Acronis

acronis.com

# Acronis Cyber Files

8.10

Administrator Guide

REVISION: 10/19/2023

# Index

# Table of contents

# Using this help

This help adapts dynamically to the device that you are using to view it.

***Desktop devices and laptops***

***Navigating the content***

On desktop devices and laptops, the navigation pane is expanded by default and the **Contents** tab is selected, so you can view the hierarchy of topics and navigate the content.

To collapse the navigation pane while you read, click  on the top of the pane.

The pane collapses and an expand button () appears on the left of your screen.

***Index and Glossary***

Index and glossary appear in separate tabs in the navigation pane to the left.

***Search***

The search in the upper right returns results only from topics content. To search the index or the glossary, switch the tab and use the tab search.

***Mobile devices***

***Navigating the content***

On hand-held devices, the navigation pane is collapsed by default and the Welcome page is displayed. You can use the arrows in the upper right to go to the next or previous topic.

To view the table of contents, click the menu button in the upper left and select **Contents**.

***Index and Glossary***

Index and glossary are accessible through the menu in the upper left of the screen.

***Search***

The main search returns results only from topics content. To search the index or the glossary, use the menu to the upper left to switch the tab, and use the tab search.

Search is not case-sensitive.

To search for a specific phrase, enclose it in quotes. If you search for multiple words without quotes, the boolean operator AND will be inferred. For example, if you search for `"backup schedule"`, the search results will include topics that contain the phrase "backup schedule", case insensitive. If you search for `backup schedule`, the search query will be equivalent to backup AND schedule. In this case, search results will include all topics that contain both words "backup" and "schedule", regardless of their location.

You cannot search for partial words.

You can use boolean operators to narrow down or extend your search results:

- AND - find only topics that contain all of the listed words. Space between words is always inferred to AND unless you enclose the search query in quotes. Quotes mean you are searching for a phrase.
- OR - use to find topics that contain any of the listed words. This operator extends the search results.

Boolean operators are not case-sensitive. For example, using `AND` or `and` in your search query will not affect the search result.

# Introduction

This guide provides documentation for Acronis Cyber Files administrators.

***About Cyber Files***

Cyber Files is a secure access, sync, and share solution that provides enterprise IT with complete control over business content to ensure security, maintain compliance, and enable BYOD. Cyber Files lets employees use any device - desktop, laptop, tablet or smartphone – to securely access and share content with authorized internal and external individuals, including employees, customers, partners, and vendors.

Cyber Files functionality can be split into two categories.

***Mobile device access***

Mobile device access enables enterprise IT to provide simple, secure and managed access to enterprise file servers, SharePoint and NAS devices for mobile device users, eliminating IT headaches caused by employee use of risky, consumer-based services and other non-compliant alternatives.

Cyber Files allows IT to secure and control access to content while ensuring that mobile device users have access to the content, files, and materials necessary to perform their jobs.

**Note**

For information about mobile device access, please consult the following documentation:

- Desktop and Web client
- iOS app
- Android app

***File Sync & Share***

Sync & Share functionality is the industry’s only such enterprise solution to balance end user need for simplicity and effectiveness with the security, manageability, and flexibility required by enterprise IT.

Cyber Files gives enterprise IT control over who has access to files and lets IT determine whether file-sharing activities meet the compliance and security requirements of the organization. Cyber Files also provides a level of visibility and monitoring not available with consumer-based solutions.

# Quick Start

This guide is intended to provide the easiest and quickest way to install and have Acronis Cyber Files running. It is not suitable for custom configurations. For in-depth information and instructions for each component, please read the appropriate section of the full documentation.

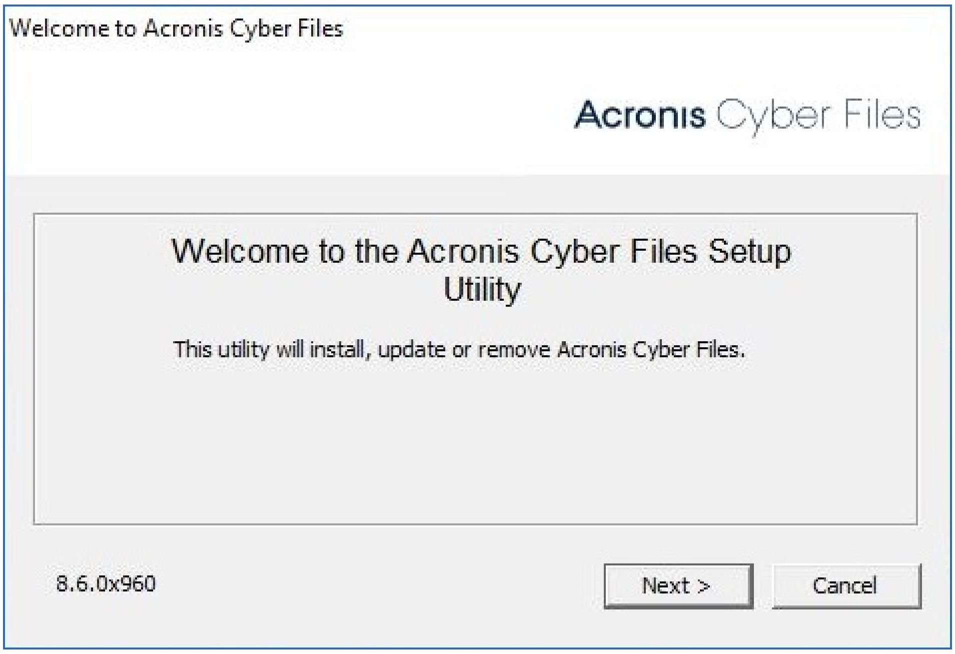
## Installation

**Note**
Please make sure you are logged in as an administrator before installing Acronis Cyber Files.

**Note**
Acronis Cyber Files 8.8 is distributed along with PostgreSQL 11 by default.

### Using the Installer

1. Download the Acronis Cyber Files installer.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



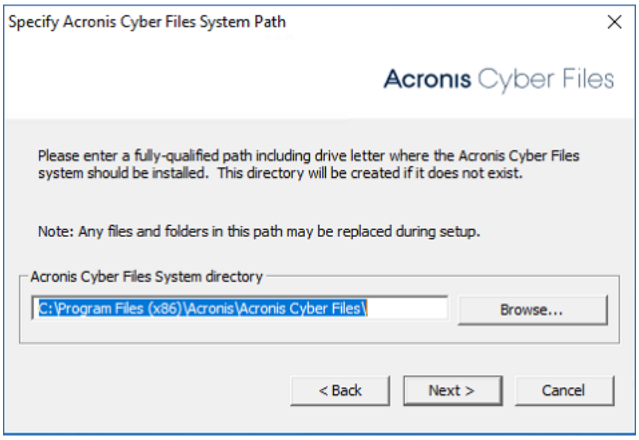
Welcome to Acronis Cyber Files

Welcome to the Acronis Cyber Files Setup Utility

This utility will install, update or remove Acronis Cyber Files.

8.6.0x960

4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.
7. Press **OK** to use the default path for the Acronis Cyber Files main folder.



Specify Acronis Cyber Files System Path

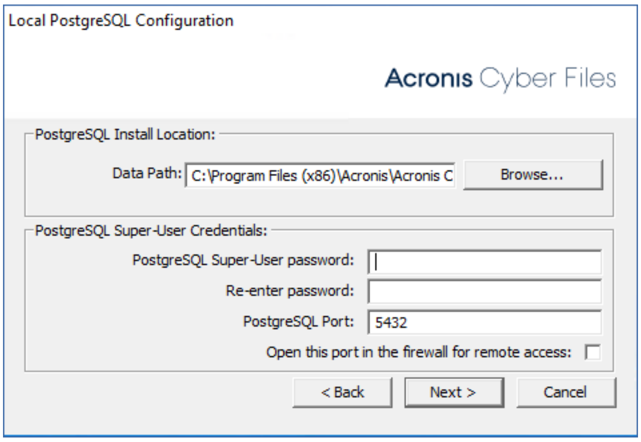
Acronis Cyber Files

Please enter a fully-qualified path including drive letter where the Acronis Cyber Files system should be installed. This directory will be created if it does not exist.

Note: Any files and folders in this path may be replaced during setup.

Acronis Cyber Files System directory: C:\Program Files (x86)\Acronis\Acronis Cyber Files\

8. Set a password for the user Postgres and write it down. This password will be needed for database backup and recovery.



Local PostgreSQL Configuration

Acronis Cyber Files

PostgreSQL Install Location:

Data Path: C:\Program Files (x86)\Acronis\Acronis C

PostgreSQL Super-User Credentials:

PostgreSQL Super-User password:

Re-enter password:

PostgreSQL Port: 5432

Open this port in the firewall for remote access: □

9. A window displaying all the components which will be installed appears. Click **OK** to continue.
10. When the Acronis Cyber Files installer finishes, click **Exit**.
11. The configuration utility will launch automatically to complete the installation.

## Using the Configuration Utility

**Note**

The settings in the Configuration Utility can be changed later on.

Use the default values for each tab and press OK to start Acronis Cyber Files.

# Initial Setup

The Setup Wizard takes the administrator through a series of steps to get the basic functionality of the server working.

**Note**

After the Configuration Utility has run, it will take 30-45 seconds for the server to come up the first time.

Navigate to the Acronis Cyber Files's web interface using the IP address of your network adapter and the desired port. You will be prompted to set the password for the default administrator account.

**Note**

If you run Acronis Cyber Files with the default certificates instead of using certificates from a Certificate Authority, you will get an error that the server is untrusted.

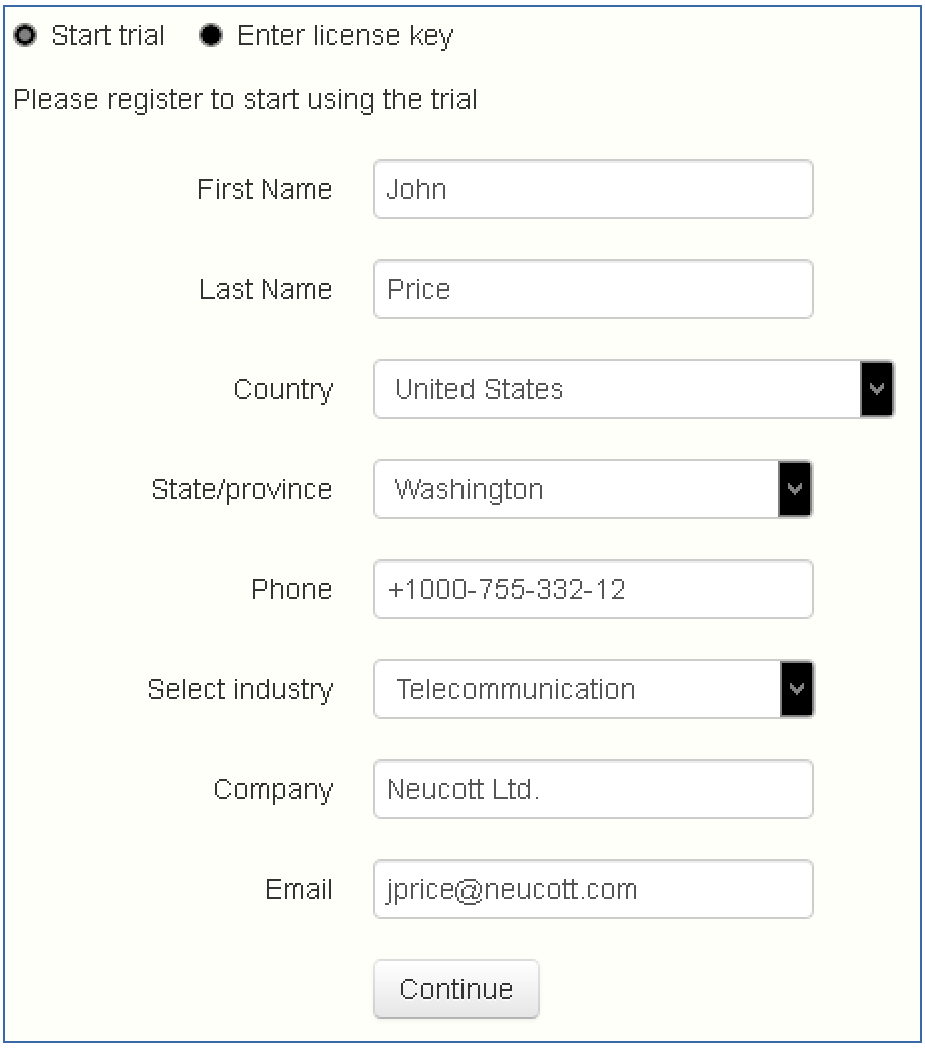
**Note**

All of the settings you see in the Initial Configuration page will also be available after you complete it. For more information on any of the settings, please visit the Server Administration articles.

## Licensing

### To start a trial:

Select **Start Trial**, enter the required information and press **Continue**.



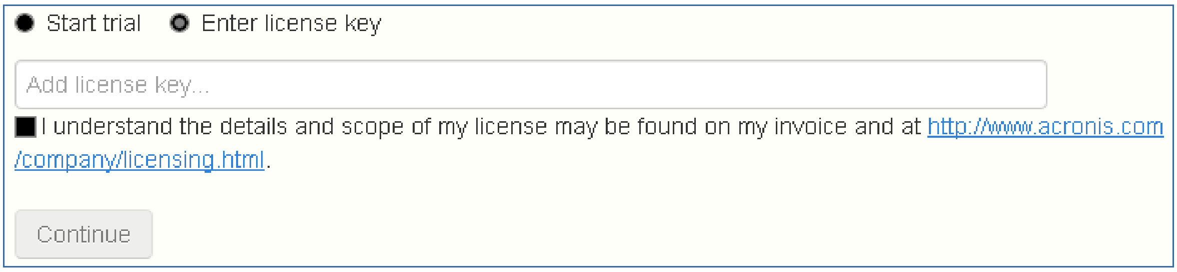
◉ Start trial ● Enter license key

Please register to start using the trial

| | |
|---|---|
| First Name | John |
| Last Name | Price |
| Country | United States |
| State/province | Washington |
| Phone | +1000-755-332-12 |
| Select industry | Telecommunication |
| Company | Neucott Ltd. |
| Email | jprice@neucott.com |

## To license your Acronis Cyber Files instance:

1. Select **Enter license keys**.
2. Enter your license key and select the checkbox.



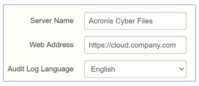
● Start trial ◉ Enter license key

Add license key...

■ I understand the details and scope of my license may be found on my invoice and at http://www.acronis.com/company/licensing.html.

3. Press **Save**.

## General Settings



Server Name: Acronis Cyber Files

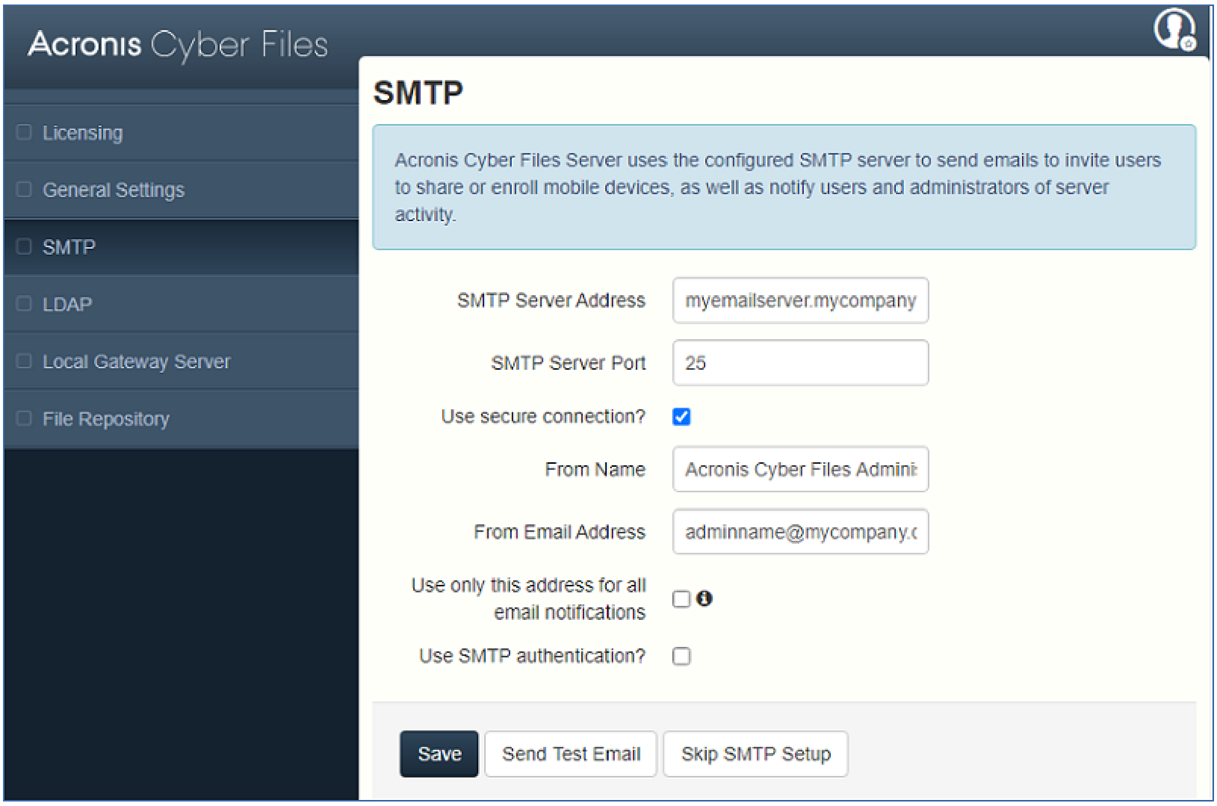
Web Address: https://cloud.company.com

Audit Log Language: English

1. Enter a Server Name.
2. Specify the root DNS name or IP address where users can access the website (starting with http:// or https://).

   Select the default language for the **Audit Log**.
3. The current options are **English, German, French, Japanese, Italian, Spanish, Czesh, Russian, Polish, Korean, Chinese Traditional and Simplified**.
4. Press **Save**.

## SMTP



SMTP

Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to share or enroll mobile devices, as well as notify users and administrators of server activity.

SMTP Server Address: myemailserver.mycompany

SMTP Server Port: 25

Use secure connection? ☑

From Name: Acronis Cyber Files Admini

From Email Address: adminname@mycompany.c

Use only this address for all email notifications ☐

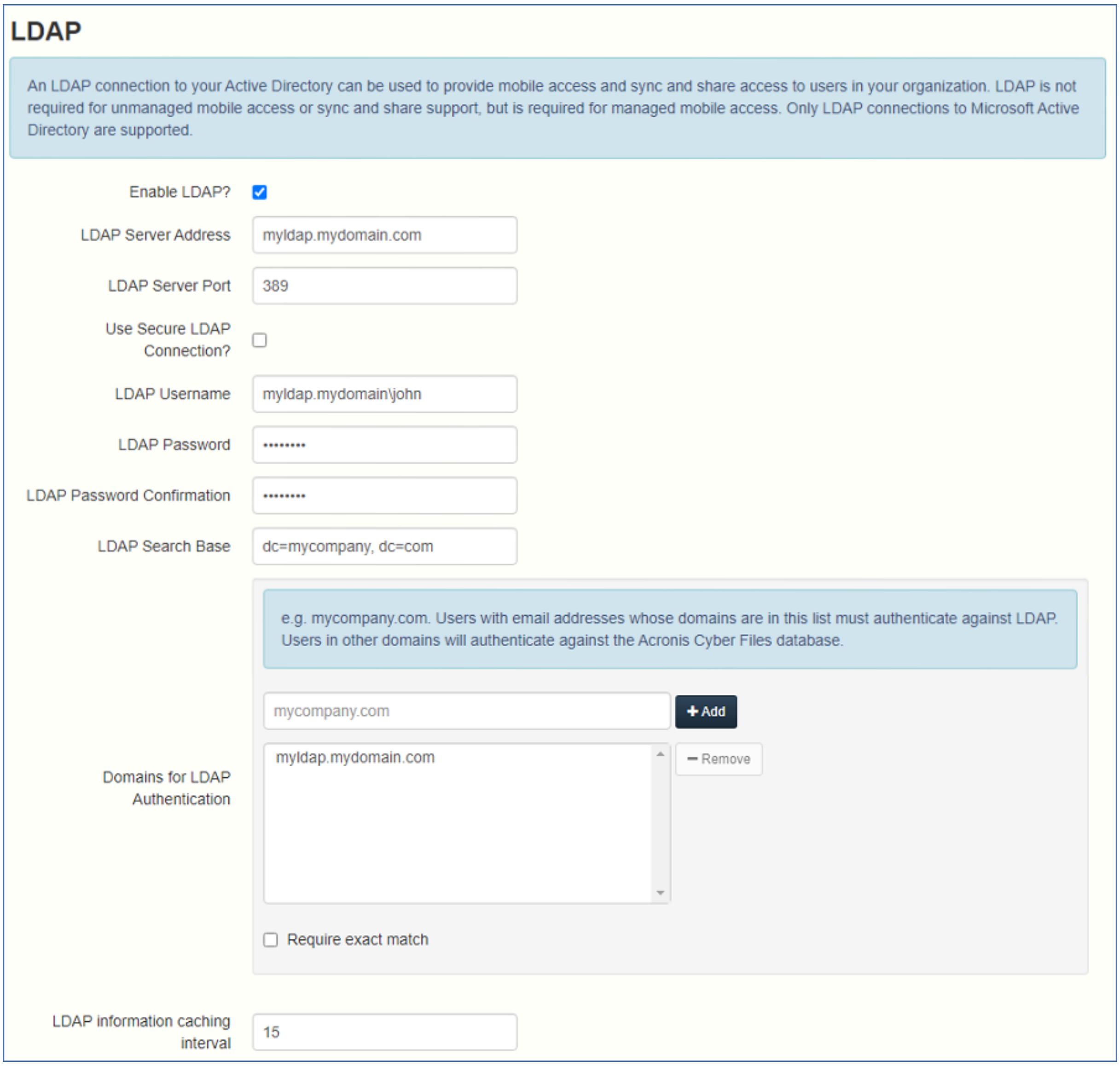
Use SMTP authentication? ☐

**Note**

You can skip this section, and configure SMTP later.

1. Enter the DNS name or IP address of your SMTP server
2. Enter the SMTP port of your server.
3. If you do not use certificates for your SMTP server, unmark **Use secure connection?**.
4. Enter the name which will appear in the "From" line in emails sent by the server.
5. Enter the address which will send the emails sent by the server.
6. If you use username/password authentication for your SMTP server, mark **Use SMTP authentication?** and enter your credentials.
7. Press **Send Test Email** to send a test email to the email address you set on step 5.
8. Press **Save**.

## LDAP



LDAP

An LDAP connection to your Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Only LDAP connections to Microsoft Active Directory are supported.

Enable LDAP? ☑

LDAP Server Address: myldap.mydomain.com

LDAP Server Port: 389

Use Secure LDAP Connection? ☐

LDAP Username: myldap.mydomain\john

LDAP Password: ••••••••

LDAP Password Confirmation: ••••••••

LDAP Search Base: dc=mycompany, dc=com

Domains for LDAP Authentication:

e.g. mycompany.com. Users with email addresses whose domains are in this list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.

mycompany.com

myldap.mydomain.com

☐ Require exact match

LDAP information caching interval: 15

### Note

You can skip this section, and configure LDAP later but some of Acronis Cyber Files' functionality will not be available until you do.

1. Mark **Enable LDAP**.
2. Enter the DNS name or IP address of your LDAP server.
3. Enter the port of your LDAP server.
4. If you use a certificate for connections with your LDAP server, mark **Use Secure LDAP Connection**.
5. Enter your LDAP credentials, with the domain. (e.g. acronis\hristo).
6. Enter your LDAP search base.

7. (i.e.to enable LDAP authentication for an account with the email **joe@glilabs.com**, you would enter **glilabs.com**)
8. Enter the desired domain(s) for LDAP authentication.
9. Press **Save**.

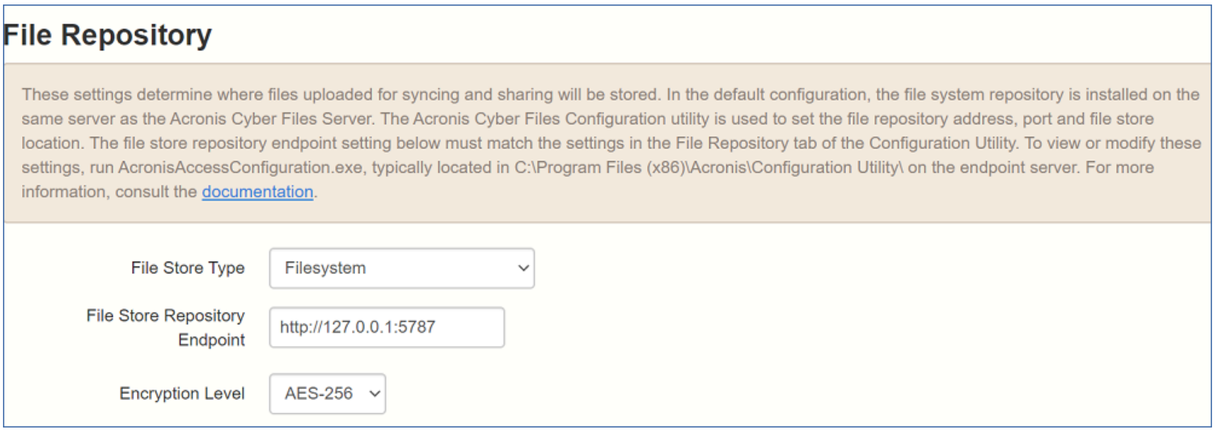
## Local Gateway Server

For KCD to work through mobile clients, it is necessary to enroll to the Local Gateway (the one installed on the same machine as the Tomcat that manages it). Then the Gateway will proxy those requests to that Tomcat (Management) Server.

**Note**
If you're installing both a Gateway Server and the Acronis Cyber Files Server on the same machine, the Gateway Server will automatically be detected and administered by the Acronis Cyber Files Server. You will be prompted to set the DNS name or IP address on which the Local Gateway Server will be reachable by clients. You can change this address later on.

1. Set a DNS name or IP address for the local Gateway Server.
2. Press **Save.**

**File Repository**



File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The file store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the documentation.

File Store Type: Filesystem

File Store Repository Endpoint: http://127.0.0.1:5787

Encryption Level: AES-256

Select a file store type. Use **Filesystem** for a file store on your computers or any of the following options for a file store on the cloud: **Acronis Storage**, **Microsoft Azure Storage**, **Amazon S3**, **Swift S3**, **Ceph S3** and **Other S3-Compatible Storage**.

**Note**
You can use the **Other S3-Compatible Storage** option with S3 storage providers not on this list, but we cannot guarantee that everything will work properly.

**Note**
MinIO S3 storage type is supported and can be configured as **Other S3-Compatible Storage** option, however, we do not support it over a non-secure HTTP connection.

1. Enter the DNS name or IP address for the file repository service.

**Note**
The Cyber Files Configuration utility is used to set the file repository address, port and file store location. The File Store Repository Endpoint setting must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility` on the endpoint server.

2. Select an encryption level. Choose between **None**, **AES-128** and **AES-256**.
3. Select the minimum free space available before your server sends you a warning.
4. Press **Save**.

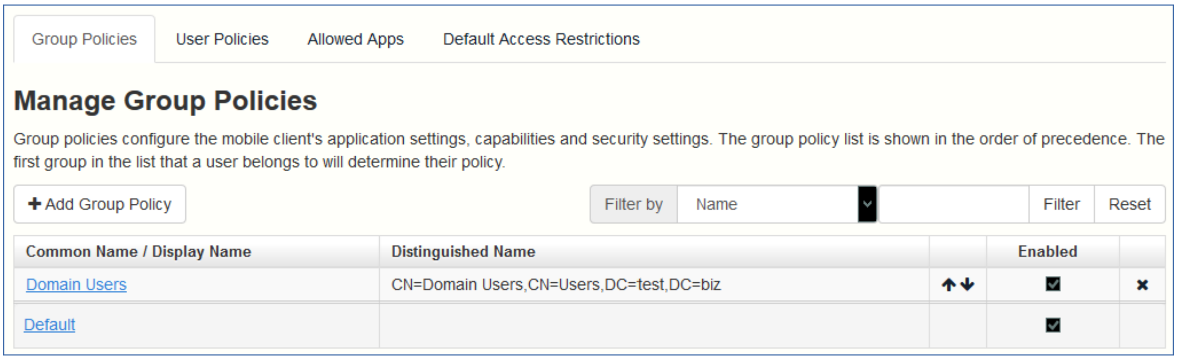
# Mobile Access

## Configuring the Default policy

All mobile clients enrolled in management with the Acronis Cyber Files Web Server have their functionality governed and controlled by a User or Group policy. The Default policy is created automatically on installation and has the lowest priority (the highest being a personal User policy), but it affects all users that do not have a User policy and are not members of a Group policy. The Default policy is enabled by default.

### Configuring the Default policy

1. Open the Acronis Cyber Files web console.
2. Navigate to **Mobile Access** -> **Policies** -> **Group Policies**.



**Manage Group Policies**

Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

| Common Name / Display Name | Distinguished Name | | Enabled | |
|---|---|---|---|---|
| Domain Users | CN=Domain Users,CN=Users,DC=test,DC=biz | ↑↓ | ☑ | ✖ |
| Default | | | ☑ | |

3. Make sure that there is a check under the **Enabled** field and click on the **Default** policy.
4. View the settings and make changes if desired. For an in-depth overview of all the settings, please visit the Policies section.

## Mobile Clients

When you run the Acronis Cyber Files app for the first time, you can either try the app in demo mode or you can enroll to your company's server.

### To test out the app in the demo mode

Demo mode allows users to try the Acronis Cyber Files app even if their company doesn't have a Acronis Cyber Files Web Server. This is an environment setup for demonstration purposes only, not all features are accessible.

1. Install the app and open it.
2. After the welcome screen, select **Use our demo server**
3. You will be enrolled to the demo server.

> **Note**
> Once enrolled, you will have read-only access to a few shared folders on the demo server, as well as a couple of sync folders. These folders contain sample files, PDFs, image files, etc. You are able to browse, search, view & edit these available files and save edited files locally within the app if you so desire.

4. You can switch to your company's server at any point in time.

### To enroll to your company's server

1. Install the app and open it.
2. After the welcome screen, select **Use your company server**.
3. Fill in your server's address, your PIN (if required), username and password.
4. After completing the entire form, tap the **Enroll** button.
5. Depending on the configuration of your company's server, you may be warned that your management server's security certificate is not trusted. To accept this warning and proceed, you can click **Proceed Always**.
6. If an application lock password is required for your Acronis Cyber Files mobile app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

A confirmation window may appear if your management policy restricts the storage of files in Acronis Cyber Files or disables your ability to add individual servers from within the Acronis Cyber Files mobile app. If you have files stored locally in the Acronis Cyber Files mobile app, you will be asked to confirm that any files in your **My Files** local file storage will be deleted. If you select No, the management enrollment process will be canceled and your files will remain unchanged.

## Client guides

For information about Cyber Files clients, please consult the client guide documentation below:

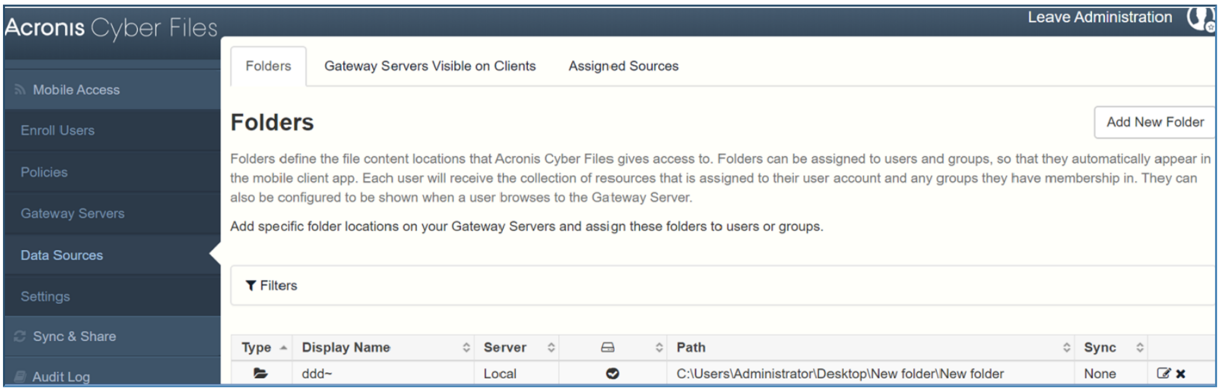
- Desktop and Web client
- iOS app
- Android app

# Sync&Share

## Sync&Share Data Source

Once you install and configure Acronis Cyber Files, it will automatically create a Data Source called "**Sync&Share**" and will add the **Domain Users** group to the assigned users and groups list by default. At any time the administrator(s) can change or remove this Data Source folder.

This default Data Source will be available to all newly created users who are part of the **Domain Users** group and it is reachable via mobile, desktop and web clients.



Folders

Folders define the file content locations that Acronis Cyber Files gives access to. Folders can be assigned to users and groups, so that they automatically appear in the mobile client app. Each user will receive the collection of resources that is assigned to their user account and any groups they have membership in. They can also be configured to be shown when a user browses to the Gateway Server.

Add specific folder locations on your Gateway Servers and assign these folders to users or groups.

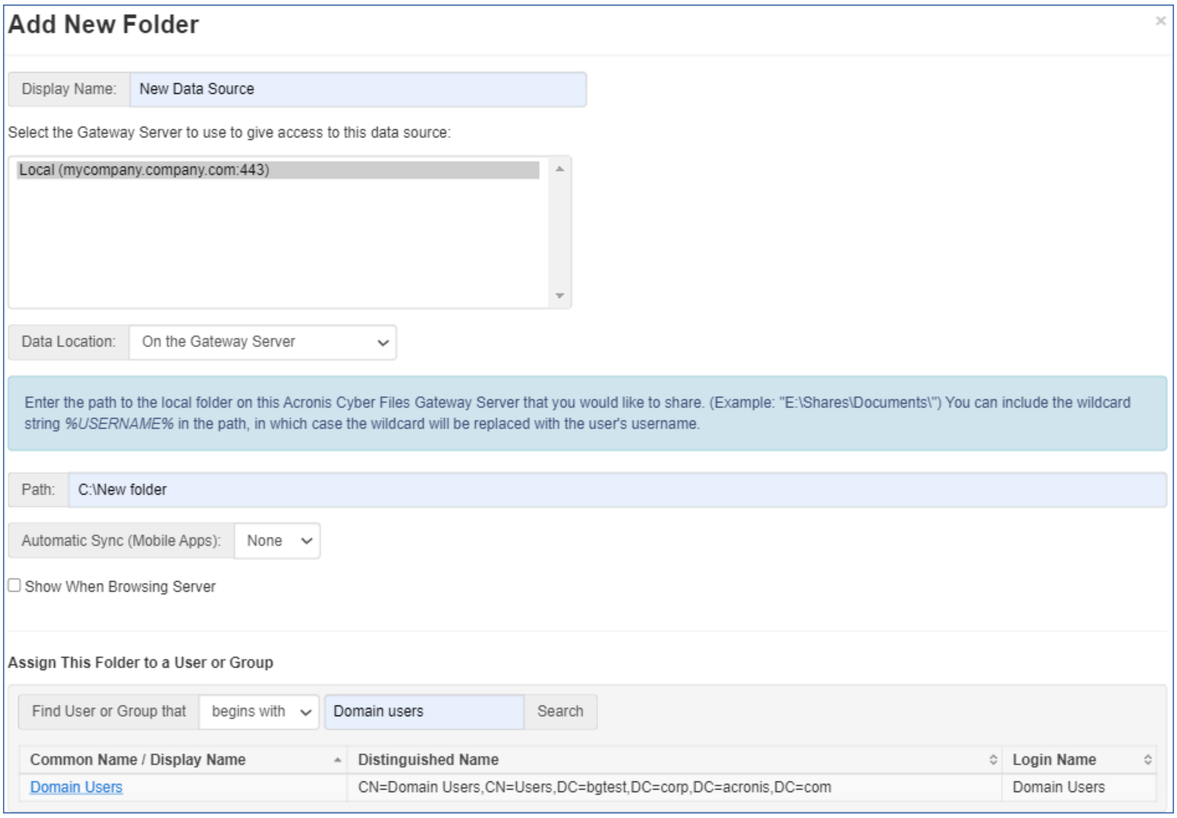
| Type | Display Name | Server | 🖴 | Path | Sync | |
|---|---|---|---|---|---|---|
| 📂 | ddd~ | Local | ✓ | C:\Users\Administrator\Desktop\New folder\New folder | None | ✎ ✖ |

## Sharing content to your users

Sharing existing content only requires that you setup a Data Source for it and assign that Data Source to the desired users or groups.

### Creating a Data Source

1. Open the Acronis Cyber Files Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Data Sources** tab.
4. Go to **Folders**.
5. Click **Add New Folder**.



Add New Folder

Display Name: New Data Source

Select the Gateway Server to use to give access to this data source:

Local (mycompany.company.com:443)

Data Location: On the Gateway Server

Enter the path to the local folder on this Acronis Cyber Files Gateway Server that you would like to share. (Example: "E:\Shares\Documents\") You can include the wildcard string *%USERNAME%* in the path, in which case the wildcard will be replaced with the user's username.

Path: C:\New folder

Automatic Sync (Mobile Apps): None

□ Show When Browsing Server

Assign This Folder to a User or Group

Find User or Group that begins with Domain users Search

| Common Name / Display Name | Distinguished Name | Login Name |
|---|---|---|
| Domain Users | CN=Domain Users,CN=Users,DC=bgtest,DC=corp,DC=acronis,DC=com | Domain Users |

6. Enter a display name for the folder.
7. Select the Gateway Server that will give access to this folder.
8. Select the location of the data. This can be on the actual Gateway Server, on another SMB server, on a SharePoint Site or Library or on a Sync & Share server.

**Note**
You are not allowed to use a folder from a removable media as a shared folder. Please choose one from a different location.

**Note**
When selecting Sync & Share, make sure to enter the full path to the server with the port number. e.g.: https://mycompany.com:3000

9. Based on your choice of location, enter the path to that folder, server, site or library.
10. Select the **Sync** type of this folder.
11. Enable **Show When Browsing Server** if you want this Data Source to be visible when Acronis Cyber Files mobile clients browse the Gateway Server.

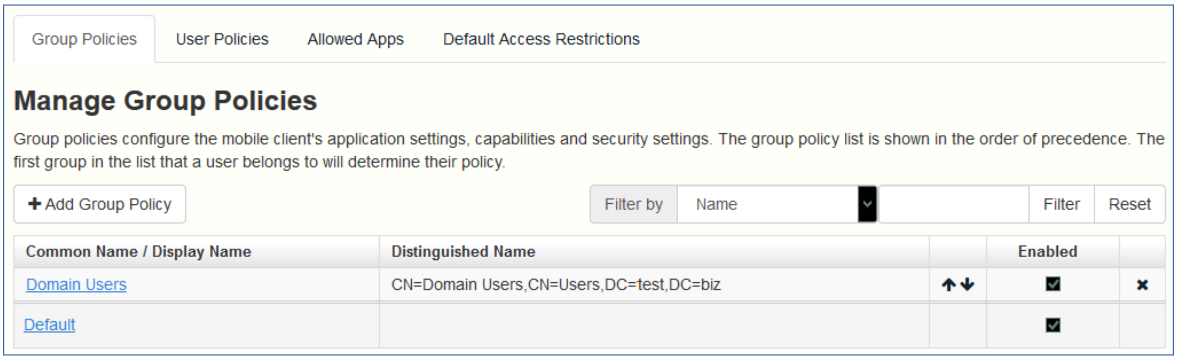
**Note**
When creating SharePoint Data Sources, you will have the option to enable the displaying of SharePoint followed sites.

12. Click the **Save** button.

## Allowing Web client users to access File Servers and more

By default, users cannot open NAS, File Servers and SharePoint resources from the Web client. However, enabling it is simple and grants more possibilities to the web users.

1. Open the Web Interface and browse to **Mobile Access** --> **Policies**. (Note even though policies primarily relate to the mobile app, the setting for web access is there too.)
2. Select the policy you want to change. If you haven't made any new ones, select the **Default** policy.

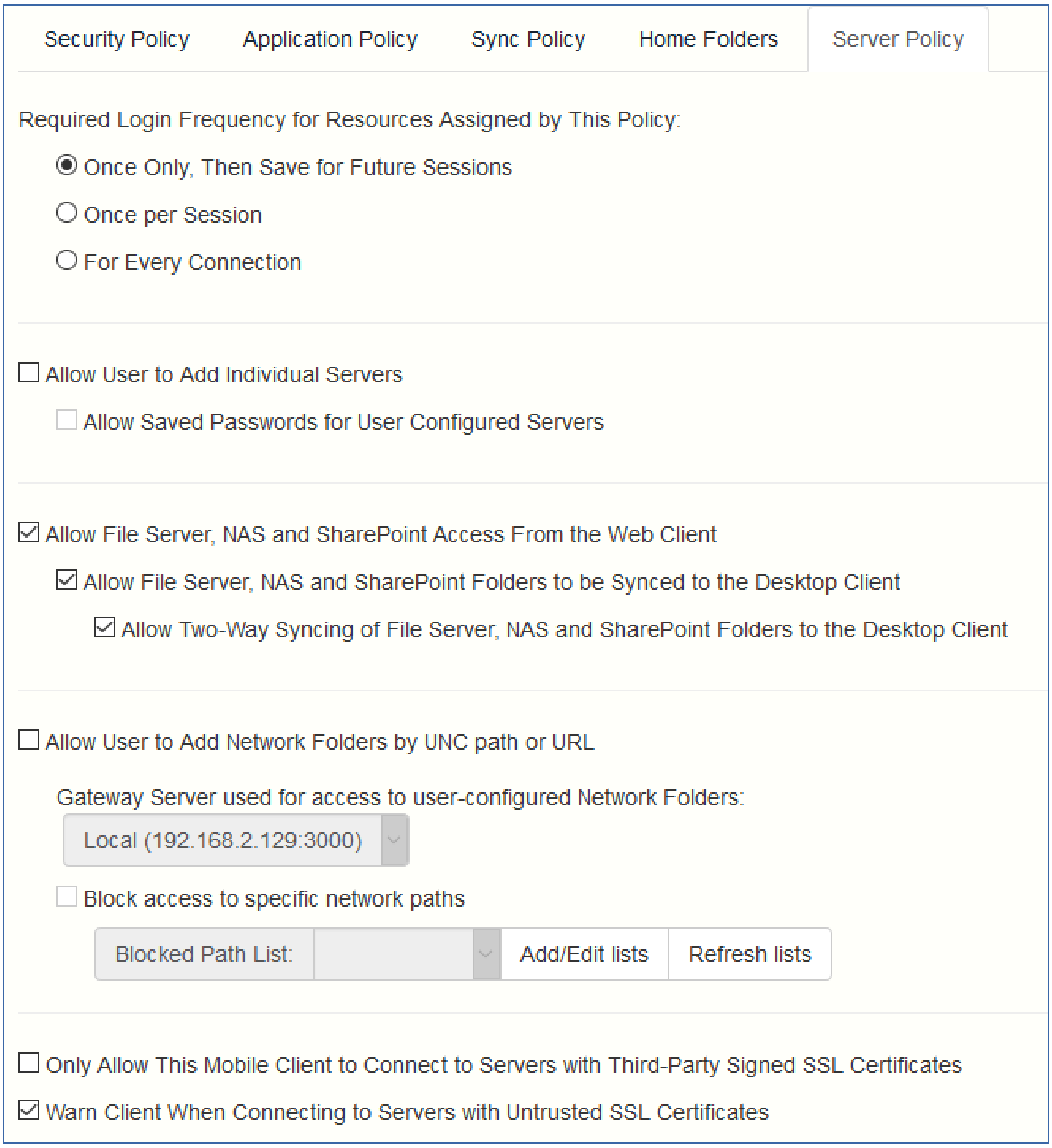


Manage Group Policies

Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

| Common Name / Display Name | Distinguished Name | | Enabled | |
|---|---|---|---|---|
| Domain Users | CN=Domain Users,CN=Users,DC=test,DC=biz | ↑↓ | ☑ | ✖ |
| Default | | | ☑ | |

3. On the **Server Policy** tab, select the box **Allow File Server, NAS, and SharePoint Access from the Web Client**.



Required Login Frequency for Resources Assigned by This Policy:

● Once Only, Then Save for Future Sessions

○ Once per Session

○ For Every Connection

□ Allow User to Add Individual Servers

□ Allow Saved Passwords for User Configured Servers

☑ Allow File Server, NAS and SharePoint Access From the Web Client

☑ Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client

☑ Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client

□ Allow User to Add Network Folders by UNC path or URL

Gateway Server used for access to user-configured Network Folders: Local (192.168.2.129:3000)

□ Block access to specific network paths

□ Only Allow This Mobile Client to Connect to Servers with Third-Party Signed SSL Certificates

☑ Warn Client When Connecting to Servers with Untrusted SSL Certificates

4. Consider whether you want to also enable desktop syncing, for the chosen policy, using the sub-options **Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client** and **Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client**.
5. Click **Save**.

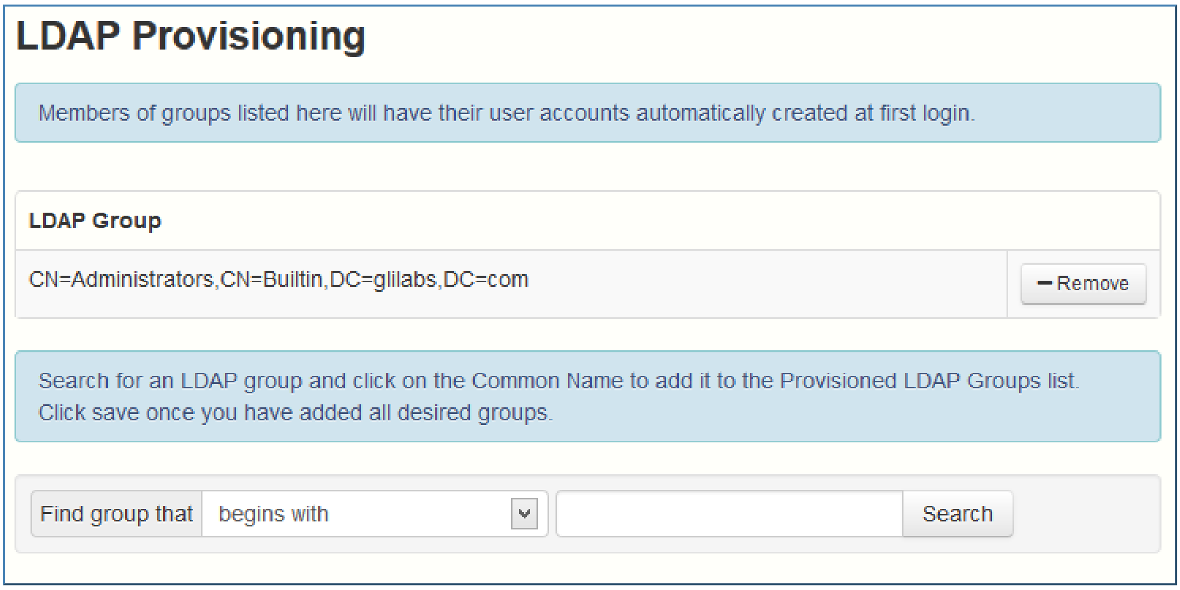
This is implemented as a per-policy setting to provide more flexibility. You may want to enable the setting for another group or some individual policies.

## LDAP Provisioning

Enabling LDAP Provisioning allows your users to login with their LDAP credentials and have their accounts created automatically instead of the administrator having to invite each user (or group) individually. These accounts take up a license from your license pool so choose a specific LDAP group (or groups) for provisioning.

## Enabling LDAP Provisioning

1. Open the Acronis Cyber Files web console.
2. Navigate to **Sync&Share** > **LDAP Provisioning**.



LDAP Provisioning

Members of groups listed here will have their user accounts automatically created at first login.

| LDAP Group | |
|---|---|
| CN=Administrators,CN=Builtin,DC=glilabs,DC=com | − Remove |

Search for an LDAP group and click on the Common Name to add it to the Provisioned LDAP Groups list. Click save once you have added all desired groups.

3. Enter the name of an LDAP group (or groups).
4. Select the desired group(s) and click **Save**.

The users in the selected group(s) will now have their Acronis Cyber Files accounts automatically generated the moment they try to login to Acronis Cyber Files with their LDAP credentials.

# Web and Desktop clients

- The Web client allows all users with valid Acronis Cyber Files credentials to access and share files and folders from their preferred browser.
- The Desktop client enables users to share big files easily and ensures that their files are always up to date.

# Client guides

For information about Cyber Files clients, please consult the client guide documentation below:

- Desktop and Web client
- iOS app
- Android app

# Installing

## Requirements

You must be logged in as an administrator before installing Acronis Cyber Files. Verify that you meet the following requirements.

### Operating System Requirements

**Note**
Acronis Access Advanced 7.2.3 is the last version that supports 32bit operating systems. Newer versions of Acronis Cyber Files will support only 64bit ones.

**Note**
Acronis Access Advanced 7.4.x is the last version that supports Windows XP and Vista. Newer versions of Acronis Cyber Files will not support connections from those operating systems.

#### Recommended:

- Windows Server 2016 Standard & Datacenter
- Windows Server 2012 R2 Standard & Datacenter

#### Supported:

- Windows Server 2019 Standard & Datacenter
- Windows Server 2016 Standard & Datacenter
- Windows Server 2012 R2 Standard & Datacenter
- Windows Server 2012 Standard & Datacenter

**Note**
For testing purposes, the system can be installed and run on Windows 7 or later. These desktop class configurations are not supported for production deployment.

### Mobile client requirements

#### Supported mobile devices

- Apple-branded devices running versions of iOS or iPadOS supported by Acronis Cyber Files, as below.
- Devices running versions of Android supported by Acronis Cyber Files, as below.

**Important**
x86 family processors are not supported.

## Minimum supported mobile operating systems

**Note**
For Ivanti MDM or Microsoft Intune deployments, support for operating system versions is contingent on support in the specific SDK versions included in the mobile client app. SDK version details can be found in the linked release notes.

- For iOS or iPadOS, the supported minimum is version 14.
  For support details for newer operating system versions, see the release notes for Acronis Cyber Files app for iOS.
- For Android, the supported minimum is version 7.
  For support details for newer operating system versions, see the release notes for Acronis Cyber Files app for Android.

## Mobile app downloads

- For iOS.
- For Android.

**Note**
The standard and MDM Android APK can be download from the product download page.

# Minimum Hardware Requirements

## Example deployments

These deployment figures assume that all of Acronis Cyber Files components are running on the same virtual machine or physical server.

**Note**
The recommended disk space assumes that the File Repository's file purging of old & deleted revisions is configured.

**Note**
The recommended disk size is only a starting point and may need to be increased, depending on the size & number of files being synced by users.

**Note**
Acronis Cyber Files Web Server can be installed on virtual machines.

**Note**
Make sure that you have enough space to run the Acronis Cyber Files installer. 1GB of space is required for the installer to run.

**Note**
These values are our requirements for a production environment. If you plan on starting a trial or installing Acronis Cyber Files for testing purposes, you may start with the Small Deployments hardware requirements, and increasing as needed, depending on your test load.

### Small Deployments

- Up to 25 users

> **Note**
> 'Users', in this context, means the sum total of all user account and group objects contained within the LDAP search base entered in Acronis Cyber Files at **General Settings** > **LDAP**.

- CPU: Intel i7 Xeon class with 4 cores or AMD equivalent.
- RAM: 16 GB
- Disk Space: 100 GB

### Medium Deployments

- Up to 500 users

> **Note**
> 'Users', in this context, means the sum total of all user account and group objects contained within the LDAP search base entered in Acronis Cyber Files at **General Settings** > **LDAP**.

- CPU: Intel i7 Xeon class with 8 cores or AMD equivalent.
- RAM: 40 GB
- Disk Space: 2 TB RAID

### Large Deployments

- Up to 2500 users.

> **Note**
> 'Users', in this context, means the sum total of all user account and group objects contained within the LDAP search base entered in Acronis Cyber Files at **General Settings** > **LDAP**.

- CPU: Intel i7 Xeon class with 16 cores or AMD equivalent.
- RAM: 64 GB
- Disk Space: 10 TB RAID

**Note**
For deployments larger than 2500 users, a clustered server configuration is recommended. Please contact Acronis support for deployments larger than 2500 users.

**Note**
You may need substantially more resources, depending on your workflows and other applications running on the server.

## Network Requirements

- 1 Static IP Address. 2 IP addresses may be needed for certain configurations.
- Optional but recommended: DNS names matching the above IP addresses.
- Network access to your Domain Controller if you plan on using Active Directory (LDAP).
- Network access to an SMTP server for email notifications and invitation messages.
- The address **127.0.0.1** is used internally by the mobile app and should not be routed through any kind of tunnel - VPN, MobileIron, etc.
- All machines running the Acronis Cyber Files Web Server or the Gateway Server need to be bound to the Windows Active Directory.

There are two components that handle HTTPS traffic, the Gateway Server and the Acronis Cyber Files Web Server. The Gateway Server is used by mobile clients to access both files and shares from the Data Sources. The Acronis Cyber Files Web Server provides the web user interface for Sync & Share clients, and is also the administration console for both Mobile Access and Sync & Share.

For most deployments it is recommended that one IP address is used for both servers, with different ports and separate DNS entries. This one IP address configuration is sufficient for most installations. The server can be configured to use separate IP addresses for each component if your specific deployment and/or setup requires it.

**If you want to allow mobile devices access from outside your firewall, there are several options:**

- **Port 443 access**: Acronis Cyber Files uses HTTPS for encrypted transport, so it fits in naturally with common firewall rules allowing HTTPS traffic on port 443. If you allow port 443 access to your Acronis Cyber Files Web Server, authorized iPad clients can connect while inside or outside of your firewall. The app can also be configured to use any other port you prefer.
- **VPN:** The Acronis Cyber Files mobile app supports access through a VPN connection. Both the built in iOS VPN client and third-party VPN clients are supported. iOS management profiles can optionally be applied to devices using Mobile Device Management (MDM) systems or the Apple iPhone Configuration Utility to configure the certificate-based iOS “VPN-on-demand” feature, giving seamless access to Acronis Cyber Files Web Servers and other corporate resources.
- **Reverse proxy server:** If you have a reverse proxy server set up, iPad clients can connect without the need for an open firewall port or a VPN connection. The Acronis Cyber Files mobile app supports reverse proxy pass-through authentication, username / password authentication, Kerberos constrained authentication delegation and certificate authentication. For details on adding certificates to the Acronis Cyber Files mobile app, visit the Using client certificates article.
- **MobileIron AppConnect enrolled app**: If the Acronis Cyber Files mobile app is enrolled with MobileIron's AppConnect platform, then all network communication between Acronis Cyber Files

mobile app clients and Gateway Servers can be routed through the MobileIron Sentry. For more information see the MobileIron AppConnect manual page.

**Certificates:**
AcronisCyber Files ships and installs with self-signed certificates for testing purposes. Production deployments should implement proper CA certificates.

**Note**
Certain web browsers will display warning messages when using self-signed certificates. Dismissing those messages allows the system to be used without problems. Using self-signed certificates for production conditions is not supported.

**Note**
When enabling the LDAP secure connection feature, Acronis Cyber Files requires the fully qualified domain name of the LDAP server to be present in the certificate either as a Common Name (CN) or as a Subject Alternative Name (SAN).

# Desktop Client Requirements

## System requirements

### Supported operating systems

- Windows 7, 8, 8.1, 10, and 11

  **Note**
  Desktop client 7.4 is the last version compatible with Windows XP and Vista. To use a newer version of the Acronis Cyber Files desktop client, update your Windows OS. Access Advanced 7.4 is the last server version to allow connections from Windows XP or Vista.

  **Note**
  Acronis Cyber Files will not support Windows Server 2008 R2 starting with 8.6 release (Microsoft official announcement reference).

- macOS X 10.13 to 10.15 with Mac compatible with 64-bit software
- macOS 11 Big Sur and macOS 12 Monterey with both Intel x86-64 and Apple silicon CPUs

  **Note**
  Desktop client 7.1.2 is the last version compatible with macOS X 10.6 and 10.7. Desktop client 8.5 is the last one compatible with macOS X 10.12. To use a newer version of the Acronis Cyber Files desktop client, update your macOS.

**Note**

When installing the Acronis Cyber Files Desktop client, make sure that the sync-folder you create is not in a folder synchronized by another software. For a list of known conflicts, visit Conflicting Software.

### Supported web browsers:

- Mozilla Firefox 60 and later
- Microsoft Edge 25 or later
- Google Chrome 64 and later
- Safari 12 and later
- Opera 72 and later

## Additional requirements

The installation process requires that you have:

- Acronis Cyber Files Desktop Client installer executable and appropriate rights to run it.
- Address of the server you are going to use (provided by your administrator or via email).
- Login credentials for the server (from Active Directory, or provided by your administrator, or via email).

## PostgreSQL Administrator requirements

The Acronis Cyber Files PostgreSQL Administrator GUI application (pgAdmin) is installed together with PostgreSQL.

This requires one of the following web browsers, running on the server where PostgreSQL is installed.

- Chrome 90+
- Firefox 78+
- Edge 91+

# Installing Acronis Cyber Files on your server

The following steps will allow you to perform a fresh install and test Acronis Cyber Files with HTTPS using the provided self-signed certificate.

**Note**

For upgrade instructions, see the upgrading section.

**Note**

For instructions on installing on a cluster, see the load balancing section.

The installation of Cyber Files involves three steps:

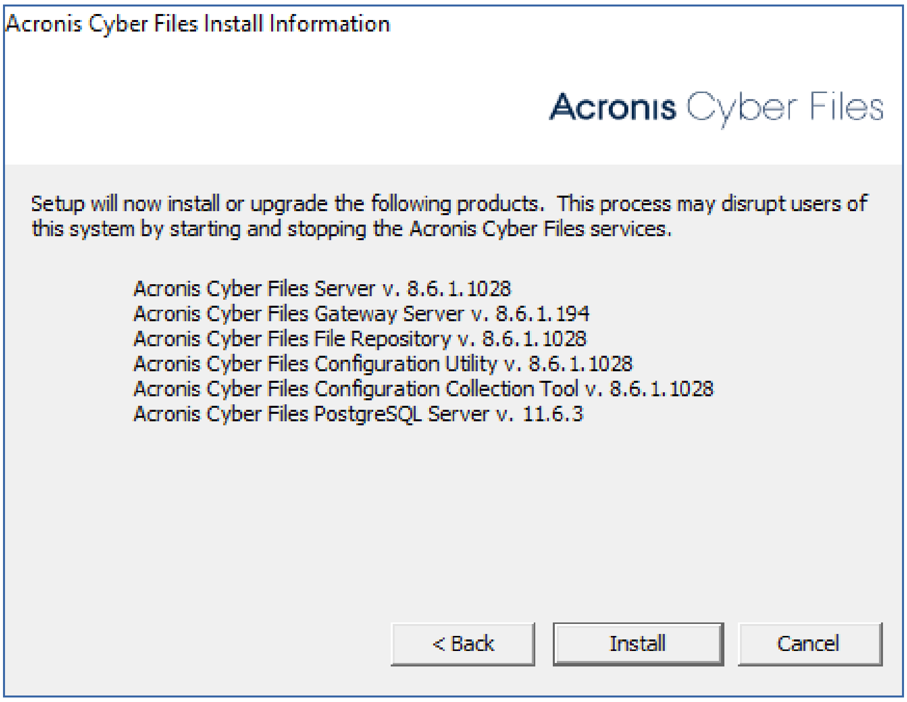
1. Installation of the Cyber Files web server installer.
2. Configuration of the network ports and SSL certificates used by the Cyber Files web server.
3. Using the web-based setup wizard to configure the server for your use.

## Installing Cyber Files

Make sure you are signed in as an administrator before installing Cyber Files.

1. Download the Cyber Files installer.
2. Disable any anti-virus software you have to avoid possible interruption of the installation procedure. Interruption results in a failed installation.
3. Open the installer executable.
4. Select **Next**.
5. Read and accept the license agreement.
6. Select **Install**.

> **Note**
> If you're deploying multiple Cyber Files servers, or you are installing a non-standard configuration, you can select which components to install from the **Custom Install** button.



Acronis Cyber Files Install Information

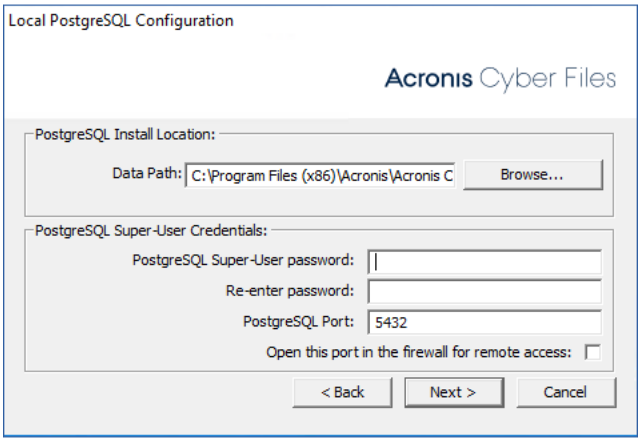
Setup will now install or upgrade the following products. This process may disrupt users of this system by starting and stopping the Acronis Cyber Files services.

Acronis Cyber Files Server v. 8.6.1.1028
Acronis Cyber Files Gateway Server v. 8.6.1.194
Acronis Cyber Files File Repository v. 8.6.1.1028
Acronis Cyber Files Configuration Utility v. 8.6.1.1028
Acronis Cyber Files Configuration Collection Tool v. 8.6.1.1028
Acronis Cyber Files PostgreSQL Server v. 11.6.3

7. Either use the default path or select a new one for the Cyber Files main folder.
8. Select **OK**.
9. Specify a password for the PostgreSQL super-user.

**Note**

The PostgreSQL super-user password cannot include a colon (**:**), a semi-colon (**;**), or an asterisk (*****).



Local PostgreSQL Configuration

PostgreSQL Install Location:

Data Path: C:\Program Files (x86)\Acronis\Acronis C

PostgreSQL Super-User Credentials:

PostgreSQL Super-User password:

Re-enter password:

PostgreSQL Port: 5432

Open this port in the firewall for remote access: □

**Important**

Write the PostgreSQL super-user password down and store it somewhere safe. It is needed for database backup and recovery.

10. Select **OK** to close the list of installed components.
11. Select **Exit** when the Cyber Files installer finishes.
12. The configuration utility launches automatically.

**Note**

For instructions on using the configuration utility, see Using the Configuration Utility.

# Using the configuration utility

The Acronis Cyber Files installer comes with a configuration utility, which allows you to quickly and easily set up the access to your Cyber Files Gateway server, File Repository, and Cyber Files Web Server.

**Note**

See the Network Requirements section for more information on best practices for the IP address configurations of Cyber Files.

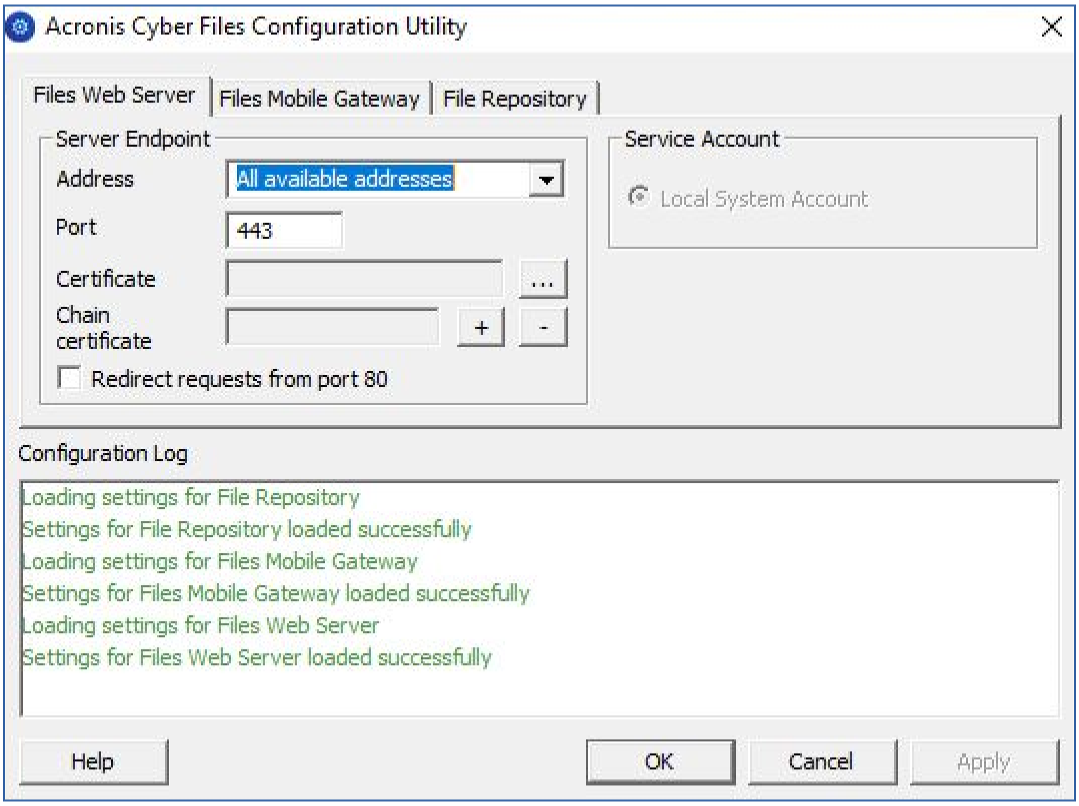
**Note**

For information on adding your certificate to the Microsoft Windows Certificate Store, visit the Using Certificates article.

## Configuration utility overview

The settings in the configuration utility can be modified at any time by running the utility and making the necessary changes. It will automatically adjust the necessary configuration files and restart the services for you.

### Files Web Server tab



Address: All available addresses

Port: 443

Certificate:

Chain certificate:

□ Redirect requests from port 80

● Local System Account

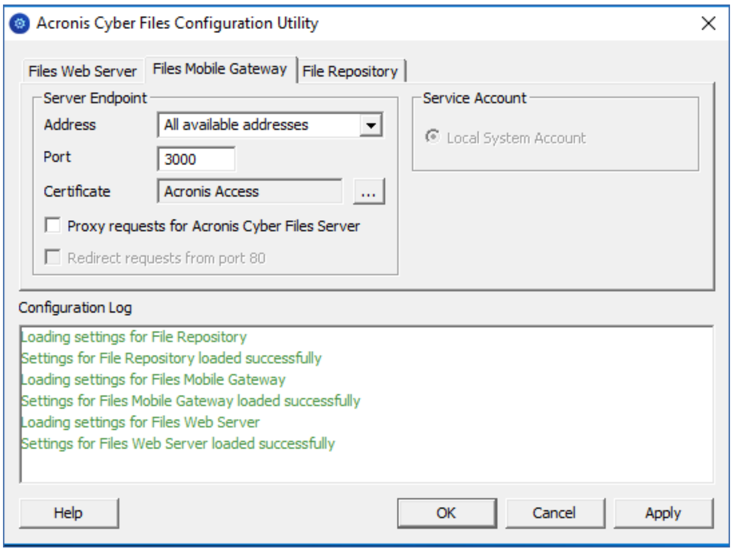
```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

The Cyber Files Web Server provides the web user interface for Cyber Files clients, and is also the administration console for both Mobile Access and Sync & Share.

- **Address** - The IP address of your Web Interface or pick **All Addresses** to listen on all available interfaces.
- **Port** - The port of your Web Interface.
- **Certificate** - Path to the certificate for your Web Interface. You can choose a certificate from the Microsoft Windows Certificate Store.
- **Chain Certificate** - Path to the Intermediate certificate for your Web Interface. You can choose one from the Microsoft Windows Certificate Store. This certificate is only required if your Certificate Authority has also issued you an Intermediate certificate.
- **Redirect requests from port 80** - When selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.

- **Service Account -** This allows the Cyber Files Web Server service to run in the context of another account.  This is normally not required in typical installations.

## Files Mobile Gateway tab



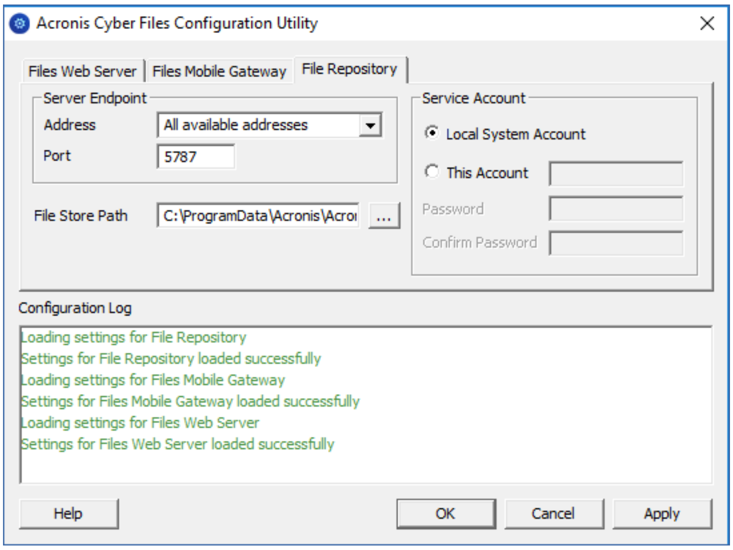
Address: All available addresses
Port: 3000
Certificate: Acronis Access
☐ Proxy requests for Acronis Cyber Files Server
☐ Redirect requests from port 80
● Local System Account

```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

The Gateway Server is used by mobile clients to access both files and shares.

- **Address -** The IP address of your Gateway Server or pick **All Addresses** to listen on all interfaces.
- **Port -** The port of your Gateway Server.
- **Certificate -** Path to the certificate for your Gateway Server. You can choose a certificate from the Microsoft Windows Certificate Store.
- **Service Account -** This allows the Gateway Server service to run in the context of another account.  This is normally not required in typical installations.
- **Proxy requests for Cyber Files Server** - When checked, users will connect to the Gateway Server which will then proxy them to the Cyber Files Server. This is available on when you have an Cyber Files Server and Gateway server installed on the same machine.
- **Redirect requests from port 80** - When selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.

## File Repository tab



Address: All available addresses

Port: 5787

File Store Path: C:\ProgramData\Acronis\Acro

● Local System Account

○ This Account

Password

Confirm Password

```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

The File Repository is used by Sync & Share functionality. If you haven't enabled Sync & Share, you can accept the standard values. If you are using Sync & Share, the file store path should specify the disk location to be used for storage. If you plan to use Amazon S3 for storage, then the default values are ok.

- **Address -** The IP address of your File Repository or pick **All Addresses** to listen on all interfaces. If you specify an IP or DNS address, the same address should also be specified in the **File Repository** section of the web interface. For more information on it, visit the File Repository article.
- **Port -** The port of your File Repository. The same port should also be specified in the **File Repository** section of the web interface. For more information on it, visit the File Repository article.
- **File Store Path -** UNC path to your File Store. If you change the File Store path, you MUST manually copy any files that are already in the original File Store location to your new location.

  **Note**

  If you move the File Store to another location, you should upload a new file to make sure it is going into the correct new location. Another thing is downloading a file that was already in the file store to make sure all of the files that were in the original location can be accessed at the new location.

- **Service Account -** If the file storage for the repository is on a remote network share, then the service account should be configured to be one that has permissions to that network share. This account must also have read and write access to the Repository folder (e.g. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\File Repository\Repository`) to write the log file.

**Note**
If you use a specific account for the service instead of the **Local System Account**, you will have to open the **Services** control panel, open the properties for the **Cyber Files File Repository** service and edit the **Log On** tab. You need to manually enter the account and its password in the appropriate fields.

### Proceeding to the setup wizard

After you have filled in all the necessary fields, selecting **Apply** or **OK** will restart the services you have made changes to.

**Note**
It will take 30-45 seconds after the services have started before the Cyber Files Web Server is available.

1. Once you are done with the initial setup of the Configuration Utility, a web browser will automatically open the Cyber Files web interface.
2. On the login page, you will be prompted to set the **administrator** password and then the Setup Wizard will guide you through the setup process.

**Important**
Write down the administrator passwor. It cannot be recovered if forgotten!

# Using the Setup wizard

After installing the software and running the configuration utility to setup network ports and SSL certificates, the administrator now needs to configure the Acronis Cyber Files server. The Setup Wizard takes the administrator through a series of steps to get the basic functionality of the server working.

**Note**
After the configuration utility has run, it will take 30-45 seconds for the server to come up the first time.

If you did not setup the administrator account in the previous step, on the login page you will be prompted to set the **administrator** password.

***Write down the administrator password, as it cannot be recovered if forgotten!***

## Going through the initial configuration process

Navigate to the Acronis Cyber Files's web interface using the IP address and port specified in the configuration utility. You will be prompted to set the password for the default administrator account.

**Note**
Additional administrators can be configured later on, for more information, visit the Server Administration section.

This wizard helps you setup the core settings for the functionality of your product.

- General Settings cover settings of the web interface itself, like the language, the color scheme, the server name used in admin notifications, licensing and administrators.
- LDAP settings allow you to use Active Directory credentials, rules and policies with our product.

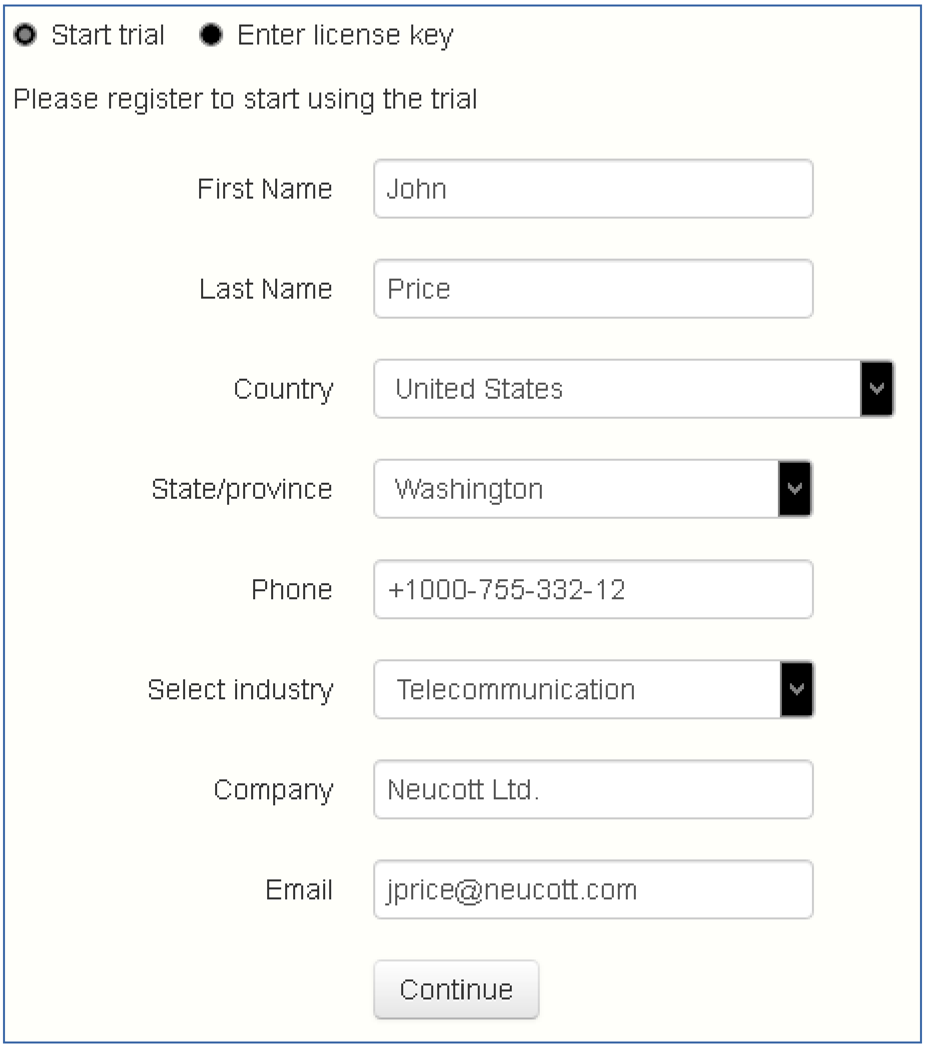
SMTP settings cover functionality in both Mobile Access features and Sync & Share features. For Mobile Access, the SMTP server is used when sending enrollment invitations. Sync & Share features use the SMTP server to send folder invitations, warnings, summaries of errors.

All of the settings you see in the Initial Configuration page will also be available after you complete it. For more information on any of the settings, please visit the Server Administration articles.

## Licensing

### To start a trial:

Select **Start Trial**, enter the required information and click **Continue**.



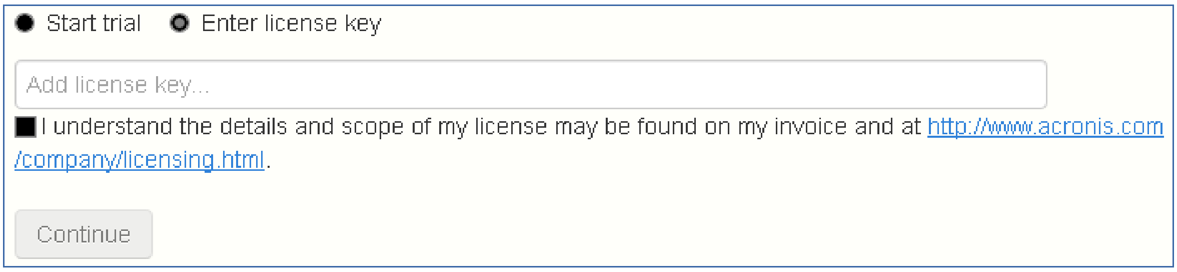
◉ Start trial ● Enter license key

Please register to start using the trial

| | |
|---|---|
| First Name | John |
| Last Name | Price |
| Country | United States |
| State/province | Washington |
| Phone | +1000-755-332-12 |
| Select industry | Telecommunication |
| Company | Neucott Ltd. |
| Email | jprice@neucott.com |

## To license your Acronis Cyber Files instance:

1. Select **Enter license keys**.
2. Enter your license key and select the checkbox.



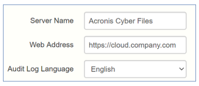
● Start trial ◉ Enter license key

Add license key...

■ I understand the details and scope of my license may be found on my invoice and at http://www.acronis.com/company/licensing.html.

3. Click **Save**.

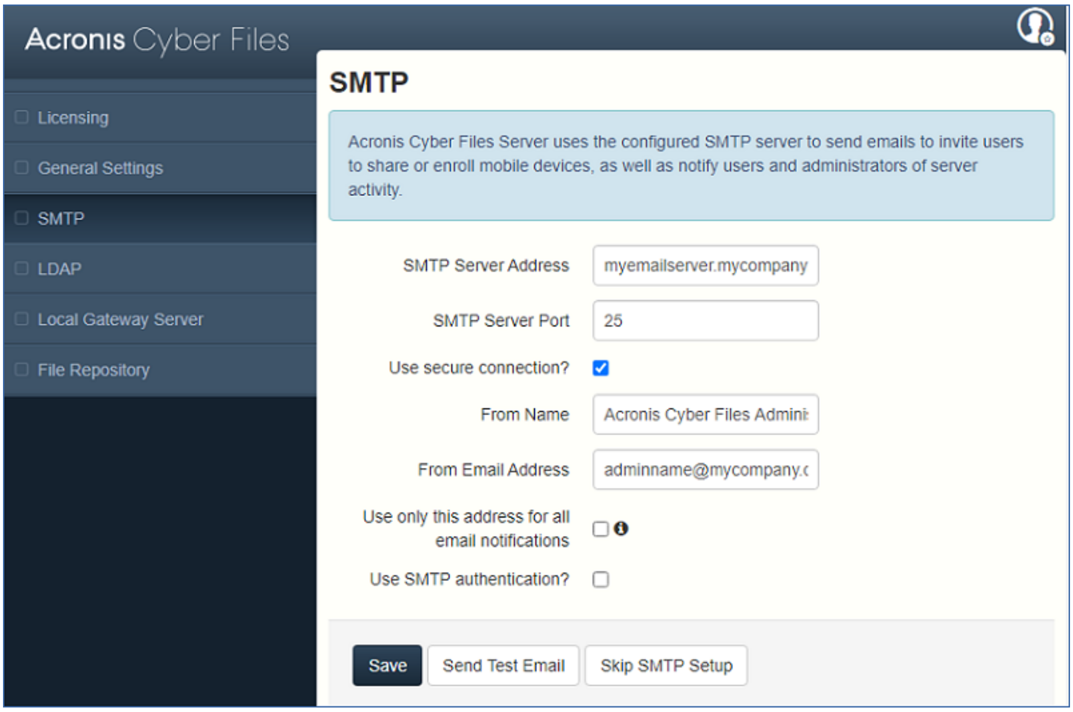
## General Settings



| | |
|---|---|
| Server Name | Acronis Cyber Files |
| Web Address | https://cloud.company.com |
| Audit Log Language | English |

1. Enter a Server Name.
2. Specify the root DNS name or IP address where users can access the website (starting with http:// or https://).
3. Select the default language for the **Audit Log**. The current options are English, German, French, Japanese, Italian, Spanish, Czesh, Russian, Polish, Korean, Chinese Traditional and Simplified.
4. Click **Save**.

## SMTP



SMTP

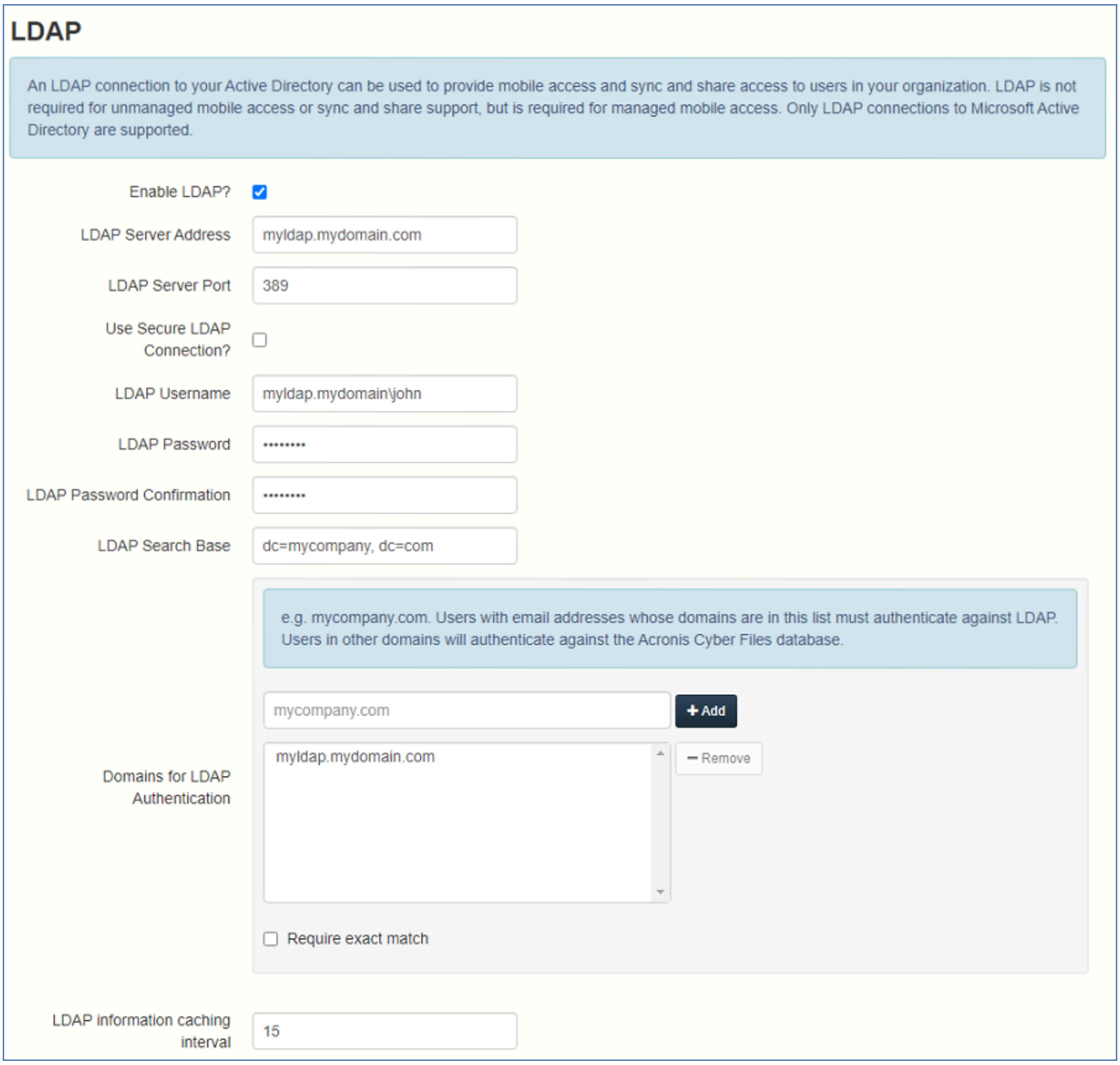
Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to share or enroll mobile devices, as well as notify users and administrators of server activity.

SMTP Server Address: myemailserver.mycompany
SMTP Server Port: 25
Use secure connection? ☑
From Name: Acronis Cyber Files Admini
From Email Address: adminname@mycompany.c
Use only this address for all email notifications ☐
Use SMTP authentication? ☐

**Note**
You can skip this section and configure SMTP later.

1. Enter the DNS name or IP address of your SMTP server.
2. Enter the SMTP port of your server.
3. If you do not use certificates for your SMTP server, clear the **Use secure connection?** option.
4. Enter the name which will appear in the "From" line in emails sent by the server.
5. Enter the address which will send the emails sent by the server.
6. If you use username/password authentication for your SMTP server, select **Use SMTP authentication?** and enter your credentials.
7. Click **Send Test Email** to send a test email to the email address you set on step 5.
8. Click **Save**.

# LDAP



LDAP

An LDAP connection to your Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Only LDAP connections to Microsoft Active Directory are supported.

| | |
|---|---|
| Enable LDAP? | ☑ |
| LDAP Server Address | myldap.mydomain.com |
| LDAP Server Port | 389 |
| Use Secure LDAP Connection? | ☐ |
| LDAP Username | myldap.mydomain\john |
| LDAP Password | •••••••• |
| LDAP Password Confirmation | •••••••• |
| LDAP Search Base | dc=mycompany, dc=com |
| Domains for LDAP Authentication | e.g. mycompany.com. Users with email addresses whose domains are in this list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.<br>mycompany.com [+ Add]<br>myldap.mydomain.com [− Remove]<br>☐ Require exact match |
| LDAP information caching interval | 15 |

**Note**

You can skip this section and configure LDAP later but some of Acronis Cyber Files' functionality will not be available until you do.

1. Select **Enable LDAP**.
2. Enter the DNS name or IP address of your LDAP server.
3. Enter the port of your LDAP server.
4. If you use a certificate for connections with your LDAP server, select **Use Secure LDAP Connection**.
5. Enter your LDAP credentials, along with the domain. (e.g. acronis\hristo).
6. Enter your LDAP search base.

7. Enter the desired domain(s) for LDAP authentication. (to enable LDAP authentication for an account with the email joe@glilabs.com, you would enter glilabs.com)
8. Click **Save**.

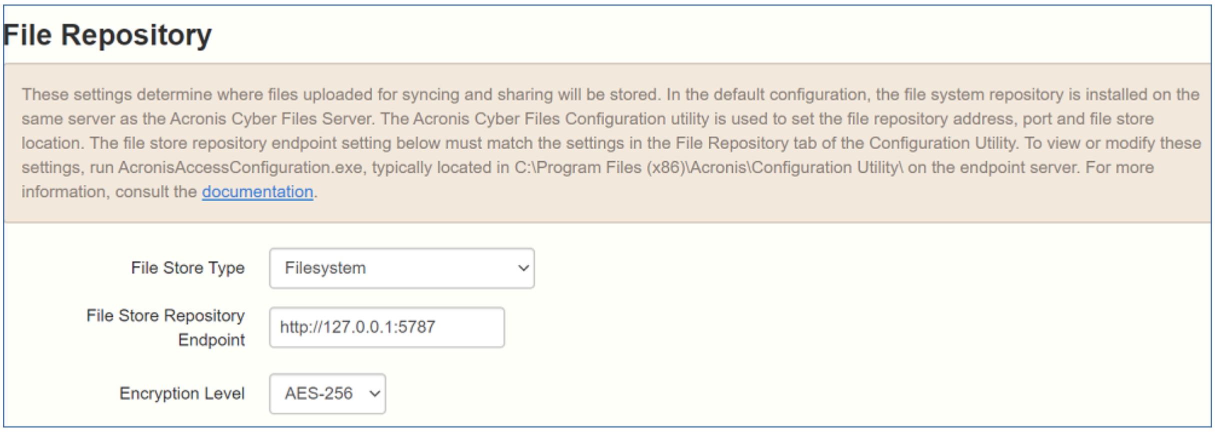
## Local Gateway Server

For KCD to work through mobile clients, it is necessary to enroll to the Local Gateway (the one installed on the same machine as the Tomcat that manages it). Then the Gateway will proxy those requests to that Tomcat (Management) Server.

**Note**
If you're installing both a Gateway Server and the Acronis Cyber Files Server on the same machine, the former will automatically be detected and administered by the latter. You will be prompted to set the DNS name or IP address, on which the Local Gateway Server will be reachable by clients. You can change this address later on.

1. Set a DNS name or IP address for the local Gateway Server.
2. Click **Save.**

## File Repository


File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The file store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the documentation.

File Store Type: Filesystem

File Store Repository Endpoint: http://127.0.0.1:5787

Encryption Level: AES-256

1. Select a file store type. Use **Filesystem** for a file store on your computers or any of the following options for a file store on the cloud: **Acronis Storage**, **Microsoft Azure Storage**, **Amazon S3**, **Swift S3**, **Ceph S3** and **Other S3-Compatible Storage**.

   **Note**
   You can use the **Other S3-Compatible Storage** option with S3 storage providers not on this list, but we cannot guarantee that everything will work properly.

   **Note**
   MinIO S3 storage type is supported and can be configured as **Other S3-Compatible Storage** option, however, we do not support it over a non-secure HTTP connection.

2. Enter the DNS name or IP address for the file repository service.

**Note**
The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The File Store Repository Endpoint setting must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility` on the endpoint server.

3. Select an encryption level. Choose between **None**, **AES-128** and **AES-256**.
4. Select the minimum free space available before your server sends you a warning.
5. Click **Save**.

# Clustering Acronis Cyber Files

Acronis Cyber Files allows the configuration of high-availability setups without needing third-party clustering software. This is configured through the new Cluster Groups feature introduced in Acronis Access 5.1. The setup procedure is simple, but provides high-availability for the Acronis Cyber Files Gateway Servers as they are the component under the heaviest load. All of these configurations are managed through the Acronis Cyber Files Server.

For more information and instructions on setting up a Cluster Group, visit the Cluster Groups article.

Although we recommend using the built-in Cluster Groups feature, Acronis Cyber Files also supports Microsoft Failover Clustering, for more information visit the Supplemental Material section.

# Load balancing

Acronis Cyber Files supports load balancing.

**Note**
For more information, see Installing AcronisCyber Files in a load balanced configuration, Migrating to a load balanced configuration, and Cluster Groups.

# Upgrading

## Upgrading Acronis Cyber Files to a newer version

The upgrade procedure from a previous version of Acronis Cyber Files is a simplified process and requires almost no configuration.

**Note**
In-place upgrades of operating systems are not supported. Please contact Acronis Mobility Technical Support if you have any questions.

**Note**
If you are upgrading from a version of Acronis Cyber Files (formerly Acronis Access) earlier than 7.5, please contact Acronis support at https://support.acronis.com/mobility/

**Note**
Before upgrading, please review the Minimum Hardware Requirements.

**Note**
Depending on your deployment, some of the paths used in this article might not be the same as yours. Upgrades from previous versions of Acronis Cyber Files and custom installations can affect the folder structures of your deployment.

**Note**
When upgrading to Acronis Cyber Files version 8.6 or higher, PostgreSQL is not automatically upgraded to version 11. For more information on how to do that, refer to Upgrading PostgreSQL to a newer Major version.

### Backup the vital components

#### The Apache Tomcat folder

Upon upgrade, Apache Tomcat may be upgraded too and all of its configuration files replaced and log files removed. We recommend you to make a copy of the Apache Tomcat folder, which by default can be found at the following location: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\`.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 8.6 and newer, you can find a backup at: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml`.
If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

### Purge unnecessary audit logs

If you have not setup automatic log purging, your server may have a lot of logs which may slow down the backup process. We recommend exporting and purging the older logs before proceeding with the database backup.

## The PostgreSQL database

The following method creates an *.sql file containing a text representation of the source database.

1. Open a Command Prompt window and navigate to the `11.6\bin` folder located in the PostgreSQL installation directory.

   e.g. `cd "C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.6\bin"`
2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

   ```
   pg_dump -U postgres -f mybackup.sql acronisaccess_production
   ```

   where `mybackup.sql` is the desired file name for the produced backup file. It can include a full path to the location where you want the backup file to be created, for instance: `D:\Backups\mybackup.sql`

   **Note**

   `acronisaccess_production` must be entered exactly as shown as it is the name of the Acronis Cyber Files database
3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Cyber Files installation process.

   **Note**

   Typing the password will not result in any visual changes in the Command Prompt window.
4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

**Note**

If you want to backup the entire PostgreSQL database set you can use the following command:

```
pg_dumpall -U postgres > alldbs.sql
```

Where `alldbs.sql` will be the generated backup file. It can include a full path specification, for instance `D:\Backups\alldbs.sql`

For full syntax on this command, refer to: https://www.postgresql.org/docs/11/app-pg-dumpall.html

**Note**

For more information on PostgreSQL backup procedures and command syntax, refer to: https://www.postgresql.org

### The Gateway Server(s) database(s)

1. Go to the server on which you have your Acronis Cyber Files Gateway Server installed.
2. Navigate to the folder containing the database.

> **Note**
> The default location is: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`

3. Copy the **mobilEcho.sqlite3** file and paste it in a safe location.

### The Acronis Cyber Files configuration file

1. Navigate to the Acronis Cyber Files installation folder containing the configuration file.

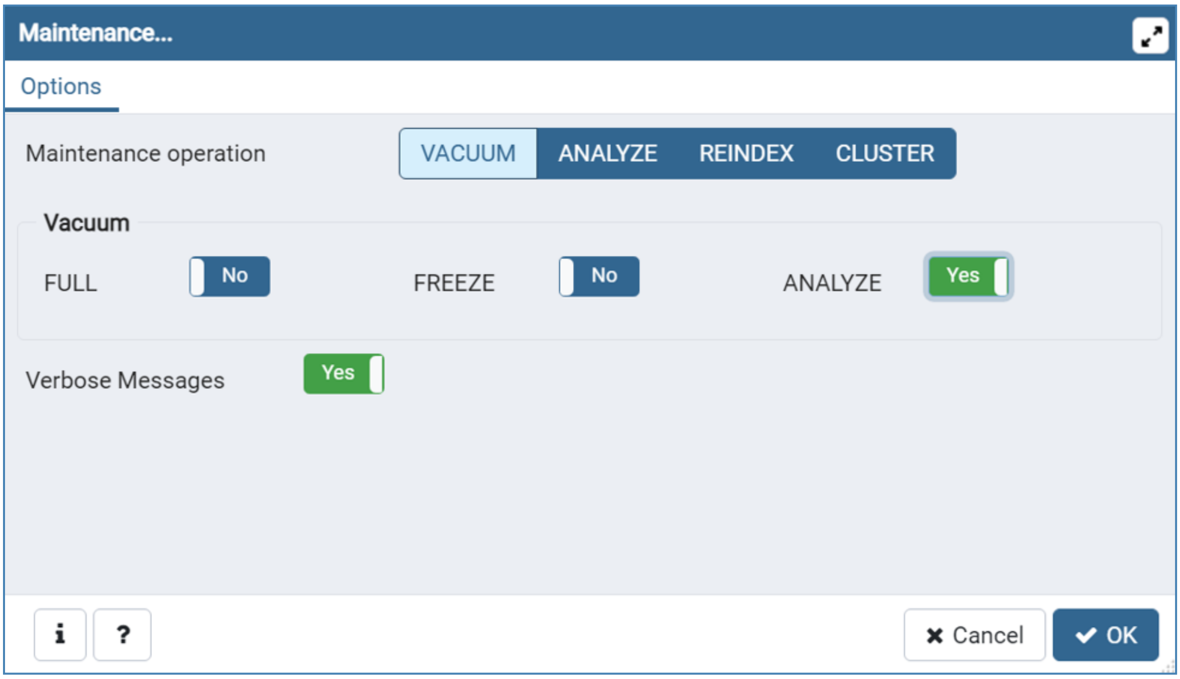
> **Note**
> The default location is: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`

2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

## Vacuum the database before upgrading

> **Note**
> Please, check the following recommendations before executing the below steps.

1. Open the Acronis Cyber Files PostgreSQL Administrator tool. You can find it in the Start menu, in the Acronis Cyber Files folder. Double-click **localhost** to connect to your server.
2. Right-click the `acronisaccess_production` database and choose **Maintenance**.
3. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance operation: VACUUM

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

**Warning!**
The vacuum might take a long time. Run this process when the server load is low.

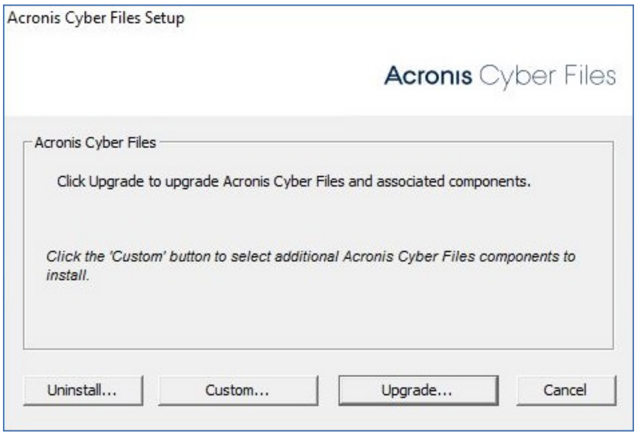
4. Click **OK**.
5. When the **Vacuum** process finishes, click **Done**.
6. Close the PostgreSQL Administrator tool.

# Upgrade

**Note**
Disable any anti-virus software you have or it may interrupt the procedure, resulting in a failed installation.

1. Double-click on the installer executable.

2. On the screen that opens next, click **Upgrade**.



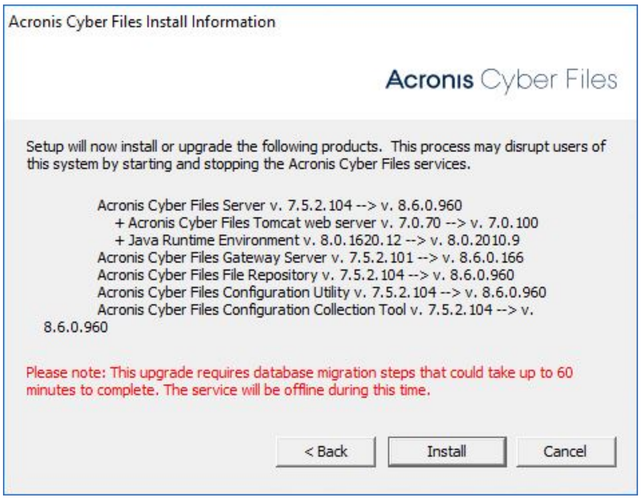
Acronis Cyber Files Setup

Acronis Cyber Files

Click Upgrade to upgrade Acronis Cyber Files and associated components.

*Click the 'Custom' button to select additional Acronis Cyber Files components to install.*

3. Review the components that will be installed and click **Install**.



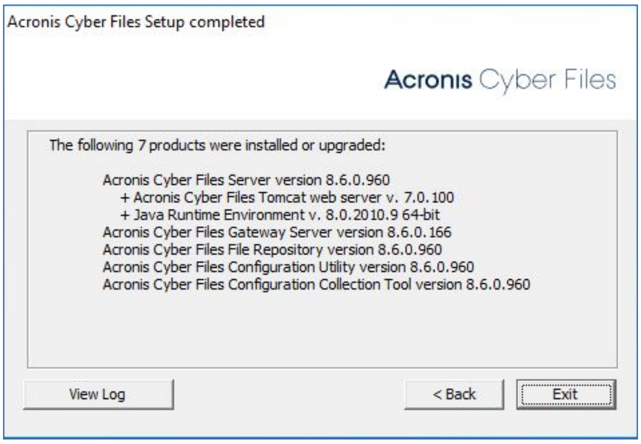
Acronis Cyber Files Install Information

Setup will now install or upgrade the following products. This process may disrupt users of this system by starting and stopping the Acronis Cyber Files services.

```
            Acronis Cyber Files Server v. 7.5.2.104 --> v. 8.6.0.960
               + Acronis Cyber Files Tomcat web server v. 7.0.70 --> v. 7.0.100
               + Java Runtime Environment v. 8.0.1620.12 --> v. 8.0.2010.9
            Acronis Cyber Files Gateway Server v. 7.5.2.101 --> v. 8.6.0.166
            Acronis Cyber Files File Repository v. 7.5.2.104 --> v. 8.6.0.960
            Acronis Cyber Files Configuration Utility v. 7.5.2.104 --> v. 8.6.0.960
            Acronis Cyber Files Configuration Collection Tool v. 7.5.2.104 --> v.
   8.6.0.960
```

Please note: This upgrade requires database migration steps that could take up to 60 minutes to complete. The service will be offline during this time.

4. Review the already installed components and close the installer.

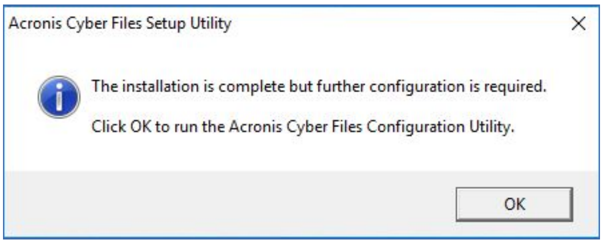


Acronis Cyber Files Setup completed

The following 7 products were installed or upgraded:

```
        Acronis Cyber Files Server version 8.6.0.960
           + Acronis Cyber Files Tomcat web server v. 7.0.100
           + Java Runtime Environment v. 8.0.2010.9 64-bit
        Acronis Cyber Files Gateway Server version 8.6.0.166
        Acronis Cyber Files File Repository version 8.6.0.960
        Acronis Cyber Files Configuration Utility version 8.6.0.960
        Acronis Cyber Files Configuration Collection Tool version 8.6.0.960
```

5. The following message confirms that the upgrade has finished:

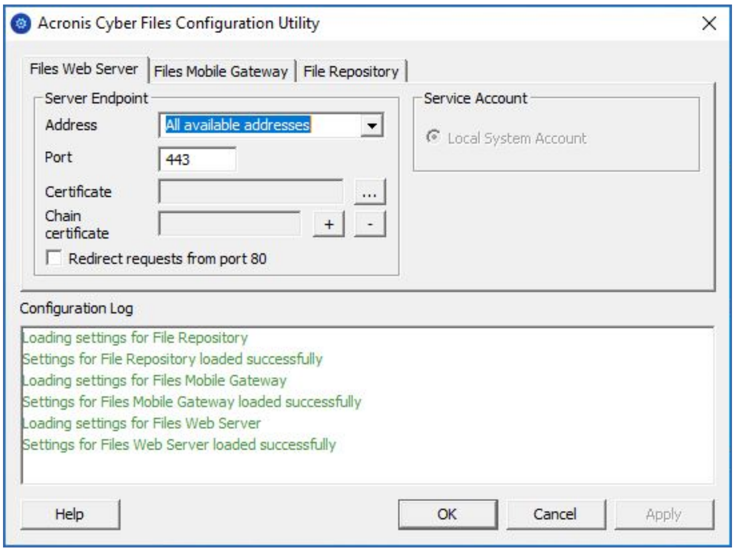


Acronis Cyber Files Setup Utility

The installation is complete but further configuration is required.

Click OK to run the Acronis Cyber Files Configuration Utility.

6. You will be prompted to open the Configuration Utility, click **OK**.
7. Check if the settings in the Configuration Utility have the right values. If these are all as expected, press **OK** to close the Configuration Utility and start the Acronis Cyber Files services.



Acronis Cyber Files Configuration Utility

Address: All available addresses

Port: 443

Certificate:

Chain certificate:

□ Redirect requests from port 80

○ Local System Account

Configuration Log

```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

**Warning!**
Database migrations take place right after the upgrade procedure. During this period, the actual website and all of its services are not available for usage. All these important processes may take even longer than an hour, for example, if you haven't upgraded for some time. It is strongly recommended to avoid any server restarts or services' interruptions, until the website starts responding in a browser.

# Upgrading Gateway Clusters

To upgrade a Acronis Cyber Files clustered configuration, you need to upgrade both the Acronis Cyber Files Web Server and the Gateway Servers in your Cluster Group.

**Note**
For information on upgrading a Microsoft Failover Clustering configuration, visit the Supplemental Material section.

**Note**

For instructions on upgrading the Acronis Cyber Files Web Server, visit the Upgrading from Acronis Cyber Files to a newer version article

***For each Gateway Server, you will need to do the following upgrade procedure:***

***Before performing any upgrades, please review our Backup articles and backup your configuration.***

**Note**

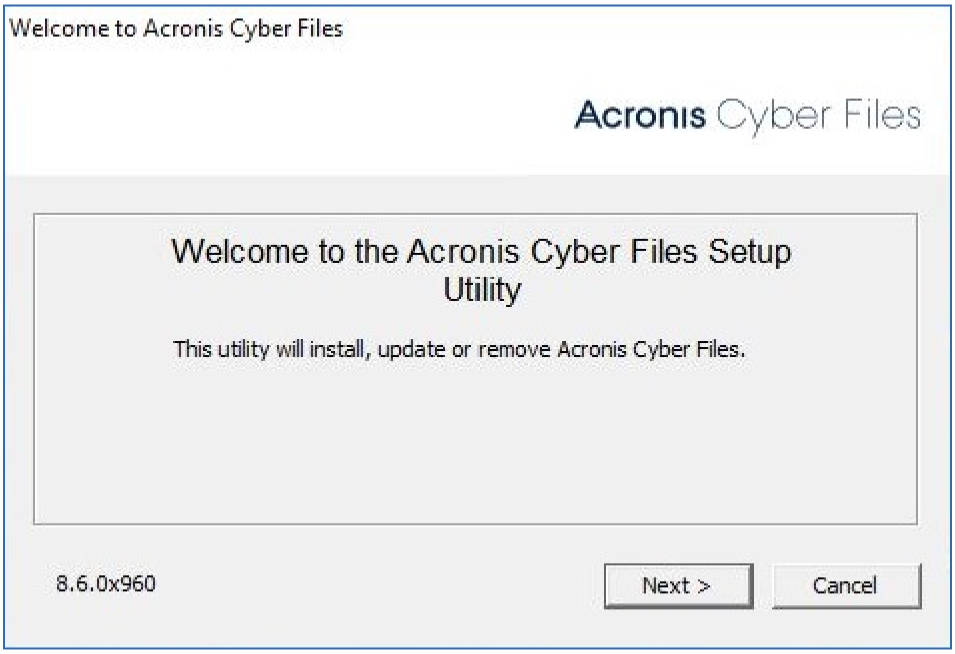
Before upgrading, please review the Minimum Hardware Requirements.

**Note**

Depending on your deployment, some of the paths used in this article might not be the same as yours. Upgrades from previous versions of Acronis Cyber Files and custom installations can affect the folder structures of your deployment.

## Upgrading a Gateway Server

1. Run the Acronis Cyber Files installer on the desired server.
2. Click **Next** on the **Welcome** screen.

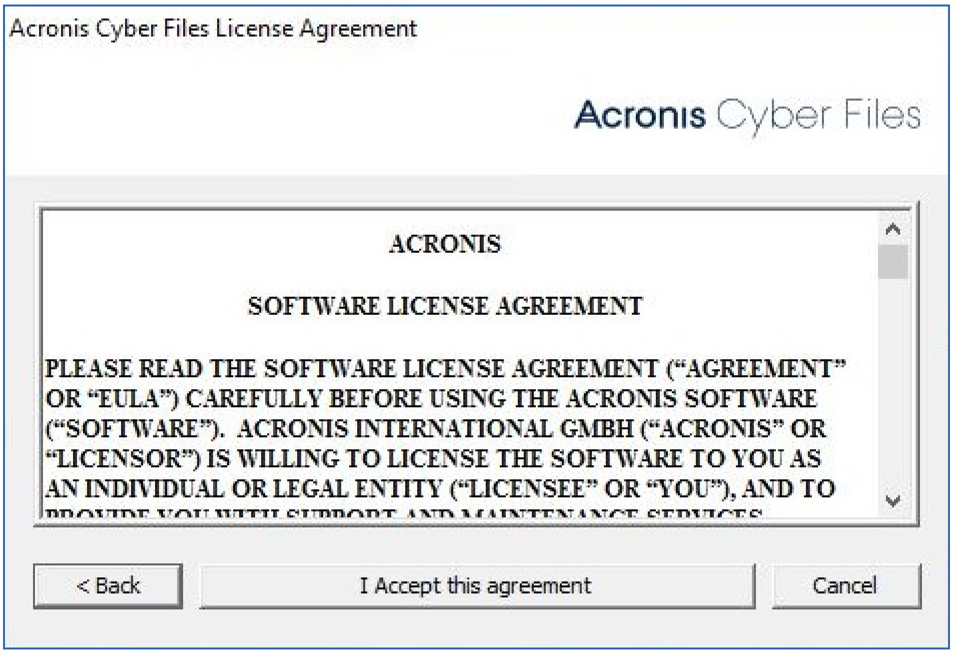


Welcome to Acronis Cyber Files

Welcome to the Acronis Cyber Files Setup Utility

This utility will install, update or remove Acronis Cyber Files.

3. Read and accept the license agreement.



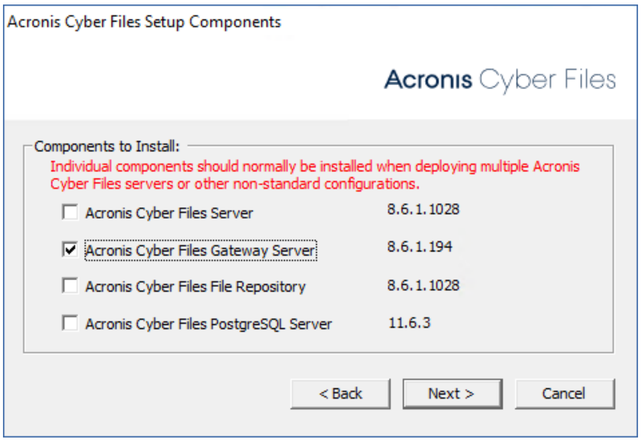
Acronis Cyber Files License Agreement

ACRONIS

SOFTWARE LICENSE AGREEMENT

PLEASE READ THE SOFTWARE LICENSE AGREEMENT ("AGREEMENT" OR "EULA") CAREFULLY BEFORE USING THE ACRONIS SOFTWARE ("SOFTWARE"). ACRONIS INTERNATIONAL GMBH ("ACRONIS" OR "LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR LEGAL ENTITY ("LICENSEE" OR "YOU"), AND TO

4. Select **Custom**.
5. Select only the **Acronis Cyber Files Gateway Server** component and click **Next**.



Acronis Cyber Files Setup Components

Components to Install:

Individual components should normally be installed when deploying multiple Acronis Cyber Files servers or other non-standard configurations.

| | |
|---|---|
| □ Acronis Cyber Files Server | 8.6.1.1028 |
| ☑ Acronis Cyber Files Gateway Server | 8.6.1.194 |
| □ Acronis Cyber Files File Repository | 8.6.1.1028 |
| □ Acronis Cyber Files PostgreSQL Server | 11.6.3 |

6. Review the components and click **Install**.
7. Once the installation finishes, review the **Summary**, and close the installer.
8. You will be prompted to open the **Configuration Utility**. Open it to review that all of your previous Gateway Server settings are in place. Make any changes if necessary and click **OK**.

# Upgrading Load-balanced configurations

This guide is intended for deployments that are load-balancing Acronis Cyber Files and all of its components.

***Before performing any upgrades, please review our Backup articles and backup your configuration.***

**Note**

Before upgrading, please review the Minimum Hardware Requirements.

**Note**

Depending on your deployment, some of the paths used in this article might not be the same as yours. Upgrades from previous versions of Acronis Cyber Files and custom installations can affect the folder structures of your deployment.

## Before you begin

**Warning!**

Acronis Cyber Files does not support versions of Tomcat, Java and PostgreSQL newer than the ones included with each release. To request information about a specific version, contact the Acronis Support team.

**Note**

We strongly recommend that you run a test upgrade outside of your production environment.

All paths listed on this page correspond to default locations. Yours may be different if you upgraded or performed a custom install. In such cases, use the Windows Services [name of service] entry to locate the exact path to the program executable folder.

### Important things to pay attention to, regarding your current configuration:

- Are the Acronis Cyber Files Server and PostgreSQL server on the same machine?
- What port is PostgreSQL running on?
- What is the locale of your current PostgreSQL installation? You can check this by openning the PostgreSQL Administration tool and clicking on the `acronisaccess_production` database. On the right, under **Properties**, you will see the **Encoding** and **Character type**.

  **Warning!**

  Make sure that your new PostgreSQL installation has the same **Encoding** and **Character type**, otherwise you will not be able to upgrade successfully.

- What is the IP and/or DNS name of the machine running PostgreSQL?
- What is the PostgreSQL version number of your current server. The easiest way to find this is to look at the folder name inside the main PostgreSQL folder (by default:. `C:\Program Files (x86)\Acronis\Cyber Files\Common\PostgreSQL`), the inside folder's name is the PostgreSQL major version number (e.g. 9.2; 9.3; 9.4).
- Note that, for customers upgrading to Acronis Cyber Files from older product versions, such as Access or Files Advanced, directory paths may look different.
  For example:

  - `C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL`
  - `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`
  - `C:\Program Files\PostgreSQL\`
- Make sure that all necessary permissions in the file system(s) are configured.

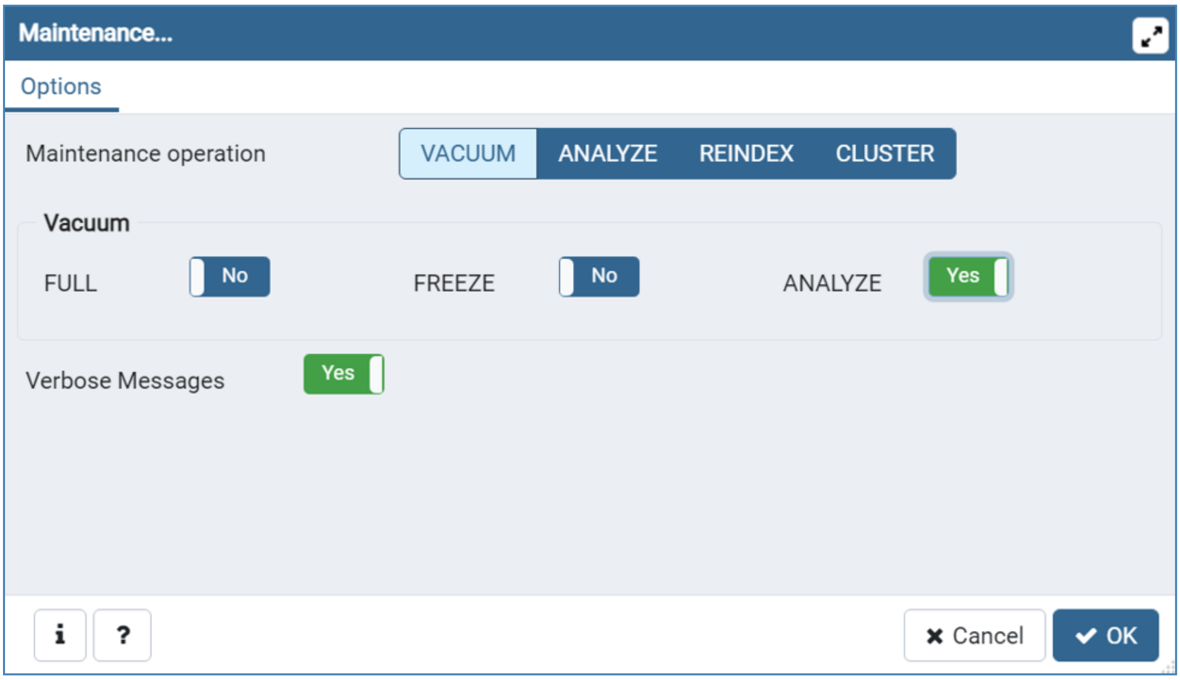
Pick one of the Acronis Cyber Files Web Server machines to act as the **Primary**. This machine is the **Primary** node only in the sense that it will be upgraded first and it will migrate any changes/settings to the PostgreSQL database. If the database is very large, these migrations can take several minutes.

**Warning!**
**DO NOT** upgrade any other Tomcat servers until the **Primary** server is upgraded and you can log into the web interface to test it out.

## Vacuum the database

This will help speed up the backup and restore process by optimizing your database

1. Open the Acronis Cyber Files PostgreSQL Administrator tool. You can find it in the Start menu, in the Acronis Cyber Files folder. Double-click **localhost** to connect to your server.
2. Right-click the `acronisaccess_production` database and choose **Maintenance**.
3. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance...

Options

Maintenance operation: VACUUM

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

**Warning!**
The vacuum might take a long time. Run this process when the server load is low.

4. Click **OK**.
5. When the **Vacuum** process finishes, click **Done**.
6. Close the PostgreSQL Administrator tool.

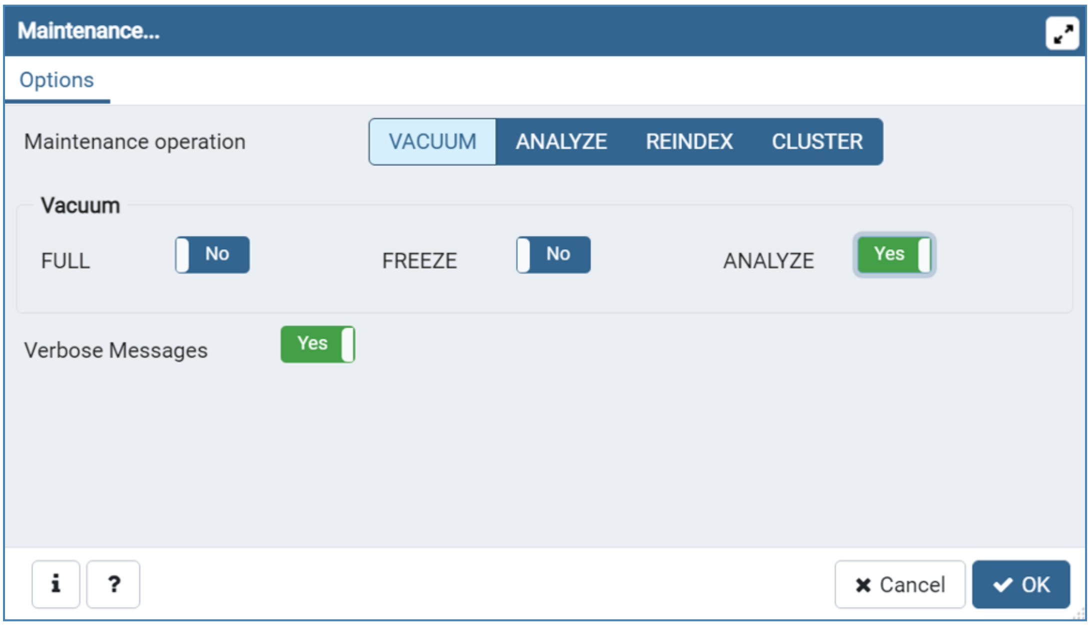
## Backup your Loadbalanced components

***For in-depth information on backup and restore procedures, please visit the Backing up and Restoring Acronis Cyber Files article.***

### Backup your PostgreSQL database

1. Stop all Acronis Cyber Files Tomcat services.

2. Open the Acronis Cyber Files PostgreSQL Administrator tool. You can find it in Windows Start menu, under the Acronis Cyber Files folder. Connect to the database server. You may be prompted to enter the password for your `postgres` user.
3. Expand **Databases** and right-click on the `acronisaccess_production` database.
4. Choose **Maintenance.**
5. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance...

Options

Maintenance operation: VACUUM

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

6. Click **OK**.
7. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.
8. Close the PostgreSQL Administrator tool and open an elevated command prompt.
9. In the command prompt, navigate to the PostgreSQL bin directory.

   **e.g.**`cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

**Note**

You will need to edit the path to point to your PostgreSQL bin folder if you use an older or a custom installation (e.g. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

1. Enter the following command: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`
   - `alldbs.sql` will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: `--file D:\Backups\alldbs.sql`
   - If you are using a non-default port, change `5432` to the correct port number.
   - If you are not using the default PSQL administrative account `postgres`, please change `postgres` to the name of your administrative account in the command above.
   - You will be prompted to enter the `postgres` user's password several times for this process. For each prompt, enter the password and hit Enter.

   **Note**
   Typing the password will not result in any visual changes in the Command Prompt window.

2. Copy the backup file to a safe location.
3. Do **NOT** shutdown the Postgres service as PostreSQL itself will not be upgraded.

## Backup additional important components

1. Backup the Tomcat **conf** and **logs** folders. By default located in: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\`

   **Note**
   Replace <version> with the correct version of your Acronis Cyber Files Tomcat instance, e.g. `\apache-tomcat.70.0.70\`

2. Backup the **acronisaccess.cfg** file. By default located in: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`
3. Backup all **web.xml** files. located by default in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`.
4. Backup the **newrelic.yml** file. Its location depends entirely on where you have saved it. You can skip this step if you are not using New Relic monitoring.

## Backup the Gateway Servers databases

1. Turn off all the Acronis Cyber Files Gateway services
2. Go to the Gateway database folders, by default `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`
3. Make a backup of the **mobilEcho.sqlite3** file.
4. Repeat these steps for each Gateway Server.

## Stop all Acronis Cyber Files services on all machines

**It is vital that all Acronis Cyber Files Tomcat services are stopped before you upgrade. We recommend also stopping all other Acronis Cyber Files services, except the PostgreSQL**

**service as it must remain running.**

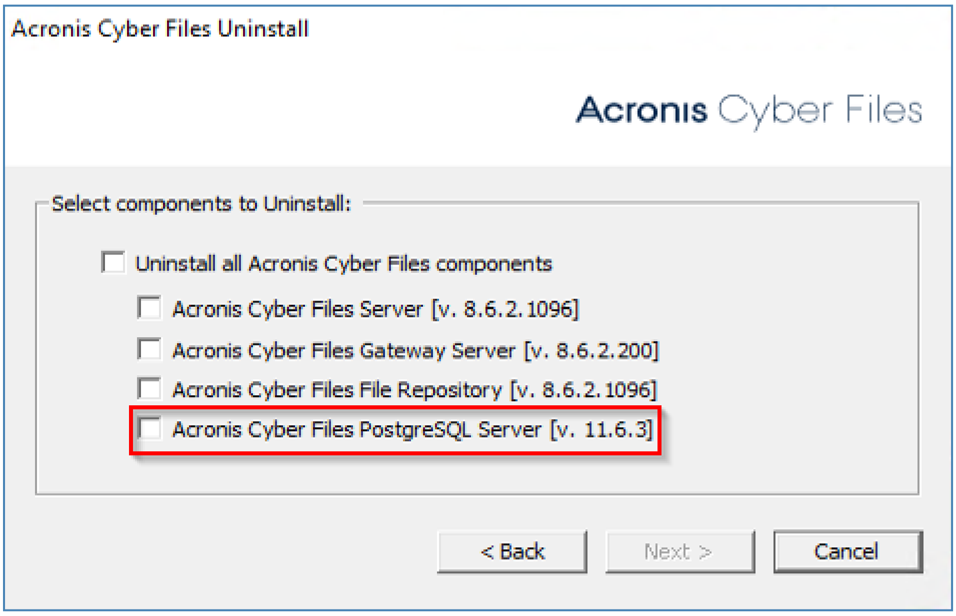
## Upgrading PostgreSQL

### Step 1: Uninstall PostgreSQL

Start the old Acronis Cyber Files Server installer.

Click **Next** on the Welcome screen.

1. Read and click **OK** to accept the End User License Agreement (EULA).
2. Click **Uninstall**.
3. Select only the Acronis Cyber Files PostgreSQL Server and click **Next**.



Acronis Cyber Files Uninstall

Select components to Uninstall:

□ Uninstall all Acronis Cyber Files components

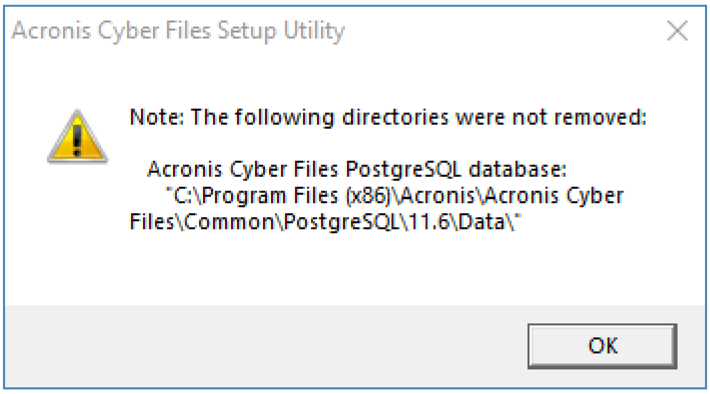
□ Acronis Cyber Files Server [v. 8.6.2.1096]

□ Acronis Cyber Files Gateway Server [v. 8.6.2.200]

□ Acronis Cyber Files File Repository [v. 8.6.2.1096]

□ Acronis Cyber Files PostgreSQL Server [v. 11.6.3]

4. After the uninstall is complete, the following warning dialog appears.

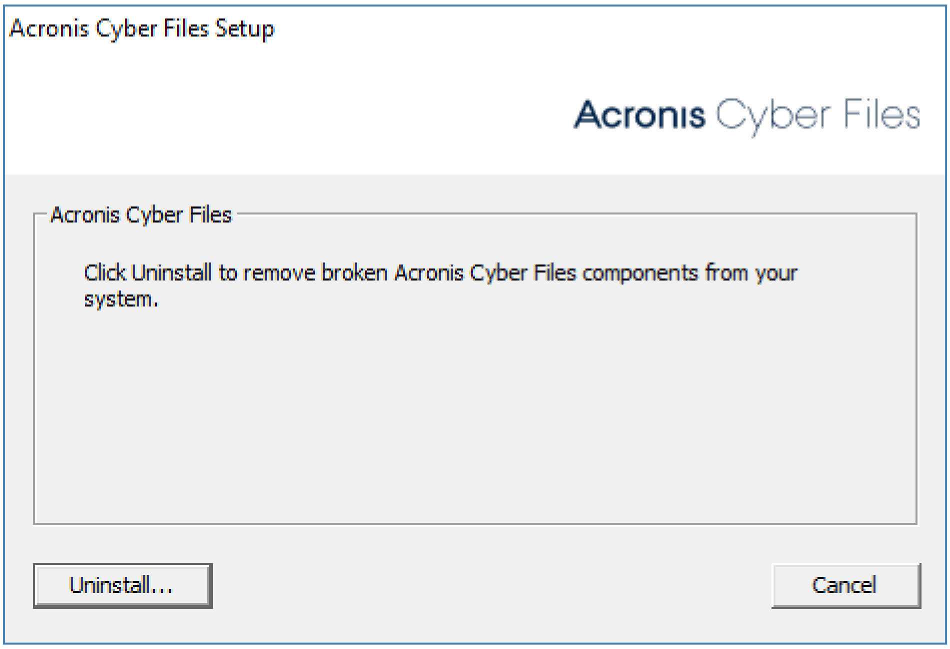


Acronis Cyber Files Setup Utility

Note: The following directories were not removed:

Acronis Cyber Files PostgreSQL database:
"C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.6\Data\"

5. Click **OK**.
   The following window appears.



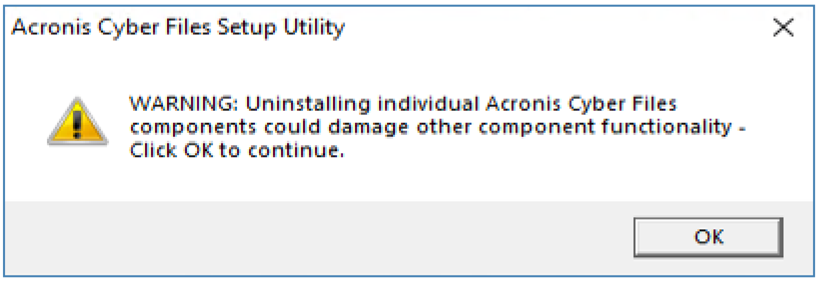
Acronis Cyber Files Setup

Acronis Cyber Files

Click Uninstall to remove broken Acronis Cyber Files components from your system.

6. Click **Uninstall...** .

   The following warning dialog appears.

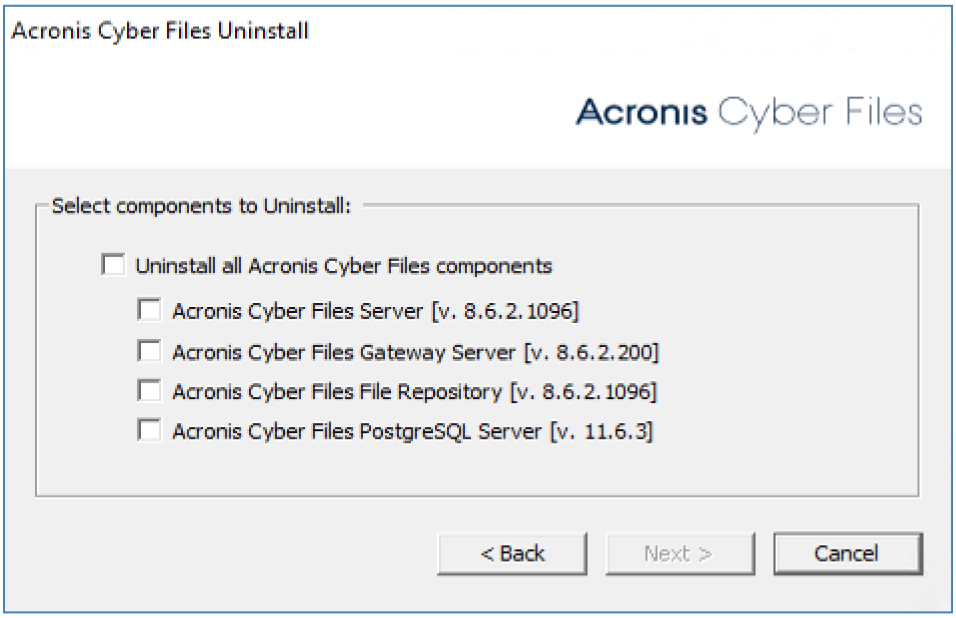


Acronis Cyber Files Setup Utility

WARNING: Uninstalling individual Acronis Cyber Files components could damage other component functionality - Click OK to continue.

7. Click **OK**.

   The initial Acronis Cyber Files Uninstall window appears again.



Acronis Cyber Files Uninstall

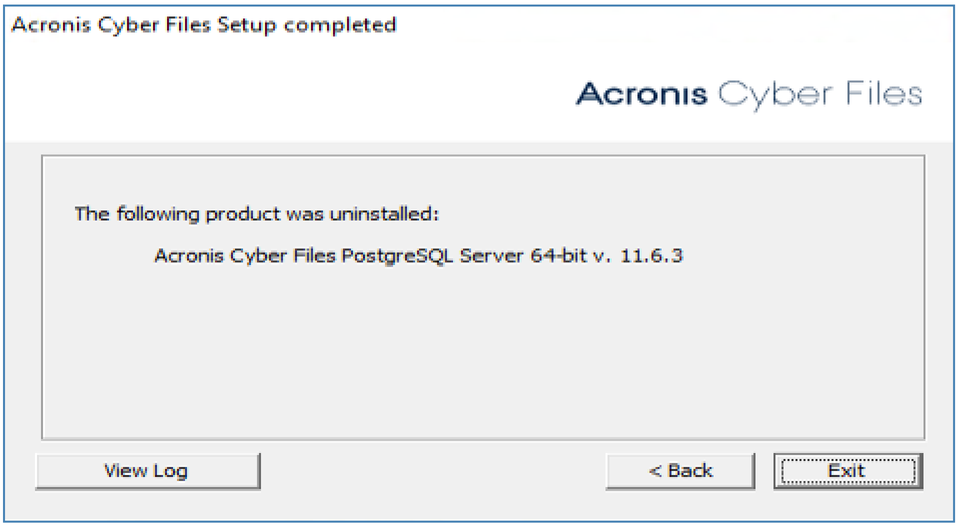
Select components to Uninstall:

□ Uninstall all Acronis Cyber Files components

- □ Acronis Cyber Files Server [v. 8.6.2.1096]
- □ Acronis Cyber Files Gateway Server [v. 8.6.2.200]
- □ Acronis Cyber Files File Repository [v. 8.6.2.1096]
- □ Acronis Cyber Files PostgreSQL Server [v. 11.6.3]

8. Click **Cancel**.

   The following confirmation window appears.



Acronis Cyber Files Setup completed

The following product was uninstalled:

Acronis Cyber Files PostgreSQL Server 64-bit v. 11.6.3

9. Click **Exit**.
10. Restart the server machine.
11. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common` and delete the `PostgreSQL` folder, as indicated in step 6.

**Note**

After the uninstall is complete, **AcronisAccessPostgreSQL** should no longer be listed in Windows services.

## Step 2: Install the new version of PostgreSQL

***To install the newer version of PostgreSQL***

1. Open the **Services** control panel and stop the Acronis Cyber Files Tomcat service.
2. Start the new Acronis Cyber Files Server installer.

   **Note**

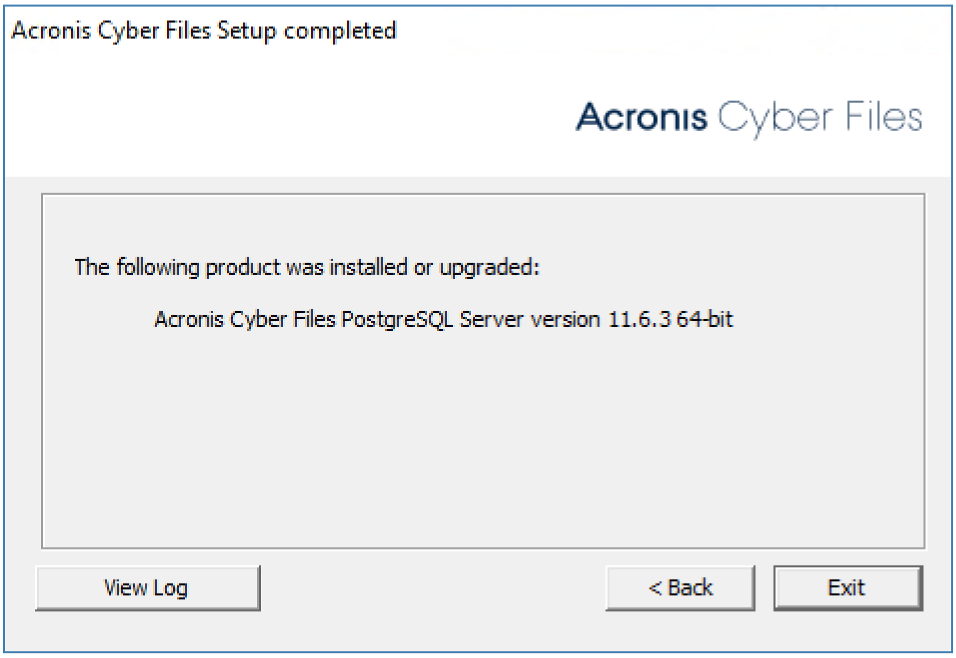
   The latest version of Acronis Cyber Files Server installer can be downloaded at https://www.acronis.com/products/file-sync-and-share-downloads/ or contact our technical support at https://support.acronis.com/mobility.

3. Click **Next** on the Welcome screen.
4. Read and click **OK** to accept the End User License Agreement (EULA).
5. Click **Custom**.
6. Select only the Acronis Cyber Files PostgreSQL Server component and click **Next**.
7. Confirm the default location on which the DB is to be installed and click **Next**.
8. Set a DB password and click **Next.**
9. Click **Install** to start the installation of the PostgreSQL DB.

**Note**

The duration of this process depends on server resources.

When the installation is complete, the following window appears.



Acronis Cyber Files Setup completed

The following product was installed or upgraded:

Acronis Cyber Files PostgreSQL Server version 11.6.3 64-bit

10. Click **Exit**.

**Note**

After installation is complete, **AcronisAccessPostgreSQL** should once again be listed in Windows services.

## Step 3: Import the DB Content

***To import the DB content***

1. Open the Acronis Cyber Files PostgreSQL Administrator application, connect to the local database server, and select **Databases**.
2. Confirm there is a database called `acronisaccess_production`.
3. Right-click on the database and click **Refresh**.
4. Expand it and expand **Schemas**, then expand **Public** and verify that there are zero (0) **Tables**.

**Note**

If there are any tables in the database, right click on the database and rename it to `oldacronisaccess_production`.

Finally, go to **Databases**, right-click and create a new database called `acronisaccess_production`.

5. Close the PostgreSQL Administrator and open an elevated command prompt.
6. In the command prompt, navigate to the PostgreSQL bin directory.
   **e.g.** `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

7. Copy the database backup file `alldbs.sql` (or whatever you have named it) into the **bin** directory.
8. In the command prompt, enter the following command: `psql -U postgres -f alldbs.sql`
9. Enter your `postgres` password when prompted for it.

> **Note**
> The restore can take some time. How long depends on the size of your database.

10. After the restore is complete, close the command prompt window.
11. Open the **Acronis Cyber Files PostgreSQL Administrator** again and connect to the local database server.
12. Select **Databases**.
13. Expand the `acronisaccess_production` database, expand **Schemas** and expand **Public**. Verify that the number of **Tables** is the same as it was on the original server.
14. Start the database service Acronis Cyber Files PostgreSQL Server.

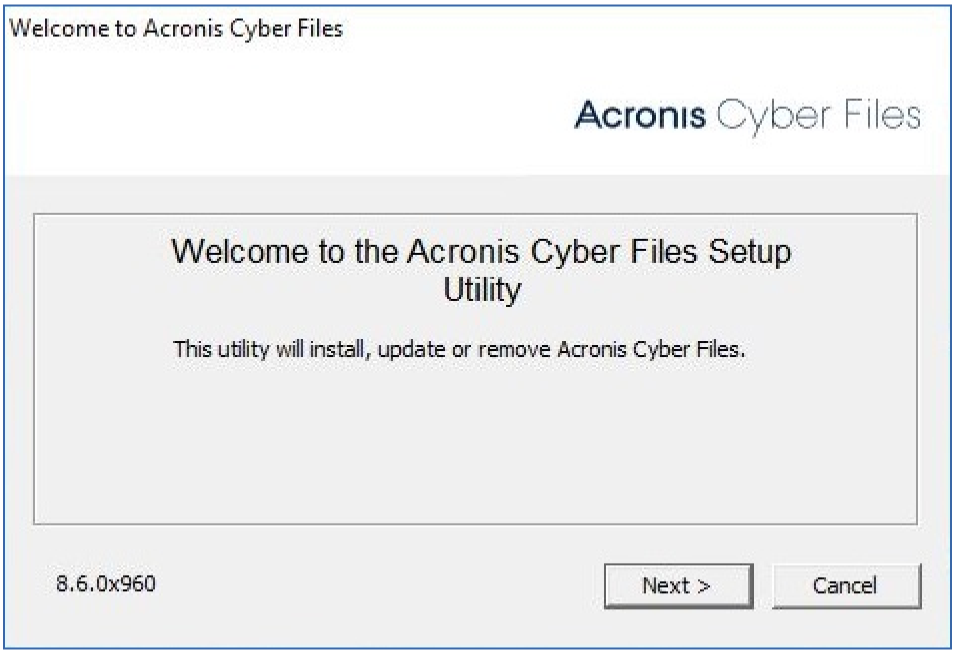
## Upgrading the File Repository

***Upgrade the File Repository first regardless of where it is located.***

1. Copy the Acronis Cyber Files installer to the machine with the File Repository component and run the installer.

> **Note**
> If you have multiple File Repository services, repeat these steps for all repositories before you proceed with the other components.

2. On the **Welcome** screen, click **Next**.



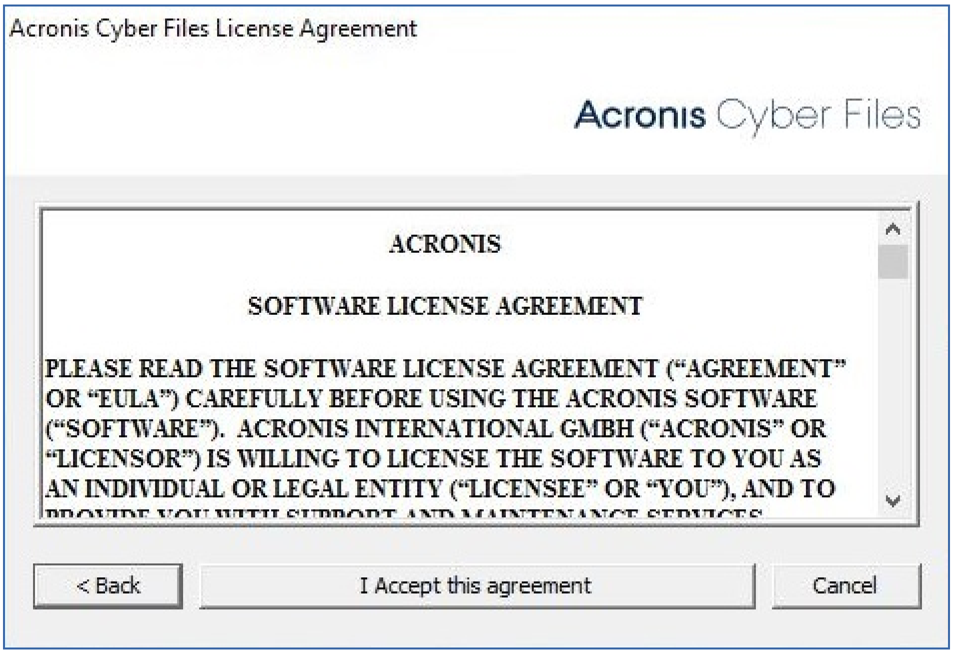
Welcome to Acronis Cyber Files

Welcome to the Acronis Cyber Files Setup Utility

This utility will install, update or remove Acronis Cyber Files.

8.6.0x960

3. Accept the License Agreement.

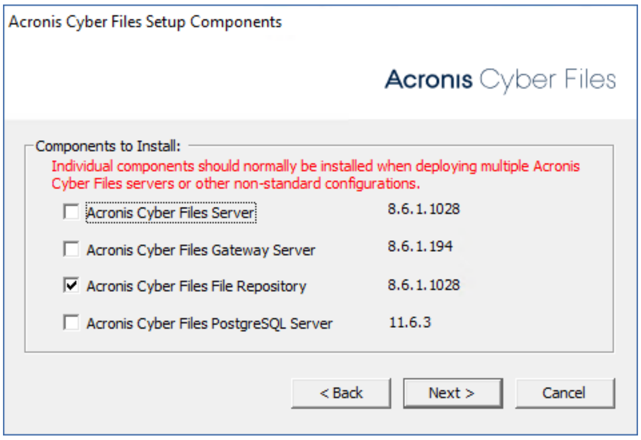


ACRONIS

SOFTWARE LICENSE AGREEMENT

PLEASE READ THE SOFTWARE LICENSE AGREEMENT ("AGREEMENT" OR "EULA") CAREFULLY BEFORE USING THE ACRONIS SOFTWARE ("SOFTWARE"). ACRONIS INTERNATIONAL GMBH ("ACRONIS" OR "LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR LEGAL ENTITY ("LICENSEE" OR "YOU"), AND TO PROVIDE YOU WITH SUPPORT AND MAINTENANCE SERVICES

4. Choose **Custom**... and select only the **Acronis < PRODUCT_NAME> File Repository** to upgrade.



Components to Install:

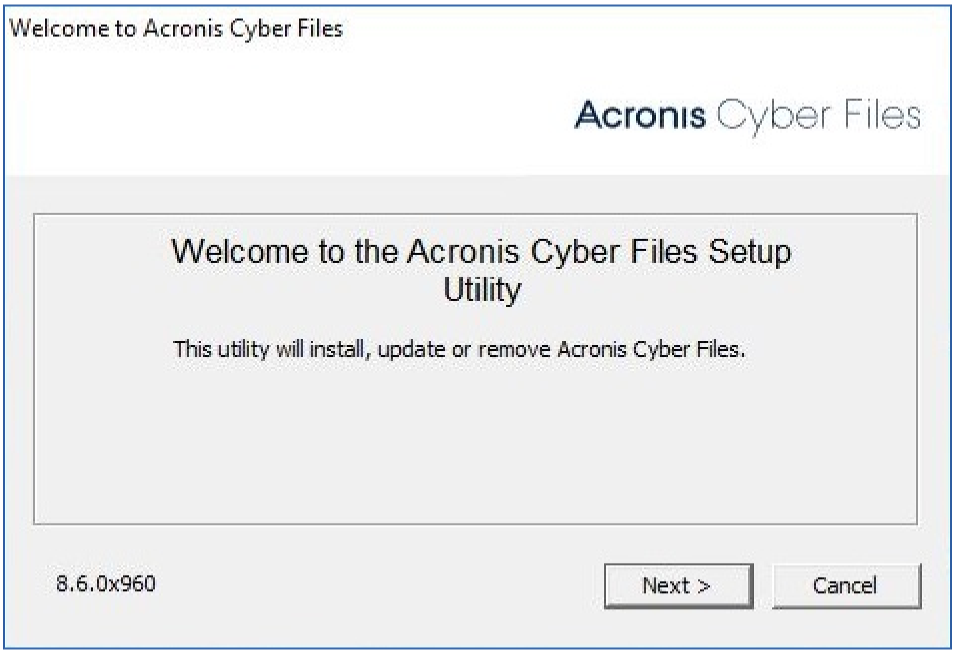
Individual components should normally be installed when deploying multiple Acronis Cyber Files servers or other non-standard configurations.

| | | |
|---|---|---|
| □ | Acronis Cyber Files Server | 8.6.1.1028 |
| □ | Acronis Cyber Files Gateway Server | 8.6.1.194 |
| ☑ | Acronis Cyber Files File Repository | 8.6.1.1028 |
| □ | Acronis Cyber Files PostgreSQL Server | 11.6.3 |

5. Click **Next**, review what is going to be installed and click **Install**.
6. When the upgrade is done, click **Exit**. When the Configuration Utility launches, click **OK**.
7. Continue by upgrading your **Primary** Acronis Cyber Files Web Server on its corresponding machine.

## Upgrading the Primary Cyber Files Server

1. Copy the Acronis Cyber Files Advanced installer to the **Primary** Acronis Cyber Files Web Server machine.
2. On the **Primary** node, start the Acronis Cyber Files installer.



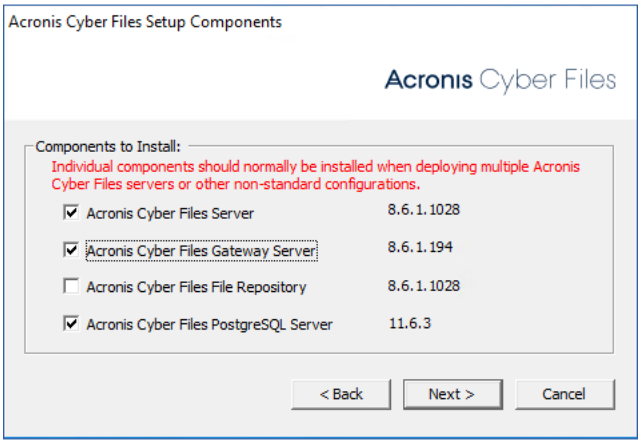
Welcome to Acronis Cyber Files

Welcome to the Acronis Cyber Files Setup Utility

This utility will install, update or remove Acronis Cyber Files.

8.6.0x960

3. Click **Next** on the Welcome screen and then **Custom**. This will allow you to upgrade only the necessary services that are already installed on the machine, without installing others.
4. Select the Acronis Cyber Files services that you are going to upgrade. Choose only the Acronis Cyber Files Web Server and any components that are already present on the machine.



Acronis Cyber Files Setup Components

Components to Install:

Individual components should normally be installed when deploying multiple Acronis Cyber Files servers or other non-standard configurations.

☑ Acronis Cyber Files Server 8.6.1.1028

☑ Acronis Cyber Files Gateway Server 8.6.1.194

□ Acronis Cyber Files File Repository 8.6.1.1028

☑ Acronis Cyber Files PostgreSQL Server 11.6.3

5. Click **Install,** let the installer finish and launch the the **Configuration Utility**.

**Note**

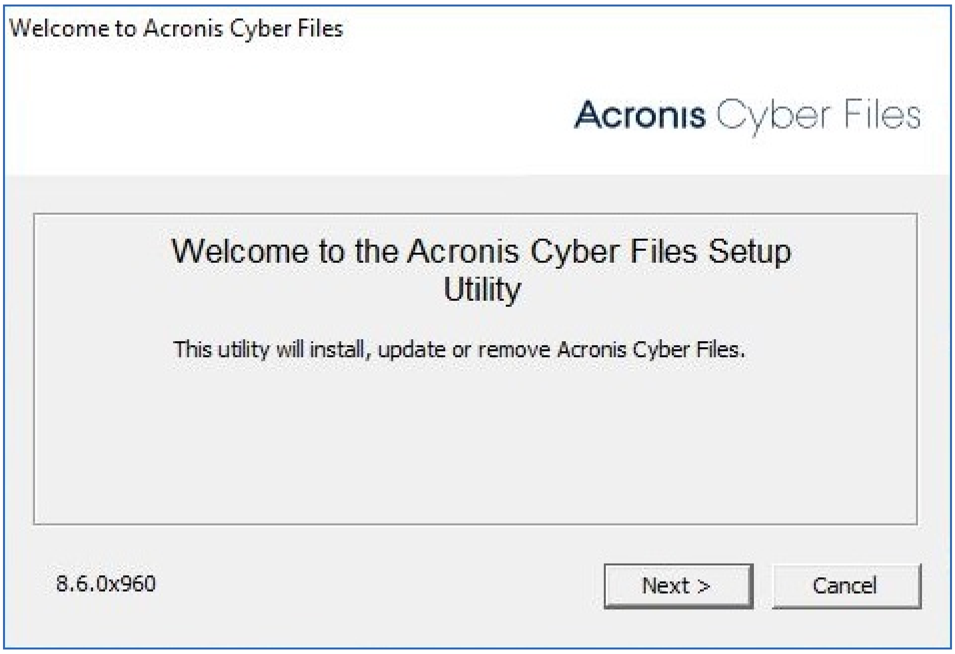
Do not change any settings in the **Configuration Utility**! Changing settings can cause issues with your configuration.

6. Once the Configuration Utility starts all the necessary services, and the database migrations are finished, verify that Acronis Cyber Files web interface on the **Primary** server works as expected. A web browser will launch automatically and display the Acronis Cyber Files server log-in screen.
7. Log in as an administrator and verify that the settings are the same and there are no changes or issues.
8. Leave this instance of Acronis Cyber Files running while you update all other components.

**Warning!**
Do not upgrade or start any other Acronis Cyber Files Tomcat server until the Primary Tomcat server is running and you have verified that it is working correctly.

## Upgrading Gateway Servers

1. Copy the Acronis Cyber Files installer to any machine with only a Gateway Server and run the installer.
2. On the Welcome screen, click **Next**.



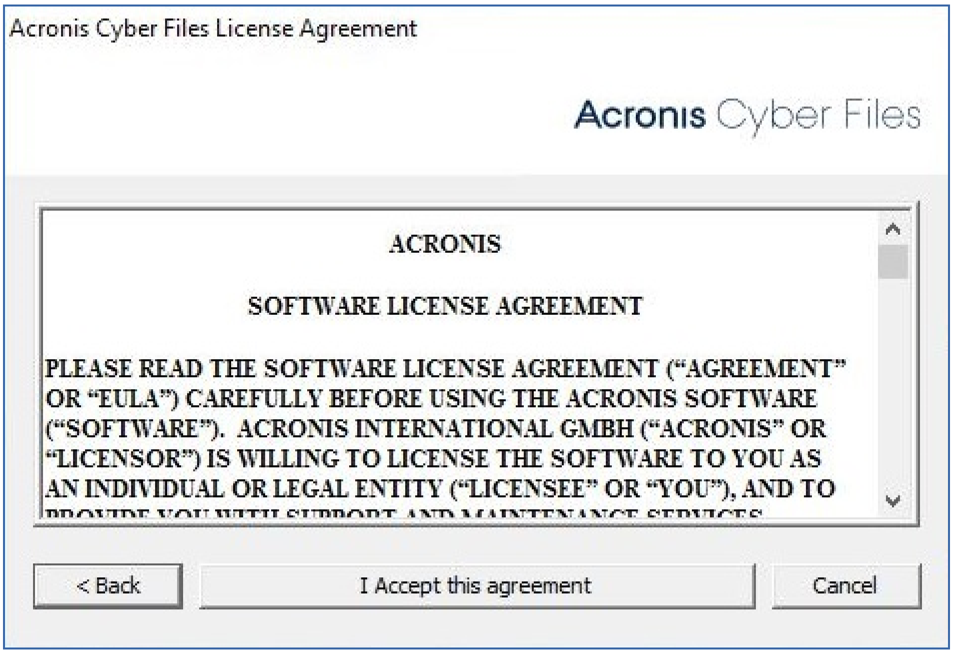
Welcome to Acronis Cyber Files

Welcome to the Acronis Cyber Files Setup Utility

This utility will install, update or remove Acronis Cyber Files.

8.6.0x960

3. Accept the License Agreement.



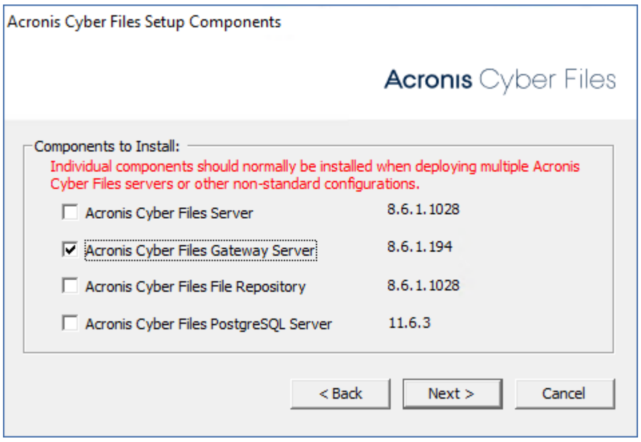
Acronis Cyber Files License Agreement

ACRONIS

SOFTWARE LICENSE AGREEMENT

PLEASE READ THE SOFTWARE LICENSE AGREEMENT ("AGREEMENT" OR "EULA") CAREFULLY BEFORE USING THE ACRONIS SOFTWARE ("SOFTWARE"). ACRONIS INTERNATIONAL GMBH ("ACRONIS" OR "LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR LEGAL ENTITY ("LICENSEE" OR "YOU"), AND TO

4. Choose **Custom**... and select only the Acronis Cyber Files Gateway Server to upgrade.



Acronis Cyber Files Setup Components

Components to Install:

Individual components should normally be installed when deploying multiple Acronis Cyber Files servers or other non-standard configurations.

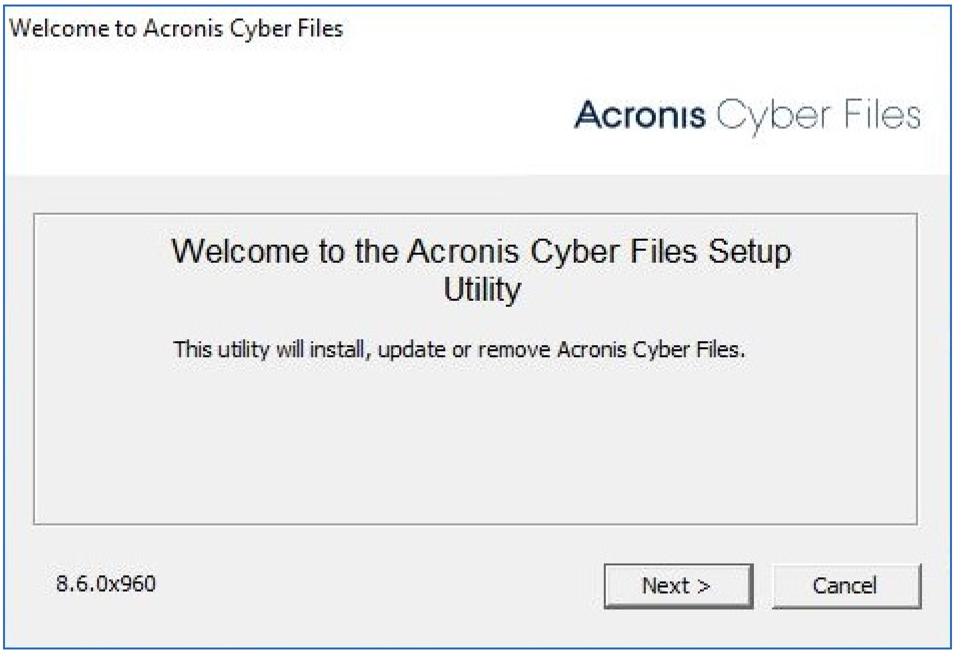
| | |
|---|---|
| □ Acronis Cyber Files Server | 8.6.1.1028 |
| ☑ Acronis Cyber Files Gateway Server | 8.6.1.194 |
| □ Acronis Cyber Files File Repository | 8.6.1.1028 |
| □ Acronis Cyber Files PostgreSQL Server | 11.6.3 |

5. Click **Next**, review what is going to be installed and click **Install**.
6. When the upgrade is done, click **Exit**. When the Configuration Utility launches, click **OK**.

## Upgrading all remaining nodes

Once you have successfully updated the **Primary** Acronis Cyber Files node, all File Repository servers and all Gateway Servers, continue by upgrading the rest of the Acronis Cyber Files Servers.

1. Copy the Acronis Cyber Files installer to the desired node and start it.



Welcome to Acronis Cyber Files

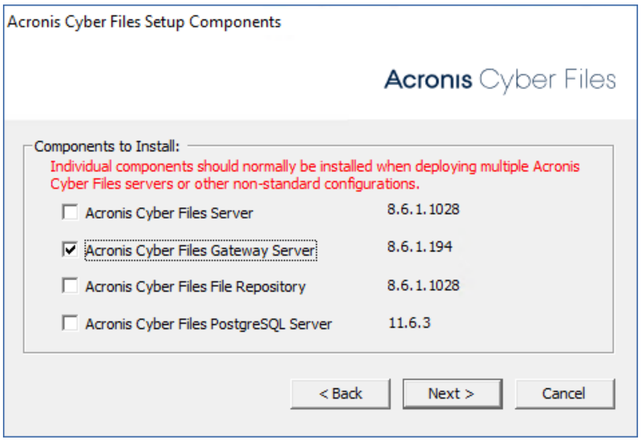
Welcome to the Acronis Cyber Files Setup Utility

This utility will install, update or remove Acronis Cyber Files.

8.6.0x960

2. Click **Next** on the Welcome screen and then **Custom**. This will allow you to upgrade only the necessary services that are already installed on the machine, without installing others.
3. Select any Acronis Cyber Files services that you wish to upgrade. Choose only the ones that are already present on the machine.

   **e.g.** If there is only a Gateway server installed, select only the Gateway Server component in the installer.



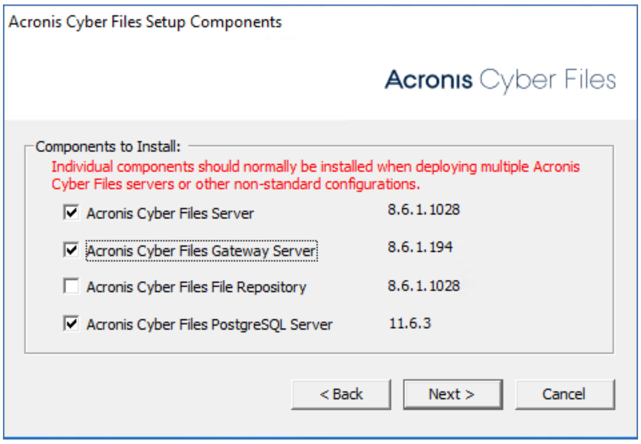
Acronis Cyber Files Setup Components

Components to Install:

Individual components should normally be installed when deploying multiple Acronis Cyber Files servers or other non-standard configurations.

| | |
|---|---|
| □ Acronis Cyber Files Server | 8.6.1.1028 |
| ☑ Acronis Cyber Files Gateway Server | 8.6.1.194 |
| □ Acronis Cyber Files File Repository | 8.6.1.1028 |
| □ Acronis Cyber Files PostgreSQL Server | 11.6.3 |

**e.g.** If there is a Gateway Server and a Acronis Cyber Files Server, select both.



Acronis Cyber Files Setup Components

Components to Install:

Individual components should normally be installed when deploying multiple Acronis Cyber Files servers or other non-standard configurations.

| | |
|---|---|
| ☑ Acronis Cyber Files Server | 8.6.1.1028 |
| ☑ Acronis Cyber Files Gateway Server | 8.6.1.194 |
| □ Acronis Cyber Files File Repository | 8.6.1.1028 |
| ☑ Acronis Cyber Files PostgreSQL Server | 11.6.3 |

4. Click **Install** and let the installer finish and launch the the **Configuration Utility**.

**Note**

Do not change any settings in the **Configuration Utility**. Changing settings can cause issues with your configuration.

5. Once the Configuration Utility starts all the necessary services, verify that the Acronis Cyber Files components on this node work as expected.

# Mobile Access

This section of the web interface covers all the settings and configurations affecting mobile device users.

## Concepts

Acronis Cyber Files mobile clients connect directly to your server rather than utilizing a third-party service, leaving you in control. Acronis Cyber Files server can be installed in the same network as existing file servers, allowing iPads, iPhones and Android devices to access files located on that network. These are typically the same files already available to PCs using Windows file sharing and Macs using Files Connect Server.

Clients access Acronis Cyber Files servers using their Active Directory user account. No additional accounts need to be configured within Acronis Cyber Files. The Acronis Cyber Files app also supports file access using local computer accounts configured on the Windows server Acronis Cyber Files is running on, in the event you need to give access to non-AD users. The client management features described below require AD user accounts.

A minimal deployment consists of a single Windows server running a default installation of Acronis Cyber Files. This default installation includes the Acronis Cyber Files Server component installed and the local Acronis Cyber Files Gateway Server installed. This scenario allows Acronis Cyber Files users to connect to this single file server, and allows for client management on mobile devices. If client management is not needed, Data Sources can be setup on the local Gateway Server and the Acronis Cyber Files mobile clients will be able to access these Data Sources, but the users will be in control of their app settings.

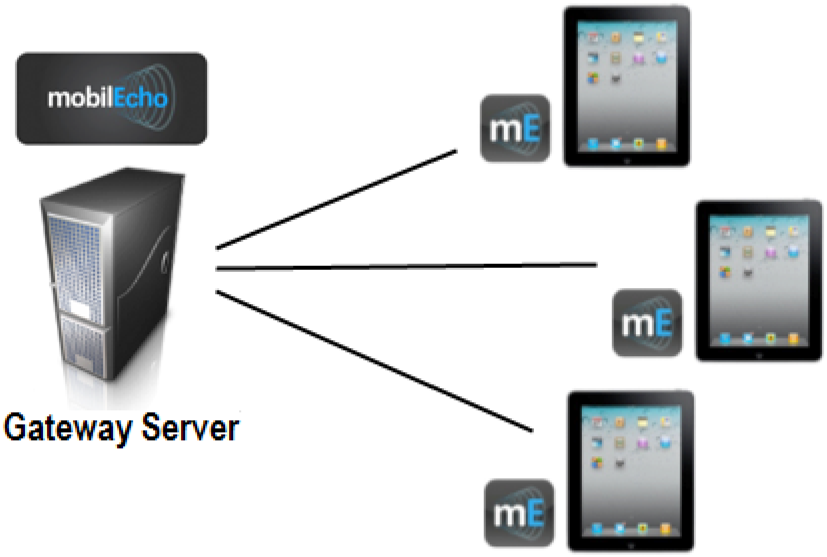


Fig 1. Single Acronis Cyber Files server with a Local Gateway Server

Any number of Gateway Servers can later be added to the network and configured for access from the Cyber Files clients.

**Note**
Details on installing Acronis Cyber Files are included in the Installing section of this guide. Configuration of Gateway Servers and Data Sources is explained in the Mobile Access section.

If you wish to remotely manage your mobile clients, Acronis Cyber Files Management allows you to create policies per Active Directory user or group. Only one Acronis Cyber Files Server is required and these policies can:

- Configure general application settings
- Assign servers, folders, and home directories to be displayed in the client app
- Restrict what can be done with files
- Restrict the other third party apps that Acronis Cyber Files files can be opened into
- Set security requirements (server login frequency, application lock password, etc.)
- Disable the ability to store files on the device
- Disable the ability to include Acronis Cyber Files files in iTunes backups
- Remotely reset a user's application lock password
- Perform a remote wipe of the mobile app's local data and settings
- And many additional configuration and security options

A typical network employing client management includes one server with the Acronis Cyber Files Server and Acronis Cyber Files Gateway Server components installed and several additional Gateway Servers acting as file servers. In this scenario, all mobile clients are configured to be managed by the Acronis Cyber Files Server, and will contact this server each time the Acronis Cyber Files application is started, to check for any changed settings and to accept application lock password resets and remote wipe commands if necessary.

Acronis Cyber Files clients can be assigned a list of servers, specific folders within shared volumes, and home directories in their management policy. These resources will automatically appear in the Acronis Cyber Files app and the client app will contact these servers directly as needed for file access.

**Note**
Details on enabling and configuring the client management are included in the Policies and Managing Mobile Devices section of this guide.

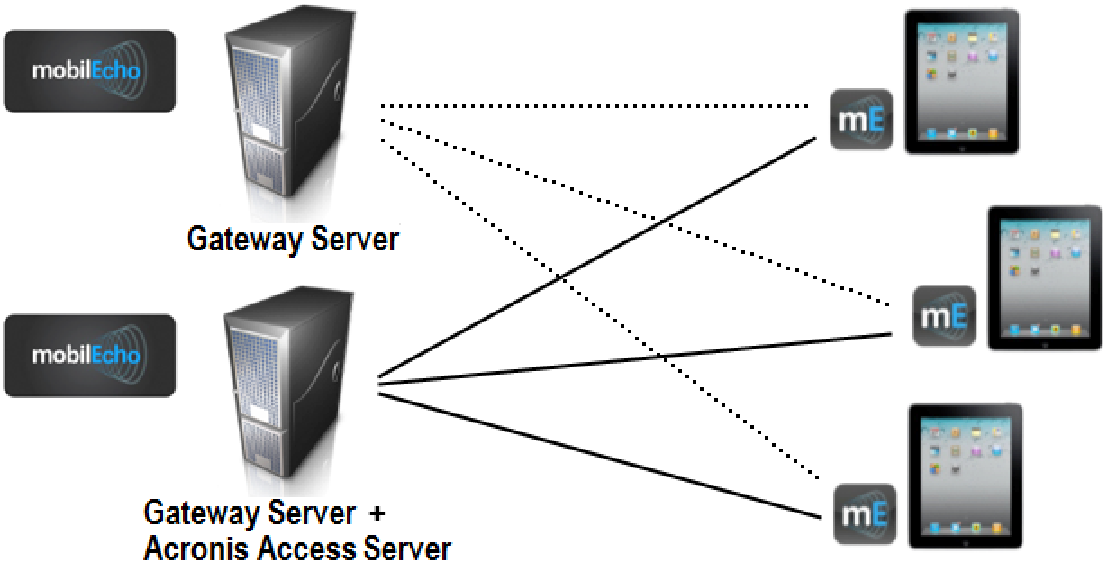


Fig 2. One Gateway Server, one Gateway Server + Acronis Cyber Files Server

# Policies

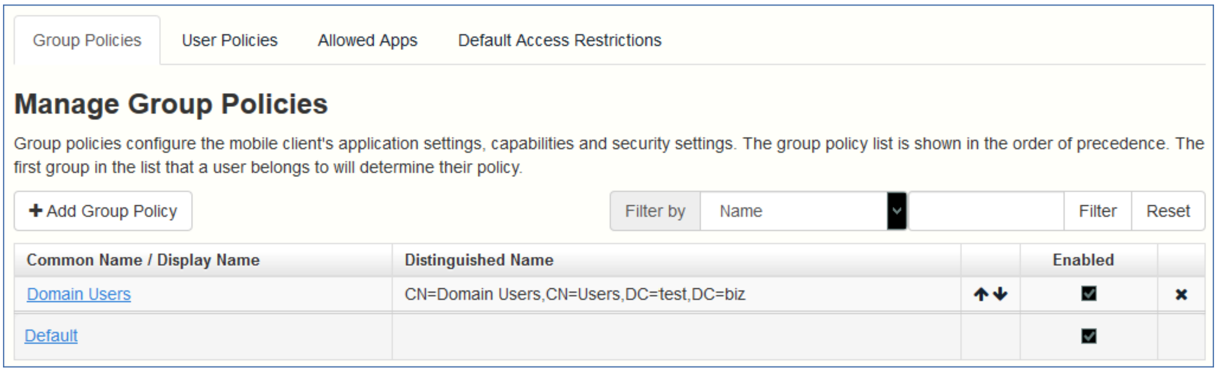
Acronis Cyber Files allows policies to be assigned to Active Directory groups. Group policies will usually address most or all of your client management requirements. The group policies list is displayed in order of precedence, with the first group in the list having the highest priority. When a user contacts the Acronis Cyber Files server, their settings are determined by the single highest priority group policy they are a member of.

User policies are used when you want to enforce specific settings on a user regardless of the groups he is in, as User policies have a higher priority than Group policies. User policies will override all Group policies.

**Note**

**Group Management Tips**

If you would like all or most of your users to receive the same policy settings, you can use the **Default** group policy. All users which are not members of a group policy and do not have an explicit user policy, become members of the **Default** group. The **Default** group is enabled by default. If you would like to deny a group of users access to Acronis Cyber Files management, ensure that they are not members of any configured group policies. As long as a user account does not match any group policies, they will be denied the ability to enroll in Acronis Cyber Files client management.



Manage Group Policies

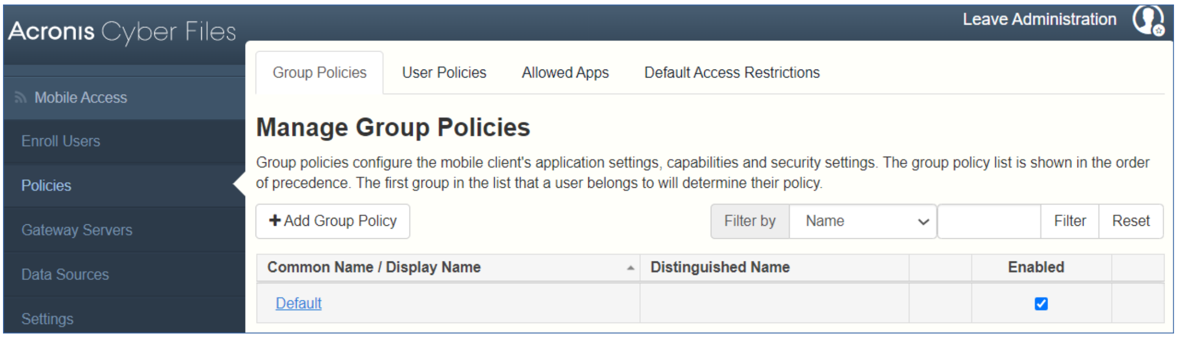
Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

| Common Name / Display Name | Distinguished Name | | Enabled | |
|---|---|---|---|---|
| Domain Users | CN=Domain Users,CN=Users,DC=test,DC=biz | ↑↓ | ☑ | ✖ |
| Default | | | ☑ | |

## Adding a New Policy

### To add a new group policy:

1. Open the **Group Policies** tab.
2. Click the **Add new policy** button to add a new group policy. This will open the **Add a new group policy** page.



Manage Group Policies

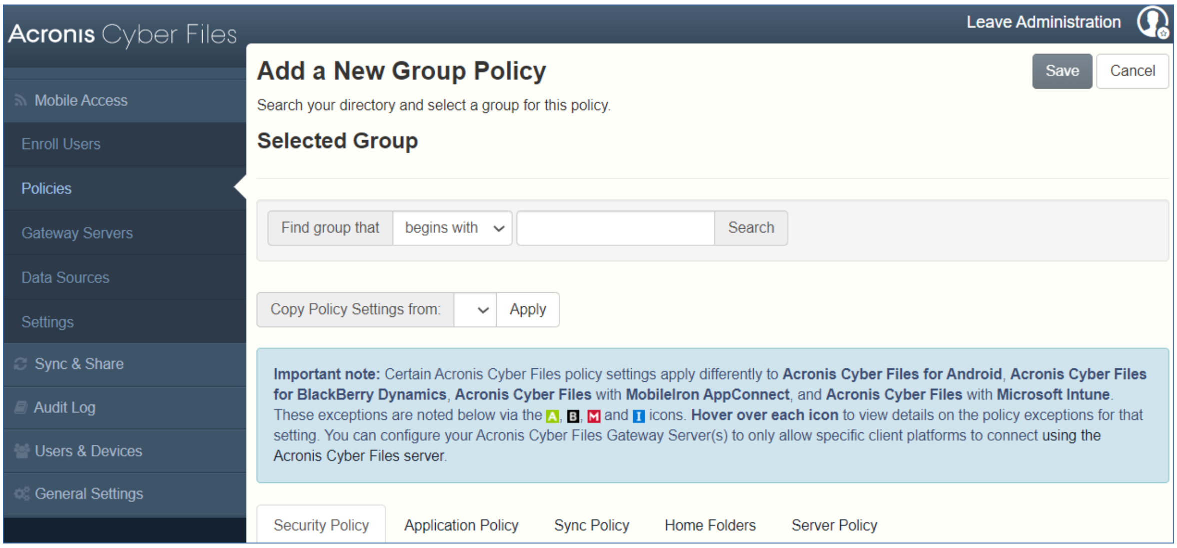
Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

| Common Name / Display Name | Distinguished Name | | Enabled | |
|---|---|---|---|---|
| Default | | | ☑ | |

3. In the **Find group** field, enter the partial or complete Active Directory group name for which you'd like to create a policy. You can perform '**begins with**' or '**contains**' searches for Active Directory groups. Begins with search will complete much faster than contains searches.
4. Click **Search** and then find and click the group name in the listed results.
5. Make the necessary configurations in each of the tabs (Security, Application, Sync, Home Folders and Server) and click **Save**.

### To add a new user policy:

1. Open the **User policies** tab.
2. Click the **Add new policy** button to add a new user policy. This will open the **Add a new user policy** page.



Add a New Group Policy

Search your directory and select a group for this policy.

Selected Group

**Important note:** Certain Acronis Cyber Files policy settings apply differently to **Acronis Cyber Files for Android**, **Acronis Cyber Files for BlackBerry Dynamics**, **Acronis Cyber Files** with **MobileIron AppConnect**, and **Acronis Cyber Files** with **Microsoft Intune**. These exceptions are noted below via the A, B, M and I icons. **Hover over each icon** to view details on the policy exceptions for that setting. You can configure your Acronis Cyber Files Gateway Server(s) to only allow specific client platforms to connect using the Acronis Cyber Files server.

3. In the **Find user** field, enter the partial or complete Active Directory user name for which you'd like to create a policy. You can perform '**begins with**' or '**contains**' searches for Active Directory users. Begins with search will complete much faster than contains searches.
4. Click **Search** and then find and click the user name in the listed results.
5. Make the necessary configurations in each of the tabs (Security, Application, Sync, Home Folders and Server) and click **Save**.

# Modifying Policies

Existing policies can be modified at any time. Changes to policies will be applied to the relevant mobile app users the next time they launch the mobile app.

**Note**

**Connectivity requirements**

Acronis Cyber Files clients must have network access to the Acronis Cyber Files server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access Acronis Cyber Files, they also need to connect to the VPN before management commands are accepted.

## To modify a group policy

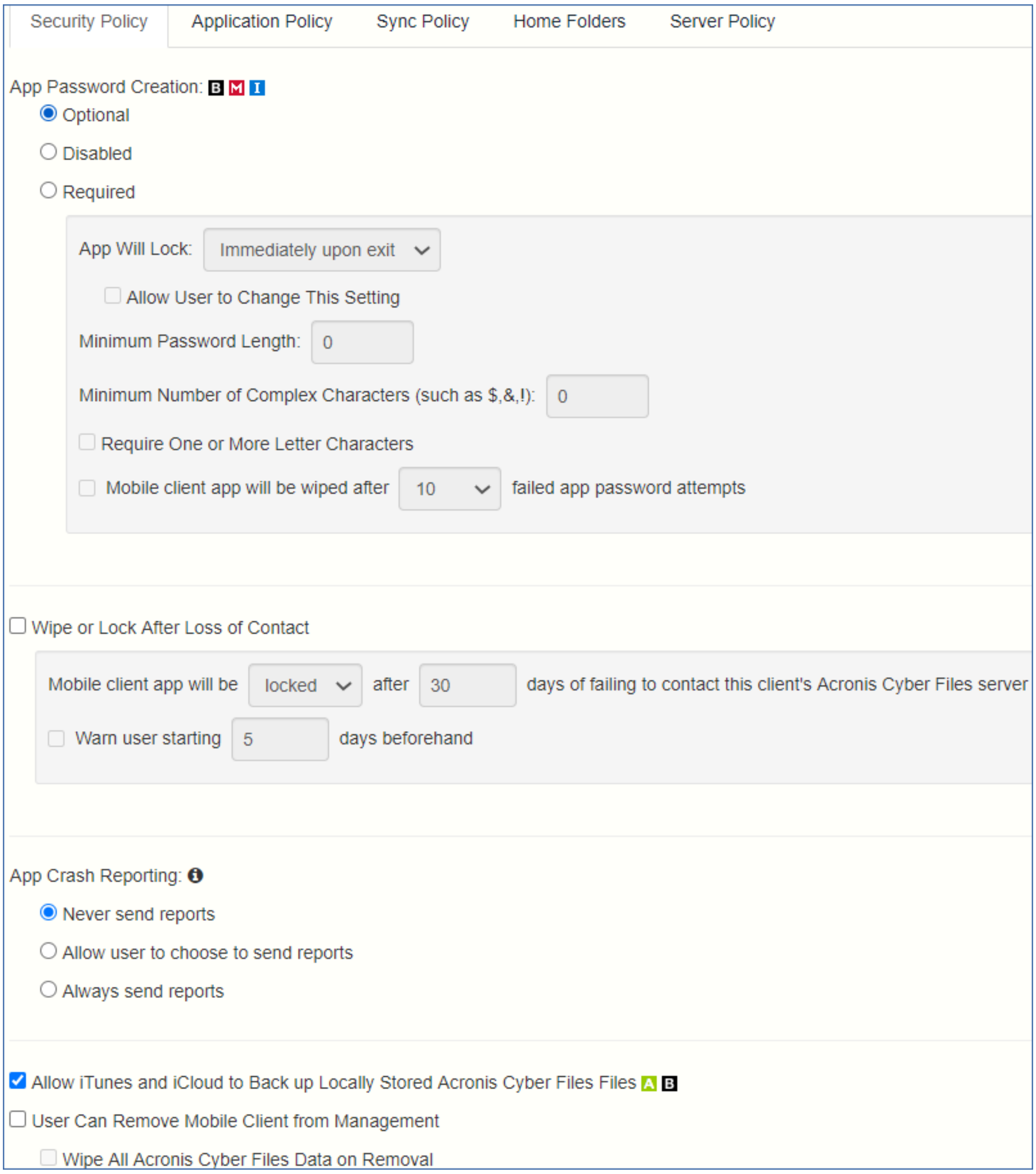
1. Click the **Groups Policies** option in top menu bar.
2. Click on the group you would like to modify.
3. Make any changes necessary on the **Edit Group Policy** page and press **Save**.
4. To temporarily disable a policy, uncheck the check box in the **Enabled** column for the desired group. This change takes effect immediately.
5. To change a group's priority, click the up or down arrow in the Manage Groups Profiles list. This will move the profile up or down one level.

### To modify a user policy:

1. Open the **User Policies** tab.
2. Click on the user you would like to modify.
3. Make any changes necessary on the **Edit User Policy** page and press **Save**.
4. To temporarily disable a policy, uncheck the check box in the **Enabled** column for the desired user.This change takes effect immediately.

# Policy Settings

## Security Policy



App Password Creation: B M I

● Optional

○ Disabled

○ Required

App Will Lock: Immediately upon exit

□ Allow User to Change This Setting

Minimum Password Length: 0

Minimum Number of Complex Characters (such as $,&,!): 0

□ Require One or More Letter Characters

□ Mobile client app will be wiped after 10 failed app password attempts

□ Wipe or Lock After Loss of Contact

Mobile client app will be locked after 30 days of failing to contact this client's Acronis Cyber Files server

□ Warn user starting 5 days beforehand

App Crash Reporting:

● Never send reports

○ Allow user to choose to send reports

○ Always send reports

☑ Allow iTunes and iCloud to Back up Locally Stored Acronis Cyber Files Files A B

□ User Can Remove Mobile Client from Management

□ Wipe All Acronis Cyber Files Data on Removal

- **App password creation** - The mobile application can be set with a lock password that must be first entered when launching the application.
    - **Optional** - This setting will not force the user to configure an application lock password, but they will be able to set one from the **Settings** menu within the app if they desire.
    - **Disabled** - This setting will disable the ability to configure an application lock password from the **Settings** menu within the app. This might be useful in the case of shared mobile devices where you prefer that a user cannot set an app password and will lock other users out of the mobile app.
    - **Required** - This setting will force the user to configure an application lock password if they do not already have one. The optional application password complexity requirements and failed password attempt wipe setting only apply when **App password creation** is set to **Required**.
        - **App will lock** - This setting configures the application password grace period. When a user switches from the Acronis Cyber Files mobile app to another application on their device, if they return to the mobile app before this grace period has elapsed, they will not be required to enter their application lock password. To require that the password is entered every time, choose **Immediately upon exit**. If you would like the user to be able to modify their **App will lock** setting from within the mobile app settings, select **Allow user to change this setting**.
        - **Minimum password length** - The minimum allowed length of the application lock password.
        - **Minimum number of complex characters** - The minimum number of non-letter, non-number characters required in the application lock password.
        - **Require one or more letter characters** - Ensures that there is at least one letter character in the application password.
        - **Mobile Client app will be wiped after X failed app password attempts** - When this option is enabled, the settings and data in the mobile app will be wiped after the specified number of consecutive failed app password attempts.
- **Wipe or lock after loss of contact**- Enable this setting if you would like the mobile app to automatically wipe or lock in the case that it has not made contact with this Acronis Cyber Files server in a certain number of days.

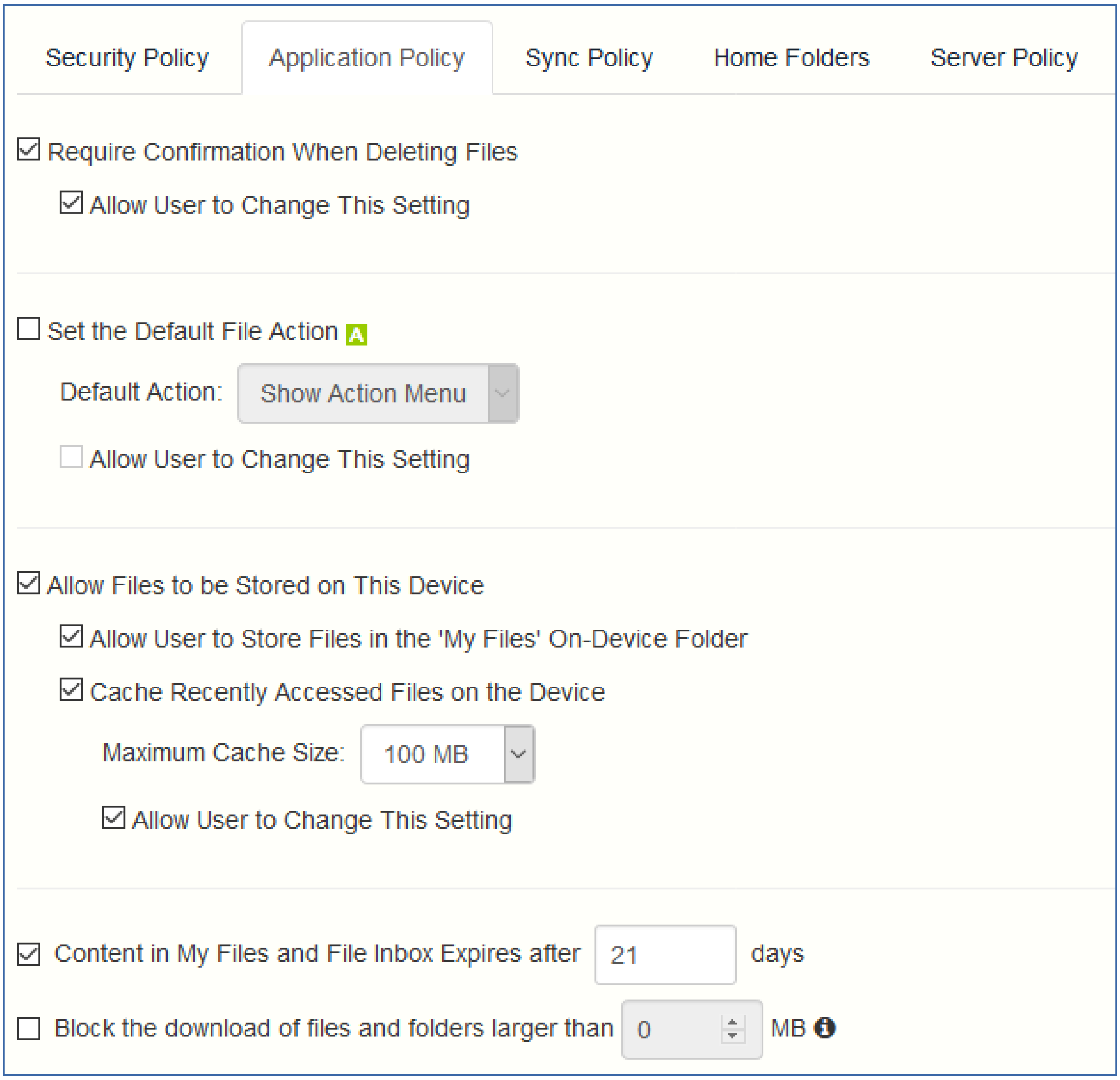
    **Warning!**
    If the app fails to authenticate to the server for whatever reason, it will not count as contacting the server, even if the server is reachable!

    - Locked clients will automatically unlock in the event that they later contact the server successfully.
    - Wiped clients immediately have all the local files stored in the mobile app deleted, their client management policy removed, and all settings reset to defaults. Wiped clients will have to be re-enrolled in management to gain access to gateway servers.
    - **Mobile Client app will be locked/wiped after X days of failing to contact this client's Acronis Cyber Files server -** Set the default action after the client fails to contact this Acronis

Cyber Files server for a number of days.

  - **Warn user starting [ ] days beforehand** - The Mobile app can optionally warn the user when a 'loss of contact' wipe or lock is going to happen in the near future. This gives them the opportunity to reestablish a network connection that allows the Mobile app to contact it's Acronis Cyber Files Server and prevent the lock or wipe.
- **App Crash Reporting** - Sends reports to Acronis if the mobile apps crash. No private data or identifying information is sent.
  - **Never send reports**
  - **Allow user to choose to send reports**
  - **Always send reports**
- **Allow iTunes and iCloud to back up locally stored Acronis Cyber Files files** - When this setting is disabled, the mobile app will not allow iTunes or iCloud to back up its files. This will ensure that no files within Acronis Cyber Files' secure on-device storage are copied into the backups.
- **User can remove Mobile Client from management**- Enable this setting if you would like your Acronis Cyber Files users to be able to uninstall their management policy from within Acronis Cyber Files. Doing so will return the application to full functionality and restore any configuration that was changed by their policy.
  - **Wipe all Acronis Cyber Files data on removal** - When user removal of policies is enabled, this option can be selected. If enabled, all data stored locally within the mobile application will be erased if it is removed from management, ensuring that corporate data does not exist on a client not under management controls.

## Application policy



☑ Require Confirmation When Deleting Files

☑ Allow User to Change This Setting

□ Set the Default File Action A

Default Action: Show Action Menu

□ Allow User to Change This Setting

☑ Allow Files to be Stored on This Device

☑ Allow User to Store Files in the 'My Files' On-Device Folder

☑ Cache Recently Accessed Files on the Device

Maximum Cache Size: 100 MB

☑ Allow User to Change This Setting

☑ Content in My Files and File Inbox Expires after 21 days

□ Block the download of files and folders larger than 0 MB

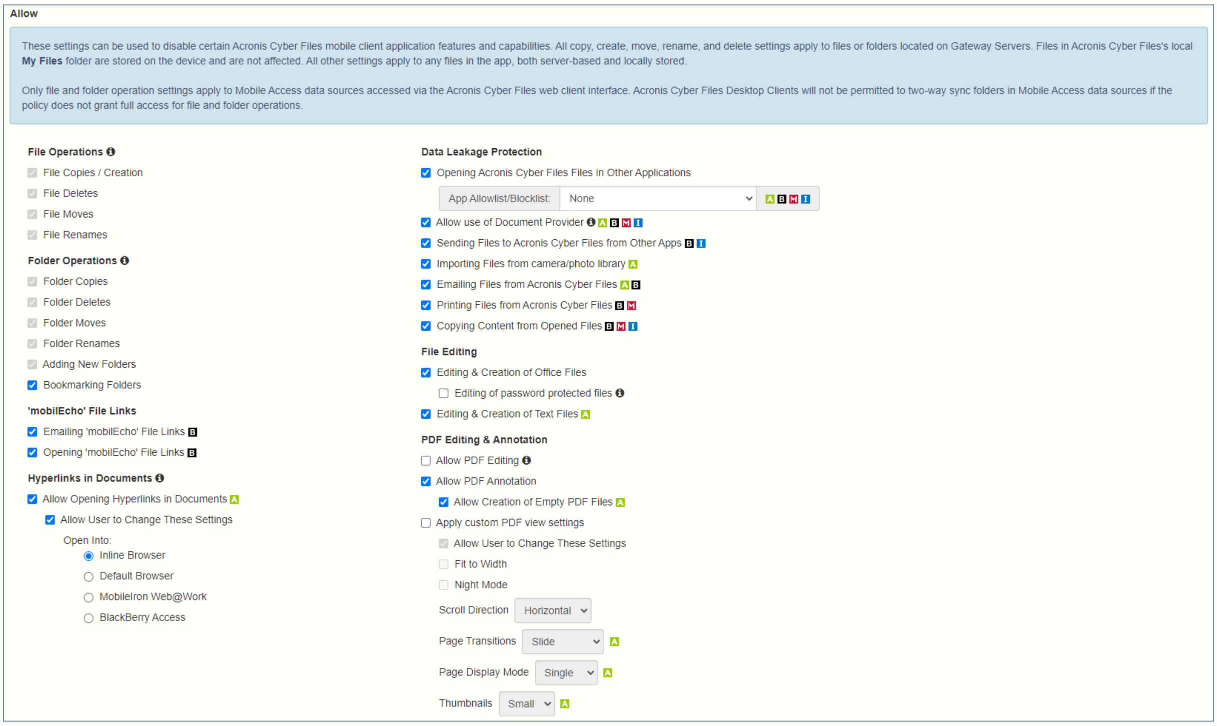
- **Require Confirmation When Deleting Files** - When enabled, the user will be asked for confirmation each time they delete a file. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Set the Default File Action** - This option determines what will happen when a user taps a file in the Mobile application. If this is not set, the client application defaults to **Action Menu**. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Allow Files to be Stored on the Device** - This setting is enabled by default. When enabled, files will be permitted to remain on the device, within Cyber Files' sandboxed storage. Individual features that store files locally (My Filesfolder, sync folders, recently accessed file caching) can be enabled or disabled using additional policy settings. If this option is disabled, no files will be stored on the device, ensuring that no corporate data is on the device if it is lost or stolen. If this

setting is disabled, the user will not be able to save or sync files for offline use, cache files for improved performance, or send files from other applications to the Cyber Files Mobile Client using the "Open In" function.

  - **Allow User to Store Files in the 'My Files' On-Device Folder** - If enabled, files can be copied into the 'My Files' folder for offline access and editing. This is a general purpose storage area within Cyber Files' on-device storage sandbox.
  - **Cache Recently Accessed Files on the Device** - If enabled, server-based files that have been recently access will be saved in a local cache on the device, for use if they are accessed again and have not changed, providing performance and bandwidth conservation benefits. **Maximum Cache Size** can be specified and the user can optionally be allowed to change this setting.

- **Content in My Files and File Inbox Expires after X days** - If this option is enabled, files in **My Files** will be deleted from the device after the set number of days.
- **Block the download of files and folders larger than XMB** - When enabled, files or folders larger than the set amount will not be downloaded by the mobile apps.

### *Allow*



Allow

These settings can be used to disable certain Acronis Cyber Files mobile client application features and capabilities. All copy, create, move, rename, and delete settings apply to files or folders located on Gateway Servers. Files in Acronis Cyber Files's local **My Files** folder are stored on the device and are not affected. All other settings apply to any files in the app, both server-based and locally stored.

Only file and folder operation settings apply to Mobile Access data sources accessed via the Acronis Cyber Files web client interface. Acronis Cyber Files Desktop Clients will not be permitted to two-way sync folders in Mobile Access data sources if the policy does not grant full access for file and folder operations.

**File Operations** ℹ

☑ File Copies / Creation
☑ File Deletes
☑ File Moves
☑ File Renames

**Folder Operations** ℹ

☑ Folder Copies
☑ Folder Deletes
☑ Folder Moves
☑ Folder Renames
☑ Adding New Folders
☑ Bookmarking Folders

**'mobilEcho' File Links**

☑ Emailing 'mobilEcho' File Links B
☑ Opening 'mobilEcho' File Links B

**Hyperlinks in Documents** ℹ

☑ Allow Opening Hyperlinks in Documents A
☑ Allow User to Change These Settings
Open Into:
● Inline Browser
○ Default Browser
○ MobileIron Web@Work
○ BlackBerry Access

**Data Leakage Protection**

☑ Opening Acronis Cyber Files Files in Other Applications
App Allowlist/Blocklist: None A B M I
☑ Allow use of Document Provider ℹ A B M I
☑ Sending Files to Acronis Cyber Files from Other Apps B I
☑ Importing Files from camera/photo library A
☑ Emailing Files from Acronis Cyber Files A B
☑ Printing Files from Acronis Cyber Files B M
☑ Copying Content from Opened Files B M I

**File Editing**

☑ Editing & Creation of Office Files
□ Editing of password protected files ℹ
☑ Editing & Creation of Text Files A

**PDF Editing & Annotation**

□ Allow PDF Editing ℹ
☑ Allow PDF Annotation
☑ Allow Creation of Empty PDF Files A
□ Apply custom PDF view settings
☑ Allow User to Change These Settings
□ Fit to Width
□ Night Mode
Scroll Direction: Horizontal
Page Transitions: Slide A
Page Display Mode: Single A
Thumbnails: Small A

These settings can be used to disable certain Mobile application features and capabilities. All copy, create, move, rename, and delete settings apply to files or folders located on Gateway servers. Files in the mobile client's local My Files folder are stored on the device and are not affected. All other settings apply to any files in Cyber Files, both server-based and locally stored on the client.

### File Operations

- **File Copies / Creation** - If this option is disabled, the user will not be able to save files from other applications or from the iPad Photos library to a Gateway Server. They will also be unable to copy or create new files or folders on the Gateway Server server Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file creation.

- **File Deletes** - If this option is disabled, the user will not be able to delete files from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file deletion.
- **File Moves** - If this option is disabled, the user will not be able to move files from one location to another on the Gateway Server, or from the server to the Mobile application's local My Files storage. This setting supersedes any NTFS permissions that client may have that allow file or folder moves.
- **File Renames** - If this option is disabled, the user will not be able to rename files from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file renames.

**Folder Operations**

- **Folder Copies** - If this option is disabled, the user will not be able to copy folders on or to the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow folder creation. **File copies / creation** must be enabled for this setting to be enabled.
- **Folder Deletes** - If this option is disabled, the user will not be able to delete folders from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow folder deletion.
- **Folder Moves** - If this option is disabled, the user will not be able to move folders from one location to another on the Gateway Server, or from the server to the Acronis Cyber Files mobile application's local My Files storage. This setting supersedes any NTFS permissions that client may have that allow file or folder moves. **Folder copies** must be enabled for this setting to be enabled.
- **Folder Renames** - If this option is disabled, the user will not be able to rename or folders from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow folder renames.
- **Adding New Folders** - If this option is disabled, the user will not be able to create new, empty folders on the Gateway Server.
- **Bookmarking Folders** - If this option is disabled, the user will not be able to bookmark on-device or on-server Acronis Cyber Files folders for quick shortcut access.

**'mobilEcho' File Links**

- **Emailing 'mobilEcho' File Links** - If this option is disabled, users will not be able to send mobilEcho:// URLs to Acronis Cyber Files files or folders to other Acronis Cyber Files users. These links are only functional if opened from a device where the recipient has the Acronis Cyber Files Mobile Client installed and configured with a server or assigned folder that has access to the link location. The user must also have file/folder-level permission to read the item.
- **Opening 'mobilEcho' File Links** - If this option is disabled, users will not be allowed to open mobilEcho:// URLs to Acronis Cyber Files files or folders.

**Hyperlinks in Documents**

- **Allow Opening Hyperlinks in Documents** - When enabled, users will be able to open any hyperlinks that are saved in their documents.
  - **Allow User to Change These Settings** - When enabled, users will be able to enable or disable this feature based on their preference.

  Open into:
  - **Inline Browser** - Hyperlinks will be opened directly in the Acronis Cyber Files app.
  - **Default Browser** - Hyperlinks will be opened in the default browser selected on your device.
  - **MobileIron Web@Work** - Hyperlinks will be opened in the MobileIron Web@Work app.

**Data Leakage Protection**

- **Opening Acronis Cyber Files Files in Other Applications** - If this option is disabled, the Mobile application will omit the **Open In** button and not allow files in Acronis Cyber Files to be opened in other applications. Opening a file in another application results in the file being copied to that application's data storage area and outside of Acronis Cyber Files control.
  - **App Allowlist/Blocklist** - Select a predefined allowlist or blocklist that restricts that third party apps that Acronis Cyber Files files can be opened into on the device. To create an allowlist or blocklist, click **Allowed Apps** in the top menu bar.
- **Allow use of Document Provider** - Allows mobile devices to use the Document Provider extension for Acronis Cyber Files. The Document Provider Extension can be affected by certain configurations:
  a. If a client is managed by an older server, the Document Provider Extension is enabled unless either **Opening Acronis Cyber Files Files in Other Applications** is **disabled** or there is a block/allow list **enabled**.
  b. If a client is managed by a new server (version 7.3.1 and newer) and **Allow use of Document Provider** is enabled, even if **Opening Acronis Cyber Files Files in Other Applications** is **disabled** or there are allow/block lists **enabled**, users will still be able to share files with other apps. Even specifically blocked ones.
  c. If **Allow use of Document Provider** is enabled, but the creation of files is disabled, the Document Provider Extension will work but users will not be able to save files from other apps to any Acronis Cyber Files Data Sources.
- **Sending Files to Acronis Cyber Files from Other Apps** - If this option is disabled, the Mobile application will not accept files sent to it from other applications' **Open In** feature.
- **Importing Files from camera/photo library** - When enabled, users will be able to import photos and videos from their device's photo library directly into Acronis Cyber Files.
- **Emailing Files from Acronis Cyber Files** - If this option is disabled, the Mobile application will omit the **Email File** button and not allow files in Acronis Cyber Files to be emailed from the application.

**Note**
The Android platform does not have a built-in email app or function that can be disabled. To block users from moving files into emails, you must instead disable Opening Acronis Cyber Files files into Other Applications.

- **Printing Files from Acronis Cyber Files** - If this option is disabled, the Mobile application will omit the **Print** button and not allow files in Acronis Cyber Files to be printed.
- **Copying text From Opened Files** - If this option is disabled, the mobile app will not allow users to select text in opened documents for copy/paste operations. This will prevent data from being copied into other applications.

**Warning!**
If a MobileIron policy is active, its `Allow Copy/Paste To` setting supersedes this setting.

### File Editing

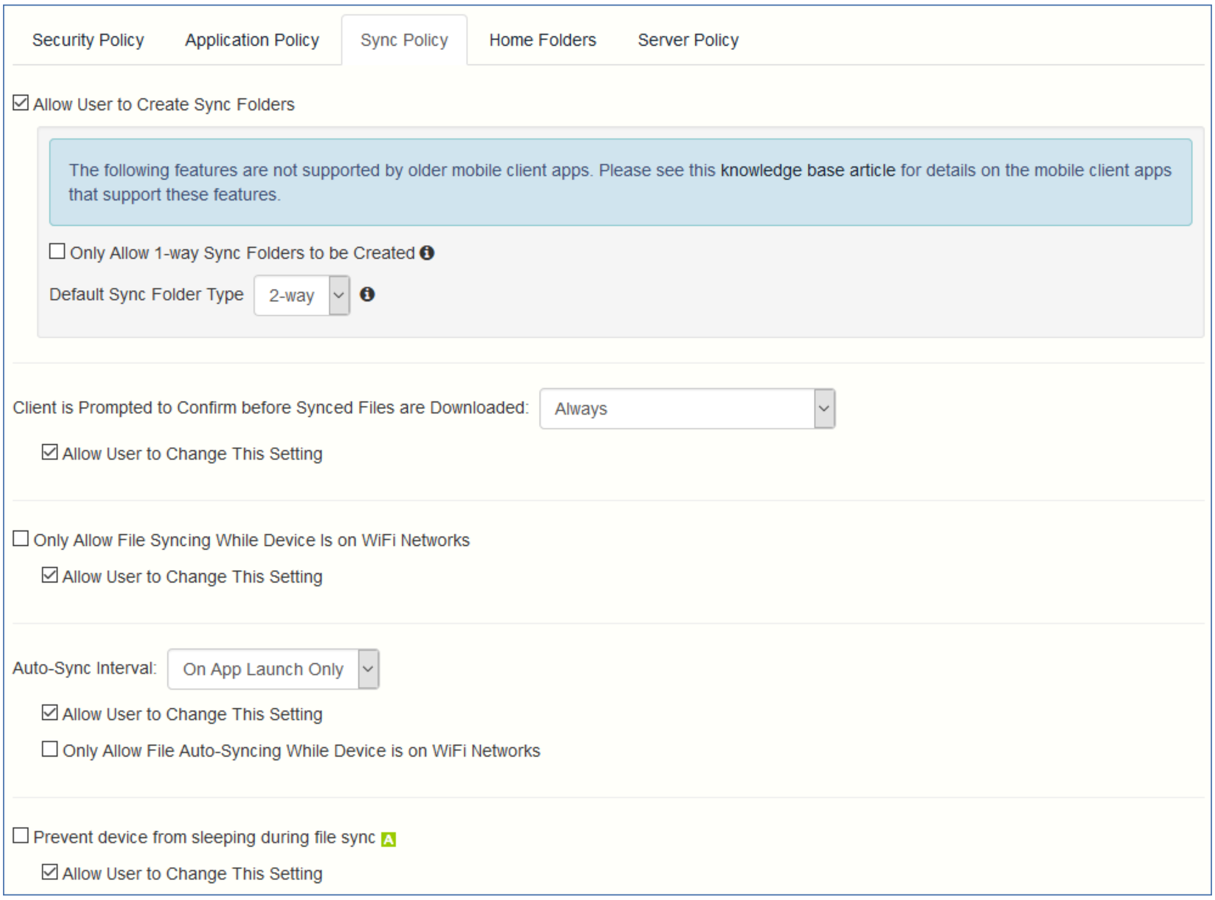
- **Editing & Creation of Office files** - If this option is disabled, users will not be allowed to edit documents using the integrated Polaris editor.
  - **Editing of password protected files** - If this option is disabled, users will not be allowed to edit password protected files.
- **Editing & Creation of Text files** - If this option is disabled, users will not be allowed to edit .txt files using the built-in text editor.

### PDF Editing and Annotation

- **Allow PDF Editing** - When enabled, users can access many PDF editing features such as creating new pages, duplicating pages, copying and pasting, reordering, rotation, deletion, and creation of new documents from a subset of selected pages.
- **Allow PDF annotation** - When this option is disabled, the mobile app will not be allowed to annotate PDFs.
  - **Allow Creation of Empty PDF Files** - When enabled, enables users to create empty PDF files which they can edit with Annotations.
- **Apply custom PDF view settings** - When enabled, all of the sub-settings will apply for all users, for all PDFs.
  - **Allow User to Change These Settings** - When enabled, users will be able to change their PDF viewing settings.
  - **Scroll Direction** – Lets you choose how the pages change – vertically or horizontally.
  - **Page Transitions** – Lets you choose the transition visual effects. **Slide** will plainly change the pages, **Continuous** will let you scroll through the pages as if they are one connected piece and **Curl** will flip the pages like a book.
  - **Page Display** – Lets you choose the view mode – one page at a time or two pages at a time.
  - **Thumbnails** – Sets the size for the PDF pages thumbnails. You can choose between **Small**, **Large** and **None**.

- **Search Mode** – Configures the display format of the search results provided by the built-in PDF viewer. There are three types of search results view:
  - **Simple** – Highlights the results and you can scroll through them with the arrow icons.
  - **Detailed** – Displays a drop-down list of all results and you can navigate by tapping on them.
  - **Dynamic** – Sets the search result view to **Simple** for iPhones and **Detailed** for iPads.
- **Hyperlink Highlighting** – Lets you choose the color for highlighting the hyperlinks. You can also disable the highlighting by selecting **Disabled**.
- **Fit to Width** – When enabled, resizes the page so it will fit the width of your device's screen.
- **Night Mode** – When enabled, your device uses the Night Mode color scheme for a more comfortable viewing experience in low-lit areas.

## Sync Policy



☑ Allow User to Create Sync Folders

The following features are not supported by older mobile client apps. Please see this knowledge base article for details on the mobile client apps that support these features.

☐ Only Allow 1-way Sync Folders to be Created

Default Sync Folder Type: 2-way

Client is Prompted to Confirm before Synced Files are Downloaded: Always

☑ Allow User to Change This Setting

☐ Only Allow File Syncing While Device Is on WiFi Networks

☑ Allow User to Change This Setting

Auto-Sync Interval: On App Launch Only

☑ Allow User to Change This Setting

☐ Only Allow File Auto-Syncing While Device is on WiFi Networks

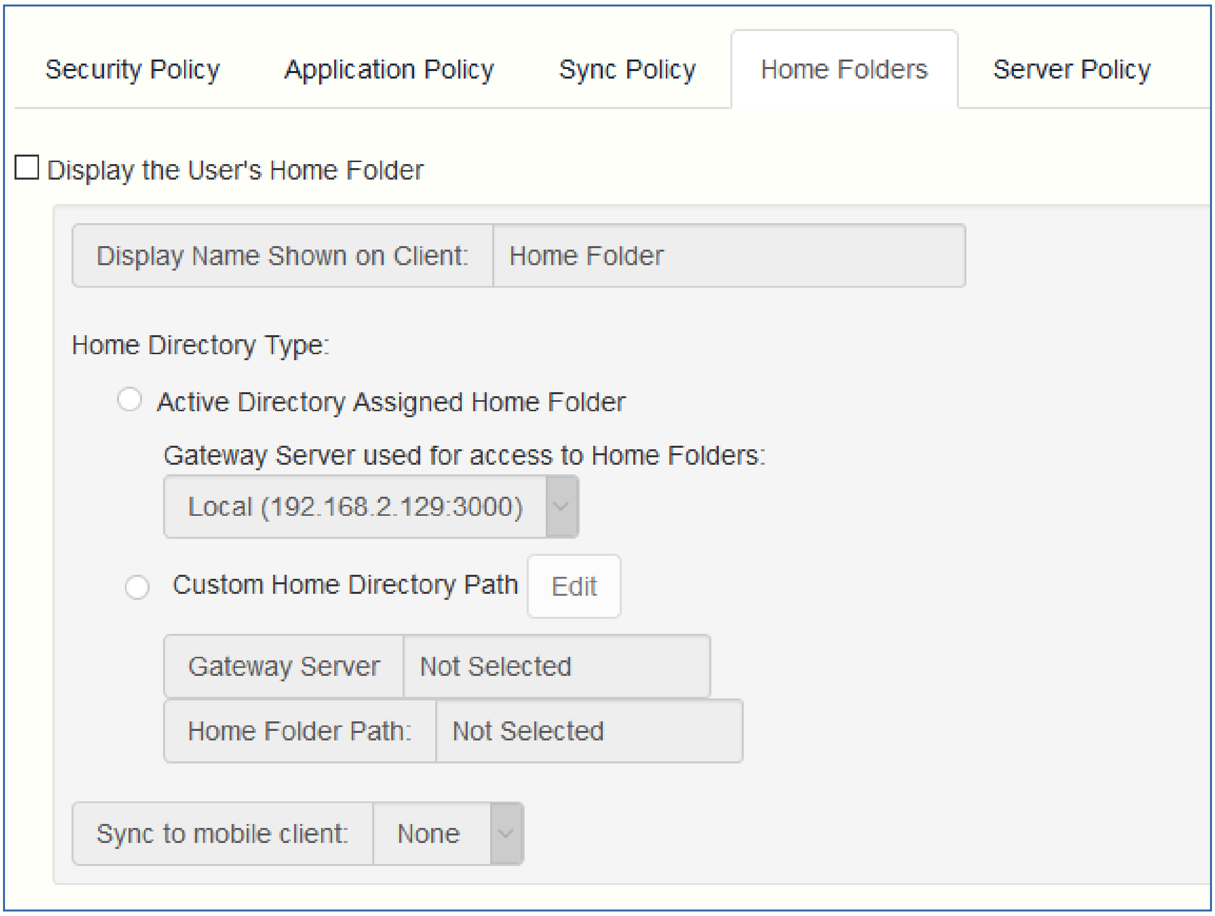
☐ Prevent device from sleeping during file sync

☑ Allow User to Change This Setting

- **Allow User to Create Sync Folders -** Allows the user to create their own sync folders.
  - **Only Allow 1-way Sync Folders to be Created** - Users will be able to create only 1-way sync folders.
  - **Default Sync Folder Type** - Sets either 1-way or 2-way as the default Sync folder type.
- **Client is Prompted to Confirm Before Synced Files are Downloaded** - Select the conditions under which the user must confirm before files in synced folders are downloaded. Options are: **Always**, **While on cellular networks only,** and **Never**. If **Allow User to Change This Setting** is enabled, clients will be able to change the confirmation options.

- **Only Allow File Syncing While Device is on WiFi Networks** - When this option is enabled, Acronis Cyber Files will not allow files to be synced over cellular connections. If **Allow User to Change This Setting** is enabled, clients will be able to enable or disable automatic file syncing while on WiFi networks.
- **Auto-Sync Interval** - When this option is enabled, Acronis Cyber Files will automatically sync **never**, **on app launch only** or on several **time intervals**.
  - **Allow User to Change This Setting** - When this option is enabled, the users will be able to change the time interval from the Acronis Cyber Files mobile app.
  - **Only Allow File Auto-Syncing While Device is on WiFi Networks** - When this option is enabled the auto-sync will not occur unless the user is connected via WiFi.
- **Prevent device from sleeping during file sync** - When enabled, devices supporting this setting will not lock/sleep if you have file syncs in progress. If **Allow User to Change This Setting** is enabled, clients will be able to change the confirmation options.

## Home Folders



□ Display the User's Home Folder

Display Name Shown on Client: Home Folder

Home Directory Type:

○ Active Directory Assigned Home Folder

Gateway Server used for access to Home Folders: Local (192.168.2.129:3000)

○ Custom Home Directory Path

Gateway Server: Not Selected

Home Folder Path: Not Selected

Sync to mobile client: None

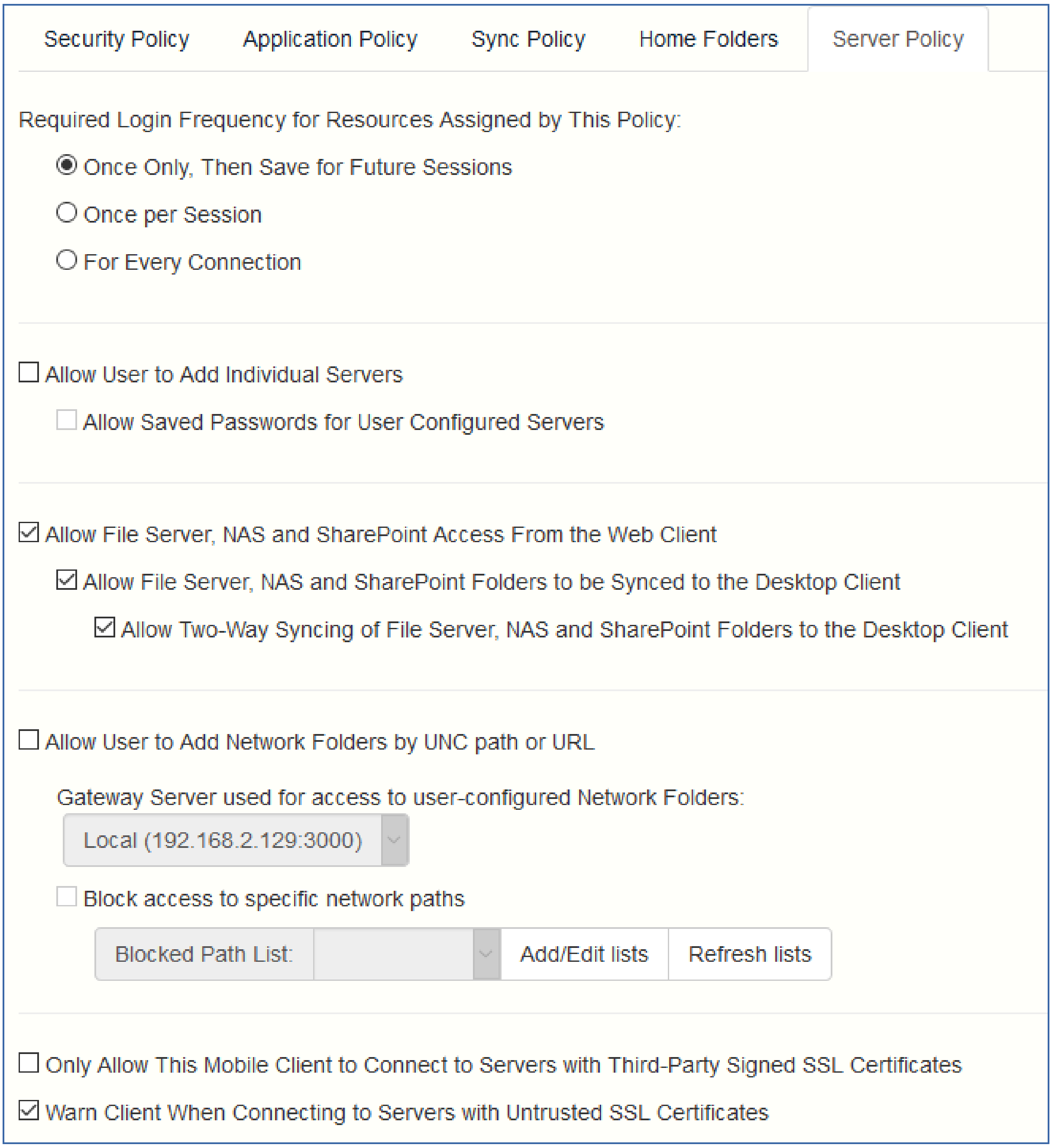
- **Display the user's home folder**- This option causes a user's personal home directory to appear in the Mobile app.
  - **Display name shown on client** - Sets the display name of the home folder item in the Mobile app. The `%USERNAME%` wildcard can be used to include the user's username in the folder name that will be displayed.

**Note**
The `%USERNAME%` wildcard cannot be used to display the user's username on any other type of data source. You can only use it on Active Directory assigned Home Folders.

- **Active Directory assigned home folder** - The home folder shown in the Mobile app will connect the user to the server/folder path defined in their AD account profile.
  The Home Folder will be accessible via the selected Gateway.
- **Custom home directory path** - The home folder shown in the Mobile app will connect the user to the server and path defined in this setting. The `%USERNAME%` wildcard can be used to include the user's username in the home folder path for any data source type. %USERNAME% must be capitalized.
- **Sync to mobile client –** This option selects the type of sync of your Home Directory.

**Note**
This option does **NOT** affect the user's ability to sync their Home Folder with the desktop client.

## Server Policy



Required Login Frequency for Resources Assigned by This Policy:

● Once Only, Then Save for Future Sessions

○ Once per Session

○ For Every Connection

□ Allow User to Add Individual Servers

□ Allow Saved Passwords for User Configured Servers

☑ Allow File Server, NAS and SharePoint Access From the Web Client

☑ Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client

☑ Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client

□ Allow User to Add Network Folders by UNC path or URL

Gateway Server used for access to user-configured Network Folders: Local (192.168.2.129:3000)

□ Block access to specific network paths

Blocked Path List:

□ Only Allow This Mobile Client to Connect to Servers with Third-Party Signed SSL Certificates

☑ Warn Client When Connecting to Servers with Untrusted SSL Certificates

- **Required login frequency for resources assigned by this policy**- sets the frequency that a user must log into the servers that are assigned to them by their policy.
  - **Once only, then save for future sessions** - The user enters their password when they are initially enrolled in management. This password is then saved and used for any file server connections they later initiate.
  - **Once per session** - After launching the Acronis Cyber Files mobile, the user is required to enter their password at the time they connect to the first server. Until they leave the Acronis Cyber Files mobile application, they can then connect to additional servers without having to

reenter their password. If they leave the Acronis Cyber Files mobile for any period of time and then return, they will be required to enter their password again to connect to the first server.

  - **For every connection** - The user is required to enter their password each time they connect to a server.

- **Allow user to add individual servers** - If this option is enabled, users will be able to manually add servers from within the Acronis Cyber Files mobile application, as long as they have the server's DNS name or IP address. If you want the user to only have their policy **Assigned Servers** available, leave this option disabled.
  - **Allow saved passwords for user configured servers** - If a user is allowed to add individual servers, this sub-option determines whether they are allowed to save their password for those server.
- **Allow File Server, NAS and Sharepoint Access From the Web Client** - When enabled, Web Client users will be able to see and access mobile Data Sources as well.
  - **Allow File Server, Nas and SharePoint Folders to be Synced to the Desktop Client** - When enabled, desktop clients will be allowed to 1-way sync **Network** content.
    - **Allow Two-Way Syncing of File Server, Nas and SharePoint Folders to the Desktop Client** - When enabled, desktop clients will be allowed to 2-way sync **Network** content.

      **Note**

      To enable the 2-way syncing of **Network** content for the desktop clients, you must also have allowed the following file and folder actions on the **Application Policy** tab: **Creation** (**Adding** for folders), **Copies**, **Deletes**, **Moves** and **Renames**.

- **Allow User to Add Network Folders by UNC path or URL** - When enabled, the mobile client users will be able to add and access network folders and SharePoint sites not assigned to them or not accessible through the existing Data Sources. The selected Gateway Server must have access to those SMB shares or SharePoint sites.
  - **Block access to specific network paths** - When enabled, allows the administrator to create and use blocklists of network paths which the users shouldn't be allowed to self-provision.
- **Only allow this Mobile Client to connect to servers with third-party signed SSL certificates** - If this option is enabled, the Access Mobile Client Acronis Cyber Files mobile will only be permitted to connect to servers with third-party signed SSL certificates.

  **Note**

  If the management server does not have a third-party certificate, the client will be unable to reach the management server after it's initial configuration. If you enable this option, ensure you have third-party certificates on all your Gateway Servers.

- **Warn client when connecting to servers with untrusted SSL certificates** - If your users are routinely connecting to servers that will be using self-signed certificates, you may choose to disable the client-side warning dialog message they will receive when connecting to these servers.
- **Client timeout for unresponsive servers** - This option sets the client login connection timeout for unresponsive servers. If your clients are on especially slow data connections, or if they rely on

a VPN-on-demand solution to first establish a connection before a Gateway Server is reachable, this timeout can be set to a value greater than the 30 second default. If you want the client to be able to change this through the Acronis Cyber Files mobile app, check **Allow user to change this setting.**

## Exceptions for policy settings

For users running the **Acronis Cyber Files mobile for Android** and **Acronis Cyber Files mobile with Mobile Iron AppConnect** apps, there are some exceptions to the way Acronis Cyber Files management policies are applied to the Mobile app. In the case of Android, a few features are not yet supported, so the related policies do not apply. With MobileIron, a few of the standard Acronis Cyber Files policy features are deferred to the MobileIron AppConnect platform. These exceptions are noted on the Acronis Cyber Files policy configuration pages. Hover over the Android and MobileIron logos for more details on the individual policy exceptions.

# Creating a Blocked Path list

You can create blocklists for paths you do not want your users to be able to self-provision from mobile devices. These lists must be assigned to a User or Group policy and are valid only for self-provisioned paths. When the list has been created and assigned to the proper Users and/or Groups, you need to enable the **Block access to specific network paths** for every User/Group policy that you want it to affect.

### To create a list:

1. Open the web interface as an administrator.
2. Open the Policies page.
3. Click on the desired User policy or Group policy.
4. Open the Server Policy tab.
5. Select the **Block access to specific network paths** check box.

   **Note**
   You must perform this step for each User/Group policy that you want to assign the blocklist to.

6. Press **Add/Edit lists**.
7. On the **Blocked Path Lists** page press **Add List**.
8. Enter a name for the list.
9. Enter a path or list of paths that will be blocklisted. Each entry should be on a new line.
10. Open the **Apply to User or Group** tab.
11. Assign the list to the desired user(s)/group(s).
12. Press **Save**.

### To enable the blocklist for a User or Group policy:

1. Open the web interface as an administrator.
2. Open the Policies page.
3. Click on the desired User policy or Group policy.
4. Open the Server Policy tab.
5. Select the **Block access to specific network paths** check box.

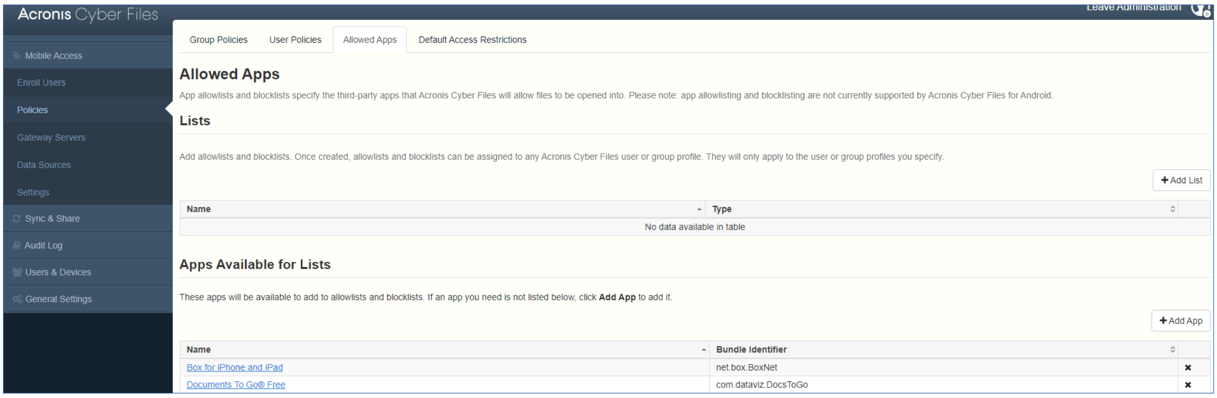
> **Note**
> You must perform this step for each User/Group policy that you want to assign the blocklist to.

6. Select the desired list from the drop-down menu.

> **Note**
> Pressing **Refresh lists** will refresh the options in the drop-down menu.

7. Press **Save** to save and exit the policy.

## Allowed Apps



Allowed Apps

App allowlists and blocklists specify the third-party apps that Acronis Cyber Files will allow files to be opened into. Please note: app allowlisting and blocklisting are not currently supported by Acronis Cyber Files for Android.

Lists

Add allowlists and blocklists. Once created, allowlists and blocklists can be assigned to any Acronis Cyber Files user or group profile. They will only apply to the user or group profiles you specify.

| Name | Type |
|---|---|
| No data available in table | |

Apps Available for Lists

These apps will be available to add to allowlists and blocklists. If an app you need is not listed below, click **Add App** to add it.

| Name | Bundle Identifier | |
|---|---|---|
| Box for iPhone and iPad | net.box.BoxNet | ✖ |
| Documents To Go® Free | com.dataviz.DocsToGo | ✖ |

Acronis Cyber Files Client Management allows you to create allowlists or blocklists that restrict the Acronis Cyber Files mobile's ability to open files into other apps on a mobile device. These can be used to ensure that any files accessible through the Acronis Cyber Files mobile can only be opened into secure, trusted apps.

**Allowlists** - allow you to specify a list of apps that Acronis Cyber Files files are allowed to be opened into. All other apps are denied access.

**Blocklists** - allow you to specify a list of apps that Acronis Cyber Files files are not allowed to be opened into. All other apps are allowed access.

In order for Acronis Cyber Files to identify a particular app, it needs to know the app's **Bundle Identifier**. A list of common apps, and their bundle identifiers, are included in the Acronis Cyber Files Web Interface by default. If the app you need to allowlist or blocklist is not included, you will need to add it to the list.

**Note**

App allowlisting and blocklisting are not currently supported by the Acronis Cyber Files mobile for Android.

**Lists**

Add allowlists and blocklists. Once created, allowlists and blocklists can be assigned to any Acronis Cyber Files user or group policy. They will only apply to the user or group policies you specify.

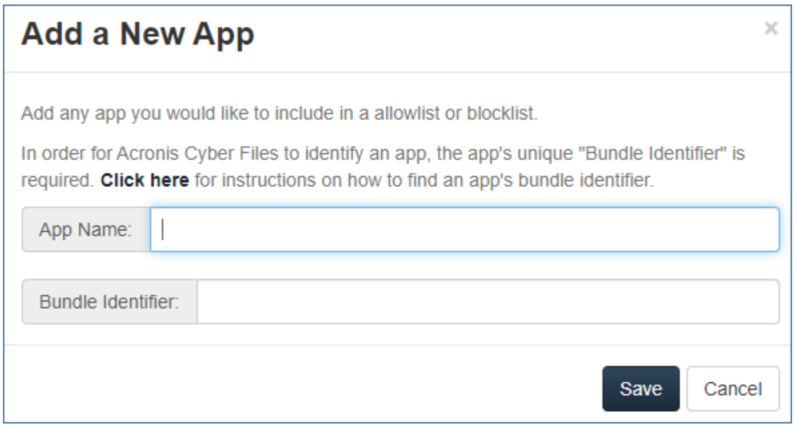
- **Name** - Shows the name of the list set by the administrator.
- **Type** - Shows the type of the list (allowlist/blocklist)
- **Add List** - Opens the Add a New Allowlist or Blocklist menu.

## Adding Apps Available for Lists

To add an app to be included in an allowlist or blocklist:

1. Click **Allowed Apps** in the top menu bar.
2. Click **Add app** in the **Apps Available for Lists** section.
3. Enter the **App name**. This can be the name of the app as it appears in the App Store, or an alternate name of your choosing.
4. Enter the app's **Bundle identifier**. This must match the intended apps bundle identifier exactly, or it will not allow or blocklisted.
5. Click **Save**.

You can find the bundle identifier either by browsing the files on your device or you can view it in an iTunes Library.



Add a New App

Add any app you would like to include in a allowlist or blocklist.

In order for Acronis Cyber Files to identify an app, the app's unique "Bundle Identifier" is required. **Click here** for instructions on how to find an app's bundle identifier.

App Name:

Bundle Identifier:

## Finding an App's bundle identifier

### Finding an app's bundle identifier by browsing the files on your device

If you use software that allows browsing the contents of your device's storage, you can locate a app on the device and determine its **bundle identifier** . One app that can be used for this is iExplorer .

1. Connect your device to your computer with USB and open iExplorer or a similar utility.
2. Open the Apps folder on the device and locate the app you require.
3. Open that app's folder and locate its **iTunesMetadata.plist** file.
4. Open this PLIST file in a text editor.
5. Find the **softwareVersionBundleId** key in the list.
6. The **string** value below it is the bundle identifier value that you will need to enter for the app in Acronis Cyber Files. These are commonly formatted as: **com.companyname.appname**

### Finding an app's bundle identifier in an iTunes Library

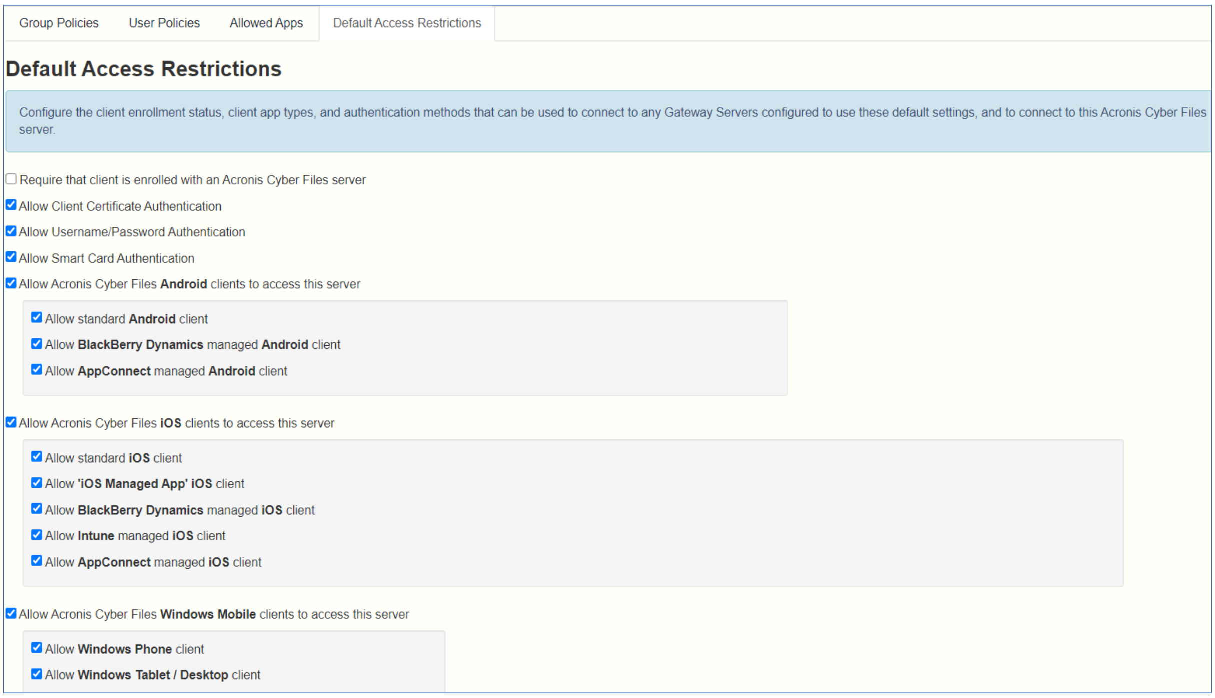
If you sync your device with iTunes and the app you desire is either on your device, or was downloaded through iTunes, it will exist on your computer's hard drive. You can locate it on your hard drive and look inside the app to find the **bundle identifier**.

1. Navigate to your iTunes Library and open the **Mobile Applications** folder.
2. On a Mac, this is typically in your home directory, in ~/Music/iTunes/Mobile Applications/
3. On a Windows 7 PC, this is typically in `C:\Users\username\My Music\iTunes\Mobile Applications/`
4. If you have recently installed the app on your device, make sure you have performed an iTunes sync before you continue.
5. Locate the app that you require in the **Mobile Applications** folder.
6. Duplicate the file and rename the extension to .ZIP
7. Unzip this newly created ZIP file and you'll end up with a folder with the application name.
8. Inside that folder is a file called **iTunesMetadata.plist**
9. Open this PLIST file in a text editor.
10. Find the **softwareVersionBundleId** key in the list.
11. The **string** value below it is the bundle identifier value that you will need to enter for the app in Acronis Cyber Files. These are commonly formatted as: **com.companyname.appname**

## Default Access Restrictions

This section allows you to set restrictions for clients contacting the management server and these restrictions are also the default restrictions for Gateway Servers.

**Note**
For information on setting custom access restrictions for your Gateway Servers visit the Editing Gateway Servers article in the Managing Gateway Servers section.



Default Access Restrictions

Configure the client enrollment status, client app types, and authentication methods that can be used to connect to any Gateway Servers configured to use these default settings, and to connect to this Acronis Cyber Files server.

- ☐ Require that client is enrolled with an Acronis Cyber Files server
- ☑ Allow Client Certificate Authentication
- ☑ Allow Username/Password Authentication
- ☑ Allow Smart Card Authentication
- ☑ Allow Acronis Cyber Files **Android** clients to access this server
  - ☑ Allow standard **Android** client
  - ☑ Allow **BlackBerry Dynamics** managed **Android** client
  - ☑ Allow **AppConnect** managed **Android** client
- ☑ Allow Acronis Cyber Files **iOS** clients to access this server
  - ☑ Allow standard **iOS** client
  - ☑ Allow **'iOS Managed App' iOS** client
  - ☑ Allow **BlackBerry Dynamics** managed **iOS** client
  - ☑ Allow **Intune** managed **iOS** client
  - ☑ Allow **AppConnect** managed **iOS** client
- ☑ Allow Acronis Cyber Files **Windows Mobile** clients to access this server
  - ☑ Allow **Windows Phone** client
  - ☑ Allow **Windows Tablet / Desktop** client

Configure the client enrollment status, client app types and authentication methods that can be used to connect to this Acronis Cyber Files server and any Gateway Servers configured to use the default access restrictions.

- **Require that client is enrolled with an Acronis Cyber Files server** - If you select this option, all Acronis Cyber Files mobiles connecting to this server are required to be managed by a Acronis Cyber Files server that is listed under Allowable Acronis Cyber Files servers. This option ensures that all clients accessing the server have the settings and security options you require. The server name entered must match the management server name configured in the Mobile app. Partial names may also be used to allow multiple client management servers in a domain, for instance. Partial names do not need wildcard symbols.
- **Allow Client Certificate Authentication** - If you uncheck this option, users will not be able to connect via certificate and will be able to connect via client username and password or smart card.
- **Allow Username/Password Authentication** - If you uncheck this option, users will not be able to connect via username and password and will be able to connect via client certificate or smart card.
- **Allow Smart Card Authentication** - If you uncheck this option, users will not be able to connect via smart card and will be able to connect via client username and password or certificate.
- **Allow Acronis Cyber Files Android clients to access this server** – If you uncheck this option, Android devices will not be able to connect to the Acronis Cyber Files server and you won't be able to access management as well. If you select this option, you can further set which clients can connect by the options below.
  - **Allow standard Android client** - If you select this option, this Acronis Cyber Files server will allow users running the standard Android Acronis Cyber Files client app to connect. If you do not want to allow Android users to access this Acronis Cyber Files server, you can uncheck this

setting.

  - **Allow AppConnect managed Android client** - If you select this option, this Acronis Cyber Files server will allow Android users with Acronis Cyber Files clients enrolled in MobileIron. If you do not want to allow Android users enrolled in MobileIron to access this Acronis Cyber Files server, you can uncheck this setting.
- **Allow Acronis Cyber Files iOS clients to access this server –** If you uncheck this option, iOS devices will not be able to connect to the AcronisCyber Files server and you won't be able to access management as well. If you select this option, you can further set which clients can connect by the options below.
  - **Allow standard iOS Client** – If you select this option, this Acronis Cyber Files server will allow users running the standard iOS Acronis Cyber Files mobile app to connect. If you do not want to allow iOS users to access this Acronis Cyber Files server, you can uncheck this setting.
  - **Allow 'iOS Managed App' iOS Client** – If you select this option, this Acronis Cyber Files server will allow users running the Acronis Cyber Files managed iOS app to connect. In order to be in this state, a client must received a Managed App Configuration containing at least one parameter. If you do not want to allow managed iOS users to access this Acronis Cyber Files server, you can uncheck this setting.
  - **Allow Intune managed iOS clients** – If you select this option, this Acronis Cyber Files server will allow users using the iOS Acronis Cyber Files mobile Intune managed client to connect. If you do not want to allow users managed by Intune to access this Acronis Cyber Files server, you can uncheck this setting.
  - **Allow AppConnect managed iOS clients** – If you select this option, this Acronis Cyber Files server will allow iOS users with Acronis Cyber Files mobile enrolled in MobileIron. If you do not want to allow iOS users enrolled in MobileIron to access this Acronis Cyber Filesserver, you can uncheck this setting.

# On-boarding Mobile Devices

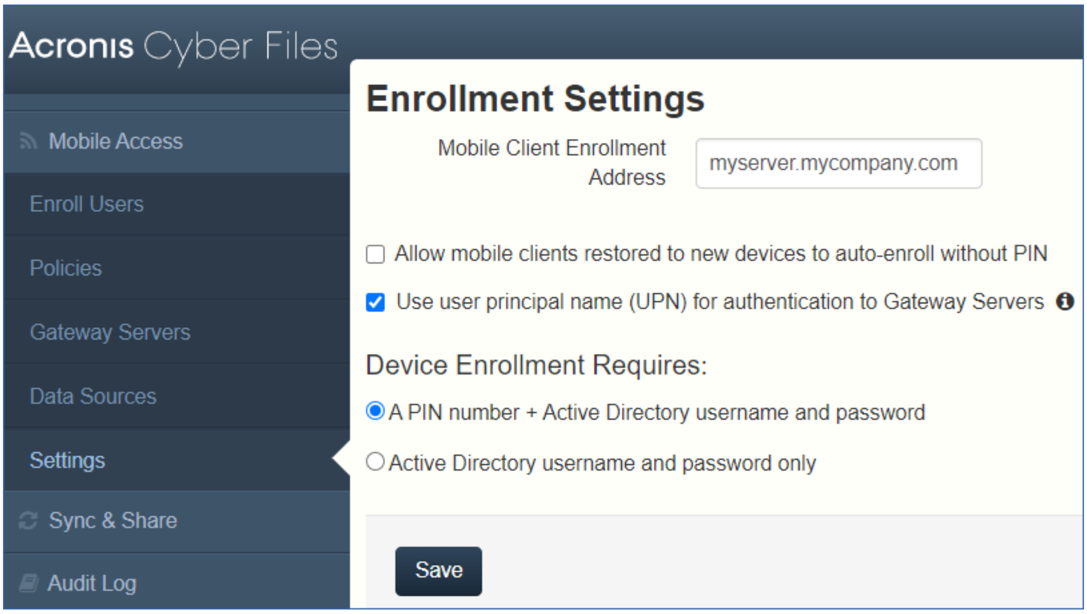
To get started with the Acronis Cyber Files mobile app, users need to install the app through their respective App Store - iTunes or Google Play. If your company is using client management, the users also need to enroll the Acronis Cyber Files mobile app on their device with the Acronis Cyber Files Server. Once enrolled, their mobile client configuration, security settings, and capabilities are controlled by their Acronis Cyber Files user or group policy.

The mobile application settings and features controlled by the management policy include:

- Requiring a Acronis Cyber Files application lock password
- App password complexity requirements
- Ability to remove the Acronis Cyber Files app from management
- Allow emailing and printing files from the Acronis Cyber Files app
- Allow storing files on the device
- Allow Acronis Cyber Files app on-device files to be included in iTunes backups
- Allow sending files to the Acronis Cyber Files from other applications

- Allow opening Acronis Cyber Files files in other applications
- Restrict the other applications that Acronis Cyber Files files are allowed to be opened into
- Allow PDF annotation
- Allow file and folder creation, renames and deletes
- Allow moving files
- Require confirmation when deleting
- Servers, folders, and home directories can be assigned so they automatically appear in the Acronis Cyber Files app
- Assigned folders can be configured to perform 1-way to 2-way syncing with the server

## Server-side Management Enrollment Process



Enrollment Settings

Mobile Client Enrollment Address: myserver.mycompany.com

☐ Allow mobile clients restored to new devices to auto-enroll without PIN

☑ Use user principal name (UPN) for authentication to Gateway Servers

Device Enrollment Requires:

● A PIN number + Active Directory username and password

○ Active Directory username and password only

1. Open the Acronis Cyber Files web interface.
2. Log in as an administrator.
3. Open the **Mobile Access** tab.
4. Open the **Settings** tab.
5. Select the desired device enrollment requirements

## Enrollment Settings

**Allow mobile clients restored to new devices to auto-enroll without PIN** - when enabled, this allows users managed by older versions of Acronis Cyber Files mobile to enroll to your new server without needing a PIN.

**Use user principal name (UPN) for authentication to Gateway Servers** - when enabled, users will authenticate to Gateway Servers with their UPN (e.g. user@company.com). When disabled, users will authenticate with their domain name and username (e.g. domain/user).

## Device Enrollment Mode

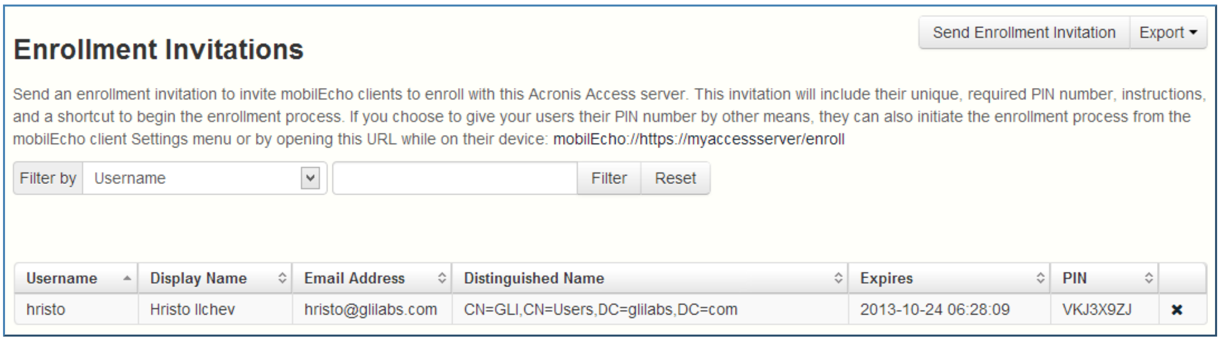
Acronis Cyber Files includes two device enrollment mode options. This mode is used for all client enrollments. You will need to select the option that fits your requirements:

- **PIN number + Active Directory username and password** - In order to activate their Acronis Cyber Files app and gain access to Acronis Cyber Files servers, a user is required to enter an expiring, one-time use PIN number and a valid Active Directory username and password. This option ensures that a user can only enroll one device, and only after receiving a PIN number issued by their IT administrator. This option is recommended when the enhanced security of two-factor device enrollment is required.
- **Active Directory username and password only** - A user can activate their Acronis Cyber Files app using only their Active Directory username and password. This option allows a user to enroll one or more devices at any point in the future. Users just need to be given the name of their Acronis Cyber Files server, or a URL pointing to their Acronis Cyber Files server, which can be posted on a web site or emailed, simplifying the rollout of Acronis Cyber Files to large numbers of users. This option is preferred in environments where two-factor enrollment is not required and many users may need access to Acronis Cyber Files at any time, such as student deployments.

# Inviting a user to enroll

Users are typically invited to enroll with the Acronis Cyber Files Server with an email that is sent from an Acronis Cyber Files Administrator. If required by the server, this email contains a one-time use PIN number that is valid for a configurable number of days. The PIN number can be used to enroll the Mobile app on one device only. If a user has multiple devices, they will need to be sent one invitation email for each device that needs access. This email includes a link to the Mobile app in the App Store, in the case the app first needs to be installed. It also includes a second link that, when tapped while on the device, will open the Acronis Cyber Files mobile and auto-complete the client enrollment form with the Acronis Cyber Files Server's name, the unique enrollment PIN number, and the user's username. By using this link, a user simply enters their account password to complete client enrollment.

- Once an enrollment invitation is generated, the invited users are displayed on the **Enrollment Invitations** page. Each user's PIN number is listed, in the case that you need to communicate it by a means other than the automatic email.
- Once a user successfully enrolls their Acronis Cyber Files mobile using their one-time use PIN number, they will no longer appear in this list.
- To revoke a user's invitation PIN number, press delete to remove them from the list.



Enrollment Invitations

Send an enrollment invitation to invite mobilEcho clients to enroll with this Acronis Access server. This invitation will include their unique, required PIN number, instructions, and a shortcut to begin the enrollment process. If you choose to give your users their PIN number by other means, they can also initiate the enrollment process from the mobilEcho client Settings menu or by opening this URL while on their device: mobilEcho://https://myaccessserver/enroll

| Username | Display Name | Email Address | Distinguished Name | Expires | PIN | |
|---|---|---|---|---|---|---|
| hristo | Hristo Ilchev | hristo@glilabs.com | CN=GLI,CN=Users,DC=glilabs,DC=com | 2013-10-24 06:28:09 | VKJ3X9ZJ | ✖ |

## Using basic URL enrollment links when PIN numbers are not required

If your server is configured to not require PIN numbers for client enrollment, you can give your users a standard URL that will automatically start the enrollment process when tapped from the mobile device.

To determine the enrollment URL for your management server, open the **Mobile Access** tab and open the **Enroll Users** tab. The URL is displayed on this page.

**Note**

For more information on the two modes, visit the Settings section.

### To generate a Acronis Cyber Files enrollment invitation:

1. Open the **Mobile Access** tab and open the **Enroll Users** tab.
2. Click the **Send Enrollment Invitation** button.
3. Enter an Active Directory user name or group name and click Search. If a group is chosen, you can press Add to show each email address in that group in the Users to invite list. This will allow you to batch invite all members in a group. You can optionally remove one or more of those group members before sending the invitations. You can perform 'begins with' or 'contains' searches for Active Directory groups. Begins with search will complete much faster than contains searches.
4. Once you've added your first user or group, you can issue a new search and continue to add additional users or groups to the list.
5. Review the list of Users to invite. You can Delete any users you would like to remove them from the list.
6. If a user does not have an email address associated with their account, you will see **No email address assigned - click here to edit** in the Email Address column. You can click any of these entries to manually enter an alternate email address for that user. If a user is left with **No email address assigned**, a PIN number will still be generated for them, and will be visible on the Enroll Users page. You will need to convey this PIN number to the user by another means before they can enroll their Acronis Cyber Files mobile.

**Note**

If you prefer to manually communicate enrollment PIN numbers to the users, you can uncheck the **Send an enrollment invitation email to each user with a specified address** option. Each PIN number will be visible on the **Enrollment Invitations** page.

7. Choose the number of days you'd like the invitation to be valid for in the Number of days until invitation expires field.
8. Choose the number of PINs you'd like to send to each user on the invitations list. This can be used in cases where a user may 2 or 3 devices. They will receive individual emails containing each unique one-time-use PIN.

**Note**

Acronis Cyber Files licensing allows each licensed user to activate up to 3 devices, each additional device beyond 3 is counted as a new user for licensing purposes.

9. Choose the version or versions of the Acronis Cyber Files mobile that you would like your users to download and install on their device. You may choose iOS, Android, or Both.
10. Click **Send**.

**Note**

If you get an error message when sending, confirm that the SMTP settings in the SMTP tab under General Settings are correct. Also, if you're using **Secure connection**, verify that the certificate you are using matches the host name of your SMTP server.

## User-side Management Enrollment Process

Each user sent a management enrollment invitation will receive an email that contains:

- A link to install the Acronis Cyber Files mobile from the Apple App Store.
- A link used to launch the Mobile app and automate the enrollment process.
- A one-time use PIN number.
- Their management server address.
- The email guides them through the process of installing the Acronis Cyber Files mobile and entering their enrollment information.

If the Mobile app has already been installed, and the user taps the "Tap this link to automatically begin enrollment..." option while viewing this email on their device, Acronis Cyber Files will automatically launch and the enrollment form will be displayed. The user's server address, PIN number, and username are also encoded in this URL, so these fields are auto-completed in the enrollment form. At this point, the user simply enters their password to complete the enrollment process.

The username and password required are the user's Active Directory username and password. These credentials are used to match them to the proper user or group management policy, for access to Gateway servers and if their management policy allows it, the saving of their credentials for Acronis Cyber Files server logins.

If their management policy requires an application lock password, they will be prompted to enter one. All password complexity requirements configured in their policy will be enforced for this initial password, and for any change of their application lock password in the future.

If their policy restricts the local storage of files on their device, they will be warned that existing files will be removed and allowed to cancel the management setup process if there are files they need to deal with before they are removed.

## To enroll in management

### Enroll automatically via enrollment email

1. Open the email sent to you by your IT administrator and tap the **click here to install the Acronis Cyber Files** link if you have not yet installed Acronis Cyber Files.
2. Once Acronis Cyber Files is installed, return to the invitation email on your device and tap **Click this link to automatically begin enrollment** in step 2 of the email.
3. An enrollment form will be displayed. If you used the link in the invitation email to start the enrollment process, your Server Address, PIN, and Username will be automatically filled out.

   **Note**
   If your server does not require a PIN number, it will not be displayed in the enrollment form.

4. Enter your password and tap **Enroll Now** to continue.

   **Note**
   The Username and Password are your standard company username and password. This is likely the same as you use to log into your computer or to your email.

5. After completing the entire form, tap the **Enroll** button.
6. Depending on the configuration of your company's server, you may be warned that your management server's security certificate is not trusted. To accept this warning and proceed, you can click **Proceed Always**.
7. If an application lock password is required for your Acronis Cyber Files mobile app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

A confirmation window may appear if your management policy restricts the storage of files in Acronis Cyber Files or disables your ability to add individual servers from within the Acronis Cyber Files mobile app. If you have files stored locally in the Acronis Cyber Files mobile app, you will be asked to confirm that any files in your **My Files** local file storage will be deleted. If you select No, the management enrollment process will be canceled and your files will remain unchanged.

### Manual enrollment

1. Open the Acronis Cyber Files app.
2. Open **Settings**.
3. Tap **Enroll**.
4. Fill in your server's address, your PIN (if required), username and password.
5. After completing the entire form, tap the **Enroll** button.
6. Depending on the configuration of your company's server, you may be warned that your management server's security certificate is not trusted. To accept this warning and proceed, you can click **Proceed Always**.
7. If an application lock password is required for your Acronis Cyber Files mobile app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

A confirmation window may appear if your management policy restricts the storage of files in Acronis Cyber Files or disables your ability to add individual servers from within the Acronis Cyber Files mobile app. If you have files stored locally in the Acronis Cyber Files mobile app, you will be asked to confirm that any files in your **My Files** local file storage will be deleted. If you select No, the management enrollment process will be canceled and your files will remain unchanged.

## Ongoing Management Updates

After the initial management setup, Acronis Cyber Files mobiles will attempt to contact the management server each time the client app is started. Any settings changes, server or folder assignment changes, application lock password resets, or remote wipes will be accepted by the client app at that time.

**Note**

**Connectivity requirements**

Acronis Cyber Files clients must have network access to the Acronis Cyber Files server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access Acronis Cyber Files, they also need to connect to the VPN before management commands are accepted.

## Removing Management

There are two options to remove your Acronis Cyber Files mobile from management:

- Turn off the Use Management option (if allowed by your policy)
- Remove the Mobile application

Depending on your Acronis Cyber Files management policy settings, you may have the right to remove the Acronis Cyber Files mobile from management. This will likely result in you not being able to access corporate files servers. If you are allowed to do so, follow these steps to unmanage your device:

### To unmanage your device follow the steps below:

1. Tap the **Settings** menu.
2. Turn OFF the **Use Management** option.
3. Your profile may require that your Acronis Cyber Files mobile data is wiped when removing the device from management. You can cancel the process at this point if you don't want to lose your files.
4. Confirm removing Acronis Cyber Files from management by tapping **YES** in the confirmation window.

**Note**
If your Acronis Cyber Files policy does not allow you to unmanage your client, the **Use Management** option will not be displayed on the **Settings** menu. In this case the only way to remove the device from management is by uninstalling the Mobile application. Uninstalling the application will erase all existing Acronis Cyber Files mobile data and settings and will return the user to default application settings after reinstalling.

### To uninstall the Acronis Cyber Files Mobile app, follow the steps below:

**For iOS:**

1. Hold your finger on the Mobile app icon until it starts shaking.
2. Tap the "**X**" button on the Mobile application and confirm the uninstall process.

**For Android:**

**Note**
Android devices software vary and your settings might look slightly different.

1. Open your App menu and select **Edit/Remove**.
2. Find the Acronis Cyber Files app and select it.
3. Press **Remove**.

# Managing Gateway Servers

The Acronis Cyber Files Gateway Server is the server contacted by the Acronis Cyber Files mobile app that handles accessing and manipulating files and folders in file servers, SharePoint respositories, and/or Sync & Share volumes. The Gateway Server is the "gateway" for mobile clients to their files.

The Acronis Cyber Files Server can manage and configure one or more Gateway Servers from the same management console. The Gateway Servers under management appear in the **Gateway Servers** section of the **Mobile Access** menu.

- **Type** - Shows the type of the gateway, at the moment it can only be of the Server type.
- **Name** - Cosmetic name given to the gateway when you create it.

- **Address** - DNS name or IP address of the gateway.
- **Version** - Shows the version of the Acronis Cyber Files Gateway Server.
- **Status** - Shows whether the server is Online or Offline.
- **Active Sessions** - Number of currently active sessions to this Gateway Server.
- **Licenses Used** - Number of licenses used and the number of available licenses.
- **License** - Shows the current type(s) of license(s) used by the Gateway Server.

You can register a new Gateway Server using the **Add new Gateway Server** button.

From the **actions** menu for each Gateway Server, an administrator can:

- get more details on a server and its performance.
- edit its configuration.
- change the access restrictions for the server.
- change licensing for the server.
- remove the server.

**Warning!**
Bookmarks for data sources are irreversibly lost upon removal of the Gateway Server where they reside. Adding back the server and related data sources to the Cyber Files Server Administration console cannot undo this action.

**Note**
The Gateway Server uses the Windows `HTTP.sys` service and will enforce the relevant Windows settings on the machine, including the Microsoft Secure Channel (schannel) ones that manage TLS encryption security.
Customers who wish to modify the Gateway Server service security will need to use a non-Acronis tool, such as IIS Crypto, to manage these Windows settings.

# Gateway Server Search Options

## Requirements

Acronis Cyber Files uses **Windows Search** to allow searching in Network data sources. **Windows Search** is a built-in feature of Windows Server but it is not enabled by default.

To turn it on, do the following:

- Add/install the **File Services** Role in the Server Manager.
- Make sure that the **Windows Search Service** is enabled and started.

**Note**
If the above requirements are not met, it will not be possible to search in Network data sources.

The search is *not* supported also in those cases:

- for NAS file servers, CMIS and SharePoint data locations. However, there is support for SMB/CIFS file servers.
- at the root of file servers (`//server`); it will rather work only in actual shares inside (`//server/share`)
- if the service account on the Gateway machine doesn't have access (windows permissions) to the computer that hosts the remote share. To check this, try running the Gateway service with an admin service account.

The **Search** field appears disabled if:

- it is not possible to search for any reason
- the indexed directory is empty

## Index local data sources for filename search

Searching in Network data sources relies on the Acronis Cyber Files Gateway server and Windows Search index. If Windows Search index is enabled for the desired volume and it has been indexed, both deep and content searches can be performed there.

By default, indexed searching is enabled on all Gateway Servers. You can disable or enable indexed searching for each Gateway Server in the Gateway's **Edit Server** dialog.

1. Open the Acronis Cyber Files Administration console.
2. Navigate to **Mobile Access** > **Gateway server** > **Edit** > **Search**.
3. Select:
   - the **Index local data sources for filename search** check box
   - Optionally, the **Support content search using Microsoft Windows Search where available** check box.

## Default path

By default on a standalone server, Acronis Cyber Files stores index files in the **Search Indexes** directory in the Acronis Cyber Files Gateway Server application folder. If you would like to locate the index files in a different location, enter the path to a new folder.

## Support content search using Microsoft Windows Search where available

Support for content search of shared folders is enabled by default, it can be turned on and off using this option. You can enable or disable content searching for each Gateway Server individually.

**Windows Search** can be configured to index the necessary Data Sources by right-clicking the Windows Search icon in the Start bar and selecting **Windows Search Options**. You can do Windows content searches on Windows reshares but the remote machine(s) must be in the same domain as the Gateway Server.

**Note**
The Data Source's volume path must be a hostname or a fully qualified name in order to use content search on Windows Reshares. IP addresses are not supported by Windows Search.

### Additional Configurations

Content search indexing can be configured to only index the contents of certain file types.

1. On your server hosting the Gateway Server, open **Control Panel** -> **Indexing Options**.
2. Select **Advanced** and open the **File Types** tab.
3. Find the file types you wish to enable/disable content search for (e.g. **doc**, **txt** and etc.).
4. Select the desired file type and under **How should this file be indexed** select either **Index Properties and File Contents** to enable content search for this file type or **Index Properties** to disable it. Repeat this step for all desired file types.

## SharePoint

Entering these credentials is optional for general SharePoint support, but required to enumerate site collections. For example, say you have two site collections: http://sharepoint.example.com and http://sharepoint.example.com/SeparateCollection. Without entering credentials, if you create a volume pointing to http://sharepoint.example.com, you will not see a folder called SeparateCollection when enumerating the volume. The account needs to have Full Read access to the web application.

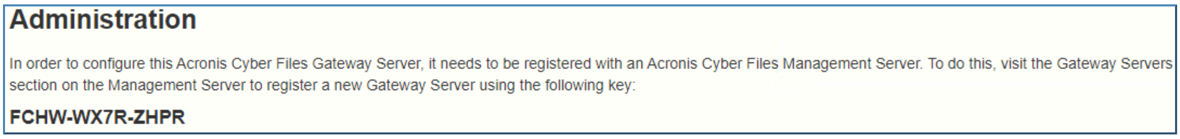
# Registering new Gateway Servers

With the exception of automatic registration of a Gateway Server running on the same machine as the management web application, registration of Gateway Servers is a multi-step, manual process.

1. Go to the computer on which you have the Gateway Server installed.
2. Based on your settings in the **Configuration Utility**:
   a. If you have selected **All available addresses**, open **https://localhost:3000/gateway_admin**.
   b. If you have selected a specific IP address, open **https://<specific_ip_address>:3000/gateway_admin**.

   **Note**
   The port 3000 is the default port. If you have changed the default port, add your port number after localhost or the IP address.

3. Write down the **Administration Key**.

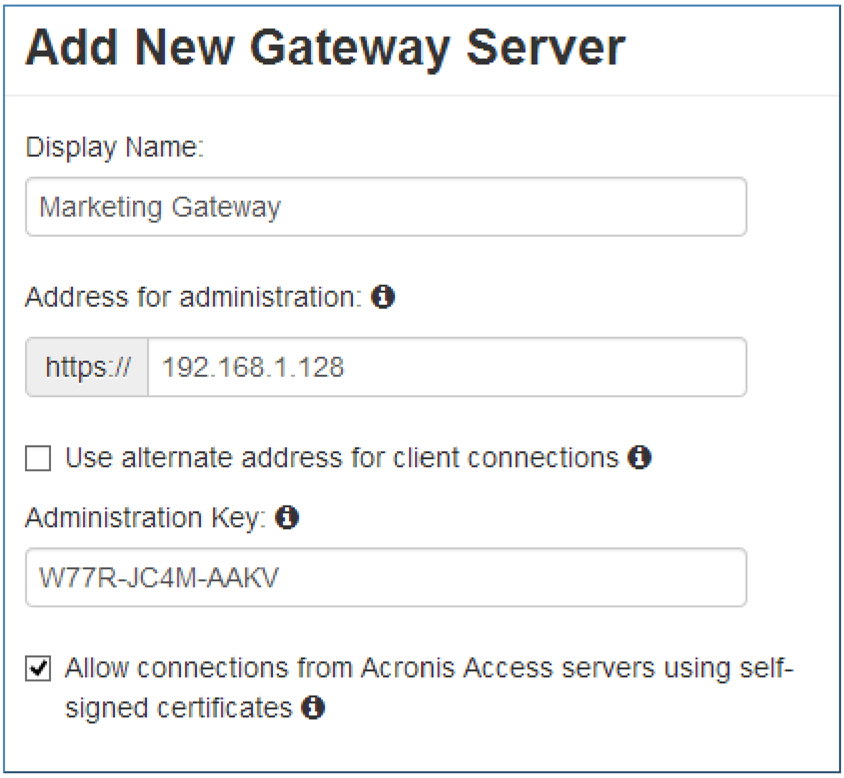


Administration

In order to configure this Acronis Cyber Files Gateway Server, it needs to be registered with an Acronis Cyber Files Management Server. To do this, visit the Gateway Servers section on the Management Server to register a new Gateway Server using the following key:

FCHW-WX7R-ZHPR

4. Open the Acronis Cyber Files Web Interface.
5. Open the **Mobile Access** tab.
6. Open the **Gateway Servers** page.
7. Click the **Add New Gateway Server** button.



Add New Gateway Server

Display Name:

Marketing Gateway

Address for administration: ℹ

https:// 192.168.1.128

☐ Use alternate address for client connections ℹ

Administration Key: ℹ

W77R-JC4M-AAKV

☑ Allow connections from Acronis Access servers using self-signed certificates ℹ

8. Enter a Display Name for your Gateway Server.
9. Enter the DNS name or IP address of your Gateway Server.

**Note**
If your mobile clients connect to the gateway by going through a reverse proxy server or loadbalancer you should enable **Use alternate address for client connections** and enter the DNS name or IP address of your reverse proxy server or loadbalancer.

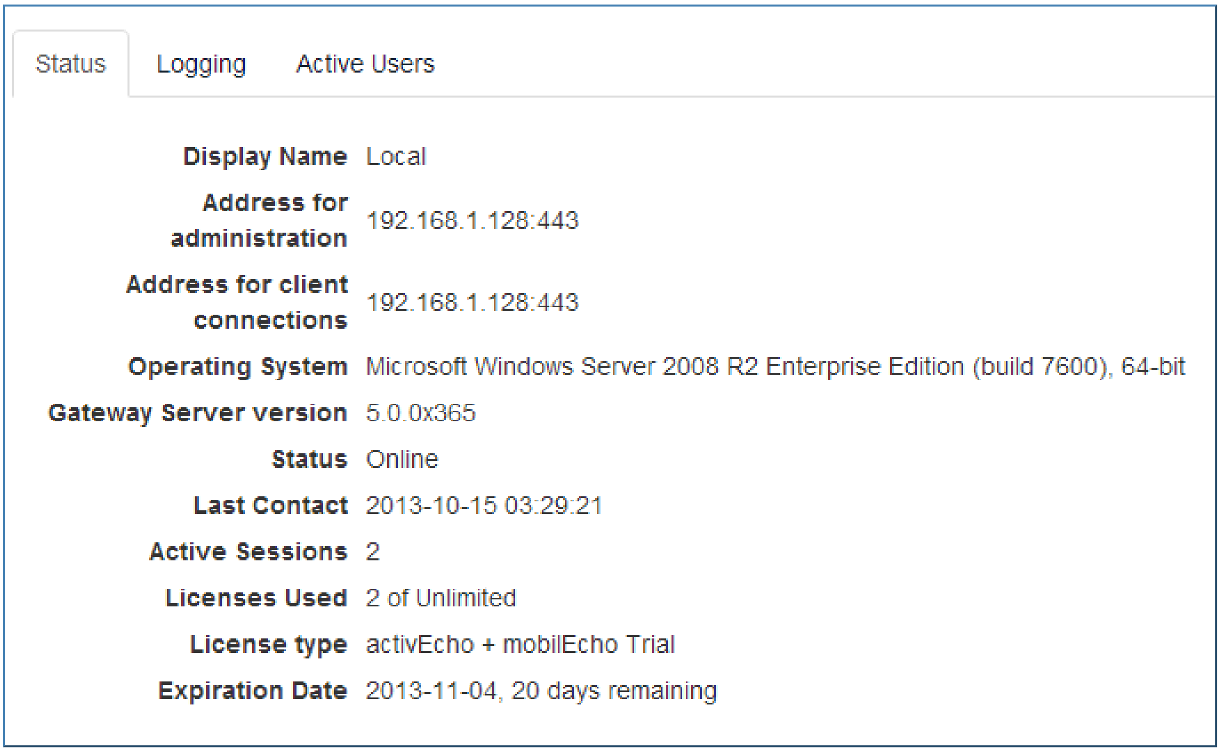
10. Enter the **Administration Key**.
11. If required, allow connections with self-signed certificates to this gateway by enabling **Allow connections from Acronis Cyber Files servers using self-signed certificates**.
12. Click the **Save** button.

After you've registered your Gateway Server, you may want to configure custom access restrictions for this Gateway Server. For more information on this, visit the Editing Gateway Servers section.

## Server Details

Opening the **Details** page of a Gateway Server gives you a lot of useful information about that specific server and its users.

## Status



**Display Name** Local

**Address for administration** 192.168.1.128:443

**Address for client connections** 192.168.1.128:443

**Operating System** Microsoft Windows Server 2008 R2 Enterprise Edition (build 7600), 64-bit

**Gateway Server version** 5.0.0x365

**Status** Online

**Last Contact** 2013-10-15 03:29:21

**Active Sessions** 2

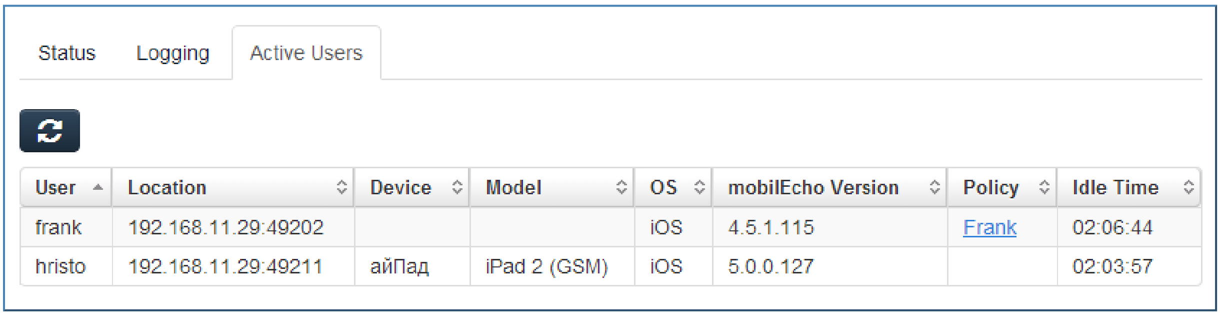
**Licenses Used** 2 of Unlimited

**License type** activEcho + mobilEcho Trial

**Expiration Date** 2013-11-04, 20 days remaining

The Status section gives you information about the Gateway Server itself. Information like the operating system, the type of the license, number of licenses used, version of the Gateway Server and more.

## Active Users



| User | Location | Device | Model | OS | mobilEcho Version | Policy | Idle Time |
|---|---|---|---|---|---|---|---|
| frank | 192.168.11.29:49202 | | | iOS | 4.5.1.115 | Frank | 02:06:44 |
| hristo | 192.168.11.29:49211 | айПад | iPad 2 (GSM) | iOS | 5.0.0.127 | | 02:03:57 |

Displays a table of all users currently active in this Gateway Server.

- **User** - Shows the user's Active Directory (full) name.
- **Location** - Shows the IP address of the device.
- **Device** - Shows the name given to the device by the user.
- **Model** - Shows the type/model of the device.
- **OS** - Shows the operating system of the device.
- **Client Version** - Shows the version of the Acronis Cyber Files app installed on the device.

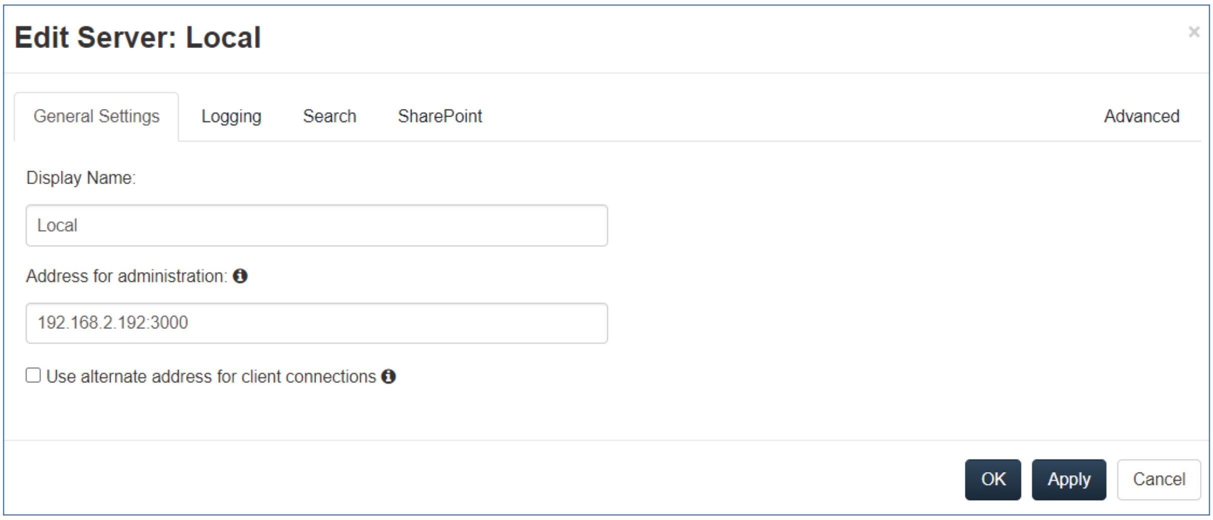
- **Policy** - Shows the policy for the account used by the device.
- **Idle Time** - Shows the time the user has spent connected to the gateway.

## Gateway Server Configurations

To change your Gateway Server's configuration you need to enter the settings menu.

1. Navigate to the **Mobile Access** -> **Gateway Servers** tab.
2. Click on the arrow next to **Details** for the desired server.
3. Select **Edit**.

### General Settings



Edit Server: Local

Display Name: Local

Address for administration: 192.168.2.192:3000

□ Use alternate address for client connections

- **Display Name** - Sets the display name of the Gateway Server. The name is purely cosmetic and is used to differentiate between servers easily.
- **Address for administration** - Sets the default address on which the Gateway Server is reachable by the Acronis Cyber Files Server and mobile clients. We recommend using a DNS address instead of an IP address.

  **Note**
  This is default address on which mobile clients will connect to the Gateway Server unless **Use alternate address for client connections** is enabled.

- **Use alternate address for client connections** - When enabled, overrides the address on which mobile clients will connect to the Gateway Server.

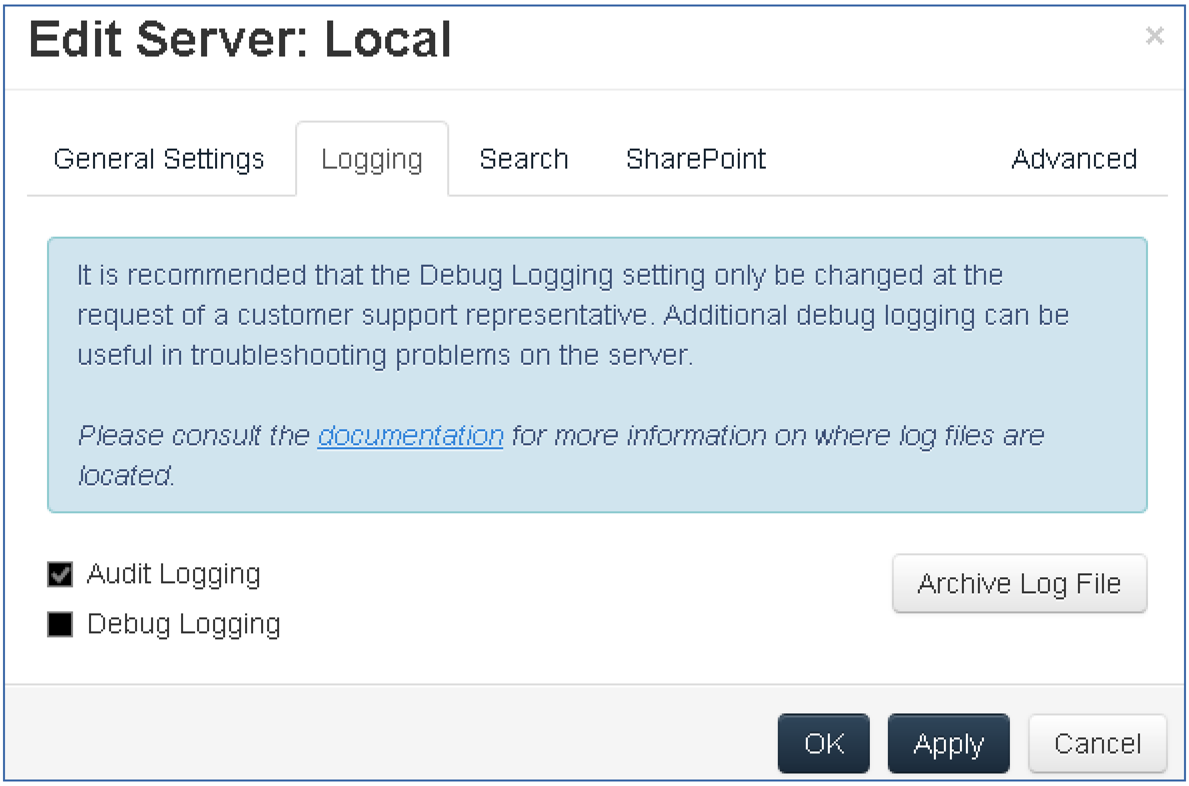
  **Note**
  This setting should be used only in specific configurations where connections to your Gateway Servers pass through a load-balancer or any kind of proxy (e.g. MobileIron or others). Regular deployments should not enable it.

  - **Address for client connections** - When **Use alternate address for client connections is** enabled, this becomes the address that mobile clients will use to connect to the Gateway

Server. We recommend using a DNS address instead of an IP address.

## Gateway Server Logging

The Logging section allows you to control whether the logging events from this specific Gateway Server will be shown in the Audit Log and allows you to enable Debug logging for this server.



Edit Server: Local

It is recommended that the Debug Logging setting only be changed at the request of a customer support representative. Additional debug logging can be useful in troubleshooting problems on the server.

*Please consult the documentation for more information on where log files are located.*

☑ Audit Logging

■ Debug Logging

**To enable Audit Logging for a specific gateway server:**

1. Open the web interface.
2. Log in as an administrator.
3. Open the **Mobile Access** tab.
4. Open the **Gateway Servers** tab.
5. Find the server for which you want to enable **Audit Logging.**
6. Press the **Details** button.
7. In the **Logging** section check **Audit Logging**.
8. Click the **Save** button.

**To enable Debug Logging for a specific gateway server:**

**Note**

The default location for the debug logs is: `C:\Program Files (x86)\Acronis\Access\Gateway Server\Logs\AcronisAccessGateway`

1. Open the web interface.
2. Log in as an administrator.

3. Open the **Mobile Access** tab.
4. Open the **Gateway Servers** tab.
5. Find the server for which you want to enable **Debug Logging.**
6. Press the **Details** button.
7. In the **Logging** section check **Debug Logging**.
8. Click the **Save** button.

## Gateway Server Search Options

### Requirements

Acronis Cyber Files uses **Windows Search** to allow searching in Network data sources. **Windows Search** is a built-in feature of Windows Server but it is not enabled by default.

To turn it on, do the following:

- Add/install the **File Services** Role in the Server Manager.
- Make sure that the **Windows Search Service** is enabled and started.

**Note**
If the above requirements are not met, it will not be possible to search in Network data sources.

The search is *not* supported also in those cases:

- for NAS file servers, CMIS and SharePoint data locations. However, there is support for SMB/CIFS file servers.
- at the root of file servers (`//server`); it will rather work only in actual shares inside (`//server/share`)
- if the service account on the Gateway machine doesn't have access (windows permissions) to the computer that hosts the remote share. To check this, try running the Gateway service with an admin service account.

The **Search** field appears disabled if:

- it is not possible to search for any reason
- the indexed directory is empty

### Index local data sources for filename search

Searching in Network data sources relies on the Acronis Cyber Files Gateway server and Windows Search index. If Windows Search index is enabled for the desired volume and it has been indexed, both deep and content searches can be performed there.

By default, indexed searching is enabled on all Gateway Servers. You can disable or enable indexed searching for each Gateway Server in the Gateway’s **Edit Server** dialog.

1. Open the Acronis Cyber Files Administration console.
2. Navigate to **Mobile Access** > **Gateway server** > **Edit** > **Search**.

3. Select:
   - the **Index local data sources for filename search** check box
   - Optionally, the **Support content search using Microsoft Windows Search where available** check box.

### Default path

By default on a standalone server, Acronis Cyber Files stores index files in the **Search Indexes** directory in the Acronis Cyber Files Gateway Server application folder. If you would like to locate the index files in a different location, enter the path to a new folder.

### Support content search using Microsoft Windows Search where available

Support for content search of shared folders is enabled by default, it can be turned on and off using this option. You can enable or disable content searching for each Gateway Server individually.

**Windows Search** can be configured to index the necessary Data Sources by right-clicking the Windows Search icon in the Start bar and selecting **Windows Search Options**. You can do Windows content searches on Windows reshares but the remote machine(s) must be in the same domain as the Gateway Server.

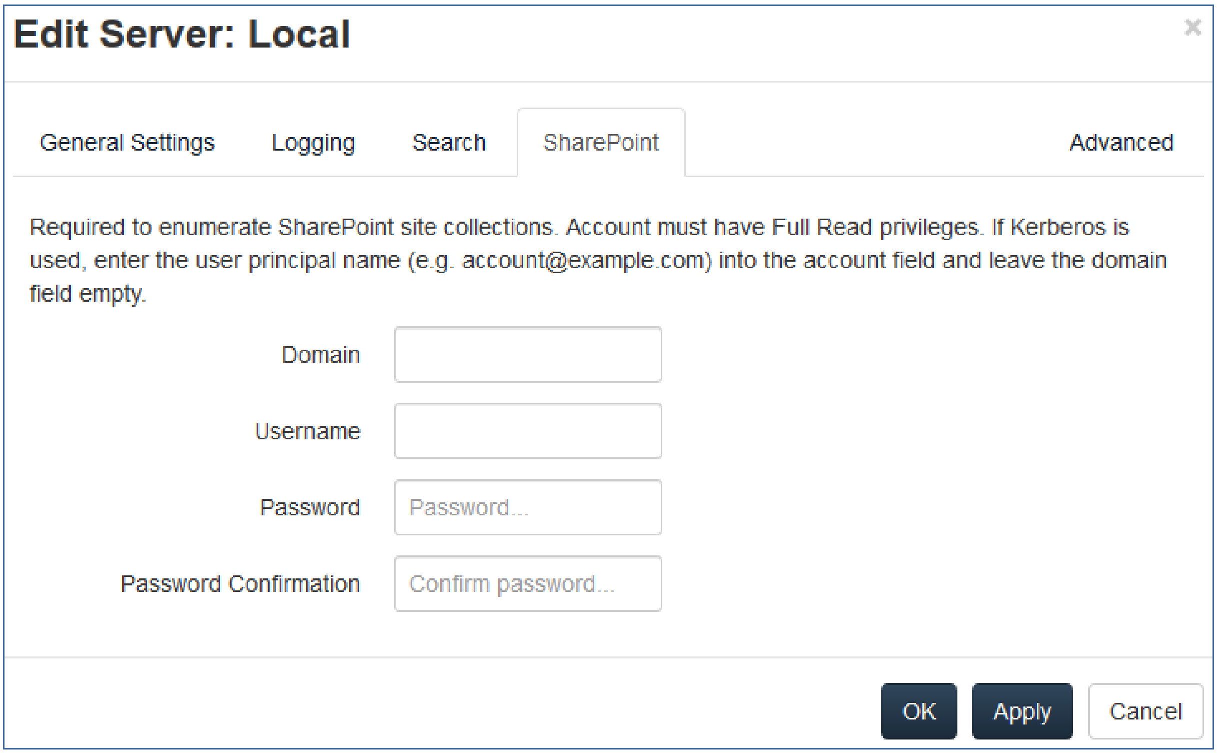
**Note**
The Data Source's volume path must be a hostname or a fully qualified name in order to use content search on Windows Reshares. IP addresses are not supported by Windows Search.

## Additional Configurations

Content search indexing can be configured to only index the contents of certain file types.

1. On your server hosting the Gateway Server, open **Control Panel** -> **Indexing Options**.
2. Select **Advanced** and open the **File Types** tab.
3. Find the file types you wish to enable/disable content search for (e.g. **doc**, **txt** and etc.).
4. Select the desired file type and under **How should this file be indexed** select either **Index Properties and File Contents** to enable content search for this file type or **Index Properties** to disable it. Repeat this step for all desired file types.

## SharePoint Settings



Edit Server: Local

Required to enumerate SharePoint site collections. Account must have Full Read privileges. If Kerberos is used, enter the user principal name (e.g. account@example.com) into the account field and leave the domain field empty.

Domain

Username

Password: Password...

Password Confirmation: Confirm password...

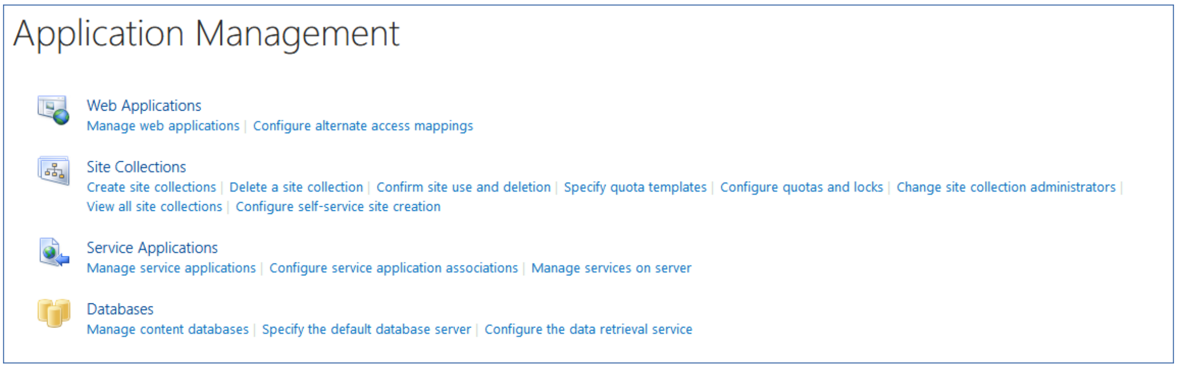
Entering these credentials is optional for general SharePoint support, but required to enumerate site collections. For example, say you have two site collections:

- `http://sharepoint.example.com` and `http://sharepoint.example.com/SeparateCollection`.

Without entering credentials, if you create a volume pointing to **http://sharepoint.example.com**, you will not see a folder called **SeparateCollection** when enumerating the volume. The account needs to have **Full Read** access to the web application.

### To give your account Full Read permission, follow these steps (for SharePoint 2016 and SharePoint 2010):

1. Open the **SharePoint Central Administration**.
2. Click on **Application Management**.



Application Management

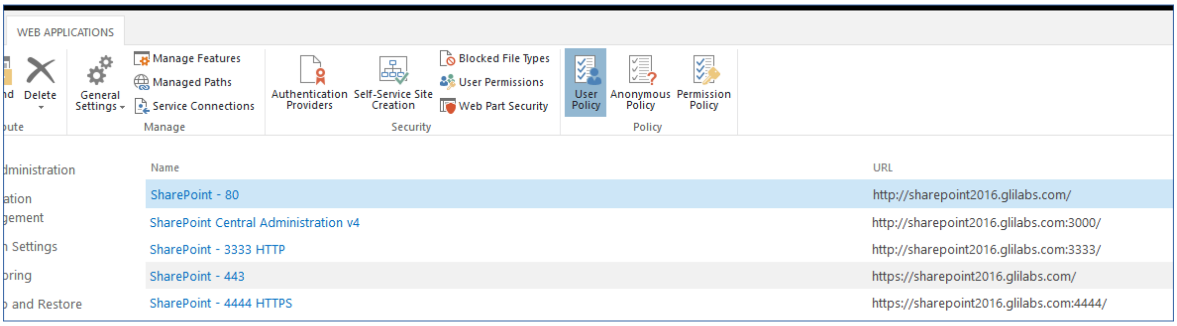
Web Applications
Manage web applications | Configure alternate access mappings

Site Collections
Create site collections | Delete a site collection | Confirm site use and deletion | Specify quota templates | Configure quotas and locks | Change site collection administrators | View all site collections | Configure self-service site creation

Service Applications
Manage service applications | Configure service application associations | Manage services on server

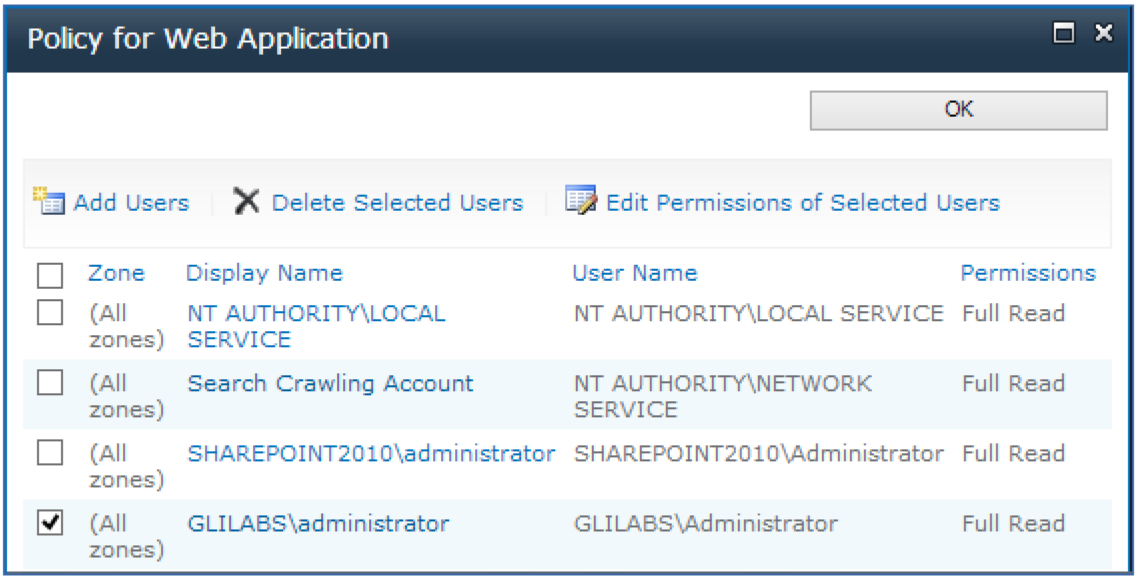
Databases
Manage content databases | Specify the default database server | Configure the data retrieval service

3. Under **Web Applications** click on **Manage web applications**.
4. Select your web application from the list and click on **User Policy**.



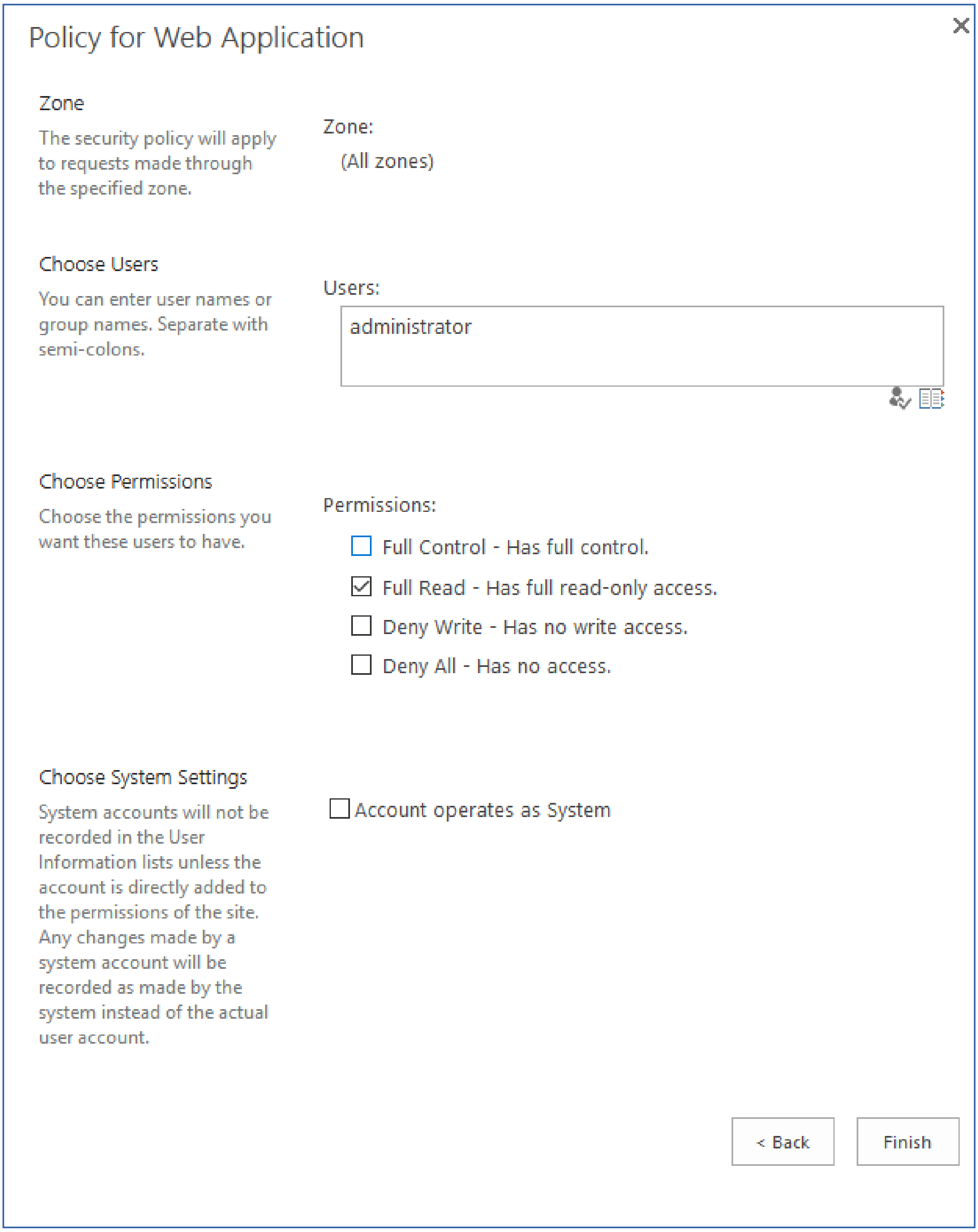
| Name | URL |
|---|---|
| SharePoint - 80 | http://sharepoint2016.glilabs.com/ |
| SharePoint Central Administration v4 | http://sharepoint2016.glilabs.com:3000/ |
| SharePoint - 3333 HTTP | http://sharepoint2016.glilabs.com:3333/ |
| SharePoint - 443 | https://sharepoint2016.glilabs.com/ |
| SharePoint - 4444 HTTPS | https://sharepoint2016.glilabs.com:4444/ |

5. Select the checkbox of the user you want to give permissions to and click on **Edit Permissions of Selected Users**. If the user is not in the list, you can add him by clicking on **Add Users**.


Policy for Web Application
OK
Add Users
Delete Selected Users
Edit Permissions of Selected Users

| □ | Zone | Display Name | User Name | Permissions |
|---|---|---|---|---|
| □ | (All zones) | NT AUTHORITY\LOCAL SERVICE | NT AUTHORITY\LOCAL SERVICE | Full Read |
| □ | (All zones) | Search Crawling Account | NT AUTHORITY\NETWORK SERVICE | Full Read |
| □ | (All zones) | SHAREPOINT2010\administrator | SHAREPOINT2010\Administrator | Full Read |
| ☑ | (All zones) | GLILABS\administrator | GLILABS\Administrator | Full Read |

6. From the **Permission Policy** Levels section, select the checkbox for **Full Read - Has Full read-only access**.



Policy for Web Application

Zone

The security policy will apply to requests made through the specified zone.

Zone:

(All zones)

Choose Users

You can enter user names or group names. Separate with semi-colons.

Users:

administrator

Choose Permissions

Choose the permissions you want these users to have.

Permissions:

□ Full Control - Has full control.

☑ Full Read - Has full read-only access.

□ Deny Write - Has no write access.

□ Deny All - Has no access.

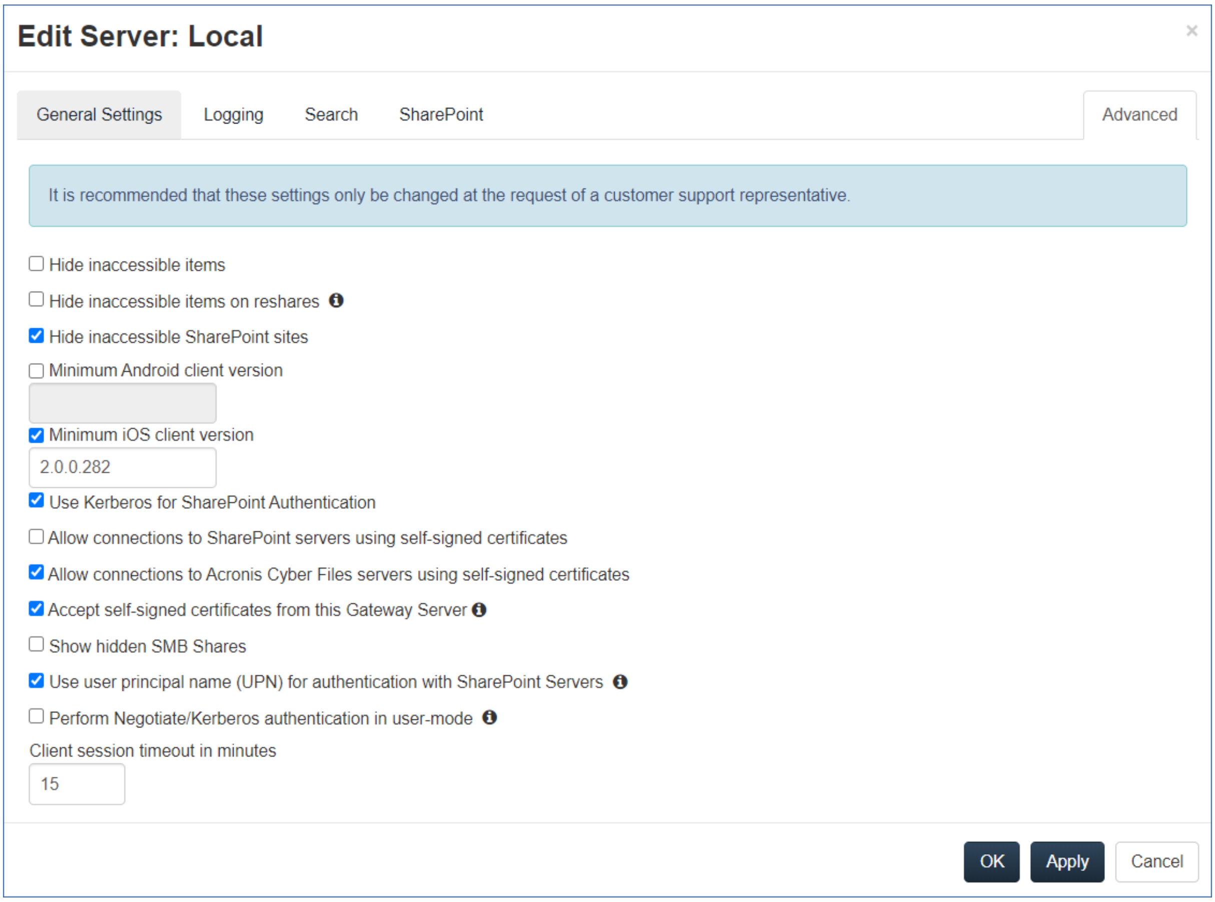
Choose System Settings

System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes made by a system account will be recorded as made by the system instead of the actual user account.

□ Account operates as System

7. Click the **Save** button.

## Advanced Settings



Edit Server: Local

It is recommended that these settings only be changed at the request of a customer support representative.

- □ Hide inaccessible items
- □ Hide inaccessible items on reshares
- ☑ Hide inaccessible SharePoint sites
- □ Minimum Android client version
- ☑ Minimum iOS client version: 2.0.0.282
- ☑ Use Kerberos for SharePoint Authentication
- □ Allow connections to SharePoint servers using self-signed certificates
- ☑ Allow connections to Acronis Cyber Files servers using self-signed certificates
- ☑ Accept self-signed certificates from this Gateway Server
- □ Show hidden SMB Shares
- ☑ Use user principal name (UPN) for authentication with SharePoint Servers
- □ Perform Negotiate/Kerberos authentication in user-mode

Client session timeout in minutes: 15

**Note**
It is recommended that these settings only be changed at the request of a customer support representative**.**

- **Hide inaccessible items** - When enabled,files and folders for which the user does not have the Read permission will not be shown.
- **Hide inaccessible items on reshares** - When enabled,files and folders located on a network reshare for which the user does not have the Read permission will not be shown.

  **Note**
  Enabling this feature can have a significant negative impact while browsing folders.

- **Hide inaccessible SharePoint sites** - When enabled,SharePoint sites for which the user does not have the necessary permissions will not be shown.
- **Minimum Android client version** - When enabled,users connecting to this Gateway will be required to have this or a later version of the Acronis Cyber Files Android client app.
- **Minimum iOS client version** - When enabled,users connecting to this Gateway will be required to have this or a later version of the Acronis Cyber Files iOS client app.

- **Use Kerberos for SharePoint Authentication** - If your SharePoint server requires Kerberos authentication, you should enable this setting. You will also need to make an update to the Active Directory computer object for the Windows server or servers that are running the Gateway server software. The Acronis Cyber Files Windows server needs to be given permission to present delegated credentials to your SharePoint server on behalf of you users. Enabling the Acronis Cyber Files Windows server to perform Kerberos Delegation:
  1. In **Active Directory Users and Computers**, locate the Windows server or servers that you have the Gateway Server installed on. They are commonly in the **Computers** folder.
  2. Open the **Properties** window for the Windows server and select the **Delegation** tab.
  3. Select **Trust this computer for delegation to specified services only**
  4. Select **Use any authentication protocol**, this is required for negotiation with the SharePoint server.
  5. You must now add any SharePoint servers that you would like your users to be able to access using Acronis Cyber Files . If your SharePoint implementation consists of multiple load balanced nodes, you will need to add each SharePoint/Windows node to this list of permitted computers. Click **Add...** to search for these Windows computers in AD and add them. For each, you will need to select the "http" service type only.

  **Note**
  Please allow 15 to 20 minutes for these change to propagate through AD and be applied before testing client connectivity. They will not take effect immediately.

- **Allow connections to SharePoint servers using self-signed certificates** - When enabled, allows connections from this Gateway to SharePoint servers using self-signed certificates.
- **Accept self-signed certificates from this Gateway Server** - When enabled, allows connections from this Acronis Cyber Files Server to this Gateway Server even if this Gateway Server is using a self-signed certificate.
- **Allow connections to Acronis Cyber Files servers with self-signed certificates** - When enabled, allows connections from this Gateway Server to Acronis Cyber Files servers even if the Acronis Cyber Files servers are using self-signed certificates.
- **Show hidden SMB Shares** - When enabled, shows hidden system SMB shares to the users.
- **Client session timeout in minutes** - Sets the time before an inactive user is kicked out of the Gateway Server.
- **Use user principal name (UPN) for authentication with SharePoint Servers** - When enabled, users will authenticate to SharePoint servers via their user principal name (e.g. hristo@glilabs.com), otherwise they will authenticate with domain/username (e.g. glilabs/hristo).
- **Perform Negotiate/Kerberos authentication in user-mode** - When enabled, the Gateway Server will authenticate to Data Sources using the connecting user's Kerberos ticket. This is only used for configurations requiring Kerberos (e.g. Single Sign-On, loadbalancing and etc.).

## Custom Access Restrictions

You can use the default access restrictions set in the Policies section or you can set custom access restrictions for each Gateway Server.

### Setting custom access restrictions for a specific Gateway Server

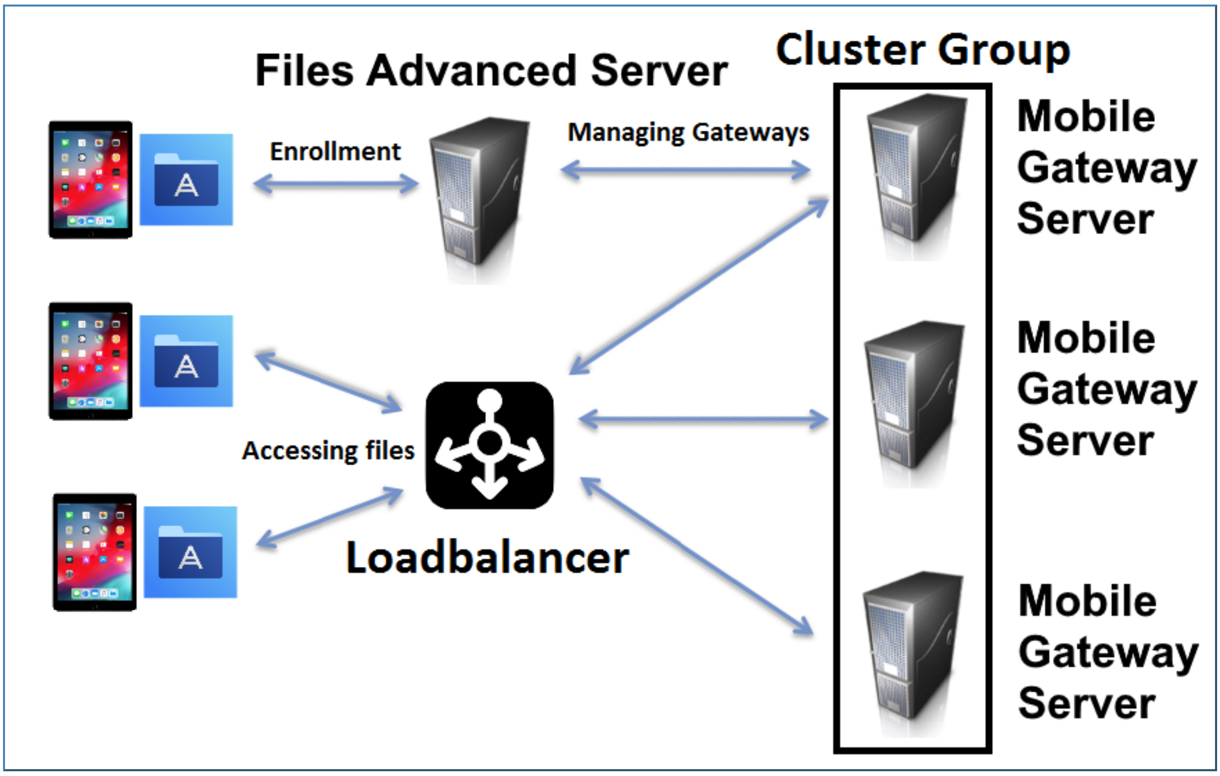
1. Navigate to the **Mobile Access** -> **Gateway Servers** tab.
2. Click on the arrow next to **Details** for the desired server.
3. Select **Access Restrictions**.
4. Open the **Use Custom settings** tab.
5. Select the specific access restrictions you want for this Gateway Server.
6. Press **Apply**.

## Cluster Groups

In Acronis Cyber Files, you have the ability to create a cluster group of Gateway Servers.

A cluster group is a collection of Gateway Servers that share the same configuration. This allows you to control all of the Gateways in that group at once instead of having to configure the same settings on every Gateway individually. Typically these servers are placed behind a load balancer to provide high availability and scalability for mobile clients.

For a clustered gateway setup, you need a load balancer, two or more gateways and an Acronis Cyber Files Server. All of your Gateway Servers should be added to a Cluster Group in the Acronis Cyber Files web interface and placed behind the load balancer. Your Acronis Cyber Files Server acts as both your management server and the server with which mobile clients enroll in client management. Its role is to manage all policies, devices and settings while the gateways' role is to provide access to the file shares.



## To create a cluster group:

Please make sure that you have already configured a correct **Address for Administration** on each Gateway before proceeding. This is the DNS or IP address of the Gateway server.

1. Open the Acronis Cyber Files Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Gateway Servers** page.
4. Click the **Add Cluster Group** button.
5. Enter a display name for the group.
6. Enter the DNS name or IP address of the load balancer.
7. If necessary, select an alternative address for Acronis Cyber Files Server connections by enabling the checkbox and entering the address.
8. Mark the checkbox for each Gateway you want to be in the group.
9. Select the Gateway which will control the group's settings. All of the existing settings on that Gateway (including assigned Data Sources and excluding the address for administration) will be copied to every Gateway in the group.
10. Click **Create**.

## Editing a cluster group:

Editing cluster groups does not differ from editing regular Gateways. For more information visit the Editing Gateway Servers article.

### Adding members to an existing cluster group:

1. Open the web interface and navigate to **Mobile Access** -> **Gateway Servers**.
2. Open the action menu for the desired cluster group and select **Add Cluster Members** from the available actions.
3. Select the desired Gateway Servers from the list and press **Add**.

### Changing the Master Gateway Server:

1. Open the web interface and navigate to **Mobile Access** -> **Gateway Servers**.
2. Expand the desired cluster group.
3. Find the Gateway Server that you want to promote to be the Master.
4. Click the **Actions** button and select **Become Group Master**.

# Managing Data Sources

You can share NTFS directories located on your Windows server, on CMIS systems or on a remote SMB/CIFS file share for access by your Acronis Cyber Files users. When users connect, they will see these directories as file share volumes.

## Access to SharePoint 2007, 2010, 2013, and 2016 content

Acronis Cyber Files can provide access to files residing in document libraries on SharePoint 2007, 2010, 2013, and 2016 servers. An Acronis Cyber Files SharePoint data source can point to an entire SharePoint server, a specific SharePoint site or subsite, or a specific document library. These files can be opened, PDF annotated, edited, and synced, just like files that reside in traditional file server or NAS storage. Acronis Cyber Files also supports **Check Out** and **Check In** of SharePoint files.

### SharePoint authentication methods supported

Acronis Cyber Files supports SharePoint servers that allow client authentication using NTLMv1, NTLMv2, Claims based and Kerberos. If your SharePoint server requires Kerberos authentication, you will need to make an update to the Active Directory computer object for the Windows server or servers that are running the Acronis Cyber Files server software. The Acronis Cyber Files Windows server needs to be given permission to present delegated credentials to your SharePoint server on behalf of you users.

## Access to OneDrive for Business content

Acronis Cyber Files can be setup to allow users access their personal OneDrive for Business content via a SharePoint data source. There are some requirements and limitations.

## Changing Permissions for Shared Files and Folders

Acronis Cyber Files uses the existing Windows user accounts and passwords. Because Acronis Cyber Files enforces Windows NTFS permissions, you should normally use Windows' built-in tools for adjusting directory and file permissions. The standard Windows tools provide the most flexibility for setting up your security policy.

Acronis Cyber Files Data Sources that reside on another SMB/CIFS file server are accessed using an SMB/CIFS connection from the Gateway Server to the secondary server or NAS. In this case, access to the secondary server is performed in the context of the user logged into one of the Acronis Cyber Files clients. In order for that user to have access to files on the secondary server, their account will need both "Windows Share Permissions" and NTFS security permissions to access those files.

Permissions to files residing on SharePoint servers are regulated in accordance to the SharePoint permissions configured on the SharePoint server. Users receive the same permissions through Acronis Cyber Files as they receive when they access SharePoint document libraries using a web browser.

### Folders

Folders can be assigned to Acronis Cyber Files user and group policies, allowing them to automatically appear in a user's Acronis Cyber Files app. Folders can be configured to point to any folder residing on a Gateway Server, a remote share, a CMIS volume or even a SharePoint Library. This allows you to give a user direct access to any folders that might be important to them without users having to navigate to the folder or even knowing the exact server, shared volume name, and path to the folder.

Folders can point to any type of content that Acronis Cyber Files provides access to as long as it is not on a removable media. They simply refer to locations in Gateway Servers that have already been configured within the Acronis Cyber Files management. This can be a local file share volume, a "network reshare" volume providing access to files on another file server or NAS, a DFS share, a CMIS volume or a SharePoint volume.

**Note**
When creating a DFS Data Source you need to add the full path to the DFS in the following way:
**\\company.com\namespace\share**

**Note**
On a clean installation of Acronis Cyber Files, if you have enabled Sync & Share and you have a Gateway Server present, you will have a Sync & Share Data Source created automatically. It points to the URL you set in the **Server** section of the initial configuration. This folder allows your mobile users to access your Sync & Share files and folders.

## Syncing Folders

Folders can optionally be configured to sync to the client device. The Acronis Cyber Files folder sync options include:

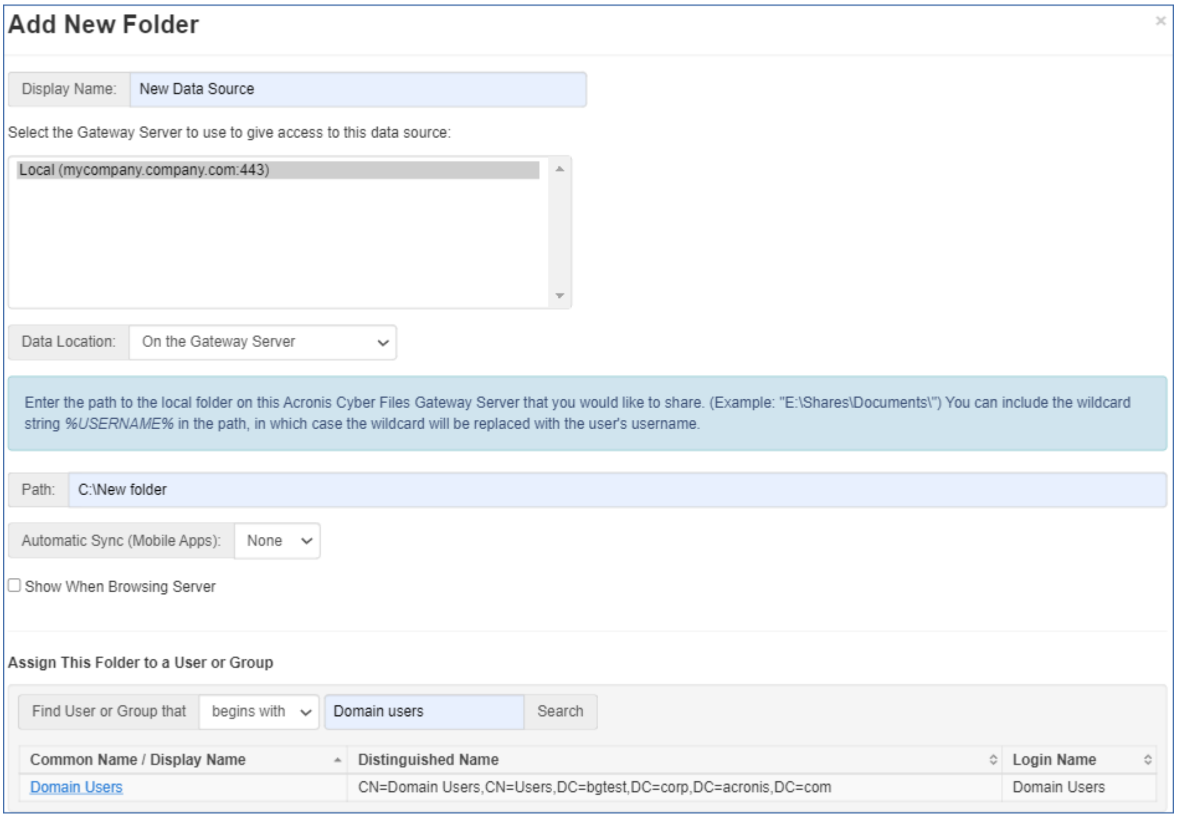
**Note**
This setting does not affect the desktop client.

- **None -** The folder will appear as a network-based resource in the Acronis Cyber Files app and can be accessed and worked with just like a Gateway server.
- **1-Way** - The folder will appear as a local folder in the Acronis Cyber Files app. Its complete contents will be synced from the server to the device and it will be kept up to date if files on the server are added, modified, or deleted. This folder is intended to give local/offline access to a set of server-based files and appears as read-only to the user.
- **2-Way** - The folder will appear as a local folder in the Acronis Cyber Files app. Its complete contents will initially be synced from the server to the device. If files in this folder are added, modified, or deleted, either on the device or on the server, these changes will be synced back to the server or device.

## Creating and editing a Data Source

### Creating a Data Source

1. Open the Acronis Cyber Files Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Data Sources** tab.
4. Go to **Folders**.
5. Click **Add New Folder**.



Add New Folder

Display Name: New Data Source

Select the Gateway Server to use to give access to this data source:

Local (mycompany.company.com:443)

Data Location: On the Gateway Server

Enter the path to the local folder on this Acronis Cyber Files Gateway Server that you would like to share. (Example: "E:\Shares\Documents\") You can include the wildcard string *%USERNAME%* in the path, in which case the wildcard will be replaced with the user's username.

Path: C:\New folder

Automatic Sync (Mobile Apps): None

□ Show When Browsing Server

Assign This Folder to a User or Group

Find User or Group that begins with Domain users Search

| Common Name / Display Name | Distinguished Name | Login Name |
|---|---|---|
| Domain Users | CN=Domain Users,CN=Users,DC=bgtest,DC=corp,DC=acronis,DC=com | Domain Users |

6. Enter a display name for the folder.
7. Select the Gateway Server that will give access to this folder.
8. Select the location of the data. This can be on the actual Gateway Server, on another SMB server, on a SharePoint Site or Library or on a Sync & Share server.

**Note**

You are not allowed to use a folder from a removable media as a shared folder. Please choose one from a different location.

**Note**

When selecting Sync & Share, make sure to enter the full path to the server with the port number. e.g.: https://mycompany.com:3000

9. Based on your choice of location, enter the path to that folder, server, site or library.
10. Select the **Sync** type of this folder.
11. Enable **Show When Browsing Server** if you want this Data Source to be visible when Acronis Cyber Files mobile clients browse the Gateway Server.

**Note**

When creating SharePoint Data Sources, you will have the option to enable the displaying of SharePoint followed sites.

12. Click the **Save** button.

### Editing a Data Source

1. Open the **Data Sources** section and find the Data Source you want to edit.
2. Click on the **Pencil** icon for your Data Source at the right side of the table.
3. Change all desired parameters and press **Save**.

## SharePoint Sites and Libraries

You can give easy access to SharePoint sites and libraries to your Acronis Cyber Files mobile users by creating a Data Source. There are a couple of ways to create SharePoint Data Sources depending on your SharePoint configuration.

**Note**
Every time you provide URL, make sure its root is the default site collection.

## Creating a data source for a whole SharePoint site or subsite

When creating a data source for a **SharePoint site** or **subsite**, you only need to fill in the **URL** field. This should be address of your SharePoint site or subsite.

```
e.g. https://sharepoint.mycompany.com:43222
e.g. https://sharepoint.mycompany.com:43222/subsite name
```

## SharePoint Followed Sites

SharePoint Followed Sites can be enabled when creating the Data Source for your site. This is done with the Display Followed Sites checkbox. When enabled, all users that are following sites will see a folder "Followed Sites" in Acronis Cyber Files that will contain the resources they have permissions to access from those sites.

**Note**
SharePoint Followed Sites cannot be synced.

## Creating a Data Source for a SharePoint Library

When creating a Data Source for a SharePoint Library, you need to fill both the **URL** and **Document Library Name** fields. In the URL field, enter the address of your SharePoint site or subsite, and for the Document Library Name field, enter the name of your Library.

```
e.g. URL: https://sharepoint.mycompany.com:43222
e.g. Document Library Name: My Library
```

## Creating a Data Source for a specific folder within a SharePoint Library

When creating a data source for a specific folder within a SharePoint Library, you will have to fill in all fields. In the URL field you enter the address of your SharePoint site or subsite, for the Document

Library Name field you enter the name of your Library and for the Subpath field you enter the name of the desired folder.

```
e.g. URL: https://sharepoint.mycompany.com:43222
e.g. Document Library Name: Marketing Library
e.g. Subpath: Sales Report
```

**Note**
When creating a Data Source pointing to a SharePoint resource using a Subpath, you cannot enable the **Show When Browsing Server** option.

The Acronis Cyber Files mobile supports NTLM, Kerberos Constrained Delegation, Claims based and SharePoint 365 authentication. Depending on your SharePoint setup, you may need to make some additional configurations to the Gateway Server used to connect to these Data Sources. For more information visit the Editing Gateway Servers article.

## CMIS (Content Management Interoperability Services) volumes

The supported CMIS volumes are **Alfresco (CMIS)** and **Documentum (CMIS)** volumes. You can also try using other CMIS vendors that use the **AtomPub** protocol with the **Generic CMIS (AtomPub)** option. This option may or may not work with your vendor and is not supported by Acronis.

We recommend having a Gateway server on the machine hosting the CMIS volumes to decrease timeouts on slow networks.

**Note**
CMIS volumes have a limitation that does not allow copying folders.

## OneDrive for Business

Since OneDrive for Business is SharePoint based, its content can be reached by creating a SharePoint Data Source in Acronis Cyber Files. As such however, there are some limitations.

- The Data Source **must** point to the wildcard for a user's main personal folder. You cannot create Data Sources pointing to sub-folders, but they are accessible and browsable from the main folder.
- These Data Sources will not work if the Gateway server is added manually in the app - they must be assigned through a policy.
- Your Active Directory must either use Federated AD Services, or be an Azure AD.
- Each user will only be able to see their own OneDrive data and will not have access to other users' data, regardless if it is shared and accessible through the Microsoft portal.

### Creating the Data Source

1. Open the Acronis Cyber Files Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Data Sources** tab.

4. Go to **Folders**.
5. Press the **Add New Folder** button.
6. Enter a display name for the folder.
7. Select the Gateway Server which will give access to the resources.
8. In the **Data Location** field, select the **SharePoint** option. The following fields will appear:
    a. **URL** - enter the SharePoint location of the OneDrive for Business server, site or subsite you would like to give access to, for example:
    `https://sharepoint.company.com/mysite/mysubsite/%USERNAME%`
    This URL cannot point to references beyond subsite level (do not include `default.aspx`). The `%USERNAME%` wildcard string should be part of the path, to be replaced by the user's main personal folder.
    b. Leave empty the **Document Library Name** and **Subpath** fields.
9. Press the **Save** button.

## Assigned Sources

On this page, you can search for a User or Group to find which resources are assigned to them. The resources are listed in 2 tables - Servers and Folders.

- The Servers table lists the Gateway Server's display name, DNS name or IP address and the policies to which this server is assigned.
- The Folders table lists the Data Source's display name, Gateway Server, sync type, path and the policies to which this Data Source is assigned.
- By pressing the **Edit resources assigned to** button, the administrator can quickly edit the assignments for this policy.

## Gateway Servers Visible on Clients

Gateway Servers can be assigned to User or Group policies and can be used as Data Sources. This page displays all Gateway Servers visible from within the user's Acronis Cyber Files mobile app as well as whether those Gateway Servers are assigned to a particular User or Group policy. You can also edit these assignments here. When the Acronis Cyber Files mobile users browse into a Gateway Server, they will see the Data Sources with **Show When Browsing Gateway Server** option enabled.

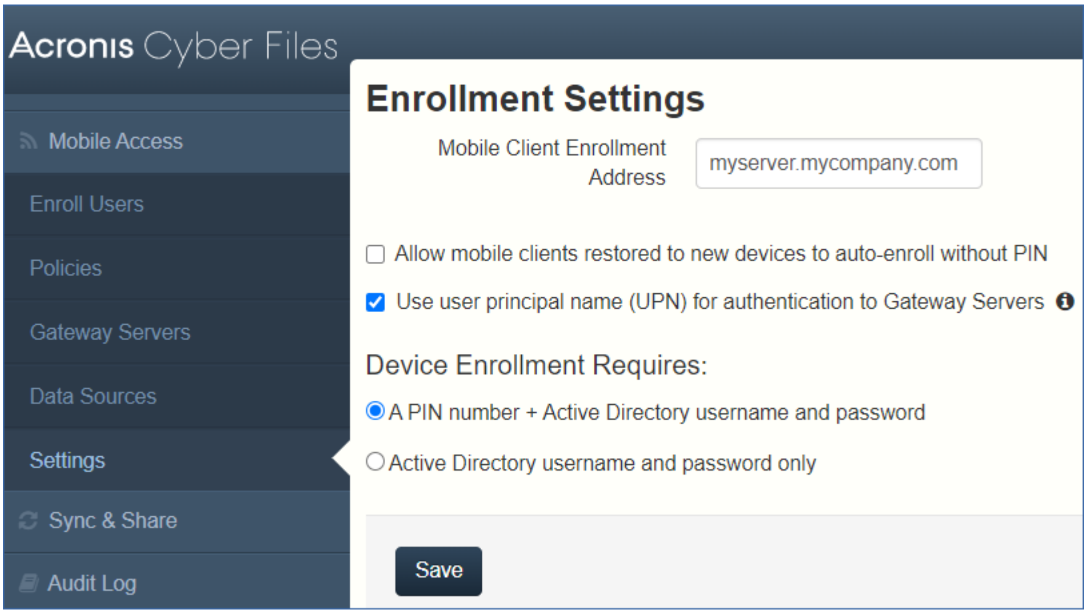
### To edit the current assignment of a server:

1. Click the **Edit** button on that server.
    - To unassign this server from a user, click **X** for that user.
    - To assign a new User or Group to this server, find and click the User/Group name.
2. Click the **Save** button.

**Note**

If you remove a Gateway Server from the Cyber Files Server Administration console, all users' mobile bookmarks for data sources on this server will be permanently deleted. Their recovery is impossible even if the same server and data sources are added back.

# Settings



Enrollment Settings

Mobile Client Enrollment Address: myserver.mycompany.com

□ Allow mobile clients restored to new devices to auto-enroll without PIN

☑ Use user principal name (UPN) for authentication to Gateway Servers

Device Enrollment Requires:

● A PIN number + Active Directory username and password

○ Active Directory username and password only

## Enrollment Settings

- **Mobile Client Enrollment Address** - specifies the address which mobile clients should use when enrolling in client management.

  **Note**

  It is highly recommended to use a DNS name for the mobile client enrollment address. After successfully enrolling in Client Management, the Acronis Cyber Files mobile app stores the address of the Acronis Cyber Files server. If that address is an IP address and it changes, the users cannot reach the server, the app cannot be unmanaged and the users will have to delete the whole app and enroll in management again.

- **Allow mobile clients restored to new devices to auto-enroll without PIN** – when enabled, allows users managed by older versions of Acronis Cyber Files mobile to enroll to your new server without needing a PIN.
- **Use user principal name (UPN) for authentication to Gateway Servers** - when enabled, users will authenticate to Gateway Servers with their UPN (e.g. user@company.com). When disabled, users will authenticate with their domain name and username (e.g. domain/user).

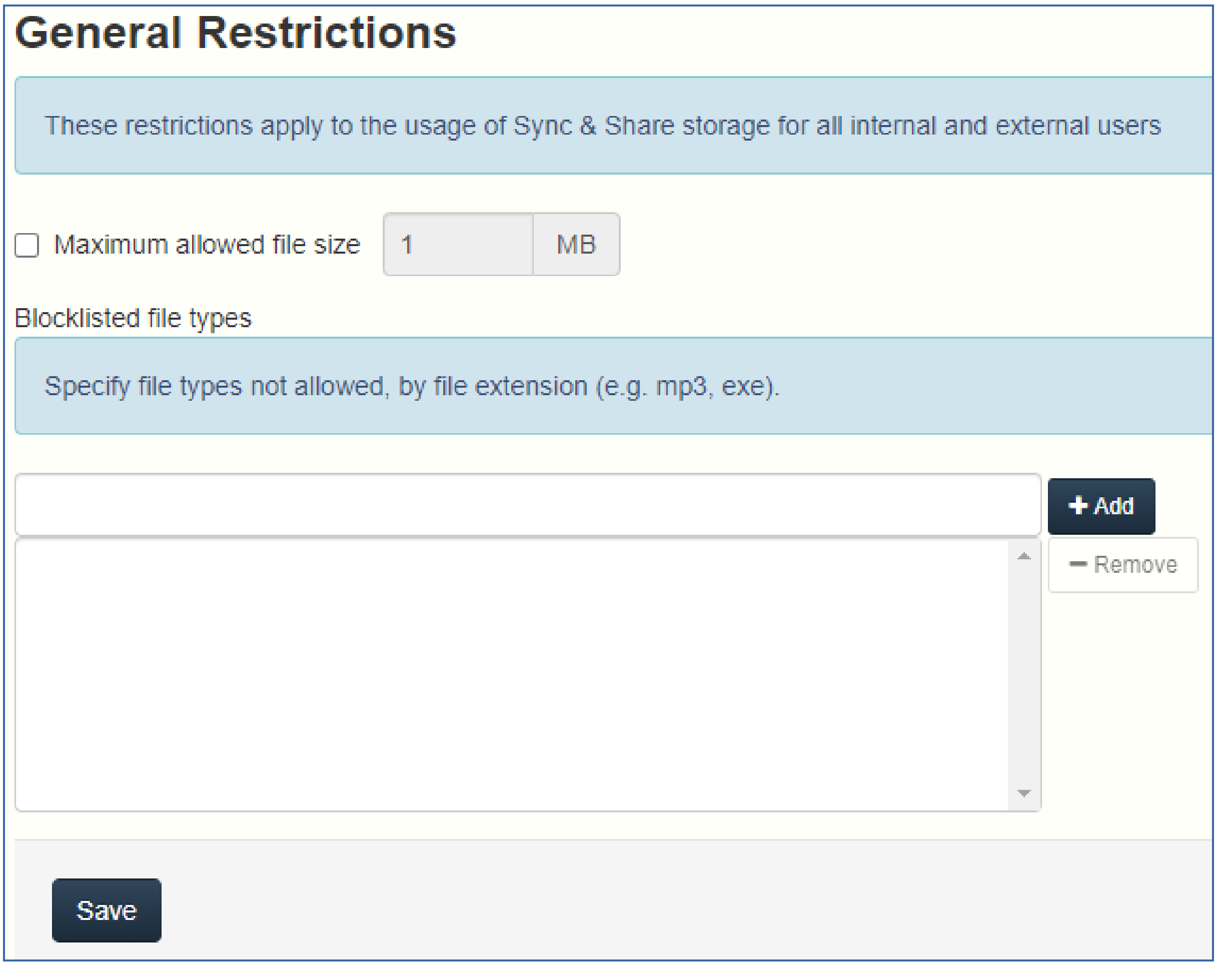
## Device Enrollment Requires:

- **PIN number + Active Directory username and password** - In order to activate their Acronis Cyber Files app and gain access to Acronis Cyber Files servers, a user is required to enter an expiring, one-time use PIN number and a valid Active Directory username and password. This option ensures that a user can only enroll one device, and only after receiving a PIN number issued by their IT administrator. This option is recommended when the enhanced security of two-factor device enrollment is required.
- **Active Directory username and password only** - A user can activate their Acronis Cyber Files app using only their Active Directory username and password. This option allows a user to enroll one or more devices at any point in the future. Users just need to be given the name of their Acronis Cyber Files server, or a URL pointing to their Acronis Cyber Files server, which can be posted on a web site or emailed, simplifying the rollout of Acronis Cyber Files to large numbers of users. This option is preferred in environments where two-factor enrollment is not required and many users may need access to Acronis Cyber Files at any time, such as student deployments.

# Sync & Share

This section of the Web Interface is available only if you have enabled Sync & Share functionality. Otherwise you will see a button **Enable sync & share support**.

## General Restrictions



General Restrictions

These restrictions apply to the usage of Sync & Share storage for all internal and external users

□ Maximum allowed file size 1 MB

Blocklisted file types

Specify file types not allowed, by file extension (e.g. mp3, exe).

You can set basic restrictions such as blocklisting file types and files over a certain size.

**Maximum allowed file size** - Allows you to set a maximum file size for all Sync & Share files.

**Blocklisted file types** - Allows you to block the use of certain file types with the Sync & Share functionality.

## To set a file type blocklist:

1. In the web console, expand the **Sync & Share** tab and open **General Restrictions**.
2. In the **Add field** under **Blocklisted file types**, enter a comma separated list of all file types you wish to prohibit.
3. Click **Save**.

**Note**

Any preexisting files of that type will no longer be synced and will not be movable. You can only manually download them or remove them.

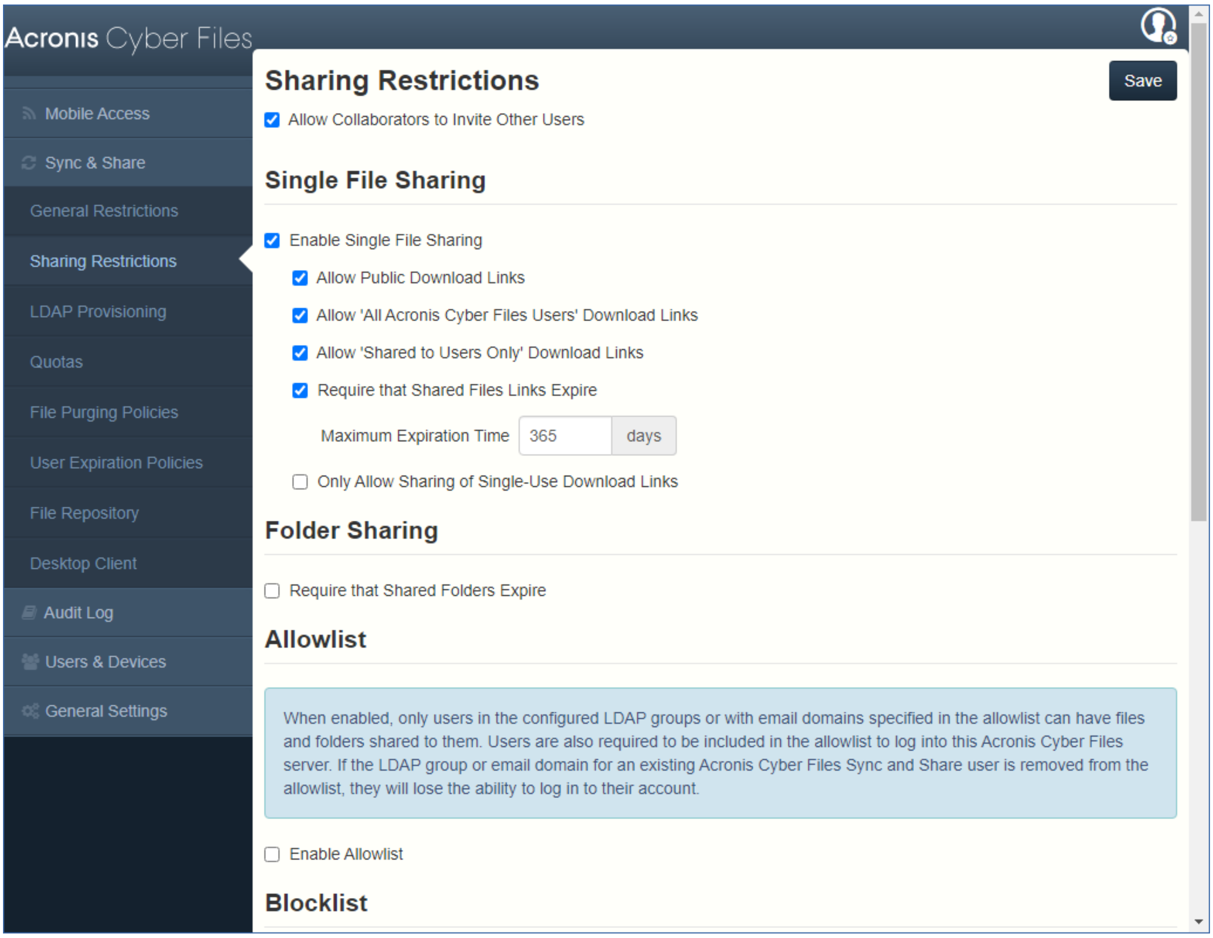
## To set a maximum file size limit:

1. In the web console, expand the **Sync & Share** tab and open **General Restrictions**.
2. Select the **Maximum allowed file size** checkbox and enter the desired maximum file size in the text field (in MBs).
3. Click **Save**.

**Note**

Any preexisting files of a bigger size will no longer be synced and will not be movable. You can only manually download them or remove them.

# Sharing Restrictions



**Sharing Restrictions**

☑ Allow Collaborators to Invite Other Users

**Single File Sharing**

☑ Enable Single File Sharing

- ☑ Allow Public Download Links
- ☑ Allow 'All Acronis Cyber Files Users' Download Links
- ☑ Allow 'Shared to Users Only' Download Links
- ☑ Require that Shared Files Links Expire
  - Maximum Expiration Time 365 days
- ☐ Only Allow Sharing of Single-Use Download Links

**Folder Sharing**

☐ Require that Shared Folders Expire

**Allowlist**

When enabled, only users in the configured LDAP groups or with email domains specified in the allowlist can have files and folders shared to them. Users are also required to be included in the allowlist to log into this Acronis Cyber Files server. If the LDAP group or email domain for an existing Acronis Cyber Files Sync and Share user is removed from the allowlist, they will lose the ability to log in to their account.

☐ Enable Allowlist

**Blocklist**

**Allow Collaborators to Invite Other Users** - If this setting is disabled, the checkbox **Allow collaborators to invite other collaborators** will not appear when inviting users to folders. This will prevent invited users from inviting other users.

## Single File Sharing Expiration

**Enable Single File Sharing** - When enabled, allows the sharing of single file links and lets you control how users access them and the duration for which they are accessible.

- **Allow Public Download Links** - When enabled, anybody can access the shared file if they have the link.
- **Allow 'All Acronis Cyber Files Users' Download Links** - When enabled, only users that possess credentials for Acronis Cyber Files will be able to access the shared file.
  - **Allow Only Internal (AD) Users to Download** - When enabled, only users that possess Active Directory credentials for Acronis Cyber Files will be able to access the shared file.
- **Allow 'Shared to' Users Only Download Links** - When enabled, allows the use of links usable only be the users that they are shared to.
- **Require that Shared File Links Expire** - When enabled, forces file links to have an expiration date.
  - **Maximum Expiration Time** - Controls the maximum amount of time (in days) before the file expires.
- **Only Allow Sharing of Single-Use Download Links** - When enabled, users will be able to send only single-use links. These links will be revoked after the first download.

### Folder Sharing

**Require that Shared Folders Expire** - When enabled, all shared folders will be required to have an expiration date.

- **Maximum Expiration Time** - Controls the maximum amount of time (in days) before the folder expires.

## Allowlist

If the allowlist is enabled, only users in the configured LDAP groups or with the email domains (like example.com) specified in the list can login. Wildcards can be used for domains (e.g. *.example.com). LDAP groups must be specified by their distinguished names, such as CN=mygroup,CN=Users,DC=mycompany,DC=com.

## Blocklist

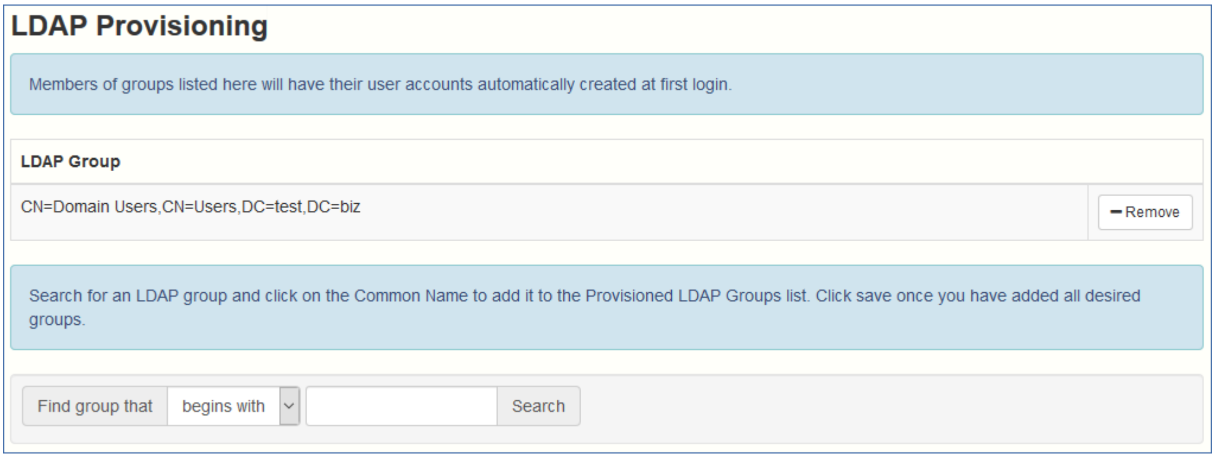
Users in LDAP groups or with the email domains (like example.com) specified in the blocklist will not be permitted to log into the system, even if they are in the allowlist. Wildcards can be used for domains (e.g. *.example.com). LDAP groups must be specified by their distinguished names, such as CN=mygroup,CN=Users,DC=mycompany,DC=com.

**Note**

Wildcard entries can only contain one star and it should be always at the beginning of the string and followed by a period, (e.g. *.example.com, *.com).

# LDAP Provisioning

Members of the groups listed here will have their user accounts automatically created at first login. This simplifies the account creation process so the administrator doesn't have to send each user an invitation.



LDAP Provisioning

Members of groups listed here will have their user accounts automatically created at first login.

| LDAP Group | |
|---|---|
| CN=Domain Users,CN=Users,DC=test,DC=biz | − Remove |

Search for an LDAP group and click on the Common Name to add it to the Provisioned LDAP Groups list. Click save once you have added all desired groups.

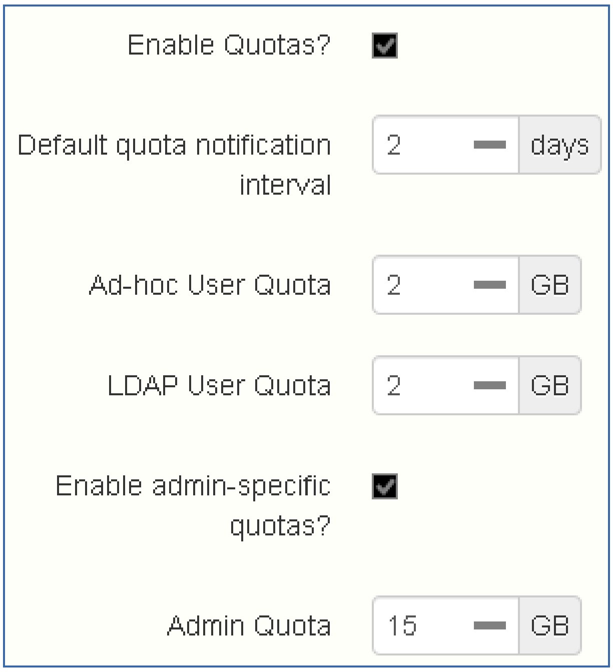
## LDAP Group

This is the list of currently selected groups.

- **Common Name / Display Name** - The display name given to the user or group.
- **Distinguished Name** - The distinguished name given to the user or group. A distinguished name is a unique name for an entry in the Directory Service.

# Quotas

Administrators can set the amount of space dedicated to each user in the system. There are distinct default settings for external (ad-hoc) and internal (Active Directory - LDAP) users.
Administrators can also assign different quota values based on individual users or Active Directory group membership.



Enable Quotas? ☑

Default quota notification interval: 2 days

Ad-hoc User Quota: 2 GB

LDAP User Quota: 2 GB

Enable admin-specific quotas? ☑

Admin Quota: 15 GB

- **Enable Quotas?** - If enabled, limits the maximum space a user has by a quota.
  - **Default quota notification interval** - Time interval in days that sets how often users nearing their quota limit will receive notification emails.
  - **Ad-hoc User Quota** - Sets the quota for Ad-Hoc users.
  - **LDAP User Quota** - Sets the quota for LDAP users.
  - **Enable admin-specific quotas?** - If enabled, administrators will have a separate quota applied to them.
    - **Admin Quota** - Sets the quota for administrators.

**Note**
If a user is a member of multiple groups, only the biggest quota is applied.

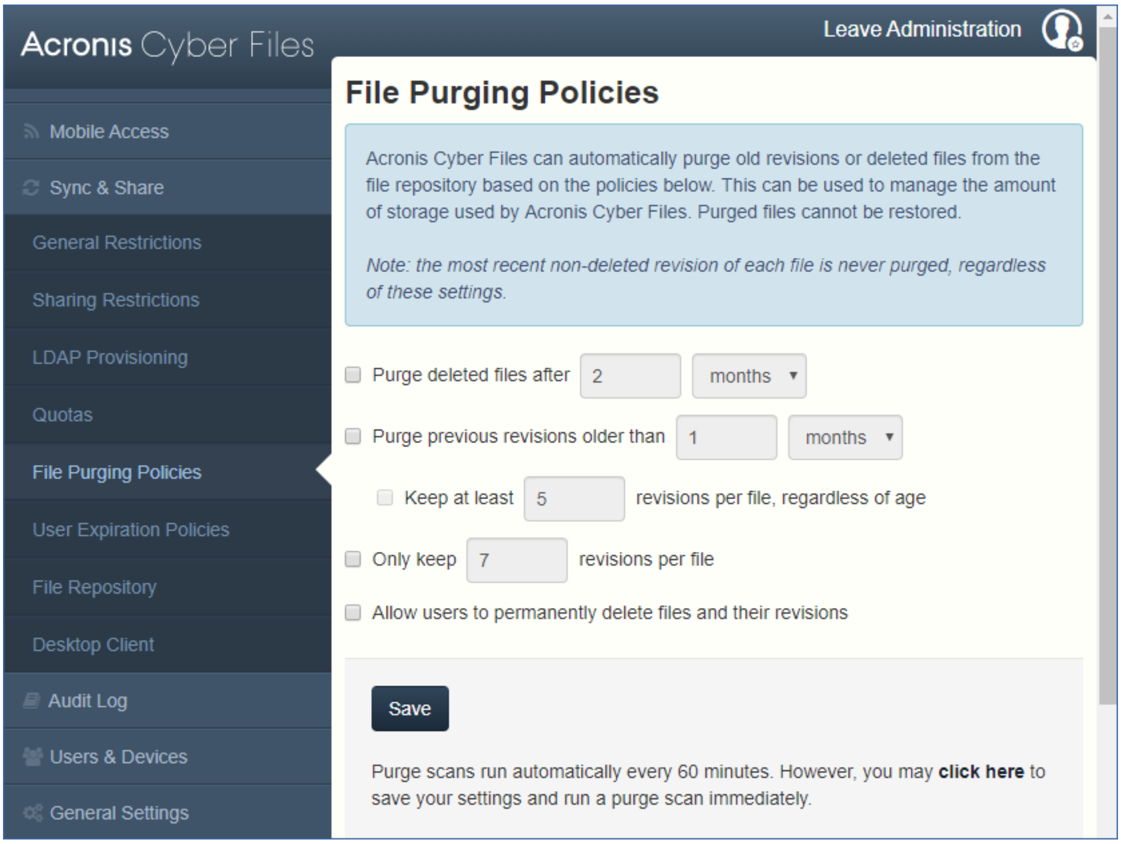
**Note**
Quotas can be specified for individual users. Individual quota settings override all other quota settings. To add individual user quotas for other users, please edit the user on the **Users** page.

**Note**
Quotas can be set in megabytes by specifying a size that is smaller than 1 GB. **e.g. 0.5**, **0.3**, **0.9** and etc.

# File Purging Policies

In Acronis Cyber Files, documents, files and folders are normally preserved in the system unless explicitly eliminated. This allows users to recover deleted files and maintain previous versions of any document. Acronis Cyber Files allows administrators to define policies to determine how long deleted files will be preserved, the maximum number of revisions to keep and when older revisions will be deleted.

Acronis Cyber Files can automatically purge old revisions or deleted files from the file repository based on the policies below. This can be used to manage the amount of storage used by Acronis Cyber Files. Purged files cannot be restored.



File Purging Policies

Acronis Cyber Files can automatically purge old revisions or deleted files from the file repository based on the policies below. This can be used to manage the amount of storage used by Acronis Cyber Files. Purged files cannot be restored.

*Note: the most recent non-deleted revision of each file is never purged, regardless of these settings.*

□ Purge deleted files after 2 months

□ Purge previous revisions older than 1 months

□ Keep at least 5 revisions per file, regardless of age

□ Only keep 7 revisions per file

□ Allow users to permanently delete files and their revisions

Purge scans run automatically every 60 minutes. However, you may **click here** to save your settings and run a purge scan immediately.

**Note**

The most recent non-deleted revision of each file is never purged, regardless of these settings.

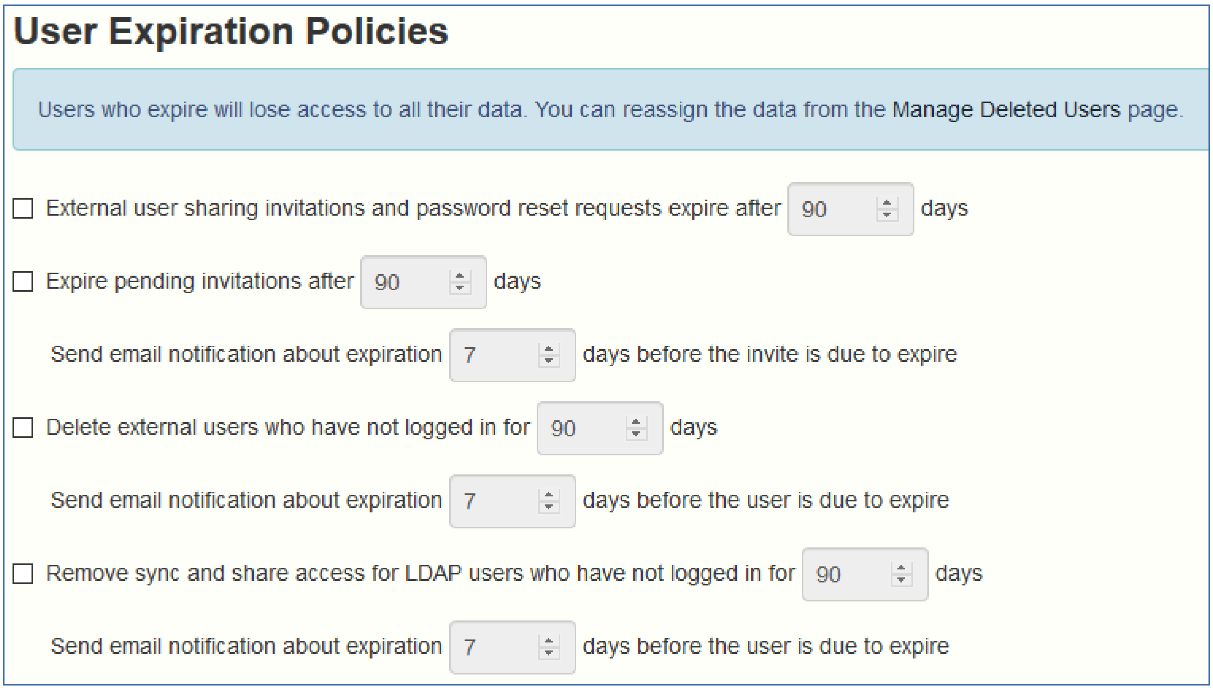
- **Purge deleted files after** - If enabled, files older than this setting will be purged.
- **Purge previous revisions older than** - If enabled, file revisions older than this setting will be purged.
  - **Keep at least X revisions per file, regardless** - If enabled, keeps a minimum number of revisions per file, regardless of their age.
- **Only keep X revisions per file** - If enabled, limits the maximum number of revisions per file.
- **Allow users to permanently delete files and their revisions** - If enabled, files and their revisions will be completely erased, without any possibility to be recovered from this moment on.

**Note**

Use the **Save** button to keep your settings. To start a purge immediately, in addition to saving the settings, use the **click here** option, otherwise a regular scan runs every 60 minutes.

# User Expiration Policies

You can set invitations and user accounts to expire after a specified period of inactivity.



User Expiration Policies

Users who expire will lose access to all their data. You can reassign the data from the Manage Deleted Users page.

□ External user sharing invitations and password reset requests expire after 90 days

□ Expire pending invitations after 90 days

Send email notification about expiration 7 days before the invite is due to expire

□ Delete external users who have not logged in for 90 days

Send email notification about expiration 7 days before the user is due to expire

□ Remove sync and share access for LDAP users who have not logged in for 90 days

Send email notification about expiration 7 days before the user is due to expire

- **External user sharing invitations and password reset requests expire after X days**- If enabled, invitations and password reset requests for External users will expire after a set number of days.
- **Expire pending invitations after X days** - If enabled, all pending invitations will expire after a set number of days.
  - **Send email notification about expiration X days before the invite is due to expire** - If enabled, sends a notification a set number of days before the invite is due to expire.
- **Delete external users who have not logged in for X days** - If enabled, deletes external users who have not logged in for a set number of days.
  - **Send email notification about expiration X days before the user is due to expire** - If enabled, sends a notification a set number of days before the adhoc user is due to expire.
- **Remove sync and share access for LDAP users who have not logged in for X days** - If enabled, removes sync and share access for LDAP users who have not logged in for a set number of days.
  - **Send email notification about expiration X days before the user is due to expire** - If enabled, sends a notification a set number of days before the user is due to expire.

## What happens to Expired User Account content?

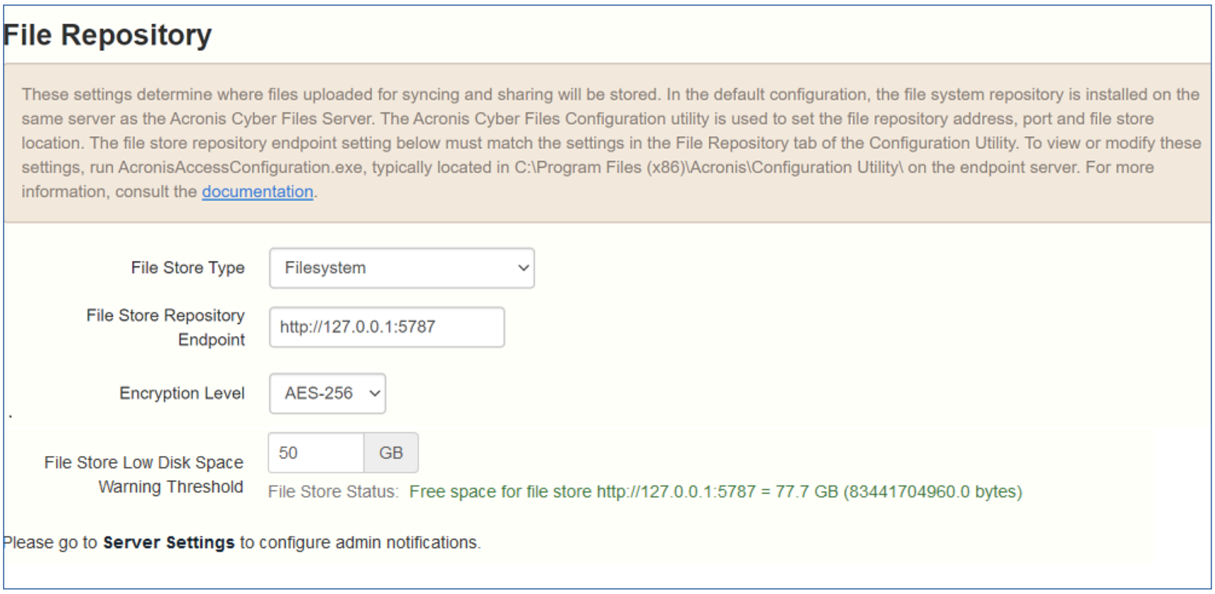
Users whose accounts expire lose access to and ownership of all their content, but the content is preserved in the system.

You must either reassign or permanently delete it from the **Manage Deleted Users** page.

**Important**
Until you permanently delete the content of an expired user account, the space consumed by that content will not be freed up. File purging will only remove content which the expired user had previously deleted.

# File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The File Repository is used to store Acronis Cyber Files Sync & Share files and previous revisions. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The **File Store Repository Endpoint** setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility`.



File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The file store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the documentation.

File Store Type: Filesystem

File Store Repository Endpoint: http://127.0.0.1:5787

Encryption Level: AES-256

File Store Low Disk Space Warning Threshold: 50 GB

File Store Status: Free space for file store http://127.0.0.1:5787 = 77.7 GB (83441704960.0 bytes)

Please go to **Server Settings** to configure admin notifications.

- **File Store Type** - Select the storage location you would like to use for the virtual file system's repository. The options are **File System**, **Acronis Storage**, **Microsoft Azure Storage**, **Amazon S3**, **Swift S3**, **Ceph S3** and **Other S3-Compatible Storage**.

  **Note**
  You can use the **Other S3-Compatible Storage** option with S3 storage providers not on this list, but we cannot guarantee that everything will work properly.

  **Note**
  MinIO S3 storage type is supported and can be configured as **Other S3-Compatible Storage** option, however, we do not support it over a non-secure HTTP connection.

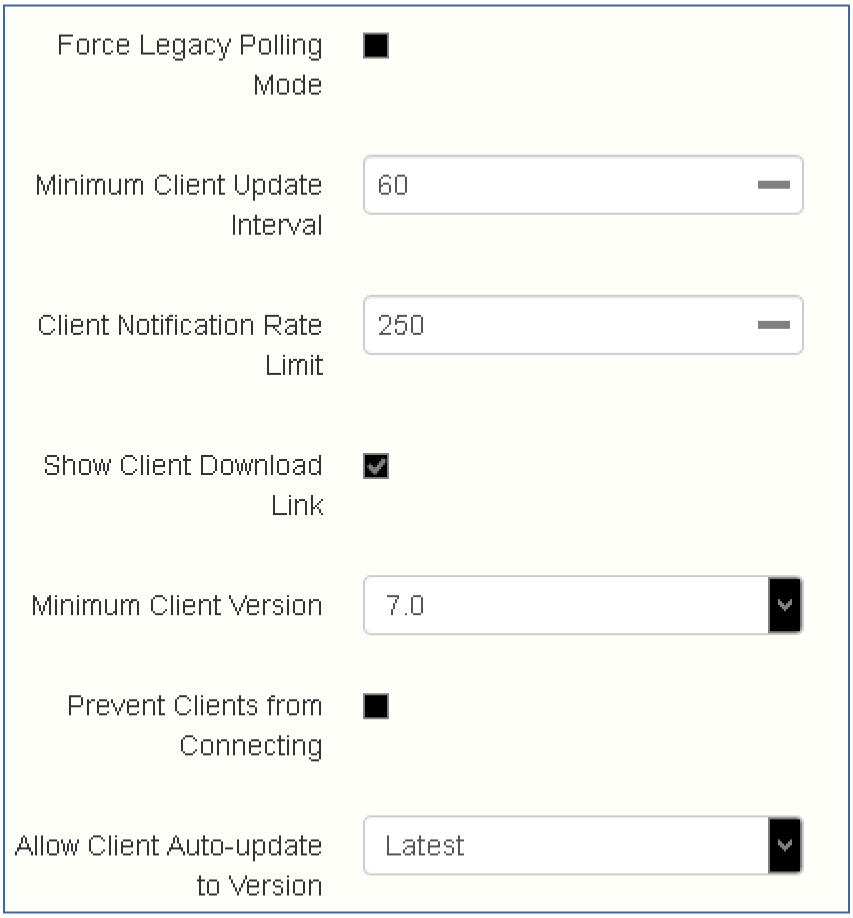
**Note**

If multiple users upload the same file, the total consumed storage will be equal to the number of these users times the file size i.e the space used will be proportional to the number of users and uploads. The consumed storage will correspond to the total volume of all files uploaded by all participating users. However, the amount of storage occupied will not depend on the type(s) of backend storage used as well as the fact that they are uploading the same file.

- **File Store Repository Endpoint** - Set the URL address of the file system repository endpoint.
- **Encryption Level** - Specify the type of encryption that should be used to encrypt files stored in the virtual file system's repository. The options are None, AES-128 and AES-256. The default is AES-256.
- **File Store Low Disk Space Warning Threshold** - After the free space goes below this threshold, the administrator will receive notifications of low disk space.

# Acronis Cyber Files Client

These settings are for the Desktop client.



Force Legacy Polling Mode ■

Minimum Client Update Interval 60

Client Notification Rate Limit 250

Show Client Download Link ☑

Minimum Client Version 7.0

Prevent Clients from Connecting ■

Allow Client Auto-update to Version Latest

- **Force Legacy Polling Mode** - Forces the clients to poll the server instead of being asynchronously notified by the server. You should only enable this option if instructed to do so by

Acronis support.
    - **Client Polling Time** - Sets the time intervals in which the client will poll the server. This option is available only when **Force Legacy Polling Mode** is enabled.
- **Minimum Client Update Interval** - Sets the minimum time (in seconds) the server will wait before re-notifying a client that updated content is available.
- **Client Notification Rate Limit** - Sets the maximum number of client update notifications the server will send per minute.
- **Show Client Download Link** - If enabled, web users will be shown a link to download the desktop client.
- **Minimum Client Version** - Sets the minimum client version that can connect to the server.

**Note**
As of Acronis Cyber Files Server version 7.5, only desktop clients newer than version 6.1 can connect.

- **Prevent Clients from Connecting** - If enabled, Desktop clients will not be able to connect to the server. In general, this should be enabled only for administrative purposes. This does not prevent connections to the web interface.
- **Allow Client Auto-update to Version** - Sets the Desktop client version that will be deployed to all Desktop clients via auto-update checks. Select **Do not allow updates** to prevent clients from auto-updating at all.

# Users&Devices

## Managing Devices

Once Acronis Cyber Files users connect to the Acronis Cyber Files Web Server, their devices appear on the **Devices** list.

Here you can view detailed status information about all used devices. You can also wipe Acronis Cyber Files app or change its password.

- **User Name** – Active Directory (AD) display name for an LDAP user or a name chosen by an Ad-hoc user.
- **Device name** – Device name set by the user.
- **Model** – Product name of the user's mobile device.
- **OS** – Type and version of the mobile or desktop operating system.
- **Version** – Version of the Acronis Cyber Files app or the desktop client used.
- **Status** – Status of the Acronis Cyber Files app, which could be:
  - Managed;
  - Managed, pending remote wipe;
  - Unmanaged, remote wipe succeeded;
  - Unmanaged, pending remote wipe;
  - Unmanaged by user;
  - Wiped after user entered incorrect password.

For the desktop client, the single status is Sync & Share.

- **Last Contact** – Date and time of the last connection between the management server and the Acronis Cyber Files app/desktop client.
- **Policy** – Name and link to the management policy applied to a user.
- **Actions**
  - **More Info** – Shows additional details about the device and editable device **Notes** field.
  - **App password reset** (for mobile devices only) – Resets the Acronis Cyber Files app lock password on the selected device. To do this, you have to generate a confirmation code by using the password reset code shown on the user’s device screen.
  - **Remote wipe** (for mobile devices only) – If selected, all the files in the Acronis Cyber Files app and its own settings are deleted, once the device connects to the management server. No other apps or OS data is affected.
  - **Remove from list** – This removes a desktop client from the **Device** list. For mobile devices, this removes the selected device from the list and un-manages it without wiping it. This is typically used to remove a device that you do not expect to ever contact the Acronis Cyber Files management server again. If you have enabled **"Allow mobile clients restored to new devices to auto-enroll without PIN "**, such a new device will automatically appear as managed, once it connects to the server.

## Exporting the data about the devices

The data about all devices in this list could be exported in txt, csv or xml file.

To do this, click on the **Export** button and select the desired file format.

**Exported data consists of:**

1. User Name
2. Name of the mobile device or computer used
3. Model of the mobile device
4. OS type and version of the device
5. Acronis Cyber Files app or desktop client version
6. Mobile device or desktop client status
7. Date and time of Acronis Cyber Files app enrollement with the Acronis Cyber Files Web Server
8. Date and time of the last contact between the Acronis Cyber Files app or desktop client with the Acronis Cyber Files Web Server
9. Name of the user policy applied
10. Notes

# Performing Remote Application Password Resets

The Acronis Cyber Files app can be secured with a lock password that must be entered when the app is launched. If a user forgets this password, they will not be able to access Acronis Cyber Files. The app password is independent of the user's Active Directory account password.

When an app lock password is lost, the only options are to perform a remote password reset or to let the user uninstall Acronis Cyber Files app from their device and reinstall it. Uninstalling deletes any existing data and settings, which maintains security but will likely leave users with no access to Acronis Cyber Files servers until they are sent a new management invitation.

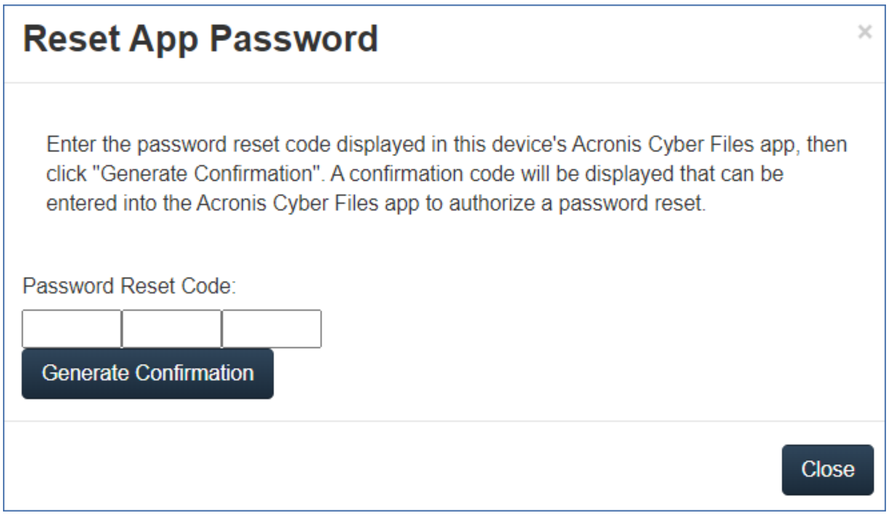
## Resetting an application password

Acronis Cyber Files on-device files have always been protected using Apple Data Protection (ADP) file encryption. To further protect files on devices being backed up into iTunes and iCloud, devices without device-level lock codes enabled, and as a general security enhancement, we introduced a second layer of full-time custom encryption applied directly by the Acronis Cyber Files app.

One aspect of this encryption is that Acronis Cyber Files app users can not have their application lock password reset over the air. Instead, a password reset code and a confirmation code must be exchanged between the user and the Acronis Cyber Files IT administrator, in order to enable Acronis Cyber Files to decrypt its settings database and allow the user to set a new app password.

**To reset the password for Acronis Cyber Files app for iOS or Android:**

1. An end user asks you to reset their password for the Acronis Cyber Files app and tells you the **Password Reset Code**, shown on their device screen.
2. Open the **Users & Devices** tab.
3. Open the **Devices** tab.
4. Find the device whose app password you want to reset and click the **Actions** button.
5. Press **App password reset...**
6. Enter the **Password Reset Code**, then click **Generate Confirmation**.
7. Tell or email the user the **Confirmation Code** that is displayed.
8. The user enters this code into the app's password reset dialog and then is prompted to set a new password. If the user aborts this process without setting a proper app password, they are denied access to Acronis Cyber Files app and have to repeat the app password reset process.



Reset App Password

Enter the password reset code displayed in this device's Acronis Cyber Files app, then click "Generate Confirmation". A confirmation code will be displayed that can be entered into the Acronis Cyber Files app to authorize a password reset.

Password Reset Code:

## Performing Remote Wipes

Acronis Cyber Files allows a mobile app to be remotely wiped. This removes all files that are locally stored or cached within the Acronis Cyber Files app. All app settings are reset to the previous defaults and any servers that have been configured in the app are removed.

**To do this:**

1. Open the Acronis Cyber Files web interface.
2. Open the **Users & Devices** tab and navigate to **Devices**.
3. Find the device you want to wipe remotely and press the **Actions** button.
4. Press **Remote Wipe...**
5. Confirm the remote wipe by pressing **Wipe**.
6. A **'Pending remote wipe'** status appears in the **Status** column for that device.

**Note**

Administrator can cancel a pending remote wipe but only before the app connects to the management server. This option appears in the **Actions** menu after a remote wipe has been issued.

7. Remote wipe will be completed when the device connects to the server again. This step is irreversible.

**Note**

**Connectivity requirements**

Acronis Cyber Files clients must have network access to the Acronis Cyber Files server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access Acronis Cyber Files, they also need to connect to the VPN before management commands are accepted.

# Managing Users

You can manage all your Sync & Share users from the **Users** section.

You can invite new users from the **Add User** button or edit/delete current users from the **Actions** button. While editing users, you can give them administrative rights (if you have the right to do so), change their email, change their password or disable/enable their account.

If quotas are enabled, you can set a custom quota for specific users, but only if they have Sync & Share access.

## Types of Sync & Share users

There are three types of Sync & Share user accounts:

### External (ad-hoc) user accounts

These accounts have to be manually created via an email invitation sent by an administrator or via another user’s invitation to shared content (file or folder).

There are two subtypes of the External account: **Free** and **Licensed**.

By default, every newly created External account is Free. Only a Acronis Cyber Files administrator can convert a Free External account to a Licensed External account.

Users with a Licensed account can create, upload, edit, and delete files and folders in their own Sync & Share space. They can also share their content with other people.

Users with a Free account do not have a Sync & Share space. If they are given the respective rights, Free account users can create new files, upload files from another location, and edit and delete existing files only in a folder shared with them. If they are given read-only rights, they cannot create, upload, edit or delete files, but can only browse, preview, and download the files that the shared folder contains.

Free account users can neither invite new users to the shared resource, nor can they see the other users with whom this resource is shared – even though they might have been assigned such rights when their account was created.

If a file is shared with a free account user, they can only preview and download it.

Free account users cannot use the Acronis Cyber Files desktop client or mobile apps.

**Note**
All newly created External accounts need to be manually activated. Users receive an email with instructions for how to do this.

## Internal (LDAP) user accounts

These accounts rely on Active Directory (AD) integration. They are created either manually – as the External ones – or an administrator can set up a Provisioned LDAP group and allow the AD users to have their accounts automatically created when they first log in to Acronis Cyber Files.

The internal accounts are automatically licensed at their creation.

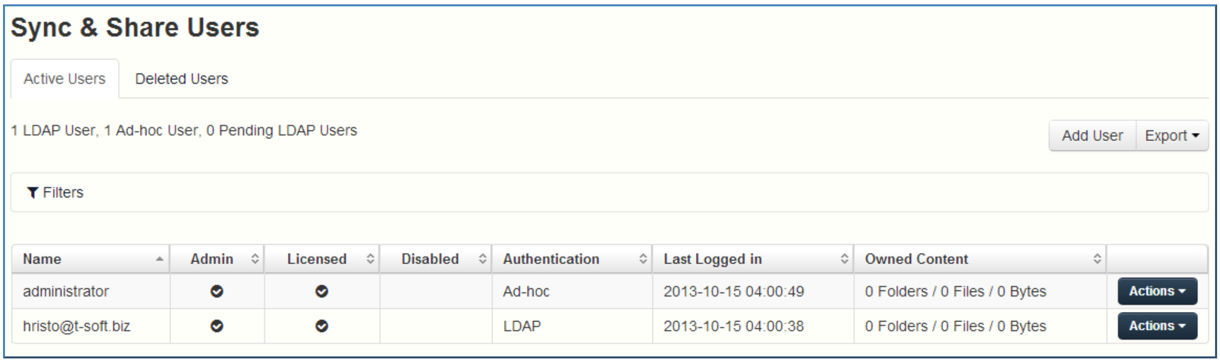
Users with internal accounts can create, upload, edit, and delete files and folders in their own Sync & Share space or in folders shared with them. They can also share their content with other people.

They can use the Acronis Cyber Files desktop client and mobile apps.

## No Access user accounts

These are administrative accounts without Sync & Share access. They are not licensed, by default. Users with these accounts cannot use Acronis Cyber Files desktop client and mobile apps.

**Note**
Administrators without Sync & Share access do not need to set an email address for their account – they can simply log in with their LDAP credentials. Such accounts can be created without having to set up SMTP for your Acronis Cyber Files Server. For more information, please see: Administrators and Privileges.



Sync & Share Users

1 LDAP User, 1 Ad-hoc User, 0 Pending LDAP Users

| Name | Admin | Licensed | Disabled | Authentication | Last Logged in | Owned Content | |
|---|---|---|---|---|---|---|---|
| administrator | ✓ | ✓ | | Ad-hoc | 2013-10-15 04:00:49 | 0 Folders / 0 Files / 0 Bytes | Actions |
| hristo@t-soft.biz | ✓ | ✓ | | LDAP | 2013-10-15 04:00:38 | 0 Folders / 0 Files / 0 Bytes | Actions |

In the **Users** tab you can view the following information:

- **Name** – Shows the name of the user (Active Directory (AD) display name for the LDAP users, or a name chosen by an Ad-hoc user).
- **Username** (optional) – Shows the logon name of the LDAP users.
- **UPN** (optional) – Shows the Universal principal name of the LDAP users.
- **Domain** (optional) – Shows the domain of the LDAP users.
- **Email** –Shows the email address of the user.
- **Sync & Share**
  - **Status** – Indicates the type of license used.
  - **Usage** – Shows the total size of the user's content.
- **Last Logged in** – Shows the time and date of the last login.
- **Actions**
  - **More Info** – Displays additional information about the user.
  - **Show Devices** – Displays information about the devices of this user.
  - **Reset Sync & Share Password** – Sends a password resetting email.
  - **Convert to Licensed** – Converts a free user to a licensed user.
  - **Edit User** – Allows you to edit this user by changing their email, disabling or enabling their account, giving them full or specific administrative rights, or setting a custom quota for their account. For external users, you are allowed to change their mobile phone numbers, used for 2FA.
  - **Delete** – Deletes the user.

## Exporting the data about the users

The data about all enrolled users can be exported in txt, csv or xml file.

To do this, click the **Export** button and select the desired file format.

**Exported data consist of:**

1. Name of the user
2. User's logon name (for LDAP users)
3. Universal principal name (for LDAP users)
4. LDAP domain (for LDAP users)
5. Email
6. Policy name
7. Pending status
8. Administrative permissions
9. Licensed user status
10. Disabled user status
11. LDAP authentication
12. Number of folders owned by the user
13. Number of files owned by the user
14. Size of user's content (in bytes)

15. Size of user's quota (in bytes)
16. Date and time of the last login

## Adding an External (Ad-hoc) user

**To add an External (Ad-hoc) user:**

1. Open the Acronis Cyber Files web interface.
2. Log in with an administrator account. An account with the **Manage Users** rights can be used as well.
3. Open the **Users & Devices** tab.
4. Open the **Users** tab.
5. Press the **Add Sync & Share User** button.
6. Write the email of the user.
7. Select the language of the invitation.
8. Press the **Add** button.

The user receives an email with a link. Once they open the link, they are asked to set a password. Then the user receives an email to confirm their account. Once they open the link in the email, their account registration is complete.

## Adding an Internal (LDAP) user

**To add an Internal (LDAP) user:**

1. Open the Acronis Cyber Files web interface.
2. Log in with an administrator account. An account with the **Manage Users** rights can be used as well.
3. Open the **Users & Devices** tab.
4. Open the **Users** tab.
5. Press the **Add Sync & Share User** button.
6. Write the email of the user.
7. Select the language of the invitation.
8. Press the **Add** button.

The user can now log in with their LDAP credentials. Once the user logs in, their account registration is complete.

**Note**
If you have LDAP enabled, and have a provisioned LDAP Administrator Group, users in that LDAP group can log in directly with their LDAP credentials and have full administrative rights.

## Setting a custom quota

You can set a custom quota for any user with Sync & Share access.

**Todo so:**

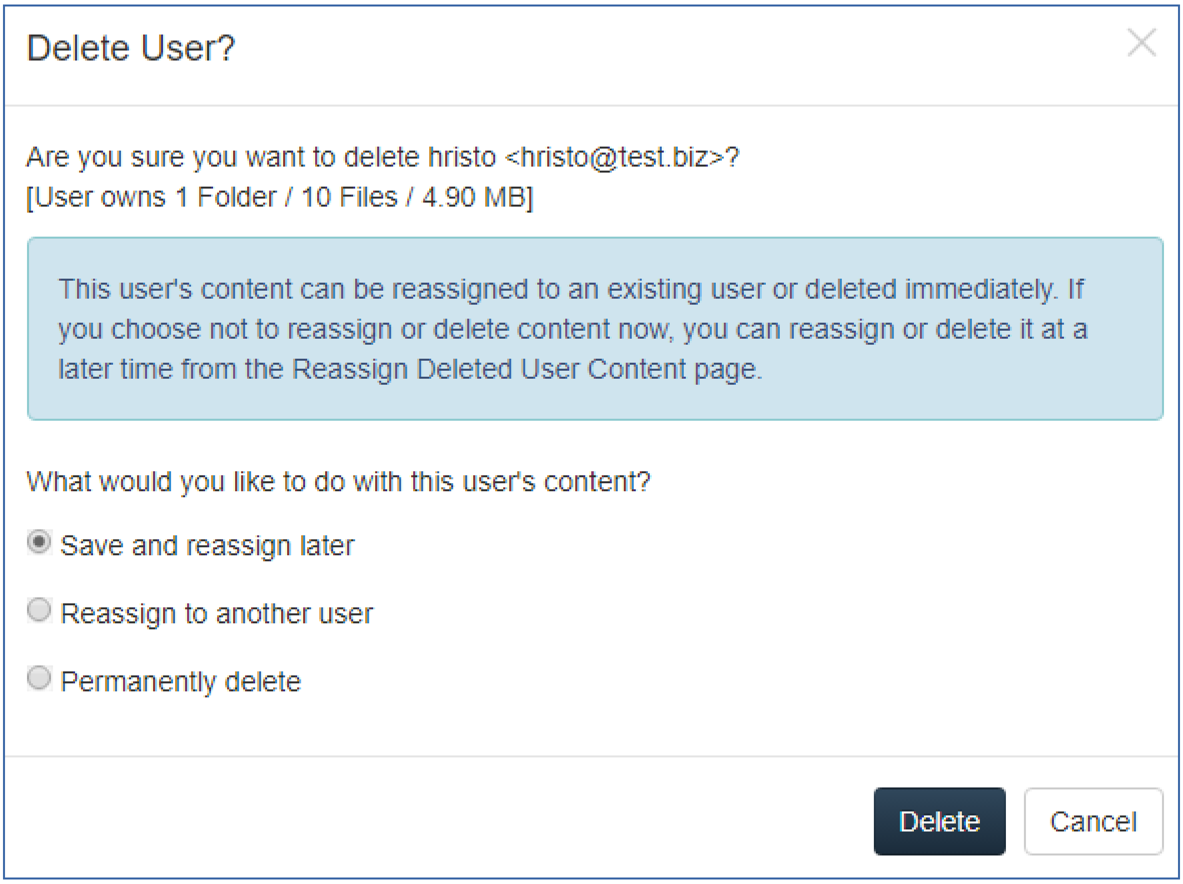
1. In the web interface, open the **Users & Devices** tab.
2. Locate the desired user and click the **Actions** button.
3. Select **Edit User** and enable **Use custom quota?**.
4. Enter the desired quota size and press **Save**.

**Note**
**Use custom quota?** checkbox is only accessible if the global option **Enable Quotas?** has been enabled beforehand.

## Deleting a user and their content

Deleting a user who has no content will completely remove the account.

When deleting a user with content (including expired users), you must choose what to do with their content.



Delete User?

Are you sure you want to delete hristo <hristo@test.biz>?
[User owns 1 Folder / 10 Files / 4.90 MB]

This user's content can be reassigned to an existing user or deleted immediately. If you choose not to reassign or delete content now, you can reassign or delete it at a later time from the Reassign Deleted User Content page.

What would you like to do with this user's content?

● Save and reassign later

○ Reassign to another user

○ Permanently delete

- **Save and reassign later** – The user's content is temporarily left in the system and can be managed in **Reassign Deleted User Content** tab. Such content can either be reassigned or permanently deleted.

**Note**

Purging policies will still be enforced over this content in the same way as for active users' content.

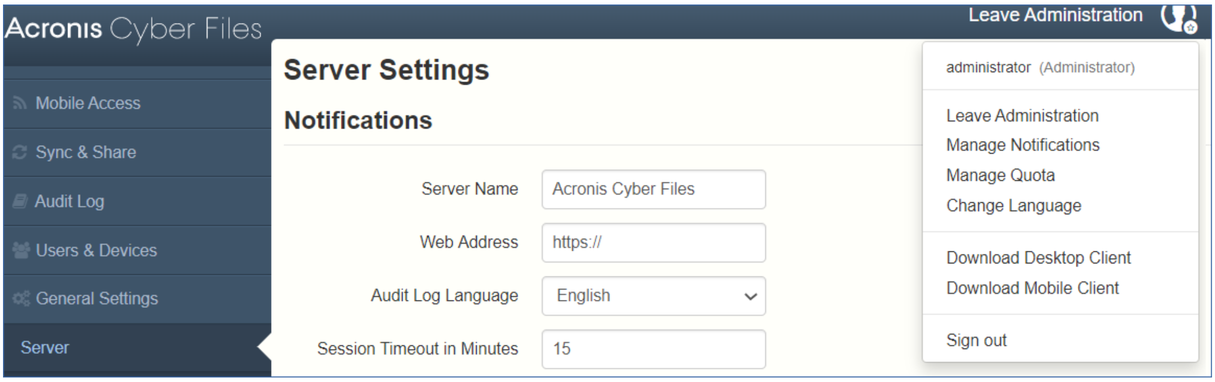
- **Reassign to another user** – The content is immediately reassigned to a user which you select, and a new folder named `Content inherited from DeletedUserName <deletedusersemail>` is created in their Sync & Share space. The selected user becomes the owner of the inherited content, including folders previously shared by the deleted user.
- **Permanently delete** – Immediately delete both the user's account and content.

# Server Administration

## Administering a Server

If you are an administrator logging in to the web interface, you can switch between **Administration** and **User** modes.

- To enter **Administration** mode, click on the user icon and press the **Administration Console**.
- To enter **User** mode, press the **Leave Administration** button at the top-right.



Server Settings

Notifications

Server Name: Acronis Cyber Files

Web Address: https://

Audit Log Language: English

Session Timeout in Minutes: 15

**Note**

Administrators have access to the API documentation. You can find the link in the footer of the web interface when you are in Administration mode.

## Administrators and Privileges

### Administration page access restrictions

- **Only connections from configured IP address ranges will be allowed to access the Administration pages** - allows the administrator to allow only certain IP addresses to accessing the Administration web interface.
  - **IP addresses allowed to access the Administration pages** - the administrator enters the IP addresses that can access the **Administration** page. They can be comma-separated IPs, subnets or IP ranges, **e.g.** 10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99.

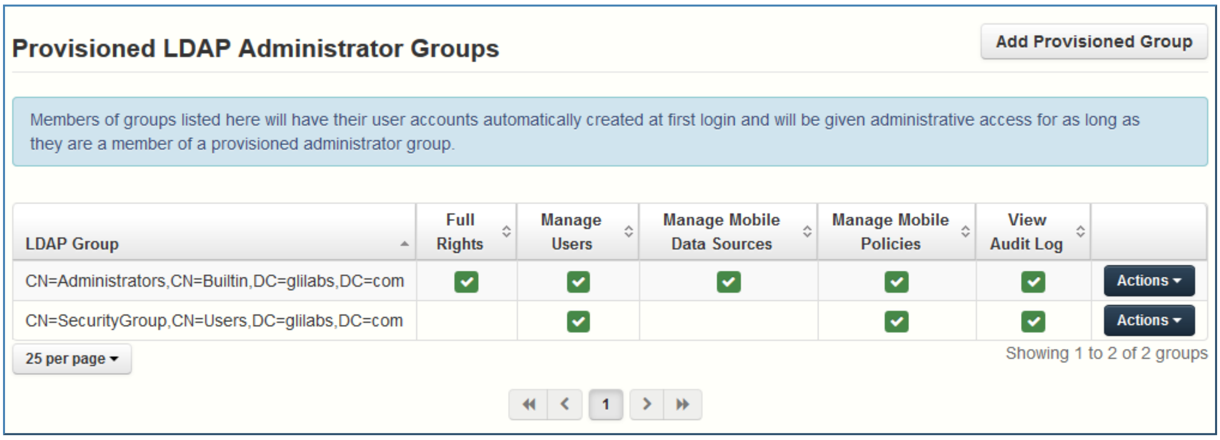
**Note**

Administrator access from localhost cannot be restricted.

**Note**

This feature does **not** work for servers that are using the Gateway Server to proxy requests for the Acronis Cyber Files server.

# Provisioned LDAP Administrator Groups



### Provisioned LDAP Administrator Groups

Members of groups listed here will have their user accounts automatically created at first login and will be given administrative access for as long as they are a member of a provisioned administrator group.

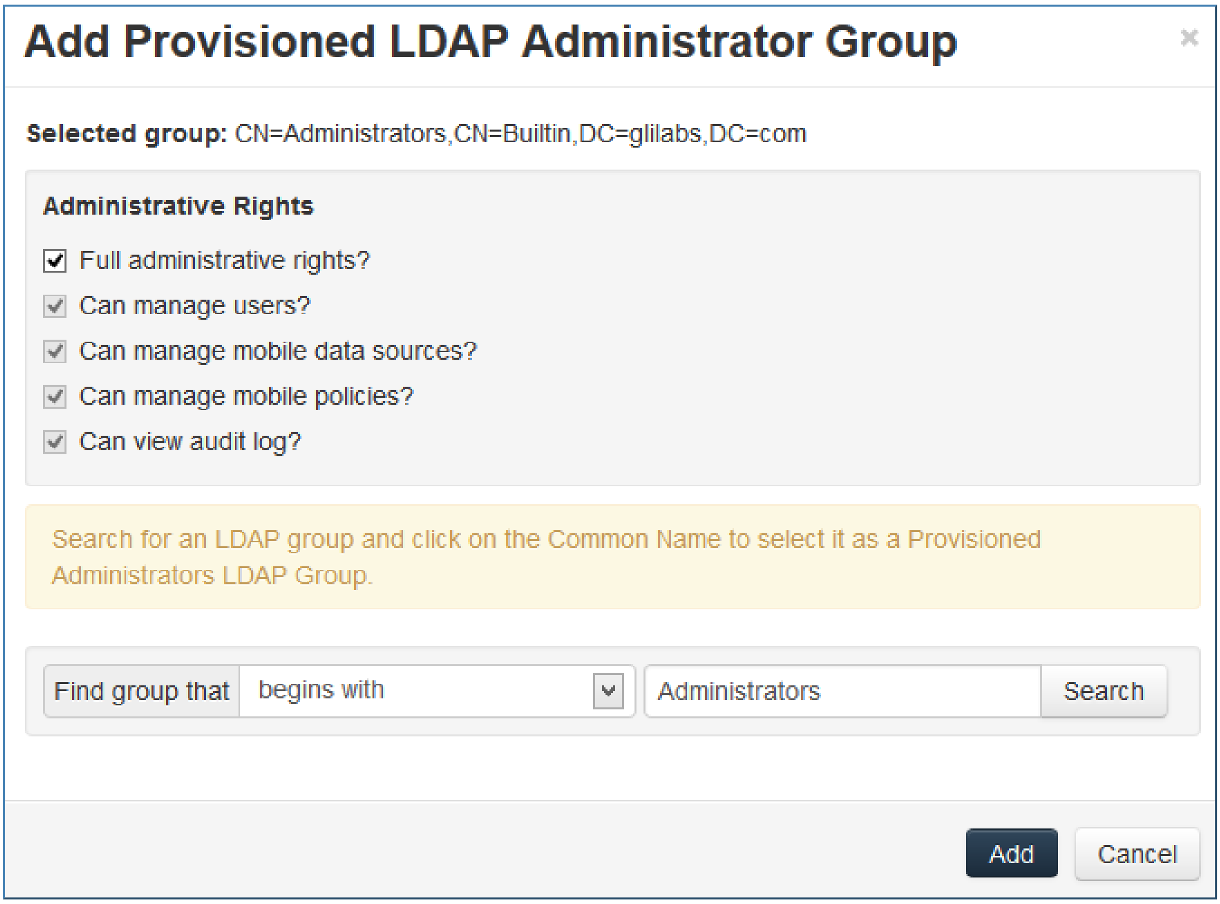
| LDAP Group | Full Rights | Manage Users | Manage Mobile Data Sources | Manage Mobile Policies | View Audit Log | |
|---|---|---|---|---|---|---|
| CN=Administrators,CN=Builtin,DC=glilabs,DC=com | ✓ | ✓ | ✓ | ✓ | ✓ | Actions ▾ |
| CN=SecurityGroup,CN=Users,DC=glilabs,DC=com | | ✓ | | ✓ | ✓ | Actions ▾ |

Showing 1 to 2 of 2 groups

This section allows you to manage your administrative groups. Users in these groups will automatically receive the group's administrative privileges. All of the rights are shown in a table, the ones that are currently enabled have a green mark.

Using the **Actions** button you can delete or edit the group. You can edit the group's administrative rights.

## To add a provisioned LDAP administrator group:



### Add Provisioned LDAP Administrator Group

**Selected group:** CN=Administrators,CN=Builtin,DC=glilabs,DC=com

**Administrative Rights**

- ☑ Full administrative rights?
- ☑ Can manage users?
- ☑ Can manage mobile data sources?
- ☑ Can manage mobile policies?
- ☑ Can view audit log?

Search for an LDAP group and click on the Common Name to select it as a Provisioned Administrators LDAP Group.

Find group that: begins with — Administrators

1. Click the **Add Provisioned Group**.
2. Mark if the group should have Sync & Share functionality.
3. Mark all of the administrative rights you want your group users to have.
4. Find the group.
5. Click on the group name.
6. Click **Save**.

## Administrative Users

This section lists all your Users with administrative rights, their authentication type (Ad-Hoc or LDAP), whether they have Sync & Share rights and their status (Disabled or Enabled).

You can invite a new user with full or partial administrative rights using the **Add Administrator** button. Using the **Actions** button you can delete or edit the user. You can edit his administrative rights, status, email address and password.

### Inviting a single administrator

1. Open the AcronisCyber Files Web Interface.
2. Log in with an administator account.
3. Expand the **General Settings** tab and open the **Administrators** page.
4. Click the **Add Administrator** button under **Administrative Users**.
5. Select either the **Active Directory/LDAP** or **Invite by Email** tab depending on what type of user you are inviting and what you want them to administer.
    a. **To invite via Active Directory/LDAP do the following:**

    1. Search for the user you want to add in the Active Directory and then click on their Common Name to select a user.

    **Note**
    The **LDAP User** and **Email** fields will fill in automatically.

    2. Enable/Disable the Sync & Share functionality.
    3. Select which administrative rights the user should have.
    4. Click **Add**.

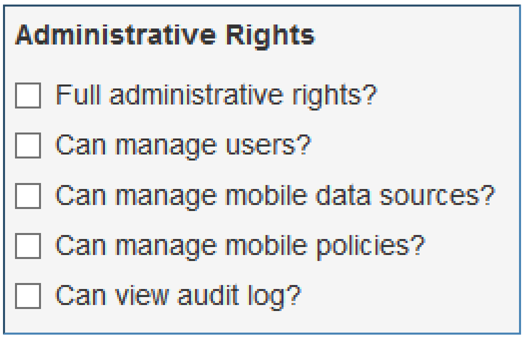
    b. **To invite by Email do the following:**

    1. Enter the email address of the user you want to add as an administrator.

    **Note**
    Ad-hoc users invited by email will always have Sync & Share functionality.

    2. Select whether this user should be licensed.
    3. Select which administrative rights the user should have.
    4. Select the language of the Invitation email.
    5. Click **Add**.

## Administrative rights



**Administrative Rights**

□ Full administrative rights?

□ Can manage users?

□ Can manage mobile data sources?

□ Can manage mobile policies?

□ Can view audit log?

- **Full administrative rights** - Gives the user full administrative rights.
- **Can manage users** - Gives the user the right to manage users. This includes inviting new users, LDAP group provisioning, sending Acronis Cyber Files enrollment invitations and managing the connected mobile devices.
- **Can manage mobile Data Sources** - Gives the user the right to manage the mobile Data Sources. This includes adding new Gateway Servers and Data Sources, managing the assigned sources, gateways visible on clients and legacy Data Sources.
- **Can manage mobile policies** - Gives the user the right to manage the mobile policies. This includes managing user and group policies, allowed apps and default access restrictions.
- **Can view audit log** - Gives the user the right to view the audit log.

**Note**

New users who are in both a LDAP provisioned administrators group and a LDAP provisioned sync & share group will get the combined permissions.

### To give a user administrative rights:

1. Open the **Sync & Share** tab.
2. Open the **Users** tab.
3. Click the **Actions** button for the User you want to edit.
4. Click **Edit**.
5. Mark all of the administrative rights you want your user to have.
6. Click **Save**.

### To give an administrator specific rights:

1. Click the **Actions** button for the User you want to edit.
2. Click **Edit**.
3. Mark all of the administrative rights you want your user to have.
4. Click **Save**.

# Audit Log

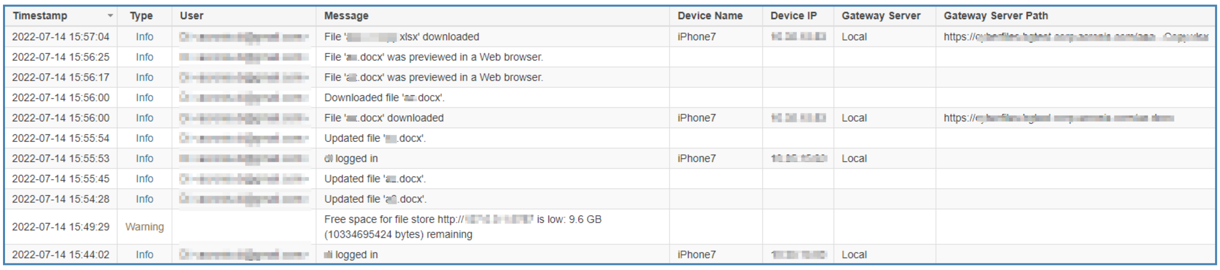
## Log

Here you can see details of recent events which generated a log entry (depending on your purging policy, the time limit might be different).

**Note**

If you wish to configure a Gateway Server's logging and level of logging, please visit Gateway Server Logging.

### *The Log List*



| Timestamp | Type | User | Message | Device Name | Device IP | Gateway Server | Gateway Server Path |
|---|---|---|---|---|---|---|---|
| 2022-07-14 15:57:04 | Info | [redacted] | File '[redacted].xlsx' downloaded | iPhone7 | [redacted] | Local | https://[redacted] |
| 2022-07-14 15:56:25 | Info | [redacted] | File '[redacted].docx' was previewed in a Web browser. | | | | |
| 2022-07-14 15:56:17 | Info | [redacted] | File '[redacted].docx' was previewed in a Web browser. | | | | |
| 2022-07-14 15:56:00 | Info | [redacted] | Downloaded file '[redacted].docx'. | | | | |
| 2022-07-14 15:56:00 | Info | [redacted] | File '[redacted].docx' downloaded | iPhone7 | [redacted] | Local | https://[redacted] |
| 2022-07-14 15:55:54 | Info | [redacted] | Updated file '[redacted].docx'. | | | | |
| 2022-07-14 15:55:53 | Info | [redacted] | [redacted] logged in | iPhone7 | [redacted] | Local | |
| 2022-07-14 15:55:45 | Info | [redacted] | Updated file '[redacted].docx'. | | | | |
| 2022-07-14 15:54:28 | Info | [redacted] | Updated file '[redacted].docx'. | | | | |
| 2022-07-14 15:49:29 | Warning | | Free space for file store http://[redacted] is low: 9.6 GB (10334695424 bytes) remaining | | | | |
| 2022-07-14 15:44:02 | Info | [redacted] | [redacted] logged in | iPhone7 | [redacted] | Local | |

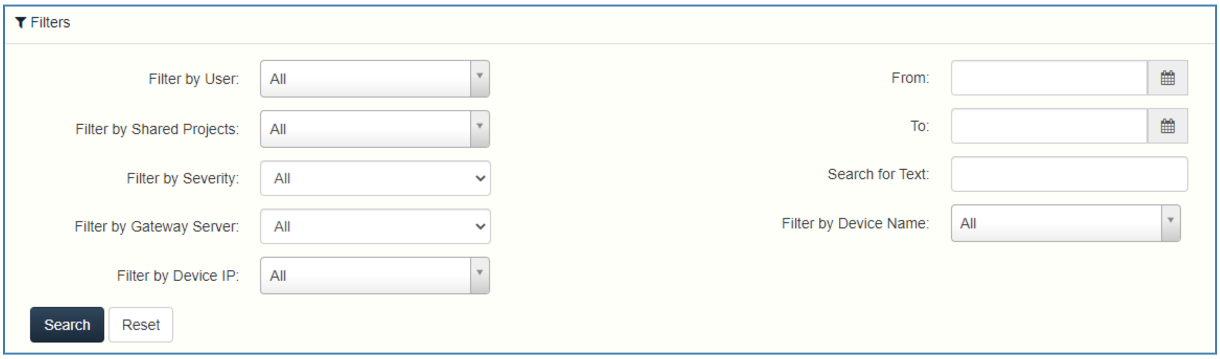
- **Timestamp** – shows the date and time of the event.
- **Type** – shows the level of severity of the event.
- **User** – shows the user account responsible for the event.
- **Message** – shows information on what happened.

If you have enabled Audit logging on a Gateway Server, you will also see the activity of your mobile clients. If you have allowed Desktop and Web clients to access mobile Data Sources, they will also be reflected in the log.

- **Device Name** – name of the connected device.
- **Device IP** – shows the IP address of the connected device.
- **Gateway Server** – shows the name of the Gateway Server to which the device is connected.
- **Gateway Server Path** – shows the path to the data source on that Gateway Server.

### *Filtering the Log List*

You can filter the log entries displayed in the log table. Open and close the filters settings panel by clicking the Filters icon at the top of the page.



Filter by User: All

Filter by Shared Projects: All

Filter by Severity: All

Filter by Gateway Server: All

Filter by Device IP: All

From:

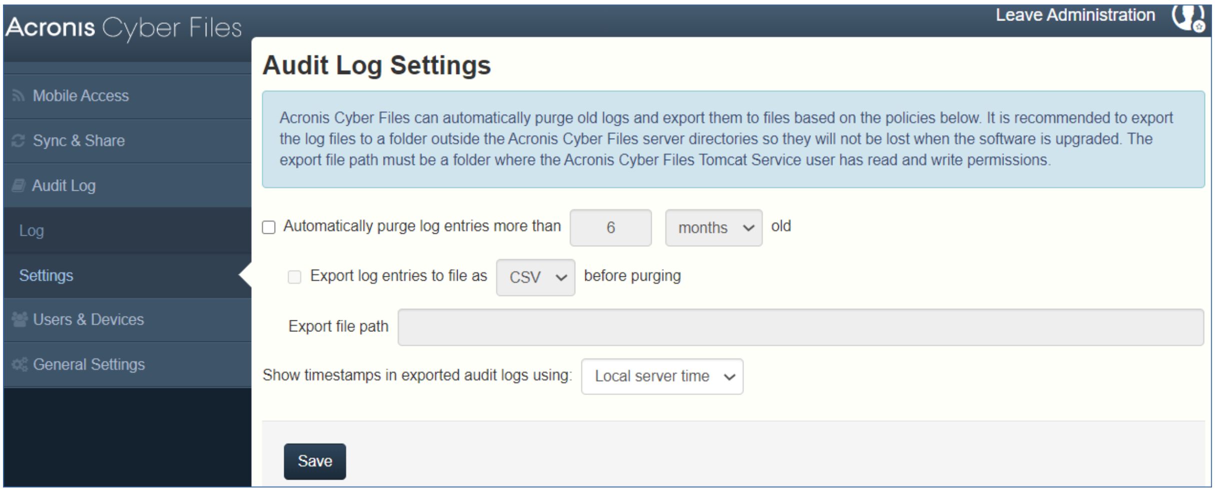
To:

Search for Text:

Filter by Device Name: All

- **Filter by User** – You can select **All**, **No user** or choose one of the available users.
- **Filter by Shared Projects** – You can select **All**, **Not shared** or choose one of the available Shared Projects.
- **Filter by Severity** – The types are **All**, **Info**, **Warning**, **Error** and **Fatal**.
- **Filter by Gateway Server** - You can select **All**, **No server** or choose one of your Gateway Servers.
- **Filter by Device IP** - You can select **All**, **No device IP**, or choose one of the device IPs which have generated a log entry.
- **From/To** – filter by date and time.
- **Search for Text** – filter by log message contents.
- **Filter by Device Name** - You can select **All**, **No device name** or choose one of the device names which have generated a log entry.

## Settings



Audit Log Settings

Acronis Cyber Files can automatically purge old logs and export them to files based on the policies below. It is recommended to export the log files to a folder outside the Acronis Cyber Files server directories so they will not be lost when the software is upgraded. The export file path must be a folder where the Acronis Cyber Files Tomcat Service user has read and write permissions.

☐ Automatically purge log entries more than 6 months old

☐ Export log entries to file as CSV before purging

Export file path

Show timestamps in exported audit logs using: Local server time

Acronis Cyber Files can automatically purge old logs and export them to files based on certain policies.

- **Automatically purge log entries more than X Y old** - When enabled, logs older than a number of days/weeks/months will be automatically purged.
  - **Export log entries to file as X before purging** - When enabled, exports a copy of the logs before purging them in either CSV, TXT or XML. The exporting is automatically set for 03:00

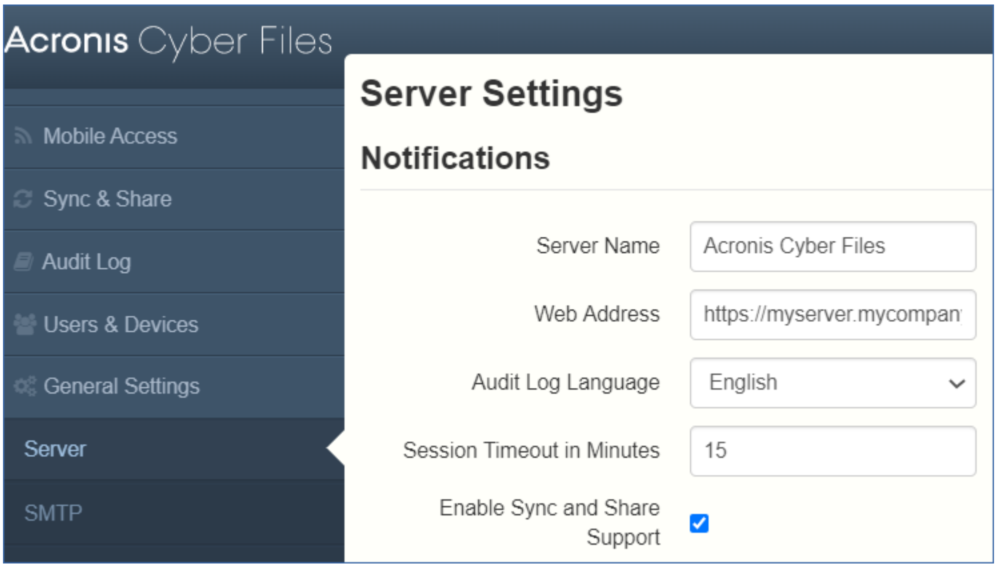
local server time. This setting cannot be modified.

  - **Export file path** - Sets the folder where the exported logs will go.

**Important**
We recommend exporting the logs to a folder that is outside of the Acronis Cyber Files installation folder so that they are not lost on upgrade. The folder you specify must have read/write access for the user account that the Acronis Cyber Files Tomcat service is running as. If you haven't changed the defaults, the account should be the Local System account.

- **Show timestamps in exported audit logs using X** - Lets you choose if your audit logs should use the local server time or another time format (UTC).

# Server



Server Settings

Notifications

Server Name: Acronis Cyber Files

Web Address: https://myserver.mycompan

Audit Log Language: English

Session Timeout in Minutes: 15

Enable Sync and Share Support: ☑

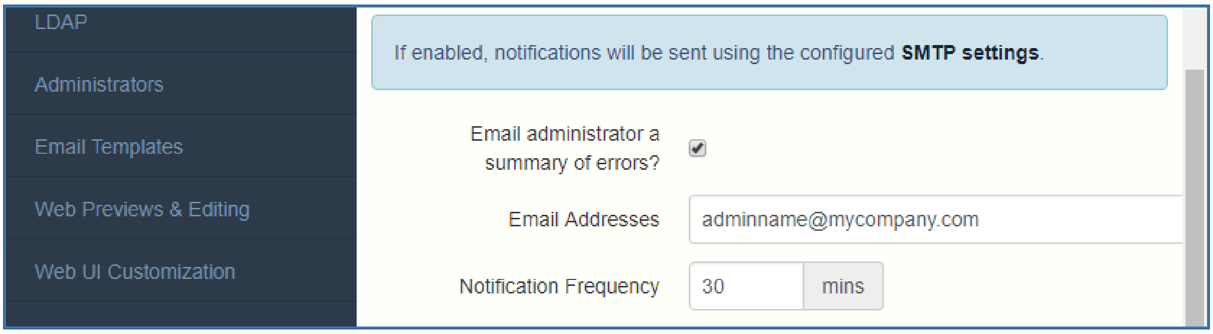
## Server Settings

- **Server Name** – cosmetic server name used as the title of the web site as well as identifying this server in admin notification email messages.
- **Web Address** – specify the root DNS name or IP address where users can access the website (starting with http:// or https://). Do not use 'localhost' here; this address will also be used in email invitation links.
- **Audit Log Language** – select the default language for the Audit Log. The current options are **English, German, French, Japanese, Italian, Spanish, Czesh, Russian, Polish, Korean, Chinese Traditional and Simplified**. The default is **English**.
- **Session timeout in minutes** – sets the amount of time before inactive users are logged out. If no actions are performed for the selected duration, the user will be shown a timed dialog prompting them to take an action or get logged out.

**Note**

If the user has started an upload or download that will take longer than the session timeout, the user will remain logged in until the upload finishes.

- **Enable Sync and Share Support** - this checkbox enables/disables the Sync and Share features.



If enabled, notifications will be sent using the configured **SMTP settings**.

Email administrator a summary of errors? ☑

Email Addresses: adminname@mycompany.com

Notification Frequency: 30 mins

## Notification Settings

- **Email administrator a summary of errors?** – If enabled, a summary of errors will be sent to specified email addresses.
  - **Email Addresses** – one or more email addresses which will receive a summary of errors.
  - **Notification Frequency** – frequency for sending error summaries. Sends emails only if errors are present.

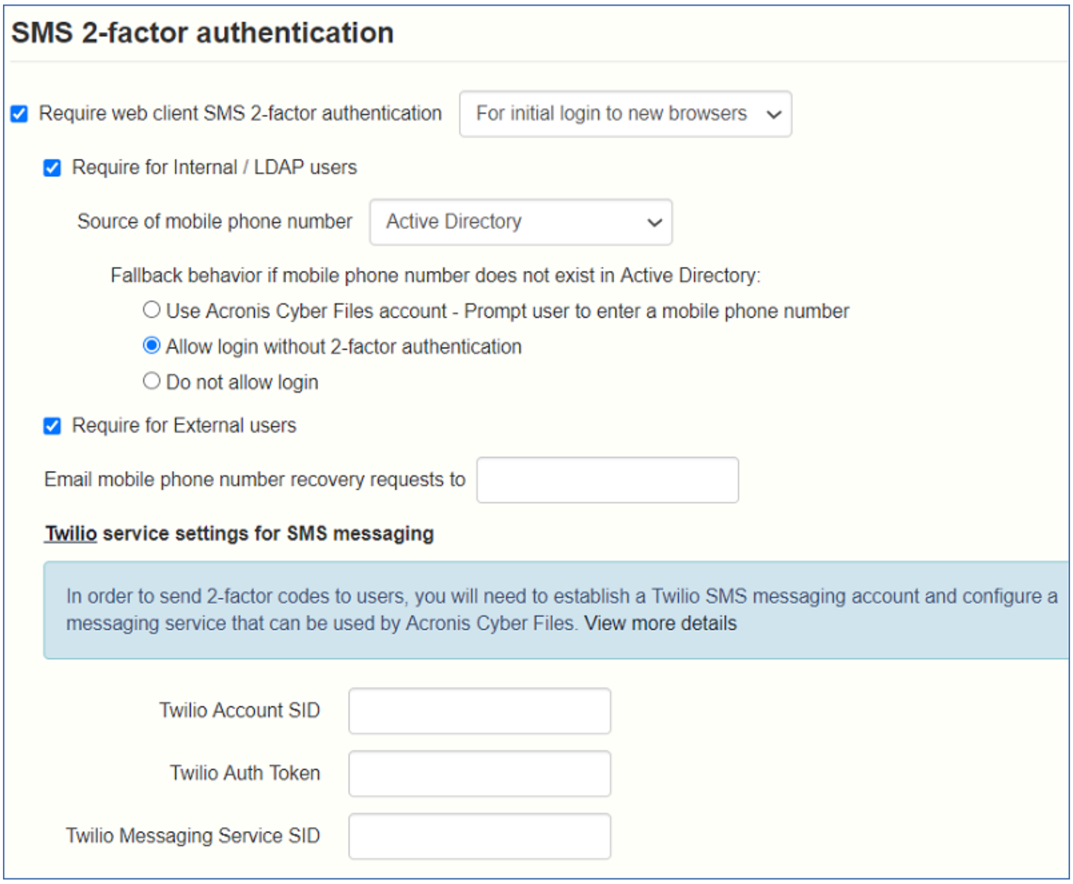
## SMS two-factor Authentication

An option for SMS two-factor authentication for web client login is included. You can use AD mobile phone numbers or user-provided phone numbers. Two-factor authentication can be required for every login, at a specified time interval, or only for login from new browsers.

Sending of SMS codes will require that an account is established with the Twilio SMS messaging service. For more information, please visit https://www.twilio.com/sms. For information on running a trial of Twilio, please visit Twilio Free Trial.

**Note**

You only need 1 account with Twilio, and that account is used by the Acronis Cyber Files Server, you do not need accounts for every user.



SMS 2-factor authentication

☑ Require web client SMS 2-factor authentication: For initial login to new browsers

☑ Require for Internal / LDAP users

Source of mobile phone number: Active Directory

Fallback behavior if mobile phone number does not exist in Active Directory:

○ Use Acronis Cyber Files account - Prompt user to enter a mobile phone number
● Allow login without 2-factor authentication
○ Do not allow login

☑ Require for External users

Email mobile phone number recovery requests to:

Twilio service settings for SMS messaging

In order to send 2-factor codes to users, you will need to establish a Twilio SMS messaging account and configure a messaging service that can be used by Acronis Cyber Files. View more details

Twilio Account SID:

Twilio Auth Token:

Twilio Messaging Service SID:

**Note**

Make sure to choose at least one of the options: **Require for Internal / LDAP** or **Require for External users**.

**Require web client SMS 2-factor authentication:**

- **For initial login to new browsers** - Will require SMS authentication the first time when a new user opens the Acronis Cyber Files Server webpage. Once you enter the verification code and register your browser, you will not be prompted to enter an SMS code again unless you use a different browser or computer.
- **At a specified interval** - Will require SMS authentication at a specified time interval regardless of number of login attempts.
- **For every login** - Will require SMS authentication every time a user tries to connect.

**Twilio settings:**

- **Twilio Account SID** - Your company's Twilio account security identifier (SID).
- **Twilio Auth Token** - Your company's Twilio authentication token.

  Both of these can be found in the Twilio console at https://www.twilio.com/console
- **Twillio Messaging Service SID** - The SID of your Two-factor authentication messaging service. This SID is located at https://www.twilio.com/console/sms/dashboard. If you have multiple Twilio messaging servcies, use only the SID of the one you will use for two-factor authentication. When

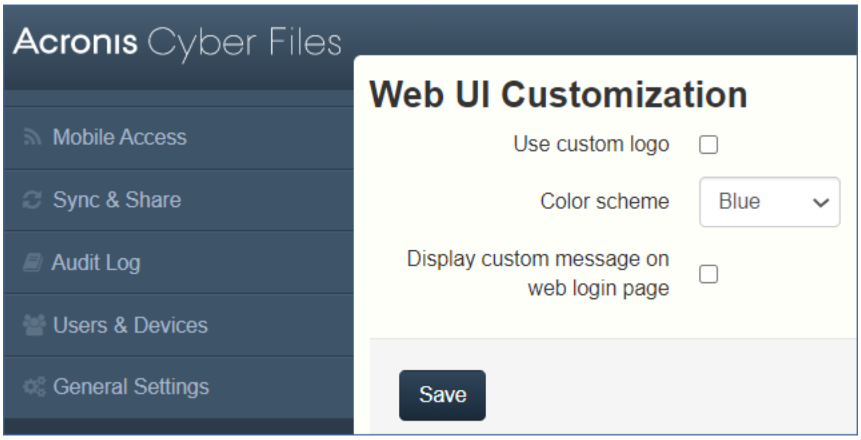
creating a Twilio messaging service, for **Use Case** leave it blank or select two-factor authentication.

**Note**
In the Twilio console, you will have to select the countries that are allowed to use the messaging service. Simply select the checkboxes for the desired countries.

# Web UI Customization

You can easily customize the logos and color scheme of your Acronis Cyber Files server.

**Note**
You can also make these customizations through the Acronis Cyber Files API, for more information check out Web UI API customization.



Web UI Customization

Use custom logo □

Color scheme: Blue

Display custom message on web login page □

Save

## Using custom logos

1. Open the AcronisCyber Files web interface and login as an administrator.
2. Navigate to **General Settings** > **Web UI Customization**.
3. Select the **Use Custom Logo** checkbox.
4. Choose the files for the logos you wish to change and make sure they are selected from the drop-down menu.

   **Note**
   The image size limits are written in brackets **()**.

5. Click **Save**.

## Using a custom welcome message

1. Open the AcronisCyber Files web interface and login as an administrator.
2. Navigate to **General Settings** -> **Web UI Customization**.

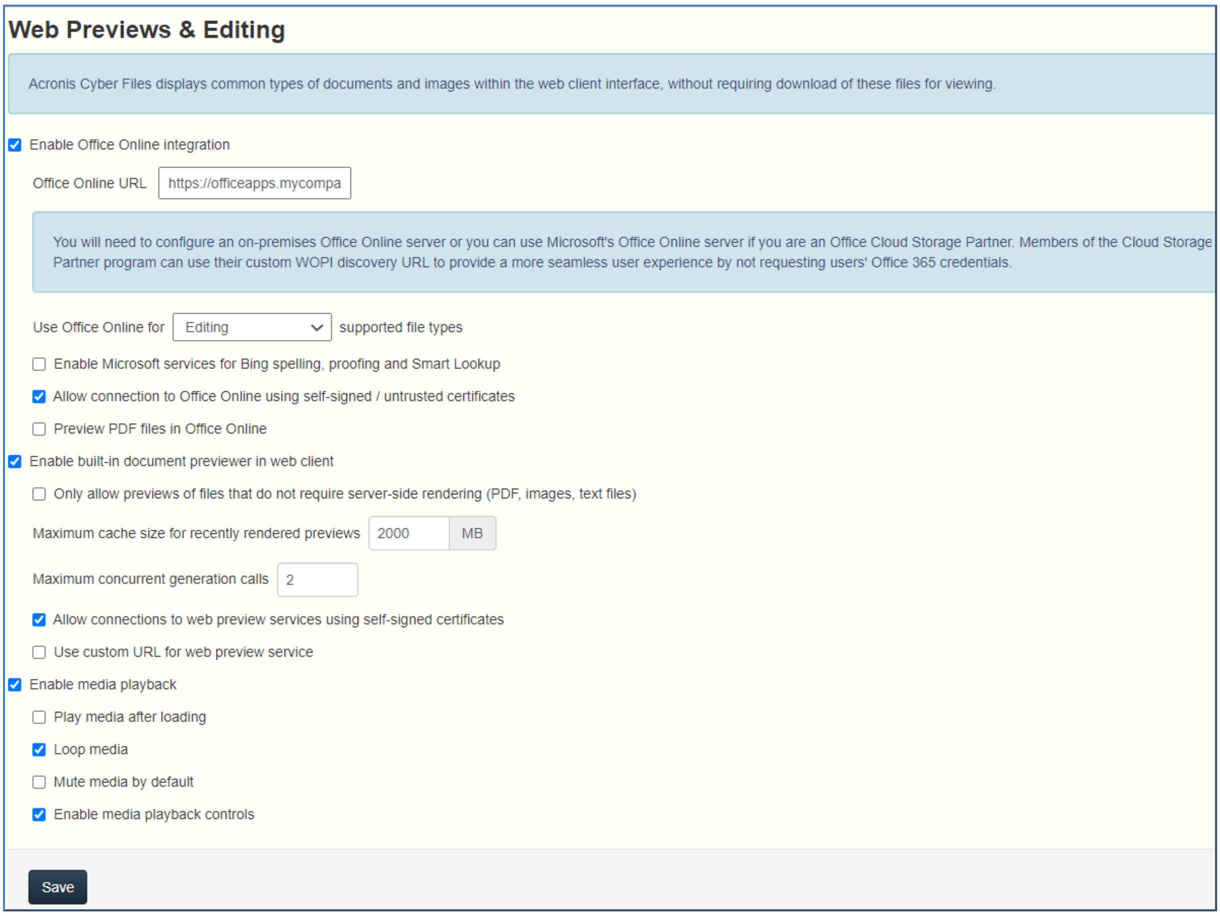
3. Select the **Display custom message on web login page** checkbox.
4. Enter the desired message in the text box and click **Save**.

## Using color schemes

1. Open the AcronisCyber Files web interface and login as an administrator.
2. Navigate to **General Settings** -> **Web UI Customization**
3. Click on the **Color Scheme** drop-down and pick a scheme.
4. Click **Save**.

# Web Previews & Editing

Acronis Cyber Files can preview and edit common types of documents and images within the web client interface, without downloading these files.



Web Previews & Editing

Acronis Cyber Files displays common types of documents and images within the web client interface, without requiring download of these files for viewing.

☑ Enable Office Online integration

Office Online URL: https://officeapps.mycompa

You will need to configure an on-premises Office Online server or you can use Microsoft's Office Online server if you are an Office Cloud Storage Partner. Members of the Cloud Storage Partner program can use their custom WOPI discovery URL to provide a more seamless user experience by not requesting users' Office 365 credentials.

Use Office Online for: Editing supported file types

☐ Enable Microsoft services for Bing spelling, proofing and Smart Lookup

☑ Allow connection to Office Online using self-signed / untrusted certificates

☐ Preview PDF files in Office Online

☑ Enable built-in document previewer in web client

☐ Only allow previews of files that do not require server-side rendering (PDF, images, text files)

Maximum cache size for recently rendered previews: 2000 MB

Maximum concurrent generation calls: 2

☑ Allow connections to web preview services using self-signed certificates

☐ Use custom URL for web preview service

☑ Enable media playback

☐ Play media after loading

☑ Loop media

☐ Mute media by default

☑ Enable media playback controls

- **Enable Office Online integration** - Enables Office Online integrated functionality.
  - **Office Online URL** - Enter your Office Online's WOPI discovery URL. For on-premises Acronis Cyber Files installations, you must be using an on-premises Office Online setup to be able to provide this URL. Microsoft's Office Online cloud service is limited to service provider use and is not publicly accessible without special certification and allow listing.

- ◦ **Use Office Online for** - **Editing** allows you to edit Microsoft Office files - **DOCX**, **PPTX**, **XSLX**- while **Viewing and Editing** allows you to edit the mentioned files while also being able to preview **DOC**, **XLS** and **PPT** files as well. If this setting is disabled, all Office files and PDF files will open in Acronis Cyber Files internal previewer.
  - **Enable Microsoft services for Bing spelling, proofing and Smart Lookup** - Uses Microsoft's Bing services for spell-check capabilities.
  - **Allow connection to Office Online using self-signed / untrusted certificates** - When enabled, users can access Office Online servers which use untrusted certificates.
  - **Preview PDF files in Office Online** - When enabled, users will preview PDF files in Office Online, given that **Use Office Online for** is set to **Viewing and Editing**. In all other cases PDF files will be previewed in Acronis Cyber Files internal previewer.

- **Enable built-in document previewer in web client** - Enables web previewing.

  **Note**

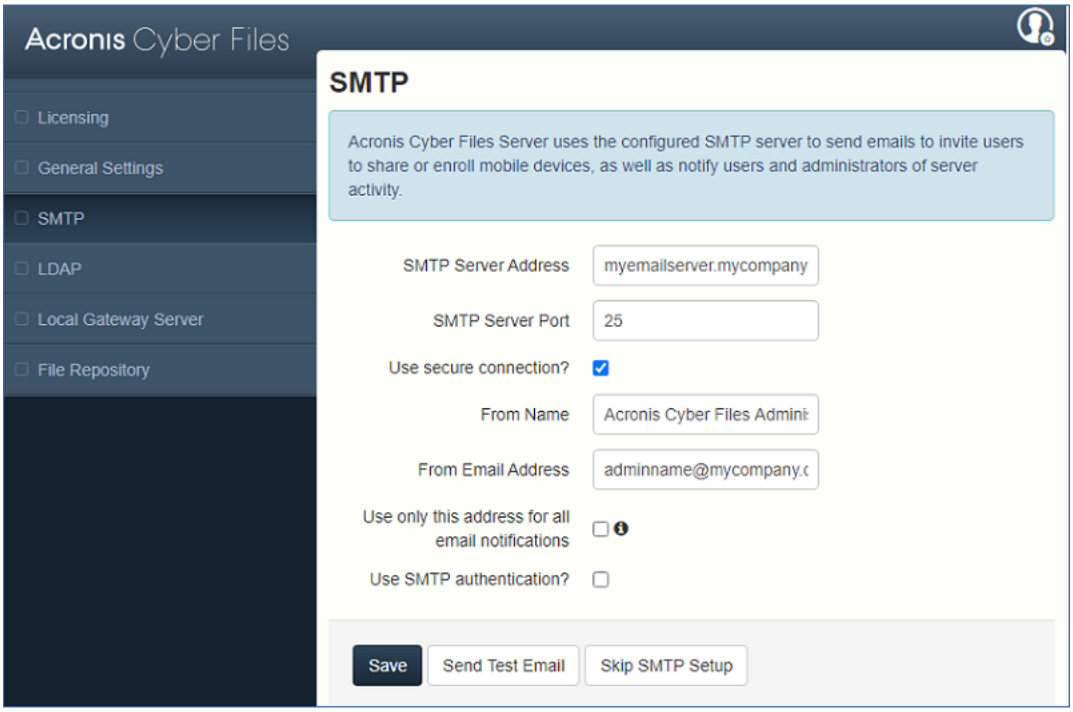
  Password-protected files do not have thumbnails and cannot be previewed.

  - **Only allow previews of files that do not require server-side rendering (PDF, images, text files)** - Decreases the load caused by web previews by only previewing files that do not require additional rendering. These files are PDFs, Images and simple text files.
  - **Maximum cache size for recently rendered previews** - Sets the maximum size of the cache that is stored when you preview a file. This greatly increases the speed at which files open for preview if they have been recently opened.
  - **Maximum concurrent generation calls** - Sets the maximum number of concurrent preview generation requests.
  - **Allow connections to web preview services using self-signed certificates** - Allows you to contact web preview services that are using self-signed certificates. These are other Acronis Cyber Files Tomcat services.
  - **Use custom URL for web preview service** - Enable if you have multiple Acronis Cyber Files servers and you wish to specify which one should handle the web previewing.

- **Enable media playback** - Allows you to control the default media playback settings, enabling video preview in a browser, without the necessity to download the whole file.
  - **Play media after loading** - Starts the video automatically, without having to click the **Play** button.
  - **Loop media** - The video restarts playing automatically each time.
  - **Mute media by default** - Specifies whether the audio will play, along with the video. If selected, the video will be soundless.
  - **Enable media playback controls** - Allows usage of buttons to control playing the video - **Play/Pause**, **Volume +/-**, etc.

# SMTP

Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to a shared resource or enroll mobile devices, as well as notify users and administrators of server activity.



SMTP

Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to share or enroll mobile devices, as well as notify users and administrators of server activity.

SMTP Server Address: myemailserver.mycompany

SMTP Server Port: 25

Use secure connection? ☑

From Name: Acronis Cyber Files Admini

From Email Address: adminname@mycompany.c

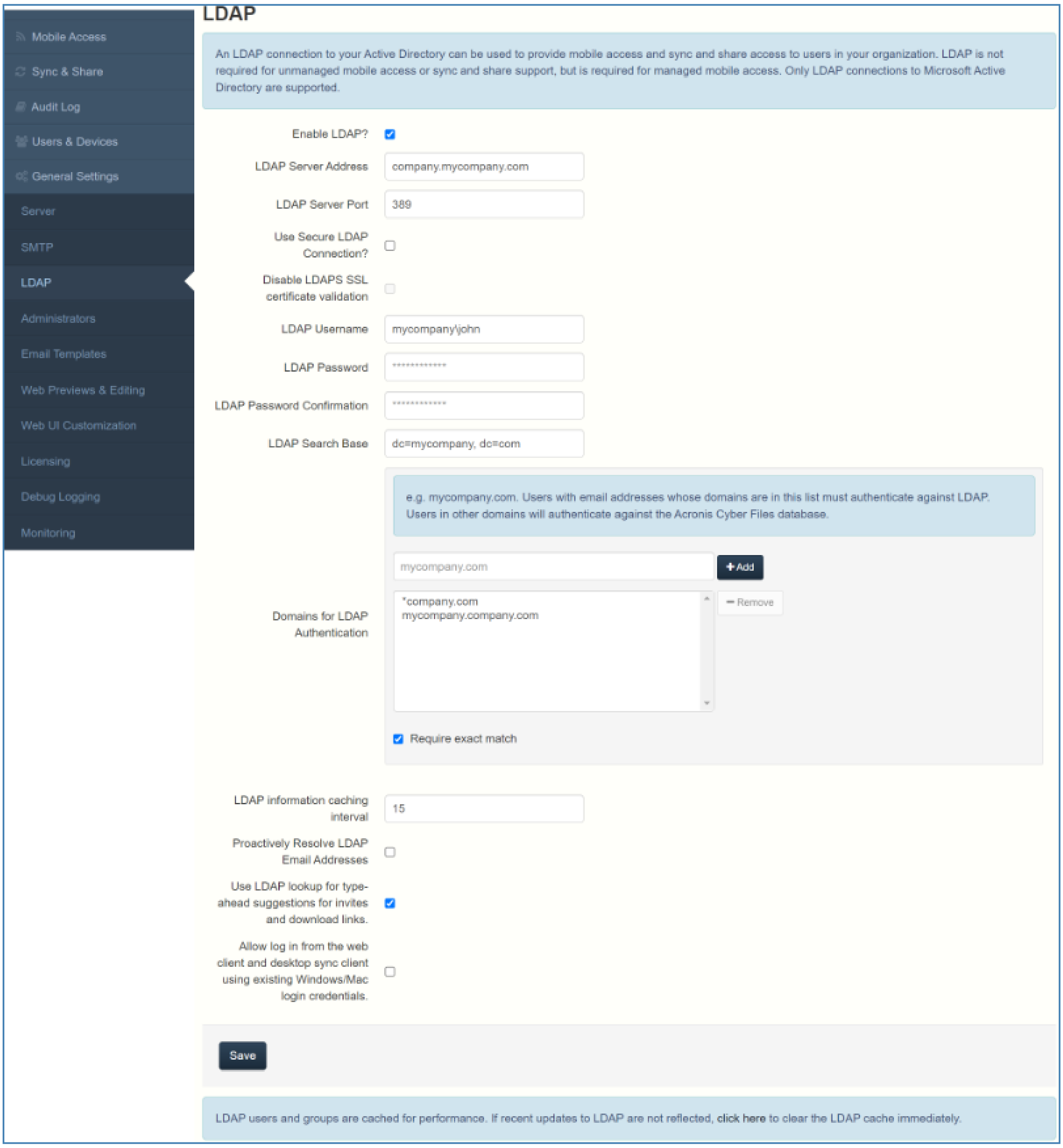
Use only this address for all email notifications ☐

Use SMTP authentication? ☐

- **SMTP Server Address** – Enter the DNS name of an SMTP server that will be used to send email invitations to your users.
- **SMTP Server Port** – Enter your SMTP server port. This setting defaults to port 587.
- **Use secure connection?** – This setting allows a secure SSL connection to your SMTP server. It is enabled by default. Uncheck the box to disable the secure SMTP.
- **From Name** – This is the username that appears in the "From" line of the emails sent by the server.
- **From Email Address** – This is the email address that appears in the "From" line of the emails sent by the server.
- **Use only this address for all email notifications** – When enabled, Acronis Cyber Files will send all email notifications only from this email address.
- **Use SMTP authentication?** – Enable this option to connect with an SMTP username and password or disable it to connect without them.
  - **SMTP username** – Enter a username for SMTP authentication.
  - **SMTP password** – Enter a password for SMTP authentication.
  - **SMTP password confirmation** – Re-enter the SMTP password to confirm it.
- **Send Test Email** – Sends an email to ensure all configurations are working as expected.

# LDAP

Microsoft Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Other Active Directory products (i.e. Open Directory) are not supported at this time.



LDAP

An LDAP connection to your Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Only LDAP connections to Microsoft Active Directory are supported.

| | |
|---|---|
| Enable LDAP? | ☑ |
| LDAP Server Address | company.mycompany.com |
| LDAP Server Port | 389 |
| Use Secure LDAP Connection? | □ |
| Disable LDAPS SSL certificate validation | □ |
| LDAP Username | mycompany\john |
| LDAP Password | ************ |
| LDAP Password Confirmation | ************ |
| LDAP Search Base | dc=mycompany, dc=com |
| Domains for LDAP Authentication | e.g. mycompany.com. Users with email addresses whose domains are in this list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.<br>mycompany.com + Add<br>*company.com<br>mycompany.company.com<br>− Remove<br>☑ Require exact match |
| LDAP information caching interval | 15 |
| Proactively Resolve LDAP Email Addresses | □ |
| Use LDAP lookup for type-ahead suggestions for invites and download links. | ☑ |
| Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials. | □ |

Save

LDAP users and groups are cached for performance. If recent updates to LDAP are not reflected, click here to clear the LDAP cache immediately.

- **Enable LDAP?** - If enabled, you will be able to configure LDAP.
  - **LDAP server address** - enter the DNS name or IP address of the Active Directory server you would like to use for regulating access.

- **LDAP server port** - the default Active Directory port is 389. This will likely not need to be modified.

  **Note**
  If you're supporting multiple domains you should probably use the global catalog port.

- **Use secure LDAP connection?** - disabled by default. Check the box to connect to Active Directory using secure LDAP (also known as LDAPS).

  **Note**
  When enabling the LDAP secure connection feature, Acronis Cyber Files requires the fully qualified domain name of the LDAP server to be present in the certificate either as a Common Name (CN) or as a Subject Alternative Name (SAN).

- **Disable LDAPS SSL certificate validation -** check this box if you don't want to verify the LDAPS certificate when connecting to an LDAP server. This is convenient when the LDAP server certificate is not trusted by a public certificate authority.

  Since version 8.7.0, this option is disabled by default on fresh installs (LDAPS certificates will be validated). However, it is enabled by default upon upgrade from versions lower than 8.7.0 (LDAPS certificates will not be validated). The existing setting will be preserved upon upgrade from version 8.7.0 and higher.

  **Note**
  Do not disable this option if you don't know the exact type of certificate you are using or if your LDAPS certificates are not issued by a public trusted authority.

- **LDAP username / password** - this login credentials will be used for all LDAP queries. Ask your AD administrator to find out if you have designated service accounts that should be used.
- **LDAP Search Base** - enter the root level you would like searches for users and groups to begin. If you would like to search your entire domain, enter "dc=domainname, dc=domainsuffix".
- **Domains for LDAP authentication** - users with email addresses whose domains are in this comma-delimited list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.

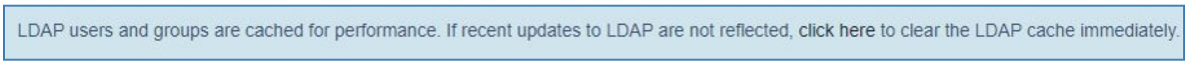
  **Note**
  Internal domains are not supported here. Only email domains with public names are allowed.

  - **Require exact match** - When enabled, only users from the domains entered in **Domains for LDAP authentication** will be treated as LDAP users. Users that are members of other domains and sub-domains will be treated as Ad-hoc.
- **LDAP information caching interval** - sets the interval in which Acronis Cyber Files is caching the Active Directory structure.

- **Proactively resolve LDAP email addresses** - When this setting is enabled, Acronis Cyber Files will search Active Directory for the user with the matching email address on login and invite events. This allows users to log in with their email addresses and get immediate feedback on invitations, but may be slow to execute if the LDAP catalog is very large. If you encounter any performance problems or slow response on authentication or invite, uncheck this setting.
- **Use LDAP lookup for type-ahead suggestions for invites and download links -** LDAP lookup for type-ahead will search LDAP for users with matching email addresses. This lookup may be slow against large LDAP catalogs. If you encounter performance problems with type-ahead, uncheck this setting.
- **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials.** Enables all valid LDAP users to login to the web interface and desktop client without having to enter their credentials. See Configuring Single-Sign-on.

***Clearing LDAP Cache***

All recent LDAP changes are propagated to the LDAP server. However, there is a slight delay in updating the LDAP cache held in memory. Click the message bar at the bottom of the page to clear the LDAP cache, which will make LDAP changes available instantaneously.

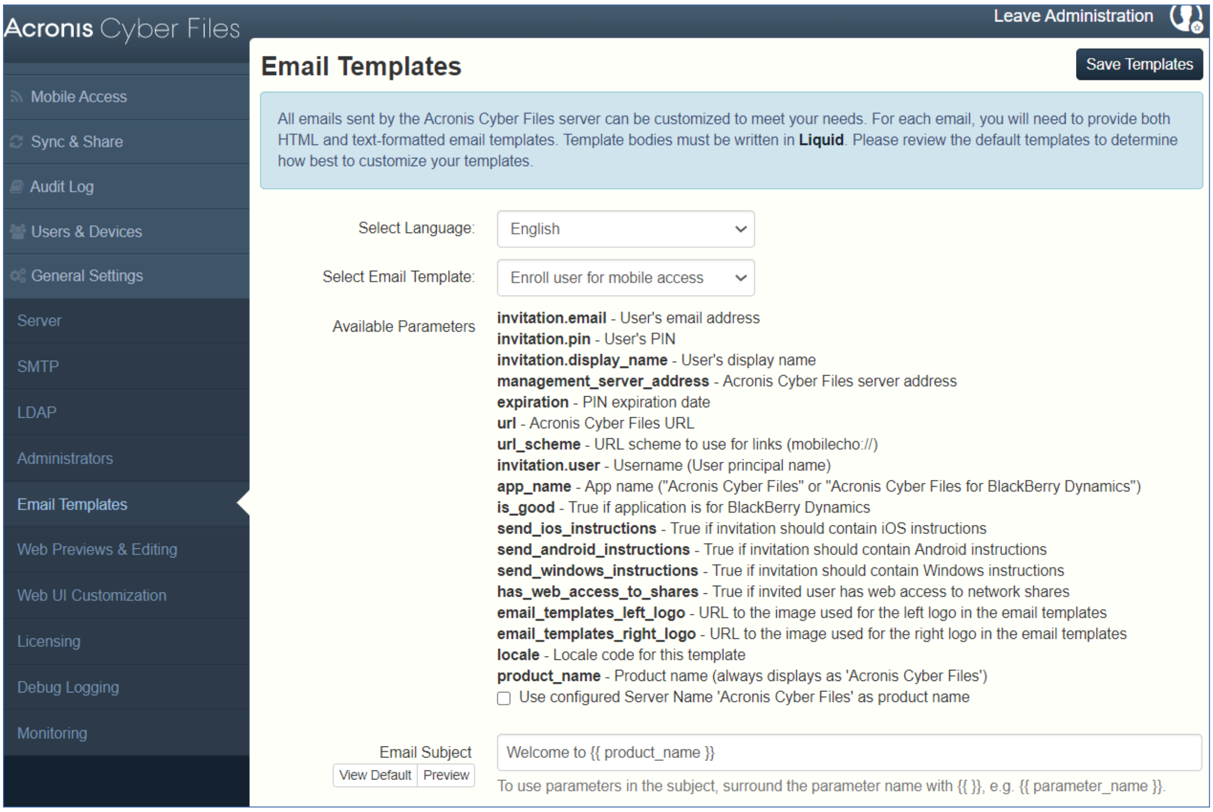


LDAP users and groups are cached for performance. If recent updates to LDAP are not reflected, click here to clear the LDAP cache immediately.

# Email Templates

Acronis Cyber Files makes extensive use of email messages to provide dynamic information to users and administrators. Each event has an HTML and text associated template. You can click the Email Template pull down menu to select an event and edit both templates.

All emails sent by the Cyber Files server can be customized to meet your needs. For each email, you will need to provide both HTML and text-formatted email templates. Template bodies must be written in Liquid. Please review the default templates to determine how best to customize your templates.



Email Templates

All emails sent by the Acronis Cyber Files server can be customized to meet your needs. For each email, you will need to provide both HTML and text-formatted email templates. Template bodies must be written in **Liquid**. Please review the default templates to determine how best to customize your templates.

Select Language: English

Select Email Template: Enroll user for mobile access

Available Parameters

**invitation.email** - User's email address
**invitation.pin** - User's PIN
**invitation.display_name** - User's display name
**management_server_address** - Acronis Cyber Files server address
**expiration** - PIN expiration date
**url** - Acronis Cyber Files URL
**url_scheme** - URL scheme to use for links (mobilecho://)
**invitation.user** - Username (User principal name)
**app_name** - App name ("Acronis Cyber Files" or "Acronis Cyber Files for BlackBerry Dynamics")
**is_good** - True if application is for BlackBerry Dynamics
**send_ios_instructions** - True if invitation should contain iOS instructions
**send_android_instructions** - True if invitation should contain Android instructions
**send_windows_instructions** - True if invitation should contain Windows instructions
**has_web_access_to_shares** - True if invited user has web access to network shares
**email_templates_left_logo** - URL to the image used for the left logo in the email templates
**email_templates_right_logo** - URL to the image used for the right logo in the email templates
**locale** - Locale code for this template
**product_name** - Product name (always displays as 'Acronis Cyber Files')
☐ Use configured Server Name 'Acronis Cyber Files' as product name

Email Subject: Welcome to {{ product_name }}

To use parameters in the subject, surround the parameter name with {{ }}, e.g. {{ parameter_name }}.

**Note**

As of Acronis Access Advanced version 7.3, Liquid is the default template markup. If you have custom templates written in ERB, then ERB will be the default template markup for your server even if you upgrade.

**Note**

If you are using custom images in the email templates, these images should be hosted and must be somewhere accessible on the internet.

- **Select Language** - Select the default language of the invitation emails.

  **Note**

  When sending an enrollment invitation or an invitation to a share or sharing a single file, you can select another language in the invitation dialog.

- **Select Email Template** - Select the template you want to view or edit. Each template is used for a specific event (e.g. Enrolling a user for mobile access, resetting a user's password).

  **Note**

  Custom templates are **not** automatically updated when you update Cyber Files. If you want to use these updates introduced by Acronis, you must manually implement them in your custom templates. You will have to do this for all languages that you support and use.

- **Available Parameters** - The available parameters are different for each template and will change based on the template you've selected.
- **Email Subject** - The subject of the invitation email.
  Pressing the **View Default** link will show you the default subject for that language and email template.
- **HTML Email template** - Shows the HTML-coded email template. If you enter valid HTML code, it will be displayed.
  Pressing the **Preview** button will show you a preview of how your current template looks.
- **Text Email template** - Shows the text-based email template.
  Pressing the **Preview** button will show you a preview of how your current template looks.

**Note**
Always remember to click the **Save Templates** button when you finished modifying your templates.

**Note**
Editing a template in English does not edit the other languages. You need to edit each template separately for each language.

Notice that templates allow you to include dynamic information by including parameters. When a message is delivered these parameters are replaced with the appropriate data.

Different events have different available parameters.

**Note**
Pressing the **View Default** button will show you the default template.

# Licensing

You will see a list of all your licenses.

- **License** - Type of the license (Trial, subscription, etc).
- **Sync & Share Licensed Client Usage** - Currently used Sync & Share LDAP user licenses.
- **Sync & Share Free Client Usage** - Currently used Sync & Share free external user licenses.
- **Mobile Access Client Usage** - Currently used Mobile Client licenses.

## Adding a new license

1. Copy your license key.
2. Paste it in the **Add license key** field.
3. Read and accept the licensing agreement by selecting the checkbox.
4. Click **Add License**.

**Note**
If your licenses have the same unique ID, the number of allowed users will be summed.

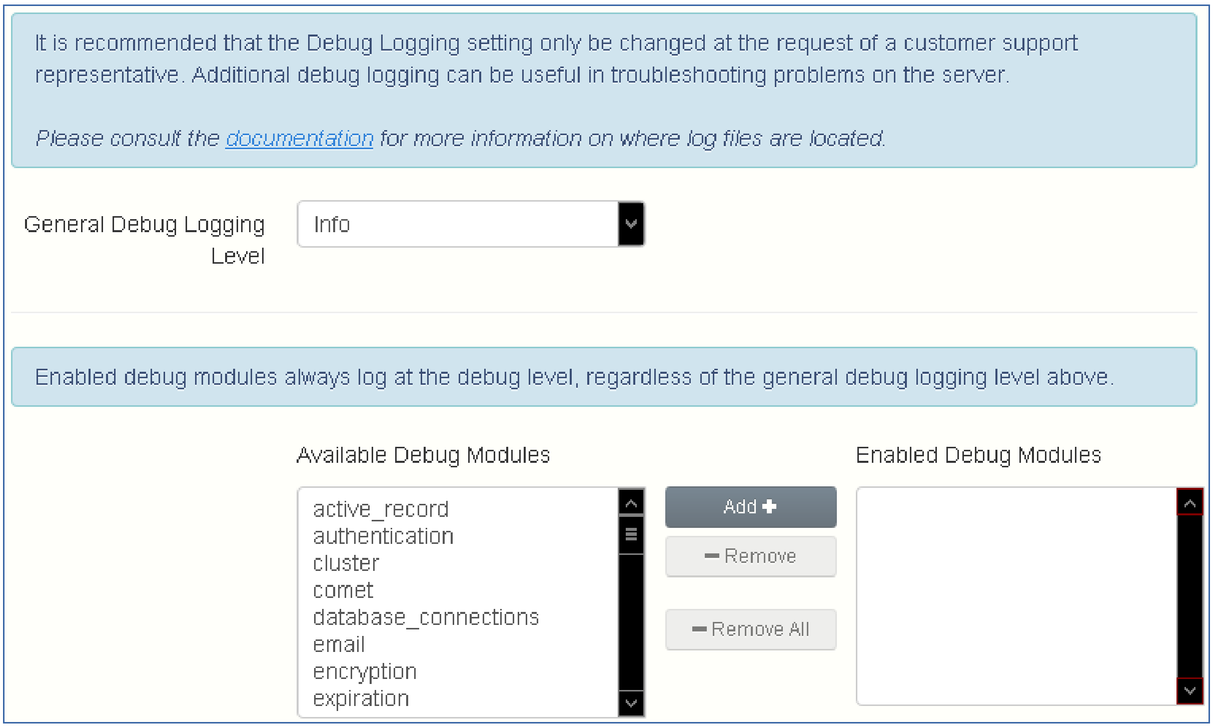
## Adding a new license for a Gateway Server is not necessary

Starting from Acronis Access version 6.0, the Acronis Cyber Files server and the Gateway servers share the same license. This means that you will not have to manually add licenses to your Gateway servers.

# Debug Logging

Settings in this page are designed to enable extended logging information that might be useful when configuring and troubleshooting Acronis Cyber Files. It is recommended that these settings only be changed at the request of a customer support representative. Additional debug logging can be useful in troubleshooting problems on the server.

**Note**
For information on enabling/disabling debug logging for a specific Gateway Server visit the Editing Gateway Servers article.



It is recommended that the Debug Logging setting only be changed at the request of a customer support representative. Additional debug logging can be useful in troubleshooting problems on the server.

*Please consult the documentation for more information on where log files are located.*

General Debug Logging Level: Info

Enabled debug modules always log at the debug level, regardless of the general debug logging level above.

As of version 7.0 of the Acronis Cyber Files Server, the **exceptions** module has been removed from the list of available modules and is enabled at all times by default. Users that have upgraded from a previous version of Acronis Cyber Files may still see the **exceptions** module in the list. Once you make a change to the logging options and press **Save**, it will disappear.

**Warning!**
These settings should not be used during normal operation and production conditions.

- **General Debug Logging Level** - Sets the main level you want to be logged (Info, Warnings, Fatal errors etc.)

  **Note**
  Enabled debug modules always log at the debug level, regardless of the general debug logging level above.

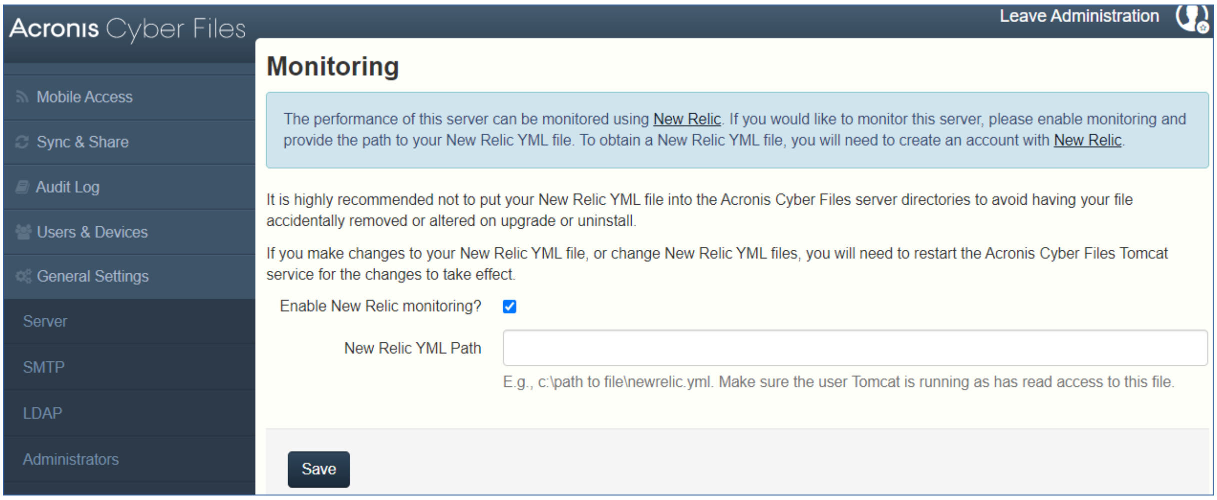
- **Available Debug Modules** - Shows a list of available modules.
- **Enabled Debug Modules** - Shows the active modules.

**Note**
In the cases where the product was updated and not a new installation, the log files will be in `C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs`.

**Note**
On a clean installation of Acronis Cyber Files, the log files will be in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.42\logs`

# Monitoring

The performance of this server can be monitored using New Relic. If you would like to monitor this server, please enable monitoring and provide the path to your New Relic YML file. To obtain a New Relic YML file, you will need to create an account with New Relic.



## Monitoring

The performance of this server can be monitored using New Relic. If you would like to monitor this server, please enable monitoring and provide the path to your New Relic YML file. To obtain a New Relic YML file, you will need to create an account with New Relic.

It is highly recommended not to put your New Relic YML file into the Acronis Cyber Files server directories to avoid having your file accidentally removed or altered on upgrade or uninstall.

If you make changes to your New Relic YML file, or change New Relic YML files, you will need to restart the Acronis Cyber Files Tomcat service for the changes to take effect.

Enable New Relic monitoring? ☑

New Relic YML Path

E.g., c:\path to file\newrelic.yml. Make sure the user Tomcat is running as has read access to this file.

**Note**
It is highly recommended not to put your New Relic YML file into the Acronis Cyber Files server directories to avoid having your file accidentally removed or altered on upgrade or uninstall.

**Note**

If you make changes to your New Relic YML file, or change New Relic YML files, you will need to restart the Acronis Cyber Files Tomcat service for the changes to take effect.

**Enable New Relic monitoring?** - If enabled, you are required to provide a path to the **New Relic** configuration file (newrelic.yml)

## Installing New Relic. Monitoring Acronis Cyber Files with New Relic

# Monitoring Acronis Cyber Files with New Relic

This type of installation will let you monitor your Acronis Cyber Files Server application, not the actual computer on which it is installed.

1. Open http://newrelic.com/ and create a New Relic account or log in with an existing account. Once that is done, proceed with your Application configuration.
2. For Application Type select **APM**.
3. For platform, select **Ruby**.
4. Download the New Relic script shown in Step 3 of the New Relic Starting Guide (newrelic.yml).
5. Open your Acronis Cyber Files web console.
6. Navigate to **Settings** -> **Monitoring**.
7. Enter the path to the newrelic.yml including the extension (e.g `C:\software\newrelic.yml`). We recommend you put this file in a folder outside of the Acronis Cyber Files folder so that it will not be removed or altered on upgrade or uninstall.
8. Click **Save** and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
9. If more than 10 minutes pass, restart your Acronis Cyber Files Tomcat service and wait a couple of minutes. The button should be active now.
10. You should be able to monitor you Acronis Cyber Files server via the New Relic website.

**Note**

All the information the Acronis Cyber Files server logs about trying to connect to New Relic and set up monitoring is in a file called **newrelic_agent.log** found here - `C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs`. If you have any problems, you can find information in the log file.

**Note**

There is frequently a warning/error that starts like this:

**WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which** That's a side effect of the code used to patch another New Relic bug and is innocuous.

**If you want to monitor the actual computer as well**

1. Open http://newrelic.com/ and log in with your account.
2. Press Servers and download the New Relic installer for your operating system.
3. Install the New Relic monitor on your server.
4. The New Relic server monitor requires Microsoft .NET Framework 4. The link the New Relic installer takes you to is only for the Microsoft .NET Framework 4 Client Profile. You will need to go to the Microsoft Download Center and download the entire .NET 4 Framework from the internet and install it before running the New Relic Server Monitor installer.
5. Wait until New Relic detects your server.

# Maintenance Tasks

**Note**
To backup all of Acronis Cyber Files's elements and as part of your best practices and backup procedures, you may want to read the Disaster Recovery guidelines article.

## Disaster Recovery guidelines

High availability and fast recovery is of extreme importance for mission critical applications like Acronis Cyber Files. Due to planned or unplanned circumstances ranging from local hardware failures to network disruptions to maintenance tasks, it may be required to provision the means for restoring Acronis Cyber Files to a working state in a very short period of time.

### Introduction:

For mission critical applications like Acronis Cyber Files, high availability is of extreme importance. Due to various circumstances ranging from local hardware failures to network disruptions to maintenance tasks, it may be required to provision the means for restoring Acronis Cyber Files to a working state in a very short period of time.

There are different ways to implement disaster recovery, including backup-restore, imaging, virtualization and clustering. We will describe the backup-restore approach in the following sections.

### Description of the Acronis Cyber Files elements:

Acronis Cyber Files is a solution composed of several discrete but interconnected elements:

**Acronis Cyber Files Gateway Server**

**Note**
Normally located here: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server`

**Acronis Cyber Files Server**

**Note**
Normally located here: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`

**Acronis Cyber Files Configuration Utility**

**Note**
Normally located here: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Configuration Utility`

**File Store**

The location of the **File Store** is set during the installation when you first use the **Configuration Utility.**

**Note**
The FileStore structure contains user files and folders in encrypted form. This structure can be copied or backed up using any standard file copy tool (robocopy, xtree). Normally this structure should be located in a high availability network volume or NAS so the location may differ from the default.

**PostGreSQL** database. This is a discrete element running as a Windows service, installed and used by Acronis Cyber Files. The Acronis Cyber Files database is one of the most critical elements because it maintains all configurations, relationships between users and files, and file metadata.

All those components are needed in order to build a working instance of Acronis Cyber Files.

## Resources needed to implement a fast recovery process

The resources needed to fulfill the disaster recovery process are:

- Appropriate hardware to host the operating system, application and its data. The hardware must meet the system and software requirements for the application.
- A backup and restore process in place to ensure all software and data elements are available at the time the switch is needed.
- Network connectivity, including internal and external firewall and routing rules that permit users to access the new node with no or minimal need to change client side settings.
- Network access for Acronis Cyber Files to contact an Active Directory domain controller and SMTP server.
- Fast or automated DNS switching ability to redirect incoming request to the secondary node.

## The process

### Backup Setup

The recommended approach to provide a safe and fast recovery scenario can be described like this:

1. Have an installation of Acronis Cyber Files, including all elements in the secondary, restore, node. If this is not possible, a full (source) machine backup or image is a good alternative. In virtualized environments, periodic snapshots prove to be effective and inexpensive.
2. Backup the Acronis Cyber Files server software suite (all elements mentioned above, including the entire Apache Software branch) regularly. Use any standard, corporate class backup solution for the task.
3. Backup the FileStore as frequently as possible. A standard backup solution can be used, but an automated differential copy tool is a good and sometimes preferred alternative due to the amount of data involved. A differential copy minimizes the time this operation takes by updating what is different between the source and target FileStores.

4. Backup the Acronis Cyber Files database as frequently as possible. This is performed by an automated database dump script triggered by Windows Task Scheduler. The database dump should then be backed up by a standard backup tool.

**Recovery**

Provided the conditions described in the section above have been met and implemented, the process to bring online the backup resources is relatively simple:

1. Boot up the recovery node. Adjust any network configuration like IP Address, Host Name if needed. Test Active Directory connectivity and SMTP access,
2. If needed restore the most recent Acronis Cyber Files software suite backup.
3. Verify that Tomcat is not running (Windows Control Panel/Services).
4. If needed, restore the FileStore. Make sure the relative location of the FileStore is the same as it was in the source computer. If this is not the case, the location will need to be adjusted by using the Configuration Utility.
5. Verify that the PostgreSQL service is running (Windows Control Panel/Services).
6. Restore the Acronis Cyber Files database.
7. Start the Acronis Cyber Files Tomcat service.
8. Migrate DNS to point to the new node.
9. Verify Active Directory and SMTP are working.

# Best practices

***1. Backup your database regularly***

Keeping your database backed-up is one of the most important aspects of managing Acronis Cyber Files. The Backup process can be entirely automated to help you keep your backups up to date.

**Deployments with very large Acronis Cyber Files server databases may want to use a different backup and restore method than the one provided.**

Deployments with databases of several gigabytes and more may require some additional configurations during the **Backup&Restore** process to speed it up or otherwise improve it. For assistance with your specific configuration, please contact our technical support at http://www.acronis.com/en-us/mobilitysupport/ for help and instructions.

***2. We recommend that very large deployments 'vacuum' and 'analyze' their database(s) monthly***

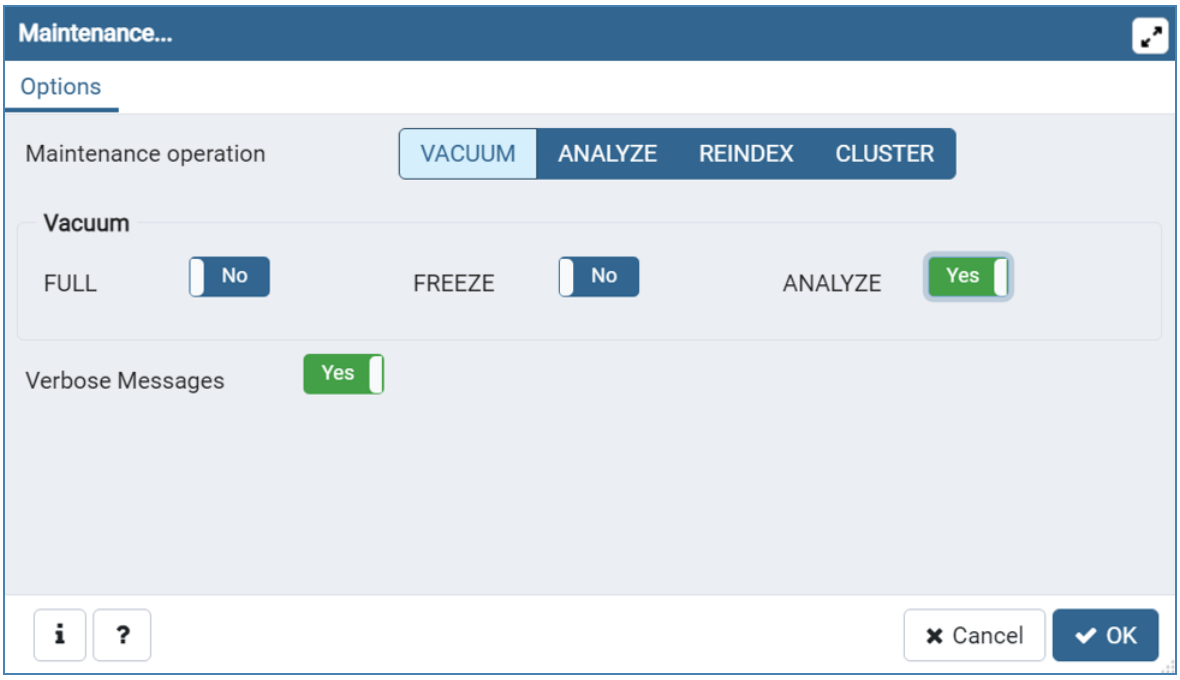
PostgreSQL databases require periodic maintenance known as `vacuuming`. The **VACUUM** command has to process each table on a regular basis to:

- Recover or reuse disk space occupied by deleted or updated rows.
- Protect against loss of very old data.
- Update data statistics and speed up index scanning.

The **ANALYZE** command collects statistics about the contents of tables in the database, and stores the results. Subsequently, the query planner uses these statistics to help determine the most efficient execution plans for queries.

### To manually vacuum and analyze your database(s), do the following:

1. Open the Acronis Cyber Files PostgreSQL Administrator tool. You can find it in the Start menu, in the Acronis Cyber Files folder. Double-click **localhost** to connect to your server.
2. Right-click the `acronisaccess_production` database and choose **Maintenance**.
3. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance operation: VACUUM

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

**Warning!**
The vacuum might take a long time. Run this process when the server load is low.

4. Click **OK**.
5. When the **Vacuum** process finishes, click **Done**.
6. Close the PostgreSQL Administrator tool.

**To setup automatic vacuuming, please read our article at:** Automated Database Vacuuming

***3. For big deployments, you should consider running a load-balanced setup or clustering gateway servers.***

# Backing up and Restoring Acronis Cyber Files

In case you need to upgrade, update or maintain your Acronis Cyber Files server. This article will give you the basics of backing up your database and restoring it. For load-balanced configurations the process is almost entirely identical as a regular backup and restore. Any specifics will be added to the relevant steps.

**Note**
If your Acronis Cyber Files server database is very large, several gigabytes, you may want to use a different backup and restore method for your database. Please contact our technical support at https://support.acronis.com/mobility for help and instructions.

**Note**
On a Microsoft Failover Cluster, some of the paths may be different, but the backup process is the same. It should be performed on the Active node and you should make sure the role will not failover and start during the backup.

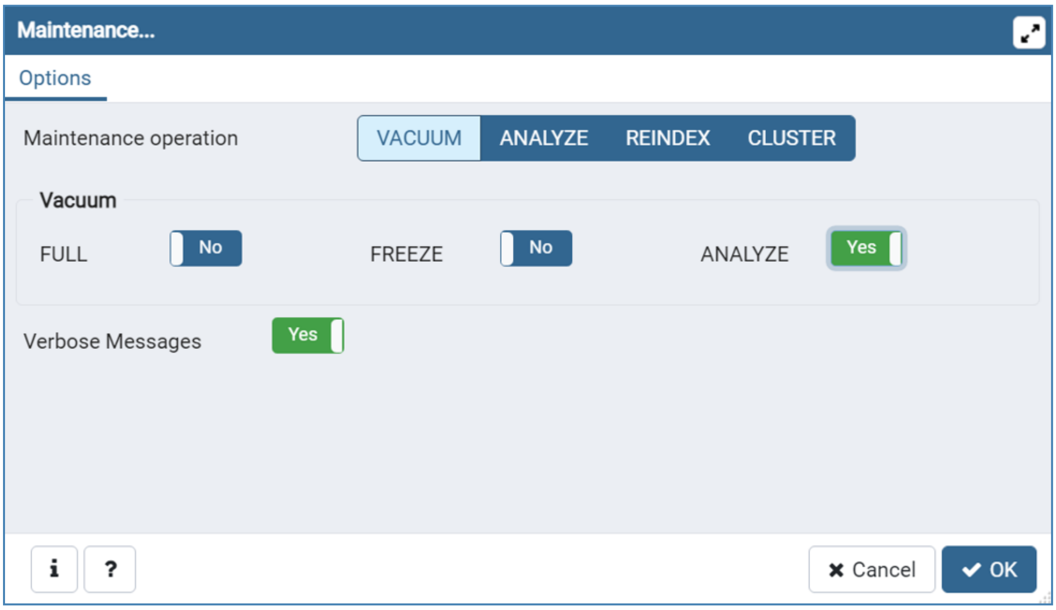
***We strongly recommend you perform a test backup/restore in a test environment before proceeding with backing up/restoring your production environment.***

## Backing up the Cyber Files database

1. Stop the Acronis Cyber Files Tomcat service.

   **Note**
   If you are load-balancing multiple Acronis Cyber Files Tomcat services, stop all of them.

2. Open the AcronisCyber Files PostgreSQL Administrator tool. You can find it in Windows Start menu, under the AcronisCyber Files folder. Connect to the database server. You may be prompted to enter the password for your `postgres` user.
3. Expand **Databases** and right-click on the `acronisaccess_production` database.
4. Choose **Maintenance.**
5. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance...

Options

Maintenance operation: VACUUM (selected) | ANALYZE | REINDEX | CLUSTER

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

6. Press **OK**.
7. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.
8. Close the PostgreSQL Administrator tool and open an elevated command prompt.
9. In the command prompt, navigate to the PostgreSQL bin directory.
   **e.g.**`cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

   **Note**
   You will need to edit the path to point to your PostgreSQL bin folder if you use an older or a custom installation (e.g. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

10. Enter the following command: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`
    - `alldbs.sql` will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: `--file D:\Backups\alldbs.sql`
    - If you are using a non-default port, change `5432` to the correct port number.
    - If you are not using the default PSQL administrative account `postgres`, please change `postgres` to the name of your administrative account in the command above.
    - You will be prompted to enter the `postgres` user's password several times for this process. For each prompt, enter the password and hit Enter.

    **Note**
    Typing the password will not result in any visual changes in the Command Prompt window.

11. Copy the backup file to a safe location.
12. Navigate to and copy the `postgresql.conf` file to a safe location, as it may contain important settings. It is located in the PostgreSQL Data folder - by default in `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`.

## Backing up the Gateway Server database

1. Stop the Acronis Cyber Files Gateway service.
2. Go to the Gateway Server database folder, by default located at:
   `C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database`
3. Copy the `mobilEcho.sqlite3` file to a safe location.
4. If you have multiple Gateway Servers, repeat this process for each one and make sure the database files don't get mixed up.

## Additional files to Backup

If you have made changes to any of these files, it is recommended to make backups so you can transfer your settings when restoring or migrating your Acronis Cyber Files product.

The `postgresql.conf` file, as it may contain important settings relevant to your database. It is typically located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.

- `web.xml` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`. Contains Single Sign-On settings.
- `server.xml` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Contains Tomcat settings.
- `krb5.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Contains Single Sign-On settings.
- `login.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`.
- Your certificates and keys used for Acronis Cyber Files.
- `acronisaccess.cfg` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.
- Custom color schemes located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\`.
- `pg_hba.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.
- `newrelic.yml` file if you are using **New Relic** to monitor your Acronis Cyber Files server.

## Restoring the Cyber Files database

1. Open the **Services** control panel and stop the AcronisCyber Files Tomcat service.

   **Note**
   For load-balanced configurations, stop all AcronisCyber Files Tomcat services.

2. Open the AcronisCyber Files PostgreSQL Administrator application, connect to the local database server, select **Databases**, and confirm there is a database called `acronisaccess_production`.
3. Right-click on the database and select **Refresh**.
4. Expand it and expand **Schemas**, expand **Public** and verify that there are zero (0) **Tables**.
   - If there are any tables in the database, right click on the database and rename it to `oldacronisaccess_production`. Finally, go to **Databases**, right-click and create a new database called `acronisaccess_production`.
5. Close the PostgreSQL Administrator and open an elevated command prompt.
6. In the command prompt, navigate to the PostgreSQL bin directory.
   **e.g.**`cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
7. Copy the database backup file `alldbs.sql` (or whatever you have named it) into the **bin** directory.
8. In the command prompt, enter the following command: `psql -U postgres -f alldbs.sql`
9. Enter your `postgres` password when prompted for it.

**Note**

Depending on the size of your database, the restore can take some time.

10. After the restore is complete, close the command prompt window.
11. Open the Acronis Cyber Files PostgreSQL Administrator application again and connect to the local database server.
12. Select **Databases**.
13. Expand the `acronisaccess_production` database, expand **Schemas** and expand **Public**. Verify that the number of **Tables** is the same as it was in step 5 of the "Backup the Acronis Cyber Files's database" section.

**Note**

If the Acronis Cyber Files Server version you restore the database to is newer than the version from your database backup, and the Acronis Cyber Files Tomcat service has already been started, the number of tables in the new Acronis Cyber Files Server database could be larger than the number of tables you had when you did the backup.

## Restoring the Gateway Server database

1. Stop the Acronis Cyber Files Gateway service.
2. Copy the `mobliEcho.sqlite3` Gateway Server database backup into the new Gateway Server's database folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database`) replacing the existing file.
3. Repeat this process for all Gateway Servers.

## Restoring additional files and customizations

Make sure to copy any customizations made to Acronis Cyber Files' configuration files (web.xml, server.xml, krb5.conf, certificates, custom color schemes, email templates, pg_hba.conf or newrelic.yml), and move them to the new files.

## Testing your restored Cyber Files Server

After you have successfully performed a backup/restore or a migration to another machine, it's time to bring Acronis Cyber Files back online and to verify that all settings are correct.

### Bringing regular deployments online

1. Start the Acronis Cyber Files Configuration Utility and make sure all settings found there are correct.
2. Press OK to start all services.
3. This should bring all services online simultaneously and restore all Acronis Cyber Files functionality.

4. If any of the components are on a separate machine, make sure to go to that machine and start them as well. In this case, the PostgreSQL service must be running in order for the Acronis Cyber Files Tomcat service to start without errors.

## Bringing load-balanced deployments online

1. Pick one of your Acronis Cyber Files Servers to act as a Primary. It will be the Primary only in the sense that it will be brought online first.
2. If the PostgreSQL service is on another machine, make sure to start it first as it will affect the Acronis Cyber Files Server.
3. Go to the machine for the Primary Acronis Cyber Files Server and start the Acronis Cyber Files Configuration Utility.
4. Make sure all settings found there are correct. If there are no issues, press OK to start all services.
5. Open the Acronis Cyber Files web console and login as an administrator. Verify that all settings are correct.
6. Once you have verified your settings, proceed to go over each machine that has a Acronis Cyber Files component and starting it via the Configuration Utility.

# Tomcat Log Management on Windows

As part of its normal operation Tomcat creates and writes information to a set of log files.

Unless periodically purged, these files accumulate and consume valuable space. It is commonly accepted by the IT community that the informational value those logs provide degrades rapidly. Unless other factors like regulations or compliance with certain policies play, keeping those log files in the system a discrete number of days is what is required.

***Introduction***

As part of its normal operation Tomcat creates and writes information to a set of log files. On Windows, these files are normally located in the following directory:

“`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs`” Acronis Cyber Files saves its own logs in the same directory as separate files.

**Note**
Acronis Cyber Files's log files are named **acronisaccess_date**.

There are many tools capable of automating the task of deleting unneeded log files. For our example, we will use a built-in Windows command called ForFiles.

**Note**
For information on ForFiles, syntax and examples visit http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx

***A sample process***

The sample process described below automates the process of purging log files older than a certain number of days. Inside the sample batch file, this number is defined as a parameter so it can be changed to fit different retention policies.

**Note**

The sample script (batch) file is designed to work on Windows Server 2008. Click here to download the script.

Optionally you could copy and paste the script code into an empty text document and save it as "AASTomcatLogPurge.bat"

**Full batch script code:**

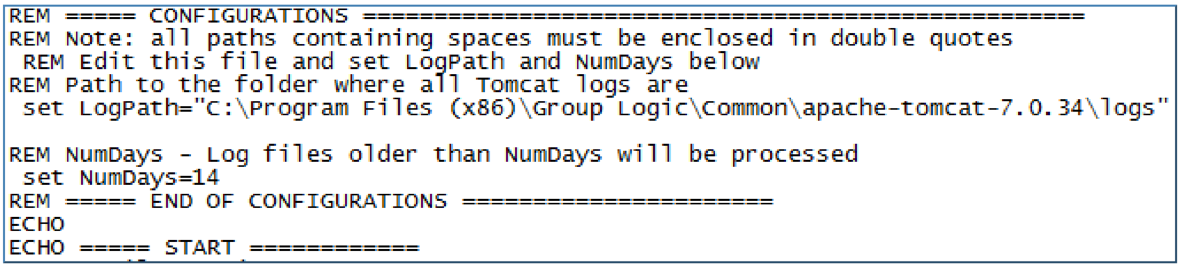
```
ECHO OFF

REM Script: aETomcatLogsPurge.bat

REM 2012-05-12: Version: 1.0: MEA: Created

ECHO This script will delete files older than a number of days from a directory

ECHO Run it from the command line or from a scheduler

ECHO Make sure the process has permissions to delete files in the target folder

REM ===== CONFIGURATIONS ===================================================

REM Note: all paths containing spaces must be enclosed in double quotes

REM Edit this file and set LogPath and NumDays below

REM Path to the folder where all Tomcat logs are

set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays - Log files older than NumDays will be processed

set NumDays=14

REM ===== END OF CONFIGURATIONS ======================

ECHO

ECHO ===== START ============

REM ForFiles options:

REM "/p": the path where you want to delete files.

REM "/s": recursively look inside other subfolders present in the folder mentioned in the
batch file path

REM "/d": days for deleting the files older than the present date. For instance "/d -7" means
older than 7 days

REM "/c": command to execute to actually delete files: "cmd /c del @file".
```

```
forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"

:End

ECHO ===== BATCH FILE COMPLETED ============================================
```

**Warning!**
We provide this example as a guideline so you can plan and implement your own process based on the specifics of your deployment. The example is not meant nor tested to apply to all situations and environments so use it as a foundation and at your own risk. **Do not use it in production environments without comprehensive offline testing first.**

***Steps***

1. Copy the script to the computer running Acronis Cyber Files (Tomcat) and open it with Notepad or a suitable plain text editor.
2. Locate the section illustrated in the picture below and edit the LogPath and NumDays variables with your specific paths and retention settings:

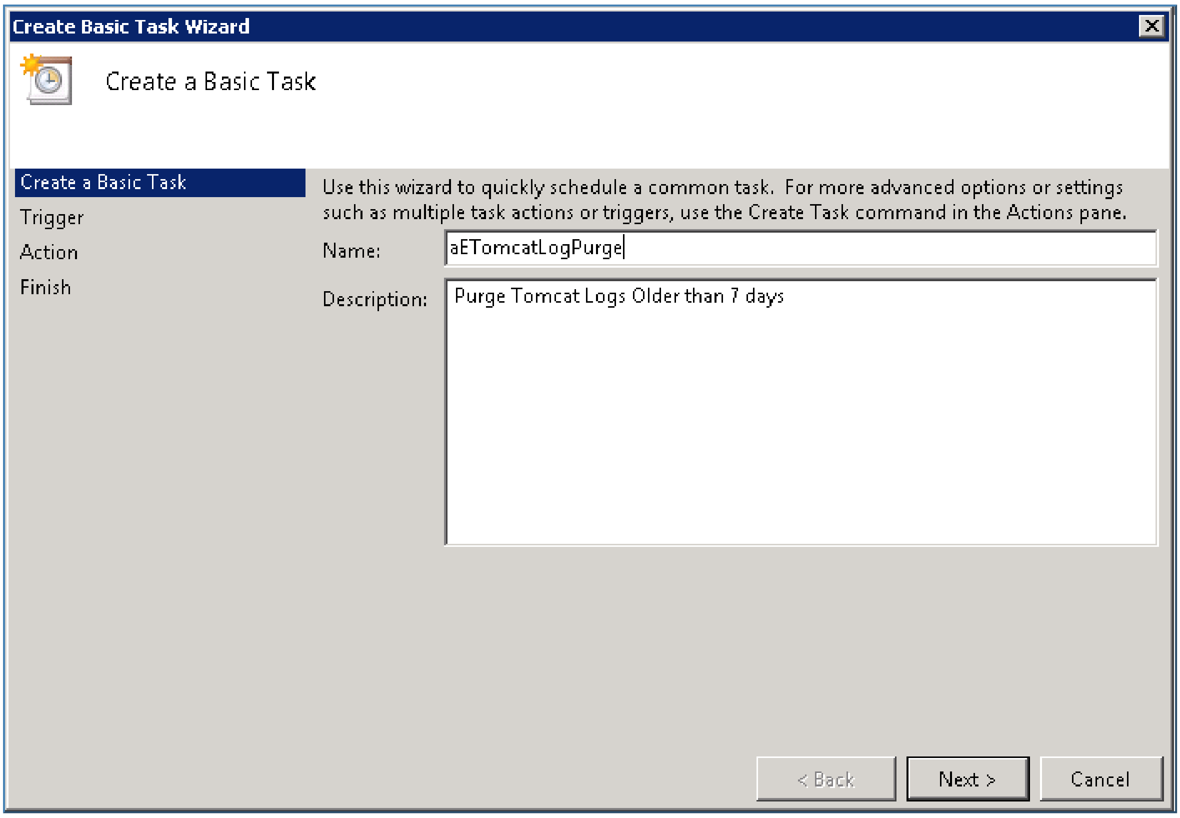


```
REM ===== CONFIGURATIONS ===================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays - Log files older than NumDays will be processed
 set NumDays=14
REM ===== END OF CONFIGURATIONS ======================
ECHO
ECHO ===== START ============
```

**Note**
In Acronis Cyber Files the log files are stored in the same folder as Tomcat's. (`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs`)

3. Save the file.

4. To automate the process, open **Task Scheduler** and create a new task. Define a name and a description for the task.



Create Basic Task Wizard

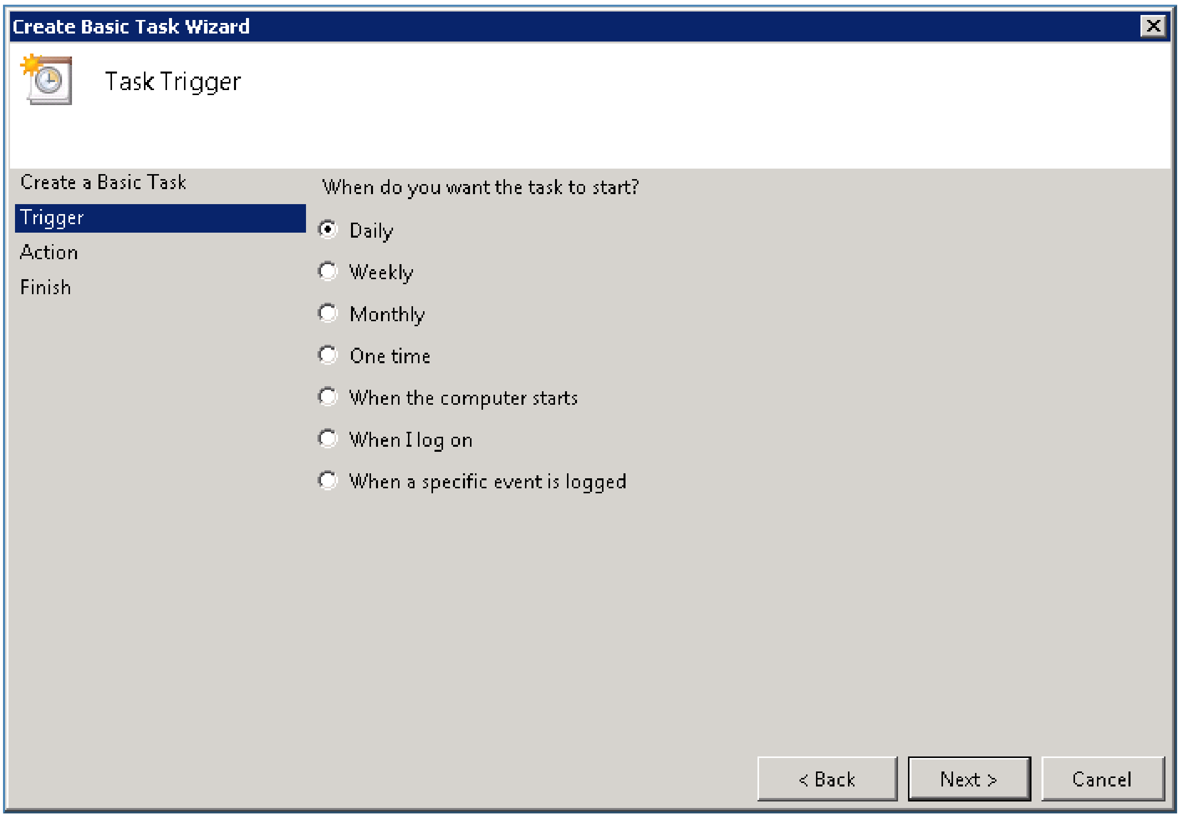
Create a Basic Task

Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: aETomcatLogPurge

Description: Purge Tomcat Logs Older than 7 days

5. Set the task to run daily.



Create Basic Task Wizard

Task Trigger

When do you want the task to start?

● Daily

○ Weekly

○ Monthly

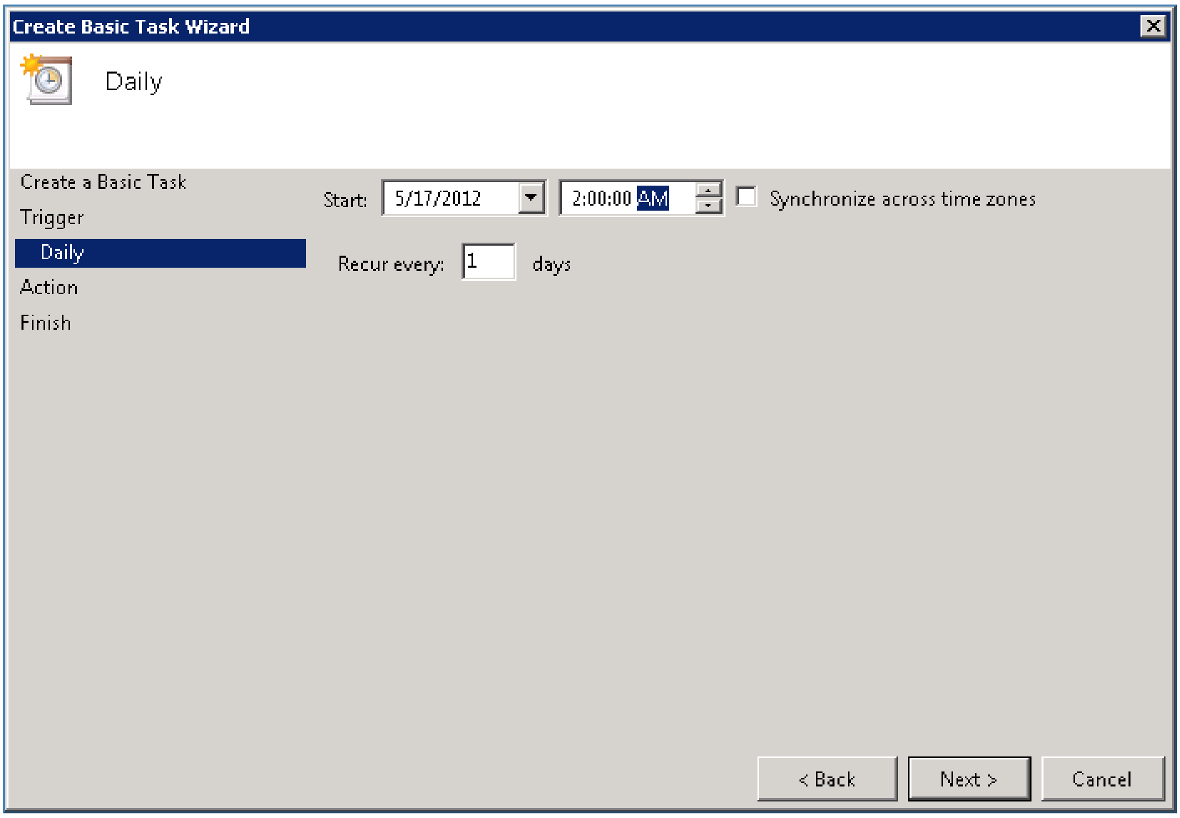
○ One time

○ When the computer starts

○ When I log on

○ When a specific event is logged

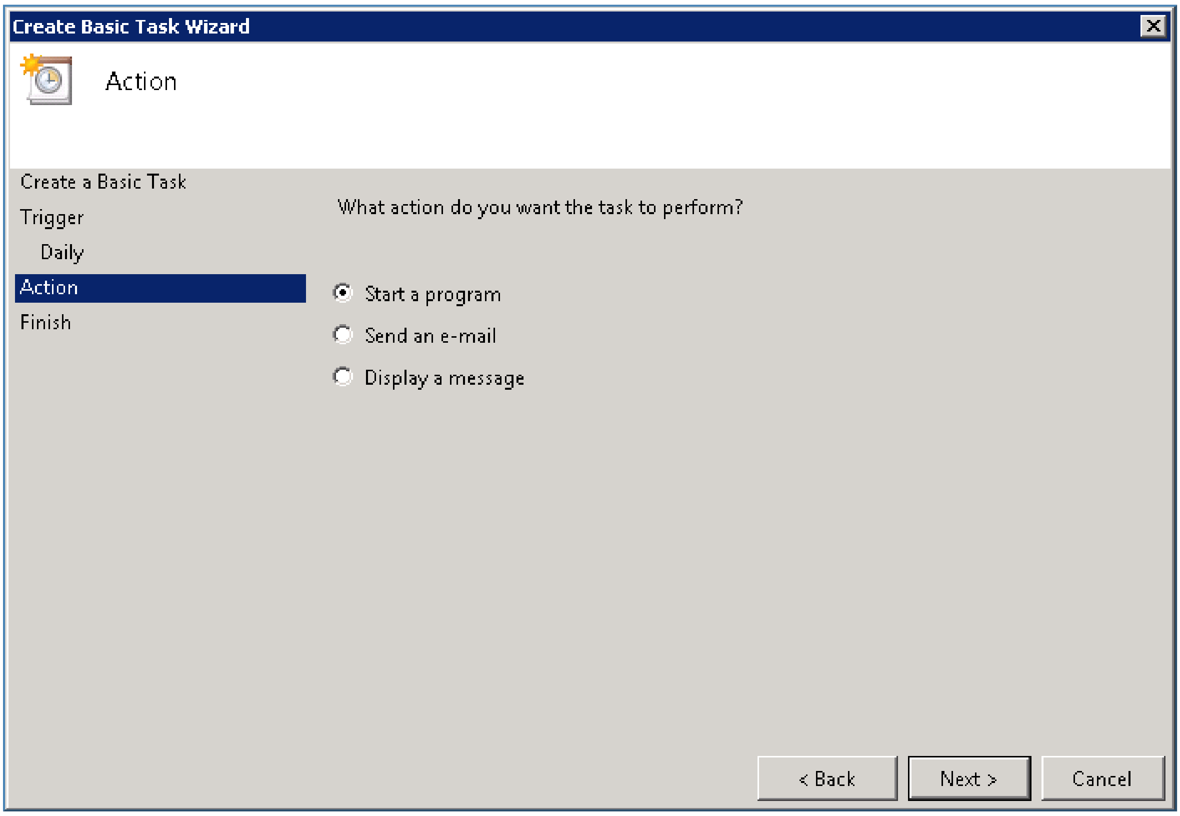
6. Define at what time the task should start. It is recommended to run this process when the system is not under extreme load or other maintenance processes are running.



Start: 5/17/2012 2:00:00 AM □ Synchronize across time zones

Recur every: 1 days

7. Set the action type to "**Start a program**".



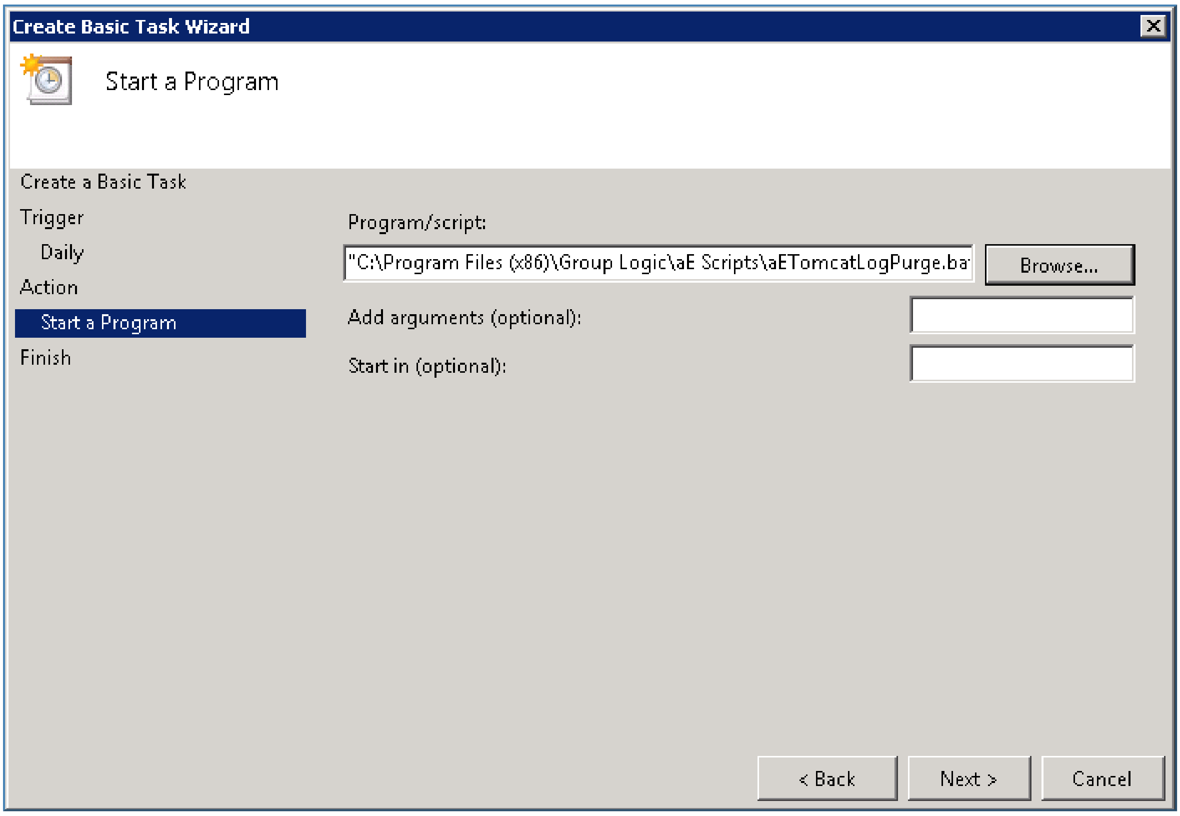
What action do you want the task to perform?

● Start a program

○ Send an e-mail

○ Display a message

8. Click the **Browse** button, locate and select the script (batch) file.

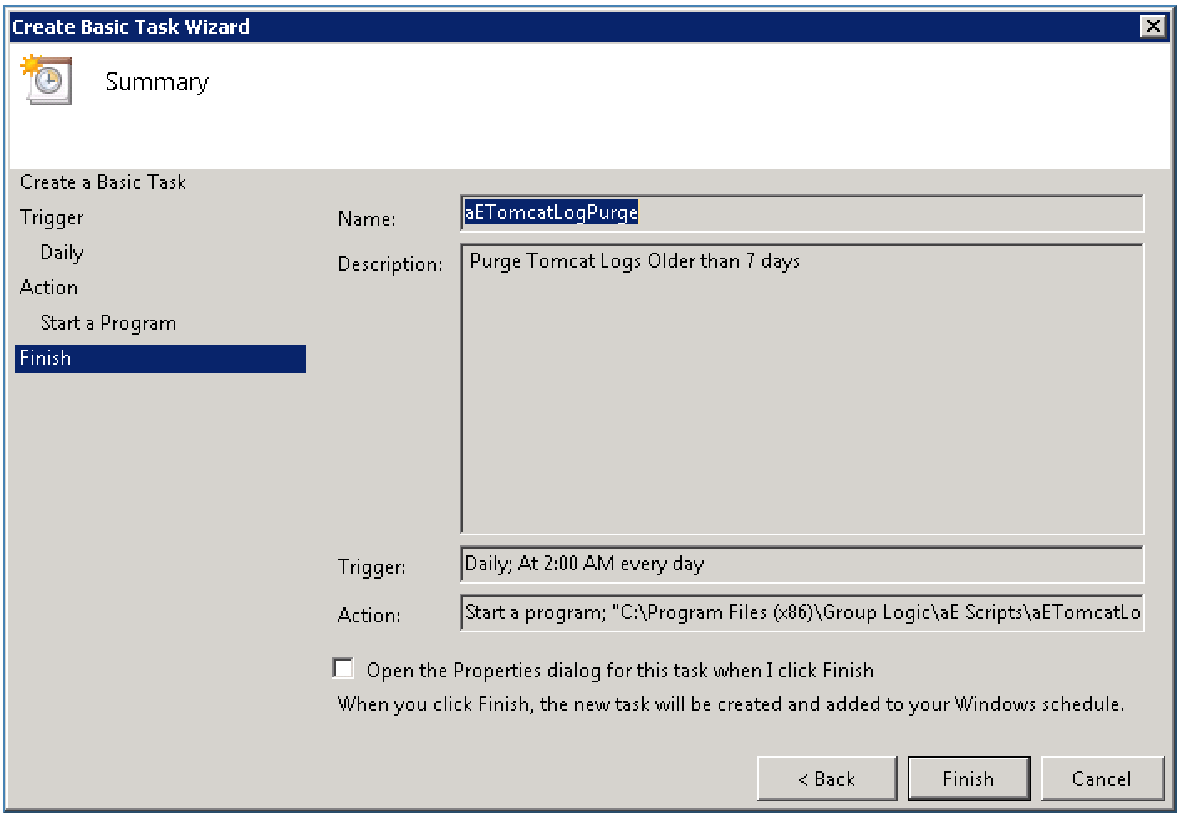


Program/script: "C:\Program Files (x86)\Group Logic\aE Scripts\aETomcatLogPurge.ba

Add arguments (optional):

Start in (optional):

9. When done, click **Finish**.



Name: aETomcatLogPurge

Description: Purge Tomcat Logs Older than 7 days

Trigger: Daily; At 2:00 AM every day

Action: Start a program; "C:\Program Files (x86)\Group Logic\aE Scripts\aETomcatLo

☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

10. In the tasks list you may want to right click on the task, select properties and verify the task will run whether a user is logged on or not, for unattended operation.

11. You can verify the task is properly configured and running properly by selecting the task, right clicking on it and selecting “Run”. The scheduler’s log should report start, stop and any errors.

# Automated Database Backup

With the help of the Windows Task Scheduler, you can easily setup an automated backup schedule for your Acronis Cyber Files database.

## Creating the database backup script

1. Open **Notepad** (or another text editor) and enter the following:

```
@echo off
```

```
for /f "tokens=1-4 delims=/ " %%i in ("%date%") do (
```

```
set dow=%%i
```

```
set month=%%j
```

```
set day=%%k
```

```
set year=%%l
```

```
)
```

```
set datestr=%month%_%day%_%year%
```

```
echo datestr is %datestr%
```

```
set BACKUP_FILE=AAS_%datestr%_DB_Backup.sql
```

```
echo backup file name is %BACKUP_FILE%
```

```
SET PGPASSWORD=password
```

```
echo on
```

```
bin\pg_dumpall -U postgres -f %BACKUP_FILE%
```

```
move "%BACKUP_FILE%" "C:\destination folder"
```

2. Replace "**password**" with the password for user **postgres** you have entered when you installed Acronis Cyber Files.
3. Replace **C:\destination folder** with the path to the folder where you want to save your backups.
4. Save the file as **DatabaseBackup.bat** (the extension is important!) and select **All Files** for the file type.
5. Move the file to the PostgreSQL installation folder in the version number directory (e.g. \9.3\).

### Creating the scheduled task

1. Open the **Control Panel** and open **Administrative Tools**.
2. Open the **Task Scheduler**.
3. Click on **Action** and select **Create Task**.

**On the General tab:**

1. Enter a name and description for the task (e.g. AAS Database Backup).
2. Select **Run whether user is logged in or not**.

**On the Triggers tab:**

1. Click **New**.
2. Select **On a schedule for Begin the task**.
3. Select daily and select the time when the script will be run and how often the script should be rerun (how often you want to backup your database).
4. Select **Enabled** from the **Advanced settings** and press **OK**.

**On the Actions tab:**

1. Click **New**.
2. Select **Start a program** for **Action**.
3. For **Program/Script** press **Browse**, navigate to and select the **DatabaseBackup.bat** file.
4. For **Start in (optional)**, enter the path to the folder in which the script resides. e.g. If the path to the script is `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\PSQL.bat` enter `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\`
5. Click **OK**.
6. Configure any additional settings on the other tabs and press **OK**.
7. You will be prompted for the credentials for the current account.

## Automated Database Vacuum

This guide will help you create a scheduled task that will run and vacuum the PostgreSQL database. Vacuuming is an important process especially if your deployment has a big database (several gigabytes).

**Note**
PostgreSQL is set to auto-vacuum in its configuration file. For deployments under high load, though, the auto vacuum may never run, as it is designed not to run when the server is under high load. For these cases, it is best to set up a scheduled task to run the Vacuum at least once a month.

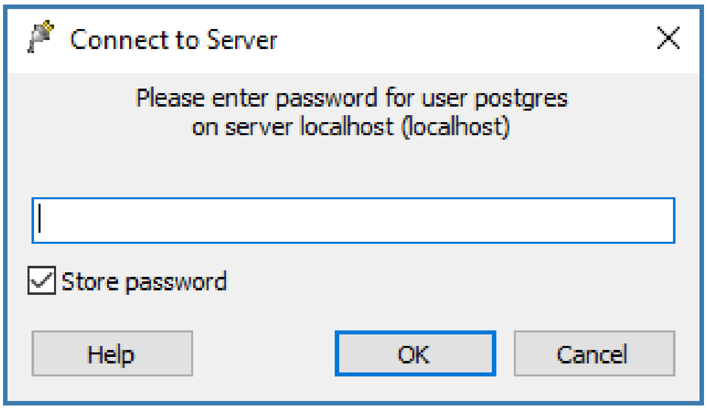
# Configuring PostgreSQL and creating the script

## Making sure the task will be able to run

You must make sure that you have the postgres user's password saved into the pgpass file, otherwise the script won't be able to run. The easiest way to do this is from the Acronis Cyber Files PostgreSQL Administrator tool:

1. Open the Acronis Cyber Files PostgreSQL Administrator. You can find it in the Windows Start Menu, under the folder Acronis Cyber Files.
2. Connect to the database and on the dialog that opens to enter the password, enable the **Store Password** checkbox and click **OK**. This will save the postgres user's password to the pgpass file. This file will be created in `C:\Users\<currentUser>\AppData\Roaming\postgresql`.

   **Note**
   You may see a dialog with information on Saving passwords, this is expected. Click **OK**.

   Connect to Server

   Please enter password for user postgres
   on server localhost (localhost)

   ☑ Store password

   - Alternatively, you can manually create a file called **pgpass.conf** and enter the following text into it: `localhost:5432:*:postgres:yourpassword`
   - Be sure to enter your **actual** postgres user password and correct port. Save the file.
3. For our example, we will copy the **pgpass.conf** file and place the copy in the **D:\Backup\** folder. The user running the scheduled task, must have read access to the file.

## Creating the script

In the example below, the PostgreSQL `bin` directory path is set to `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\bin\`.

**Note**

Note: You will need to edit the path to point to your PostgreSQL `bin` folder if you use an older or a custom installation (e.g. C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\bin\).

1. Create a folder where the log files will be stored and give the user running the task read, write and execute permissions to the folder. We recommend you use the machine's administrator as the user. In our example the log folder is `D:\Backup\`.
2. Open the text editor of your choice (e.g. Notepad) and paste the following example script:

```
SET PGPASSFILE=D:\Backup\pgpass.conf
"C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\bin\psql.exe" --
host=localhost --port 5432 --username=postgres -d acronisaccess_production -c "VACUUM
VERBOSE ANALYZE" >"D:\Backup\vacuum_report_%date:/=.%.log" 2>&1
```

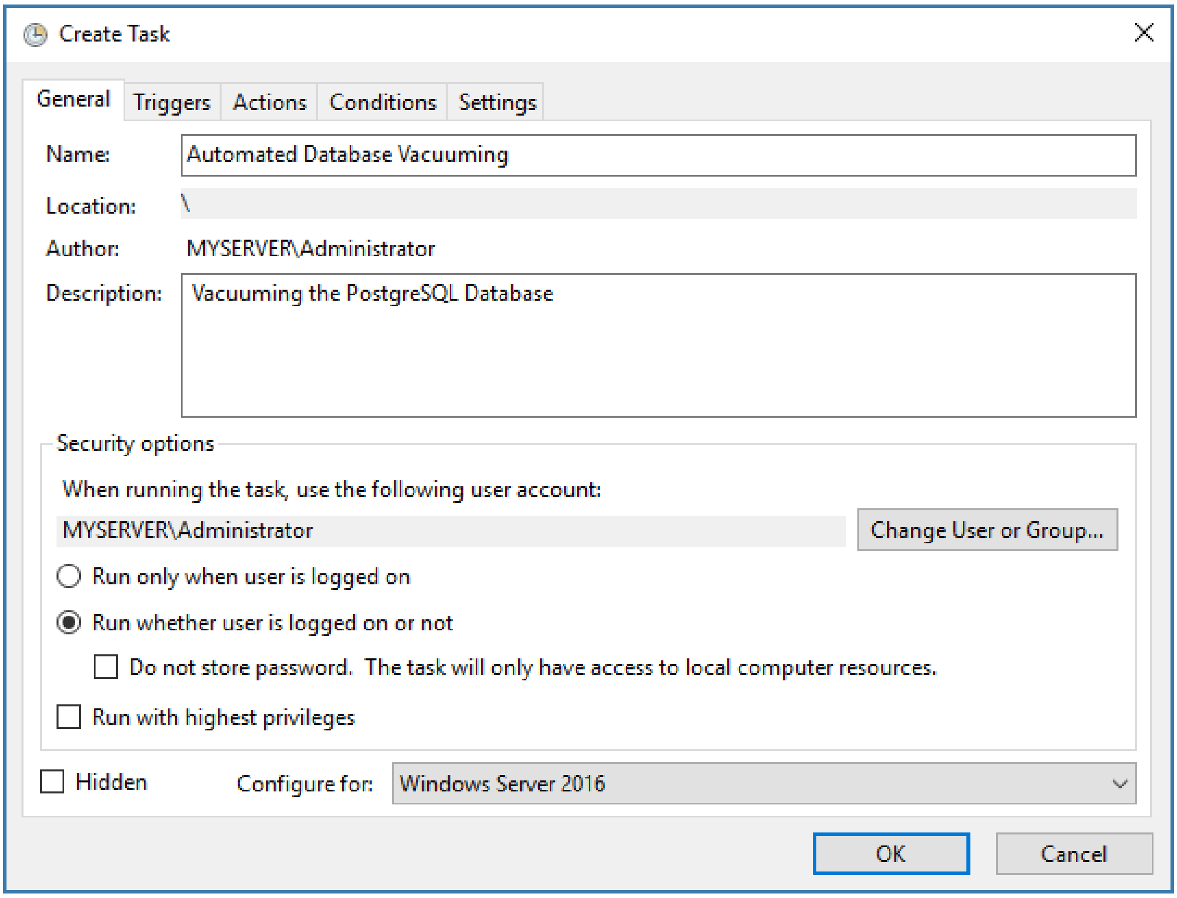
3. Edit this script to match your deployment.
   - Change the path to the `psql.exe` file with your path to the file.
   - Change the `--port` setting to the correct port number if you have changed the default.
   - If you are using a different PostgreSQL user, change `--username=` by replacing `postgres` with your desired user.
   - Change the `D:\Backup\` part of the path for the logs to your desired log folder.
   - Change the `D:\Backup\` part of the path for the pgpass.conf file to your path to the file.
4. Save the file as **vacuum.bat**. Make sure that you have selected **All types** under **Save as file type**.

   **Note**

   Depending on your date format, this **.log** file creation may fail. To find the date format you can open a command prompt and run: `echo %date%`. If there are any illegal characters in the date, like forward slashes, they have to be converted. In the above example the extra `:/=.` is the conversion part. If you encounter issues, please contact Acronis support.

## Configuring the Task Scheduler

1. Open the **Task Scheduler** from **Control Panel** -> **Administrative Tools** -> **Task Scheduler**.
2. Right-click on **Task Scheduler (local)** and select **Create Task**.



Name: Automated Database Vacuuming

Location: \

Author: MYSERVER\Administrator

Description: Vacuuming the PostgreSQL Database

Security options

When running the task, use the following user account:

MYSERVER\Administrator

○ Run only when user is logged on

● Run whether user is logged on or not

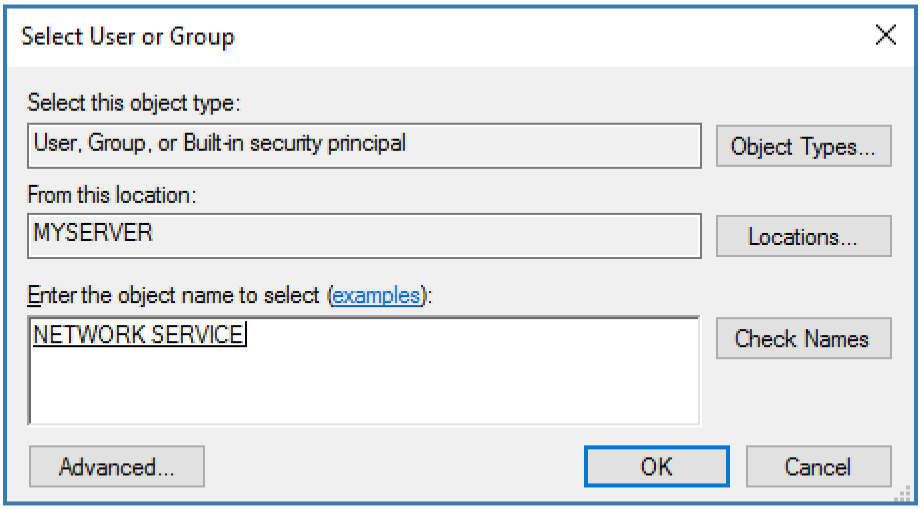
□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden

Configure for: Windows Server 2016

3. In the **General** tab:
   - Set the **Name** and **Description**.
   - Choose **Run whether user is logged on or not**.
   - Set the **User account** as the user that will run this task. We recommend using the machine NETWORK SERVICE account.



Select this object type:

User, Group, or Built-in security principal

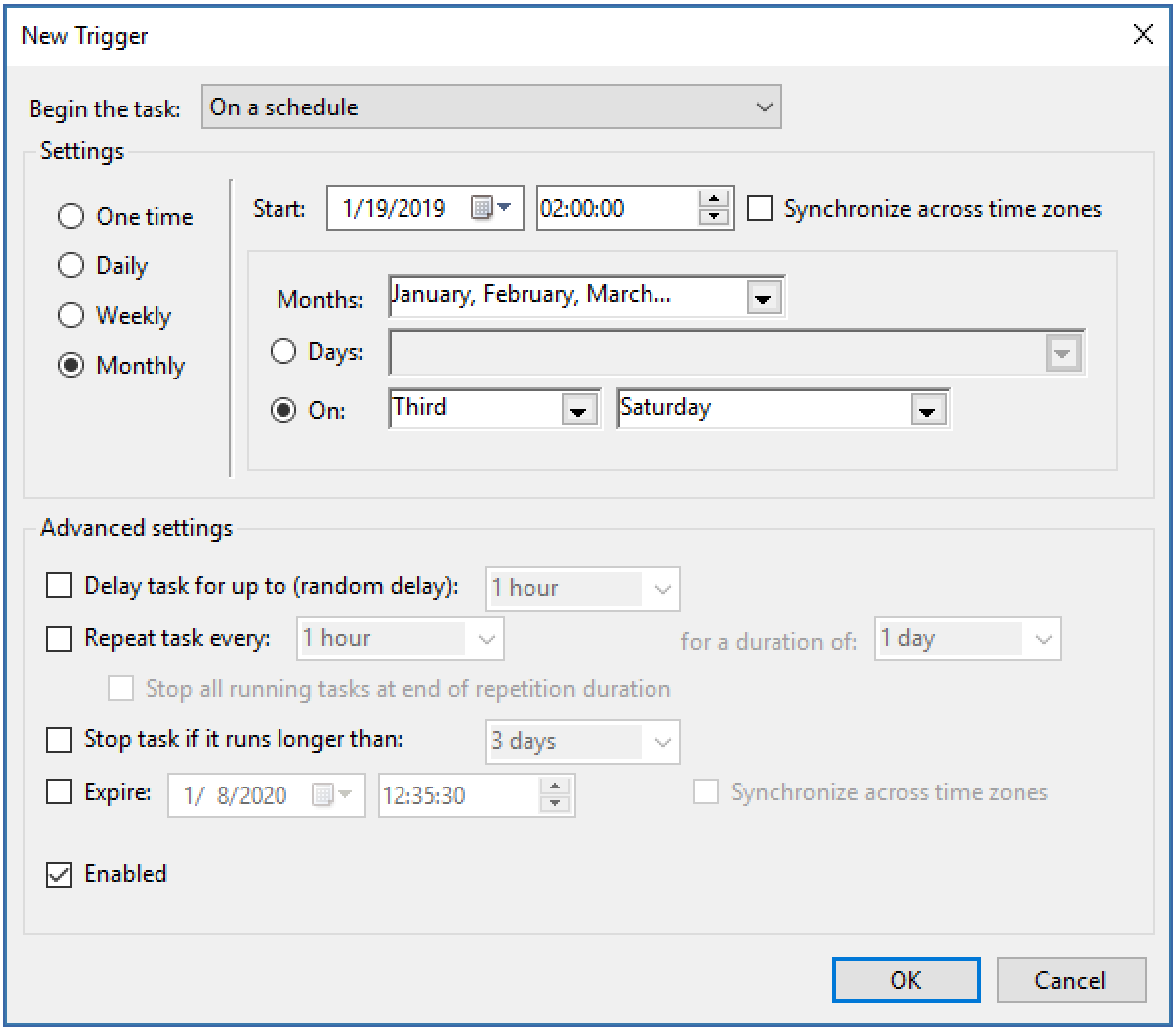
From this location:

MYSERVER

Enter the object name to select (examples):

NETWORK SERVICE

4. In the **Triggers** tab:



New Trigger

Begin the task: On a schedule

Settings

○ One time
○ Daily
○ Weekly
● Monthly

Start: 1/19/2019 02:00:00 □ Synchronize across time zones

Months: January, February, March...

○ Days:

● On: Third Saturday

Advanced settings

□ Delay task for up to (random delay): 1 hour

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

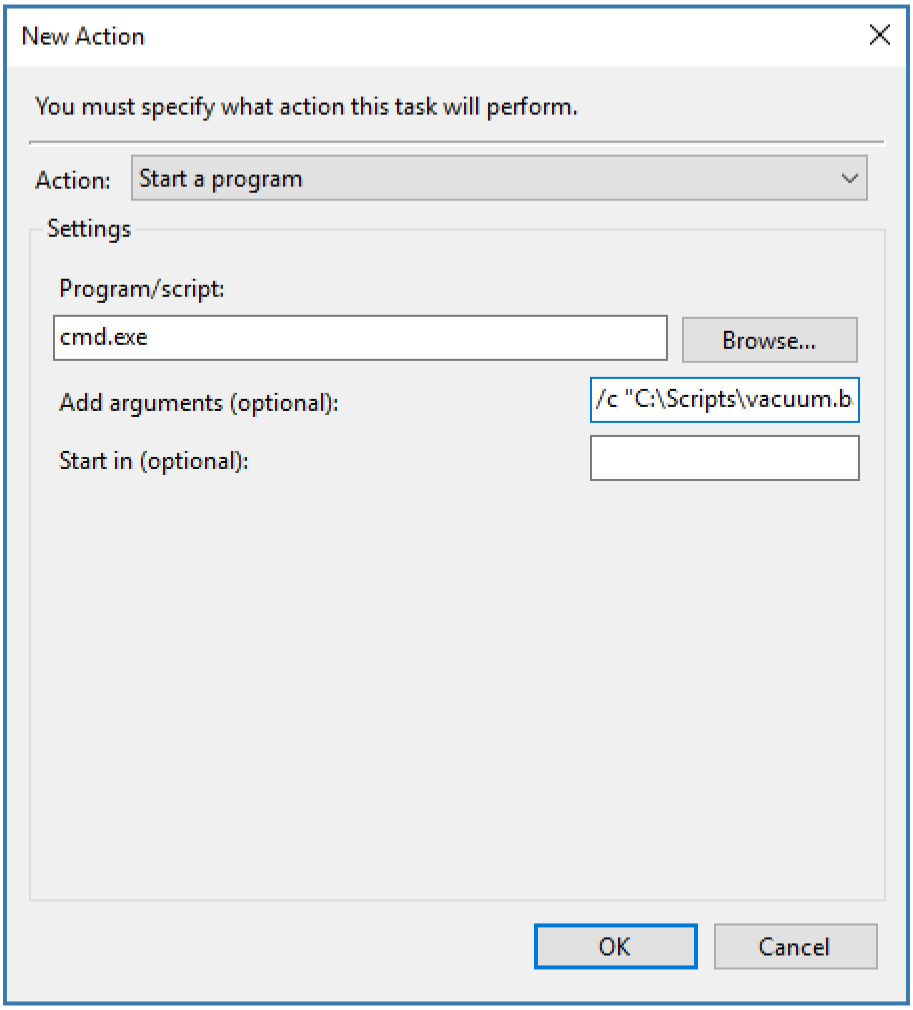
□ Stop task if it runs longer than: 3 days

□ Expire: 1/ 8/2020 12:35:30 □ Synchronize across time zones

☑ Enabled

- Click **New** and set the schedule you want the vacuum to run on. This should be a time of low load on the server. We recommend running the vacuum at least once a month.

5. In the **Action** tab:



New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: cmd.exe

Add arguments (optional): /c "C:\Scripts\vacuum.b

Start in (optional):

- Click **New** and for the **Action** select **Start a program**.
- For the **Program/script** enter `cmd.exe`
- In the **Add arguments** enter: `/c "C:\Scripts\vacuum.bat"`

**Note**

Make sure to edit the path in this command to reflect the actual path to your vacuum.bat file.

- Leave all the defaults for the **Conditions** and **Settings** tabs.
- Click **OK** to save the new task. It may prompt you to enter an administrator password.

### Verify that the task works as expected

1. From the Task Scheduler, run the vacuum task manually to test it out and make sure it is writing the log file into the proper folder.
2. Check that the scheduled task runs at the time it is set for.

## Same-server Migration of Acronis Cyber Files

This guide will help you migrate your Acronis Cyber Files setup on the current machine(s).

**Important**

Before migrating the production server(s), we strongly recommend that you perform these steps in a test environment. To ensure compatibility in the production environment, the test deployment should have the same architecture as the production server(s), along with a couple of test user desktop and mobile clients.

## Before you begin a same-server migration

**Warning!**

**We strongly recommend that you run a test backup/restoration outside of your production environment.**

**Important things to take note of, regarding your current configuration:**

- Are the Cyber Files Web Server, PostgreSQL, and the Gateway and File Repository all on one machine?
- Note the DNS, the IP and port of the Cyber Files Web Server.
- Note the DNS, the IP and port of the Gateway server.
- Note the Address and Port of the File Repository.
- Note the location of the File Store.
- Note the PostgreSQL version number of your current server.

  The easiest way to do this is to look at the folder name inside the main PostgreSQL folder (by default, `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`), the inside folder's name is the PostgreSQL major version number (for example, **9.2**; **9.3**; **9.4**).

**Note**

Much of this information can be found in the Configuration Utility.

### Basic outline of the same-server migration process

Make sure that you are prepared to do all of these steps before you begin the migration.

1. Backup PostgreSQL.
2. Backup the Gateway Server database.
3. Backup some additional files.
4. Uninstall Acronis Cyber Files.
5. Remove PostgreSQL Data directory.
6. [Optional] Remove Java.
7. Install Acronis Cyber Files using the same version installer as you uninstalled.
8. Restore the Gateway Server database.
9. Configure the server.
10. Verify Acronis Cyber Files administrative settings.
11. Test your new configuration.

# Migrating Acronis Cyber Files

## To migrate Acronis Cyber Files

1. ***Backup PostgreSQL***

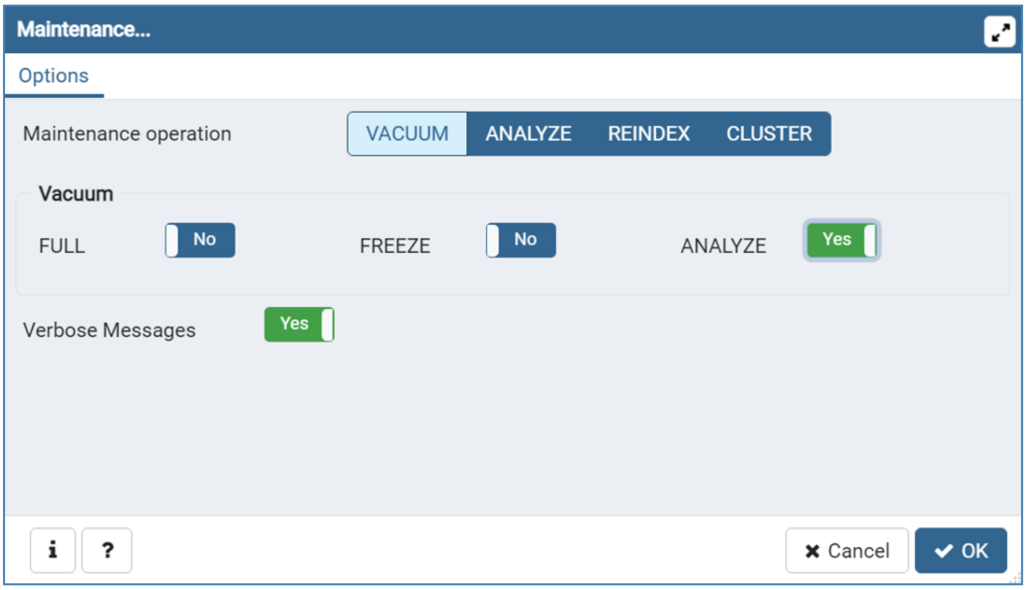
   a. Open the **Services** control panel and stop the Acronis Cyber Files Tomcat service.

   b. Open the Acronis Cyber Files PostgreSQL Administrator tool. You can find it in Windows Start menu, under the Acronis Cyber Files folder. Connect to the database server. You may be prompted to enter the password for your `postgres` user.

   c. Expand **Databases** and right-click on the `acronisaccess_production` database.

   d. Choose **Maintenance.**

   e. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance...

Options

Maintenance operation: VACUUM | ANALYZE | REINDEX | CLUSTER (VACUUM selected)

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

   f. Click **OK**.

   g. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.

   h. Close the PostgreSQL Administrator tool and open an elevated command prompt.

   i. In the command prompt, navigate to the PostgreSQL bin directory.

   **e.g.** `cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

   **Note**

   Note: You will need to edit the path to point to your PostgreSQL bin folder if you use an older or a custom installation (e.g. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

j. Enter the following command: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`

   - `alldbs.sql` will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: `--file D:\Backups\alldbs.sql`
   - If you are using a non-default port, change `5432` to the correct port number.
   - If you are not using the default PSQL administrative account `postgres`, please change `postgres` to the name of your administrative account in the command above.
   - You will be prompted to enter the `postgres` user's password several times for this process. For each prompt, enter the password and hit **Enter**.

   **Note**

   Typing the password will not result in any visual changes in the Command Prompt window.

2. *Backup the Gateway Server database*

   a. Stop the **Acronis Cyber Files Gateway** service.

   b. Go to the Gateway Server database folder, by default located at:

      `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`

   c. Make a backup copy of the `mobilEcho.sqlite3` file.

3. ***Additional files to backup***

   If you have made changes to any of these files, it is recommended to make backups so you can transfer your settings when restoring or migrating your Acronis Cyber Files product.

   - The `postgresql.conf` file, as it may contain important settings relevant to your database. It is typically located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.
   - `web.xml` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`. Contains Single Sign-On settings.
   - `server.xml` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Contains Tomcat settings.
   - `krb5.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Contains Single Sign-On settings.
   - `login.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`.
   - Your certificates and keys used for Acronis Cyber Files.
   - `acronisaccess.cfg` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.
   - Custom color schemes located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\`.
   - `pg_hba.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.

4. ***Uninstall Acronis Cyber Files***

   a. Open the Acronis Cyber Files installer.
   b. Accept the license agreement and click **Uninstall**.
   c. Select all components and click **Uninstall**.

5. ***Remove PostgreSQL Data directory***

   The PostgreSQL server will not automatically remove its **Data** directory. Manually remove the entire PostgreSQL directory found here by default: `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\`

   **Note**

   You need to edit the path if you use an older or a custom installation (for example, `C:\Program Files\Acronis\Access\Common\PostgreSQL\`).

6. ***[Optional] Remove Java***

   You may also want to remove the Java that was installed for the Acronis Cyber Files Web Server. Java can also be removed from the control panel.

7. ***Reinstall** Acronis Cyber Files*

   a. Start the new Acronis Cyber Files installer and click **Next**.
   b. Read and accept the license agreement.
   c. Choose **Install** and follow the installer screens.

      **Note**

      If the Acronis Cyber Files Web Server, PostgreSQL, and Gateway are going on separate machines, choose **Custom** and select the desired component(s).

   d. On the PostgreSQL Configuration screen, enter the same password for the PostgreSQL superuser that was used originally.
   e. Click **Next**.
   f. Review the components being installed and click **Install**.
   g. Once the installer has finished, click **Exit** and a dialog will appear telling you that the Configuration Utility will run next.
   h. When the Configuration Utility opens, leave it open without pressing **OK** or **Apply**.
   i. Open the **Services** control panel and stop the Acronis Cyber Files Tomcat service.

      **Note**

      For load-balanced configurations, stop all Acronis Cyber Files Tomcat services.

   j. Open the Acronis Cyber Files PostgreSQL Administrator application, connect to the local database server, select **Databases**, and confirm there is a database called `acronisaccess_production`.
   k. Right-click on the database and select **Refresh**.
   l. Expand it and expand **Schemas**, expand **Public** and verify that there are zero (0) **Tables**.
      - If there are any tables in the database, right click on the database and rename it to `oldacronisaccess_production`.

- Then, go to **Databases**, right-click and create a new database called `acronisaccess_production`.

m. Close the PostgreSQL Administrator and open an elevated command prompt.

n. In the command prompt, navigate to the PostgreSQL bin directory.

**e.g.** `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

o. Copy the database backup file `alldbs.sql` (or whatever you have named it) into the **bin** directory.

p. In the command prompt, enter the following command: `psql -U postgres -f alldbs.sql`

q. Enter your `postgreSQL` password when prompted.

**Note**

Depending on the size of your database, the restore can take some time.

r. After the restore is complete, close the command prompt window.

s. Open the **Files Advanced PostgreSQL Administrator** again and connect to the local database server.

t. Select **Databases**.

u. Expand the `acronisaccess_production` database, expand **Schemas** and expand **Public**. Verify that the number of **Tables** is the same as it was originally.

8. ***Restore the Gateway Server database***

Copy the `mobilEcho.sqlite3` Gateway Server database backup file you created into the new Gateway Server database folder (by default `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`), replacing the existing file.

9. ***Configure the server***

**Note**

It is highly recommended that you do not change the DNS names used by Acronis Cyber Files, only the IP addresses they are pointing to. The following instructions assume you are re-using the DNS names of the previous instance of Acronis Cyber Files.

a. Go back to the Acronis Cyber Files Configuration Utility that you left open and set the settings for the Gateway Server, Acronis Cyber Files Web Server and File Repository.

b. Click **Apply**, and then click **OK**.

c. At the next dialog, click **OK.** A browser will launch with the Acronis Cyber Files web interface.

d. Log into the Access server.

e. Click on **Administration**.

f. Navigate to the **Mobile Access** -> **Gateway Servers** page.

g. In the list of Gateway Servers you should see your Gateway server listed.

h. If the address for your gateway server is a DNS entry, you should not need to make any changes to the server as long as the DNS entry is pointing to your server machine. If the address for your gateway is an IP address, ensure it is the IP address of the gateway server.

10. ***Verify Acronis Cyber Files administrative settings***

Once you have completed the database restore, we highly recommend that you sign in to the web interface and verify that your settings have restored correctly, and that they are still relevant before proceeding. Here are some examples of important items to check:

- Audit Logging - Make sure that the new Acronis Cyber Files logs folder has all the necessary permissions so that logs can be written.
- Administration settings - Make sure all your LDAP, SMTP and general administrative settings are correct.
- Gateway Servers and Data Sources - Make sure all your Gateway Servers are still reachable on the correct addresses and check if all your Data Sources have valid paths.

## Testing the new configuration

After you have completed the migration, ensure that everything is working by doing the following actions:

- Navigate the web interface and check if everything is working as expected. Check that your settings are there and haven't been modified.
- Upload a file through the web interface to the Sync & Share section. Do the same for any network nodes you have set up (if any).
- Download a Sync & Share file that existed before the migration, to confirm the connection to the existing File Store still works.
- Connect to the new configuration with a desktop client and/or a mobile client.
- Upload and download some files through the desktop and/or the mobile clients.

# Migrating Acronis Cyber Files to another server

This guide will help you move your existing Acronis Cyber Files setup to new machines.

**Important**

Before migrating the production server, we strongly recommend that these steps be performed in a test environment. The test deployment should have the same architecture as the production servers, along with a couple of test user desktop and mobile clients to ensure compatibility in the production environment.

## Before you begin

**Warning!**

**We strongly recommend that you run a test backup/restoration outside of your production environment.**

**Important things to take note of, regarding your current configuration:**

- Are the Cyber Files Web Server, PostgreSQL, and the Gateway and File Repository all on one machine?

- Note the DNS, the IP and port of the Cyber Files Web Server.
- Note the DNS, the IP and port of the Gateway server.
- Note the Address and Port of the File Repository.
- Note the location of the File Store.
- Note the PostgreSQL version number of your current server.

  The easiest way to do this is to look at the folder name inside the main PostgreSQL folder (by default, `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL`), the inside folder's name is the PostgreSQL major version number (for example, **9.2**; **9.3**; **9.4**).

**Note**
Much of this information can be found in the Configuration Utility.

**Basic outline of the migration process:**

Make sure that you are prepared to do all of these steps before you begin the migration.

1. Change the DNS entries to point to the new server machine.
2. Backup your current database files and certificates.
3. Move the database files and certificates to the new machine.
4. Migrate the File Store.
5. Install Acronis Cyber Files Web Server on the new machine.
6. Move certificates to the new machine.
7. Put database files into new Acronis Cyber Files Web Server installation.
8. Use Configuration Utility to start up new Acronis Cyber Files Web Server.
9. Confirm Acronis Cyber Files Mobile Gateway address is correct.
10. Test your new configuration.

## Migrating the Acronis Cyber Files Web Server and Gateway databases

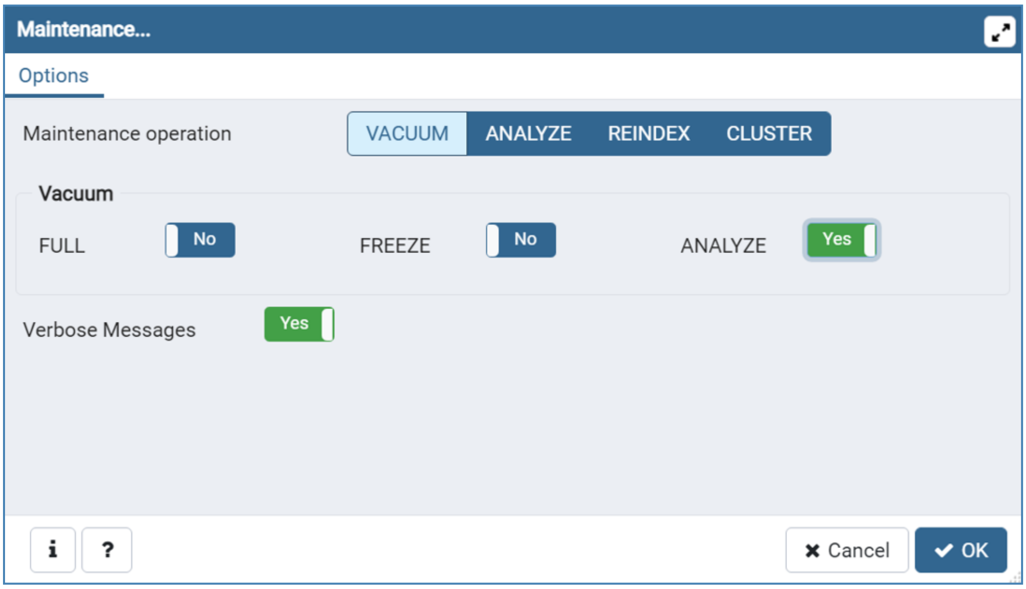
### On the original server, where Tomcat/Gateway/PostgreSQL are running now

**Note**
If your Acronis Cyber Files Web Server database is very large (several gigabytes) you may want to use a different backup and restore method for your database.
Please contact our technical support at https://support.acronis.com/mobility for help and instructions.

1. Stop the Acronis Cyber Files Tomcat service
   i. Open the Acronis Cyber Files PostgreSQL Administrator tool. You can find it in Windows Start menu, under the AcronisCyber Files folder. Connect to the database server. You may be prompted to enter the password for your `postgres` user.
   ii. Expand **Databases** and right-click on the `acronisaccess_production` database.

iii. Choose **Maintenance.**

iv. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance operation: VACUUM

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

v. Click **OK**.

vi. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.

vii. Close the PostgreSQL Administrator tool and open an elevated command prompt.

viii. In the command prompt, navigate to the PostgreSQL bin directory.

**e.g.** `cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

**Note**

Note: You will need to edit the path to point to your PostgreSQL bin folder if you use an older or a custom installation (e.g. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`).

ix. Enter the following command: `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql`

- `alldbs.sql` will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: `--file D:\Backups\alldbs.sql`
- If you are using a non-default port, change `5432` to the correct port number.
- If you are not using the default PSQL administrative account `postgres`, please change `postgres` to the name of your administrative account in the command above.
- You will be prompted to enter the `postgres` user's password several times for this process. For each prompt, enter the password and hit Enter.

**Note**

Typing the password will not result in any visual changes in the Command Prompt window.

2. ***Backup the Gateway Server's database***
   a. Stop the **AcronisCyber Files Gateway** service.
   b. Go to the Gateway Server database folder, by default located at:
      `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`
3. Copy the `mobilEcho.sqlite3` file to the new machine that will host the Gateway Server.

## Additional files to Backup

If you have made changes to any of these files, it is recommended to make backups so you can transfer your settings when restoring or migrating your Acronis Cyber Files product.

The `postgresql.conf` file, as it may contain important settings relevant to your database. It is typically located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.

- `web.xml` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`. Contains Single Sign-On settings.
- `server.xml` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Contains Tomcat settings.
- `krb5.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`. Contains Single Sign-On settings.
- `login.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf`.
- Your certificates and keys used for Acronis Cyber Files.
- `acronisaccess.cfg` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.
- Custom color schemes located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\`.
- `pg_hba.conf` located by default at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`.
- `newrelic.yml` file if you are using **New Relic** to monitor your Acronis Cyber Files server.

## On the new server that will be hosting the Acronis Cyber Files Server

### Install Acronis Cyber Files

1. Start the Acronis Cyber Files installer and press **Next**. Read and accept the license agreement.
2. Choose **Install** and follow the installer screens.

**Note**

If the Acronis Cyber Files Web Server, PostgreSQL, Gateway are going on separate machines, choose **Custom** and select the desired component(s).

3. On the PostgreSQL Configuration screen enter the same password for the PostgreSQL superuser that was used on the original server. Press **Next**.
4. Review the components being installed and press **Install**.
5. Once the installer is done, press **Exit** and dialog will come up telling you the Configuration Utility will run next.
6. When the Configuration Utility comes up, leave it open without pressing **OK** or **Apply**.
7. Open the **Services** control panel and stop the AcronisCyber Files Tomcat service.

**Note**

For load-balanced configurations, stop all AcronisCyber Files Tomcat services.

8. Open the AcronisCyber Files PostgreSQL Administrator application, connect to the local database server, select **Databases**, and confirm there is a database called `acronisaccess_production`.
9. Right-click on the database and select **Refresh**.
10. Expand it and expand **Schemas**, expand **Public** and verify that there are zero (0) **Tables**.
    - If there are any tables in the database, right click on the database and rename it to `oldacronisaccess_production`. Finally, go to **Databases**, right-click and create a new database called `acronisaccess_production`.
11. Close the PostgreSQL Administrator and open an elevated command prompt.
12. In the command prompt, navigate to the PostgreSQL bin directory.

    **e.g.** `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
13. Copy the database backup file `alldbs.sql` (or whatever you have named it) into the **bin** directory.
14. In the command prompt, enter the following command: `psql -U postgres -f alldbs.sql`
15. Enter your `postgres` password when prompted for it.

**Note**

Depending on the size of your database, the restore can take some time.

16. After the restore is complete, close the command prompt window.
17. Open the **Files Advanced PostgreSQL Administrator** again and connect to the local database server.
18. Select **Databases**.
19. Expand the `acronisaccess_production` database, expand **Schemas** and expand **Public**. Verify that the number of **Tables** is the same as it was on the original server.

**Note**

If the Acronis Cyber Files Web Server version you restore the database to is newer than the Acronis Cyber Files Web Server version from your database backup, and the Acronis Cyber Files Tomcat service has already been started, the number of tables in the new Acronis Cyber Files Web Server database could be larger than the number of tables you had when you did the backup.

### Restore the Gateway Server database

Copy the `mobliEcho.sqlite3` Gateway Server database that came from the old server into the new Gateway Server's database folder (by default `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`) replacing the existing file.

### Configure your new server

**Note**

It is highly recommended that you do not change the DNS names used by Acronis Cyber Files, only the IP addresses they are pointing to.The following instructions assume you are re-using the DNS names of the previous instance of Acronis Cyber Files.

1. Go back to the Acronis Cyber Files Configuration Utility that you left open and set the settings for the Gateway Server, Acronis Cyber Files Web Server and File Repository.
2. Click **Apply**, and then **OK**. At the next dialog click **OK** and a browser will launch with the Acronis Cyber Files web interface.
3. Log into the Access server.
4. Click on **Administration**. Navigate to the **Mobile Access** -> **Gateway Servers** page.
5. In the list of Gateway Servers you should see your Gateway server listed.
6. If the address for your gateway server is a DNS entry you should not need to make any changes to the server as long as the DNS entry is now pointing to your new server machine. If the address for your gateway is an IP address, then you will need to edit the gateway server.

### Verify Acronis Cyber Files administrative settings

Once you have successfully finished your database's restoration, we highly recommend that you login to the web interface and verify that your settings have carried over and that they are still relevant before proceeding with anything else. Here are some examples of important items to check:

- Audit Logging - Make sure that the new Acronis Cyber Files logs folder has all the necessary permissions so that logs can be written.
- New Relic - If you are using New Relic, copy the `newrelic.yml` file from the old machine to this one and make sure that the path in the Acronis Cyber Files web interface points to the file.
- Administration settings - Make sure all your LDAP, SMTP and general administrative settings are correct.

- Gateway Servers and Data Sources - Make sure all your Gateway Servers are still reachable on the correct addresses and check if all your Data Sources have valid paths.

## Testing your new configuration

After you have the new server set up, make sure that everything is working by doing a couple of simple actions:

- Navigate the web interface and check if everything is working as expected. Check if your settings are there and haven't been modified.
- Upload a file through the web interface to the Sync and Share section and do the same for any Network nodes you have set up (if any).
- Connect to the new server with a desktop client and a mobile client applications.
- Upload and download some files through the desktop and/or mobile clients.

## Cleanup of the original server

Once you have verified that your new server is running correctly and you do not intend to use the old server again, we recommend you uninstall Acronis Cyber Files from the old machine.

Open the Acronis Cyber Files installer, accept the license agreement and click Uninstall. Select all components and press uninstall. This will remove all Acronis Cyber Files components from your machine.

**Note**
If you don't have an Acronis Cyber Files installer, open the control panel, uninstall the Acronis Cyber Files PostgreSQL Server, Acronis Cyber Files Gateway Server, and the Acronis Cyber Files File Repository Server, Acronis Cyber Files Web Server, Acronis Cyber Files Configuration Collection Tool, the Acronis Cyber Files Configuration Utility and LibreOffice.

- The PostgreSQL server will not automatically remove its **Data** directory. Manually remove the entire PostgreSQL directory found here by default: `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\`

  **Note**
  You need to edit the path if you use an older or a custom installation (for example, `C:\Program Files\Acronis\Access\Common\PostgreSQL\`).

- You may also want to remove the Java that was installed for the Acronis Cyber Files Web Server. Java can also be removed from the control panel.

# Upgrading PostgreSQL to a newer major version

Major PostgreSQL releases often add new features that change some of the internal workings of PostgreSQL.

Single server installs can use the complete Same-Server Migration steps.

**Important**

Acronis Cyber Files only supports upgrading PostgreSQL using the Cyber Files installer. The official PostgreSQL distribution is not supported. No version other than the one which is shipped is supported.

**Note**

Upgrading PostgreSQL can be a time-consuming process.

**Important**

We **strongly** recommend that you run a test upgrade outside of your production environment.

# Supplemental Material

## Conflicting Software

There are some software products that may cause problems with Acronis Cyber Files. The currently known conflicts are listed below:

- **VMware View™ Persona Management** - This application will cause issues with the Acronis Cyber Files desktop client syncing process and issues with deleting files. Placing the Acronis Cyber Files sync folder outside of the **Persona Management user profile** should avoid the known conflicts.
- **Anti-virus software** should not scan sync folders, as it may cause conflicts with the sync process. It is recommended that the Acronis Cyber Files Filestore folder is added to your anti-virus' ignore or allow list. Unless you have turned off encryption, all the items in the Filestore folder will be encrypted and the anti-virus will not be able to detect anything but it may cause issues with some items.

## For Acronis Cyber Files Server

### Load balancing Acronis Cyber Files

There are two main ways you can load balance Acronis Cyber Files:

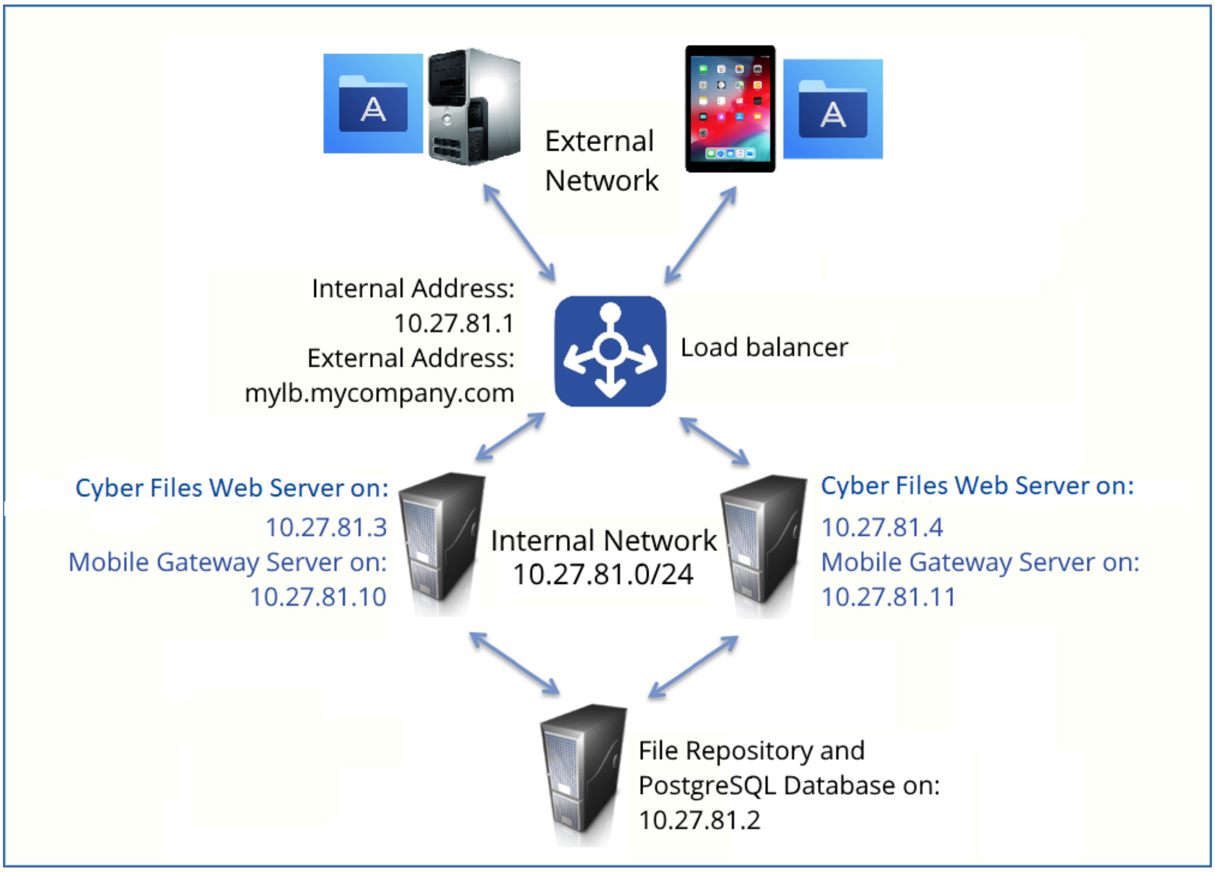
**Load balancing only the Acronis Cyber Files Mobile Gateways**

This configuration ensures that the components under the heaviest loads, the Acronis Cyber Files Mobile Gateway Servers, are load balanced and always accessible for your mobile clients. The Acronis Cyber Files server is not behind the load balancer as it is not required in order to connect to the Acronis Cyber Files Mobile Gateways for unmanaged access. For more information visit the Cluster Groups article.

**Load balancing all of Acronis Cyber Files**

This configuration load balances all of Acronis Cyber Files' components and ensures high-availability for all users. You will need at least two separate machines in order to test this setup. Many of the settings when configuring load balancing differ between different software and hardware so they will not be covered in this guide.

In the setup example we will use three separate machines. One of them will act as our File Repository and Database and the other two as both Acronis Cyber Files Web Servers and Acronis Cyber Files Mobile Gateways. Below you can see a guide on how to configure this setup.


External Network
Internal Address: 10.27.81.1
External Address: mylb.mycompany.com
Load balancer
Cyber Files Web Server on: 10.27.81.3
Mobile Gateway Server on: 10.27.81.10
Internal Network 10.27.81.0/24
Cyber Files Web Server on: 10.27.81.4
Mobile Gateway Server on: 10.27.81.11
File Repository and PostgreSQL Database on: 10.27.81.2

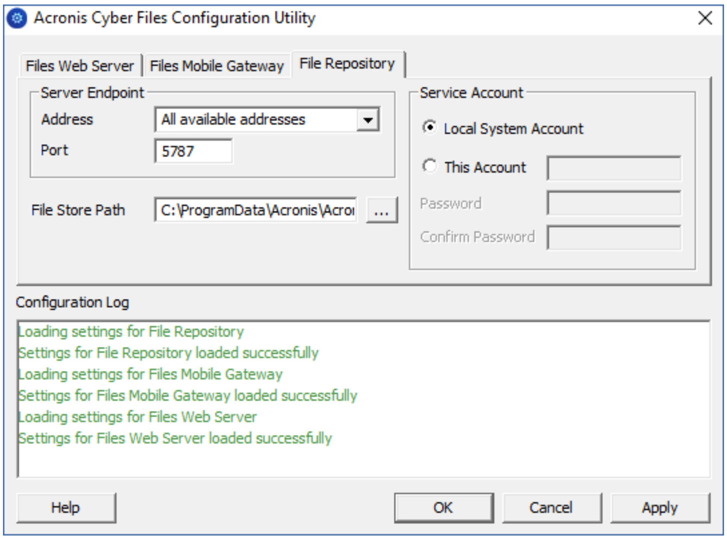
This guide will provide the details necessary to properly load balance the Acronis Cyber Files product in your environment.

## On the server that will be hosting your PostgreSQL database and File Repository, perform the following steps:

1. Start the Acronis Cyber Files installer and press **Next**. Read and accept the license agreement.
2. In the Acronis Cyber Files installer, choose **Custom**, and select **Acronis Cyber Files File Repository** and **PostgreSQL Database Server** and press **Next**.
3. Select where the File Repository and Configuration Utility will be installed.
4. Select where PostgreSQL should be installed and enter a password for the superuser **postgres**.
5. Open TCP port 5432. You will be using it to access the PostgreSQL database from the remote machines.
6. After finishing the installation procedure, proceed with going through the Configuration Utility.
   a. You will be prompted to open the Configuration Utility. Press **OK**.
   b. Select the address and port on which your File Repository will be accessible.

**Note**
You will need to set the same address and port in the Acronis Cyber Files web interface. For more information visit the Using the Configuration Utility and File Repository articles.

c. Select the path to the File Store. This is where the actual files will reside.



Server Endpoint

Address: All available addresses

Port: 5787

File Store Path: C:\ProgramData\Acronis\Acro

Service Account

● Local System Account

○ This Account

Password

Confirm Password

Configuration Log

```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

d. Click **OK** to apply changes and close the **Configuration Utility**.

7. Navigate to the PostgreSQL installation directory (for example, `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\data\`) and edit **pg_hba.conf** with a text editor.
8. Include host entries for each of your Acronis Cyber Files servers using their internal addresses and save the file.The **pg_hba.conf** (HBA stands for host-based authentication) file controls client authentication and is stored in the database cluster's data directory. In it you specify which servers will be allowed to connect and what privileges they will have. e.g.:

```
# TYPE DATABASE USER ADDRESS METHOD

# First Acronis Cyber Files & Gateway server

host all all 10.27.81.3/32 md5

# Second Acronis Cyber Files & Gateway server

host all all 10.27.81.4/32 md5

In these examples all users connecting from the First Acronis Cyber Files server
(10.27.81.3/32) and the second Acronis Cyber Files server (10.27.81.4/32) can access the
database with full privileges (except the replication privilege) via a md5 encrypted
connection.
```

9. If you wish to enable remote access to this PostgreSQL instance, you will have to edit the **postgresql.conf** file. Follow the steps below:

a. Navigate to and open the **postgresql.conf**. By default it is located at: `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\Data\postgresql.conf`

b. Find the line `#listen_addresses = 'localhost'`

c. Enable this command by removing the **#** symbol at the start of the line.

d. Replace `localhost` with ***** to listen on all available addresses. If you want PostgreSQL to listen only on a specific address, enter the IP address instead of *****.

- **e.g.** `listen_addresses = '*'` - This means that PostgreSQL will listen on all available addresses.

- **e.g.**`listen_addresses = '192.168.1.1'` - This means that PostgreSQL will listen only on that address.

e. Save any changes made to the **postgresql.conf**.

f. Restart the Acronis Cyber Files PostgreSQL service.

10. Open the **Acronis Cyber Files  PostgreSQL Administrator tool**.You can find it in Windows Start menu, under the Acronis Cyber Files folder. Connect to your local server, select **Databases**, and either right-click or select **New Database** from the **Edit** -> **New Object** menu to create a new database. Name it **acronisaccess_production**.

**Note**
PostgreSQL uses port 5432 by default. Make sure that this port is open in any firewall or routing software.

## On the two servers that will be acting as both Acronis Cyber Files Servers and Acronis Cyber Files Gateways, perform the following steps:

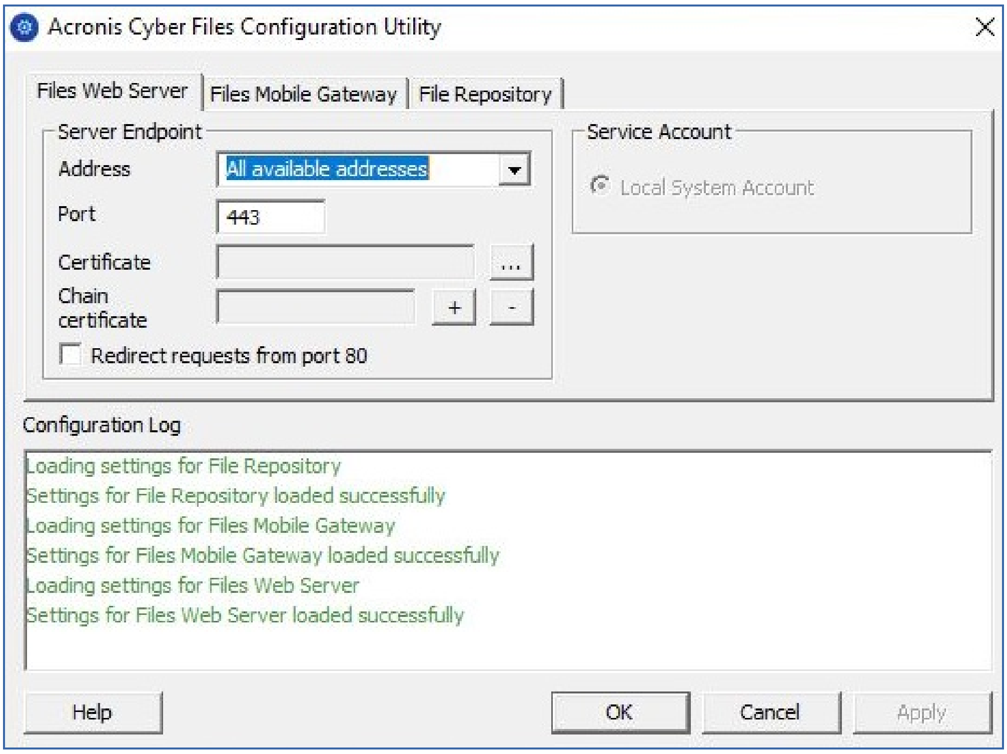
1. Start the Acronis Cyber Files installer and press **Next**. Read and accept the license agreement.
2. In the Acronis Cyber Files installer, choose **Custom**, and select only **Acronis Cyber Files Web Server** and **Acronis Cyber Files Mobile Gateway** and continue with the installation procedure.
3. After finishing the installation procedure, proceed with going through the Configuration Utility.

   a. You will be prompted to open the Configuration Utility. Press **OK**.

   b. **On the AcronisCyber Files Web server tab:**

   - Enter the address and port on which your Acronis Cyber Files management server will be reachable (i.e. 10.27.81.3 and 10.27.81.4).
   - Select your certificate. This should be the same SSL certificate that is tied to the DNS address of the load balancer.
   - Click **Apply**.

   **Note**
   If you don't have a certificate, a self-signed certificate will be created by Acronis Cyber Files. This certificate should NOT be used in production environments.

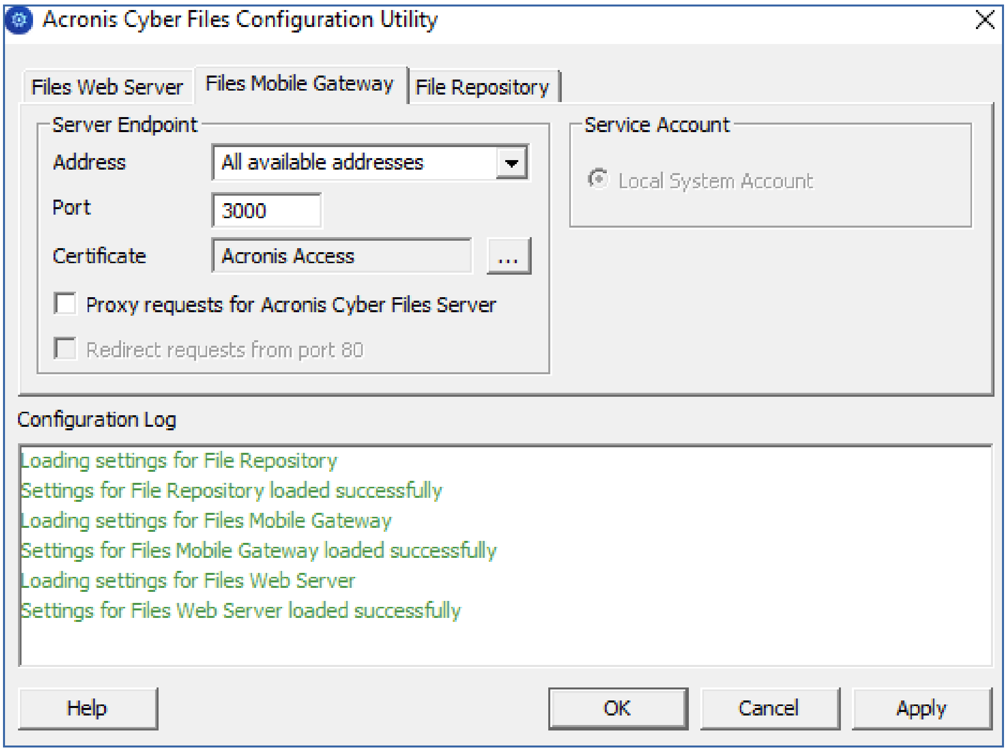


```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

c. **On the Acronis Cyber Files Mobile Gateway tab**:
   - Enter the address and port on which your Gateway Server will be reachable (i.e. 10.27.81.10 and 10.27.81.11).
   - Select your certificate. This should be the same SSL certificate that is tied to the DNS address of the load balancer.
   - Click **Apply**.

**Note**

If you don't have a certificate, a self-signed certificate will be created by Acronis Cyber Files. This certificate should NOT be used in production environments.



Server Endpoint

Address: All available addresses

Port: 3000

Certificate: Acronis Access

□ Proxy requests for Acronis Cyber Files Server

□ Redirect requests from port 80

Service Account

● Local System Account

Configuration Log

```
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Files Mobile Gateway
Settings for Files Mobile Gateway loaded successfully
Loading settings for Files Web Server
Settings for Files Web Server loaded successfully
```

4. Navigate to the Acronis Cyber Files installation directory (e.g. C:\Program Files (x86)\Acronis\Files Advanced\Acess Server\) and edit **acronisaccess.cfg** with a text editor.
5. Set the username, password, and internal address of the server that will be running the PostgreSQL database and save the file. This will configure your Acronis Cyber Files server to connect to your remote PostgreSQL database. e.g.:

```
DB_DATABASE =acronisaccess_production

DB_USERNAME =postgres

DB_PASSWORD =password123

DB_HOSTNAME =10.27.81.2

DB_PORT =5432
```

6. Open Services.msc and restart the Acronis Cyber Files services.

## On one of your Acronis Cyber Files Web Servers and Acronis Cyber Files Mobile Gateways, perform the following steps:

This is the server which you will configure first and it's settings will be replicated across all other servers. After the settings get replicated, all servers will be identical. It does not matter which server you choose.

1. Open Services.msc and restart the **Acronis Cyber Files Tomcat** service. This will populate the database you have created.
2. Visit https://myaccess (i.e. https://10.27.81.3 or https://10.27.81.4) in your web browser and complete the Setup Wizard.
   a. **Under the Licensing tab:**
      - Enter your license key, mark the checkbox and press **Continue**.

b. **Under the General Settings tab:**
   - Enter a Server Name.
   - The Web Address should be the external address of your load balancer (i.e. mylb.company.com). If you are not using port 443 you will have to write the port as well.
   - The Client Enrollment Address should be the external address of your load balancer (i.e. mylb.company.com).
   - Select your Color Scheme.
   - Select the language for the Audit Log messages.

c. **Under the SMTP tab:**
   - Enter the DNS name or IP address of your SMTP server
   - Enter the port of your SMTP server.
   - If you do not use certificates for your SMTP server, unmark **Use secure connection?.**
   - Enter the name which will appear in the "From" line in emails sent by the server.
   - Enter the address which will send the emails sent by the server.
   - If you use username/password authentication for your SMTP server, mark Use SMTP authentication? and enter your credentials.
   - Click **Save**.

d. **Under the LDAP tab:**
   - Mark **Enable LDAP**.
   - Enter the DNS name or IP address of your LDAP server.
   - Enter the port of your LDAP server.
   - If you use a certificate for connections with your LDAP server, mark Use Secure LDAP Connection.
   - Enter your LDAP credentials, with the domain. (for example, mycompany\myname).
   - Enter your LDAP search base.
   - Enter the desired domain(s) for LDAP authentication. (i.e.to enable LDAP authentication for an account with the email joe@glilabs.com, you would enter glilabs.com)
   - Click **Save**.

e. **Under the Local Gateway tab:**

   **Note**
   If you're installing both a Files Advanced Mobile Gateway and the Acronis Cyber Files Web Server on the same machine, the Gateway will automatically be detected and administered by the Acronis Cyber Files Web Server.

   - Set a DNS name or IP address for the local Gateway Server. This is an internal address behind the load balancer (i.e. 10.27.81.10).
   - Click **Save**.

f. **Under the File Repository tab:**
   - The File Repository Address should be the internal address of the server you have created for the file repository role (i.e. 10.27.81.2).

3. Once you've completed the Setup Wizard, press **Finish** and navigate to **Mobile Access** > **Gateway Servers**.
4. It is time to register your second Gateway server:
   a. Enter a **Display name** for the second Gateway.
   b. The **Address For Administration** should be an internal address behind the load balancer (i.e. 10.27.81.11).
   c. Enter the **Administration Key**. You can obtain it by going to the machine on which the Gateway you are adding is installed, navigating to https://mygateway:443 (i.e. https://10.27.81.10 or https://10.27.81.11) and the key will be displayed there. For more information visit the Registering new Gateway Servers article.
   d. Click **Save**.
5. Create a Cluster Group and add all of your Gateway servers to it. Your primary server should be the one you have already gone through the Setup Wizard on. For more information visit the Cluster Groups article.

**Note**

Please make sure that you have already configured a correct Address for Administration on each Gateway before proceeding. This is the DNS or IP address of the Gateway server.

   a. Expand the **Mobile Access** tab.
   b. Open the **Gateway Servers** page.
   c. Click the **Add Cluster Group** button.
   d. Enter a display name for the group.
   e. Enter the internal DNS name or IP address of the load balancer (i.e. 10.27.81.1).
   f. Mark the checkbox for each Gateway you want to be in the group.
   g. Select the Gateway which will control the group's settings. This should be the Gateway which you configured first. All of the existing settings on that Gateway (including assigned Data Sources and excluding the address for administration) will be copied to every Gateway in the group.

## On the load balancer:

1. Enable duration-based session stickiness (or your load balancer's equivalent) on your load balancer and configure it to not expire.
2. If a health-check is required (looking for an HTTP status of 200 to be returned), a ping to https://INTERNALSERVERNAME:MANAGEMENTPORT/signin will satisfy it (i.e. https://myaccessserver1.company.com/signin and https://myaccessserver2.company.com/signin).

Using a browser, open https://mylb.company.com to verify the configuration is working.

## Installing Acronis Cyber Files in a Load Balanced setup

This guide is provided as a general overview on the requirements of a loadbalanced setup and the processes involved in deploying Acronis Cyber Files in a load balanced environment. Your setup may differ from our example, but the way the components interact is the same.

The recommended configuration is to split all of the parts of the Acronis Cyber Files Server onto separate machines behind load balancers. The File Repository and File Store can reside on the same machine.

We strongly recommend that these steps be performed in a test environment. The test deployment should have the same architecture as the planned production setup, along with a couple of test user desktop and mobile clients to ensure compatibility in your environment.

### System Requirements

#### Hardware Requirements

In a production environment, we recommend you have at least three (3) Acronis Cyber Files Tomcat Servers and three (3) Gateway Servers so that in the event that one server were to fail you would still have the load spread over two active servers.

**Note**
This proposed setup assumes that these servers will be hosted on a Virtual Machine server. If multiple servers are used, we recommend low latency interconnects between the guest Virtual Machines.

- 1 Load Balancer for the Acronis Cyber Files Web servers.
- 1 Load Balancer for the Acronis Cyber Files Gateway servers.
- 3 Acronis Cyber Files Tomcat servers, each with 32 GB RAM and a 16 core CPU.
- 3 Acronis Cyber Files Gateway servers, each with 8 GB RAM and a 4 core CPU.

  **Note**
  The Gateway Server cares more about the Disk and Network speeds than the CPU or memory.

- 1 PostgreSQL server with 32 GB RAM and a 16 core CPU.
- 1 File Repository Service + File Store. The parameters of this server are not that important.

#### Network Connections

- The Load Balancer for the Acronis Cyber Files Tomcat Servers must be configured to use the DNS address of the current Acronis Cyber Files .
- The Load Balancer for the Gateway Servers must be configured to use the DNS address of the current Gateway Server.

- The Tomcat server should connect to the Gateway load balancer for the desktop network node syncing and for browsing network nodes on the Web Interface. In this clustered setup, in the Acronis Cyber Files webUI's Administration and Gateway Servers pages, the "Address for client connections" is the external load balancer's address. For the Gateway Servers we also use the "Use Alternate address for Acronis Cyber Files Server connections" setting, and in the "Address for Acronis Cyber Files Web Server connections" is the internal address of the Gateway load balancer.
- The Gateway Server should connect to the Tomcat Load Balancer for the mobile client connections.

**Note**

For the Sync&Share Data Source, you have to modify the address to be the Tomcat load balancer's address.

## Installing and Configuring PostgreSQL

### Installing the PostgreSQL Server component

1. Start the Acronis Cyber Files installer and press **Next**. Read and accept the license agreement.
2. Click **Custom** and select only the PostgreSQL Database Server. Press **Next**.
3. Select where PostgreSQL should be installed and enter a password for the superuser `postgres` and press Next.
4. Select **Open port 5432 in the firewall**. You will be using this port to access the PostgreSQL database remotely.
5. Finish the installation.

### Allowing your Tomcat servers to connect

1. When the installation is complete, navigate to the PostgreSQL **data** folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data`) and open `pg_hba.conf` with a text editor.
2. Include host entries for each of your Acronis Cyber Files Tomcat servers using their internal addresses and save the file.

   The `pg_hba.conf` (HBA stands for host-based authentication) file controls client authentication and is stored in the database cluster's data directory. In it you specify which servers will be allowed to connect and what privileges they will have, e.g.:

   ```
   # TYPE DATABASE USER ADDRESS METHOD

   # Loadbalancer1 (First Acronis Cyber Files & Gateway server)

   host acronisaccess_production postgres 10.144.70.247/32 md5
   ```

   **Note**

   In this example, the user account named `postgres` can connect from the server at 10.144.70.247 and access the `acronisaccess_production` database with full privileges (except the **replication** privilege) via a `md5 encrypted` connection.

### Setting up the proper number of connections

1. Find and change `max_connections` to `510`.
2. Remove the leading # from the following line: `#listen_addresses = 'localhost'.` Replace `localhost` with `*`. It should look like this: `listen_addresses = '*'`
3. Remove the leading # from the following line: `#effective_cache_size = 128MB` and replace **128MB** with **12GB**. It should look like this: `effective_cache_size = 12GB`
4. Add the following note: - `#NOTE: this tuning setting assumes that PostgreSQL is running by itself on a #VM with at least 16 GB RAM. More information at #https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server`
5. Save all changes and close the **postgresql.conf** file.
6. Restart the Acronis Cyber Files PostgreSQL Server service.

## Installing Acronis Cyber Files Servers

### Installing only the Acronis Cyber Files Web Server

1. Start the Acronis Cyber Files installer and accept the license agreement.
2. Select **Custom** and select ONLY the Acronis Cyber Files Tomcat Server.

   **Note**
   Clicking on the Tomcat server automatically selects the PostgreSQL server as well, but you can disable it with a click.

3. Finish the installation and make sure the Acronis Cyber Files Tomcat service is stopped.

### Server Configuration

All settings that you change on one Acronis Cyber Files Web Server must be made the same on all other Acronis Cyber Files Web Servers.

**Note**
Don't forget to add an entry in the `pg_hba.conf` file for each Acronis Cyber Files Web Server!

### Configure the server to connect to the proper database

1. Navigate to the Acronis Cyber Files Web Server folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Access Server`) and open the `acronisaccess.cfg` file. This file tells the server where the PostgreSQL database service is located.
2. Set these values:

```
DB_HOSTNAME =10.144.70.248

DB_PORT =5432

DB_POOLSIZE =250
```

**Note**

`DB_HOSTNAME` is the IP address where the PostgreSQL is now running. In our example, that is 10.144.70.248.

**Note**

We recommend setting `DB_POOLSIZE` to at least 250.

3. Save the file.

## Configure the maximum number of threads

In a load balanced Tomcat setup it is important that the total number of all threads that all Tomcat instances could possibly spawn do not exceed the maximum number of connections the PostgreSQL database is configured to accept.

There are 3 important settings that determine this:

- In the `acronisaccess.cfg` file: `DB_POOLSIZE = 200`. We recommend setting this value to at least 250.
- In the Tomcat `server.xml` file: `maxThreads = 150`. We recommend leaving this set to the default of 150.
- In the `postgresql.conf` file: `max_connections`. This should already be configured in the previous steps. It should not be less than the sum of all the Tomcat DB_POOLSIZE values set for every Acronis Cyber FilesWeb Server + 10. e.g. 510 for 2 Tomcat servers and 760 for 3 Tomcat servers and etc.

**Note**

Changes made to the these files require that you restart their corresponding services.

## Configure proper logging

In a Load balanced configuration, the Acronis Cyber Files Tomcat service does not map the proper IP addresses in the logs. To ensure that each connection is properly logged, make the following changes:

1. In the server.xml file, find the line `<Valve className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t &quot;%r&quot; %s %b”/>`.
2. Add `requestAttributesEnabled=”true”` at the end of it.
3. Under the same line, add the following:
   ```
   <Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
   ```
4. Save the file and restart the Acronis Cyber Files Tomcat Service.

# Installing Gateway Servers

## Installing a new Gateway Server

1. On a new machine, run the Acronis Cyber Files Installer and accept the license agreement.
2. Select **Custom** and install only the Gateway server component. Finish the installation.
3. In the Configuration utility set the Gateway address, port and certificate. This should be the same SSL certificate that is tied to the DNS address of the Gateway load balancer.

# FileStore and File Repository settings

***If you plan on using S3 storage, you do not need to install the File Repository service, as the File Store will be hosted in the S3 storage of your choice.***

## Installing the File Repository service

1. Copy the Acronis Cyber Files installer to the machine where the File Repository and File Store will reside.
2. Start the installer, accept the license agreement and select Custom.
3. Select only the File Repository option and press Next.
4. Select the desired installation paths and press Next.
5. Follow the prompts until the installation is finished.
6. The Configuration Utility will launch. Select the address and port on which the File Repository service will be reachable.
7. Select the destination of the File Store. The default location is `C:\ProgramData\Acronis\Acronis Cyber Files\FileStore`.

   **Note**
   If the File Store is on a remote network share, the computer or user account on which the File Repository service is running must have full permissions to the File Store folder on the network share.

   **Note**
   The account must also have read and write access to the local Repository folder (e.g. C:\Program Files (x86)\Acronis\Acronis Cyber Files\File Repository\Repository) to write the log file.

8. Start Acronis Cyber Files File Repository service.

## Acronis Cyber Files Settings

1. Open the Acronis Cyber Files web interface and log in as an administrator.
2. Navigate to Sync&Share -> File Repository and make sure the File Store Repository Endpoint address is the same one you picked in the Configuration Utility.

### Loadbalancer-specific settings

1. Using a browser, open https://mylb.company.com to verify the configuration is working.
2. Enable duration-based session stickiness (or your load balancer's equivalent) on your load balancer and configure it to not expire.
3. If a health-check is required (looking for an HTTP status of 200 to be returned), a ping to https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version (i.e. https://myaccessserver.company.com/signin and https://myaccessserver.company.com/api/v1/server_version).
4. To ensure the proper logging of IP addresses and connections in a loadbalanced setup, you must configure your loadbalancer to set the following headers:
   - `X-Forwarded-For` This will provide the real ip address of the clients that are connecting instead of each connection showing the ip address of the loadbalancer.
   - `X-Forwarded-Proto` This will provide the real protocol used.

## Migrating to a load balanced configuration

This guide is provided as a general overview on the requirements of a load balanced setup and the processes involved in migration to a load balanced deployment. Your setup may differ from our example, but the way the components interact and their settings are the same.

The recommended configuration is to split all of the parts of the Acronis Cyber Files Server onto separate machines behind load balancers. The File Repository and File Store can reside on the same machine.

Before migrating the production server, we strongly recommend that these steps be performed in a test environment. The test deployment should have the same architecture as the production servers, along with a couple of test user desktop and mobile clients to ensure compatibility in your environment.

***This guide uses an example setup of Acronis Cyber Files running in a standard deployment, with every component is installed on the same machine.***

**Note**

In our example, we will keep the original Acronis Cyber Files Tomcat service running and connect it to the new configuration. This is not mandatory.

***Before proceeding with any changes to your deployment, read our Backup & Recovery articles.***

### System Requirements

#### Hardware Requirements

In a production environment, we recommend you have at least three (3) Acronis Cyber Files Tomcat Servers and three (3) Gateway Servers so that in the event that one server were to fail you would still have the load spread over two active servers.

**Note**

This proposed setup assumes that these servers will be hosted on a Virtual Machine server. If multiple servers are used, we recommend low latency interconnects between the guest Virtual Machines.

- 1 Load Balancer for the Acronis Cyber Files Web servers.
- 1 Load Balancer for the Acronis Cyber Files Gateway servers.
- 3 Acronis Cyber Files Tomcat servers, each with 32 GB RAM and a 16 core CPU.
- 3 Acronis Cyber Files Gateway servers, each with 8 GB RAM and a 4 core CPU.

  **Note**

  The Gateway Server cares more about the Disk and Network speeds than the CPU or memory.

- 1 PostgreSQL server with 32 GB RAM and a 16 core CPU.
- 1 File Repository Service + File Store. The parameters of this server are not that important.

### Network Connections

- The Load Balancer for the Acronis Cyber Files Tomcat Servers must be configured to use the DNS address of the current Acronis Cyber Files .
- The Load Balancer for the Gateway Servers must be configured to use the DNS address of the current Gateway Server.
- The Tomcat server should connect to the Gateway load balancer for the desktop network node syncing and for browsing network nodes on the Web Interface. In this clustered setup, in the Acronis Cyber Files webUI’s Administration and Gateway Servers pages, the “Address for client connections” is the external load balancer’s address. For the Gateway Servers we also use the “Use Alternate address for Acronis Cyber Files Server connections” setting, and in the “Address for Acronis Cyber Files Web Server connections” is the internal address of the Gateway load balancer.
- The Gateway Server should connect to the Tomcat Load Balancer for the mobile client connections.

**Note**

For the Sync&Share Data Source, you have to modify the address to be the Tomcat load balancer’s address.

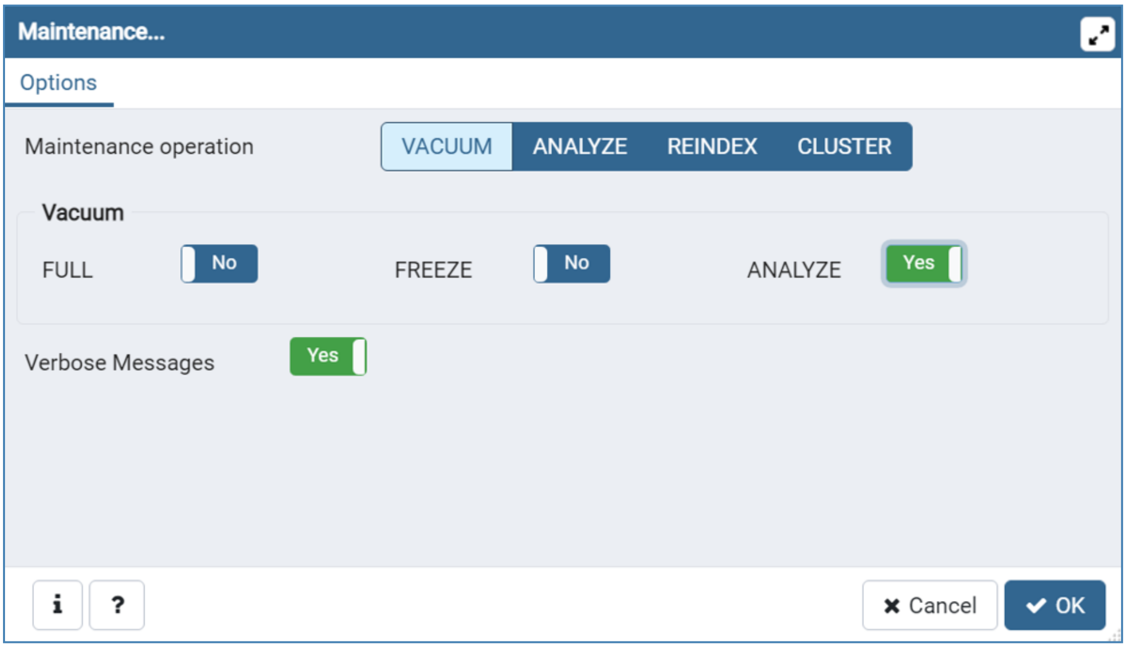
## Migrating the PostgreSQL server

Your database is the most important component and should be migrated first.

### Configuration on your existing PostgreSQL server

1. Open the **Services** control panel (`services.msc`) and stop the **Acronis Cyber Files Tomcat** service.

2. Open the **Acronis Cyber Files PostgreSQL Administrator** application and connect to the database server. Click the **+** next to **Databases**.
3. Right click on the `acronisaccess_production` database.
4. Choose **Maintenance**.
5. Select **VACUUM** and set **ANALYZE** to 'Yes'.



Maintenance operation: VACUUM

Vacuum

FULL: No

FREEZE: No

ANALYZE: Yes

Verbose Messages: Yes

6. Click **OK**.
7. Open an elevated command prompt and navigate to the Postgres **bin** directory with the **cd** command. (by default `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\bin`).
8. Once your current Command Prompt directory is the **bin** folder, enter the following command:

```
pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql
```

**Note**

**alldbs.sql** will be the generated backup file and will be saved in the **bin** folder. It can include a full path if you want it to be saved elsewhere, for instance **D:\Backups\alldbs.sql.**

**Note**

If you are using a different port and/or a different user, change the command accordingly.

9. Once the backup finishes, stop and disable the **Acronis Cyber Files PostgreSQL Server** service.
10. Copy and move the backup file to the new machine which will be hosting PostgreSQL.

## Configurations on your new PostgreSQL server

1. Start the Acronis Cyber Files installer and press **Next**. Read and accept the license agreement.
2. Click **Custom** and select only the PostgreSQL Database Server. Press **Next**.
3. Select where PostgreSQL should be installed and enter a password for the superuser `postgres`.

**Note**

The location should be reachable by all other server and the password should be the same as previously used on the original PostgreSQL server.

4. Select **Open port 5432 in the firewall** and proceed with the installation. You will be using this port to access the PostgreSQL database remotely.

## Configuring access to the PostgreSQL database

1. When the installation is complete, navigate to the PostgreSQL **data** folder (by default `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data`) and open `pg_hba.conf` with a text editor.
2. Include host entries for each of your Access Tomcat servers using their internal addresses and save the file. If you do not know all the servers' addresses, you can come back at a later time and edit the file, but until you do, the servers will not be able to connect to the database.

   The `pg_hba.conf` (HBA stands for host-based authentication) file controls client authentication and is stored in the database cluster’s data directory. In it you specify which servers will be allowed to connect and what privileges they will have, e.g.:

   ```
   # TYPE DATABASE USER ADDRESS METHOD

   # Loadbalancer1 (First Acronis Cyber Files & Gateway server)

   host acronisaccess_production postgres 10.144.70.247/32 md5
   ```

**Note**

In this example, the user account named `postgres` can connect from the server at 10.144.70.247 and access the `acronisaccess_production` database with full privileges (except the **replication** privilege) via a `md5 encrypted` connection.

## Open the postgresql.conf file and make the following changes

1. Remove the leading # from the following line: `#listen_addresses = 'localhost'.` Replace `localhost` with `*`. It should look like this: `listen_addresses = '*'`
2. Remove the leading # from the following line: `#effective_cache_size = 128MB` and replace **128MB** with **12GB**. It should look like this: `effective_cache_size = 12GB`
3. Add the following note: - `#NOTE: this tuning setting assumes that PostgreSQL is running by itself on a #VM with at least 16 GB RAM. More information at #https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server`
4. Find and change `max_connections` to the correct value. It should not be less than the sum of all the Tomcat `DB_POOLSIZE` settings configured for every Access Server node + 10. We recommend setting `DB_POOLSIZE` to `250`.

   In our example, we have set the `DB_POOLSIZE to 250`, and we have two Access Tomcat Servers, so `max_connections` should be set to `510`. For three Access Tomcat Servers it would be `760`.
5. Save all changes and close the **postgresql.conf** file.
6. Restart the Acronis Cyber Files PostgreSQL Server service.

### Importing your database

#### On the new PostgreSQL server

1. Open the Acronis Cyber Files PostgreSQL Administrator application, connect to the local database server, select **Databases**, and confirm there is a database called `acronisaccess_production`.
2. Copy the backup database file **alldbs.sql** into the **bin** directory of your PostgreSQL installation. (by default `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin`)
3. Open an elevated command prompt window and navigate to the PostgreSQL **bin** directory using the **cd** command.
4. Enter the following command: `psql -U postgres -f alldbs.sql`
5. Enter the password for the `postgres` user when prompted for it. This will restore the database from the old PostgreSQL server to the new PostgreSQL server.

## Acronis Cyber Files Server Configurations

### Connecting additional Acronis Cyber Files Servers

#### Installing only the Acronis Cyber Files Web Server

1. Start the Acronis Cyber Files installer and accept the license agreement.
2. Select **Custom** and select ONLY the Acronis Cyber Files Web Server.

   **Note**
   Clicking on the Acronis Cyber Files Web Server, automatically selects the PostgreSQL server as well, but you can disable it with a click.

3. Finish the installation and make sure the Acronis Cyber Files Tomcat service is stopped.

#### Server Configuration

All settings that you change on one Acronis Cyber Files Web Server must be made the same on all other Acronis Cyber Files Web Servers.

**Note**
Don't forget to add an entry in the `pg_hba.conf` file for each Acronis Cyber Files Web Server!

# Configure the server to connect to the proper database

1. Navigate to the Acronis Cyber Files Web Server folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Access Server`) and open the `acronisaccess.cfg` file. This file tells the server where the PostgreSQL database service is located.
2. Set these values:

```
DB_HOSTNAME =10.144.70.248

DB_PORT =5432

DB_POOLSIZE =250
```

**Note**
`DB_HOSTNAME` is the IP address where the PostgreSQL is now running. In our example, that is 10.144.70.248.

**Note**
We recommend setting `DB_POOLSIZE` to at least 250.

3. Save the file.

## Configure the maximum number of threads

In a load balanced Tomcat setup it is important that the total number of all threads that all Tomcat instances could possibly spawn do not exceed the maximum number of connections the PostgreSQL database is configured to accept.

There are 3 important settings that determine this:

- In the `acronisaccess.cfg` file: `DB_POOLSIZE = 200`. We recommend setting this value to at least 250.
- In the Tomcat `server.xml` file: `maxThreads = 150`. We recommend leaving this set to the default of 150.
- In the `postgresql.conf` file: `max_connections`. This should already be configured in the previous steps. It should not be less than the sum of all the Tomcat DB_POOLSIZE values set for every Acronis Cyber FilesWeb Server + 10. e.g. 510 for 2 Tomcat servers and 760 for 3 Tomcat servers and etc.

**Note**
Changes made to the these files require that you restart their corresponding services.

## Configure proper logging

In a Load balanced configuration, the Acronis Cyber Files Tomcat service does not map the proper IP addresses in the logs. To ensure that each connection is properly logged, make the following changes:

1. In the server.xml file, find the line `<Valve className=”org.apache.catalina.valves.AccessLogValve” directory=”logs” prefix=”localhost_access_log.” suffix=”.txt” pattern=”%h %l %u %t &quot;%r&quot; %s %b”/>`.
2. Add `requestAttributesEnabled=”true”` at the end of it.
3. Under the same line, add the following:

```
<Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
```

**Warning!**

If IP address restrictions feature is also in use, avoid setting the XFF header because this may affect user's security, related to that feature. Instead, it is recommended to configure the load balancing to trust XFF addresses, added by a proxy. In this case, the XFF header from the requests will be copied too (if there is already such).

4. Save the file and restart the Acronis Cyber Files Tomcat Service.

### Connecting the old Acronis Cyber Files server

If you wish to keep using your existing Acronis Cyber Files server, you can, but you need to connect it to the new database.

### Connecting Acronis Cyber Files to the remote database

1. Navigate to the Acronis Cyber Files Server folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Access Server`) and open the `acronisaccess.cfg` file. This file tells the server where the PostgreSQL database service is located.
2. Set these values to the following:

   ```
   DB_HOSTNAME =10.144.70.248
   DB_PORT =5432
   DB_POOLSIZE = 250
   ```

**Note**

`DB_HOSTNAME` sets the IP address where the PostgreSQL database is. In this example, it is 10.144.70.248.

3. Save the file and then start the **Acronis Cyber Files Tomcat Service** in the **Services** control panel (services.msc).
4. All unused Acronis Cyber Files components can be uninstalled.

## FileStore and File Repository migration

Please read our Moving the File Store and File Repository guide. The only additional setting you may need to check, is to verify that all Acronis Cyber Files components have access to the machine that will host the File Repository and File Store.

If you plan on using S3 storage, you do not need to install the File Repository service, as the File Store will be hosted in the S3 storage of your choice.

If you plan on keeping the File Repository and File Store where they are, you only need to make sure that your new Acronis Cyber Files servers are pointing to the proper Repository endpoint.

# Migrating Your Gateway Server

## Installing a new Gateway Server

1. On a new machine, run the Acronis Cyber Files Installer and accept the license agreement.
2. Select **Custom** and install only the Gateway server component. Finish the installation.
3. In the Configuration utility set the Gateway address, port and certificate. This should be the same SSL certificate that is tied to the DNS address of the Gateway load balancer.

## Migrating all settings from the previous Gateway Server

1. On the old machine with both Tomcat and the Gateway, open the Acronis Cyber Files web interface and open the Gateway Servers page. You will see an entry for the old Gateway.
2. Add the new Gateway by pressing **Add Gateway Server** and entering all the relevant data.
3. Click **Add Cluster Group**.
   - Enter a display name,
   - Enter the **Address for client connections**. In the cluster the “**Address for client connections**” is the external load balancer address, and then click the “**Use Alternate address for … Server connections**”, and in the “**Address for Acronis Cyber Files  Server connections**” enter the internal address of the Gateway load balancer.
4. Under **Gateway Servers Available for Clustering** check the **Include** box for both Gateway Servers.
5. Under **Gateway Server to use for Settings** select the old Gateway server.
6. Click **Add** and on the Gateway Server page you will see the new cluster. Expand it with the +.
7. The new Gateway should now have all settings migrated to it. Make the new Gateway the master of the cluster by clicking on the **Actions** drop down menu for it and picking **Become Group Master**.
8. You can leave the old Gateway as-is, Remove it from the Cluster Group or Remove and Delete it. We recommend leaving it as part of the cluster until your set up is all up and running correctly.

# Log Management and Purging

After installing additional Acronis Cyber Files servers, make sure to go to the folder where the Acronis Cyber Files Tomcat Logs are kept and set the correct permissions on those folders so the Logs can be written and purged.

# Loadbalancer-specific settings

1. Using a browser, open https://mylb.company.com to verify the configuration is working.
2. Enable duration-based session stickiness (or your load balancer’s equivalent) on your load balancer and configure it to not expire.
3. If a health-check is required (looking for an HTTP status of 200 to be returned), a ping to https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version (i.e.

https://myaccessserver.company.com/signin and https://myaccessserver.company.com/api/v1/server_version).

4. To ensure the proper logging of IP addresses and connections in a loadbalanced setup, you must configure your loadbalancer to set the following headers:
   - `X-Forwarded-For` This will provide the real ip address of the clients that are connecting instead of each connection showing the ip address of the loadbalancer.
   - `X-Forwarded-Proto` This will provide the real protocol used.

## Cleanup of the original server(s)

If you continue to use the Acronis Cyber Files Tomcat that is on the original production server, we recommend that you uninstall the Acronis Cyber Files items that are no longer in use on that server.

From the control panel you can uninstall the Acronis Cyber Files PostgreSQL Server, Acronis Cyber Files Gateway Server, and the Acronis Cyber Files File Repository Server (if there is one).

# Customizing the Web Interface through the API

Using the API to update your web interface's color scheme can be done easily and without having to restart any services or have any downtime. Some of these customizations can be done through the web interface of Acronis Cyber Files .

## Installing CURL

1. You will need to install Curl in order to use any API commands.
   a. Download Curl from the official site at: https://curl.haxx.se/download.html

   **Note**
   Make sure to download a version that supports SSL!

   b. Follow the prompts from the Curl installer until the installation is finished or just extract the Curl archive.

## Creating a custom color scheme

1. Open an elevated command prompt and enter the following command:

```
curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@<path_to_
file> -F customization_settings[color_scheme_client_scss_file]=@<path_to_file> -u
<user>:<password> https://<your_site>/api/v1/settings/customization -v
```

   **Note**
   The filenames have to use a specific naming syntax! `color_scheme_`<**name_of_scheme>**.css for the Administration console and `web_client_`<**name_of_scheme>**.scss for the Web client console. <**name_of_scheme>** is the name of your new scheme which will be displayed in the Acronis Cyber Files interface and it must be the same for both files.

The above command will:

- Select a **.css** file for the Administration console.
- Select a **.scss** file for the Web Client console.
- Create a new theme which will be selectable from the **Color Scheme** drop-down in the web interface.

**Note**

If you only wish to change one part of a color scheme, when entering the above command, you must use the new .css scheme for the changed part and the existing .css scheme for the part you do not want to change.

2. Here is an example of how the command looks if you want to upload a scheme for the Administration part of the interface and a scheme for the web client that are located.
3. In this example both files are located in `D:\WebUI` and we pick **NewColor** as the color scheme name that will be visible in the web interface:

```
curl -X PUT -F customization_settings[color_scheme_administration_css_
file]=@D:\WebUI\color_scheme_NewColor.css -F customization_settings[color_scheme_client_
scss_file]=@D:\WebUI\web_client_NewColor.scss -u administrator:123456
https://myCompany.com/api/v1/settings/customization
```

4. You can also use the `-F customization_settings[color_scheme]=<name_of_scheme>` command to switch your current theme to the new theme you are adding. Adding this command to the rest looks like this:

```
curl -X PUT -F customization_settings[color_scheme_administration_css_
file]=@D:\WebUI\color_scheme_NewColor.css -F customization_settings[color_scheme_client_
scss_file]=@D:\WebUI\web_client_NewColor.scss -F customization_settings[color_
scheme]=NewColor -u administrator:123456
https://myCompany.com/api/v1/settings/customization -v
```

## Troubleshooting

- The command executes but you don't see the new theme in the interface

  Make sure that file names follow the proper syntax of **color_scheme_<name_of_scheme>.css** and **web_client_<name_of_scheme>.scss**
- Getting a **Protocol https not supported or disabled in libcurl** error

  Remove any single-quotes ('') surrounding your address. If you need to use quotes, use double-quotes ("") instead. e.g. "https://myCompany.com/api/v1/settings/customization"
- Getting a certificate error

  If you are using self-signed certificates or are running the commands using an IP address, you will need to add the **-k** flag at the end of the command, to ignore certificate errors.

# Unattended desktop client configuration

With the use of Microsoft's Group Policy Management, you can easily install and setup the Acronis Cyber Files Desktop client on multiple machines remotely. The only thing end users will have to do is start the client and enter their password. The Group Policy Management also ensures that users cannot change/replace the correct settings by accident. If this happens, they can simply log off and when they log in, the correct settings will be re-applied.

**Creating and configuring theGroup Policy Managementobject:**

1. On your domain controller, open the **Group Policy Management** console.
2. Right-click on your desired domain and select **Create a GPO in this domain, and Link it here...**.
3. Give it a name and press **OK**.
4. Expand the **Group Policy Objects** section and select your new policy.
5. Under the **Scope** tab select the desired sites, domains, OUs, groups, users and/or computers.

# Unattended installation of the client

This section will help you install the Acronis Cyber Files Desktop client silently on user login on all desired machines.

## Creating an installer distribution point

All computers that will have the client installed, must have access to the installer. This is done by creating a folder, sharing it with the desired user group and placing the installer in it.

1. Right-click on the folder with the installer and select **Properties**.
2. Open the **Sharing** tab and press **Share**.
3. Enter the domain group, OU or users that you will install the Access client on. This group (or etc.) should be the same as the one you select for the **Group Policy Object**.
4. Press **OK**/**Done** and close all remaining dialogs.

**Note**
Make sure that the installer is reachable by the desired machines by its network address (e.g. `\\WIN2008\Software\AAClientInstaller.msi`)

## Getting the installer on the user's machine

1. On the domain controller, expand the **Group Policy Objects** section and right click on your new Policy Object.
2. Select **Edit** and expand **User Configuration** -> **Preferences** -> **Windows Settings** -> **Files**.
3. Right-click on Files and select New -> File.
4. Select **Create** for **Action**.

5. For **Source file(s)** either click on the browse button and navigate to the Access client installer or enter the full path to it. (e.g. \\WIN2008\Software\AAClientInstalelr.msi)
6. For **Destionation file** enter the destination folder and destination filename. This will copy the Access client installer from the network share and will place it in the destination folder on the user's machine on logon.

   > **Note**
   > If you enter **C:\Folder\ThisFile.msi,** the client installer will get placed in the user's **C** drive, in the folder Folder and will be named **ThisFile.msi**.

7. Press **OK**.

## Installing the client

### Making the installation script

1. Create an empty text file and paste the following script into it:

   ```
   msiexec /i "C:\AAC.msi" /quiet
   sleep 180
   DEL /F /S /Q /A "C:\AAC.msi"
   ```

   This script will open a command prompt, install the Access client without displaying anything and delete the Access client installer after 3 minutes.
2. Change the path `C:\AAC.msi` in both places, to the path you entered in the **Destination File** field and press **File** -> **Save As...**.
3. Enter a name for the script and make sure it ends with **.bat**. For the **Save as type:** field, select **All Files**. Make sure that the file is either on the domain controller or is reachable by it. This file is important and must not be changed or deleted so place it in a specific location that won't get changed.

### Using the script on user logon

1. Open the **Group Policy Manager** and expand the **Group Policy Objects** section and right click on your new **Policy Object**.
2. Select **Edit** and expand **User Configuration** -> **Policies** -> **Windows Settings** -> **Scripts (Logon/Logoff)**.
3. Double-click on **Logon** and press **Add**.
4. In the **Add Script** dialog, press **Browse (...)** and navigate to the folder where you saved the script.
5. Select the script and press **Open**.
6. Press **OK** and press **OK** again on the following dialog.
7. Done. All users in the specified group or OU will now get the Acronis Cyber Files client installed on logon.

## Creating the folder and registry entries:

In this example we will create entries for the Username, Sync-Folder, Server URL, the Auto-Update checkbox and if the client should connect to servers with self-signed certificates.

1. Expand the **Group Policy Objects** section and right click on your new Policy Object.
2. Select **Edit** and expand **User Configuration** -> **Preferences** -> **Windows Settings**.

**Creating the sync folder:**

1. Right-click on **Folders** and select **New** -> **Folder**.
2. Set the **Action** to **Create**.
3. For the path, enter the following token: `%USERPROFILE%\Desktop\AAS Data Folder`

**Creating the registry:**

1. Right-click on **Registry** and select **New** -> **Registry Item**.
2. Set the **Action** to **Create**.
3. For **Hive**, select **HKEY_CURRENT_USER**.
4. For the path, enter the following: `Software\Group Logic, Inc.\activEcho Client\`
5. Now do the following for the desired entries:
6. For the Username:
   a. For **Value name** enter "**Username**".
   b. For **Value type** select **REG_SZ**.
   c. For **Value data** enter the following token: `%USERNAME%@%USERDOMAIN%`

   **Note**
   If you wish to use **Single Sign-on**, do **not** configure the Username token. Instead, do the following:

   - **For SSO**:
   - For **Value name** enter "**AuthenticateViaSSO"**.
   - For **Value type** select **REG_SZ**.
   - For **Value data** enter **1**.
7. For the Server URL:
   a. For **Value name** enter "**Server URL**".
   b. For **Value type** select **REG_SZ**.
   c. For **Value data** enter the address of your Acronis Cyber Files server. e.g. **https://myaccess.com**
8. For the Sync-Folder:
   a. For **Value name** enter "**activEcho Folder**".
   b. For **Value type** select **REG_SZ**.
   c. For **Value data** enter the following token and path: `%USERPROFILE%\Desktop\AAS Data Folder`
9. For the Auto-Update:

   a. For **Value name** enter "**AutoCheckForUpdates**".
   b. For **Value type** select **DWORD**.
   c. For **Value data** enter "**00000001**". The value "**1**" enables this setting and the client will automatically check for updates. Setting the value to "**0**" will disable the setting.

10. For the Certificates:
    a. For **Value name** enter "**AllowInvalidCertificates**".
    b. For **Value type** select **DWORD**.
    c. For **Value data** enter "**00000000**". The value "**0**" disables this setting and the client will not be able to connect to Acronis Cyber Files servers with invalid certificates. Setting the value to "**1**" will enable the setting.

## Configuring Single Sign-On

This guide will lead you through an advanced configuration to enable Single Sign-On functionality with Acronis Cyber Files.

**Note**
Single Sign-On is only usable in a working domain.

**Note**
Single Sign-On does **NOT** work when you are running Acronis Cyber Files in a single port configuration (when the Gateway Server is proxying the requests for the Acronis Cyber Files server).

**Note**
Single Sign-On does **NOT** work if Acronis Cyber Files is installed on the Domain Controller. In addition, even disregarding the SSO limitations, it is highly recommended for performance reasons that the Acronis Cyber Files server not be installed on a Domain Controller.

The Single Sign-On functionality allows all valid LDAP users to login to the web interface and desktop client without having to enter their credentials. The user must have a Acronis Cyber Files account or LDAP Provisioning must be enabled on the server.

- Acronis Cyber Files displays a link on the login page that will log in the user with the account that was used to login into this computer.

  **Note**
  You have to open the Acronis Cyber Files interface using its FQDN (e.g. https://access.company.com) for SSO to work. Single Sign-on does **NOT** work if you open the interface via IP address.

  UPNs should be in the same domain as the main SSO setup for users to be able to access their Sync & Share folder via KCD from mobile applications.

- For the Desktop Client, there is a new radio button that enables SSO. The users will only have to enter the Acronis Cyber Files server's URL. It will automatically log them in with the account that they have used to login into the computer.

**Note**
This will work only for the Windows client. Mac support will come in a follow-up release.

**Note**
Single Sign-On from a Desktop Client requires access to the corporate network. This means that SSO users should have access to their own network as well.

## Acronis Cyber Files Web Server and Gateway on the same machine

This configuration is the most common and consists of 1 Acronis Cyber Files Web server and 1 Acronis Cyber Files Gateway server, with both residing on the same machine. This is the default installation.

### On the Domain

This is a one-time step that must be performed in order to register the Acronis Cyber Files Web Server with the Kerberos server on the domain. We will use 'setspn.exe' to specify which LDAP account will be queried for SSO authentication checks.

**Note**
If you want to use **mobile clients with certificate authentication**, the DNS entry for the Acronis Cyber Files Web Server **must be different** than the name of the computer. If the Acronis Cyber Files Web Server's SPN is just the name of the computer, the Gateway server will treat the Acronis Cyber Files Web Server as "on my machine", and will not attempt to perform Kerberos authentication.
For example, `computerAccess.domain.com` / `computer.domain.com` and `computerAccess.domain.com` / `computerGW.domain.com` will work and `computer.domain.com` / `computerGW.domain.com` will NOT work.

### Configuring the LDAP account that will handle SSO

**Note**
If you want to use SMB or SharePoint Data Sources, you must configure the Active Directory account to permit Kerberos delegation to each of your SMB and SharePoint data sources. For more information, please visit the Advanced Delegation Configurations article.

1. Open a command prompt.

   **Note**
   You must be logged in with a domain account and have the rights to use **setspn**

2. Enter the command `setspn -s HTTP/`**computername.domain.com account name**

**e.g.** If your Acronis Cyber Files Web Server is installed on `ahsoka.acme.com` and you want to use `john@acme.com` as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:

```
setspn -s HTTP/ahsoka.acme.com john
```

**Note**
The LDAP account name used in the command above **MUST** match the account which you will specify by the `spnego.preauth.username` property in `web.xml`.

**Note**
This account will typically match the LDAP account specified by the administrator in the Acronis Cyber Files web interface at **General Settings** -> **LDAP** -> **LDAP Username** / **LDAP Password**, but this is not mandatory.

3. If your Acronis Cyber Files Web Server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number.
   **e.g.** If your server is running on port 444, the command will be:
   ```
   setspn -s HTTP/ahsoka.acme.com:444 john
   ```

**Note**
The **HTTP** in the commands above refer to the **HTTP** service class, not the **HTTP** protocol. The **HTTP** service class handles both **HTTP** and **HTTPS** requests. You do not need to, and **should NOT**, create an SPN using **HTTPS** as a service class name.

4. Go to the domain controller and open **Active Directory Users and Computers**.
5. Find the user that you used in the above commands (in this case - **john**).
6. Click on the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**.
7. Press **OK**.

## Configuring the SPN for the Gateway Server

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running setspn and specifying the hostname of the server on which it is running as the 'user' in the setspn command.

**For this configuration to work, you will need to set an additional DNS entry for your Gateway server.**

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (`A record`) for the Gateway server.
2. Enter a name. This will be the DNS address that will be used to reach the Gateway server.
   **e.g.**`ahsoka-gw.acme.com`

3. Enter the IP address of the Gateway Server (without the port). If you're running the Gateway and the Acronis Cyber Files Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.
5. Go back to the machine with Acronis Cyber Files.
6. Open the command prompt.
7. Enter the following **setspn** command: `setspn -s HTTP/`**gatewaydns.domain.com computername**

   For example, if you gateway server is running on host `'ahsoka'` in the domain and your DNS entry is `ahsoka-gw.acme.com`, run this command:

   ```
   setspn -s HTTP/ahsoka-gw.acme.com ahsoka
   ```
8. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/ahsoka-gw.acme.com:444 ahsoka
   ```
9. Change your desired Gateway Server's **Address for administration** and **Address for client connections** to the new Gateway Server DNS entry you created in step 4.

   **Note**

   Both addresses should be the same and should be updated to the correct DNS entry.

### On the Acronis Cyber Files server

## Setting the domain account that will be used for Single Sign-on authentication

1. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`
2. Find and open the file `web.xml`. In this file you will set the domain username and password that the SSO service will run under. This account **must** match the account that you used to register the HTTP service with Kerberos in the **On the Domain** section.
3. In `web.xml` there are two properties that need to be set - the domain username and password that the SSO service will use. Find the following lines:

   ```
   <init-param>
     <param-name>spnego.preauth.username</param-name>
     <param-value>yourusername</param-value>
     </init-param>
     <init-param>
     <param-name>spnego.preauth.password</param-name>
     <param-value>yourpassword</param-value>
     </init-param>
   ```
4. Replace **yourusername** with the desired LDAP username.

5. Replace **yourpassword** with the LDAP password for the LDAP account specified above. If you have one of these five special characters in your password: **&**, **>**, **"**, **'** , or **<**, you will have to properly escape them in the XML document. To do so, you will have to replace them with the following:
   - **<** with **&lt;**
   - **>** with **&gt;**
   - **"** with **&quot;**
   - **'** with **&apos;**
   - **&** with **&amp;**

   e.g. if your password is `<my&best'password"` you will have to write it in the `web.xml` file as follows: `&lt;my&amp;best&apos;password&quot;`

## Setting the Kerberos domain lookup

1. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf`
2. Find and open the file `krb5.conf`
3. In `krb5.conf` there are only two properties that are needed from the administrator:
   a. The domain for single sign-on (e.g., `ACME.COM`). Please note that this is the name of your domain, **not** the DNS name of the server.

   **Note**
   The domain in `krb5.conf` must always be in **UPPERCASE** or Kerberos ticket lookups may fail.

   b. The Kerberos Key Distribution Center's address (typically matches the address of your primary domain controller; e.g., `acmedc.ACME.COM`)
4. The `krb5.conf` file that we install looks like this:

```
[libdefaults]
   default_realm = ACME.COM
   default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   permitted_enctypes  = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   [realms]
   ACME.COM = {
   kdc = acmedc.ACME.COM
   default_domain = ACME.COM
   [domain_realm]
   .ACME.COM = ACME.COM
```

5. Replace all instances of `ACME.COM` with your domain (**in uppercase!**). Please note that this is the name of your domain, **not** the DNS name of the server.
6. Replace the value for "`kdc =`" with the name of your domain controller. The domain must be written in uppercase. e.g. `kdc = yourdc.YOURDOMAIN.COM`

7. After the above configuration files are updated the Acronis Cyber Files server (the Acronis Cyber Files Tomcat service) must be restarted in order for the changes to take effect.

## Enabling Single sign-on in the web interface:

1. Open the Acronis Cyber Files web interface and log in as an administrator.
2. Expand the **General Settings** tab and open the **LDAP** page.
3. At the bottom of the page, enable the checkbox **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials.**
4. Click **Save**.

### Adding more Gateway Servers

**Note**
These steps work only if the machines that will host the Gateway Servers are in the same domain as the Acronis Cyber Files Web Server.

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running setspn and specifying the hostname of the server on which it is running as the 'user' in the setspn command.

## For any Gateway Servers that reside on a different machine from the Acronis Cyber Files Web Server

1. Open the command prompt.
2. Enter the following **setspn** command: `setspn -s HTTP/`**computername.domain.com computername**

   For example, if you gateway server is running on host `'cody'` in the domain, run this command:

   ```
   setspn -s HTTP/cody.acme.com cody
   ```
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/cody.acme.com:444 cody
   ```
4. Repeat this section for all additional Gateway servers.

### One-time Configuration for a Domain Forest

There is a minor, one-time configuration that must be done to enable Single Sign-On support for the browser.

**Important**
This must be done for each user, on each machine.

**Note**

In the config instructions, we use *acme.com* as an example. If you have services in multiple domains, repeat the steps which specify *acme.com* for all your domains. (**e.g.** add `*.acme.com` and `*.another.com and *.yetanother.com`).

## Acronis Cyber Files Server and Gateway on separate machines

### On the Domain

This is a one-time step that must be performed in order to register the Acronis Cyber Files Server with the Kerberos server on the domain. We will use 'setspn.exe' to specify which LDAP account will be queried for SSO authentication checks.

**Note**

If you want to use **mobile clients with certificate authentication**, the DNS entry for the AcronisCyber Files Web Server **must be different** than the name of the computer. If the AcronisCyber Files Web Server's SPN is just the name of the computer, the Gateway server will treat the AcronisCyber Files Web Server as "on my machine", and will not attempt to perform Kerberos authentication.

For example:

`computerAccess.domain.com` / `computer.domain.com` and `computerAccess.domain.com` / `computerGW.domain.com` will work and `computer.domain.com` / `computerGW.domain.com` will NOT work.

### Configuring the LDAP account that will handle SSO

**Note**

If you want to use SMB or SharePoint Data Sources, you must configure the Active Directory account to permit Kerberos delegation to each of your SMB and SharePoint data sources. For more information, please visit the Advanced Delegation Configurations article.

1. Open a command prompt.

   **Note**

   You must be logged in with a domain account and have the rights to use **setspn**

2. Enter the command `setspn -s HTTP/`**computername.domain.com account name**

   **e.g.** If your Acronis Cyber Files server is installed on `ahsoka.acme.com` and you want to use `john@acme.com` as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:

   ```
   setspn -s HTTP/ahsoka.acme.com john
   ```

**Note**

The LDAP account name used in the command above **MUST** match the account which you will specify by the `spnego.preauth.username` property in `web.xml`.

**Note**

This account will typically match the LDAP account specified by the administrator in the Acronis Cyber Files web interface at **General Settings** -> **LDAP** -> **LDAP Username** / **LDAP Password**, but this is not mandatory.

3. If your Acronis Cyber Files server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number.

   **e.g.** If your server is running on port 444, the command will be:

   ```
   setspn -s HTTP/ahsoka.acme.com:444 john
   ```

**Note**

The **HTTP** in the commands above refer to the **HTTP** service class, not the **HTTP** protocol. The **HTTP** service class handles both **HTTP** and **HTTPS** requests. You do not need to, and **should NOT**, create an SPN using **HTTPS** as a service class name.

4. Go to the domain controller and open **Active Directory Users and Computers**.
5. Find the user that you used in the above commands (in this case - **john**).
6. Click on the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**.
7. Press **OK**.

### Configuring the SPN for the Gateway Server

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running setspn and specifying the hostname of the server on which it is running as the 'user' in the setspn command.

## For any Gateway Servers that reside on a different machine from the Acronis Cyber Files Server

1. Open the command prompt.
2. Enter the following **setspn** command: `setspn -s HTTP/`**computername.domain.com computername**

   For example, if you gateway server is running on host `'cody'` in the domain, run this command:

   ```
   setspn -s HTTP/cody.acme.com cody
   ```
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

```
setspn -s HTTP/cody.acme.com:444 cody
```

4. Repeat this section for all Gateway servers.

## If there is a Gateway Server on the same machine as the Acronis Cyber Files Server

This is required only if you have a Gateway Server on the same machine as the Acronis Cyber Files Server. If you do not, skip this section. For this configuration to work, you will need to set an additional DNS entry for your Gateway server.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (`A record`) for the Gateway server.
2. Enter a name. This will be the DNS address that will be used to reach the Gateway server.
   **e.g.**`codygw.acme.com`
3. Enter the IP address of the Gateway Server (without the port). If you're running the Gateway and the Acronis Cyber Files Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.
5. Go back to the machine with Acronis Cyber Files.
6. Open the command prompt.
7. Enter the following **setspn** command: `setspn -s HTTP/`**gatewaydns.domain.com computername**

   For example, if you gateway server is running on host `'cody'` in the domain and your DNS entry is `codygw.acme.com`, run this command:

   ```
   setspn -s HTTP/codygw.acme.com cody
   ```
8. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/codygw.acme.com:444 cody
   ```
9. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created in step 4.

### On the Acronis Cyber Files server

## Editing the `web.xml` file:

1. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access server\Web Application\WEB-INF\`
2. Find and open the file `web.xml`. In this file you will set the domain username and password that the SSO service will run under. This account **must** match the account that you used to register the HTTP service with Kerberos in the **On the Domain** section.
3. In `web.xml` there are two properties that need to be set - the domain username and password that the SSO service will use. Find the following lines:

   ```
    <init-param>
      <param-name>spnego.preauth.username</param-name>
   ```

```
<param-value>yourusername</param-value>
</init-param>
<init-param>
<param-name>spnego.preauth.password</param-name>
<param-value>yourpassword</param-value>
</init-param>
```

4. Replace **yourusername** with the desired LDAP username.
5. Replace **yourpassword** with the LDAP password for the LDAP account specified above. If you have one of these five special characters in your password: **&**, **>**, **"**, **'** , or **<**, you will have to properly escape them in the XML document. To do so, you will have to replace them with the following:
   - **<** with **&lt;**
   - **>** with **&gt;**
   - **"** with **&quot;**
   - **'** with **&apos;**
   - **&** with **&amp;**

   e.g. if your password is `<my&best'password"` you will have to write it in the `web.xml` file as follows: `&lt;my&amp;best&apos;password&quot;`

## Editing the `krb5.conf` file:

1. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf`
2. Find and open the file `krb5.conf`
3. In `krb5.conf` there are only two properties that are needed from the administrator:
   a. The domain for single sign-on (e.g., `ACME.COM`)

   **Note**
   The domain in `krb5.conf` must always be in **UPPERCASE** or Kerberos ticket lookups may fail.

   b. The Kerberos Key Distribution Center's address (typically matches the address of your primary domain controller; e.g., `acmedc.ACME.COM`)
4. The `krb5.conf` file that we install looks like this:

```
[libdefaults]
   default_realm = ACME.COM
   default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   permitted_enctypes  = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
   [realms]
   ACME.COM = {
   kdc = acmedc.ACME.COM
```

```
default_domain = ACME.COM
[domain_realm]
.ACME.COM = ACME.COM
```

5. Replace all instances of `ACME.COM` with your domain (**in uppercase!**).
6. Replace the value for "`kdc =`" with the name of your domain controller. The domain must be written in uppercase. e.g. `kdc = yourdc.YOURDOMAIN.COM`
7. After the above configuration files are updated the Acronis Cyber Files server (the Acronis Cyber Files Tomcat service) must be restarted in order for the changes to take effect.

## Enabling Single sign-on in the web interface:

1. Open the Acronis Cyber Files web interface and log in as an administrator.
2. Expand the **General Settings** tab and open the **LDAP** page.
3. At the bottom of the page, enable the checkbox **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials.**
4. Click **Save**.

### One-time Configuration for a Domain Forest

There is a minor, one-time configuration that must be done to enable Single Sign-On support for the browser.

**Important**
This must be done for each user, on each machine.

**Note**
In the config instructions, we use *acme.com* as an example. If you have services in multiple domains, repeat the steps which specify *acme.com* for all your domains. (**e.g.** add `*.acme.com` and `*.another.com` and `*.yetanother.com`).

## Acronis Cyber Files in a Domain Forest

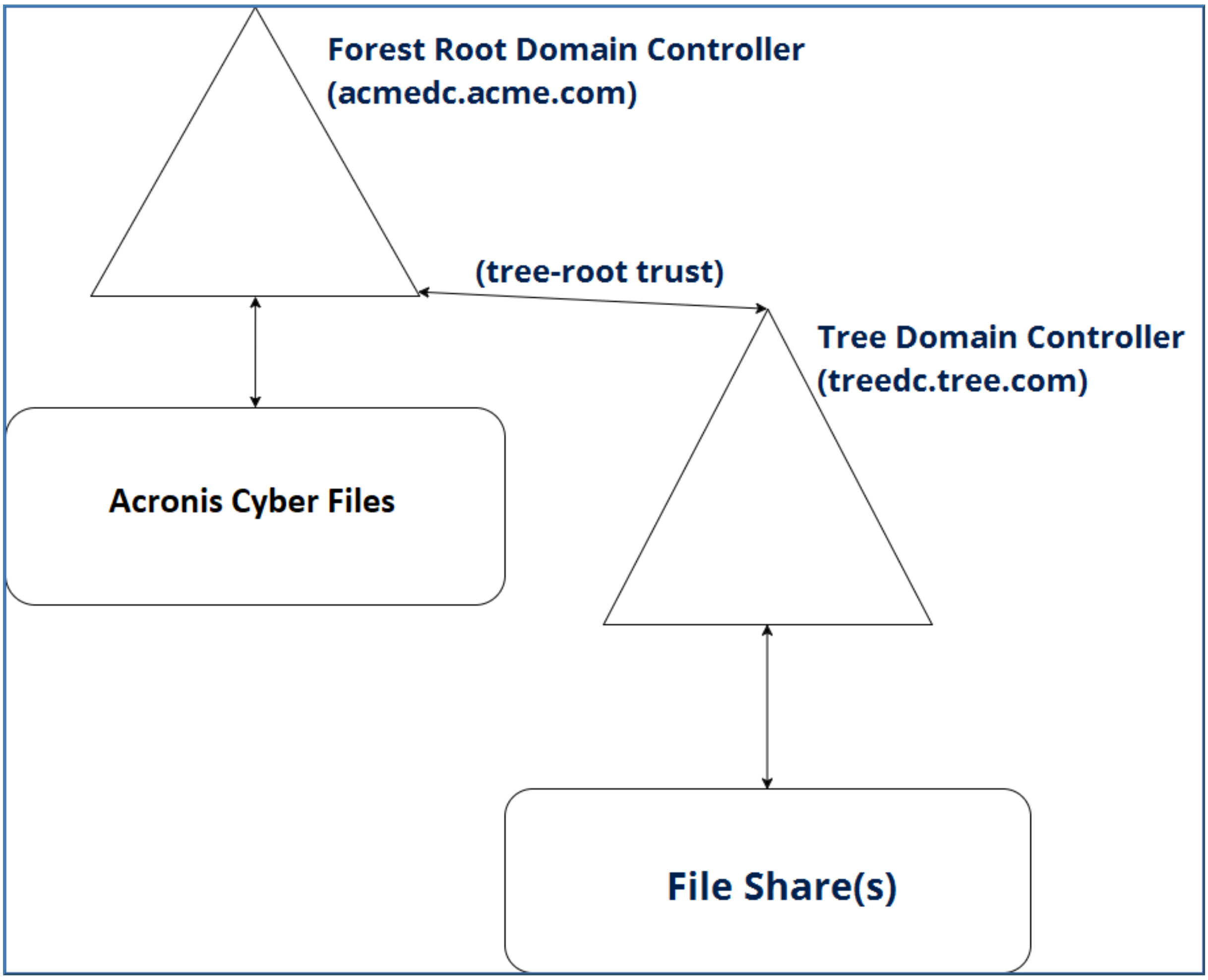
As of Windows Server 2012, Microsoft have added Resource **Based Kerberos Constrained Delegation**, which allows cross-forest constrained delegation. This enables deployments to use Single sign-on even if they have resources in multiple domains (within the same Forest), without having to install a Gateway server on the resources.

**Note**
In order to make use of this feature, all of your domains in the forest must run in **domain functional level 2012** or higher.

This article will guide you through:

- Setting up your Acronis Cyber Files server for SSO.
- Setting up your Gateway server(s) for SSO.

- All Configurations on your domain in order to get cross-forest constrained delegation working.
- The setup users have to do in order to use SSO.



## Requirements

This guide is intended for multi-domain configuration running in a single Forest. As such, we assume that your LDAP is properly configured, users can login to the domain without issue and that the connectivity between the domains inside the forest is properly configured.

- This type of Constrained Delegation is available only in domain controllers running in **domain functional level 2012** or higher. Windows Server 2012 is the first to allow Resource Based Kerberos Constrained Delegation.
- You need to have **Global Catalog** enabled and running.

## One-time Configuration for a Domain Forest

There is a minor, one-time configuration that must be done to enable Single Sign-On support for the browser.

**Important**
This must be done for each user, on each machine.

**Note**

In the config instructions, we use *acme.com* as an example. If you have services in multiple domains, repeat the steps which specify *acme.com* for all your domains. (**e.g.** add `*.acme.com` and `*.another.com` and `*.yetanother.com`).

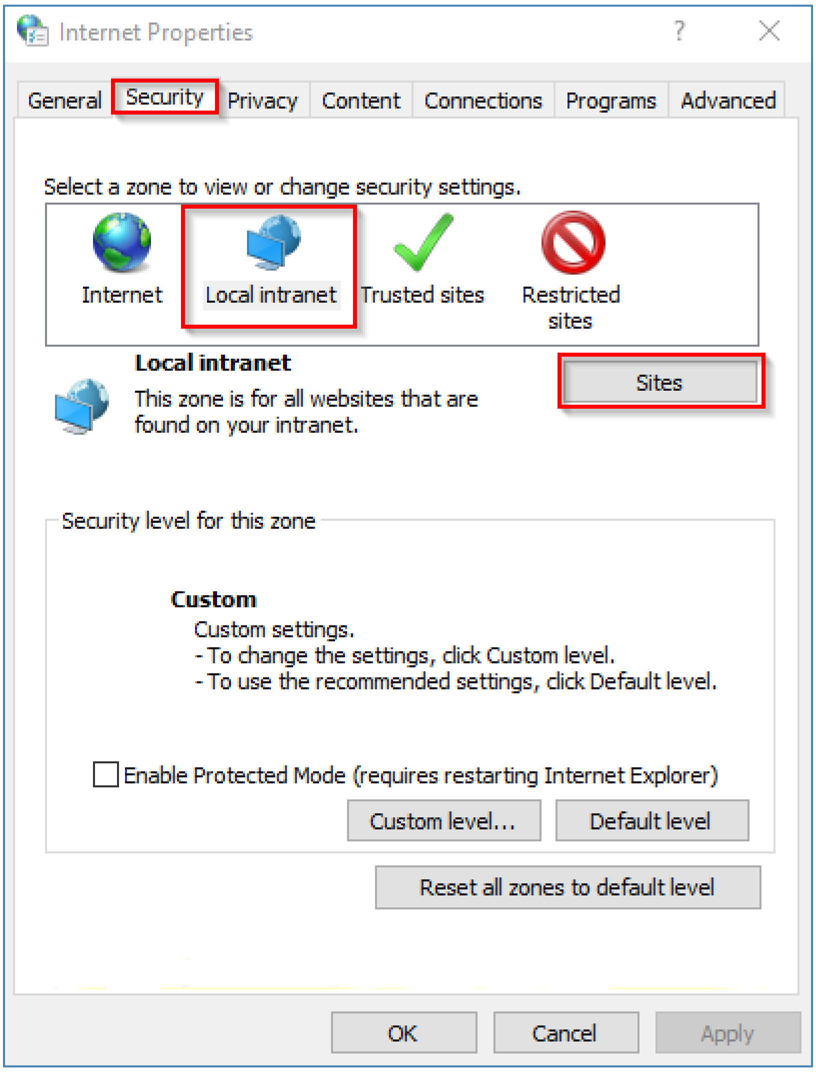
### One-Time Configuration for Windows

## For Microsoft Edge and Google Chrome

The configuration for both Microsoft Edge and Google Chrome is done through Microsoft Windows' Internet Options.

***Windows Internet Options configuration***

1. Open Windows **Control Panel**.
2. Select **Internet Options**.
3. In the **Security** tab, click **Local Intranet**.



Select a zone to view or change security settings.

**Local intranet**

This zone is for all websites that are found on your intranet.

Security level for this zone

**Custom**

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☐ Enable Protected Mode (requires restarting Internet Explorer)

4. Click **Sites**, then **Advanced**.
5. Add the address of your Acronis Cyber Files server (e.g., `https://ahsoka.acme.com` or just `*.acme.com`).
6. Click **OK**.
7. Restart your browser.

***To allow credential delegation on Chrome***

**Important**
Credential delegation is necessary for browsing network nodes from the Web interface. Microsoft Edge, this is enabled by default. To enable credential delegation on Chrome, you must configure the browser to allow it.

1. Open the registry editor (**regedit32.exe**)
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`
3. Create the `Google\Chrome` keys if they don't already exist.
   a. Right click on the Policies folder and select **New** -> **Key**.
   b. Type in **Google** for the folder name.
   c. Right click on the **Google** folder and select **New** -> **Key**.
   d. Type in **Chrome** for the folder name.
   e. Click on the Chrome folder and in the white panel on the right, right-click and select **New** -> **String Value**.
   f. Enter the key name: `AuthNegotiateDelegateWhitelist`.
4. Set your domain name (e.g. `ahsoka.acme.com` or `*.acme.com`) as the value for the `AuthNegotiateDelegateWhitelist` registry key.
5. Restart Chrome.

## For Firefox

1. Type `about:config` in the address bar and press enter.
2. Find and edit the preference `network.negotiate-auth.trusted-uris` and add `https://ahsoka.acme.com` , or `just .acme.com`, [the list is comma-separated].

   **Note**
   To add all subdomains use the format "`.example.com`" (**NOT** `*.example.com`)

3. To enable Network **Data Sources** support, you will need to also edit `network.negotiate-auth.delegation-uris` by adding `ahsoka.acme.com` or just the domain name - `acme.com`.
4. Restart **Firefox**.

### One-Time Configuration for Mac

**Note**

This needs to be done for each user on each machine.

## For Safari

It will just work.

## For Firefox

1. Type `about:config` in the address bar and press enter.
2. Find and edit the preference `network.negotiate-auth.trusted-uris` and add `https://ahsoka.acme.com` , or `just .acme.com`, [the list is comma-separated].

   **Note**

   To add all subdomains use the format "`.example.com`" (**NOT** `*.example.com`)

3. To enable Network **Data Sources** support, you will need to also edit `network.negotiate-auth.delegation-uris` by adding `ahsoka.acme.com` or just the domain name - `acme.com`.
4. Restart **Firefox**.

## For Chrome

1. Using the **Ticket Viewer** application (**/System/Library/CoreServices/Ticket Viewer**), you can check if you have a Kerberos ticket and create one if it hasn't been created automatically.

   **Note**

   You also can create a ticket via the **Terminal** by entering `kinit` and then your password.

2. To configure Chrome's allowlist to allow authentication against any domains you will be using, open the **Terminal** and run the following commands:

   ```
   $ defaults write com.google.Chrome AuthServerWhitelist “*.acme.com”
   ```

   ```
   $ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist “*.acme.com”
   ```

3. Restart the Chrome browser.

### For the Acronis Cyber Files Server

### Configuring the domain account used for Single Sign-on authentication

1. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\`
2. Find and open the file `web.xml`. In this file you will set the domain username and password that the SSO service will run under.

This account **must** match the account that you will use to register the **HTTP** service with Kerberos in the following sections, so we recommend writing it down.

3. In `web.xml` there are two properties that need to be set - the domain username and password that the SSO service will use. Find the following lines:

```
<init-param>
  <param-name>spnego.preauth.username</param-name>
  <param-value>yourusername</param-value>
  </init-param>
  <init-param>
  <param-name>spnego.preauth.password</param-name>
  <param-value>yourpassword</param-value>
  </init-param>
```

4. Replace **yourusername** with the desired LDAP username.
5. Replace **yourpassword** with the LDAP password for the LDAP account specified above. If you have one of these five special characters in your password: **&**, **>**, **"**, ' , or **<**, you will have to properly escape them in the XML document. To do so, you will have to replace them with the following:
   - **<** with **&lt;**
   - **>** with **&gt;**
   - **"** with **&quot;**
   - **'** with **&apos;**
   - **&** with **&amp;**

   **e.g.** if your password is `<my&best'password"` you will have to write it in the `web.xml` file as follows: `&lt;my&amp;best&apos;password&quot;`

## Setting the Kerberos domain lookup

1. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf`
2. Find and open the file `krb5.conf`
3. In `krb5.conf` there are only two properties that are needed from the administrator:
   a. The domain for single sign-on (e.g., `ACME.COM`).
      - This must be the domain where your Acronis Cyber FilesWeb Server and Gateway servers reside.
      - Please note that this is the name of your domain, **not** the DNS name of the server.

   **Note**
   The domain in `krb5.conf` must always be in **UPPERCASE** or Kerberos ticket lookups may fail.

   b. The Kerberos Key Distribution Center's address (typically matches the **DNS** address of your primary domain controller; e.g., `acmedc.ACME.COM`). This is the address of the domain controller in the domain where Acronis Cyber Files and its components reside.

4. The `krb5.conf` file that we install looks like this:

```
[libdefaults]
        default_realm = ACME.COM
        default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-
crc
        default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-
crc
        permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-
crc
    [realms]
        ACME.COM = {
            kdc = acmedc.ACME.COM
            default_domain = ACME.COM
    [domain_realm]
        .ACME.COM = ACME.COM
```

5. Replace all instances of `ACME.COM` with your domain (**in uppercase!**). Please note that this is the name of your domain, **not** the DNS name of the server.
6. Replace the value for "`kdc =`" with the DNS name of your domain controller. The domain portion must be written in uppercase. e.g. `kdc = yourdc.YOURDOMAIN.COM`
7. After the above configuration files are updated the Acronis Cyber Files Server (the Acronis Cyber Files Tomcat service) must be restarted in order for the changes to take effect.

### Enabling Single sign-on in the web interface

1. Open the Acronis Cyber Files web interface and log in as an administrator.
2. Expand the **General Settings** tab and open the **LDAP** page.
3. At the bottom of the page, enable the checkbox **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials.**
4. Press **Save**.

### Configuring the LDAP account that will handle SSO

## Configure an additional DNS entry for your Acronis Cyber Files Web server

If you have a Gateway server on this machine, you must have a separate DNS entry for your Acronis Cyber Files Web Server.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry `(A record)` for the Acronis Cyber Files Web Server.
2. Enter a name. This will be the DNS address that will be used to reach the Acronis Cyber Files Web server.

   **e.g.**`ahsokaccess.acme.com`

3. Enter the IP address of the Acronis Cyber Files Web Server (without the port). If you're running the Gateway and the Acronis Cyber Files Web Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.

## Setting the SPN for the **Acronis** Cyber Files Web Server

1. On the machine where Acronis Cyber Files is running, open a command prompt.

   **Note**
   You must be logged in with a domain account and have the rights to use **setspn**

2. Enter the command `setspn -s HTTP/`**access_DNS_name.domain.com account name**

   **Note**
   The LDAP account name used in this command **MUST** match the account which you have specified in the `web.xml` file.

   - for example, if your Acronis Cyber Files Web server is installed on `ahsoka.acme.com` and you want to use `john@acme.com` as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:
     ```
     setspn -s HTTP/ahsokaaccess.acme.com john
     ```
   - for example, if your Acronis Cyber Files Web Server is installed on `ahsoka.acme.com` and you want to use `jane@tree.com` as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:
     ```
     setspn -s HTTP/ahsokaaccess.acme.com tree\jane
     ```

   **Note**
   This account will typically match the LDAP account specified by the administrator in the Acronis Cyber Files web interface in the **LDAP settings**, but this is not mandatory.

3. If your Acronis Cyber Files Web server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number.

   **e.g.** If your server is running on port 444, the command will be:

   `setspn -s HTTP/ahsokaaccess.acme.com:444 john` OR

   `setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane`

   **Note**
   The **HTTP** in the commands above refer to the **HTTP** service class, not the **HTTP** protocol. The **HTTP** service class handles both **HTTP** and **HTTPS** requests. You do not need to, and **should NOT**, create an SPN using **HTTPS** as a service class name.

4. Go to the domain controller where your users reside and open **Active Directory Users and Computers**. If you have multiple domains with users, open the one which contains the user used in the previous steps.

5. Find the user that you used in the above commands (in this case - **john** or **jane**).
6. Click on the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**. Enabling this setting allows the LDAP object to delegate authentication to any service. In our case that is the Gateway Server service.
7. Click **OK**.

## Verify you can log into **Acronis** Cyber Files

1. Go to a machine other than your Domain Controller or your Acronis Cyber Files Web Server.
2. Open your Acronis Cyber Files web console and use the link under the password field on the login page.

**Note**
You need to be logged into the machine with a domain user that was either invited to Acronis Cyber Files , has already logged in or is a member of a Provisioned LDAP group.

**Note**
You must complete the On any user's machine section in order for your browser to accept SSO requests.

### For the Gateway Server

#### Configuring the SPN for the Gateway Server

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the Gateway server, the gateway service must be registered with the KDC server by running **setspn** and specifying the hostname of the server on which it is running as the 'user' used in the **setspn** command.

# Configure an additional DNS entry for your Gateway server

In order for this configuration to work, you must have a separate DNS entry for your Gateway Server as well.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (`A record`) for the Gateway server.
2. Enter a name. This will be the DNS address that will be used to reach the Gateway server.
   **e.g.**`codygw.acme.com`
3. Enter the IP address of the Gateway Server (without the port). If you're running the Gateway and the Acronis Cyber Files Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.

## Configure the SPN for the local Gateway Server

1. Go to the machine with Acronis Cyber Files.
2. Open the command prompt.
3. Setup the SPN for the Gateway Server:
   a. If your Gateway Server is running as the Local System account, the command is:
   b. `setspn -s HTTP/`**gatewaydns.domain.com computername**

   For example, if you gateway server is running on host `'cody'` in the domain and your DNS entry is `codygw.acme.com`, run this command:

   ```
   setspn -s HTTP/codygw.acme.com cody
   ```

   c. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/codygw.acme.com:444 cody
   ```

4. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created (i.e. `codygw.acme.com`).

## Verify that the SPNs were set correctly for the Gateway

1. If you have a local volume for the local Gateway, you can verify that the SPNs and delegation are working by logging in with SSO. This must be done on a machine other than the Acronis Cyber Files server and the Domain Controller, otherwise SSO will not work.
2. Browse the local Gateway Server's volume. If that works, you can proceed forward, otherwise please verify you have successfully configured the proper SPNs for the proper objects.

   **Note**
   If you try a volume on a remote file server, you should get an Access Denied error.

### Set Resource Based Constrained Delegation

**Note**
This type of Constrained Delegation is available only in domain controllers running in domain functional level 2012R2 or higher. Windows Server 2012 is the first to allow cross-domain Kerberos Constrained Delegation.

You can use Resource Based Constrained Delegation to grant users access to file servers or other network resources located in another domain.

1. Go to the domain controller for the domain where your file server resides and open **PowerShell**.
2. If your Gateway Server is running as the **LocalSystem** account:
   a. **$computer1 = Get-ADComputer -Identity <gateway_server_computer> -server <domain_controller_for_this_domain>**

   e.g. `$computer1 = Get-ADComputer -Identity cody -server dc.acme.com`

   This command gets the computer object for the gateway server, specifies the AD Domain

Services instance to connect to and saves this information in the **$computer1** variable.

   b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount $computer1**

      e.g. `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $computer1`

      This command sets the property **Principals Allowed To Delegate To Account** of the file server computer object, to the computer object for the gateway server. This allows the gateway server's computer to delegate to the file server's computer.

3. If your Gateway Server is running as a **User Account**:

   a. **$user1 = Get-ADUser -Identity <logon_user_of_the_gateway_service> -server <domain_controller_for_this_domain>**

      e.g. `$user1 = Get-ADUser -Identity jane -server dc.acme.com`

      This command gets the user object for the user that the gateway server runs as, specifies the AD Domain Services instance to connect to and saves this information in the **$user1** variable.

   b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount $user1**

      e.g. `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $user1`

      This command sets the property **Principals Allowed To Delegate To Account** of the file server computer object, to the user object that the gateway server runs as. This allows the selected user to delegate to the file server's computer.

4. To verify the Gateway user account was added as an account allowed to be delegated credentials to, you can run the following:

   **Get-ADComputer <file_server_machine> -Properties PrincipalsAllowedToDelegateToAccount**

   e.g. `Get-ADComputer omega -Properties PrincipalsAllowedToDelegateToAccount`

5. Repeat these steps for all your File Servers.

***It will take some time for the delegation to be propagated – 10 to 15 minutes for small LDAP deployments and even more for larger structures.***

## Adding more Gateway Servers

**Note**

These steps work only if the machines that will host the Gateway Servers are in the same domain as the Acronis Cyber Files Web Server.

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running setspn and specifying the hostname of the server on which it is running as the 'user' in the setspn command.

### For any Gateway Servers that reside on a different machine from the Acronis Cyber Files Web Server

1. Open the command prompt.
2. Enter the following **setspn** command: `setspn -s HTTP/`**computername.domain.com computername**

   For example, if you gateway server is running on host `'cody'` in the domain, run this command:

   ```
   setspn -s HTTP/cody.acme.com cody
   ```
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/cody.acme.com:444 cody
   ```
4. Repeat this section for all additional Gateway servers.

#### Configuring a Gateway Server in another domain

If you do not have access to **Resource Based Kerberos Constrained Delegation**, another way to configure SSO to remote shares and resources located in another domain is by installing a Gateway Server on a machine in that domain. This allows you to use regular Kerberos Constrained Delegation and **works on domains in functional level 2008**.

## Install a Gateway Server on a machine in the desired domain

1. Download the Acronis Cyber Files installer and move it to the machine.
2. Start the Acronis Cyber Files installer, accept the license agreement and press **Next**.
3. Select **Custom...** installation and select only the Gateway Server's checkbox.
4. Press **Install**. After the installation finishes, close the installer.
5. In the **Configuration Utility**, set the IP address of the gateway and the port.

## Make the Gateway service run as a User Account

1. Open **Control Panel** -> **Administrative Tools** -> **Services**.
2. Find the Acronis Cyber Files Gateway Server service, right-click on it and select **Properties**.
3. Select the **Log On** tab and select the **This account** radio button.
4. Select the User that the service will run as either by pressing **Browse** and searching or just by entering the username and password of the user. The user **must** be from the domain where Acronis Cyber Files is installed. We recommend using a dedicated account and no the one used for the Acronis Cyber Files Server's SPNs.
5. Press **OK** and can close the **Services** control panel. Do not restart the service yet, as without the necessary permissions for the user account, the service will not start.

## Grant the selected User the necessary rights

1. In order for the service to run as a user, that user must be granted **Act as part of the operating system** and must be a part of the Local Administrators group.
2. Open the **Local Security Policy** and navigate to **Local Policies** -> **User Rights Assignment**. You may have to make this change in the **Group Policy Manager** depending on your deployment.
3. Open the **Act as part of the operating system** object and press **Add User** or **Group**.
4. Select the dedicated user for the Gateway service.
5. Close all open dialogs and open **Control Panel** -> **User Accounts** -> **Manage Accounts**.
6. Press **Add** and enter the domain and username of the dedicated account.
7. You can now restart the Acronis Cyber Files Gateway service in the **Services** control panel.

# Configure the SPN for the remote Gateway Server

1. Go to any machine in the domain where the Acronis Cyber Files Server resides.
2. Open the command prompt.
3. To configure the SPN, the command is: **setspn –s HTTP/gatewaydns.domain.com useraccountfor_gw**

   e.g. If your gateway server is running on host `'magpie'` in the **tree.com** domain and is running as the `peter` user account from the **acme.com** domain, run this command:

   ```
   setspn -s HTTP/magpie.tree.com peter
   ```

   If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/magpie.tree.com:444 peter
   ```
4. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created (i.e. `magpie.tree.com`).
5. Make sure that the Gateway Server has **Perform Negotiate/Kerberos authentication in user-mode** enabled. You have to restart the Acronis Cyber Files Gateway service after you enable this setting.
6. When creating **data sources** for the resources in the second domain, make sure to use the Gateway Server that resides in that domain.

   **e.g.** If you want to grant your users access to the files on `repository.tree.com`, you will have to pick the gateway server that is located in `tree.com` (e.g. `magpie.tree.com`)

## Verify that the SPNs were set correctly for the Gateway

1. If you have a local volume for the local Gateway, you can verify that the SPNs and delegation are working by logging in with SSO.
2. Browse the local Gateway Server's volume. If it doesn't work please verify you have successfully configured the proper SPNs for the proper objects.
3. Delegation changes might take some time to propagate (e.g. 10-15 minutes for small LDAP deployments and more for larger ones).

## Verify that an SPN is registered

To query whether the desired SPN is registered properly:

1. Open an elevated command prompt.
2. Enter the `setspn -Q HTTP/`**computername.domain.com** command.

   e.g. `setspn -Q HTTP/ahsoka.acme.com`
3. To query the SPNs registered to a particular domain user, use the `-l` (lowercase `L`) switch;

   e.g. `setspn -l john`
4. After registering the SPN, before you can authenticate to it with SSO you will need to either reboot the client machine or run this command on the client machine:

   `klist purge`

## Using SMB or SharePoint Data Sources

If you want to use SMB or SharePoint Data Sources, you must configure the Active Directory account to permit Kerberos delegation to each of your SMB and SharePoint data sources.

### For network shares and SharePoint servers, do the following:

Following these steps, you will enable delegation from the Gateway server to the target server(s).

1. Open **Active Directory Users and Computers**.
2. Find the computer object corresponding to the Gateway server.

   **Note**

   If you are running the Gateway server under a **User** account, select that **User** object instead.
3. Right-click on the user and select Properties.
4. Open the **Delegation** tab.
5. Select **Trust this computer for delegation to specified services only**.
6. Under that select **Use any authentication protocol**.
7. Click **Add**.
8. Click **Users or Computers**.
9. Search for the sever object for the SMB share or SharePoint server and click **OK**.
   - For SMB shares, select the **cifs** service.
   - For SharePoint, select the **http** service.
10. Repeat these steps for each server that the Acronis Cyber Files Gateway server will need to access.
11. Repeat this process for each Gateway server.

These delegation changes, can take a few minutes to propagate depending on the size of the domain forest. You may need to wait up to 15 minutes (possibly more) for the changes to take effect. If it's still not working after 15 minutes, try restarting the Acronis Cyber Files Gateway service.

## Using mobile clients with client certificate authentication

This is an additional step that you have to perform. You need to set up delegation from the Gateway Server to the Acronis Cyber Files server regardless if they are on the same machine or not.

### Kerberos Constrained Delegation

This type of delegation will work if the Acronis Cyber Files server and the Gateway Server are in the same domain.

1. To do this, open the Active Directory on the domain controller.
2. Find and edit the Gateway server's computer object and go to the delegation tab.
3. Select **Trust this computer for delegation to specified services only** and **Use any authentication protocol**.
4. To select the Acronis Cyber Files server's SPN, click Add and enter the username of the account that's associated with the Acronis Cyber Files server's **HTTP** SPN.

   **Note**
   Do not search for the computer that the Acronis Cyber Files server is running on - you'll have to do the lookup by username.

   **Note**
   Kerberos authentication to the Acronis Cyber Files server is not compatible with single port mode.

5. Once you search for the user, you should see the **HTTP** services, so select them (there might be two if you registered the SPN twice - once with the port and once without).
6. Press **Apply** and close all dialogs.

### Resource Based Kerberos Constrained Delegation

This type of delegation will work even if the Access and Gateway servers are in separate domains in a domain forest.

**Note**
In order to make use of this feature, all of your domains that Acronis Cyber Files will have access to must run in **domain functional level 2012** or higher.

1. Double-check that the DNS entry dedicated for the Acronis Cyber Files server and for which you have set an SPN is in fact set as the address for your S&S volume in the Data Sources page.
2. Configure delegation between the Gateway Server and the Acronis Cyber Files server. This time the delegation will be from the Gateway Server to the Acronis Cyber Files server.

3. Execute the following commands for the following users:

   **$pc1 = Get-ADComputer -Identity <name_of_gateway_machine>**

   **Set-ADUser <Access_SSO_user_account> -PrincipalsAllowedToDelegateToAccount $pc1**

   e.g: `$pc1 = Get-ADComputer -Identity ahsoka`

   ```
   Set-ADUser john -PrincipalsAllowedToDelegateToAccount $pc1
   ```

4. If your Gateway is running as a user account you will need to set the delegation to be between the two user accounts, with the following commands:

   **$user1 = Get-ADUser -Identity <Gateway_User_Account>**

   **Set-ADUser <Access_SSO_user_account> -PrincipalsAllowedToDelegateToAccount $user1**

   e.g: `$user1 = Get-ADUser -Identity gwuser`

   ```
   Set-ADUser john -PrincipalsAllowedToDelegateToAccount $user1
   ```

***It will take some time for the delegation to be propagated – 10 to 15 minutes for small LDAP deployments and even more for larger structures.***

## For Load Balanced environments

The Gateway Server has the option to perform all HTTP authentication in user mode rather than have the web server attempt to do Kerberos/Negotiate authentication. This is required to get SSO working for the Gateway(s) running behind a load balancer.

To enable this feature, Open the web interface and go to **Mobile Access** -> **Gateway Servers**, click the **Edit** option in the cluster group, go to **Advanced** and enable the checkbox "**Perform Negotiate/Kerberos authentication in user-mode**"

### Enabling Network Nodes

In order to be able to access Network nodes in the Web, while using SSO, several changes will be required. Since the Gateway Servers are running behind a load balancer, registering with Kerberos will need to happen with a user account, not computer name.

For this to work, the gateway services will need to run under a user account. You can either use the same LDAP user under which the Acronis Cyber Files server is registered, or you can select a new one, dedicated to your Gateway services.

Either way, the user you choose will need to be given the right to act as part of the operating system on the machines where the Gateway Servers are installed.

### Selecting a user to act as part of the operating system

1. On the machine with the Gateway server, click **Start** -> **Run**
2. Type **gpedit.msc** and press **OK**
3. Expand **Windows Settings** and expand **Security Settings**.
4. Expand **Local Policies** and click on **User Rights Assignment**.
5. Right-click on **Act as part of the operating system** in the list and select **Properties**.

6. In this window, you can add users and groups or remove them. Enter the desired username and press OK.
7. Close all remaining windows and restart the server for the change to take effect.

### Running the Gateway Server's service as the selected user account

Once you have added the user you will be running the service as, you must set the Gateway service to run as them. To do so, complete the following steps:

1. On the machine where the Gateway Server is installed, click **Start** and select **Run**.
2. Type in **services.msc** and click **OK**. Alternatively, open the **Control Panel** and go to **Administrative Tools** -> **Services**.
3. Right-click **Acronis Cyber Files  Gateway** in the list and select **Properties**.
4. Click on the **Log On** tab.
5. Select the radio button for **This account:** and enter the credentials of the user you granted operating system rights to.
6. Click **OK** and close all windows

## Configuring the SPNs for the Gateway Cluster

In order for the Key Distribution Center Kerberos server to be able to authenticate users to the gateway cluster, each Gateway Server and the load balancer for the Gateways must be registered with the KDC server by running **setspn** and specifying the account name as which the service will be running as.

1. Open the command prompt.
2. Enter the following command:

   ```
   setspn -s HTTP/computername.domain.com username
   ```

   For example, if your gateway service is running as user **john**, the command will be:

   ```
   setspn -s HTTP/gatewayserver1.acme.com john
   ```
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

   ```
   setspn -s HTTP/gatewayserver1.acme.com:444 john
   ```
4. Repeat these steps for each Gateway Server and for the load balancer. The SPN for the load balancer should look like this:

   ```
   setspn -s HTTP/gwloadbalancerdns.acme.com john
   ```

**Note**

If you have a load balancer that splits the traffic between 2 Gateways (in this case `gwloadbalancerdns.acme.com`), do not enroll to it, because in half of the cases, the requests will not reach the correct Gateway (the local one). If the LB server forwards the request to the wrong Gateway, the login will fail. DNS names can't point to other service after launching.

If you need further assistance, please contact the Support team.

## Troubleshooting Single Sign On

- Desktop or Web client users must be on a separate machine from the one running the Acronis Cyber Files server (but in the domain) or SSO will not work.
- Single Sign-On usage from the Desktop Client requires connection to the corporate network. This means that SSO users should have access to their own network as well.
- You must access the server using the exact same FQDN as the SPN is using; e.g., `https://ahsoka.acme.com`. You cannot use other DNS names or IP addresses e.g., `https://localhost` or `https://10.20.56.33`.
- Verify that you can log in to the Acronis Cyber Files server without using SSO by entering the exact same LDAP credentials as your client windows machine uses. This will verify that your account credentials are valid for Acronis Cyber Files regardless of SSO configurations.
- Verify that you can access all Data sources without using SSO and using the same credentials as your LDAP login account.
- If you are unable to log in via SSO, double-check that you have configured your Web browser for SSO to the FQDN to which you are connecting, and you are logged in on your client machine using a domain account.
- Single Sign-On will not work if the Acronis Cyber Files Server is running on the Domain Controller.
- Acronis Cyber Files will not work with SSO if you are trying to access it from the machine that is the Domain Controller.

**Note**
Due to how Kerberos works, you cannot authenticate via SSO from a client application or Web browser running on the Domain Controller or the Acronis Cyber Files server.

**Note**
Additionally, the Acronis Cyber Files server cannot authenticate to the Domain Controller when the Acronis Cyber Files server is running on the Domain Controller.

- If you get a **401 Error** when trying to log in using SSO, check the username and password in the **web.xml** file and make sure that any special characters are escaped properly. The special characters are: **&**, **>**, **"**, **'** , or **<**, for information on how to escape them, please see **step 5** of the **Editing the web.xml file** section.

## Using trusted server certificates with Acronis Cyber Files

This section explains how to configure Acronis Cyber Files with trusted server certificates.

By default, Acronis Cyber Files provides self-generated SSL certificates for testing purposes. Using a certificate signed by a trusted Certificate Authority will establish the identity of the server and allow clients to connect without errors.

**Note**

Web browsers will display warning messages when using self-signed certificates. Dismissing those messages allows the system to be used for testing.

***Using self-signed certificates for production deployments is not supported. Production deployments should implement proper CA certificates.***

## Creating a Certificate Request

**Note**

Creating certificates is not and will never be a function of Acronis Cyber Files. This certificate request is in no way necessary for the operation of Acronis Cyber Files but it is required by Certificate vendors.

**Note**

If prompted by your vendor to select a server type, choose **IIS**.The certificates must be installed in the Windows Certificate Store before Acronis Cyber Files can use them.

### Generating a certificate request via IIS:

For more information on this procedure, please refer to the following Microsoft Knowledge Base article: http://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx

### Generating a certificate request via OpenSSL:

**Note**

For this guide you need to have OpenSSL installed.

**Note**

Contact your preferred certificate vendor for more information or help with this procedure.

**To generate a pair of private key and public Certificate Signing Request (CSR) for the web server "AAServer":**

1. Open an elevated command prompt and enter the following command:

   ```
   openssl req -new -nodes -keyout myserver.key -out AAServer.csr -newkey rsa:2048
   ```

2. This creates a two files. The file **myserver.key** contains a private key; do not disclose this file to anyone. Be sure to backup the private key, as there is no means to recover it should it be lost. The private key is used as input in the command to generate a **Certificate Signing Request (CSR)**.

**Note**

In case you receive this error: **WARNING: can't open config file: /usr/local/ssl/openssl.cnf** run the following command: **set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg** change the path, depending on where you installed OpenSSL. After you have completed this procedure, attempt step 1 again.

3. You will now be asked to enter details to be entered into your CSR. Use the name of the web server as **Common Name (CN)**. If the domain name is **mydomain.com** append the domain to the hostname (use the fully qualified domain name).
4. The fields email address, optional company name and challenge password can be left blank for a web server certificate.
5. Your CSR will now have been created. Open the **server.csr** in a text editor and copy and paste the contents into the online enrollment form when requested by the certificate vendor.

## Installing your certificate to the Windows certificate store

**Requirements**

The certificate you are using must contain it's private key. The certificate file must be in either the **.PFX** or **.P12** format.
It doesn't matter which one since they are interchangeable.

**Note**

If your Certificate Vendor provided you with a certificate and a key as two separate files, you can combine them into one **.PFX** file with the following command:

```
openssl pkcs12 -export -in <yourcertificate.extension> -inkey <yourkey.extension> -out
<newfile.pfx>
```

**e.g.** `openssl pkcs12 -export -in acmecert.crt -inkey acmecertkey.key -out acmecombined.pfx`

**This command requires OpenSSL to be installed.**

**Installing your certificate to the Windows certificate store**

**Note**

If your Acronis Cyber Files and Gateway Servers are using different certificates, repeat these steps for both.

1. On the server, click **Start**, then **Run**.
2. In the **Open box**, type **mmc**, then click **OK**.
3. On the **File menu**, click **Add/Remove snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, then **Add**.

6. In the **Certificates snap-in** dialog box, click **Computer account** (this is not selected by default), and then click **Next**.
7. In the **Select Computer** dialog box, click **Local computer**: (the computer this console is running on), then **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the left pane of the console, double-click **Certificates** (**Local Computer**).
11. Right-click **Personal**, point to **All Tasks**, and then click **Import**.
12. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
13. On the **File to Import page**, click **Browse**, locate your certificate file, and then click **Next**.

    **Note**
    If you are importing a PFX file, you will need to change the file filter to **"Personal Information Exchange (*.pfx, *.p12)**" to display it.

14. If the certificate has a password, type the password on the **Password** page, and then click **Next**.
15. Check the following boxes:
    a. **Mark this key as exportable**
    b. **Include all extended properties**
16. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.
17. Click **Finish**, then click **OK** to confirm that the import was successful.

All of the certificates successfully installed in the Windows Certificate Store will be available when using the Acronis Cyber Files Configuration Utility.

## Configure Cyber Files to use your certificate

After you've successfully installed your certificate to the Windows certificate store, you have to configure Acronis Cyber Files to use that certificate.

1. Launch the Acronis Cyber Files Configuration Utility. There should be a shortcut in the Windows Start menu.

    **Note**
    The Configuration Utility is located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility` by default.

2. On the **Web Server** tab, press the **[...]** button and select your certificate from the list.
3. On the **Mobile Gateway** tab, press the **[...]** button and select your certificate from the list.
4. Click **Apply**. This will restart the web services and after about a minute they should be back online and using your certificate. You can check to confirm they are serving the correct certificates.

## Using Intermediate certificates

If the Certificate Authority has issued you an Intermediate certificate along with your certificate, it must also be added to the Acronis Cyber Files Server through the Configuration Utility.

**Note**
The Configuration Utility only searches in the **Intermediate Certificates** certificate store. If your certificate was installed in one of the other stores, open **certmgr.msc** and move your Intermediate certificate from the store it is in, to the **Intermediate Certification Authorities** -> **Certificates** store.

1. Launch the Acronis Cyber Files Configuration Utility. There should be a shortcut in the Windows Start menu.

   **Note**
   The Configuration Utility is located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility` by default.

2. On the **Web Server** tab, press the **[...]** button and select your certificate from the list.
3. Press the plus (**+**) button next to the **Chain Certificate** field and select the **intermediate certificate** you wish to use from the list. If the desired certificate is not in the list, please check if it was properly installed and which store it was installed in.
4. On the **Mobile Gateway tab**, press the **[...]** button and select your certificate from the list. No additional steps are required for intermediate certificates.
5. Click **Apply**. This will restart the service and after it comes back online, you can check to confirm it is serving the selected certificates.

## Supporting different Desktop Client versions

If you want to use a version of Acronis Cyber Files Desktop Client which is different from the latest, follow these steps:

1. Download the version of the desktop client which you want to use. Make sure you have these 4 files:
   - ACFClientMac.zip
   - ACFClientInstaller.msi
   - AcronisCyberFilesInstaller.dmg
   - AcronisCyberFilesClientInstaller.exe
2. Copy the files.
3. On the server, open the Acronis Cyber Files Desktop Clients folder ( `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\clients` ).
4. Create a sub-folder for this version of the client. It should be named with the **client version number** (e.g. **8.5.0x664**, **8.6.2x632**).

5. Paste the 4 files in the sub-folder you just created.
6. Next, open the **Web User Interface** of your Acronis Cyber Files server.
7. Log-in as an **administrator** and go to the **Sync & Share** tab and open the **Acronis Cyber Files Client** page.
8. Find this setting: **Allow client auto-update to version**.
9. From the drop-down menu select your desired version.

**Note**
The download link in the **Action menu** for your account, will still download the latest available Acronis Cyber Files Desktop Client version. If you do not want the users to download the latest version, go to the **\Acronis\Acronis Cyber Files\Access Server\Web Application\clients** folder and rename the latest client version (e.g. 8.6.2x632) folder to "**do not use version number**" (e.g. "**do not use 8.6.2x632**").

# Moving the FileStore to a non-default location

## The service is running as the Local System account

1. Go to the machine on which Cyber Files is installed.
2. Stop the **Cyber Files File Repository Server** and **Cyber Files Tomcat** services.
3. You will find the current **FileStore** in the folder which you selected with the **Configuration Utility**. The default location is `C:\ProgramData\Acronis\Acronis Cyber Files\FileStore`.
4. Copy or move the entire **FileStore** folder with all of its contents to the desired location.

   For example, `D:\MyCustom Folder\FileStore`

**Note**
If the **File Store** is on a remote network share, the computer on which the **File Repository** service is running must have full permissions to the **File Store** folder on the network share.

5. Open the **Configuration Utility**.
6. In the **File Repositor**y tab, change the path of the **FileStore** to the new path where you've moved the **FileStore** folder.
7. Start **Acronis  Cyber Files File Repository Server** service.
8. Start the **Acronis Cyber Files Tomcat** service and close the **Services** control panel.

## The service is running as a User account

1. Go to the machine on which Cyber Files is installed.
2. Stop the **Cyber Files File Repository Server** and **Cyber Files Tomcat** services.
3. You will find the current **FileStore** in the folder which you selected with the **Configuration Utility**. The default location is `C:\ProgramData\Acronis\Acronis Cyber Files\FileStore`.
4. Copy or move the entire **FileStore** folder with all of its contents to the desired location.

   For example, `D:\MyCustom Folder\FileStore`

5. Open the **Configuration Utility**.
6. In the **File Repositor**y tab, change the path of the **FileStore** to the new path where you've moved the **FileStore** folder.
7. If the **File Store** is on a remote network share, the user account as which the **File Repository** service is running must have full permissions to the **File Store** folder on the network share.
8. The account must also have read and write access to the local **Repository** folder (for example, `C:\Program Files (x86)\Acronis\Acronis Cyber Files\File Repository\Repository`) to write the log file.
9. Start **Acronis  Cyber Files File Repository Server** service.
10. Start the **Acronis Cyber Files Tomcat** service and close the **Services** control panel.

## Monitoring Acronis Cyber Files with New Relic

This type of installation will let you monitor your Acronis Cyber Files Server application, not the actual computer on which it is installed.

1. Open http://newrelic.com/ and create a New Relic account or log in with an existing account. Once that is done, proceed with your Application configuration.
2. For Application Type select **APM**.
3. For platform, select **Ruby**.
4. Download the New Relic script shown in Step 3 of the New Relic Starting Guide (newrelic.yml).
5. Open your Acronis Cyber Files web console.
6. Navigate to **Settings** -> **Monitoring**.
7. Enter the path to the newrelic.yml including the extension (e.g `C:\software\newrelic.yml`). We recommend you put this file in a folder outside of the Acronis Cyber Files folder so that it will not be removed or altered on upgrade or uninstall.
8. Click **Save** and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
9. If more than 10 minutes pass, restart your Acronis Cyber Files Tomcat service and wait a couple of minutes. The button should be active now.
10. You should be able to monitor you Acronis Cyber Files server via the New Relic website.

**Note**

All the information the Acronis Cyber Files server logs about trying to connect to New Relic and set up monitoring is in a file called **newrelic_agent.log** found here - `C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs`. If you have any problems, you can find information in the log file.

**Note**

There is frequently a warning/error that starts like this:

**WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which** That's a side effect of the code used to patch another New Relic bug and is innocuous.

**If you want to monitor the actual computer as well**

1. Open http://newrelic.com/ and log in with your account.
2. Press Servers and download the New Relic installer for your operating system.
3. Install the New Relic monitor on your server.
4. The New Relic server monitor requires Microsoft .NET Framework 4. The link the New Relic installer takes you to is only for the Microsoft .NET Framework 4 Client Profile. You will need to go to the Microsoft Download Center and download the entire .NET 4 Framework from the internet and install it before running the New Relic Server Monitor installer.
5. Wait until New Relic detects your server.

## Running Acronis Cyber Files Tomcat on multiple ports

While the Configuration Utility supports setting the Tomcat service to only one port, Tomcat itself can be configured to run on multiple ports. This can be done by adding additional Connectors with the desired ports in the Tomcat server.xml file. Upgrades and restarting the Tomcat service using the CU will not affect the new connectors.

**Note**
We recommend performing this configuration after you have already run the Configuration Utility once and the Tomcat service has started successfully.

### Configuring an additional Tomcat Connector

1. Stop the Acronis Cyber Files Tomcat service if it is running.
2. Navigate to and open the `server.xml` file. By default it is located at `C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf`.

   **Note**
   The number in the path (7.0.59) might be different depending on your version of Tomcat.

3. Browse the file until you see the **Connector** section that looks like this:

   ```
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
   SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="$
   {catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}
   /conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
   SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW
   :!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
   address="0.0.0.0" port="443"/>
   ```

   **Note**
   Depending on your text editor, you will most likely see the code above displayed in a single line when you open **server.xml**.

> **Note**
> If you have selected a port other than **443** in the **Configuration Utility**, your **Connector** will have that port listed in the example shown above.

4. Copy the entire **Connector** section and paste the copy right below the original one. Both sections should be on the same level of indentation.
5. Replace **443** (or whatever port you have chosen in the **Configuration Utility**) with the desired second port that Tomcat will run on. e.g.:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW
:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
address="0.0.0.0" port="4430"/>
```

> **Note**
> Make sure that the code for the new **Connector** is written the same way as the existing one. i.e. if the old one is written as a single line, make sure the new one is as well.

6. Open the Acronis Cyber Files web interface and navigate to **General Settings** -> **Server Setting**.
7. In the **Web Address** field make sure that the address provided is using one of the ports for the Connectors. This is the address users will see in email invites and you can choose only 1 port for it.

## Multi-homing Acronis Cyber Files

Multi-homing the Acronis Cyber Files Gateway and Acronis Cyber Files servers is a simple task done through the Configuration Utility.

The only requirement is that you have 2 separate network interfaces and IP addresses.

### Configuring multi-homing

1. Open the Acronis Cyber Files Configuration Utility.
2. Open the **Web Server** tab and enter the first IP address and the 443 port.
3. Open the **Gateway Server** tab and enter the second IP address and the 443 port.
4. Click **OK**.

**Note**

Microsoft completely changed how the TCP/IP stack behaves in Windows Server 2008. A single IP transport now supports multiple layers and there is no longer a 'Primary' IP address. So, when multiple IP addresses are assigned to a single interface, all of the addresses are treated evenly and are all registered into DNS. In other words, this behavior is not a bug, but by design. However, the behavior causes issues because unless you do something about it, the IP address used will be round-robin (DNS).

You can workaround this by disabling dynamic DNS registration on the NIC and then creating the host DNS entry manually. Another easier workaround is to install the HotFix referenced on **KB975808:** **http://support.microsoft.com/?kbid=975808**. Once you have installed the HotFix, you will be able to use the `netsh skipassource` flag. When using this flag while adding new addresses you tell the stack that the new address is not used for outgoing packets. Therefore, these IP addresses will not be registered on the DNS servers. For example:

```
netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true
```

# Deploy separate Web Preview servlets

The Web Preview functionality of Acronis Cyber Files allows users to view file contents without having to download the whole file. With a lot of users, this can slow down your deployment's performance. To counter this, you can setup additional Tomcat servers with our Web Preview Servlet, which can handle the web previewing and assist your main Acronis Cyber Files Server(s).

A load balancer can be put in front of a series of Tomcat servers to further balance the load for the web preview servlets. The preview requests do not need any state, so no special configuration of the load balancer is needed.

**Note**

Password-protected files do not have thumbnails and cannot be previewed.

## Installing and configuring the servlet

### Tomcat Installation

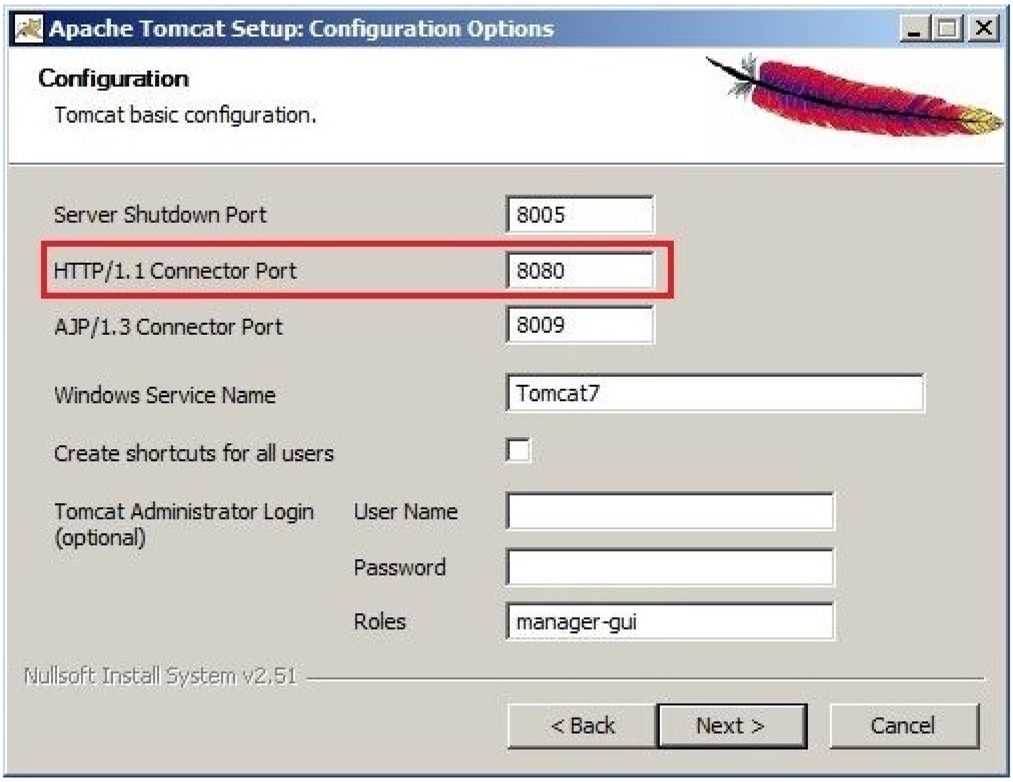
You can install an Apache Tomcat 9.0.54 server either from a .zip file or with an installation executable. We recommend using the installer, but, the .zip archive works as well. The only difference will be the way you will have to configure the Apache Tomcat 9.0.54 server.

**Requirements for both scenarios:**

1. Make sure you have a 64bit Java Runtime Environment (JRE) version installed. A 64bit Java Development Kit (JDK) will also work. Java must be version 8 or later.
2. Download a 64bit version of Apache Tomcat 9.0.54. Make sure the version you plan to use is not newer than the one supported by Acronis Cyber Files. The version used by Acronis Cyber Files is indicated at the beginning of the Acronis Cyber Files Release History document.

## Using an installation executable

1. Download an installation file with the 64bit version of Apache Tomcat 9.0.54. You can find the list of versions at Apache Tomcat's site. Find the desired version and click on it, then open the bin folder and download the .exe file (e.g. **apache-tomcat-9.0.54.exe**).
2. Start the installer and follow the steps of the installation wizard. You can use all of the default settings. You can change the listen port if necessary, the default is 8080.



Apache Tomcat Setup: Configuration Options

Configuration

Tomcat basic configuration.

Server Shutdown Port: 8005

HTTP/1.1 Connector Port: 8080

AJP/1.3 Connector Port: 8009

Windows Service Name: Tomcat7

Create shortcuts for all users: □

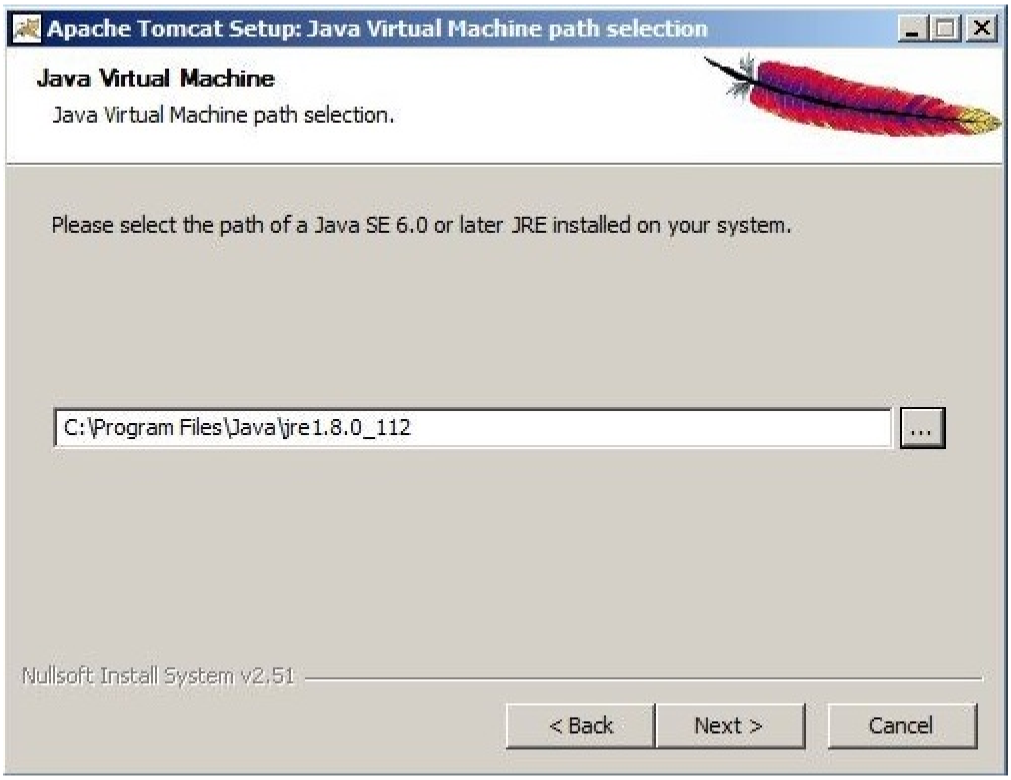
Tomcat Administrator Login (optional)

User Name:

Password:

Roles: manager-gui

**Note**
The installer will pick up the Java installation folder automatically.



Apache Tomcat Setup: Java Virtual Machine path selection

Java Virtual Machine

Java Virtual Machine path selection.

Please select the path of a Java SE 6.0 or later JRE installed on your system.

C:\Program Files\Java\jre1.8.0_112

3. Once the installation is done, go to your machine with Acronis Cyber Files and navigate to your Acronis Cyber Files installation folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Access Server\`).
4. Copy the **AccessPreviewServlet** folder to the new machine with Apache Tomcat installed and paste it in your Tomcat's **webapps** folder. (by default C:\Program Files\Apache Software Foundation\Tomcat 9.0.54\webapps)
5. Navigate to the **conf** folder of your Apache Tomcat installation (by default C:\Program Files\Apache Software Foundation\Tomcat 9.0.54\conf) and backup the **server.xml** file.
6. Now open the file, find the lines: `<Host name="localhost" appBase="webapps"unpackWARs="true" autoDeploy="true">` and place the following right under them:

```
<!-- for Access Web preview -->
```

```
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Software
Foundation\Tomcat 9.0.54\webapps\AccessPreviewServlet">
```

```
</Context>
```

**Note**

If you have installed Apache Tomcat in a location different than the default, you will have to edit the **docBase=""** path to reflect the correct path of your installation.

7. Save and close the file.

8. To start the Tomcat service, open **Control Panel** -> **Administration Tools** -> **Services** and start the Apache Tomcat service.

## Using an archived Apache Tomcat installation

1. Download a **.zip** file with the 64bit version of Apache Tomcat 9.0.54. You can find the list of versions at Apache Tomcat's site. Find the desired version and click on it, then open the bin folder and download the core .zip file (e.g. **apache-tomcat-9.0.54.zip**).
2. Extract the contents of the archive to your preferred location. e.g. **C:\Program Files\Apache Tomcat.**
3. Navigate to **C:\Program Files\Apache Tomcat\apache-tomcat-<version>** and open the **bin** folder.

**Note**
The extracted folder name contains a version number, replace **<version>** with the version of your Tomcat. e.g. **C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54**

4. Open **startup.bat** with a text editing program and find the line **setlocal**.
5. Add the following lines below it:

```
set "CATALINA_HOME=Your Tomcat Folder"
e.g.set"CATALINA_HOME=C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54"
```

**Note**
This sets the default Tomcat folder for all settings. Use the proper path for your Apache Tomcat folder.

```
set "JRE_HOME=Java main folder location"
e.g. set "JRE_HOME=C:\Program Files\Java\jre1.8.0_112"
```

**Note**
This sets the default JRE folder for all settings. Use the proper path for your Java folder.

**Note**
If you're using a JDK, the command is **JAVA_HOME** instead of **JRE_HOME**.

6. Save any changes made to the file.
7. Once that is done, go to your machine with Acronis Cyber Files and navigate to your Acronis Cyber Files installation folder (by default `C:\Program Files (x86)\Acronis\Files Advanced\Access Server\`).
8. Copy the **AccessPreviewServlet** folder to the new machine with Apache Tomcat and paste it in your Tomcat's **webapps** folder. (by default `C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54\webapps`).
9. Navigate to the **conf** folder of your Apache Tomcat installation (e.g. **C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54\conf)** and backup the **server.xml** file.

10. Now open the file, find the lines: `<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">` and place the following right under them:

    ```
    <!-- for Access Web preview -->
    ```

    ```
    <Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Tomcat\apache-tomcat-9.0.54\webapps\AccessPreviewServlet">
    ```

    ```
    </Context>
    ```

11. Edit the `docBase=""` path to reflect the correct path of your installation. Save and close the file.

    **Note**

    If you do not change the default port the server is listening on, the servlet will be listening on **8080**. To change the port, find the following lines in the **server.xml** file:

    ```
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    ```

    Replace **8080** with the desired port number.

12. To start the Tomcat service, navigate to the bin folder and double-click on the **startup.bat** file. The black DOS window must remain open while the Tomcat is running.

## Acronis Cyber Files Server Configurations

1. Open the Acronis Cyber Files web interface and open **General Settings** -> **Web Previews**.
2. Enable **Use custom URL for web preview service** and enter the address for your new web preview servlet. (**e.g.**`http://accesswp.company.com:8080`). The port number must be present in the URL you provide. If you're using a load-balanced or clustered setup, the URL will be the address of your loadbalancer.
3. Depending on the number of servers you set up to run the web preview servlet, you may want to increase the number of **Maximum concurrent generation** calls the Acronis Cyber Files server is set to.
4. Find the setting **Maximum concurrent generation calls** setting and set it to the appropriate value.

   The default value is 2. Rendering of a document can utilize the majority of one processor core. The number of rendering threads should be set to no greater than 50% of your available processor cores. Exceeding this recommendation can result in degradation of other services on the server.

## Load-balancing your Web Preview servlets

Your **Web Preview** servlets must be placed behind a load-balancer.

1. Enable duration-based session stickiness (or your load balancer's equivalent) on your load balancer and configure it to not expire.
2. If a health-check is required (looking for an HTTP status of 200 to be returned), a ping to **http://servername.yourdomain.com:port/AccessPreviewServlet/generate_preview/** will satisfy it.

   e.g. `https://servlet1.acme.com/AccessPreviewServlet/generate_preview` and `https://servlet2.acme.com/AccessPreviewServlet/generate_preview`.
3. Using a browser, open the address of your load balancer to verify the configuration is working.

   e.g. `https://loadbalancer.yourdomain.com`

# PostgreSQL Streaming Replication

The purpose of this document is to provide a step-by-step procedure on how to configure streaming replication between two PostgreSQL servers. Streaming replication is one of the many methods that exist to keep a PostgreSQL database online, but other methods won't be addressed in this document.

**Note**
This document does not describe the installation process of PostgreSQL or Acronis Cyber Files but only the streaming replication configuration.

## Streaming replication

The streaming replication process is based on Write-Ahead Logging (WAL) segment. WAL, is a standard method for ensuring data integrity. WAL's central concept is that changes to data files (where tables and indexes reside) must be written only after those changes have been logged, that is, after log records describing the changes have been flushed to permanent storage. If we follow this procedure, we do not need to flush data pages to disk on every transaction commit, because we know that in the event of a crash we will be able to recover the database using the log: any changes that have not been applied to the data pages can be redone from the log records.

Using WAL results in a significantly reduced number of disk writes, because only the log file needs to be flushed to disk to guarantee that a transaction is committed, rather than every data file changed by the transaction. The log file is written sequentially, and so the cost of syncing the log is much less than the cost of flushing the data pages.

WAL also makes it possible to support on-line backup, point-in-time recovery and replication. Streaming replication refers to continuous sending of WAL records over a TCP/IP connection between a primary server and a standby server, using the walsender protocol over replication connections. Although streaming replication can be synchronous, and considering the resources needed and the impact on performances of a synchronous process, we've decided to only consider asynchronous streaming replication as a valid scenario.

## Requirements:

- Two PotsgreSQL servers: the active server will be called “primary server” and the passive server will be called “standby server” in the procedure.

  **Note**
  **Only the Primary server can be used for Acronis Cyber Files connections.** The Standby server can be used only if a failover occurs and it gets promoted to Primary.

- PostgreSQL 11.6: We will implement features like “replication slot” that require PostgreSQL 11.6. This version is embedded with Acronis Cyber Files 8.7 and higher, and used only during new installations (not upgrades).
- One virtual IP (optional): this virtual IP will be used in all frontends that run the Acronis Cyber Files Server role and should always be owned by to the active host (the primary server).
- We recommend that Acronis Cyber Files is already installed and the primary server’s database has been initialized.

## On the Primary Server

### Create a replication user

This user will be used by the replication process to send WAL from the Primary server to the Standby server. For security reasons, it is recommended to create a dedicated user, with replication permissions, instead of using the default superuser account (i.e. **postgres**).

1. On the Primary server, run the following command:

   ```
   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -U postgres
   ```

   This command can also be run remotely using the following options:

   ```
   psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -h <IP_OF_
   PRIMARY_SERVER> -U postgres
   ```

   **Note**
   PSQL is located in the **bin** sub-folder of PostgreSQL's installation folder. Depending on your PATH environment variable, you may need to specify the path to reach the command or move to the right directory before executing the command. This note also applies for the next commands used in this procedure.

### Configure access

Edit the access control on the Primary Server to allow the connection from the Standby Server.

1. This can be done by editing the **pg_hba.conf** file (located in the **data** sub-folder) and adding the following line:

   ```
   host replication replicator <IP_OF_STANDBY_SERVER>/32 trust
   ```

2. If more security is needed between the database servers, then authentication can require the client to supply an encrypted password (md5) with an additional option to also require SSL encryption (**hostssl**) e.g.:

   ```
   host replication replicator <IP_OF_STANDBY_SERVER>/32 md5
   hostssl replication replicator <IP_OF_STANDBY_SERVER>/32 md5
   ```

## Configure streaming replication

1. Go to the PostgreSQL installation folder. Its default location is:

   ```
   C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>
   ```
2. In the `Data` folder, navigate to the `postgresql.conf` file to modify it. Locate and edit the following line:

   > **Note**
   > Make sure that this line is not preceded by a **#** symbol. If it is, commands are treated as comments and will not have any effect.

   ```
   listen_addresses = 'IP_OF_PRIMARY_SERVER, 127.0.0.1'
   ```

3. Restart the PostgreSQL service after making the above changes.

## Create a replication slot

1. On the Primary Server, run the following command:

   ```
   psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"
   ```
2. Verify that the slot is created using the following command:

   ```
   psql -U postgres -c "SELECT * FROM pg_replication_slots;"
   ```

# On the Standby Server

## Verify that all necessary servers have access to each other

In case of a fail-over, the Standby server will be promoted to be the Primary server and will reply to all Acronis Cyber Files Servers' requests.

It is recommended to configure the access to the Standby server for all Acronis Cyber Files Servers now, so that you won’t be required to reboot the PostgreSQL service on any Standby server during the fail-over process.

> **Note**
> When the Standby server is in standby mode, the database is in read-only mode (hot standby). It is not possible to configure and use the Standby server as the production database by mistake.

1. Edit the access control on the Standby server to allow the connection from all Acronis Cyber Files Servers.

2. To do this, navigate to the PostgreSQL installation folder and edit the **pg_hba.conf** file (located in the `data` sub-folder), by adding the following line for each server:

   ```
   host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
   ```

   ```
   host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
   ```

## Configure streaming replication

1. Go to the PostgreSQL installation folder. Its default location is:

   ```
   C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>
   ```

2. In the `Data` folder, navigate to the `postgresql.conf` file to modify it. Locate and edit the following lines:

   **Note**
   Make sure that these lines are not preceded by a **#** symbol. If they are, the commands are treated as comments and will not have any effect.

   - `listen_addresses = '`**IP_OF_STANDBY_SERVER**`,` 127.0.0.1`'`
   - `hot_standby = on`

   The `hot_standby` setting specifies whether or not you can connect and run queries during streaming replication. When it is enabled, the database will accept read-only request and it is then possible to look at the database and check that replication process works by looking at the database tables' content.

   **Note**
   For the `listen_addresses` parameter, a duplication of lines is possible in the `postgresql.conf` file, where the first (commented) line exists as part of the default file template and the second (uncommented) one is added by the product installer. Make sure to edit only the first line and do not uncomment any additional lines, if there are such.

   **Note**
   If the `max_connections` setting in the `postgresql.conf` file has been changed on the Primary server, to a value different from the default one, you have to change it on the Standby server as well.

   **Note**
   When using `md5` or `password` as the authentication method specified in `pg_hba.conf`, a password will be required for that connection. To "enter" this password, you have to add the following command to the `recovery.conf` file on the Standby server:
   `primary_conninfo = 'host=`<IP_ADDRESS_OF_PRIMARY_SERVER> `port=`<PORT_OF_PRIMARY_SERVER> `user=`<USERNAME> `password=`<PASSWORD_FOR_USERNAME>`'`
   e.g. this is how it would look for Postgres running on IP 10.0.0.1, port 5432, with user `replicator` and password `1234`: `primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'`

3. **Stop the PostgreSQL service on the Secondary server to do the initial seeding of the database and start the streaming replication process.**

## Backup configuration files

Make a backup of all the **.conf** configuration files, including: **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**. These files will be overwritten by the initial seeding process and you will need to restore them after this step.

## Clean the data directory

Delete (or just rename) the **data** sub-folder. Renaming the folder is a good way to keep a copy of a previous configuration and be able to revert back the Standby server’s database to a consistent state in case an issue occurs during the initial seeding or at the database startup.

## Initial seeding

The initial seeding is done using a backup of the Primary database to a folder located on the Standby server.

1. Make sure that the Primary server is not in active use. The easiest way to do this is to stop the Acronis Cyber Files Tomcat service, and then start it when the seeding is complete.
2. To start the initial seeding at Standby server level, use the following command:

   ```
   pg_basebackup.exe -h <IP_OF_PRIMARY_SERVER> -D <PATH_TO_NEW_DATA_DIR> -U replicator -v -P
   --slot=access_slot
   ```

   **Note**
   `<PATH_TO_NEW_DATA_DIR>` should be the path to the new `Data` folder. e.g. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.6\Data`

## Restore configuration files

Copy of all the **.conf** configuration files (including **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**) from the backup folder to the new `Data` folder and overwrite all existing files.

## Create a replication slot

1. On the Secondary Server, run the following command:

   ```
   psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"
   ```

2. Verify that the slot is created using the following command:

   ```
   psql -U postgres -c "SELECT * FROM pg_replication_slots;"
   ```

## Streaming replication controls

1. Open the Data folder and create (or modify) the `recovery.conf` file.
2. Add the following lines if they don't already exist:

- `standby_mode = 'on'`
- `primary_conninfo = 'host=<`**IP_OF_PRIMARY_SERVER**`> port=5432 user=replicator password=<`**PASSWORD_USED_FOR_REPLICATOR_USER**`>'`
- `primary_slot_name = 'access_slot'`
- `trigger_file = '<`**PATH_TO_TRIGGER_FILE**`>' # As an example 'failover.trigger'`
- `recovery_min_apply_delay = 5min`

3. Start the PostgreSQL service on the Standby server after saving the above changes.

**Note**
In case of a fail-over, the `recovery.conf` file will be renamed to `recovery.done`.

## Additional Information

- The `standby_mode` setting specifies to start the PostgreSQL server as a standby. In this case, the server will not stop the recovery when the end of archived WAL is reached, but will keep trying to continue the recovery by fetching new WAL segments connecting to the Primary server as specified by the `primary_conninfo` setting (that specifies a connection string to be used for the Standby server to connect with the Primary server).
- We use the replication slot created during the previous steps on the Primary server, by using the `primary_slot_name` setting.
- The `trigger_file` setting specifies a trigger file whose presence ends recovery on the Standby server and makes it the Primary server. This will be used during the fail-over process.
- Optionally, `recovery_min_apply_delay` settings can be set. By default, a Standby server restores WAL records from the Primary server as soon as possible. It may be useful to have a time-delayed copy of the data, offering opportunities to correct data loss errors. This parameter allows to delay recovery by a fixed period of time, measured in milliseconds if no unit is specified.

  For example, if you set this parameter to 5 min, the Standby server will replay each transaction commit only when the system time on the standby is at least five minutes past the commit time reported by the primary server.

  It is possible that the replication delay between servers exceeds the value of this parameter, in which case no delay is added. Note that the delay is calculated between the WAL timestamp as written on the Primary Server and the current time on the standby server. Delays in transfer because of network lag or cascading replication configurations may reduce the actual wait time significantly. If the system clocks on the Primary Server and the Standby Server are not synchronized, this may lead to recovery applying records earlier than expected; but that is not a major issue because useful settings of this parameter are much larger than typical time deviations between servers.

## Testing the fail-over

We recommend that you test the above settings and make sure the fail-over works, before implementing it in your production setup.

If the Primary server is not down, make sure to stop it before configuring the Standby server to take that role. This is done to avoid the Primary server from processing further queries leading to issues.

You can turn the Standby server into Primary by creating the trigger file mentioned in **recovery.conf**. Now that the Standby server has taken over the role of the Primary server, make sure that your Acronis Cyber Files servers are configured to use it.

**Note**
Once the fail-over process is triggered and completes successfully, the `recovery.conf` file will be renamed to `recovery.done`. The trigger file will be deleted.

This can be done by navigating to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server` and editing `acronisaccess.cfg`. Make sure that `DB_HOSTNAME` and `DB_PORT` point to the address and port of whichever PostgreSQL server is currently the Primary one. If you make any changes, you will have to restart the Acronis Cyber Files Tomcat service.

### Migrating the instance

1. To make this upgrade, you have to ensure some downtime by stopping Acronis Cyber Files.
2. Stop also both the Primary and the Standby PostgreSQL servers.
3. Upgrade the Primary server, following the instructions from "Upgrading PostgreSQL to a newer major version" (p. 211).
4. Install the same PostgreSQL major version on the Standby server.
5. Follow the Streaming Replication instructions, available for both Primary and Standby servers.

## Configuring PostgreSQL for remote access

**Important**
Remote administration is supported for PostgreSQL 9 server only.

Remote access can help you if you are managing multiple instances of PostgreSQL or you just prefer to manage your database remotely.

### To enable remote access to this PostgreSQL instance, follow the steps below

1. Navigate to the PostgreSQL installation directory: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\Data\`
2. Edit **pg_hba.conf** with a text editor.
3. Include host entries for each computer that will have remote access using their internal address and save the file. The **pg_hba.conf** (HBA stands for host-based authentication) file controls client authentication and is stored in the database cluster's data directory. In it you specify which servers will be allowed to connect and what privileges they will have. e.g.:

```
# TYPE DATABASE USER ADDRESS METHOD

# First Acronis Cyber Files & Gateway server

host all all 10.27.81.3/32 md5

# Second Acronis Cyber Files & Gateway server

host all all 10.27.81.4/32 md5
```

`In these examples all users connecting from the first computer (10.27.81.3/32) and the second computer (10.27.81.4/32) can access the database with full privileges (except the replication privilege) via a md5 encrypted connection.`

4. Navigate to and open the **postgresql.conf**. By default it is located at: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\Data\`
   a. Find the line `#listen_addresses = 'localhost'`
   b. Enable this command by removing the **#** symbol at the start of the line.
   c. Replace `localhost` with ***** to listen on all available addresses. If you want PostgreSQL to listen only on a specific address, enter the IP address instead of *****.
      - **e.g.** `listen_addresses = '*'` - This means that PostgreSQL will listen on all available addresses.
      - **e.g.**`listen_addresses = '192.168.1.1'` - This means that PostgreSQL will listen only on that address.
5. Save any changes made to the **postgresql.conf**.
6. Restart the Acronis Cyber Files PostgreSQL service.

**Note**
PostgreSQL uses port 5432 by default. Make sure that this port is open in any firewall or routing software.

## Running Acronis Cyber Files in HTTP mode

These settings are provided for situations where you are required to use unencrypted HTTP communications between Acronis Cyber Files and internal services, such as load balancing and proxy solutions. Acronis Cyber Files servers communicating on insecure local networks and over the internet should always be operated in HTTPS mode. When running in HTTP mode internally, Acronis Cyber Files network traffic will become easily visible to all parties with access to the internal network.

To switch from HTTPS to HTTP you need to change some settings in the following files:

- Tomcat's `server.xml` file, located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.75\conf`

  **Note**
  The Tomcat version number may vary depending on the version of Acronis Cyber Files you are using.

- The `acronisaccess.cfg` file, located in `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server`.

## Editing the server.xml file

In this file, the appropriate HTTP connector will need to be set and the HTTPS ones disabled.

1. Open the file with a text editor and find the existing HTTPS connector. It should look like this:

   ```
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
   SSLEnabled="true" SSLProtocol="TLSv1.2"
   SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
   SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
   SSLHonorCipherOrder="true"
   SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW
   :!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
   bindOnInit="false" port="443" address="0.0.0.0"/>
   ```

2. Disable the HTTPS connector by surround it with `<!--` and `-->`. i.e. you should put `<!--` before `<Connector maxHttp.....` and `-->` after ... `address="0.0.0.0"/>`
3. Create a new, HTTP connector, looking like this:

   ```
   <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="http" secure="true"
   connectionTimeout="-1" URIEncoding="UTF-8" port="80" address="0.0.0.0"/>
   ```

4. You can select a different port besides the default one and limit the addresses for connection to a particular one so the service does not use all available addresses.
5. Make sure that the port you decide to use is open in your Firewall.
6. Check if you have this redirecting connector in your server.xml file:

   ```
   <!-- <Connector port="80" connectionTimeout="20000" protocol="HTTP/1.1"
   redirectPort="443"/> -->
   ```

7. If you do and you would like to use port 80, disable it by commenting with `<!-` and `->` as described above.
8. Save the file after you have made the necessary changes.

## Editing the acronisaccess.cfg

The only thing that needs an update here is to set the `REQUIRE_SSL` at the end of the file from **true** to **false**, so it should look like this:

```
REQUIRE_SSL = false
```

1. Save the file after you've made the necessary changes.
2. Restart the Acronis Cyber Files Tomcat service so that all changes are in effect.

## HTTP mode limitations

- In **HTTP** mode, communication with the Gateway server is not supported as the Gateway requires **HTTPS** to work. Network node access via the Web UI or mobile clients will not work.
- Single Sign-On is not supported.
- If using Desktop clients, **HTTP** will need to be specified manually in the server address field or the connection will fail. e.g. `http://myaccess.com:3000`

# Running Acronis Cyber Files Tomcat using insecure TLS versions

**Note**
Deployments using older TLS versions may break because of changes introduced in this release. Find below how to workaround this, although Acronis no longer supports such configurations.

Beginning with Acronis Cyber Files 8.8.0, all new installations and upgrades will be configured to use TLSv1.2 only.

These steps are unsupported and provided as-is to enable TLSv1 and TLSv1.1 for those who may need to use these insecure TLS versions.

**Managing TLS configurations during Tomcat 9 upgrades**

**Note**
The Connector configuration handling/update is similar to what is described in Running Acronis Cyber Files in HTTP mode and Running Acronis Cyber Files Tomcat on multiple ports.

**Note**
Before enabling TLSv1 and TLSv1.1, make sure this is really necessary. Most web browsers have already deprecated TLSv1 and TLSv1.1, and are by default using TLSv1.2. Some other services that integrate with Acronis Cyber Files may only need an update to work with TLSv1.2, for example, Office Online needs patch KB5001973)

1. Stop the Acronis Cyber Files Tomcat service.
2. Navigate to the `server.xml` file. Its default location is:
   `C:\Program Files (x86)\Acronis\Cyber Files\Common\apache-tomcat-9.0.54\conf`

   **Note**
   Your path may be different if you've upgraded to a newer version of Acronis Cyber Files or performed a custom install. You can use the Acronis Cyber Files Tomcat entry in Windows Services to locate the path to the Apache Tomcat folder, which will contain the `conf` folder.

3. Make a copy of the original, unedited `server.xml` file with a different name, in case you need to revert to the supported version.

4. In the Connector section of the same file, locate the below content:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AACert.cer"
SSLCertificateKeyFile="${catalina.base}/conf/AACert.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL
:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" relaxedQueryChars="[,]" port="443" address="0.0.0.0"/>
```

5. Change the text in the following way:

   From

```
SSLProtocol="TLSv1.2"
```

   To

```
SSLProtocol=”TLSv1+TLSv1.1+TLSv1.2"
```

6. Finally, save the file.
7. Start the Acronis Cyber Files Tomcat service.

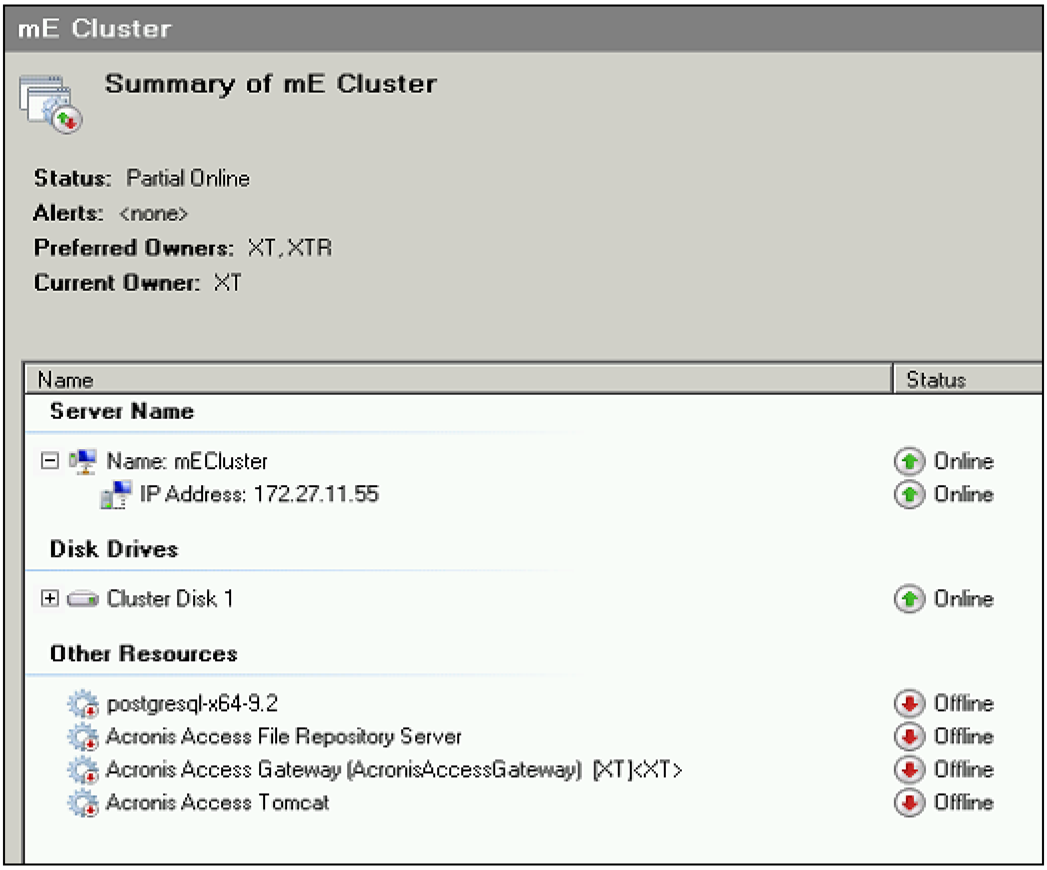
## Upgrading Acronis Cyber Files on a Microsoft Failover Cluster

The following steps will help you upgrade your Acronis Cyber Files Server cluster to a newer version of Acronis Cyber Files.

**Note**

***Before performing any upgrades, please review our Backup articles and backup your configuration.***

1. Go to the the active node.
2. Open the **Cluster Administrator**/**Failover Cluster Manager**.
3. Stop all of the Acronis Cyber Files services (including **postgres-some-version**). The shared disk must be online.



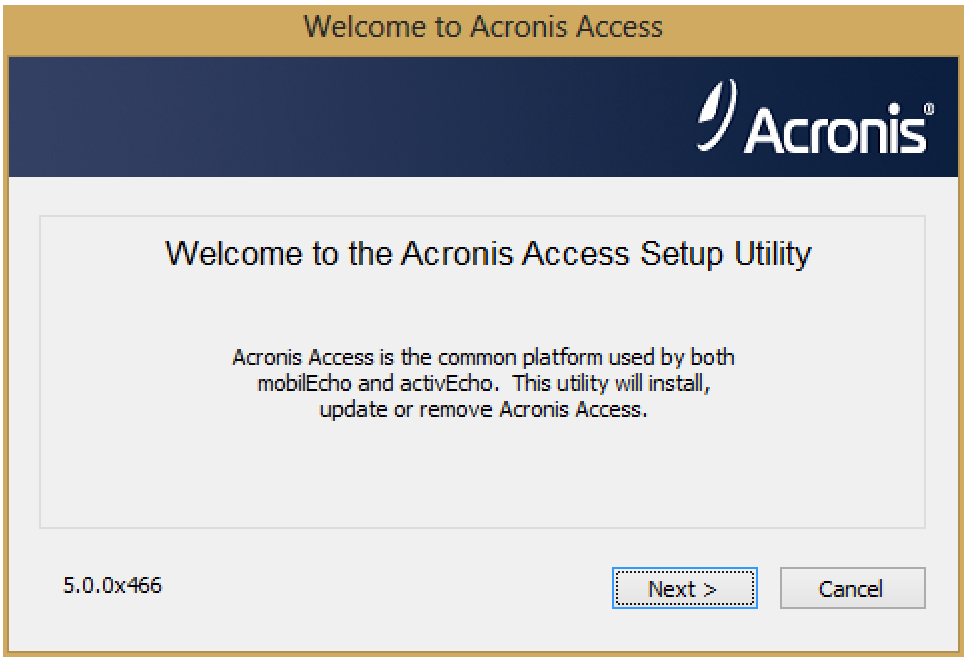
mE Cluster

Summary of mE Cluster

**Status:** Partial Online
**Alerts:** <none>
**Preferred Owners:** XT, XTR
**Current Owner:** XT

| Name | Status |
|---|---|
| **Server Name** | |
| Name: mECluster | Online |
| IP Address: 172.27.11.55 | Online |
| **Disk Drives** | |
| Cluster Disk 1 | Online |
| **Other Resources** | |
| postgresql-x64-9.2 | Offline |
| Acronis Access File Repository Server | Offline |
| Acronis Access Gateway (AcronisAccessGateway) [XT]<XT> | Offline |
| Acronis Access Tomcat | Offline |

4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
5. Double-click on the installer executable.



Welcome to Acronis Access

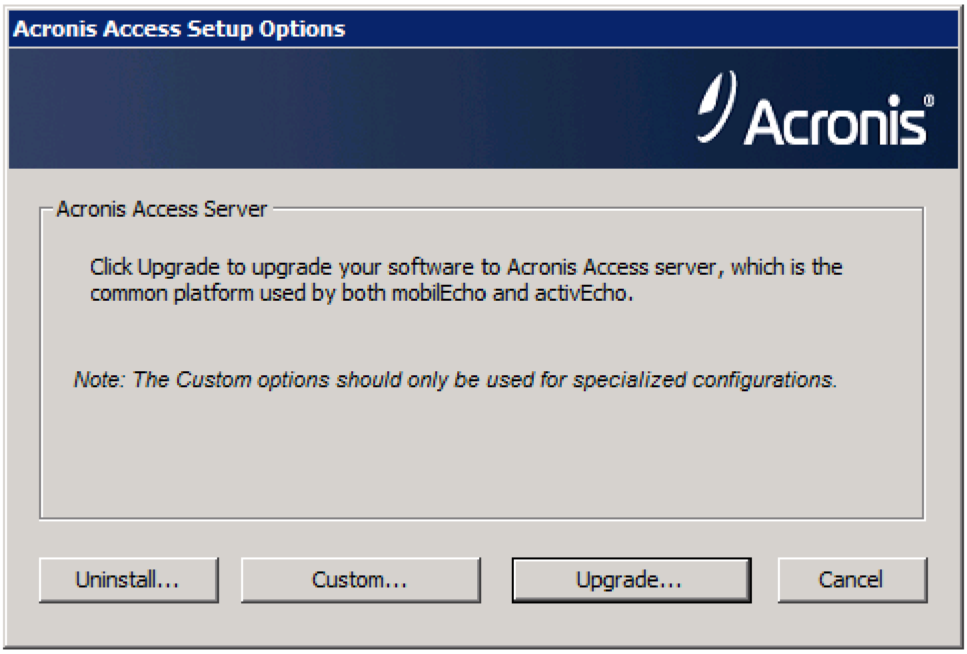
Welcome to the Acronis Access Setup Utility

Acronis Access is the common platform used by both mobilEcho and activEcho. This utility will install, update or remove Acronis Access.

5.0.0x466

6. Click **Next** to begin.
7. Read and accept the license agreement.

8. Click **Upgrade**.



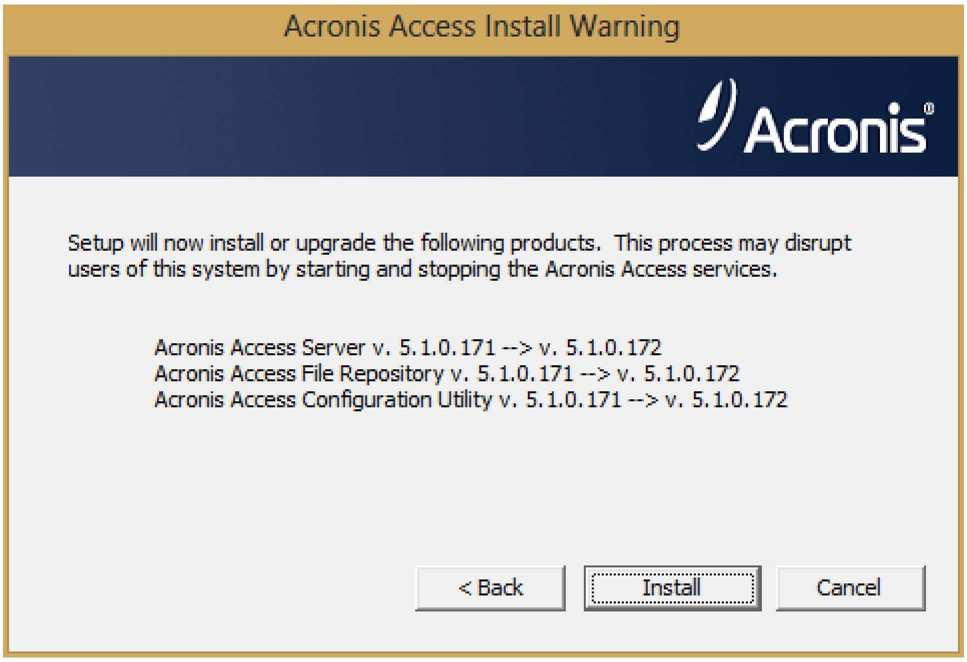
Acronis Access Setup Options

Acronis Access Server

Click Upgrade to upgrade your software to Acronis Access server, which is the common platform used by both mobilEcho and activEcho.

*Note: The Custom options should only be used for specialized configurations.*

9. Review the components which will be installed and press **Install**.



Acronis Access Install Warning

Setup will now install or upgrade the following products. This process may disrupt users of this system by starting and stopping the Acronis Access services.

Acronis Access Server v. 5.1.0.171 --> v. 5.1.0.172
Acronis Access File Repository v. 5.1.0.171 --> v. 5.1.0.172
Acronis Access Configuration Utility v. 5.1.0.171 --> v. 5.1.0.172

10. Enter the password for your **postgres** super-user and press **Next**.
11. When the installation finishes, press **Exit** to close the installer.

**Warning!**
Do not bring the cluster group online!

12. Move the cluster group to the second node.
13. Complete the same installation procedure on the second node.
14. Bring all of the Acronis Cyber Files services online.

## Installing Acronis Cyber Files on a Microsoft Failover Cluster

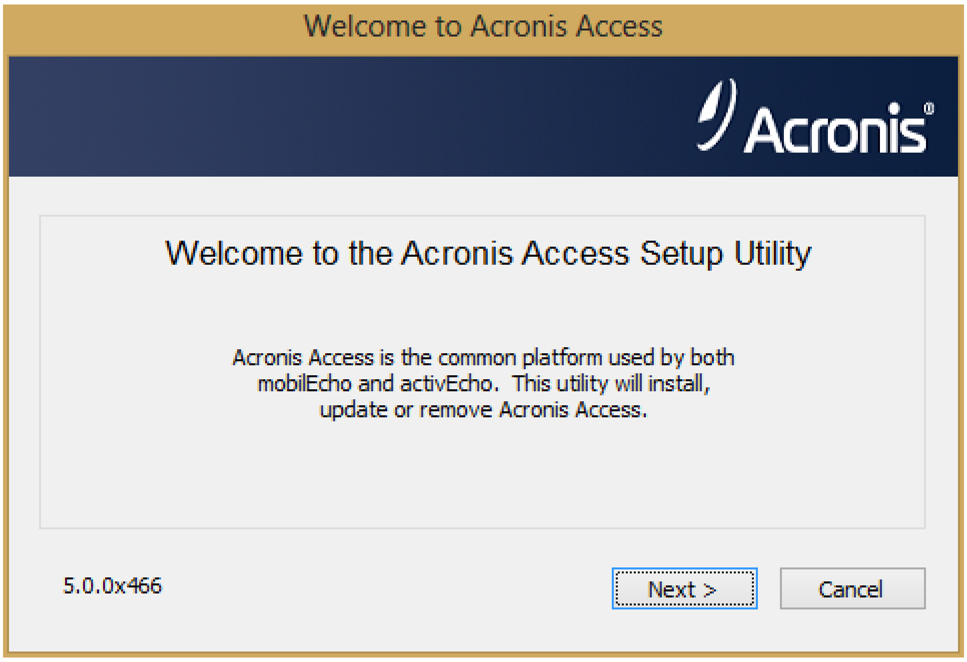
The guides listed below will help you install Acronis Cyber Files on your cluster.

## Installing Acronis Cyber Files on a Windows 2012 (R2) Microsoft Failover Cluster

### Installing AcronisCyber Files

Please make sure you are logged in as a domain administrator before installing AcronisCyber Files.

1. Download the AcronisCyber Files installer.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



Welcome to Acronis Access

Welcome to the Acronis Access Setup Utility

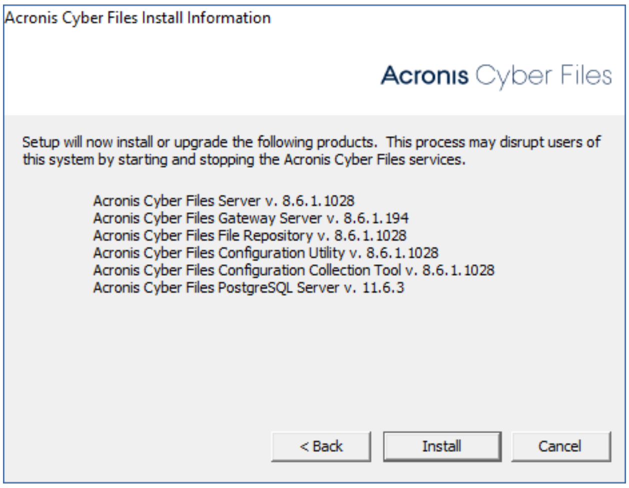
Acronis Access is the common platform used by both mobilEcho and activEcho. This utility will install, update or remove Acronis Access.

5.0.0x466

4. Click **Next** to begin.
   Read and accept the license agreement.
5. Click **Install**.

> **Note**
> If you're deploying multiple Acronis Cyber Files servers, or you are installing a non-standard configuration, you can select which components to install from the **Custom Install** button.

6. Either use the default path or select a new one for the Acronis Cyber Files main folder and click **OK**.

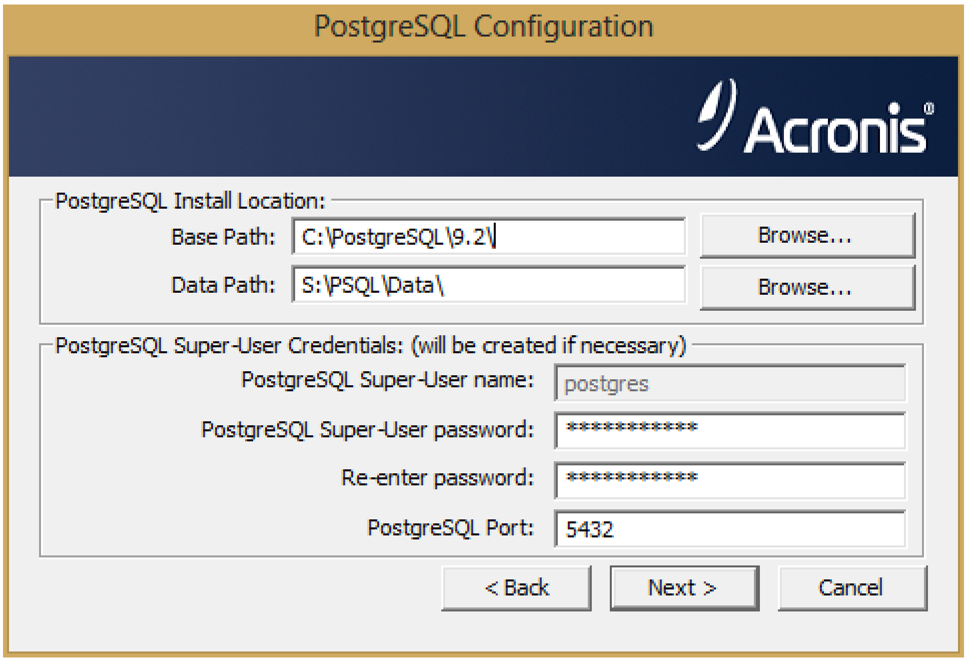


Acronis Cyber Files Install Information

Setup will now install or upgrade the following products. This process may disrupt users of this system by starting and stopping the Acronis Cyber Files services.

Acronis Cyber Files Server v. 8.6.1.1028
Acronis Cyber Files Gateway Server v. 8.6.1.194
Acronis Cyber Files File Repository v. 8.6.1.1028
Acronis Cyber Files Configuration Utility v. 8.6.1.1028
Acronis Cyber Files Configuration Collection Tool v. 8.6.1.1028
Acronis Cyber Files PostgreSQL Server v. 11.6.3

7. Set a password for the user Postgres and write it down. This password will be needed for database backup and recovery.
8. Choose a location on a shared disk for the **Postgres Data** folder and click **Next**.



PostgreSQL Configuration

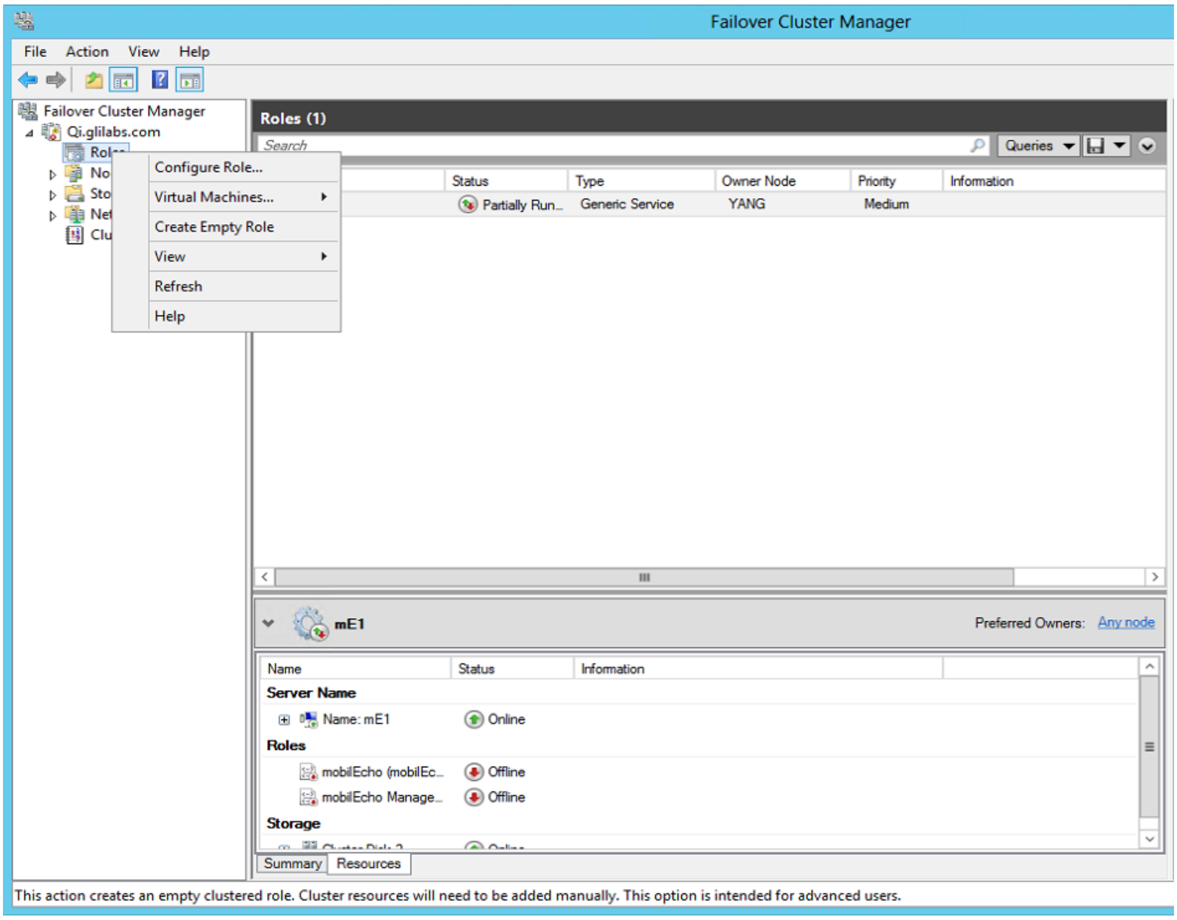
PostgreSQL Install Location:
Base Path: C:\PostgreSQL\9.2\
Data Path: S:\PSQL\Data\

PostgreSQL Super-User Credentials: (will be created if necessary)
PostgreSQL Super-User name: postgres
PostgreSQL Super-User password: ************
Re-enter password: ************
PostgreSQL Port: 5432

9. A window displaying all the components which will be installed appears. Click **OK** to continue.
10. When the Acronis Cyber Files installer finishes, click **Exit**.

## Creating the role

1. Open the **Failover Cluster Manager** and right-click on **Roles**.
2. Select **Create empty role**. Give the role a proper name. (e.g. Acronis Cyber Files, AAS Cluster)



| | Status | Type | Owner Node | Priority | Information |
|---|---|---|---|---|---|
| | Partially Run... | Generic Service | YANG | Medium | |

| Name | Status | Information |
|---|---|---|
| **Server Name** | | |
| Name: mE1 | Online | |
| **Roles** | | |
| mobilEcho (mobilEc... | Offline | |
| mobilEcho Manage... | Offline | |
| **Storage** | | |

This action creates an empty clustered role. Cluster resources will need to be added manually. This option is intended for advanced users.

## Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
   a. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\`
   b. Find the **database.yml** file and open it with a text editor.
   c. Find this line: `database_path: './database/'` and replace **./database/** with the path you want to use (e.g. `database_path: 'S:/access_cluster/database/'`).

**Note**
Use slashes(/) as a path separator.

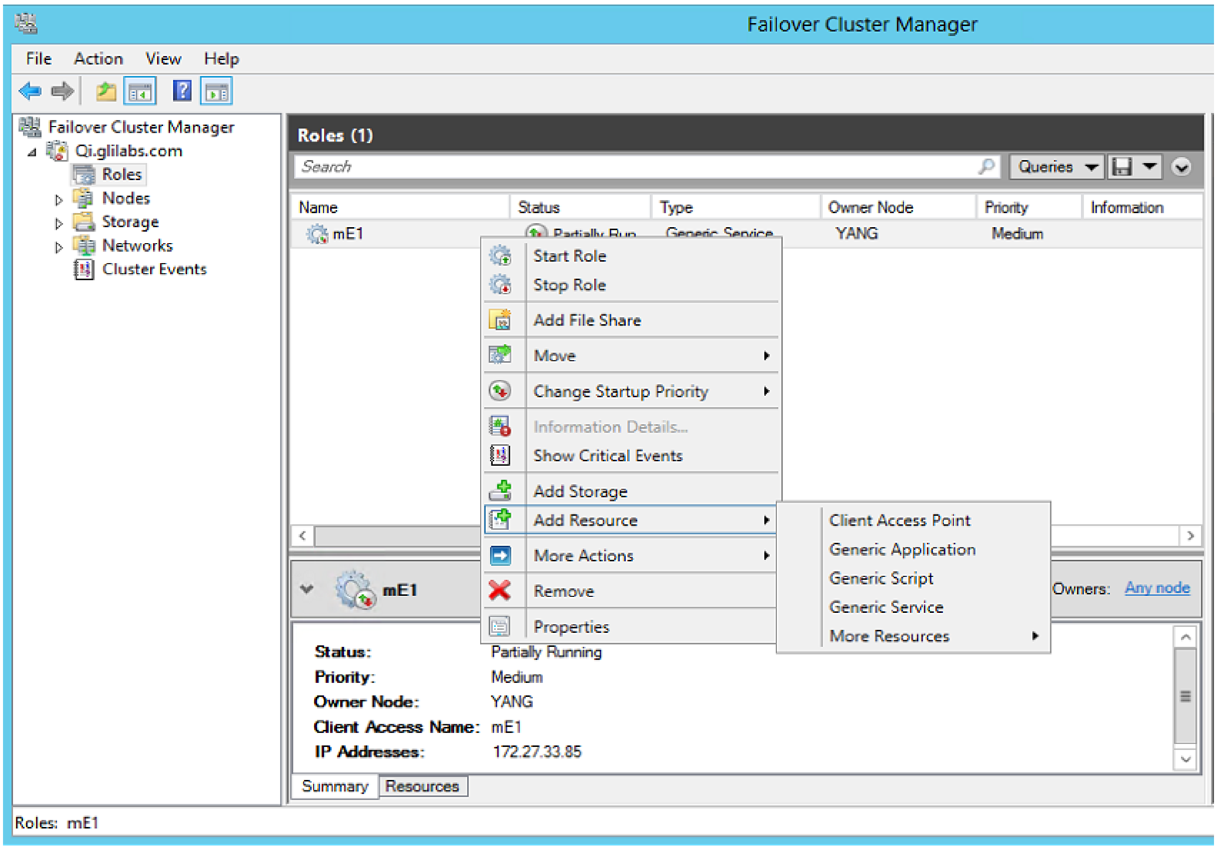
**Note**
You can copy the configured database.yml from the first node and paste it to the second node.

## Adding all of the necessary services to the Acronis Cyber Files role

Complete the following procedure for each of the following services: Acronis Cyber Files Gateway, Acronis Cyber Files PostgreSQL (this may be different depending on the version of Acronis Cyber Files), Acronis Cyber Files Repository and Acronis Cyber Files Tomcat

1. Right-click on the Acronis Cyber Files role and select **Add a resource**.

2. Select **Generic Service**.

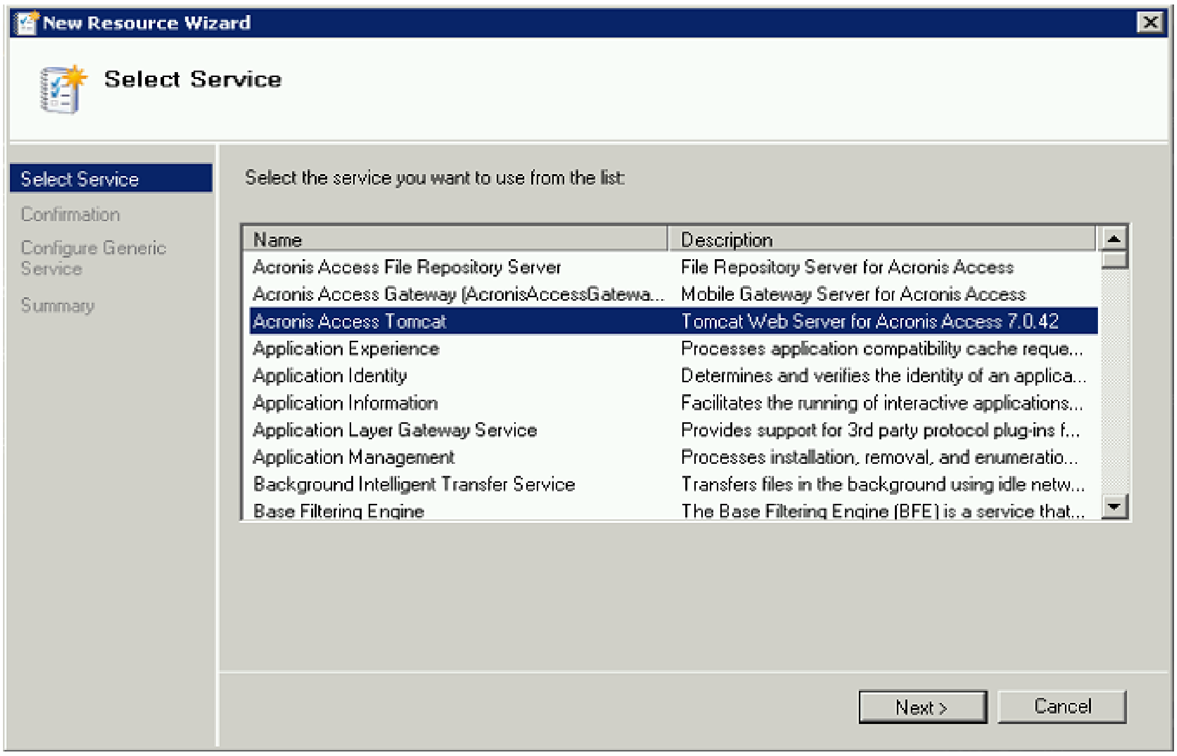


| Name | Status | Type | Owner Node | Priority | Information |
|---|---|---|---|---|---|
| mE1 | Partially Run... | Generic Service | YANG | Medium | |

**mE1**

**Status:** Partially Running
**Priority:** Medium
**Owner Node:** YANG
**Client Access Name:** mE1
**IP Addresses:** 172.27.33.85

3. Select the proper service and click **Next**.



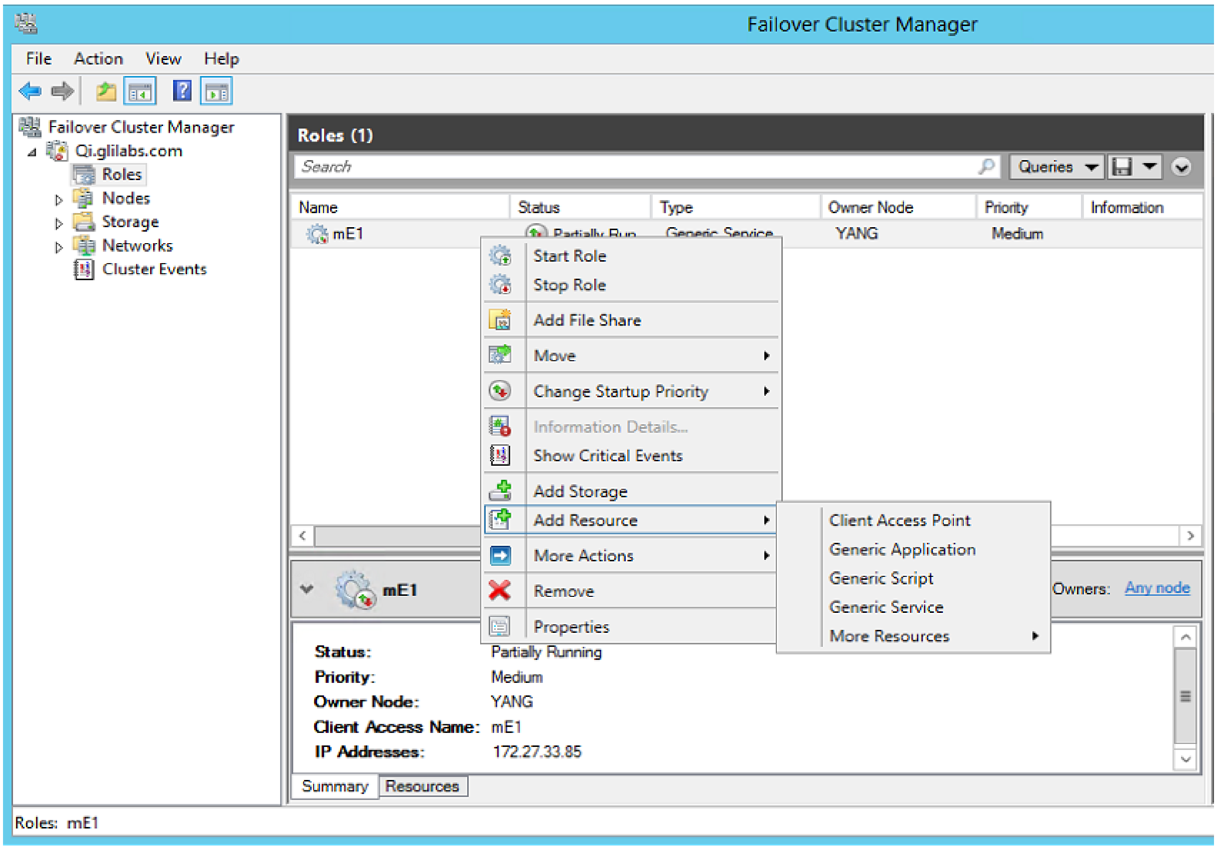
Select the service you want to use from the list:

| Name | Description |
|---|---|
| Acronis Access File Repository Server | File Repository Server for Acronis Access |
| Acronis Access Gateway (AcronisAccessGatewa... | Mobile Gateway Server for Acronis Access |
| Acronis Access Tomcat | Tomcat Web Server for Acronis Access 7.0.42 |
| Application Experience | Processes application compatibility cache reque... |
| Application Identity | Determines and verifies the identity of an applica... |
| Application Information | Facilitates the running of interactive applications... |
| Application Layer Gateway Service | Provides support for 3rd party protocol plug-ins f... |
| Application Management | Processes installation, removal, and enumeratio... |
| Background Intelligent Transfer Service | Transfers files in the background using idle netw... |
| Base Filtering Engine | The Base Filtering Engine (BFE) is a service that... |

4. In the Confirmation window, click **Next**.
5. In the summary window, click **Finish**.

## Setting an Access Point

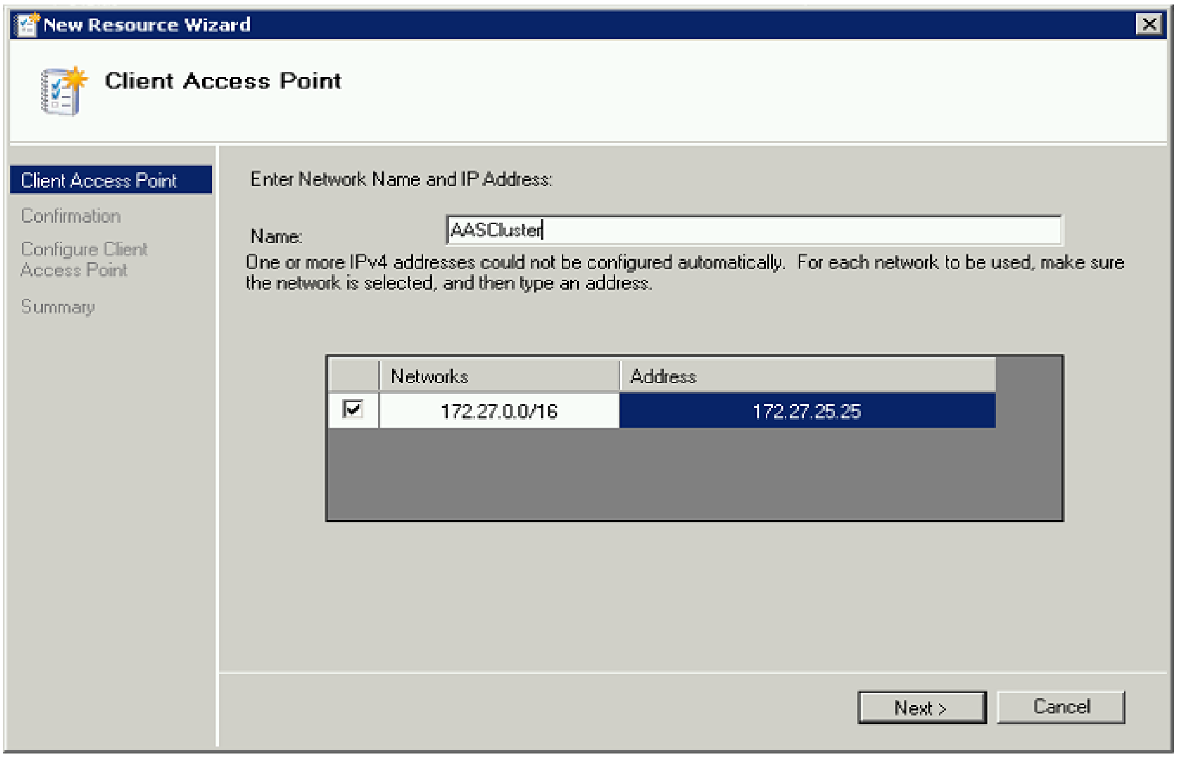
1. Right-click on the Acronis Cyber Files role and select **Add a resource**.
2. Select **Client Access Point**.



mE1

Status: Partially Running
Priority: Medium
Owner Node: YANG
Client Access Name: mE1
IP Addresses: 172.27.33.85

3. Enter a name for this access point.
4. Select a network.



Enter Network Name and IP Address:

Name: AASCluster

One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

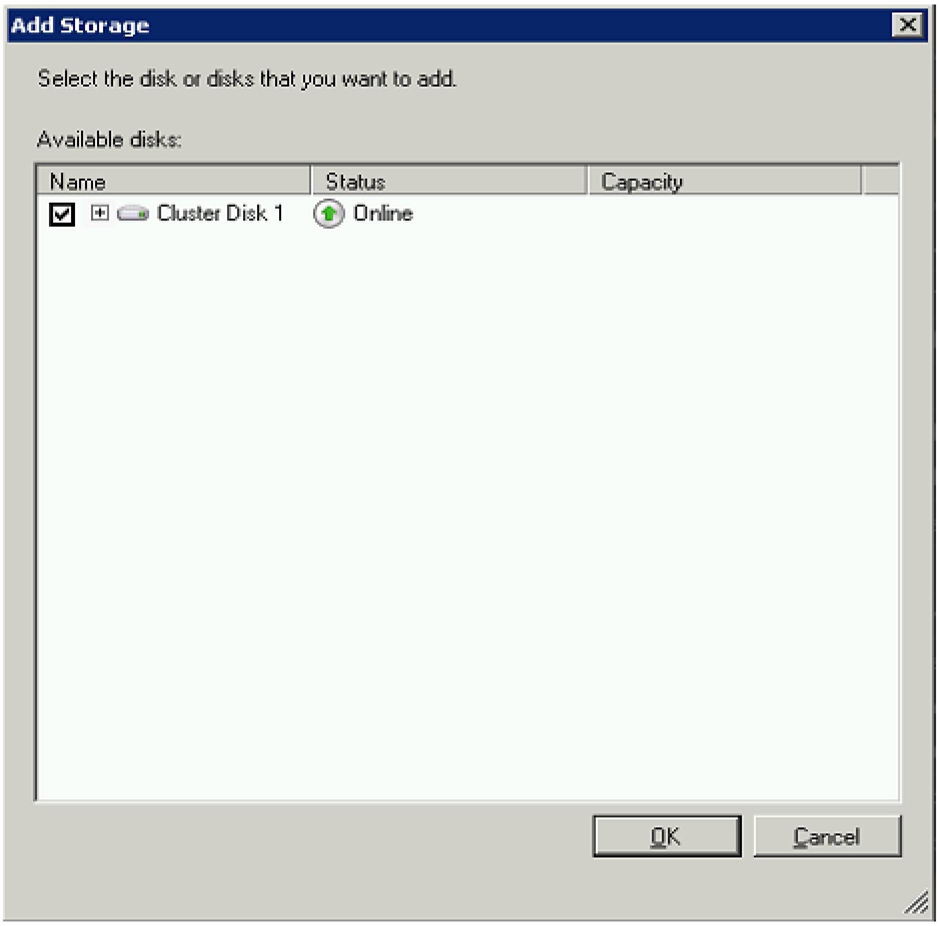
|  | Networks | Address |
|---|---|---|
| ☑ | 172.27.0.0/16 | 172.27.25.25 |

5. Enter the IP address and click **Next**.

6. In the Confirmation window, click **Next**.
7. In the summary window, click **Finish**.

## Adding a shared disk

1. Right-click on the Acronis Cyber Files role and select **Add Storage**.
2. Select the desired shared drive.



Select the disk or disks that you want to add.

Available disks:

| Name | Status | Capacity |
|---|---|---|
| ☑ ⊞ Cluster Disk 1 | Online | |

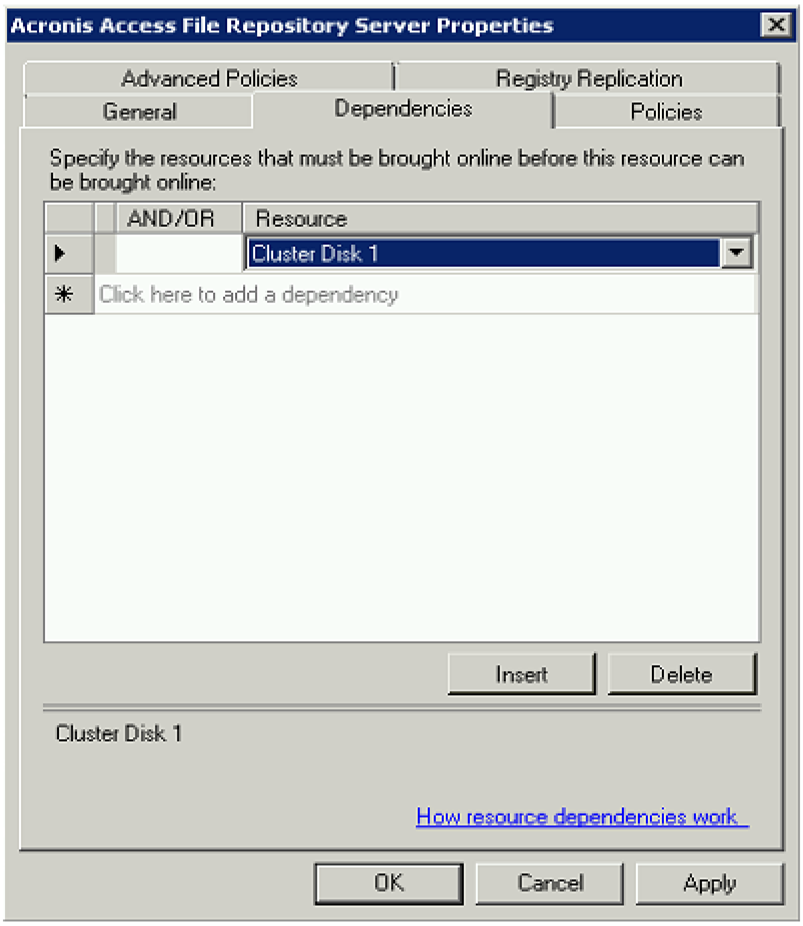
## Configuring dependencies

1. Select the Acronis Cyber Files role and click on the **Resources** tab

**For PostgreSQL and Acronis Cyber Files File Repository services do the following:**

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.

3. Click on **Resource** and select the shared disk you have added.


Acronis Access File Repository Server Properties

Specify the resources that must be brought online before this resource can be brought online:

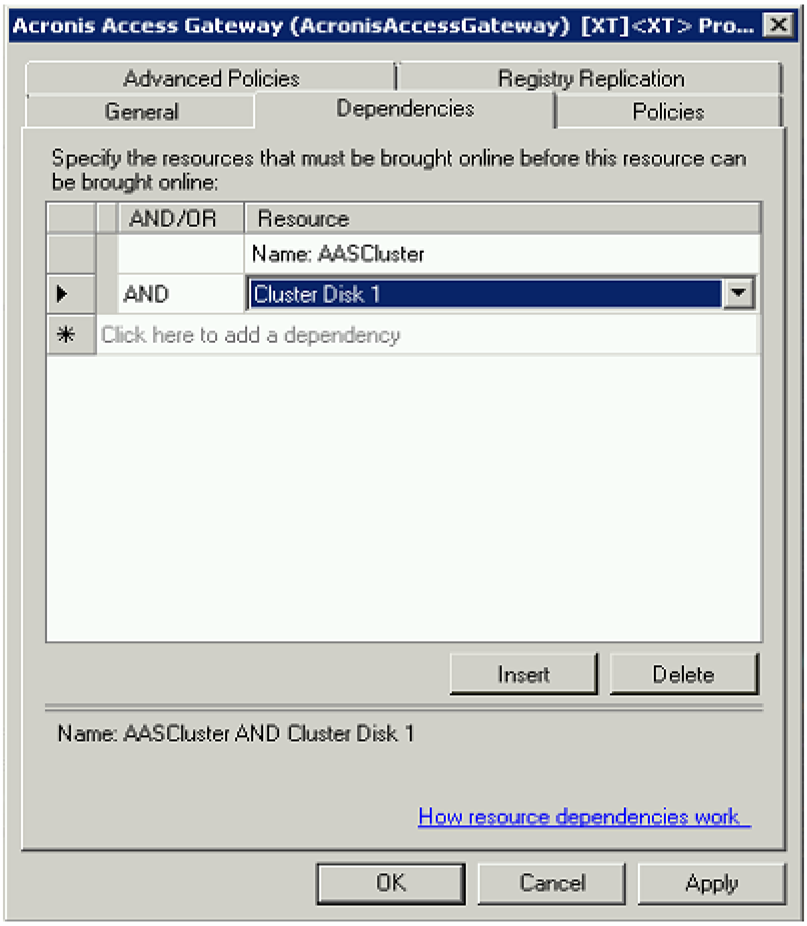
| AND/OR | Resource |
|---|---|
| | Cluster Disk 1 |
| Click here to add a dependency | |

Cluster Disk 1

4. Press **Apply** and close the window.

**For the Acronis Cyber Files Gateway Server service do the following:**

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the shared disk you have added and the **Network Name** (this is the name of the Client access point).


Acronis Access Gateway (AcronisAccessGateway) [XT]<XT> Pro...
Advanced Policies
Registry Replication
General
Dependencies
Policies

Specify the resources that must be brought online before this resource can be brought online:

| | AND/OR | Resource |
|---|---|---|
| | | Name: AASCluster |
| ▶ | AND | Cluster Disk 1 |
| ✳ | Click here to add a dependency | |

Name: AASCluster AND Cluster Disk 1

How resource dependencies work
OK
Cancel
Apply

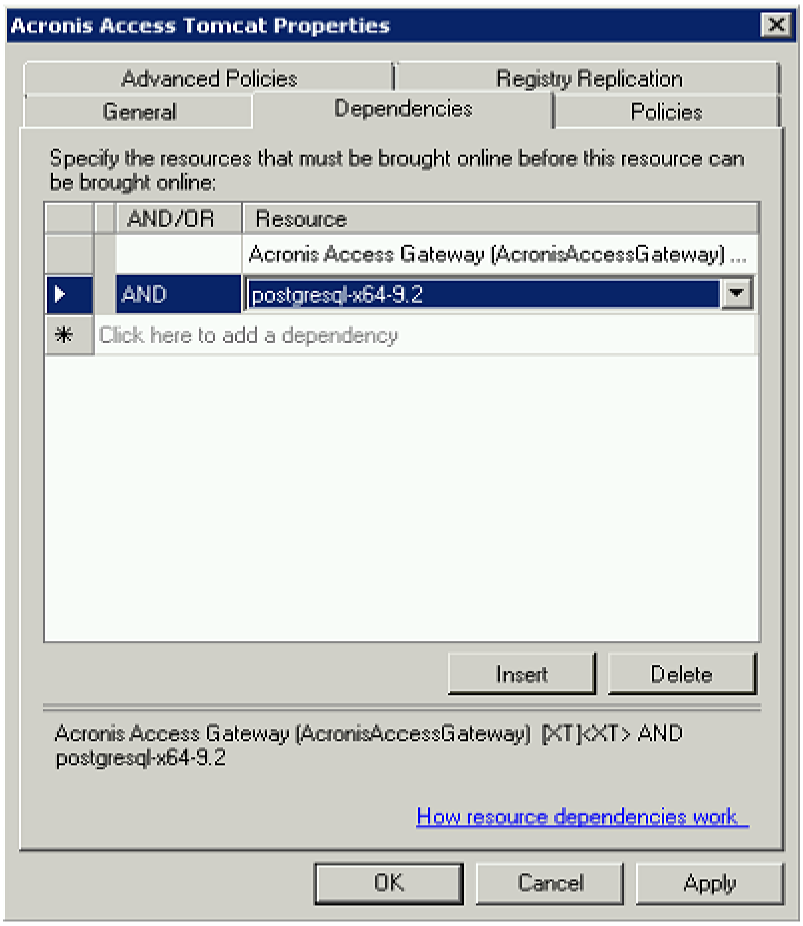
4. Press **Apply** and close the window.

**For the Acronis Cyber Files Tomcat service do the following:**

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the PostgreSQL and Acronis Cyber Files Gateway Server services as dependencies. Press **Apply** and close the window.

**Note**

If you want to run the Gateway and Acronis Cyber Files Web Servers on different IP addresses add the second IP as a resource to the Acronis Cyber Files role and set it as a dependency for the network name.



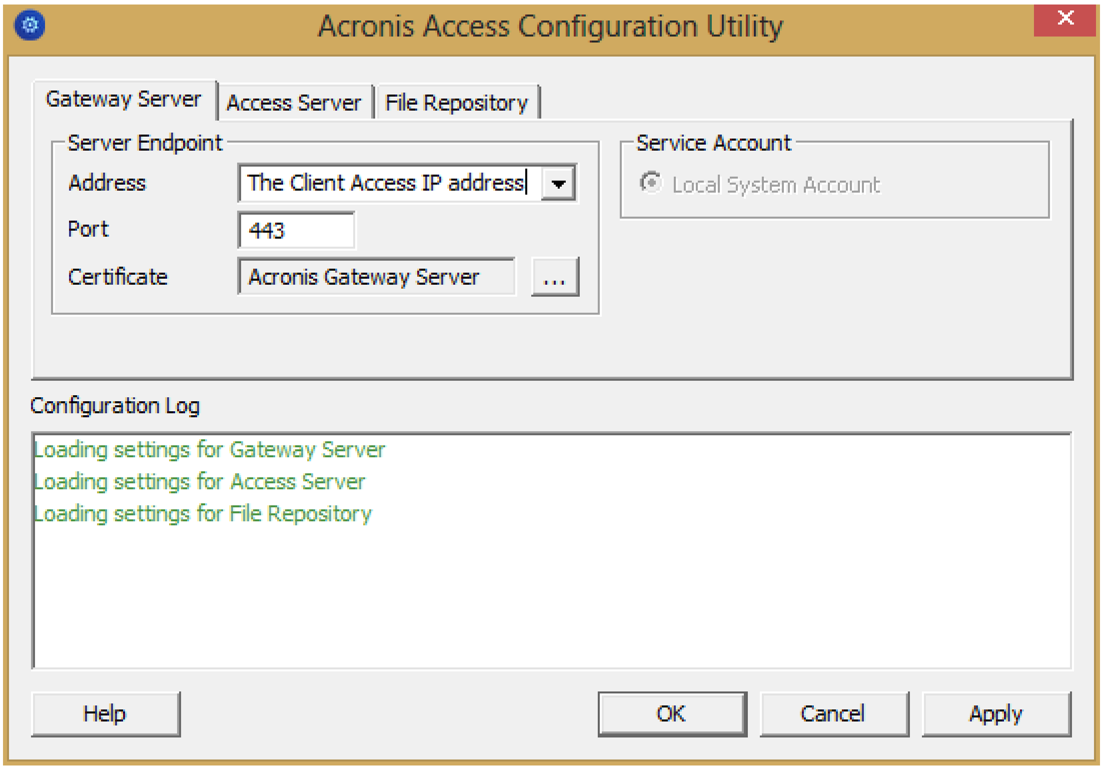
Specify the resources that must be brought online before this resource can be brought online:

| AND/OR | Resource |
|---|---|
|  | Acronis Access Gateway (AcronisAccessGateway) ... |
| AND | postgresql-x64-9.2 |
| Click here to add a dependency |  |

Acronis Access Gateway (AcronisAccessGateway) [XT]<XT> AND postgresql-x64-9.2

## Starting the role and using the Configuration Utility

1. Right-click on the AcronisCyber Files role and press **Start role**.
2. Launch the Configuration Utility. On a clean install, this is generally located at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility`
3. Configure the Acronis Cyber Files Gateway Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.



Address: The Client Access IP address

Port: 443

Certificate: Acronis Gateway Server

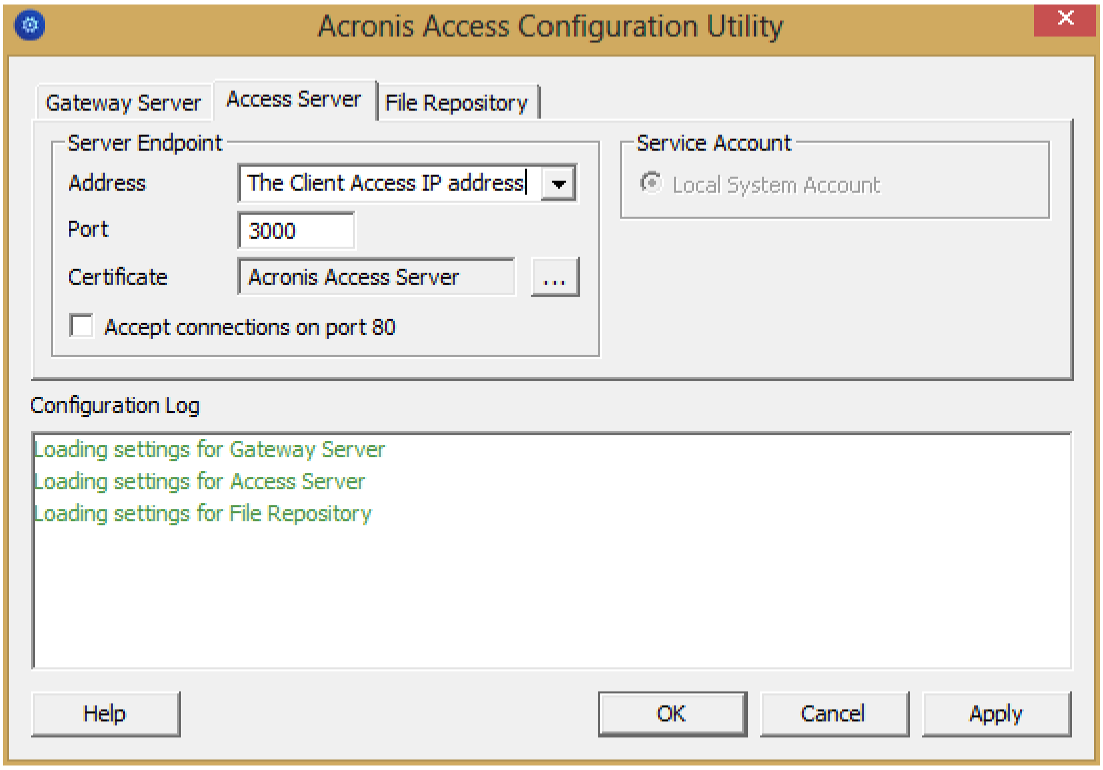
Configuration Log

```
Loading settings for Gateway Server
Loading settings for Access Server
Loading settings for File Repository
```

4. Configure the Acronis Cyber Files Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.

**Note**

If **Redirect requests from port 80** is selected,



Address: The Client Access IP address

Port: 3000

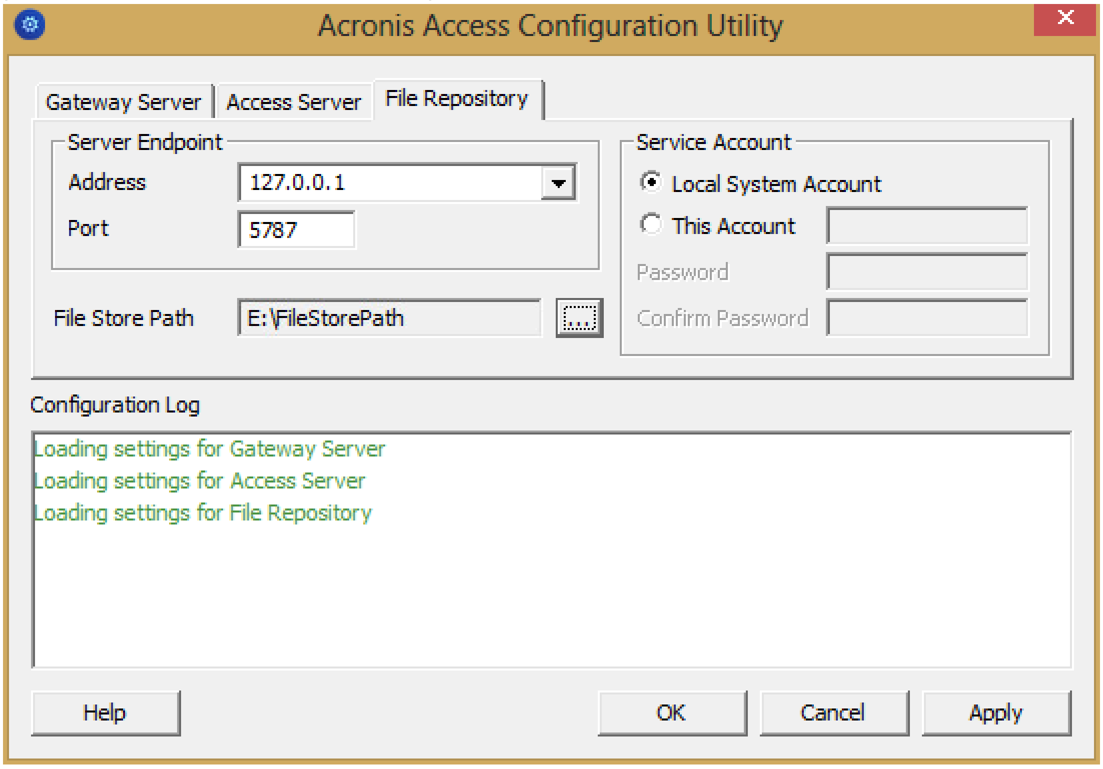
Certificate: Acronis Access Server

☐ Accept connections on port 80

Configuration Log

```
Loading settings for Gateway Server
Loading settings for Access Server
Loading settings for File Repository
```

5. Configure the Acronis Cyber Files File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



Acronis Access Configuration Utility

Gateway Server | Access Server | File Repository

Server Endpoint

Address: 127.0.0.1

Port: 5787

File Store Path: E:\FileStorePath

Service Account

● Local System Account

○ This Account

Password

Confirm Password

Configuration Log

```
Loading settings for Gateway Server
Loading settings for Access Server
Loading settings for File Repository
```

6. Click **OK** to complete the configuration and restart the services.

## Installation and configuration on the second node

1. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.

2. Install Acronis Cyber Files on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.

3. Complete the installation.

4. Configure your Gateway Server's database to be on a location on a shared disk.

   a. Navigate to `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\`

   b. Find the **database.yml** file and open it with a text editor.

   c. Find this line: `database_path: './database/'` and replace **./database/** with the path you want to use (e.g. `database_path: 'S:/access_cluster/database/'`).

   **Note**

   Use slashes(/) as a path separator.

   **Note**

   You can copy the configured database.yml from the first node and paste it to the second node.

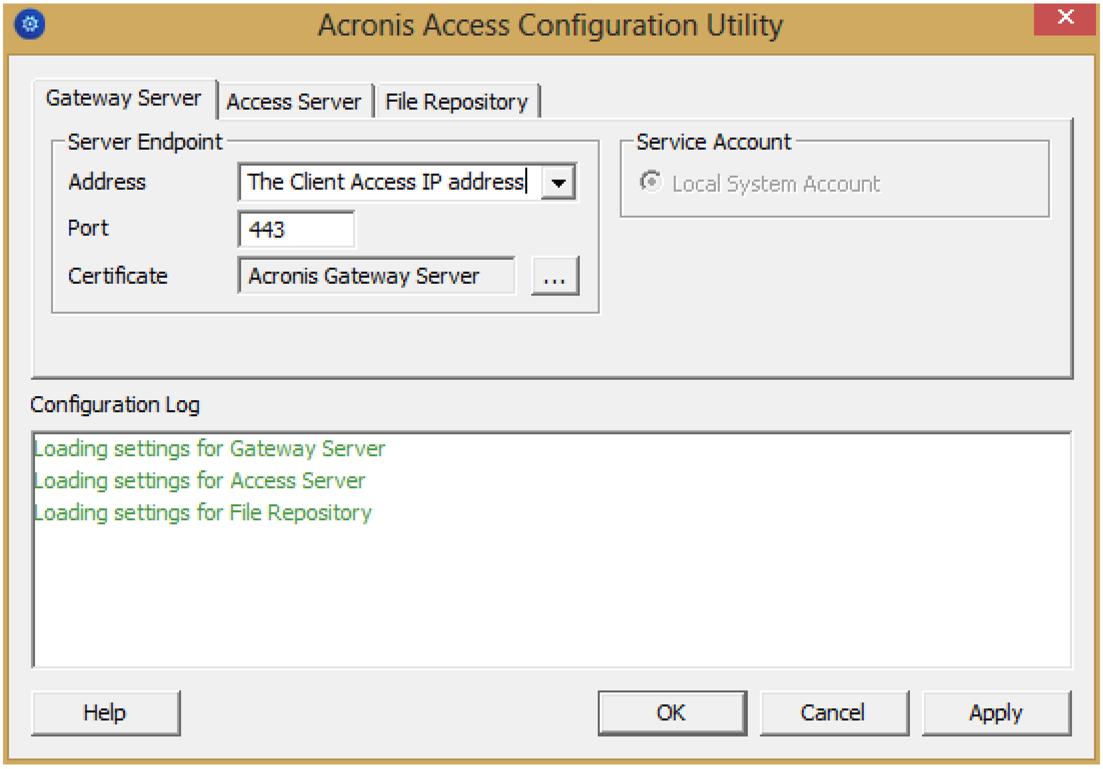
   The path should match the path set on the first node.

**For PostgreSQL do the following:**

1. Open the **Failover Cluster Manager**.
2. Find and select the PostgreSQL Generic Service resource.
3. Right-click on it and select **Properties**.
4. Click on the **Registry Replication** tab.
5. Press **Add** and enter the following: `SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\`(For older versions of Acronis Cyber Files the service may be different. e.g. **postgresql-x64-9.2**)
6. Move the Acronis Cyber Files role to the second node.

**Using the Configuration Utility on the second node**

1. Right-click on the AcronisCyber Files role and press **Start role**.
2. Launch the Configuration Utility. On a clean install, this is generally located at `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility`
3. Configure the Acronis Cyber Files Gateway Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.



Acronis Access Configuration Utility

Server Endpoint

Address: The Client Access IP address

Port: 443

Certificate: Acronis Gateway Server

Service Account

○ Local System Account

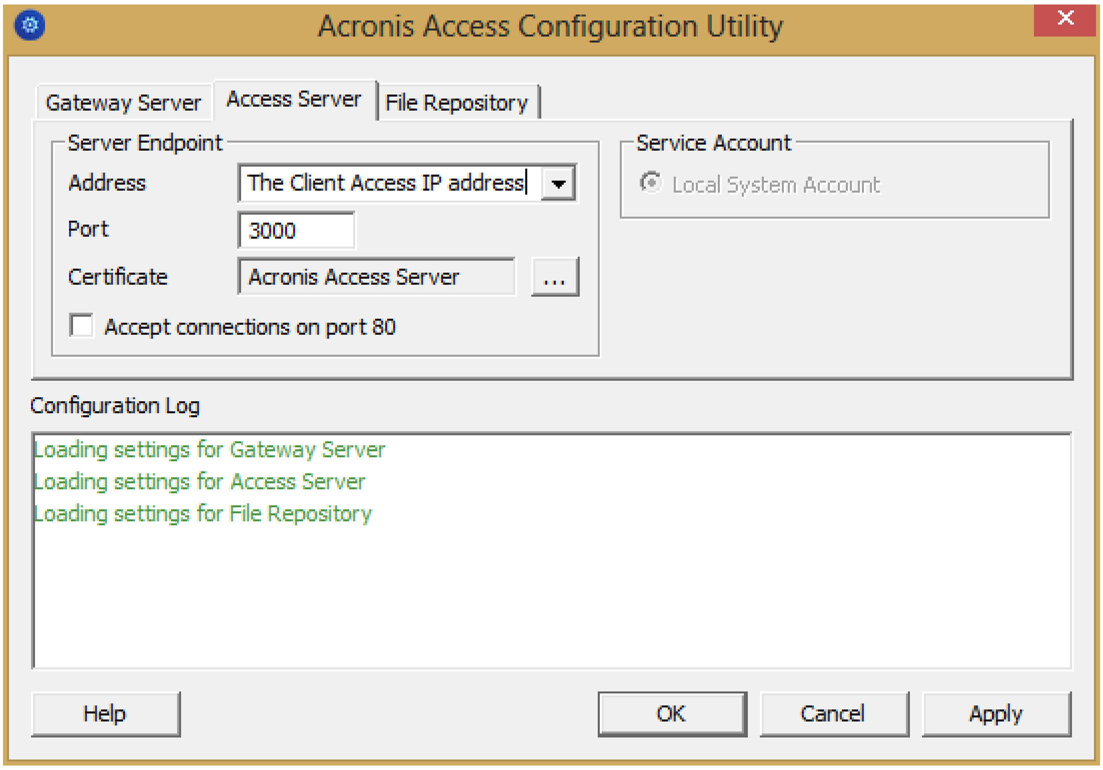
Configuration Log

```
Loading settings for Gateway Server
Loading settings for Access Server
Loading settings for File Repository
```

4. Configure the Acronis Cyber Files Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.

**Note**

If **Redirect requests from port 80** is selected,



Address: The Client Access IP address

Port: 3000

Certificate: Acronis Access Server

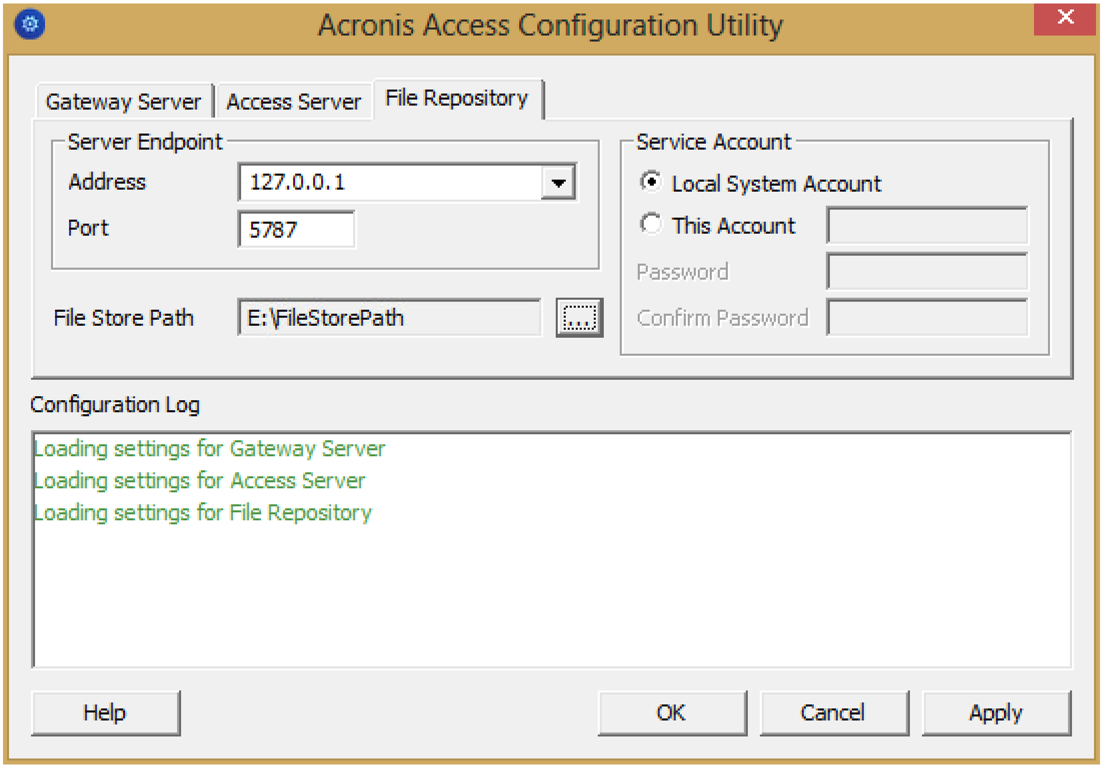
□ Accept connections on port 80

● Local System Account

Configuration Log

```
Loading settings for Gateway Server
Loading settings for Access Server
Loading settings for File Repository
```

5. Configure the Acronis Cyber Files File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



Address: 127.0.0.1

Port: 5787

File Store Path: E:\FileStorePath

● Local System Account

○ This Account

Password

Confirm Password

Configuration Log

```
Loading settings for Gateway Server
Loading settings for Access Server
Loading settings for File Repository
```

6. Click **OK** to complete the configuration and restart the services.

## IPv6 setup

***Before you begin - known limitations***

Currently, the Configuration Utility does not automatically support IPv6. After making manual changes to the `server.xml` file and the SSL Bindings, you can no longer use the Configuration Utility, since it will delete all changes that are not supported by its UI. All service restarts and edits to the server configuration will need to be done manually, until the Configuration Utility supports IPv6.

The manual changes required to the `server.xml` and `web.xml` files will not be preserved on upgrade. Please be sure to back up these files to a location outside of the Acronis Cyber Files Server installation. After an upgrade, you will need to diff your manually-edited file against the newly-installed file and port over any necessary changes.

All addressees that resolve to IPv6 must be specified as DNS addresses in the webUI.

**Note**

The Administrators page – “Administration page access restrictions” feature requires a range of IPs which are allowed to access the administration pages. The current UI format only supports IPv4.

***Performing IPv6 Setup***

There are three steps required to enable IPv6 support.

## IPv6 setup step 1: gateway setup

To make the Gateway work with IPv6, you must create an SSL binding, then add the desired address (es) to the `iplisten` list.

**Note**

To complete this step, you will need `thecerthash` value of the Acronis Access certificate thumbprint, the desired IPv6 IP address, and the port on which the Gateway will be listening. To discover how to get the certhash value, see Obtaining an Acronis Access certificate thumbprint.

### Creating an SSL binding

You can bind for for all IPv6 addresses or for a specific IPv6 address.

***Binding to all IPv6 addresses***

The command should look like this:

```
netsh http add sslcert ipport=[::]:YourPortNumber certhash=YourCerthashValue appid={72876ec6-d443-48ef-add3-fa7a0cbc4762} certstorename=MY clientcertnegotiation=enable dsmapperusage=enable
```

**Important**

You should enter the port on which you would like your Gateway to be listening, and replace the `certhash` value with the value from your certificate

**Note**

To bind to a *specific* IPv6 address, replace "`::`" with the desired address.

**Note**

If you need to delete an SSL binding, use the following command, substituting the address and port with those you would like to remove:

netsh http delete sslcert ipport=[**AddressToRemove**]:**PortToRemove**

## Adding the desired IPv6 address to the `iplisten` list

You can add either all IP addresses or a specific IP address to the `iplisten` list.

***Adding all IPv6 IP addresses to the `iplisten` list***

1. Use the following command: `netsh http add iplisten ipaddress=::`

   **Note**

   To add a *specific* IPv6 IP address to the iplisten list, replace "**::**" with the desired IPv6 IP address.

   ```
   E.g.: netsh http add iplisten ipaddress=fd59:ffdf:9580::3
   ```

2. Restart the Gateway Service from Windows Services.

**Note**

You should now be able to access the Gateway both via localhost (::1) and any IP address.

If you set up a specific IPv6 IP address, you will not be able to access the Gateway via localhost, and only on the specified address.

**Warning!**

If you would like to be able to access the Gateway via localhost, after having set up a specific IP address, you will need to remove the specific address from the `iplisten` list with the following command and restart the Gateway Service from Windows Services.

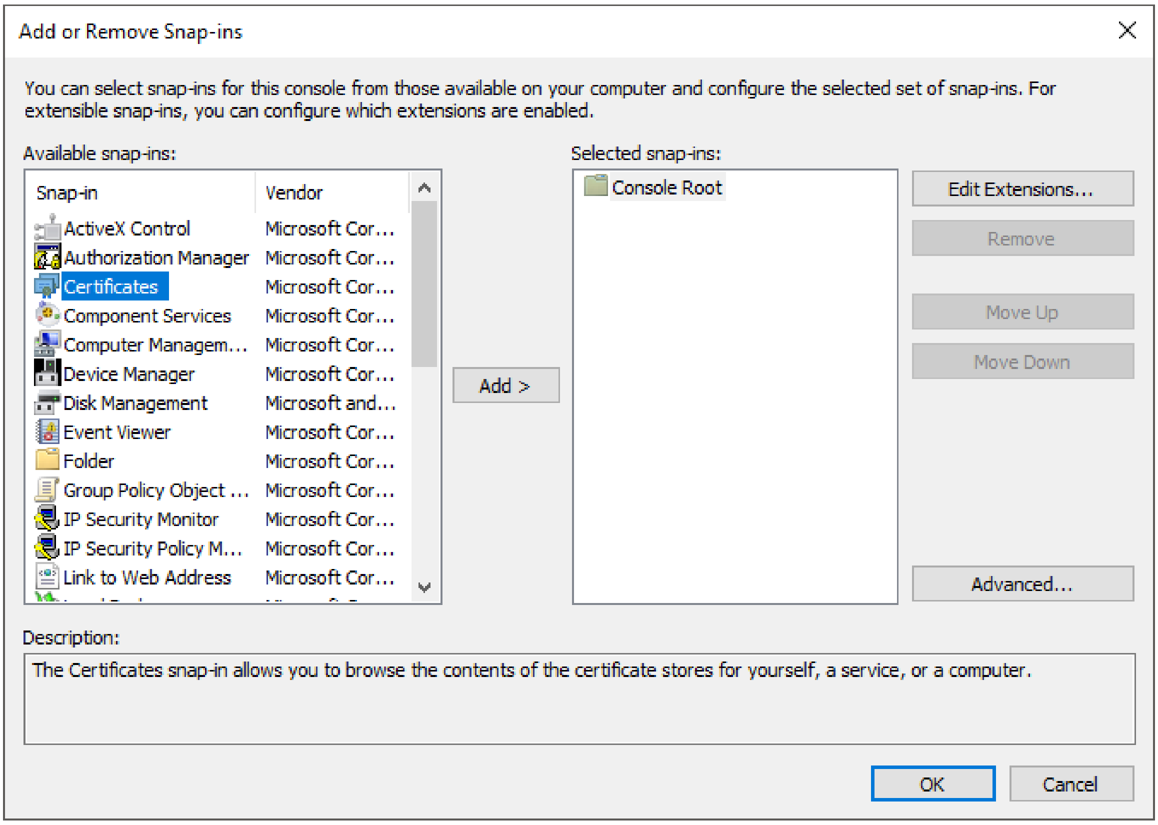
E.g.: netsh http delete iplisten ipaddress=fd59:ffdf:9580::3

## Obtaining an Acronis Access certificate thumbprint

There are two ways to obtain the Acronis Access certificate thumbprint. One is from the certificate details tab in the certificate snap-in. The other is from an already setup SSL binding, using the command prompt.

***To obtaining the certificate thumbprint from the certificate snap-in***

1. Open the **Run** dialog and type `mmc.exe` to open the **Microsoft Management Console**.
2. Click **File -> Add/Remove Snap-in...**
3. Select **Certificates**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

| Snap-in | Vendor |
|---|---|
| ActiveX Control | Microsoft Cor... |
| Authorization Manager | Microsoft Cor... |
| Certificates | Microsoft Cor... |
| Component Services | Microsoft Cor... |
| Computer Managem... | Microsoft Cor... |
| Device Manager | Microsoft Cor... |
| Disk Management | Microsoft and... |
| Event Viewer | Microsoft Cor... |
| Folder | Microsoft Cor... |
| Group Policy Object ... | Microsoft Cor... |
| IP Security Monitor | Microsoft Cor... |
| IP Security Policy M... | Microsoft Cor... |
| Link to Web Address | Microsoft Cor... |

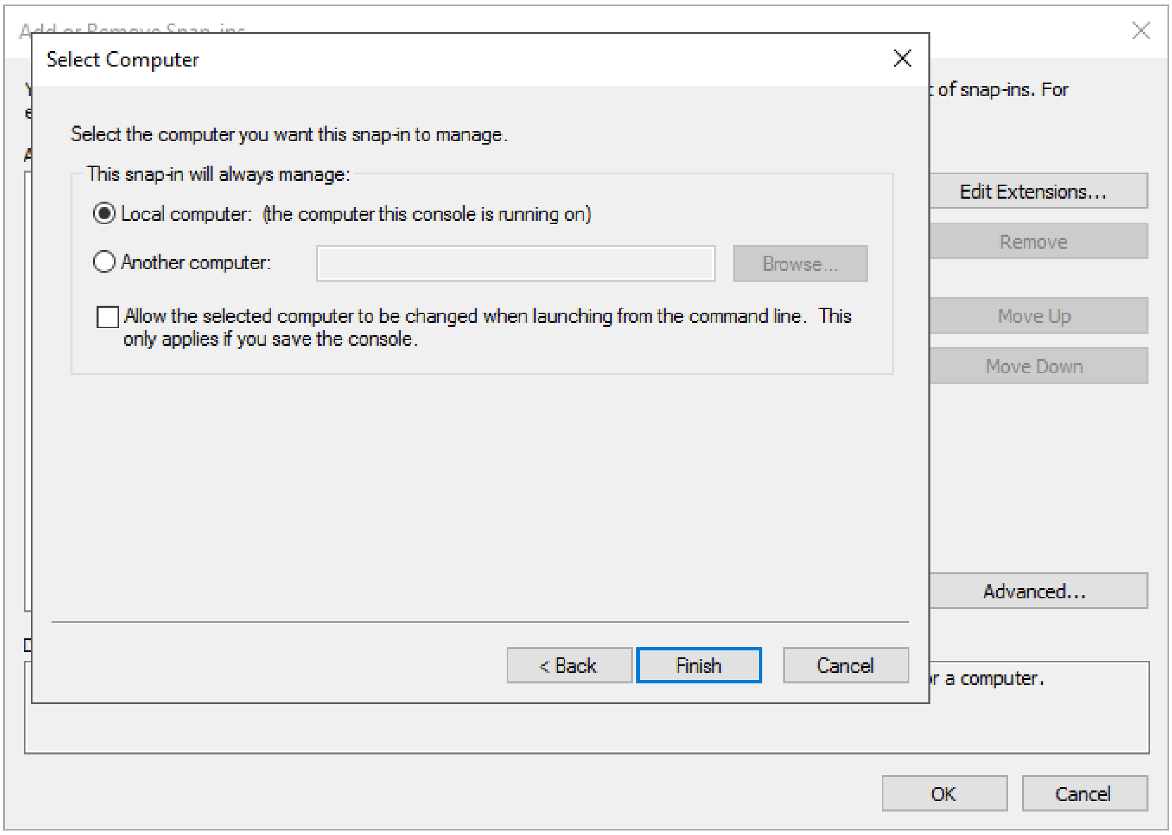
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Click **Add**, in the dialog.



Select the computer you want this snap-in to manage.

This snap-in will always manage:

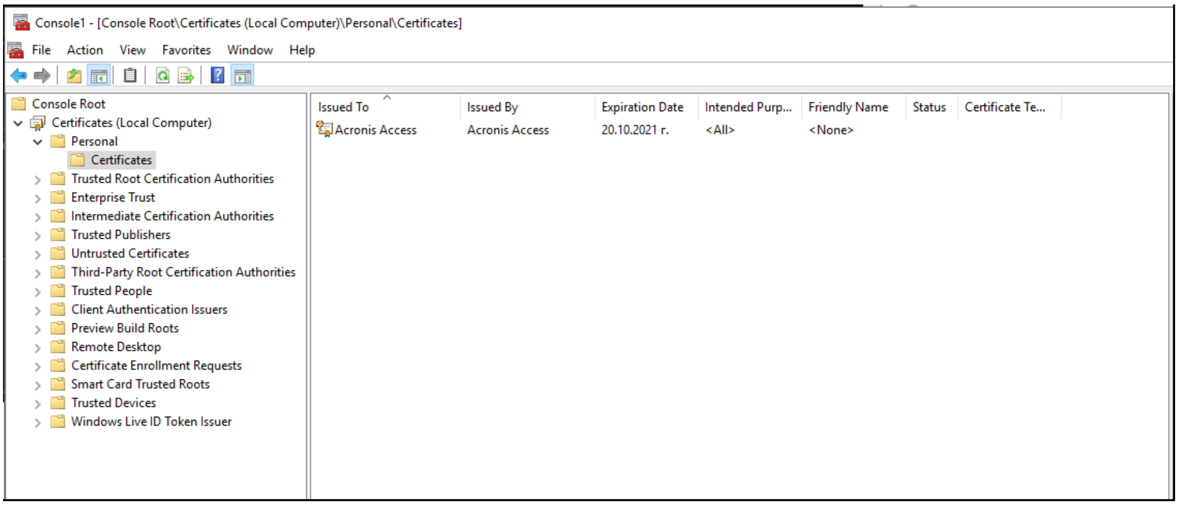
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

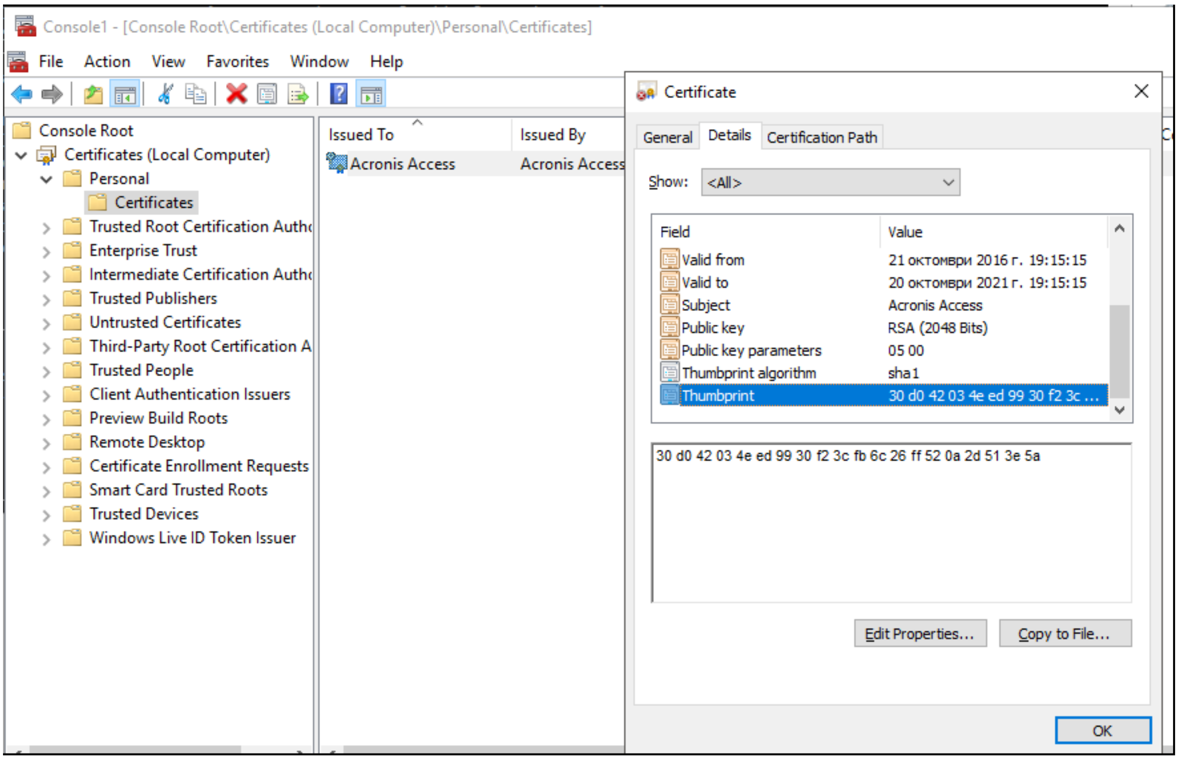
5. Select **Computer Account**, hit Next, select Local Computer and hit Finish:

6. In the Add/Remove Snap-ins... dialog click **OK**.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer

| Issued To | Issued By | Expiration Date | Intended Purp... | Friendly Name | Status | Certificate Te... |
|---|---|---|---|---|---|---|
| Acronis Access | Acronis Access | 20.10.2021 г. | <All> | <None> | | |

7. Expand the Certificates on the left-hand side, Personal -> Certificates and you should see the Acronis Access certificate.



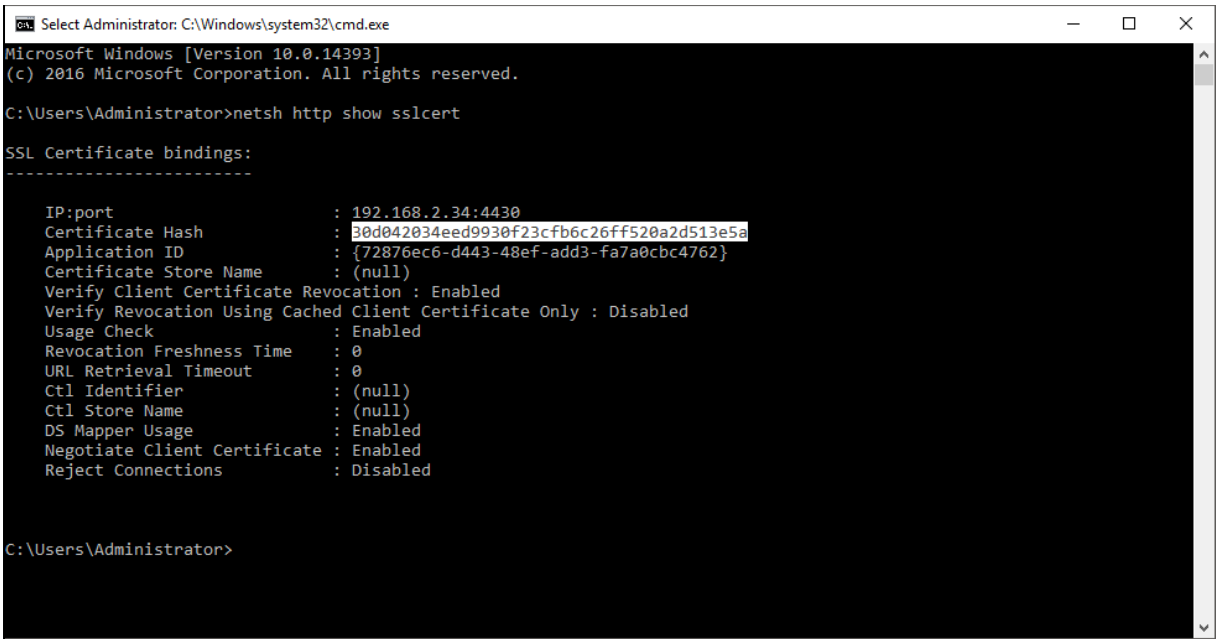
| Field | Value |
|---|---|
| Valid from | 21 октомври 2016 г. 19:15:15 |
| Valid to | 20 октомври 2021 г. 19:15:15 |
| Subject | Acronis Access |
| Public key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Thumbprint algorithm | sha1 |
| Thumbprint | 30 d0 42 03 4e ed 99 30 f2 3c ... |

```
30 d0 42 03 4e ed 99 30 f2 3c fb 6c 26 ff 52 0a 2d 51 3e 5a
```

8. Double-click the certificate, select the **Details** tab and scroll to the Thumbprint.
9. Copy it somewhere and remove the spaces. You need it without spaces for the command that creates the SSL binding.

***To obtain the certificate thumbprint using an already setup SSL binding***

1. Open a command prompt.
2. Type: `netsh http show sslcert`
3. If an SSL binding exists, it will be displayed.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netsh http show sslcert

SSL Certificate bindings:
-------------------------

    IP:port                      : 192.168.2.34:4430
    Certificate Hash             : 30d042034eed9930f23cfb6c26ff520a2d513e5a
    Application ID               : {72876ec6-d443-48ef-add3-fa7a0cbc4762}
    Certificate Store Name       : (null)
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Enabled
    Negotiate Client Certificate : Enabled
    Reject Connections           : Disabled


C:\Users\Administrator>
```

.

**Note**

The highlighted string is the certificate hash you need.

## IPv6 setup step 2: Acronis Cyber Files Server

***Enabling the server to listen locally on all IPv6 addresses.***

**Important**

To bind to a specific IPv6 address, see the note on step 4.

1. Locate the **`server.xml`** file.

   **Note**

   By default this file can be found in **`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-9.0.54\conf`**

   The number in the path (7.0.70) might be different, depending on your version of Tomcat and your path may be different if you upgraded or performed a custom install, you can use the **Acronis Cyber Files Tomcat** entry in **Windows Services** to identify the path to the Tomcat program folder, which will contain the **`conf`** folder.

2. Make a backup copy of **`server.xml`**.
3. Open the original **`server.xml`** in a text editor.
4. Add an additional connector with the address="::" to support all IPv6 addresses.
   i. In **`server.xml`**, find the part of the file that looks like this

      ```
      <Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
      disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
      SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
      ```

```
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!
LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" relaxedQueryChars="[,]" address="0.0.0.0" port="443"/>
```

ii. Then, on a new line, next to the existing connector, add this additional connector, with address="::"

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!
LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" relaxedQueryChars="[,]" address="::" port="443"/>
```

**Note**

Instead of adding all IPv6 addresses (**::**), you can set a specific IPv6 address by replacing ”`::`” with the desired address in the connector block.

E.g.:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!
LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" relaxedQueryChars="[,]" address="fd59:ffdf:9580::3" port="443"/>
```

5. Save the changes and restart the Acronis Cyber Files Tomcat Service from the Windows Services panel.

**Important**

All changes to **`server.xml`** require the Acronis Cyber Files Tomcat Service to be restarted.

**Warning!**

These manual changes WILL NOT be preserved on upgrade. Please be sure to back up these files to a location outside of the Acronis Cyber Files Server installation. After an upgrade you will need to manually merge the differences between the edited and the newly installed file and transfer any necessary changes to the new **`server.xml`** file.

## IPv6 setup step 3: Strict Transport Security (HSTS)

1. Locate the **`web.xml`** file.

   > **Note**
   > By default, **`web.xml`** is located here: **`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF`**

2. Make a backup copy of the existing **`web.xml`** file.
3. Open the original **`web.xml`** in a text editor and add the following block.

```
<filter>
      <filter-name>httpHeaderSecurity</filter-name>
      <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
     <init-param>
          <param-name>hstsMaxAgeSeconds</param-name>
          <param-value>31536000</param-value>
     </init-param>
     <init-param>
          <param-name>hstsIncludeSubDomains</param-name>
          <param-value>true</param-value>
     </init-param>
</filter>
<filter-mapping>
     <filter-name>httpHeaderSecurity</filter-name>
     <url-pattern>/*</url-pattern>
     <dispatcher>REQUEST</dispatcher>
     <dispatcher>FORWARD</dispatcher>
</filter-mapping>
```

4. Save the changes.
5. Restart the Acronis Cyber Files Tomcat Service from the Windows Services panel.

**Note**
By using the Development tools in a browser, you should be able to see the Strict-Transport-Security header for all requests.

**Warning!**
These manually changes WILL NOT be preserved on upgrade. Please be sure to back up this file to a location outside of the Acronis Cyber Files Server installation. After an upgrade you will need to diff your manually edited file against the newly installed file and port over any necessary changes to the new **`web.xml`** file.

# Mobile Device Management

Mobile Device Management (MDM) manages the usage and security of an organization's mobile devices, and of the apps installed on those devices.

Acronis has tested the Cyber Files apps with the following MDM platforms:

- **Ivanti Neurons for MDM** (formerly MobileIron Cloud) for:
  - Cyber Files app for iOS.
  - Cyber Files app for Android (without AppConnect management).
  - the Ivanti AppConnect-enabled version of Cyber Files app for Android.

  **Note**
  Click here to access the Ivanti Neurons for MDM documentation.

- **Ivanti Endpoint Manager Mobile** (formerly MobileIron Core) for:
  - Cyber Files app for iOS.
  - Cyber Files app for Android (without AppConnect management).
  - the Ivanti AppConnect-enabled version of Cyber Files app for Android.

  **Note**
  Click here to access the Ivanti Endpoint Manager Mobile (EPMM) documentation.

- **Microsoft InTune** for:
  - Cyber Files app for iOS.

## Managed App Configuration (AppConfig)

Acronis Cyber Files apps support Managed App Configuration (AppConfig).

If the prerequisites listed are met, you can add certain keys to your Mobile Device Management (MDM) configuration, and they will take effect on Cyber Files apps

***Prerequisites***

- The devices must be managed by an MDM server.
- The app binary must have be installed on the device by the MDM server.
- The MDM server must support the **ApplicationConfiguration** setting and **ManagedApplicationFeedback** commands.

***Supported keys***

| Key Name | Required? | Values | Description | Comments |
|---|---|---|---|---|
| **enrollmentServer** | Obligatory | DN address | Should be set to the DNS address of the Cyber Files server that | |

| | | | | |
|---|---|---|---|---|
| | | | the user enrolls with. | |
| **enrollmentPIN** | Optional | PIN number | If your Cyber Files server requires a PIN number for client enrollment, you can auto-complete the **PIN number** field in the enrollment form with this value. Most often, the PIN requirement on the Cyber Files server is disabled, since AppConnect can serve as the 2nd factor of authentication before a user has access, rather than the one-time-use PIN number.<br>The PIN requirement is configured on the **Settings** page of the Cyber Files web console. | |
| **userName** | Optional | Variable | To be provided into the **Username** field of the Cyber Files enrollment form.<br>You can use a variable to auto-complete this value with the specific user’s username.<br>You can use Ivanti's `$USERID$` wildcard, which will auto-complete the field with the username that the user entered when setting up their Ivanti app. | |
| **enrollmentUserNameLock** | Optional | Yes, No | When set to **Yes**, this prevents the **Username** field in the Cyber Files enrollment form from modification. | Fields are not locked if:<br>• the lock key is set to **No**. |

| | | | | |
|---|---|---|---|---|
| | | | | • the lock key is not configured at all.<br>• the field value to lock is empty. |
| **enrollmentServerNameLock** | Optional | Yes, No | When set to **Yes**, prevents the **Server address** field of the Cyber Files enrollment form from modification. | |

### *plist files*

**plist** files are XML files for storing application data. You can use a simple text editor to create and edit them.

### *Creating a plist file*

1. Open the text editor of your choice.
2. Enter the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
 <dict>
 Enter your desired keys here
 </dict>
</plist>
```

   **Example:**

```
<dict>
 <key>enrollmentServer</key>
 <string>server.example.com</string>
 <key>userName</key>
 <string>username</string>
 <key>enrollmentPIN</key>
 <string>11Y9KL</string>
</dict>
```

3. Save the file as **plist.xml**.

# Ivanti (formerly MobileIron)

## Cyber Files app for Android with Ivanti

### Ivanti AppConnect-enabled Cyber Files app for Android

To manage instances of Acronis Cyber Files app for Android using Ivanti AppConnect, you must use the Ivanti AppConnect-enabled version.

This versiobn of Cyber Files app for Android should be treated as an 'in-house' app within the Ivanti platforms.

**Note**
If you need help adding or managing 'in-house' apps, visit the Ivanti Apps documentation page.

**Important**
This version is not distributed through Google Play store.
The `.apk` file for the Ivanti AppConnect-enabled Cyber Files app for Android is available from the Cyber Files download page

### Cyber Files app for Android auto-enrollment

***Available Ivanti auto-enrollment parameters:***

- **`Server name`**
  The URL of the server.
- **`Username`**
  The user ID.
- **`Client Certificate`**
- **`Password`**
  The user's password.
- **`PIN`**
  The user's PIN.
- **`Enable auto submit`**
  With this parameter set to `Yes`, users aren't required to confirm config parameters.

### Android Enterprise

Android Enterprise allows secure and automatic enrollment of Acronis Cyber Files app for Android app users.

Android Enterprise requires Endpoint Manager Mobile (EPMM) software.

**Important**
Currently, Cyber Files only supports user auto-enrollment using Ivanti EPMM.
Therefore, you must install the AppConnect-enabled version of the Android app to use Android Enterprise.
To find out more about Ivanti EPMM, consult the Ivanti documentation.

## Cyber Files app for iOS with Ivanti

### Cyber Files app for iOS container policies

The following parameters are available:

- **Allow Print** - Select this option to allow users to print documents from Acronis Cyber Files app for iOS.
- **Allow Copy/Paste To** - Select this option to allow users to copy and paste text from documents viewed in Cyber Files app for iOS into other apps on the device that are not managed by AppConnect.

  **Warning!**
  If this is enabled, it supersedes the Cyber Files `Copying Text From Opened Files setting`.

- **Allow Open In** - Select this option to allow Cyber Files app for iOS users to open files into other apps on the device.

### Activating Cyber Files app for iOS with Ivanti

This is only required if you have not added Acronis Cyber Files app for iOS to the list of apps in your Avanti VSP console, and users are not already using the app.

If the app has been added through Ivanti, users will be able to download it from the Ivanti store, or it may be automatically installed on their devices, depending on your settings.

### App installed, not enrolled with a Cyber Files server

If Acronis Cyber Files app for iOS is installed and opened on a device before Mobile@Work and AppConnect VSP configurations are set up, starting the app may not automatically trigger the AppConnect setup process.

***To manually start the Ivanti AppConnect setup process for Cyber Files app for iOS:***

1. Open the app.
2. Open the **Settings** menu.
3. Tap the **Ivanti AppConnect** option, found towards the bottom of the list.
4. Tap the **Enable** button.

**Note**

A warning is displayed rather than an **Enable** button if the necessary Ivanti apps are not installed on the device.

The AppConnect setup process can take a few minutes to start. When it does, it will proceed as described in the previous scenario.

### App installed, enrolled with a Cyber Files server

This scenario is similar to the previous scenario, the only difference being that the AppConnect Acronis Cyber Files configuration will not be used to auto-enroll the app. If the app is already enrolled with a Cyber Files Server, it will maintain the original configuration.

***To manage Cyber Files app for iOS with AppConnect:***

**Note**

This will also enable the use of the AppConnect passcode and permissions Container Policies.

1. Open Cyber Files app for iOS.
2. Select **Settings** -> **Partner Features** -> **MobileIron**.
3. Tap **Enable AppConnect**..
4. Wait until the process completes.
5. Restart the app.

**Note**

If you require a user to enroll with a different Cyber Files server, they will need uninstall and reinstall Cyber Files app for iOS before they can be configured by AppConnect.

### App not installed

In this scenario, you need to install Acronis Cyber Files app for iOS from the Apple App Store or the Ivanti store.

When installed, the user must start the app. If a configured Ivanti app is present on the device, control is temporarily switched to it (this is known as check-in), and then switches back to Cyber Files app for iOS.

If a valid Cyber Files AppConnect configuration is found, Cyber Files app for iOS automatically enters enrollment mode and presents the user with the enrollment form.

Any fields included in the AppConnect configuration are automatically filled out. The user will typically only enter their AD password into the form and submit it. When this is complete, the relevant Cyber Files Client Management policy is applied to the app, and the app is ready for use.

**Warning!**
If a valid configuration for Cyber Files app for iOS does not exist on the VSP or, if the Ivanti app has not been configured, the user will receive an error message.
If the Ivanti app has not been installed on the device, Cyber Files app for iOS will start up in standard mode, without AppConnect enabled.

### Ivanti check-in

When Acronis Cyber Files apps are managed by Ivanti AppConnect, any changes you make to applicable policies will be received by installed apps when they next check in with the Ivanti app.

The check-in causes Cyber Files apps to briefly switch over to the Ivanti app.

As a result, users may experience a momentary pause if they are active at that time.

On the other hand, revocation of access to Cyber Files apps, etc., is also applied at check in, so the check-in frequency for your organization should be chosen carefully.

**Note**
Check-in frequency is set in the Ivanti product.

## Microsoft Intune

Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. To enroll mobile devices you must set Intune as your mobile device authority and then configure the infrastructure to support the platforms you want to managed. This requires establishing a trust relationship with the device.

**Note**
This feature is only supported by the Acronis Cyber Files iOS client, version 7.0.5 or newer.

**Note**
To apply a **Device Policy**, Acronis Cyber Files must be installed through the **Microsoft Intune Company Portal** and **Allow Intune managed iOS client and 'iOS Managed App' iOS client** must be enabled in the **Acronis Cyber Files  Default Access Restrictions** (**Mobile Access** > **Policies** > **Default Access Restrictions**) or for each Gateway's Access Restrictions.

**Note**
To apply an **Application Policy** and for Acronis Cyber Files to be managed by Intune, **Trigger Intune Mobile Application Management enrollment must be enabled** via the Acronis Cyber Files server, in **Mobile Access** > **Policies** >  **Server Policy**.

## Active Directory Group

***To create an Active Directory Group:***

1. Open the Microsoft Azure portal.
2. Select **All Services.**
3. **E**nter **azure** in the searchbox, and select **Azure Active Directory**.
4. Open **Groups**.
5. Select **New group** and enter the required information.
6. Select the desired members of the group.
7. Select **Create**.

## Cyber Files app for iOS added to Intune

If you want to use an Intune **Device Policy**, Cyber Files app for iOS should be installed through your Intune company portal.

To add Cyber Files app for iOS to InTune:

1. Open the Microsoft Azure portal.
2. Click on **All Services.**
3. Enter **Intune** in the searchbox and select **Microsoft Intune**.
4. In the Intune portal, open **Mobile Apps.**
5. Open **Apps**.
6. Select **Add** and select the **Add App** options:
   - Select **iOS** for **App type**.
   - Click on **Search the App Store** and search for **Acronis Cyber Files** . Select the app.
   - Click on **App information** and make any configuration changes you wish.
7. Enable **Display this as a featured app in the Company Portal**.
8. Select **OK** .
9. Click on the app in the list and select **Assignments**.
10. Select the users or groups you want to assign it to.

## Device policy

***To add a device policy for Cyber Files app for iOS:***

1. Open the Microsoft Azure portal.
2. Click on **All Services**.
3. Enter **Intune** in the searchbox and select Microsoft Intune.
4. Open **Device Configuration** -> **Profiles.**
5. Select **Create Profile**.
6. Enter the name, choose **iOS** as the **Platform** and select the restrictions you want to apply to the device.

7. For Cyber Files app for iOS, we support only the following restrictions:
   - **App Store, Doc Viewing, Gaming -> Viewing corporate documents in unmanaged apps**. If you want to block unmanaged apps from showing in the **Open In**/**Save to** lists for managed apps, select **Block** for this option.
   - **App Store, Doc Viewing, Gaming -> Viewing non-corporate documents in corporate apps**.
     If you want to block managed apps from showing in the **Open In**/**Save to** lists for unmanaged apps, select **Block** for this option.
8. When the app is added to the list, tap on it and select **Assignments**.
9. Select the users/groups you want to assign to.

**Note**

In order to apply a **Device Policy** to any app, the app needs to be downloaded from your Intune Company Portal.

## App protection policy

**Note**

This policy also acts as your Mobile App Management policy.

1. Open the Microsoft Azure portal.
2. Click on **All Services.**
3. Enter **Intune** in the searchbox and select **Microsoft Intune**.
4. Open **Mobile apps .**
5. Open **App protection policies**.
6. Select **Add a policy.**
7. Enter a name for the policy.
8. Select **Acronis Cyber Files** as a required app.
9. Tap on **Settings** and choose the protection policies you want to apply.
10. When the app is added to the list, tap on it.
11. Select **Assignments.**
12. Select the users / groups you want to assign to.

**Note**

When **Send Org data to other apps/Receive data from other apps** is set to **Policy managed apps**, in order for the **Acronis Cyber Files Document Provider Extension** to work in other Microsoft Intune Managed apps you need to apply separate **App configuration policies** with the **IntuneMAMUPN** key – both to the Microsoft managed app and the Acronis Cyber Files app.

**Note**

When a device is considered MDM managed with the IntuneMAMUPN key, the **Send Org data to other apps** and **Receive data from other apps** options in the **App protection policy** stop being relevant and the MDM settings **Viewing corporate documents in unmanaged apps** and **Viewing non-corporate documents in corporate apps** in the **Device configuration profile** are used.

To ensure that corporate documents are opened between Intune managed apps only, you must navigate to the specific profile's **Properties > Settings > App Store, Doc Viewing, Gaming** and set both **Viewing corporate documents in unmanaged apps** and **Viewing non-corporate documents in corporate apps** to **Block**.

**Note**

For the Document Provider Extension to work with policy managed apps, the **Send Org data to other apps** option must be set to either **Policy managed apps with OS sharing** or **All apps**.

**Note**

To open files in Word (or other Microsoft apps) from Acronis Cyber Files, you need to have a separate Intune **App Protection policy** for the desired Microsoft application and **Target to all types** must be set to **YES**.

## App configuration policies

To automatically enroll with Intune credentials, you must create an **App Configuration Policy**, or add to your own policy.

***To add to your configuration policy:***

1. Open the Microsoft Azure portal.
2. Click on **All Services** .
3. Enter **Intune** in the searchbox and select **Microsoft Intune**.
4. Open **Mobile apps**.
5. Open **App configuration policies**.
6. Select **Add** and enter a name for the policy.
7. Choose **Managed devices** as **Device enrollment type**.
8. Choose **iOS** as **Platform.**
9. Select the required app to which you want to deploy this configuration.
10. For **Configuration** settings, you have two options: **XML** or **Configuration designer**.
    - For **XML**, enter the following:

```
<dict>
<key>IntuneMAMUPN</key>
<string>{{userprincipalname}}</string>
</dict>
```

   - For **Configuration designer** enter the following:
      - **IntuneMAMUPN** for the **Configuration Key**.
      - **{{userprincipalname}}** for the **Configuration Value**.
      - Select **String** for the **Value Type**.

11. For auto-enrollment with Cyber Files credentials, use the following keys in **XML**:

    ```
    <dict>
    <key>enrollmentServerName</key>
    <string>192.168.1.10</string>
    <key>enrollmentUserName</key>
    <string>jprice</string>
    <key>enrollmentAutoSubmit</key>
    <string>Yes</string>
    </dict>
    ```

12. When the app is added to the list, select it.
13. Select **Assignments .**
14. Select the users / groups you want to assign to.

# What's New

For more information about what's included in the current and previous releases, refer to the Acronis Cyber Files release history documentation.

# Known Issues

- Some people may experience problems syncing files with the desktop client.
  The workaround is to completely uninstall and then re-install the desktop client app and re-establish connection to the server.
- The PostgreSQL data directory cannot be modified.
  The default path presented by the installer, which will be inside the PostgreSQL software installation directory, must be used for the installer to succeed.

# Documentation for older versions

For older versions of Acronis Cyber Files documentation, please check the links below:

**Note**
Your preferred language might be unavailable for older documentation.

- 8.9.x
- 8.8.x
- 8.7.x
- 8.6.x
- 8.9.x
- 8.8.x
- 8.5.x
- 8.1.x
- 8.0.x
- 7.5.x
- 7.4.x
- 7.3.x
- 7.2.x
- 7.1.x
- 7.0.x
- 6.0.x
- 5.0.x

# Copyright statement

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at https://kb.acronis.com/content/7696

# Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.