Acronis

Acronis Cyber Files 8.7

ADMINISTRATOR GUIDE

Revision: 2/16/2022

Table of contents

1 Introduction **9**

1.1 About Acronis Cyber Files 9

1.2 About Acronis Cyber Files for Mobile 9

1.3 About Sync & Share 9

2 Quick Start **11**

2.1 Installation 11

2.1.1 Using the Installer 11

2.1.2 Using the Configuration Utility 12

2.2 Initial Setup 12

2.3 Mobile Access 18

2.3.1 Configuring the Default policy 18

2.3.2 Mobile Clients 18

2.3.3 Client Guides 19

2.4 Sync&Share 20

2.4.1 Sync&Share Data Source 20

2.4.2 LDAP Provisioning 23

2.5 Web and Desktop clients 24

2.6 Client Guides 24

3 Installing **25**

3.1 Requirements 25

3.1.1 Operating System Requirements 25

3.1.2 Mobile Client Requirements 25

3.1.3 Minimum Hardware Recommendation 26

3.1.4 Network Requirements 27

3.1.5 Desktop Client Requirements 29

3.2 Installing Acronis Cyber Files on your server 30

3.2.1 Installing Acronis Cyber Files 30

3.3 Using the Configuration Utility 32

3.3.1 Configuration Utility Overview 32

3.3.2 Proceeding to the Setup Wizard 35

3.4 Using the Setup wizard 36

3.4.1 Going through the initial configuration process 36

3.5 Clustering Acronis Cyber Files 41

3.6 Load balancing Acronis Cyber Files 41

4 Upgrading **42**

4.1 Upgrading Acronis Cyber Files to a newer version 42
4.1.1 Backup the vital components 42
4.1.2 Vacuum the database before upgrading 44
4.1.3 Upgrade 44
4.2 Upgrading from mobilEcho 4.5 or earlier 47
4.3 Upgrading from activEcho 2.7 or earlier 47
4.4 Upgrading Gateway Clusters 47
4.4.1 Upgrading a Gateway Server 48
4.5 Upgrading Load-balanced configurations 49
4.5.1 Before you begin 50
4.5.2 Backup your Loadbalanced components 51
4.5.3 Upgrading the File Repository 52
4.5.4 Upgrading the Primary Cyber Files Server 54
4.5.5 Upgrading Gateway Servers 55
4.5.6 Upgrading all remaining nodes 57
5 Mobile Access 59
5.1 Concepts 59
5.2 Policies 61
5.2.1 Adding a New Policy 62
5.2.2 Modifying Policies 63
5.2.3 Policy Settings 64
5.2.4 Creating a Blocked Path list 77
5.2.5 Allowed Apps 78
5.2.6 Default Access Restrictions 80
5.3 On-boarding Mobile Devices 82
5.3.1 Server-side Management Enrollment Process 83
5.3.2 User-side Management Enrollment Process 87
5.4 Managing Gateway Servers 91
5.5 Gateway Server Search Options 92
5.5.1 SharePoint 93
5.5.2 Registering new Gateway Servers 94
5.5.3 Server Details 95
5.5.4 Gateway Server Configurations 97
5.5.5 Custom Access Restrictions 106
5.5.6 Cluster Groups 106
5.6 Managing Data Sources 108
5.6.1 Access to SharePoint 2007, 2010, 2013, 2016 and 365 content 108

5.6.2 Access to OneDrive for Business content 109
5.6.3 Changing Permissions for Shared Files and Folders 109
5.6.4 Folders 109
5.6.5 Assigned Sources 114
5.6.6 Gateway Servers Visible on Clients 114
5.7 Settings 115
5.7.1 115
5.7.2 Enrollment Settings 115
5.7.3 Device Enrollment Requires: 116
6 Sync & Share 117
6.1 General Restrictions 117
6.1.1 To set a file type blacklist: 117
6.1.2 To set a maximum file size limit: 118
6.2 Sharing Restrictions 118
6.2.1 Single File Sharing Expiration 119
6.2.2 Folder Sharing 119
6.2.3 Whitelist 119
6.2.4 Blacklist 119
6.3 LDAP Provisioning 120
6.3.1 LDAP Group 120
6.4 Quotas 120
6.5 File Purging Policies 121
6.6 User Expiration Policies 123
6.7 File Repository 124
6.8 Acronis Cyber Files Client 125
7 Users&Devices 127
7.1 Managing Devices 127
7.1.1 Exporting the data about the devices 128
7.1.2 Performing Remote Application Password Resets 128
7.1.3 Performing Remote Wipes 129
7.2 Managing Users 130
7.2.1 Types of Sync & Share users 130
7.2.2 Adding an External (Ad-hoc) user 133
7.2.3 Adding an Internal (LDAP) user 133
7.2.4 Setting a custom quota 133
7.2.5 Reassign Deleted User Content 134
8 Client Guides 136

9 Server Administration **137**
9.1 Administering a Server 137
9.2 Administrators and Privileges 137
9.2.1 Administration page access restrictions 137
9.2.2 Provisioned LDAP Administrator Groups 138
9.2.3 139
9.2.4 Administrative Users 139
9.2.5 Administrative rights 140
9.3 Audit Log 141
9.3.1 Log 141
9.3.2 Settings 143
9.4 Server 144
9.4.1 Server Settings 144
9.4.2 Notification Settings 145
9.4.3 SMS two-factor Authentication 145
9.5 Web UI Customization 147
9.5.1 147
9.5.2 Using custom logos 147
9.5.3 Using a custom welcome message 147
9.5.4 Using color schemes 148
9.6 Web Previews & Editing 148
9.7 SMTP 149
9.8 LDAP 150
9.9 Email Templates 152
9.10 Licensing 154
9.10.1 Adding a new license 154
9.10.2 Adding a new license for a Gateway Server is not necessary 155
9.11 Debug Logging 155
9.12 Monitoring 156
9.12.1 Installing New Relic 157
9.13 Monitoring Acronis Cyber Files with New Relic 157
10 Maintenance Tasks **159**
10.1 Disaster Recovery guidelines 159
10.1.1 Introduction: 159
10.1.2 Description of the Acronis Cyber Files elements: 159
10.1.3 Resources needed to implement a fast recovery process 160
10.1.4 The process 160

10.2 Best Practices ... 161
10.2.1 1. Backup your database regularly ... 161
10.2.2 2. We recommend that very large deployments "Vacuum" and "Analyze" their database(s) monthly ... 161
10.2.3 3. For big deployments, you should consider running a load-balanced setup or clustering Gateway servers. ... 162
10.3 Backing up and Restoring Acronis Cyber Files ... 162
10.3.1 Backing up the Cyber Files database ... 163
10.3.2 Backing up the Gateway Server database ... 164
10.3.3 Additional files to Backup ... 164
10.3.4 Restoring the Cyber Files database ... 165
10.3.5 Restoring the Gateway Server database ... 166
10.3.6 Restoring additional files and customizations ... 166
10.3.7 Testing your restored Cyber Files Server ... 166
10.4 Tomcat Log Management on Windows ... 167
10.4.1 Introduction ... 167
10.4.2 A sample process ... 167
10.4.3 Steps ... 168
10.5 Automated Database Backup ... 172
10.5.1 Creating the database backup script ... 172
10.5.2 Creating the scheduled task ... 173
10.6 Automated Database Vacuum ... 173
10.6.1 Configuring PostgreSQL and creating the script ... 174
10.6.2 Configuring the Task Scheduler ... 175
10.7 Increasing the Acronis Cyber Files Tomcat Java Maximum Memory Pool ... 179
10.7.1 To increase the maximum memory pool: ... 179
10.8 Migrating Acronis Cyber Files to another server ... 179
10.8.1 Before you begin ... 179
10.8.2 Migrating the Acronis Cyber Files Web Server and Gateway databases ... 180
10.8.3 Additional files to Backup ... 181
10.8.4 Testing your new configuration ... 184
10.8.5 Cleanup of the original server ... 184
10.9 Upgrading PostgreSQL to a newer Major version ... 185
10.9.1 Before you begin ... 185
10.9.2 Using pg_dumpall ... 186
10.9.3 Using pg_upgrade ... 188
11 Supplemental Material ... 193

11.1 Conflicting Software 193
11.2 For the Acronis Cyber Files Server 193
11.2.1 Load balancing Acronis Cyber Files 193
11.2.2 Installing Acronis Cyber Files in a Load Balanced setup 199
11.2.3 Migrating to a load balanced configuration 205
11.2.4 Configure Tomcat's max memory usage 209
11.2.5 Configure the server to connect to the proper database 209
11.2.6 Configure the maximum number of threads 210
11.2.7 Configure proper logging 210
11.2.8 Customizing the Web Interface through the API 213
11.2.9 Unattended desktop client configuration 215
11.2.10 Configuring Single Sign-On 218
11.2.11 Configure an additional DNS entry for your Acronis Cyber Files Web server 239
11.2.12 Setting the SPN for the Acronis Cyber Files Web Server 239
11.2.13 Verify you can log into Acronis Cyber Files 240
11.2.14 Configure an additional DNS entry for your Gateway server 241
11.2.15 Configure the SPN for the local Gateway Server 241
11.3 Install a Gateway Server on a machine in the desired domain 244
11.4 Make the Gateway service run as a User Account 244
11.4.1 Grant the selected User the necessary rights 244
11.5 Configure the SPN for the remote Gateway Server 244
11.5.1 Using trusted server certificates with Acronis Cyber Files 250
11.5.2 Supporting different Desktop Client versions 254
11.5.3 Moving the FileStore to a non-default location 255
11.5.4 Monitoring Acronis Cyber Files with New Relic 256
11.5.5 Running Acronis Cyber Files Tomcat on multiple ports 257
11.5.6 Multi-homing Acronis Cyber Files 258
11.5.7 Deploy separate Web Preview servlets 259
11.5.8 PostgreSQL Streaming Replication 264
11.5.9 Configuring PostgreSQL for remote access 270
11.5.10 Running Acronis Cyber Files in HTTP mode 270
11.5.11 Upgrading Acronis Cyber Files on a Microsoft Failover Cluster 272
11.5.12 Installing Acronis Cyber Files on a Microsoft Failover Cluster 275
11.6 For the Mobile Clients 289
11.6.1 Using iOS Managed App Configuration features 289
11.6.2 MobileIron AppConnect support 291
12 Creating the App Policy 309

13 Creating the App Configuration **310**
14 Create a new label **312**
15 Apply label to new configurations **313**
16 Apply label to iOS device **314**
17 Testing the iOS client **315**
17.1 For network shares and SharePoint servers, do the following: 329
17.1.1 Acronis Cyber Files for BlackBerry Dynamics 329
17.1.2 Microsoft Intune 346
18 What's New **351**
18.1 Acronis Cyber Files Server 351
18.2 Previous Releases 351
18.2.1 activEcho 351
18.2.2 mobilEcho 361
19 Documentation for older versions **379**

1 Introduction

This guide provides the documentation for Acronis Cyber Files and all of its features. For the client documentation, please visit the Client Guides section.

1.1 About Acronis Cyber Files

Acronis 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. Acronis Cyber Files lets employees use any device - desktop, laptop, tablet or smartphone – to securely access and share content with authorized internal and external constituents, including employees, customers, partners, and vendors.

Acronis Cyber Files's functionality can roughly be split up into two main categories: Mobile Access and Sync & Share.

1.2 About Acronis Cyber Files for Mobile

Acronis Cyber Files's Mobile Access functionality enables enterprise IT to provide simple, secure and managed access to enterprise file servers, SharePoint and NAS devices for mobile device users, eliminating any IT headaches caused by employee use of risky, consumer-based services and other non-compliant alternatives. Acronis Cyber Files allows IT to secure and control access to the content while ensuring that its mobile users have access to content, files and materials necessary to perform their jobs.

1.3 About Sync & Share

Acronis Cyber Files's Sync & Share functionality is the industry's only Enterprise File Sharing and Syncing solution that balances the end user's need for simplicity and effectiveness with the security, manageability and flexibility required by Enterprise IT.

Acronis 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 their organization. And, Acronis Cyber Files provides a level of visibility and monitoring not available from consumer-based solutions.

Quick Links				
Acronis Cyber Files **Installing the Acronis Cyber Files Server** **Upgrading an existing activEcho or mobilEcho server**		**Acronis Cyber Files for Mobile** **Acronis Cyber Files for MobileQuickStart Guide** **Mobile Client Guides** **Managing mobile clients and policies, configuring access to data sources**		**Sync & Share** **Sync & Share QuickStart Guide** **Desktop**

Basic Server administration				**Client Guide** **Managing Sync & Share policies**

2 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.

2.1 Installation

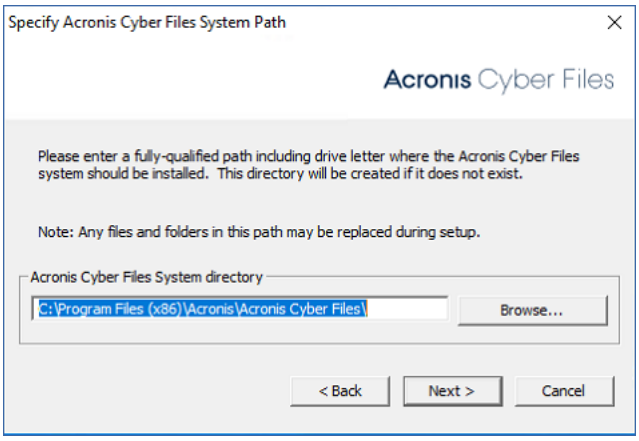
Note
Please make sure you are logged in as an administrator before installing Acronis Cyber Files.

Note
Acronis Cyber Files 8.6 is distributed along with PostgreSQL 11 by default.

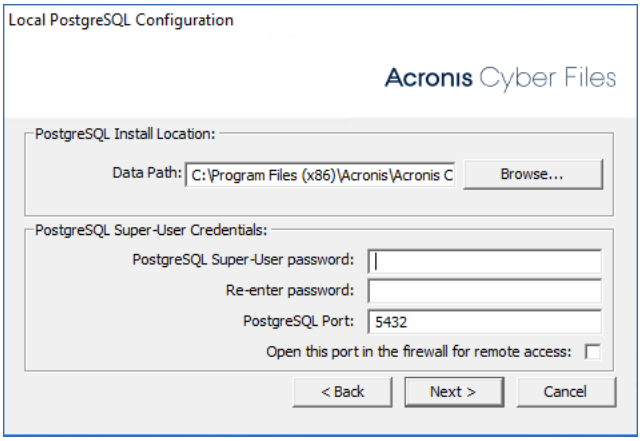
2.1.1 Using the Installer

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.

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.



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



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

2.1.2 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.

2.2 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.

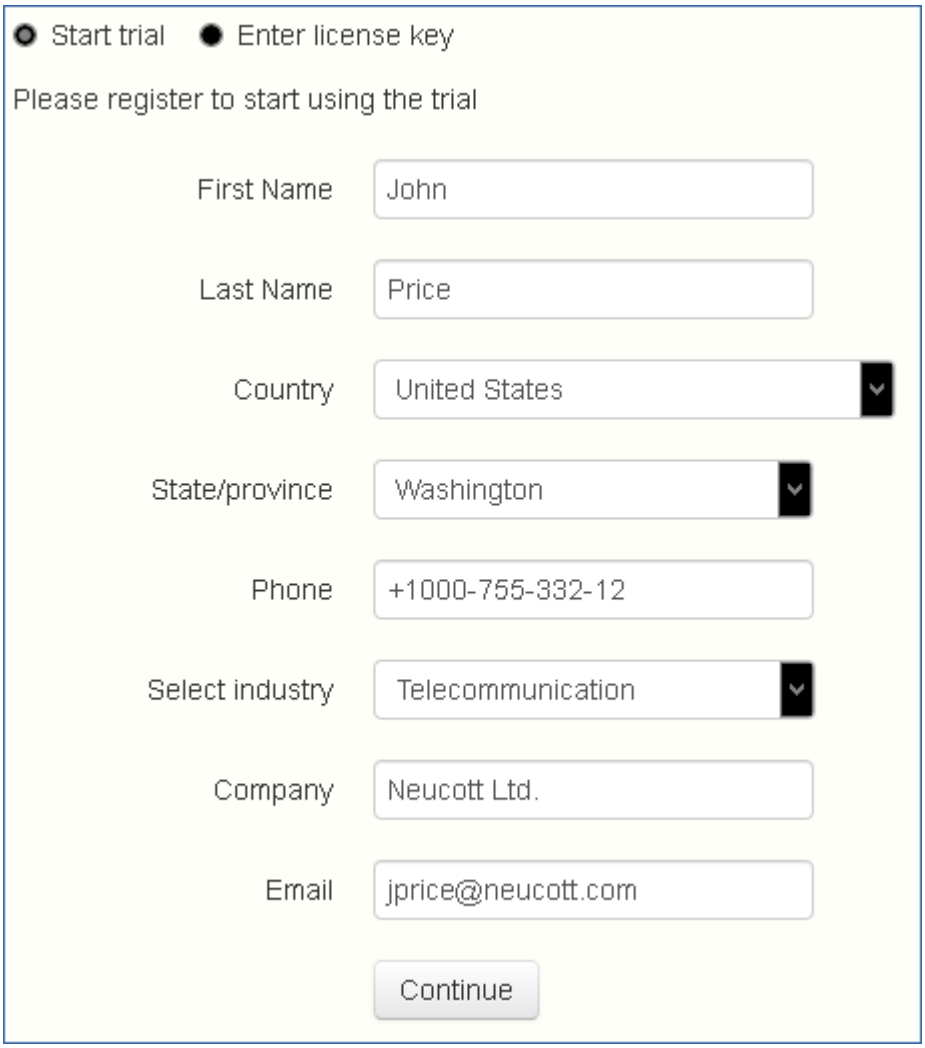
Note
All of the settings you see in the Initial Configuration page will also be available after you complete it. For more information on any of the settings, please visit the Server Administration articles.

Note
Internet Explorer 8 and 9 are not supported.

Licensing

To start a trial:

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

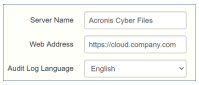


To license your Acronis Cyber Files instance:

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

3. Press **Save**.

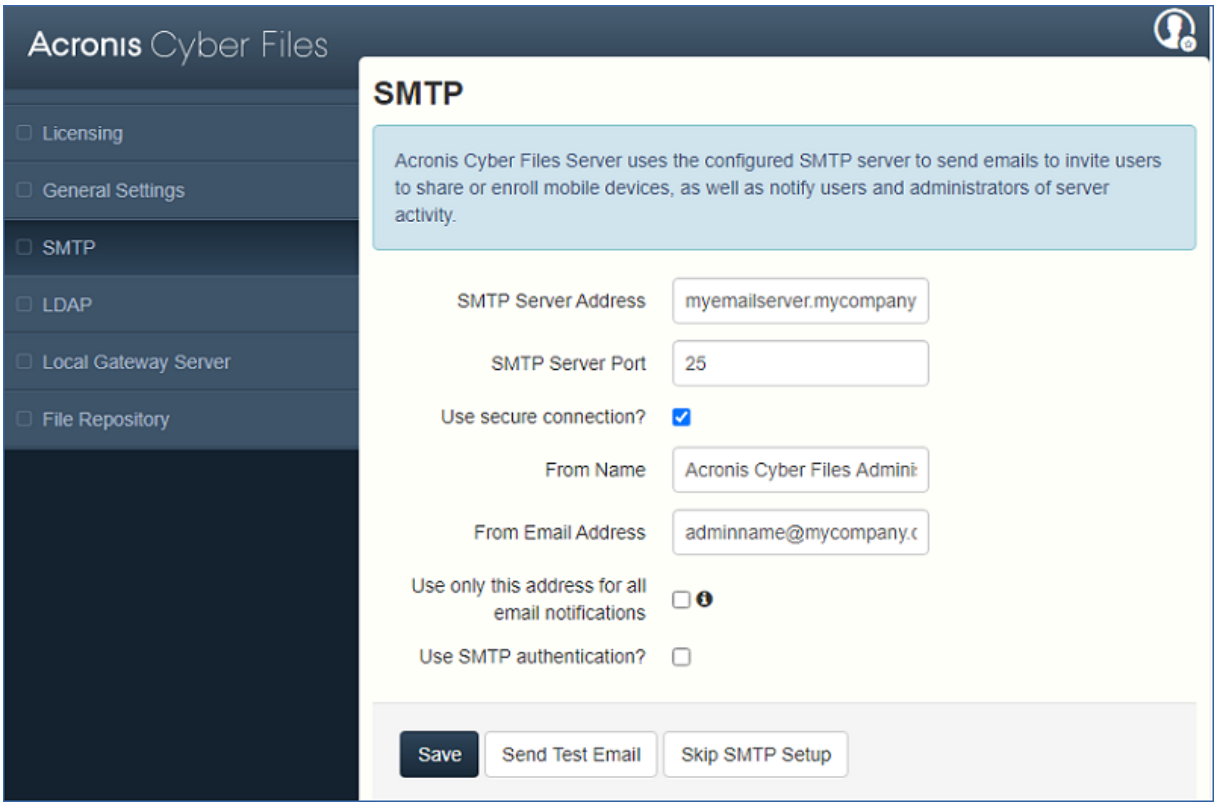
General Settings



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

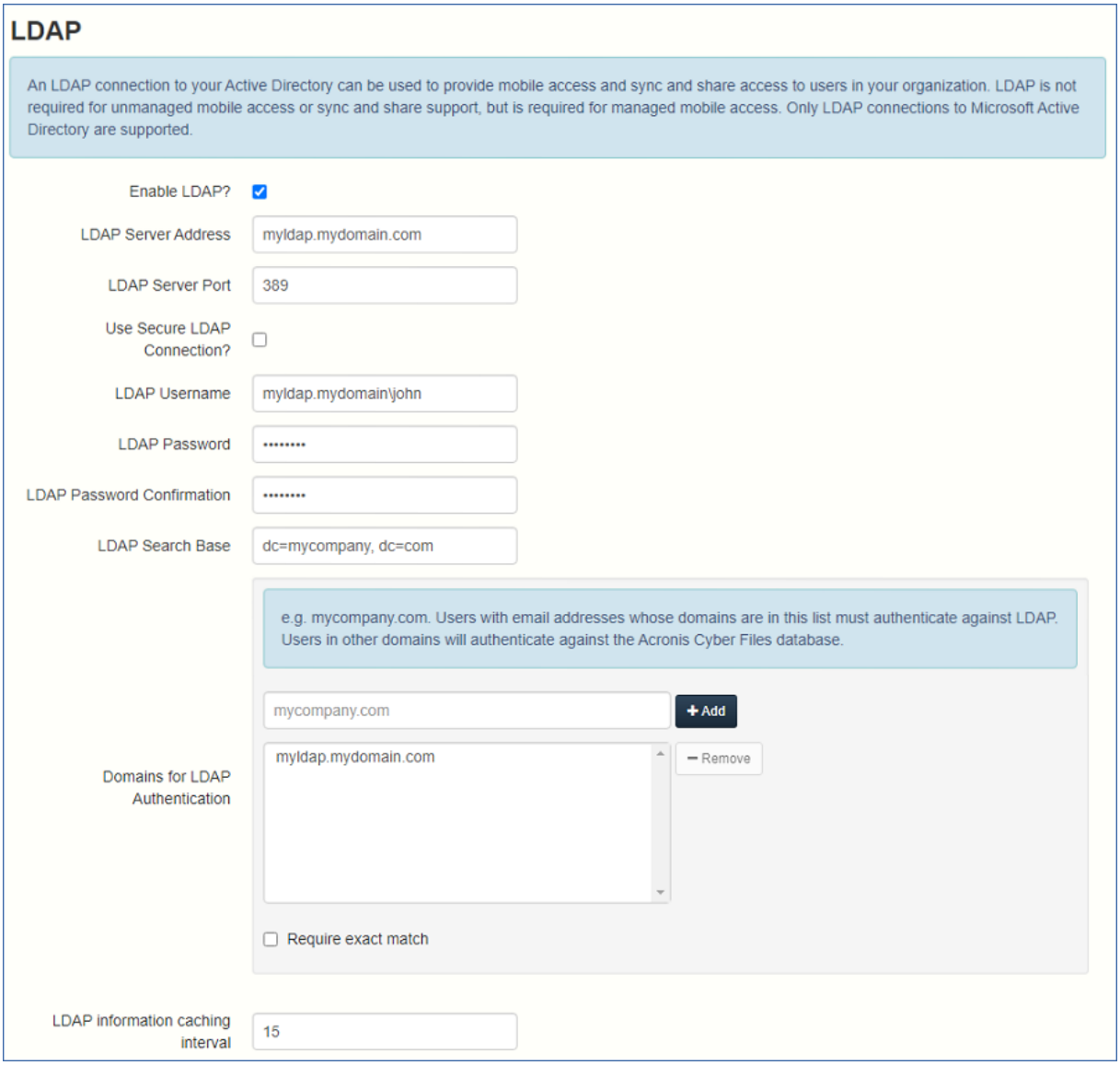


Note

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



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**.

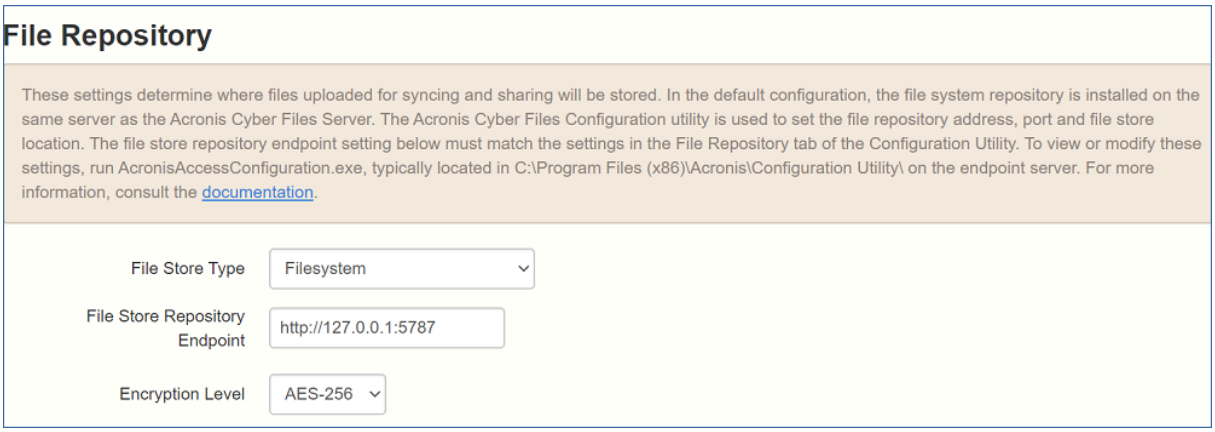
Local Gateway Server

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



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**.

1. **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 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. Press **Save**.

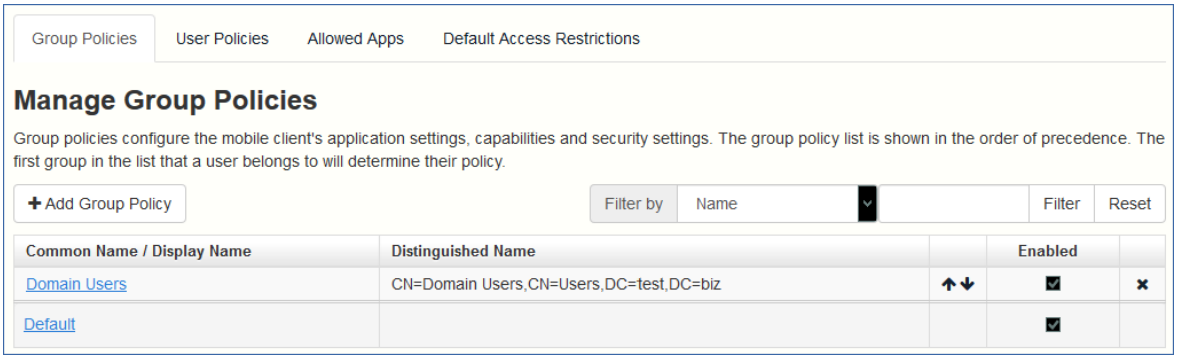
2.3 Mobile Access

2.3.1 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**.



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.

2.3.2 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.
7. 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.

2.3.3 Client Guides

For information on using the Acronis Cyber Files clients, please visit the specific client guide documentation for your app from the list below:

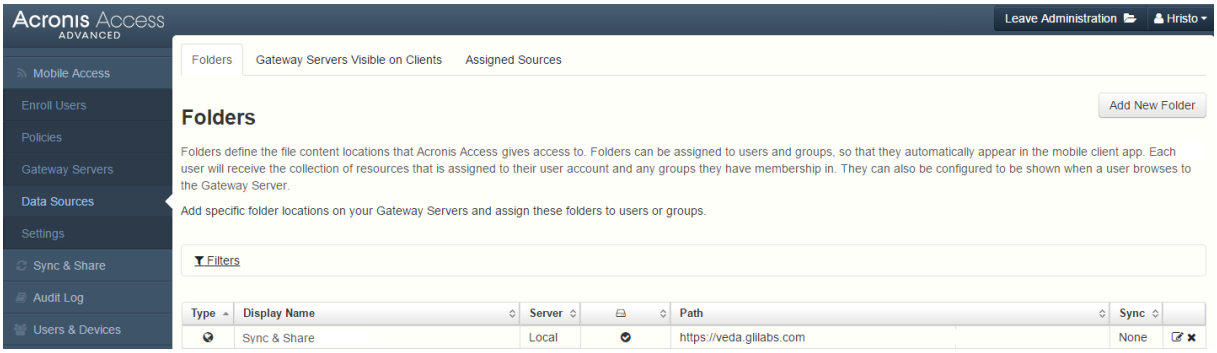
- Desktop and Web client
- iOS app
- Android app

2.4 Sync&Share

2.4.1 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.

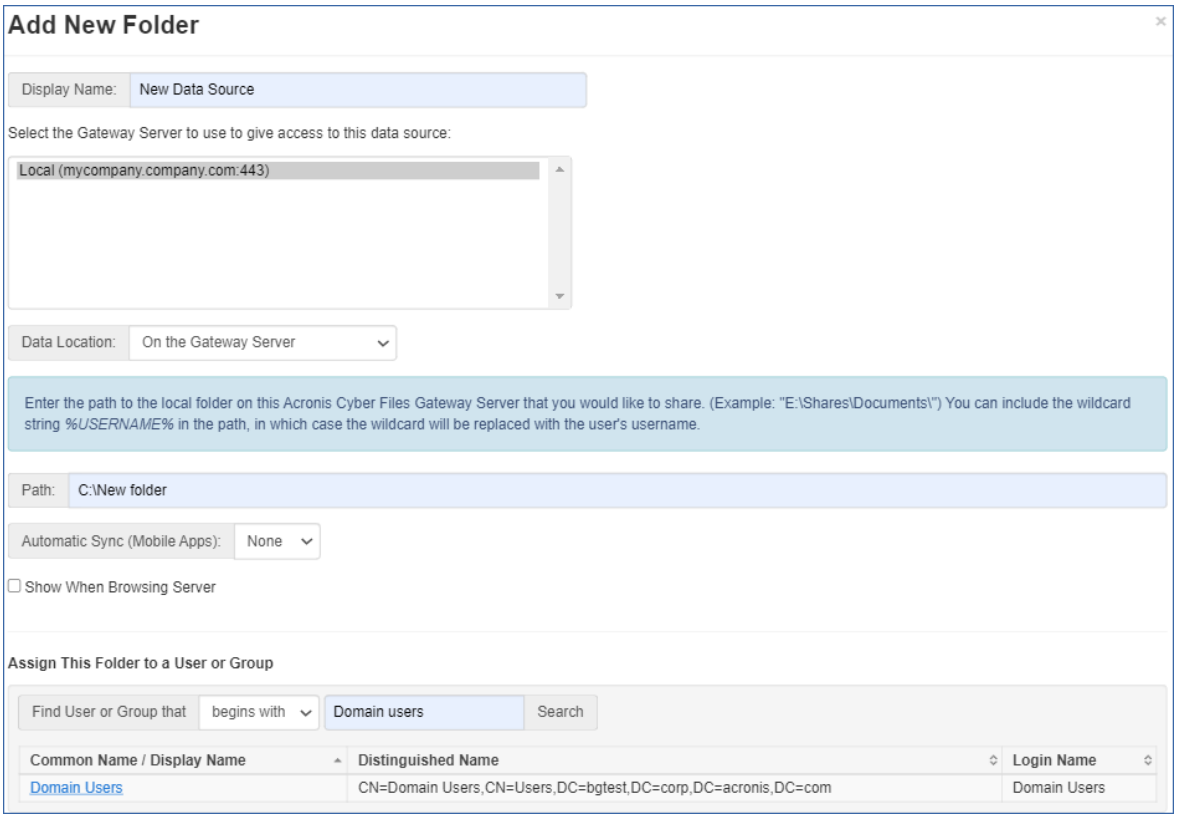


Sharing content to your users

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. Press the **Add New Folder** button.



6. Enter a display name for the folder.
7. Select the Gateway Server which 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.

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.

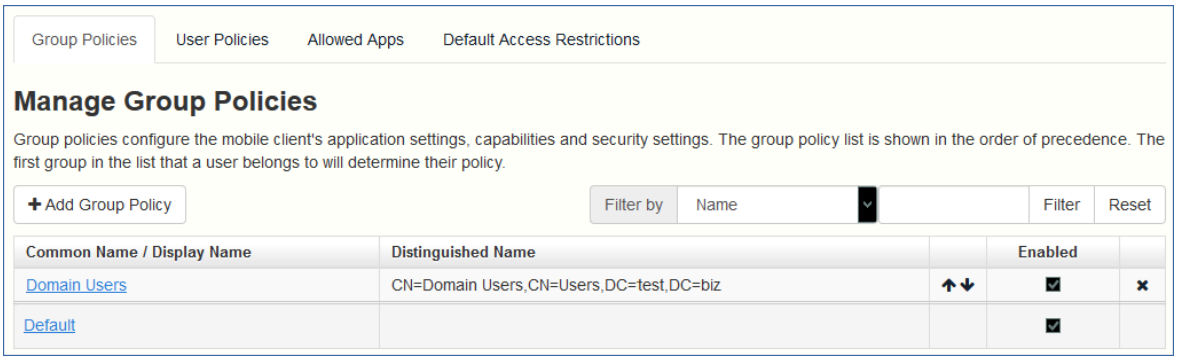
Note
When creating SharePoint Data Sources, you will have the option to enable the displaying of SharePoint followed sites.

12. Press the Save button.

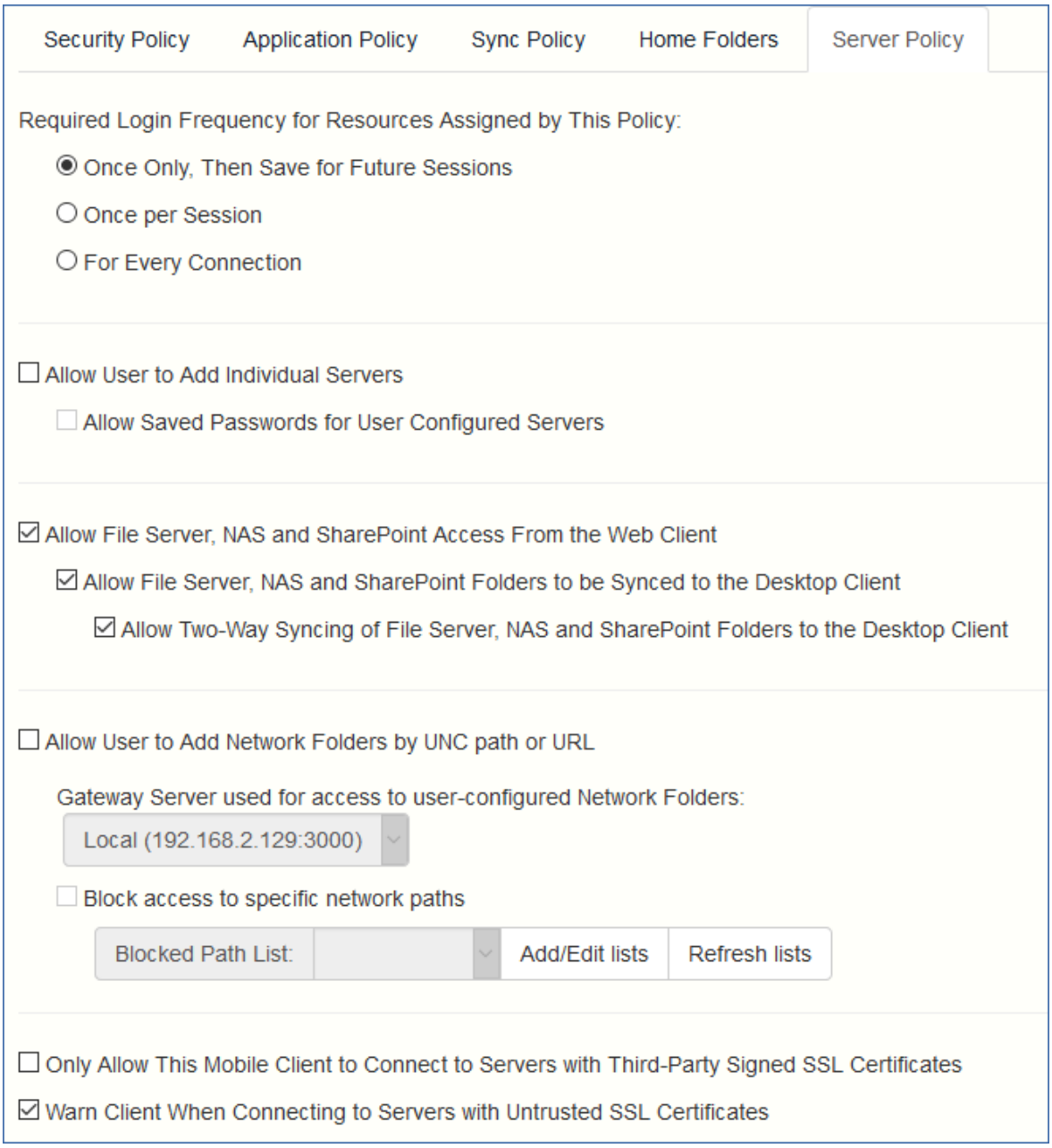
Allowing Web client users to access File Servers and more

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.



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



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.

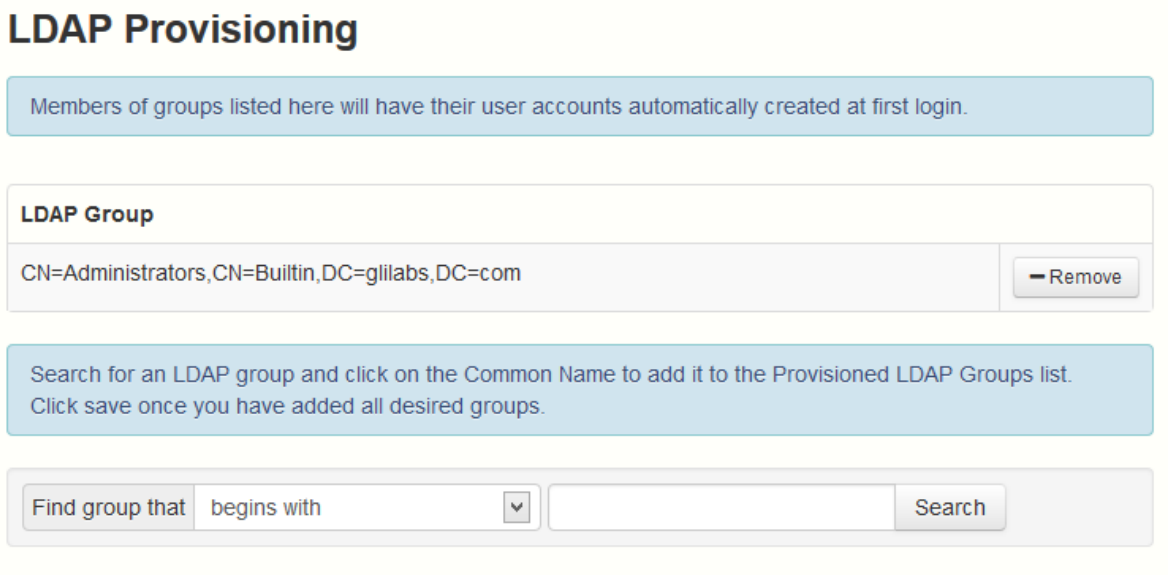
2.4.2 LDAP Provisioning

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**.



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

2.5 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.

2.6 Client Guides

For information on using the Acronis Cyber Files clients, please visit the specific client guide documentation for your app from the list below:

- Desktop and Web client
- iOS app
- Android app

3 Installing

3.1 Requirements

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

3.1.1 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.

3.1.2 Mobile Client Requirements

Supported devices:

- Apple iPad 4th generation and later
- Apple iPad mini 2nd generation and later
- Apple iPad Pro 1st generation and later
- Apple iPhone 5 and later
- Apple iPod Touch 6th generation and later
- Android smartphones and tablets (devices with x86 processor architecture are not supported).

Supported Operating Systems:

- iOS 11 to 13

> **Note**
> If you use MobileIron or Intune-enabled Files app, note that we do not support iOS versions that are not supported by the MDM vendors themselves in their respective SDKs. Information about the SDK version, used in Files as well as the supported iOS version can be found at the corresponding MDM.

- Android 4.1 or later (devices with x86 processor architecture are not supported).

The Acronis Cyber Files app can be downloaded from:

- For iOS.
- For Android.

3.1.3 Minimum Hardware Recommendation

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 recommendations for a production environment. If you plan on starting a trial or installing Acronis Cyber Files for testing purposes, you can step-down the hardware depending on your test load.

Small Deployments

- Up to 25 users
- CPU: Intel i7 Xeon class with 4 cores or AMD equivalent.
- RAM: 16 GB
- Disk Space: 100 GB

Medium Deployments

- Up to 500 users
- 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.
- 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.

3.1.4 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, BlackBerryDynamics and 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.
- **BlackBerry Dynamics enabled app:** The Acronis Cyber Files mobile app includes the ability to be enrolled in and managed by the BlackBerry Dynamics platform. In this configuration, all network communication between Acronis Cyber Files mobile apps and Gateway Servers is routed through the BlackBerry Dynamics secure communication channel and BlackBerry Proxy Server. For more details, see the Acronis Cyber Files mobile app for BlackBerry Dynamics manual page.
- **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.

Note
Certificates:
Acronis Cyber 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).

3.1.5 Desktop Client Requirements

System requirements

Supported operating systems:

- Windows 7, Windows 8 and 8.1, Windows 10

> **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 and higher with Mac compatible with 64-bit software.

> **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
- Internet Explorer 10 and later
- Microsoft Edge 42 or later

> **Note**
> To be able to download files when using Internet Explorer, make sure that the **Do not save encrypted pages to disk** check box is cleared. This setting is found under **Internet Options > Advanced > Security**.

> **Note**
> Internet Explorer 11 and earlier do not support uploads of files larger than 4GB.

- Google Chrome 64 and later.

- Safari 12 and later.

Note
Safari is supported on macOS and iOS but not on Windows.

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).

3.2 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 visit the Upgrading section.

Note
For instructions on installing on a cluster visit the Loadbalancing section.

The installation of Acronis Cyber Files involves three steps:

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

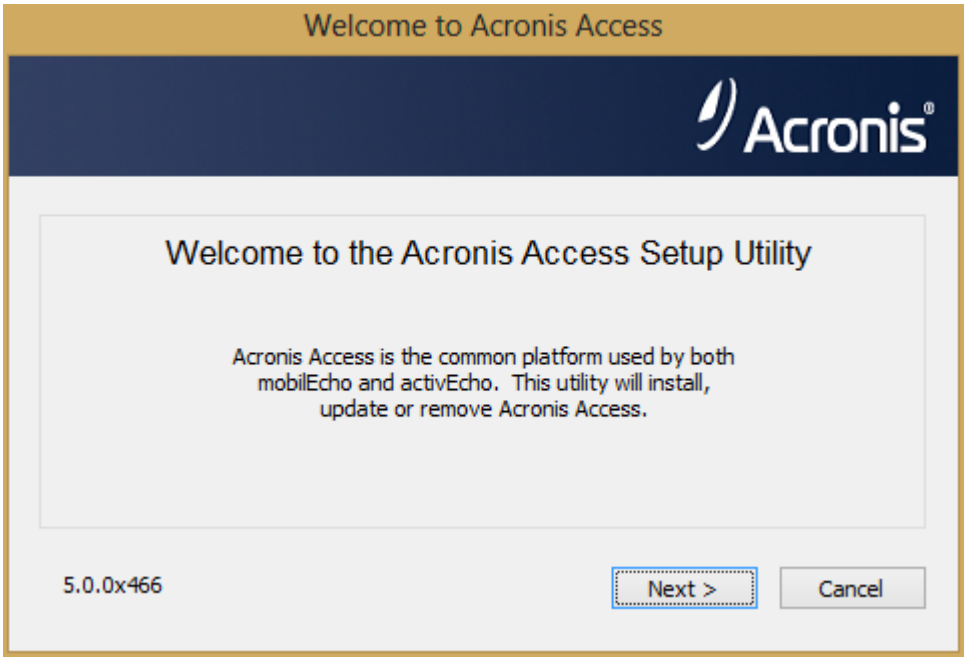
3.2.1 Installing Acronis Cyber Files

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

1. Download the Acronis Cyber Files installer.

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

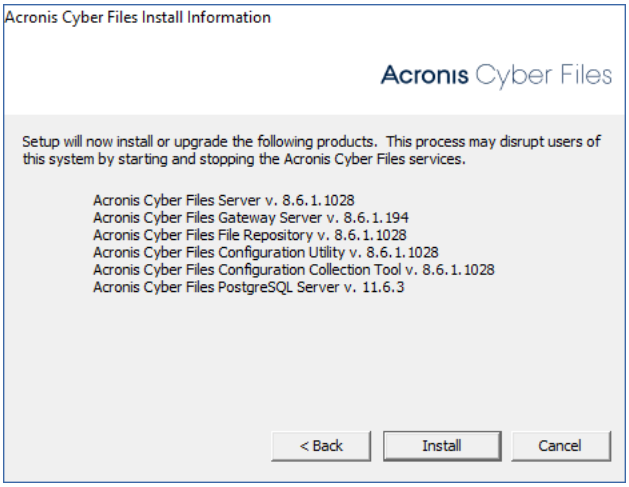
2. Double-click on the installer executable.



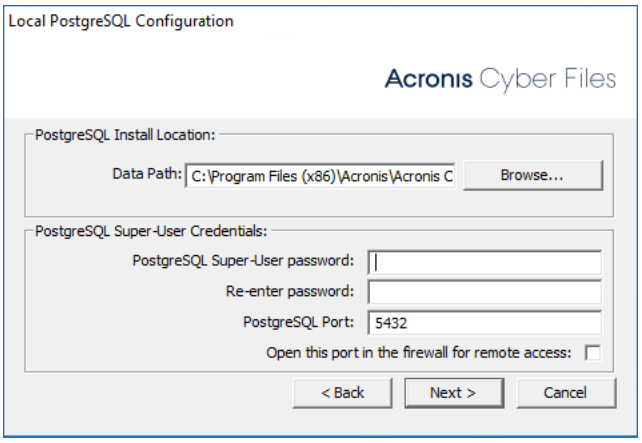
3. Press **Next** to begin.
4. Read and accept the license agreement.
5. Press **Install**.

> **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 press OK.



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

- 

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

For instructions on using the Configuration utility, visit the Using the Configuration Utility page.

3.3 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 Acronis Cyber Files Gateway server, File Repository and Acronis Cyber Files Web Server.

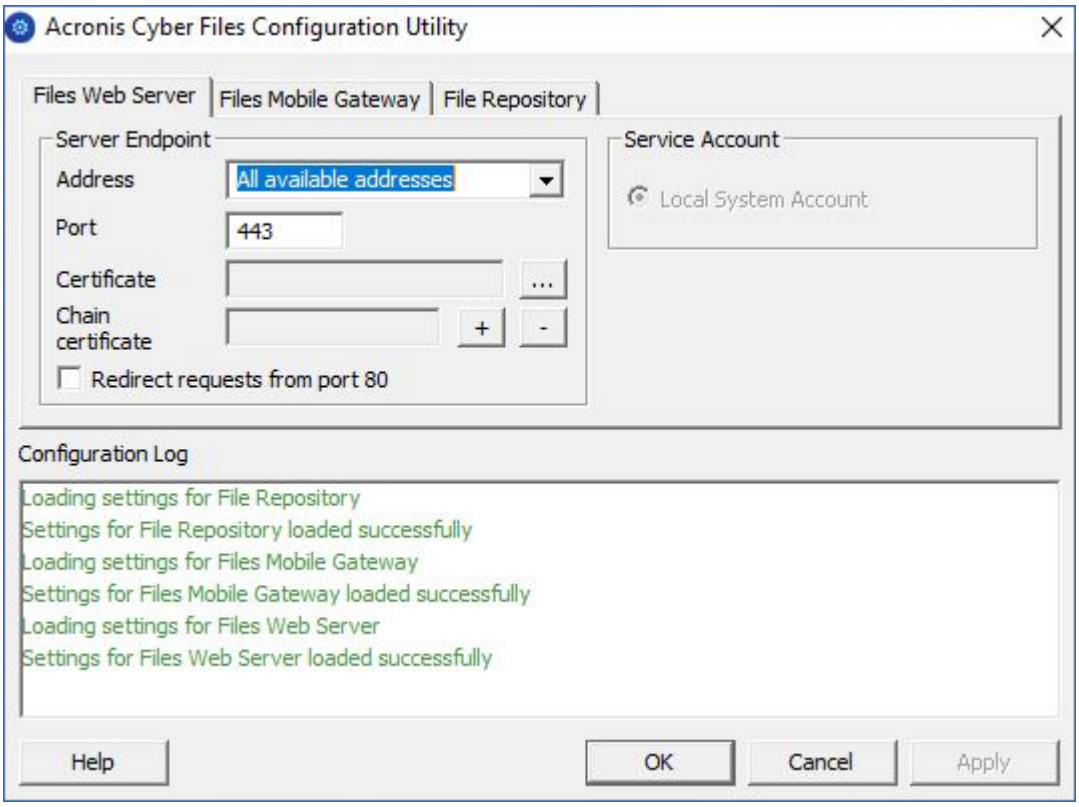
Note
See the Network Requirements section for more information on best practices for the IP address configurations of Acronis Cyber Files.

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

3.3.1 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.

Web Server tab



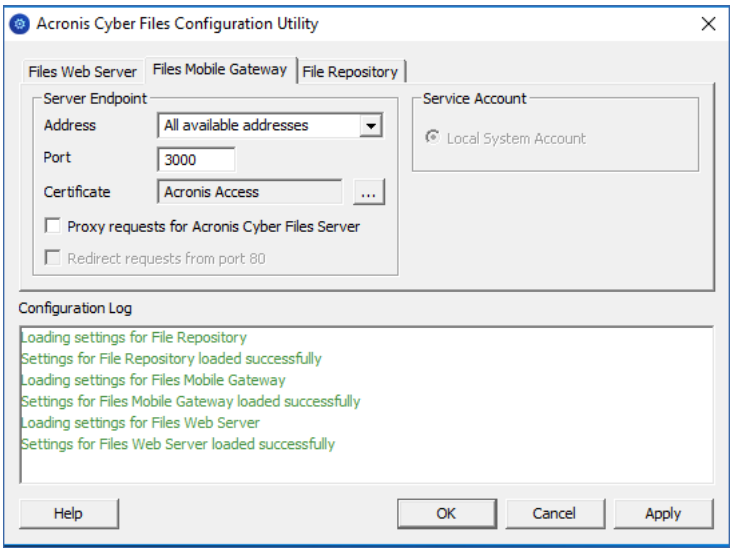
The Acronis Cyber Files Web Server provides the web user interface for Acronis Cyber Files clients, and is also the administration console for both Mobile Access and Sync & Share.

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

Mobile Gateway tab



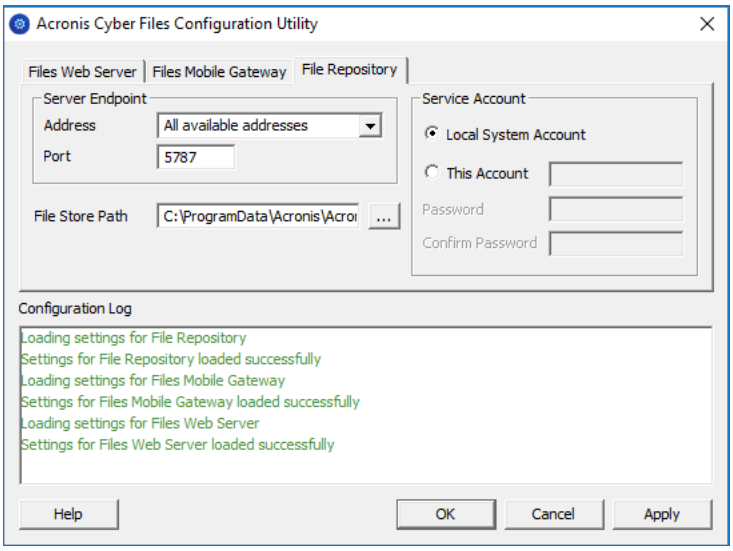
The Gateway Server is used by mobile clients to access both files and shares.

- **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 Acronis Cyber Files Server - When checked, users will connect to the Gateway Server which will then proxy them to the Acronis Cyber Files Server. This is available on when you have an Acronis 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



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 **Acronis 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.

3.3.2 Proceeding to the Setup Wizard

After you have filled in all the necessary fields, pressing **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 Acronis 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 Acronis 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.

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

3.4 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!

3.4.1 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.

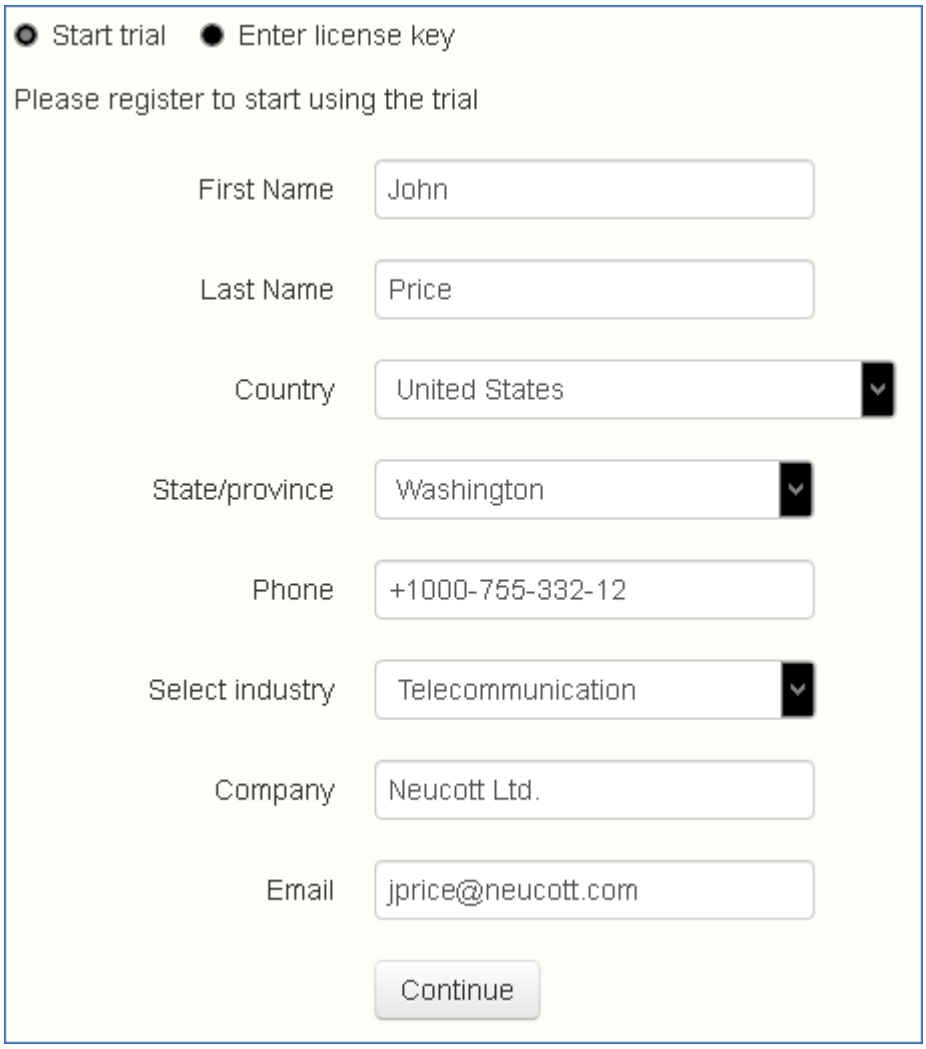
SMTP settings cover functionality in both Mobile Access features and Sync & Share features. For Mobile Access, the SMTP server is used when sending enrollment invitations. Sync & Share features use the SMTP server to send folder invitations, warnings, summaries of errors.

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 press **Continue**.

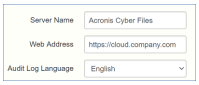


To license your Acronis Cyber Files instance:

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

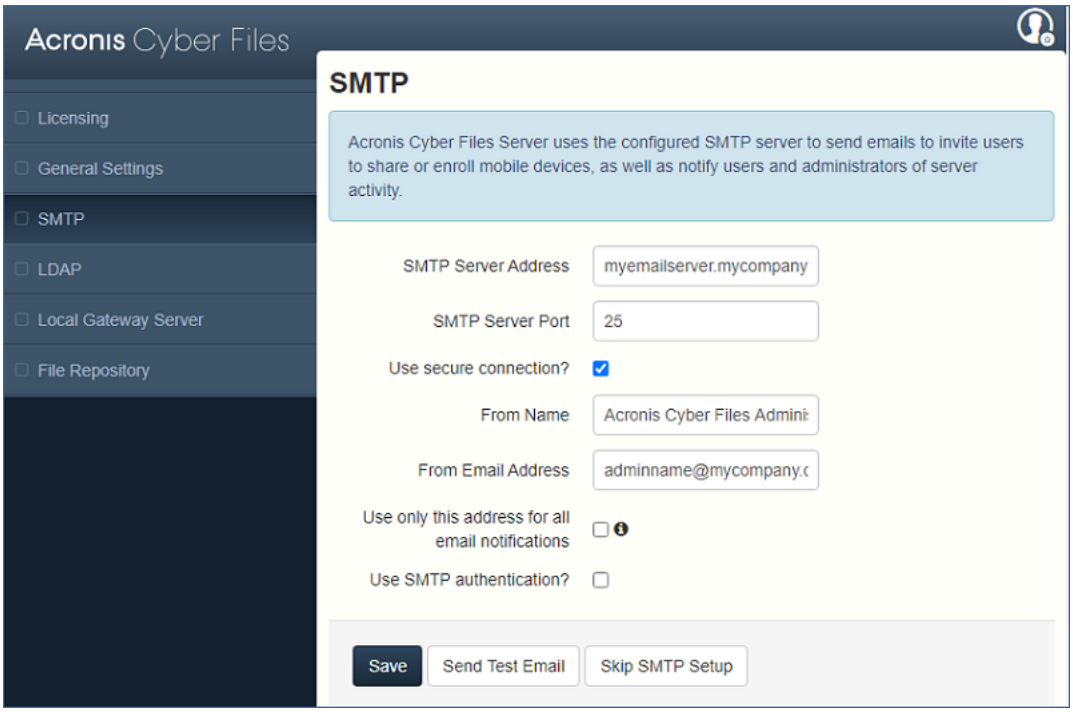
3. Press **Save**.

General Settings



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. Press **Save**.

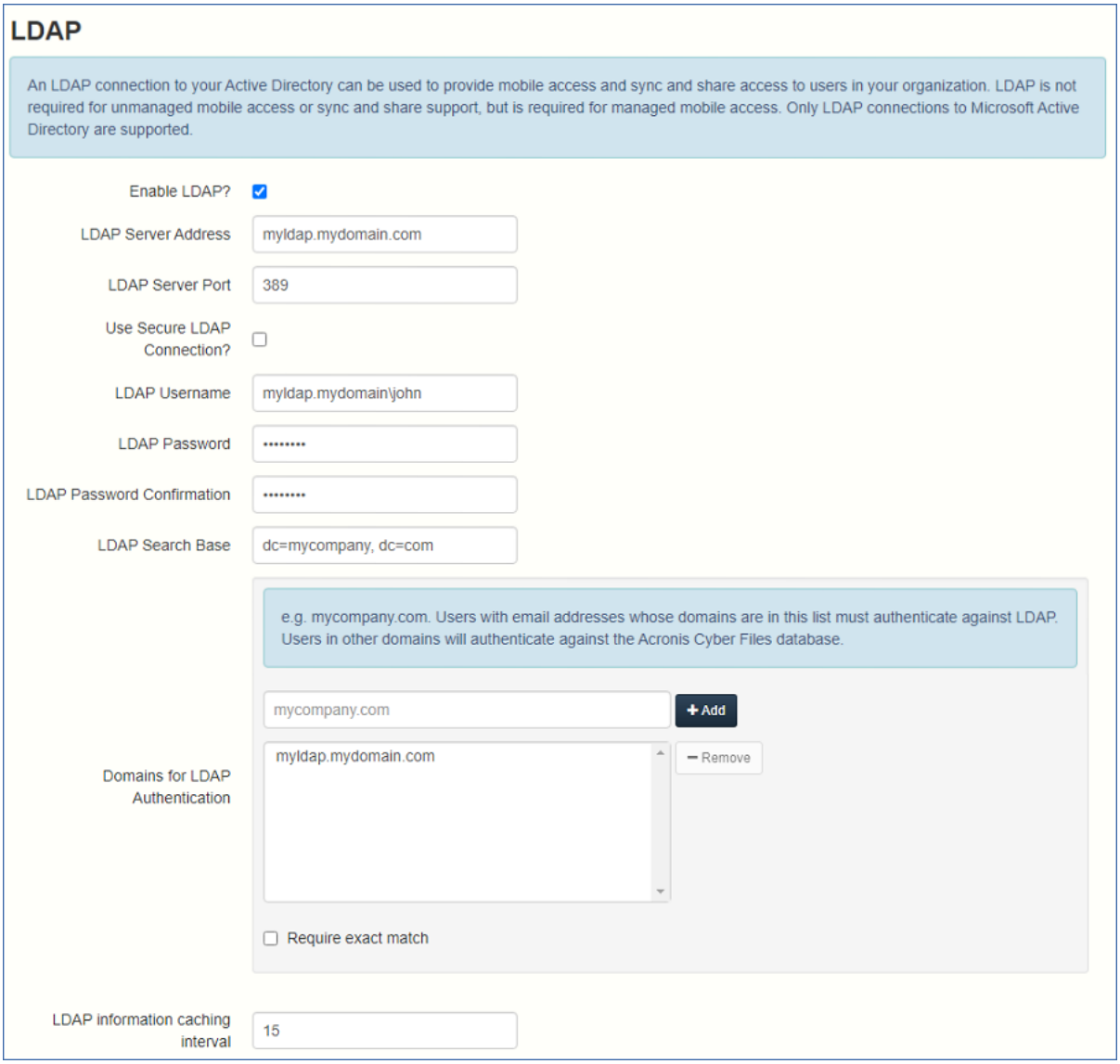
SMTP



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. Press **Send Test Email** to send a test email to the email address you set on step 5.
8. Press **Save**.

LDAP



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. Press **Save**.

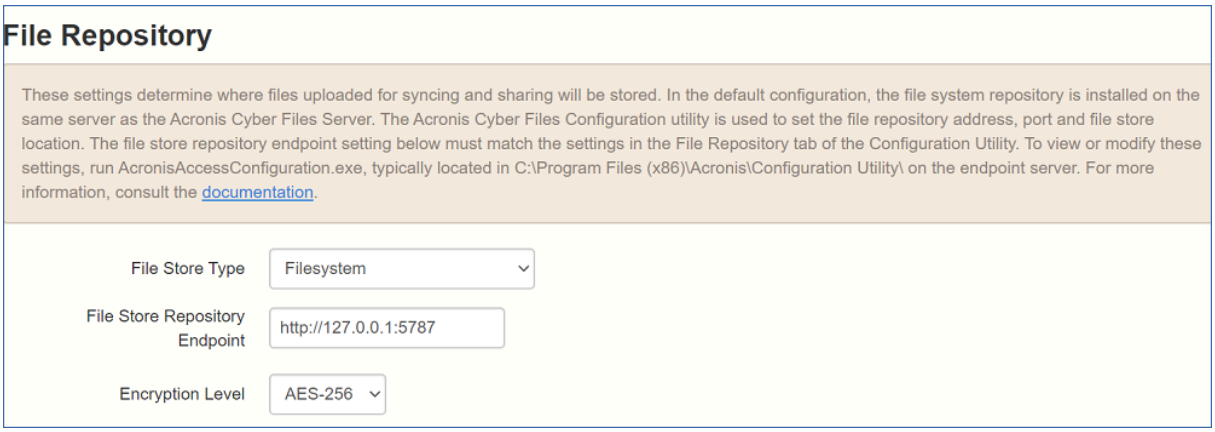
Local Gateway Server

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 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. Press **Save.**

File Repository



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. Press **Save**.

3.5 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.

3.6 Load balancing Acronis Cyber Files

Acronis Cyber Files supports load balancing. For more information please visit the Load Balancing Acronis Cyber Files ,Installing Acronis Cyber Files in a load balanced configuration , Migrating to a load balanced configuration and Cluster Groups articles.

4 Upgrading

4.1 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
If you are upgrading from a version of Acronis Cyber Files (formerly Acronis Access) earlier than 7.5, please contact Acronis support at http://www.acronis.com/mobilitysupport/.

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 Acronis Cyber Files to its latest version 8.6, the PostgreSQL version is not automatically changed to 11 too. For more information on how to do that, refer to Upgrading PostgreSQL to a newer Major version.

4.1.1 Backup the vital components

The Apache Tomcat folder

On upgrade the Apache Tomcat may be upgraded and all of the current Tomcat configuration filesand log files will be removed. We recommend you make a copy of the Apache Tomcat folder, which by default is found here:C:\Program Files (x86)\Acronis\Files Advanced\Common\.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at C:\Program Files (x86)\Acronis\Files Advanced\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 9.2\bin folder located in the PostgreSQL installation directory.
   e.g. cd "C:\PostgreSQL\9.2\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 see: http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html

Note
For more information on PostgreSQL backup procedures and command syntax please read this: http://www.postgresql.org/docs/9.2/static/backup.html

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\Files Advanced\Gateway Server\database

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

The Acronis Cyber Files configuration file

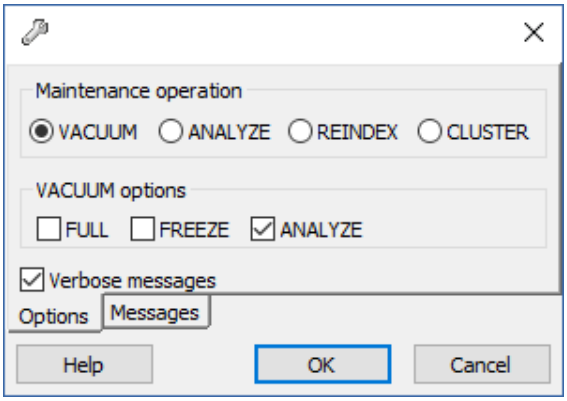
1. Navigate to the Acronis Cyber Files installation folder containing the configuration file.

Note
The default location is: C:\Program Files (x86)\Acronis\Files Advanced\Access Server

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

4.1.2 Vacuum the database before upgrading

1. Open the Acronis Cyber Files PostgreSQL Administrator tool (it could also be called PgAdmin). You can find it in Windows Start menu, under the Acronis Cyber Files folder. Double-click on **localhost** to connect to your server.
2. Right-click on the acronisaccess_production database and choose **Maintenance**.
3. Select the **VACUUM** radio button and the **ANALYZE** checkbox.



Warning!
The vacuum can take some time. This process should be run during periods of low load on the server.

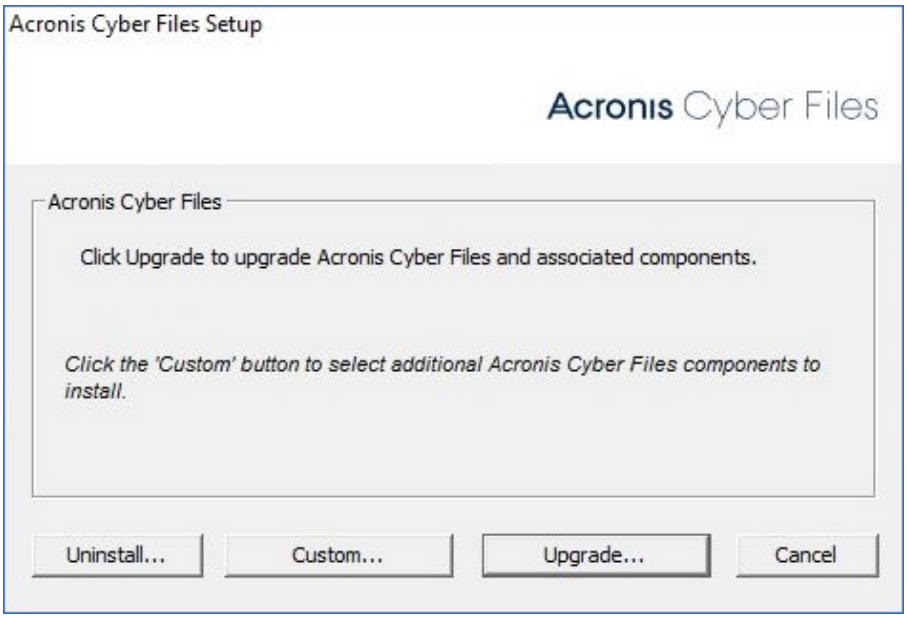
4. Press **OK**.
5. When the **Vacuum** process finishes, click **Done**.
6. Close the PostgreSQL Administrator tool.

4.1.3 Upgrade

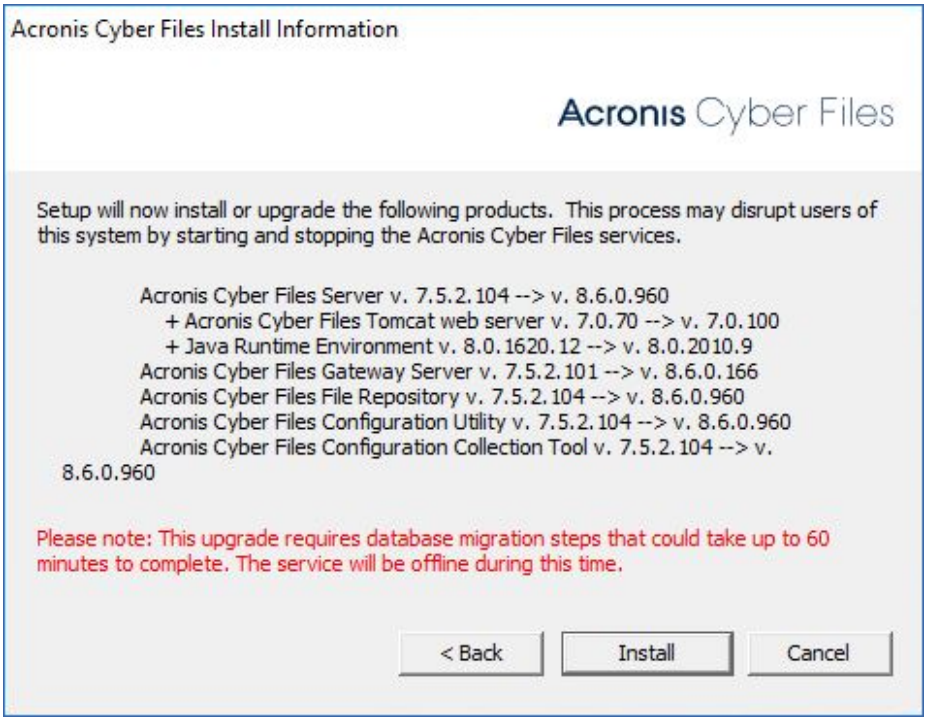
Note
Disable any anti-virus software you have or it may interrupt the procedure, resulting in a failed

installation.

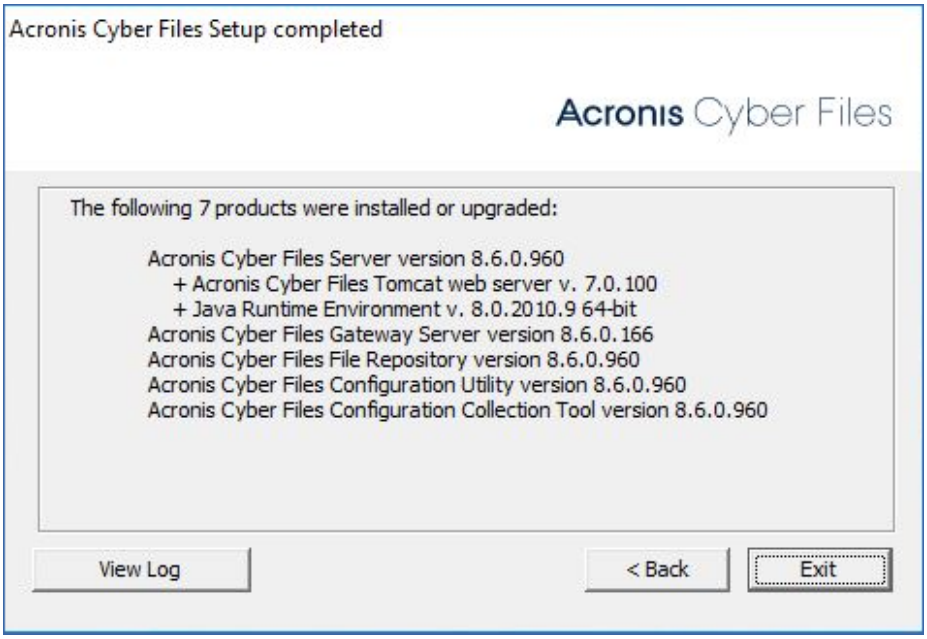
1. Double-click on the installer executable.
2. On the screen that opens next, press **Upgrade**.



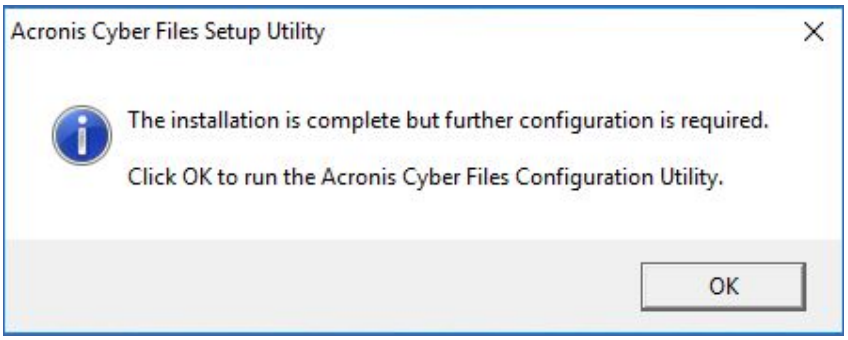
3. Review the components that will be installed and click **Install**.



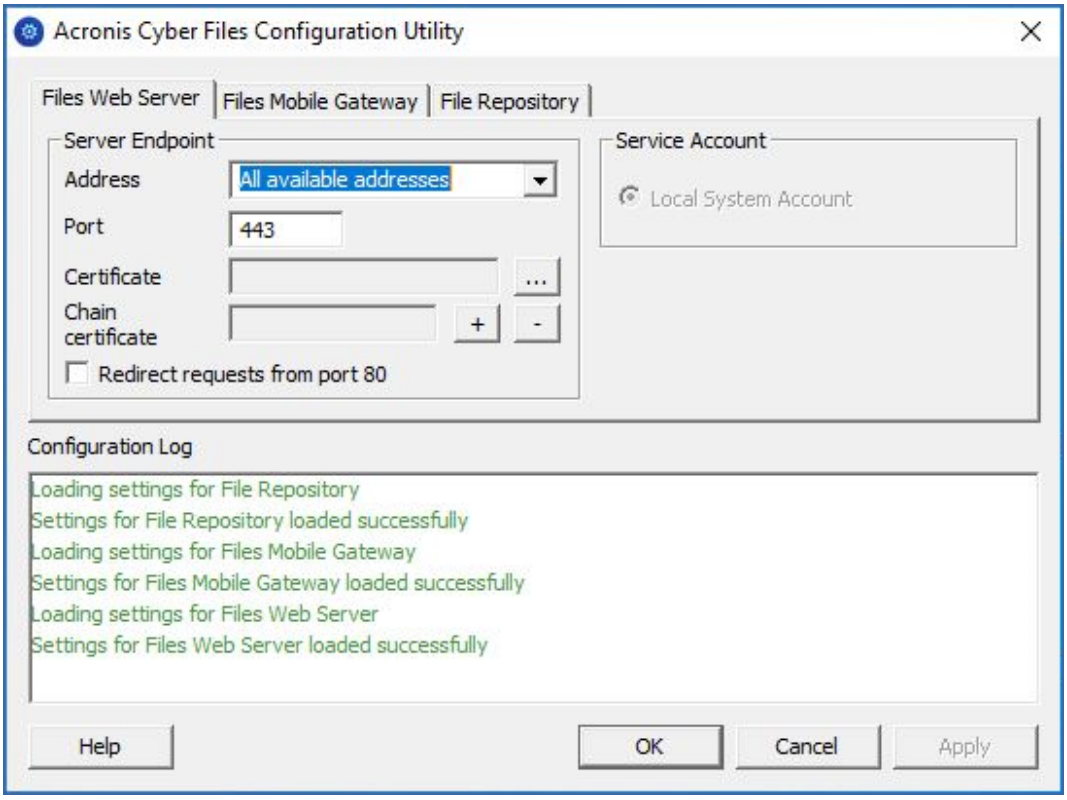
4. Review the already installed components and close the installer.



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



6. You will be prompted to open the Configuration Utility, press **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.



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.

4.2 Upgrading from mobilEcho 4.5 or earlier

To upgrade from mobilEcho, please contact Acronis Technical support at http://www.acronis.com/mobilitysupport.

4.3 Upgrading from activEcho 2.7 or earlier

To upgrade from activEcho, please contact Acronis Technical support at http://www.acronis.com/mobilitysupport.

4.4 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.

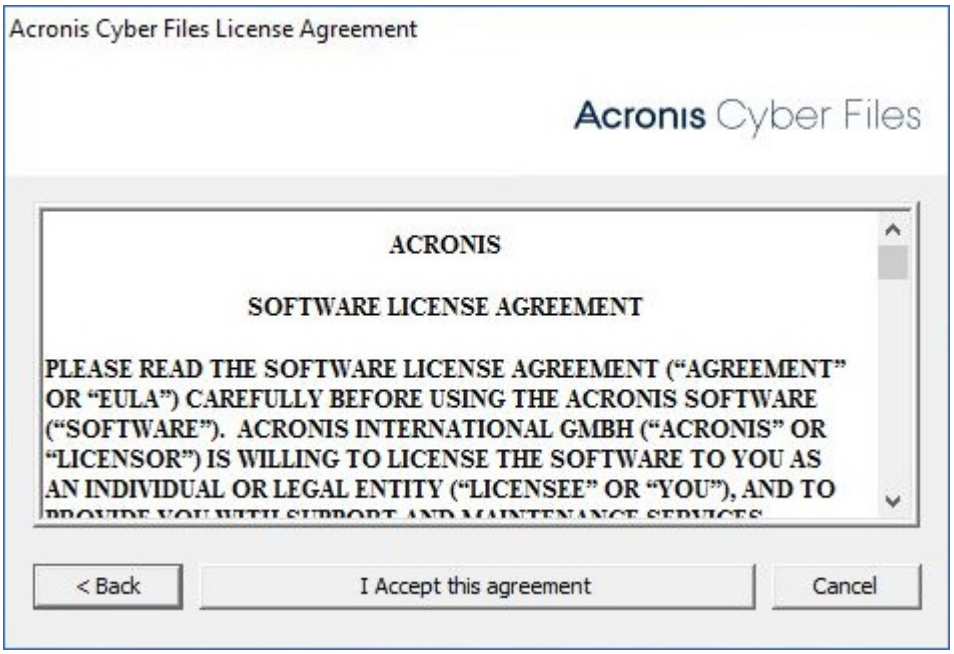
Note
Before upgrading, please review the Minimum Hardware Requirements.

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.

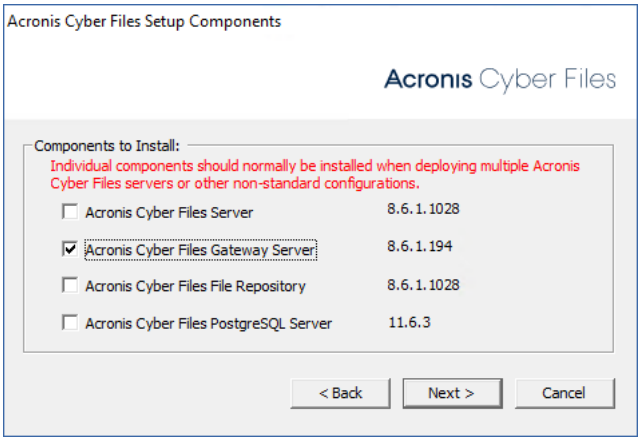
4.4.1 Upgrading a Gateway Server

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

3. Read and accept the license agreement.



4. Select **Custom**.
5. Select only the **Acronis <P RODUCT_NAME> Gateway Server** component and press **Next**.



6. Review the components and press **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 press **OK**.

4.5 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.

4.5.1 Before you begin

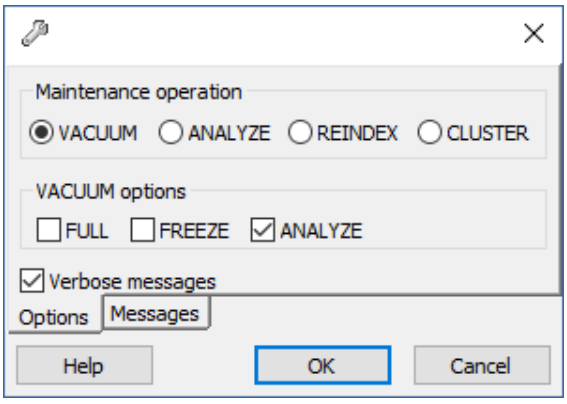
Pick one of the Acronis Cyber Files Web Server machines to act as the **Primary**. This machine is the **Primary** node only in the sense that it will be upgraded first and it will migrate any changes/settings to the PostgreSQL database. If the database is very large, these migrations can take several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

Warning!
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 (it could also be called PgAdmin). You can find it in Windows Start menu, under the Acronis Cyber Files folder. Double-click on **localhost** to connect to your server.
2. Right-click on the acronisaccess_production database and choose **Maintenance**.
3. Select the **VACUUM** radio button and the **ANALYZE** checkbox.



Warning!
The vacuum can take some time. This process should be run during periods of low load on the server.

4. Press **OK**.

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

4.5.2 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.
   a. 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.
   b. Expand **Databases** and right-click on the **acronisaccess_production** database.
   c. Choose **Maintenance** and select the **Vacuum** radio button and the **ANALYZE** checkbox. Press **OK**.
   d. 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.
   e. Close the PostgreSQL Administrator tool and open an elevated command prompt.
   f. 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\).

   a. 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.

4.5.3 Upgrading the File Repository

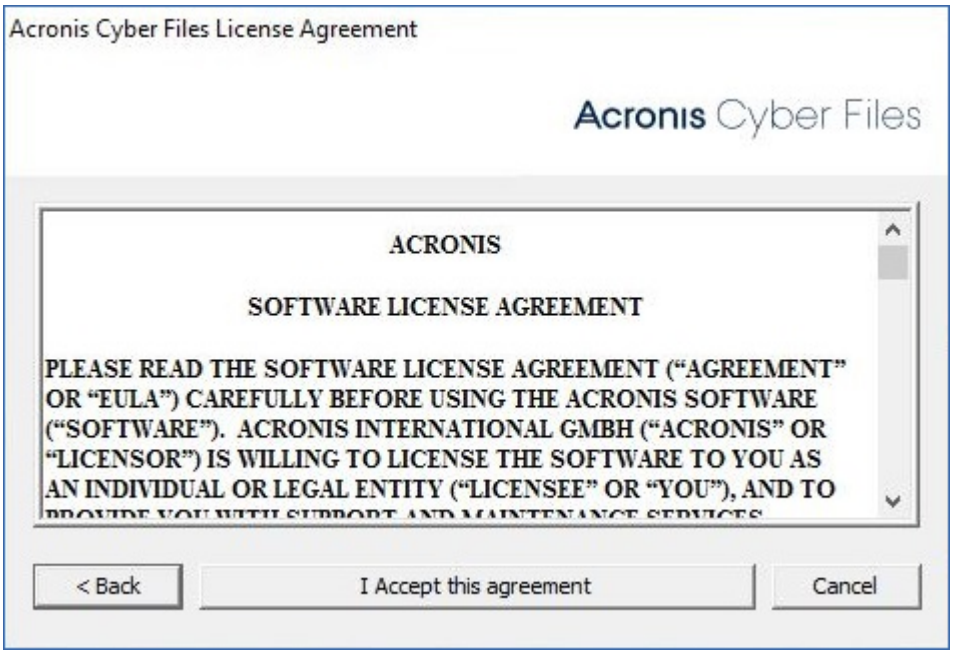
Upgrade the File Repository first regardless of where it is located.

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

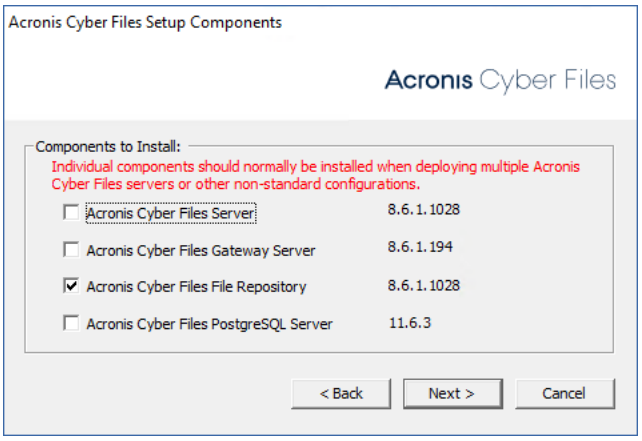
   Note
   If you have multiple File Repository services, repeat these steps for all repositories before you proceed with the other components.

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

3. Accept the License Agreement.



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

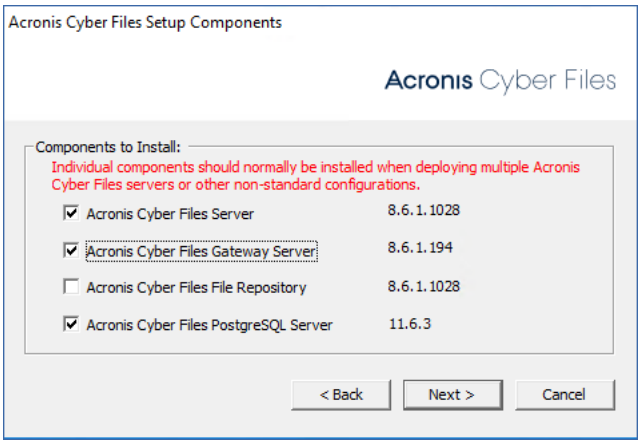


5. Click **Next**, review what is going to be installed and click **Install**.
6. When the upgrade is done, click **Exit**. When the Configuration Utility launches, click **OK**.
7. Continue by upgrading your **Primary** Acronis Cyber Files Web Server on its corresponding machine.

4.5.4 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.

3. Press **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.



Note
Our installer will not update PostgreSQL. If you wish to update your version of PostgreSQL please view our article on the subject and contact Acronis support before proceeding.

5. Press **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.

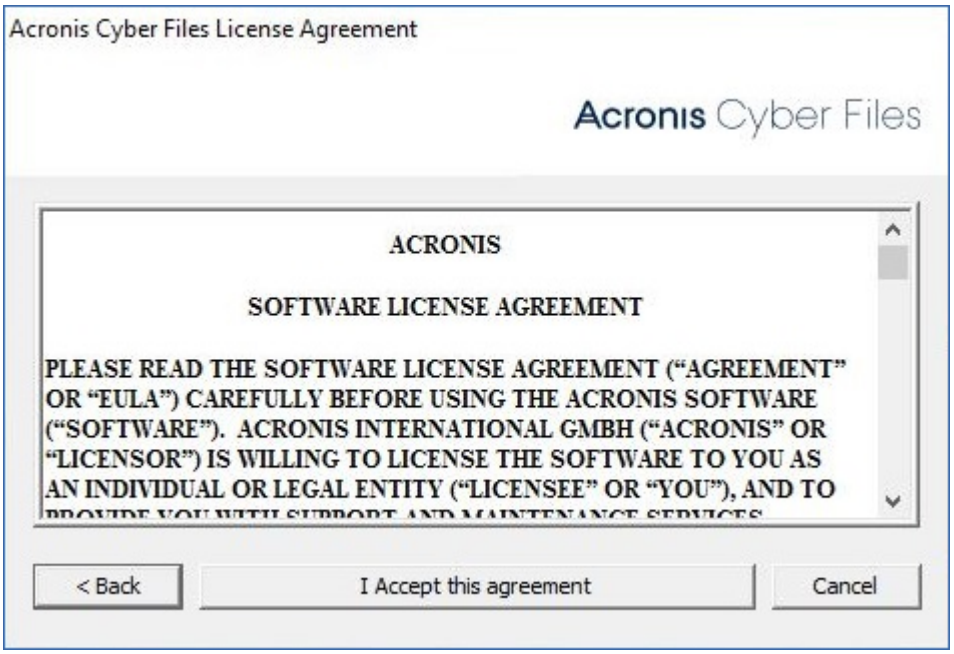
6. Once the Configuration Utility starts all the necessary services, and the database migrations are finished, verify that Acronis Cyber Files web interface on the **Primary** server works as expected. A web browser will launch automatically and display the Acronis Cyber Files server log-in screen.
7. 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!
upgrade or start any other Acronis Cyber Files Tomcat server until the **Primary** server is back up and you have verified that it is working correctly.

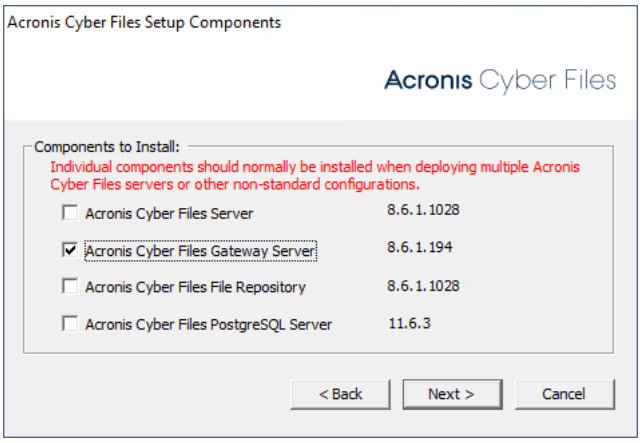
4.5.5 Upgrading Gateway Servers

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**.

3. Accept the License Agreement.



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



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**.

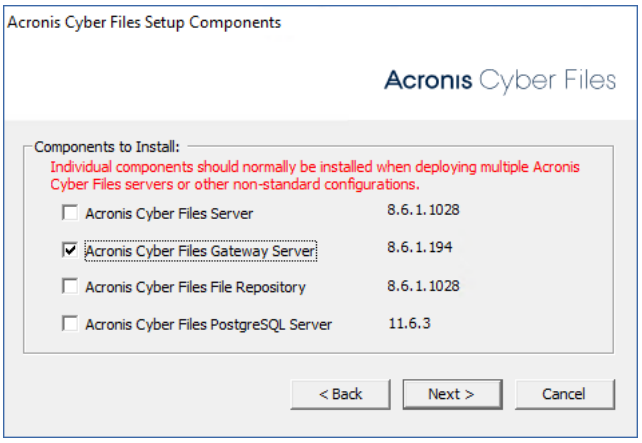
4.5.6 Upgrading all remaining nodes

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.

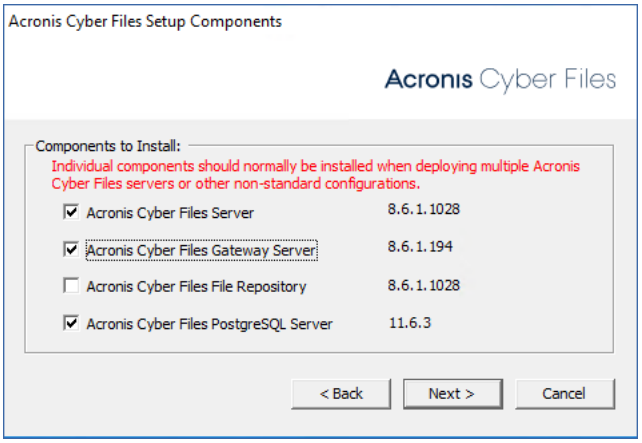
1. Copy the Acronis Cyber Files installer to the desired node and start it.

2. Press **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.



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



Note

Our installer will not update PostgreSQL. If you wish to update your version of PostgreSQL please view our article on the subject and contact Acronis support before proceeding.

4. Press **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.

5 Mobile Access

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

5.1 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.

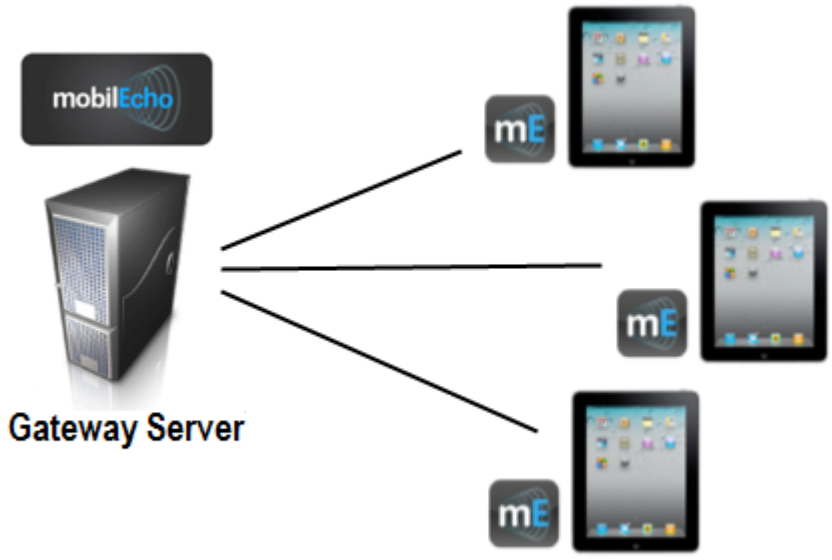


Fig 1. Single Acronis Cyber Files server with a Local Gateway Server

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.

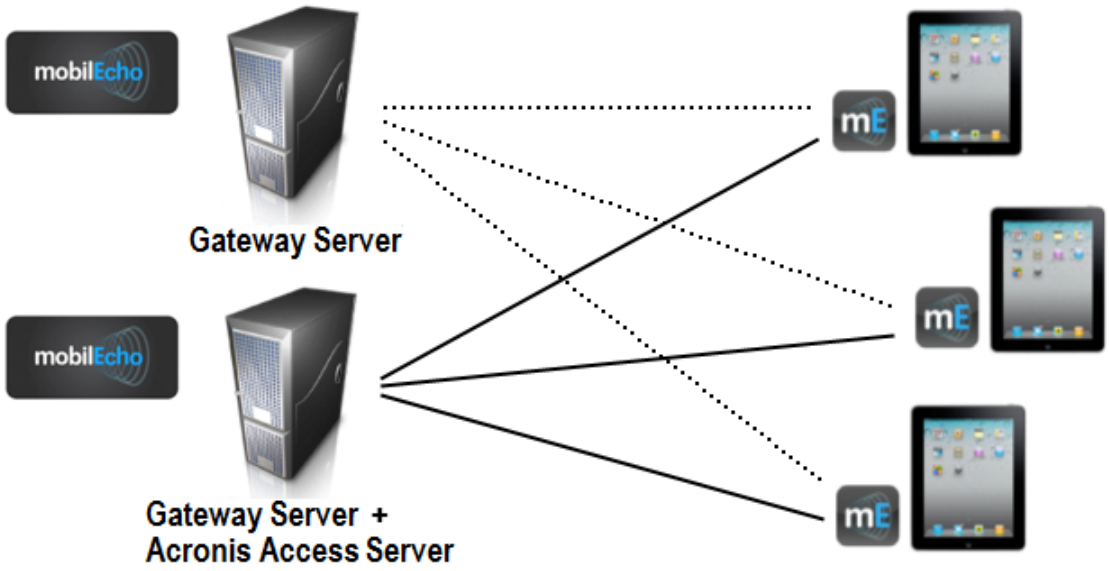


Fig 2. One Gateway Server, one Gateway Server + Acronis Cyber Files Server

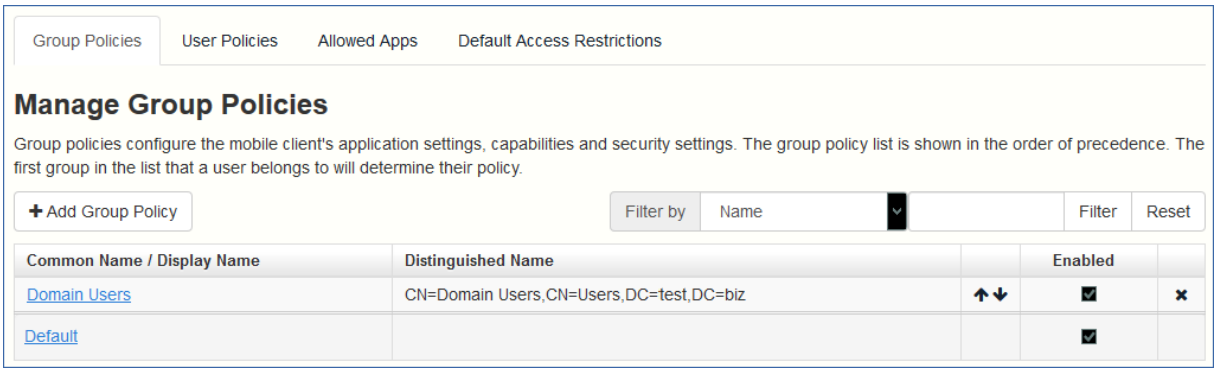
5.2 Policies

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

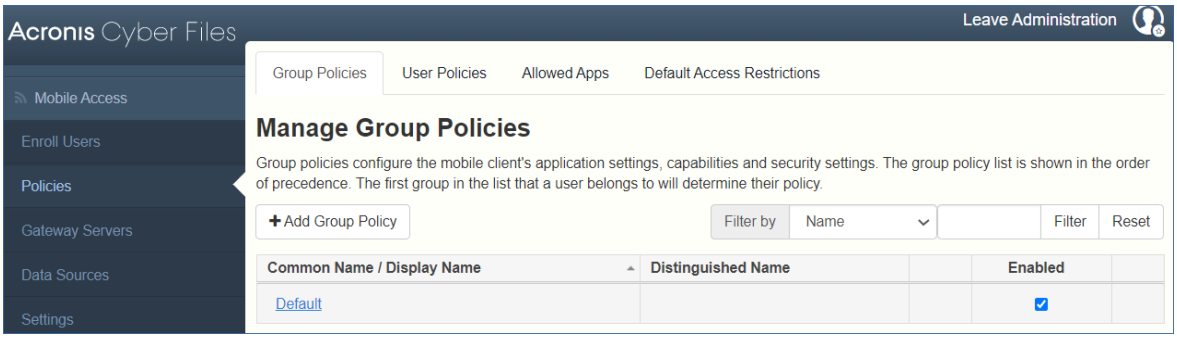
If you would like all or most of your users to receive the same policy settings, you can use the **Default** group policy. All users which are not members of a group policy and do not have an explicit user policy, become members of the **Default** group. The **Default** group is enabled by default. If 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.



5.2.1 Adding a New Policy

To add a new group policy:

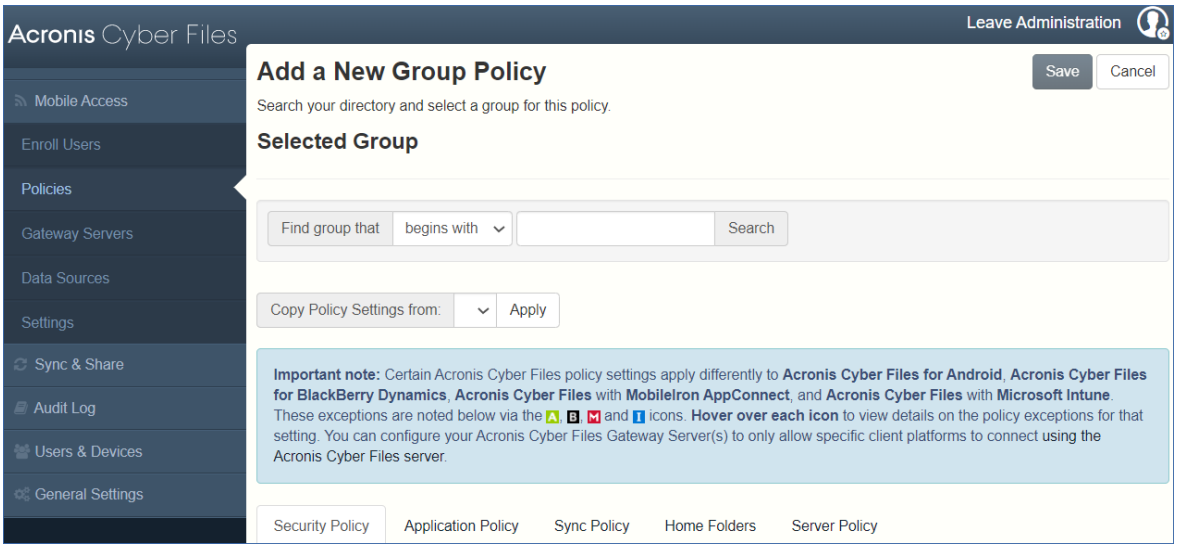
1. Open the **Group Policies** tab.
2. Click the **Add new policy** button to add a new group policy. This will open the **Add a new group policy** page.



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 press **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.



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 press **Save**.

5.2.2 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

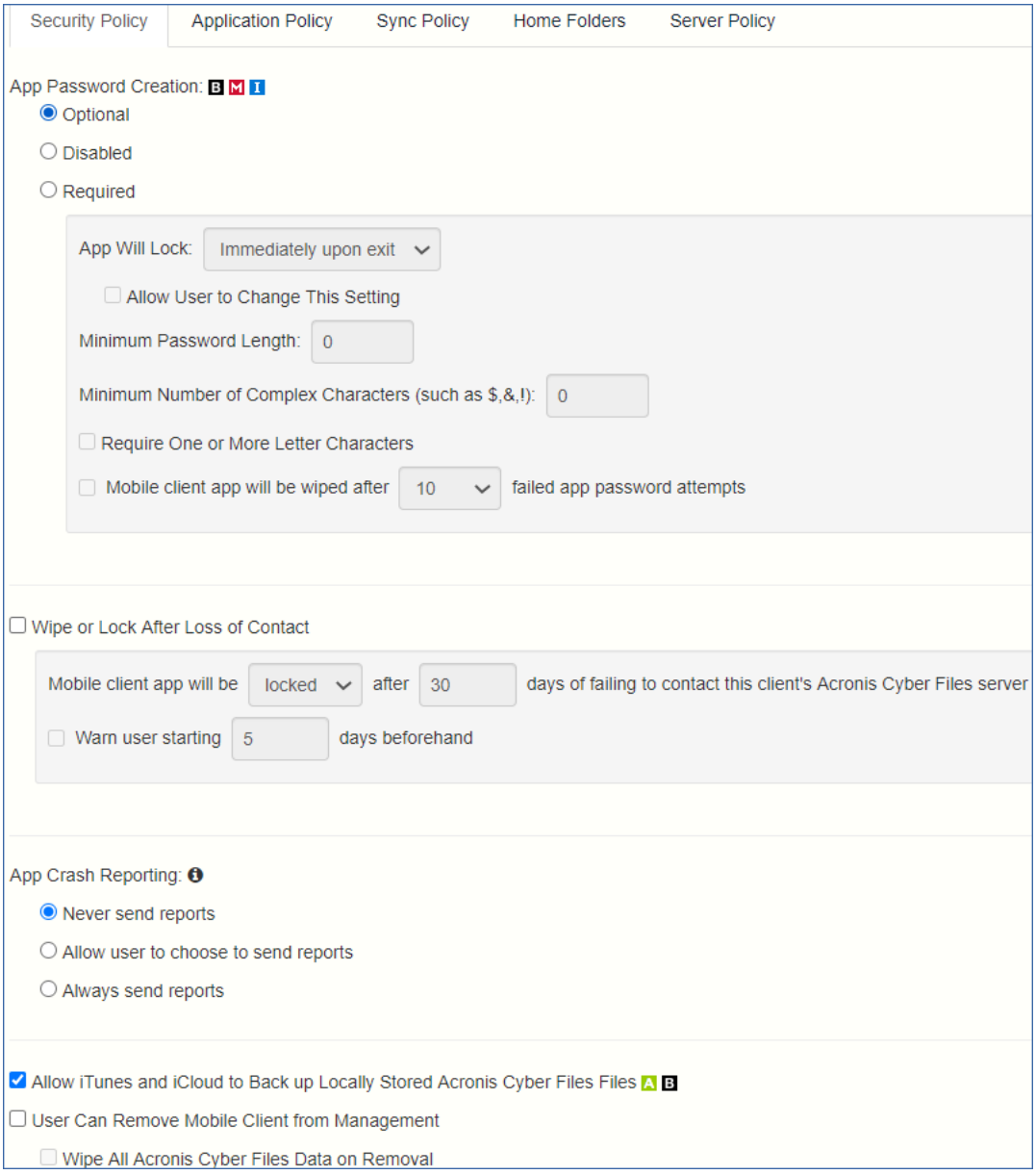
1. Click the **Groups Policies** option in top menu bar.
2. Click on the group you would like to modify.
3. Make any changes necessary on the **Edit Group Policy** page and press **Save**.
4. To temporarily disable a policy, uncheck the check box in the **Enabled** column for the desired group. This 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.

5.2.3 Policy Settings

Security Policy



- **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.

  Note
  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!

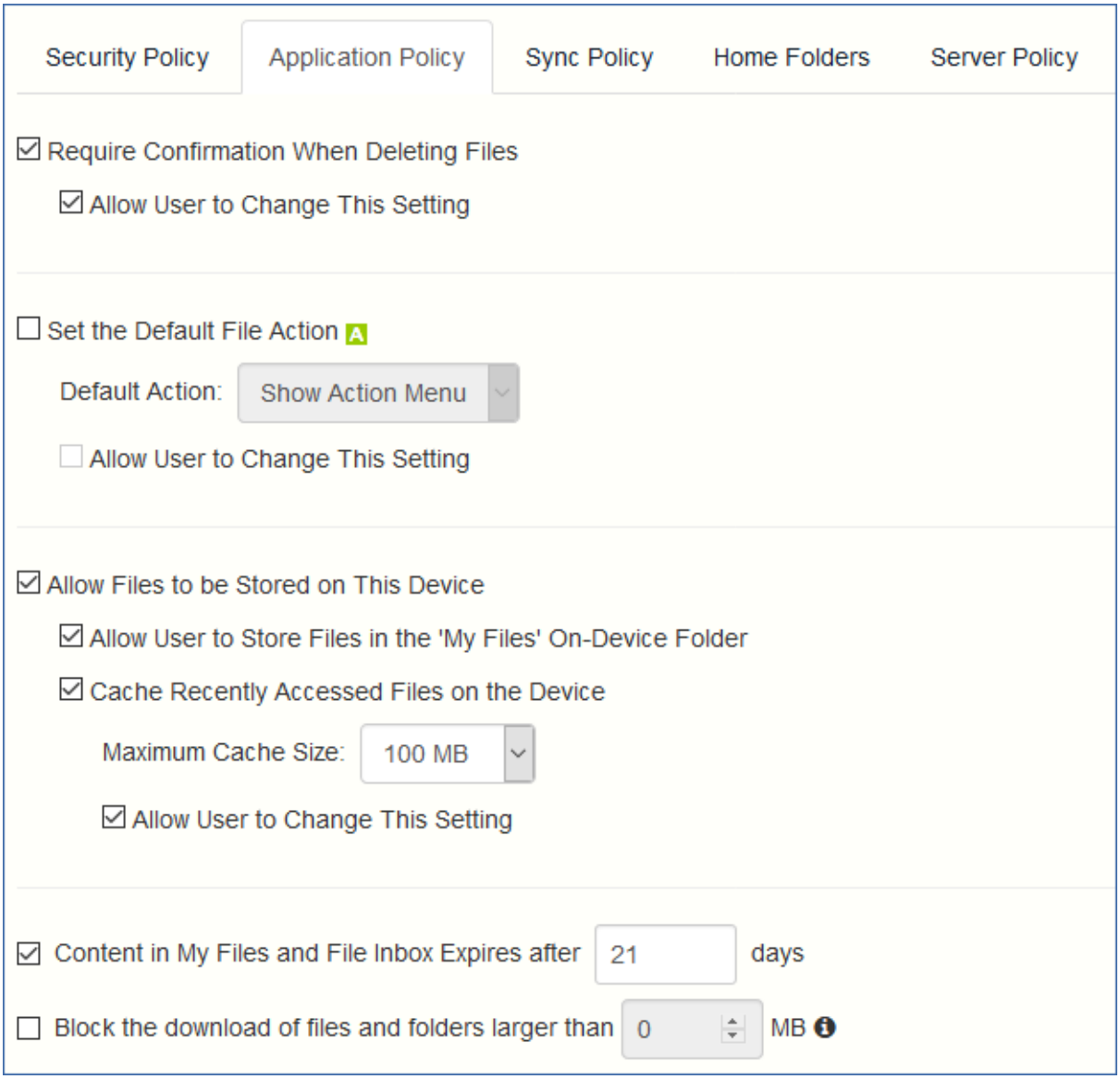
  - Locked clients will automatically unlock in the event that they later contact the server successfully.
  - Wiped clients immediately have all the local files stored in the mobile app deleted, their client management policy removed, and all settings reset to defaults. Wiped clients will have to be re-enrolled 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



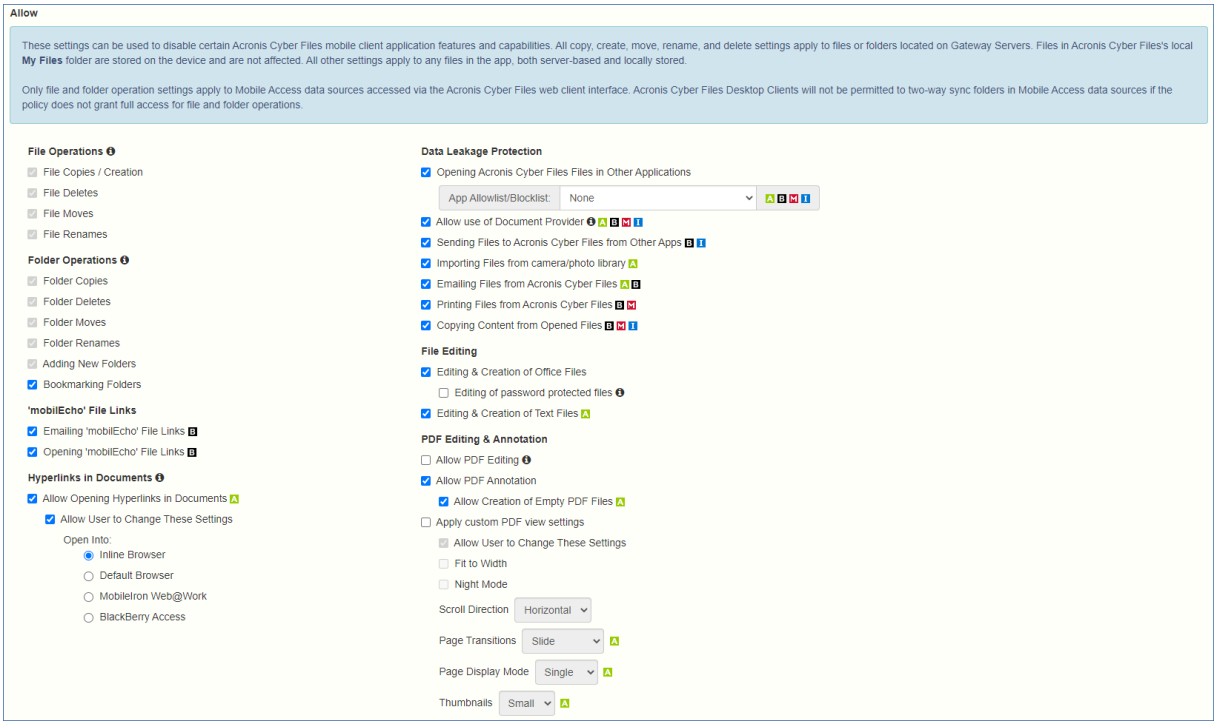
- **Require Confirmation When Deleting Files** - When enabled, the user will be asked for confirmation each time they delete a file. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Set the Default File Action** - This option determines 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 Acronis 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 Acronis 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 Acronis 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



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 Acronis 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.
  - **Blackberry Access** - Hyperlinks will be opened in BlackBerry Access 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 Whitelist/Blacklist** - Select a predefined whitelist or blacklist that restricts that third party apps that Acronis Cyber Files files can be opened into on the device. To create a whitelist or blacklist, 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 black/white 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 white/black 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 the user to select text in opened documents for copy/paste operations. This will prevent data from being copied into other applications.

File Editing

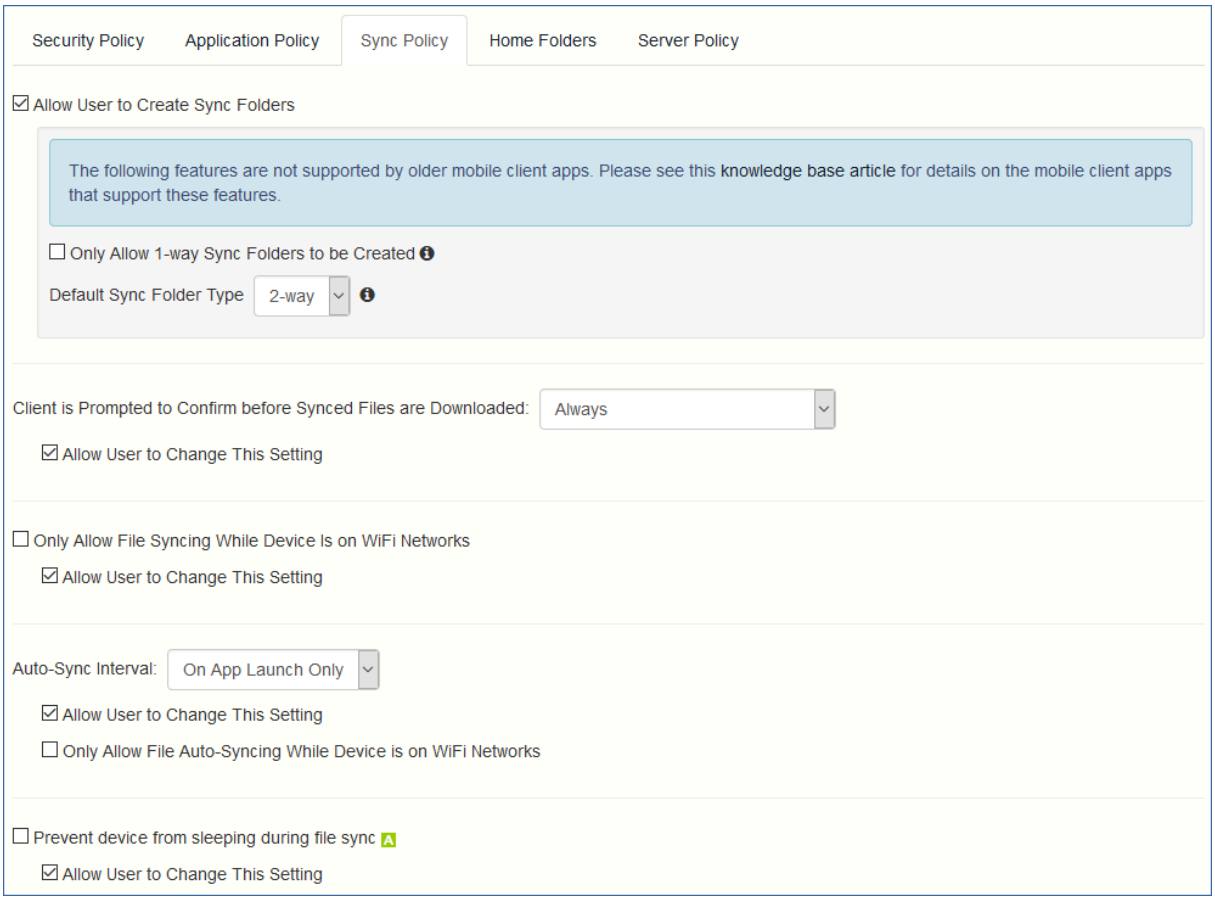
- **Editing & Creation of Office files** - If this option is disabled, users will not be allowed to edit documents using the integrated SmartOffice editor.
  - **Editing of password protected files** - If this option is disabled, users will not be allowed to edit password protected files.
- **Editing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

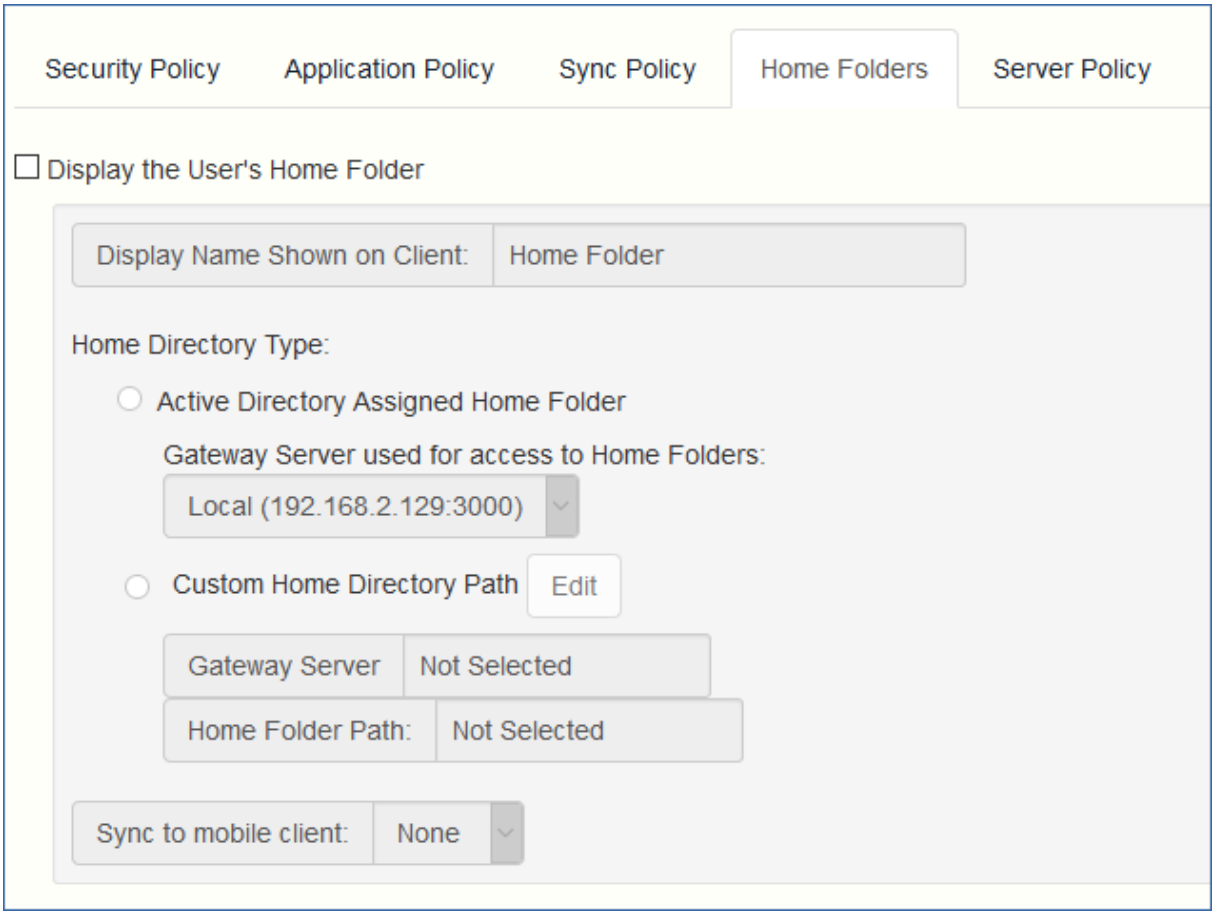


- **Allow User to Create Sync Folders -** Allows the user to create their own sync folders.
    - **Only Allow 1-way Sync Folders to be Created** - Users will be able to create only 1-way sync folders.
    - **Default Sync Folder Type** - Sets either 1-way or 2-way as the default Sync folder type.
- **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**- 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**- 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 blacklists 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, Acronis Cyber Files mobile for Good Dynamics** (iOS) and **Acronis Cyber Files mobile with Mobile Iron AppConenct** 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 of the features of the iOS client are not yet supported, so the related policies do not apply. In the case of Good Dynamics, a few of the standard Acronis Cyber Files mobile policy features are deferred to the Good Dynamics system and the Good Dynamics policy set that you have configured on your Good Control server. 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 Good, Android and MobileIron logos for more details on the individual policy exceptions.

5.2.4 Creating a Blocked Path list

You can create blacklists 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 blacklist 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 blacklisted. 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 blacklist 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.

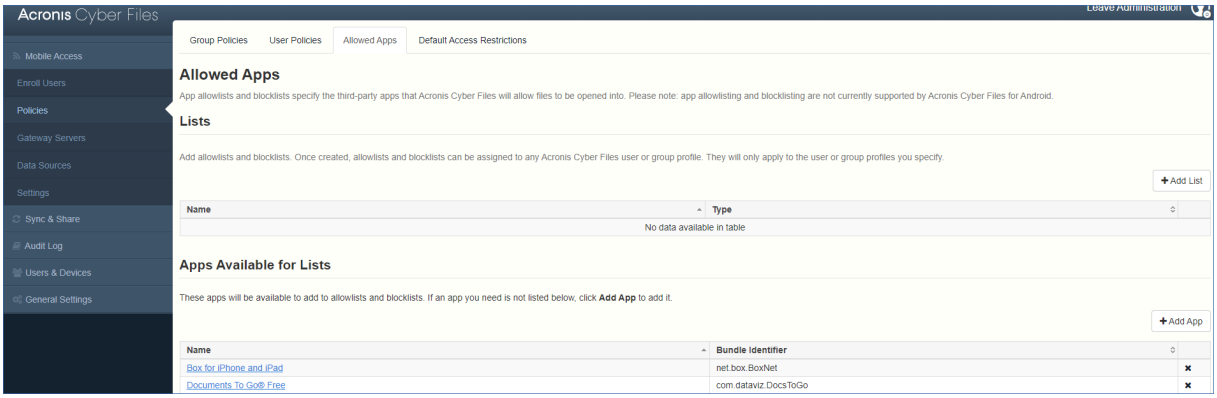
> **Note**
> You must perform this step for each User/Group policy that you want to assign the blacklist to.

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.

5.2.5 Allowed Apps



Acronis Cyber Files Client Management allows you to create whitelists or blacklists 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.

Whitelists - 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.

Blacklists - 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 whilelist or blacklist is not included, you will need to add it to the list.

Note
App whitelisting and blacklisting are not currently supported by the Acronis Cyber Files mobile for Android.

Lists

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

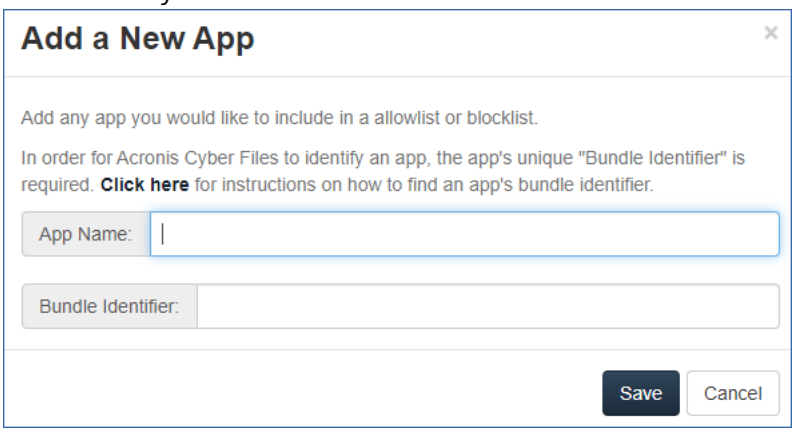
- **Name** - Shows the name of the list set by the administrator.
- **Type** - Shows the type of the list (whitelist/blacklist)
- **Add List** - Opens the Add a New Whitelist or Blacklist menu.

Adding Apps Available for Lists

To add an app to be included on a whitelist or blacklist:

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 white or blacklisted.
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.



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

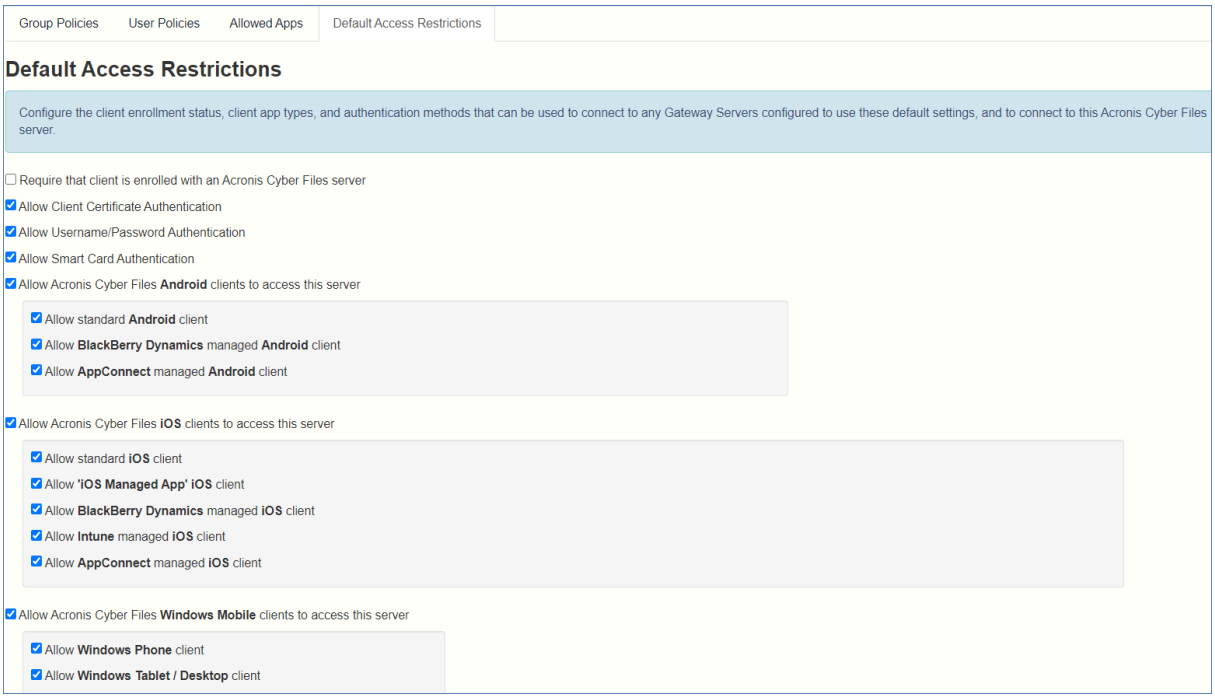
If you sync your device with iTunes and the app you desire is either on your device, or was downloaded through iTunes, it will exist on your computer's hard drive. You can locate it on your hard drive and look inside the app to find the **bundle identifier**.

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**

5.2.6 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.



- 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 Blackberry Dynamics managed Android clients** – If you select this option, this Acronis Cyber Files server will allow users using the Android Acronis Cyber Files mobile BlackBerry Dynamics managed client to connect. If you do not want to allow users with the Android Acronis Cyber Files mobile app BlackBerry Dynamics client 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 Blackberry Dynamics managed iOS clients** – If you select this option, this Acronis Cyber Files server will allow users using the iOS Acronis Cyber Files mobile BlackBerry Dynamics managed client to connect. If you do not want to allow users with the iOS Acronis Cyber Files mobile BlackBerry Dynamics client 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.

5.3 On-boarding Mobile Devices

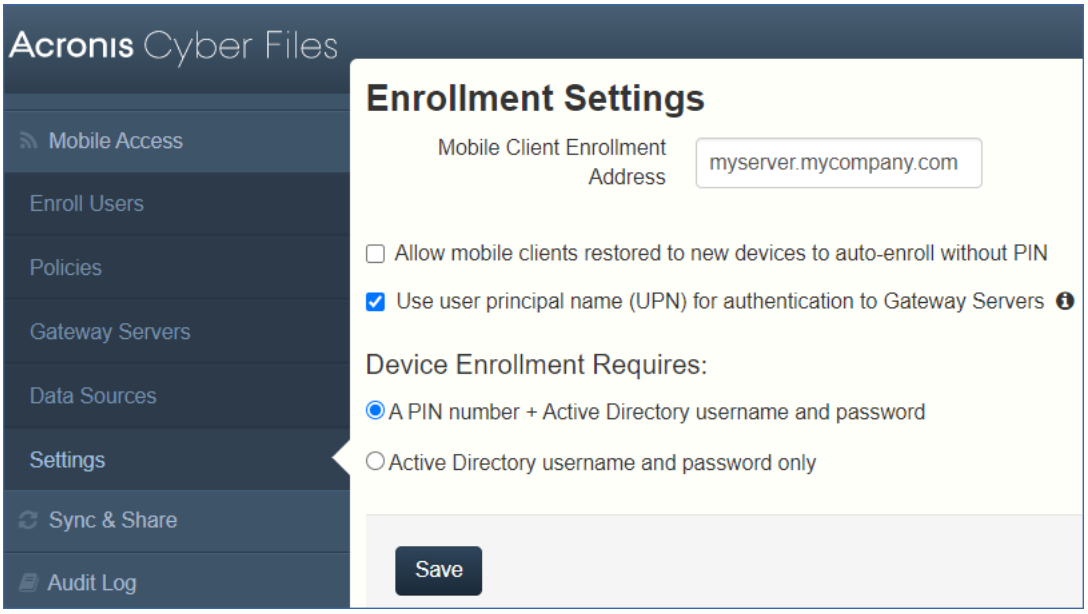
To get started with the Acronis Cyber Files mobile app, users need to install the app through their respective App Store - iTunes or Google Play. If your company is using client management, the users also need to enroll the Acronis Cyber Files mobile app on their device with the Acronis Cyber Files

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

5.3.1 Server-side Management Enrollment Process



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 -

Use user principal name (UPN) for authentication to Gateway Servers - will use username@domain.com for authentication when enabled instead of domain/username.

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:

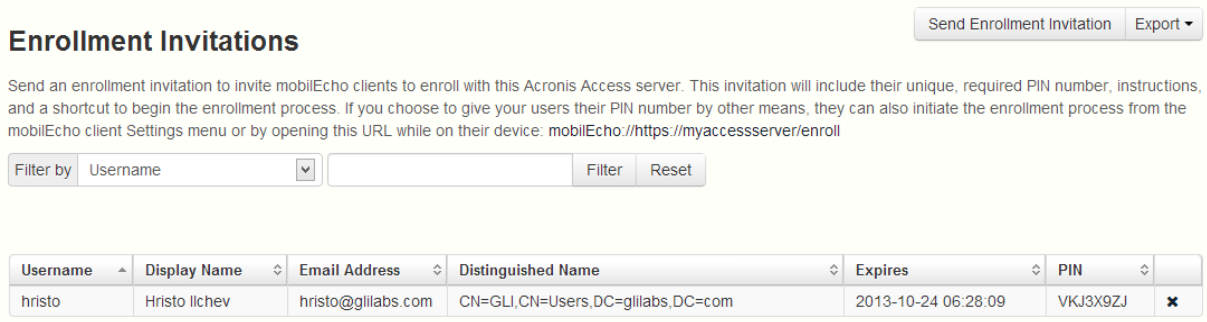
- **PIN number + Active Directory username and password** - In order to activate their Acronis Cyber Files app and gain access to Acronis Cyber Files servers, a user is required to enter an expiring, one-time use PIN number and a valid Active Directory username and password. This option ensures that 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.



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. Press 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. If you are using Acronis Cyber Files for Good Dynamics, you can select that option and your users will only be directed to download the Good Dynamics version of the Acronis Cyber Files mobile.
10. Press 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.

Inviting users previously enrolled by mobilEcho 4.5 or earlier

mobilEcho 2.X did not require a PIN number to enroll a client in the Client Management system. There are two options for migrating mobilEcho 2.X clients to the Acronis Cyber Files management system. By default, mobilEcho servers that are upgraded from 2.X allow clients previously managed by the 2.X server to auto-enroll and appear in the Acronis Cyber Files **Devices** list without having to enter a PIN number. If you would like to ensure that all devices accessing the system have enrolled with a PIN number, you can disable this setting. In that case, if the user doesn't have **User can remove Mobile Client from management** privileges, the user will need to delete Acronis Cyber Files from their device and reinstall a new copy from the App Store before they can enroll using a PIN number.

Also note that when this auto-enroll setting is enabled, it will be possible to do an iTunes backup of a device running a managed version of mobilEcho 2.X or 3.0, restore that backup to a new device, and as long as the user has the active directory username and password for the associated account, that new device can be automatically enrolled in client management without a PIN number.

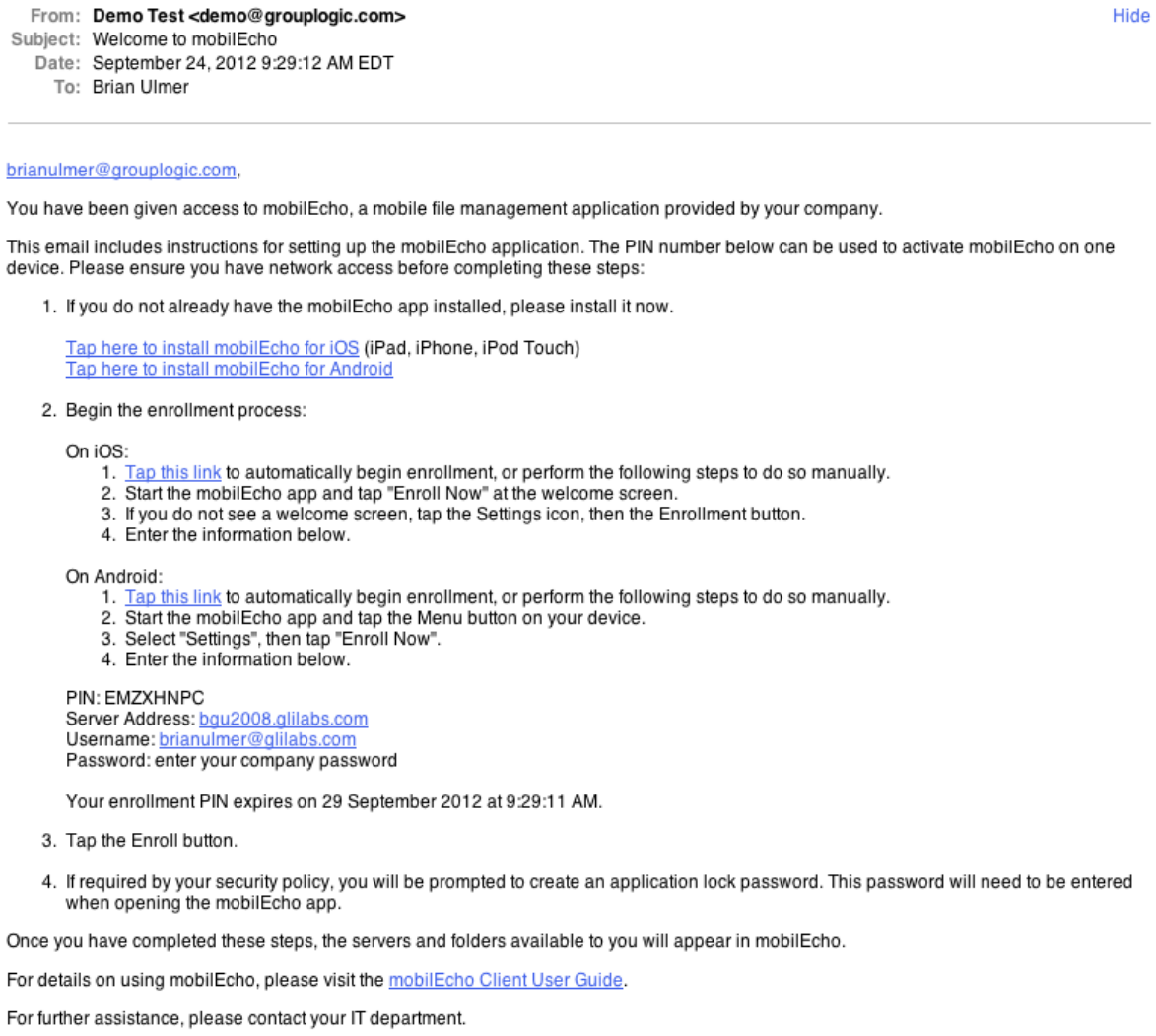
It is recommended that you disable the auto-enroll setting after your previously managed clients have all accessed the management server for the first time. They will appear in the Devices list when this happens.

To allow mobilEcho clients that were already enrolled in mobilEcho 2.X Client Management to automatically enroll after your mobilEcho Client Management server is upgraded to the Acronis Cyber Files Server, enable the **Allow mobilEcho clients previously managed by 2.X servers and managed mobilEcho clients restored to new devices to auto-enroll without PIN** setting.

5.3.2 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.



From: **Demo Test <demo@grouplogic.com>** Hide
Subject: Welcome to mobilEcho
Date: September 24, 2012 9:29:12 AM EDT
To: Brian Ulmer

brianulmer@grouplogic.com,

You have been given access to mobilEcho, a mobile file management application provided by your company.

This email includes instructions for setting up the mobilEcho application. The PIN number below can be used to activate mobilEcho on one device. Please ensure you have network access before completing these steps:

1. If you do not already have the mobilEcho app installed, please install it now.

   Tap here to install mobilEcho for iOS (iPad, iPhone, iPod Touch)
   Tap here to install mobilEcho for Android

2. Begin the enrollment process:

   On iOS:
   1. Tap this link to automatically begin enrollment, or perform the following steps to do so manually.
   2. Start the mobilEcho app and tap "Enroll Now" at the welcome screen.
   3. If you do not see a welcome screen, tap the Settings icon, then the Enrollment button.
   4. Enter the information below.

   On Android:
   1. Tap this link to automatically begin enrollment, or perform the following steps to do so manually.
   2. Start the mobilEcho app and tap the Menu button on your device.
   3. Select "Settings", then tap "Enroll Now".
   4. Enter the information below.

   PIN: EMZXHNPC
   Server Address: bgu2008.glilabs.com
   Username: brianulmer@glilabs.com
   Password: enter your company password

   Your enrollment PIN expires on 29 September 2012 at 9:29:11 AM.

3. Tap the Enroll button.

4. If required by your security policy, you will be prompted to create an application lock password. This password will need to be entered when opening the mobilEcho app.

Once you have completed these steps, the servers and folders available to you will appear in mobilEcho.

For details on using mobilEcho, please visit the mobilEcho Client User Guide.

For further assistance, please contact your IT department.

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.
8. 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.
8. 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 you settings might look slightly different.

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

5.4 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 new Gateway Servers using the **Add new Gateway Server** button. From the actions menu for each Gateway Server the 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, or remove the Gateway Server.

5.5 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.

5.5.1 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.

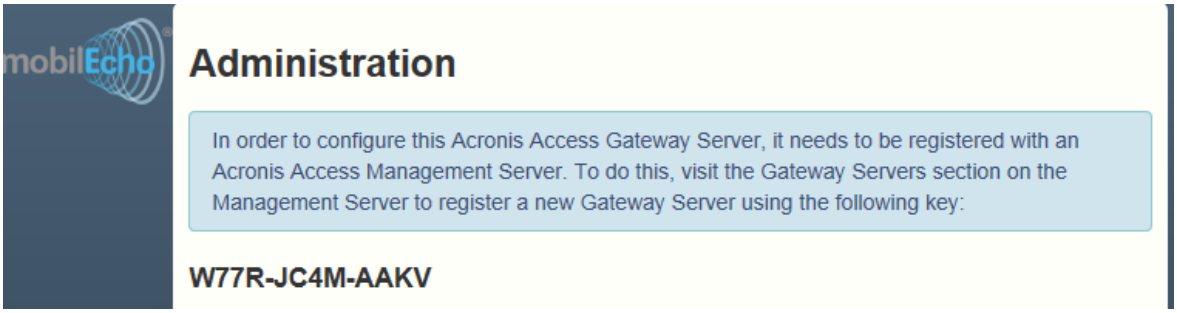
5.5.2 Registering new Gateway Servers

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**.



4. Open the Acronis Cyber Files Web Interface.
5. Open the **Mobile Access** tab.
6. Open the **Gateway Servers** page.

7. Press the **Add New Gateway Server** button.

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.

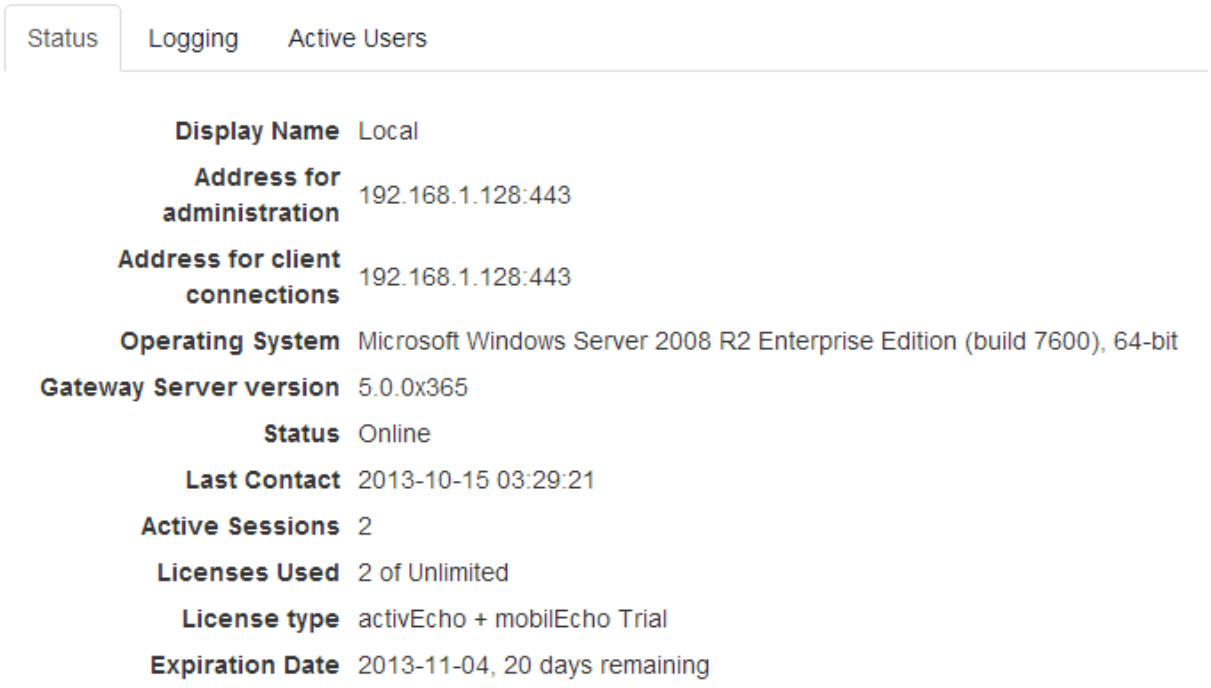
10. Enter the **Administration Key**.
11. If required, allow connections with self-signed certificates to this gateway by enabling **Allow connections from Acronis Cyber Files servers using self-signed certificates**.
12. Press the **Save** button.

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.

5.5.3 Server Details

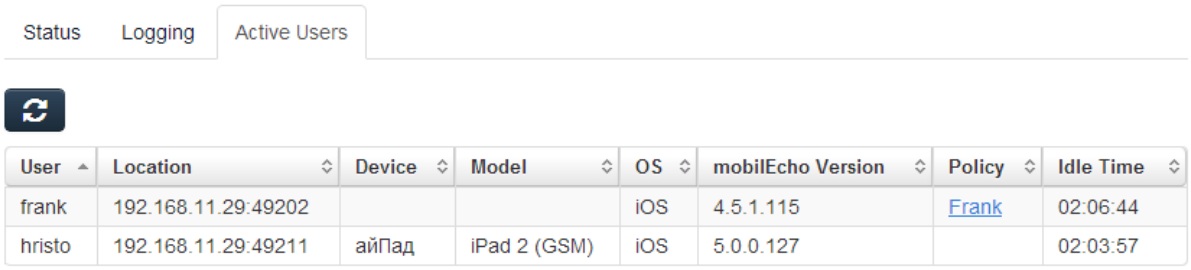
Opening the **Details** page of a Gateway Server gives you a lot of useful information about that specific server and its users.

Status



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



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.

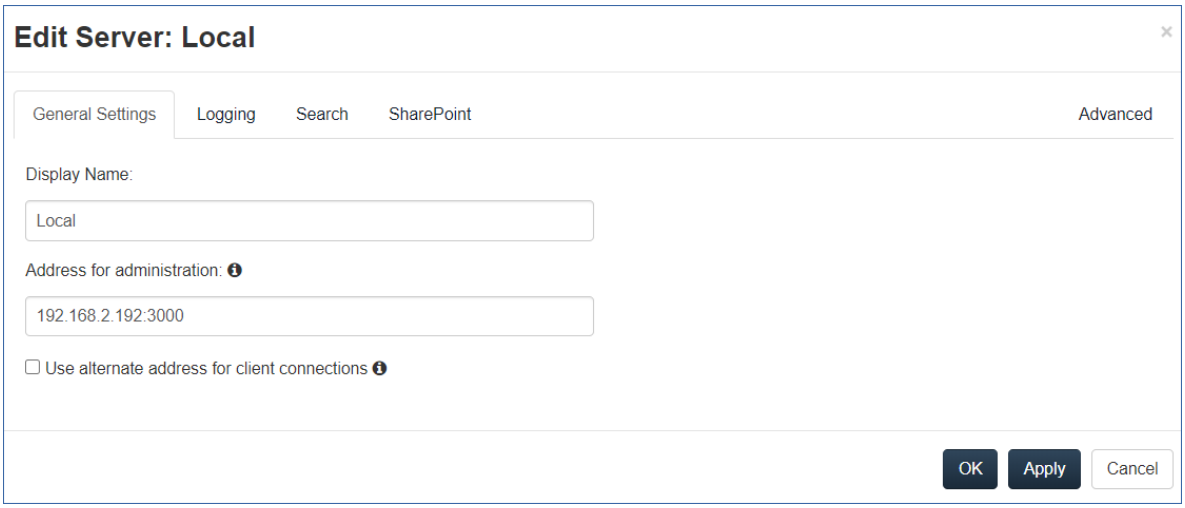
- **Policy** - Shows the policy for the account used by the device.
- **Idle Time** - Shows the time the user has spent connected to the gateway.

5.5.4 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

- 

- **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.

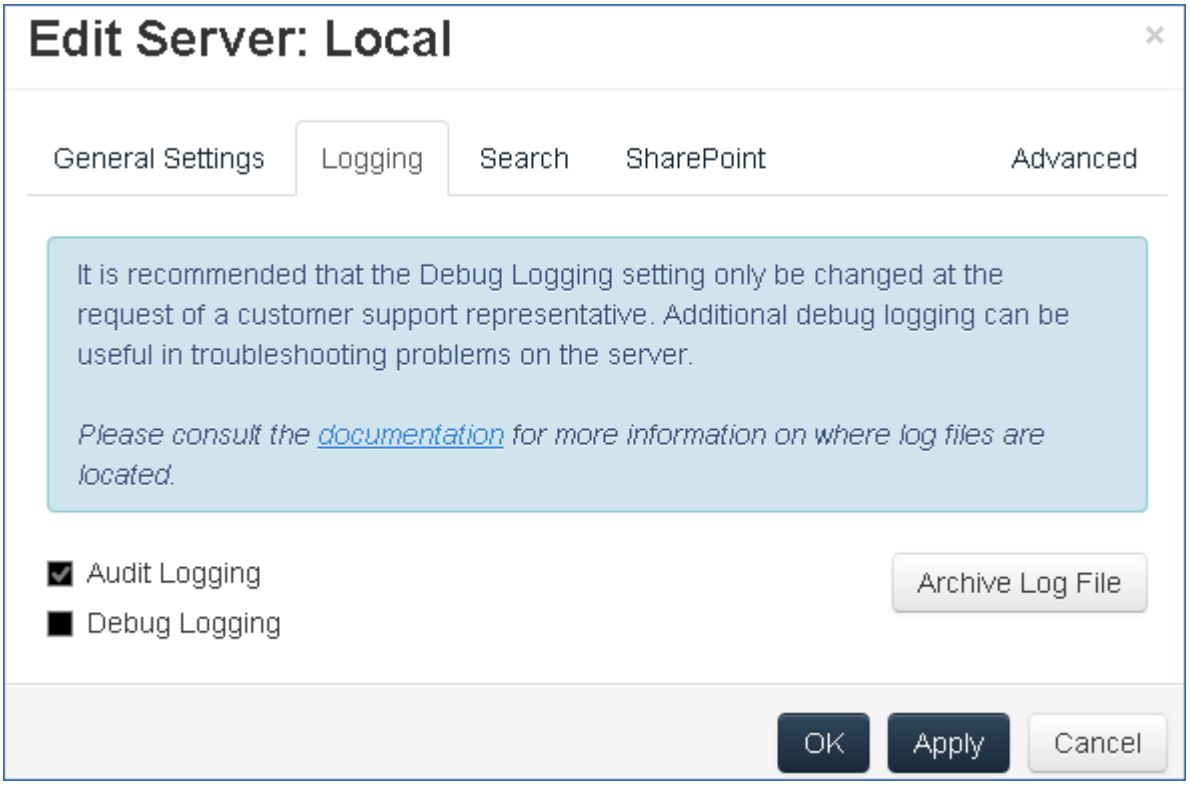
> **Note**
> This setting should be used only in specific configurations where connections to your Gateway Servers pass through a load-balancer or any kind of proxy (e.g. BlackBerry Dynamics, MobileIron and etc.). Regular deployments should not enable it.

  - **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.



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 arrow next to the **Details** button and select **Edit**.
7. In the **Logging** section check **Audit Logging**.
8. Press 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\Files Advanced\Gateway Server\Logs\AcronisFilesAdvancedGateway

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 arrow next to the **Details** button and select **Edit**.
7. In the **Logging** section check **Debug Logging**.
8. Press 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.

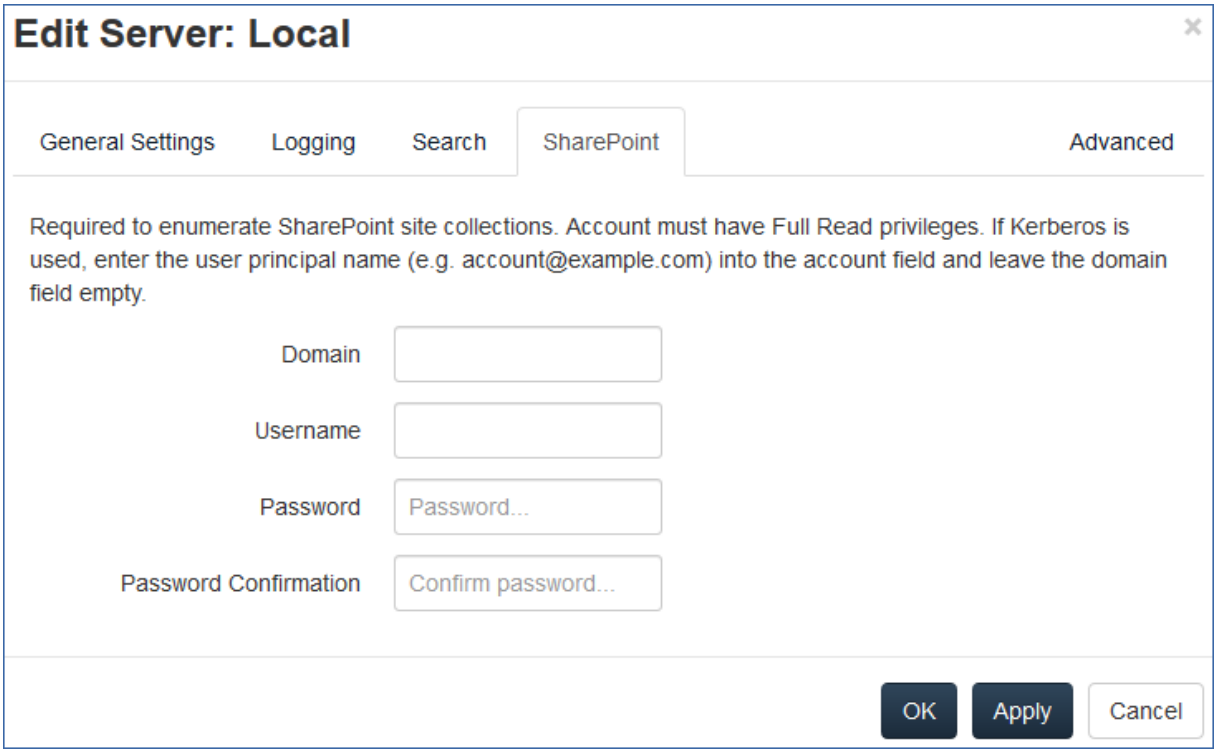
Note
The Data Source's volume path must be a hostname or a fully qualified name in order to use content search on Windows Reshares. IP addresses are not supported by Windows Search.

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



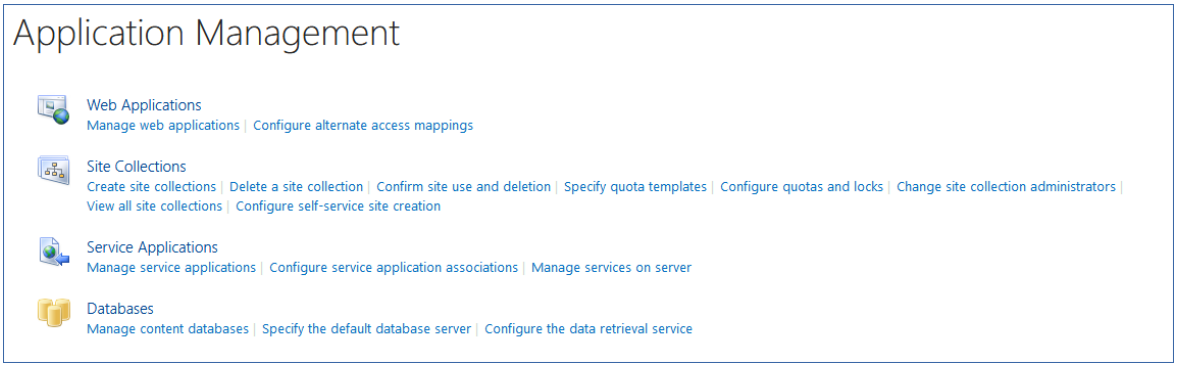
Entering these credentials is optional for general SharePoint support, but required to enumerate site collections. For example, say you have two site collections:

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

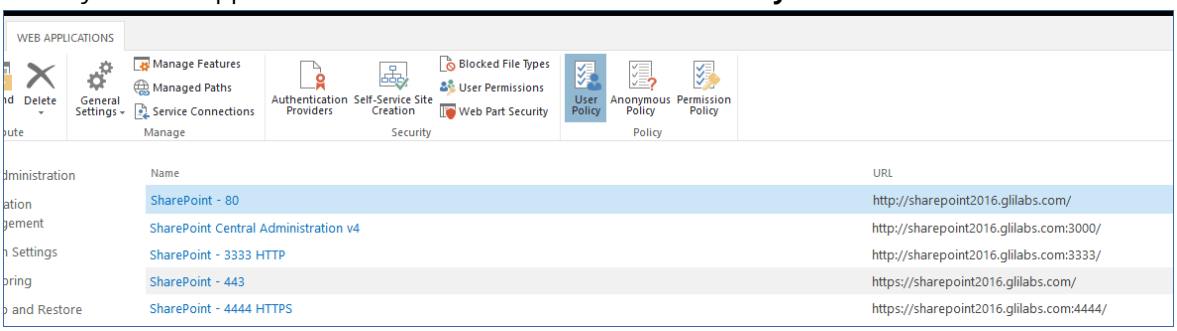
Without entering credentials, if you create a volume pointing to **http://sharepoint.example.com**, you will not see a folder called **SeparateCollection** when enumerating the volume. The account needs to have **Full Read** access to the web application.

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

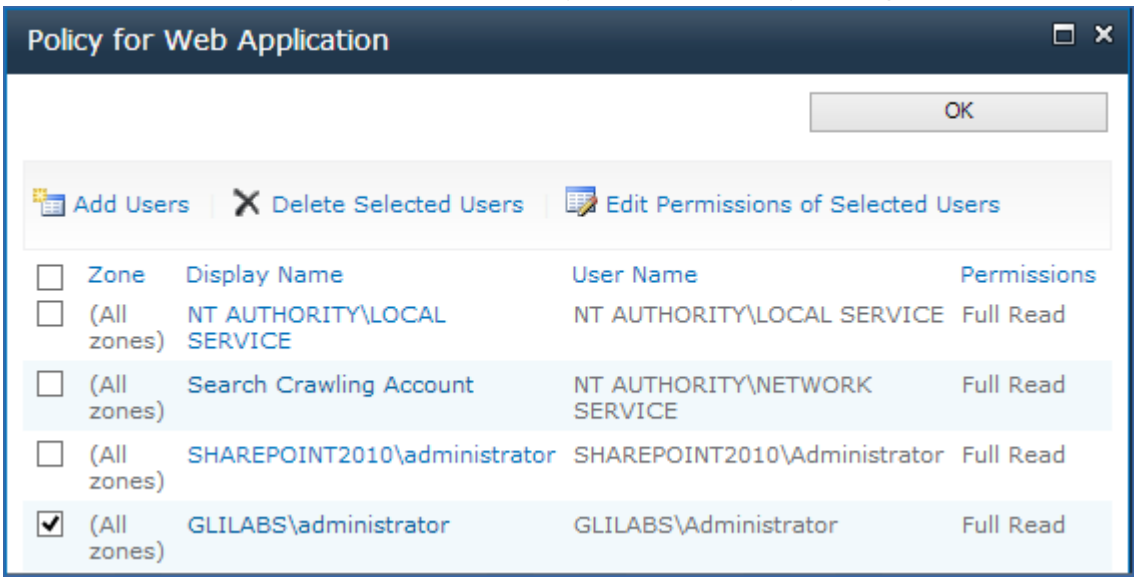
1. Open the **SharePoint Central Administration**.
2. Click on **Application Management**.



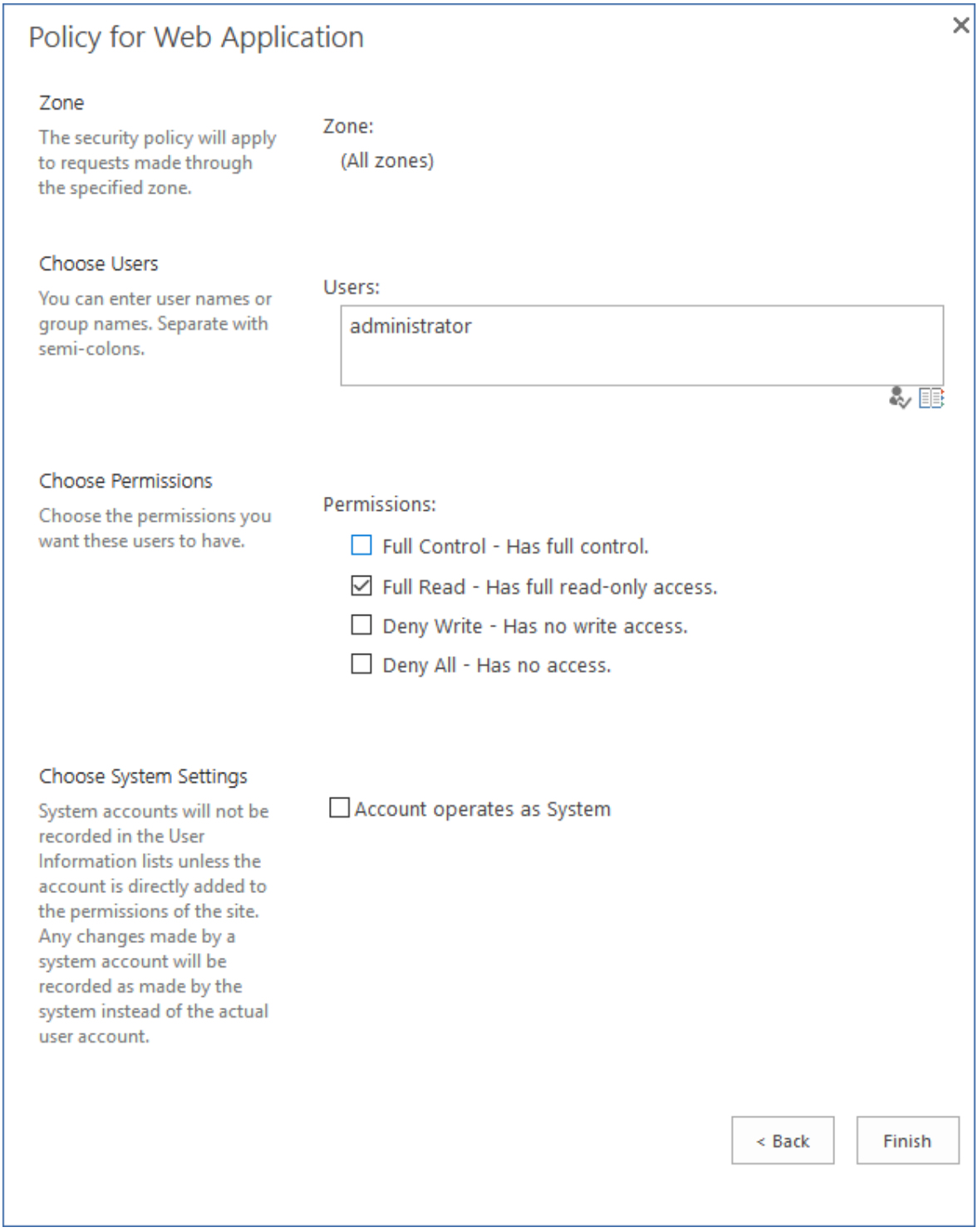
3. Under **Web Applications** click on **Manage web applications**.
4. Select your web application from the list and click on **User Policy**.



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**.

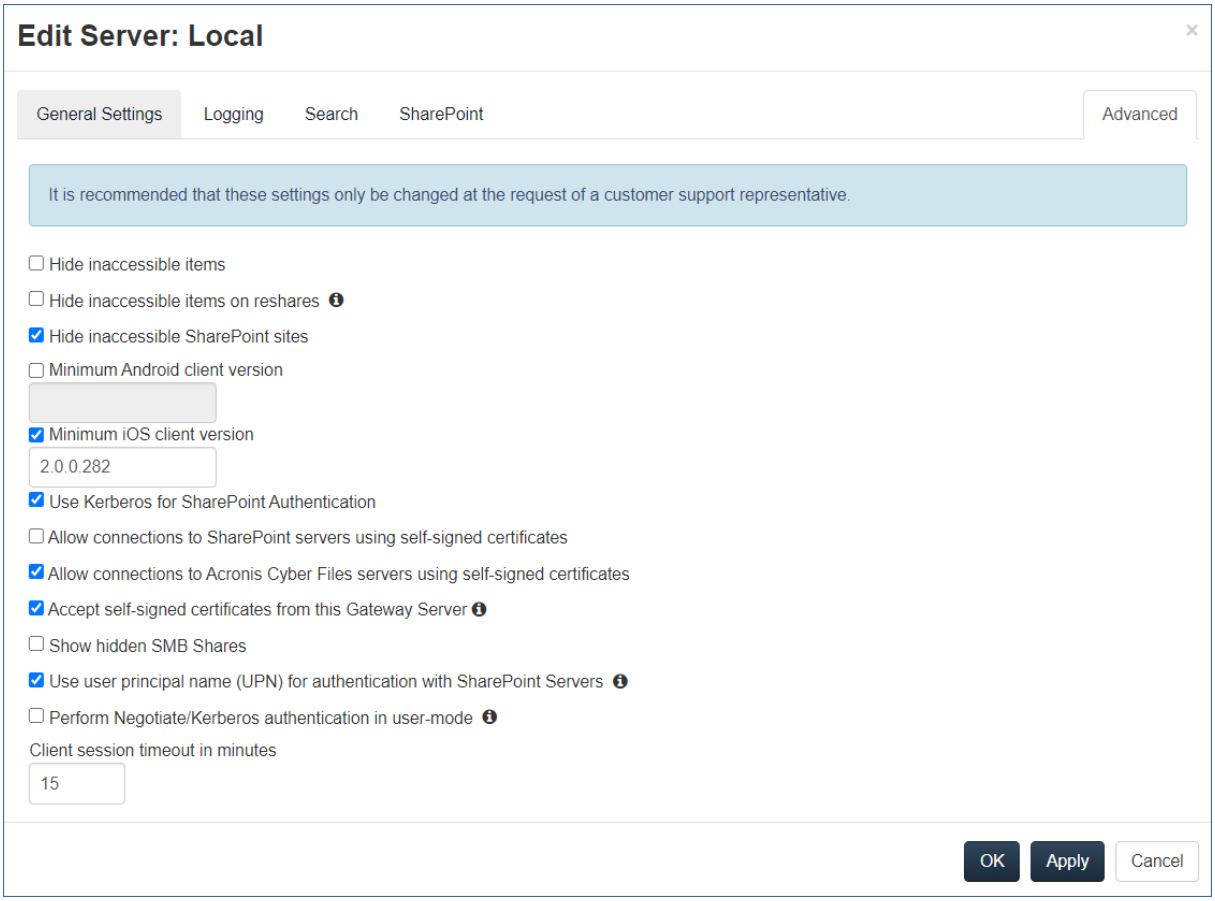


6. From the **Permission Policy** Levels section, select the checkbox for **Full Read - Has Full read-only access**.



7. Press the **Save** button.

Advanced Settings



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.).

5.5.5 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

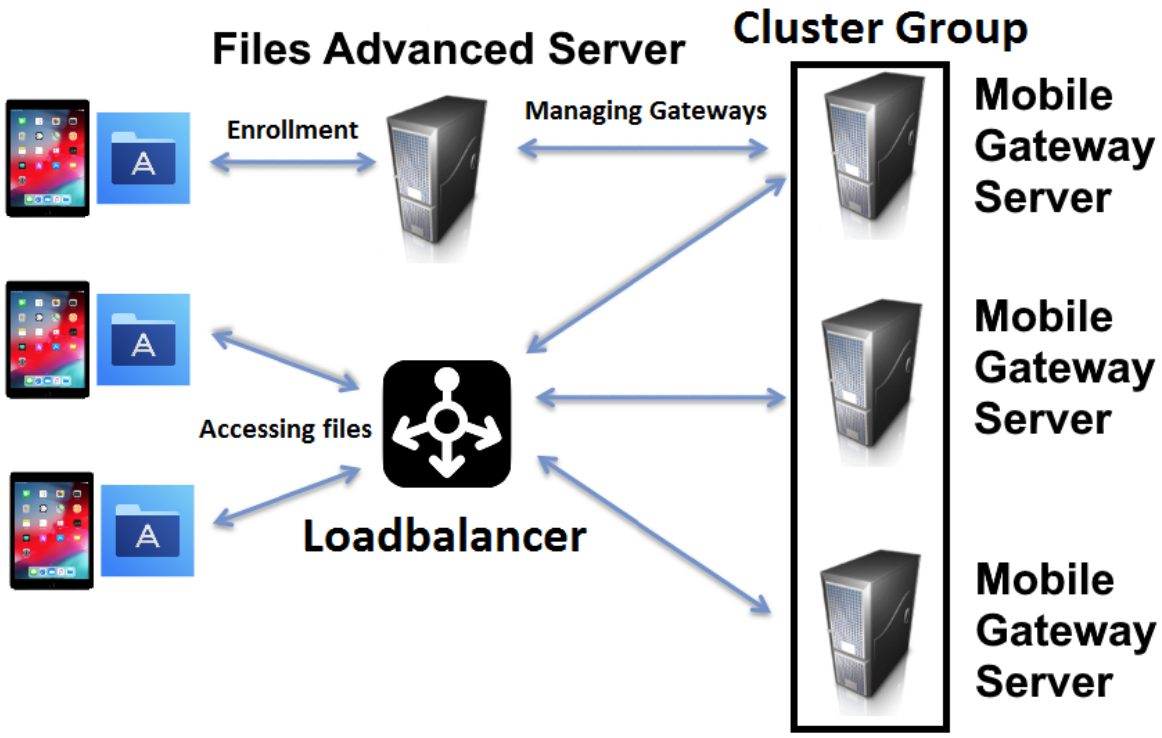
1. Navigate to the **Mobile Access** -> **Gateway Servers** tab.
2. Click on the arrow next to **Details** for the desired server.
3. Select **Access Restrictions**.
4. Open the **Use Custom settings** tab.
5. Select the specific access restrictions you want for this Gateway Server.
6. Press **Apply**.

5.5.6 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. Press 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. Press **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. Press the **Actions** button and select **Become Group Master**.

5.6 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.

5.6.1 Access to SharePoint 2007, 2010, 2013, 2016 and 365 content

Acronis Cyber Files can provide access to files residing in document libraries on SharePoint 2007, 2010, 2013, 2016 and 365 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.

Claims based authentication involves authenticating with an authentication server, obtaining an authentication token, and providing that token to the SharePoint server, rather than authenticating with the SharePoint server directly. Acronis Cyber Files supports claims based authentication to Office 365 SharePoint sites. To authenticate, the gateway server first contacts Microsoft Online to determine the location of the authentication server. This server may be hosted by Microsoft Online, or may be within the corporate network (via Active Directory Federated Services). Once authentication is complete and an binary security token is obtained, this token is sent to the SharePoint server, which returns an authentication cookie. This cookie is then provided to SharePoint in lieu of other user credentials.

5.6.2 **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.

5.6.3 **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.

5.6.4 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:

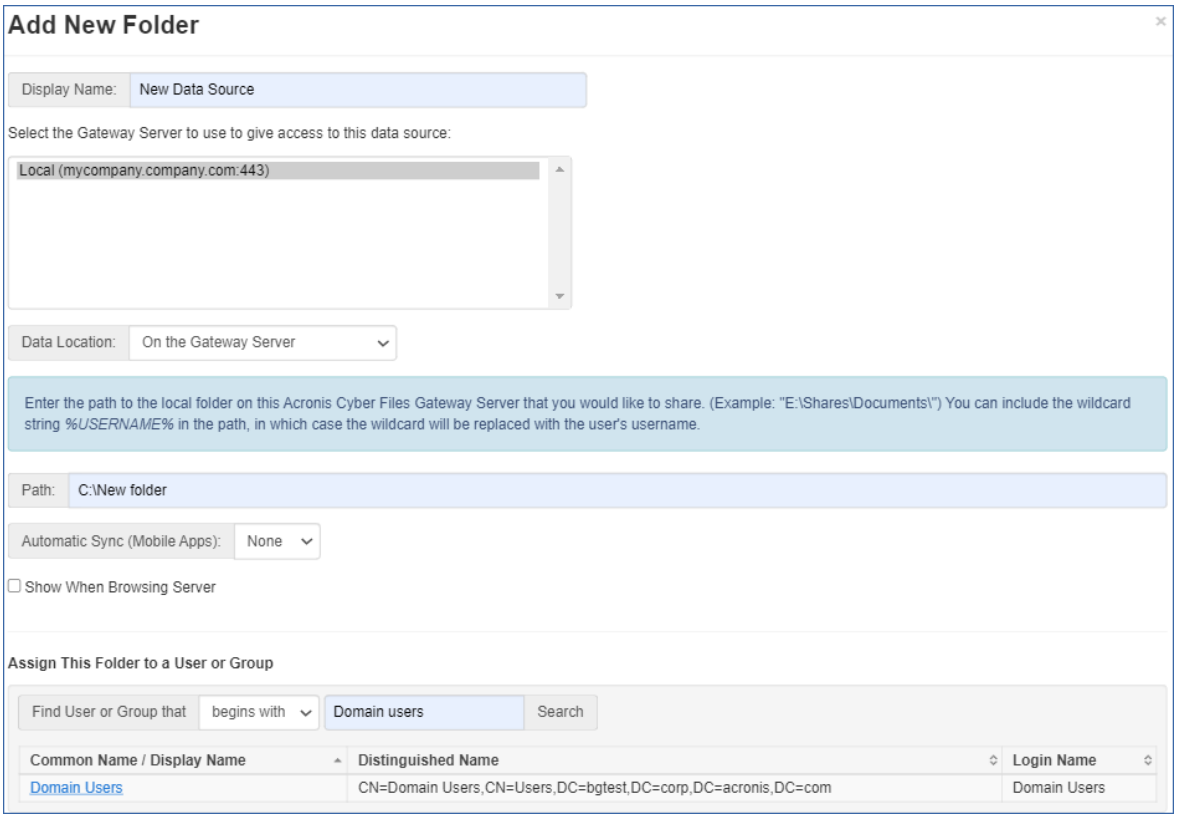
Note
This setting does not affect the desktop client.

- **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. Press the **Add New Folder** button.



6. Enter a display name for the folder.
7. Select the Gateway Server which 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.

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. Press 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 you enter the address of your SharePoint site or subsite and for the Document Library Name field you 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.
- You Active Directory must be either linked with Office 365, use Federated AD Services or must 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. Enter the location of your OneDrive for Business main site, followed by the path for a personal folder, with the **%USERNAME%** wildcard.
   e.g. https://mycompany.sharepoint.com/personal/%USERNAME%
9. Press the **Save** button.

Active Directory integration

Note
Managing Active Directory or Microsoft Azure is **not** a function of Acronis Cyber Files! If you are experiencing issues with Azure or Office 365, please contact **Microsoft Support.**

Office 365 uses cloud-based user identity management from the Azure Active Directory Service to manage users. If you are already using Azure AD Services, you only have to create the Data Source.

If not, you can integrate your on-premises Active Directory with Azure AD by synchronizing your on-premises environment with Office 365.

A third option would be to manually re-create the necessary accounts in the Offfice 365 admin panel, but this method is only recommended if you need to use very few accounts.

5.6.5 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.

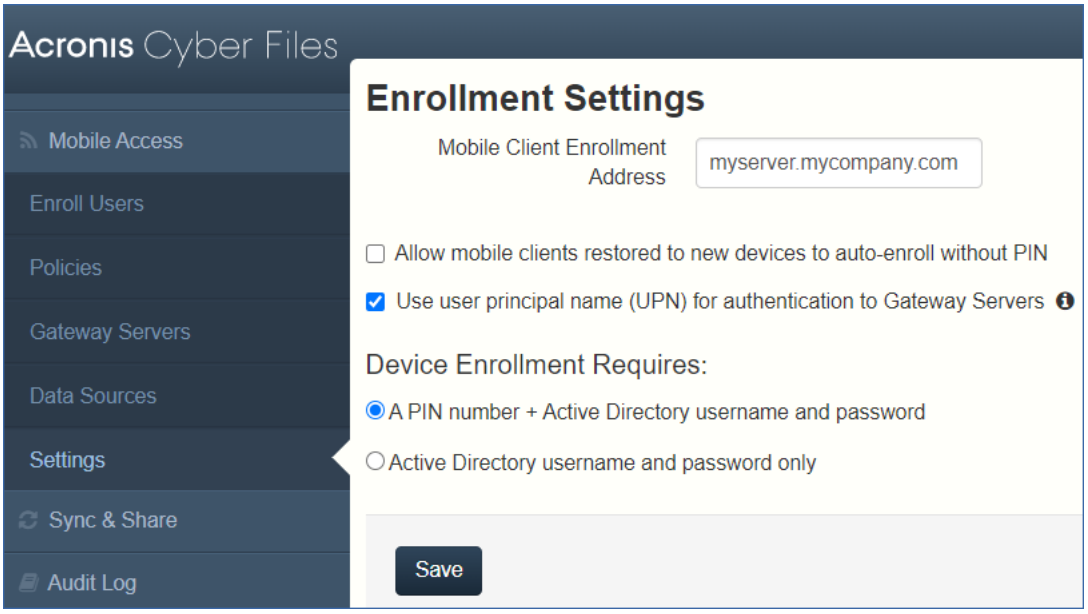
5.6.6 Gateway Servers Visible on Clients

Gateway Servers can be assigned to User or Group policies and can be used as Data Sources. This page displays all Gateway Servers displayed on the user's Acronis Cyber Files mobile app and if those Gateway Servers are assigned to a User or Group policy. You can also edit these assignment here. When the Acronis Cyber Files mobile users browse into a Gateway Server, they will see the Data Sources which have the **Show When Browsing Gateway Server** option enabled.

To edit the current assignment of a server:

1. Press the **Edit** button on that server.
   - If you want to unassign this server from a user, press the **X** for that user.
   - If you want to assign a new User or Group to this server, find the User/Group name and press it.
2. Press the **Save** button.

5.7 Settings



5.7.1

5.7.2 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).

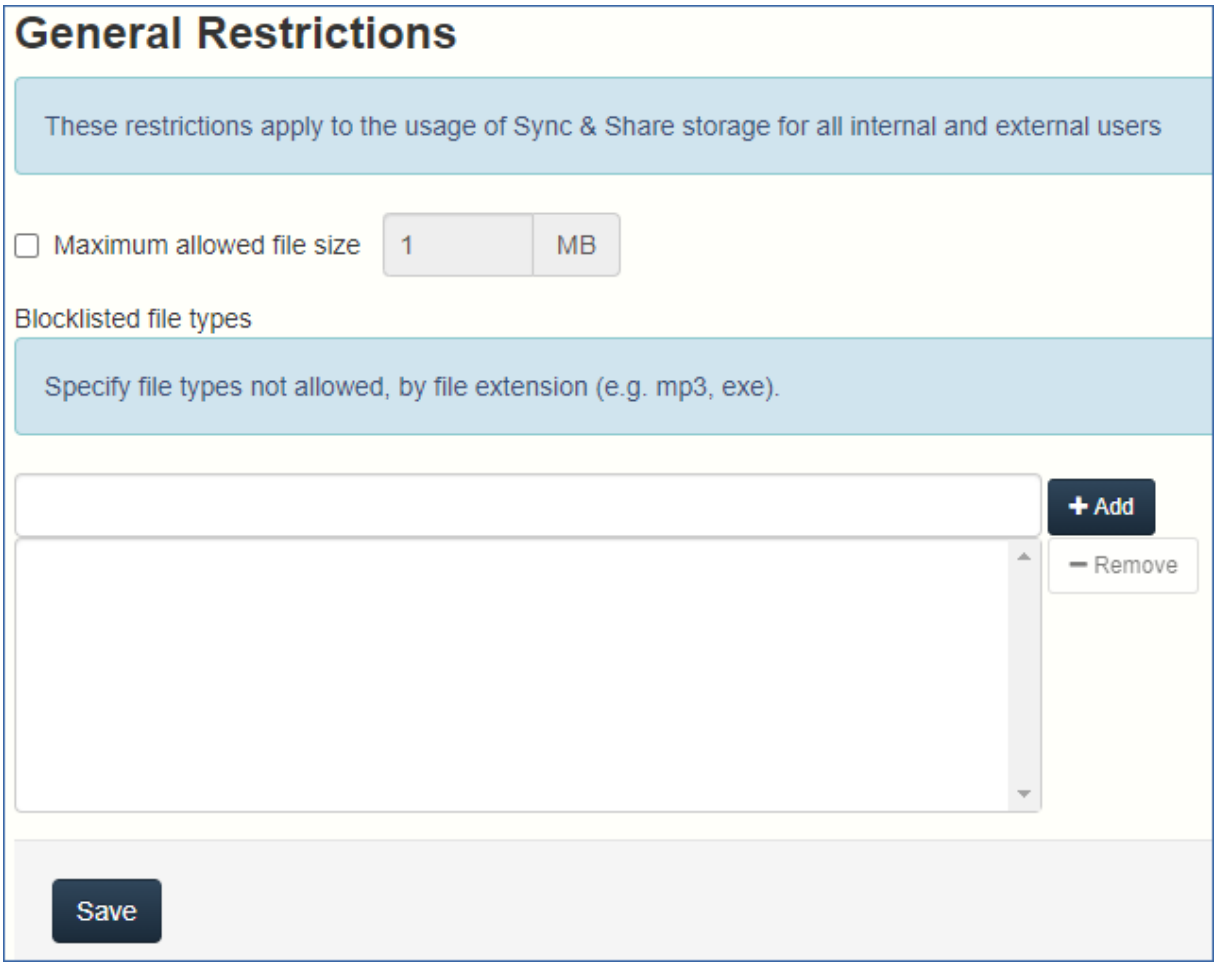
5.7.3 Device Enrollment Requires:

- **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.

6 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**.

6.1 General Restrictions



You can set basic restrictions such as blacklisting 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.

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

6.1.1 To set a file type blacklist:

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

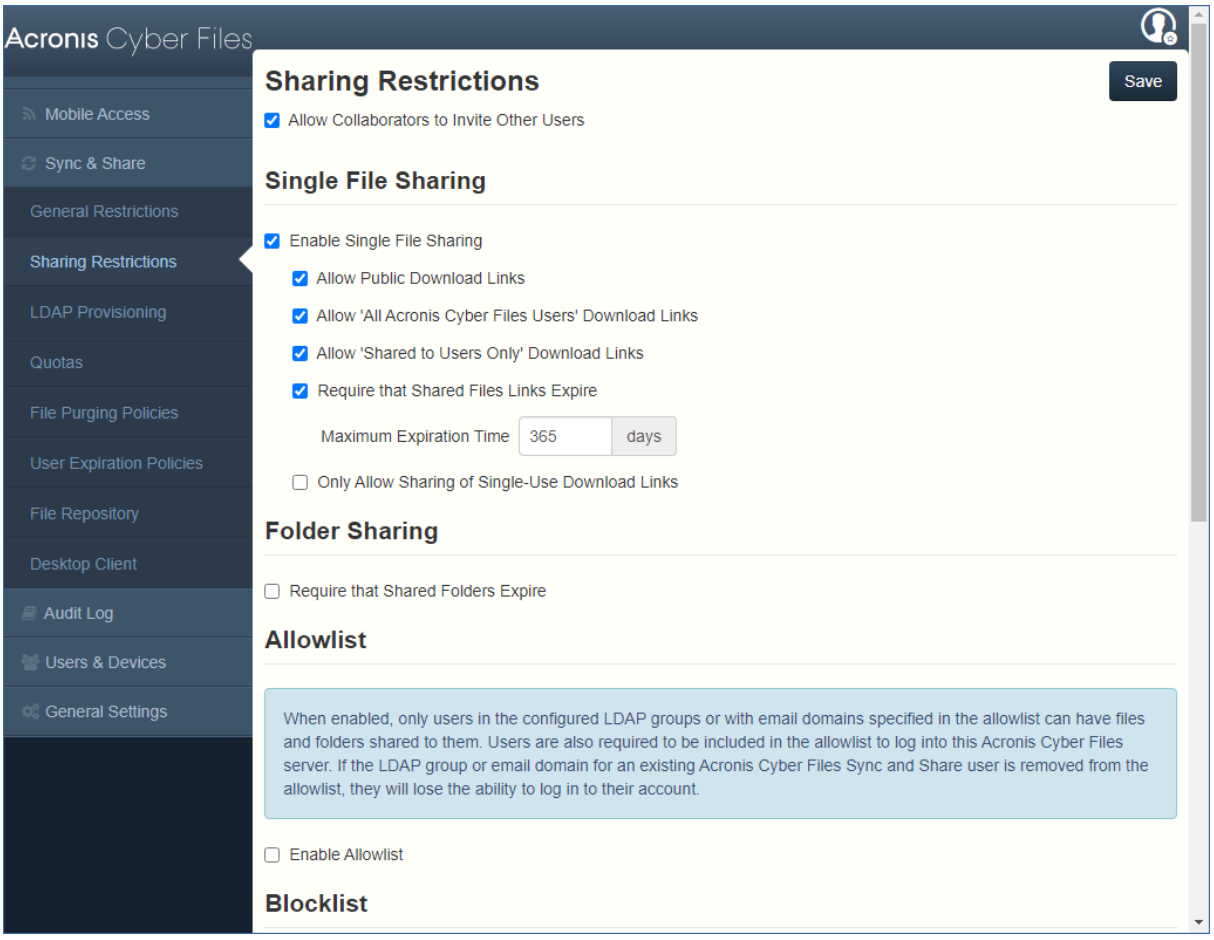
Note
Any preexisting files of that type will no longer be synced and will not be movable. You can only manually download them or remove them.

6.1.2 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. Press **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.

6.2 Sharing Restrictions



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.

6.2.1 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.

6.2.2 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.

6.2.3 Whitelist

If the whitelist 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.

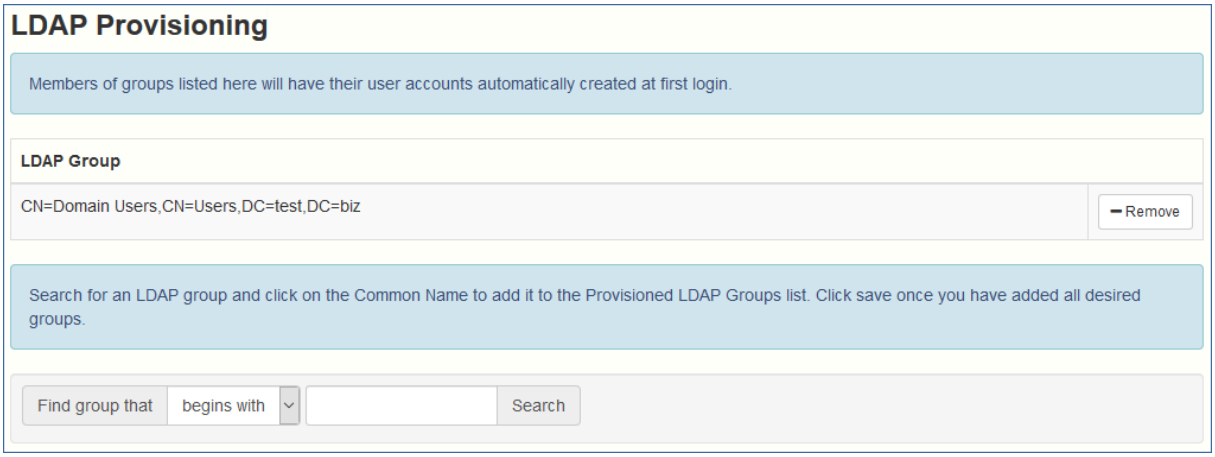
6.2.4 Blacklist

Users in LDAP groups or with the email domains (like example.com) specified in the blacklist will not be permitted to log into the system, even if they are in the whitelist. 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).

6.3 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.



6.3.1 **LDAP Group**

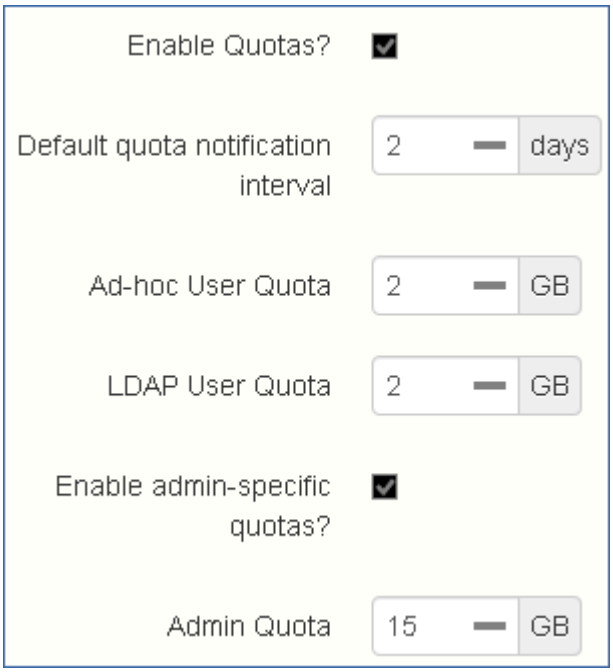
This is the list of currently selected groups.

- **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.

6.4 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?** - 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.

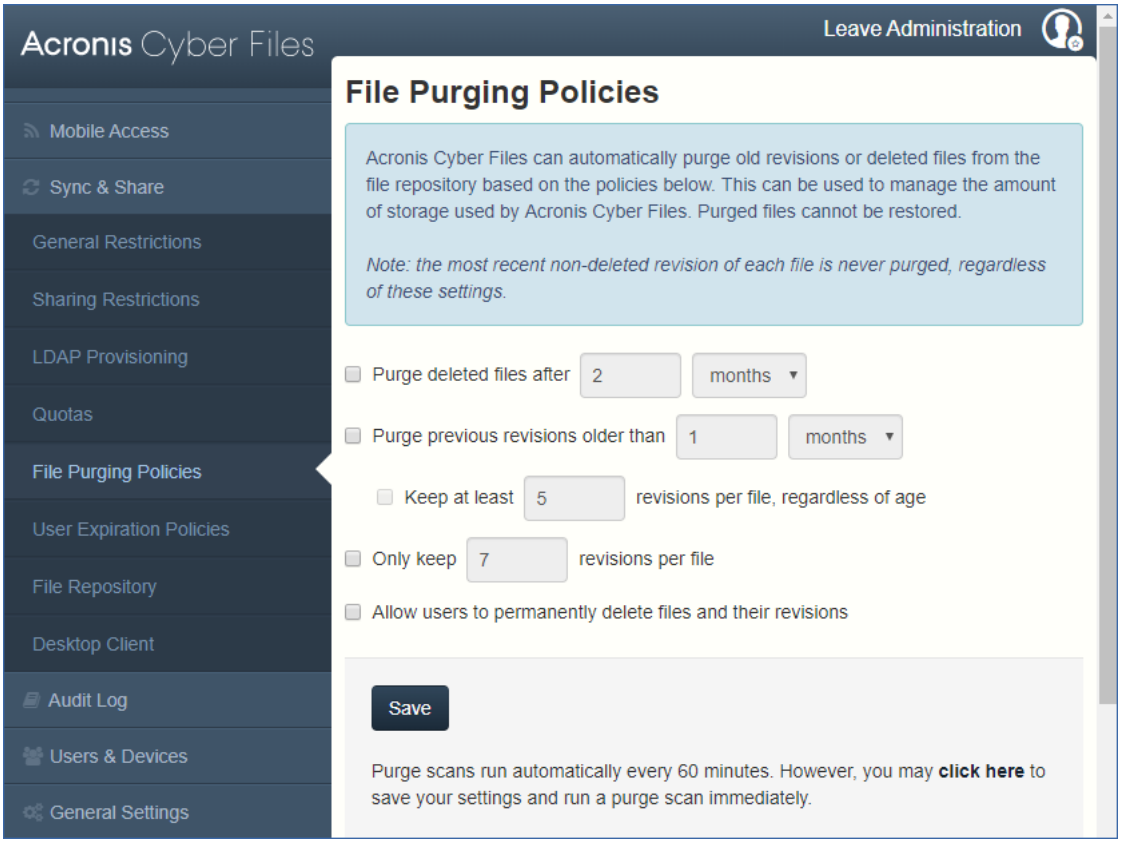
Note
Quotas can be set in megabytes by specifying a size that is smaller than 1 GB. **e.g. 0.5**, **0.3**, **0.9** and etc.

6.5 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.



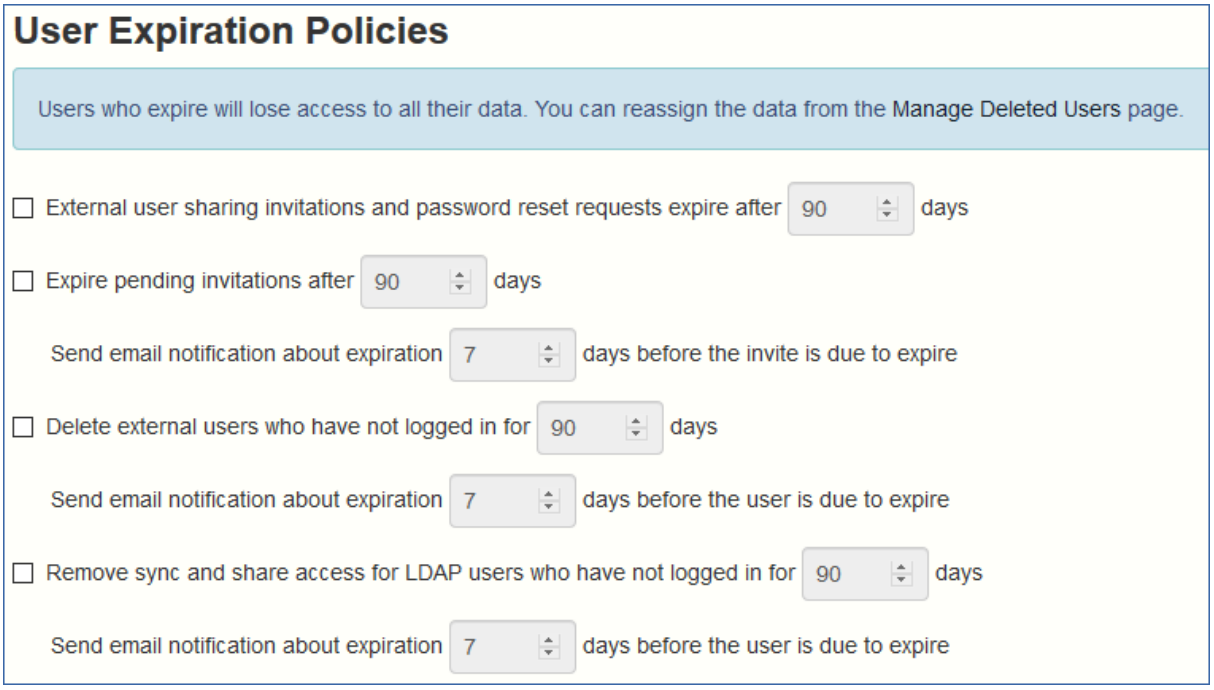
Note
The most recent non-deleted revision of each file is never purged, regardless of these settings.

- **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
Pushing the Save button will start a purge immediately, otherwise a regular scan runs every 60 minutes.

6.6 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 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.

6.7 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 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**.

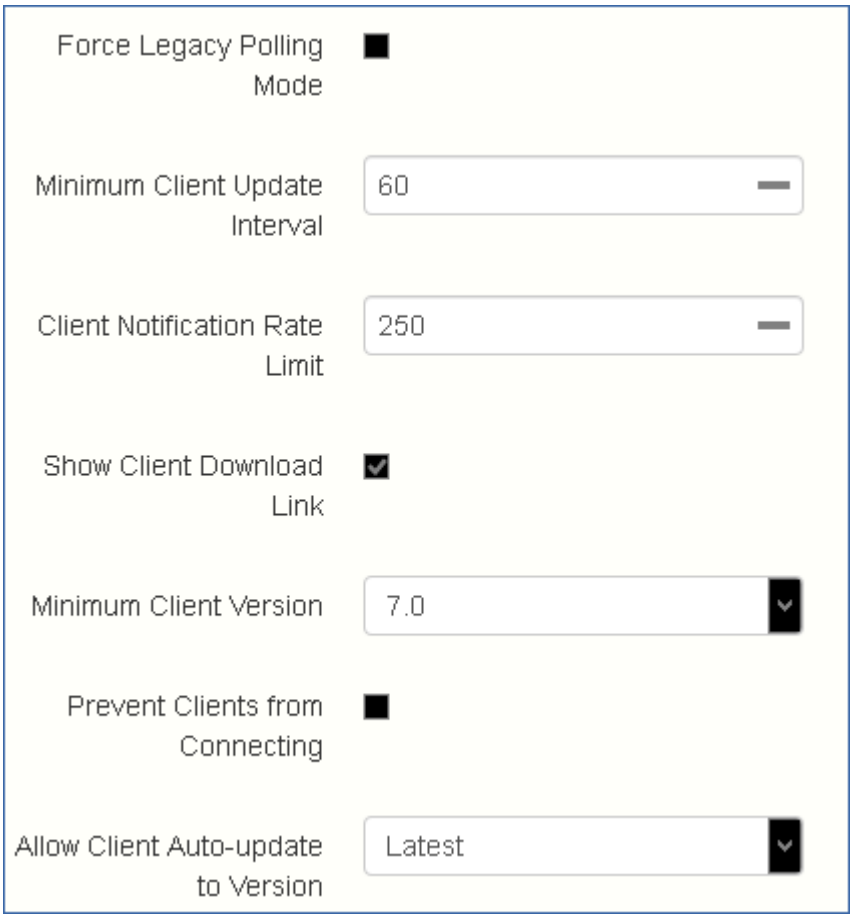
- **Note:** You can use the **Other S3-Compatible Storage** option with S3 storage providers not on this list, but we cannot guarantee that everything will work properly.

> **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.

- **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.

6.8 Acronis Cyber Files Client

These settings are for the Desktop client.



- **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.

7 Users&Devices

7.1 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.

7.1.1 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. Blackberry Dynamics Mobile application management status
7. Mobile device or desktop client status
8. Date and time of Acronis Cyber Files app enrollement with the Acronis Cyber Files Web Server
9. Date and time of the last contact between the Acronis Cyber Files app or desktop client with the Acronis Cyber Files Web Server
10. Name of the user policy applied
11. Notes

7.1.2 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.

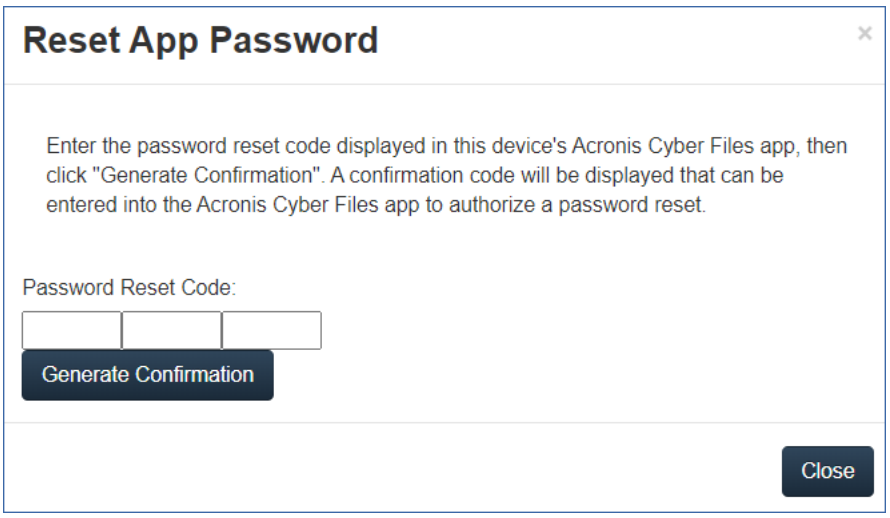
Resetting an application password

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.



7.1.3 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.

7.2 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.

7.2.1 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.

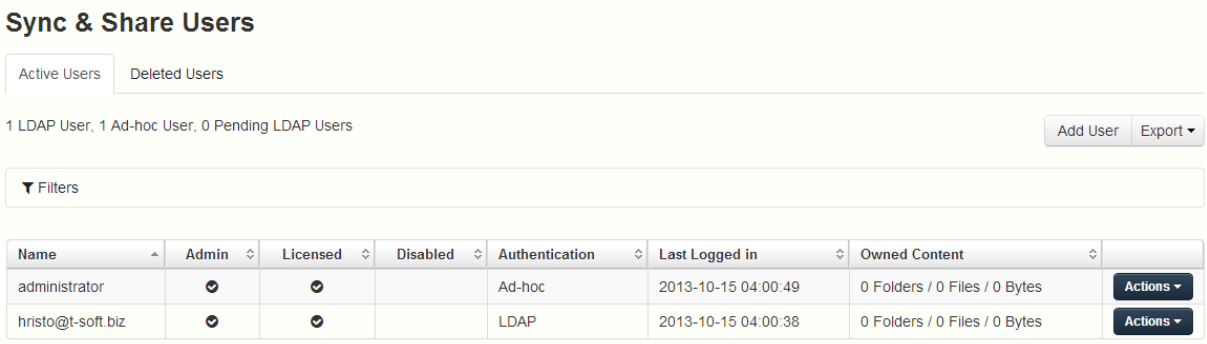
Users with internal accounts can create, upload, edit, and delete files and folders in their own Sync & Share space or in folders shared with them. They can also share their content with other people.

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.



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

7.2.2 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.

7.2.3 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.

7.2.4 Setting a custom quota

You can set a custom quota for any user with Sync & Share access.

Todo so:

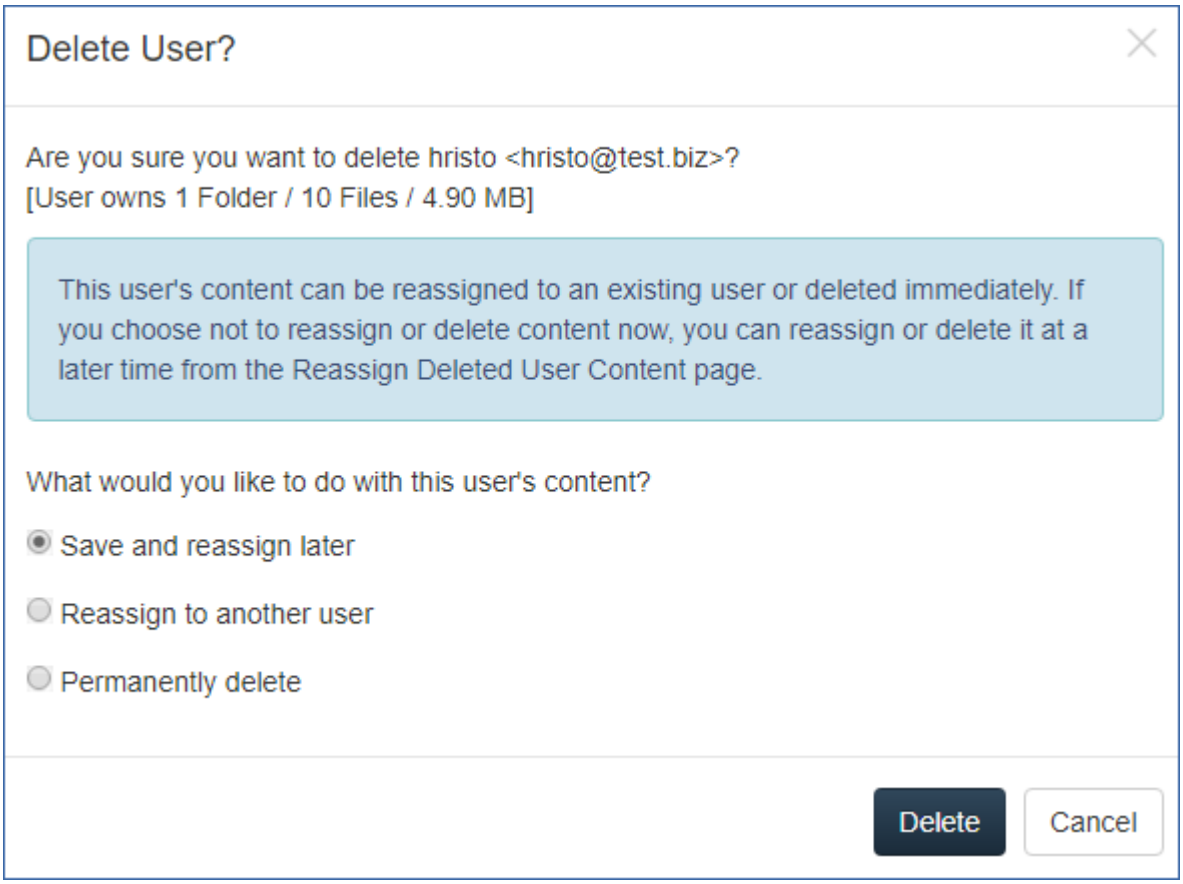
1. In the web interface, open the **Users & Devices** tab.
2. Locate the desired user and click the **Actions** button.
3. Select **Edit User** and enable **Use custom quota?**.
4. Enter the desired quota size and press **Save**.

Note
Use custom quota? checkbox is only accessible if the global option **Enable Quotas?** has been enabled beforehand.

7.2.5 Reassign Deleted User Content

Deleting a user without any content completely removes this account.

When deleting a user with content, you can choose to reassign this content to another existing user (now or later) or to permanently delete it.



- **Save and reassign later** – The user's content is temporary left in the system and can be managed in **Reassign Deleted User Content** tab. The content here can be either reassigned, or permanently deleted.

Note
Purging policies will still be enforced over this content the same way as for active users.

- **Reassign to another user** – The content is immediately reassigned to another user, whose Sync & Share space receives a folder named **Content inherited from DeletedUserName <deletedusersemail>**. The new user becomes owner of the inherited content, including folders shared by the deleted user.
- **Permanently delete** – Immediately delete the user's account and content.

8 Client Guides

For information on using the Acronis Cyber Files clients, please visit the specific client guide documentation for your app from the list below:

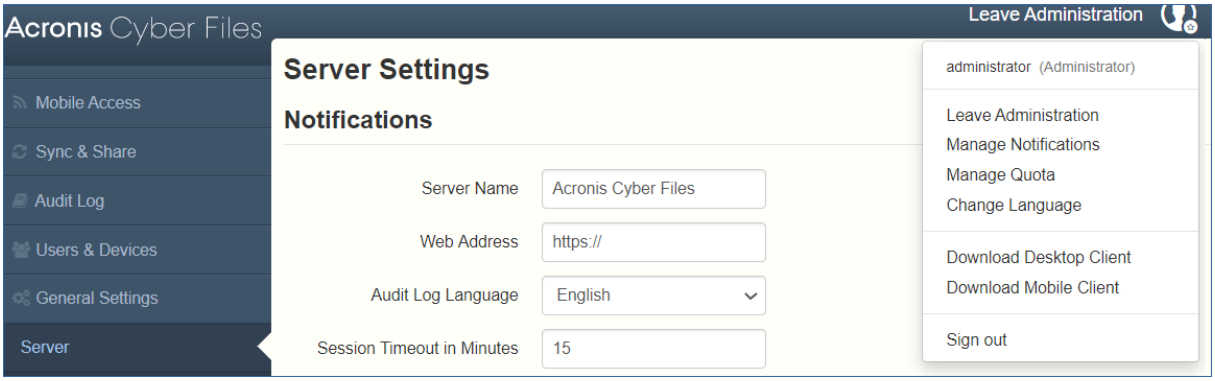
- Desktop and Web client
- iOS app
- Android app

9 Server Administration

9.1 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.



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.

9.2 Administrators and Privileges

9.2.1 Administration page access restrictions

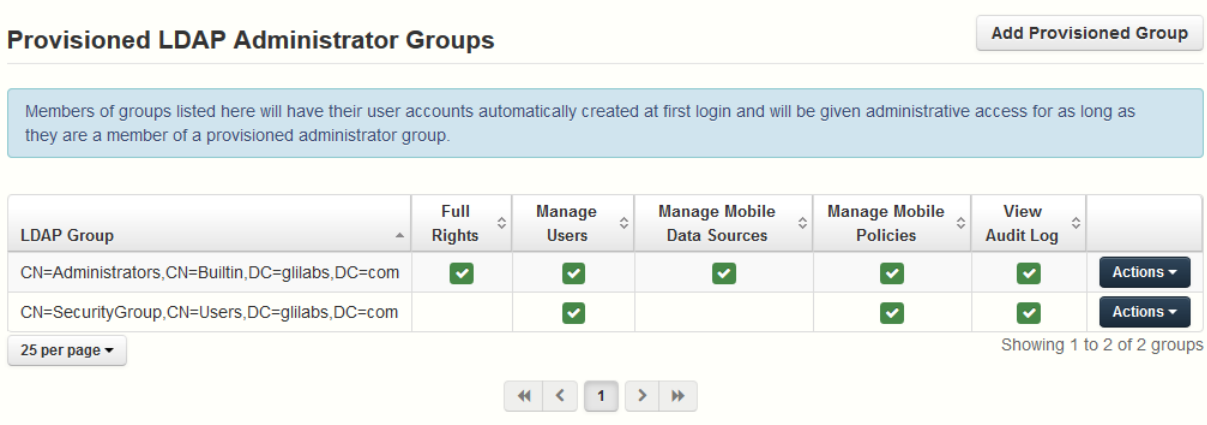
Only connections from configured IP address ranges will be allowed to access the Administration pages - allows the administrator to allow only certain IP addresses to accessing the Administration web interface.

- **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.

9.2.2 Provisioned LDAP Administrator Groups

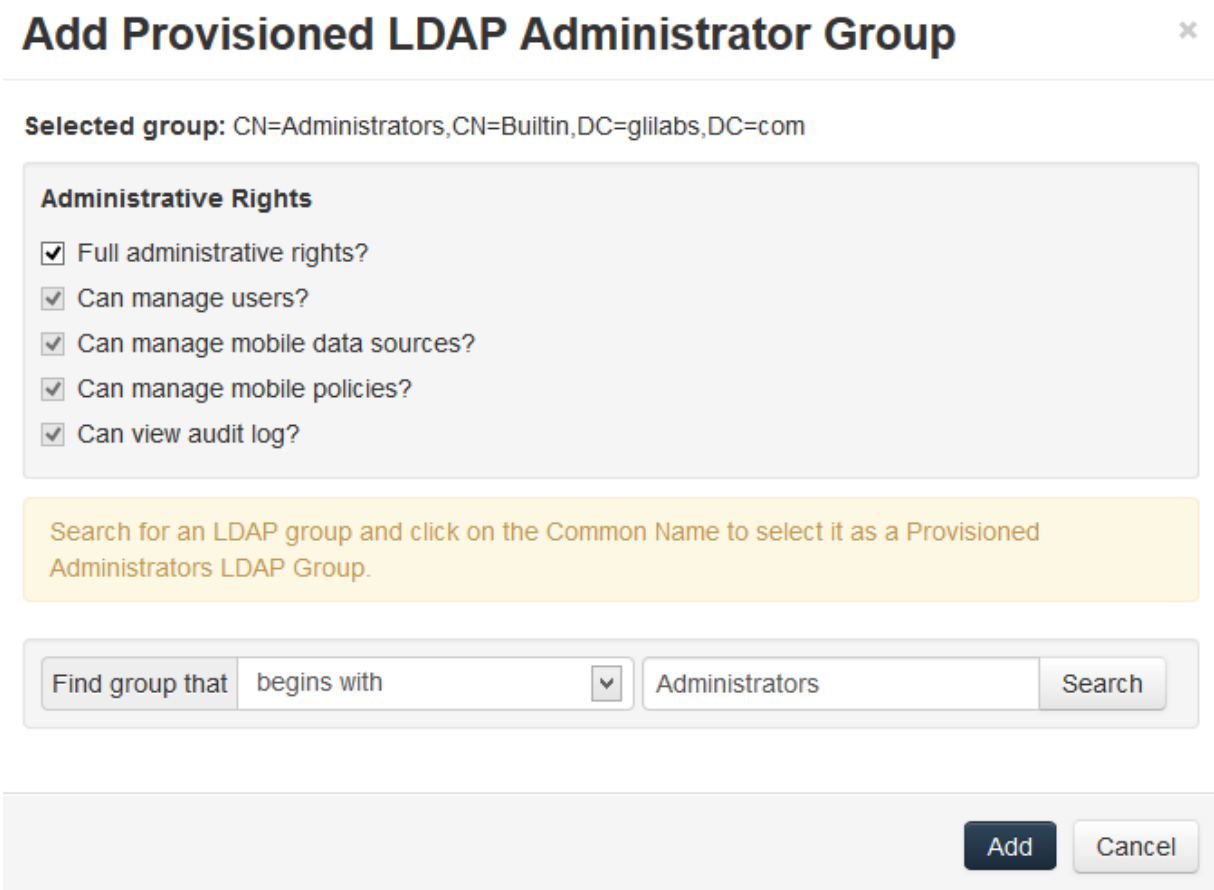


This section allows you to manage your administrative groups. Users in these groups will automatically receive the group's administrative privileges. All of the rights are shown in a table, the ones that are currently enabled have a green mark.

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:

9.2.3



1. Press 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. Press **Save**.

9.2.4 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 Acronis Cyber Files Web Interface.
2. Log in with an administator account.
3. Expand the **General Settings** tab and open the **Administrators** page.
4. Press the **Add Administrator** button under **Administrative Users**.
5. LDAP users without emails cannot be given Sync & Share functionality.
6. 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.

   To invite via Active Directory/LDAP do the following:

   a. 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.

   b. Enable/Disable the Sync & Share functionality.Select which administrative rights the user should have.Press Add.

   To invite by Email do the following:

   a. 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.

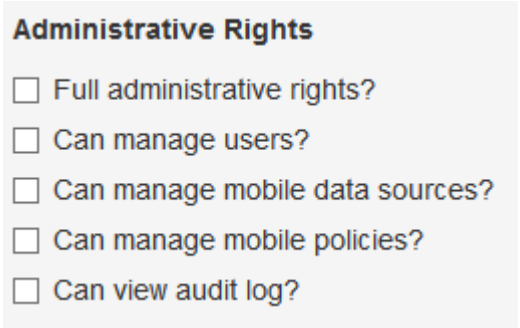
   Select whether this user should be licensed.

   a. Select which administrative rights the user should have.

   Select the language of the Invitation email.

   b. Press Add.

9.2.5 Administrative rights



- **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. Press the **Actions** button for the User you want to edit.
4. Press **Edit**.
5. Mark all of the administrative rights you want your user to have.
6. Press **Save**.

To give an administrator specific rights:

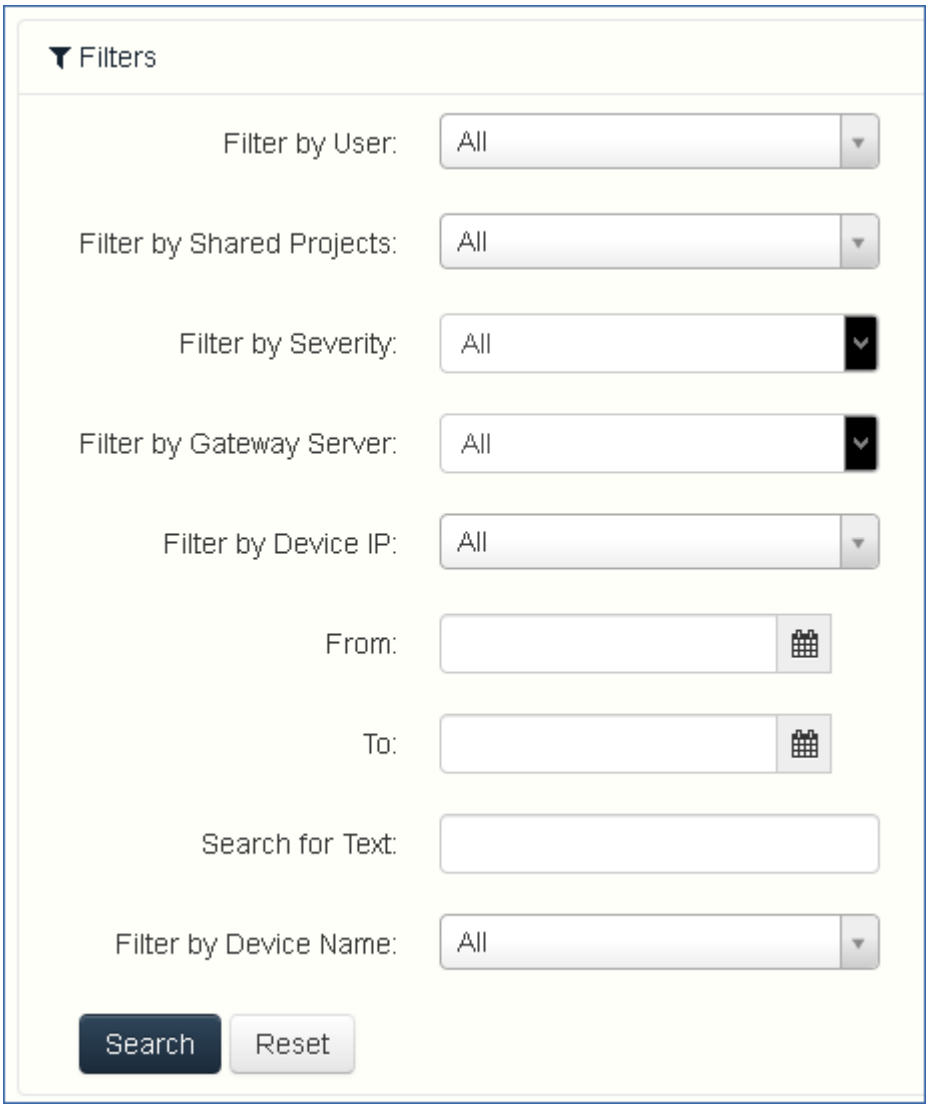
1. Press the **Actions** button for the User you want to edit.
2. Press **Edit**.
3. Mark all of the administrative rights you want your user to have.
4. Press **Save**.

9.3 Audit Log

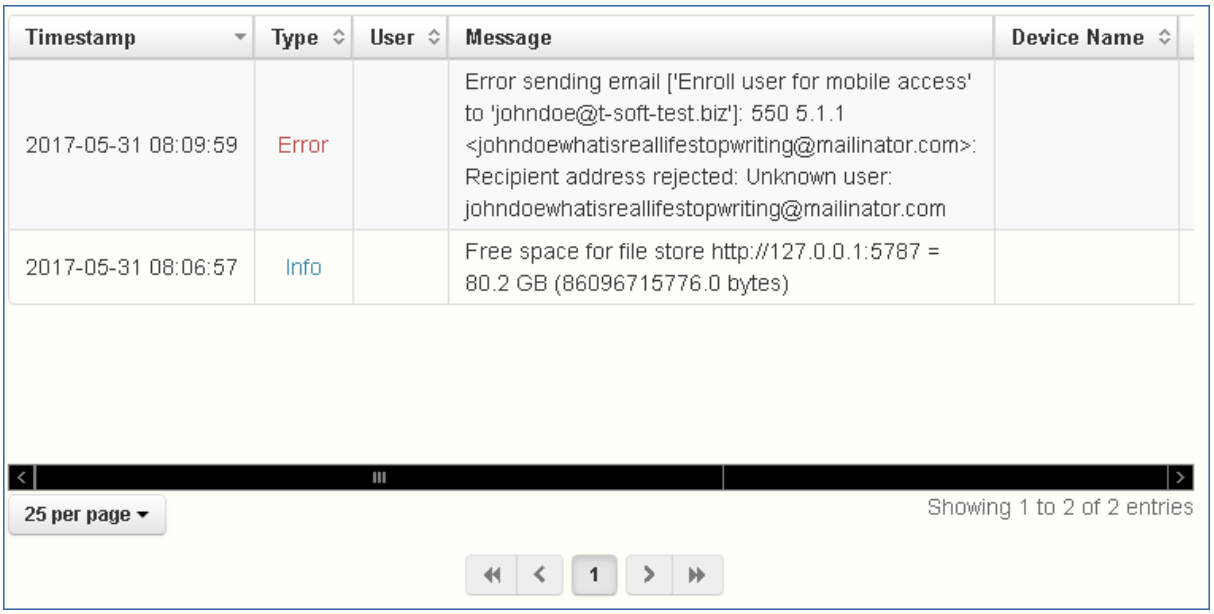
9.3.1 Log

Here you can see all of the recent events (depending on your purging policy, the time limit might be different), the users from which the log originated and a message explaining the action.

Note
If you wish to configure a Gateway Server's logging and level of logging, please visit Gateway Server Logging.



- **Filter by User** – filters the logs by User. You can select **All**, **No user** or choose one of the available users.
- **Filter by Shared Projects** – filters the logs by Shared Project. You can select **All**, **Not shared** or choose one of the available Shared Projects.
- **Filter by Severity** – filters the logs by type. The types are **All**, **Info**, **Warning**, **Error** and **Fatal**.
- **From/To** – filter by date and time.
- **Search for Text** – filter by log message contents.

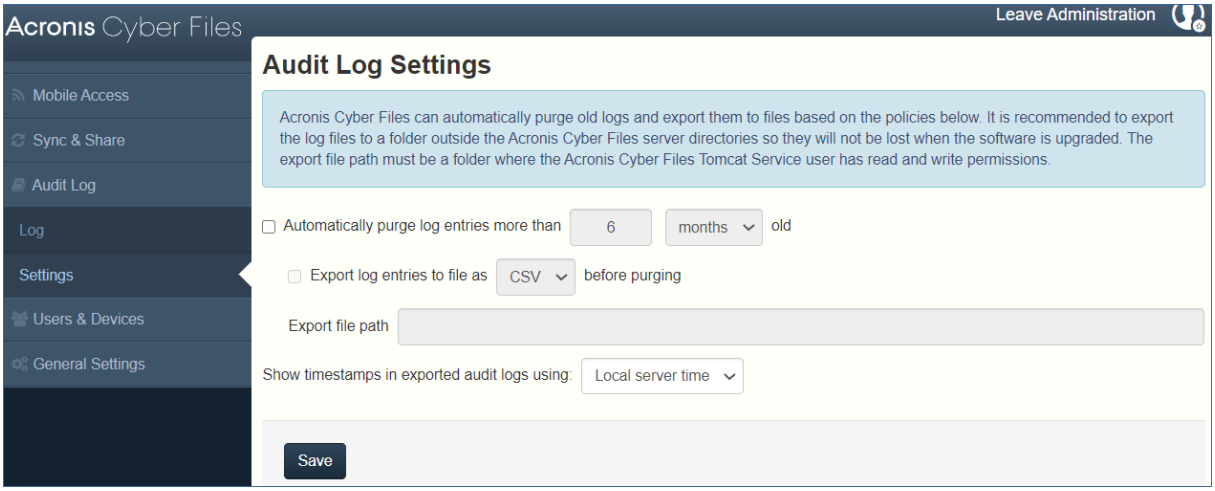


- **Timestamp** – shows the date and time of the event.
- **Type** – shows the level of severity of the event.
- **User** – shows the user account responsible for the event.
- **Message** – shows information on what happened.

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.

9.3.2 Settings



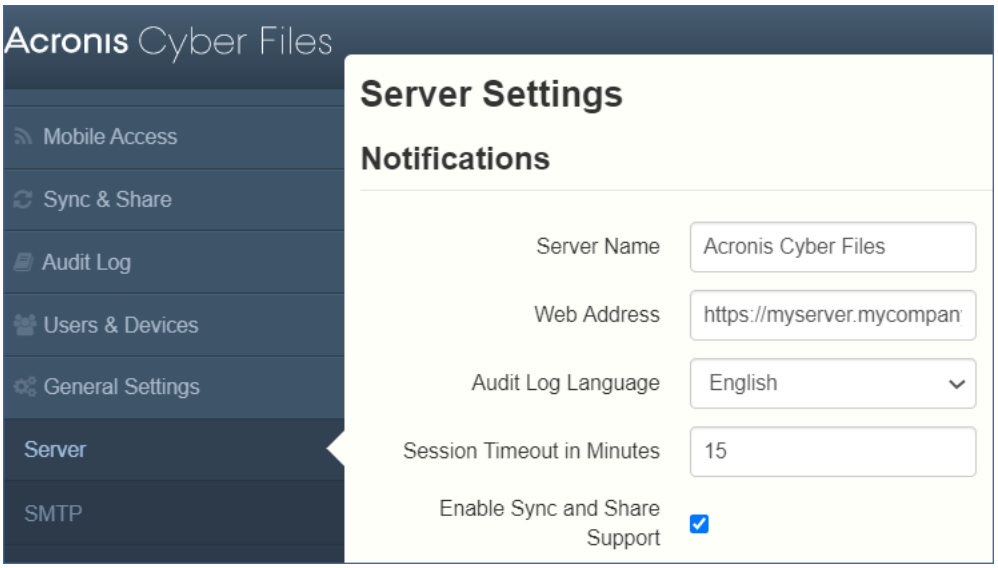
Acronis Cyber Files can automatically purge old logs and export them to files based on certain policies.

- **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.

> **Note**
> 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 usingX** - Lets you choose if your audit logs should use the local server time or another time format (UTC).

9.4 Server



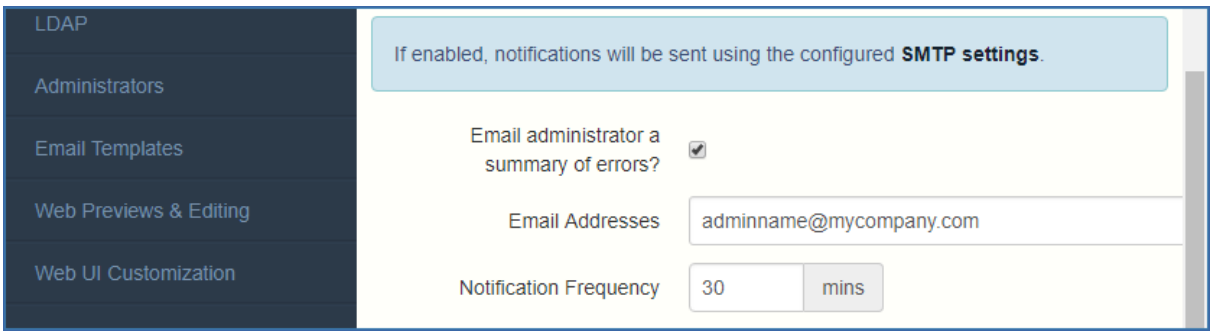
9.4.1 Server Settings

- **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.



9.4.2 Notification Settings

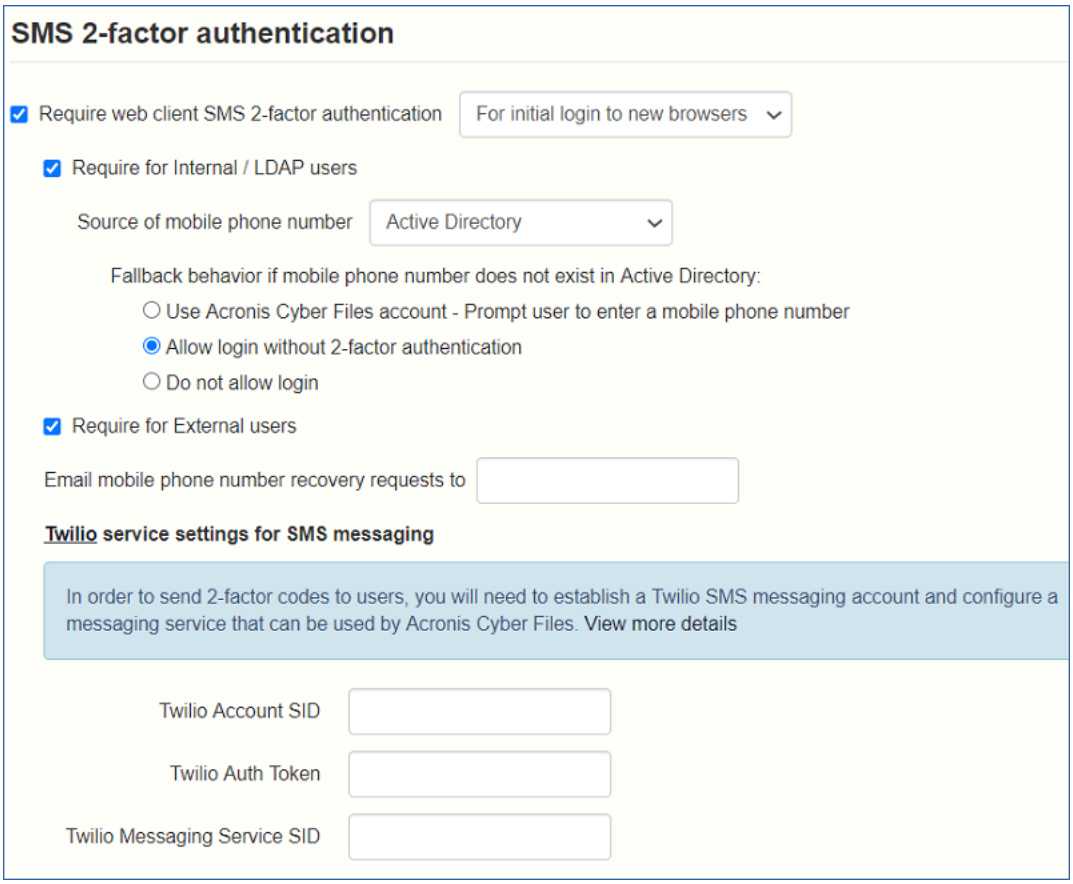
- **Email administrator a summary of errors?** – If enabled, a summary of errors will be sent to specified email addresses.
  - **Email Addresses** – one or more email addresses which will receive a summary of errors.
  - **Notification Frequency** – frequency for sending error summaries. Sends emails only if errors are present.

9.4.3 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.



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

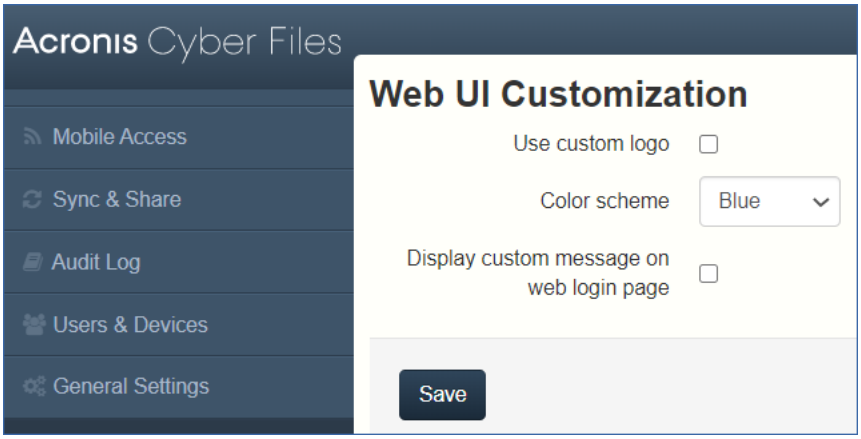
creating a Twilio messaging service, for **Use Case** leave it blank or select two-factor authentication.

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.

9.5 Web UI Customization

You can easily customize the logos and color scheme of your Acronis Cyber Files server.

Note
Note: You can also make these customizations through the Acronis Cyber Files API, for more information check out Web UI API customization.



9.5.1

9.5.2 Using custom logos

1. Open the Acronis Cyber 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. Press **Save**.

9.5.3 Using a custom welcome message

1. Open the Acronis Cyber Files web interface and login as an administrator.
2. Navigate to **General Settings** -> **Web UI Customization**.

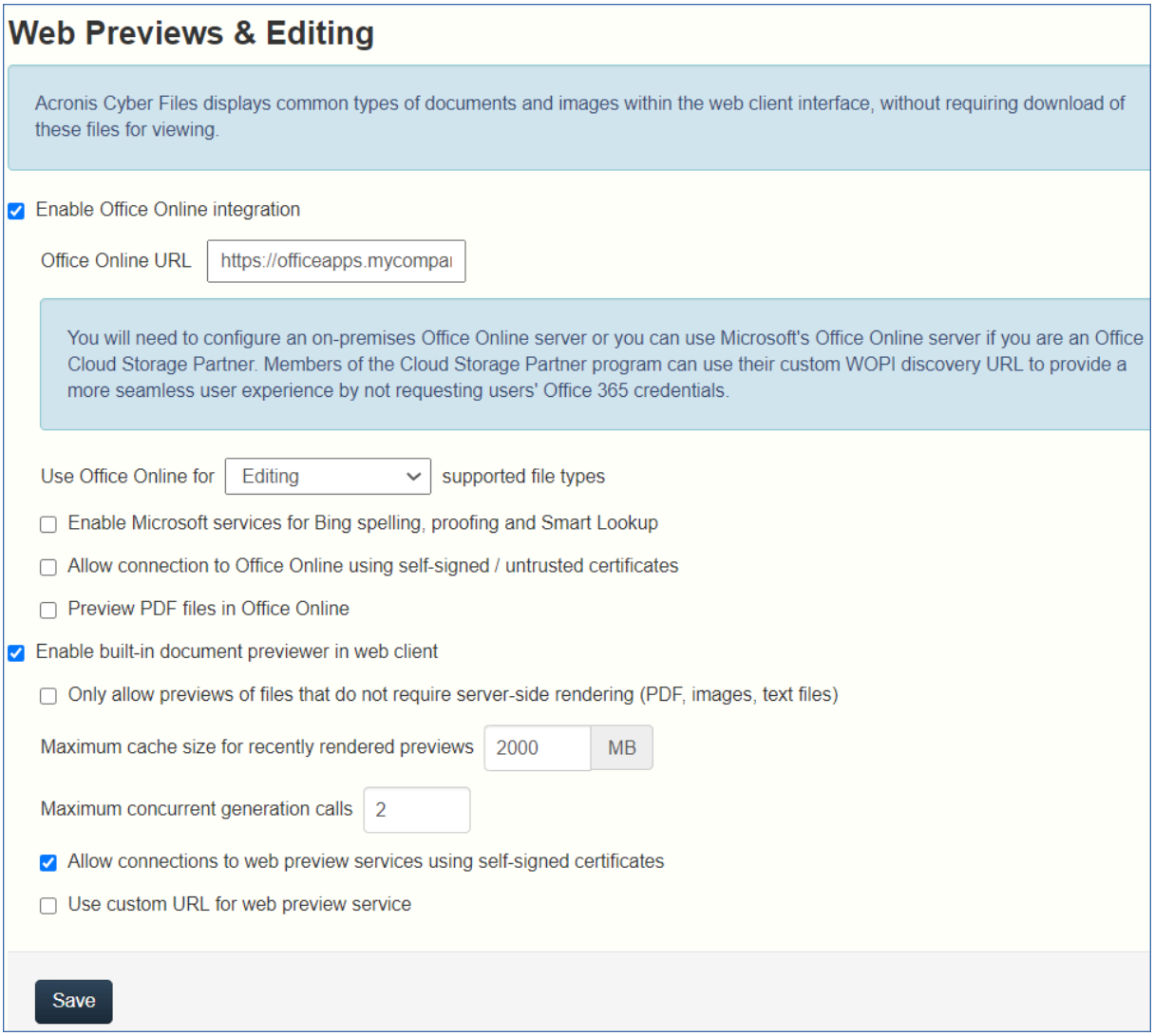
3. Select the **Display custom message on web login page** checkbox.
4. Enter the desired message in the text box and press **Save**.

9.5.4 Using color schemes

1. Open the Acronis Cyber 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. Press **Save**.

9.6 Web Previews & Editing

Acronis Cyber Files can display common types of documents and images within the web client interface, without downloading these files.



Enable Office Online integration - Enables Office Online integrated functionality.

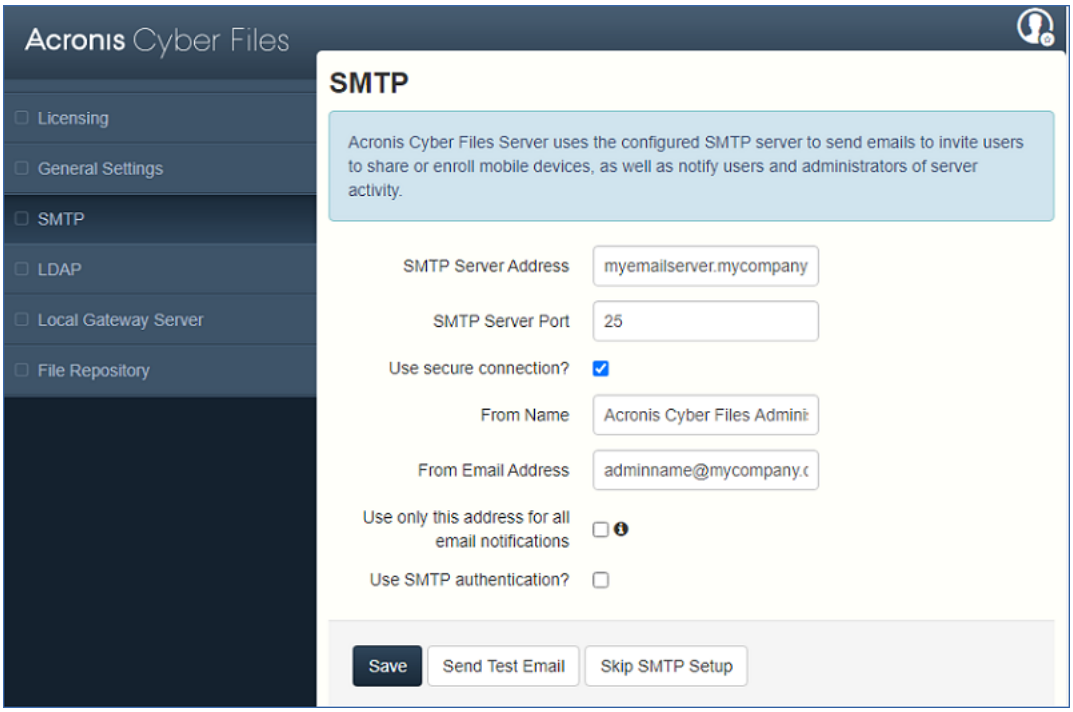
- **Office Online URL** - Enter your Office Online's WOPI discovery URL. For on-premises Acronis Cyber Files installations, you must be using an on-premises Office Online setup to be able to provide this URL. Microsoft's Office Online cloud service is limited to service provider use and is not publicly accessible without special certification and white 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.

- **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.

9.7 SMTP

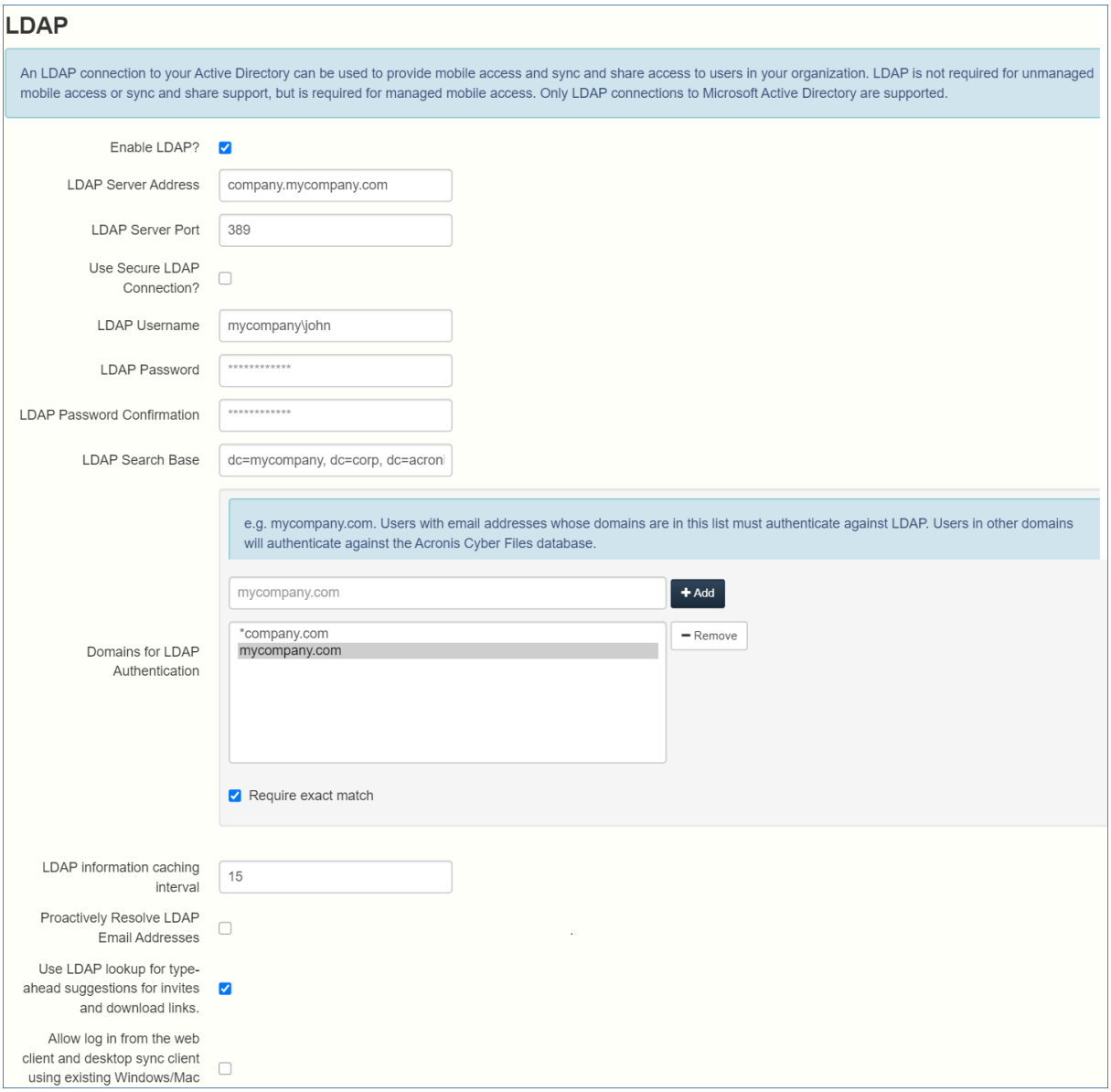
Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to a shared resource or enroll mobile devices, as well as notify users and administrators of server activity.



- **SMTP 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.

9.8 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.



- **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 LDAP secure connection?** - disabled by default. Check the box to connect to Active Directory using secure LDAP.

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).

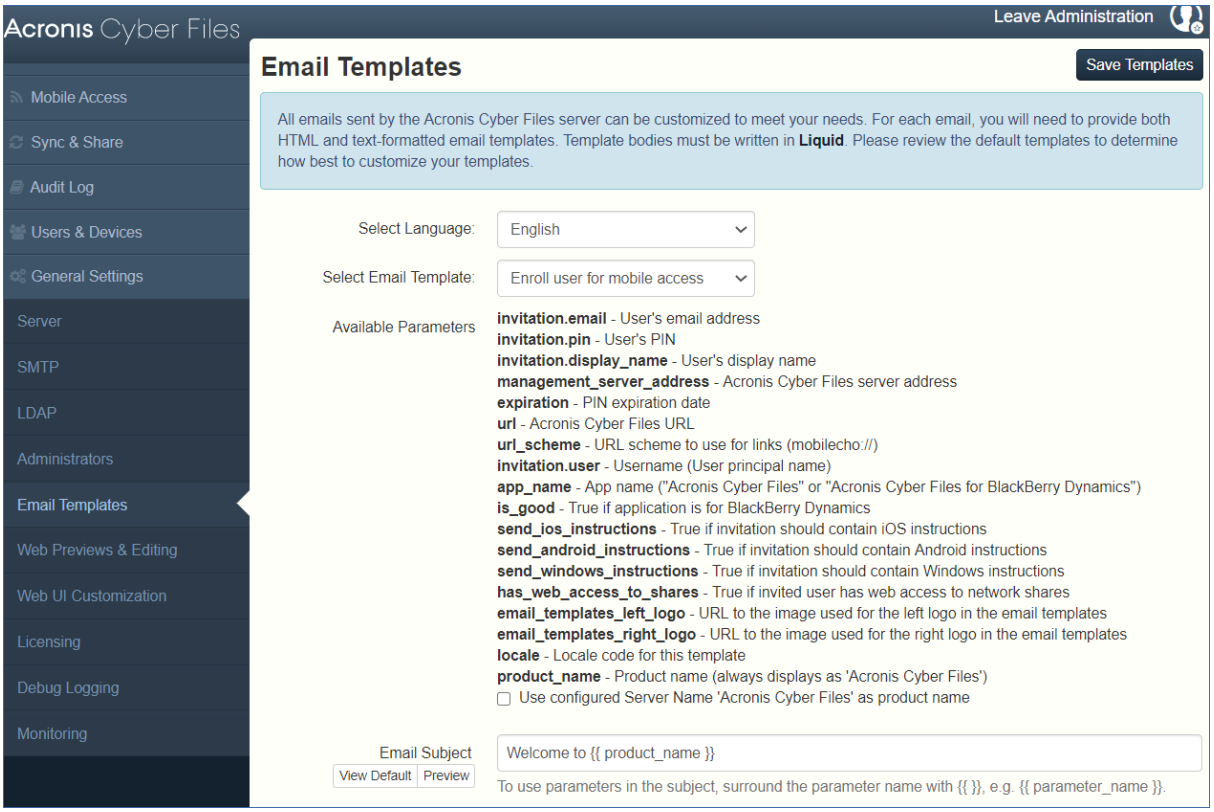
- **LDAP username / password** - this login credentials will be used for all LDAP queries. Ask your AD administrator to find out if you have designated service accounts that should be used.
- **LDAP Search Base** - enter the root level you would like searches for users and groups to begin. If you would 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.
  1. (i.e.to enable LDAP authentication for an account with the email **joe@glilabs.com**, you would enter **glilabs.com**)

  . Users in other domains will authenticate against the Acronis Cyber Files database.
  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.

9.9 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 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.



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.

If you have upgraded from mobilEcho, the customizations you have done to the email templates are not migrated and you will need to customize the new templates. A copy of your previous mobilEcho templates can be found in the **Legacy mobilEcho files** folder by default located here: C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files. The files are named **invitation.html.erb** and **invitation.txt.erb**.

- **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 Acronis 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.

9.10 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.

9.10.1 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. Press **Add License**.

Note
If your licenses have the same unique ID, the number of allowed users will be summed.

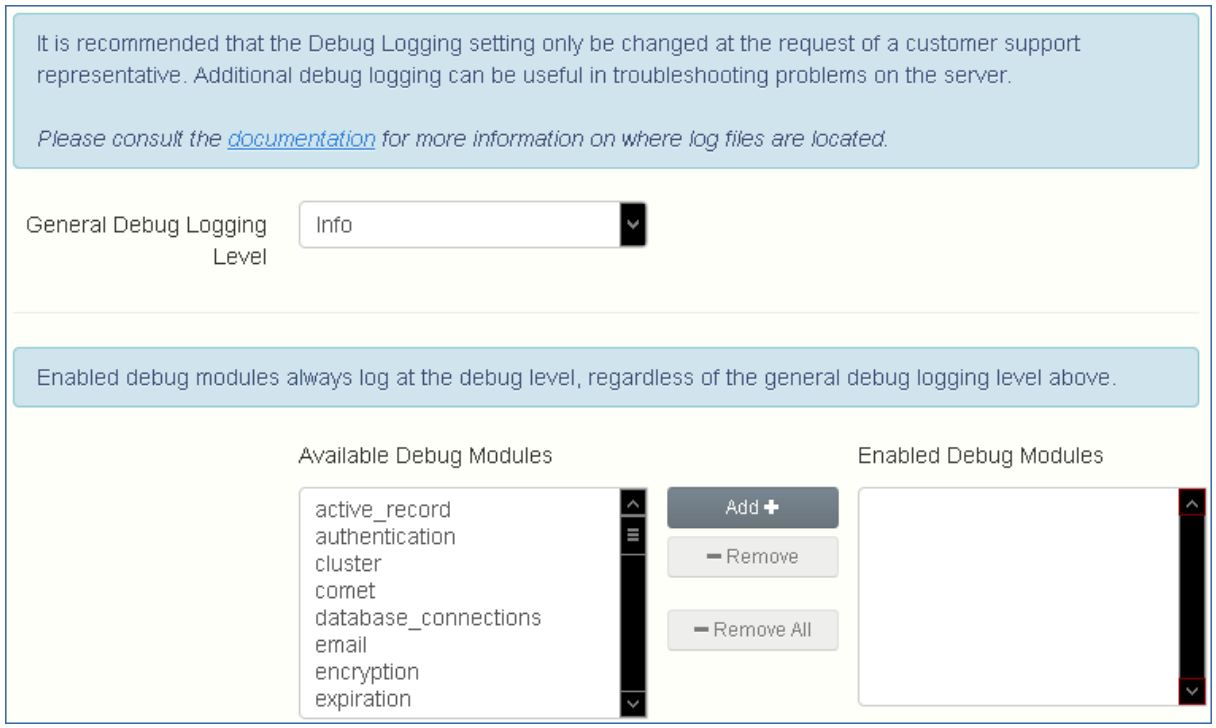
9.10.2 Adding a new license for a Gateway Server is not necessary

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.

9.11 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.



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.

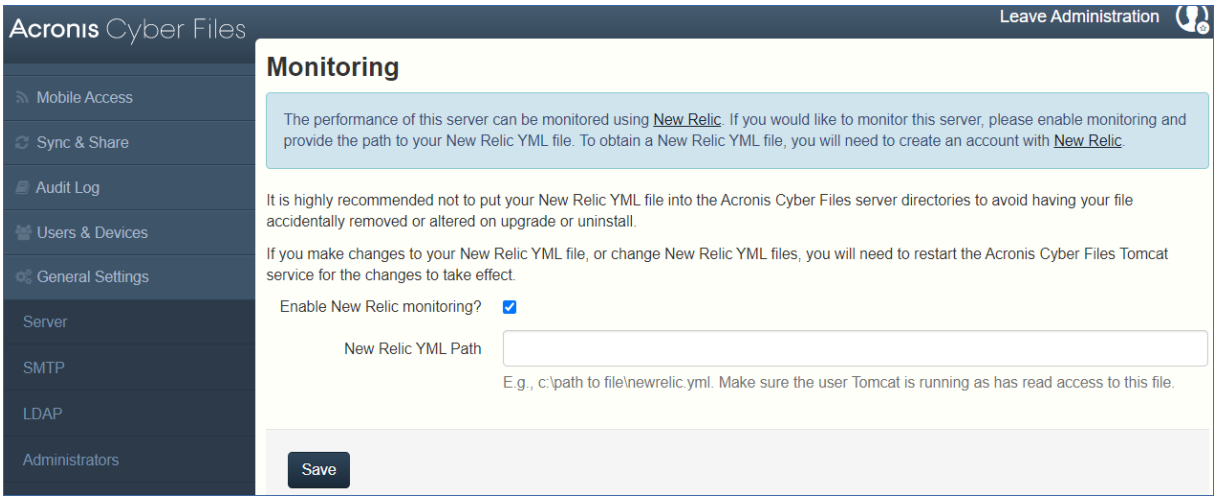
- **Available Debug Modules** - Shows a list of available modules.
- **Enabled Debug Modules** - Shows the active modules.

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

9.12 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.



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)

9.12.1 **Installing New Relic**

9.13 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

Note
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.

10 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.

10.1 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.

10.1.1 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.

10.1.2 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.

10.1.3 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.

10.1.4 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.

10.2 Best Practices

10.2.1 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.

10.2.2 2. We recommend that very large deployments "Vacuum" and "Analyze" their database(s) monthly

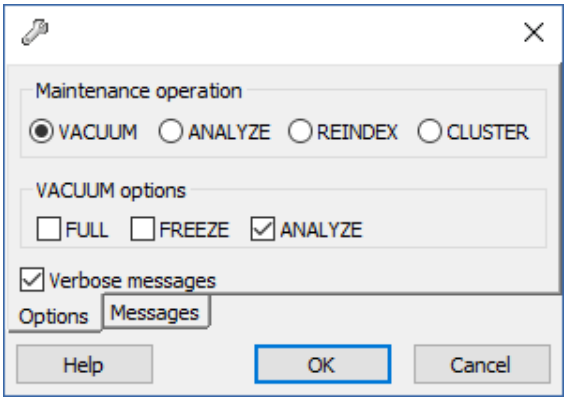
PostgreSQL databases require periodic maintenance known as vacuuming. The **VACUUM** command has to process each table on a regular basis to:

- 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 (it could also be called PgAdmin). You can find it in Windows Start menu, under the Acronis Cyber Files folder. Double-click on **localhost** to connect to your server.
2. Right-click on the acronisaccess_production database and choose **Maintenance**.
3. Select the **VACUUM** radio button and the **ANALYZE** checkbox.



Warning!
The vacuum can take some time. This process should be run during periods of low load on the server.

4. Press **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

10.2.3 3. For big deployments, you should consider running a load-balanced setup or clustering Gateway servers.

10.3 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.

10.3.1 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.

   a. 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.
   b. Expand **Databases** and right-click on the **acronisaccess_production** database.
   c. Choose **Maintenance** and select the **Vacuum** radio button and the **ANALYZE** checkbox. Press **OK**.
   d. 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.
   e. Close the PostgreSQL Administrator tool and open an elevated command prompt.
   f. 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\).

   a. 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. 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.

10.3.2 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.

10.3.3 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.
- newrelic.yml file if you are using **New Relic** to monitor your Acronis Cyber Files server.

10.3.4 Restoring the Cyber Files database

1. 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.

2. 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.
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.

10.3.5 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.

10.3.6 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.

10.3.7 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.

10.4 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.

10.4.1 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
Info: For information on ForFiles, syntax and examples visit http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx

10.4.2 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
Info: 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"

Note
Click here for the full batch script code...

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.**

10.4.3 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:

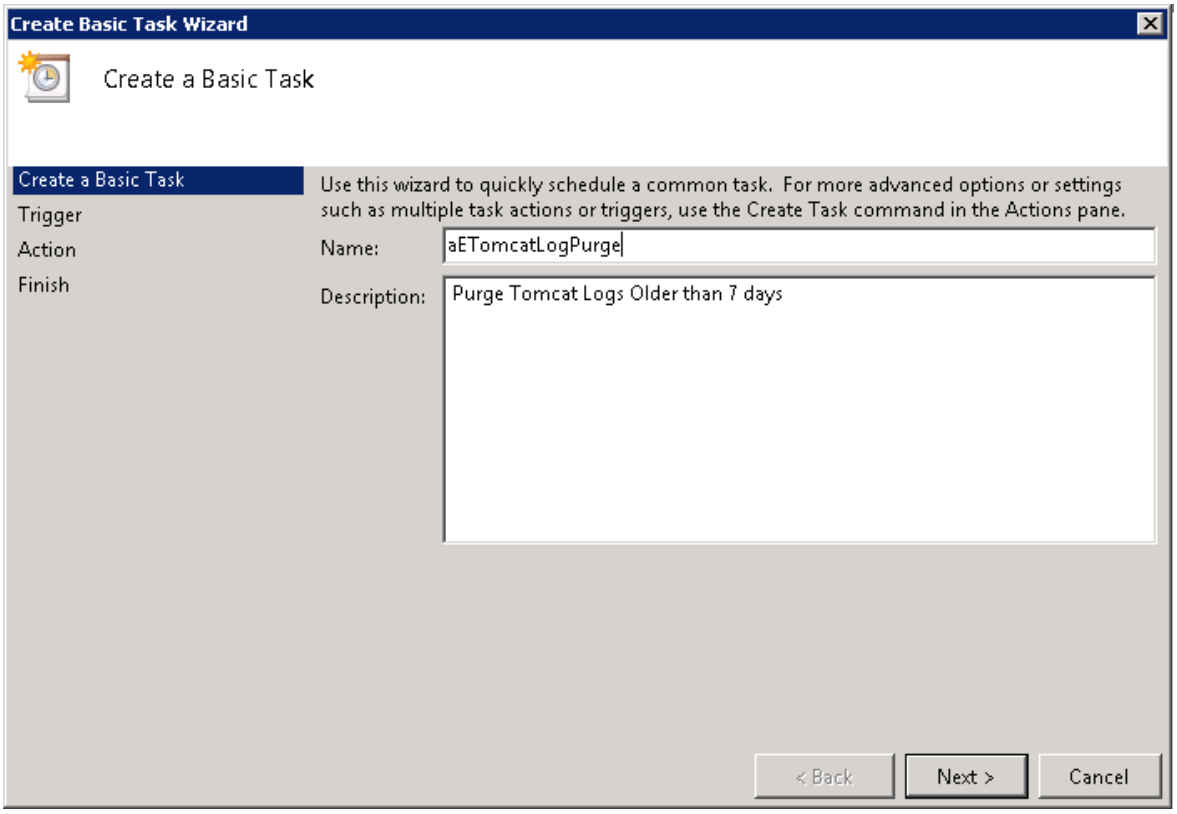
```
REM ===== CONFIGURATIONS ====================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays - Log files older than NumDays will be processed
 set NumDays=14
REM ===== END OF CONFIGURATIONS ======================
ECHO
ECHO ===== START ============
```

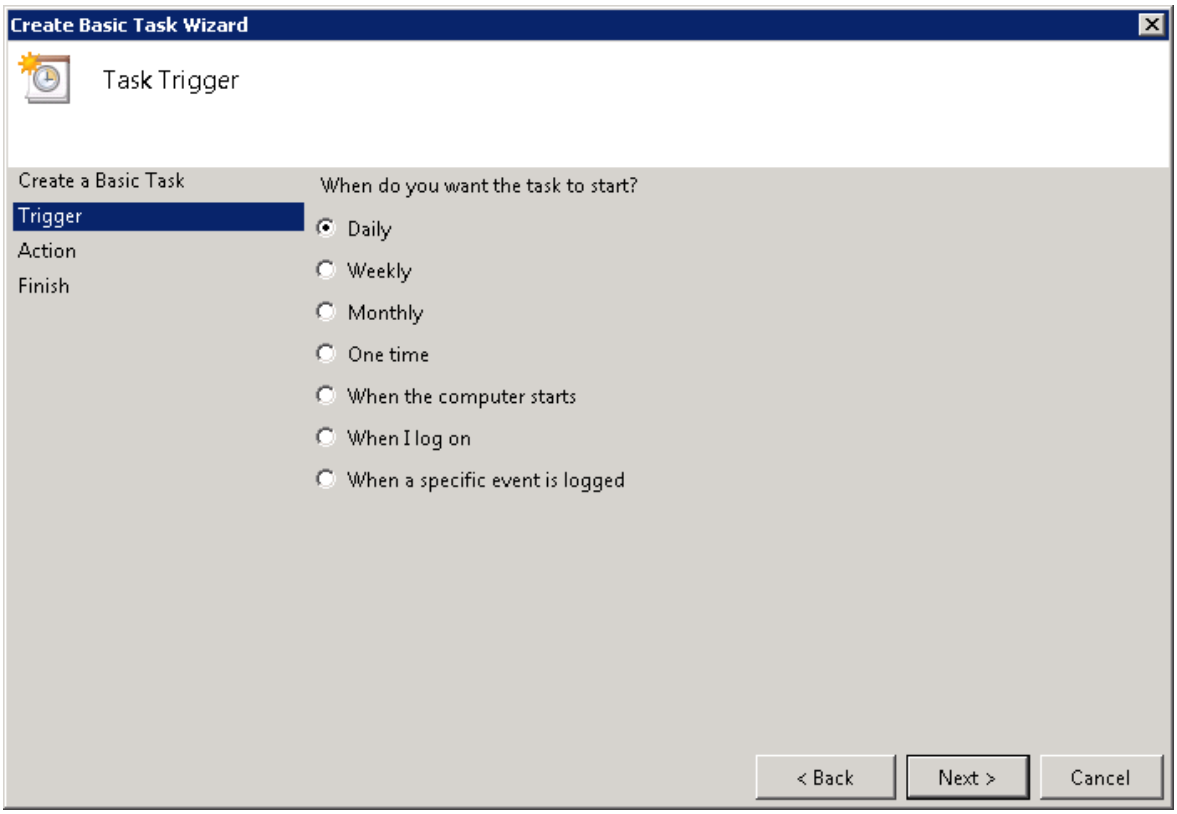
Note
In Acronis Cyber Files the log files are stored in the same folder as Tomcat's. (C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs)

3. Save the file.

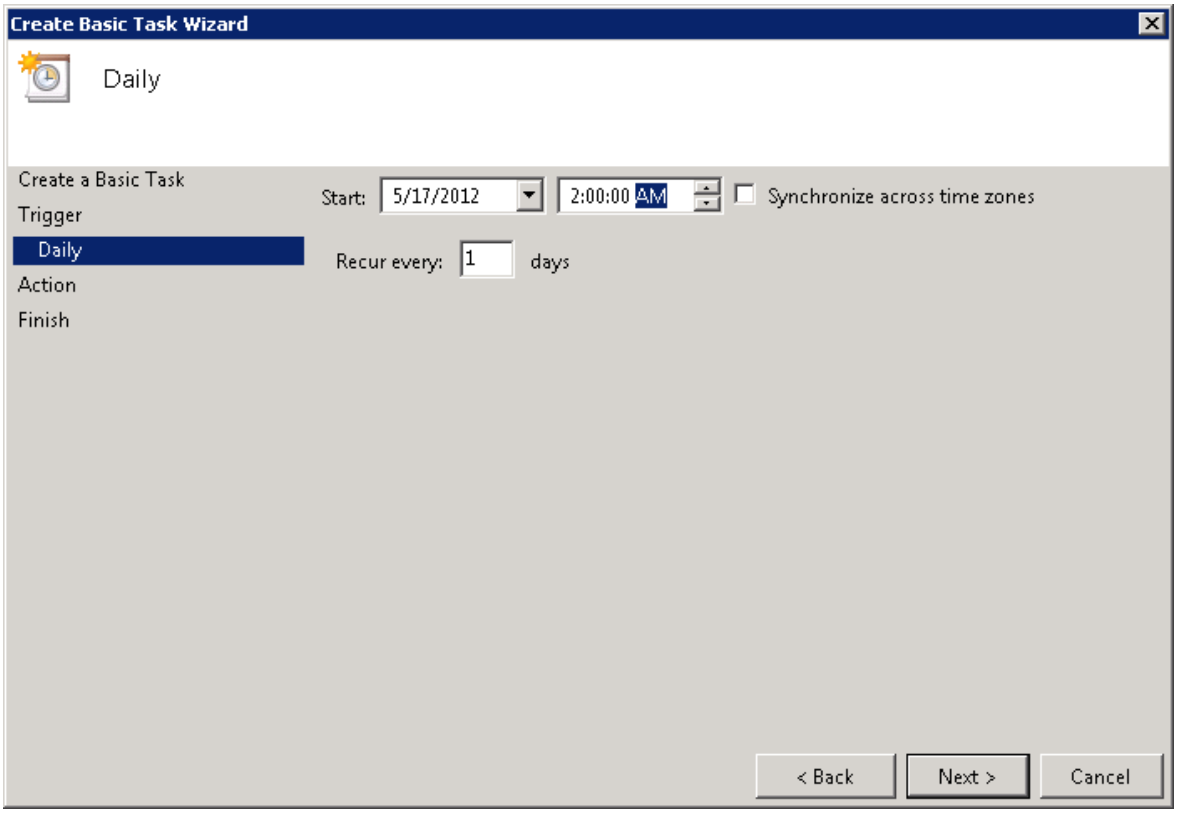
4. To automate the process, open Task Scheduler and create a new task. Define a name and a description for the task.



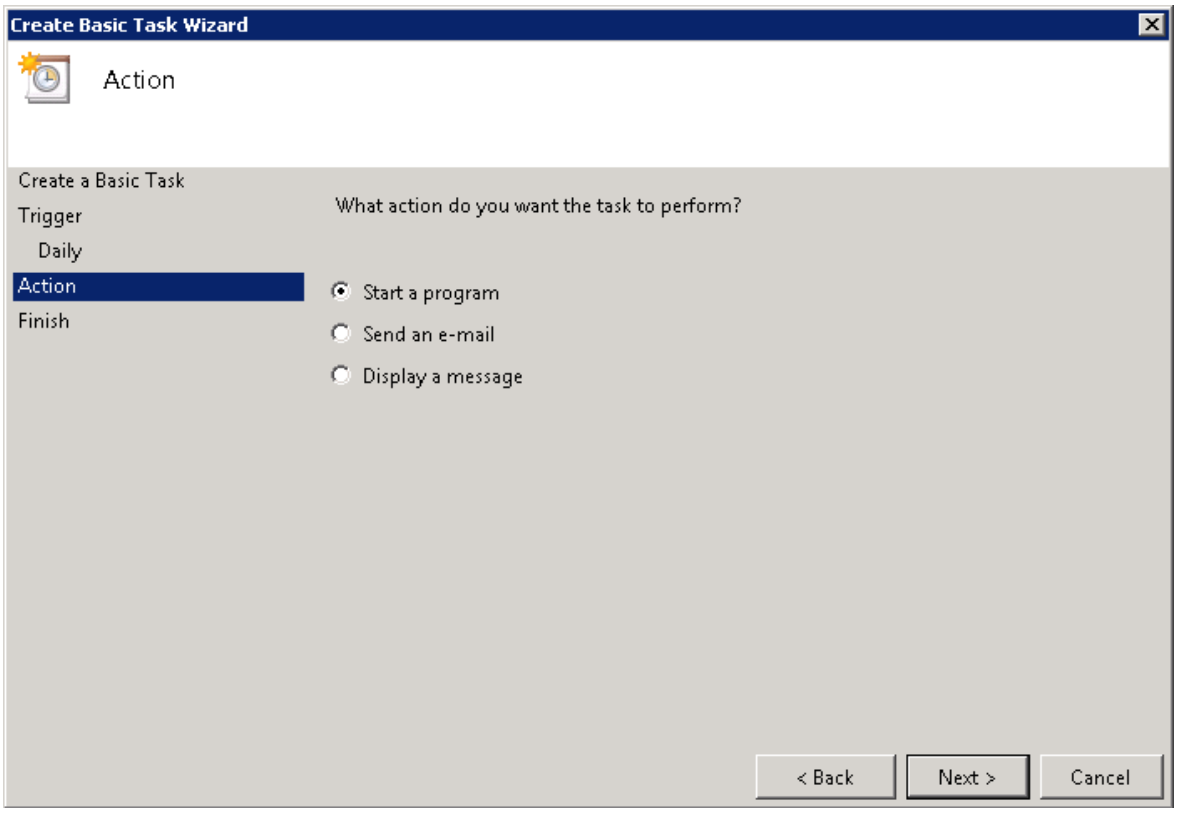
5. Set the task to run daily.



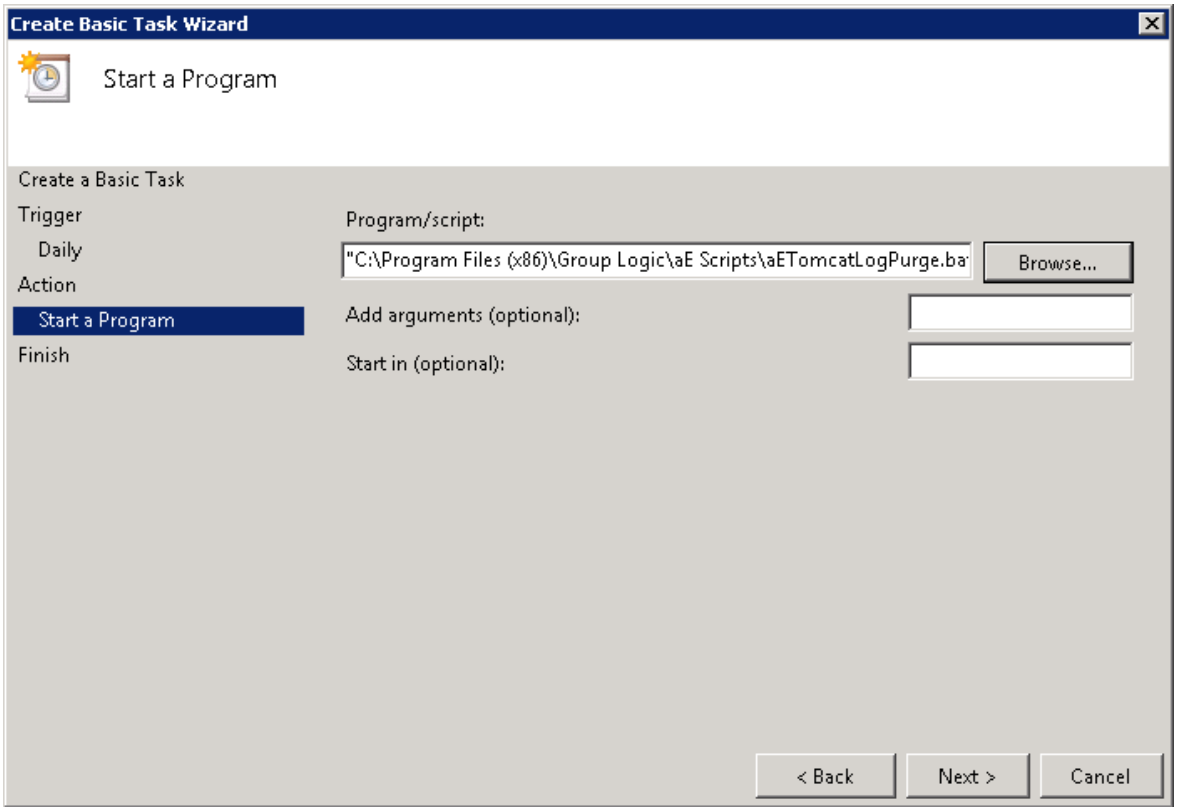
6. Define at what time the task should start. It is recommended to run this process when the system is not under extreme load or other maintenance processes are running.



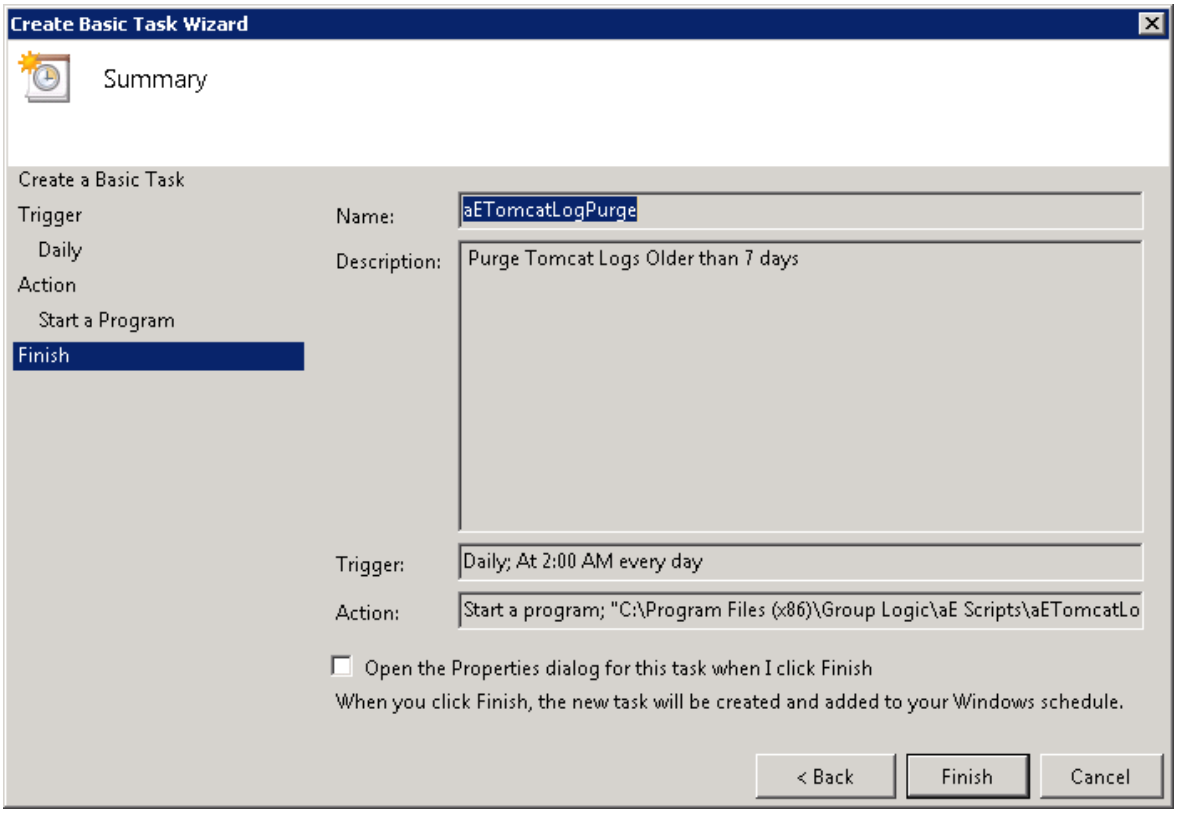
7. Set the action type to “Start a program”.



8. Click the Browse button, locate and select the script (batch) file.



9. When done, click Finish.



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.

10.5 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.

10.5.1 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"
```

1. Replace "**password**" with the password for user **postgres** you have entered when you installed Acronis Cyber Files.
2. Replace **C:\destination folder** with the path to the folder where you want to save your backups.
3. Save the file as **DatabaseBackup.bat** (the extension is important!) and select **All Files** for the file type.
4. Move the file to the PostgreSQL installation folder in the version number directory (e.g. \9.3\).

10.5.2 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. Press **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.

10.6 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.

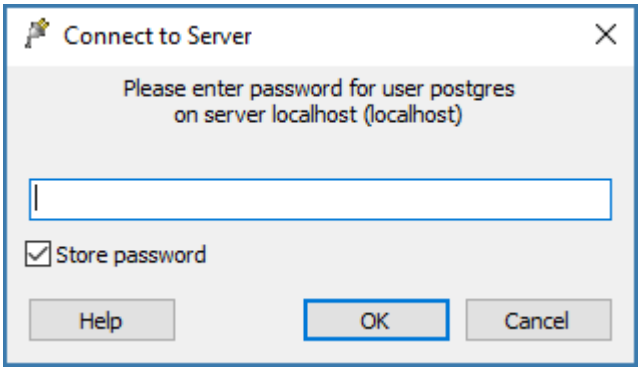
10.6.1 Configuring PostgreSQL and creating the script

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. Press OK.

   - 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:

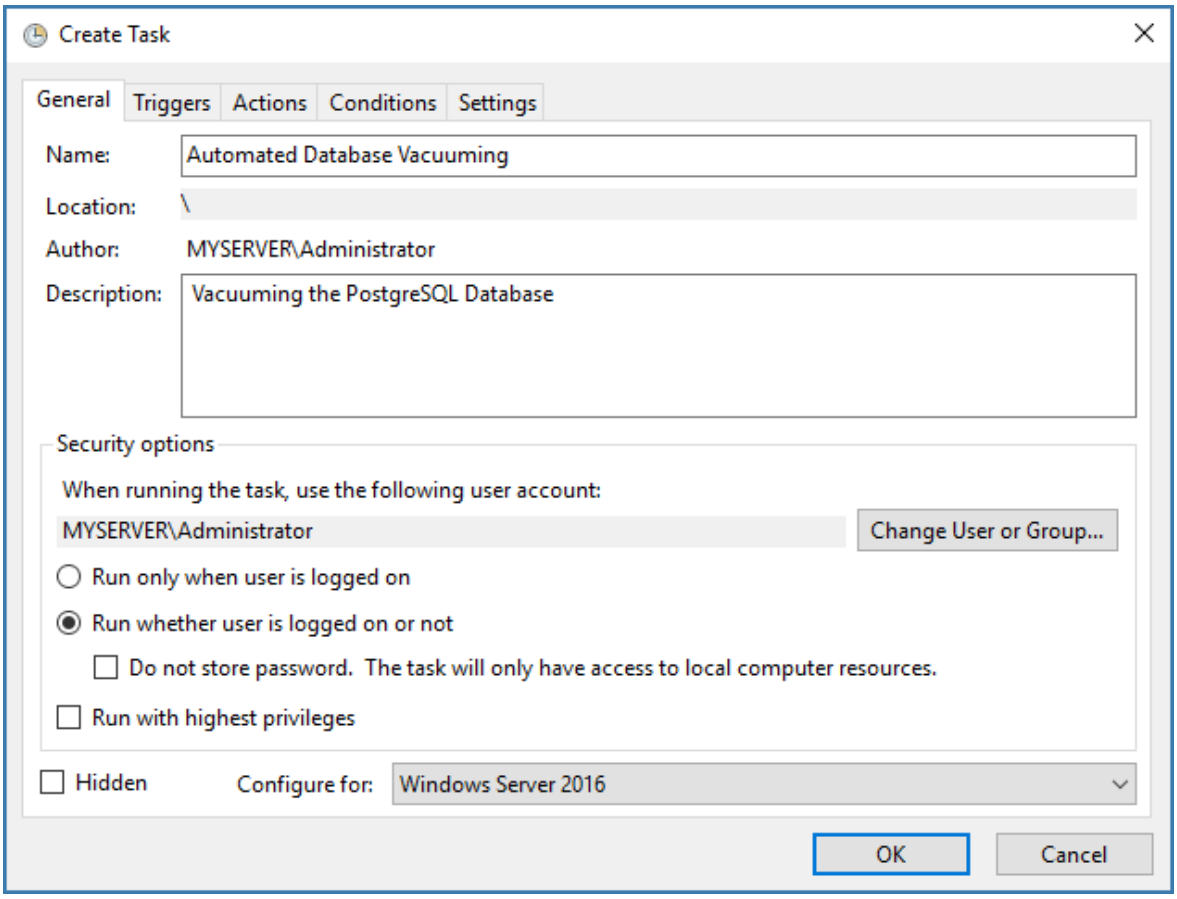
   ```
   SET PGPASSFILE=D:\Backup\pgpass.conf
   "C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\bin\psql.exe" --host=localhost --port 5432 --username=postgres -d acronisaccess_production -c "VACUUM VERBOSE ANALYZE" >"D:\Backup\vacuum_report_%date:/=.%.log" 2>&1
   ```
3. Edit this 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

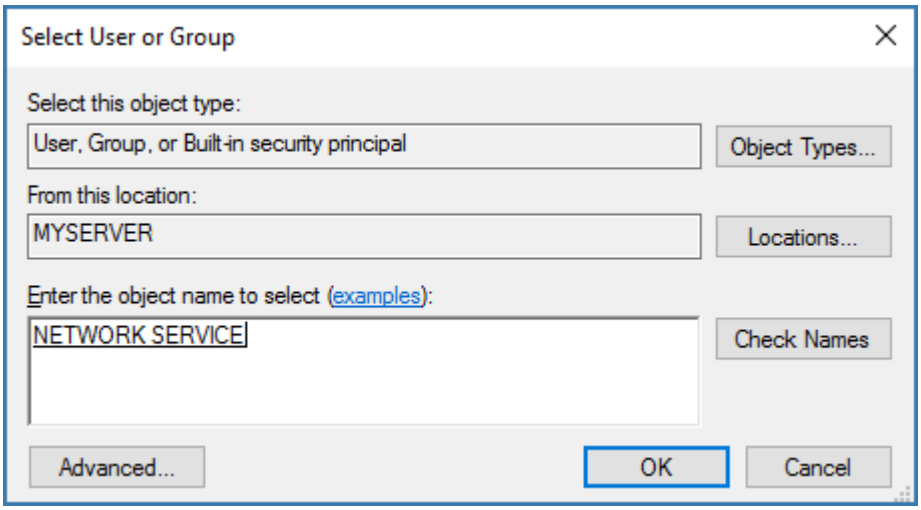
   Depending on your date format, this **.log** file creation may fail. To find the date format you can open a command prompt and run: echo %date%. If there are any illegal characters in the date, like forward slashes, they have to be converted. In the above example the extra :/=. is the conversion part. If you encounter issues, please contact Acronis support.

10.6.2 Configuring the Task Scheduler

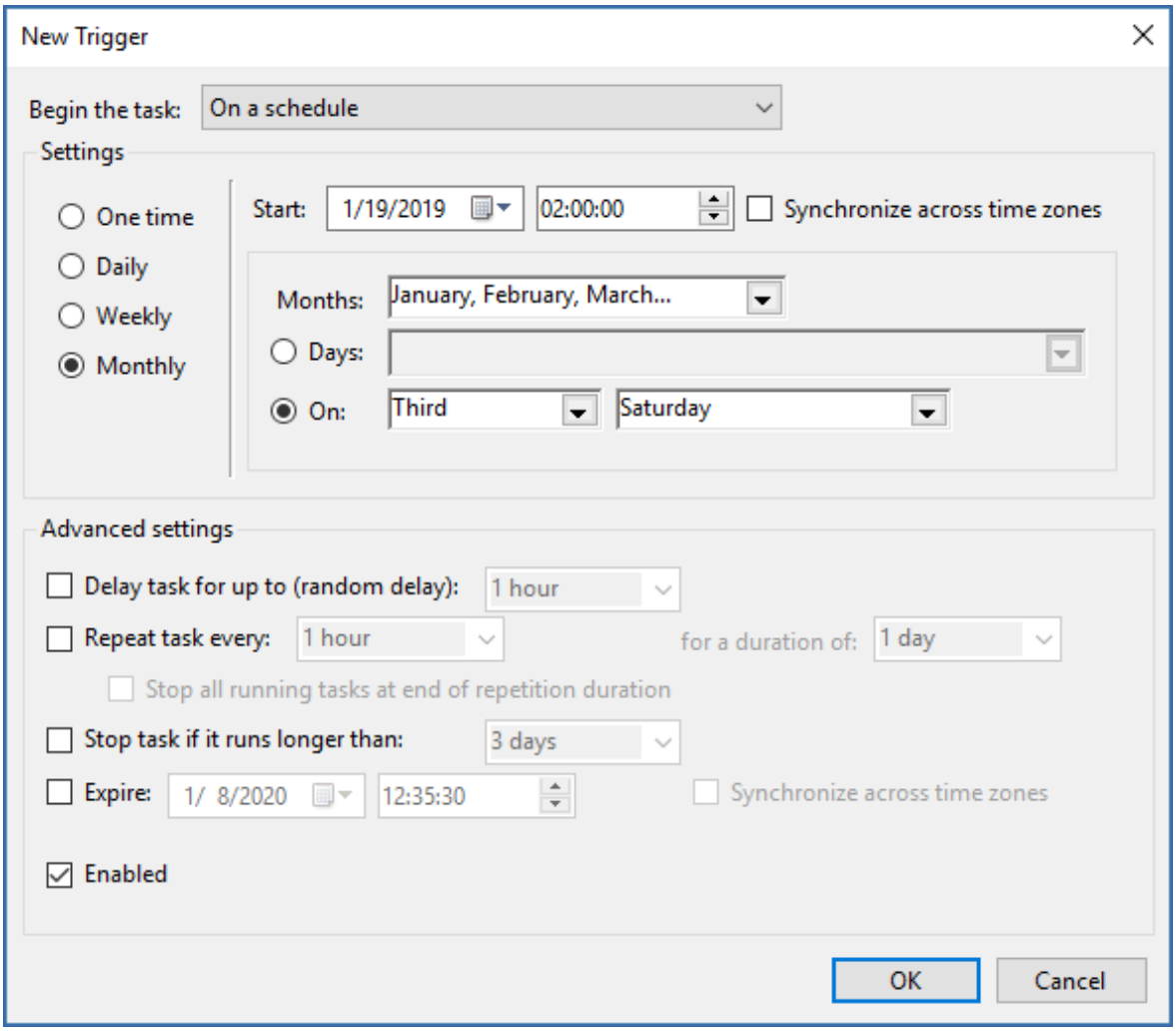
1. Open the **Task Scheduler** from **Control Panel** -> **Administrative Tools** -> **Task Scheduler**.
2. Right-click on **Task Scheduler (local)** and select **Create Task**.



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.

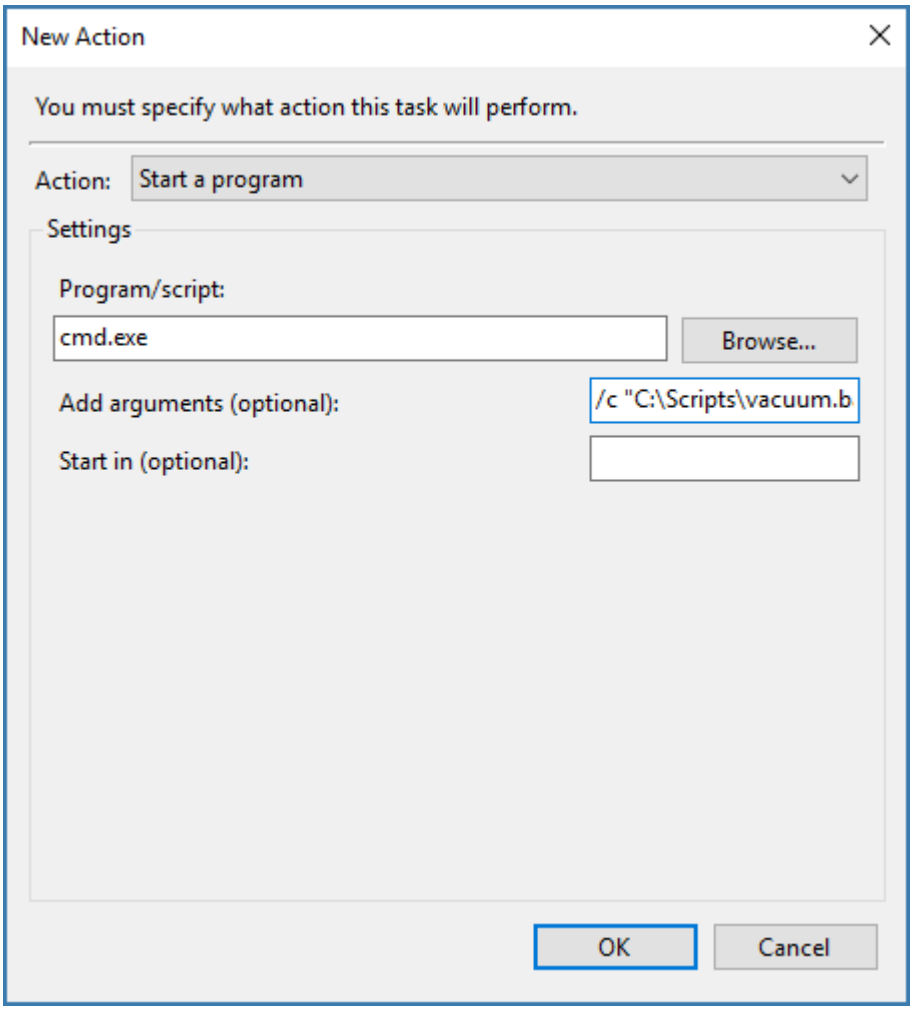


4. In the **Triggers** tab:



- 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:



- 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.

10.7 Increasing the Acronis Cyber Files Tomcat Java Maximum Memory Pool

By dfault, the Acronis Cyber Files Tomcat's Java Maximum Memory Pool setting on a 64 bit operating system is 24GBs. Depending on your deployment, you may need more.

10.7.1 To increase the maximum memory pool:

1. Click on the Start menu and navigate to **All Programs** -> Acronis Cyber Files.
2. Click on the **Acronis Cyber Files Tomcat Service Configuration** tool shortcut.
3. Open the **Java** tab.
4. Change the **Maximum memory pool** to the desired size and press **OK**.
5. Restart the Acronis Cyber Files Tomcat service.

10.8 Migrating Acronis Cyber Files to another server

This guide will help you move your existing Acronis Cyber Files setup to new machines.

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.

10.8.1 Before you begin

Note
We strongly recommend that you run a test backup/restoration outside of your production environment.

Important things to take note of, of your current configuration:

- Are the Cyber Files Web Server, Postgres 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**).

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.

10.8.2 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
   a. 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.
   b. Expand **Databases** and right-click on the **acronisaccess_production** database.
   c. Choose **Maintenance** and select the **Vacuum** radio button and the **ANALYZE** checkbox. Press **OK**.
   d. 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.
   e. Close the PostgreSQL Administrator tool and open an elevated command prompt.
   f. 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\).

a. 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.

Backup the Gateway Server's 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

2. Copy the mobilEcho.sqlite3 file to the new machine that will host the Gateway Server.

10.8.3 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.
- 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, perform the following steps:

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 Acronis Cyber Files Tomcat service.

   Note
   For load-balanced configurations, stop all Acronis Cyber Files Tomcat services.

8. 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.
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.

10.8.4 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.

10.8.5 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
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.

10.9 Upgrading PostgreSQL to a newer Major version

Major PostgreSQL releases often add new features that change some of the internal workings of PostgreSQL. There are two main ways to upgrade your PSQL instance - by dumping your entire database and then re-inserting it in the new instance (pg_dumpall) or with the new pg_upgrade command. Both methods have their benefits and their drawbacks.

- Usually, using pg_dumpall to dump the whole database and then re-insert it into the new instance is the best way to ensure data integrity but for large databases it can be a very slow process.
- Using pg_upgrade is a lot faster than dumping the entire database, but it doesn't work with older versions of PSQL.

Warning!
As PostgreSQL is a third-party product, Acronis cannot guarantee that these methods will work the same for everyone. Always consult PostgreSQL's documentation for your version of PostgreSQL before implementing anything in your production environment.

Note
Please consult the PostgreSQL documentation if pg_upgrade is usable with your version of PostgreSQL and the new version you're planning to use.

10.9.1 Before you begin

Warning!
Acronis Cyber Files 8.6 is distributed along with PostgreSQL 11 by default.

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, please contact Acronis Support.

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

Note: 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 Cyber Files from older product versions like Access or Files Advanced, directories' 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.
- Make sure that access between the two instances is allowed via the pg_hba.conf. This is very important if your new PostgreSQL instance is not on the same machine.

10.9.2 Using pg_dumpall

Dumping the database from the old instance

Note
We strongly recommend that you run a test backup/restoration outside of your production environment.

1. Stop the Acronis Cyber Files Tomcat service.
2. Make sure that the Old instance of PostgreSQL is running and that the New instance is stopped.
3. Open the Acronis Cyber Files PostgreSQL Administrator application and connect to the database server. You may be prompted to enter the password for your postgres user.
4. Expand **Databases** and right-click on the acronisaccess_production database.

5. Choose **Maintenance** -> **Vacuum** and press **OK**.
6. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This will help you verify that the database transfer is successful.
7. Close the PostgreSQL Administrator and open an elevated command prompt.
8. In the command prompt, navigate to the PostgreSQL bin directory.
   e.g. `cd "C:\Program Files(x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\bin"`

   If you are using a different product version, your directory path may not be the same. In such cases, you can refer to the choices, listed in the Before you begin section.
9. 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.
10. Once you verify that the dump process is finished, stop the Old PostgreSQL instance and start the New one.

Inserting the database in the new instance

1. Make sure that the New instance of PostgreSQL is running and that the Old instance is stopped.
2. Open the Acronis Cyber Files PostgreSQL Administrator application, connect to the local database server, select **Databases**, and check if there is a database called `acronisaccess_production`. If there isn't one, you will have to create it.
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**.
5. 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`.
6. Close the PostgreSQL Administrator and open an elevated command prompt.
7. Copy the database backup file `alldbs.sql` (or whatever you have named it) into the bin directory of the new instance.
8. In the command prompt, navigate to the PostgreSQL `bin` directory.
   e.g. `cd "C:\Program Files\PostgreSQL\<version>\bin"`

9. Enter the following command: psql -U postgres -f alldbs.sql
10. Enter your postgres password when prompted for it.

> **Note**
> Depending on the size of your database, the restore can take some time.

11. After the restore is complete, close the command prompt window.

Verify that the new instance has the correct database

1. Open the Acronis Cyber Files PostgreSQL Administrator application and connect to the New database server. You may be prompted to enter the password for your postgres user.
2. Expand **Databases** and right-click on the acronisaccess_production database.
3. Expand the database, expand **Schemas** and expand **Public**.
4. Verify that the **Tables** section contains the same number of tables as the one you saw before.
5. Stop the AcronisAccessPostgreSQL (the old DB service) as you no longer need it.
6. Start the new database service postgresql-x64-11.
7. Start the Files Advanced Tomcat service.

10.9.3 Using pg_upgrade

The upgrading proccess

1. Stop the Acronis Cyber Files Tomcat service.
2. Make sure that both instances of PostgreSQL are running. The new instance will typically choose a different port if the Old one is running on the default port.
3. Open the Acronis Cyber Files PostgreSQL Administrator application and connect to the Old database server. You may be prompted to enter the password for your postgres user.
4. Expand **Databases**, expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This will help you verify that the database transfer is successful.
5. Close the PostgreSQL Administrator.
6. Make sure that both PostgreSQL instances can access each-other. This can be done by checking if the pg_hba.conf file has an entry for localhost (127.0.0.1/32) with **Trust** as the authentication method.

> **Note**
> If the New instance is on another machine, you must configure access to that machine.

7. Open an elevated command prompt and navigate to the New PostgreSQL bin directory with the cd command.
   e.g. cd C:\Program Files\PostgreSQL\<version>\bin
8. Use the pg_upgrade command with the following parameters:

pg_upgrade -b <**OLD_BIN_FOLDER**> -B <**NEW_BIN_FOLDER**> -d <**OLD_DATA_FOLDER**> -D <**NEW_DATA_FOLDER**> -U postgres

Note
OLD_BIN_FOLDER refers to the bin folder of the PostgreSQL installation that you wish to upgrade. It's the same for the Data folder.

Note
NEW_BIN_FOLDER refers to the bin folder of the new PostgreSQL installation. It's the same for the Data folder.

Verify that the new instance has the correct database

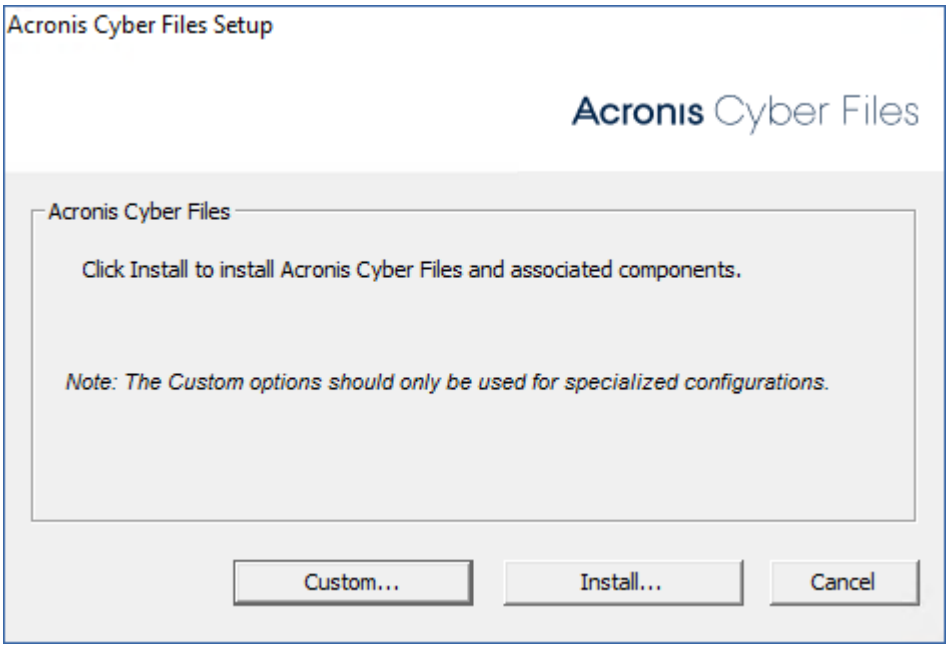
1. Open the Acronis Cyber Files PostgreSQL Administrator application and connect to the New database server. You may be prompted to enter the password for your postgres user.
2. Expand **Databases** and right-click on the acronisaccess_production database.
3. Choose **Maintenance** -> **Vacuum** and press **OK**.
4. Right-click on the acronisaccess_production database again.
5. Choose **Maintenance** -> **Reindex** and press **OK**.
6. Expand the database, expand **Schemas** and expand **Public**.
7. Verify that the **Tables** section contains the same number of tables as the one you saw before.
8. Stop the AcronisAccessPostgreSQL (the old DB service) as you no longer need it.
9. Start the new database service postgresql-x64-11.
10. Start the Files Advanced Tomcat service.

Installing the PostgreSQL database on a remote server

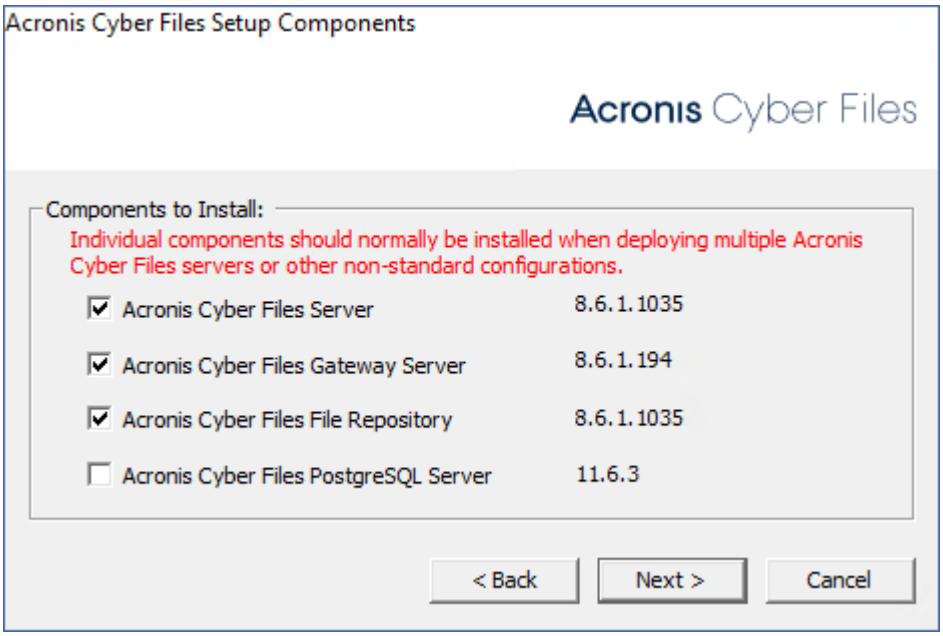
1. Run the PostgreSQL installer. Make sure to remember the PostgreSQL user password.
2. When the installation is complete, update the pg_hba.conf file:
   a. Go to the following location:
      C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\data

      If you are using a different product version, your directory path may not be the same. In such cases, you can refer to the choices, listed in the Before you begin section.
   b. Locate the pg_hba.conf file and open it for edit.
   c. Navigate to the **# IPv4 local connections** row at the bottom.
   d. Change the row below it to: host all all <the tomcat server IP or IP range> md5
3. Update the postgresql.conf file:
   a. Go to the location, corresponding to your product version - should be one of the variants listed in step 2a above
   b. Verify that port **5432** is enabled
   c. Check whether it listens to '*' (listen_addresses = '*')
4. Restart the postgresql-x64-11 service and make sure it starts backup.

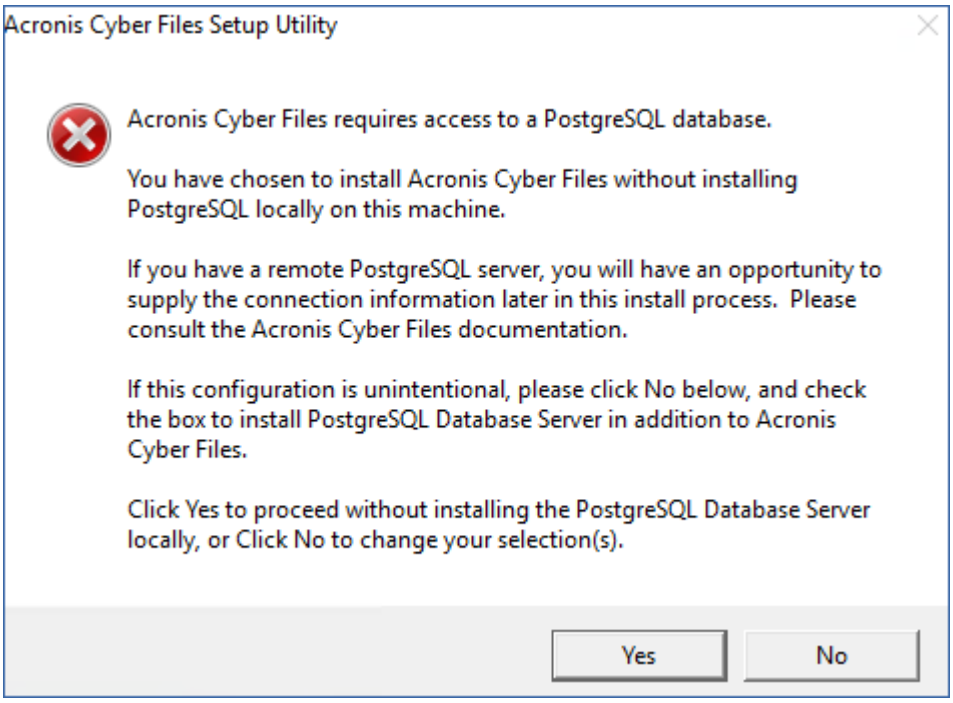
5. Go to the Server where Acronis Cyber Files will be installed.
6. Run a **Custom** installation.



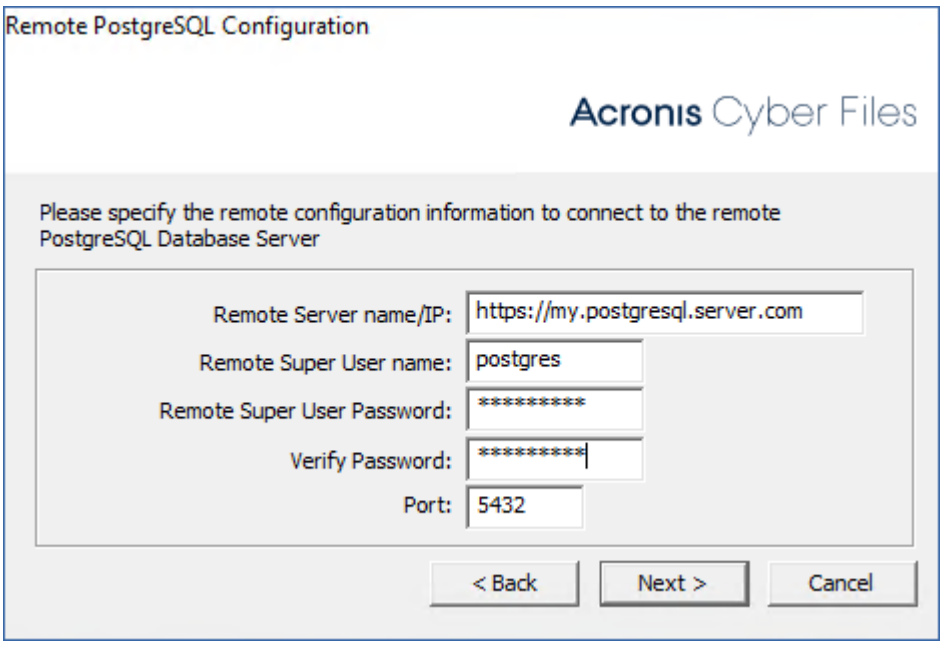
7. Select **Acronis Cyber Files Server, Gateway Server** and **File Repository.** Clear the **PostgreSQL** option.



8. Confirm that you have a remote PostgreSQL.



9. On the **Remote PostgreSQL Configuration** screen, write down the necessary data from the remote server:



   a. Find the remote IP address
   b. Enter the password created in step 1 above
   c. Click **Next**
   d. Continue ONLY if the connection is successful. If not, check for any issues with the configuration files from steps 2 and 3.

10. Finish the installation.

Note

To run the new PostgreSQL for the first time, you should open it using any browser.

11 Supplemental Material

11.1 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 white 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.

11.2 For the Acronis Cyber Files Server

11.2.1 Load balancing Acronis Cyber Files

There are two main ways you can load balance Acronis Cyber Files:

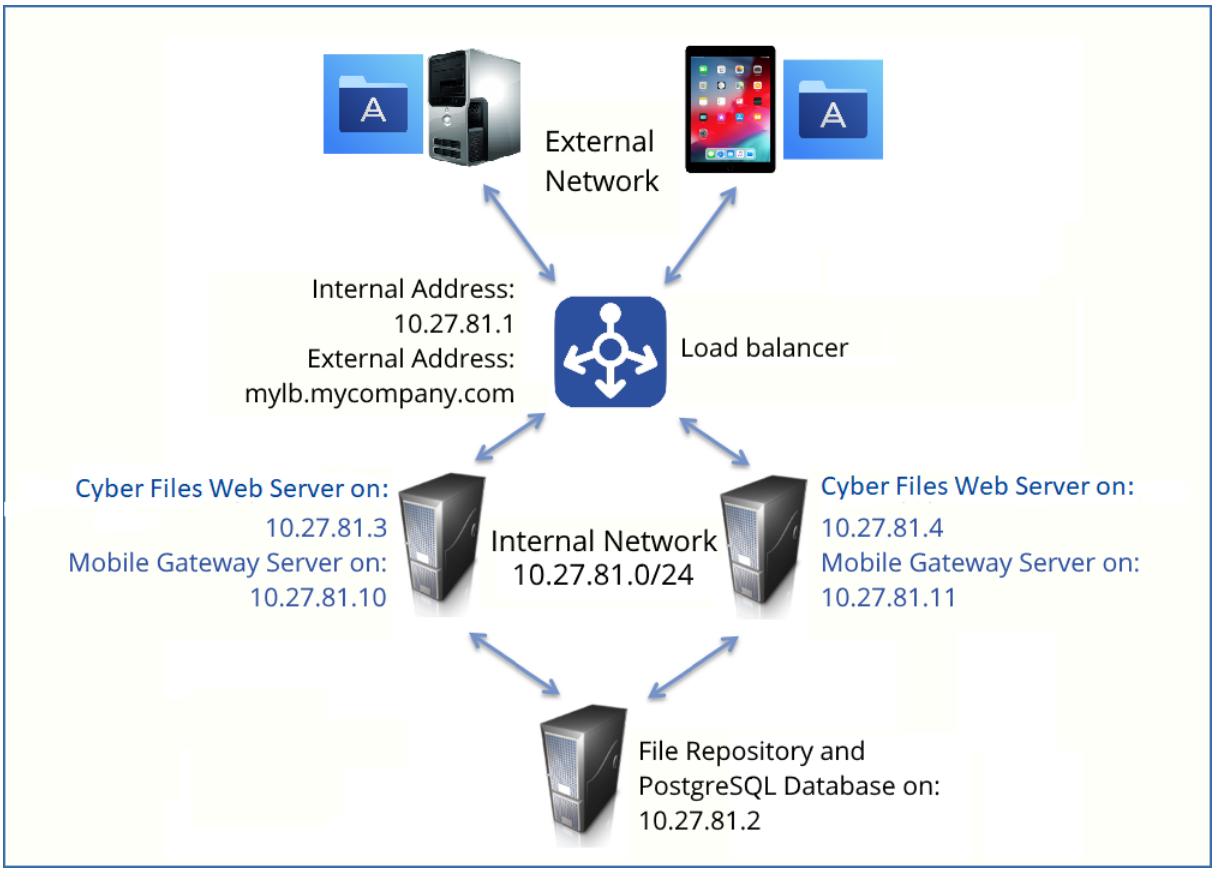
Load balancing only the Acronis Cyber Files Mobile Gateways

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.



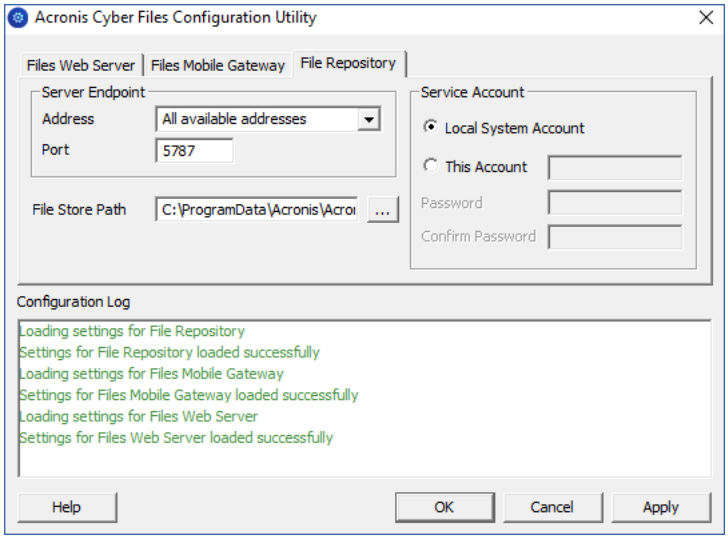
This guide will provide the details necessary to properly load balance the Acronis Cyber Files product in your environment.

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**.
7. a. 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.

b. Select the path to the File Store. This is where the actual files will reside.



c. Click **OK** to apply changes and close the **Configuration Utility**.

8. 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.
9. 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.
10. 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.

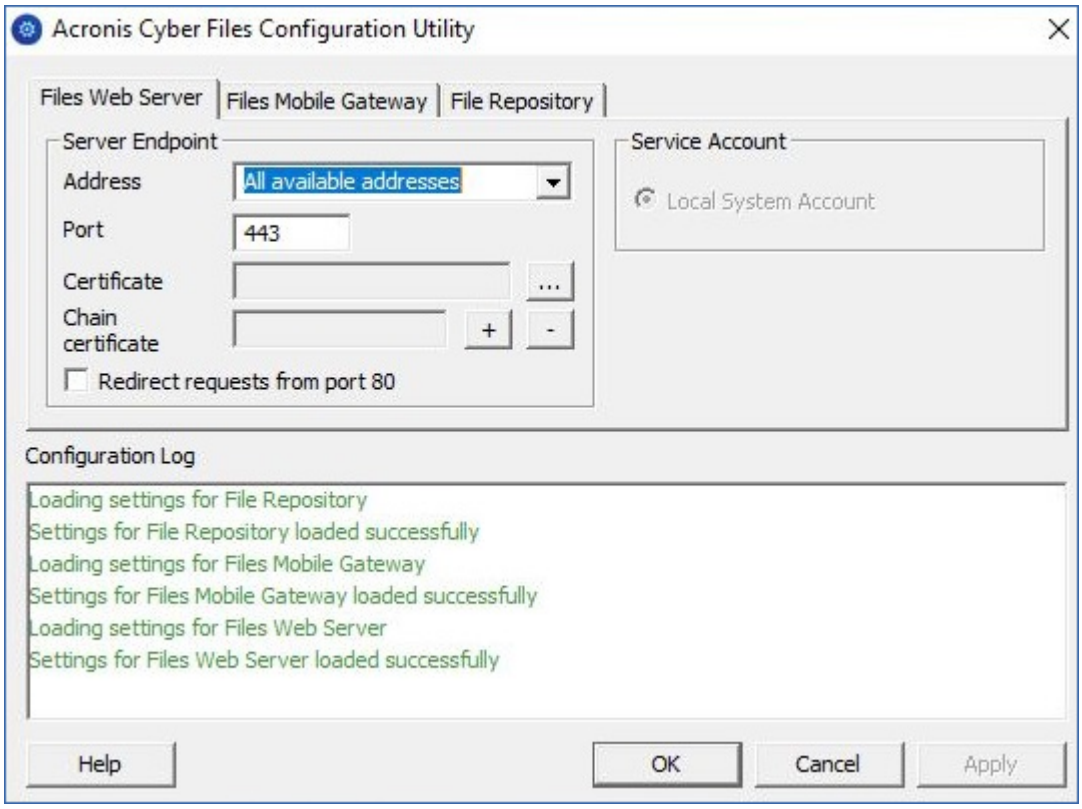
11. Open the **Acronis Cyber Files PostgreSQL Administrator tool** (it could also be called PgAdmin).You can find it in Windows Start menu, under the Acronis Cyber Files folder. Connect to your local server, select **Databases**, and either right-click or select **New Database** from the **Edit** -> **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**.
4. a. **On the Acronis Cyber 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.
   - Press **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.

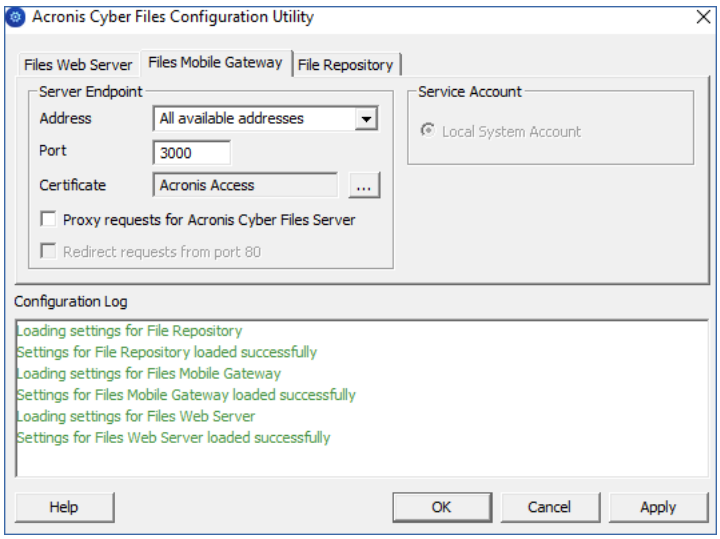


b. **On the Acronis Cyber Files Mobile Gateway tab:**

- 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.
- Press **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.



5. 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.
6. 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
7. 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.
2. This will populate the database you have created.
3. 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.

- Press **Save**.

d. **Under the LDAP tab:**

Note
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)
- Press **Save**.

a. **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).
- Press **Save**.

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.

11.2.2 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 Tomcat's max memory usage

1. Start the **Acronis Cyber Files Tomcat Service Configuration** tool from your desktop. If it's not there, go to **Start** –> **All Programs** –> **Acronis Cyber Files** and click on the shortcut.
2. Click on the **'Java'** tab.
3. Increase the '**Maximum memory pool**' setting to **24576** and click **OK**.

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 "%r" %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.

11.2.3 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.

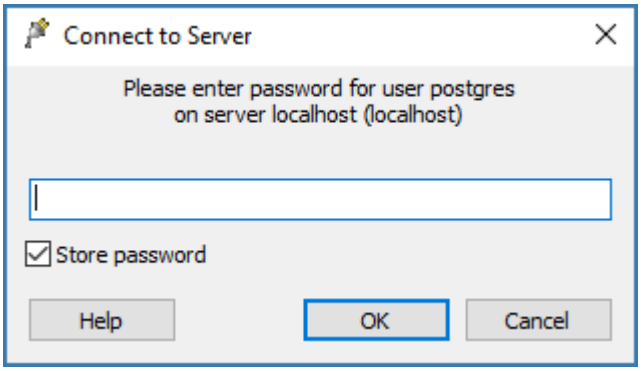
Migrating the PostgreSQL server

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 and choose **Maintenance** -> **Vacuum** -> **OK**.



4. 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).
5. 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
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.

6. Once the backup finishes, stop and disable the **Acronis Cyber Files PostgreSQL Server** service.
7. 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!

11.2.4 Configure Tomcat's max memory usage

1. Start the **Acronis Cyber Files Tomcat Service Configuration** tool from your desktop. If it's not there, go to **Start** –> **All Programs** –> **Acronis Cyber Files** and click on the shortcut.
2. Click on the **'Java'** tab.
3. Increase the '**Maximum memory pool**' setting to **24576** and click **OK**.

11.2.5 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.

11.2.6 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.

11.2.7 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 "%r" %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 fo r Acronis <P RODUCT_NAME> 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).

11.2.8 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!

   a. 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.

11.2.9 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.

11.2.10 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.

  Note: 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

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.

Note
for example, computerAccess.domain.com / computer.domain.com and computerAccess.domain.com / computerGW.domain.com will work

Note
for example, 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 **<**
   - **>** with **>**
   - **"** with **"**
   - **'** with **'**
   - **&** with **&**

   e.g. if your password is <my&best'password" you will have to write it in the web.xml file as follows: <my&best'password"

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.

   a. 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:

   Note
   [libdefaults]

   Note
   default_realm = ACME.COM

   Note
   default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

   Note
   default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
[realms]

Note
ACME.COM = {

Note
kdc = acmedc.ACME.COM

Note
default_domain = ACME.COM

Note
[domain_realm]

Note
.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. Press **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.

On any user's machine

This is a small, one-time configuration that must be made on the client machine to enable Single Sign-On support for your browser.

Note
This needs to be done for each user on each machine.

Note
If you have services in multiple domains, repeat the section for your browser with the second domain name. **e.g.** add both *.acme.com and *.tree.com.

Windows:

For Internet Explorer:

- Open Internet Explorer and go to **Tools** -> **Internet Options** -> **Security** -> **Local Intranet** -> **Sites** -> **Advanced** and add the address of your Acronis Cyber Files server - e.g. https://ahsoka.acme.com (or just *.acme.com) and restart the browser.

For Chrome:

Chrome uses the same settings as **Internet Explorer**, so once you've configure it for SSO, **Chrome** will just work as well. However, to enable credential delegation, which is necessary for browsing network nodes from the Web interface, you must configure **Chrome** to allow it (**Internet Explorer** allows it by default):

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**.

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 whitelist 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.

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

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.

Note
for example, computerAccess.domain.com / computer.domain.com and computerAccess.domain.com / computerGW.domain.com will work

Note
for example, 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 **<**
   - **>** with **>**
   - **"** with **"**
   - **'** with **'**
   - **&** with **&**

   e.g. if your password is **<my&best'password"** you will have to write it in the web.xml file as follows: `<my&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.

   a. 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:

Note
[libdefaults]

Note
default_realm = ACME.COM

Note
default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
[realms]

Note
ACME.COM = {

Note
kdc = acmedc.ACME.COM

Note
default_domain = ACME.COM

Note
[domain_realm]

Note
.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. Press **Save**.

On any user's machine

This is a small, one-time configuration that must be made on the client machine to enable Single Sign-On support for your browser.

Note
This needs to be done for each user on each machine.

Note
If you have services in multiple domains, repeat the section for your browser with the second domain name. **e.g.** add both *.acme.com and *.tree.com.

Windows:

For Internet Explorer:

- Open Internet Explorer and go to **Tools** -> **Internet Options** -> **Security** -> **Local Intranet** -> **Sites** -> **Advanced** and add the address of your Acronis Cyber Files server - e.g. https://ahsoka.acme.com (or just *.acme.com) and restart the browser.

For Chrome:

Chrome uses the same settings as **Internet Explorer**, so once you've configure it for SSO, **Chrome** will just work as well. However, to enable credential delegation, which is necessary for browsing network nodes from the Web interface, you must configure **Chrome** to allow it (**Internet Explorer** allows it by default):

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**.

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 whitelist 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.

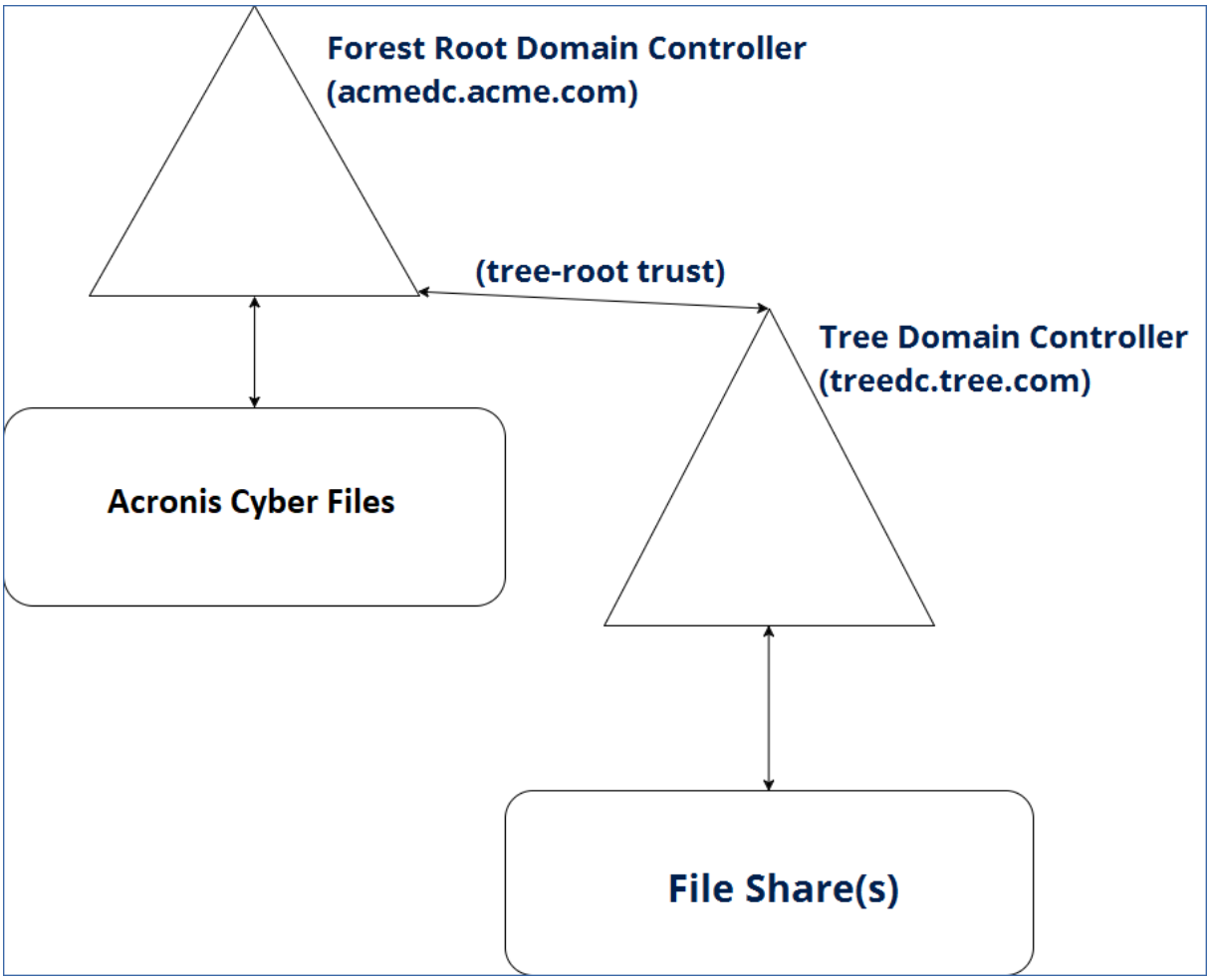
Acronis Cyber Files in a Domain Forest

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.

On any user's machine

This is a small, one-time configuration that must be made on the client machine to enable Single Sign-On support for your browser.

Note
This needs to be done for each user on each machine.

Note
If you have services in multiple domains, repeat the section for your browser with the second domain name. **e.g.** add both *.acme.com and *.tree.com.

Windows:

For Internet Explorer:

- Open Internet Explorer and go to **Tools** -> **Internet Options** -> **Security** -> **Local Intranet** -> **Sites** -> **Advanced** and add the address of your Acronis Cyber Files server - e.g. https://ahsoka.acme.com (or just *.acme.com) and restart the browser.

For Chrome:

Chrome uses the same settings as **Internet Explorer**, so once you've configure it for SSO, **Chrome** will just work as well. However, to enable credential delegation, which is necessary for browsing network nodes from the Web interface, you must configure **Chrome** to allow it (**Internet Explorer** allows it by default):

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**.

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 whitelist 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 **<**
   - **>** with **>**
   - **"** with **"**
   - **'** with **'**
   - **&** with **&**

   e.g. if your password is <my&best'password" you will have to write it in the web.xml file as follows: <my&best'password"

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.

   a. 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:

Note
[libdefaults]

Note
default_realm = ACME.COM

Note
default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

Note
[realms]

Note
ACME.COM = {

Note
kdc = acmedc.ACME.COM

Note
default_domain = ACME.COM

Note
[domain_realm]

Note
.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

11.2.11 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**.

11.2.12 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.

   - fore 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. Press **OK**.

11.2.13 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.

11.2.14 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**.

11.2.15 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
   a. 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**.

11.3 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.

11.4 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.

11.4.1 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.

11.5 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.

11.5.1 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
```

1. 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.

2. 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).
3. The fields email address, optional company name and challenge password can be left blank for a web server certificate.
4. 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:

Note
openssl pkcs12 -export -in <yourcertificate.extension> -inkey <yourkey.extension> -out <newfile.pfx>

Note
e.g. openssl pkcs12 -export -in acmecert.crt -inkey acmecertkey.key -out acmecombined.pfx

Note
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**, and then click **Run**.
2. In the **Open box**, type **mmc**, and 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**, and then click **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), and then click **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**, and 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.

11.5.2 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**").

11.5.3 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
5. **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.
6. Open the **Configuration Utility**.
7. In the **File Repositor**y tab, change the path of the **FileStore** to the new path where you've moved the **FileStore** folder.
8. Start **Acronis Cyber Files File Repository Server** service.
9. 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.

11.5.4 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

Note
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.

11.5.5 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+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:!aN
   ULL:!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+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:!aN
   ULL:!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.

11.5.6 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. Press **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).

Note
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:

Note

netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true

11.5.7 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.

Installing and configuring the servlet

Tomcat Installation

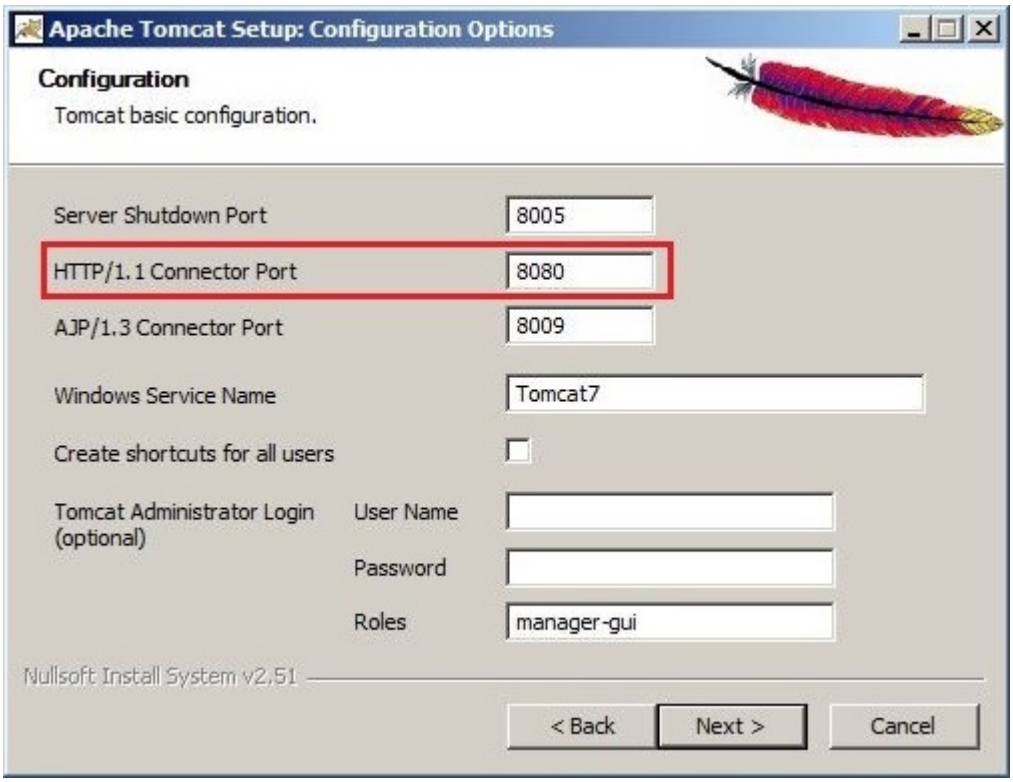
You can install an Apache Tomcat 7 server either from a .zip file or with an installation executable. We recommend using the installer, but, the .zip archive works as well. The only difference will be the way you will have to configure the Apache Tomcat 7 server.

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 7. 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 listed in the What's New section.

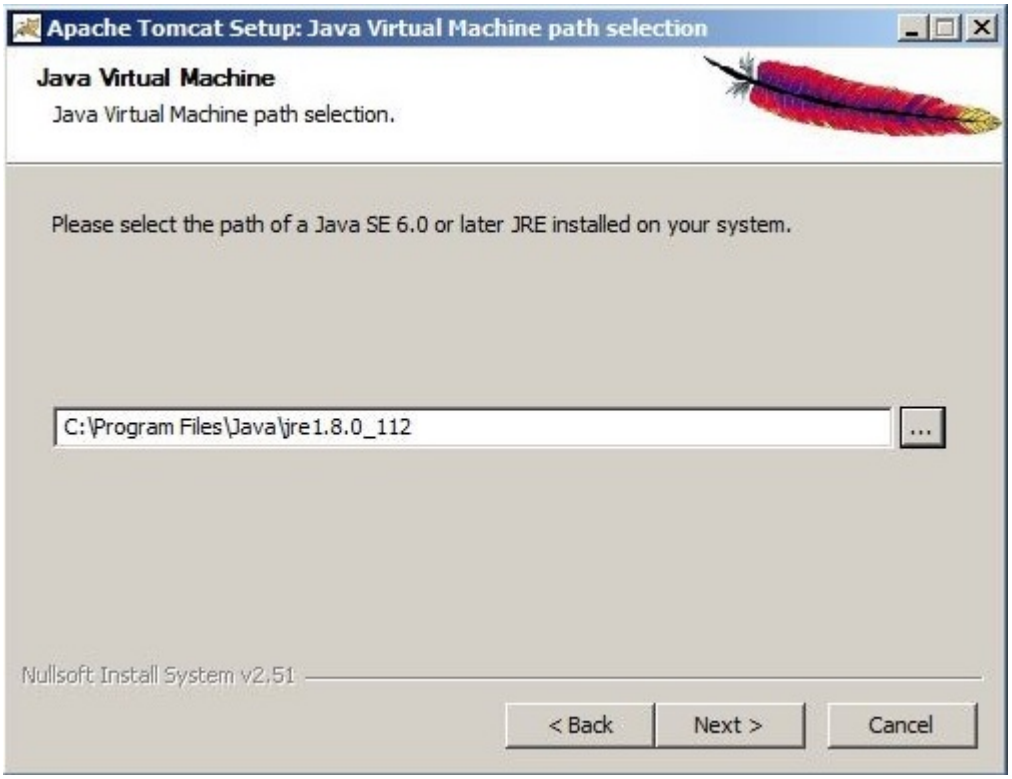
Using an installation executable

1. Download an installation file with the 64bit version of Apache Tomcat 7. 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-7.0.50.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.



Note

The installer will pick up the Java installation folder automatically.



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 7.0\webapps)
5. Navigate to the **conf** folder of your Apache Tomcat installation (by default C:\Program Files\Apache Software Foundation\Tomcat 7.0\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 7.0\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 7. 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-7.0.50.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-7.0.75**

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-7.0.75"

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-7.0.75\webapps).
9. Navigate to the **conf** folder of your Apache Tomcat installation (e.g. **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\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-7.0.75\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:

Note
<Connector port="**8080**" protocol="HTTP/1.1"

Note
connectionTimeout="20000"

Note
redirectPort="8443" />

Note
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

11.5.8 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 9.4: We will implement features like "replication slot" that require PostgreSQL 9.4. This version is actually embedded with Acronis Access Advanced 7.2 and is installed only during new installations (and 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) and/or only allow 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. Navigate to the PostgreSQL installation folder. By default, it is located in `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>`
2. Navigate into the `Data` folder and modify the `postgresql.conf` file. Find and edit the following lines:

Note
Make sure that these lines are not preceded by a **#** symbol. If they are, the commands are regarded as comments and will not have any effect.

3.
   - listen_address = '**IP_OF_PRIMARY_SERVER**, 127.0.0.1'
   - wal_level = hot_standby
   - max_wal_senders = 3
   - checkpoint_segments = 8
   - wal_keep_segments = 8
   - max_replication_slots = 3
4. 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. This can be done by navigating to the PostgreSQL installation folder and editing the **pg_hba.conf** file (located in the data sub-folder) and by adding the following line for each server:
   ```
   host all all <IP_OF_FILES_ADVANCED_SERVER_1>/32 md5
   host all all <IP_OF_FILES_ADVANCED_SERVER_1>/32 md5
   ```

Configure streaming replication

1. Navigate to the PostgreSQL installation folder. By default, it is located in C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>
2. Navigate into the Data folder and modify the postgresql.conf file. Find and edit the following lines:

   Note
   Make sure that these lines are not preceded by a **#** symbol. If they are, the commands are regarded as comments and will not have any effect.

3. - listen_address = '**IP_OF_STANDBY_SERVER**, 127.0.0.1'
   - wal_level = hot_standby
   - max_wal_senders = 3
   - checkpoint_segments = 8
   - wal_keep_segments = 8
   - max_replication_slots = 3
   - 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
   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.

   Note
   primary_conninfo = 'host=<IP_ADDRESS_OF_PRIMARY_SERVER> port=<PORT_OF_PRIMARY_SERVER> user=<USERNAME> password=<PASSWORD_FOR_USERNAME>'

   Note
   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'

4. **Stop the PostgreSQL service on the Primary 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 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 --xlog-method=stream

   Note
   <PATH_TO_NEW_DATA_DIR> should be the path to the renamed/deleted Data folder. e.g. C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\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.

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 the Primary server by creating the trigger file that was mentioned in the **recovery.conf**. Now that 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.

This can be done by navigating to C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server and editing acronisaccess.cfg. Make sure that the DB_HOSTNAME and DB_PORT are pointed to the address and port of whichever PostgreSQL server is currently the Primary Server. If you make any changes, you will have to restart the Acronis Cyber Files Tomcat service.

11.5.9 Configuring PostgreSQL for remote access

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.

11.5.10 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+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" 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:

1. REQUIRE_SSL = false
2. Save the file after you've made the necessary changes.
3. 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

11.5.11 Upgrading Acronis Cyber Files on a Microsoft Failover Cluster

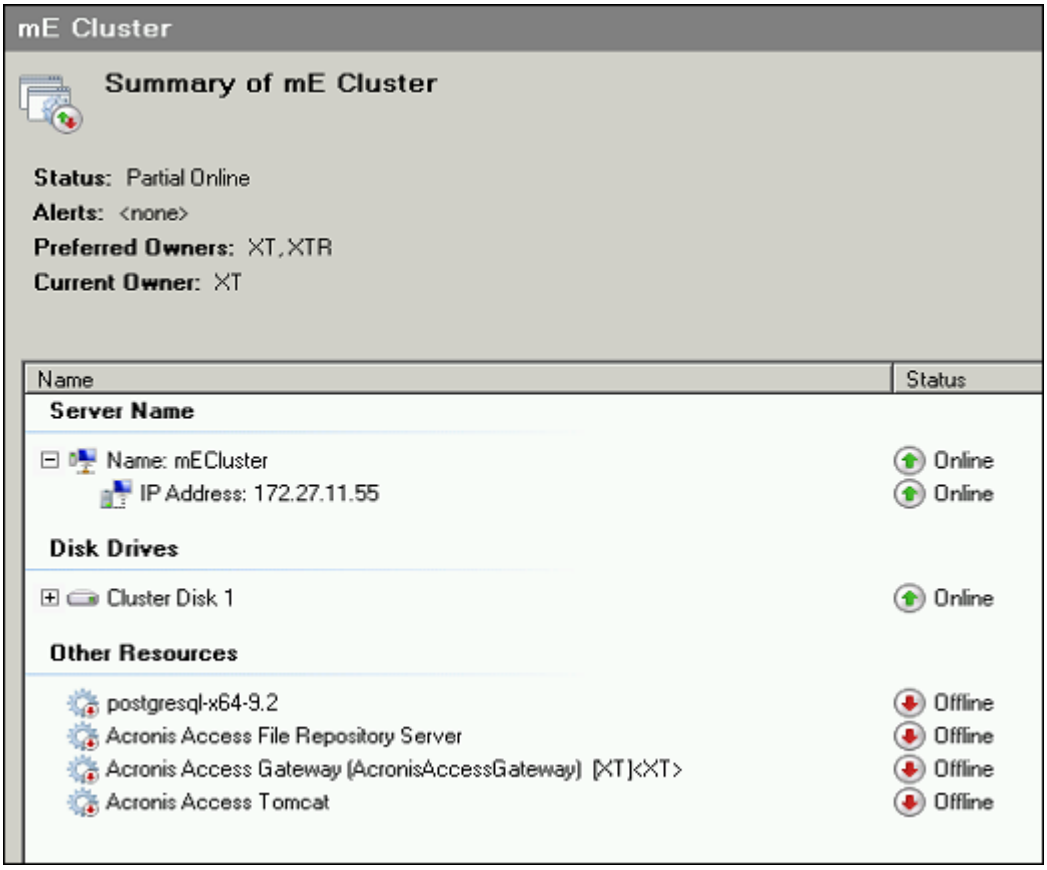
The following steps will help you upgrade your Acronis Cyber Files Server cluster to a newer version of Acronis Cyber Files.

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

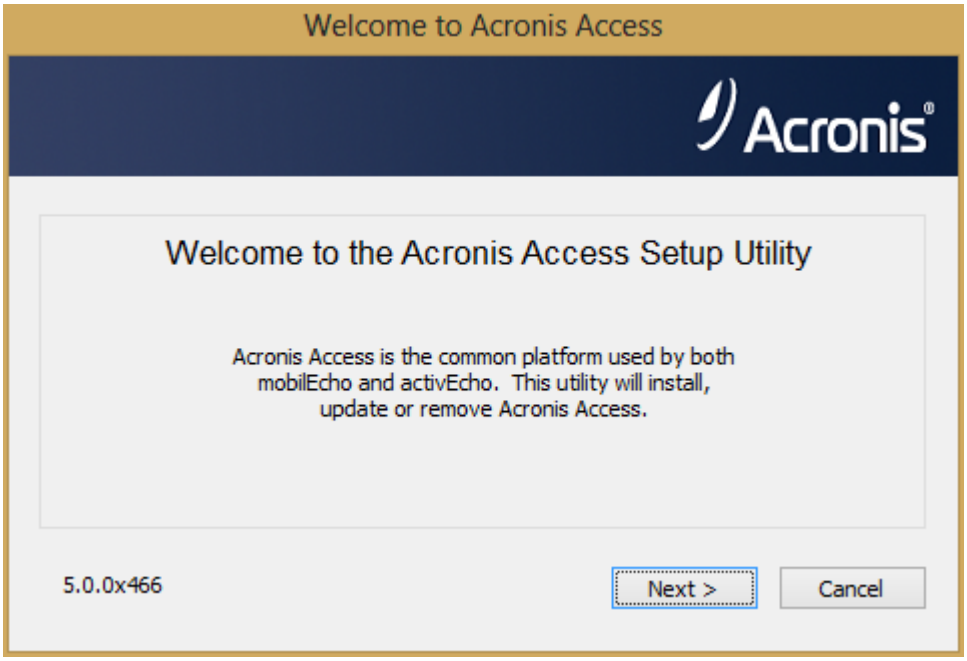
---

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

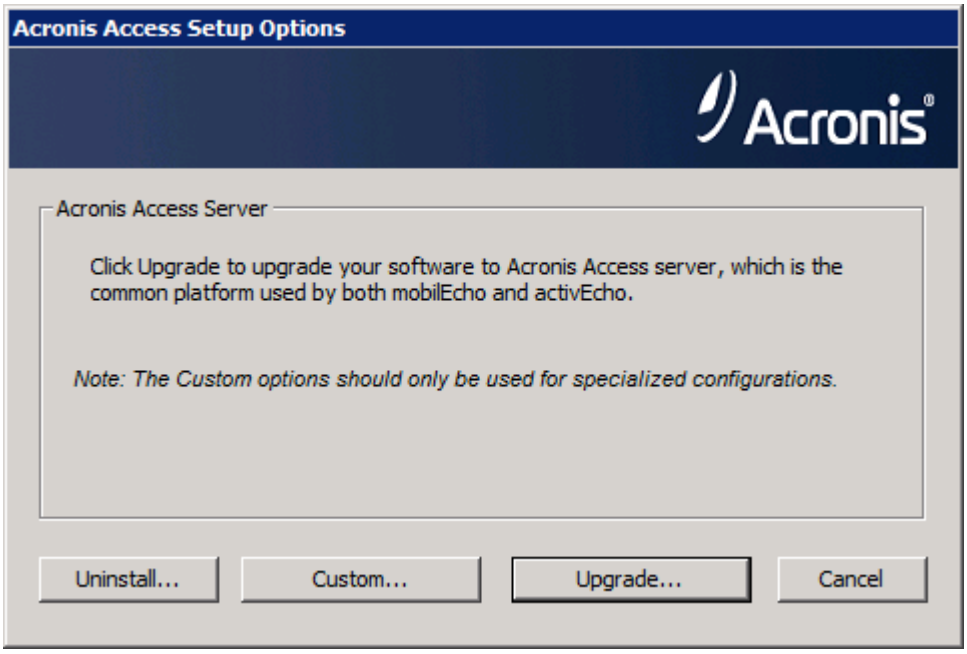
must be online.



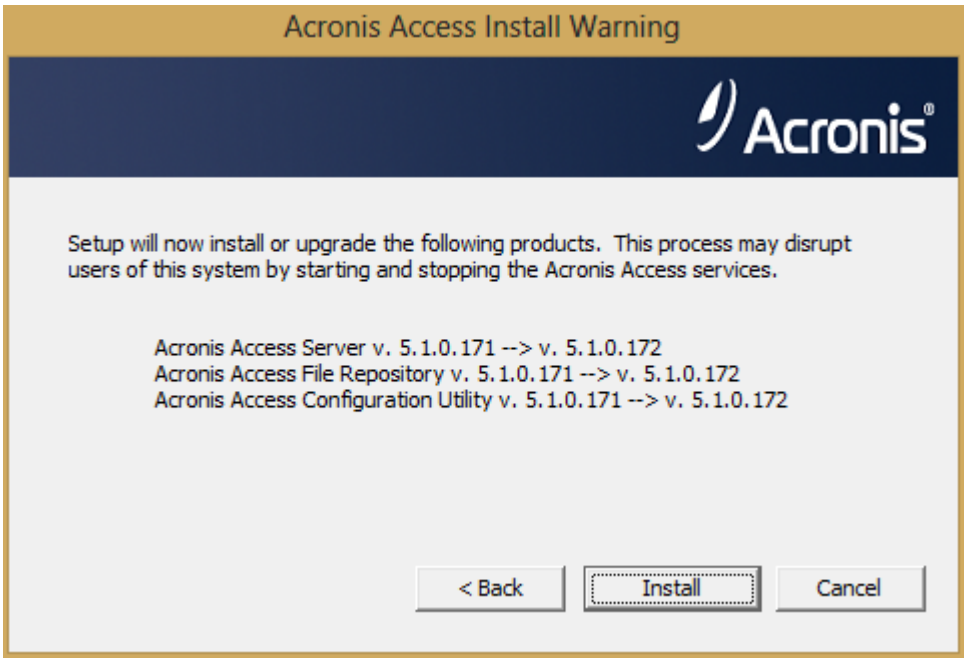
1. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
2. Double-click on the installer executable.



3. Press **Next** to begin.
4. Read and accept the license agreement.
5. Press **Upgrade**.



6. Review the components which will be installed and press **Install**.



7. Enter the password for your **postgres** super-user and press **Next**.
8. When the installation finishes, press **Exit** to close the installer.

Warning!
Do not bring the cluster group online!

9. Move the cluster group to the second node.

10. Complete the same installation procedure on the second node.
11. Bring all of the Acronis Cyber Files services online.

11.5.12 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

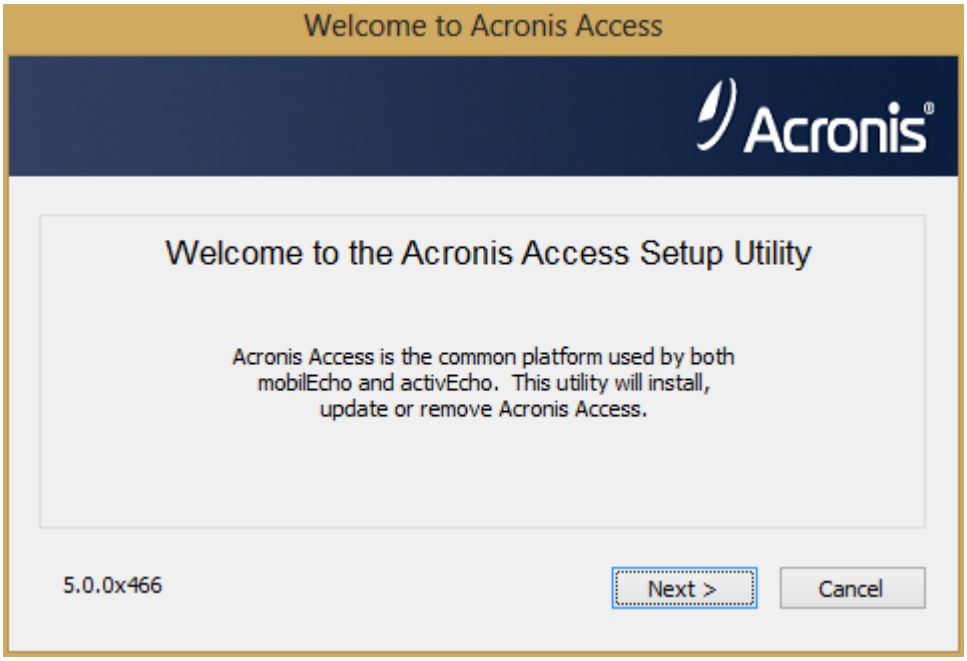
Installing Acronis Cyber Files

Please make sure you are logged in as a domain administrator before installing Acronis Cyber Files.

1. Download the Acronis Cyber Files installer.

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

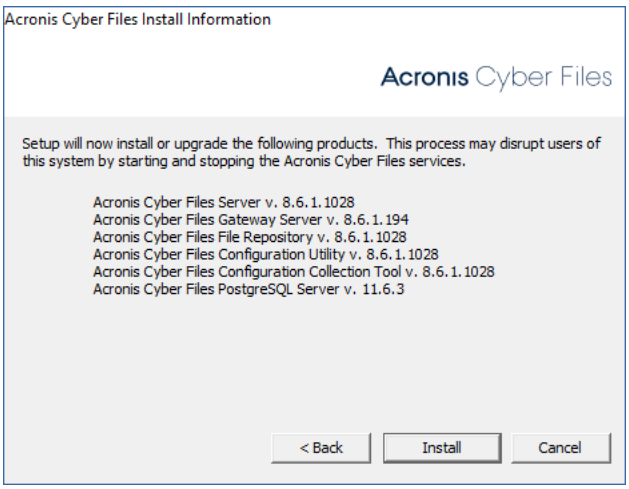
2. Double-click on the installer executable.



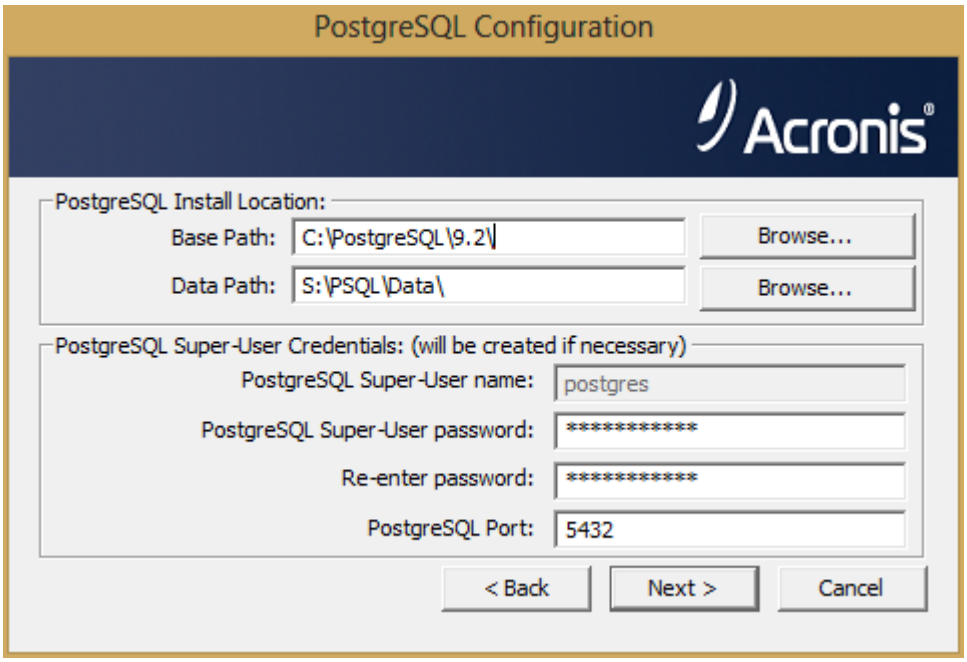
3. Press **Next** to begin.
4. Read and accept the license agreement.
5. Press **Install**.

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 press OK.



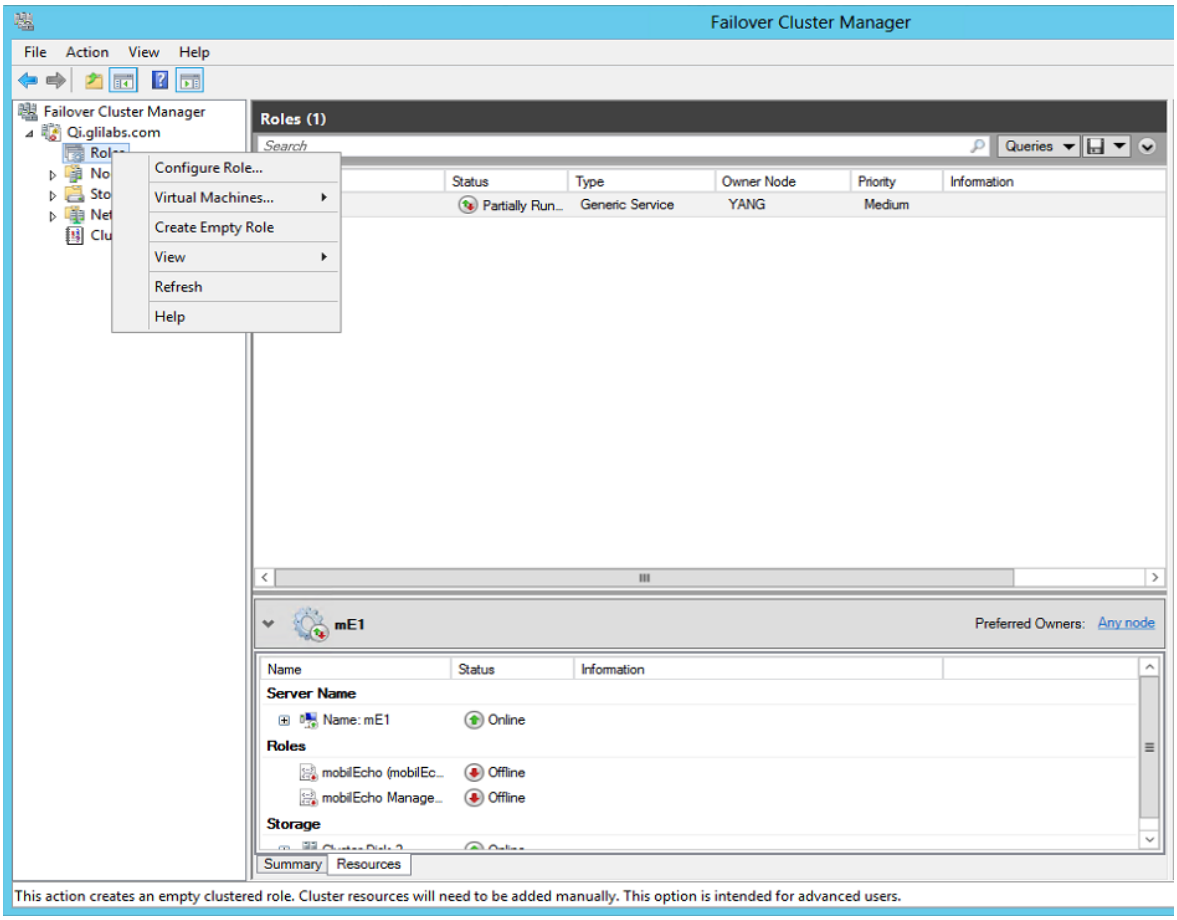
7. Set a password for the user Postgres and write it down. This password will be needed for database backup and recovery.
8. Choose a location on a shared disk for the **Postgres Data** folder and press **Next**.



9. A window displaying all the components which will be installed appears. Press **OK** to continue.
10. When the Acronis Cyber Files installer finishes, press **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)



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/').

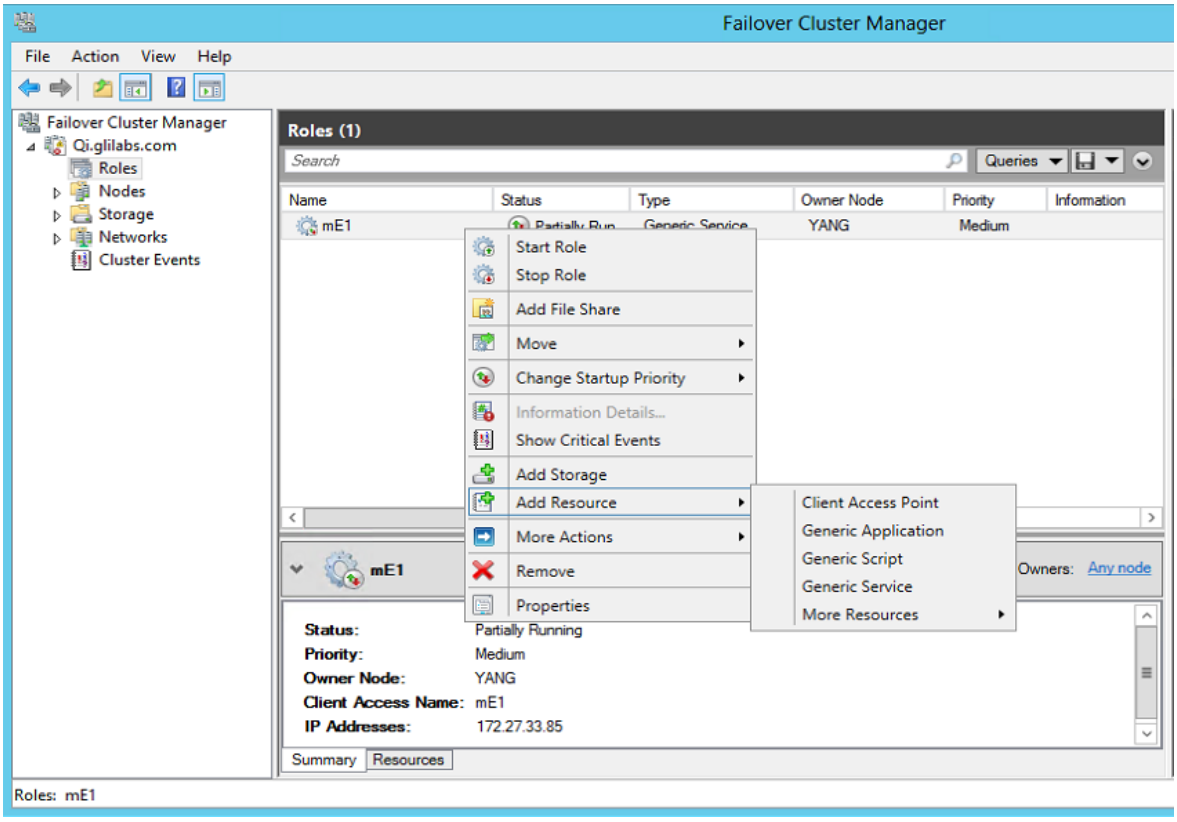
> **Note**
> Use slashes(/) as a path separator.

> **Note**
> You can copy the configured database.yml from the first node and paste it to the second node.

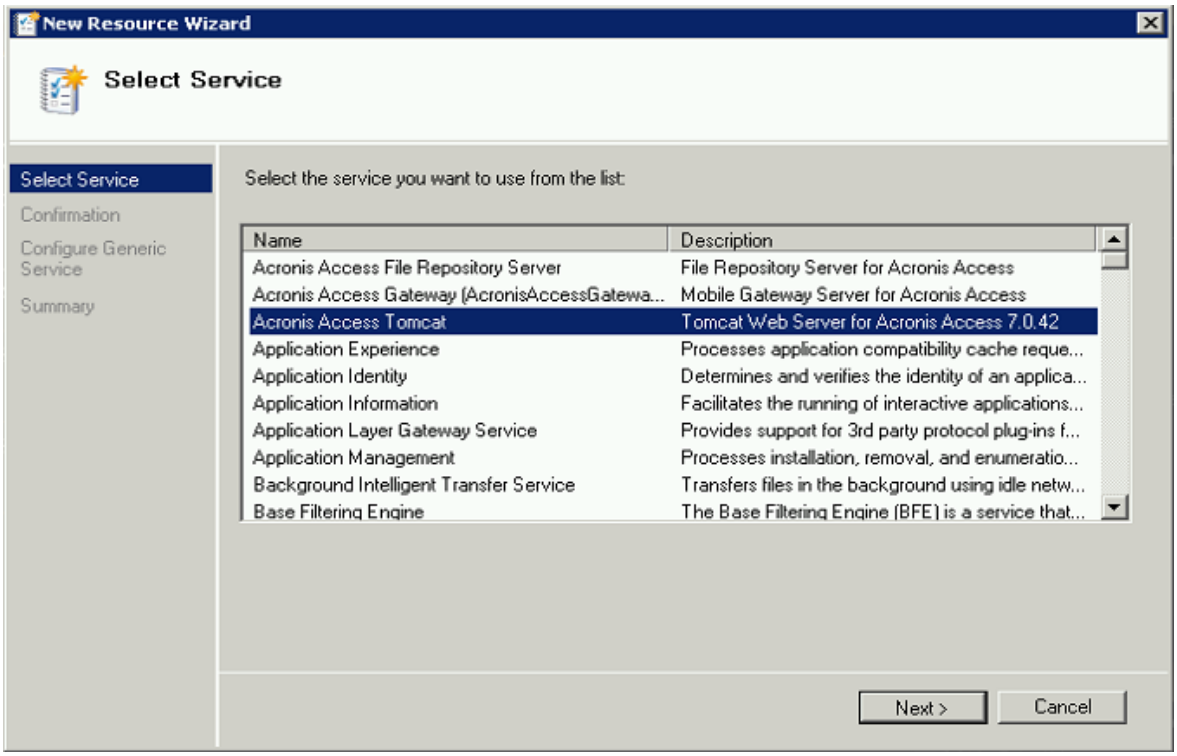
Adding all of the necessary services to the Acronis Cyber Files role

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**.

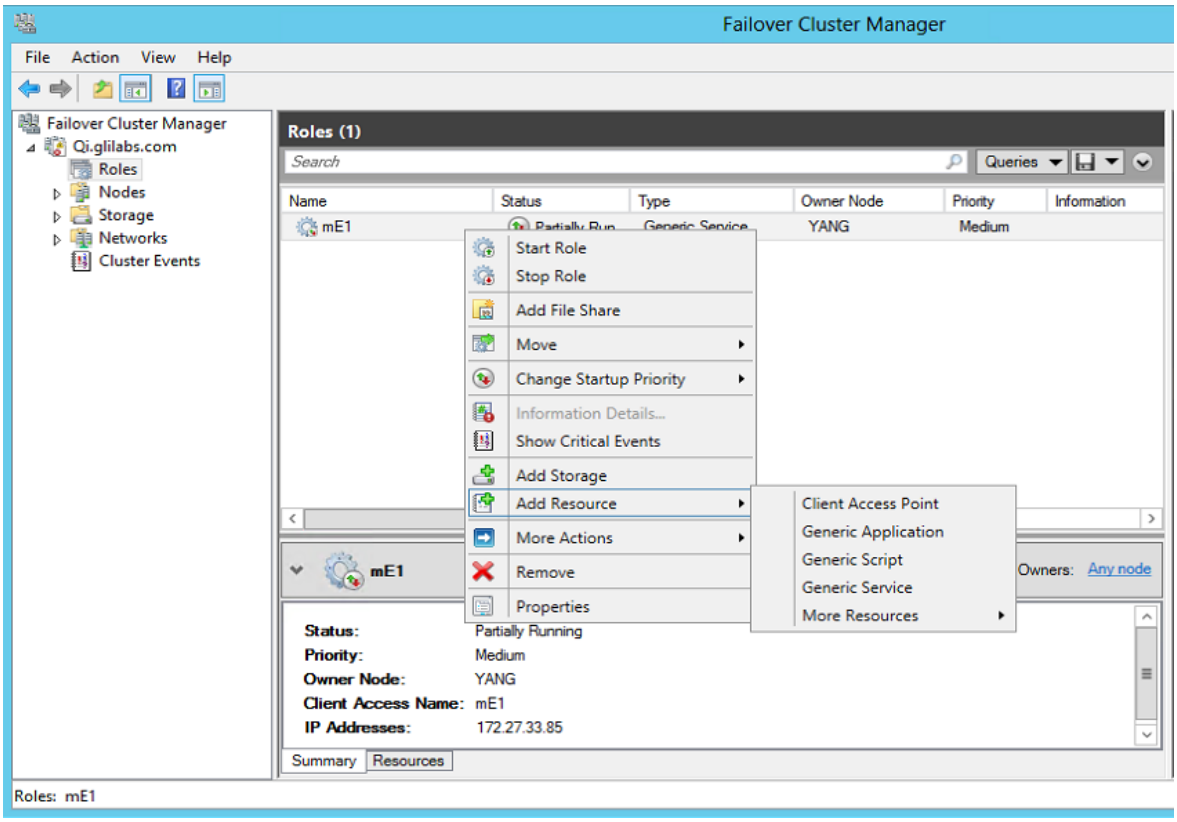
2. Select **Generic Service**.
3. 

4. Select the proper service and press **Next**.

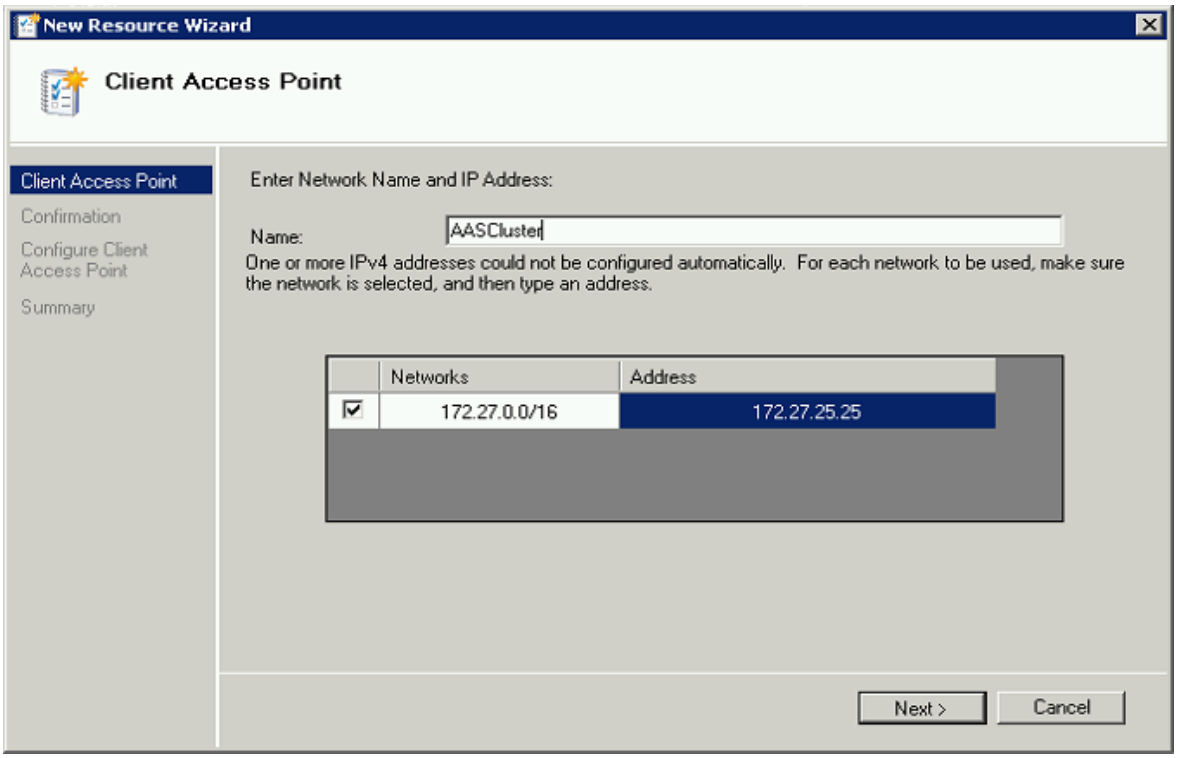


5. On the Confirmation window press **Next**.
6. On the summary window press **Finish**.

Setting an Access Point

1. Right-click on the Acronis Cyber Files role and select **Add a resource**.
2. Select **Client Access Point**.
3. 

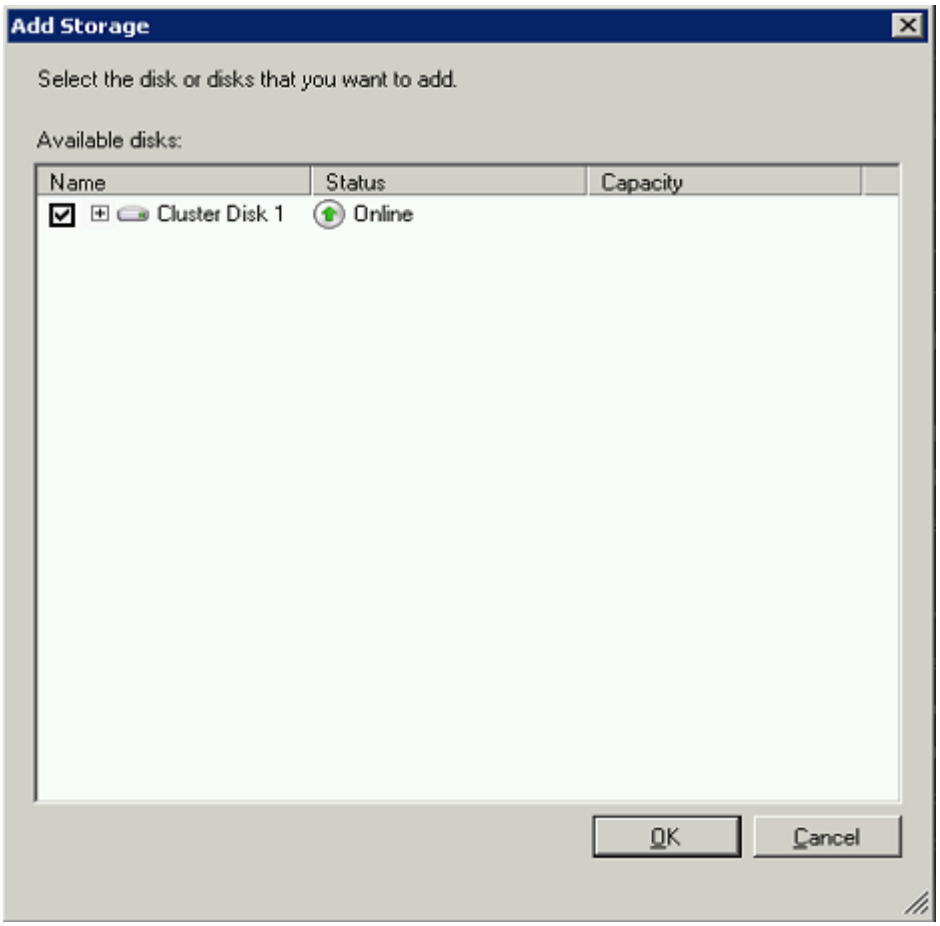
4. Enter a name for this access point.
5. Select a network.



6. Enter the IP address and press **Next**.
7. On the Confirmation window press **Next**.
8. On the summary window press **Finish**.

Adding a shared disk

1. Right-click on the Acronis Cyber Files role and select **Add Storage**.
2. Select the desired shared drive.



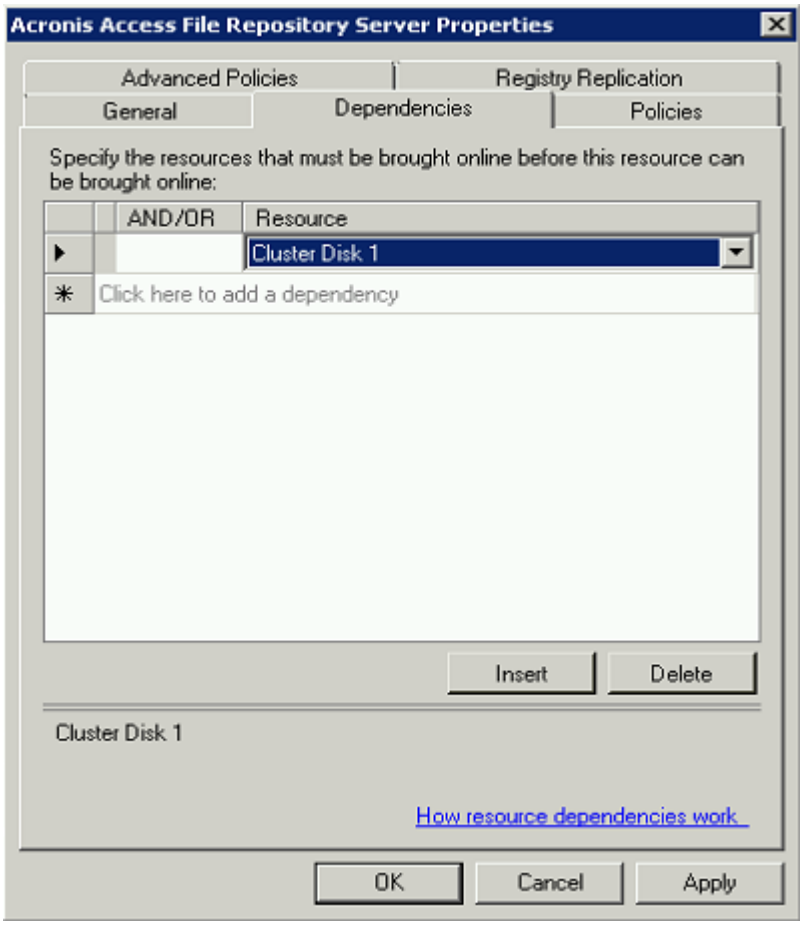
Configuring dependencies

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.

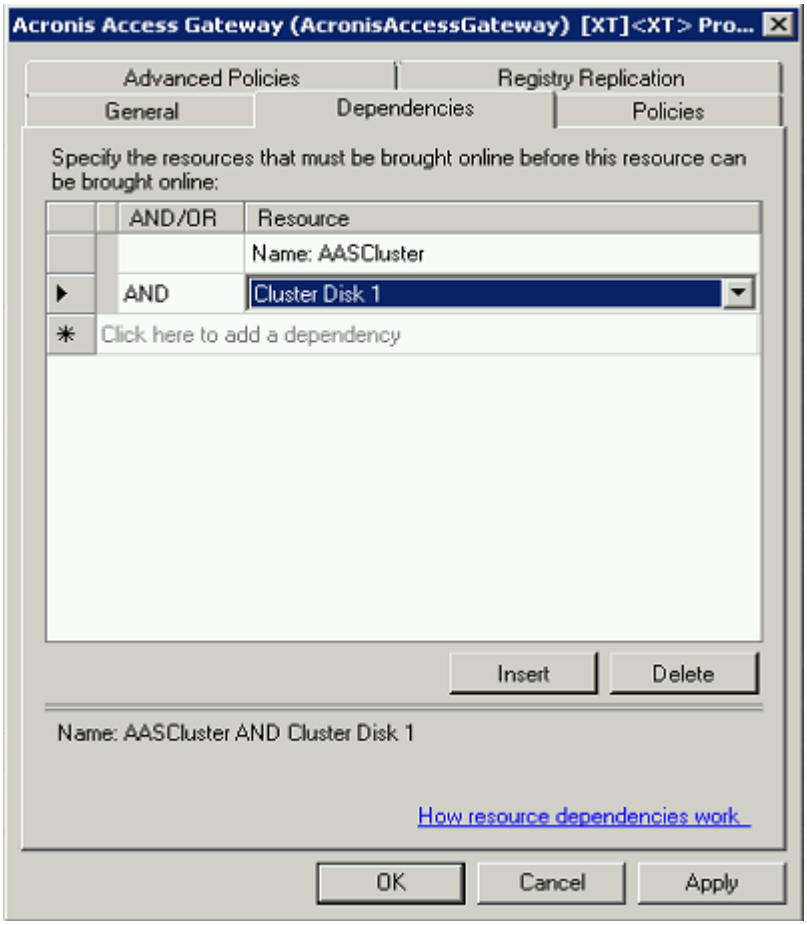
3. Click on **Resource** and select the shared disk you have added.



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).

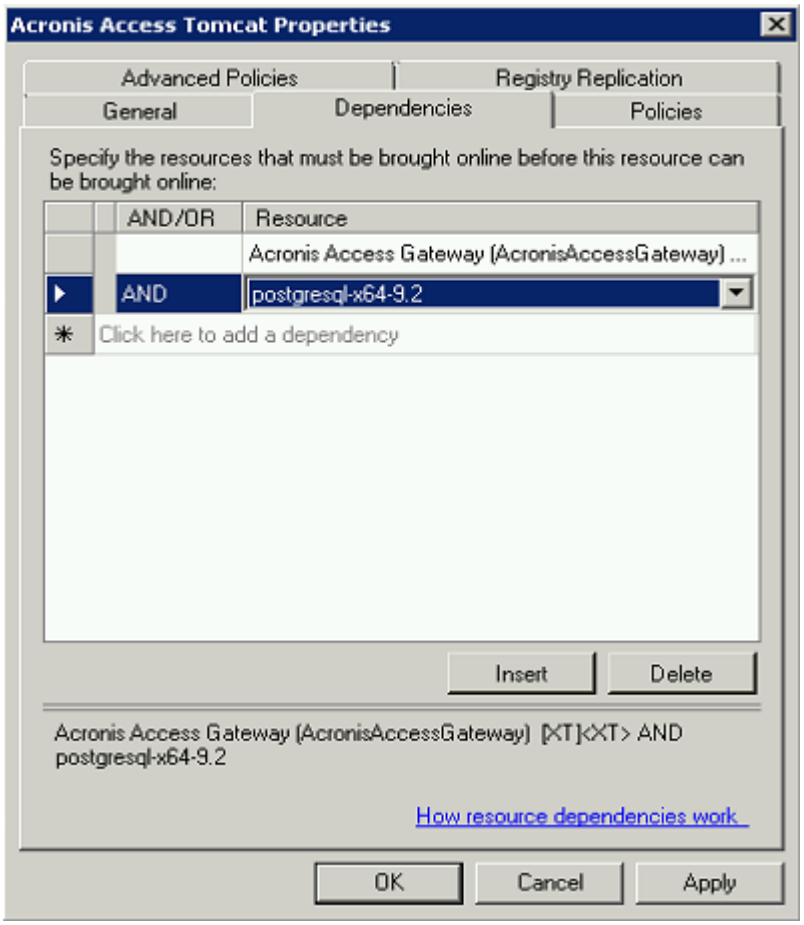


4. Press **Apply** and close the window.

For the Acronis Cyber Files Tomcat service do the following:

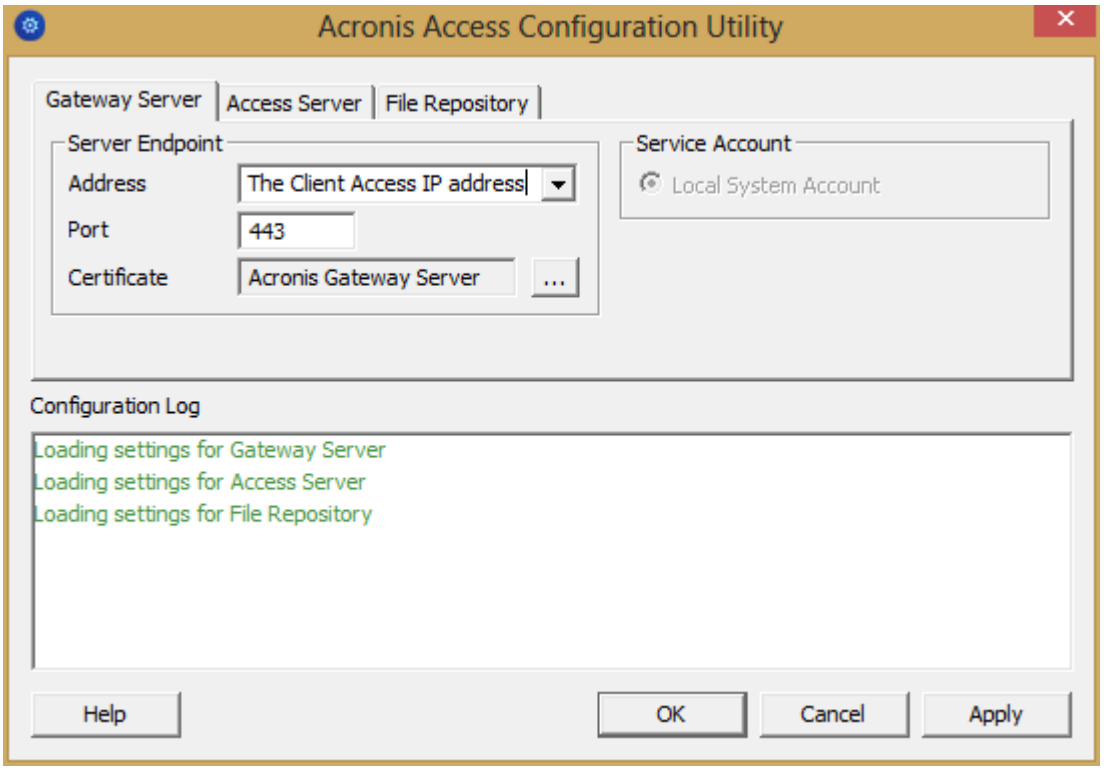
1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the PostgreSQL and Acronis Cyber Files Gateway Server services as dependencies. Press **Apply** and close the window.

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.

- 

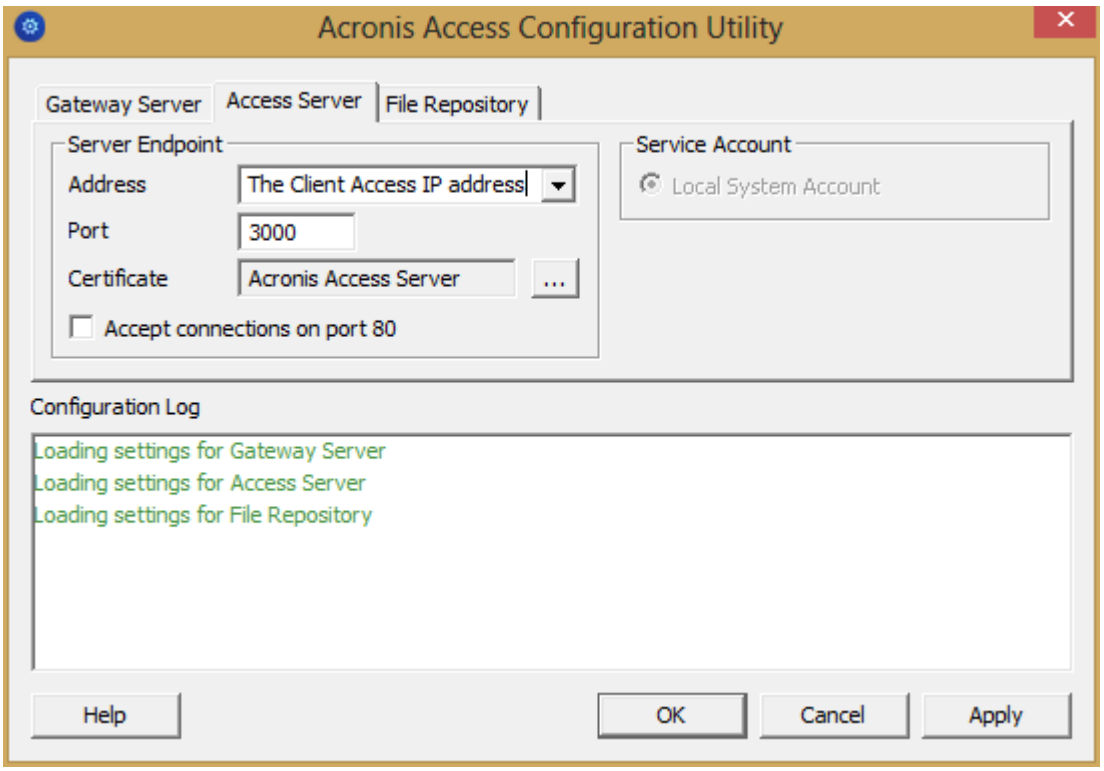
Starting the role and using the Configuration Utility

1. Right-click on the Acronis Cyber 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.

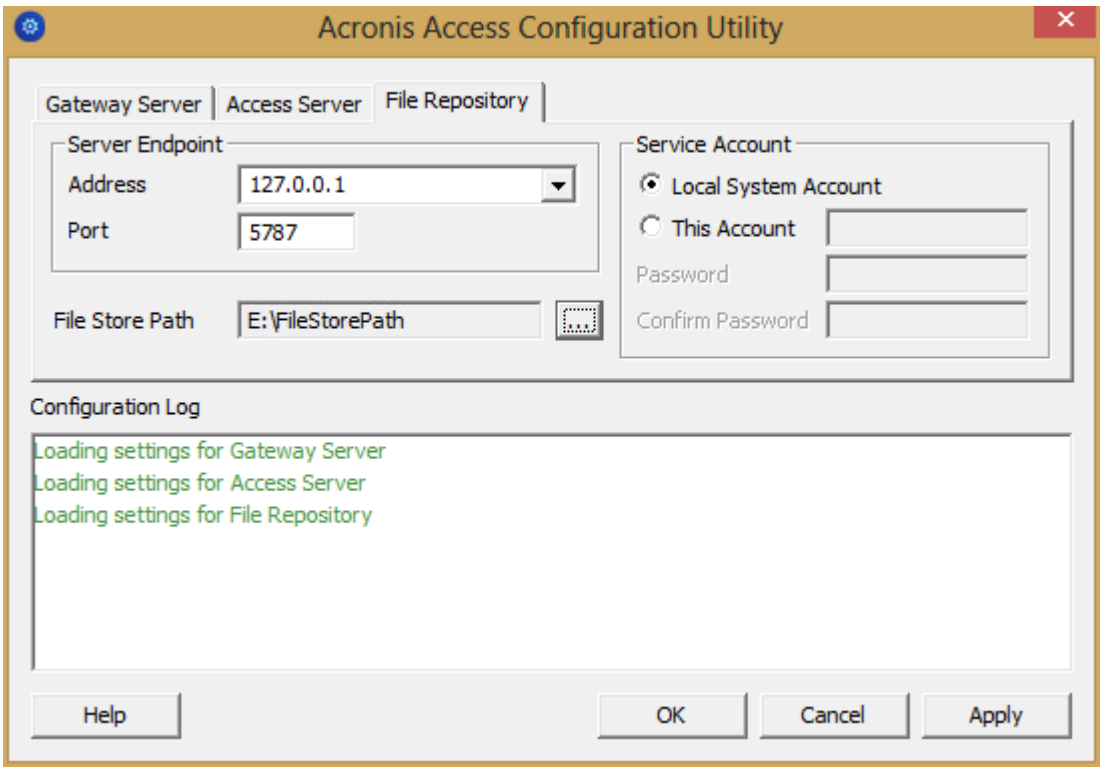


4. Configure the Acronis Cyber Files Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.

Note
If **Redirect requests from port 80** is selected,



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.



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.

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.

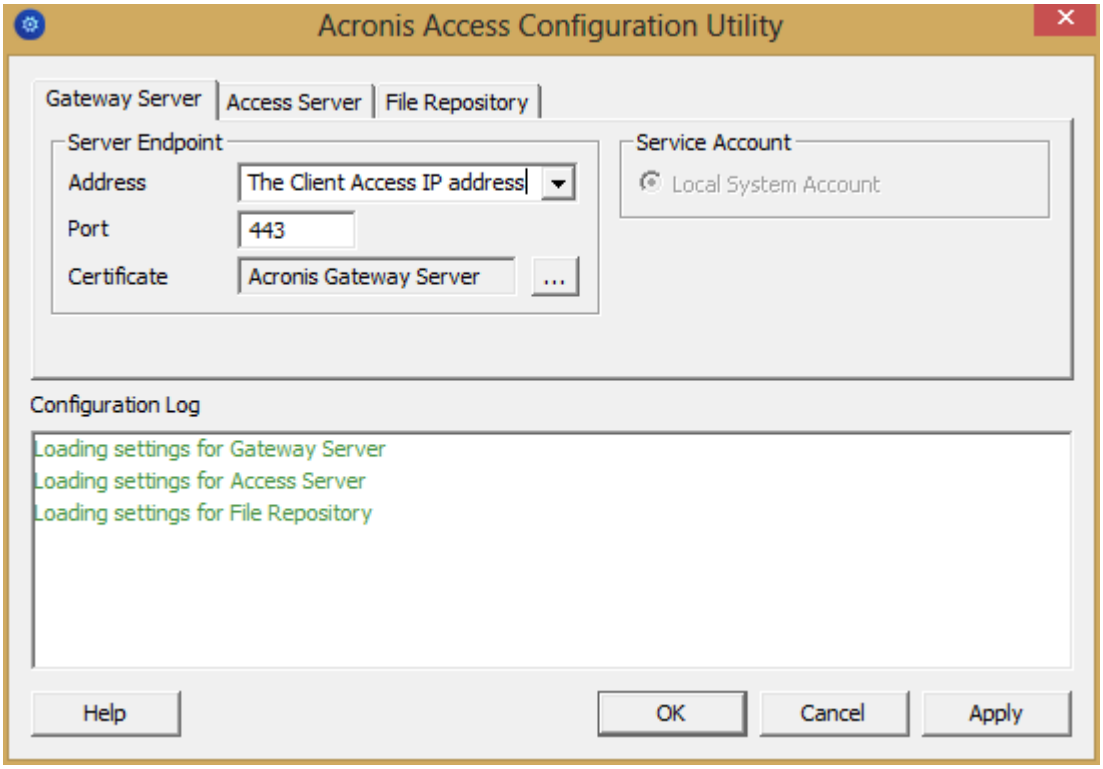
Note
The path should match the path set on the first node.

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

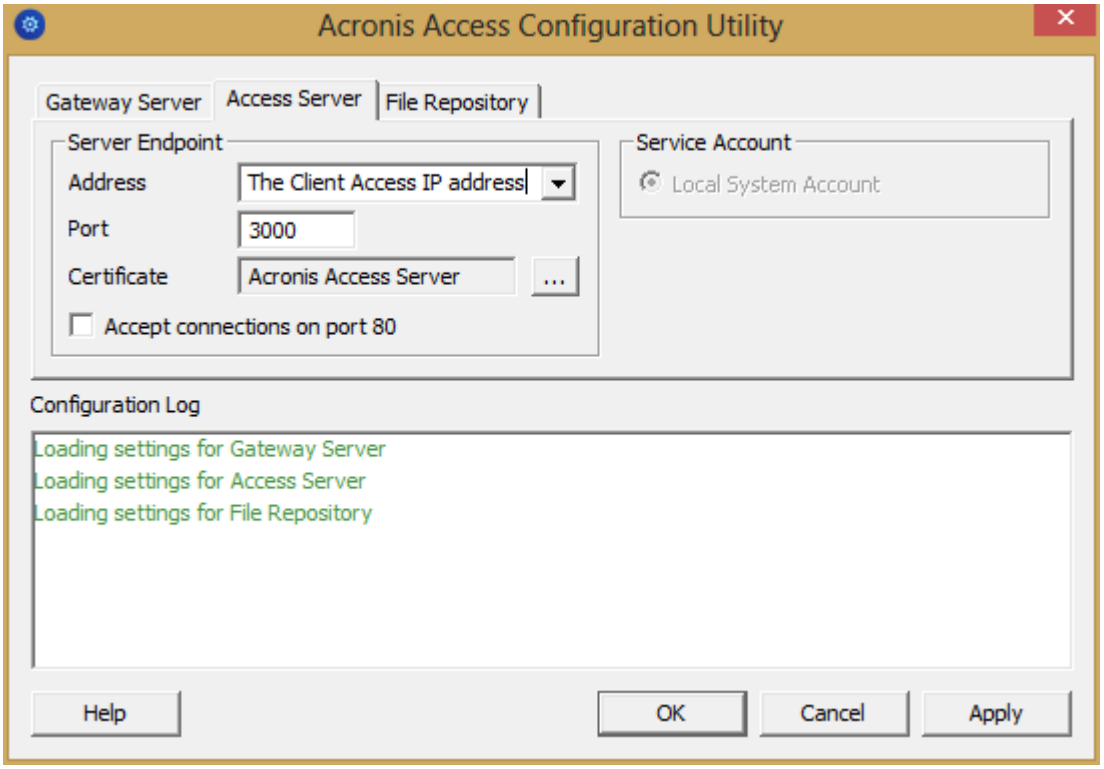
7. Launch the Configuration Utility. On a clean install, this is generally located at C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility
8. Configure the Acronis Cyber Files Gateway Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.



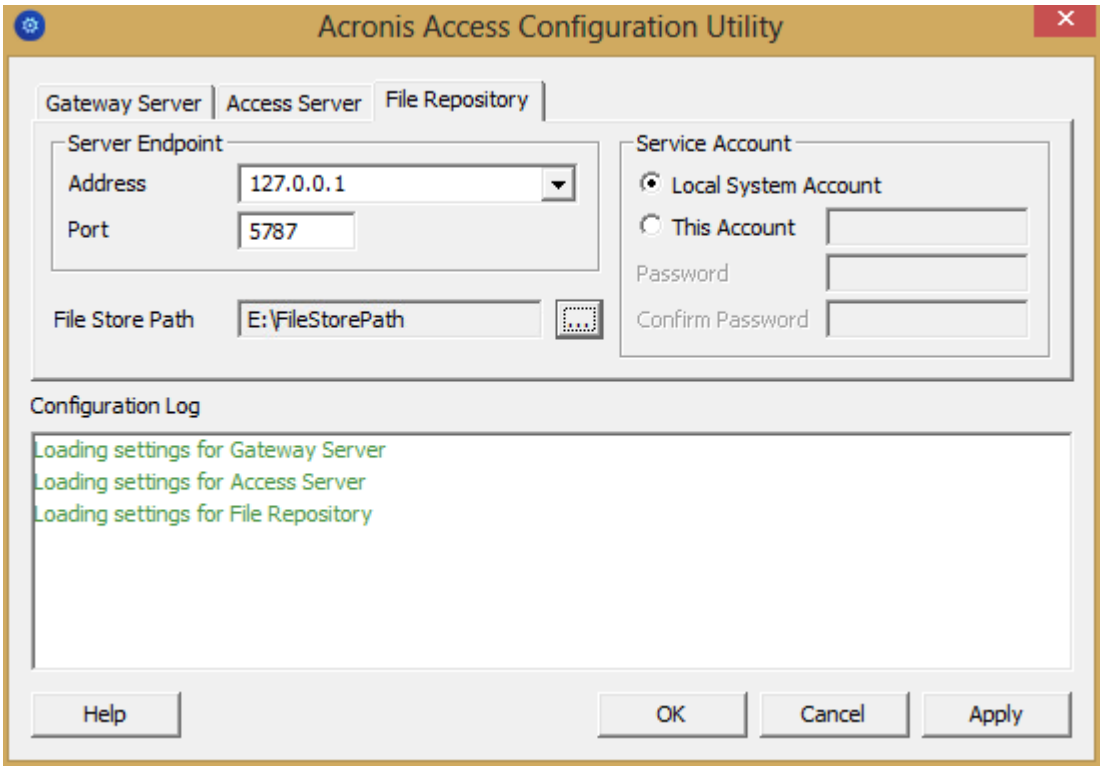
9. Configure the Acronis Cyber Files Server service to listen on the IP address(es) for the Acronis Cyber Files Service group.

Note

If **Redirect requests from port 80** is selected,



10. 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.



11. Click **OK** to complete the configuration and restart the services.

11.6 For the Mobile Clients

11.6.1 Using iOS Managed App Configuration features

The Acronis Cyber Files mobile supports iOS 7's Managed App Configuration features. If the prerequisites listed below are met, you can add certain keys to your MDM configuration and they will affect the Acronis Cyber Files mobile.

- Your device must be managed by a MDM server.
- The Acronis Cyber Files application binary must be installed on the device by the MDM server.
- The MDM server must support the **ApplicationConfiguration** setting and **ManagedApplicationFeedback** commands.

We support the use of the following keys:

- **enrollmentServer** - The value of this key should be set to the DNS address of the Acronis Cyber Files Server that the user should enroll with.
- **enrollmentPIN** – This key is optional. If your Acronis Cyber Files Server requires a PIN number for client enrollment, you can auto-complete the PIN number field in the Acronis Cyber Files enrollment form with this value. This PIN requirement is configured on the **Settings** page of the **Acronis Cyber Files** web console.
- **userName** – This key is optional. The value of this key will be inserted into the Username field in the Acronis Cyber Files enrollment form. You can use a variable to autocomplete this value with the specific user's username.

Creating a plist file

plist is a format for storing application data. It was originally defined by Apple, for use in iPhone devices and later spread to other applications. Since plists are actually XML files, you can use a simple text editor to create and edit them.

Creating the plist file

1. Open a 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>

Note
Example:
<dict>

Note
<key>enrollmentServer</key>

Note
<string>server.example.com</string>

Note
<key>userName</key>

Note
<string>username</string>

Note
<key>enrollmentPIN</key>

Note
<string>11Y9KL</string>

Note
</dict>

3. Save the file as **plist.xml**.

Uploading the plist file to MobileIron

1. Open your MobileIron administration portal.
2. Navigate to **Policies & Configurationss > Configurations > Add New > iOS and OSX** > **Managed App Configuration** and upload the plist file.

Uploading the plist file to Microsoft Intune

Note
For an in-depth guide, please visit the Microsoft Intune Documentation on the subject.

1. In the Microsoft Intune administration console, choose **Policy > Overview > Add Policy**.
2. In the list of policies, expand **iOS**, choose **Mobile App Configuration**, and then choose **Create Policy**.

- In the General section of the **Create Policy** page, supply a name and an optional description for the mobile app configuration policy.
- In the Mobile App Configuration Policy section of the page, in the box, enter or paste an XML property list that contains the app configuration settings.

3. Click Validate to ensure that the XML that you entered is in a valid property list format.
4. When you are done, click **Save** Policy.

11.6.2 MobileIron AppConnect support

Introduction

Acronis and MobileIron have partnered to bring Acronis Cyber Files's mobile file management to the MobileIron AppConnect platform. This Acronis Cyber Files capability allows the standard Mobile app to optionally be auto-configured and managed, along with other AppConnect-enabled apps, by AppConnect defined policies. The Acronis Cyber Files also supports MobileIron AppTunnel for remote access to Acronis Cyber Files Gateway servers residing inside the corporate data center.

The components of Acronis Cyber Files with MobileIron AppConnect include:

- **MobileIron Virtual Smartphone platform (VSP)** - A server-based console that allows the enterprise to enable client access to AppConnect-enabled apps, auto-configure those apps, create policies that govern app capabilities, and the ability to revoke access to or wipe AppConnect-enabled apps on specific devices.
- **MobileIron Sentry** - This service is used to provide network access for AppConnect-enabled apps needing to communicate with on-premise application servers, such as a Acronis Cyber Files Gateway server.
- **MobileIron Mobile@Work app** - This app brokers the authentication and configuration of AppConnect-enabled apps. It must be installed on the mobile device before AppConnect-enabled apps can be configured and managed.
- **Acronis Cyber Files iOS app** - The standard version of Acronis Cyber Files for iOS (version 5.0 or later), which is available on the Apple App Store, includes the ability to be configured and managed by AppConnect and to communicate with Acronis Cyber Files Gateway servers through AppTunnel.
- **Acronis Cyber Files Android app** - A special MobileIron version of the app is required. It can be downloaded from http://support.grouplogic.com/?page_id=4566. This version of the app must be added to your **Apps@Work** store.
- **Acronis Cyber Files Server** - The standard version of Acronis Cyber Files Server (version 5.0 or later), is fully compatible with mobile clients managed by AppConnect.

Testing a trial version of Acronis Cyber Files with AppConnect

The process of trialing Acronis Cyber Files with AppConnect is very much the same as a regular Acronis Cyber Files trial.

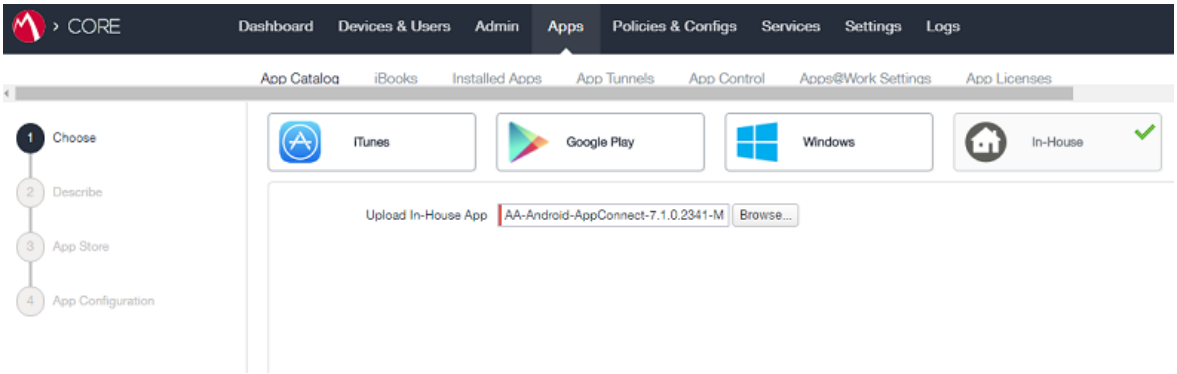
1. A trial version of the server-side software can be requested by visiting the Trial page. Once this request form has been submitted, you will receive an email with links to download the Acronis Cyber Files server trial installer and to the Quick Start Guide to assist in initial setup.
2. The Acronis Cyber Files iOS client app is a free download from the Apple App Store.
3. The Acronis Cyber Files Android app is a free download from one of our support sites http://support.grouplogic.com/?page_id=4566.
4. The Acronis Cyber Files mobile apps need to have an AppConnect configurations and policies created on your MobileIron Virtual Smartphone platform (VSP) before they can be auto-configured for access to your Acronis Cyber Files Gateway server(s).
5. Mobile devices also need to have the MobileIron Mobile@Work app installed before any AppConnect-enabled apps can be activated and before the Acronis Cyber Files app can be installed. Mobile@Work is a free download from both the Apple app store and the Google Play store.
6. When you are ready to activate Acronis Cyber Files Mobile Clients with AppConnect, please proceed to the following sections of this document.

Integrating the Acronis Cyber Files Android client with MobileIron

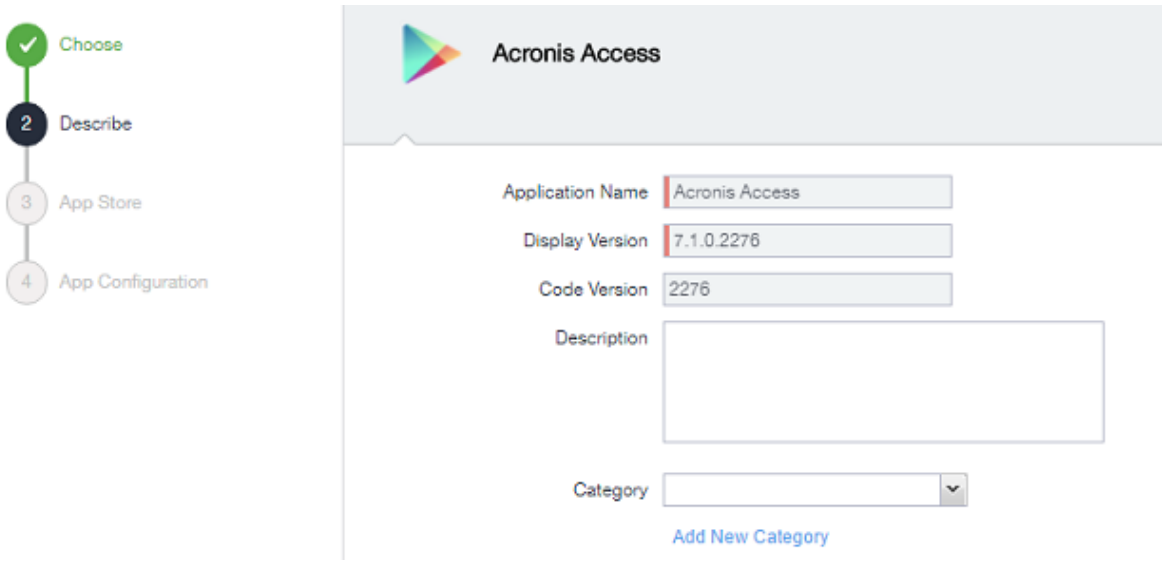
1. For Acronis Cyber Files Android to work with MobileIron device management, you must download a special version from http://www.grouplogic.com/web/aalatest, located under Acronis Cyber Files Client Installers.

   Note
   Make sure that the version you download is compatible with your version of MobileIron's **Secure Apps Manager.**

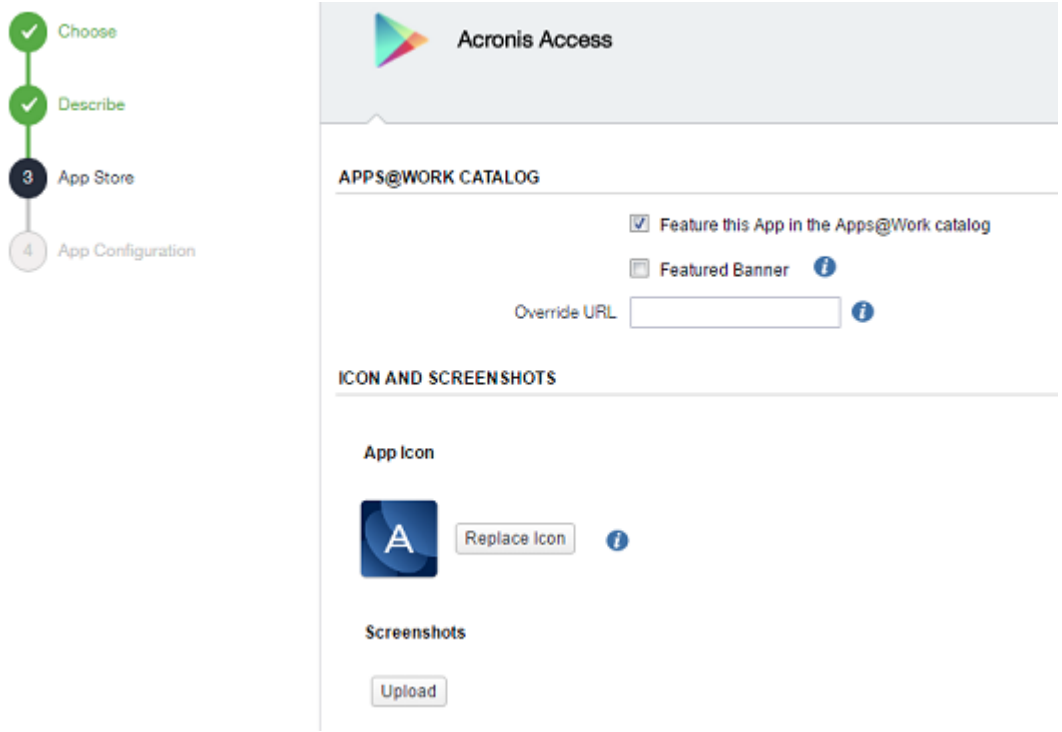
2. Log in to your MobileIron Core console.
3. Open the **Apps** tab and select **App Catalog**.
4. Press **Add+** and select **In-House**.
5. Press **Browse**, navigate to and select the Acronis Cyber Files Android .apk.



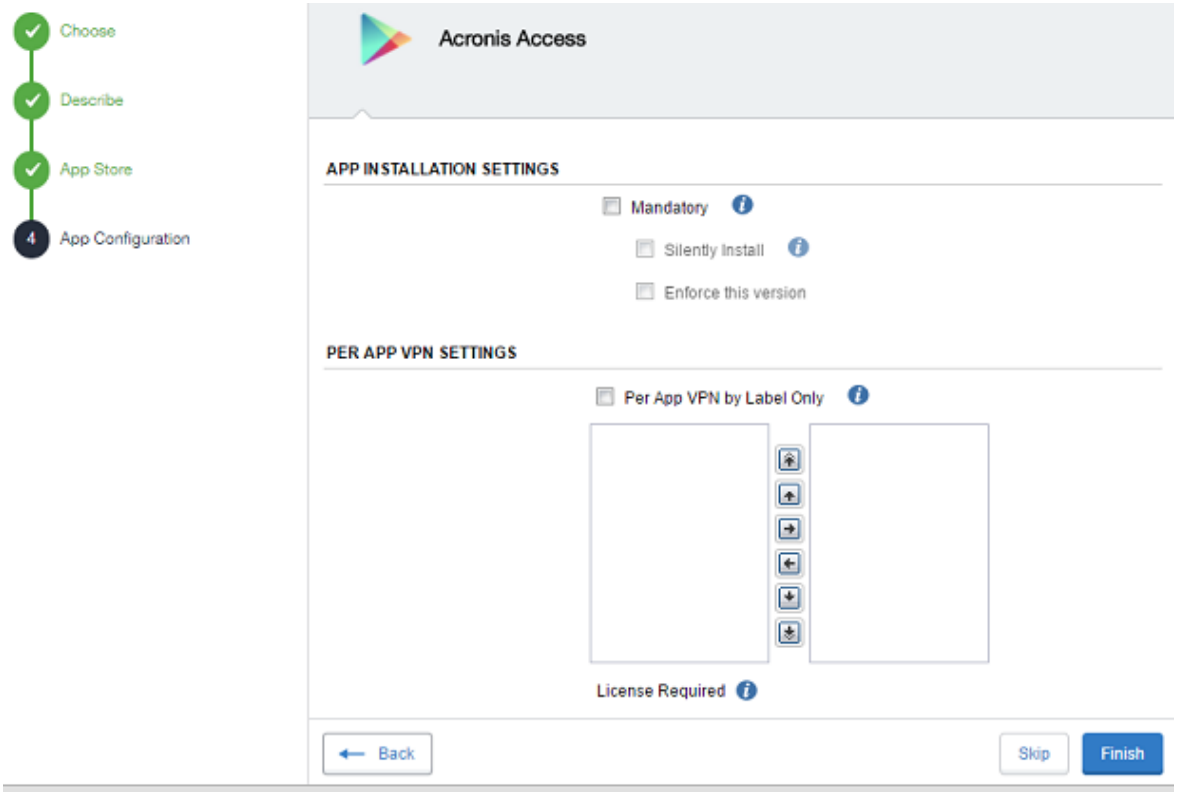
6. Press **Next**. Enter a description for the app and press **Next**.



7. For **App Store**, make sure that **Apps@Work Catalog** -> **Feature this App in the Apps@Work catalog** is enabled and press **Next**.



8. Select if the app should be a mandatory install on all users and press **Finish**.



Integrating the Acronis Cyber Files iOS app with MobileIron

Note
This is required only if you wish to have the app in your Apps@Work store and to allow the selection of the app across the MobileIron console, instead of having to write the bundle ID of the app.

1. Log in to your MobileIron Core console.
2. Open the **Apps** tab and select **App Catalog**.
3. Press **Add+** and select **iTunes**.
4. Enter **Acronis Cyber Files** in the search-box and press **Browse**, select the latest version of Acronis Cyber Files.
5. Press **Next**. Enter a description for the app and press **Next**.
6. For **App Store**, make sure that **Apps@Work Catalog** -> **Feature this App in the Apps@Work catalog** is enabled and press **Next**.

   Note
   You may need to also enable **This is a free** app.

7. For **App Configuration**, select any additional configurations you wish to do and press **Finish**.

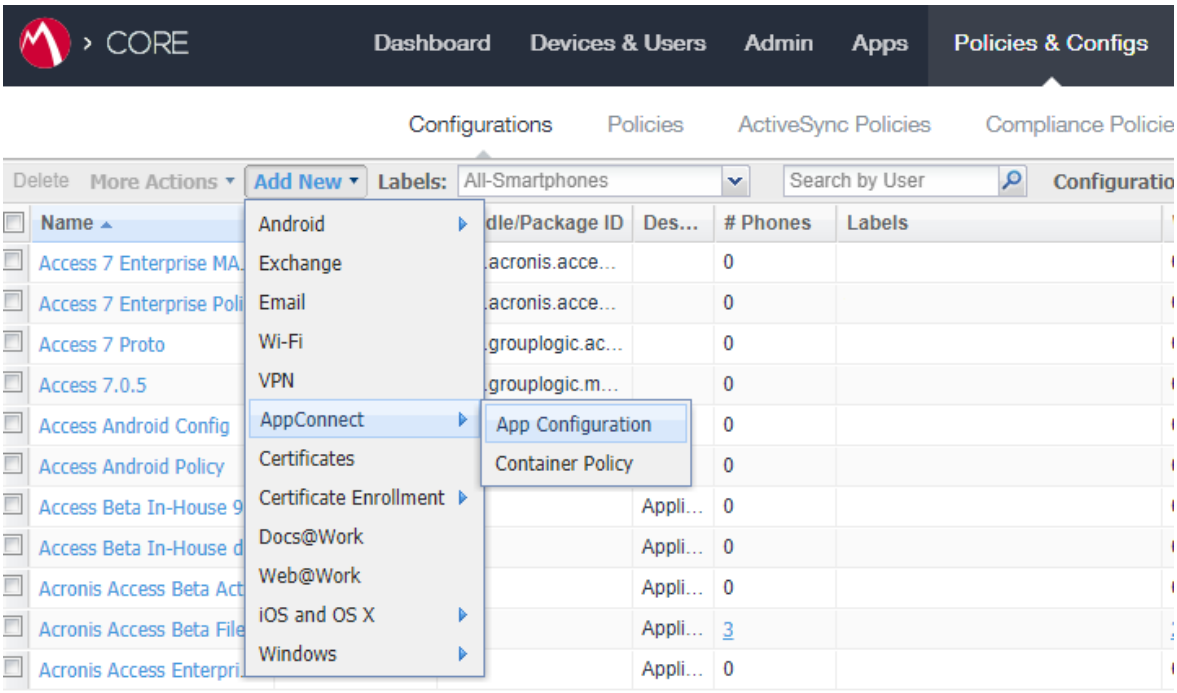
Creating an AppConnect configuration and policy for Acronis Cyber Files on your MobileIron VSP

Before you can start on-boarding Acronis Cyber Files users. You will need to create two items on your MobileIron VSP:

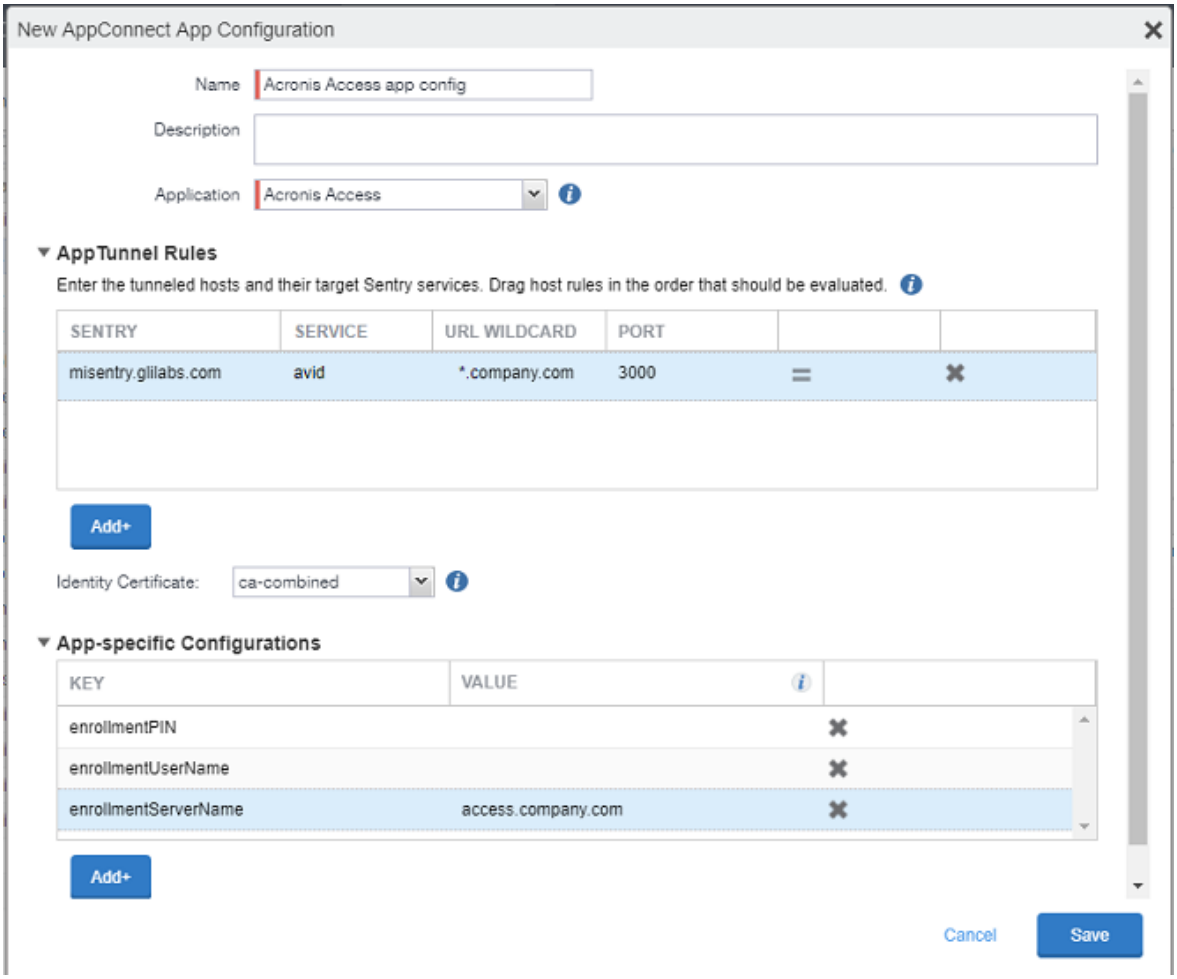
1. Mobile app **Configuration** – this allows AppConnect to auto-configure the Mobile app, completing some or all of the Acronis Cyber Files "Enrollment Form" and taking the place of the Acronis Cyber Files user invitation process.
2. Mobile app **Container Policy** – this policy allows the restriction of some of the capabilities of Acronis Cyber Files.

Creating a Mobile app Configuration

1. Log into your MobileIron VSP web console and select the **Policies & Configs** tab.
2. Click on the **Configurations** tab and press Add New.
3. In the drop-down menu, navigate to **AppConnect**
4. and select **App Configuration**.



5. Within this new **AppConnect App Configuration**, enter the following information:



Name – This can be any name you'd like to assign to this configuration. You may create more than one configuration and assign those configurations to different MobileIron labels.

Description – This can be any description you like.

Application – Select the Acronis Cyber Files app from the list. If you are using both iOS and Android devices, make sure to select the proper app for the desired clients.

AppTunnel – The **AppTunnel** settings are optional and only needed if you are using **AppTunnel** to provide access to your Acronis Cyber Files server(s).

- **Sentry** - select which of your MobileIron Sentry servers will be used.
- **Service** - this setting selects the service that the app in this configuration will be able to connect to through the **AppTunnel**. You can either select **<ANY>** to allow the app to connect to all internal services or select a dedicated **Service** for Acronis Cyber Files. The dedicated service option requires that you have added a custom **Service** for your Acronis Cyber Files Server.

Note
<TCP_ANY> is not the same as **<ANY>** and will not work!

Note
To add a custom service, navigate to **Services** -> **Sentry** and press **Edit** for the desired **Sentry**. Then, under the **AppTunnelConfiguration** section, press the **+** button under **Services**. Enter a **Service Name**, select an authentication method, make sure that the **TLS Enabled** checkbox is selected and for **Server List** enter the DNS address(es) of your Acronis Cyber Files server and/or Gateway.

- **URL Wildcard** - the DNS address of your Acronis Cyber Files server(s) or your domain as a whole. e.g. ***.domain.com**
- **Port** - Acronis Cyber Files' services use ports 443 and 3000 by default. Enter the one you need, depending which service your users will be enrolling to.

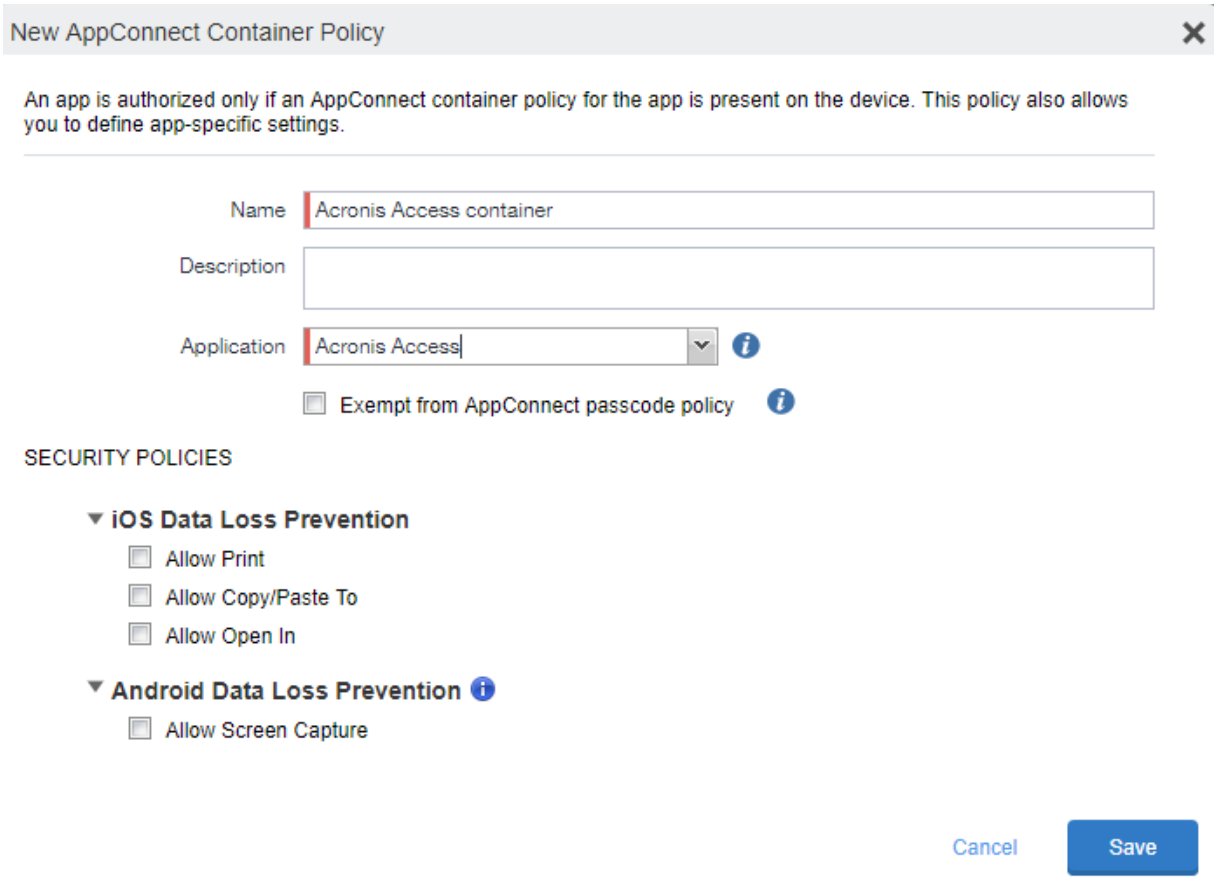
App-specific Configurations – This section allows you to specify values that will be used to auto-complete the Acronis Cyber Files enrollment form for the users who this configuration applies to, based on MobileIron label. The following **Keys** can be added:

- **enrollmentServerName** – This key field is required.
  - The value of this key should be set to the DNS address of the Acronis Cyber Files Server that the user should enroll with.
  - **enrollmentPIN** – This key is optional. If your Acronis Cyber Files Server requires a PIN number for client enrollment, you can auto-complete the PIN number field in the Acronis Cyber Files enrollment form with this value. It is typical that the PIN requirement on the Acronis 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. This PIN requirement is configured on the **Settings** page of the **Acronis Cyber Files** web console.

  enrollmentAutoSubmit - This key is optional. This will cause the enrollment form to be submitted automatically, so that they user does not have to tap the “Enroll Now” button to proceed. To enable this key, set its value to: **Yes**
  - **requirePIN** – This key is optional. If you are distributing a PIN to Acronis Cyber Files mobile users that they will need to manually enter into the Acronis Cyber Files enrollment form, you can specify that the PIN field is immediately shown in the form by setting this key’s value to: **Yes**
  - **enrollmentUserName** – This key is optional. The value of this key will be inserted into the Username field in the Acronis Cyber Files enrollment form. You can use MobileIron's $USERID$ wildcard, which will auto-complete the field with the username which the user has entered when setting up their Mobile@Work app.
  - **enrollmentPassword** – This key is optional. The value of this key will be inserted into the Password field in the Acronis Cyber Files enrollment form. You can use MobileIron's $PASSWORD$ wildcard, which will auto-complete the field with the password which the user has entered when setting up their Mobile@Work app.

Creating a Acronis Cyber Files app Container Policy

1. Log into your MobileIron VSP web console and select the **Policies & Configs** tab.
2. Click on the **Configurations** tab and press Add New.
3. In the drop-down menu, navigate to **AppConnect**
4. and select **Container Policy**.
5. Within this new **Container Policy**, enter the following information:



Name – This can be any name you'd like to assign to this configuration. You may create more than one configuration and assign those configurations to different MobileIron labels.

Description – This can be any description you like.

Application – Select the Acronis Cyber Files app from the list. If you are using both iOS and Android devices, make sure to select the proper app for the desired clients.

Exempt from AppConnect passcode policy - Select this option if you would like users to be able to open Acronis Cyber Files without having to first authenticate with their AppConnect passcode.

Allow Copy/Paste To - Select this option if you would like users to be allowed to copy and paste text from documents viewed in the Acronis Cyber Files mobile into other apps on the device that are not managed by AppConnect.

Allow Print - Select this option if you would like Acronis Cyber Files users to be allowed to print documents to available AirPrint capable printers.

Allow Screen Capture - This option is not yet supported in the AppConnect SDK. In the Acronis Cyber Files mobile users will always be allowed to perform screen captures, unless they are disabled on a device-wide level by their MDM configuration.

Allow Open In - Select this option if you would like to allow Acronis Cyber Files users to open files into other applications on the device. If selected, this option will also allow you to specify a list of specific apps that are allowed.

Assign labels to the new Configuration and Container Policy

In order for these new policies to be applied to mobile devices, ensure that you assign the MobileIron labels for any required users to both the **Configuration** and the **Container Policy**.

Activating the Acronis Cyber Files iOS client with AppConnect

Note
This method of activating the Acronis Cyber Files app applies only to the iOS version and is required only if you have not added the Acronis Cyber Files app to your list of apps in the MobileIron VSP console and the users are not already using Acronis Cyber Files.

Note
If the app has been added through the MobileIron console, users will be able to download it from the **Apps@Work** store or it may be automatically installed on their device, depending on your settings.

Once the needed Configuration and Container Policy have been created on the MobileIron VSP, you are ready to install and configure Acronis Cyber Files on client devices.

Ensure Mobile@Work is installed and configured

Before installing or activating the Acronis Cyber Files mobile app, ensure that you have installed the MobileIron Mobile@Work iOS app on your device. This app serves as the conduit through which Acronis Cyber Files communicates with the MobileIron VSP and receives AppConnect configuration and commands.

After Mobile@Work is installed, you must configure it with your user account information and the address of your VSP server.

Once Mobile@Work is installed and configured, you're ready to move forward with Acronis Cyber Files. There are three possible scenarios for setting up Acronis Cyber Files with AppConnect:

Acronis Cyber Files has already been installed on the device, but has not yet been enrolled with a Acronis Cyber Files Server

In the scenario where the Acronis Cyber Files iOS app may have been installed on a device and opened previously before Mobile@Work and AppConnect VSP configurations have been set up. Simply starting the Acronis Cyber Files mobile may not trigger the AppConnect setup process. In this case, it is possible to manually start the AppConnect setup process by opening the Settings menu within the Acronis Cyber Files app, tapping the MobileIron AppConnect option towards the bottom of the settings list, and selecting the Enable button. If the AppConnect setup does not begin immediately, please leave the Acronis Cyber Files app open for a few minutes to allow it to begin. Once setup begins, it will proceed as described in the previous scenario.

If the Mobile@Work app is not present on the device, Acronis Cyber Files will display a warning on this **Settings** menu rather than an **Enable** button.

Acronis Cyber Files has already been installed on the device, and has already been enrolled with a Acronis 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 Mobile app. If the Mobile app is already enrolled with a Acronis Cyber Files Server, it will maintain that original configuration.

For Acronis Cyber Files to become managed by AppConnect and begin using the AppConnect passcode and permissions Container Policies, the user must first open the Acronis Cyber Files app, go to **Settings** -> **Partner Features** -> **MobileIron** and tap on **Enable AppConnect**. The user will then have to wait a little bit and restart the app.

If you require a user to enroll with a different Acronis Cyber Files Server, you will need to have them uninstall Acronis Cyber Files and reinstall the app before they can be configured by AppConnect.

Acronis Cyber Files has not yet been installed on the device

In this scenario, you will need to install Acronis Cyber Files from the Apple App Store or from the MobileIron Apps@Work store.

Once installed, start Acronis Cyber Files.

Acronis Cyber Files will check for the presence of a configured Mobile@Work app, temporarily switch over to the Mobile@Work app, and then switch back to Acronis Cyber Files . If a valid Acronis Cyber Files AppConnect configuration is found, Acronis Cyber Files will automatically enter enrollment mode and present the user with the Acronis Cyber Files mobile enrollment form. Any fields included in the AppConnect configuration will be automatically filled out. The user will typically just have to enter their AD password into the form and then submit it. Once this is completed, the relevant Acronis Cyber Files Client Management policy will be applied to Acronis Cyber Files and the user will be ready to begin using the app.

If a valid configuration for Acronis Cyber Files does not exist on the VSP, or if the Mobile@Work app has not been installed or configured, the user will receive an error message or, in the case Mobile@Work is not installed, Acronis Cyber Files will simply start up in it's standard mode without AppConnect enabled.

Ongoing AppConnect management of Acronis Cyber Files mobiles

Once Acronis Cyber Files is being actively managed by AppConnect, any changes to the applicable Container Policy will be received by the Acronis Cyber Files mobile when it checks in with the Mobile@Work app on its device. The interval at which this check in occurs is set on your MobileIron VSP and will cause the Acronis Cyber Files app to temporarily switch over to the Mobile@Work app to perform the check. This will interrupt the user, so it's recommended that this check-in interval be made long enough to not frequently interfere with their use of the app.

Any changes to Container Policy, revocation of access to Acronis Cyber Files, etc, will be applied to the app at the next time it checks in.

Using AppConnect with Kerberos Constrained Delegation

This article serves to explain how to configure the required system components to connect the Acronis Cyber Files iOS mobile app to the Acronis Cyber Files server proxied through MobileIron AppTunnel with authentication handled via Kerberos Constrained Delegation.

The Android mobile app does not support this configuration.

Note
The documentation on how to configure MobileIron for Kerberos Constrained Delegation is provided as a courtesy to help get the configuration setup. However, all of the steps up until verification that the Sentry is receiving the Kerberos ticket from the KDC, involve MobileIron software exclusively. If you are having difficulties getting through these steps and successfully receiving a Kerberos ticket, please contact **MobileIron** support.

As this is a complex setup in order to reduce errors and simplify troubleshooting, it will be accomplished in two phases. The first phase will establish an AppTunnel using username/password to authentication to the Acronis Cyber Files server. This infrastructure will be built on in phase two to add on Kerberos Constrained Delegation. It is highly recommended to test the tunnel works with username/password authentication before moving on to Kerberos to eliminate steps in problem determination.

Before you begin

- Kerberos Constrained Delegation, abbreviated KCD, allows users to authenticate to network resources by Kerberos after their identity is established using a non-Kerberos authentication method. In the case of Acronis Cyber Files, this allows users to authenticate using iOS device-level identity certificates distributed by MobileIron. Without KCD, the Acronis Cyber Files app would only be able to use a certificate installed directly into the app.

Note
All of the configuration related to KCD is done through MobileIron. There are no special changes to make in Acronis Cyber Files itself.

- Key Distribution Center, abbreviated KDC, is a network service that supplies session tickets and temporary session keys to users and computers within an Active Directory domain.
- Only the Gateway Server accepts Kerberos authentication. The Acronis Cyber Files server does not.
  - The Acronis Cyber Files mobile app must be enrolled in client management with a Acronis Cyber Files Server. This is necessary for the authentication to work properly.

    Note
    The client app address cannot be changed post-enrollment. Enabling KCD for already enrolled apps that use wrong address, is not possible. The only solution is to re-install the app and then enroll to the correct address.

    If there is a load balancer that splits the traffic between 2 Gateways, 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.

    For further assistance, please contact the Support team.

  - Mobile clients using Kerberos authentication will be able to authenticate to Network shares, Sync&Share folders and SharePoint sites.

Prerequisites

The following software should already be installed and configured:

- MobileIron VSP (5.9 used in this document)
- For Kerberos to work properly the user accounts on the VSP should come from the Active Directory that will be configured to support Kerberos
- MobileIron Sentry (4.8 used in this document)
- Acronis Cyber Files server installed (6.0.2 used in this document)
- Servers interoperability
  - The time on the VSP, Sentry, Domain Controller, and Acronis Cyber Files servers must all be synchronized (NTP recommended)
  - Domain name resolution (DNS). The Sentry will ask for a ticket from the KDC using the DNS name it has been configured to contact. This name must match the computer name set up for Kerberos delegation or the KDC will refuse to grant a ticket.
  - The VSP must be able to reach the Sentry (ports 9090 and 443 by defaults – others based on your configuration).

    - The Sentry must be able to reach the Active Directory and Acronis Cyber Files server (ports 88, 389, 636).
    - Ports 88 (UDP and TCP) and 389 (TCP) between Active Directory and Sentry (or port 636 (TCP) if you are using SSL-enabled Active Directory) need to be opened to allow communication. Port 88 is used for Kerberos protocol communication. Port 389 (or 636) is used for the LDAP ping between Sentry and the KDC to verify that the KDC IP is the same as the Active Directory IP.
- The iOS device must be able to reach the VSP and the Sentry.
- iOS Device registered on VSP.
- Mobile@Work installed on the device and registered in the VSP. The MDM profiles properly installed during the registration.

Configuring an AppConnect tunnel between the Acronis Cyber Files mobile and the Acronis Cyber Files server via username/password authentication

The first step towards configuring an AppConnect tunnel between the Acronis Cyber Files mobile and the Acronis Cyber Files server is to add and configure the Sentry to the VSP. This is a muti-step process broken down into the following phases.

- Generate a new Local CA
- Create a new SCEP
- Add and Configure the Sentry
- Configuring Acronis Cyber Files on the VSP

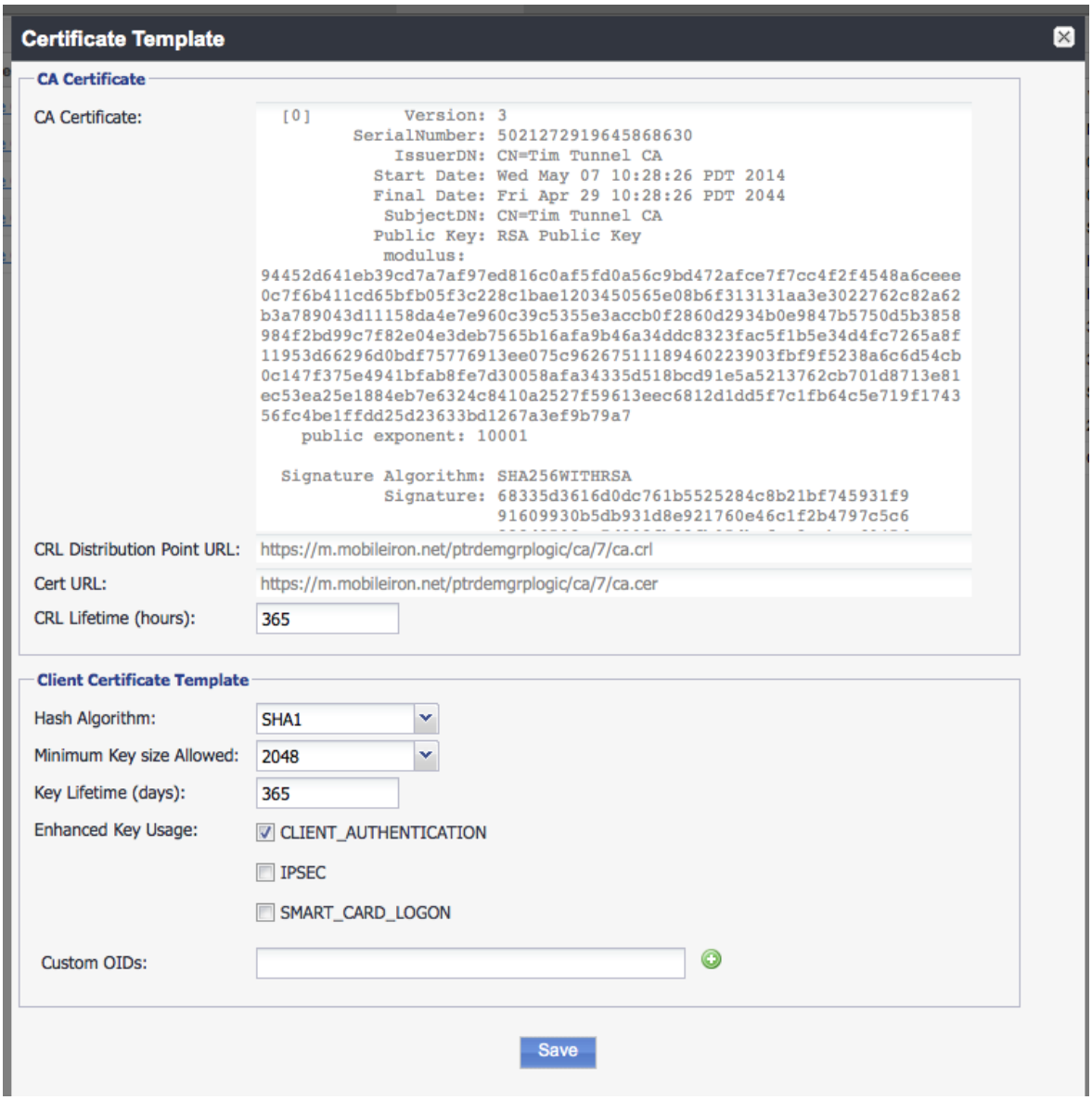
You may have an alternate Certificate Authority (CA) and Simple Certificate Enrollment Protocol (SCEP) provider but this guide assumes you do not for completeness sake. Please consult MobileIron documentation for configuring a third party CA and SCEP provider.

Generate a new Local CA

1. Open the MobileIron VSP Admin Portal.
2. Select **Settings** and open **Local CA**.
3. Press **Add New** and select **Generate Self-Signed Cert**.

- **Local CA Name:** Enter a name based on your preference.
- **Key Length**: Select **2048**.
- **Issuer Name:** Enter a name based on your preference, but it must start with **CN=**.

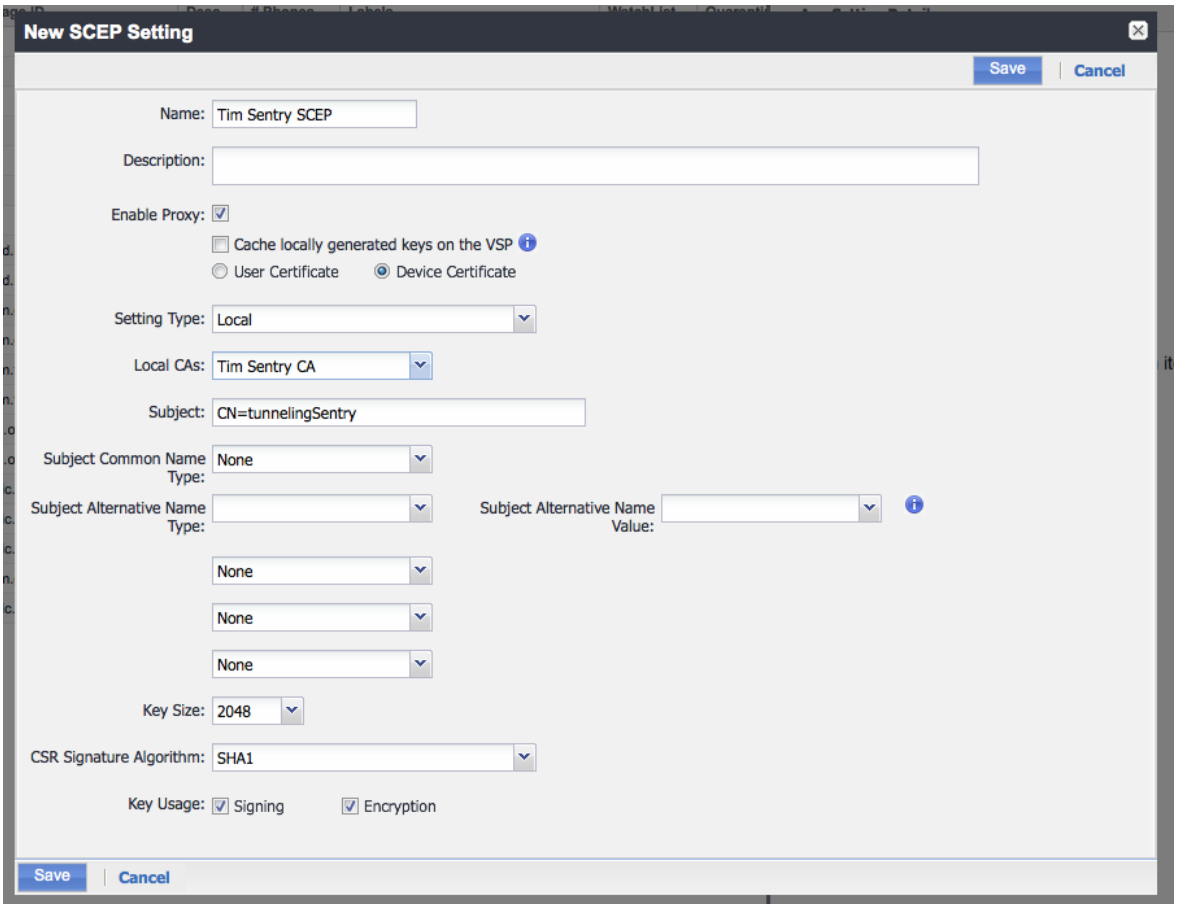
4. Click **Generate**.



5. Then click **Save**.
6. Click **View Certificate** on the new CA.
7. Copy the certificate to a new text file and save to the desktop.

Create a new SCEP

1. Open the MobileIron VSP Admin Portal.
2. Select **Policies & Configs** and open **Configuration**.
3. Press **Add New** and select **SCEP**.

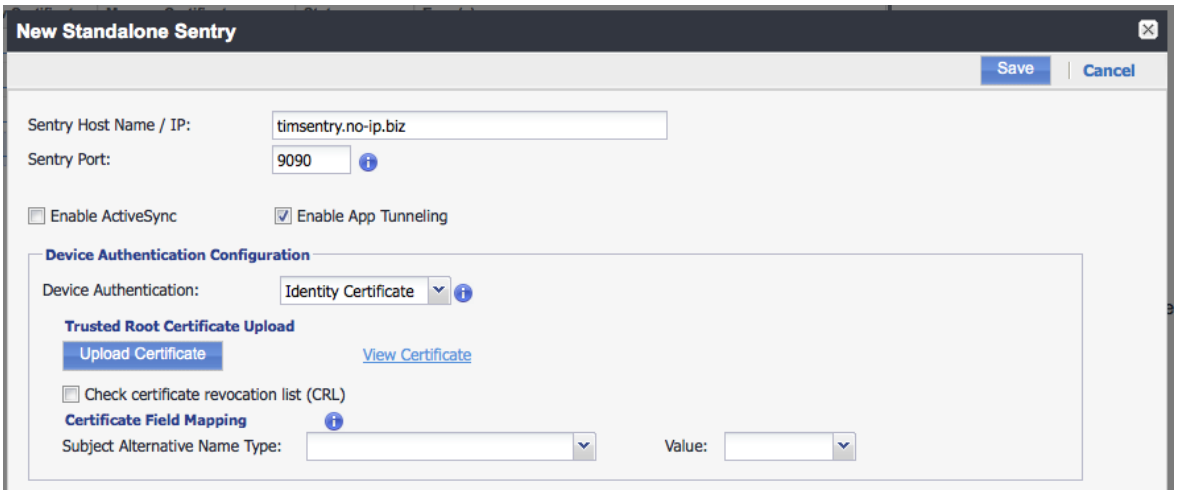


- **Name**: Enter a name based on your preference.
- **Setting Type**: Select **Local**.
- **Local CAs**: Name of the CA created in "Generate a new Local CA".
- **Subject**: Enter a name based on your preference (e.g. CN=tunneling) but it must start with **CN=**..
- **Key Size**: Select the same value you selected when generating the CA. In this case, select **2048**.

4. Click **Save**.

Add and Configure the Sentry

1. Still within the MobileIron VSP Admin Portal, select **Settings** open **Sentry**.
2. Press **Add New** and select **Standalone Sentry**.

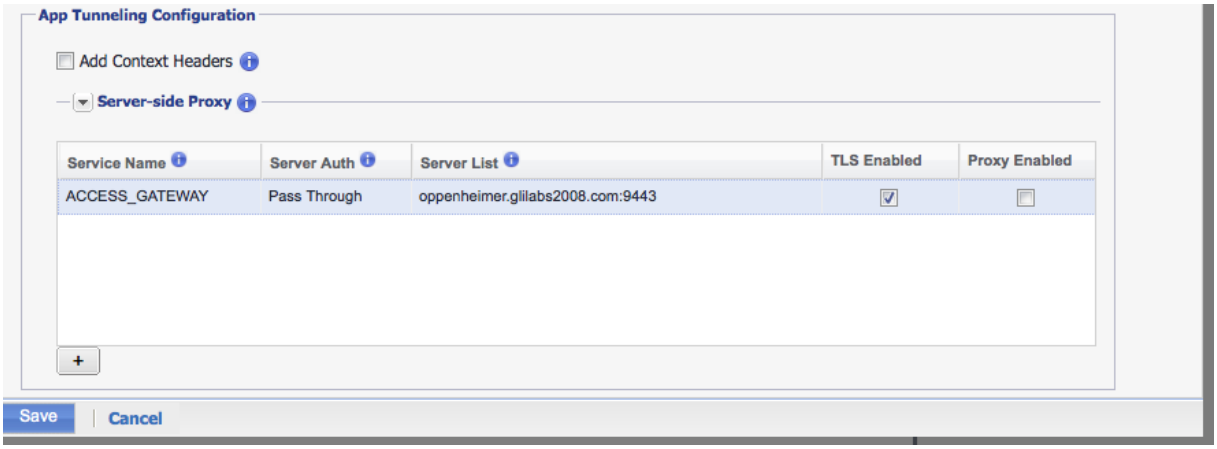


- **Sentry Host Name/IP**: The DNS name your sentry is installed on. It must be reachable via the MobileIron VSP.
- **Sentry Port**: The port open for connection via the MobileIron VSP (default is 9090).
- **Enable App Tunneling**: Mark the checkbox.
- **Device Authentication**: Select **Identity Certificate**.

3. Click **Upload Certificate**.
4. Browse and select the text file you saved to desktop in "Generate a new local CA".
5. Click **Upload Certificate**.

App Tunneling Configuration

In this section you setup Services to map to Acronis Cyber Files Gateway servers. The management server does not support Kerberos Constrained Delegation however you can enroll using the Gateway that is installed on the same machine as the management server. That is the configuration that should be used to support enrollment using Kerberos Constrained Delegation.



- **Service Name**: Enter a name based on your preference.
- **Server Auth**: Select **Pass Through**. This will be changed in a later part of this guide.

- **Server List**: Semi-colon separated list of servers. For this document we will use a single server. That will be the DNS address of the Acronis Cyber Files Gateway server and the port it is listening on.
- **TLS Enabled**: Mark the checkbox.

Click **Save**.

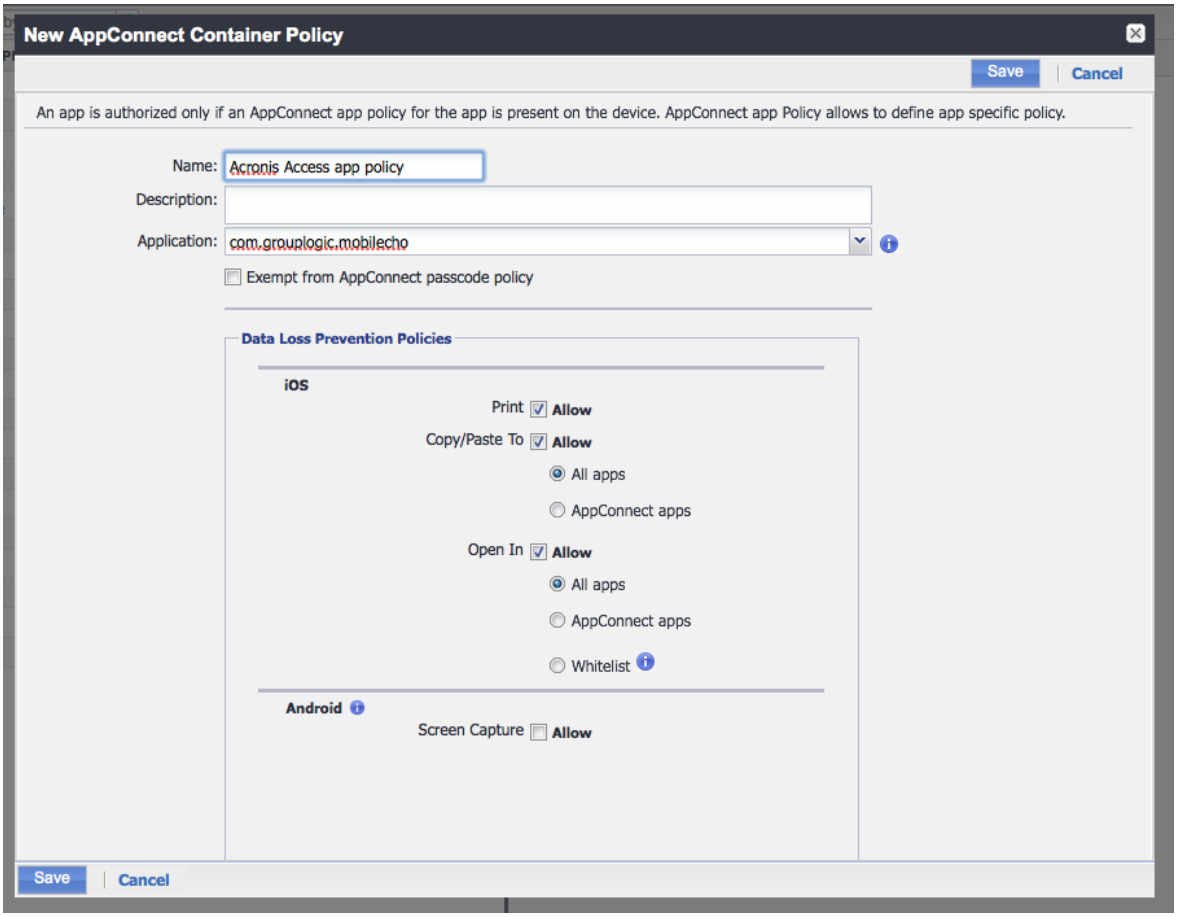
Click "**View Certificate**" on the new Sentry entry. This tests the connection between the VSP and Sentry. If you can't get the certificate check the connections and ports between the VSP and Sentry. Do not proceed until this works.

Configuring Acronis Cyber Files on the VSP

Once the Sentry is setup, the App Policy and App Configuration needs to be created for Acronis Cyber Files. This is a multi-step process that will include the following steps.

12 Creating the App Policy

1. Still within the MobileIron VSP Admin Portal, select **Policies & Configs** and open **Configurations**.
2. Press **Add New**, select **AppConnect** and select **Container Policy**.

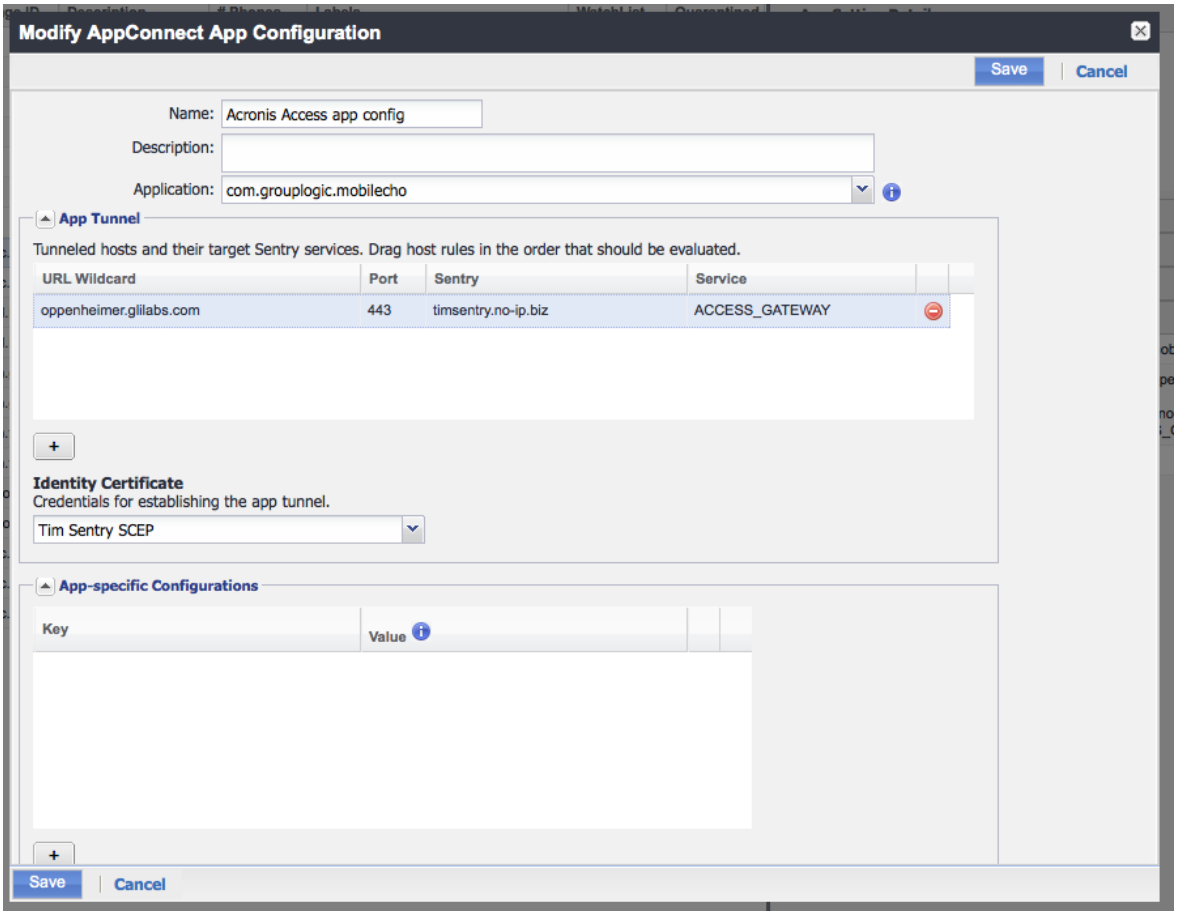


- **Name**: Enter a name based on your preference.
- **Application**: Enter **com.grouplogic.mobilecho**. This is a Bundle ID from the iOS App Store.
- **Policies**: Set whatever MobileIron policies you want to use for managing Acronis Cyber Files.

3. Click **Save**.

13 Creating the App Configuration

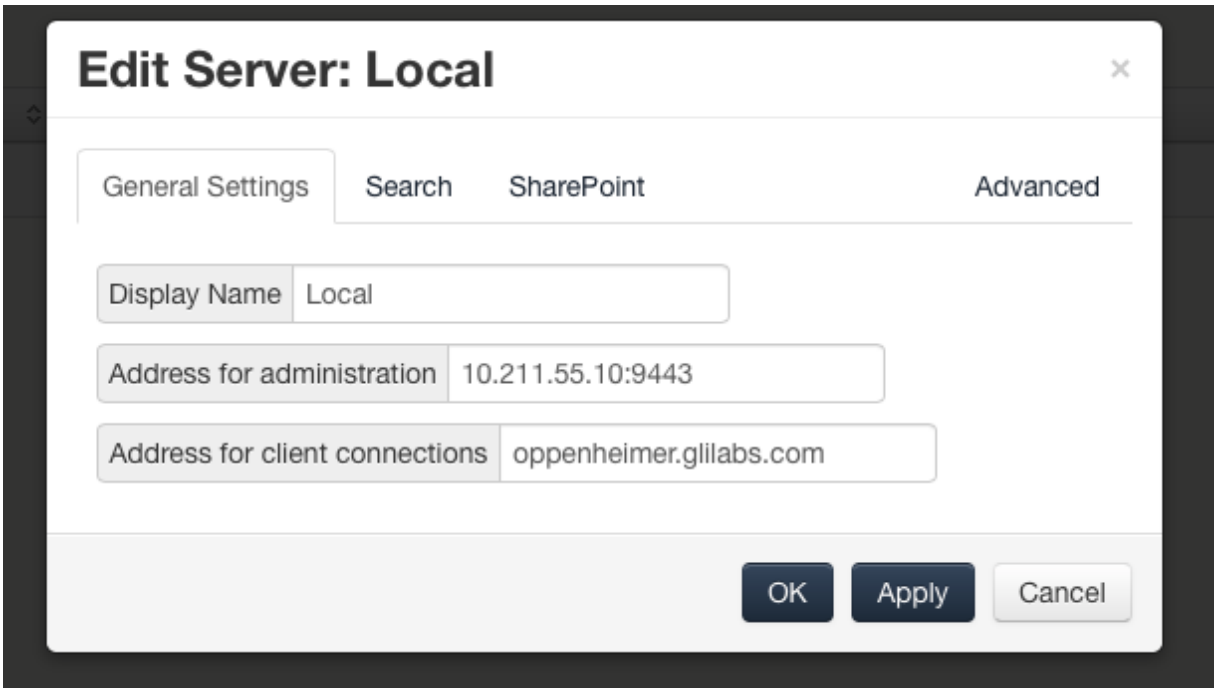
1. Still within the MobileIron VSP Admin Portal, select **Policies & Configs** and open **Configurations**.
2. Press **Add New**, select **AppConnect** and select **Configuration**.



- **Name**: Enter a name based on your preference.
- **Application**: Enter com.grouplogic.mobilecho. This is the Bundle ID as seen in the Apple store.
- **App Tunnel**
  - **URL Wildcard**: The URL that the client will try to contact the Acronis Cyber Files Gateway server on. This must match the "Address for client connections" configured for the Gateway server in the Acronis Cyber Files admin interface. This can be a regular expression to match multiple gateways but for the purpose of this document we will enter the exact hostname.*
  - **Port**: The port the client will try to make connections on (443 by default).
  - **Sentry**: The sentry created in "Add and Configure the Sentry".
  - **Service**: The service configured for the Gateway in "Add and Configure the Sentry".
  - **Identity Certificate**: The SCEP created in "Create a new SCEP".

3. Click **Save**.

*Address for client connections from the Acronis Cyber Files web interface. This address will be used in profiles sent to the mobile client for making file system connections. The sentry **URL Wildcard** must match this address and port to route those connections through to the sentry.



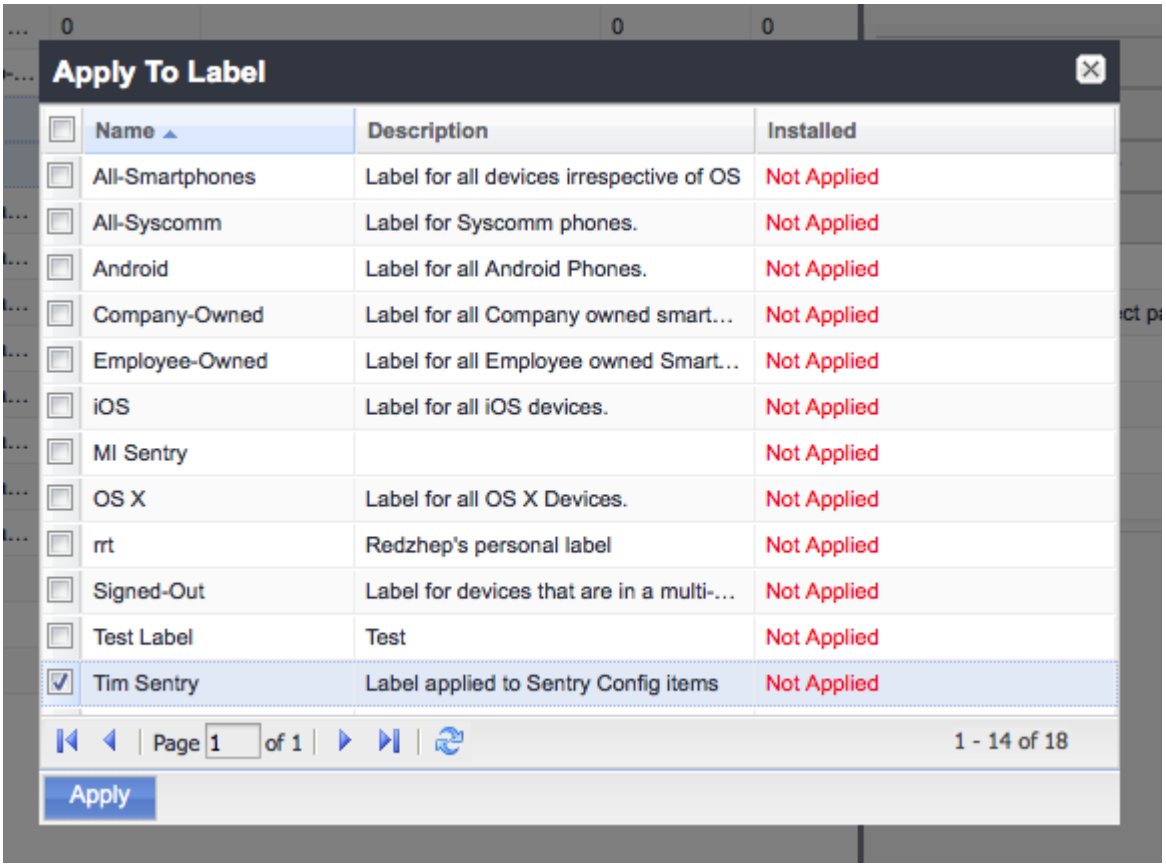
14 Create a new label

1. Still within the MobileIron VSP Admin Portal, select **Users & Devices** and open **Labels**.
2. Press **Add new**.

   - **Name**: Enter a name based on your preference.
   - **Description**: Enter a description based on your preference.
3. Click **Save**.

15 Apply label to new configurations

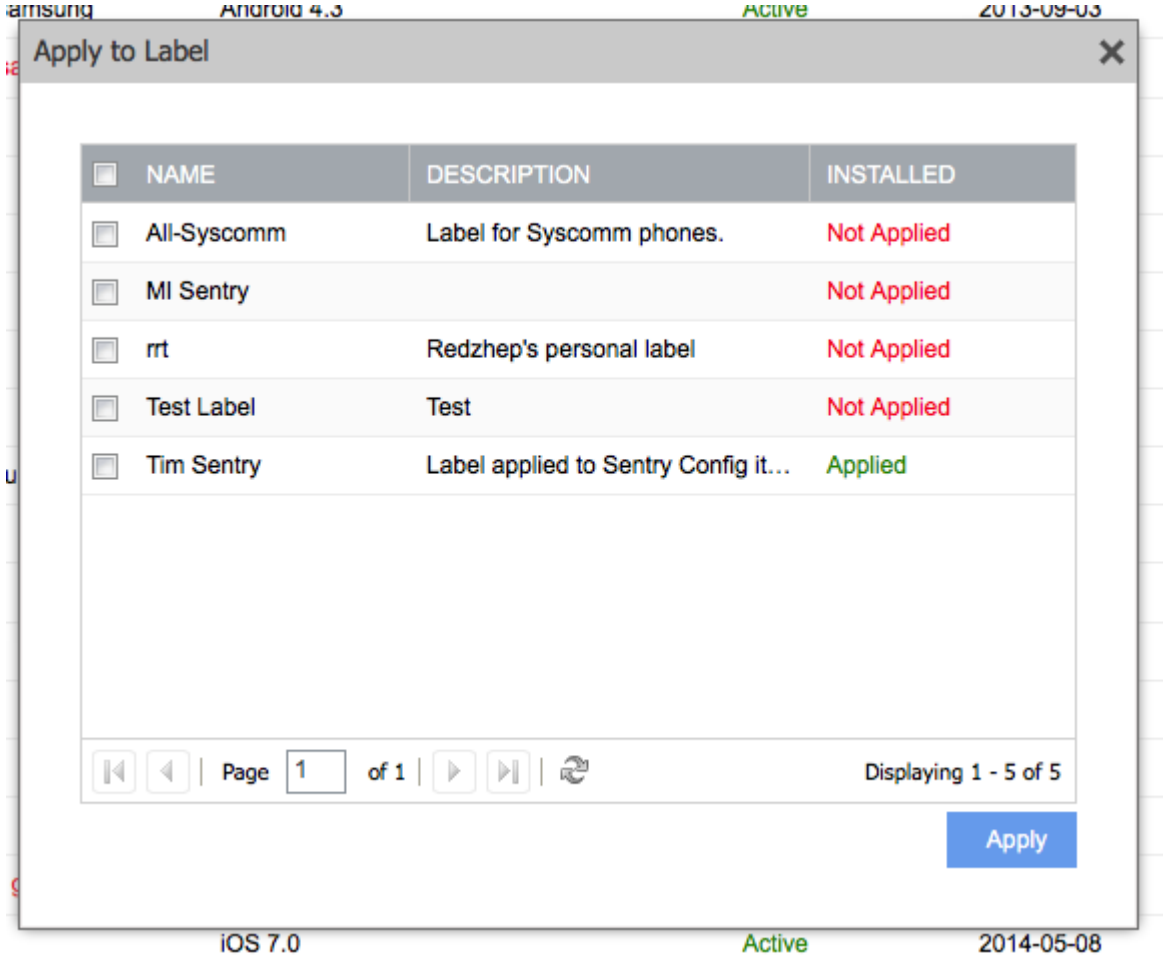
1. Still within the MobileIron VSP Admin Portal, select **Policies & Configs**.
2. Mark the SCEP, AppConnect policies, and AppConnect configurations you created while following this document. Open **Configurations** to view them listed.



3. Press **More Actions** and select **Apply to Label**.
4. Mark the Label created in "Create a new label".
5. Click **Apply**.

16 Apply label to iOS device

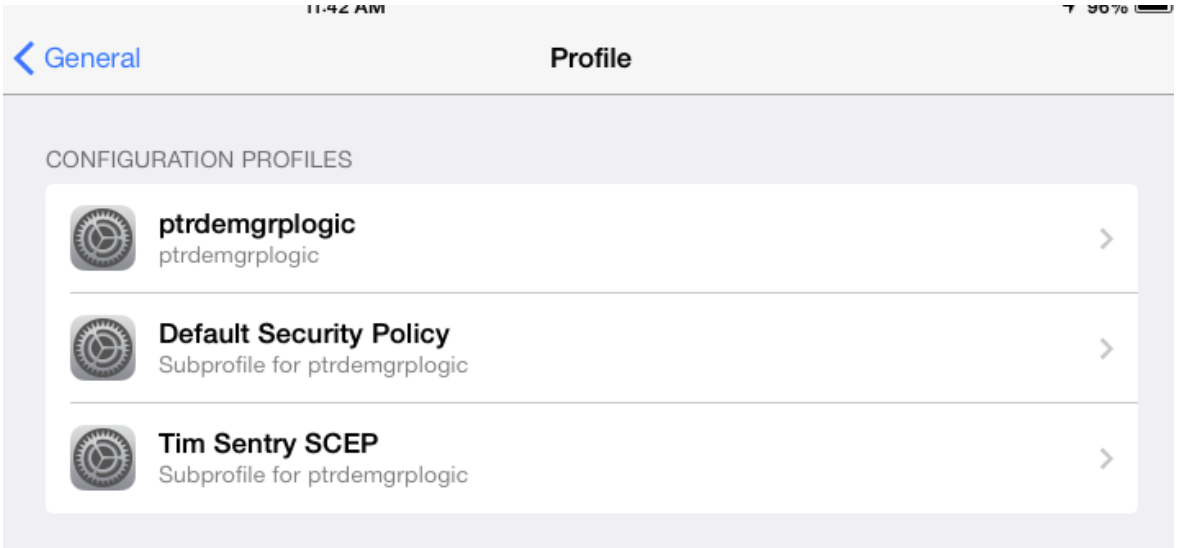
1. Still within the MobileIron VSP Admin Portal, Select **Users & Devices** and open **Devices**.
2. Mark the iOS device to be used for Sentry testing.



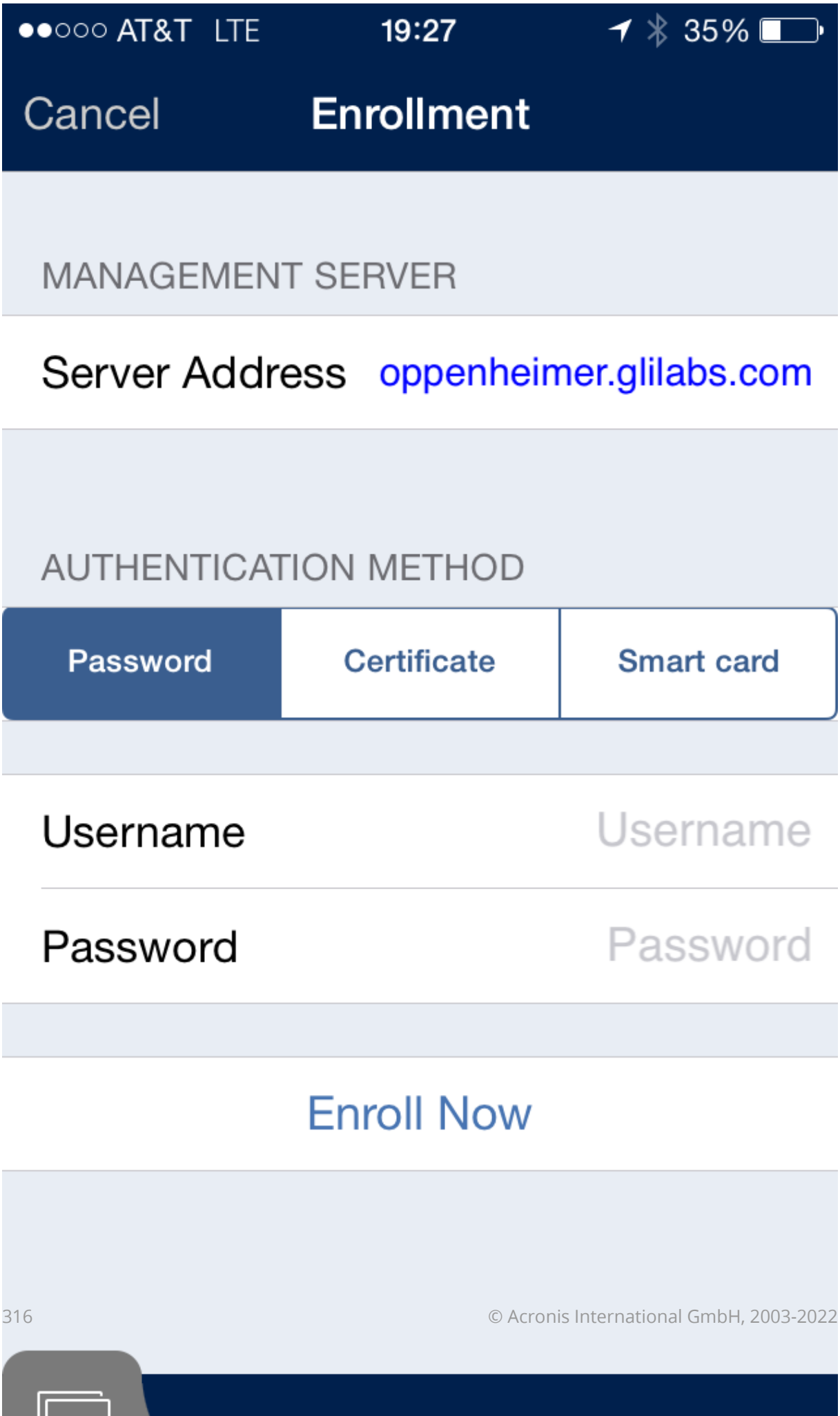
3. Select **Actions** -> **Apply to Label**.
4. Check Label created in "Create a new label".
5. Click **Apply**.

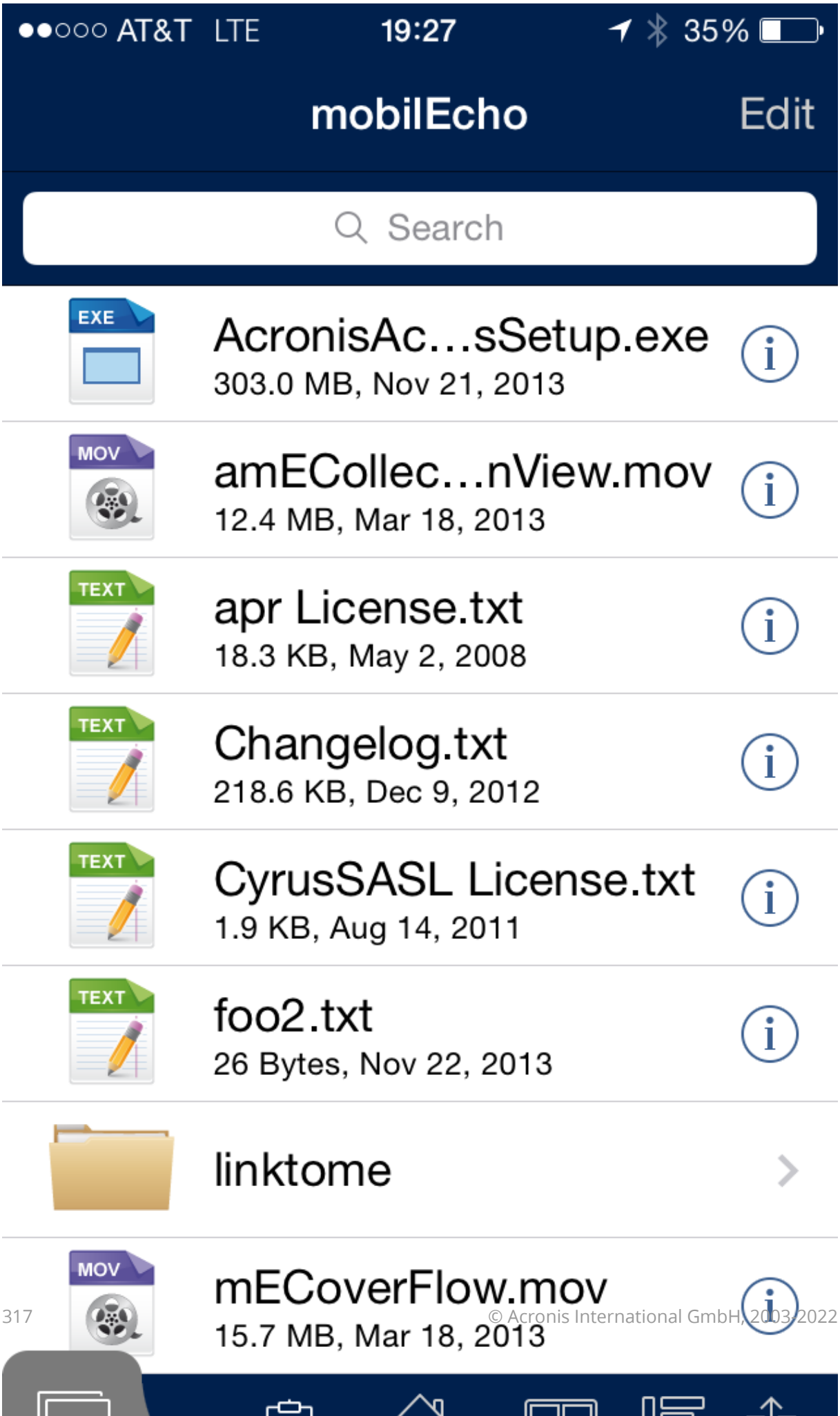
17 Testing the iOS client

1. Open the Mobile@Work app and open the **Settings**.
2. Tap on Check for Updates.
3. Tap on **Force Device Check-In**. If this is successful the SCEP configured in this document should show up in the device settings at **Settings** -> **General** -> **Profiles**.



4. Install Acronis Cyber Files from the App Store and Launch it.
5. Select **Enroll Now** on the Welcome view or go to **Settings** and scroll down to **Enrollment**.





1. Enter the address used for client connections to the <Acronis Cyber Files> Gateway and configured in the **AppConnect Configuration**. For a true test this URL should not be reachable by the mobile client (use celluar or an external network).
2. Tap **continue**.
3. Enter **Username** and **Password** and tap **Enroll Now**.

You should see "You are now enrolled with Acronis Cyber Files client management."

If the data sources in your profile are all part of the Acronis Cyber Files Gateway that has been configured to route through the sentry you should be able to browse those sources via the AppTunnel also at this point.

Verify AppTunnel usage

You can verify this traffic is going through the AppTunnel by logging into the MobileIron Sentry System Manager.

1. Select Troubleshooting and open **Logs**.
2. Check **Sentry**, **To/From Device**, **To/From Service**, and **Level 4**.
3. Select **Apply**.
4. Under "**View Module Logs**" select **Sentry**.
5. When traffic comes from the mobile device you should see the sentry log scroll with entries related to the hostname configured.

Adding Kerberos Constrained Delegation Authentication

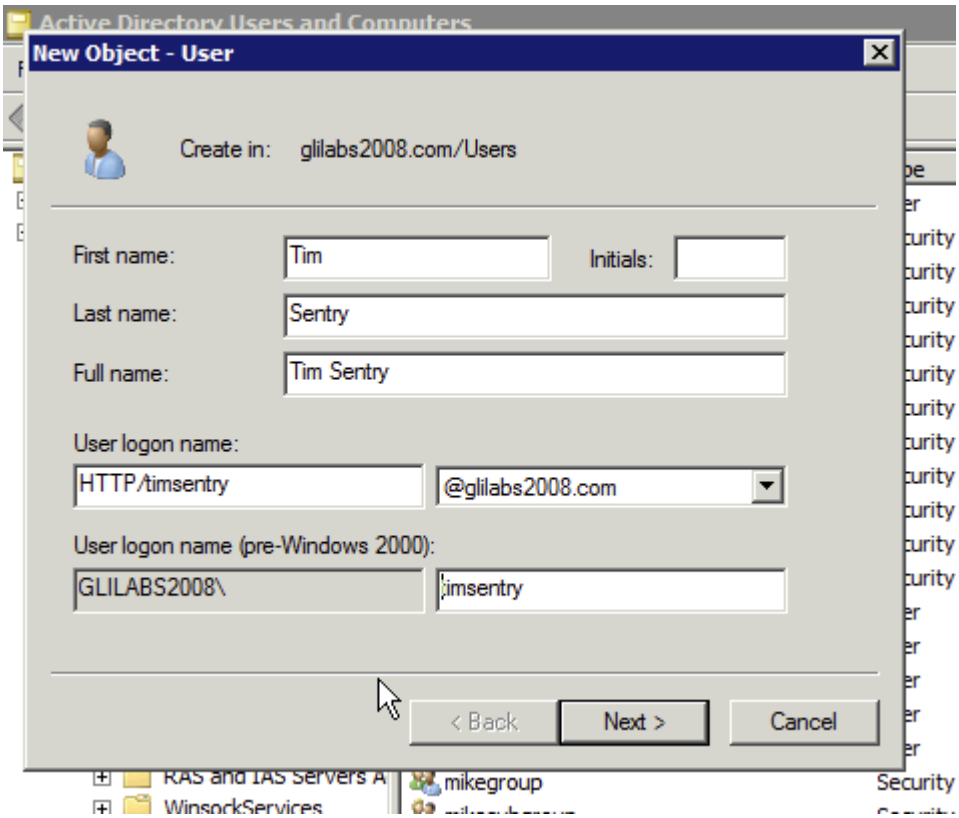
Once you have setup and verified the AppTunnel works via Username/Password authentication for Acronis Cyber Files, you can modify the configurations created to allow Kerberos Constrained Delegation authentication to the Acronis Cyber Files Gateway. When this is properly configured the end user will not have to supply a username or password to enroll with management or to browse data sources.

This document will set up the basic configuration and delegate to one Acronis Cyber Files Gateway server running on the same server as the management server to allow enrollment to that local management server and browsing of datasources configured on that gateway. Additional delegation will be required for additional Gateways, Sharepoint servers, and reshares.

If you are going to use the same iOS device to test the Kerberos Constained Delegation it is recommended you uninstall the Acronis Cyber Files mobile at this time.

Create a Kerberos Service Account

1. Log in to your KDC server as an administrator.
2. From the Windows Start menu, select **All Programs**, select **Administrative Tools > Active Directory Users and Computers**.
3. In the newly opened console, expand the domain (Kerberos refers to a domain as a realm).
4. Right-click **Users** and select **New > User**.



- Enter a **Name** and a **User Logon Name** for the Kerberos service account. Use standard alphanumeric characters with no whitespace for the **User Logon Name**, as it is entered in a command prompt later in the guide.
- The name must start with **HTTP/**. If **HTTP/** automatically appears next to the **User logon name (pre-Windows 2000)** field, delete it from that field.

5. Ensure that the correct domain name is selected in the field next to the **User Logon Name** field. If the correct domain is not selected, choose the correct domain name from the drop-down list next to the **User Logon Name** field.

Create a keytab for the Kerberos Service Account

When you create a keytab, the Sentry service account is concurrently mapped to the **servicePrincipalName**.

1. On the KDC server, open a command prompt window
2. At the prompt, type the following command: **ktpass /out nameofsentry.keytab /mapuser nameofuser@domain /princ HTTP/nameofuser /pass password**

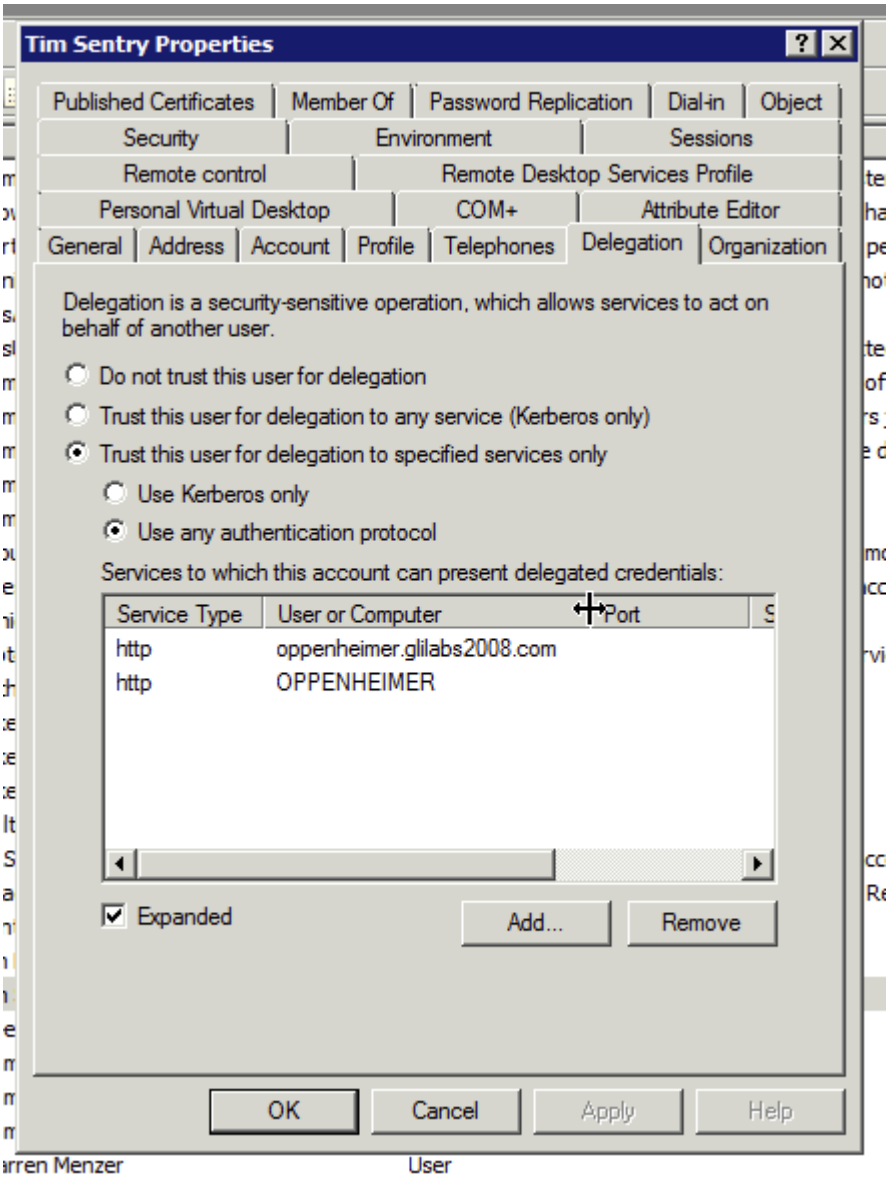
> E.g. ktpass /out timsentry.keytab /mapuser timsentry@glilabs2008.com /princ HTTP/timsentry@glilabs2008.com /pass 123456

This warning can be ignored.

Delegate HTTP service to the Cyber Files Gateway server

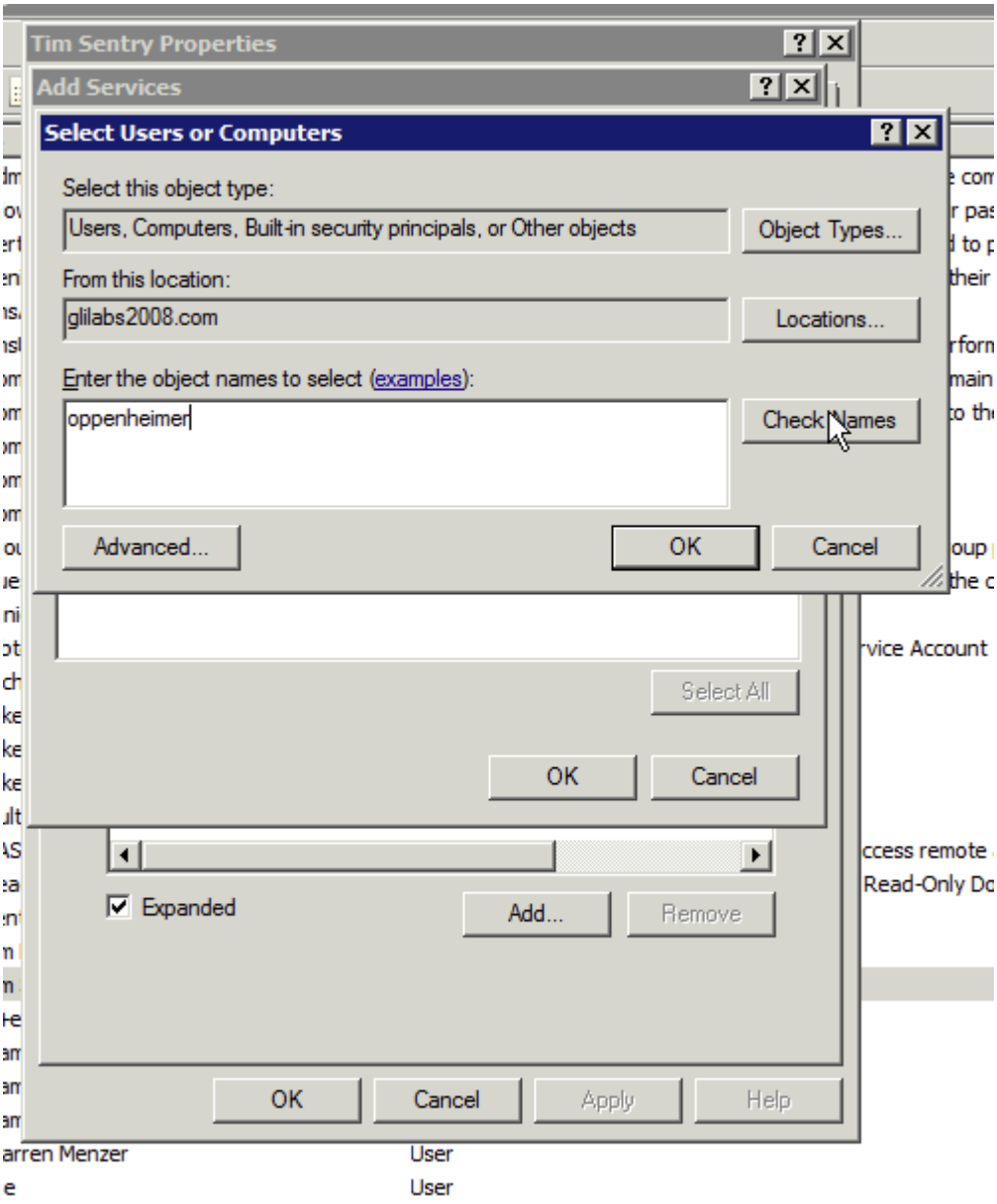
1. From the Windows Start menu, select **All Programs** and open **Administrative Tools > Active Directory Users and Computers**.
2. In the newly opened console, expand the realm (domain).
3. Click on **Users**.
4. Find and select the Kerberos user account that you created in "Create a Kerberos Service Account".
5. Right-click on the account and select **Properties**.
   - Click on the **Delegation** tab.
   - Select **Trust This User For Delegation To Specified Services Only**.

- Select **Use Any Authentication Protocol**.

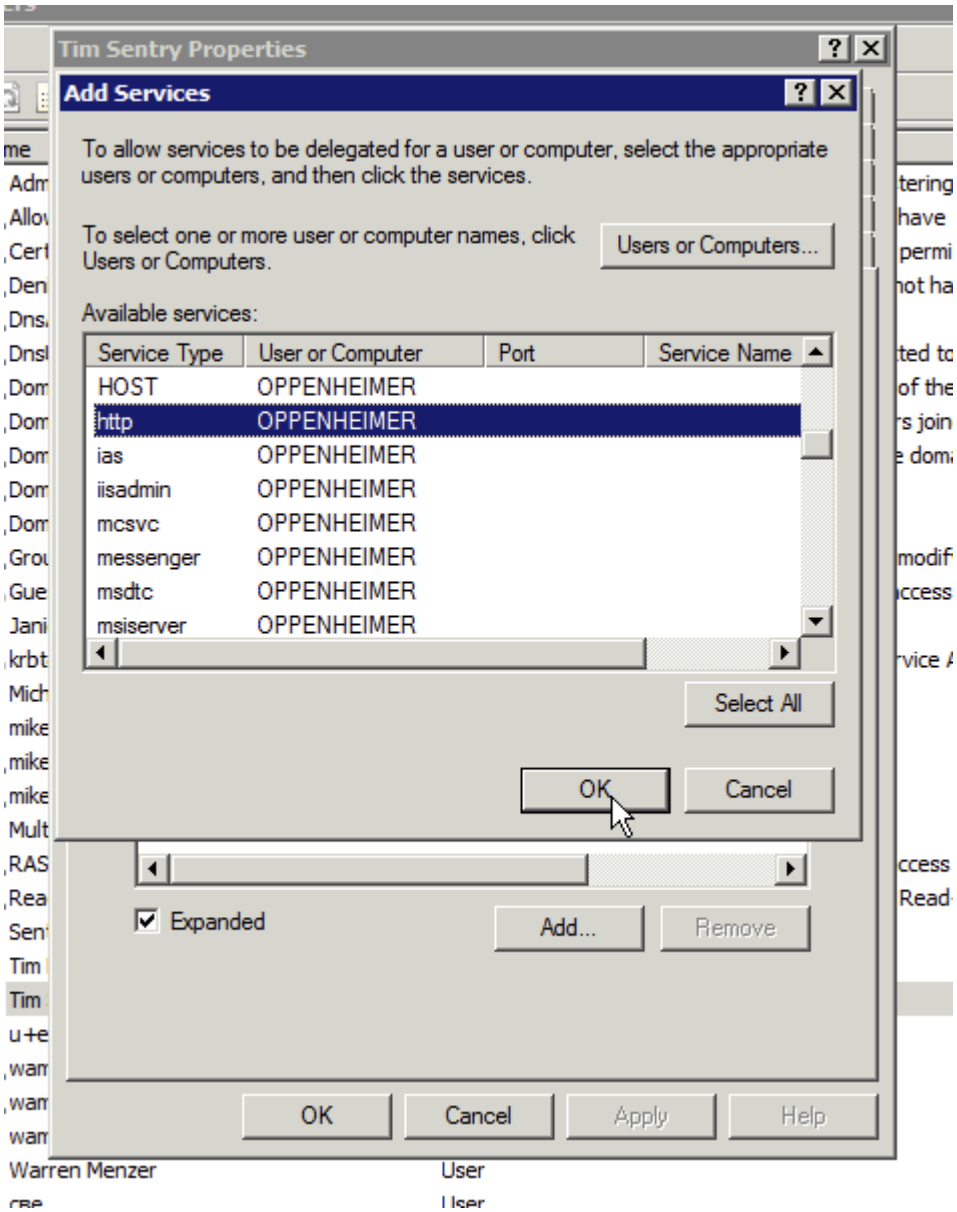


6. Press **Add...**.
7. Press **Users or Computers...**.
   - Enter the computer name of the Cyber Files Gateway Server.
   - Click on **Check Names**.

- The correct computer name should appear in the object name box.



8. Click **OK**.
9. Find and select the "**http**" service in the **Add Services** window.



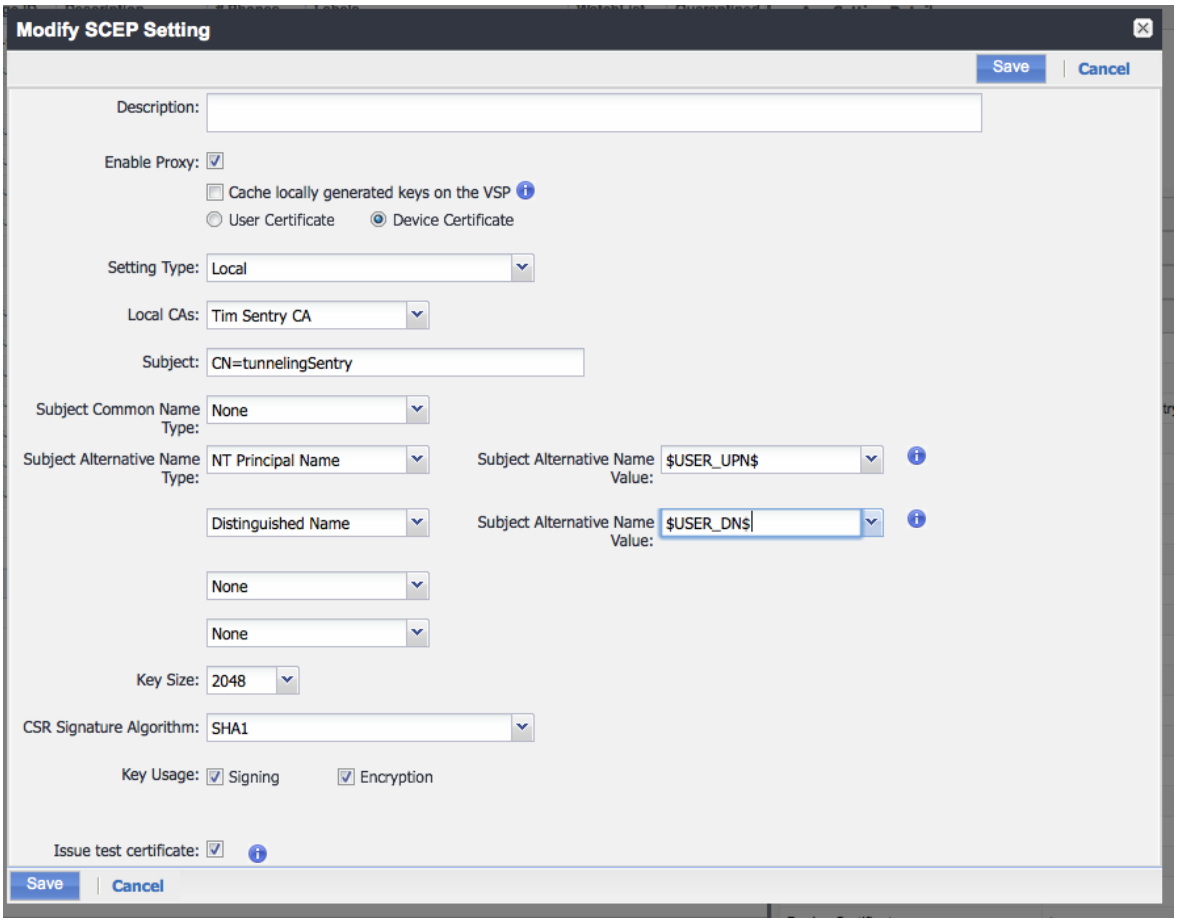
10. Click **OK**.

Note

For a large deployment with multiple Gateway Servers you should repeat steps 6 through 10 for each Gateway Server. However, for the initial setup, it's best to begin with a single Gateway Server hosting some local test folders. Once you have confirmed access to those, then you can expand to additional Gateway Servers and non-local folders.

Additional SCEP configuration

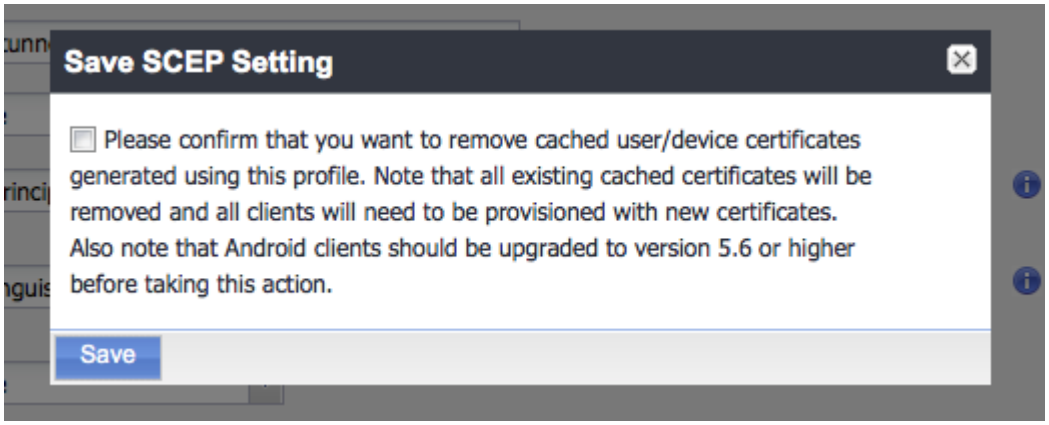
1. Open the MobileIron VSP Admin Portal.
2. Select **Policies & Configs** and open **Configurations**.
3. Find the SCEP created in "Create a new SCEP".
4. Click on its name and click **Edit** in the panel on the right.



- Enter two **Subject Alternative Name Types**
  - **NT Principal Name**: **$USER_UPN$**
  - **Distinguished Name**: **$USER_DN$**

> **Note**
> These entries require user accounts on the VSP to come from the active directory and these variables to be supplied by it. This configuration is beyond the scope of this document.

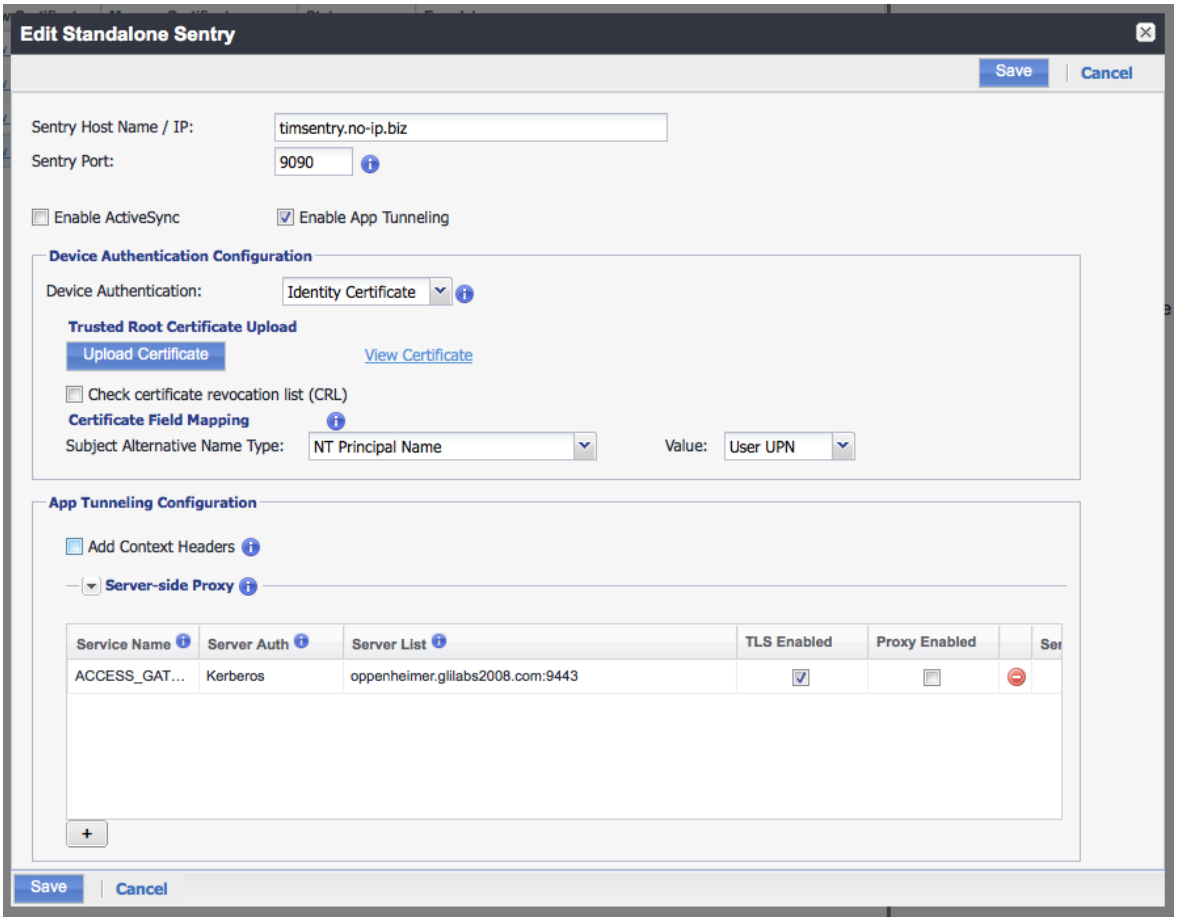
5. Click **Save**.



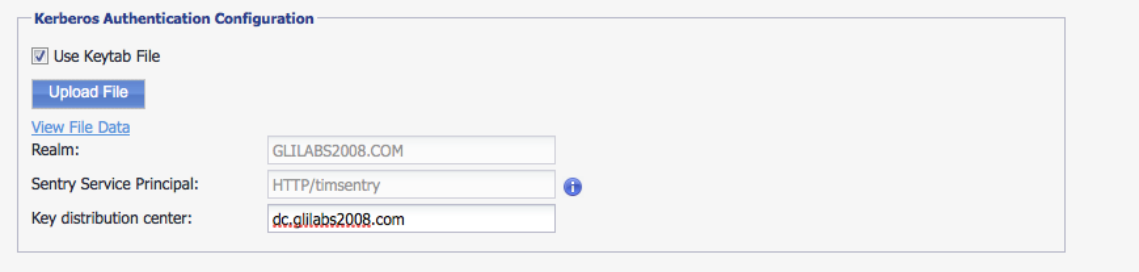
6. Since you have modified the SCEP, you will have to re-provision the device in Mobile@Work before testing the iOS client.

Additional Sentry configuration

1. Still in the MobileIron VSP Admin Portal, select **Settings** and open **Sentry**.
2. Find the **Sentry** created in "Add and Configure the Sentry".
3. Click on the **Edit** icon.



- In the **Device Authentication Configuration** select the following for the **Certificate Field Mapping**:
  - **Subject Alternative Name Type**: **NT Principal Name**
  - **Value**: **User UPN**
- In the **App Tunneling Configuration** change the **Server Authentication** to Kerberos.



- In the **Kerberos Authenication Configuration** section.
  - Check **Use Keytab File**.
  - Click **Upload File**.

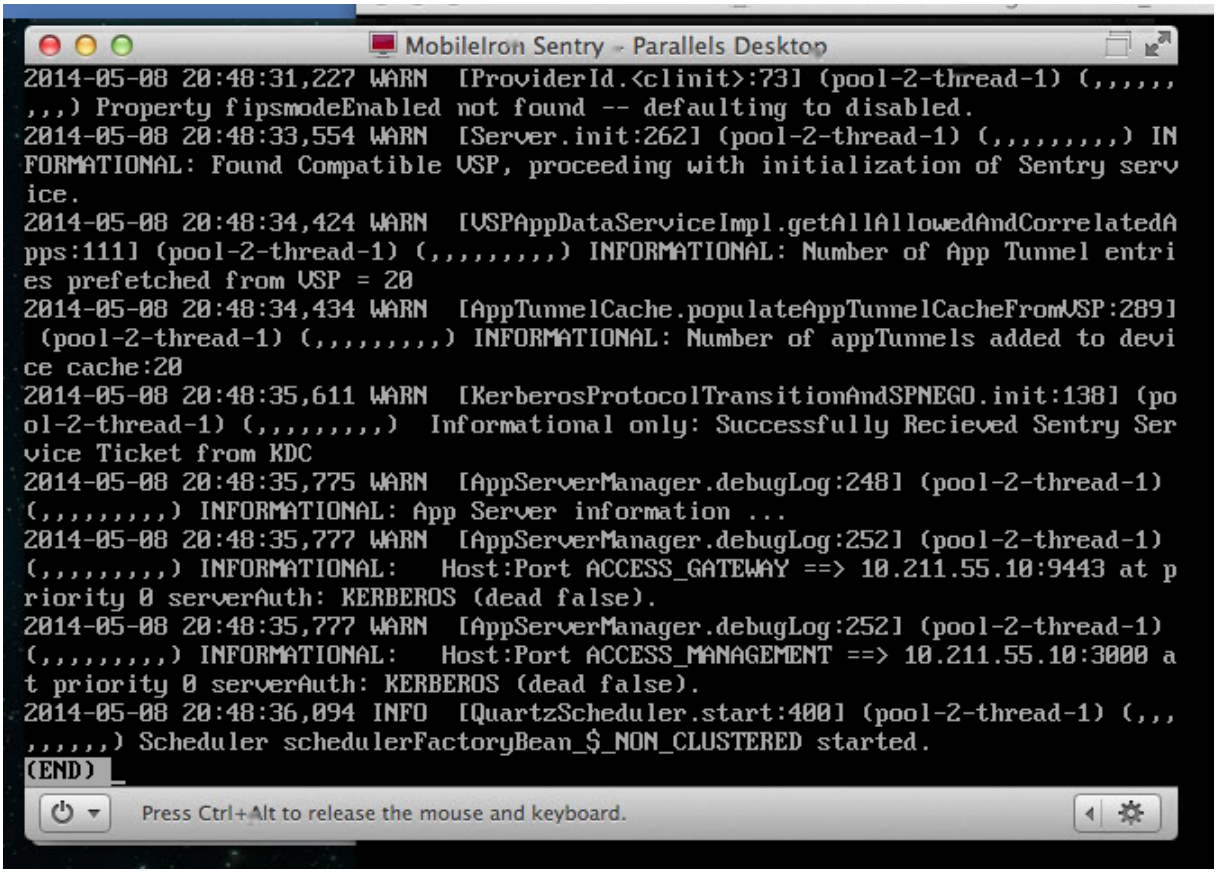
- Upload the keytab file created in "Create a keytab for the Kerberos Service Account".
- Put the domain controller in the Key distribution center.

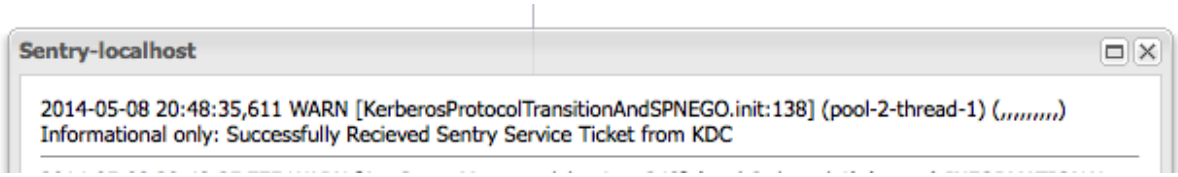
4. Click **Save**.

Verify sentry/KCD communication

Using either the **Sentry EXEC** or the Sentry logs in the **System Manager** verify the Sentry is able to reach and receive a Kerberos ticket from the KDC.

Find the line "**Informational only: Successfully Received Sentry Service Ticket from KDC**". This verifies the Sentry is able to reach and communicate with the KDC.



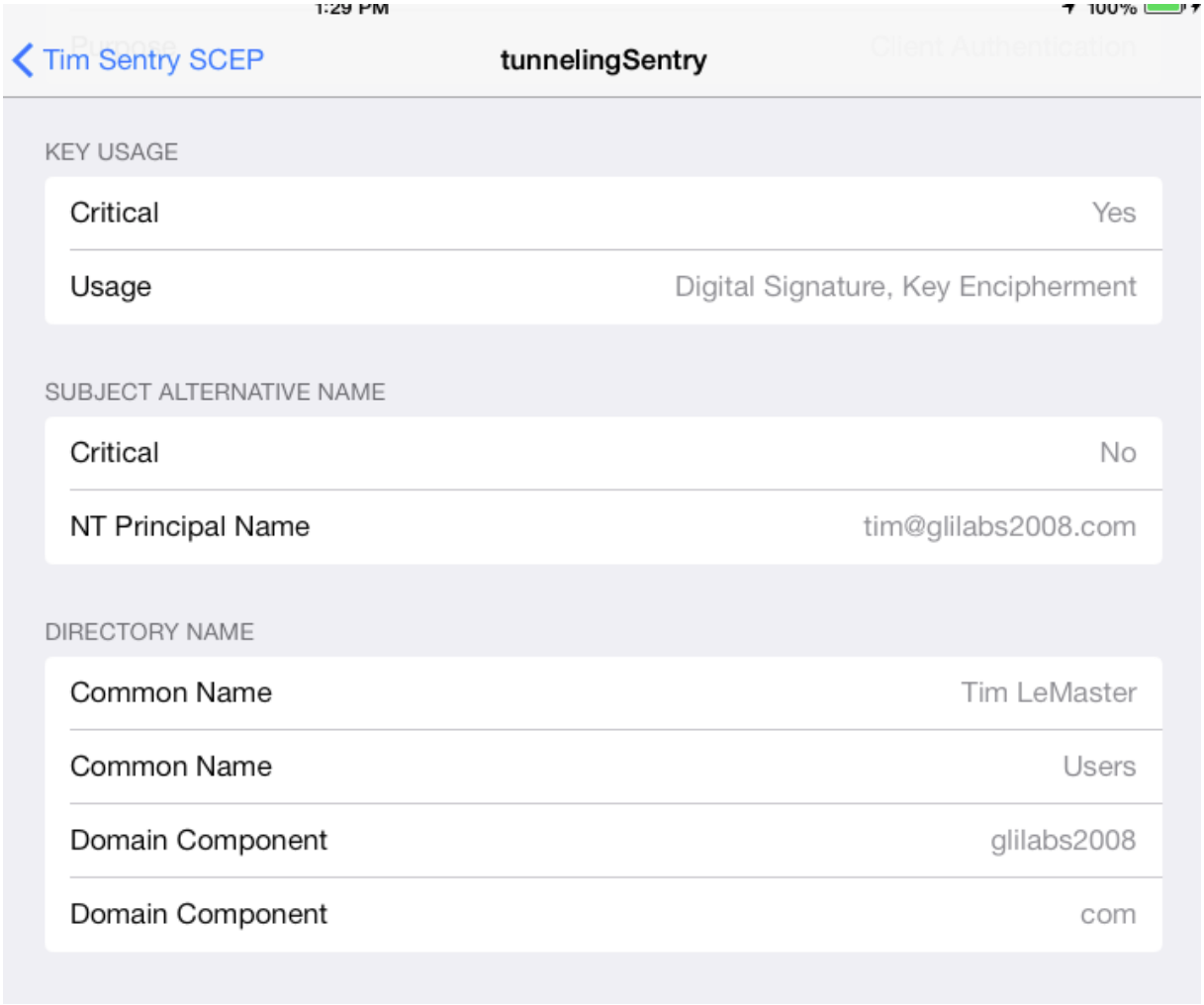


Testing the iOS client

The changes we made to the SCEP must be pushed down to the iOS device. The changes we made to the Sentry can take several minutes to be pushed down to it.

On the device, open the AppConnect app -> Settings -> Check for updates and tap on "Re-Enroll Device" and follow the prompts.

You can verify the SCEP is properly updated using the iOS Settings app. Under Settings -> General -> Profiles -> The SCEP name you created -> More Details -> Certificate -> The portion after CN= you enter in the subject name of the SCEP, you should see entries for "Subject Alternative Name" and "Directory Name". If this is properly pulled from Active Directory it should match the user that you used to activate Mobile@Work.



If that is correct reinstall the Acronis Cyber Files mobile. Repeat the enrollment steps from before but leave the username and password fields blank. If all is successful you should be enrolled using the account that matched the NT Principal Name in the profile you just examined.

Delegation for network shares and SharePoint

This article will help you configure MobileIron credential delegation methods with network shares and SharePoint sites. This guide requires that you have already configured both MobileIron and Acronis Cyber Files, their interoperability and their respective Active Directory accounts that delegate authentication.

17.1 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.

17.1.1 Acronis Cyber Files for BlackBerry Dynamics

For iOS

Introduction

Acronis Cyber Files and BlackBerry Technology have partnered to bring Acronis Cyber Files's mobile file management to the BlackBerry Dynamics platform. This optional Acronis Cyber Files capability allows the Acronis Cyber Files mobile app to be managed, along with other BlackBerry enabled apps, using a unified set of BlackBerry Dynamics policies and services.

The components of the BlackBerry Dynamics platform include:

- **BlackBerry Control server** - A server-based console that allows the enterprise to enable client access to BlackBerry Dynamics enabled apps, create policy sets that govern application permissions and the device types they are allowed to run on, and the ability to revoke access to or wipe BlackBerry Dynamics apps on specific devices.
- **BlackBerry Proxy server** - This service is installed on an on-premise server and is used to provide network access for BlackBerry Dynamics apps needing to communicate with on-premise application servers, such as a Acronis Cyber Files Gateway server.
- **Acronis Cyber Files for BlackBerry Dynamics app** - BlackBerry Dynamics enabled apps, such as **Acronis Cyber Files for BlackBerry Dynamics**, include built-in BlackBerry Dynamics services that allow the app to be remotely managed using the BlackBerry Dynamics platform and also provide the app with FIPS 140-2 certified on-device encrypted secure storage and BlackBerry secure communication.

Acronis Cyber Files for BlackBerry Dynamics requires:

- **Acronis Cyber Files for BlackBerry Dynamics client app** - The Acronis Cyber Files for BlackBerry Dynamics client app available on the Apple App Store is specifically designed as a BlackBerry Dynamics integrated application. When first installed and run on a device, the Acronis Cyber Files for BlackBerry Dynamics app will prompt the user to activate the app in BlackBerry Dynamics. This activation is required before the user can proceed with enrolling the app with their Acronis Cyber Files server and accessing file.
- **Acronis Cyber Files server** - Acronis Cyber Files for BlackBerry Dynamics uses the same server-side software as standard Acronis Cyber Files. No server-side changes are required for Acronis Cyber Files servers to work with BlackBerry Dynamics enabled Acronis Cyber Files clients. This can be used to ensure that all the Acronis Cyber Files that have access to Acronis Cyber Files files are managed by BlackBerry Dynamics.

Once a Acronis Cyber Files for BlackBerry Dynamics client is enrolled in BlackBerry Dynamics, all communication with the Gateway servers is routed though the BlackBerry Dynamics secure communication channel.

Testing a trial version of Acronis Cyber Files for BlackBerry Dynamics

The process of trialing Acronis Cyber Files for BlackBerry Dynamics is very much the same as a regular Acronis Cyber Files trial.

1. A trial version of the server-side software can be requested by visiting the Acronis site. Once this request form has been submitted, you will receive an email with links to download the Acronis Cyber Files server trial installer and to the Quick Start Guide to assist in initial setup.
2. The Acronis Cyber Files for BlackBerry Dynamics client app is a free download from the Apple App Store.

Note
Acronis Cyber Files for BlackBerry Dynamics client apps need to be activated in your BlackBerry Dynamics system before they can be configured for access to Gateway Servers. When you are ready to enroll Acronis Cyber Filess in BlackBerry Dynamics, please proceed to the following sections of

this document.

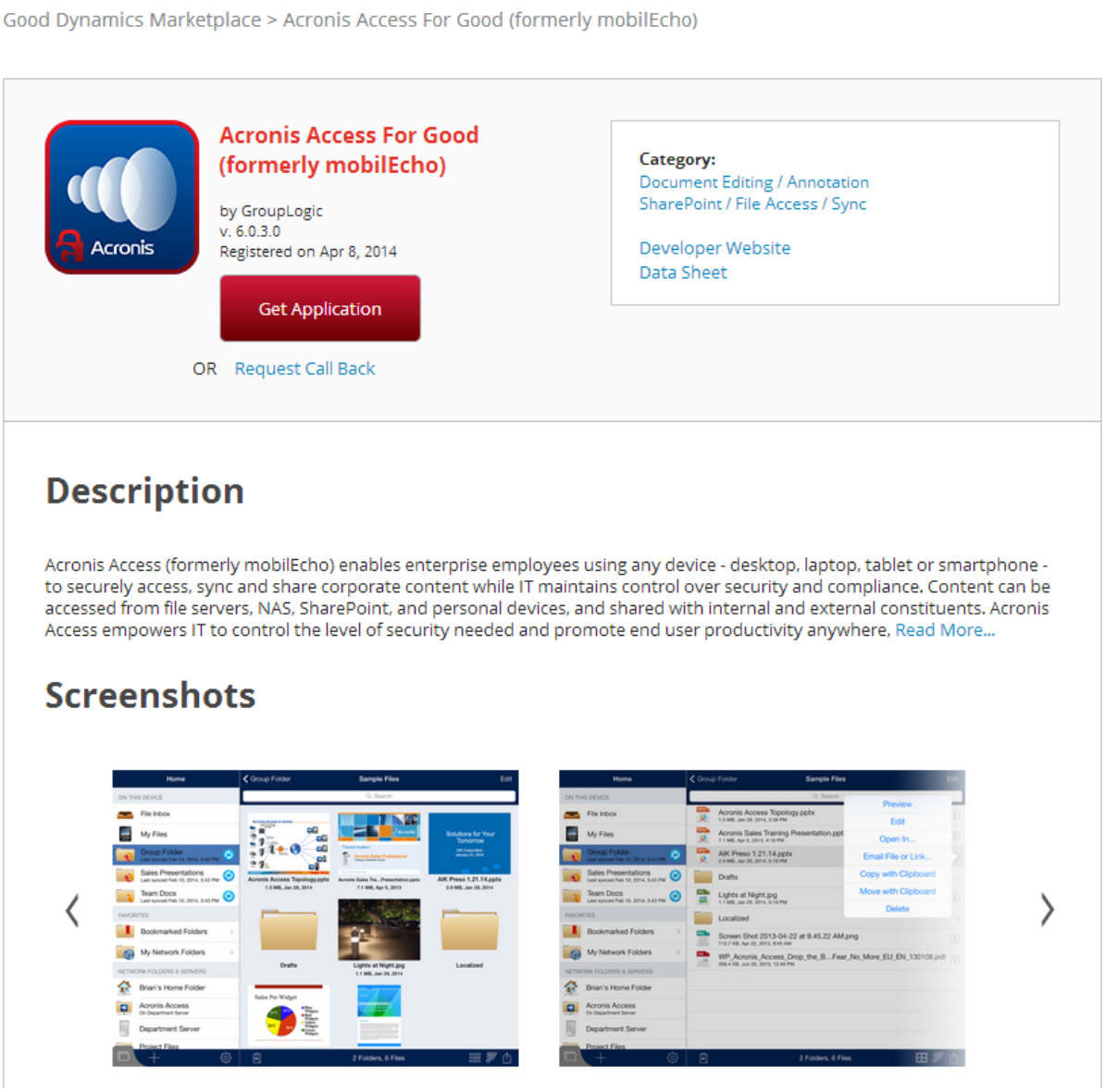
Requesting and configuring Acronis Cyber Files within BlackBerry Control

Before a Acronis Cyber Files for BlackBerry Dynamics client app can be enrolled in BlackBerry Dynamics, Acronis Cyber Files must be added to the list of **Managed Applications** on your BlackBerry Control server. For this to happen, you must request access to the **Acronis Cyber Files for Good** app using the BlackBerry Dynamics **Communities** site. If you are not currently a registered member of the site, another member of your organization may be responsible for managing vendor relationships on this site, or you may simply need to register for an account with BlackBerry .

Requesting access to Cyber Files for Good Dynamics

To request access to **Acronis Cyber Files for** BlackBerry , visit the BlackBerry marketplace (https://begood.good.com/marketplace.jspa) and locate **Acronis Cyber Files for** BlackBerry in the list of available BlackBerry **Dynamics** apps.

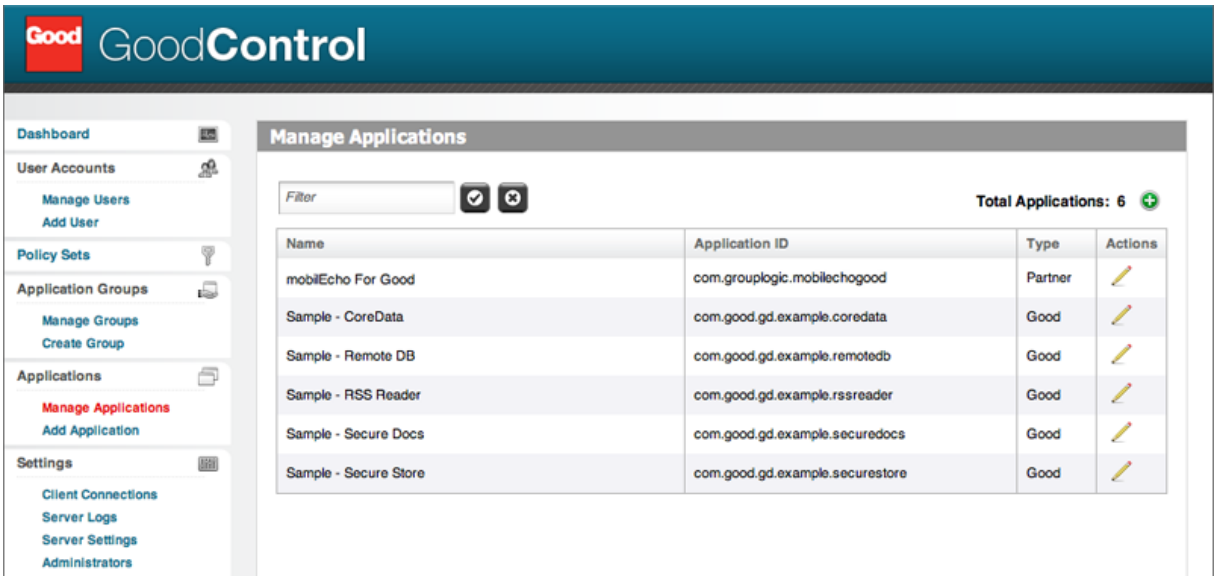
On the Acronis Cyber Files for BlackBerry app page, click the Start Trial button to request a trial or get the licensed version of the app.



If you select a trial version of the app, your access should be granted within a few minutes. You should receive a notification from the BlackBerry site when your request has been accepted and notify you that the **Acronis Cyber Files for** BlackBerry app as been published to your BlackBerry Control server.

Note
If you do not receive access, please contact BlackBerry Dynamics support.

Once this has happened, log into your BlackBerry Control server and click **Manage Apps** in the lefthand menu. Acronis Cyber Files should now be listed in your applications list. If it's not listed, give it 15 minutes or so and check again. This will allow the change time to propagate to your server.



Configuring Good Proxy access to your Cyber Files Gateway server(s)

In order for Acronis Cyber Files to be able to access your Acronis Cyber Files Gateway server through the BlackBerry Proxy server, you will need to configure access to the domain where your Acronis Cyber Files Gateway servers reside. This is done on the **Client Connections** page in the Good Control console.

Allowing access from your domain

This setting allows all BlackBerry clients to connect to all servers in the specified domain(s). If you don't want that, setup **Additional Servers** instead.

1. Open the **Client Connections** settings from the lefthand menu.
2. Expand **Allowed Domains**. Unless **Allow all domains** is enabled, press the plus (+) icon and enter the name of your domain (e.g. mycompany.com).
3. Press **Submit**.

Assigning your domain as a default domain for connections

1. Expand **Default Domains**.
2. Press the plus (+) icon and enter the name of your domain.
3. Press **Sumbit**.

Allowing specific servers to connect

Use this setting instead of the **Allowed Domains** if you wish that your Good clients connect only these specific servers instead of every server in the domain.

1. Open the **Client Connections** settings from the lefthand menu.
2. Expand **Additional Servers**.

3. Press the plus (+) icon and enter the DNS name and port of the server you want to grant access to. Repeat this step for all Acronis Cyber Files servers you want your BlackBerry clients to connect.

BlackBerry Dynamics Policy Sets and Acronis Cyber Files

The Acronis Cyber Files for BlackBerry Dynamics app respects the policy settings included in a user's assigned **Policy Set**. Policy sets are configured on the BlackBerry Control server.

Note
If you enable FIPS in the BlackBerry portal for a user's **Policy Set**, their Acronis Cyber Files app will not be able to access Gateway Servers using third-party certificates by IP address.

These settings include:

- Application lock password requirements
- Lock screen policies
- Data leakage protection
- Permitted OS versions and hardware models
- Connectivity verification
- Jailbreak/root detection

Data Leakage Protection effects and limitations

If **Data Leakage Protection** is enabled in a policy set, the Acronis Cyber Files app will not be permitted to:

- Open files into standard 3rd party applications on the device
- Receive files from other standard 3rd party applications on the device
- Email files using the default email client
- Print files
- Copy and paste text from within opened files

Note
If you require these features, you will need to enable the **Disable Data Leakage Protection** check box in the applicable BlackBerry Policy Set.

Note
Acronis Cyber Files for BlackBerry Dynamics includes a BlackBerry Dynamics feature called "Secure Docs". This allows files to be transferred between the Acronis Cyber Files for BlackBerry Dynamics app and the BlackBerry for Enterprise app. Once a file is opened into the BlackBerry for Enterprise app, it can then be opened into other 3rd party BlackBerry Dynamics enabled apps that include this feature. This functionality will be available, even with the BlackBerry Control **Data Leakage Protection** policy setting enabled.

Granting Acronis Cyber Files access to a BlackBerry Dynamics User or Group

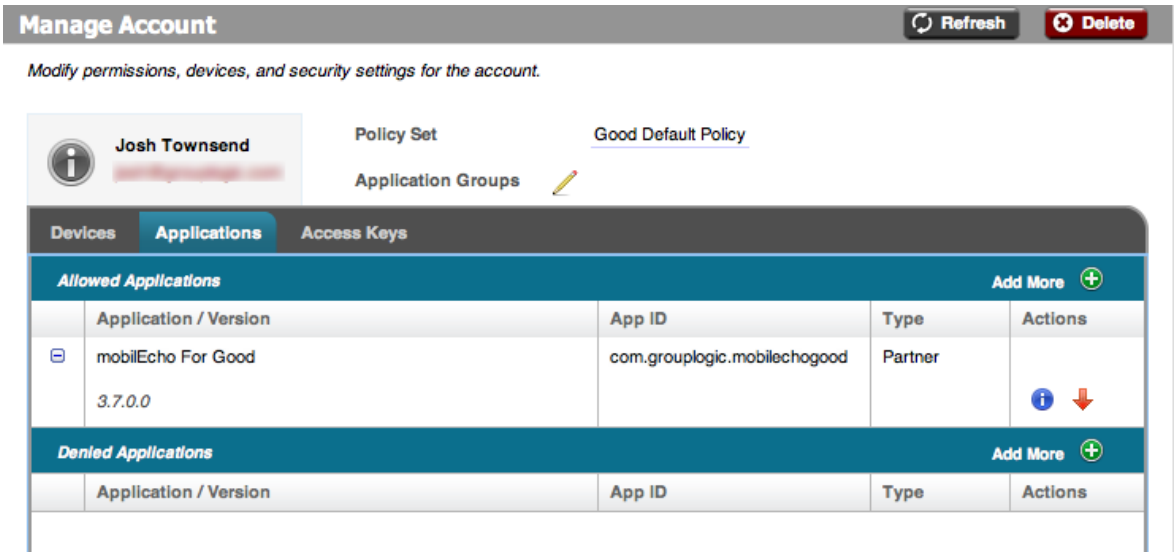
Before a user can enroll their Acronis Cyber Files app in BlackBerry Dynamics, they must have the Acronis Cyber Files application added to their user accounts **Allowed Applications** list or to an allowed **Application Group** they belong to. In addition, a unique **Access Key** must be sent to the user and entered into the Acronis Cyber Files app during the enrollment process.

Important
When you assign access to BlackBerry Dynamics applications to individual users, you are required to select specific version numbers of the app to allow. If you manage access on the user level, when new versions of Acronis Cyber Files for BlackBerry are released, you will need to return to the users' BlackBerryControl configuration and add the new version before they are allowed to run that version.

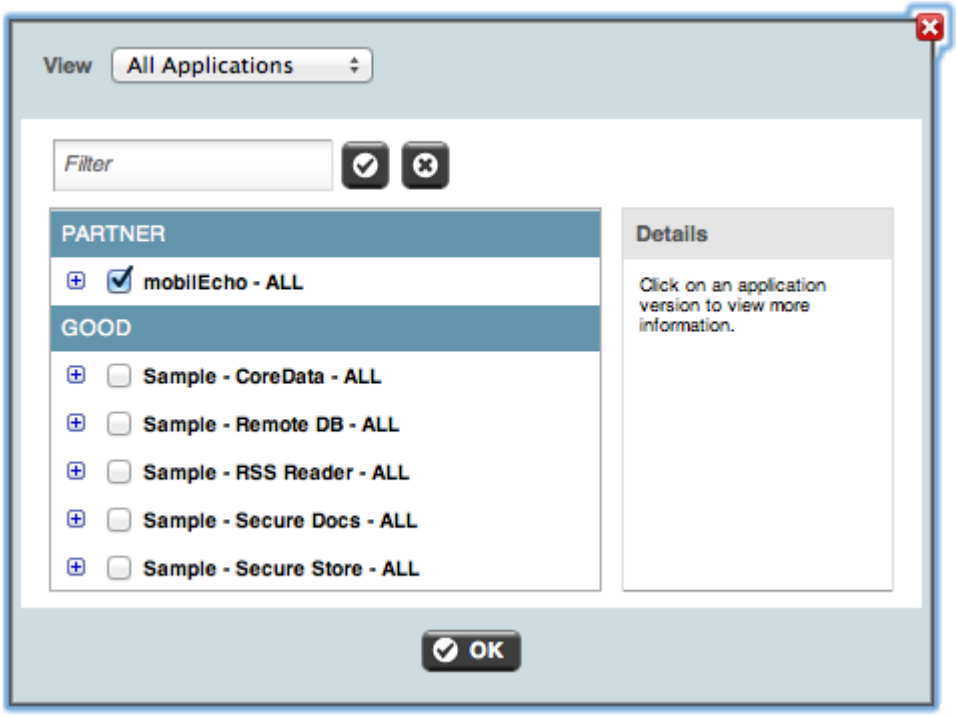
Note
We **highly recommend** that you allow access to BlackBerry Dynamics apps using the **Manage Groups** functionality in the BlackBerry Control console. BlackBerry Control allows you to give a group access to ALL versions of an app, so that future versions will be allowed without IT admin intervention.

To add the Acronis Cyber Files app to an Allowed Applications list in a User Account or Application Group:

1. Select **App Groups** or **Manage Users** from the lefthand menu in the BlackBerry Control console.
2. Select the group or user you'd like to give access to Acronis Cyber Files for BlackBerry and edit them.
3. In the **Apps** section, click the **Add More** button.

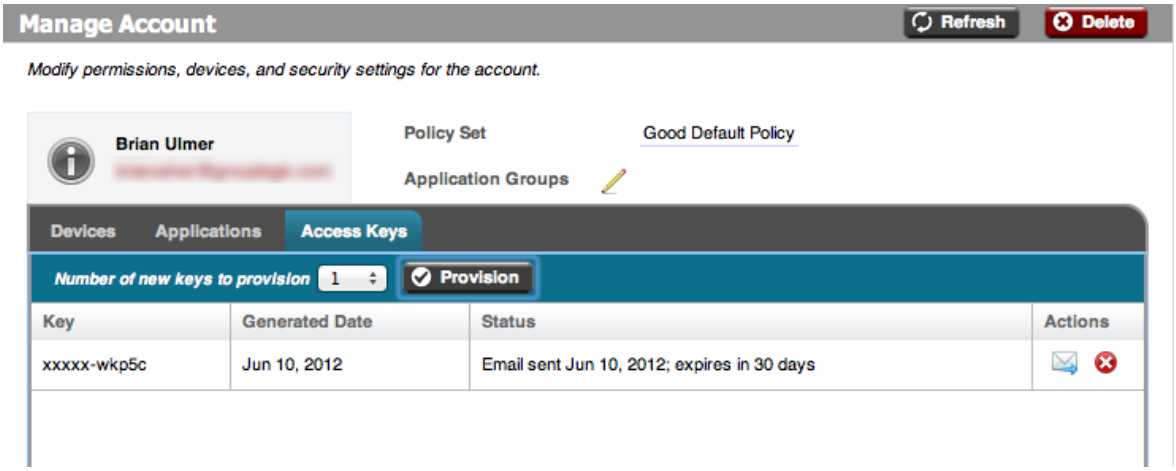


4. Select **Acronis Cyber Files for** BlackBerry from the list of available applications and click **OK**.



To generate an Access Key that will allow a user to enroll their Acronis Cyber Files for BlackBerry **app with** BlackBerry **Dynamics:**

1. Select **Manage Users** from the lefthand menu in the BlackBerry Control console.
2. Select the user you'd like to create an **Access Key** for and edit them.
3. On the **Access Keys** tab, press New **Access Key**.



The user will receive an email that includes the **Access Key** and some basic BlackBerry Dynamics instructions.

Enrolling the Acronis Cyber Files client app in BlackBerry Dynamics

The Acronis Cyber Files for BlackBerry client app available on the Apple App Store is purpose built as a BlackBerry Dynamics integrated application. When first installed on a device, the Acronis Cyber

Files app starts and requires the user to activate it in your BlackBerry Dynamics system.

To enroll a Acronis Cyber Files client app in BlackBerry **Dynamics:**

Note
Easy Activation requires at least one BlackBerry application (BlackBerry Work, BlackBerry Access, or BlackBerry Agent) to be installed for activation to succeed. Applications that have been upgraded from a prior version of Acronis Cyber Files that was activated using a third-party application should continue to function as expected

1. Launch **Acronis Cyber Files for** BlackBerry **Dynamics** on your device.
2. Enter your **Email Address** and the **Access Key** that was emailed to you by your IT administrator.
3. Progress will be displayed as your app is enrolled with BlackBerry Dynamics.
4. If required by your BlackBerry Dynamics policy, you will be asked to set an application lock password. If you are also using BlackBerry for Enterprise, Acronis Cyber Files may require that you log into BlackBerry for Enterprise in order to gain access to the Acronis Cyber Files app. Once this process is completed, you will be taken to the Acronis Cyber Files application's home screen.

From this point on, when you start the Acronis Cyber Files app, you may be required to enter the Acronis Cyber Files for BlackBerry Dynamics application password that you configured earlier, or you may be required to authenticate with your BlackBerry for Enterprise app before Acronis Cyber Files opens.

Aside from that requirement, Acronis Cyber Files for BlackBerry Dynamics functions the same way that the standard Acronis Cyber Files app does. Some features in the app may be restricted based on your BlackBerry Dynamics policy set. This includes features such as opening Acronis Cyber Files files into other 3rd party applications, emailing and printing files, copying and pasting text from Acronis Cyber Files files, etc.

Note
Once the Acronis Cyber Files for BlackBerry Dynamics app has been activated in BlackBerry Dynamics, it is not possible to deactivate. If you need to switch to a standard version of Acronis Cyber Files, you will need to delete the Acronis Cyber Files for BlackBerry Dynamics app and reinstall the standard Acronis Cyber Files app

Side-loading Acronis Cyber Files

The BlackBerry Dynamics version of the Acronis Cyber Files app now supports the **iTunes File Sharing** feature. This feature allows files and folders to be copied directly into the Documents folder of the app's sandbox. Once in the app sandbox, they will automatically be imported into the correct sync folders in the app's encrypted storage.

Side-loading of files is limited by the free storage space on the device and will require additional free space, equivalent to at least the size of the largest file being imported, to complete the side-loading process. This feature is intended for 2-way file transfer, it does not give users rights to read or copy the files.

Note
The Acronis Cyber Files app is not actively involved in the iTunes File Sharing file transfer process.

Note
This procedure requires a fresh install of Acronis Cyber Files for BlackBerry Dynamics that isn't enrolled in management.

Preparing Documents for Side Loading

Note
Ensure that the device has sufficient free storage space before side-loading and do not interrupt the sync process once it begins.

1. In the Acronis Cyber Files web administration, navigate to Mobile Access --> Data Sources.
2. If you already have Data Sources that you wish to use, make sure they are marked as 1-way or 2-way sync folders. If you don't have Data Sources that you want to side-load, create new ones.
3. Assign the Data Sources to a group containing the users whose iOS devices will be side loaded. For this example we will create a folder named Reference.
4. On a computer, create a folder called To Import and copy the desired folders inside it. So in this example we have a To Import folder containing the Reference folder, which contains the documents that the server would normally try to sync to the iOS device over the internet.

   Note
   The folders inside the To Import folder must be named exactly like the Data Sources' display names. For example, you have a Data Source called Reference, and in the To Import folder you will create a folder called Reference.

5. If you are performing this procedure on a Windows machine, you will have to install iTunes.

Sync the items through iTunes

1. Install the Acronis Cyber Files for BlackBerry Dynamics app.
2. Connect the iOS device to a computer using a cable. Cables that can only charge the device will not work.
3. Open iTunes and select the device. Click Trust on the computer and device if prompted.
4. In iTunes, click on the device icon and then on the Apps section in the left sidebar.
5. Scroll down to the File Sharing section of the page and select Acronis Cyber Files.
6. Drag the "To Import" folder you created into the Acronis Cyber Files Documents section in iTunes.
7. Click Sync. Follow other iTunes prompts if needed and let the sync to complete.

Enrolling and importing the side-loaded documents

1. After the iTunes sync is complete, launch the Acronis Cyber Files for BlackBerry app.

   Note
   The importing of the files and folders will take place before the Acronis Cyber Files app is enrolled with the Acronis Cyber Files server. The procedure must be performed on a clean install.

   Note
   This feature performs an initial loading of sync folder content and then hands off the folder syncing responsibilities to the Acronis Cyber Files app. All onward syncing will proceed as usual.

2. Enter the BlackBerry email address and Access Key for your user.
3. Follow the wizard to complete enrollment with the Acronis Cyber Files server. You will be prompted to enter your Acronis Cyber Files username and password.
4. Dismiss the tutorial that appears on the first run.
5. The import process will begin. At this point, the Acronis Cyber Files app will import the documents that were side-loaded into its secure container. It will then check with the server to confirm which documents match the corresponding sync folder. If everything is the same, the device will be in sync with the server, for the side-loaded sync folder(s).

Important notes

- Any assigned sync folders that do not have a corresponding folder in the To Import folder will be silently ignored and will perform a standard, full over-the-air initial sync after the import process completes.
- Any folders in the To Import folder that do not match an assigned network sync folder will be silently ignored and deleted from the device.
- If the user leaves the app while the import is executing, it will continue to run in the background for up to 10 minutes. This time period is depended on iOS app management out of Acronis Cyber Files control. If the Acronis Cyber Files app is shut down by iOS or the end user, the import process will continue where it left off the next time the app is started.
- After the preloaded files and folders have been copied into the appropriate sync folders, the app will perform an over-the air sync. During this first sync, the app will consider any files side-loaded into the app as up-to-date as long as the server version of that file has the same file size. The timestamps on the files will not be expected to match, so if the sizes match, the local file's timestamp will be updated so that it matches the server version. If the sizes do not match, the file will be automatically synced down from the server and replaced. This will not trigger any conflict detection behavior.
- A policy setting will be added to the BlackBerry Dynamics application policy section for Acronis Cyber Files (on the BlackBerry Control server) that governs whether this side-loading behavior is active. By default, this feature will be disabled. If disabled in the BlackBerry Dynamics policy, the

enrolled/activated Acronis Cyber Files for BlackBerry app will delete any files and folders that are copied into the Documents folder via iTunes File Sharing, each time the app starts up.

For Android

Introduction

Acronis and BlackBerry Technology have partnered to bring Acronis Cyber Files's mobile file management to the BlackBerry Dynamics platform. This optional Acronis Cyber Files capability allows the Acronis Cyber Files mobile app to be managed, along with other BlackBerry enabled apps, using a unified set of BlackBerry Dynamics policies and services.

The components of the BlackBerry Dynamics platform include:

- **BlackBerry Control server** - A server-based console that allows the enterprise to enable client access to BlackBerry Dynamics enabled apps, create policy sets that govern application permissions and the device types they are allowed to run on, and the ability to revoke access to or wipe BlackBerry Dynamics apps on specific devices.
- **BlackBerry Proxy server** - This service is installed on an on-premise server and is used to provide network access for BlackBerry Dynamics apps needing to communicate with on-premise application servers, such as a Acronis Cyber Files Gateway server.
- **Cyber Files for BlackBerry Dynamics app** - BlackBerry Dynamics enabled apps, such as **Acronis Cyber Files for BlackBerry Dynamics**, include built-in BlackBerry Dynamics services that allow the app to be remotely managed using the BlackBerry Dynamics platform and also provide the app with FIPS 140-2 certified on-device encrypted secure storage and BlackBerry secure communication.

Cyber Files for BlackBerry Dynamics requires:

- **Acronis Cyber Files for BlackBerry Dynamics client app** - The Acronis Cyber Files for BlackBerry Dynamics client app available on the Apple App Store is specifically designed as a BlackBerry Dynamics integrated application. When first installed and run on a device, the Acronis Cyber Files for BlackBerry Dynamics app will prompt the user to activate the app in BlackBerry Dynamics. This activation is required before the user can proceed with enrolling the app with their Acronis Cyber Files server and accessing file.
- **Acronis Cyber Files server** - Acronis Cyber Files for BlackBerry Dynamics uses the same server-side software as standard Acronis Cyber Files. No server-side changes are required for Acronis Cyber Files servers to work with BlackBerry Dynamics enabled Acronis Cyber Files clients. This can be used to ensure that all the Acronis Cyber Files Mobile Clients that have access to Acronis Cyber Files files are managed by BlackBerry Dynamics.

Once a Acronis Cyber Files for BlackBerry Dynamics client is enrolled in BlackBerry Dynamics, all communication with the Gateway servers is routed though the BlackBerry Dynamics secure communication channel.

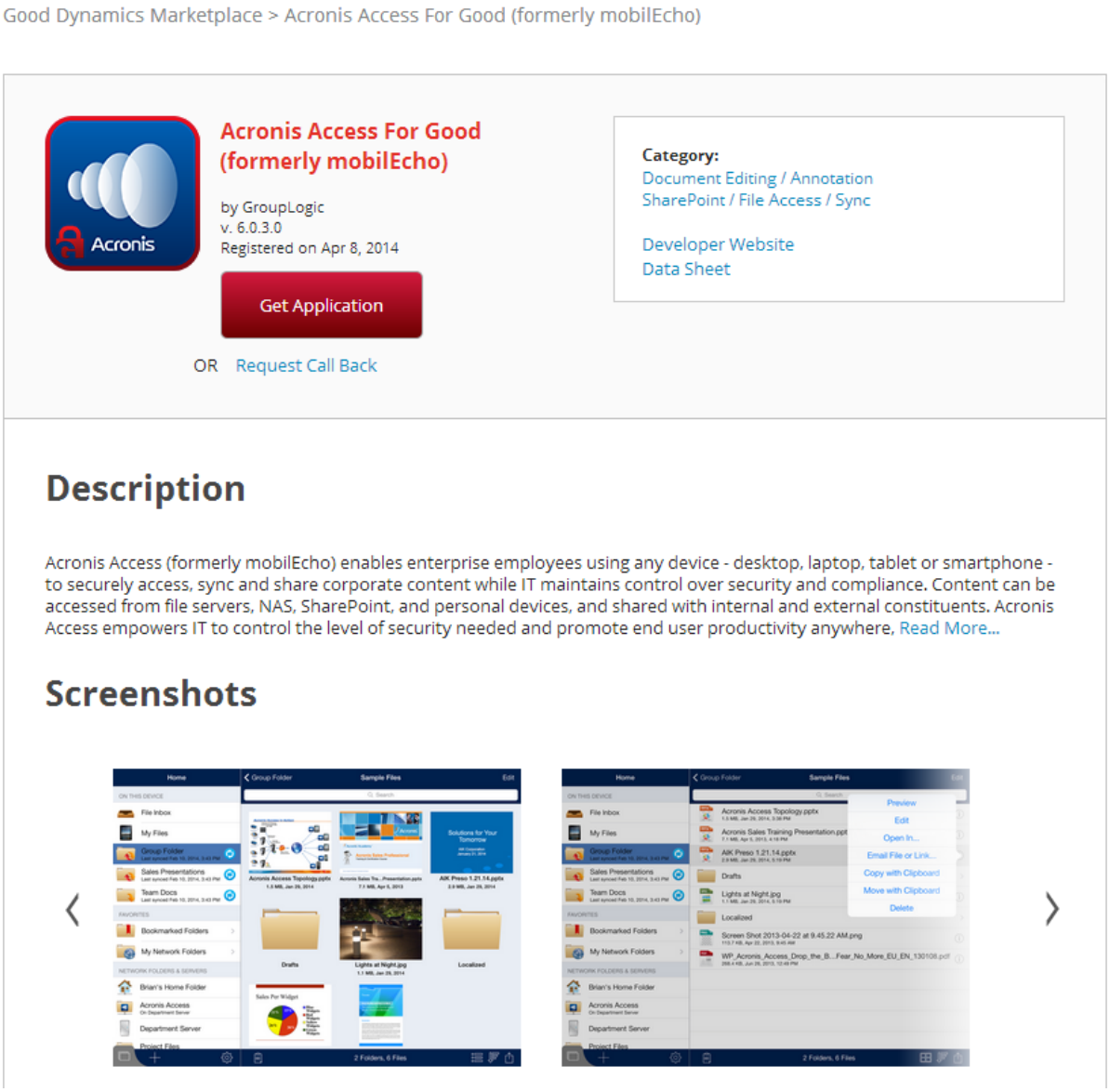
Requesting and configuring Acronis Cyber Files within BlackBerry Control

Before a Acronis Cyber Files for BlackBerry Dynamics client app can be enrolled in BlackBerry Dynamics, Acronis Cyber Files must be added to the list of **Managed Applications** on your BlackBerry Control server. For this to happen, you must request access to the **Acronis Cyber Files for Good** app using the BlackBerry Dynamics **Communities** site. If you are not currently a registered member of the site, another member of your organization may be responsible for managing vendor relationships on this site, or you may simply need to register for an account with BlackBerry .

Requesting access to Cyber Files for Good Dynamics

To request access to **Acronis Cyber Files for** BlackBerry , visit the BlackBerry marketplace (https://begood.good.com/marketplace.jspa) and locate **Acronis Cyber Files for** BlackBerry in the list of available BlackBerry **Dynamics** apps.

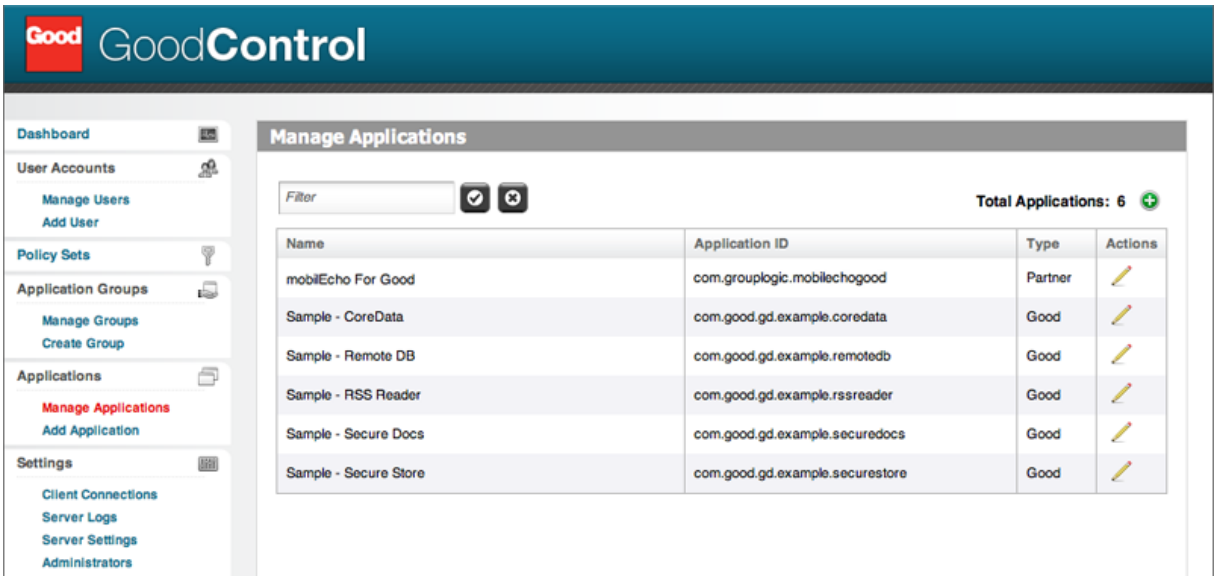
On the Acronis Cyber Files for BlackBerry app page, click the Start Trial button to request a trial or get the licensed version of the app.



If you select a trial version of the app, your access should be granted within a few minutes. You should receive a notification from the BlackBerry site when your request has been accepted and notify you that the **Acronis Cyber Files for** BlackBerry app as been published to your BlackBerry Control server.

Note
If you do not receive access, please contact BlackBerry Dynamics support.

Once this has happened, log into your BlackBerry Control server and click **Manage Apps** in the lefthand menu. Acronis Cyber Files should now be listed in your applications list. If it's not listed, give it 15 minutes or so and check again. This will allow the change time to propagate to your server.



Configuring Good Proxy access to your Cyber Files Gateway server(s)

In order for Acronis Cyber Files to be able to access your Acronis Cyber Files Gateway server through the BlackBerry Proxy server, you will need to configure access to the domain where your Acronis Cyber Files Gateway servers reside. This is done on the **Client Connections** page in the Good Control console.

Allowing access from your domain

This setting allows all BlackBerry clients to connect to all servers in the specified domain(s). If you don't want that, setup **Additional Servers** instead.

1. Open the **Client Connections** settings from the lefthand menu.
2. Expand **Allowed Domains**. Unless **Allow all domains** is enabled, press the plus (+) icon and enter the name of your domain (e.g. mycompany.com).
3. Press **Submit**.

Assigning your domain as a default domain for connections

1. Expand **Default Domains**.
2. Press the plus (+) icon and enter the name of your domain.
3. Press **Sumbit**.

Allowing specific servers to connect

Use this setting instead of the **Allowed Domains** if you wish that your Good clients connect only these specific servers instead of every server in the domain.

1. Open the **Client Connections** settings from the lefthand menu.
2. Expand **Additional Servers**.

3. Press the plus (+) icon and enter the DNS name and port of the server you want to grant access to. Repeat this step for all Acronis Cyber Files servers you want your BlackBerry clients to connect.

BlackBerry Dynamics Policy Sets and Acronis Cyber Files

The Acronis Cyber Files for BlackBerry Dynamics app respects the policy settings included in a user's assigned **Policy Set**. Policy sets are configured on the BlackBerry Control server.

Note
If you enable FIPS in the BlackBerry portal for a user's **Policy Set**, their Acronis Cyber Files app will not be able to access Gateway Servers using third-party certificates by IP address.

These settings include:

- Application lock password requirements
- Lock screen policies
- Data leakage protection
- Permitted OS versions and hardware models
- Connectivity verification
- Jailbreak/root detection

Data Leakage Protection effects and limitations

If **Data Leakage Protection** is enabled in a policy set, the Acronis Cyber Files app will not be permitted to:

- Open files into standard 3rd party applications on the device
- Receive files from other standard 3rd party applications on the device
- Email files using the default email client
- Print files
- Copy and paste text from within opened files

Note
If you require these features, you will need to enable the **Disable Data Leakage Protection** check box in the applicable BlackBerry Policy Set.

Note
Acronis Cyber Files for BlackBerry Dynamics includes a BlackBerry Dynamics feature called "Secure Docs". This allows files to be transferred between the Acronis Cyber Files for BlackBerry Dynamics app and the BlackBerry for Enterprise app. Once a file is opened into the BlackBerry for Enterprise app, it can then be opened into other 3rd party BlackBerry Dynamics enabled apps that include this feature. This functionality will be available, even with the BlackBerry Control **Data Leakage Protection** policy setting enabled.

Granting Acronis Cyber Files access to a BlackBerry Dynamics User or Group

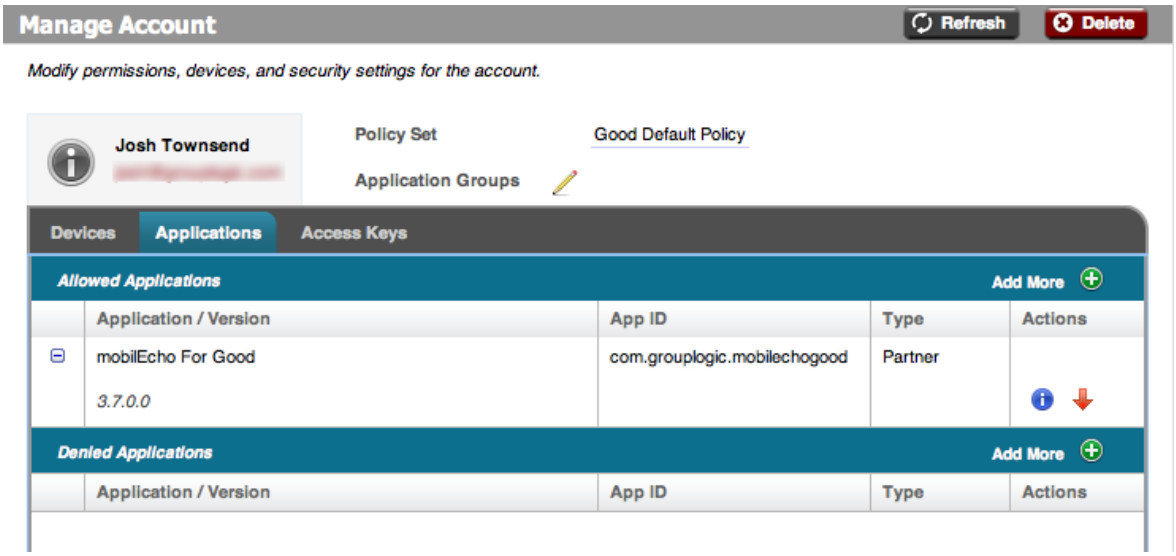
Before a user can enroll their Acronis Cyber Files app in BlackBerry Dynamics, they must have the Acronis Cyber Files application added to their user accounts **Allowed Applications** list or to an allowed **Application Group** they belong to. In addition, a unique **Access Key** must be sent to the user and entered into the Acronis Cyber Files app during the enrollment process.

Important
When you assign access to BlackBerry Dynamics applications to individual users, you are required to select specific version numbers of the app to allow. If you manage access on the user level, when new versions of Acronis Cyber Files for BlackBerry are released, you will need to return to the users' BlackBerryControl configuration and add the new version before they are allowed to run that version.

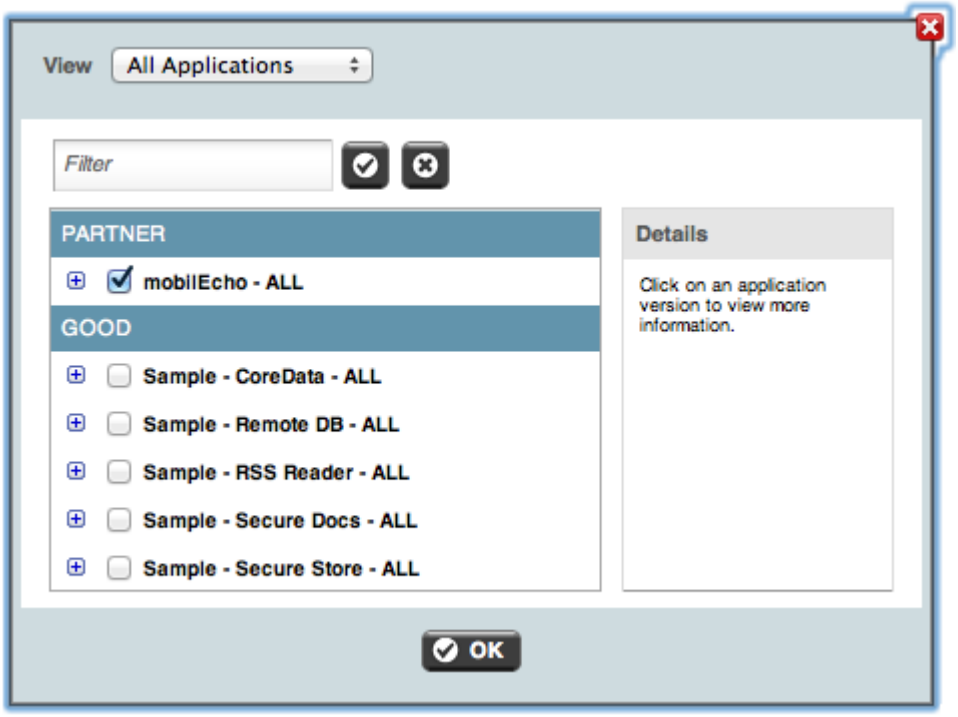
Note
We **highly recommend** that you allow access to BlackBerry Dynamics apps using the **Manage Groups** functionality in the BlackBerry Control console. BlackBerry Control allows you to give a group access to ALL versions of an app, so that future versions will be allowed without IT admin intervention.

To add the Acronis Cyber Files app to an Allowed Applications list in a User Account or Application Group:

1. Select **App Groups** or **Manage Users** from the lefthand menu in the BlackBerry Control console.
2. Select the group or user you'd like to give access to Acronis Cyber Files for BlackBerry and edit them.
3. In the **Apps** section, click the **Add More** button.

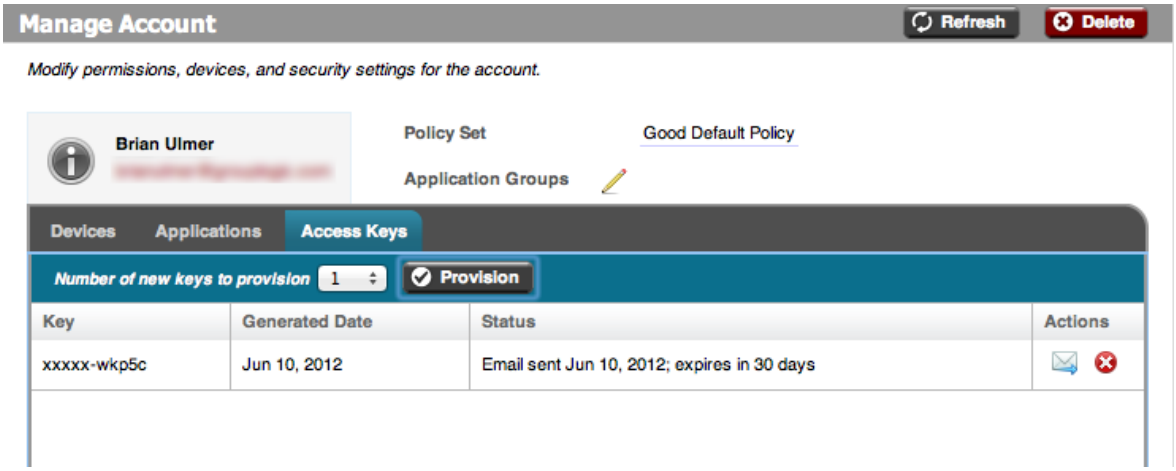


4. Select **Acronis Cyber Files for** BlackBerry from the list of available applications and click **OK**.



To generate an Access Key that will allow a user to enroll their Acronis Cyber Files for BlackBerry **app with** BlackBerry **Dynamics:**

1. Select **Manage Users** from the lefthand menu in the BlackBerry Control console.
2. Select the user you'd like to create an **Access Key** for and edit them.
3. On the **Access Keys** tab, press New **Access Key**.



The user will receive an email that includes the **Access Key** and some basic BlackBerry Dynamics instructions.

17.1.2 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**.

Creating an Active Directory Group

1. Open the Microsoft Azure portal.
2. Click on **All Services**, enter **azure** in the searchbox and select **Azure Active Directory**.
3. Open **Groups**, select **New group** and enter the required information.
4. Select the desired members of the group and press **Create**.

Adding the Acronis Cyber Files app to Intune

If you want to use an Intune **Device Policy**, Acronis Cyber Files should be installed through your Intune company portal.

To do so, you must first add the Acronis Cyber Files App to the portal:

1. Open the Microsoft Azure portal.
2. Click on **All Services,** enter **Intune** in the searchbox and select **Microsoft Intune**.
3. In the Intune portal, open **Mobile Apps** and open **Apps**.
4. Press **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.
5. Enable **Display this as a featured app in the Company Portal** and press **OK** to finish adding the app.
6. Click on the app in the list and select **Assignments**.
7. Select the users or groups you want to assign it to.

Creating a Device Policy

1. Open the Microsoft Azure portal.
2. Click on **All Services** and enter **Intune** in the searchbox and select Microsoft Intune.
3. Open **Device Configuration** -> **Profiles** and select **Create Profile**.
4. Enter the name, choose **iOS** as the **Platform** and select the restrictions you want to apply to the device.
5. For the Acronis Cyber Files app 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.
6. When the app is added to the list tap on it and select **Assignments**, select the users/groups you want to assign to.

In order to apply a Device Policy to any app, the app needs to be downloaded from your Intune Company Portal.

Creating an 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** and enter **Intune** in the searchbox and select **Microsoft Intune**.
3. Open **Mobile apps** and then open **App protection policies**.
4. Select **Add a policy** and enter a name for the policy, select **Acronis Cyber Files** as a required app.
5. Tap on **Settings** and choose the protection policies you want to apply.
6. When the app is added to the list tap on it and select **Assignments**, 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
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**.

Creating App Configuration policies

To enroll with Intune credentials automatically you need to create an **App Configuration Policy** or add the following changes to your own:

1. Open the Microsoft Azure portal.
2. Click on **All Services** and enter **Intune** in the searchbox and select **Microsoft Intune**.
3. Open **Mobile apps** and then open **App configuration policies**.
4. Press **Add** and enter a name for the policy.
5. Choose **Managed devices** as **Device enrollment type**, choose **iOS** as **Platform** and select the required app you want to deploy this configuration to.
6. 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**.
7. For auto-enrollment with Acronis Cyber Files credentials, you can use the following keys in **XML**:

   ```
   <dict>
   <key>enrollmentServerName</key>
   <string>192.168.1.10</string>
   ```

<key>enrollmentUserName</key>
<string>jprice</string>
<key>enrollmentPassword</key>
<string>password123</string>
<key>enrollmentAutoSubmit</key>
<string>Yes</string>
</dict>

8. When the app is added to the list, tap on it and select **Assignments** and select the users/ groups you want to assign to.

18 What's New

18.1 Acronis Cyber Files Server

For more information about the current and previous releases, refer to the Acronis Cyber Files Release notes.

18.2 Previous Releases

18.2.1 activEcho

Cyber Files Server 6.0

The mobilEcho and activEcho products have been combined into a single new product called Acronis Access Server. This changes the branding and product names in the mobile and desktop clients as well as the web application. Acronis Access Server 6.0 can be installed as an upgrade to mobilEcho and/or activEcho and existing licenses will continue to work. Customers are entitled to exchange their existing mobilEcho and/or activEcho license(s) for a new Acronis Access license that will enable the full functionality of the combined product. To request this upgrade, please **submit this web form**. For the latest information, please visit the What' New in Cyber Files Server article.

activEcho 5.1.0

BUG FIXES

- Improved performance displaying the log for non-administrative users
- Expired license notifications will no longer appear when activEcho is disabled via the Cyber Files server administrator
- New users that receive an invite email now receive a message to set their initial password instead of changing the password
- The Upload New Files dialog no longer shows an extra field when using Internet Explorer 8 or 9
- The Windows Desktop Client will no longer re-upload content in some situations when the user's password expires and is re-entered
- Miscellaneous fixes to the file sync logic in the Desktop Client

activEcho 5.0.3

BUG FIXES

- Email notifications are now sent properly after an upgrade when custom templates were used.

activEcho 5.0.2

ENHANCEMENTS

- Improved performance of the activEcho client when there are a large number of updates.

BUG FIXES

- Upgrades from activEcho 2.7 now work properly on non-English PostgreSQL installations.

activEcho 5.0.1

- No changes.

activEcho 5.0.0

ENHANCEMENTS

- Redesigned, easier to use Projects view for end users.
- activEcho Clients (Mac/Windows) have been localized in German, Japanese and French.
- Support for HTML5 drag and drop file uploading directly to the web interface. One or many files can be uploaded via Drag and Drop in a single operation.
- Improved file upload handling, including progress indicators in the web interface and the ability to cancel uploads.
- Folders can be downloaded as a ZIP file from the Projects view in the Web UI.
- Individual files can be shared with other users. Those users will get a link to download the files, which can be configured to expire.
- Sharing invitation dialogs now support type-ahead against both local users and users in Active Directory / LDAP.
- The previous revisions feature for finding / downloading / restoring previous versions of files has been redesigned and is more flexible. Previous revisions can be selected to be "made current".
- activEcho desktop clients (Mac/Windows) now show progress indicators files being synchronized.
- New "unsubscribe" button is available in folders shared to you.
- Sorting criteria chosen by the end user is now saved when browsing project folders.
- Event Notifications can now be configured globally as default settings for all shares. Users can override the defaults for individual shares.
- Notifications can now be configured to be sent when a file is downloaded / synced.
- activEcho clients on Windows now perform validation of SSL certificates using the built-in Windows certificate store. This improves compatibility with 3rd party certificate authorities.
- Improved user interface responsivness for re-assigning content when there are 1000s of users in the system.
- The Amazon S3 access key no longer displayed in plain text on the administration pages.
- Improved page load times when there are many users and/or files, especially when quotas are in use.
- Improved support for email invitations using different formats of email addresses.
- Wildcards can now be used in domains for sharing black and whitelists.
- Administrators can now globally hide the checkbox "Allow collaborators to invite other collaborators".
- New Administration mode toggles between a user's individual project / log views and the administration console.

- mobilEcho client management has been fully integrated into a common web administration interface. This can be used for managing mobile clients for activEcho, or if a mobilEcho license is provided the single console can manage all mobilEcho and activEcho functions.
- Users list can now be exported.

BUG FIXES

- Folders that cannot be shared no longer have the Invite... option.
- Users can now remove themselves from the share even if they do not have permission to invite other users to the share.
- If a file or folder cannot be downloaded to a Windows client because the name is too long, unchecking the Sync to devices option in the web interface now resolves the error on the client by removing the entire shared folder.
- activEcho clients properly handle error when uploading files and user is out of quota space.
- Users can now be deleted even if they are listed on the black list.
- Files can be uploaded to the repository when encryption is disabled.

activEcho 2.7.3 (Released: June 2013)

ENHANCEMENTS:

Switched to using the official AWS library file for Amazon S3 connections.

Files now can be successfully uploaded to any of the eight Amazon S3 bucket regions.

BUG FIXES:

Pending users can now be deleted without error.

Files which were not fully uploaded to the Amazon S3 file repository will now be removed from the repository if the repository is accessible after the upload failure occurs.

Files can be uploaded and downloaded when the file repository is not using encryption.

activEcho 2.7.2 (Released: May 2013)

BUG FIXES:

Files which were not fully uploaded to the file repository will now be removed from the

repository if the repository is accessible after the upload failure occurs.

Fixed a rare case where the activEcho client would fail to sync due to the structure of a system file ID.

activEcho 2.7.1 (Released: April 2013)

ENHANCEMENTS:

The activEcho web server and system can now be monitored using the New Relic monitoring tools. For more information about the new functionality and obtaining a license, refer to http://newrelic.com/

Upgrading will now maintain intermediate certificate files configured for the activEcho Tomcat installation's HTTPS connections.

Improved load speed of users page by caching content usage.

BUG FIXES:

Web users running on Internet Explorer 8 or Internet Explorer 9 in compatibility

mode will no longer receive an error that their browser is incompatible with activEcho.

Folders with names in the format YYYYMMDD will no longer fail to sync from the activEcho client to the server.

activEcho 2.7.0 (Released: February 2013)

ENHANCEMENTS:

Mac and Windows sync clients will now be notified when they have updated content available for download. These notifications will reduce load on the server and improve performance by avoiding many unnecessary requests from clients to the server to check for updates when none are available.

Mac and Windows sync clients have been made more resilient to errors on single files and folders. The client syncing process will no longer stop if a single locked file is updated. All other files which can be successfully updated will be. The client syncing process will also no longer stop is a file cannot be successfully downloaded. All other files which can be successfully downloaded will be.

Mac and Windows sync clients can now automatically download and install updates.

Download speed of large numbers of files to sync client has been improved.

Altering the preferences on the client will no longer cause a paused client to begin syncing.

Windows sync client now offers a "Show previous activEcho versions" context menu option.

The Projects tab in the web interface has been optimized for increased performance and smoother user interaction.

The Projects tab now supports pagination, sorting, filtering.

The move dialog in the web interface now loads quickly, even when the user has a large hierarchy of folders.

All client connections can be disabled for administrative purposes from the Server Settings page in the web UI.

All timestamps used for comparison or calculation will now be set to database time instead of server time to ensure proper operation in a cluster scenario.

The web interface now provides support for non-US date-time formats.

Duplicate folder updates will no longer cause multiple revisions of the folder to be created.

The default PostgreSQL installation is now configured with more carefully tuned parameters to improve performance.

User proxy AD objects can now successfully authenticate to activEcho.

Multiple domains can now be provided for LDAP configuration to be automatically pre-pended to usernames for login.

Links in emails when sharing a folder to a new user will now direct the user into the new share on the website. Note that if the default templates have been altered, the passkey paths in the notification email template will need to be modified to look like this:

<%= @root_web_address %>

<%= passkey_path(@passkey, { :redirect_path =>

show_contents_node_path(@node.uuid, {:show_sync_lightbox => true}) }) %>

Files will no longer be marked deleted if they can't be found in the repository. They will need to manually be removed.

Tomcat no longer needs to be restarted when S3 repository settings are changed.

All activEcho server logging is now written to a date-stamped activEcho.log file which is rotated daily. This log file can be found inside the Tomcat logs folder.

A configuration flag has been added to allow the activEcho web server to support HTTP connections instead of HTTPS. To allow HTTP connections, set REQUIRE_SSL to false in activEcho.cfg.

The Windows client MSI file is now available in the clients download directory.

ActivEcho's web application is now installed in the following location:

C:\Program Files (x86)\Group Logic\activEcho Server\activEcho Web Application

ActivEcho's Tomcat server is now installed in the following location:

C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34

ActivEcho's Tomcat is now configured to redirect HTTP to HTTPS by default.

Customers not needing redirection refer to the online documentation:

https://docs.grouplogic.com/display/ActivEcho/activEcho+Server#activEchoServer-RedirectingHTTPrequeststoHTTPS

The list of shares has now been removed from the left panel of the projects web page to improve the page performance.

Filtering options have been added to projects page sidebar.

Improved shutdown speed of the Mac and Windows sync clients.

Upgraded default Tomcat installation to version 7.0.34 and Tomcat Native (tcnative-1.dll) to version 1.1.24.

Upgraded default version of PostgreSQL to 9.2.1.

Validation of support for Windows 2012 Server.

Validation of support for Java 7 update 15.

Validation of support for Windows 8 for the Windows sync client.

Users on IE7 will now explicitly receive an error message that IE7 is not supported.

BUG FIXES:

Fixed a couple of rare instances where the sync client could receive a database

error and could no longer sync.

Under load, client will no longer occasionally corrupt files on download and upload the corrupted versions.

Duplicate files will no longer appear in the web interface if you pause and resume the client in the middle of uploading a file.

Fixed a Mac client bug where the client receives an error when a file is deleted off the server side while the client is downloading the file.

The sync client will no longer fail to complete in rare cases where folders are aggressively renamed with similar names.

The sync client will no longer attempt to delete files repeatedly if it cannot succeed.

Tomcat settings have been changed to ensure that syncing requests from the client will succeed even when there are many top-level folders.

File and folders with names containing %, _, and ! will now be handled properly.

Multiple bug fixes to sync client context menu options to support a variety of file and folder names which previously would fail.

LDAP authentication by email will now work properly for LDAP domains where authentication by common name is not permitted.

Fixed various case-sensitivity bugs with LDAP authentication.

Adding trial server licenses will no longer occasionally fail.

Unsharing a folder with Unicode characters in the name using "Remove all" will no longer cause an error.

A pending user can now be removed from a shared folder if you have the appropriate permissions, even if you are not an administrator.

Users can no longer share deleted folders.

Improved error handling for SMTP errors.

Miscellaneous other bug fixes.

activEcho 2.6.1 (Released: October 2012)

BUG FIXES:

Reassigning content from deleted users now works when quotas are disabled.

activEcho 2.6.0 (Released: October 2012)

ENHANCEMENTS:

Log and Users tabs support pagination, sorting, filtering.

Log and Users tabs have been optimized for increased performance and smoother user interaction.

Log tab provides new start and end date display filters.

Quotas can be defined for individual Active Directory and Ad-hoc users, overriding group policies.

Quotas can now be defined specifically for administrative users.

Automatic purging of user accounts if no activity has occurred, or a specific absolute time has passed.

Support for configuring the length of time before expiration of shared links.

New share permissions allow owner to hide display of share members to non-owners, and prevent non-owners from inviting others.

New behavior when unsharing projects, local data will be deleted from the client on next connection.

New administrative setting to hide the "Download the activEcho client" link to control which users can download and install the activEcho sync client.

Users accounts can be disabled to temporarily prevent access and login to activEcho.

New administrative setting to control the minimum supported version number of the sync client.

Support provided for creating Tomcat server clusters running activEcho for load balancing and resilience.

Improved diagnostic logging provided in the file repository service.

Desktop Sync clients on Mac and Windows now provide a menu option to display recently updated files.

Clicking an entry in the list opens the folder containing the file.

Mac OS X sync client now supports Gatekeeper signing and notification center on OS X 10.8.

Recommend upgrading to the latest version of the client due to significant performance and stability improvements in both Windows and Mac desktop clients.

The sync client on Mac and Windows now sets a custom icon for the activEcho sync folder.

The server installer allows setting the user account the file repository service runs under to store the repository on network volumes.

Projects tab can now be filtered by items shared by a user, or shared with a user.

Change the default email template when inviting a user to a share to allow the user to select to start syncing the content immediately. If you have customized the invite to share template in the past, update the following items:

<%= show_contents_node_path(@node.uuid) %>

to

<%= show_contents_node_path(@node.uuid, {:show_sync_lightbox => true}) %>

Validation of support for Java 7 update 7.

BUG FIXES:

Various improvements to LDAP authentication, including case sensitivity issues with domain names and support for multiple email domains.

The domain for LDAP authentication list can use either ; or , as a delimiter.

Various improvements on syncing files and folders where an item or the parent folder(s) have been deleted.

Fixed files modification dates that were not set properly based on timezones under some circumstances.

Period is a valid character in S3 bucket names when using Amazon S3 for the file repository.

Fixed high CPU usage on both Mac and Windows desktop clients.

Miscellaneous other bug fixes.

activEcho 2.5.1 (Released: July 2012)

ENHANCEMENTS:

Support for mobilEcho 4.0 for access to activEcho using mobile devices. mobilEcho 4.0 now allows sharing of activEcho, file shares, and SharePoint servers simultaneously.

Additional license is required for accessing file shares and SharePoint with mobilEcho.

Uploading and downloading of files via mobile devices is faster.

Mobile devices can now copy files and folders within an activEcho share.

Support for Mac OS X 10.8 "Mountain Lion"

BUG FIXES:

Improved upgrade experience when automatically restarting Tomcat when there is a large amount of user data to be migrated.

Server installer now correctly upgrades activEcho when files were originally installed in a custom location.

Mobile devices can now navigate shares that have trailing spaces in their name.

Authentication of LDAP users only worked against the first entry in the Provisioned LDAP table.

Improved support for syncing files from Mac OS X with / in their filenames.

Improvements to the sync clients reduce the potential for a full re-sync being required.

Fixed issue when saving with some applications (Microsoft Publisher, TextEdit, etc.) on Windows and Mac OS X could result in a file being treated as a new file and disassociated from its revision history.

Miscellaneous other bug fixes

activEcho 2.5.0 (Released: July 2012)

The activEcho 2.5 client is not compatible with the 2.1 server. Please upgrade your server to 2.5 first, and then upgrade the clients.

The activEcho 2.1 client is compatible with the 2.5 server but will not have all of the new features available.

ENHANCEMENTS:

Support for quotas. Different quotas values can be set for Active Directory vs. ad-hoc users, as well as based on Active Directory group membership. End users can manage their quota usage by using the web to selectively purge old revisions and deleted files. See the user manual for more information.

Support for read-only ("download only") shares. This setting can be enabled when inviting members to a share, and from the Members page for the share.

Support for selective syncing. Via the web, users can pick which folders they want to have synced to their desktop vs. only accessible via the web. This allows users to have access to shared content but not necessarily have all content synced to their local desktop.

Administrators can now reassign ownership of content when deleting a user from activEcho, or can choose to delete a user and later reassign the content using the Manage Deleted Users page.

When a user's permission to share is removed from a shared folder, the folder is now removed from their client activEcho sync folder.

activEcho clients support pausing / resuming syncing.

Syncing files to Mac OS X clients is significantly faster.

The file repository can now be configured to store content on a UNC path to support network drives.

New Notification setting allows the administrator to be notified when the file repository free space goes below a set threshold.

Default email templates can now be viewed in the management settings.

Web Projects page now provides a summary of the number of files and folders.

Web Users page provides the administrator a summary of individual user's content and quota usage.

Sync clients no longer time out if the initial sync contains more than 50,000 files.

Windows client installer is now available as a MSI package for use in automate deployment.

Deleting many files at once from the web browser is much faster.

Web now provides an "Invite" button for the folder the user is viewing.

Web log view now has a reset filters button.

Master encryption key has been migrated from the Tomcat directory into the activEcho database to prevent accidental data loss if Tomcat is uninstalled without proper backups.

BUG FIXES:

Email template notification errors could occur after a user is deleted from activEcho if they were sharing content.

LDAP settings are no longer validated if LDAP has been disabled in the management settings.

When a folder is unshared, the owner can now see past events in the web log for that folder.

The web log allows filtering of past events for users who are no longer part of the shared folder.

Improved the Windows desktop sync client upgrade experience to not occasionally request that Explorer be restarted.

Email addresses containing the following characters are now valid when inviting or adding a user: ! $ & * - = ^ ` | ~ # % ' + / ? _ { }.

Tomcat web.xml configuration file can no longer be retrieved via a web browser.

Miscellaneous bug fixing in desktop syncing.

activEcho 2.1.1 (Released: June 2012)

ENHANCEMENTS:

Email addresses for LDAP authenticated users now update when the primary email address changes in LDAP.

Improved LDAP performance.

BUG FIXES:

Improved authentication against LDAP to avoid timeouts against large catalogs.

activEcho 2.1.0 (Released: May 2012)

ENHANCEMENTS:

Automatic purging of previous revisions and deleted files based on administrative rules.

Customizeable email templates.

Export log to TXT, CSV, or XML files.

Improved, administrator configurable trace logging for diagnostics.

Significantly improved performance when sharing and syncing a large number of files.

Ability to unsubscribe from shared folders as a user, or for the owner to unshare to all users.

Notifications are now available for folder changes in addition to files.

More than one email address can be provided for notifications.

Support for 64-bit Java installations.

Improved LDAP performance.

Miscellaneous usability enhancements.

BUG FIXES:

Various bug fixes related to authentication with Active Directory via email addresses.

The built-in Administrator account will now never use Active Directory for authentication.

Miscellaneous bug fixes in desktop syncing.

activEcho 2.0.2 (Released: March 2012)

BUG FIXES:

Improvements to desktop syncing when Microsoft Office files are edited directly in the activEcho Folder.

Various bug fixes in desktop syncing.

Bug fixes in activEcho server installer to fix future upgrades.

activEcho 2.0.1 (Released: March 2012)

BUG FIXES:

Improvements to the server administration user experience.

Various bug fixes in desktop syncing.

Improvements to the client installer upgrade process.

activEcho 2.0.0 (Released: February 2012)

Initial release

18.2.2 mobilEcho

Cyber Files Server 6.0

The mobilEcho and activEcho products have been combined into a single new product called Acronis Access Server. This changes the branding and product names in the mobile and desktop clients as well as the web application. Acronis Access Server 6.0 can be installed as an upgrade to mobilEcho and/or activEcho and existing licenses will continue to work. Customers are entitled to exchange their existing mobilEcho and/or activEcho license(s) for a new Acronis Access license that will enable the full functionality of the combined product. To request this upgrade, please **submit this web form**. For the latest information, please visit the What' New in Cyber Files Server article.

mobilEcho 5.1.0

ENHANCEMENTS

- Users with mobilEcho 5.1 or later on iOS can now create their data sources directly from the application to access any file share or SharePoint location. Users enter UNC paths or SharePoint URLs from the client. New policy settings have been introduced on the management server to control whether clients are allowed to create these data sources, and which Gateway Servers are used for these requests.
- Multiple Gateway Servers can now share a common configuration via a Cluster Group. Changes to the settings and policies assigned to the Cluster Group are automatically pushed to all members of the Group. This will typically be used when multiple Gateway Servers are placed behind a load balancer for high availability.
- Gateway Servers now support authentication using Kerberos. This can be used to in scenarios using Kerberos Constrained Delegation to authenticate mobilEcho iOS clients through a reverse proxy using client certificates. It also can be used to authenticate mobile devices with client certificates using MobileIron AppTunnel. Note that when using this form of authentication, mobile clients cannot access activEcho shares.
- The required data sources are now automatically created when assigning home folders to a user or group policy. Previously administrators needed to manually create a data source for the server hosting the home directory.
- The address of a legacy Gateway Server can now be modified
- The policy exceptions for Android have been updated to reflect the functionality of the mobilEcho Android 3.1 client

BUG FIXES

- Removing a user or group policy with a custom home folder now properly removes the volume on the Gateway Server.
- Displaying Assigned Sources for a user now displays sources assigned to that user through their group memberships.
- Improved the ordering of the tabs in the Data Sources administration page.
- Changing a Gateway Server administration address no longer dismisses the edit dialog when clicking Apply.
- mobilEcho clients enrolling for management using client certificates will no longer fail periodically if the user was not already in the server's LDAP cache.
- Adding white space to Gateway Server addresses no longer prevents the Gateway Server from being properly managed.
- Notes in the Device Information dialog are now saved properly.
- When policies are disabled, they now appear grayed out in the policy list.
- On upgrade from mobilEcho Server 4.5 the mobilEcho users are now imported properly even if the wrong LDAP search base is entered in the configuration wizard.
- License keys starting with YD1 are now displayed properly as trials with an expiration date on the licensing page, instead of perpetual licenses.

- Enrollment email invitations now have proper links for Android clients.
- Editing SharePoint credentials for a Gateway Server is now disabled if the Gateway Server does not have a license supporting SharePoint connectivity.

mobilEcho 5.0.3

BUG FIXES

- When configuring data sources the %USERNAME% token can now be used as part of a folder name, instead of the whole name.
- Newly created data sources are now checked to see if they are searchable immediately. Previously they were only checked in 15 minute intervals.
- Search is now available on data sources that add search indexing after the Gateway Server has started.

mobilEcho 5.0.2

ENHANCEMENTS

- The Folder list in Data Sources now shows the assigned Gateway Server using its Display Name instead of its IP Address.

BUG FIXES

- Clients can now access data sources with a colon in their name.
- Upgrades from mobilEcho 4.5 now properly handle migrating SharePoint data sources.
- After an upgrade, the Assigned Sources tab in Data Sources now properly displays resources assigned to a user.
- Sorting the Active Users table by Policy or Idle Time no longer generates an error.
- Clients can now access Gateway Servers that are provisioned to be visible on clients and that have different addresses for client connections.
- Fixed a bug where home folders could fail to open in the mobilEcho client if the Access Server contained data sources with similar paths (for example "\\homes" and "\\homes2")

mobilEcho 5.0.1

BUG FIXES

- Fixed an issue where the database migration from mobilEcho 4.5 to 5.0 would fail if there were device password resets still pending which had been created in an earlier version of mobilEcho. This caused an error to be displayed in the web browser when starting up the server similar to the following:

  ActiveRecord::JDBCError: ERROR: value too long for type character varying(255): INSERT INTO "password_resets" ....
  Customers that have this condition can upgrade to this new version of the server and the problem will be resolved automatically.

- Fixed an issue that could cause some clients to go into restricted mode after the upgrade to mobilEcho 5.0.
- The management server data sources table now shows the Gateway Server's display name instead of IP address.

mobilEcho 5.0

ENHANCEMENTS

- The mobilEcho Client Management Server is integrated with Cyber Files Server and built on Apache Tomcat and PostgreSQL database for improved scalability and resilience.
- The mobilEcho Administrator previously used to manage individual mobilEcho servers has been removed; Access Gateway Servers (formerly mobilEcho File Access Servers) are now managed directly within the Cyber Files Server web administration user interface.
- mobilEcho Client Management Server configuration file has been removed; configuration settings previously in the configuration file are automatically migrated and are now managed through the Cyber Files Server web administration user interface.
- Configuration of data sources (formerly assigned "Folders") to be shared to mobile devices has been redesigned.
- New "Assigned Sources" capability allows administrators to get a report of all of the assigned resources that a particular Active Directory user or group will receive.
- Audit logging can be enabled to report on mobile user activity across multiple Cyber Files Gateway Servers.
- Administrators can now be granted different permissions for administrative activity, including managing users, data sources, mobile policies or viewing the audit log. This can be based on individual users and/or membership in Active Directory groups.
- Devices operations such as remote wipe or removing devices from the device list can now be performed in batches.
- A catch-all "default" policy can be configured which applies to all users that don't match configured Active Directory user or group policies.
- New policy options allow specification that content on the device within the "My Files" and "File Inbox" folders expires and is removed after a certain amount of time.
- When sending an enrollment invitation to an Active Directory group, users who are already enrolled through another group can be filtered out.
- A warning is presented if a user is invited for enrollment but does not match any existing user/group policy.
- The devices table now lists the user or group policy in use for each device.
- Cached Active Directory / LDAP information about users is now updated periodically in the background.
- Content searching is now available against remote Windows file shares running Windows Search.
- A policy cannot be be deleted if a device is being managed by it
- mobilEcho enrollment invitation templates can be modified directly from within the web administration console. Multiple languages for each template are supported.

- A new token is available in the enrollment invitation templates to include the Active Directory user's Display Name.
- Devices list and device details screen now show whether devices are managed by Good Dynamics or MobileIron AppConnect.
- Support for authenticating to the web administration console using SSLv2 has been deprecated by the transition to the Apache Tomcat web server.
- Support for trace logging and performance monitoring via New Relic.

BUG FIXES

- Home directory configuration is now retrieved properly when LDAP is configured to use the global catalog.
- Improved handling of Active Directory lookups when trailing spaces are used.
- The "Enrolled at" date is now formatted properly when exporting to .CSV file.
- Improved support for displaying Unicode via the web administration user interface.
- SharePoint folders ending with a space can now be enumerated by clients.
- SharePoint libraries that have extra slashes now support file deletion and copy properly.

mobilEcho 4.5.2 (Released: October 2013)

ENHANCEMENTS:

Added support for smart card authentication, and added a setting to allow or disallow clients using this new authentication method.

mobilEcho 4.5.1 (Released: September 2013)

ENHANCEMENTS:

The mobilEcho server now supports requiring that mobilEcho Android clients are managed by MobileIron AppConnect.

BUG FIXES:

Fixed an issue where clients could time out trying to connect to a server if mobilEcho was configured to enumerate site collections.

Fixed an issue where the mobilEcho server selected when configuring a custom home directory path could fail to save properly when saving a user or group profile.

mobilEcho 4.5 (Released: August 2013)

ENHANCEMENTS:

Added support for giving access to SharePoint Online for Office 365.

Added the ability to enumerate and browse into individual SharePoint site collections.

Added support for client certificate authentication to mobilEcho file servers.

Added profile options to enable or disable the client's ability to edit text and/or Office files, to configure an auto-sync interval, and to automatically sync a user's home folder.

Increased the maximum volume name length to 127 UTF-8 characters to allow for longer volume names when using Unicode characters.

Added separate columns to the exported .csv devices list for display name and common name to make the usernames more clear.

BUG FIXES:

Fixed an issue where the exported .csv devices list would display the domain name incorrectly if the domain name contained numerical characters.

Fixed an issue where the server would respond incorrectly to a client request to delete a folder that was the root of an SMB share.

Fixed an issue where network path mapping could fail if two path mappings were created for two similar paths (e.g. \\server\vol and \\server\vol2).

mobilEcho 4.3.2 (Released: April 2013)

BUG FIXES:

Fixed an issue where mobilEcho Administrator could fail to create an activEcho volume when the product is licensed with a Retail serial number.

Fixed an issue where a mobilEcho client could fail to open its home directory if the home directory is configured using the %USERNAME% wildcard and the server domain and the user's domain have a trust relationship.

Fixed an issue where the server could incorrectly send an error message to Android clients when those clients attempted to obtain their profile.

mobilEcho 4.3.1 (Released: April 2013)

ENHANCEMENTS:

The mobilEcho server now supports mobilEcho clients that identify themselves using a custom device identifier, rather than Apple's device identifier.

BUG FIXES:

Fixed an issue where the Users and Groups pages of the mobilEcho Client Management web console could load very slowly if there were a large number of configured profiles.

Fixed an issue where the enrollment link in client enrollment invitation emails could fail to open properly on Android clients.

Fixed an issue where iOS clients could fail to connect to the server after upgrading from 4.0.1 server or earlier to 4.3 server.

mobilEcho 4.3 (Released: March 2013)

ENHANCEMENTS:

The mobilEcho server now supports mobilEcho clients with optional support for MobileIron AppConnect activated. The server now allows administrators to require or restrict mobilEcho access to iOS clients with AppConnect enabled. This setting is located in the "Settings" window of the "mobilEcho Administrator" application, on the "Security" tab.

BUG FIXES:

Fixed an issue where clients upgrading from mobilEcho Server 4.0.x or earlier could incorrectly receive a "specified account does not have a management profile" error when attempting to retrieve their management profile.

Fixed an issue where the mobilEcho server's memory usage could increase if the "mobilEcho Administrator" was left open for a long period of time.

Fixed an issue where the client would fail to show an error or would show an incorrect error message if the user's AD account password had expired, or the account was locked out or disabled.

Fixed an issue where the server upgrade process could fail if mobilEcho had been installed to a non-system drive.

Fixed an issue where a JavaScript error would occur each time a user or group profile was added via the mobilEcho Client Management web console when using IE8.

mobilEcho 4.2 (Released: February 2013)

ENHANCEMENTS:

mobilEcho 4.2 servers now support mobilEcho 4.2 clients localized in German, French and Japanese. The 4.2 server will ensure that these clients receive server error messages in their local language. In addition, the mobilecho_manager_intl.cfg file contains settings to configure the client enrollment invitation email subjects in these three languages.

The mobilEcho Client Management service will now automatically detect crashes in the client management web application and stop the service so that administrators can properly detect these errors. Additional error information will be written to the ManagementUI\log folder.

BUG FIXES:

Fixed a problem where the user could repeatedly be asked to enter proxy credentials when accessing the mobilEcho server through an HTTPS reverse proxy server.

Fixed a problem where the mobilEcho Client Management Server web UI could fail to restart because the client management database schema was not updated properly on upgrade. This would occur if the database was configured to be stored on a disk that was not available at upgrade time.

Sorting devices by "Last Contact" now sorts newest to oldest by default.

Fixed a problem where whitelists and blacklists could not be assigned when adding or editing a user or group profile.

Fixed a problem where files that were already on the device could sync again unnecessarily if the sync source was within an activEcho volume.

The password field on the login page of the client management web UI now has auto-complete disabled.

Removing a user or group profile now causes the name information for that user/group to be removed from cache. This ensures that re-adding a profile for that user/group will always force the management UI to retrieve the latest name from Active Directory.

Fixed a problem where "set the default file action" and "cache recently accessed files on this device" could be enabled in profiles after upgrading mobilEcho server.

Fixed a problem where the app password reset functionality in the management server UI might not work properly in Firefox.

Fixed a problem on the Invitations page of the client management server web UI where users within distribution subgroups could fail to be found in LDAP searches.

Fixed a problem where the server check for free disk space in a folder would incorrectly check the free space at the root of the mobilEcho volume.

Fixed a problem where open file handles would not be closed for 24 hours if a client disconnected in the middle of a file transfer. These handles will now be closed when the session times out, after 15 minutes.

Fixed a problem where the "Allow iTunes and iCloud to back up locally stored mobilEcho files" profile setting would always revert to enabled after saving management profile.

mobilEcho 4.1 (Released: December 2012)

ENHANCEMENTS:

Added an alternative client management server authentication mechanism so that mobilEcho clients that are configured to not save credentials for assigned servers and folders can authenticate to the management server to retrieve their profile without requiring their Active Directory password be stored on the device.

Modified the app password reset process. This was necessary to support the new custom on-device encryption that is included in the mobilEcho 4.1 client app. If a managed client forgets their app password, they now provide their administrator with a code generated by the app. The administrator enters this code into the mobilEcho Client Management web console and receives a second code that they give back to the client. This code allows the user to reset their app password and get into the app.

Enhanced the way resources (servers and folders) are provisioned to clients. Provisioned resources are no longer assigned directly to user/group profiles. Users or groups are now assigned directly to individual assigned resources and each user receives the full collection of resources assigned to their user account or a group they are a member of.

Added the ability to send up to three enrollment invitations to the same email address automatically for users with multiple devices.

Added a column to the LDAP search table for Distinguished Name so that users with the same name in different subdomains can be distinguished.

Added new management profile setting to allow or disallow users from opening and/or sending links to files.

Added client Good Dynamics status in the management server Devices list. Devices enrolled with Good Dynamics will no longer have the "Reset App Password" option available. The app password is managed within the Good Control console in this scenario.

BUG FIXES:

Fixed a problem where hiding inaccessible files on reshares when one of the volumes was a SharePoint volume could cause some of the volumes to fail to appear on the client.

Fixed a problem where the Client Management Administrator could fail to filter the devices or invitations tables, or could take a very long time to complete the filter. Filtering is now done without the need to perform additional LDAP requests.

Fixed a problem where attempting to read a file on an activEcho volume that no longer exists would result in a corrupted file being read rather than an error being returned.

Fixed a problem where the presence of a misconfigured or unavailable activEcho volume could cause clients to time out when attempting to retrieve the volume list.

Fixed a misleading message in the Client Management Administrator if a profile was configured to have 'App password must contain complex characters' greater than the 'Minimum password length'.

Fixed a problem when the client management server was configured to use a non-default port (i.e. not port 3000) and the server was upgraded. The first time the management server would run after upgrade it would attempt to use port 3000 rather than the configured port.

Modified the message in the Client Management Administrator when removing a currently managed client from the devices list to indicate that the client may automatically reenroll at a later time if enrollment PINs are not being used.

Fixed a problem where the Client Management Administrator could display an error if a profile was configured to use a home folder with an empty custom path.

Fixed a problem where 0-byte files would fail to download or sync with a "device not ready" error.

Content search is now automatically disabled on activEcho and SharePoint volumes since content search is not available.

Fixed a problem where users with email address beginning with underscore (e.g. "_ user@example.com") could fail to receive enrollment invitations.

Client Management Administrator now returns a better error message than "unknown result" if the LDAP server requires SSL.

Fixed a problem where sessions could time out while downloading very large files.

Fixed a problem where configuring an assigned folder with an invalid path (e.g. "C:\foo\bar") could cause the Users page to show the error "can't modify frozen string".

Fixed a problem where selecting the "Reindex all volumes" button in the mobilEcho Administrator would generate an invalid error message.

Fixed a problem where filtering on a Unicode string in the Client Management Administrator could generate an "incompatible character encodings" error.

SharePoint "Wiki Page Gallery" libraries are now removed from site enumerations because they are not supported by mobilEcho.

Fixed a problem where new profile settings could become corrupted on upgrade.

Fixed a problem where a SharePoint document library volume would fail to work if the document library name was URL encoded, e.g. "My%20Library".

mobilEcho 4.0.3 (Release: October 2012)

ENHANCEMENTS:

Added support for SharePoint custom document libraries.

BUG FIXES:

Fixed a problem accessing SharePoint sites and document libraries whose paths are multiple levels below their parent site.

Fixed a problem accessing SharePoint sites that use Claims Based Authentication.

mobilEcho 4.0.2 (Released: September 2012)

ENHANCEMENTS:

Added support for Android clients.

Added settings to the mobilEcho Administrator for restricting access by iOS and/or Android clients.

Added support for sending enrollment instructions for iOS, Android and Good clients.

BUG FIXES:

Fixed a problem where exporting the devices list to a .csv file could result in a server error, or could result in some fields displaying as "Not found in AD".

Fixed a problem where non-Good clients could enroll with a management server that was configured to require clients be enrolled with Good Dynamics. Previously, clients could enroll, but would receive an error when contacting the server to access data. Clients are now disallowed from enrolling in the first place.

mobilEcho 4.0.1 (Released: August 2012)

ENHANCEMENTS:

Added profile settings for "Number of days to warn of pending lock" and "Number of days to warn of pending wipe". These settings relate to existing settings that can wipe or lock the mobilEcho app if the device does not contact the management server for a specified period of time.

Added pagination, filtering and sorting to the Users and Groups pages within the mobilEcho Client Management server.

BUG FIXES:

Fixed a crash that could occur when attempting to authenticate with SharePoint volumes using Kerberos authentication.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their user principal name (UPN) had a different domain than their Windows 2000 domain.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their username contained Unicode characters and authentication was performed using NTLM.

Fixed a problem where users could fail to authenticate with SharePoint volumes if the user was a member of a subdomain and authentication was performed using NTLM.

SharePoint document libraries will now display all items, regardless of the settings of the library's default view.

The "Last Contact Time" column on the Devices page of the mobilEcho Client Management server now properly sorts by date.

Filters in the mobilEcho Client Management server now work properly with Unicode characters.

Filters in the mobilEcho Client Management server now "stick" after pagination settings are changed.

Disabled the "Indexed Search" and "Content Search" checkboxes when adding or editing reshare volumes in the mobilEcho Administrator, since search is not supported on those volumes.

The mobilEcho Administrator now automatically fills in the existing path when editing a SharePoint, activEcho or reshare volume path.

The mobilEcho server now returns a better error code if the user attempts to overwrite a file via Save Back that is checked out to another user.

mobilEcho 4.0 (Released: July 2012)

ENHANCEMENTS:

Added support for accessing data in SharePoint 2007 and 2010 document libraries.

The mobilEcho server can now simultaneously support activEcho and other volume types. Previous versions required switching into activEcho-only mode to access activEcho data.

Improved performance of the mobilEcho Client Management server by making LDAP queries "begins with" rather than "contains" by default. Administrators may choose "contains" when searching to obtain the previous behavior.

The mobilEcho Client Management server can now filter the invitations tables by username.

The mobilEcho Client Management server can now export the devices list to a .csv file.

The mobilEcho Client Management server now sorts and paginates the devices, users, groups and invitations tables.

Added a profile setting to allow/disallow users from creating bookmarks.

Added a profile setting to disable My Files while still allowing sync folders.

Added a profile setting to automatically lock the mobilEcho app or wipe all mobilEcho data if the device does not contact the management server for a specified period of time.

Added a profile setting to prevent users from setting an app password.

Files can now be copied within activEcho volumes by transferring data through the client.

Improved performance reading and writing to activEcho volumes.

BUG FIXES:

Fixed a problem where files and folders ending in a period or space could fail to be accessible on activEcho volumes.

Fixed a problem where the Devices page could fail to load in mobilEcho Client Management server after Japanese and Chinese users have enrolled.

mobilEcho 3.7 (Released: June 2012)

ENHANCEMENTS:

Improved performance of the mobilEcho Client Management server by caching user information to minimize the number of LDAP queries.

BUG FIXES:

Active Directory distribution groups are no longer found when searching for groups on the group profile page.

Fixed a problem when the path of a provisioned folder ends with a backslash.

mobilEcho 3.6.1 (Released: May 2012)

BUG FIXES:

Fixed a problem where files on an activEcho server could fail to preview, copy or sync.

Fixed a problem where users could fail to preview, copy or sync files in a home directory if the home directory was set up with a network reshare path mapping in the mobilEcho Client Management server.

Fixed a problem where users could fail to see their home directories if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

Fixed a problem where the "%USERNAME%" wildcard would fail to use the correct username if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

mobilEcho 3.6 (Released: April 2012)

ENHANCEMENTS:

Improved performance of Active Directory lookups for users and groups.

Searches of Active Directory in the mobilEcho Client Management server now search on both common names and display names.

Add profile settings for allowing/denying the ability of users to create sync folders, and to perform a Quickoffice® "Save Back".

The mobilEcho Client Management server can now be configured to store database and profile information in a different location than the application directory, allowing for the management server service to be failed over to other cluster nodes.

The mobilEcho Administrator now displays the number of licenses currently being occupied, and will only display a single session for each user/device if the user has reconnected to the mobilEcho server multiple times.

The mobilEcho Administrator now automatically runs with elevated privileges.

The enrollment email subject can now be customized in the 'mobilEcho_management.cfg' file.

BUG FIXES:

mobilEcho no longer permits Active Directory "Distribution" groups to be used to create mobilEcho Client Management group policies. Distribution groups are provided by Microsoft for email purposes only. If you are using AD "Distribution" groups for any of your mobilEcho Client Management policies, please use the "Active Directory Users and Computers" control panel to convert these groups to "Security" groups.

Fixed a problem where a user that used different username formats to enroll with multiple devices would occupy multiple licenses. For example, if one device was enrolled as "user@example.com" and a second device was enrolled as "example\user", the licensing logic would treat those as two separate user accounts for licensing purposes.

Fixed a problem where a user could fail to get the appropriate group profile if the user's Active Directory primary group was not set to the default of "Domain Users".

Fixed a problem where a user could fail to get the appropriate group profile if the user's group was a "universal" Active Directory group.

Fixed a problem where users with Unicode characters in their usernames would not have their credentials saved after enrolling with mobilEcho Client Management.

Fixed a problem where the server could allow mobilEcho clients to overwrite files that were flagged as read-only.

Fixed some mobilEcho Client Management display issues on Mac Safari.

Fixed a problem where Verizon iPad 3 devices were displayed as "AT&T" (and vice versa) in the mobilEcho Client Management devices page.

Fixed a problem where the mobilEcho Administrator could crash when viewing the list of connected users.

Fixed a problem where the invitation email would fail to show the username.

mobilEcho 3.5 (Released: February 2012)

ENHANCEMENTS:

Added support for 2-way sync folders. Client-side changes made in 2-way sync enabled folders will be synced back to the server automatically. These 2-way sync folders can be provisioned through the mobilEcho Client Management server.

Added support for reverse proxy authentication. Reverse proxy servers, such as Microsoft Forefront Threat Management Gateway (TMG), can be configured to require authentication before granting access to internal network resources. The mobilEcho client now supports both HTTP username/password and SSL Client Certificate authentication methods. To use SSL Client Certificate authentication, a certificate must be installed in the mobilEcho keychain. See this Knowledge Base article for more information: http://support.grouplogic.com/?p=3830

Added additional options for configuring mobilEcho device enrollment requirements. mobilEcho can now be optionally configured to accept enrollment requests from devices without the need for a one-time PIN. In addition, when mobilEcho is configured to require such PINs, these PINs can be viewed within the management interface.

Added support for client app whitelisting and blacklisting. A managed mobilEcho client can be configured so that files can only be opened into a restricted whitelist or blacklist of third-party iOS apps.

Improved browsing performance of network reshare volumes by disabling the filtering of inaccessible file and folders by default on such volumes.

Added support for network reshare to SMB/CIFS volumes on NetApp storage.

Added the ability to configure mobilEcho provisioned folder paths that include a username wildcard.

Added the ability to configure mobilEcho home folders with custom paths. These paths may include a username wildcard.

mobilEcho no longer requires that users have "list folder" permissions at the root of a share containing their home folder.

Added a new registry setting to control whether or not hidden shares on a network reshare are visible to mobilEcho clients. To enable this feature, set the following registry setting to 1:

HKEY_LOCAL_

MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\GetShowHiddenSMBShares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would appear to allow access without a proper username and password.

Fixed a problem where files would incorrectly require a sync after a change in daylight savings time.

Fixed a problem where renamed files would continue to be returned in search results when searching under the old filename. This problem would only occur for volume that were configured to use "indexed search" (not Windows Search).

Fixed a problem where mobilEcho could fail to install or run on systems missing a system DLL (normaliz.dll).

Fixed a problem where the client could fail to copy a file to the server if the user account did not have permission to calculate the amount of free space on the volume. The client would report an error about there not being enough free space on the volume.

Removed extraneous logging from the mobilEcho LOG.TXT file.

Fixed a problem where folders could not be provisioned for servers whose display name contained parentheses.

mobilEcho 3.1 (Released: November 2011)

ENHANCEMENTS:

Client management profiles can now be configured with the following new settings:

- The number of incorrect app password attempts that can be made before the local data

within the mobilEcho app is automatically wiped. This feature is disabled by default.

- Whether the user is required to confirm before syncing occurs (options are:

"Always", "Never", and "Only on 3G").

- Whether syncing is allowed any time, or only while on WiFi networks.

- Client timeout for unresponsive servers now accepts additional values of 90, 120 and 180 seconds.

The mobilEcho Client Management server can now be configured to communicate with Active Directory via secure LDAP.

Profiles now default to allow files to be cached on the local device. If caching is disabled or if the "Allow files to be stored on this device" setting is disabled, no files will be cached.

The text of enrollment invitation emails can be customized. Please visit the GroupLogic Knowledge Base for more information: http://support.grouplogic.com/?p=3749

Added a setting to the management configuration file to control the name that enrollment invitation emails appear from (e.g. "mobilEcho Invitation <mobilEcho_invitation@example.com>". Version 3.0 only allowed an address to be specified (e.g. "mobilEcho_invitation@example.com").

The VALID_LOGIN_NAMES field of the management configuration file now supports Active Directory groups in addition to specific users that can administer the mobilEcho Client Management service.

Changing SMTP settings within the management configuration file no longer requires a restart of the mobilEcho Client Management service.

Profiles for users and groups that no longer exist in Active Directory are now marked as such in the mobilEcho Client Management service.

Added the ability to show inaccessible items only on reshare volumes. This can be useful in cases where determining file and folder accessibility is causing performance problems. This behavior can be adjusted by modifying the following registry setting and restarting the service:

HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\HideInaccessibleItemsOnReshares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path if the associated 'Network reshare path mapping' included a trailing backslash.

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path that only included a server and share name. (i.e. \\servername\sharename)

Fixed a problem that could prevent network reshare volumes configured with paths to the root of a server (i.e. \\servername) from appearing properly in the mobilEcho client.

mobilEcho clients now always log into provisioned servers using fully qualified domain accounts. In previous versions of mobilEcho, the credentials entered at enrollment time would be used to authenticate with file servers, even if these credentials did not include a domain name (e.g. domain\user). This could cause problems if the provisioned server was on a different domain than the management server and access to the server in the secondary domain relied on a domain trust with the primary domain. This behavior can be reverted to the previous default by setting the following registry value to 0 and restarting the service:

HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\DomainAndUsernameShouldBeSentToClient

Fixed a problem where the mobilEcho Client Management server did not properly sort "Last contact date" properly on the Devices page.

Fixed a problem in the mobilEcho Administrator where the Help button would not adjust properly as the Users window was resized.

mobilEcho 3.0 (Released: October 2011)

ENHANCEMENTS:

Centrally managed device enrollment. Client enrollment invitations are now generated and emailed to the user from the mobilEcho Client Management Administrator. These invitations include a one-time use PIN number required for client enrollment.

Remote wipe and remote reset of app passwords is now performed on a per-device basis.

Individual device status is now displayed in the mobilEcho Client Management Administrator. This includes device user name, device name, device type, iOS version, mobilEcho version, mobilEcho status, last contact time.

Users' Active Directory assigned network home folders can now be automatically displayed in the mobilEcho client app.

Specific mobilEcho shared volumes or folders within shared volumes can now be assigned to user or group profiles. These shared volumes or folders are then automatically displayed in the mobilEcho client app.

Shared volumes or folders assigned to user or group profiles can be configured to automatically one-way sync from server to mobilEcho client, making the contained files available for online or offline use.

BUG FIXES:

Fixed a problem where the mobilEcho server would not properly report free space for server-to-server copies.

Improved error messages and processing if a user attempts to copy or move files into the root of a network reshare.

Fixed a problem where a user could be authenticated with AD by contacting mobilEcho via a web browser. This could cause a user account to become locked.

Improved the speed of installation, particularly for upgrades.

Fixed a problem where files and folders ending a period or space could fail to copy properly.

Fixed a problem logging into the management UI with a username containing numbers, e.g. "e12345".

Updated OpenSSL library to latest version. OpenSSL libraries are used for encryption.

mobilEcho 2.1.1 (Released: July 2011)

BUG FIXES:

Fixed a bug when listing the contents of folders which may have resulted in slow performance or client timeouts if many of the folders were not accessible to the client.

mobilEcho 2.1.0 (Released: July 2011)

ENHANCEMENTS:

Added the ability to create mobilEcho shares that reshare data on a remote system. The mobilEcho reshare feature is only available for customers with an enterprise license. Reshares can be a particular share (e.g. "\\server\share") or an entire server ("\\server\").

The mobilEcho client can now perform copy and move operations on folders when connected to a server running mobilEcho Server 2.1 or later, and the management UI now has settings to allow or disallows these operations.

The management UI now has the ability to add a new group or user using settings from an existing user or group.

Management profiles can now be disabled so that the corresponding user or group cannot receive their profile.

Added the ability to prevent clients from connecting to servers with self-signed certificates.

Added a management setting to enable or disable copying text from a previewed document.

Added a management setting that tells the client to store files so that they are not backed up by iTunes.

mobilEcho 2.0.0 (Released: May 2011)

ENHANCEMENTS:

Added the ability to manage mobilEcho clients using server-defined profiles using mobilEcho Client Management.

Added the ability to reset mobilEcho app passwords from the server.

Added the ability to force a remote wipe for a particular mobilEcho user.

mobilEcho will now use an internal filename index for satisfying search requests if Windows Search is not installed or available.

The mobilEcho administrator now allows for volumes to be seamlessly replicated from SMB and/or ExtremeZ-IP shares.

mobilEcho 1.0.0 (Released: January 2011)

Initial release.

19 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.

- 8.6.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