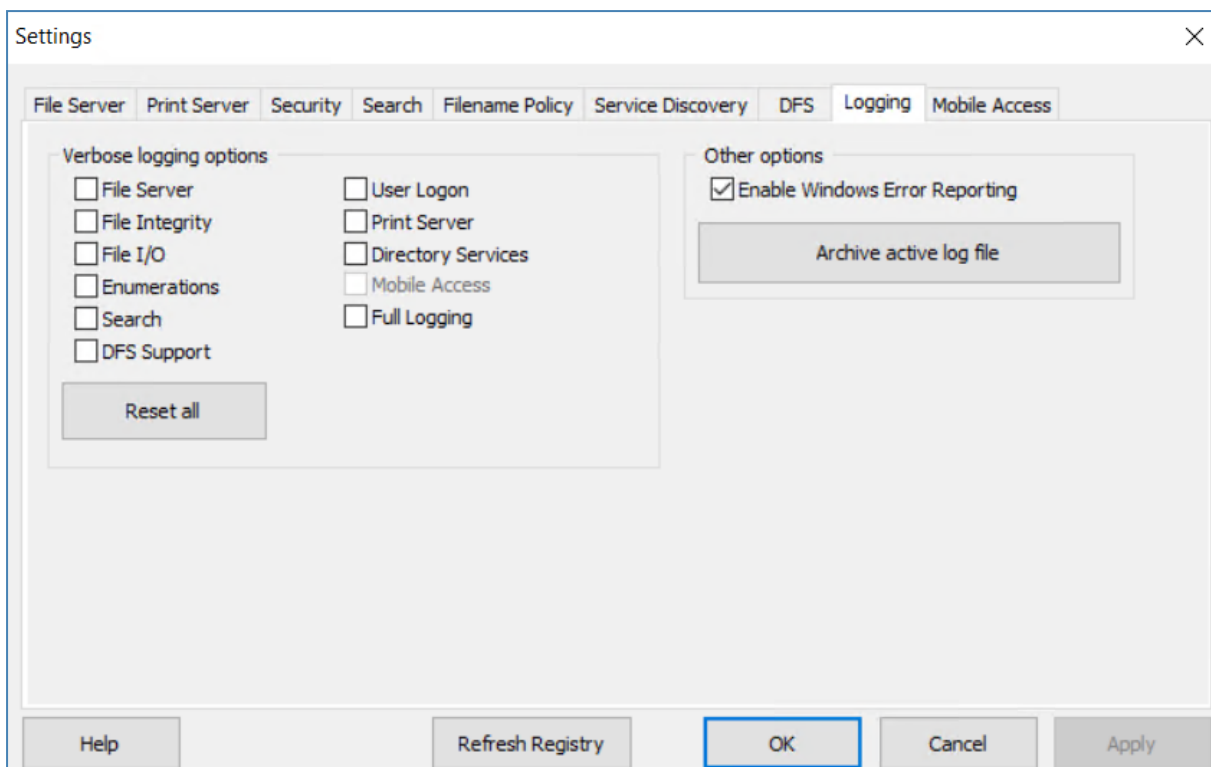
You are returned to the **DFS** tab, which is updated with the newly added namespace's information. You will find your namespace listed on the left and the target servers in that namespace listed on the right. The **Valid** column in the **Namespaces** list will indicate if the namespace was successfully validated. DFS namespaces can later be removed by selecting the namespace and clicking the **Remove** button.

## Target servers

The protocol used by Mac users to connect to each target server can be configured on a per target server basis. When a namespace is first added, Acronis Files Connect will attempt to detect, for each target server in the namespace, whether it supports the AFP protocol. If AFP is supported, the target server will be set to **AFP** by default. If AFP support cannot be confirmed, the target server will be set to **OFF**. Links to target servers set to **OFF** will not be visible to Mac users in the DFS volume(s). If you would like Mac machines to connect to a target server using SMB, you can select the **SMB** option for each individual server. If you later install Acronis Files Connect on a target server, you can return to the DFS settings tab and select **AFP** for that server.

## Logging

Acronis Files Connect allows the customization and configuration of its logging functionality and its ability to generate Windows Error Reports.



## Verbose logging options

***Enabling verbose logging could potentially have an impact on performance and should only be done at the direction of Acronis technical support.***

When enabled, these logging options increase the level of detail recorded in the Acronis Files Connect log file. Options are available for various aspects of Acronis Files Connect operations. The **Reset all** button will return all Acronis Files Connect logging to default settings.

## Enable Windows Error Reporting

When enabled, Windows will give you the option of sending error reports in the event of an issue. These error reports can be used by Acronis to identify and address potential problems.

## Archive active log file

Click this button to ZIP archive the current Acronis Files Connect log file and start a new log file. This can be used to reduce the size of your existing log file for archiving or to package your log file for delivery to Acronis technical support. Log files are located in the \Program Files\Group Logic\Acronis Files Connect\Logs\Acronis Files Connect\ folder on your system drive by default.

## Setting Mobile Access

The Mobile Access feature allows Acronis Access mobile users to access your Acronis Files Connect Volumes, including the ability to view, upload, sync, annotate and edit files from within the Acronis Access mobile app.

---

**Note**

This feature is not yet supported on clustered versions of Acronis Files Connect.

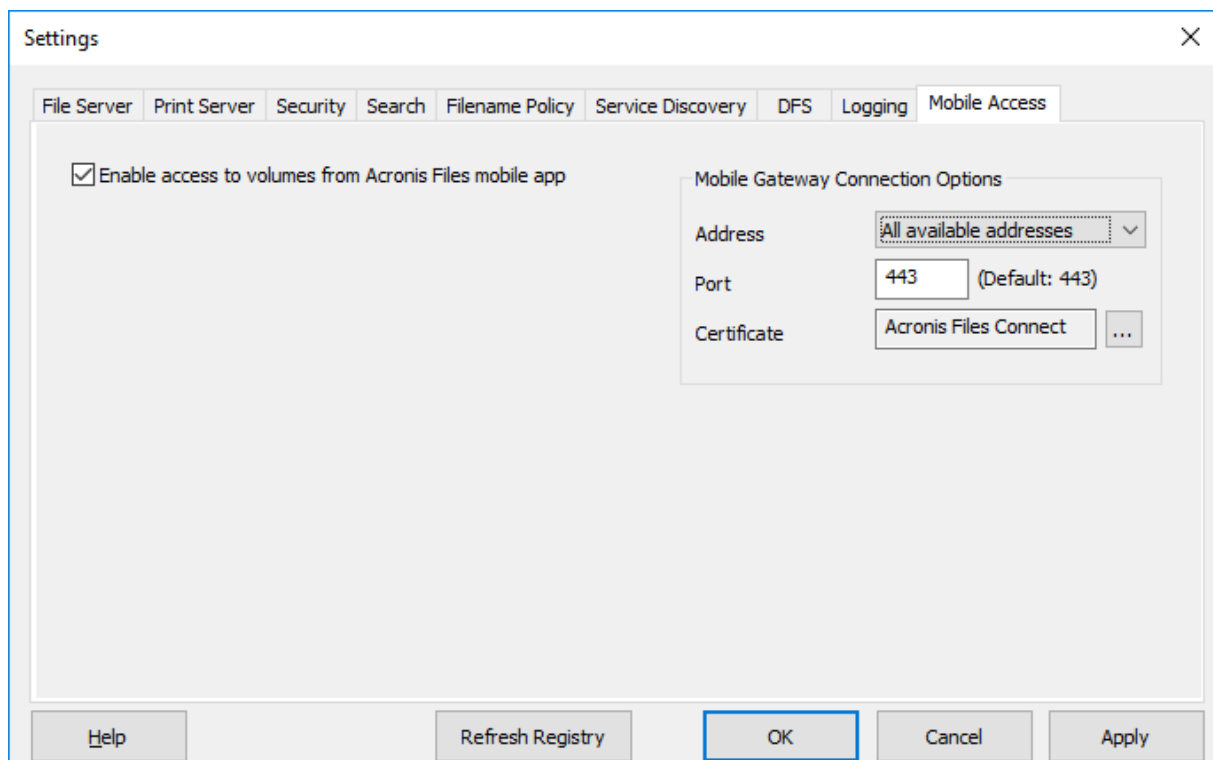
---

**Note**

Volumes defined as **Time Machine** volumes and volumes that are configured as **AFP Home Directories** will **NOT** be shared out by the Mobile Access Gateway.

---

**Enable access to Volumes from Acronis Access mobile apps** - When enabled, Acronis Access mobile clients will be able to navigate to and access Acronis Files Connect Volumes. This setting is affects all volumes.

**Mobile Gateway Connection Options**

**Address** – Network IP address for the mobile access gateway service. This is also the address that the mobile clients will connect to.

**Port** - Network port that the mobile access gateway service will run on. The default port is 443. If you change the port, you will need to enter it at the end of the Gateway address when connecting from a mobile device.

**Certificate** – Choose an SSL or self-signed certificate for the mobile access gateway service. You can choose a certificate from the Microsoft Windows Certificate Store.

# Configuring network reshare support

## Introduction

Acronis Files Connect has traditionally only included the ability to share files and folders located on the Windows server where Acronis Files Connect is installed, or on storage that is directly attached to that server. A folder within this local storage can be selected as an Acronis Files Connect volume and made available to Mac users as a standard Mac AFP file share.

With the introduction of '**Network Reshare**' in version 8.0, Acronis Files Connect now includes the ability to create file share volumes that point to folders located on other servers and NAS devices on your network. Mac machines continue to connect to Acronis Files Connect using the standard AFP file sharing protocol, while Acronis Files Connect utilizes the SMB/CIFS file sharing protocol to access files that are requested by Mac users from remote servers and NAS systems. By doing so, those users retain all the benefits of AFP file sharing while gaining access to resources that have traditionally only been available through SMB/Windows file sharing.

Acronis Files Connect Network Reshare allows access to both standard SMB/CIFS file shares, as well as Distributed File System (DFS) file shares. More details on Network Reshare of DFS resources can be found in the Acronis Support Portal (Knowledge base) article [here](#).

## A common use case: AFP access to NAS storage

A common real world Network Reshare use case involves Mac access to NAS storage, such as NetApp NAS systems. Most NAS systems do not include the ability to host AFP file shares. Mac users are left with no choice but to connect to NAS file shares using the native OS X SMB client. This typically results in suboptimal file browsing, transfer, and search performance, along with frequent Mac application incompatibilities, file name issues, file corruptions, etc.

Using Network Reshare, file shares on NAS systems can be made available to Macs through a Windows server running Acronis Files Connect. Macs connect to Acronis Files Connect AFP file shares and Acronis Files Connect interfaces with the NAS system through the NAS's existing SMB/CIFS file shares. In this way, incompatibilities and issues on the Mac side are addressed by allowing native AFP access and Acronis Files Connect's uses Windows server-side SMB access to NAS storage, which provides improved performance and throughput compared to Mac SMB client access. As a result, the performance of Mac AFP file share access through Acronis Files Connect to NAS storage is most often better than that same Mac accessing the same NAS files directly over SMB.

## Requirements

The Network Reshare feature allows a single Acronis Files Connect server to provide AFP file access to many additional file servers or NAS systems.

This feature is enabled only for the Acronis Files Connect trial and with an Acronis Files Connect Multi-Server License.

---

## Note

For information on supported operating systems and specific hardware requirements, see to [System Requirements](#).

---

## Recommendations

### Acronis Files Connect Server Network Interface Card Performance

Network Reshare routes all communication between your Mac users and your file server or NAS storage through the Windows server where Acronis Files Connect is installed. Installing Acronis Files Connect on a server with the fastest available NICs, and ideally one or more dedicated NICs for communicating with the servers or NAS being reshared, will result in the highest level of performance.

### Kerberos for Acronis Files Connect Network Reshare

In order to support Kerberos logins you will need configure Active Directory to 'Trust this computer for delegation'. More information can be found in the following article [Network Reshare and Kerberos authentication](#)

## Limitations

- To support real-time indexed filename search, Acronis Files Connect requires file system notifications provided by Windows in order to keep its search index up to date when files change. These notifications are not available over the SMB connection Acronis Files Connect uses to access file servers and NAS systems being reshared. For this reason, traditional index-based filename search is disabled on Network Reshare volumes. **Acronis Files Connect 9.0** introduces a new Acronis Content Indexing option. This indexing is performed based on a defined schedule, rather than tracking real-time changes. With this option enabled, users can take advantage of fast indexed filename searches.
- To support full content Network Spotlight search, Acronis Files Connect utilizes either the Windows Search index maintained by the Windows Search service on the server Acronis Files Connect is installed on, or the Acronis Content Indexing service. Windows Search can be configured to index remote shares that are hosted on a Windows Server that has Windows search installed and indexing. Acronis Content Indexing can be configured to index any remote shares, even those residing on a non-Windows server or NAS.
- If Network Spotlight search, either using Windows Search or Acronis Content Indexing, is not enabled, Macs searching Acronis Files Connect Network Reshare volumes will receive search results based on filename, but searches will take additional time to complete compared to searching indexed local volumes.
- It is required for the Acronis Files Connect service account to have unlimited rights in the file system as it is necessary in order to properly work with files and their metadata, including security descriptors. If the necessary rights are not given, you may encounter the "ERROR\_INVALID\_OWNER" error.

- If you have more than one Active Directory server, and Acronis Files Connect is installed on your domain controller, you will encounter AD replication issues by following the Network Reshare and Kerberos authentication steps.
- When using the Acronis Files Connect reshare feature to publish a DFS namespace, the maximum file size that can be copied to a DFS Namespace target is limited by the amount of free space available on the volume that hosts the DFS Namespace root emulator volume. Acronis Files Connect reports its free space to Mac users, regardless of the available free space on the DFS Namespace target itself.

## Initial Network Reshare configuration

---

### Note

Network Reshare support is only available for Acronis Files Connect version 8 and newer.

---

Acronis Files Connect runs as a standard Windows service on the Windows server it is installed on. By default, the Acronis Files Connect service runs in the context of the Windows local SYSTEM account. By acting as this account, Acronis Files Connect has access to the files and folders in Acronis Files Connect volumes that are located directly on the server's storage.

In order to use Network Reshare volumes, the Acronis Files Connect service needs access to the files and folders on the remote file servers and NAS devices that are being reshared. To be allowed access to these files, the Acronis Files Connect service has to be reconfigured to run in the context of an Active Directory (AD) user account that has Administrator access to the local Windows server and Full Control access to any necessary file shares that exist on remote servers or NAS systems being reshared.

### Note

On the machine running the Acronis Files Connect service, you must not have a local account with the same name and password as the Active Directory account used by the Acronis Files Connect service.

---

### Note

It is also possible to configure Acronis Files Connect , so that you can access Network Reshare volumes with the Acronis Files Connect service running under the Windows local SYSTEM account, and not under a dedicated Active Directory user account. This setup does not meet the highest security standards and it is not recommended for production environments. However, if you need exactly this type of configuration, please refer to [Network Reshare and Kerberos authentication under the local SYSTEM account](#).

---

## To configure Network Reshare:

1. Ensure that you have launched the Acronis Files Connect Administrator application at least once and you have allowed the Acronis Files Connect service to start up.

---

**Note**

Leaving the Acronis Files Connect Administrator application running may negatively impact the stability of the service. Make sure you open the application, perform the necessary tasks, and then close the application.

---

2. Configure the Active Directory account which will handle authentication for Acronis Files Connect:
  - a. **In Active Directory:** Create or identify an AD user account that will handle authentication for Acronis Files Connect. Ensure that the used AD account:
    - is dedicated to this Acronis Files Connect Server
    - has a fixed password
    - is not subject to group policies for password expiration
    - is a subject to any domain group policy necessary to grant the rights to "**Act as part of the operating system**" and "**Log on as a service**".
  - b. **On the Acronis Files Connect Server machine:** Add the dedicated AD user account to the local Windows server Administrators group. To do so, from **Windows Administrative Tools** in the **Windows Start menu**, navigate to **Computer management > Local users and groups > Groups > Administrators > Properties > Add**. This user account needs Full Control permissions to the C:\Program Files (x86)\Acronis\Access\Files Connect folder and to any locally shared volumes.

---

**Note**

In older versions of Acronis Files Connect, this path might be C:\Program Files (x86)\Group Logic\Files Connect

---

- a. **On the remote SMB shares server:** The dedicated Acronis Files Connect account needs Full Control access to the remote shared volumes as defined in NTFS or NAS device permissions.

---

**Note**

On EMC Isilon, true Full Control requires that the dedicated account is granted the Isilon right Run as root.

---

---

**Note**

On NetApp, true Full Control requires that the dedicated account is part of the NetApp's Administrators group.

---

---

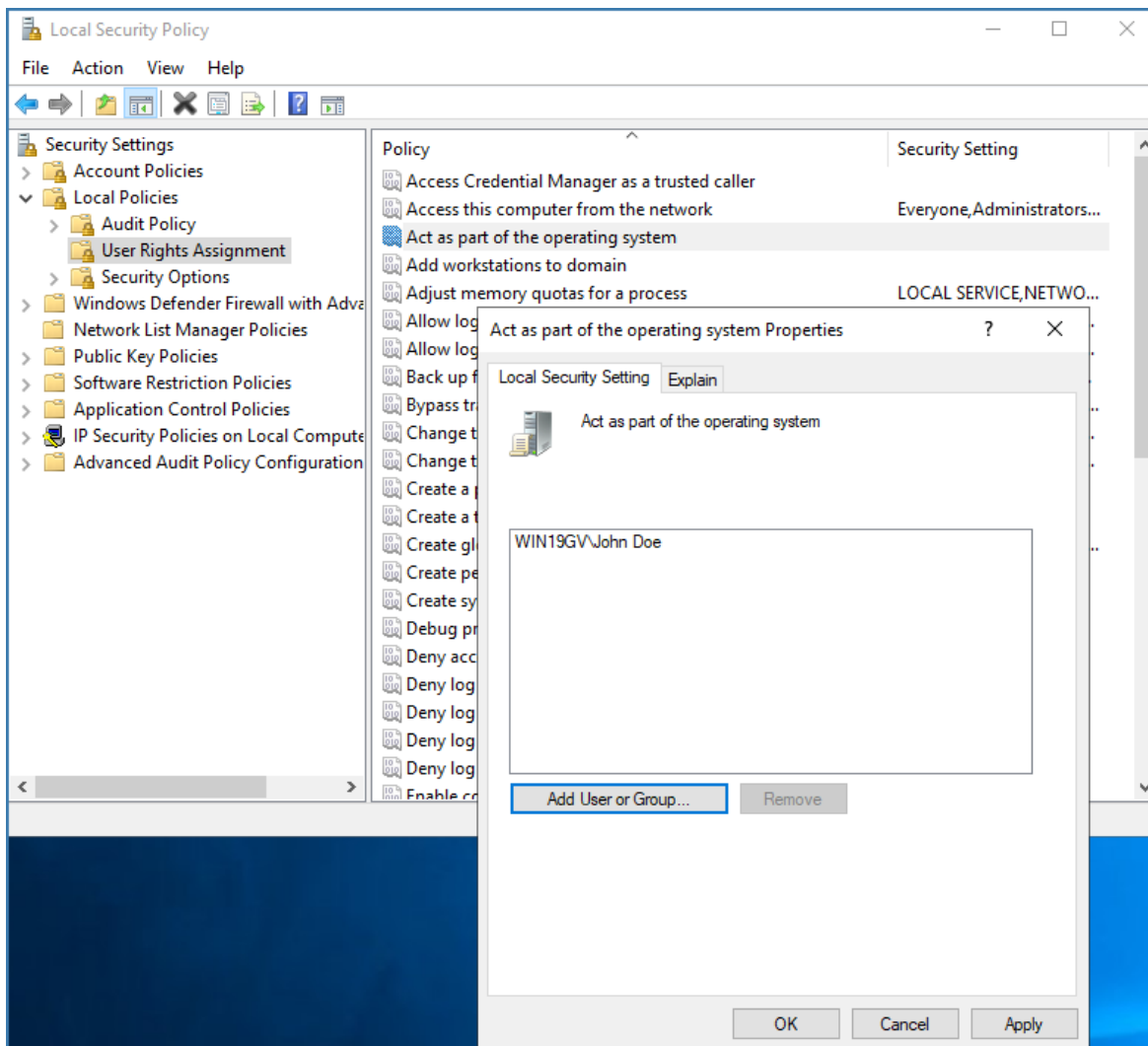
**Note**

On Windows server, the dedicated account must be added to the Windows local administrators group.

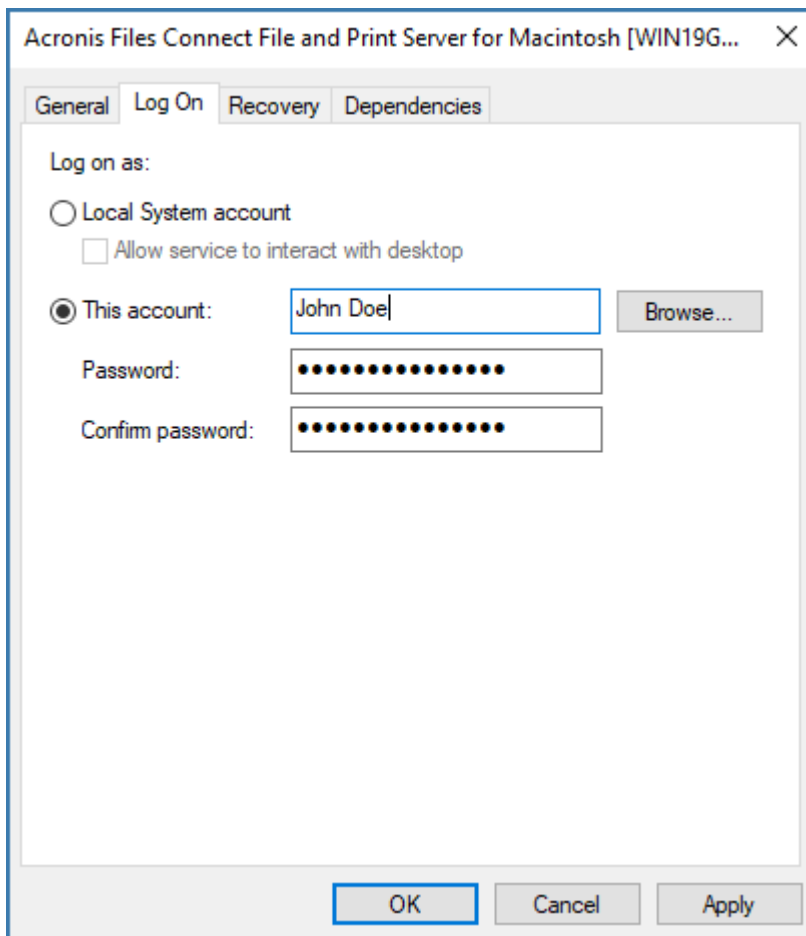
---

3. **On the Acronis Files Connect Server machine**, add the selected user to the Windows server's local security policy:

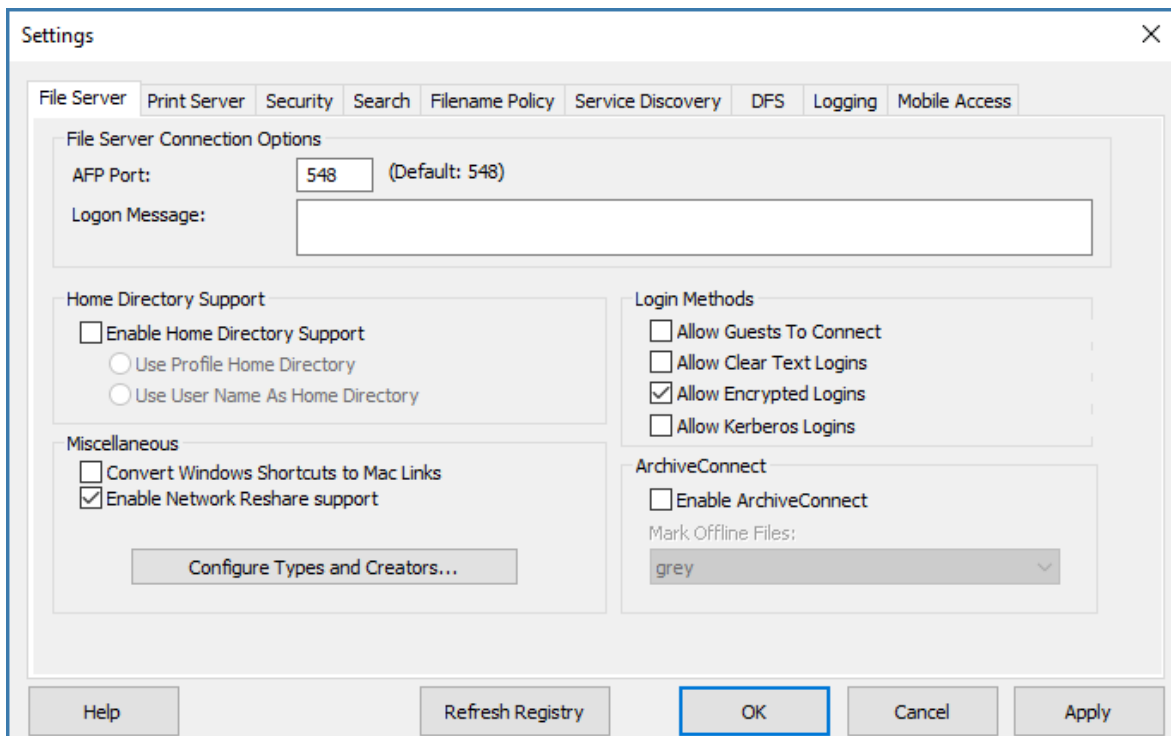
- a. From **Windows Administrative Tools** on the **Windows Start menu**, open **Local Security Policy**. This policy is found under **Security Settings > Local Policies > User Rights Assignment** section.
- b. Double click **Act as part of the operating system** and add the chosen user. You may have to reboot Windows for this setting to take effect.



4. On the Acronis Files Connect Server machine, open the **Services** control panel.
5. Open the **Acronis Files Connect File and Print Server for Macintosh** service's properties by right clicking on the service name.
  - a. Select the **Log On** tab and choose the **This account** radio button.
  - b. Configure the service to log on as the same AD service account used in step 3. Keep the **Services** control panel open. You will need it again in step 7.



6. Turn on **Network Reshare support**:
  - a. Start the Acronis Files Connect Administrator application.
  - b. Click the **Settings** button.
  - c. Open the **File Server** tab.
  - d. Select the **Enable Network Reshare support** button.
  - e. Click **OK**.
  - f. Press the **Close** button to close the Acronis Files Connect Administrator.



7. In the **Services** control panel, restart the **Acronis Files Connect File and Print Server for Macintosh** service.

## Network Reshare and Kerberos authentication

Mac users using Kerberos can access SMB/CIFS reshares through Acronis Files Connect. To enable Kerberos authentication to Network Reshare volumes, follow these steps:

### Configuring the permissions for the Active Directory account

1. Open **Active Directory Users and Computers** and locate the Acronis Files Connect dedicated user account object.
2. Right-click on it and select **Properties**.
3. Open the **Security** tab and press **Advanced**.

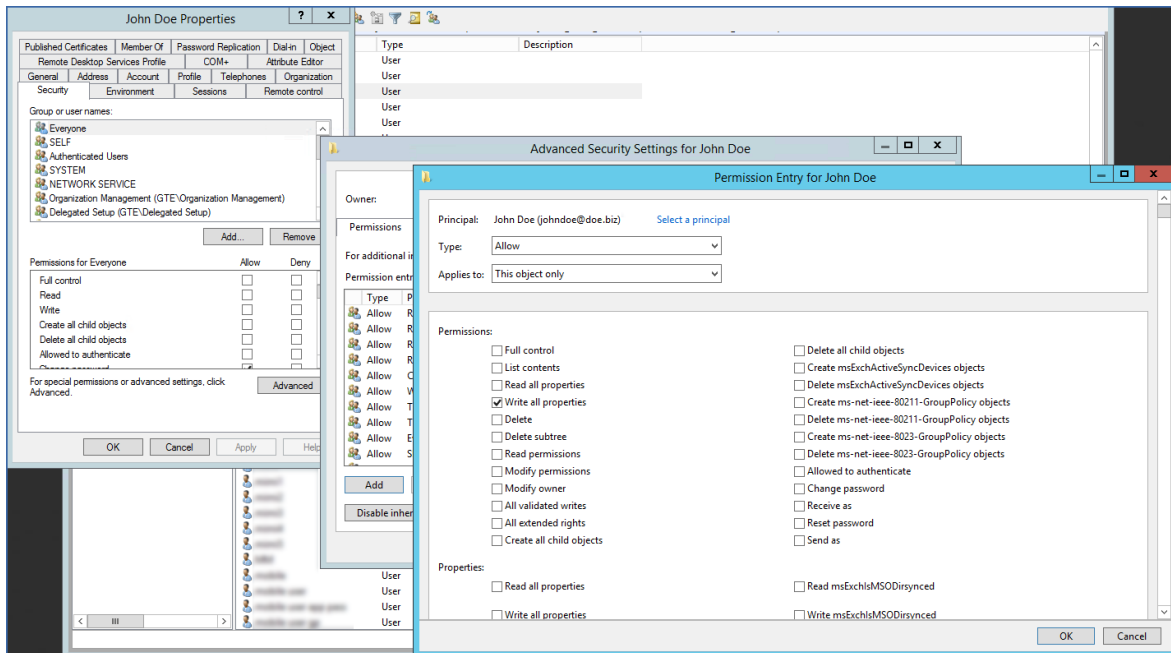
---

#### Note

If you don't see the **Security** tab, enable **Advanced Features** from **Active Directory Users and Computers** > **View** menu, and then reopen the **Active Directory Users and Computers**.

---

4. In the **Advanced security settings** dialog box that opens, press **Add**.
5. Fill in the **Permission Entry** dialog box that opens, as follows:
  - Click **Select a principal** and enter the name of the same user object
  - For **Type**, select **Allow**
  - For **Applies To**;, select **This object only**



6. Scroll to the bottom of this dialog box and select **Clear all** permissions; then select only **Write all properties** check box.
7. Close all open dialog boxes by pressing **OK**.
8. Restart the **Acronis Files Connect File and Print Server** service.

## Enabling Kerberos authentication

1. Open the Acronis Files Connect Administrator and from **Settings**, select **File Server**.
2. Select the **Allow Kerberos Logins** check box and press **OK**.

Enabling this setting creates SPN attributes (afpserver/NetBIOSname and afpserver/FDQName) for the Active Directory user account, dedicated to the Acronis Files Connect service.

## Configuring the delegation

1. Open **Active Directory Users and Computers** and locate the Windows server on which Acronis Files Connect is installed. It is commonly found in the **Computers** container.

### Note

If you can not find the computer object for the server that runs Acronis Files Connect, in the default **Computers** container in Active Directory, you have to edit the [ActiveDirectoryComputers registry key](#), so that the Acronis Files Connect service can construct the correct distinguished name for the Acronis Files Connect server's computer object. Once the key is configured, restart the Acronis Files Connect service and proceed with the steps below.

If the Acronis Files Connect server's computer object is in the default **Computers** container, there is no need to configure this registry key and you can proceed with the steps below.

2. Right-click the Acronis Files Connect server and select **Properties**.
3. Open the **Delegation** tab.

4. Select **Trust this computer for delegation to specified services only**.
5. Select **Use any authentication protocol**. This is required for negotiation with the SMB server.
6. Add the Windows servers or NAS devices that you want your users to access through reshare. Click **Add...** to search for these Windows computers in the Active Directory and add them. Select only the **cifs** service type.
7. Repeat these steps for all Acronis Files Connect servers for which you want to enable Kerberos authentication.

---

**Note**

It may take 15 to 20 minutes for these changes to propagate through the Active Directory forest.

---

**Note**

If you have more than one Active Directory server, and Acronis Files Connect is installed on your domain controller, you will encounter AD replication issues with this setup.

---

## Network Reshare volume configuration

**To configure a Network Reshare volume:**

1. Open the **Acronis Files Connect Administrator**.
2. Click **Volumes**, and then click **Create**.
3. Click **On another server**.
4. Enter the UNC path of the SMB/CIFS file share that you want to reshare as an Acronis Files Connect volume, and then click **OK**.

This UNC path is in the typical \\servername\sharename format. For example,  
\\nas.mycompany.com\myshare

---

**Note**

Ensure that you use an FQDN or NetBIOS name, and not an IP address, otherwise Kerberos logins will fail.

---

Distributed File System (DFS) UNC paths can also be entered for Network Reshare volumes. DFS target resolution will all occur in the SMB reshare layer and Macs will be able to browse and access the reshared DFS resource. For more information on DFS with Network Reshare, refer to [Accessing DFS files using Acronis Files Connect](#).

5. In the **Volume Properties** dialog box, modify the **Volume Name** if needed, and then click **OK**.

---

**Note**

If you receive an error stating: *The specified path is not available*, you may have entered an invalid UNC path, or the user account that you selected during the [Initial Network Reshare configuration](#) may not have Full Control access to this file share at this UNC path. If this is a Windows file share, ensure that this user account has both **Sharing** and **Security** permissions to the file share.

---

## Mirroring File servers and SMB shares

Acronis Files Connect can be configured to mirror a file server and all SMB shares on that server will automatically be added as AFP file share volumes in Acronis Files Connect. When set up to run automatically, any SMB shares that are added, modified or removed on the mirrored server, will be updated or removed from the Acronis Files Connect server in a set time interval. You can also force the mirroring manually, if needed.

---

### Note

If you choose to mirror multiple file servers, multiple NAS, or a server with a large number of SMB shares, Acronis Files Connect will create volumes for all of these shares. Depending on the number of shares, your server and network performance, and your usage patterns, this could result in a heavy load on your Acronis Files Connect server.

---

### Note

Add mirrored servers incrementally or in a test environment first, to determine the optimal limits for your specific environment.

---

By default, mirroring is disabled.

### To enable mirroring:

1. In the Acronis Files Connect Administrator, go to **Settings > File Server** and enable **Network Reshare support**. Ensure that it runs properly.
2. Edit the following registry keys:
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Refreshable\SupportServerMirroring – This is the main on/off switch for the Mirroring feature. To enable it, set this registry key's value data to 1.
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Refreshable\ServerMirroringInterval – This key sets the interval between updates to the mirrored shares. By default, it is 900 seconds (15 minutes). Setting this interval to 0 will suspend the automatic updates.
3. In the Acronis Files Connect Administrator, go to **Settings** and click on **Refresh Registry**.
4. Restart the Acronis Files Connect Administrator and check that the **Mirror Servers...** button is enabled.

### To mirror a file server:

1. Open the Acronis Files Connect Administrator and go to **Volumes**.
2. Select **Mirror Servers...**
3. Select **Add Server...** and enter the address of the server that you want to mirror.
4. Add a custom name for this server and select the desired search type – **Acronis Content Indexing** or **Windows Search**. This optional name is displayed in the Acronis Files Connect client, helping users to find what they need if there are a lot of shares with the same name.

5. Click **OK**.
6. All SMB shares from the selected server will now be available as regular volumes in the Acronis Files Connect Administrator. From there, you can manage their settings individually.

### To remove a mirrored file server:

1. Open the Acronis Files Connect Administrator and go to **Volumes**.
2. Select **Mirror Servers...**
3. Choose the specific server you want to remove and select **Remove...**

---

#### Note

You cannot remove individual SMB shares from a mirrored server. You can only remove all the SMB shares from a specific mirrored server by removing the whole server.

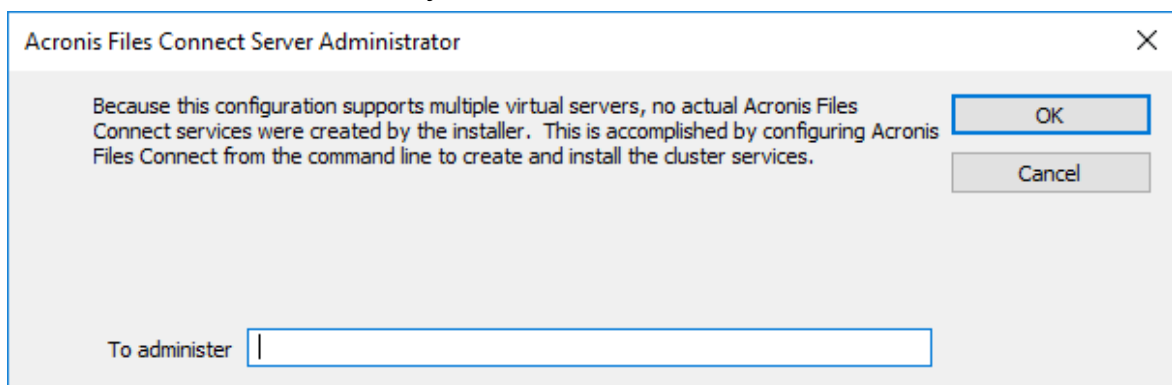
---

## Administering Acronis Files Connect remotely

You can configure Acronis Files Connect on a remote computer if Acronis Files Connect is already installed on that computer. You must have Windows Administrative privileges on the remote computer. The experience of administering a remote server is very similar to that of the local server Administrator, except that the title of the Administrator dialog box shows the name or IP Address of the remote computer whose Acronis Files Connect service you are configuring and you cannot browse for folders to share. Otherwise, you can configure the remote server just as you would a local server.

### To administer a remote Acronis Files Connect server, do the following:

1. Hold down the **Control** key while you launch the Acronis Files Connect Administrator. Alternatively, if there is no local installation of Acronis Files Connect, Acronis Files Connect Administrator will start immediately in remote mode.



2. Type the name or IP Address of the remote computer and click **OK**.
3. The Administrator will attempt to use your Windows credentials to log onto the server. If necessary, you will be prompted for an alternate username and password.

# Configuring client computers to print to Acronis Files Connect

To make use of the Acronis Files Connect lpd/lpr print service, Mac users follow specific steps, depending on their operating system. Once you add print queues through the **Acronis Files Connect Administrator Print Queues** dialog box, they are immediately available for clients to print to them.

A Mac user can select an Acronis Files Connect queue to print to in a number of ways, depending on the operating system they are using and the functionality they need. When using macOS, the following are the primary ways to set up a printer:

- The Acronis Files Connect Mac client app displays a list of server print queues that you can install. To do this, select a print queue from this list and click the **Add printer** button.
- The macOS command `lpadmin` may be used to add printers. Find more details on the macOS man page.

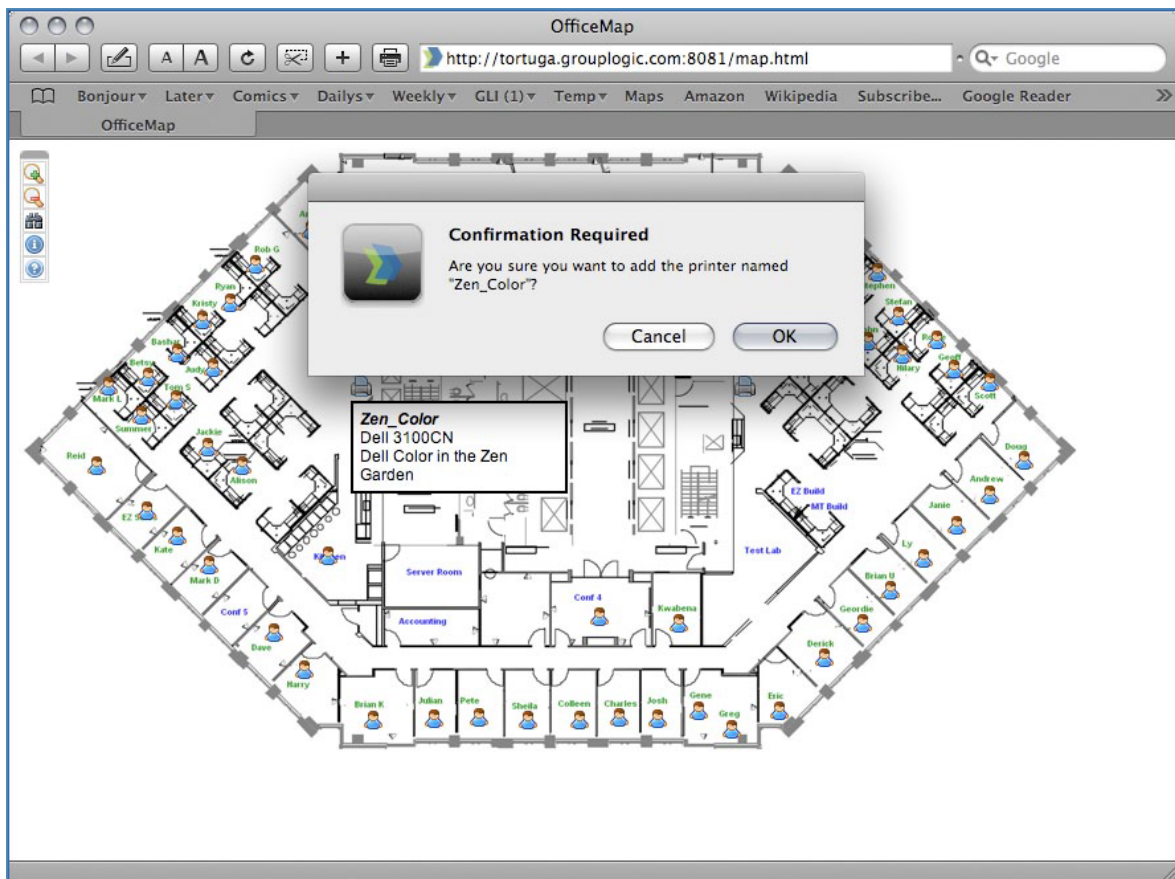
## Adding a printer from a Web Page

The helper application can be used as an Internet protocol helper for `ezip://` URLs. This enables Safari or another web browser to create a printer when you click on a specially formatted link from a standard web page such as an office map with links for different areas. If you click on a URL to invoke the helper application, it asks if you want to add the printer.

Creating a web-based Printer Location Map is a very effective way to let users easily find and add printers. Taking a scan of the map and making a PDF in Adobe Acrobat is one simple way to create a web page with a map of the user's floor. Acrobat will let you add links for areas of the picture without having to know any HTML.

**To add a printer from a Web page, do the following:**

1. Click the icon of the nearest printer on the map.
2. Click **OK** to confirm the dialog asking if the printer should be added.



## Mac users configuration for DFS support

In order for the Mac users to be able to access Acronis Files Connect DFS volumes, each of them has to be configured to properly locate and mount DFS resources. This configuration can be accomplished through the installation of the Acronis Files Connect Mac client app.

If Mac machines are using home directories located on DFS volumes, the Acronis Files Connect Mac client app must be installed.

## Acronis Files Connect Mac client app

The Acronis Files Connect Mac client app is the best way to connect your Mac users to all the resources shared with your Acronis Files Connect server.

It is a full-fledged app that has many advantages over the widget.

- It can search through your file servers and shares. New search features for performing spotlight searches of AFP file volumes. Fast, full-content search of files in SMB file shares which can then be accessed by the Mac via SMB.
- You can search through many volumes without mounting them but you can mount only desired volumes or resources.
- All available printers are listed in a user-friendly manner.

Find [more information](#) about the Acronis Files Connect Mac client app as well as some usage instructions.

## Adding a License Serial Number

You can enter a serial number for any upgrade, without stopping the Acronis Files Connect service. When you enter a serial number while the Acronis Files Connect service is running, Mac machines stay connected and continue to use Acronis Files Connect volumes.

---

### Note

Only license keys associated with an active support and maintenance agreement are supported by Acronis Files Connect. Check the status of your license key at:

<https://www.acronis.com/products/file-sync-and-share-downloads/>.

---

### Note

Adding a new license serial number **will replace** the existing one.

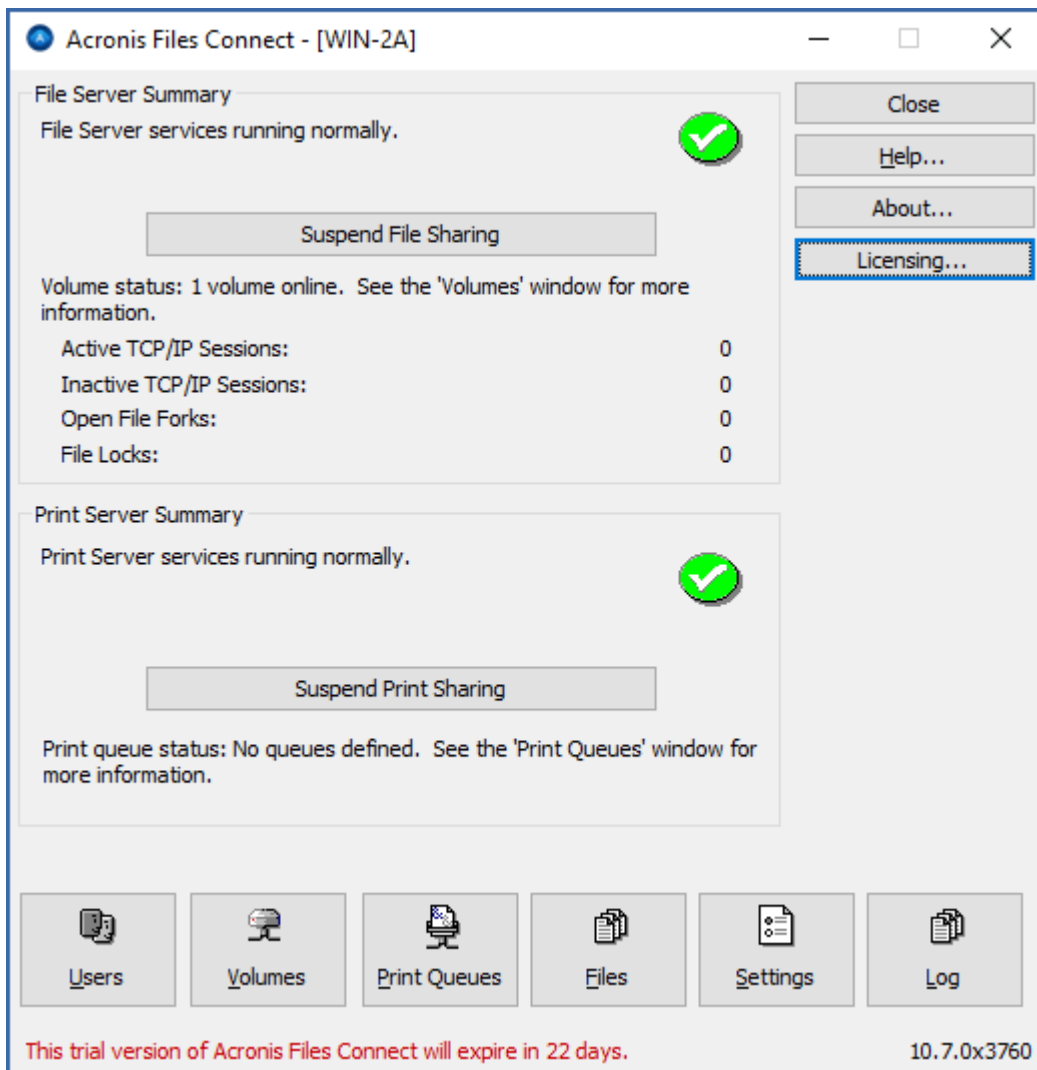
---

## You need to enter a new license serial number when:

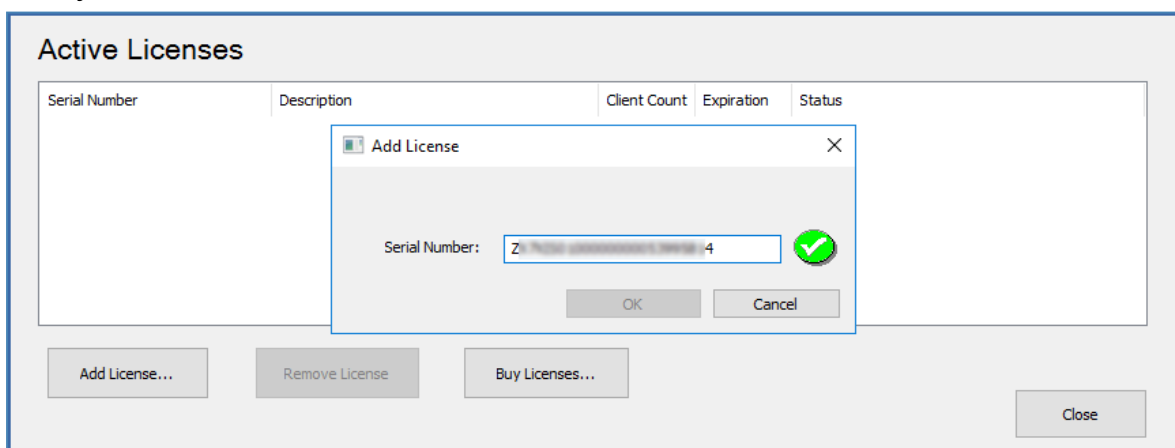
- You have a trial version of Acronis Files Connect installed and you purchase a license for the product.
- You are upgrading or downgrading your client count.
- Your ELP serial is expiring and you need to enter your new ELP serial.
- You upgraded from a very old version and your previous perpetual serial was replaced with a new serial that can be used with current versions.

## To add a license serial number

1. Open the **Acronis Files Connect Administrator**.
2. Click **Licensing**.



3. In the **Active Licenses** window that opens, click **Add License**.
4. Enter your serial number, then click **OK**.



5. The serial number will be displayed in the **Active Licenses** list and will take effect immediately.
6. Click **Close** to return to the **Acronis Files Connect Administrator**.

# Searching with Acronis Files Connect

The macOS performs three types of file searches – enumeration searches, index searches, and Spotlight searches.

## Enumeration search

When the macOS performs an enumeration search, it scans each file in the folder and all of its subfolders across the network. An enumeration search is performed if searching a subfolder of a volume or if catalog search is disabled. The process of the client enumerating the entire directory structure below the folder being searched results in drastically reduced search performance.

## Catalog search

Acronis Files Connect supports Catalog Search queries on AFP volumes.

The last version of macOS to natively support Catalog Search was macOS 10.8 Mountain Lion, so Catalog Search queries from Macs now require the use of third-party apps.

Acronis recommends using the [Acronis Files Connect Mac client app](#) app to perform searches.

## Spotlight search

Spotlight search allows files to be found by searching on content, in addition to file names and file attributes. When enabled, Spotlight search replaces both Enumeration search and Catalog search, and provides results when searching both at the root of a volume, and within subfolders.

Spotlight search can be enabled either for all volumes, or for individual ones.

### To enable Spotlight Search for all volumes:

1. In the **Acronis Files Connect Administrator**, open **Settings**
2. Under **Search** tab, select **Enable Spotlight Search on all volumes (global)** check box
3. Click **OK**

---

#### Note

Note: If the setting **Enable Spotlight Search on all volumes (global)** is selected, you cannot disable Spotlight search for individual volumes.

---

### To enable Spotlight Search for individual volumes:

1. In the **Acronis Files Connect Administrator**, open **Volumes**
2. Select the desired volume, and then click **Modify**
3. Under **Search**, select **Support Spotlight Searching**, and then choose between **Acronis Content**

## Searching and Windows Search

4. Click **OK**

# Storing search index files

Acronis Files Connect creates a separate search index file for each Acronis Files Connect volume; the search index files are stored in a folder called Acronis Files Connect indexes. Placing index files in one location and excluding this folder from scanning prevents problems with virus scan software and backup applications. You can specify custom index file paths for individual volumes when you set up or modify a volume to be shared; see the section [Creating a Volume](#).

---

### Note

To help you locate a search index for a volume, Acronis Files Connect begins each index file name with the name of the volume to which it belongs.

---

If you do not create a custom path, search index files are stored in a one of two locations.

- **Acronis Files Connect stand-alone server:** Search index files are stored in a folder called Acronis Files Connect Indexes in the Acronis Files Connect application folder or the custom global location you have set.
- **Acronis Files Connect Cluster:** Search index files are stored in a folder called Acronis Files Connect Indexes at the root of the drive on which the volume resides.

When starting EZIP for the first time, search indexes for a volume is created in the default index path unless you have set individual custom paths for a particular volume or volumes.

# Using Acronis Files Connect

## Using the Acronis Files Connect File server

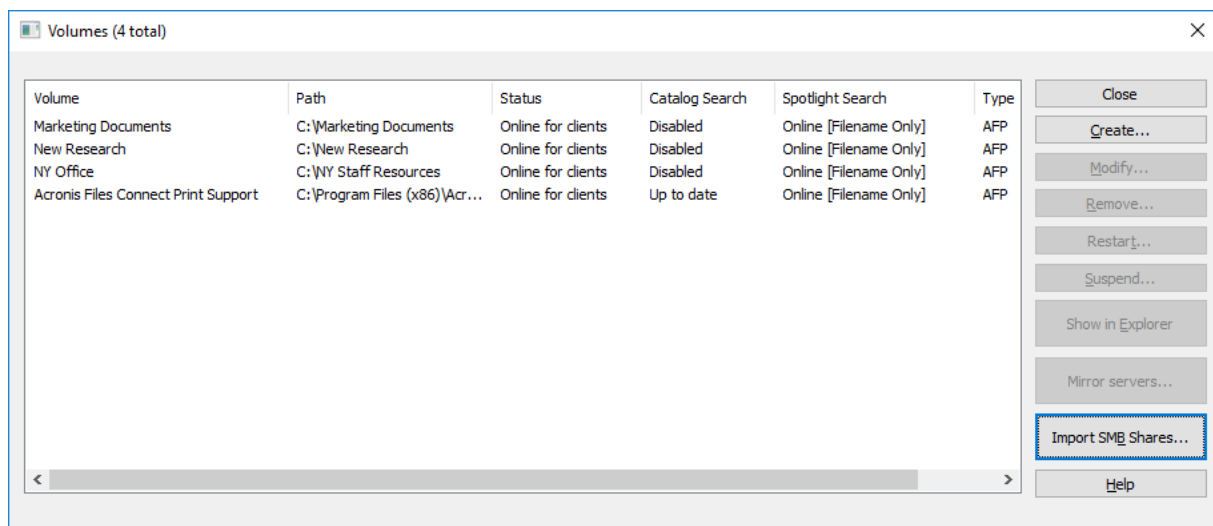
After using the **Acronis Files Connect Settings** dialog box to set up your server name, security and other settings, you can create the volumes you want to share and the printers you want your Mac users to use. After completing these tasks, Mac users can connect to your server and use the volumes and printers you set up. You can check the **Users** and **File** dialog boxes to see who is connected and which files they are accessing, In addition, you can send messages, disconnect users, and delete items from the files being viewed.

## Creating Volumes for Use with Acronis Files Connect

You can share NTFS directories located on your Windows system for Mac users.

## Viewing the Volumes window

Click on **Volumes** on the **Administrator** dialog box to display the **Volumes** dialog.



- **Create** – Creates a volume.
- **Modify** – Opens the Volume Properties window.
- **Remove** – Removes the selected volume.
- **Restart** – Restarts the volume.
- **Suspend** – Takes a volume temporarily offline so that clients cannot connect to it.

---

### Note

Suspended volumes will be resumed every time the Acronis Files Connect service is restarted.

---

- **Show in Explorer** – Shows the volume's parent folder in Windows File Explorer.

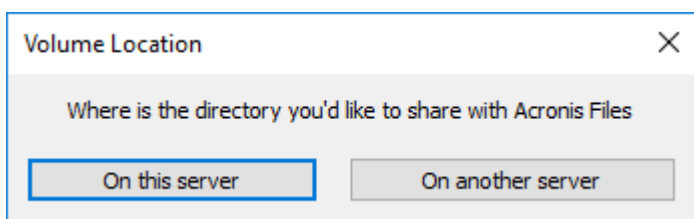
- **Mirror servers** – Mirrors one or multiple file servers so that all SMB shares on them are automatically added as AFP file share volumes in Acronis Files Connect. See more about [Mirroring SMB file servers](#).
- **Import SMB Shares** – Reshares all folders shared with Windows file sharing (SMB) with Acronis Files Connect as well.

## Creating a Volume

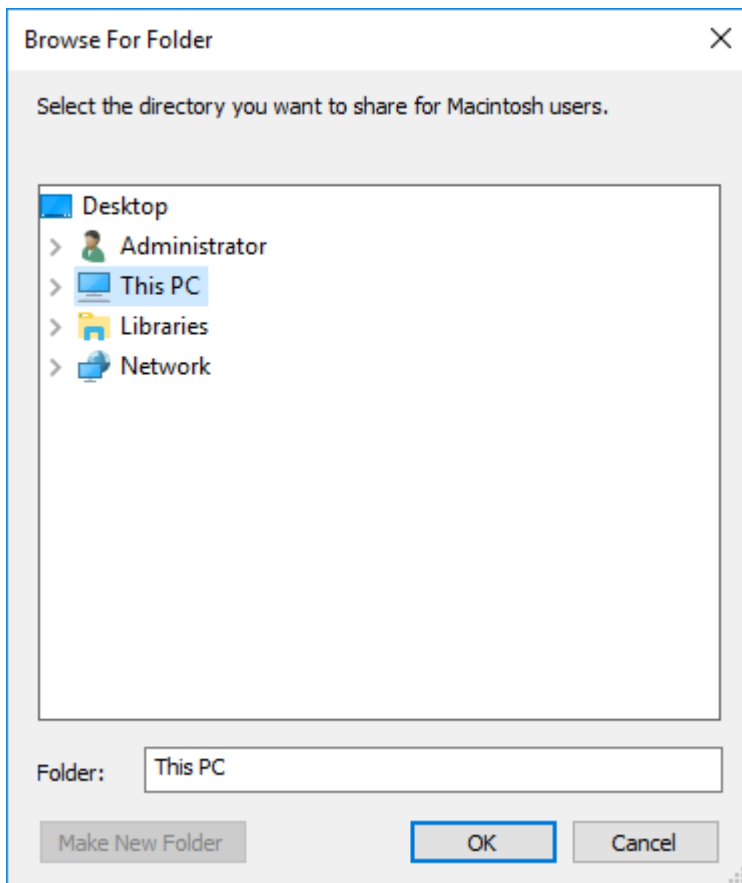
Folders can only be shared as Acronis Files Connect volumes if they reside on an NTFS formatted disk. If you try to create a volume that is not on an NTFS formatted disk, Acronis Files Connect gives an error message.

### Creating a Volume:

1. Create a new directory on an NTFS formatted volume on the server machine or find an existing directory that you want to use.
2. From the Acronis Files Connect Administrator window, click **Volumes**.
3. On the **Volumes** dialog, click **Create**.
4. If you have enabled **Network Reshare support**, choose the volume location – **On this server** or **On another server**.



5. If your desired directory is on another server, enter its UNC path in the next dialog.
6. If your desired directory is on your server, use **Browse for Folder** dialog to locate and select it.



---

**Note**

The use of removable devices as volumes is not supported. (For example, flash drives, USB drives, etc.)

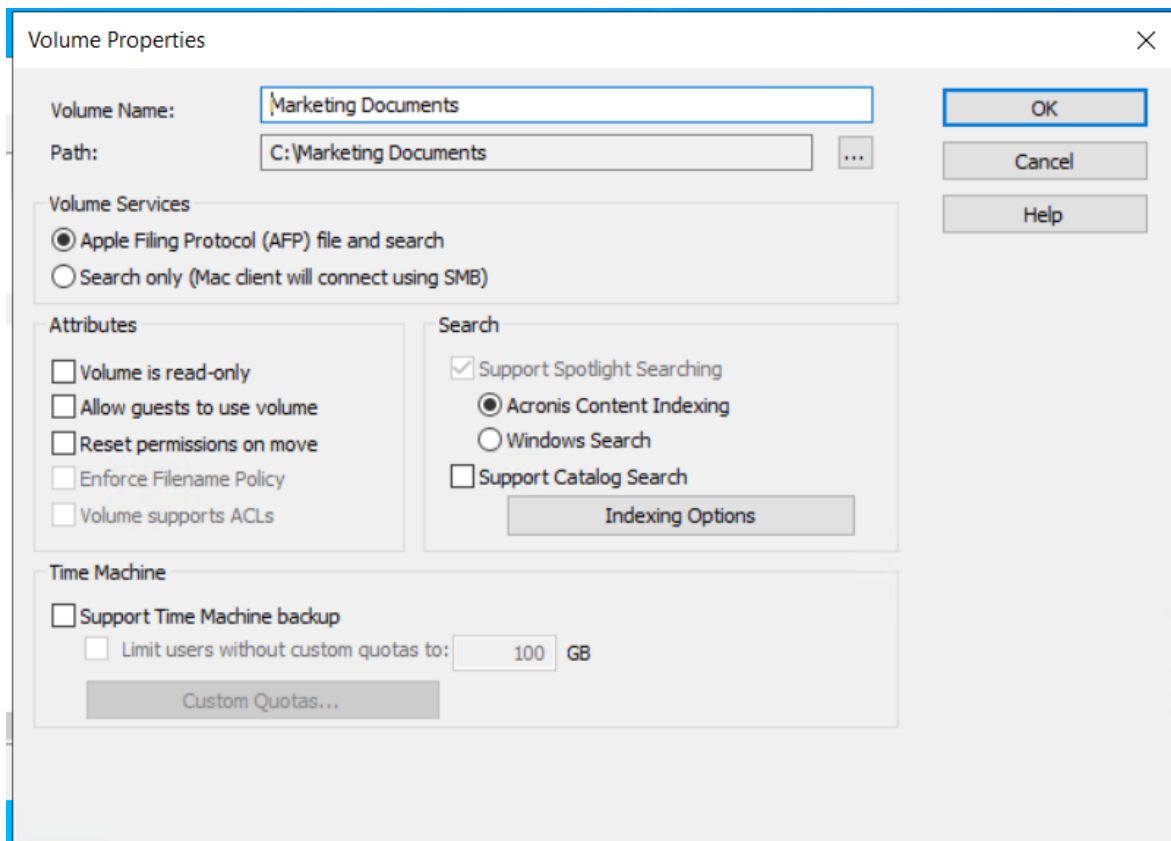
---

7. Click **OK** and the Volume Properties window will appear.
- 

**Note**

If you are in a clustered environment and you use Acronis Content Indexing, you should set a custom index file path to a folder on a shared (failover) disk. *See more about [Indexing options](#).*

---



8. Edit the **Volume name** if you want to change the automatically proposed one.

---

**Note**

You cannot edit the Volume name later. If you need to do that, you have to delete the volume and create it again with the desired name.

---

**Note**

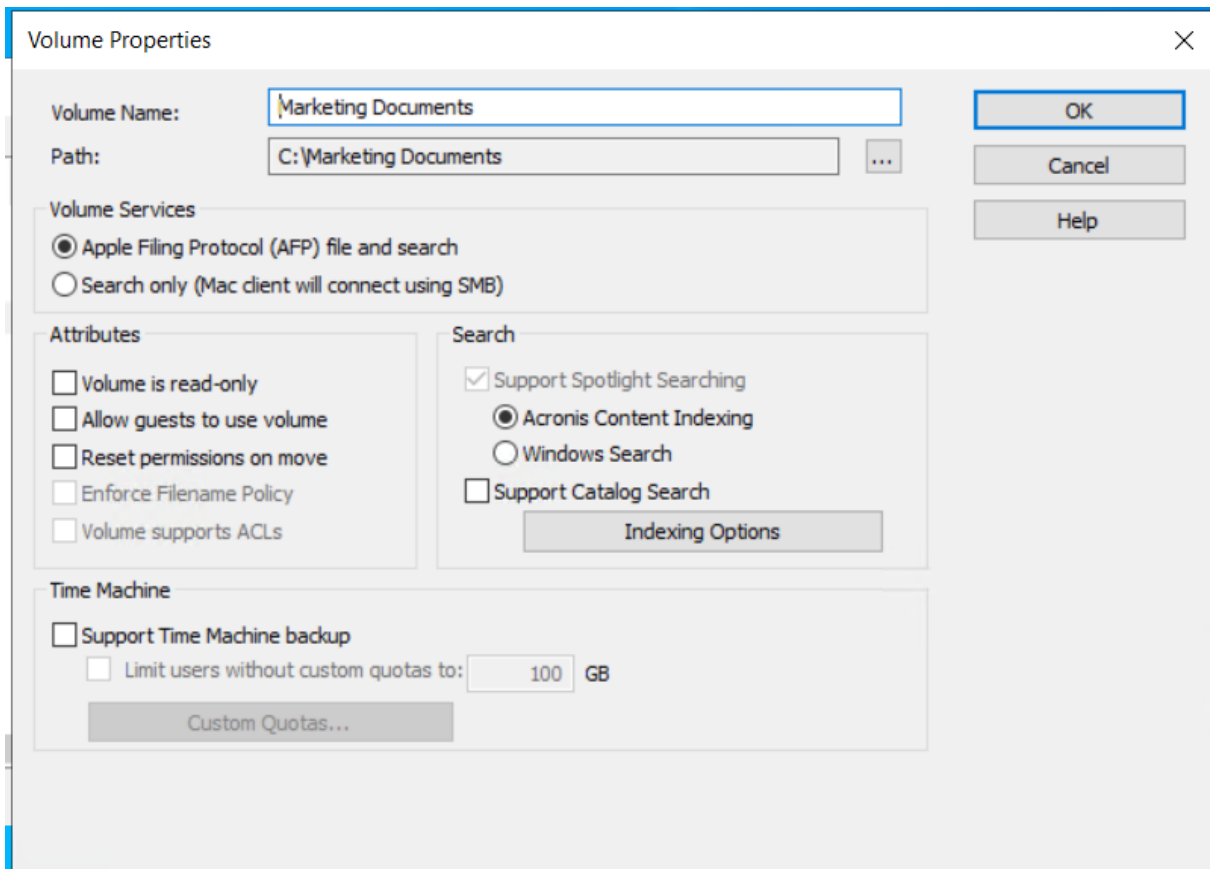
With Acronis Files Connect 8.0.4 or later, a name can have up to 127 characters for UTF-16 and 190 for UTF-8. If you enter more, Acronis Files Connect will truncate the name.

---

9. Choose any additional settings required. *See more about [Volume properties](#).*
10. Click **OK** to create the volume.

**As soon as a volume's status becomes Online for Clients, Mac users can see and connect to it.**

## Volume properties



### Warning!

**These volume properties do NOT affect the mobile clients connecting to them. Only the Catalog search settings will affect it.**

### Volume services

- **Apple Filing Protocol (AFP) file and search** – This is the default setting and creates a volume accessible by AFP. The volume will be accessible and searchable from the Acronis Files Connect Mac client app and the Mac Finder. When opening files and browsing these volumes, the Mac will connect using AFP in either case.
- **Search only (Mac client app will connect using SMB)** – With this option, the volume will be displayed in the Acronis Files Connect Mac client app and will be searchable, but it will not be shared as an AFP volume. Macs connecting to the Acronis Files Connect server using AFP will not see this volume. Macs will automatically connect to 'Search only' volumes and files found in Acronis Files Connect Mac client app search results using SMB. This connection uses preexisting Windows or NAS SMB file server shared volumes.

### Note

Acronis Files Connect Search only volumes are not supported on Microsoft Failover Clusters.

## Volume is read-only

Setting the Volume to read-only prohibits Mac users from changing any documents on the volume or adding any new files or folders.

## Allow guests to use volume

If you want a Mac user who logs into Acronis Files Connect as a guest to access the volume, select this check box.

## Reset permissions on move

If you would like files and folders to always inherit permissions from their parent folder after they have been moved, select this check box.

---

### Note

If the directory that is moved contains a large number of sub-folders, resetting the permissions can take awhile.

---

## Enforce Filename Policy

Enforcing Filename Policy will prevent Mac users from saving files to the server that do not comply with the filename policies that the administrator has set in the global **Filename Policy** settings.

## Search settings

### Support Spotlight Search

Enables Spotlight searching on the individual volume by Mac users. You must choose the desired type of indexing (Acronis Content Indexing by default).

---

### Note

Searching by Windows and Mac file tags is now supported by both types of indexing. For Windows Search, a small additional configuration is required, please visit [Windows Search Indexing](#).

---

### Acronis Content Indexing

This type of indexing is built-in Acronis Files Connect and only requires that you enable it on the **Search** tab of the **Settings** dialog before it can be enabled for the specific volume.

### Windows Search

This type of indexing relies on Microsoft Windows Search. To enable Windows Search indexing, you have to make sure Microsoft Windows Search is installed on the Acronis Files Connect server and must be enabled on the **Search** tab of the **Settings** dialog before it can be enabled for the specific volume.

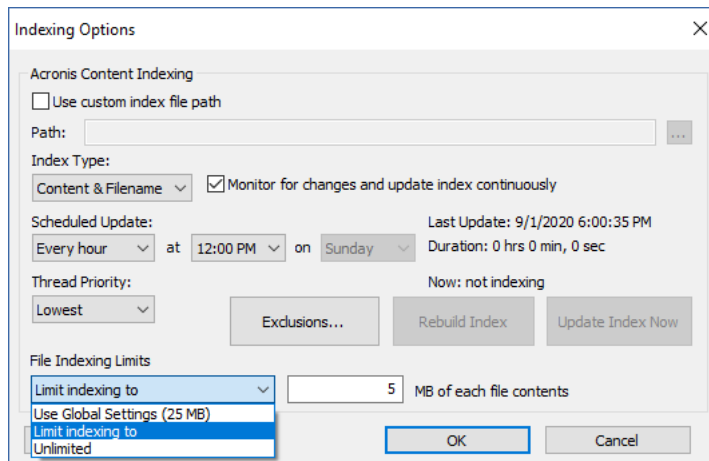
### Support Catalog Search

Enables Catalog searching on the individual volume. This is the default built-in search method.

## Volume supports ACLs

Select this check box if you want the volume to support Access Control Lists.

## Indexing options



## Acronis Content Indexing

- **Use custom index file path** – To specify an alternate index file location for a volume, select this check box and select a path for the new index file location.

---

### Note

In a clustered environment, you must specify a folder on a shared (failover) disk. You might consider a disk dedicated to storing search indexes.

---

- **Index Type** – Sets the type of indexing:
  - **Filename Only** – Indexes files only by their name. This indexing type takes less time than the content-based one. You can review the progress in **Indexing Options** as well as reduce the indexing time by adding some files and folders to the list of exclusions, or limiting the size of each file contents, used for indexing.
  - **Content & Filename** – Indexes files both by their name and contents. This type of indexing provides better search results, but takes longer. Progress is tracked and indexing time reduced, the same way as already explained for the above option.
- **Monitor for changes and update index continuously** – Continuously monitors local shares and network reshares for changes and updates the index immediately. Scheduled updates will continue to run and are still recommended to ensure that all changed files are indexed, in the event of missed notifications or service interruptions.
- **Scheduled Update** – Sets a time schedule for updating the index. This setting for indexing interval can be used as a secondary process in case some changes have not been propagated or some items were not indexed automatically.
- **Thread Priority** – Sets the process priority for indexing this volume.

- **Exclusions** – Allows the administrator to exclude certain folders or files from the index, which can drastically improve indexing speed.

---

#### Note

When adding an exclusion, you can also use Acronis Content Indexing's syntax for better filtering. To use more than one filter, separate them with spaces. **For example, filter1 filter2**

---

- **\*ExampleFile\*** matches any file whose filename contains **ExampleFile**.
- **\*\ExampleFolder\\*** matches any file in a folder named **ExampleFolder**. For folders with spaces in the path, you must use quotes, e.g. **"\*\Old Files\\***".
- **\*** in a filename filter matches any number of characters. **\*.DOC** will exclude all **.DOC** files.
- **?** in a filename filter matches any single character. **file?.doc** will exclude **file1.doc, file2.doc** and etc. but not **file123.doc**.
- **Rebuild Index** – Initiates the creation of a new search index for the volume. The previous search index will be used to satisfy search requests until the new indexing process has been completed.
- **Update Index Now** – Initiates an update of the existing index immediately.
- **File indexing limits** – select one of the options in the drop-down menu:
  - **Use Global Settings (X MB)** - the volume will use the Default server limit, set in the 'dtSearchIndexFileContentLimitGlobal' registry key value, located at: Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Spotlight\Refreshable
  - **Limit indexing to X MB of each file contents** - a custom value will be used only for this volume by limiting the indexing to only the first X megabytes of a file's contents.
  - **Unlimited** - for each file in this volume, the search engine will index all contents and metadata, regardless of their size.

## Catalog Search

- **Use custom index file path** – To specify an alternate index file location for a volume, select this check box and select a path for the new index file location.
- **Rebuild Index** – Initiates the creation of a new search index for the volume. The previous search index will be used to satisfy search requests until the new indexing process has been completed.

## Time Machine

### Support Time Machine backup

When you check the **Allow Time Machine Backup** box, Mac machines can use the selected Acronis Files Connect volume as a Time Machine backup destination. By default, the **Support Time Machine backup** setting is disabled for a volume.

---

#### Note

Time Machine is supported with macOS versions 10.10 to 13.

---

---

**Note**

You cannot enable Support Time Machine backup for volumes that are read-only or used as home directories.

---

When you enable Support Time Machine backup, Acronis Files Connect disables Volume is read-only. The opposite is also true.

**Limit users without custom quotas to X GB**

Check this box and enter a value to limit the size of Time Machine backups per user. When the Mac machine connects to the server for the first time, it sees the available space on the drive as whatever the quota was set to. On subsequent logins it will see the available space as the quota size minus however much space has been used by that user's other backups. This quota applies to all users who do not have a custom quota assigned.

---

**Note**

Because Acronis Files Connect has to tell the Mac how much space is available immediately when the user logs in, prior to Time Machine opening a specific backup file, the quota is applied on a per user basis not a per machine basis. If a user backs up both a desktop machine and a laptop, the quota will apply to the combined size of the backups.

---

**Custom quotas**

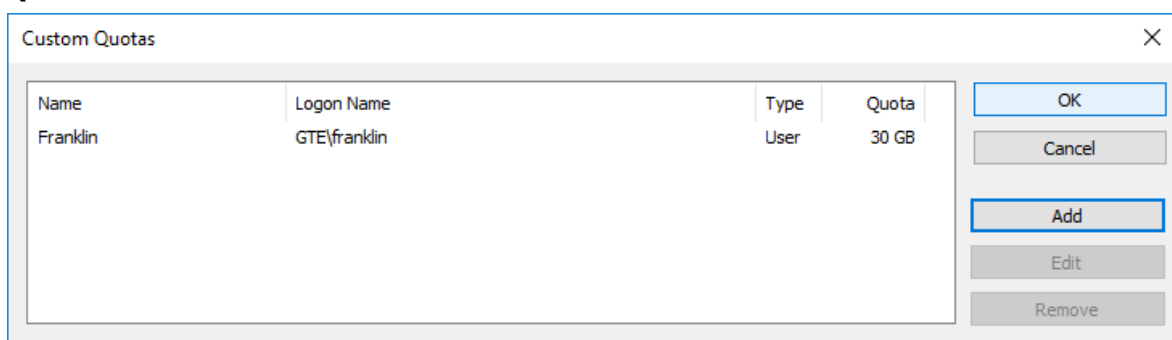
This button opens the **Custom Quotas** window.

## Using Custom Quotas

You can use **Custom Quotas** to define user-based or group-based Time Machine backup quotas. Quotas can be assigned to users and groups that exist locally on the server or within Active Directory. Custom quota settings always override the **Limit users without custom quotas** setting. Custom user quotas always override custom group quotas.

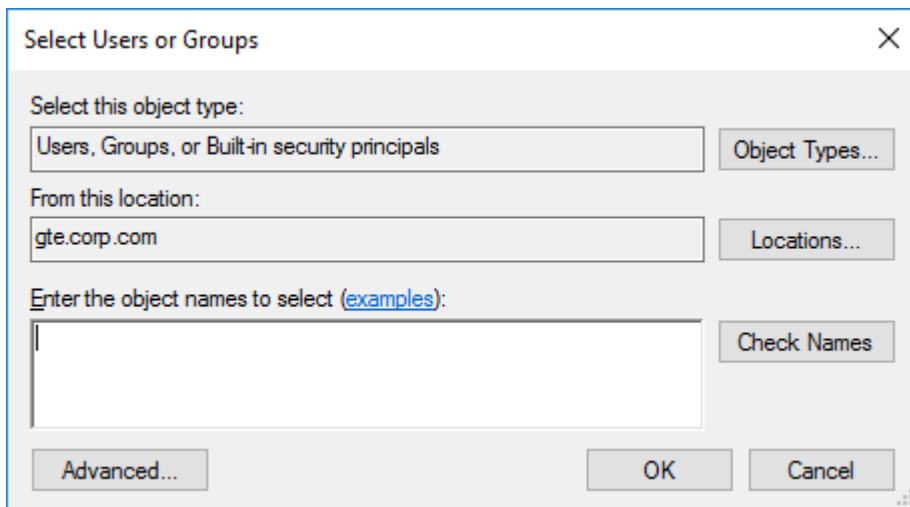
**Setting a custom quota:**

1. Click the **Custom Quotas** button on the **Volume Properties** dialog box to open the **Custom Quotas** window.

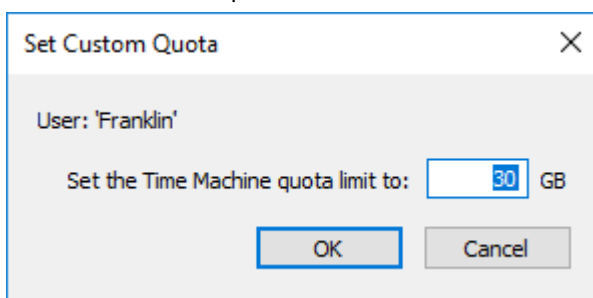


2. Click **Add** to add a new user-based or group-based quota.

- Use the **Select Users or Groups** dialog to choose the users or groups you would like to apply a quota to. You can pick more than one user or group at a time if you would like to set them all to the same quota value.



- Enter the desired quota limit value in GB and click **OK**.



## Using Advanced Volume Properties

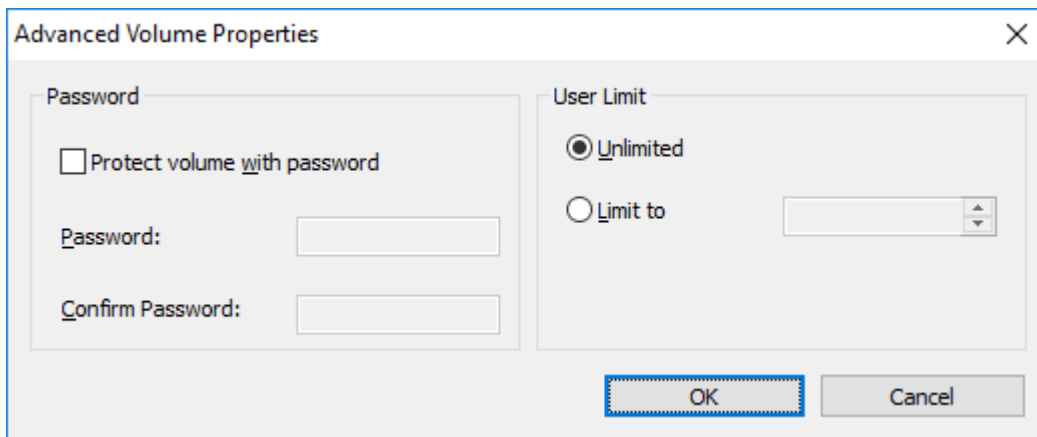
You may require that users enter an additional password, beyond their login password, when they mount volumes. You can configure this setting in the **Advanced Volume Properties** dialog box, where you can also limit the number of users who can simultaneously use a specific volume.

---

### Note

On OS X 10.11 and higher, users cannot enter the password for protected volumes. It is an issue with these OS versions.

---



This feature is disabled by default. To use it, you must enable the **Advanced...** button in the **Volume Properties** window first. To do this:

1. Edit the registry key **ShowVolumePropertiesAdvancedButton**, which is located in HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\NonRefreshable. To enable the button, change the **Value data** of this key to 1. To disable the button, revert the **Value data** to 0.
2. In Windows **Services**, restart the **Acronis Files Connect File and Print Server for Macintosh service**.
3. Restart the **Acronis Files Connect Administrator**.

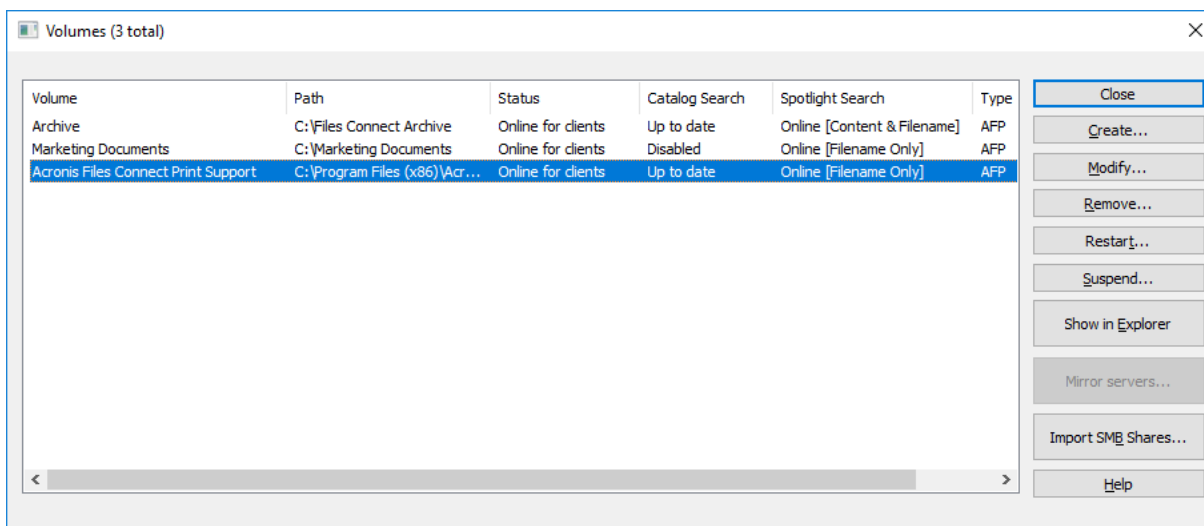
The **Advanced...** will appear in the **Volume properties** window.

## Changing permissions for shared files and folders

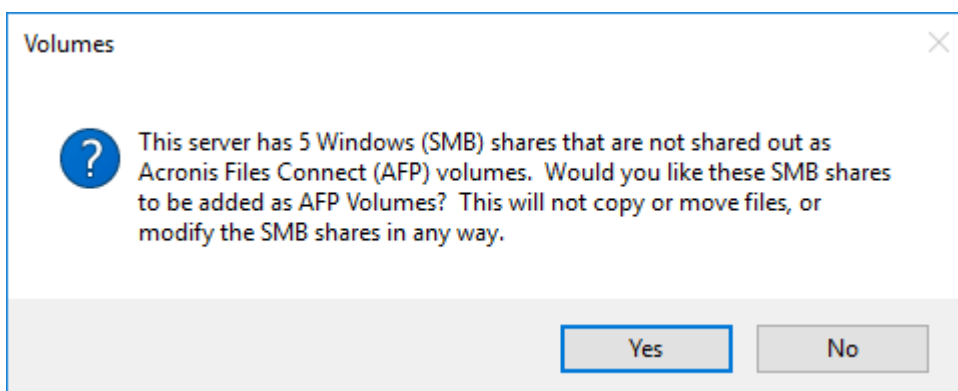
Acronis Files Connect uses the existing Windows user logon and passwords. Unless you enable ACL support, Windows and Mac computers handle folder and file properties differently and not all Windows access information is displayed on the Mac. Because Acronis Files Connect enforces Windows security settings, you should normally use Windows's built-in tools for adjusting directory and file permissions. The standard Windows tools provide the most flexibility for setting up your security policy.

## Importing volumes

Each time you reopen the **Volumes** window, Acronis Files Connect checks for any SMB volumes that are not currently shared as Acronis Files Connect volumes. If such volumes are found, the **Import SMB Shares** button is enabled.



When you click **Import SMB Shares**, you are asked for verification.



Pre-existing SMB shares will become available as Acronis Files Connect volumes. This procedure is the same as that used the first time you launch Acronis Files Connect (see the [Launching Acronis Files Connect For the First Time](#) article).

Because someone could add or remove volumes to the SMB service at any time, when you reopen the Volumes window, note the state of the **Import SMB Shares** button. If it is disabled, no new volumes have been added. If one of the corresponding Acronis Files Connect volumes is removed, the button is enabled.

---

#### Note

This button updates only when the Volumes window is opened. Changes occurring to shares have no effect on the button state while the Volumes window remains opened.

---

## Using mobile access

---

#### Note

For information on how to allow Acronis Cyber Files mobile clients to connect to your Volumes, see [Setting Mobile access](#).

---

## Connecting with a mobile client

To connect to the Gateway server, you have to add it through the mobile app. Once you have done this, you will be able to connect with a single tap.

---

### Note

For more information, see the [Acronis Cyber Files iOS app user guide](#) and the [Acronis Cyber Files Android app user guide](#).

---

## Requirements

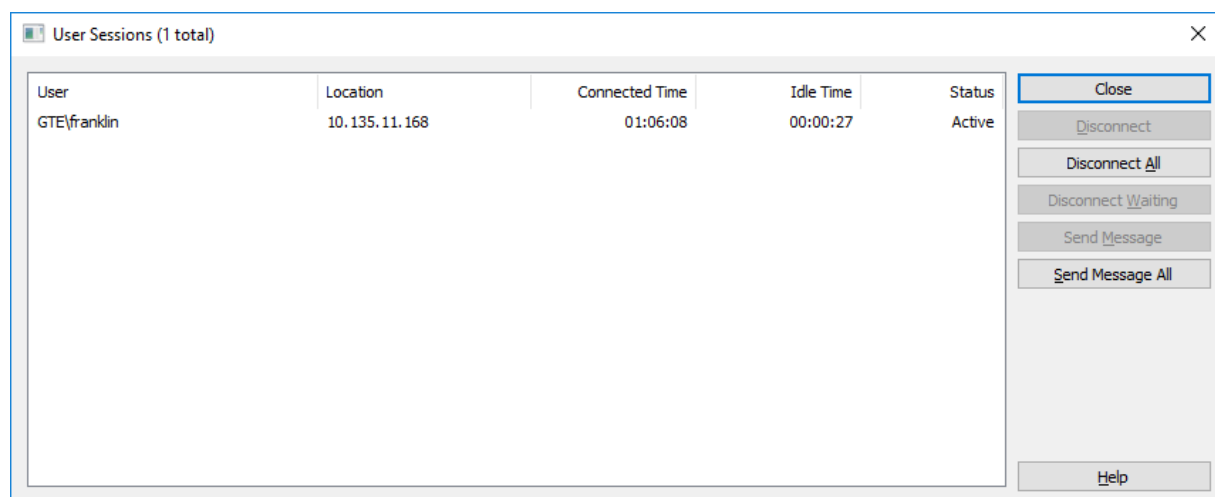
In order to be able to connect to your Acronis Files Connect Volumes via mobile client from outside your company LAN, you need to provide your mobile device(s) with network access to your company's network.

You can do this via VPN, HTTPS Reverse Proxy or opening a firewall port.

## Acronis Files Connect Users

The **Users** dialog box lets you view the users connected to the server, disconnect those users, or send messages to them. For information on user name and password entry, refer to the section [Connecting Mac Users](#). To view the **Users** dialog box, click **Users** on the Acronis Files Connect Administrator window.

Names and IP addresses identify users who are currently connected. Their connection and idle times are given. The dialog refreshes automatically. Click on a column title to sort the list by a column.



The status tells you if the Acronis Files Connect client is idle, sleeping, or being reconnected; see [Reconnecting a Dropped User Session](#).

---

**Note**

User accounts are defined in Windows. Acronis Files Connect uses this information to determine the user access privileges.

---

**Disconnect** – Disconnect a highlighted user or all users.

**Send Message** – Send a message to a highlighted user or all connected users.

---

**Note**

OS X 10.9 or later does not support sending messages.

---

The **Status** column tells you if the connection **Active**, **Sleeping** or **Waiting for Reconnect**.

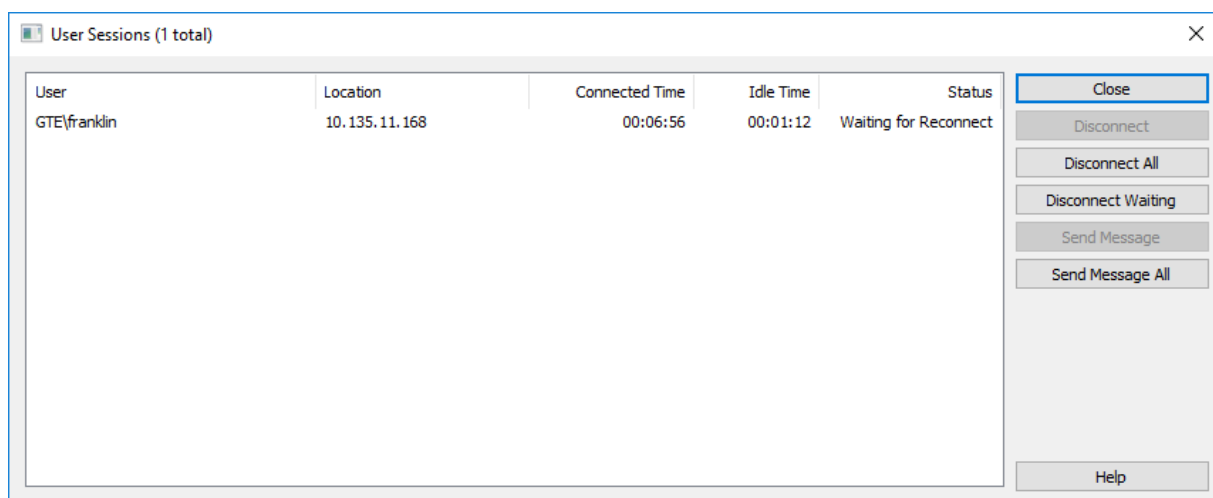
## Connecting Mac users

Acronis Files Connect supports Active Directory. When Mac users connect to the Acronis Files Connect server, they enter their user names and passwords. Acronis Files Connect authenticates this account against the primary domain of the Windows machine that it is running on. If this machine is not a member of a domain, the account must be a member of the local accounts that appear in **Windows User Manager**. If the machine is a member of a domain, then the user name you give the Mac user must be either a member of the primary domain, the local accounts, or a trusted domain.

You may specify to be authenticated against a specific domain by prefixing the user name with the domain name and a backslash (\). For example, to authenticate the user name Joe from the Marketing domain, in the user name portion of your AFP client logon enter `MARKETING\joe`.

## Reconnecting a dropped user session

Acronis Files Connect supports reconnecting user sessions in the event of a temporary network outage. In addition, it supports automatic closing of locked files if the Acronis Files Connect client crashes or reboots.



## Reconnecting if a session is dropped

When macOS X clients connect to Acronis Files Connect, they receive an encrypted reconnect credential. In the event that the connection to the server is broken, Acronis Files Connect keeps the session alive by putting it into **Waiting For Reconnect** mode. While in this mode, all files and volumes opened by the session remain open. When the client machine reestablishes contact with the server, the client (silently) supplies the server with the reconnect credential. Acronis Files Connect decrypts the credential and uses it to authenticate the user.

If the authentication is successful, the client is logged into the server. The computer follows up this login with a request to disconnect its old session. Acronis Files Connect finds the old session, transfers its open files and volumes to the new session, and deletes the old session. The new session has access to the old session's assets. If the old session is no longer available because it timed out or was manually disconnected or because the Acronis Files Connect service restarted or failed over, Acronis Files Connect returns an error to the client when the client tries to disconnect the old session. In this case, the client machine tries to reopen any files and volumes that were open in the old session. Any data written to those files are lost if those data have not yet been flushed to disk.

However, the new session has access to those files automatically. In the event that the Acronis Files Connect Mac client app crashes and reboots while connected to the Acronis Files Connect server, the old session is placed in **Waiting For Reconnect** mode as described above. The next time the Acronis Files Connect Mac client app logs into the server, Acronis Files Connect detects that a client reboot has taken place and automatically disconnects the old session and closes any files that the session had opened. Since the client has rebooted, Acronis Files Connect does not transfer files to the new session; the reboot has wiped away knowledge of the old session from the client. This feature helps alleviate the problem of a client-side crash leaving files open on the server. Sessions remain in a Waiting For Reconnect state for five minutes; then they are automatically disconnected and their open files closed. This reconnect timeout is configurable through a registry setting. You can use the registry keys to affect the way Acronis Files Connect reconnects a session; see [Appendix A: Using the Registry Keys](#).

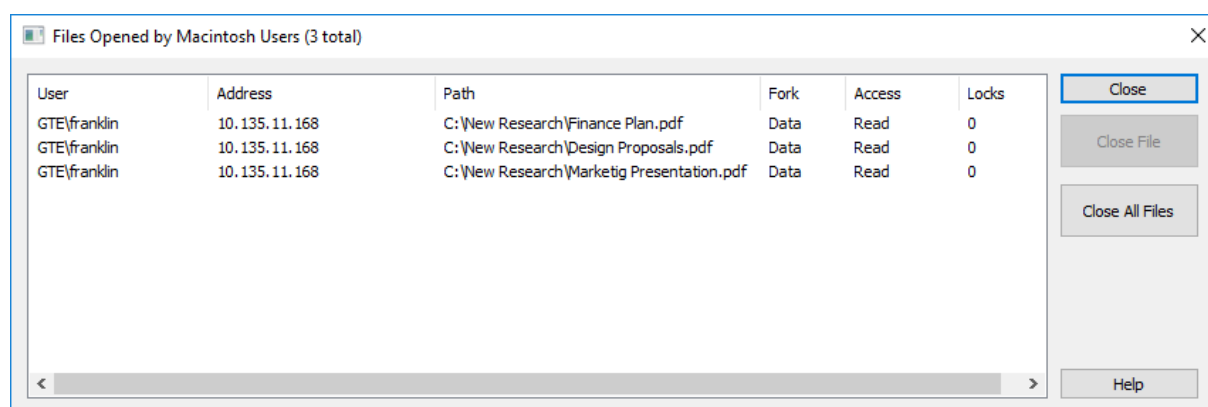
## Reconnecting with Kerberos

Authentication Kerberos is a protocol that provides secure network authentication and support for single sign-on to network resources: see [Using Kerberos](#). Because of limitations in the Windows OS, users that originally logged in using Kerberos authentication cannot reconnect automatically if their old session is no longer available. Therefore, while users logging in with cleartext or DHX-encrypted passwords silently reconnect after a cluster failover, clients logging in with Kerberos may be disconnected.

## Viewing files opened with Acronis Files Connect

The **Files Opened by Mac users** dialog box displays files currently in use. Mac users may open the data or resource fork of a file. To view the **Files Opened by Mac users** dialog box, click the **Files**

button on the **Acronis Files Connect Administrator** dialog box.



The dialog refreshes itself as new files are used by the Mac users.

**The dialog box lists the following information about each file being used:**

- **User** – the name of the Mac user using the file.
- **Address** – the IP Address from which the user is connected.
- **Path** – the name of the file being used.
- **Fork** – the fork being accessed by the user—either the Resource or Data fork.
- **Access** – access information (for example, read access or write access).
- **Locks** – a count for the number of locked sections on a file if a user has locked portions of that file for exclusive access, which happens often for database programs.

---

#### Note

You should use caution when closing a file this way because a user may experience data loss and possibly a crash. Instead, disconnect a user using the Users dialog box; this automatically closes all files opened by that user.

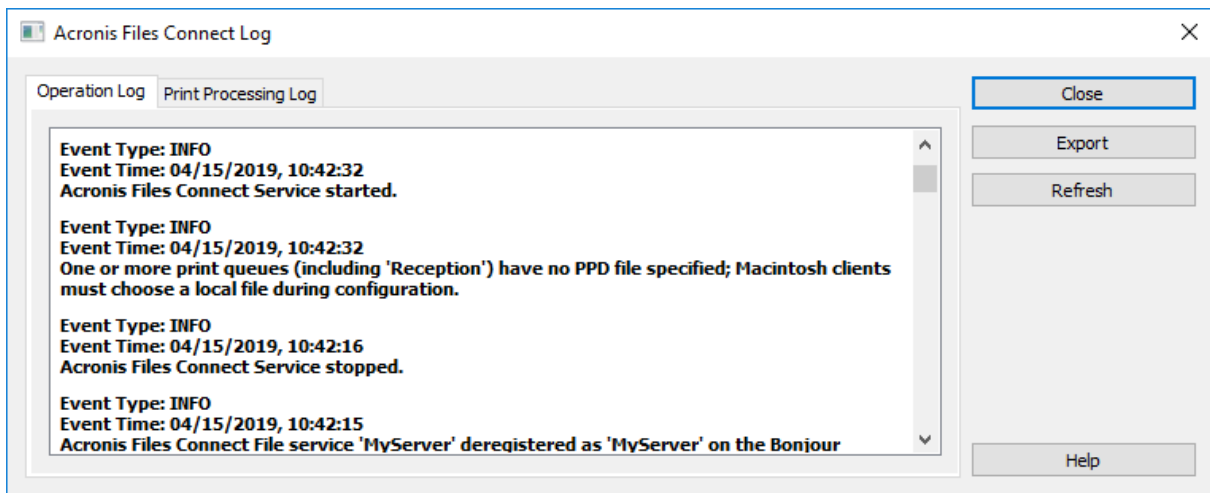
---

## Using the log

### Keeping track of activities with the operation log

The **Acronis Files Connect Administrator** provides a log of the Acronis Files Connect server's activities. The log contains details regarding the connections that have been made along with other operational information. You can export the log to a tab-delimited text file for use in other programs. Once the log is exported to a text file, you can import it into a spreadsheet or system designed to make use of the information.

To view the log, click the **Log** button on the **Acronis Files Connect Administrator** dialog box.



You can view the type of entry, the time the entry was made, and the message about the entry.

## Exporting the operation log

You can export the Log to save it in a text format in two ways:

### To export the log within Acronis Files Connect, do the following:

1. From the Acronis Files Connect **Log** window, click **Export** to save the log as text.
2. Type a name and format.
3. Click **Save** to return to the log.

### To export the log from the command line, do the following:

1. Navigate in a DOS prompt to the folder where Acronis Files Connect is installed.
2. Type `EZIPUTIL PRINT /EXPORT_LOG /PATH:fullpathoflog` where `fullpathoflog` specifies the location and name of the log file that should be exported, such as `C:\Logs\file.txt`. See the included sample batch file `Export_Print_Log.bat` that came with Acronis Files Connect.

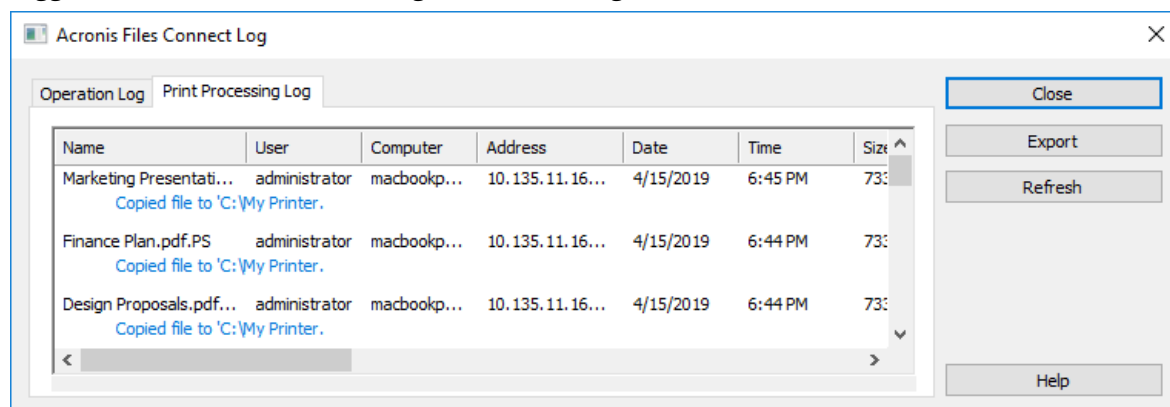
## Using the Print log

You can view a log of Acronis Files Connect activities. The log tells you what jobs have been printed and other information.

### To view the log, do the following:

1. Click **Log** on the **Acronis Files Connect Administrator** dialog box.
2. Click the **Print Processing Log** tab to display it. The **Print Processing Log** contains standard printing information. You can sort the log by any column by clicking on the column title. To

toggle the sort between ascending and descending, click the column title a second time.



Using the registry keys, you can add each new print log entry to a specified text file automatically. See Appendix A: "Using the Registry Keys" [here](#).

## Customizing Acronis Files Connect Print Processing Log columns

You can use registry keys to override the default configuration and customize your view of the [Print Processing Log](#) to display various columns in any order. Use the IP Printing format for regular Acronis Files Connect print support.

## Exporting the print log from Acronis Files Connect

You can export either log in a tab-delimited text file for use in other programs. Once the log is exported to a text file, you can import it to a spreadsheet or system designed to make use of the information.

### To export the log using the Export button, do the following:

1. Access the Acronis Files Connect Log dialog in the Acronis Files Connect Administrator.
2. To export a log, display its tab—**Print Processing** or **Operation**—and click **Export**.
3. Click **Save** to save the log. If you export the printing jobs, the file is named Acronis Files Connect Print Jobs.txt.
4. Click **Close** to return to the Acronis Files Connect Administrator.

### To export either log using the command line, do the following:

1. Navigate in a command prompt to the folder where Acronis Files Connect is installed.
2. Type `EZIPUTIL PRINT /EXPORT_LOG /PATH:fullpathoflog` where 'fullpathoflog' specifies the location and name of the log file that should be exported. See the included sample batch file `Export_Print_Log.bat` that came with Acronis Files Connect.

## Using the Acronis Files Connect Print server

The Acronis Files Connect Print Server supports IP-based printing from Mac computers. Mac users set up printers using Bonjour or the Print Center. Mac OS 9 clients set up printers using the **Chooser**

or **Choose IP Printer**, an Apple menu item.

In addition to these printing capabilities, your Mac users can access shared volumes as described in the **Acronis Files Connect File Server** chapter.

## How the Print server works

After receiving a print job from a Mac, Acronis Files Connect uses one of several processing methods. These include Windows print queues, LPR printers and 'hot folders'—special output directories where additional software, such as a RIP or OPI server, can process the job. In addition, you can view the print jobs in progress, speed or delay processing of jobs, and delete jobs from the list. Mac users can print to the Acronis Files Connect Print Server by means of IP usage.

The Acronis Files Connect Print Server logs many aspects of the print jobs that your users send to the server—job name, name of the user that sent the job, time and date of printing, page size, number of pages, size of job in bytes, address of the computer that printed the job, and the name of the print queue used. You can export this log automatically to a text file that can be imported into an accounting or other cost-tracking system.

## Setting up print queues

A print queue is a virtual printer that Mac users can access. When Mac users print files to one of your printers, the resulting print job is delivered to your server and can be tracked and processed there. Read the section on creating print queues, then read the specific section on the following paragraphs to configure specific settings for the four types of print queues: Windows, LPR and Directory (Hot Folder).

## Creating a print queue

### ***To create a print queue***

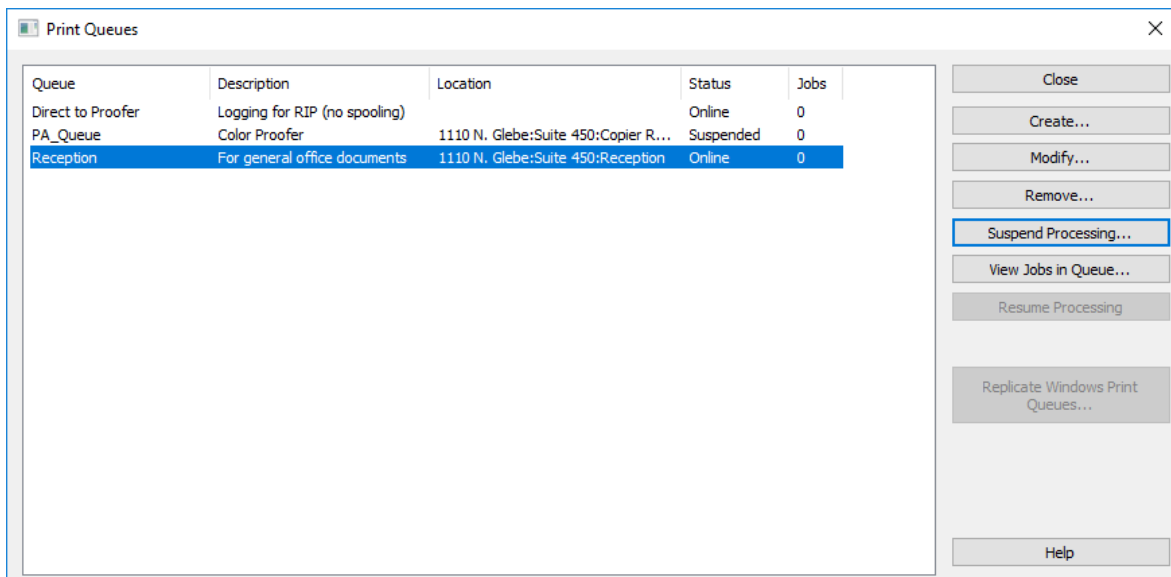
1. In the **Acronis Files Connect Administrator** dialog box, click **Print Queues**.

---

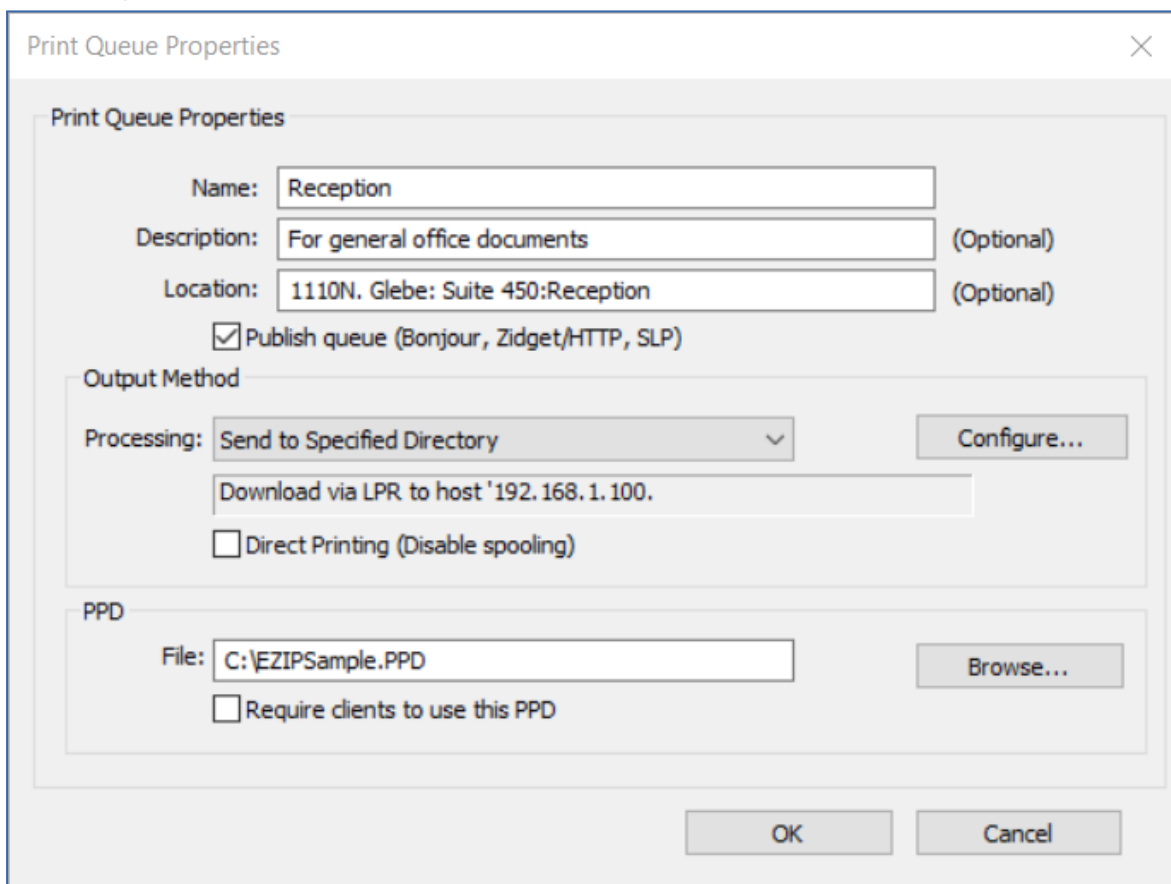
#### **Note**

Click a column title to sort the list of print queues.

---



2. Click **Create** to define a print queue. When a queue is suspended, jobs are accepted by the server. However, they are not sent to the printer until processing is resumed. Create print queues. Open a window with a list of the pending jobs. From there you can start, stop, or reorder the print jobs. Takes the existing Windows print queues and republishes them as Acronis Files Connect queues as well.



3. Provide a name for the print queue.
4. [Optional] Provide a description for the print queue.

5. [Optional] Specify a location.
6. Choose a processing method.

---

**Note**

For instructions on each method, see [Setting up processing methods](#).

---

7. Associate a PPD file with the queue.

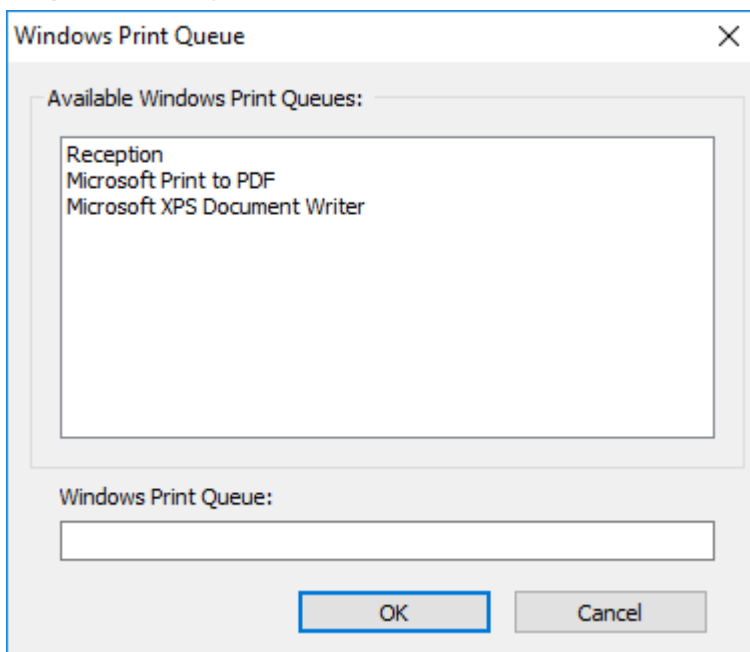
## Setting up processing methods

When Acronis Files Connect receives a job from a client, it can output the job to a Windows print queue, an LPR printer or a directory. The following section describes how to configure each of these methods.

### Sending to a Windows print queue

**To select a Windows print queue for your processing method, do the following:**

1. Select **Send to Windows Print Queue** on the **Processing** pull down menu of the **Print Queue Properties** dialog box.



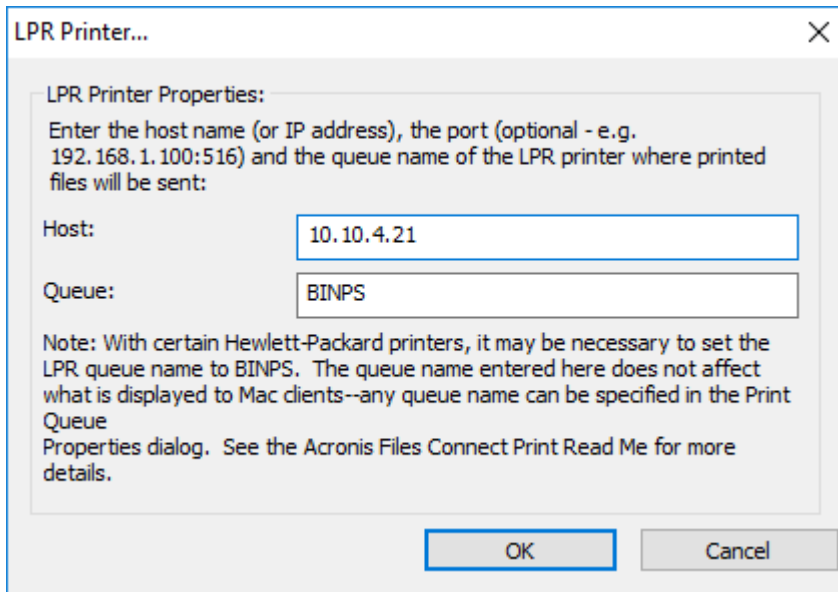
You see a list of Windows printers that you have already shared for Windows clients on the server. The PPD to be used by clients when printing to this queue. The name that you will see when you print from a Mac. Where Acronis Files Connect will send the jobs after they are received. Request from the Mac user to supply job-tracking information every time they print to this queue (refer to the Acronis Files Connect manual for additional configuration). Whether the print queue should be discoverable by clients.

2. Select a printer. If this list is empty, you must create a Windows printer from the Windows Print Wizard and set it to be shared.

## Sending to an LPR printer queue

**To select an LPR printer for your processing method, do the following:**

1. In the **Processing** pull down menu of the **Print Queue Properties** dialog box, select **Send to LPR Print Queue**.
2. Type a name for the print queue you are setting up. Queue names must be unique; you cannot have two queues with the same name. See the section Controlling printing with an LPR printer for information about controlling the LPR print queue.



## Sending to a specified directory (Hot folder)

You can create a print queue that sends files to a specified directory or hot folder. You can choose a local folder or one from the network. For network locations you use a UNC path.

---

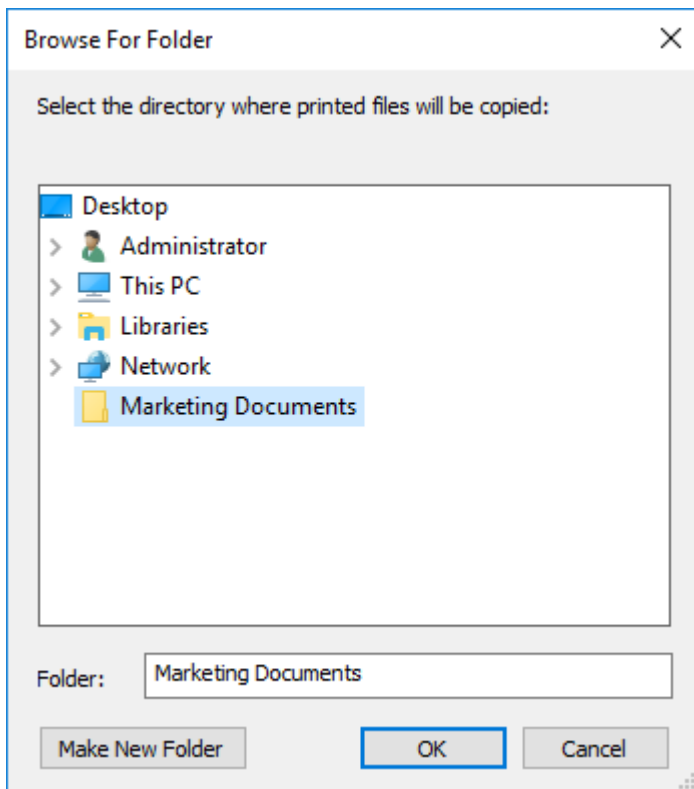
### Note

If you select a network location, the Computer account for the server in Active Directory must be given access to the network location on the remote server. Giving a computer account access to a folder is performed the same way as giving a User account access to a folder.

---

**To use a specified directory as your processing method, perform the following:**

1. Select **Send to Specified Directory** in the **Processing** pull down menu of the **Print Queue Properties** dialog box.



2. Use the **Browse for Folder** dialog to locate and select the directory.
3. Click **OK**.

## Associating a PPD File with a print queue

You may associate a PostScript Printer Description (PPD) with each queue. PPDs are used on the Macintosh when creating printers. If you provide a PPD file for the print queue, Mac users can download and configure the printer for use on their desktops without having a PPD already installed on their machines.

The Acronis Files Connect server includes an option that automatically downloads the specified PPD to Mac users when they create printers. You should obtain and use PPD files that were created on a Mac, since they include additional information such as special icons to deliver the user experience that Mac users expect. Specifying a PPD when you set up a queue makes it available for download, but its presence on the server does not affect printing.

To associate a PPD file with a print queue, enter the path to the PPD file in the PPD section of the **Print Queue Properties** dialog box or use the **Browse** button to locate the correct PPD

---

### Note

These files must be on a disk accessible by the server.

---

## Controlling the processing of jobs

You can control the processing of jobs that Mac users send to the Acronis Files Connect server. On the **Print Queues** dialog, you can do the following:

- view the status of each job in the queue in the Status column.
- suspend processing of all jobs in a print queue and a particular job in a print queue.
- resume processing when you want.
- control which jobs are processed first.
- delete jobs.

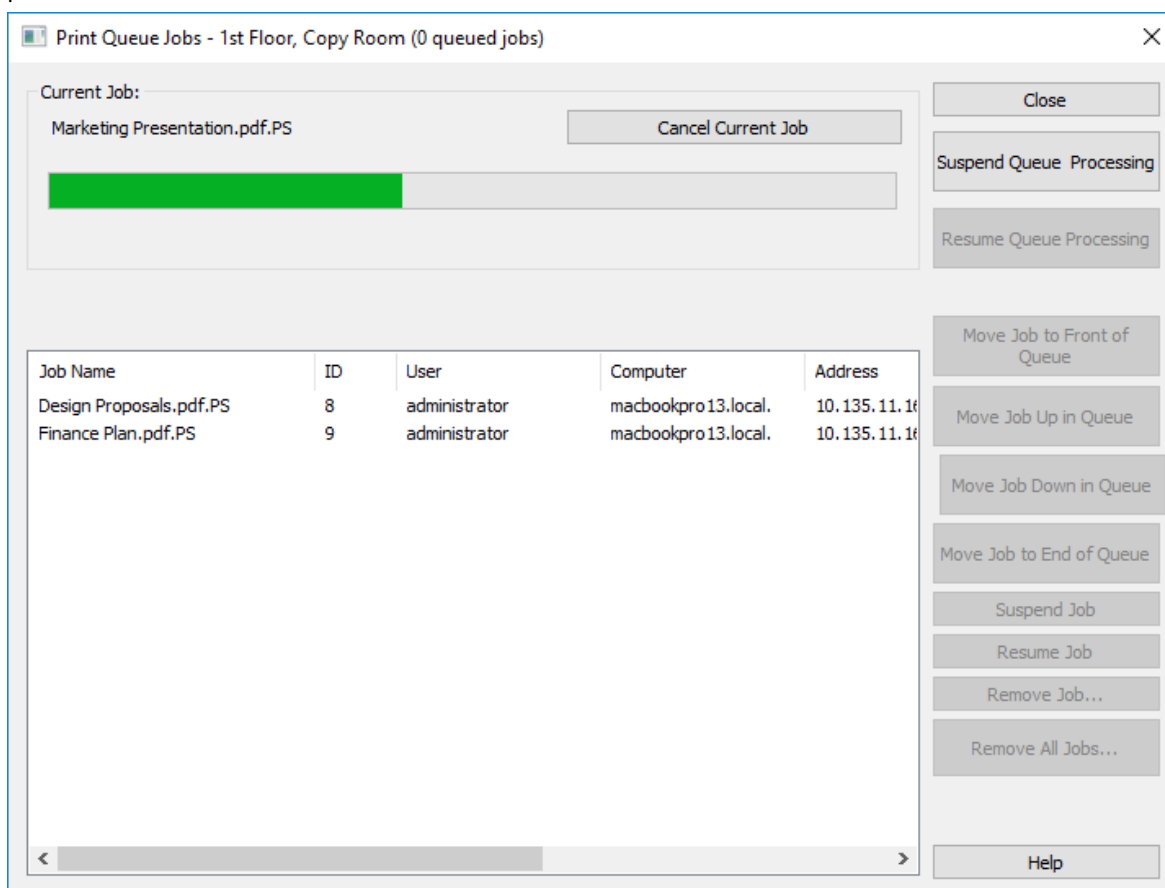
To access the Print Queues dialog, click **Print Queues** on the **Acronis Files Connect Administrator** window. This dialog lists the print queues available to Mac users.

## Viewing and managing print jobs

You can view and manage jobs being processed in the **Print Queue Jobs** dialog box for one or more print queues at the same time.

**To view a list of the jobs being processed in a print queue, do the following:**

1. Highlight a print queue in the **Print Queue** dialog box.
2. Click **View Jobs in Queue**. The **Print Queue Jobs** dialog box lists the jobs being processed. When a job is being processed, you see the progress indicator and the name of the job being processed.



## Publishing a print queue

Acronis Files Connect Print Server advertises all print queues automatically over Bonjour, HTTP and AFP. Mac users can set up and print to Bonjour printers in a single step. Once you select a printer using any of these methods, it is available as an installed printer in the print dialog. You do not have to set up your printer each time you want to print to it. You can disable the automatic advertisement of printers over Bonjour, HTTP and AFP globally for the entire server or on a queue-by-queue basis.

### **To disable any advertisement protocol, do the following:**

1. From the **Acronis Files Connect Administrator**, click **Settings**.
2. On the **Settings** dialog box, click the **Service Discovery** tab.
3. Disable the services you do not want to use; see the [Service Discovery](#) article. You can also disable publishing a specific queue so that only people who know the queue exists can use it.

# Backup and recovery

---

## Warning!

This procedure works only if you backup and recover the same version. For example, if you backup 10.6.1 and install 10.6.1 again, you can use the recovery, but if you install 10.6.3 you won't be able to use this method.

---

## Backup

### To backup your current Acronis Files Connect setup, you must do the following:

1. Open the registry editor (Open a command prompt and type **regedit**).
2. Navigate to: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ExtremeZ-IP\
3. Right click on the ExtremeZ-IP folder and press **Export**.
4. Store the registry backup on a safe location (on another machine, a flash drive, etc.) in case the server fails.
5. Backup all shared folders (copy them on another machine, etc.)
6. If you have a license key, write it down. You can find the key by pressing the **Licensing** button on the Acronis Files Connect Administrator.

### To backup your current Acronis Files Connect clustered setup, you must do the following:

1. Open the registry editor (Open a command prompt and type **regedit**).
2. Navigate to: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\`<instance>`

---

#### Note

`<instance>` should be replaced by the name of your clustered Acronis Files Connect instance on the current server.

---

3. Right click on the `<instance>` folder and press **Export**.
4. Store the registry backup on a safe location (on another machine, a flash drive, etc.) in case the server fails.
5. Backup all shared folders (copy them on another machine, etc.)
6. If you have a license key, write it down. You can find the key by pressing the **Licensing** button on the Acronis Files Connect Administrator.

## Recovery

### To recover your settings:

1. Import the registry backup(s) to the registry.
2. Paste the folders you previously had shared (or create them again – in the same place and with the same permissions as the old ones).

3. Install a fresh copy of Acronis Files Connect, using the same version you had before.
4. Enter your license key.

# Appendices

## Appendix A: Using the Registry keys

You can use Windows registry keys to change some settings in Acronis Files Connect beyond what can be configured using the Acronis Files Connect Administrator.

The registry settings for the Acronis Files Connect service are located in the `\HKLM\System\CurrentControlSet\Services\ExtremeZ-IP\` section of the registry. In the examples below this will be abbreviated as `...\RegistryKeyName`. There are two main kinds of registry keys; refreshable and nonrefreshable. Refreshable keys take effect when you click the Refresh Registry button in the Acronis Files Connect Administrator. Nonrefreshable keys on the other hand will not take effect until the service is restarted.

### Reconnecting a dropped session

Acronis Files Connect supports reconnecting user sessions in the event of a network outage, server crash, or cluster failover. In addition, it supports automatically closing locked files if the Acronis Files Connect client crashes or reboots.

**You can use the following registry keys to affect the way Acronis Files Connect reconnects after a session is disconnected:**

`...\Parameters4\Refreshable\`

- `ServerSupportsReconnectUAM`
- `ReconnectTimeout`
- `ServerSupportsAFP3Reconnect`
- `ReconnectServerKeyLifetime`
- `ServerEmbedsPasswordInReconnectCredential`
- `MaxDuplicateSessionsWaiting`
- `ReconnectUAMExpirationInterval`

### Sending password expiration notifications during session

In addition to notifying Mac users that their password is expiring at initial login, Acronis Files Connect can also be configured to notify users during their session. Notification during a session requires that notification at initial login is enabled.

---

#### Note

macOS 10.9 and later do not support sending messages. If you are using macOS 10.9 or later, the following configuration will not take effect.

---

For supported macOS versions, you can configure session-based password expiration notifications as follows:

Select the **Notify Mac users of password expiration** option on the **Security** tab of the **Settings** dialog in the **Acronis Files Connect Administrator**. Here, you will also specify the number of days from expiration that the notification should begin.

Next, you will edit the registry key named **PasswordExpirationReminderInterval** in:

```
...\Parameters4\Refreshable\
```

The value of this registry key determines the interval at which the client is notified of the upcoming password expiration in minutes. The interval can be configured from 1 minute to 1440 minutes (1 day).

## Scheduling re-indexing with EZIPUTIL

By default, Acronis Files Connect automatically re-indexes file entries for its indexed search. You can also use EZIPUTIL in a batch file or script to schedule re-indexing on a set schedule during off-hours and trigger it with a scheduling service of your choice. For more information about this tool, please refer to the [EZIPUTIL command line section](#).

1. First, disable automatic re-indexing by removing the selecting the **Automatically rebuild sparse indexes** check box found in the **Search Settings** dialog box (For more information, please refer to the Settings section).
2. EZIPUTIL.exe is located in the chosen Acronis Files Connect program installation directory on the server. Use the following command, which is included in the EZIPUTIL utility, to trigger the re-indexing of a volume manually.

You can also use it in a script or batch file to schedule re-indexing during off-hours:

```
EZIPUTIL VOLUME /REINDEX /NAME:volumename /PATH:root directory path  
[/SERVICENAME:servicename]
```

**SERVICENAME** is needed only if Acronis Files Connect is running on a cluster.

## Adding print log entries to text files

To configure the Acronis Files Connect server to add each new print log entry to a specified text file automatically, do the following.

```
..\Parameters4\PrintRefreshable
```

1. Modify the PrintAccountingLogFilePath in the registry.
2. Set the value to the full path where you want the logs (for example, C:\Logs\Log.txt)

## Customizing Acronis Files Connect Print Processing Log columns

You can use registry keys to override the default configuration and customize your view of the [Print Processing Log](#) to display various columns in any order. Use the IP Printing format for regular Acronis Files Connect print support.

## Columns

A REG\_SZ string entry in the registry controls custom configuration. The format for the string is to add types of data separated by a forward slash '/'. The format respects the order and number of types in the string value.

For example, if you wanted to restrict your view to job\_name, job\_dateandtime, and job\_printer only, you would enter 'job\_name/job\_dateandtime/job\_printer' as your string value.

- **job\_id** - a unique ID generated by Acronis Files Connect for this print job
- **job\_name** - name of the file being printed
- **job\_user** - name of user generating the print job
- **job\_ip** - IP address of computer that submitted the print job
- **job\_datetime** - month/day/year and time of day job was submitted
- **job\_size** - size of the file being printed
- **job\_pagecount** - number of pages in the print job
- **job\_pagesize** - the type of paper the job is being printed on
- **job\_numcopies** - number of copies in this print job
- **job\_queue** - name of the print queue that is processing the print job
- **job\_printer** - name of the printer processing the print job
- **job\_date** - month/day/year of submitted print job
- **job\_time** - time of day job was submitted
- **job\_imagesize** - dimensions in pixels of submitted print job

By default, Acronis Files Connect has a specific column order. If no registry key is present, that order will be used. The following examples illustrate keys that would set up the default columns. They can be used as a starting point for customization. ...Parameters4 \PrintRefreshable

**Type:** REG\_SZ

**Data**(by default): job\_name/job\_user/job\_host/job\_ip/job\_date/job\_time/job\_size/job\_pagecount/job\_pagesize/job\_imagesize/job\_numcopies/job\_queue/job\_printer/job\_code1/job\_code2/job\_code3/job\_code4/job\_code5

## Appendix B: Monitoring Acronis Files Connect

Acronis Files Connect allows administrators and Acronis' support staff to 'look inside' Acronis Files Connect to monitor the load on the server, detect problems with shares and print queues, and diagnose performance bottlenecks. Acronis Files Connect supports counters for Windows Performance Monitor, Microsoft Operations Manager (MOM), and other instrumentation platforms that support Windows Management Interface (WMI), Microsoft's generic interface for monitoring applications in production. WMI-aware applications alert administrators to errors and help diagnose problems.

Most of the counters provided in Acronis Files Connect are global for the Acronis Files Connect

instance or the server. For some of the users and volume counters, however, an administrator can choose to view a single instance. For example, 'instance' could be the number of bytes per second for an individual user.

Acronis Files Connect performance counters are compatible with Windows Server 2016, Windows Server 2019, and Windows Server 2022.

## Counters for Acronis Files Connect File server

- **Users (Total)** - The number of currently-connected users, including users that are idle or sleeping
- **Users (Idle)** - The number of currently-connected users that have been idle for at least 10 minutes
- **Users (Sleeping)** - The number of currently-connected users that are sleeping
- **Users (Active)** - The number of currently-connected users that are active (neither idle or sleeping)
- **Users (Waiting For Reconnect)** - The number of sessions representing connections that have been terminated but are waiting for users to reconnect
- **AFPCommands Replied To** - The number of AFP commands replied to
- **AFP Commands Replied To/sec** - The number of AFP commands replied to per second
- **Volumes (Total)** - The number of Acronis Files Connect volumes
- **Volumes (Offline)** - The number of Acronis Files Connect volumes that are currently offline
- **Volumes (Online)** - The number of Acronis Files Connect volumes that are currently online
- **User Disconnects** - The number of times users have disconnected from the server in an ungraceful manner
- **Failed Logons** - The number of times users have failed to login because of an invalid password, username or Kerberos ticket
- **Reconnects** - The number of times users have reconnected to the server
- **Max Files Open** - The maximum number of file forks that have been open at any one time
- **Max File Locks** - The maximum number of files locks that have been in place at any one time
- **Max Users (Active)** - The maximum number of users that have been active at any one time
- **Max Users (Idle)** - The maximum number of users that have been idle at any one time
- **Max Users (Sleeping)** - The maximum number of users that have been sleeping at any one time
- **Max Users (Total)** - The maximum number of users logged-in at any one time
- **Max Users (Waiting For Reconnect)** - The maximum number of sessions waiting for users to reconnect at any one time
- **Thread Pool Size** - The total number of threads that are in the thread pool
- **Thread Pool (Working)** - The number of threads in the thread pool that were actively working at the time of sampling
- **Thread Pool (Quiet)** - The number of threads in the thread pool that have not done any work in over a minute

- **Thread Pool (Stalled)** - The number of threads in the thread pool that have been processing a task for more than one minute
- **Max Thread Pool Size** - The maximum number of threads in the thread pool at any one time
- **Max Thread Pool (Working)** - The maximum number of threads in the thread pool that were actively working during any sample
- **User Licenses Used** - The current number of user licenses being used

## Counters for Acronis Files Connect File server users

- **Open Forks** – Number of open forks
- **File Locks** – Number of file locks
- **Bytes Received/sec** – Number of bytes read from the network per second
- **Bytes Transmitted/sec** – Number of bytes sent on the network per second
- **Commands received/sec** – Number of commands received by the server per second
- **Commands processed/sec** – Number of commands processed by the server per second

---

### Note

Users' counters can be viewed as an individual user or as a total of all activity.

---

## Counters for Acronis Files Connect File server volumes

- **Cache Hit Rate** - The node table cache hit rate
- **Bytes Read/sec** - Number of bytes read from disk per second and returned to clients
- **Bytes Written/sec** - Number of bytes written from disk per second

---

### Note

Volume counters can be viewed per volume or as a total.

---

## Counters for Acronis Files Connect Printing

- **Print Queues** - The number of print queues
- **Print Queues Online** - The number of print queues currently online
- **Print Queues Offline** - The number of print queues currently offline
- **Jobs Spooling** - Current number of print jobs spooling
- **Bytes Printed/sec** - The number of bytes printed per second

## Counters for Acronis Files Connect Print queues

- **Print Jobs Offline** - The number of print jobs currently offline
- **Job Errors** - The number of print errors since Acronis Files Connect launch
- **Total Jobs Printed** - The total number of jobs printed since Acronis Files Connect launch
- **Total Pages Printed** - The total number of pages printed since Acronis Files Connect launch
- **Is Queue Online** - Indication if the queue is online - 1 if yes, 0 if no

---

**Note**

Print Queue counters can be viewed per queue or as a total for all queues.

---

# Supplemental material

## TCP/IP ports

Acronis Files Connect uses the following TCP/IP ports

- 
- **TCP** port **443** (default) – TCP/IP Port for Acronis Files Connect Mobile app Connections.
- **TCP** port **311** (default) – TCP/IP Port for Time Machine.
- **TCP** Port **548** (default) – TCP/IP Port for AFP Connections.
- **TCP** Port **8081** (default) – TCP/IP Port for Print Configuration.
- **TCP** Port **8081** (default) – HTTP TCP/IP Port for client web services.
- **TCP** Port **8085** (default) – HTTPS TCP/IP Port for client web services.
- **TCP** Port **515** (default) – TCP/IP Port for Print Jobs.
- **TCP & UDP** Port 5353\* – Bonjour.
- **TCP & UDP** Port 5353\* – Bonjour (large data return).

---

### Note

\*Both port types must be added.

---

### Note

Bonjour ports are only necessary if you choose to install Apple Bonjour. For more information on the feature, refer to the "Bonjour" (p. 67).

---

## Additional AFP port notes

If another AFP server is already running on port 548 when Acronis Files Connect is installed, Acronis Files Connect will use the next available port, which will usually be 549. A Mac machine will, by default, connect to AFP volumes on port 548.

It is possible to connect to a shared volume on another port by specifying the port as part of the server address. For example, you can connect to an AFP server running on port 549 by specifying "fileserver.example.com:549" in the macOS **Connect to Server...** dialog.

When Acronis Files Connect is running on a port other than 548, a warning notice will be displayed in the main Acronis Files Connect Administrator window.

## Acronis Files Connect compatibility information

### Support for Microsoft Networking Domains

- Acronis Files Connect supports Microsoft Active Directory. When you connect to an Acronis Files Connect server from the Mac, you normally enter your user name and password. Acronis Files

Connect will authenticate this account against the primary domain of the Windows machine that it is running on. If this machine is not a member of a domain, then the account must be a member of the local accounts that appear in User Manager. If the machine is a member of a domain, then the user name you supply can be either a member of the primary domain, the local accounts or a trusted domain.

- You may specify to be authenticated against a specific domain by prefixing the user name with the domain name and a backslash ('\'). For example, to authenticate using the account "rob" from the "MARKETING" domain, you would enter "MARKETING\rob" in the user name portion of your AFP client logon.
- Acronis Files Connect uses the same technique for accessing owners and groups for folders in the sharing information using the Finder.

## Windows Registry Keys

Certain advanced features and debug options can be configured through the Windows Registry. It is recommended that only advanced users make these configurations.

---

### Note

Unless otherwise specified, all of the following registry keys are of type **DWORD**.

---

Most of the following parameters are on/off: value of 1 enables the particular feature, while value of 0 disables it. If the registry key does not already exist, create a new DWORD key and set it to the appropriate value.

Certain keys are *refreshable* – their state can be changed while the Acronis Files Connect service is running.

Refreshable keys take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

In order to take effect, non-refreshable keys require that the Acronis Files Connect service is restarted .

The keys are organized into the following sections:

### General parameter registry keys – non-refreshable

The following keys control certain features or behaviors of Acronis Files Connect.

The keys in this section are non-refreshable. In order to take effect, they require that the Acronis Files Connect service is restarted.

Registry location:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\NonRefreshable
```

## ActiveDirectoryComputers

- **Description:** When configuring Acronis Files Connect to support Kerberos constrained delegation for network reshare volumes, if the computer object for the server that is running Acronis Files Connect is not located in the default '**Computers**' container in Active Directory, it is necessary to edit this registry key so that Acronis Files Connect can construct the correct distinguished name for the server's computer object.

The Acronis Files Connect service can identify the server common name (**CN**) and the domain component (**DC**) segments of the distinguished name, so the **ActiveDirectoryComputers** registry key is where the custom organizational unit (**OU**) segments of the distinguished name can be entered.

---

### Note

**For example:** If the canonical name of the **Acronis Files Connect** server's computer object is: `yourdomain.com/Marketing/3rdFloor/importantComputer`

The distinguished name would be:

`CN=importantComputer,OU=3rdFloor,OU=Marketing,DC=yourdomain,DC=com`

Since Acronis Files Connect can identify the `CN=importantComputer` and `DC=yourdomain,DC=com` segments, only the `OU=3rdFloor` and `OU=Marketing` segments would need to be added.

In this example, it would be necessary to set the value of the **ActiveDirectoryComputers** registry key to '`OU=3rdFloor,OU=Marketing`' (without the quotes) in order for the Acronis Files Connect service to work with the `importantComputer` computer object.

---

- **Default:**
- **Type:** String
- **Refreshable:** No

## AllowNonIndexedSearches

- **Description:** Specifies whether or not the server allows searches that do not contain "name" as one of the criteria. These searches can be very slow and can cause the server to use a great deal of CPU while the search is occurring. Turning this key off will cause the server to reject search requests that don't include "name" as one of the criteria, and the server will send appropriate warning messages to the user attempting to perform these types of searches.
- **Default:** On
- **Refreshable:** No

## CheckNtfsLastAccessUpdate

- **Description:** Whether or not the server checks the status of the `NtfsDisableLastAccessUpdate` Windows registry setting when the server starts up. If this key is enabled and `NtfsDisableLastAccessUpdate` is off, Acronis Files Connect will log a warning to the Windows Event Log.

- **Default:** On
- **Refreshable:** No

## ClientDisconnectAtShutdownTime

- **Description:** Specifies the number of seconds the server will wait for an unresponsive client to disconnect at server shutdown before ungracefully terminating the connection. Note: this value must be greater than ClientDisconnectTime.
- **Default:** 35
- **Refreshable:** No

## ClientDisconnectTime

- **Description:** Specifies the number of seconds the server will wait for an unresponsive client to disconnect before ungracefully terminating the connection.
- **Default:** 30
- **Refreshable:** No

## CreateCrashDumps

- **Description:** Whether or not the server attempts to create crash dump files in the application directory if a service crash is detected.
- **Default:** On
- **Refreshable:** No

## CreatePrecomposedMacRoman

- **Description:** Controls whether Acronis Files Connect converts OS X MacRoman filenames into precomposed Unicode on the server. Enabling this feature will allow MacRoman files to be displayed normally in Windows Explorer, and will allow for compatibility with third party applications such as Adobe Acrobat Distiller.
- **Default:** Off
- **Refreshable:** No

## DebugLogFolder

- **Description:** File Server will write the Acronis Files Connect Log to this folder.
- **Refreshable:** No

## DisconnectStalledSession

- **Description:** Whether or not stalled sessions will be automatically disconnected.
- **Default:** Yes
- **Refreshable:** No



## IPv6Enabled

- **Description:** Enables support for IPv6 connection for both AFP & LPR when IPv6 stack is installed on the server.
- **Default:** On
- **Refreshable:** No

## IPv6Strict

- **Description:** Controls protection level on IPv6 connection. The valid values are 10 (unrestricted), 20 (default), and 30 (strict). If the value is set to 30 (strict), only same site local IPv6 address can be connected. If the value is set to 20 (default), both same site local & external IPv6 addresses can be connected. If set to 10 (unrestricted), any IPv6 addresses can be connected including Teredo NAT Traversal address.
- **Default:** 20
- **Refreshable:** No

## LogMemorySettingsNotOptimized

- **Description:** Controls whether Acronis Files Connect logs messages "Memory settings for this server are not optimized correctly".
- **Default:** On
- **Refreshable:** No

## MaxOutstandingTickles

- **Description:** The maximum number of tickles the client can fail to respond to before the server terminates the connection.
- **Default:** 5
- **Refreshable:** No

## MaxSearchIndexSize

- **Description:** Maximum amount of RAM available for indexed search caching in Megabytes. For maximum search performance, assuming available system RAM, this is best set to be equal to or greater than total size of all search index files on the server. An index file containing 1 million files should be about 32 MB in size. Note that this setting is a maximum RAM cap. If your server only contains 20 MB of index files, Acronis Files Connect search will only use 20 MB of RAM, even if this is left at the default 200 MB setting.
- **Default:** 200
- **Refreshable:** No

## MaxUnflushedIDs

- **Description:** The number of unflushed ID/index pairs that can be saved in memory before a flush is forced.
- **Default:** 60
- **Refreshable:** No

## PerformanceCounters

- **Description:** The Windows performance counters that are outputted to the log each time Acronis Files Connect logs performance data. This multi-string can contain multiple lines, where each line is <description>,<counter path>. The keyword "Backup & Recovery Online" can be specified in the counter path - this will be replaced by whatever the service name is. Note that the values entered into this setting replace the default counters.
- **Default:**  
"ZIP CPU Usage", "\Process(Backup & Recovery Online)\% Processor Time"  
"Handles", "\Process(Backup & Recovery Online)\Handle Count"  
"Threads", "\Process(Backup & Recovery Online)\Thread Count"  
"Pool Paged Bytes", "\Memory\Pool Paged Bytes"  
"Pool Nonpaged Bytes", "\Memory\Pool Nonpaged Bytes"  
"Page Faults/sec", "\Process(Backup & Recovery Online)\Page Faults/sec"
- **Refreshable:** No

## RenameLogAtStartup

- **Description:** Acronis Files Connect Debug Log will be renamed (saved off) at every service startup.
- **Default:** 1
- **Refreshable:** No

## RespondsToTicks

- **Description:** Whether or not the server responds to a tickle from the client with another tickle.
- **Default:** Off
- **Refreshable:** No

## ServerLogsPerformanceStats

- **Description:** Specifies whether or not the server loads the performance data helper DLL at startup and uses that DLL to output performance statistics to the log. Disabling this feature (which is enabled by default) can address rare issues where Acronis Files Connect hangs at startup when trying to load the PDH.dll.

- **Default:** On
- **Refreshable:** No

## ServerRevertsToSystemForAFPInfo

- **Description:** Fixes a rare problem where the default mechanism for accessing finder info is extremely slow on particular systems. The problem would manifest itself as extremely poor performance - on the order of minutes to simply display the root of the mounted volume. Please contact the Acronis Support team before enabling this key.
- **Default:** Off
- **Refreshable:** No

## ServerUsesDefaultTypeCreator

- **Description:** Prior to Acronis Files Connect 4.0.3, files with no type and creator information were given a default type/creator of text/dosa. In version 4.0.3, this default behavior was changed so that files with unknown type and creator received a blank type and creator. This change was made for performance reasons - this allows for greater performance when copying many small files, particularly over Gigabit. However, some customers may rely on the previous default behavior, where unknown files would appear as text. For these customers, the `ServerUsesDefaultTypeCreator` registry key should be enabled.
- **Default:** Off
- **Refreshable:** No

## StartFileServerAtStartup

- **Description:** Whether or not the Acronis Files Connect file server should be brought online at service start.
- **Default:** On
- **Refreshable:** No

## StartPrintServerAtStartup

- **Description:** Whether or not the Acronis Files Connect print server should be brought online at service start.
- **Default:** On, unless Acronis Files Connect was upgraded from a previous version of Acronis Files Connect that did not have a print server license
- **Refreshable:** No

## StartupDelaySeconds

- **Description:** If this key is set, Acronis Files Connect will wait the specified number of seconds after its Windows service starts before actually starting the Acronis Files Connect file and print services. This can be used in cases where Acronis Files Connect is dependent on network or storage resources that take longer than normal to become available when a server is started.

- **Default:** 0
- **Refreshable:** No

## SupportAFP3

- **Description:** Enables support for AFP 3.1 (disabling this feature forces Acronis Files Connect to support AFP 2.2 only). AFP 3.1 features include support for filenames over 32 characters, file sizes over 2GB, and Unicode strings.
- **Default:** On
- **Refreshable:** No

## SupportAFP32

- **Description:** Enables support for AFP 3.2 (disabling this feature forces Acronis Files Connect to support AFP 3.1 if the SupportAFP3 key is enabled). AFP 3.2 features include support for Access Control Lists (ACLs) and extended attributes.
- **Default:** On
- **Refreshable:** No

## SupportAFP33

- **Description:** Enables support for AFP 3.3 (disabling this feature forces Acronis Files Connect to support AFP 3.2 if the SupportAFP32 key is enabled).
- **Default:** On
- **Refreshable:** No

## SupportFileIDs

- **Description:** When enabled, the File Server will support file ID operations.
- **Default:** On
- **Refreshable:** No

## SupportNetworkReshares

- **Description:** When enabled, the File Server will allow resharing of remote servers and shares.
- **Default:** Off
- **Refreshable:** No

## SupportUNIXPermissions

- **Description:** Whether or not the server supports UNIX permissions.
- **Default:** Off
- **Refreshable:** No

## TCP\_SO\_RCVBUF

- **Description:** Size of socket receive buffer
- **Default:** 65536
- **Refreshable:** No

## TCP\_SO\_SNDBUF

- **Description:** Size of socket send buffer
- **Default:** 46720
- **Refreshable:** No

## ThreadPoolDefaultStackSize

- **Description:** The default stack size of threads in the thread pool, in bytes. A value of 0 indicates that threads created in the thread pool should use the default process stack size (usually 1MB).
- **Default:** 0
- **Refreshable:** No

## ThreadPoolInitialNumberThreads

- **Description:** The number of threads initially assigned to the thread pool.
- **Default:** 50
- **Refreshable:** No

## ThreadPoolMaxNumberThreads

- **Description:** The maximum number of threads that can be placed into the thread pool.
- **Default:** 500
- **Refreshable:** No

## ThreadStackSize

- **Description:** The size of a fragment of the process address space that will be reserved to accommodate the stack frame for each newly created thread, in kilobytes. This feature is only available on Windows XP and Windows Server 2003; valid values for this parameter are 256 to 1024.
- **Default:** 1024
- **Refreshable:** No

## TickleTime

- **Description:** Specifies how often, in seconds, the server will send a "tickle" packet to the client to keep the client connection alive. This packet will only be sent if there has been no other traffic on the socket on that time.

- **Default:** 30
- **Refreshable:** No

## UseAutoReindexing

- **Description:** Specifies whether sparse search indexes will be automatically rebuilt after they become 1/3rd stale entries.
- **Default:** On
- **Refreshable:** No

## UseLazyIndexing

- **Description:** Specifies the use of "Lazy" search indexing which will cause indexing to take longer under moderate to high server load but will have less of an impact on other server processes.
- **Default:** Off
- **Refreshable:** No

## UseMacStylePermissions

- **Description:** Enables Mac style permissions.
- **Default:** Off
- **Refreshable:** No

## UseSearchIndexing

- **Description:** Enables / disables search indexing globally.
- **Default:** On
- **Refreshable:** No

## General parameter registry keys – refreshable

The following keys control certain features or behaviors of Acronis Files Connect.

The keys in this section are refreshable. They take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

Registry location:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Refreshable
```

## AccessRightsExpirationInterval

- **Description:** How long, in minutes, Acronis Files Connect will cache user access rights before reloading the access rights from disk. Access rights must be periodically reloaded if group membership changes are to be noticed.

- **Default:** 5
- **Refreshable:** Yes

## AdjustModificationDates

- **Description:** When this Registry key is set to '1', for any file where the modified date is older than the created date, Acronis Files Connect will change the modified date presented to the Mac user to be equal to the created date. The actual modified date on disk will not be changed as a result of enabling this key. Enabling this feature may have a significant impact on workflows and is not recommended without extensive testing.
- **Default:** 0
- **Refreshable:** Yes

## AllowClearTextLogin

- **Description:** Setting the value of this key to 1 allows Mac users to connect by sending their passwords over the network in clear text form. The default value setting, which is 0, prevents Mac users from sending clear text passwords.

---

### Note

Clear text passwords may be a security risk and are limited to 8 characters. Mac OS X versions 10.5 and later do not allow clear text authentication.

---

- **Default:** 0
- **Refreshable:** Yes

## AllowPartialHexFooMatch

- **Description:** Whether Acronis Files Connect does partial matching of OS-9 style ("hex foo") filenames. This can be disabled to restore pre-6.0.3 functionality, but doing so could cause failures in certain Mac applications.
- **Default:** On
- **Refreshable:** Yes

## CopyFileExBypassCacheThreshold

- **Description:** Files larger than this size will bypass the system cache when copied server-side.
- **Default:** 2000 [MB]
- **Refreshable:** Yes

## DefaultDomainName

- **Description:** DefaultDomainName allows for the specification of one or more default domains. At login, Acronis Files Connect will attempt to log the user into the specified domains in the order they appear in the list.

- **Default:** Off (blank string)
- **Type:** Multi-String
- **Refreshable:** Yes

## DefaultGlobalPermissions

- **Description:** UNIX permissions bits that should be added from any client requests to modify UNIX permissions. For example, if the client attempts to set UNIX permissions to 700 and DefaultGlobalUmask is 022, UNIX permissions will be set to 722.
- **Default:** 0
- **Refreshable:** Yes

## DefaultGlobalUmask

- **Description:** UNIX permissions bits that should be removed from any client requests to modify UNIX permissions. For example, if the client attempts to set UNIX permissions to 777 and DefaultGlobalUmask is 022, UNIX permissions will be set to 755.
- **Default:** 0
- **Refreshable:** Yes

## DFSDownServerRecheckInterval

- **Description:** [DFS capable servers only.] How often, in seconds, Acronis Files Connect will check to see if a server marked as up is has gone offline. Since an up server responds immediately, this can be done frequently as compared to DFSUpServerRecheckInterval (above).
- **Default:** 60
- **Refreshable:** Yes

## DFSSyncInterval

- **Description:** [DFS capable servers only.] How often, in seconds, the DFS namespace will be reenumerated. If this is 0 then the lowest value for TimeToLive will be used.
- **Default:** 0
- **Refreshable:** Yes

## DFSUpServerRecheckInterval

- **Description:** [DFS capable servers only.] How often, in seconds, Acronis Files Connect will check to see if a server marked as down is back online. It takes a long time for the check to timeout if the server is still down, so this should generally be larger than DFSDownServerRecheckInterval (below).
- **Default:** 300
- **Refreshable:** Yes

## DFSUseAdminNamespaceName

- **Description:** Whether the Acronis Files Connect DFS code uses the namespace name as entered (if enabled), or as it appears in the DFS enumeration (if disabled).
- **Default:** Off
- **Refreshable:** Yes

## DisableKeywordsProvider

- **Description:** Keywords Provider is an Acronis Files Connect feature that serves Windows File Explorer tags to Mac users. Disabling this registry key may lead to a major performance hit when browsing because Acronis Files Connect will have to retrieve tags for every file. After changing this setting, you need to rebuild the Acronis Content Indexing search indexes. See more about [Indexing options](#).
- **Default:** 1
- **Refreshable:** Yes

## DisplaySerialInUI

- **Description:** Whether or not the Acronis Files Connect Administrator (local or remote) will display the serial number in the About Box and Licensing dialog.
- **Default:** On
- **Refreshable:** Yes

## EnumerationPerformanceOnLocalVolume

- **Description:** Enables Enumeration Performance on local volumes. Set to 1 to enable.
- **Default:** Off
- **Refreshable:** Yes

## EventLogOnWrap

- **Description:** EventLogOnWrap determines whether a message will be written to the event log every time the change journal wraps.
- **Default:** On
- **Refreshable:** Yes

## ForcedPasswordChangePeriod

- **Description:** The period, in days, before a user's password expires that Acronis Files Connect forces the user to change their password. This can be used to help ensure that users change their passwords before expiration.
- **Default:** 0
- **Refreshable:** Yes

## FullCrashDump

- **Description:** When set to 'On' Acronis Files Connect will generate larger crash dumps containing more detailed debugging information. These will typically be 100 to 200 MB in size, instead of the 2 to 12 MB in size when this setting is set to 'Off'.
- **Default:** Off
- **Refreshable:** Yes

## IdleTimeoutNoOpenForks

- **Description:** If idle users are timed out (see above), this controls the amount of time Acronis Files Connect will wait before disconnecting an idle user with no open forks. Setting this to 0 will prevent idle users with no open forks from being timed out. This value is specified in minutes.
- **Default:** 360 [6 hours]
- **Refreshable:** Yes

## IdleTimeoutOpenForks

- **Description:** If idle users are timed out (see above), this controls the amount of time Acronis Files Connect will wait before disconnecting an idle user with open forks. These users could potentially lose data. Setting this to 0 will prevent idle users with open forks from being timed out. This value is specified in minutes.
- **Default:** 1440 [24 hours]
- **Refreshable:** Yes

## IgnoreExchangeFileSecuritySwap

- **Description:** Whether or not the server ignores code to swap Access Control Lists (ACLs) during an ExchangeFile operation. This setting is only honored when UNIX permission support is disabled. When enabled, the file server will emulate the (incorrect) behavior in Acronis Files Connect 5.1.3 and earlier.
- **Default:** Off
- **Refreshable:** Yes

## IgnoreOffspringCount

- **Description:** When set to 'On', Acronis Files Connect will not count the number of items in any folder during an enumeration. This could potentially speed up enumeration performance, but might effect some third party applications. It is recommended you consult the Acronis Support team before enabling this setting.
- **Default:** Off
- **Refreshable:** Yes

## KeepOwnerSetByWindows

- **Description:** Whether or not Acronis Files Connect will keep the owner of files as set by Windows. If disabled, Acronis Files Connect will set the owner to the user that create the file. This can differ from the owner assigned by Windows, as files created by members of the Administrators group are assigned an owner of "Administrators" by Windows.
- **Default:** Off
- **Refreshable:** Yes

## LoginMsgW

- **Description:** The logon message sent to users immediately after login. This setting is normally edited through the Acronis Files Connect Administrator, but this setting can be edited directly in order to support longer logon messages. The Administrator restricts logon messages to 199 characters for compatibility with OS 9, but by editing this registry value directly, the message length can be increased to 1024 characters. Note that while Acronis Files Connect supports logon messages up to 1024 characters, Mac OS X will fail to display messages longer than 500 characters.
- **Default:** Blank
- **Refreshable:** Yes

## MappingFlushFrequency

- **Description:** How often, in seconds, Acronis Files Connect flushes new ID/index pairs to disk. Decreasing this setting will reduce performance, but can ensure that newly created file IDs get committed to disk in the event of a server crash.
- **Default:** 600 [10 minutes]
- **Refreshable:** Yes

## MaxDuplicateSessionsWaiting

- **Description:** The maximum number of sessions that can be waiting for reconnect from a single IP address with a single username.
- **Default:** 5
- **Refreshable:** Yes

## MaxEnumerationListSize

- **Description:** The maximum amount of memory, in MB, Acronis Files Connect will devote to caching enumeration information.
- **Default:** 32
- **Refreshable:** Yes

## MaxIdPathMapSize

- **Description:** The maximum size, in megabytes, of the ID/path map. This in-memory data structure is only used in environments where at least one Acronis Files Connect volume is on a non-NTFS filesystem.
- **Default:** 800
- **Refreshable:** Yes

## MaxIORequestsPerSession

- **Description:** The maximum number of simultaneous outstanding I/O requests for an individual session.
- **Default:** 250
- **Refreshable:** Yes

## MaxNodeTableSize

- **Description:** Size of the node table cache (in MB). The cache contains a list of information about files that are being shared. Setting a different cache size allows you to adjust the tradeoff between performance and memory usage. Acronis Files Connect retains information in RAM for the most recently accessed files, up to the limit specified. If a Mac user requests a file that is not in the node table cache, Acronis Files Connect goes to disk to retrieve the information and stores it in the node table. If the maximum cache size has been reached, Acronis Files Connect discards the oldest entry in the node table. You can specify the maximum size in the Cache Size text box of the File Server Settings dialog. The maximum allowed size is 500MB. It is possible to set a higher size via a registry key, but doing so may cause severe problems. Contact the Acronis Support team if you are interested in experimenting with sizes greater than 500MB.
- **Default:** 20
- **Refreshable:** Yes

## MigrateHiddenSMBShares

- **Description:** If disabled, the file server will not migrate hidden SMB shares.
- **Default:** 0
- **Refreshable:** Yes

## PasswordExpirationReminderInterval

- **Description:** How often, in minutes, to send connected users a message indicating that their password is about to expire. The "SendPasswordExpirationWarnings" setting must be enabled for this feature to take effect.
- **Default:** 0
- **Refreshable:** Yes

## PasswordExpirationWarningThreshold

- **Description:** Number of days prior to expiration to begin warning (value should be between 1 and 366). This can also be configured in the Acronis Files Connect Administrator.
- **Default:** 14 Days
- **Refreshable:** Yes

## PruningInterval

- **Description:** PruningInterval specifies the frequency that Acronis Files Connect will walk its list of Mac file IDs and remove obsolete records.
- **Default:** 10080 [one week]
- **Refreshable:** Yes

## ReconnectServerKeyLifetime

- **Description:** Number of minutes that the reconnect server key is valid before a new key is automatically generated.
- **Default:** 2 weeks (20160 minutes)
- **Refreshable:** Yes

## ReconnectTimeout

- **Description:** Number of minutes session waiting for reconnect will wait before disconnecting.
- **Default:** 5 minutes
- **Refreshable:** Yes

## ReconnectUAMExpirationInterval

- **Description:** Number of seconds that reconnect credentials are valid before they expire.
- **Default:** 2 days (172800 seconds)
- **Refreshable:** Yes

## ReindexOnWrap

- **Description:** ReindexOnWrap determines whether volumes will be automatically reindexed when the change journal wraps.
- **Default:** On
- **Refreshable:** Yes

## ReplayCacheSize

- **Description:** Size of the replay cache (number of cached reply requests).
- **Default:** 32
- **Refreshable:** Yes

## RetryOpeningReparsePoints

- **Description:** Whether or not Acronis Files Connect should retry opening reparse points when encountering a reparse error.
- **Default:** Yes
- **Refreshable:** Yes

## SendPasswordExpirationWarnings

- **Description:** Enables password expiration notifications. This can also be configured in the Acronis Files Connect Administrator.
- **Default:** Off
- **Refreshable:** Yes

## ServerAllows8Dot3Names

- **Description:** Whether or not the server files support the access of files and folders using their Windows 8.3 filename. While Acronis Files Connect does not communicate these 8.3 filenames to Mac users, workflows such as Prinerger that involve Windows and Mac components can result in Mac users making requests for files and folders by these names.
- **Default:** Off
- **Refreshable:** Yes

## ServerAllowsLargeEABuffers

- **Description:** Whether or not Acronis Files Connect supports extended attributes buffers larger than 4Kb. As of Mac OS X 10.5.6, the "ditto" command fails to duplicate files containing extended attributes when these files are located on a remote server. Enabling this setting allows Acronis Files Connect to workaround this client-side issue.
- **Default:** Off
- **Refreshable:** Yes

## ServerConvertsShortcutsToLinks

- **Description:** Whether or not the server displays Windows Shortcut (.lnk) files to Mac users as symbolic links.
- **Default:** On
- **Refreshable:** Yes

## ServerCreatesEmptyStreams

- **Description:** Whether or not the service creates empty alternate data streams as a marker that there are no dot underscore files to migrate. This feature was enabled in earlier versions of Acronis Files Connect but was disabled because the creation of so many empty alternate streams

could interfere with Windows-side activity, such as Rampage.

- **Default:** Off
- **Refreshable:** Yes

## ServerDeletesMigratedDotUnderscoreFiles

- **Description:** Whether or not Acronis Files Connect will delete SMB dot underscore (.\_) files after migrating to resource fork and finder information streams.
- **Default:** No
- **Refreshable:** Yes

## ServerDisconnectsGhostedUsers

- **Description:** Whether or not the server will disconnect ghosted users when clients log in. A ghosted user is defined as a user that had logged in from the logging-in user's machine with the same user/domain name as the logging-in user. This feature can ensure that clients that are waiting for reconnect get disconnected before the reconnect timeout in the event that the clients do not reconnect.
- **Default:** 1
- **Refreshable:** Yes

## ServerEmbedsPasswordInReconnectCredential

- **Description:** If the server embeds the user's password inside its reconnect credential. Doing this allows users to reconnect even after the server has been rebooted because all authentication data exists inside the credential. However, enabling this feature does mean that all users passwords are encrypted with the same server key.
- **Default:** On
- **Refreshable:** Yes

## ServerIgnoresReadOnlyFolders

- **Description:** If enabled, the server will not display any folders as locked, even if they are marked "read-only" in Windows. The read-only attribute on Windows does not truly map to the Macintosh locked attribute, since read-only directories on Windows can be renamed, deleted and have files added and removed from it. Folders are marked read-only on Windows if they have a customized view, such as a custom icon. Starting with OS 10.4.6, folders over the network can appear as locked. Enabling this setting will also cause the server to ignore requests to change the locked status of the folder.
- **Default:** On
- **Refreshable:** Yes

## ServerMigratesDotUnderscoreFiles

- **Description:** Whether or not Acronis Files Connect will migrate SMB dot underscore (.) files to resource fork and finder information streams.
- **Default:** Yes
- **Refreshable:** Yes

## ServerNotificationTime

- **Description:** How often, in seconds, the server will send clients notifications that the volumes they have open have changed. Set 0 to disable server notifications.
- **Default:** 10
- **Refreshable:** Yes

## ServerOpensExchangeFileHandlesByFullPath

- **Description:** Whether or not the server opens folders by full path (as opposed to file ID) when doing ExchangeFiles operation. This setting is useful on Windows 2008, which can blue screen if Mac users save files to an Acronis Files Connect volume through a client application using the ExchangeFiles command. This command is used by a number of applications, including Microsoft Word. By opening folders by full path rather than ID during ExchangeFiles processing, this Windows 2008 bug can be bypassed. Microsoft is aware of the issue and will be issuing a fix at an unspecified date.
- **Default:** On for Windows 2008 (and later), off for earlier OS versions
- **Refreshable:** Yes

## ServerRemovesTemporaryItems

- **Description:** Whether or not Acronis Files Connect will delete "Temporary Items" and ".TemporaryItems" folders at shutdown.
- **Default:** No
- **Refreshable:** Yes

## ServerResetsPermissionsOnMove

- **Description:** Whether or not Acronis Files Connect will reset permissions on folders after a move so that the folder inherits from its new parent folder.
- **Default:** No
- **Refreshable:** Yes

## ServerSupportsReconnectUAM

- **Description:** If the server supports the Reconnect UAM.
- **Default:** On

- **Refreshable:** Yes

## ServerTruncatesOS9Comments

- **Description:** Truncates OS 9-style comments to 127 bytes, rather than the default of 199 bytes. Enabling this key fixes a bug in Photoshop CS2, which crashes when encountering comments that are larger than 127 characters. Even though Photoshop CS2 is an OS X application, it makes a request for OS 9 comments. This problem is known to occur in Mac OS X 10.4.6.
- **Default:** Off
- **Refreshable:** Yes

## ServerUsesRelativeHandles

- **Description:** Controls whether or not Acronis Files Connect will open file handles relative to folder handles. This setting should be disabled for users of CommVault Simpana software.
- **Default:** On
- **Refreshable:** Yes

## SetEOFOnResize

- **Description:** SetEOFOnResize governs whether end of file for files being written to the server is updated as the file is in the act of being written.
- **Default:** Off
- **Refreshable:** Yes

## ShowInaccessibleFiles

- **Description:** Controls whether users are able to see files for which they do not have at least "read attributes". The "read attributes" property does not imply the ability to read a file, but only to be able to see what the permissions and other attributes of the file are.
- **Default:** On
- **Refreshable:** Yes

## ShowInaccessibleFolders

- **Description:** Controls whether users are able to see folders for which they have neither read nor write access
- **Default:** On
- **Refreshable:** Yes

## SleepTimeout

- **Description:** Amount of time (in minutes) before timing out sleeping sessions.
- **Default:** 1440
- **Refreshable:** Yes

## SlowAFPCommandLogFrequency

- **Description:** Frequency, in seconds, in which the server logs information about slow AFP commands. Setting this value to 0 will disable slow AFP command logging.
- **Default:** 3600 (1 hour)
- **Refreshable:** Yes

## SupportACLs

- **Description:** Whether or not the server supports Access Control Lists (ACLs).
- **Default:** Off
- **Refreshable:** Yes

## SupportCopyFileEx

- **Description:** Whether or not the server supports new server-side copy semantics for improved performance.
- **Default:** Yes
- **Refreshable:** Yes

## SupportSCP

- **Description:** Whether or not the server will register itself in Active Directory as a Service Connection Point (SCP).
- **Default:** On
- **Refreshable:** Yes

## TimeoutIdleUsers

- **Description:** Controls whether or not idle users are timed out after some period of time.
- **Default:** Off
- **Refreshable:** Yes

## UNIXCalculatedPermissionsMode

- **Description:** Determines how UNIX permissions are calculated for files and folders that don't already have UNIX permissions assigned. If 0, the Windows GetEffectiveRightsFromACL call is used to determine UNIX permissions. If 1, calls to GetEffectiveRightsFromACL are avoided when possible to improve performance. If 2, UNIX permissions are always returned as 777 (full rights) if no explicit UNIX permissions have been assigned.
- **Default:** 1
- **Refreshable:** Yes

## UNIXGroupPermissionsMode

- **Description:** Determines how group UNIX permissions are calculated for files and folders that don't already have UNIX permissions assigned. If 0, the calculation mode as set by UNIXCalculatedPermissionsMode is used. If 1, group permissions are the sum of the permissions for all groups (not just the primary group). If 2, group UNIX permissions are always returned as 7 (full rights) if no explicit UNIX permissions have been assigned.
- **Default:** 0
- **Refreshable:** Yes

## UnixOwnerPermissionsMode

- **Description:** This registry key is in effect only when **Support UNIX permissions and ACLs** is enabled in the product. Gives the administrator full control over files that have no owner or the owner is disabled or unreachable.
- **Default:** 7 (on upgrades it will be 0)
- **Refreshable:** Yes

## WriteFlushThreshold

- **Description:** Specifies the number of bytes that can be written to a open fork before Acronis Files Connect forces a flush of that data to disk. Setting this value to 0 indicates that these flushes should never occur. Small values force a large number of flushes, which help prevent periodic long file system delays by spreading out flushes over a large number of writes.
- **Default:** 0
- **Refreshable:** Yes

## Debug logging registry keys – refreshable

The following keys control certain features or behaviors of Acronis Files Connect. Generally, they should only be changed or enabled when requested by Acronis Support.

The keys in this section are refreshable. They take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

Registry location:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\DebugRefreshable
```

## AppleDoubleIntegrity

- **Description:** Whether or not Acronis Files Connect performs extra runtime checking of its AppleDouble code.

- **Default:** On
- **Refreshable:** Yes

## CopyDebugLog

- **Description:** Whether or not Acronis Files Connect can create new debug logs when encountering an error or at user request.
- **Default:** On
- **Refreshable:** Yes

## CriticalSectionMonitorLogFrequencyInMilliseconds

- **Description:** The frequency (in milliseconds) of critical section monitor logging (if enabled). Default is one minute.
- **Default:** 60000
- **Refreshable:** Yes

## DebugLogLimit

- **Description:** # of MB to limit log file size (should be between 1 and 999)
- **Default:** 200
- **Refreshable:** Yes

## DebugLogThrowThreadException

- **Description:** Server will throw exception and crash, for testing generation of DrWatson logs. Contact the Acronis Support team for instructions on usage.
- **Default:** Off
- **Refreshable:** Yes

## DisplayTimeAsNumeric

- **Description:** Choose whether the time is displayed as a numeric value or h-m-s-ms. Select 0 for hours-minutes-seconds-milliseconds or 1 for a numeric value.
- **Default:** Off
- **Refreshable:** Yes

## EventLogNoFC

- **Description:** Will put information in the event log if the service does not have full control permissions.
- **Default:** On
- **Refreshable:** Yes

## IdPathMapIntegrity

- **Description:** Whether or not Acronis Files Connect performs extra runtime checking of its internal ID/path map.
- **Default:** Off
- **Refreshable:** Yes

## MaxLogArchiveSize

- **Description:** Number of MB of old logs to keep before the oldest logs are automatically removed. Logs are automatically archived into .zip files to conserve space. If this is set to 0, archiving will not take place and there will be no limit to the cumulative size of the log files.
- **Default:** 200 [MB]
- **Refreshable:** Yes

## NetworkReshareIntegrity

- **Description:** When enabled, Network Reshare volume integrity will be checked at runtime. This will have an effect on performance.
- **Default:** Off
- **Refreshable:** Yes

## RenameCopyDebugLog

- **Description:** When set to 1, the current log will be renamed and a new one created when users request a new log be created. When set to 0, the current log will be copied rather than renamed. CopyDebugLog must be set to 1 for this key to take effect.
- **Default:** On
- **Refreshable:** Yes

## SpoolingLog

- **Description:** Server will spool to a new log when the active log hits its size limit (see DebugLogLimit above).
- **Default:** On
- **Refreshable:** Yes

## SupportWER

- **Description:** Whether or not Acronis Files Connect supports Windows Error Reporting (WER).
- **Default:** On
- **Refreshable:** Yes

## Debug logging registry keys – non-refreshable

The following keys control certain debug logging features of Acronis Files Connect. Generally, they should only be changed or enabled when requested by Acronis Support.

The keys in this section are non-refreshable. In order to take effect, they require that the Acronis Files Connect service is restarted.

Registry location:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\DebugNonRefreshable
```

### CompareMicrosecondsToTickCount

- **Description:** Server will log timing statistics at startup
- **Default:** On
- **Refreshable:** No

### DebugLogFolder

- **Description:** Directory in which log subfolders are placed.
- **Default:** Acronis Files Connect application directory
- **Type:** String
- **Refreshable:** No

### RenameLogAtStartup

- **Description:** At startup Acronis Files Connect will rename any existing log with current date and time for easy archiving.
- **Default:** On
- **Refreshable:** No

### UseCriticalSectionMonitor

- **Description:** Logs details about critical sections within Acronis Files Connect
- **Default:** Off
- **Refreshable:** No

## Print parameter registry keys – refreshable

The following keys control certain features or behaviors of the Acronis Files Connect Print Server, if installed.

The keys in this section are refreshable. They take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

Registry location:

\HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\PrintRefreshable

## IPPrintLPRPort

- **Description:** The port used by Acronis Files Connect to listen for incoming (LPR) print jobs.
- **Default:** 515
- **Refreshable:** Yes

## PersistentMappedNetworkFolderPrintQueues

- **Description:** Print Queues configured with '**Send To Specified Directory**' whose paths are to network folders will map the network folder to a local drive that will persist as long as the Acronis Files Connect server is running. If the registry key is set to 0, mapped network folders persist only for each individual print job.
- **Default:** On
- **Refreshable:** Yes

## PostscriptCodePage

- **Description:** The Macintosh code page used when parsing postscript files. By default, this setting is copied from the system registry value "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\MACCP".
- **Default:** 10000
- **Refreshable:** Yes

## ServerAutoDeleteOfflineJobsTime

- **Description:** How long (in seconds) a job can be offline before the server automatically deletes it. Set to 0 to disable deletion of offline jobs.
- **Default:** 0
- **Refreshable:** Yes

## ServerAutoRetryJobsFrequency

- **Description:** How often (in seconds) the server should auto-retry a job that is offline.
- **Default:** 300 [5 minutes]
- **Refreshable:** Yes

## ServerCombinesLPRPackets

- **Description:** If enabled, Acronis Files Connect will take LPR packets that were previously sent separately and combine them into larger packets.

- **Default:** On
- **Refreshable:** Yes

## ServerLogsJobErrorFrequency

- **Description:** How often (in seconds) the server should log errors that occur during auto-retry of jobs that are offline.
- **Default:** 3600 [1 hour]
- **Refreshable:** Yes

## ServerPrintJobTimeout

- **Description:** How long, in milliseconds, a job being sent to a remote printer can be "stuck" before the print server takes the job offline.
- **Default:** 300000 [5 minutes]
- **Refreshable:** Yes

## Print parameter registry keys – non-refreshable

The following keys control certain features or behaviors of the Acronis Files Connect Print Server, if installed.

The keys in this section are non-refreshable. In order to take effect, they require that the Acronis Files Connect service is restarted.

Registry location:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\PrintNonRefreshable
```

## PrintSupportEnabled

- **Description:** Whether or not the print server is enabled. Set to 0 to disable. When disabled, print cannot be enabled through the Administrator.
- **Default:** On
- **Refreshable:** No

## Filename policy registry keys – Refreshable

The following keys control certain features or behaviors of the Acronis Files Connect Filename Policy feature.

The keys in this section are refreshable. They take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

Registry location:

\\HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Refreshable\FilenamePolicy

## AppliesToAllVolumes

- **Description:** Whether or not the filename policy applies to all volumes. Set to 1 to enable.
- **Default:** On
- **Refreshable:** Yes

## AppliesToTemporaryItems

- **Description:** Whether or not filename policies apply to temporary items folders.
- **Default:** Off
- **Refreshable:** Yes

## ErrorMessage

- **Description:** Custom error message to send to users that violate the filename policy.
- **Default:**
- **Type:** String
- **Refreshable:** Yes

## EventLogMessageFrequency

- **Description:** How often, in seconds, Acronis Files Connect will log a message to the Windows Event log when a particular user violates the filename policy.
- **Default:** 600 [10 minutes]
- **Refreshable:** Yes

## GloballyEnabled

- **Description:** Whether or not the filename policy feature is globally enabled. Set to 1 to enable.
- **Default:** On
- **Refreshable:** Yes

## IllegalCharacters

- **Description:** A list of characters that will be disallowed in file and folder names by the filename policy.
- **Default:**
- **Type:** String
- **Refreshable:** Yes

## IllegalExtensions

- **Description:** A list of extensions that will be disallowed in filenames by the filename policy.
- **Default:**
- **Type:** Multi-String
- **Refreshable:** Yes

## MaxLengthFileName

- **Description:** The maximum length of file names. Set to 0 to disable this filename policy rule.
- **Default:** 0
- **Refreshable:** Yes

## MaxLengthFolderName

- **Description:** The maximum length of folder names. Set to 0 to disable this filename policy rule.
- **Default:** 0
- **Refreshable:** Yes

## MaxLengthPathName

- **Description:** The maximum full path length for files and folders. Set to 0 to disable this filename policy rule.
- **Default:** 0
- **Refreshable:** Yes

## MaxViolationsReported

- **Description:** Sets the maximum number of violations reported per volume
- **Default:** 20000 (Decimal)
- **Refreshable:** Yes

## PreventDS\_StoreFileCreation

- **Description:** When enabled, Acronis Files Connect will prevent the creation of .DS\_Store files.
- **Default:** Off
- **Refreshable:** Yes

## RejectPolicyFailures

- **Description:** Whether or not violations of the filename policy are rejected (if value is 1), or if the user is warned but the action is allowed (value of 0).
- **Default:** 1
- **Refreshable:** Yes

## RestrictNonDisplayable

- **Description:** When enabled, the filename policy will restrict characters that cannot be displayed in Windows Explorer. Set to 1 to enable.
- **Default:** Off
- **Refreshable:** Yes

## UserMessageFrequency

- **Description:** How often, in seconds, a user can be sent a message indicating that they violated the filename policy.
- **Default:** 5
- **Refreshable:** Yes

## HTTP discovery registry keys – refreshable

The following keys control certain features or behaviors of the Acronis Files Connect HTTP Discovery feature.

The keys in this section are refreshable. They take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

Registry location:

```
\\KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Refreshable\HTTPDiscovery
```

## HTTPDiscoveryDFSOption

- **Description:** When enabled, DFS volumes will be discovered by HTTP Discovery Service.
- **Default:** On
- **Refreshable:** Yes

## HTTPDiscoveryDocumentRoot

- **Description:** Location of the HTTP server's HTML files. This can be set such that different nodes of a cluster share the same HTML files.
- **Default:** Blank, which indicates files will be pulled from "<application directory>\HTML Files\", e.g. "C:\Program Files\Group Logic\Acronis Files Connect\HTML Files\"
- **Refreshable:** Yes

## HTTPDiscoveryExtraContentTypes

- **Description:** List of content types supported by Acronis Files Connect's internal web server along with their associated extensions. A standard set of extensions (html, xml, gif, jpg, ico, zip) are

automatically assigned their appropriate content types. This registry settings allows for the customization of additional content types. The format is "extension,content type", with each pair on its own line.

- **Default:** css,text/css | js,application/x-javascript | pdf,application/pdf | doc,application/msword | htm,text/html
- **Refreshable:** Yes

## HTTPDiscoveryFileOption

- **Description:** Whether or not the Acronis Files Connect File Server is discoverable over HTTP.
- **Default:** On
- **Refreshable:** Yes

## HTTPDiscoveryMasterHostName

- **Description:** Name of the Acronis Files Connect HTTP Discovery primary server.
- **Default:** "ExtremeZIPServerList"
- **Type:** String
- **Refreshable:** Yes

## HTTPDiscoveryPrintOption

- **Description:** Whether or not the Acronis Files Connect Print Server is discoverable over HTTP.
- **Default:** On
- **Refreshable:** Yes

## HTTPDiscoveryServerPort

- **Description:** TCP port number for HTTP Discovery.
- **Default:** 8081
- **Refreshable:** Yes

## HTTPDiscoveryServerZone

- **Description:** HTTP Discovery zone name.
- **Default:** "Global"
- **Type:** String
- **Refreshable:** Yes

## Spotlight registry keys – Refreshable

The following keys control certain features or behaviors of Acronis Files Connect Network Spotlight support.

The keys in this section are refreshable. They take effect when the **Refresh Registry** button, located in the **Settings** dialog box of **Acronis Files Connect Administrator**, is clicked; or when the Acronis Files Connect service is started.

Registry location:

```
\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ExtremeZ-IP\Parameters4\Spotlight\Refreshable\
```

## dtSearchExcludeFromIndexingList

- **Description:** Comma separated list of strings, paths and/or file types to not index.
- **Default:** ''
- **Type:** String
- **Refreshable:** Yes

## dtSearchIndexFileNameAndSize

- **Description:** When enabled, file size metadata will be included in Acronis Content Indexing indexes. This applies to **Filename Only** indexes; **Content & Filename** indexes always include this metadata.
- **Default:** On
- **Refreshable:** Yes

## dtSearchIndexFinderTags

- **Description:** When enabled, Finder tag metadata will be included in Acronis Content Indexing indexes. This applies to **Filename Only** indexes; **Content & Filename** indexes always include this metadata.
- **Default:** On
- **Refreshable:** Yes

## dtSearchIndexIsAccentSensitive

- **Description:** When enabled, text with diacritical marks such as accents, rings, curls, hooks, tildes, superscript or subscript dots, etc. will be found only if you use the exact special character in the search string. For example, words **façade**, **niño**, **řeka**, **barbă**, **på**, **brød** would not be found if you search for: **facade**, **nino**, **reka**, **barba**, **pa**, **brod**.

When disabled, special characters are treated as their respective base characters (ę=e, ü=u, č=c, etc.) and files will be found even if you omit or mistake some diacritical mark.

In order to obtain the desired results, you need to rebuild the Acronis Content Indexing search indexes after changing this setting. See more about [Indexing options](#).

- **Default:** Off
- **Refreshable:** Yes

## dtSearchVerifyIndex

- **Description:** Controls whether dtSearch index(es) are verified when checking their existence.
- **Default:** Off
- **Refreshable:** Yes

## NumSpotlightSearchResults

- **Description:** The maximum number of results that can be returned in a Spotlight search. A value of 0 represents "unlimited".
- **Default:** 1000
- **Refreshable:** Yes

## SpotlightDefaultSearchIsBeginsWith

- **Description:** Whether or not the default Spotlight search is a "begins with" search, or (if disabled) a "contains" search.
- **Default:** On
- **Refreshable:** Yes

## SpotlightEnabled

- **Description:** Whether or not the Network Spotlight feature is enabled.
- **Default:** Off
- **Refreshable:** Yes

## SpotlightEnabledAllVolumes

- **Description:** Whether or not Spotlight support is automatically enabled for all volumes. If disabled, Spotlight support will be configured on a volume-by-volume basis.
- **Default:** Off
- **Refreshable:** Yes

## SpotlightIgnoresUnknownTerms

- **Description:** Whether or not the server will ignore Spotlight search terms it doesn't understand. For example, with this setting enabled, if the client searches for "name = test and audio bit rate = 4096", the server will ignore the "audio bit rate" term and simply return hits matching "name = test". With the setting disabled, any search containing one or more unknown search terms will automatically return 0 results.
- **Default:** On
- **Refreshable:** Yes

## SpotlightKeypressDelay

- **Description:** The amount of time, in milliseconds, to wait before processing a Spotlight search request. This delay allows users to type in search fields without generating a series of search requests. For example, without the delay, typing in "test" would result in four searches, the first three of which will be quickly canceled: "t", "te", "tes" and finally "test".
- **Default:** 150
- **Refreshable:** Yes

## SpotlightUsesWindowsKindClassification

- **Description:** Whether or not the server uses Windows' classification of files into various "kinds" when Mac users perform a Spotlight "kind" search. For example, if the Mac user searches for "kind = Movie", the server will perform a lookup using the Windows "video" kind, and return the appropriate results. If the setting is 0, the server will take the Mac "kind", map it to a UTI, and then perform a search based on the set of file extensions that match the UTI. For example, if the Mac user searches for "kind = Movie", the server will map that to "public.movie" and find files with the corresponding extensions (e.g. .mov, .mpg). The advantage of using the Windows kinds is that the search is faster - the downside is that there are a few file types that are categorized differently on Mac and Windows. For example, .m4p (iTunes) files are considered Audio by Mac users, but are given a Windows kind of "unknown".
- **Default:** On
- **Refreshable:** Yes

## Acronis Files Connect Streams

Acronis Files Connect uses Windows NTFS alternate data streams to store information necessary for serving files to Mac users. Because alternate data streams cannot normally be seen in Windows, two command-line utilities, cpstream and delstream, are included with Acronis Files Connect. These two utilities allow access to alternate data streams on NTFS volumes. These command line utilities are low-level tools, and should only be used for specific problems. Normally, you will want to contact the Acronis Support team before using them.

- cpstream allows you to copy the secondary stream to a second visible location.
- delstream allows you to delete a secondary stream of an NTFS file or directory.

The most important secondary stream used by Acronis Files Connect is called "GLIAFP\_Mapping"; this stream is used to store the mapping between NTFS file IDs and Mac file IDs. It is located in the topmost directory of a Mac share. For example, if you were sharing the directory, "D:\Macintosh Files" as a volume for Mac users, then Acronis Files Connect would create an invisible NTFS secondary stream in this directory.

- If you are experiencing a problem accessing your Acronis Files Connect volumes, you may want to make a copy of this stream and send it to the Acronis Support team.

- To do this, you would use `cpstream` to copy it to a visible location. In the example above, you would issue the following command to make a visible copy of the stream called "EZIPINDEX":  
`cpstream "D:\Macintosh Files:GLIAFP_Mapping" "EZIPINDEX"`. You can then send the "EZIPINDEX" file to the Acronis Support team to help diagnose your problem.
- In order to correct a problem with an index stream, you may need to remove the index stream.
  - The "delstream" utility can be used to this. Before removing the index stream, stop the Acronis Files Connect service in the Services control panel. **DO NOT DELETE THE INDEX STREAM WHILE Acronis Files Connect IS RUNNING.** After Acronis Files Connect is stopped, issue the following command to remove the index stream: `delstream "D:\Macintosh Files:GLIAFP_Mapping"` When you restart Acronis Files Connect, it will begin to rebuild the index stream. This may resolve problems you are experiencing. In addition to the mapping stream Acronis Files Connect will periodically prune the mapping to remove old invalid data. If the server is stopped during pruning a second stream will exist "GLIAFP\_MappingPruned". When deleting the original mapping, users should also remove this mapping to insure all streams are removed. An example would be: `delstream "D:\Macintosh Files:GLIAFP_MappingPruned"`

## EZIPUTIL command line tool

EZIPUTIL allows you to use and manage Acronis Files Connect at the command line. To start using this tool, at the command line, navigate to the Acronis Files Connect installation directory, and run EZIPUTIL with no additional arguments. This provides you with more information about four major categories: **Server**, **Volume**, **Print** and **Session**. Selecting any one of them shows further list of available commands and examples.

---

### Note

You must add a space before every option used at the command line.

For example: `C:\Program Files (x86)\Acronis\Access\Files Connect>eziputil volume /edit /name:1 /support_acls:false`

---

**All available commands are listed below.**

## SERVER

To start Acronis Files Connect:

```
EZIPUTIL SERVER /START
```

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

To stop Acronis Files Connect:

```
EZIPUTIL SERVER /STOP
```

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To suspend file services:

EZIPUTIL SERVER /SUSPEND

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

[/DELAY:minutes] – delay in minutes (1 – 60 minutes). Default is 2 minutes

[/MESSAGE:message] – message to send to a user

[/ALLOW-LOGIN] – allow a user to login during scheduled suspend

### To cancel scheduled suspend and resume file services:

EZIPUTIL SERVER /RESUME

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To get server statistics from Acronis Files Connect:

EZIPUTIL SERVER /INFO

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To get a list of open files from Acronis Files Connect:

EZIPUTIL SERVER /FILES

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To get a list of currently logged-in users from Acronis Files Connect:

EZIPUTIL SERVER /USERS

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To refresh settings from the registry:

EZIPUTIL SERVER /REFRESH\_REGISTRY

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To manage Acronis Files Connect's Service Connection Point:

EZIPUTIL SERVER/SCP

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

[/N = fully qualified domain name] (default = local machine name)]

[/I] to Install the SCP (which overwrites any previously defined SCP)

[/U] to uninstall the SCP

[/D] to display the SCP

[/Q] 'quiet' mode – output or prompts will not be written to the window

[/L] to log the results of the operation to Exe'.\EzScpManager.log'

[/S = ServiceName] to override 'ExtremeZ-IP' stored in SCP when installing

---

### Note

/I, /U, and /D are mutually exclusive.

---

## To spool the debug log:

EZIPUTIL SERVER /SPOOL\_LOG

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To prune all volume IDIndexMaps:

EZIPUTIL SERVER /PRUNE

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To get server status from Acronis Files Connect:

EZIPUTIL SERVER /STATUS

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## VOLUME

### To add a volume:

EZIPUTIL VOLUME /ADD

/NAME:volumename

/PATH:root directory path

[/READONLY: TRUE | FALSE] – The default is FALSE

[/GUESTSALLOWED: TRUE | FALSE] – The default is TRUE

[/PASSWORD: password] – The default is **no password**

[/MAXUSERS: number | UNLIMITED] – The default is UNLIMITED

[/PERSIST: TRUE | FALSE] – The default is TRUE

[/HOMEDIRECTORY: TRUE | FALSE] – The default is FALSE

[/SEARCHINDEX: TRUE | FALSE] – The default is TRUE

[/SEARCHINDEXPATH: index path] – The default is the root of the volume

[/SERVERNAME: servername] – If not local

[/SERVICENAME: servicename] – If not 'ExtremeZ-IP'

#### Available in ExtremeZ-IP 5.2 and later:

[/RESET\_PERMISSIONS: TRUE | FALSE] – The default is FALSE

[/FILENAME\_POLICY: TRUE | FALSE] – The default is FALSE

[/IS\_TM\_VOLUME: TRUE | FALSE] – The default is FALSE

[/USE\_TM\_QUOTA: TRUE | FALSE] – The default is FALSE

[/TM\_QUOTA: number] – The default is 100

[/SUPPORT\_ACLS: TRUE | FALSE] – The default is FALSE

[/SUPPORT\_SPOTLIGHT: TRUE | FALSE] – The default is FALSE

#### To edit a volume:

EZIPUTIL VOLUME /EDIT

/NAME:volumename

[/PATH:root directory path]

[/READONLY: TRUE | FALSE] – The default is FALSE

[/GUESTSALLOWED: TRUE | FALSE] – The default is TRUE

[/PASSWORD: password] – The default is **no password**

[/MAXUSERS: number | UNLIMITED] – The default is UNLIMITED

[/HOMEDIRECTORY: TRUE | FALSE] – The default is FALSE

[/SEARCHINDEX: TRUE | FALSE] – The default is TRUE

[/SEARCHINDEXPATH:index path] – The default is the root of the volume

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

#### **Available in ExtremeZ-IP 5.2 and later:**

[/RESET\_PERMISSIONS:TRUE|FALSE] – The default is FALSE

[/FILENAME\_POLICY:TRUE|FALSE] – The default is FALSE

[/IS\_TM\_VOLUME:TRUE|FALSE] – The default is FALSE

[/USE\_TM\_QUOTA:TRUE|FALSE] – The default is FALSE

[/TM\_QUOTA:number] – The default is 100

[/SUPPORT\_ACLS:TRUE|FALSE] – The default is FALSE

[/SUPPORT\_SPOTLIGHT:TRUE|FALSE] – The default is FALSE

#### **To remove a volume:**

```
EZIPUTIL VOLUME /REMOVE
```

/NAME:volumename

[/DISCONNECT:TRUE|FALSE] – The default is FALSE. If TRUE, connected users will be disconnected

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

#### **To suspend a volume:**

```
EZIPUTIL VOLUME /SUSPEND
```

/NAME:volumename

[/DISCONNECT:TRUE|FALSE] – The default is FALSE. If TRUE, connected users will be disconnected

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

#### **To restart a volume:**

```
EZIPUTIL VOLUME /RESTART
```

/NAME:volumename

[/DISCONNECT:TRUE|FALSE] – The default is FALSE. If TRUE, connected users will be disconnected

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To rebuild volume's search index:

```
EZIPUTIL VOLUME /REINDEX
```

/NAME:volumename

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To rebuild volume's WS search index:

**(Available in Acronis Files Connect 10.6.4 and later)**

```
EZIPUTIL VOLUME /WS_REINDEX
```

/NAME:volumename

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To rebuild volume's Acronis Content Indexing search index:

**(Available in Acronis Files Connect 10.6.4 and later)**

```
EZIPUTIL VOLUME /ACI_REINDEX
```

/NAME:volumename

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To update volume's Acronis Content Indexing search index:

**(Available in Acronis Files Connect 10.6.4 and later)**

```
EZIPUTIL VOLUME /ACI_UPDATE
```

/NAME:volumename

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To get a list of volumes:

```
EZIPUTIL VOLUME /LIST
```

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To configure options on a volume:

EZIPUTIL VOLUME /SET

/NAME:volumename

[/OS9ICON:path to OS 9 icon]

[/OSXICON:path to OS X icon]

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To migrate SFM shares (Available in ExtremeZ-IP 5.2 and later):

EZIPUTIL VOLUME /MIGRATE\_SFM

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To replicate SMB shares (Available in ExtremeZ-IP 5.2 and later):

EZIPUTIL VOLUME /REPLICATE\_SMB

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## To produce File Name Policy Violations report:

EZIPUTIL VOLUME /FNPVR

[/NAME:volumename] or '\*' (asterisk), for all volumes (the default)

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## PRINT

### To add a print queue:

EZIPUTIL PRINT /ADD

/NAME:queuename

/METHOD:method – Processing method (see below)

[/PPD:PPD file path]

[/PPD\_ONLY\_FROM\_SERVER: TRUE|FALSE] – The default is FALSE

[/PERSIST: TRUE|FALSE] – The default is TRUE

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

When using the /ADD command, you may pass the following options to specify the processing method:

/METHOD:WINDOWS/PRINTER:printer

/METHOD:LPRHOST:host [/QUEUE:queue]

/METHOD:DIRECTORY/PATH:path to directory

### To rename a print queue:

EZIPUTIL PRINT /RENAME

/NAME:queuename

/NEWNAME:newqueuename

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To remove a print queue:

EZIPUTIL PRINT /REMOVE

/NAME:queuename

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To get a list of print queues:

EZIPUTIL PRINT /LIST

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To refresh validation code text files for all queues:

EZIPUTIL PRINT /REFRESH\_CODES

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To export the print processing log to a text file:

EZIPUTIL PRINT /EXPORT\_LOG

[/CLEARLOG:TRUE|FALSE] – The default is FALSE

/PATH:fullpathoflogfile  
[/SERVERNAME:servername] – If not local  
[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To restart a print queue:

```
EZIPUTIL PRINT /RESTART
```

/NAME:queuename  
[/SERVERNAME:servername] – If not local  
[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To suspend a print queue:

```
EZIPUTIL PRINT /SUSPEND
```

/NAME:queuename  
[/SERVERNAME:servername] – If not local  
[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To replicate shared Windows queues (Available in ExtremeZ-IP 5.2 and later):

```
EZIPUTIL PRINT /IMPORT:WINDOWS
```

/NAME:queuename  
[/SERVERNAME:servername] – If not local  
[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To disable the Print Server (persists until print server is explicitly restarted):

```
EZIPUTIL PRINT /STOP
```

[/SERVERNAME:servername] – If not local  
[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

### To enable the Print Server (persists until print server is explicitly stopped):

```
EZIPUTIL PRINT /START
```

[/SERVERNAME:servername] – If not local  
[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## SESSION

To send a message to connected Mac user(s):

```
EZIPUTIL SESSION /SEND_MESSAGE
```

/MSG:message – the message to send

[/USER\_NAME:username] user name or '\*' (asterisk), for all users (the default)

[/SERVERNAME:servername] – If not local

[/SERVICENAME:servicename] – If not 'ExtremeZ-IP'

## Network Reshare and Kerberos authentication under the local SYSTEM account

It is possible to configure Acronis Files Connect and Kerberos authentication so that you can access Network Reshare volumes with the Acronis Files Connect service running under the Windows local SYSTEM account, and not under a dedicated Active Directory user account.

---

### Warning!

This setup does not meet the highest security standards and it is not recommended for production environments. However, if you need exactly this type of configuration, follow the steps below.

---

## Configuring Network Reshare

### On the remote SMB shares server

1. From **Windows Administrative Tools** in the **Windows Start menu**, navigate to **Computer Management > Local users and groups > Groups**.
2. Double click **Administrators**, and then press **Add**.
3. In **Object** types, ensure that the check box **Computers** is selected.
4. Enter the object name for the Acronis Files Connect server machine and press **OK**.
5. Close all open dialog boxes by pressing **OK**.

---

### Note

Ensure that this Computer object has *Full control* permissions on the remote SMB shares. On EMC Isilon, true Full Control requires that the object is granted the Isilon right *Run as root*. On NetApp, true Full Control requires that the object is part of NetApp's Administrators group.

With some NAS devices, it might not be possible to grant full control over an SMB share to a Computer object. In such a case, create an Active Directory Group and add the specific Computer object in it, then grant full control permissions to the newly created AD group itself.

---

---

**Note**

In order for Time Machine to work on remote SMB shares, the Computer object must have explicit (not as a part of a group) Full Control permissions on them. Otherwise, such volumes could be mounted, but their backups will fail and an error message 'File not found' will be added to the log.

---

**On the Acronis Files Connect server machine**

1. Open the **Acronis Files Connect Administrator** and select **Settings**.
  2. Under the **File Server** tab, click **Enable Network Reshare support**. The **Enable Network Reshare support** button is in the **Miscellaneous** section.
  3. Restart the Acronis Files Connect service.
  4. In the **Acronis Files Connect Administrator**, select **Volumes**.
  5. In the **Volumes** dialog box, click **Create**, and then choose **On another server**.
  6. Type the UNC path to the desired SMB reshare and press **OK**.
- 

**Note**

Ensure that you use a FQDN or NetBIOS name, and not an IP address, otherwise Kerberos logins will fail.

---

## Enabling Kerberos authentication

**On the Acronis Files Connect server machine**

1. Open the **Acronis Files Connect Administrator** and select **Settings**.
2. Under the **File Server** tab, select the **Allow Kerberos Logins** check box and press **OK**. The **Allow Kerberos Logins** check box is in the **Login Methods** section.

**In Active Directory**

1. Log in to the Domain Controller and select **Users and Computers**.
  2. Right click the Acronis Files Connect Server computer object and select **Properties**.
  3. In the **Delegation** tab select the **Trust this computer for delegation to specified services only** radio button and then select **Use any authentication protocol**.
  4. Press **Add** and locate the desired SMB reshare target machine.
  5. In the **Add Services** dialog box, select service type **cifs**.
  6. Close all open dialog boxes by pressing **OK**.
- 

**Note**

If you decide to switch from using a Windows local SYSTEM account to a dedicated Active Directory account, ensure that you clear the **Allow Kerberos Logins** check box in the Acronis Files Connect Administrator first, then proceed with the [Initial Network Reshare configuration](#).

---

## Known issues

Below, you will find a list of all known software or configurations that can result in some loss of Acronis Files Connect functionality.

- Leaving the Acronis Files Connect Administrator application running may negatively impact the stability of the Acronis Files Connect service. Best practice is to open the application, perform the necessary tasks, and then close the application.
- If you have more than one Active Directory server, and Acronis Files Connect is installed on your domain controller, you will encounter AD replication issues by doing the Network Reshare and Kerberos authentication steps.
- Users are unable to input a password for protected volumes on computers running Mac OS X 10.11 and higher. This is an issue in Mac OS X 10.11 and higher.
- Volumes with volume passwords set in Acronis Files Connect cannot be mounted via Finder.app, and prevent browsing the server on which they are located.

---

### Note

The volume password is distinct from the password that a user needs to access the server.

---

- Acronis Files Connect can send messages to AFP connected clients but OS X 10.9 and above no longer natively display these server messages.
- The Acronis Files Connect service can't be sharing data at the same time as a DFS Replication job is run on that data. If it is, there is a risk of corrupting data.
- The print service does not support bi-directional communication. If Acronis Files Connect cannot find an unidirectional print driver, you will be unable to use Acronis Files Connect printing.
- Expanding local drives while they are being shared via Acronis Files Connect is not supported. The recommended procedure is to remove all affected Acronis Files Connect volumes from Acronis Files Connect, expand the desired drive(s) and re-add the volumes in Acronis Files Connect.
- When using Acronis Files Connect Network Reshare feature to share a DFS namespace, attempting to move folders from one root folder to another will result in an error.
- On non-English systems, the "Use current credentials" Kerberos single sign-on feature of the Acronis Files Connect Mac client app doesn't work.
- Kerberos single sign-on doesn't work on a cluster with Network Reshare volumes when using an Active Directory service account to run the Acronis Files Connect service.
- The Acronis Files Connect Mac Client app throws an error if the configured server address is not the server name and the server name is not in the SSL certificate.
- Acronis Files Connect Search only volumes are not supported on Microsoft Failover Clusters.
- HTTPS does not bind to IPv6, generating a warning.
- Tags applied via SMB (Server Message Block) are not returned in Advanced Content Indexing (ACI) searches.
- Time Machine is supported with macOS versions 10.10 to 13.

- Acronis Files Connect integration with Apple Bonjour requires Apple Bonjour version 3.1.0.1 or later. For more information, please refer to the [Acronis Files Connect and Apple Bonjour](#) documentation.
- When Kerberos login support is enabled, the Acronis Files Connect Windows service start-up may take up to a minute if Active Directory services are slow or not available.
- Although Acronis Files Connect supports sharing out the root of the drive, Windows treats permissions at the root of the file system differently from other folder permissions. We recommend that you do not share out drive letters directly. Instead, you should create a sub-folder for your shared volume.

## What's new

For information on current and past releases, please refer to [Acronis Files Connect Release History](#).