

Cover page Install And Admin Copyright Statement

Copyright © Acronis International GmbH, 2002-2014. All rights reserved.

“Acronis” and “Acronis Secure Zone” are registered trademarks of Acronis International GmbH.

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "Acronis Active Restore", "Acronis Instant Restore" and the Acronis logo are trademarks of Acronis International GmbH.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <http://kb.acronis.com/content/7696>

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 and patent pending applications.

Table of contents

1	Installing.....	5
1.1	Requirements	5
1.1.1	Operating System Requirements	5
1.1.2	Mobile Client requirements	5
1.1.3	Minimum Hardware Recommendation	6
1.1.4	Desktop Client Requirements	6
1.1.5	Network Requirements	7
1.2	Installing Acronis Access on your server.....	7
1.3	Using the Configuration Utility	9
1.4	Using the Setup wizard	10
2	Maintenance Tasks	18
2.1	Disaster Recovery guidelines	18
2.2	Backing up and Restoring Acronis Access.....	20
2.3	Tomcat Log Management on Windows.....	23
2.4	Automated Database Backup	27
2.5	Increasing the Acronis Access Tomcat Java Maximum Memory Pool.....	29
3	Mobile Access.....	31
3.1	Concepts	31
3.2	Policies	33
3.2.1	Group Policy.....	33
3.2.2	Default Access Restrictions.....	43
3.3	On-boarding Mobile Devices	43
3.3.1	Server-side Management Enrollment Process	44
3.3.2	User-side Management Enrollment Process	45
3.4	Managing Your Gateway Server	48
3.4.1	Server Details.....	50
3.4.2	Editing Gateway Servers.....	53
3.5	Managing Data Sources	60
3.5.1	Folders.....	62
4	Settings	66
5	Quick Start: Mobile Access	67
5.1	First Run	67
6	Configuring your Group Policy	72
6.1	Installing the Access Mobile Client application	72
6.2	Enrolling in client management.....	72
7	Quick Start: Sync & Share	77
7.1	First Run	77
8	Web Client.....	82
8.1	Using the desktop client	89

9	Server Administration	94
9.1	Administering a Server	94
9.2	Administrators and Privileges	95
9.3	Audit Log	97
9.3.1	Log	97
9.3.2	Settings	98
9.4	Server	99
9.5	SMTP	101
9.6	LDAP	102
9.7	Email Templates	104
9.8	Licensing	106
9.9	Debug Logging	107
9.10	Monitoring	108
10	Supplemental Material	110
10.1	Conflicting Software	110
10.2	Using trusted server certificates with Acronis Access	110
10.3	Changing the Acronis Access Tomcat SSL Ciphers	112
10.4	How to support different Access Desktop Client versions	113
10.5	Customizing the web interface	113
10.6	Creating a Drop Folder	114
10.7	Monitoring Acronis Access with New Relic	115
10.8	Third-party Software for Acronis Access	116
10.8.1	PostgreSQL	116
10.8.2	Apache Tomcat	117
10.8.3	New Relic	117
11	Sync & Share	118
11.1	Sharing Restrictions	118
11.2	LDAP Provisioning	118
11.3	Quotas	119
11.4	File Purging Policies	119
11.5	User Expiration Policies	121
11.6	File Repository	122
11.7	Acronis Access Client	123
12	Upgrading	125
12.1	Upgrading from Acronis Access to a newer version	125
13	Users&Devices	127
13.1	Managing Mobile Devices	127
13.1.1	Performing Remote Application Password Resets	128
13.1.2	Performing Remote Wipes	129
13.2	Managing Users	130

14	What's New	134
14.1	What's New in Acronis Access Server	134
14.2	What's New in the Acronis Access app	148
14.3	Previous Releases	149
14.3.1	activEcho	149
14.3.2	mobilEcho	160

1 Installing

In this section

Requirements.....	5
Installing Acronis Access on your server.....	7
Using the Configuration Utility	9
Using the Setup wizard	10

1.1 Requirements

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

In this section

Operating System Requirements.....	5
Mobile Client requirements.....	5
Minimum Hardware Recommendation	6
Desktop Client Requirements	6
Network Requirements.....	7

1.1.1 Operating System Requirements

Recommended:

Windows 2012 all flavors
Windows 2008 R2 64 bit

Supported:

Windows 2012 R2
Windows 2012, Standard and Datacenter editions
Windows 2008, all flavors, 32/64 bit

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

1.1.2 Mobile Client requirements

The mobile client application is compatible with:

Supported devices:

- Apple iPad 2nd, 3rd, 4th generation, Air, Air 2
- Apple iPad Mini 1st, 2nd, 3rd generation
- Apple iPhone 3GS, 4, 4S, 5, 5s, 5c, 6, 6 Plus
- Apple iPod Touch 4th, 5th generation
- Android Smartphones and Tablets (Devices with x86 processor architecture are not supported)

Supported OS's:

- iOS 6 or later

- Android 2.2 or later (Devices with x86 processor architecture are not supported)

The Acronis Access app can be downloaded from:

- For iOS <http://www.grouplogic.com/web/meappstore>
- For Android <https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho>

1.1.3 Minimum Hardware Recommendation

Processor: Intel/AMD

Note: Acronis Access server can be installed on virtual machines.

Memory:

- Production environments: 8 GB minimum. More recommended.
- Trial or Test environments: 4 GB minimum. 8 GB or more recommended.

Disk Space:

- The software installation requires 300MB of disk space.

Note: Please make sure that you have enough space to run the Acronis Access installer. 1GB of space is required for the installer to run.

- The file repository used by the Sync & Share features is installed on the local computer by default.
- Enough free space should be provided to meet testing parameters. 50 GB or more is recommended.

1.1.4 Desktop Client Requirements

Supported operating systems:

- Windows XP, Windows Vista, Windows 7, Windows 8 and 8.1

Note: In order to use the Acronis Access Desktop client on Windows XP, you will need to use relaxed SSL cipher rules. For more information: [Changing the Acronis Access Tomcat SSL Ciphers \(p. 112\)](#).

- Mac OS X 10.6.8 and higher with Mac compatible with 64-bit software.

Note: When installing the Acronis Access 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 \(p. 110\)](#).

Supported web browsers:

- Mozilla Firefox 6 and later
- Internet Explorer 9 and later

*Note: You can support an **unsecure** version of Internet Explorer 8 if necessary by following the [Changing the Acronis Access Tomcat SSL Ciphers \(p. 112\)](#) article. Internet Explorer 8 is not supported for Server Administration.*

*Note: When using Internet Explorer you have to make sure that **Do not save encrypted pages to disk** is unchecked in order to be able to download files. This setting is found under **Internet Options -> Advanced -> Security**.*

- Google Chrome
- Safari 5.1.10 or later

1.1.5 Network Requirements

- 1 Static IP Address.
- Optional but recommended: DNS name matching the above IP address.
- Network access to a Domain Controller if Active Directory will be used.
- Network access to an SMTP server for email notifications and invite messages.
- The address **127.0.0.1** is used internally by the Access Mobile Client and should not be routed through any kind of tunnel (e.g. VPN).
- The machine running Acronis Access needs to be bound to the Windows Active Directory.

Note: *It is recommended to bind the server to the domain. Mobile clients will not be able to access Data sources unless the server is bound to the domain.*

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

- **Port 443 access:** Acronis Access 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 Access server, authorized iPad clients can connect while inside or outside of your firewall. Acronis Access can also be configured to use any other port you prefer.
- **VPN:** The Access Mobile Client 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 the Apple iPhone Configuration Utility to configure the certificate-based iOS “VPN-on-demand” feature, giving seamless access to Acronis Access 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 Access Mobile Client app supports reverse proxy pass-through authentication and username / password authentication.

Note: *If you want to use a mobile device management like Good Dynamics or MobileIron, you will need to upgrade to Acronis Access Advanced.*

Certificates:

Acronis Access ships and installs with self-signed certificates for testing purposes. Production deployments should implement proper CA certificates.

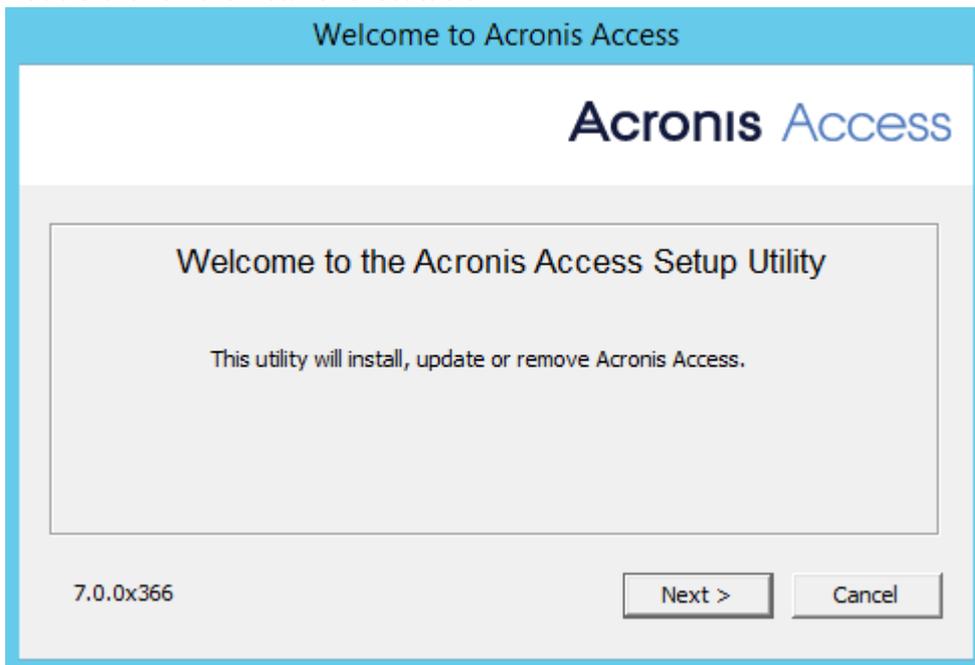
Note: *Certain web browsers will display warning messages when using self-signed certificates. Dismissing those messages allows the system to be used without problems. Using self-signed certificates for production conditions is not recommended.*

1.2 Installing Acronis Access on your server

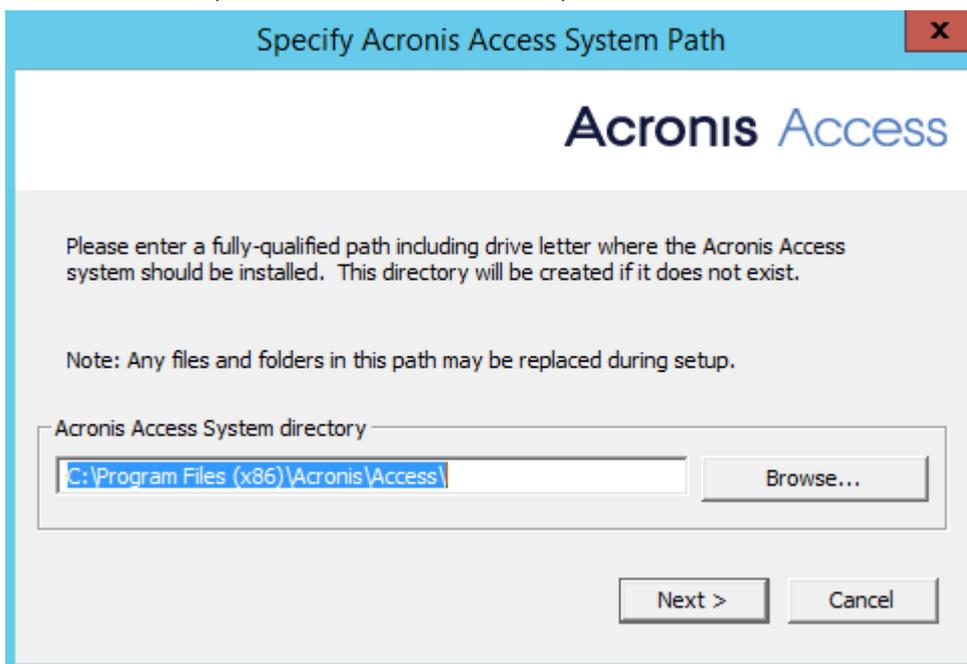
Installing Acronis Access

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

1. Download the Acronis Access 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.

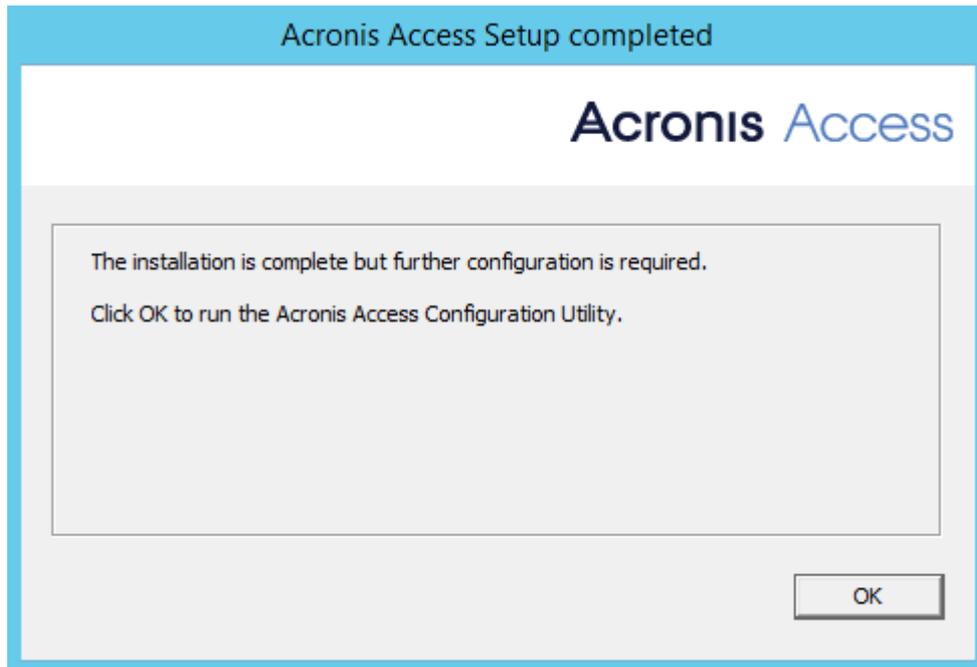


4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.
7. Select where the product will be installed and press **Next**.



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

9. Press **Exit** to close the installer.



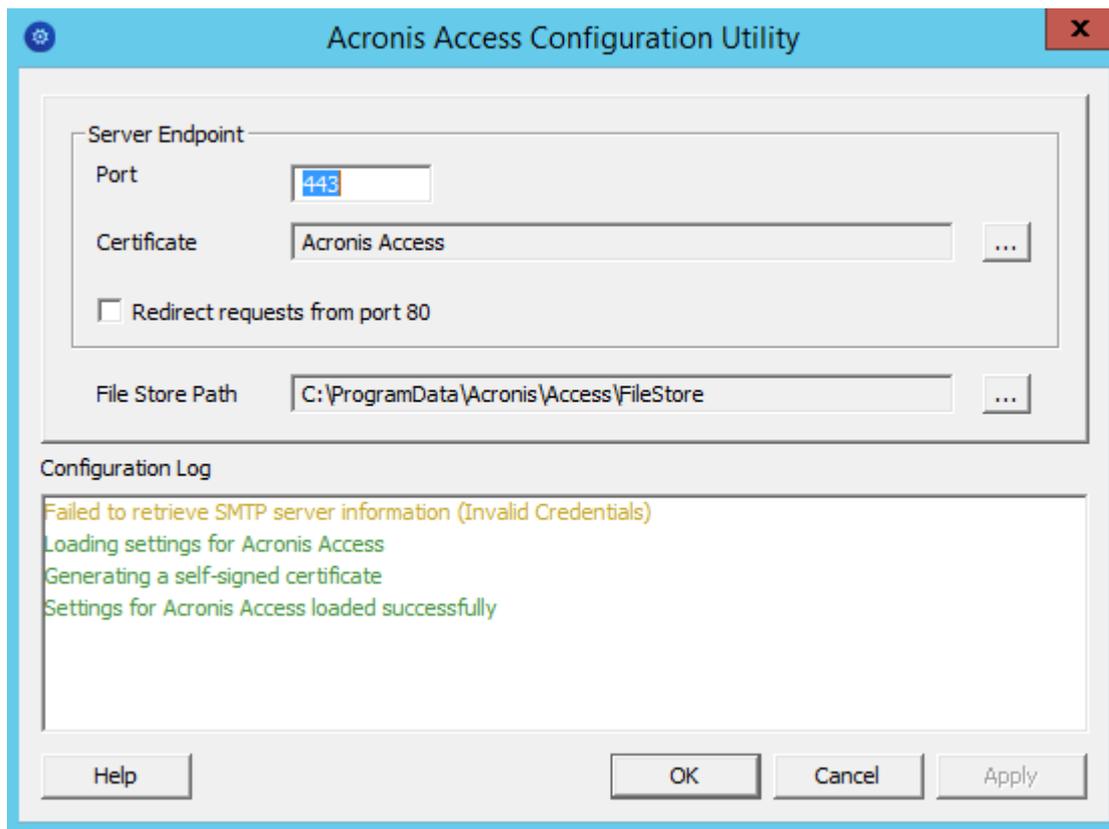
The Configuration Utility will launch automatically to complete the installation

1.3 Using the Configuration Utility

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

Note: See the *Network Requirements (p. 7)* section for more information on best practices for the IP address configurations of Acronis Access.

Note: For information on adding your certificate to the Microsoft Windows Certificate Store, visit the *Using Certificates (p. 110)* article.



- **Port** - The port of your Web Interface and Gateway Server.
- **Certificate** - SSL certificate for your Web Interface and Gateway Server. You can choose a certificate from the Microsoft Windows Certificate Store.
- **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 Store Path** - Local 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.

1.4 Using the Setup wizard

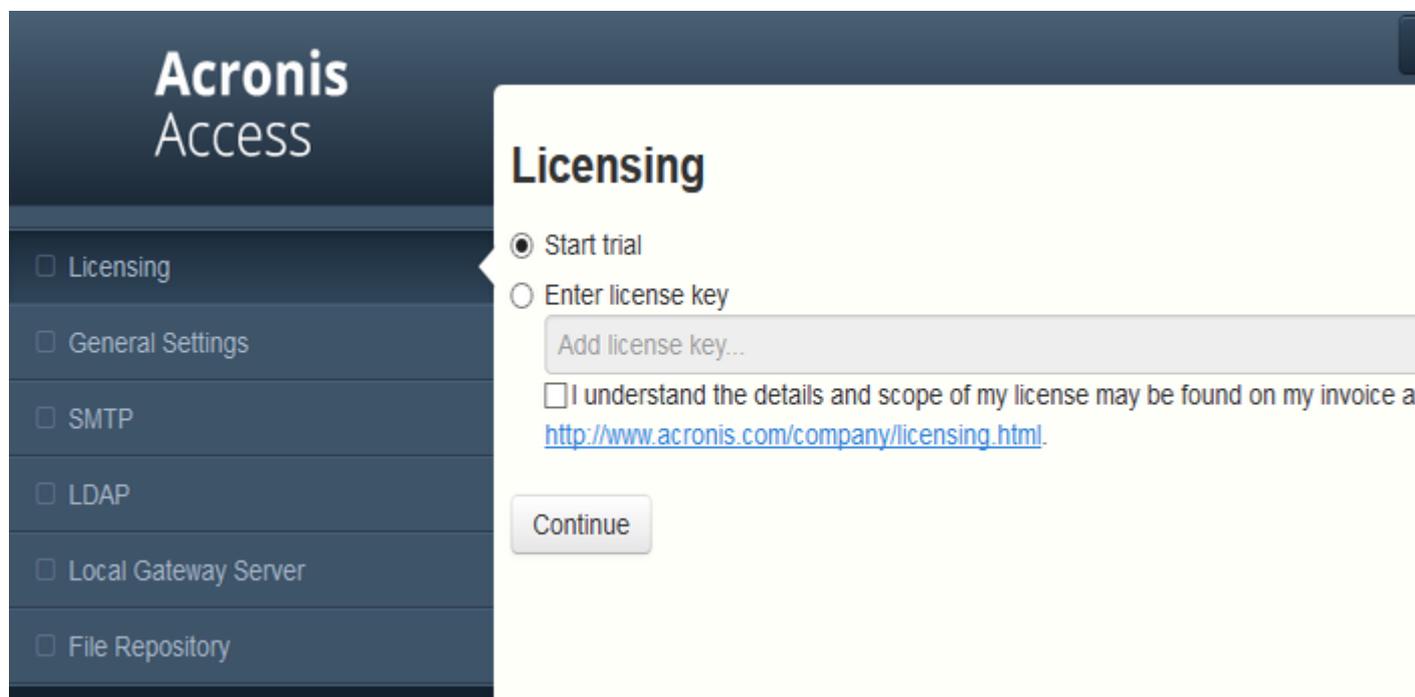
After installing the software and running the configuration utility to setup the network port and SSL certificate, the administrator now needs to configure the Acronis Access server. The Setup Wizard detects most of the necessary settings (LDAP, Server and SMTP) automatically to help you get the basic functionality of the server working. You can still change all of these settings manually before proceeding.

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 Access's web interface using any of the available IP addresses and the port specified in the configuration utility. You will be prompted to set the password for the default administrator account.

Note: Administrators can be configured later on, for more information visit the *Server Administration (p. 94)* section.

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

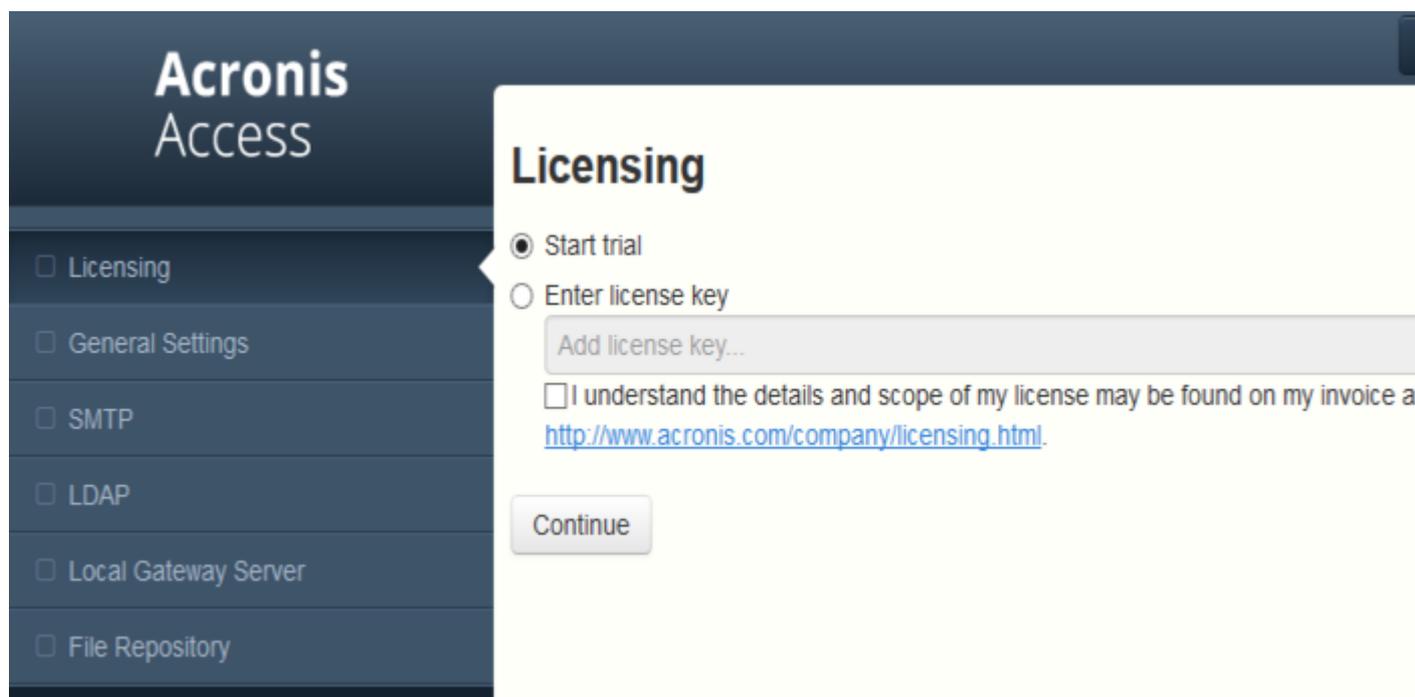


- General Settings cover settings of the web interface itself, like the language, the color scheme, the server name used in admin notifications, licensing and administrators.
- LDAP settings allow you to use Active Directory credentials, rules and policies with our product.
- SMTP settings cover functionality 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 (p. 94)* articles.

Going through the initial configuration process

Licensing



The screenshot shows the Acronis Access web interface. On the left is a dark sidebar with the 'Acronis Access' logo and a list of configuration options: Licensing, General Settings, SMTP, LDAP, Local Gateway Server, and File Repository. The 'Licensing' option is selected. The main content area is titled 'Licensing' and contains two radio button options: 'Start trial' (which is selected) and 'Enter license key'. Below the 'Enter license key' option is a text input field with the placeholder 'Add license key...'. There is also a checkbox for 'I understand the details and scope of my license may be found on my invoice a' with a link to <http://www.acronis.com/company/licensing.html>. A 'Continue' button is located at the bottom of the form.

To start a trial:

1. Select **Start Trial** and press **Continue**.

To license your Access Server:

1. Select **Enter license keys**.
2. Enter your license key and mark the checkbox.
3. Press **Save**.

General Settings

Server Settings

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://www.access.domain.com"/>
Mobile Client Enrollment Address	<input type="text" value="www.access.domain.com"/>
Use Custom Logo	<input type="checkbox"/>
Audit Log Language	<input type="text" value="English"/> 

1. Enter a Server Name.
2. Specify the root DNS name or IP address where users can access the website (starting with http:// or https://).
3. Specify the DNS name or IP address to which the mobile users will enroll to.
4. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
5. Press **Save**.

SMTP

SMTP

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

SMTP Server Address

SMTP Server Port

Use secure connection?

From Name

From Email Address

Use SMTP authentication?

Note: You can skip this section, and configure SMTP later.

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

LDAP

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

Require exact match

LDAP information caching interval

Note: You can skip this section, and configure LDAP later.

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

2 Maintenance Tasks

To backup all of Acronis Access's elements and as part of your best practices and backup procedures, you may want to read the *Disaster Recovery guidelines (p. 18)* article.

In this section

Disaster Recovery guidelines	18
Backing up and Restoring Acronis Access	20
Tomcat Log Management on Windows	23
Automated Database Backup	27
Increasing the Acronis Access Tomcat Java Maximum Memory Pool	29

2.1 Disaster Recovery guidelines

High availability and fast recovery is of extreme importance for mission critical applications like Acronis Access. 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 Access to a working state in a very short period of time.

Introduction:

For mission critical applications like Acronis Access, 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 Access to a working state in a very short period of time.

There are different ways to implement disaster recovery, including backup-restore, imaging, virtualization and clustering. We will describe the backup-restore approach in the following sections.

Description of the Acronis Access elements:

Acronis Access is a solution composed of several discrete but interconnected elements:

Acronis Access Gateway Server

Note: Normally located here: C:\Program Files (x86)\Acronis\Access\Gateway Server

Acronis Access Server

Note: Normally located here: C:\Program Files (x86)\Acronis\Access\Access Server

Acronis Access Configuration Utility

Note: Normally located here: C:\Program Files (x86)\Acronis\Access\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 Access. The Acronis Access 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 Access.

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 Access to contact an Active Directory domain controller and SMTP server.
- Fast or automated DNS switching ability to redirect incoming request to the secondary node.

The process

Backup Setup

The recommended approach to provide a safe and fast recovery scenario can be described like this:

1. Have an installation of Acronis Access, 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 Access 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 Access 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 Access 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 Access database.
7. Start the Acronis Access Tomcat service.
8. Migrate DNS to point to the new node.
9. Verify Active Directory and SMTP are working

2.2 Backing up and Restoring Acronis Access

In case you need to upgrade, update or maintain your Acronis Access server. This article will give you the basics of backing up your database and restoring it.

Backing up your databases

Backing up your Acronis Access's 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 **PostgreSQL\bin** folder located in the PostgreSQL installation directory.
e.g. **cd "C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\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 Access database

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access 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>
<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

Info: For more information on PostgreSQL backup procedures and command syntax please read this:
<http://www.postgresql.org/docs/9.2/static/backup.html>
<http://www.postgresql.org/docs/9.1/static/backup.html>

Backing up your Gateway Server's database

1. Go to the server on which you have Acronis Access installed.
2. Navigate to the folder containing the database.

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

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

Restoring Acronis Access

Restoring your Acronis Access's database

The database restore process is similar to the backup process.

1. Prior to executing the command to restore your database, make sure the source backup file is located in a directory or location where it can be accessed by the logged in user.
2. Open a Command Prompt window and navigate to the **PostgreSQL\bin** folder located in the PostgreSQL installation directory.

cd "C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\bin"

Note: This directory may be different if you installed PostgreSQL in a custom location.

3. You need to remove the old database first. To do so, stop the Acronis Access Tomcat service and enter the following line:

Warning! Do not continue with this step unless you are certain you have made a successful backup. Dropping the database is an irreversible process which deletes the entire database. All information is lost.

dropdb -U postgres acronisaccess_production

A "password for user **postgres**:" message may appear. If that happens, enter the **postgres** password that you set during the Acronis Access installation process. **acronisaccess_production** must be entered exactly as shown. This is the **Acronis Access** database name.

4. Once the operation finishes, enter the following line:
createdb -U postgres acronisaccess_production

A "password for user **postgres**:" message may appear. If that happens, enter the **postgres** password that you set during the Acronis Access installation process. **acronisaccess_production** must be entered exactly as shown. This is the **Acronis Access** database name.

5. To fill the newly created database with the information from your backup, enter the following line:

psql -U postgres -d acronisaccess_production -W -f mybackup.sql

Replace **mybackup.sql** with the fully qualified name of the backup file, for instance:
D:\Backups\mybackup.sql

A "password for user **postgres**:" message may appear. If that happens, enter the **postgres** password that you set during the Acronis Access installation process. **acronisaccess_production** must be entered exactly as shown. This is the **Acronis Access** database name.

6. Once the process has completed successfully, restart the postgres service and start the Acronis Access Tomcat service.

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

Info: For full **psql** command syntax, please visit <http://www.postgresql.org/docs/9.2/static/app-psql.html>
<http://www.postgresql.org/docs/9.0/static/app-psql.html>

Restoring your Gateway Server's database

1. Copy the **mobileEcho.sqlite3** file you have backed up.
2. Go to the server on which you have Acronis Access installed.
3. Navigate to the folder containing the database and paste the **mobileEcho.sqlite3** file.

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

4. Restart the **Acronis Access Gateway Server** service.

Restoring Acronis Access to a new instance

1. Complete the Backup procedure explained above and move the **alldbs.sql** and **mobileEcho.sqlite3** files to the new server.
2. On the new server, complete the Database restoration procedure explained above.
3. Start the Acronis Access services.
4. Complete the following procedure:

Configurations on the new instance

Note: It is highly recommended that you **do not** change the DNS names used by Acronis Access, 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 Access

1. Open the Acronis Access web interface and login.
2. Navigate to **Mobile Access -> Gateway Servers**.
3. Press on the down arrow next to the **Details** button and select **Edit**.
4. Click on the **SharePoint** tab and enter the SharePoint administrator's credentials.
5. If the **Address for administration** is set as an IP address, change it to the new IP you set for the Acronis Access Server.
6. Press **Apply**.

If you do not intend to use the same IP address as the previous instance, change the IP entries for the DNS names used by the Acronis Access and Gateway Server.

2.3 Tomcat Log Management on Windows

As part of its normal operation Tomcat creates and writes information to a set of log files.

Unless periodically purged, these files accumulate and consume valuable space. It is commonly accepted by the IT community that the informational value those logs provide degrades rapidly. Unless other factors like regulations or compliance with certain policies play, keeping those log files in the system a discrete number of days is what is required.

Introduction:

As part of its normal operation Tomcat creates and writes information to a set of log files. On Windows, these files are normally located in the following directory:

“C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.34\logs”
Acronis Access saves it's own logs in the same directory as separate files.

*Acronis Access'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.

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

A sample process:

The sample process described below automates the process of purging log files older than a certain number of days. Inside the sample batch file, this number is defined as a parameter so it can be changed to fit different retention policies.

Info: The sample script (batch) file is designed to work on Windows 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”

[Click here for the full batch script code...](#)

```
ECHO OFF

REM Script: aETomcatLogsPurge.bat

REM 2012-05-12: Version: 1.0: MEA: Created

ECHO This script will delete files older than a number of days from a directory

ECHO Run it from the command line or from a scheduler

ECHO Make sure the process has permissions to delete files in the target folder

REM ===== CONFIGURATIONS =====

REM Note: all paths containing spaces must be enclosed in double quotes

REM Edit this file and set LogPath and NumDays below

REM Path to the folder where all Tomcat logs are

set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"
```

```

REM NumDays - Log files older than NumDays will be processed

set NumDays=14

REM ===== END OF CONFIGURATIONS =====

ECHO

ECHO ===== START =====

REM ForFiles options:

REM      "/p": the path where you want to delete files.

REM      "/s": recursively look inside other subfolders present in the folder
mentioned in the batch file path

REM      "/d": days for deleting the files older than the present date. For instance
"/d -7" means older than 7 days

REM      "/c": command to execute to actually delete files: "cmd /c del @file".

forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"

:End

ECHO ===== BATCH FILE COMPLETED =====

```

Warning: We provide this example as a guideline so you can plan and implement your own process based on the specifics of your deployment. The example is not meant nor tested to apply to all situations and environments so use it as a foundation and at your own risk. **Do not use it in production environments without comprehensive offline testing first.**

Steps:

1. Copy the script to the computer running Acronis Access (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"

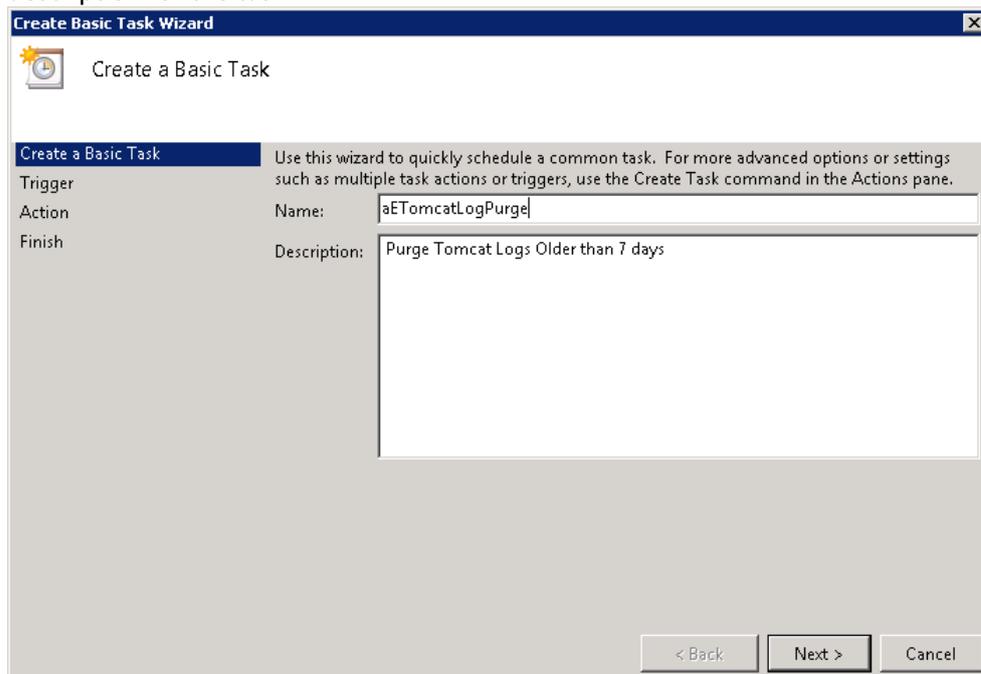
REM NumDays - Log files older than NumDays will be processed
set NumDays=14
REM ===== END OF CONFIGURATIONS =====
ECHO
ECHO ===== START =====

```

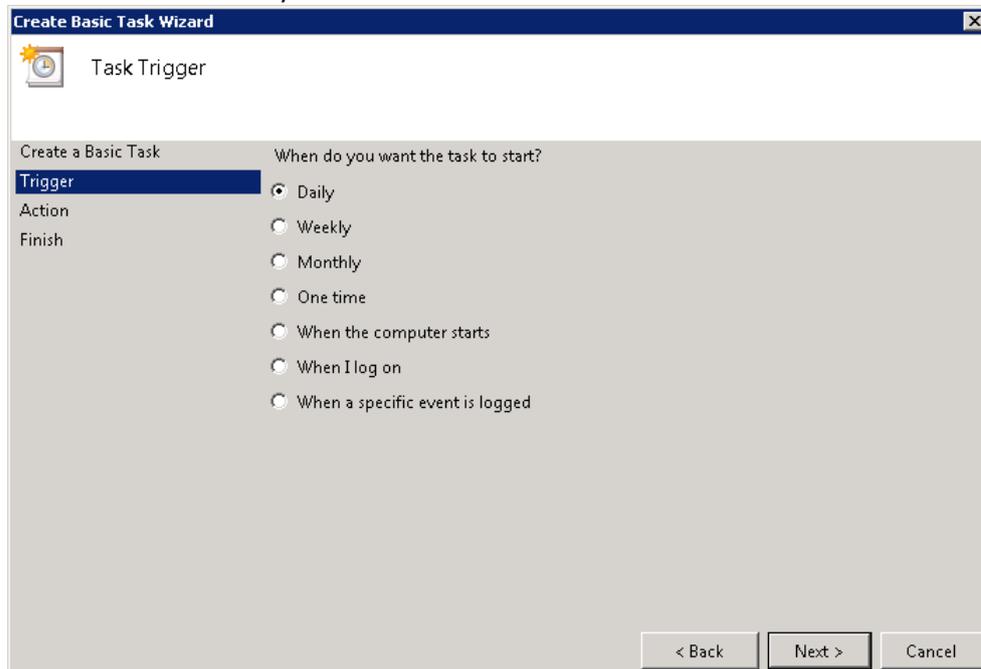
In Acronis Access the log files are stored in the same folder as Tomcat's. (C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.34\Logs)

3. Save the file.

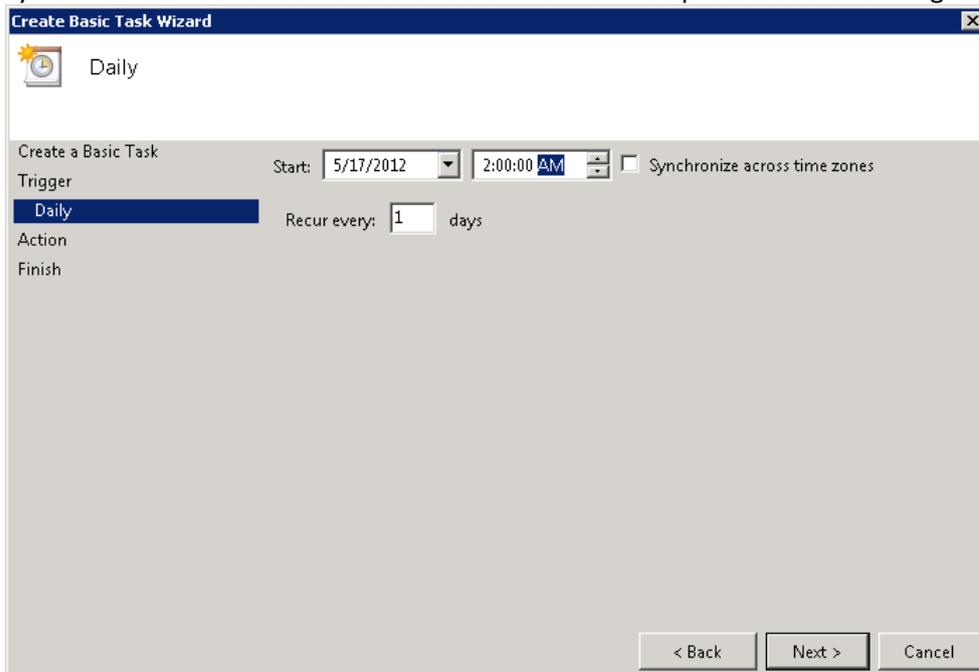
- To automate the process, open Task Scheduler and create a new task. Define a name and a description for the task.



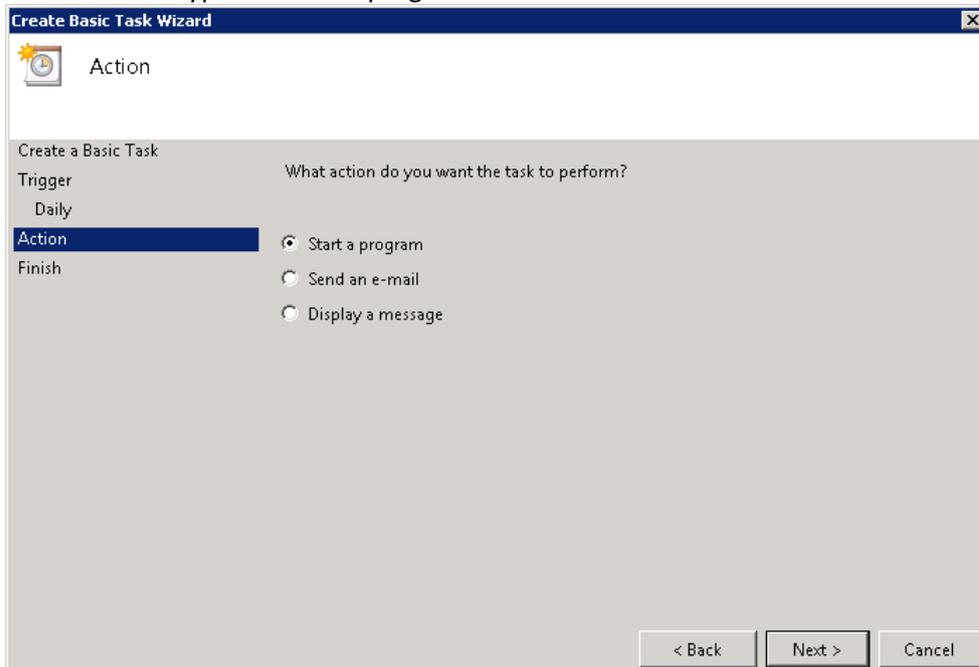
- Set the task to run daily.



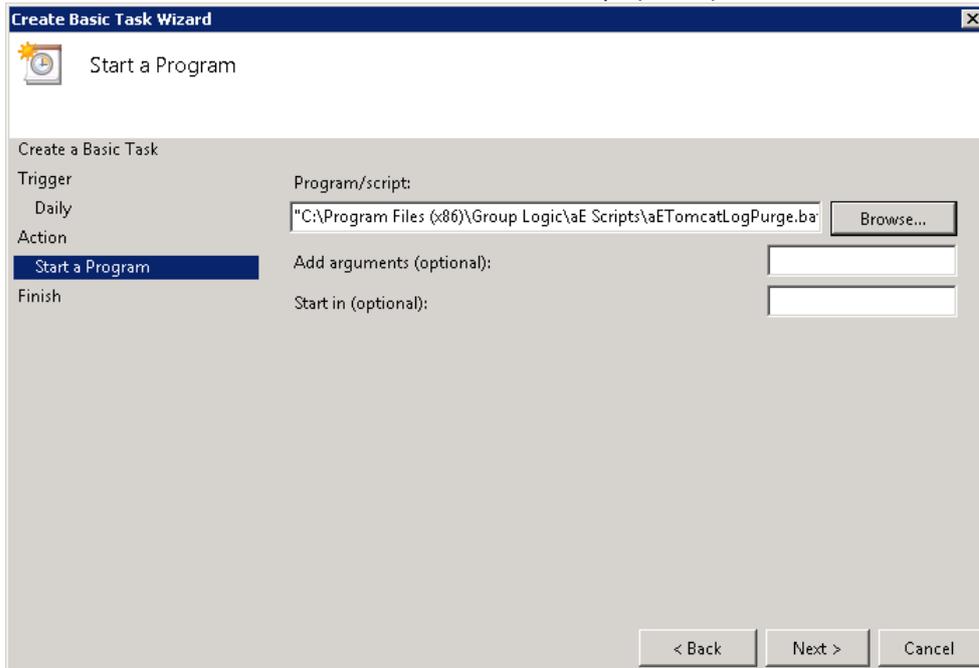
- Define at what time the task should start. It is recommended to run this process when the system is not under extreme load or other maintenance processes are running.



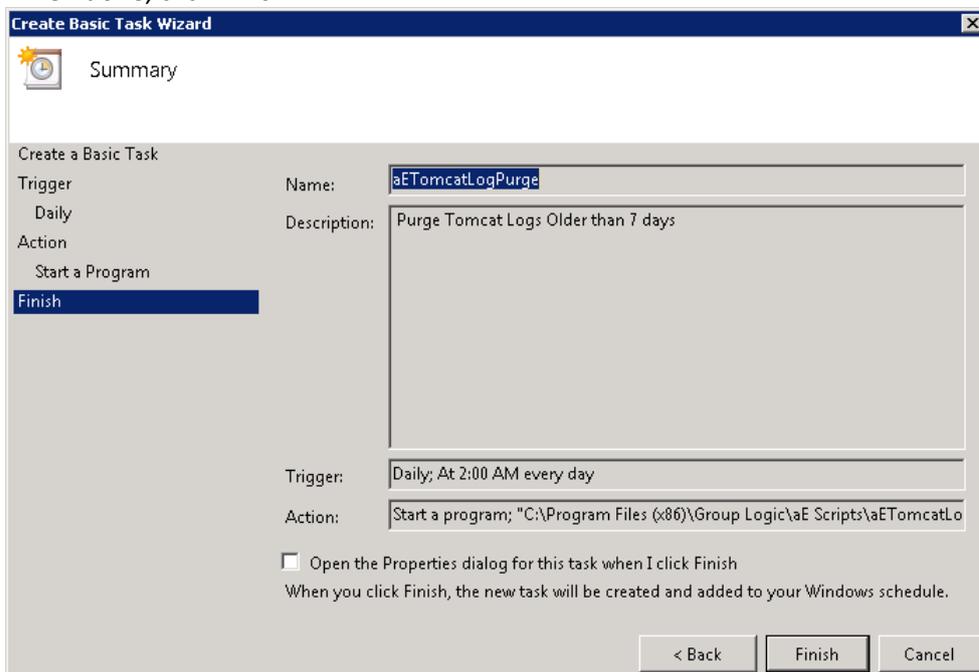
- Set the action type to "Start a program".



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.

2.4 Automated Database Backup

With the help of the Windows Task Scheduler, you can easily setup an automated backup schedule for your Acronis Access database.

Creating the database backup script

1. Open **Notepad** (or another text editor) and enter the following:

```
@echo off
for /f "tokens=1-4 delims=/ " %%i in ("%date%") do (
set dow=%%i
set month=%%j
set day=%%k
set year=%%l
)
set datestr=%month%_%day%_%year%
echo datestr is %datestr%

set BACKUP_FILE=AAS_%datestr%_DB_Backup.sql
echo backup file name is %BACKUP_FILE%
SET PGPASSWORD=password
echo on
bin\pg_dumpall -U postgres -f %BACKUP_FILE%

move "%BACKUP_FILE%" "C:\destination folder"
```

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

Creating the scheduled task

1. Open the **Control Panel** and open **Administrative Tools**.
2. Open the **Task Scheduler**.
3. Click on **Action** and select **Create Task**.

On the General tab:

1. Enter a name and description for the task (e.g. AAS Database Backup).
2. Select **Run whether user is logged in or not**.

On the Triggers tab:

1. Click **New**.
2. Select **On a schedule for Begin the task**.
3. Select **daily** and select the time when the script will be run and how often the script should be rerun (how often you want to backup your database).
4. Select **Enabled** from the **Advanced settings** and press **OK**.

On the Actions tab:

1. Click **New**.
2. Select **Start a program** for **Action**.
3. For **Program/Script** press **Browse**, navigate to and select the **DatabaseBackup.bat** file.
4. For **Start in (optional)**, enter the path to the folder in which the script resides. e.g. If the path to the script is **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.3\PSQL.bat** enter **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.3**
5. Press **OK**.

Configure any additional settings on the other tabs and press OK.

You will be prompted for the credentials for the current account.

2.5 Increasing the Acronis Access Tomcat Java Maximum Memory Pool

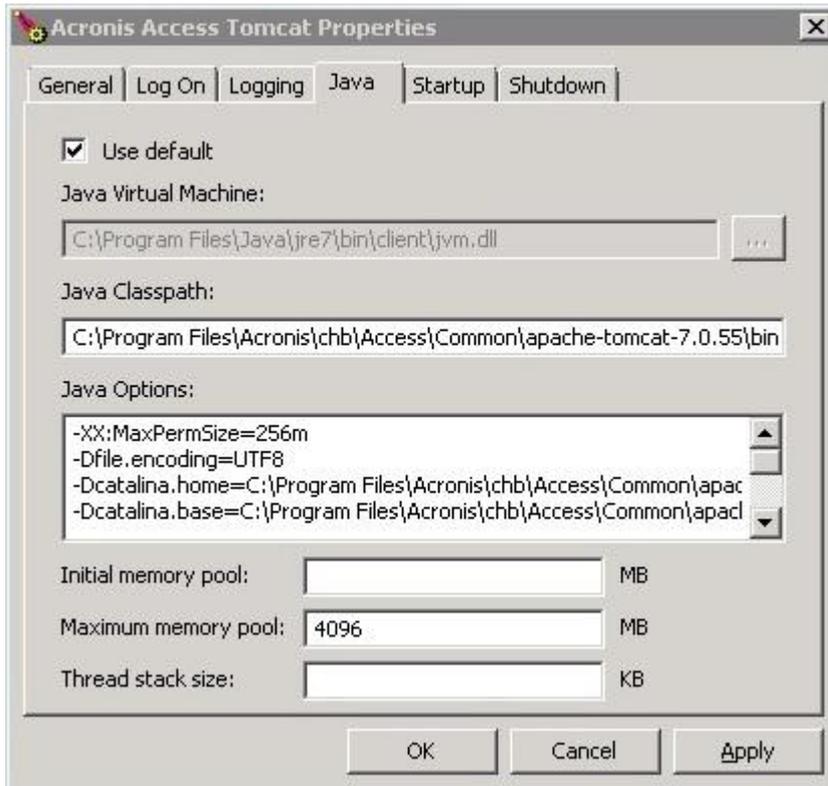
By default, the Acronis Access Tomcat's Java Maximum Memory Pool setting on a 64 bit operating system is 4GBs. Depending on your deployment, you may need more.

Note: *On a 32bit operating system, the maximum memory pool is 1GB.*

To increase the maximum memory pool:

1. Click on the Start menu and navigate to **All Programs** -> Acronis Access.

2. Click on the **Acronis Access Tomcat 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 Access Tomcat service.

3 Mobile Access

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

In this section

Concepts.....	31
Policies	33
On-boarding Mobile Devices	43
Managing Your Gateway Server.....	48
Managing Data Sources	60
Settings.....	66

3.1 Concepts

Access Mobile Clients connect directly to your server rather than utilizing a third-party service, leaving you in control. Acronis Access server can be installed on existing file servers, allowing iPads, iPhones and Android devices to access files located on that server. These are typically the same files already available to PCs using Windows file sharing and Macs using ExtremeZ-IP File Server.

Clients access Acronis Access servers using their Active Directory user account. No additional accounts need to be configured within Acronis Access. The Access Mobile Client also supports file access using local computer accounts configured on the Windows server Acronis Access 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.

The deployment consists of a single Windows server running an installation of Acronis Access. This includes the Acronis Access Server component installed and the Acronis Access Gateway Server installed. This scenario allows devices running the Access Mobile Client application to connect to this single file server, and allows for client management.

If client management is not needed, Data Sources can be setup on the local Gateway Server and the Access Mobile Clients will be able to access these Data Sources. Each user will be in control of his own app settings.



Fig 1. Single Gateway server, many Access Mobile Clients

Note: Details on installing Acronis Access are included in the *Installing* (p. 5) section of this guide. The configuration of Data Sources is explained in the *Mobile Access* (p. 31) section.

If you wish to remotely manage your Access Mobile Clients, Acronis Access allows you to use a group policy. This policy 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 Access Mobile Client files can be opened into
- Set security requirements (server login frequency, application lock password, etc.)
- Disable the ability to include Access Mobile Client files in iTunes backups
- Remotely reset a user's application lock password
- Perform a remote wipe of the Access Mobile Client app's local data and settings
- And many additional configuration and security options

Only one Acronis Access Server is allowed.

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

Acronis Access 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 Access 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 (p. 33)* and *Managing Mobile Devices (p. 127)* section of this guide.

3.2 Policies

In this section

Group Policy	33
Default Access Restrictions	43

3.2.1 Group Policy

Acronis Access uses a single Group Policy to manage all of your mobile users.

Group Policies User Policies Allowed Apps Default Access Restrictions

Manage Group Policies

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

+ Add Group Policy Filter by Name GLI

Common Name / Display Name	Distinguished Name		En
GLI	CN=hristo,CN=Users,DC=glilabs,DC=com	↑ ↓	
Default			

3.2.1.1 Exceptions for policy settings

Acronis Access does not support the **Acronis Access for Good Dynamics** and **Acronis Access with Mobile Iron AppConect** apps.

3.2.1.2 Modifying the Policy

Changes to the policy will be applied to the relevant Acronis Access client users the next time they launch the app.

Connectivity requirements

Acronis Access clients must have network access to the Acronis Access 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 Access, they will also need to connect to the VPN before management commands will be accepted.

To modify the Group policy

1. Click on the default group.
2. Make any changes necessary on the **Edit Group Policy** page and press **Save**.

3.2.1.3 Security Policy

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

App Password Creation: **G M**

- Optional
- Disabled
- Required

App Will Lock:

Allow User to Change This Setting

Minimum Password Length:

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

Require One or More Letter Characters

Mobile client app will be wiped after failed app password attempts

Wipe or Lock After Loss of Contact

Mobile client app will be after days of failing to contact this client's Acronis Access server

Warn user starting days beforehand

- Allow iTunes and iCloud to Back up Locally Stored Acronis Access Files **A**
- User Can Remove Mobile Client from Management
 - Wipe All Acronis Access Data on Removal

- **App password creation** - The Access Mobile Client 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 Access Mobile Client.

- **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 Access Mobile Client to another application on their device, if they return to the Access Mobile Client 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 Access Mobile Client 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 Access Mobile Client app will be wiped after the specified number of consecutive failed app password attempts.
- **User can remove Mobile Client from management**- Enable this setting if you would like your Acronis Access users to be able to uninstall their management policy from within Acronis Access. Doing so will return the application to full functionality and restore any configuration that was changed by their policy.
 - **Wipe all Acronis Access data on removal** - When user removal of policies is enabled, this option can be selected. If enabled, all data stored locally within the Access Mobile Client application will be erased if it is removed from management, ensuring that corporate data does not exist on a client not under management controls.
- **Allow iTunes to back up locally stored Acronis Access files** - When this setting is disabled, the Access Mobile Client will not allow iTunes to back up its files. This will ensure that no files within Acronis Access' secure on-device storage are copied into iTunes backups.

3.2.1.4 Application Policy

Security Policy Application Policy Sync Policy Home Folders Server Policy

Require Confirmation When Deleting Files

Allow User to Change This Setting

Set the Default File Action **A**

Default Action:

Allow User to Change This Setting

Allow Files to be Stored on This Device

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

Cache Recently Accessed Files on the Device **A**

Maximum Cache Size:

Allow User to Change This Setting

Content in My Files and File Inbox Expires after days **A**

- **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 Access Mobile Client 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**.
- **Display Thumbnail Previews for Server-Side Files** - When enabled, thumbnail previews will be displayed instead of filetype icons when browsing Data Sources and Gateway Servers.
 - **Thumbnail Cache Size**: - Sets how much space will be reserved for thumbnails.
 - **Only Download Thumbnail Previews on WiFi Networks** - When enabled, thumbnails will be available only if the user is connected to a WiFi network.

Allow

Allow

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

Only file and folder operation settings apply to Mobile Access data sources accessed via the Acronis Access web client interface.

File Operations

- File Copies / Creation
- File Deletes
- File Moves
- File Renames

Folder Operations

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

'mobilEcho' File Links

- Emailing 'mobilEcho' File Links **G**
- Opening 'mobilEcho' File Links **G**

Data Leakage Protection

- Opening Acronis Access Files in Other Applications

App Whitelist/Blacklist: **A G M**

- Sending Files to Acronis Access from Other Apps **G**
- Emailing Files from Acronis Access **A G**
- Printing Files from Acronis Access **A G M**
- Copying text From Opened Files **A G M**

Annotation and Editing

- Allow PDF Annotation
- Editing & Creation of Office Files
- Editing & Creation of Text Files **A**

These settings can be used to disable certain Access Mobile Client application features and capabilities. All copy, create, move, rename, and delete settings apply to files or folders located on Gateway servers. Files in 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 Access, 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 Access Mobile Client 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 Access Mobile Client 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 Access folders for quick shortcut access.

Data Leakage Protection

- **Opening Acronis Access Files in Other Applications** - If this option is disabled, the Access Mobile Client application will omit the **Open In** button and not allow files in Acronis Access 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 Access control.

3.2.1.5 Sync Policy

Security Policy Application Policy **Sync Policy** Home Folders Server Policy

Allow User to Create Sync Folders

Client is Prompted to Confirm before Synced Files are Downloaded:

Allow User to Change This Setting

Only Allow File Syncing While Device Is on WiFi Networks

Allow User to Change This Setting

Auto-Sync Interval:

Allow User to Change This Setting

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

- **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.
- **Auto-Sync Interval** - When this option is enabled, Acronis Access 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 Access Mobile Client app.
 - **Only Allow File Syncing While Device is on WiFi Networks** - When this option is enabled, Acronis Access 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.

3.2.1.6 Home Folders

Security Policy Application Policy Sync Policy **Home Folders** Server Policy

Display the User's Home Folder

Display Name Shown on Client: Home Folder

Home Directory Type:

Active Directory Assigned Home Folder

Gateway Server used for access to Home Folders:

Local (192.168.2.129:443) ▼

Custom Home Directory Path

Gateway Server: Not Selected

Home Folder Path: Not Selected

Sync: None ▼

- **Display the user's home folder**- This option causes a user's personal home directory to appear in the Access Mobile Client app.
 - **Display name shown on client** - Sets the display name of the home folder item in the Access Mobile Client app.
 - **Active Directory assigned home folder** - The home folder shown in the Access Mobile Client 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 Access Mobile Client 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. %USERNAME% must be capitalized.
 - **Sync** – This option selects the type of sync of your Home Directory.

3.2.1.7 Server Policy

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

Required Login Frequency for Resources Assigned by This Policy:

- Once Only, Then Save for Future Sessions
- Once per Session
- For Every Connection

Allow User to Add Individual Servers

Allow Saved Passwords for User Configured Servers

Allow File Server, NAS and Sharepoint Access From the Web Client

Allow User to Add Network Folders by UNC path or URL

Gateway Server used for access to user-configured Network Folders:

Local (192.168.2.129:443) ▼

Block access to specific network paths

Blocked Path List: ▼

[Add/Edit lists](#)
[Refresh lists](#)

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

Warn Client When Connecting to Servers with Untrusted SSL Certificates

Client Timeout for Unresponsive Servers: 30 seconds ▼

Allow User to Change This Setting

- **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 Access Mobile Client, the user is required to enter their password at the time they connect to the first server. Until they leave the Access Mobile Client application, they can then connect to additional servers without having to reenter their password. If they leave the Access Mobile Client 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 Access Mobile Client 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 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 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 Access Mobile Client app, check **Allow user to change this setting**.

3.2.2 Default Access Restrictions

This section allows you to set whether mobile clients need to be enrolled with the management server.

Group Policies Default Access Restrictions

Default Access Restrictions

Specify whether enrollment is required to connect to any Gateway Servers configured to use these default settings.

Require that client is enrolled with an Acronis Access server

Allowable Acronis Access Servers

192.168.2.130	^	- Remove
	v	
		+ Add

Save

3.3 On-boarding Mobile Devices

To get started with the Acronis Access app, users need to install it through the Apple App Store (iOS) or the Google Play Store (Android). Depending on your company's deployment of Acronis Access, the users may also need to enroll the Access Mobile app on their device with the Acronis Access Server. Once enrolled, their mobile client configuration, security settings, and capabilities are controlled by their Acronis Access management policy.

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

- Requiring an application lock password
- App password complexity requirements
- Ability to remove the Acronis Access app from management
- Allow Acronis Access on-device files to be included in iTunes backups
- Allow opening Acronis Access app files in other applications

- 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 Access Mobile Client app
- Assigned folders can be configured to perform 1-way to 2-way syncing with the server

In this section

Server-side Management Enrollment Process.....	44
User-side Management Enrollment Process	45

3.3.1 Server-side Management Enrollment Process

Enrollment Settings

Mobile Client Enrollment Address

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

Inviting a user to enroll

Users are typically invited to enroll with the Acronis Access Server with an email that is sent from an Acronis Access Administrator. 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 Acronis Access app in the Apple App Store or Google Play 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 Acronis Access and auto-complete the client enrollment form with the Acronis Access Server's name and the user's username. By using this link, a user simply enters their account password to complete client enrollment.

Using basic URL enrollment links:

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.

To generate a Acronis Access 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.
7. Choose the number of days you'd like the invitation to be valid for in the Number of days until invitation expires field.

Note: Acronis Access 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.

8. Choose the version or versions of the Access Mobile Client that you would like your users to download and install on their device. You may choose iOS, Android, or Both.
9. 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.

3.3.2 User-side Management Enrollment Process

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

- A link to install the Access Mobile Client from the Apple App Store.
- A link used to launch the Access Mobile Client app and automate the enrollment process.
- Their management server address.

- The email guides them through the process of installing the Access Mobile Client and entering their enrollment information.

From: **Access Administrator** <pam@glilabs.com>
Subject: Welcome to Acronis Access
Date: February 12, 2014 9:57:12 AM

[Hide](#)

pam@glilabs.com,

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

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

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

[Tap here to install Acronis Access for iOS \(iPad, iPhone, iPod Touch\)](#)

[Tap here to install Acronis Access 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 Acronis Access 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 Acronis Access app and tap the Menu button on your device.
3. Select "Settings", then tap "Enroll Now".
4. Enter the information below.

PIN: D34WNNQ

Server Address: 192.168.1.72:3000

Username: pam@glilabs.com

Password: enter your company password

Your enrollment PIN expires on Sat, 22 Feb 2014 14:59:10 +0200.

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 Acronis Access app.

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

For details on using Acronis Access, please visit the [Acronis Access Client User Guide](#).

For further assistance, please contact your IT department.

If the Access Mobile Client 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 Access will automatically launch and the enrollment form will be displayed. The user's server address and username are also encoded in this URL, so these fields are auto-completed in the enrollment form. At this point, the user simply has to enter 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 group policy, to access the Gateway server and if the policy allows it, the saving of their credentials for Acronis Access 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.

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 Access** link if you have not yet installed Acronis Access.
2. Once Acronis Access 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 and Username will be automatically filled out.
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 a application lock password is required for your Access Mobile Client app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

Manual enrollment

1. Open the Acronis Access app.
2. Open **Settings**.
3. Tap **Enroll**
4. Fill in your server's address, your 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**.

If a application lock password is required for your Access Mobile Client app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

Ongoing Management Updates

After the initial management setup, Access Mobile Clients 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.

Connectivity requirements

Acronis Access clients must have network access to the Acronis Access 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 Access, they will also need to connect to the VPN before management commands will be accepted.

Removing Management

There are two options to remove your Access Mobile Client from management:

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

Depending on your Acronis Access management policy settings, you may have the right to remove the Access Mobile Client 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 Access Mobile Client data is wiped when removing the device from management. You can cancel the process at this point if you don't want to be wiped.
4. Confirm removing Acronis Access from management by tapping **YES** in the confirmation window.

Note: If your Acronis Access management profile 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 Access Mobile Client application. Uninstalling the application will erase all existing Access Mobile Client data and settings and will return the user to default application settings after reinstalling.

To uninstall the Access Mobile Client app, follow the steps below:

1. Hold your finger on the Access Mobile Client app icon until it starts shaking.
2. Tap the "X" button on the Access Mobile Client application and confirm the uninstall process.
3. To reinstall the Access Mobile Client app, visit <http://www.grouplogic.com/web/meappstore>

3.4 Managing Your Gateway Server

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

The Acronis Access Server manages the Gateway Server 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 Access 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.

Search

Edit Server: Local ✕

General Settings
Logging
Search
SharePoint
Advanced

Index local data sources for filename search

Default Path for Search Indices

 Support content search using Microsoft Windows Search where available

OK
Apply
Cancel

Index local data sources for filename search

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.

Default path

By default on a standalone server, Acronis Access stores index files in the Search Indexes directory in the Acronis Access 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 is enabled by default, and can be enabled or disabled by checking this option. You can enable or disable content searching for each Gateway Server in the Edit Server dialog.

In addition to enabling this setting, content search requires that the Microsoft Windows Search application be installed on the Acronis Access Gateway server and be configured to index any data source where content search is enabled. Windows Search is built into Windows Vista and no additional installation is required. It is also built into Windows Server 2008, but it is not enabled by default. To enable it add the Role called **File Services** in the Server Manager, and have the Windows Search Service enabled. 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.

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.

In this section

Server Details	50
Editing Gateway Servers	53

3.4.1 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

Local



Status

Active Users

Display Name	Local
Address for administration	192.168.2.130:443
Address for client connections	192.168.2.130:443
Operating System	Microsoft Standard Edition, 64-bit
Gateway Server version	7.0.0x160
Status	Online
Last Contact	2014-11-11 18:09:58
Active Sessions	0
Licenses Used	0 of 100

Close

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

Local

Status

Active Users



User ▲	Location ◆	Device ◆	Model ◆	OS ◆	Client Version ◆	Policy ◆
fmedre	192.168.11.74:49325	T-Soft iPod touch 5G	iPod Touch 5G	iOS	6.1.0.158	Frank Medre
jprice	192.168.11.63:52087	iPad3	iPad 3 (WiFi)	iOS	6.1.0.158	John Price

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 Access 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.

3.4.2 Editing Gateway Servers

General Settings

Edit Server: Local ✕

General Settings Search SharePoint **Advanced**

Display Name Local

Address for administration access.mycompany.com

Address for client connections accessgw.mycompany.com

OK Apply Cancel

Display Name - Sets the display name of the Gateway Server.

Address for administration - Sets the address on which the Gateway Server is reachable by the Acronis Access Server.

Address for client connections - Sets the address on which mobile clients will connect to the Gateway Server.

Logging

Edit Server: Local

General Settings | **Logging** | Search | SharePoint | Advanced

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

Please consult the [documentation](#) for more information on where log files are located.

Audit Logging Archive Log File

Debug Logging

OK Apply Cancel

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 **Details** button.
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\Access\Gateway Server\Logs\AcronisAccessGateway**

1. Open the web interface.
2. Log in as an administrator.
3. Open the **Mobile Access** tab.
4. Open the **Gateway Servers** tab.
5. Find the server for which you want to enable **Debug Logging**.
6. Press the **Details** button.

7. In the **Logging** section check **Debug Logging**.
8. Press the **Save** button.

Search

The screenshot shows the 'Edit Server: Local' dialog box with the 'Search' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with five tabs: 'General Settings', 'Logging', 'Search', 'SharePoint', and 'Advanced'. The 'Search' tab is active and contains the following settings:

- Index local data sources for filename search
- Default Path for Search Indices: C:\Program Files (x86)\Acronis\Access\Gatew
- Support content search using Microsoft Windows Search where available

At the bottom right of the dialog are three buttons: 'OK', 'Apply', and 'Cancel'.

Index local data sources for filename search

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.

Default path

By default on a standalone server, Acronis Access stores index files in the Search Indexes directory in the Acronis Access 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 is enabled by default, and can be enabled or disabled by checking this option. You can enable or disable content searching for each Gateway Server in the Edit Server dialog.

In addition to enabling this setting, content search requires that the Microsoft Windows Search application be installed on the Acronis Access Gateway server and be configured to index any data source where content search is enabled. Windows Search is built into Windows Vista and no additional installation is required. It is also built into Windows Server 2008, but it is not enabled by default. To enable it add the Role called **File Services** in the Server Manager, and have the Windows Search Service enabled. 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.

SharePoint

Edit Server: Local ×

General Settings

Logging

Search

SharePoint

Advanced

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

Domain

Username

Password

Password Confirmation

OK

Apply

Cancel

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 2010):

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

The screenshot shows the SharePoint 2010 Central Administration web interface. At the top, there is a dark blue header with 'Site Actions' and 'Browse' buttons. The user is logged in as 'SHAREPOINT2010\administrator'. The main content area displays the Microsoft SharePoint 2010 logo and the navigation path 'Central Administration > Application Management'. On the left, a sidebar contains 'Central Administration' and 'Application Management' (highlighted). The main area shows 'Web Applications' with sub-links for 'Manage web applications' and 'Configure alternate access mappings'.

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

Name	URL
SharePoint - 21815	http://sharepoint2010.gililabs.com:21815/
SharePoint - 21816	http://sharepoint2010.gililabs.com:21816/
SharePoint - 2229	http://sharepoint2010.gililabs.com:2229/
SharePoint Claims - 23934	http://sharepoint2010.gililabs.com:23934/
SharePoint - 80	http://sharepoint2010/
SharePoint - 25054	http://sharepoint2010:25054/
SharePoint Central Administration v4	http://sharepoint2010:5869/
SharePoint - 13537	https://sharepoint2010.gililabs.com:13537/
SharePoint - 43224	https://sharepoint2010.gililabs.com:43224/

- 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**.

Zone	Display Name	User Name	Permissions
<input type="checkbox"/> (All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read
<input type="checkbox"/> (All zones)	Search Crawling Account	NT AUTHORITY\NETWORK SERVICE	Full Read
<input type="checkbox"/> (All zones)	SHAREPOINT2010\administrator	SHAREPOINT2010\Administrator	Full Read
<input checked="" type="checkbox"/> (All zones)	GLILABS\administrator	GLILABS\Administrator	Full Read

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

Edit Users

Users

The policy for these users will be modified.

Zone	User Name	Display Name
(All zones)	GLILABS\Administrator	GLILABS\administr

Permission Policy Levels

Choose the permissions you want these users to have.

Permissions:

- Full Control - Has full control.
- Full Read - Has full read-only access.
- Deny Write - Has no write access.
- Deny All - Has no access.

Choose System Settings

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

Account operates as System

Save **Cancel**

7. Press the **Save** button.

Advanced

Edit Server: Local



General Settings

Logging

Search

SharePoint

Advanced

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

Hide inaccessible items

Hide inaccessible items on reshares ⓘ

Hide inaccessible SharePoint sites

Minimum Android client version

Minimum iOS client version

2.0.0.282

Use Kerberos for SharePoint Authentication

Allow connections to SharePoint servers using self-signed certificates

Allow connections to Acronis Access servers using self-signed certificates

Allow connections from Acronis Access servers using self-signed certificates

Show hidden SMB Shares

Use user principal name (UPN) for authentication with SharePoint Servers ⓘ

Client session timeout in minutes

15

OK

Apply

Cancel

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 Access 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 Access 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 Access Windows server needs to be given permission to present delegated credentials to your SharePoint server on behalf of you users. Enabling the Acronis Access 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 Access . 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 propagat 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.
- **Allow connections to Acronis Access servers with self signed certificates** - When enabled, allows connections from this Gateway to Acronis Access servers using self-signed certificates.
- **Allow connections from Acronis Access servers with self signed certificates** - When enabled, allows connections to this Gateway from Acronis Access servers 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).

3.5 Managing Data Sources

You can share NTFS directories located on your Windows server or on a remote SMB/CIFS file share for access by Acronis Access users. When Acronis Access mobile users connect, they see these Data Sources as folders. You can create Data Sources that provide access to an Sync & Share server.

***Note:** With Acronis Access, you can have a total of **3** Data Sources located on remote locations. These locations include SharePoint sites, SharePoint libraries and SMB/CIFS shares.*

Access to SharePoint 2007, 2010, 2013, 365 content

Acronis Access can provide access to files residing in document libraries on SharePoint 2007, 2010, 2013 and 365 servers. An Acronis Access 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 Access also supports Check Out and Check In of SharePoint files.

SharePoint authentication methods supported

Acronis Access 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 Access server software. The Acronis Access 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 Access 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 a 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.

Changing Permissions for Shared Files and Folders

Acronis Access uses the existing Windows user accounts and passwords. Because Acronis Access 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 Access 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 the Access Mobile Client app. 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 Access as they receive when they access SharePoint document libraries using a web browser.

In this section

Folders.....62

3.5.1 Folders

In addition to Gateway Servers, Folders can also be assigned to Acronis Access user and group policies, allowing them to automatically appear in a user's Acronis Access Mobile client application. Folders can be configured to point to any Acronis Access Gateway Server, or even a subdirectory within a shared volume. This allows you to give a user direct access to any folders that might be important to them. By doing so, they don't have to navigate to the folder by knowing the exact server, shared volume name, and path to the folder.

Folders can point to any type of content that Acronis Access is providing access to. They simply refer to locations in Gateway Servers that have already been configured within the Acronis Access 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 or a SharePoint volume.

Note: When creating a DFS Data Source you need to add the full path to the DFS like so:

`\\company.com\namespace\share`

Folders can optionally be configured to sync to the client device. The Access Mobile Client folder sync options include:

- **None** - The folder will appear as a network-based resource in the Acronis Access client 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 Access client 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 Access client 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.

SharePoint Sites and Libraries

You can give easy access to SharePoint sites and libraries to your Access Mobile Client users by creating a Data Source. There are a couple of ways to create SharePoint Data Sources depending on your SharePoint configuration:

- 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**

- 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 Access Mobile Client 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 (p. 53) article.

Creating a Data Source

Add New Folder

Display Name: Marketing Project

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

Marketing Gateway (192.168.1.72:443)

Data Location: On the Gateway Server

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

Path: C:\Shares\Documents\Marketing Project

Sync: None

Show When Browsing Server

Require Salesforce.com Activity Logging 

Assign This Folder to a User or Group

Find User or Group that begins with john Search

Common Name / Display Name	Distinguished Name	Login Name
john	CN=john,CN=Users,DC=glilabs,DC=com	john

This folder is assigned to:

Common Name	Distinguished Name	
john	CN=john,CN=Users,DC=glilabs,DC=com	✕

To create a Data source:

1. Open the Acronis Access 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: 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 Access mobile clients browse the Gateway Server.
12. Press the Save button.

Note: On a clean installation of Acronis Access, 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.

4 Settings

Enrollment Settings

Mobile Client Enrollment
Address

192.168.2.130:2725

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

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 management, the Acronis Access app stores the address of the management 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.

5 Quick Start: Mobile Access

This guide provides the essential steps for configuring your Group Policy, adding a Data Source and installing the Access Mobile Client app. For more detailed instructions on configuring the Acronis Access Gateway Server and the management components, see the Mobile Access (p. 31) section.

In this section

First Run	67
Configuring your Group Policy	72
Installing the Access Mobile Client application	72
Enrolling in client management	72

5.1 First Run

If you haven't done so already, install and configure Acronis Access. For more information on doing so, check the Installing (p. 5) and Configuration Utility sections.

When you first open the web interface, you will have to set a password for the default administrator account and after you log in, you will be greeted by the **Setup Wizard**.

Warning! Please do not forget your administrator password as the support department cannot recover this password for you

Note: It may take 30-45 seconds until the application becomes available after starting it from the Configuration Utility.

Once you have completed the above, you are ready to go through the Initial Configuration described below.

General Settings

Server Settings

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://www.access.domain.com"/>
Mobile Client Enrollment Address	<input type="text" value="www.access.domain.com"/>
Use Custom Logo	<input type="checkbox"/>
Audit Log Language	<input type="text" value="English"/> ▼

1. Enter a Server Name.

2. Specify the root DNS name or IP address where users can access the website (starting with http:// or https://).
3. Specify the DNS name or IP address to which the mobile users will enroll to.
4. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
5. Press **Save**.

SMTP

SMTP

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

SMTP Server Address

SMTP Server Port

Use secure connection?

From Name

From Email Address

Use SMTP authentication?

Note: You can skip this section, and configure SMTP later.

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

LDAP

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

Require exact match

LDAP information caching interval

Note: You can skip this section, and configure LDAP later.

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. 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**)
8. Press **Save**.

6 Configuring your Group Policy

With the Group Policy, you can administer what your users can do with files and what they have access to.

Configuring your Group Policy:

1. Open the **Policies** tab.
2. Click on the **Default** policy.
3. Make the necessary configurations in each of the tabs (Security (p. 34), Application (p. 36), Sync (p. 39), Home Folders (p. 40) and Server (p. 41)) and press **Save**.

6.1 Installing the Access Mobile Client application

1. Browse to Acronis Access in the Apple App Store or Google Play store
 - From your iOS device, visit the Apple App Store and search for Acronis Access, or follow this link: <http://www.grouplogic.com/web/meapstore>
 - From your Android device, visit the Google Play store and search for Acronis Access, or follow this link: <https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho>
2. Install the Acronis Access app and tap it to launch it.
3. At the Welcome screen, tap Continue.
 - Tap the “+” icon on iOS to add a server.
 - On Android, open the **Settings** menu and tap **Add Server**.
4. Enter the Server Name or IP address of the server you installed Acronis Access on. You can optionally enter a Display Name for this server, which will appear in the server list.
5. Enter a Username that has access to the Gateway Server. Acronis Access uses standard NTFS permissions to regulate access.
6. Toggle **Save Password** to ON if you would like to save your password, then enter and confirm your password.
7. Tap **Save** to commit the server settings.
8. Tap the server listed in the left hand pane to connect and browse available volumes.
9. For full details on the Access Mobile Client application’s settings and features, visit the Mobile Client page.

6.2 Enrolling in client management

After installing Acronis Access with Mobile Access enabled, you can use the Access Mobile Client in two ways:

If your organization centrally manages the Access Mobile Client's access and settings, you will need to request access to Acronis Access from your IT department. You will receive an enrollment email once you have been granted access. The email includes the information and instructions you will need to start using the Access Mobile Client.

If your Acronis Access server allows access without your Access Mobile Client being centrally managed, you can get started by simply entering your Acronis Access server's name along with your username and password.

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

- A link to install the Access Mobile Client from the Apple App Store.
- A link used to launch the Access Mobile Client app and automate the enrollment process.
- Their management server address.

- The email guides them through the process of installing the Access Mobile Client and entering their enrollment information.

From: **Access Administrator** <pam@glilabs.com>
Subject: Welcome to Acronis Access
Date: February 12, 2014 9:57:12 AM

Hide

pam@glilabs.com,

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

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

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

[Tap here to install Acronis Access for iOS \(iPad, iPhone, iPod Touch\)](#)

[Tap here to install Acronis Access 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 Acronis Access 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 Acronis Access app and tap the Menu button on your device.
3. Select "Settings", then tap "Enroll Now".
4. Enter the information below.

PIN: D34WNNGQ

Server Address: 192.168.1.72:3000

Username: pam@glilabs.com

Password: enter your company password

Your enrollment PIN expires on Sat, 22 Feb 2014 14:59:10 +0200.

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 Acronis Access app.

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

For details on using Acronis Access, please visit the [Acronis Access Client User Guide](#).

For further assistance, please contact your IT department.

If the Access Mobile Client 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 Access will automatically launch and the enrollment form will be displayed. The user's server address and username are also encoded in this URL, so these fields are auto-completed in the enrollment form. At this point, the user simply has to enter 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 group policy, to access the Gateway server and if the policy allows it, the saving of their credentials for Acronis Access 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.

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 Access** link if you have not yet installed Acronis Access.
2. Once Acronis Access 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 and Username will be automatically filled out.
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 a application lock password is required for your Access Mobile Client app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

Manual enrollment

1. Open the Acronis Access app.
2. Open **Settings**.
3. Tap **Enroll**
4. Fill in your server's address, your 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**.

If a application lock password is required for your Access Mobile Client app, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.

Ongoing Management Updates

After the initial management setup, Access Mobile Clients 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.

Connectivity requirements

Acronis Access clients must have network access to the Acronis Access 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 Access, they will also need to connect to the VPN before management commands will be accepted.

Removing Management

There are two options to remove your Access Mobile Client from management:

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

Depending on your Acronis Access management policy settings, you may have the right to remove the Access Mobile Client 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 Access Mobile Client data is wiped when removing the device from management. You can cancel the process at this point if you don't want to be wiped.
4. Confirm removing Acronis Access from management by tapping **YES** in the confirmation window.

Note: If your Acronis Access management profile 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 Access Mobile Client application. Uninstalling the application will erase all existing Access Mobile Client data and settings and will return the user to default application settings after reinstalling.

To uninstall the Access Mobile Client app, follow the steps below:

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

To reinstall the Access Mobile Client app, visit <http://www.grouplogic.com/web/meappstore>

7 Quick Start: Sync & Share

This guide provides the essential steps for setting up Sync & Share, using the web interface to access files and using the Acronis Access desktop client. For more detailed instructions on configuring these components, see the Sync & Share and Desktop Client sections.

In this section

First Run	77
Web Client.....	82
Using the desktop client	89

7.1 First Run

If you haven't done so already, install and configure Acronis Access. For more information on doing so, check the Installing (p. 5) and Configuration Utility sections.

When you first open the web interface, you will have to set a password for the default administrator account and after you log in, you will be greeted by the **Setup Wizard**.

Warning! Please do not forget your administrator password as the support department cannot recover this password for you

Note: It may take 30-45 seconds until the application becomes available after starting it from the Configuration Utility.

Once you have completed the above, you are ready to go through the Initial Configuration described below.

General Settings

Server Settings

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://www.access.domain.com"/>
Mobile Client Enrollment Address	<input type="text" value="www.access.domain.com"/>
Use Custom Logo	<input type="checkbox"/>
Audit Log Language	<input type="text" value="English"/> 

1. Enter a Server Name.

2. Specify the root DNS name or IP address where users can access the website (starting with http:// or https://).
3. Specify the DNS name or IP address to which the mobile users will enroll to.
4. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
5. Press **Save**.

SMTP

SMTP

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

SMTP Server Address	<input type="text" value="mail.company.com"/>
SMTP Server Port	<input type="text" value="25"/>
Use secure connection?	<input checked="" type="checkbox"/>
From Name	<input type="text" value="Access Administrator"/>
From Email Address	<input type="text" value="administrator@company.com"/>
Use SMTP authentication?	<input type="checkbox"/>

Note: You can skip this section, and configure SMTP later.

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

LDAP

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

Require exact match

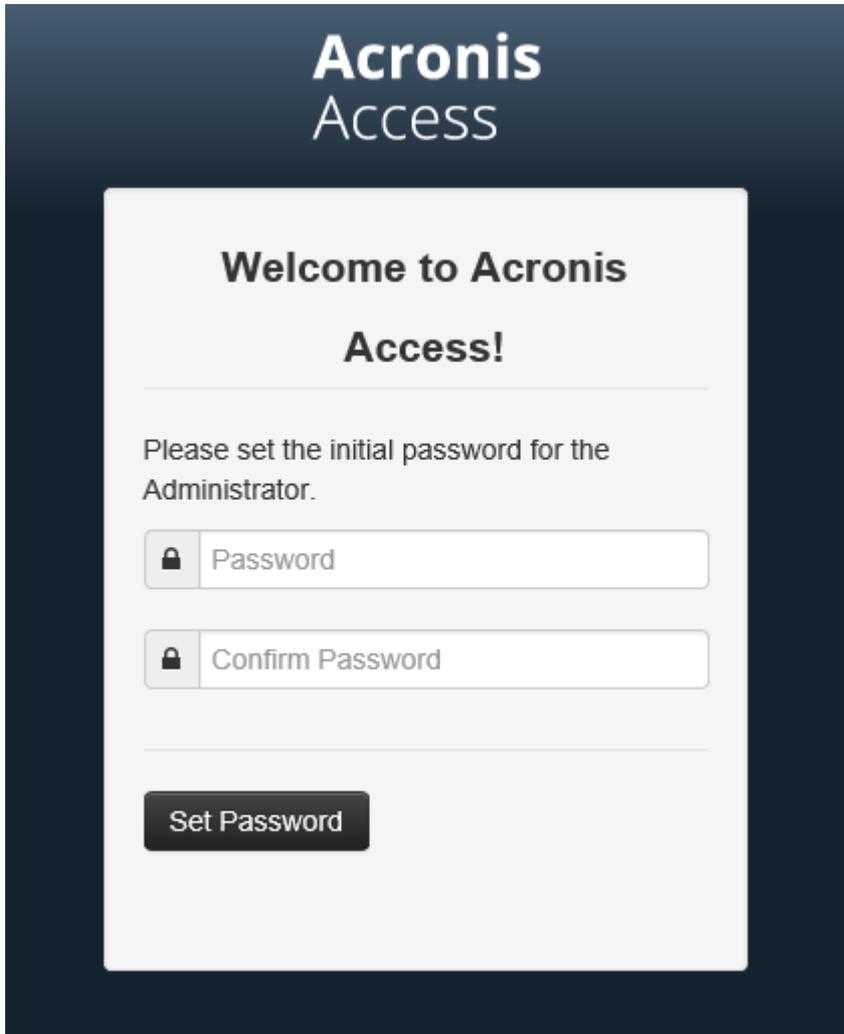
LDAP information caching interval

Note: You can skip this section, and configure LDAP later.

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

8 Web Client

1. Launch your web browser and navigate to: `https://myserver` `https://myserver`, where **myserver** is the URL or IP address of the computer running the Acronis Access server.



The screenshot shows the Acronis Access web client interface. At the top, the text 'Acronis Access' is displayed in white on a dark blue background. Below this, a white box contains the heading 'Welcome to Acronis Access!'. Underneath the heading, the text 'Please set the initial password for the Administrator.' is shown. There are two input fields: the first is labeled 'Password' and the second is labeled 'Confirm Password'. Both fields have a lock icon on the left. At the bottom of the white box, there is a dark grey button labeled 'Set Password'.

2. Login with your credentials.
 - a. If you have just installed the Acronis Access server, login as **administrator** with the password you set after the installation process. If this is the first time you open the web interface, you will be asked to set the password now.
 - b. If you received an email inviting you to Acronis Access you may need to **set your own personal password** at this point or log in using your Active Directory credentials.
 - c. If your Acronis Access server has been configured to use Active Directory for authentication and user account provisioning you should be able to login using valid network credentials.

Note: If you are logged in as the default administrator, you won't have access to the Web Client. You must use an account different from the default administrator.

Creating a folder

1. Click the **Create Folder** button and enter a name for the new folder. In this example we will use **Marketing Project**.

2. Press the **Save** button.

Sync & Share



Uploading files

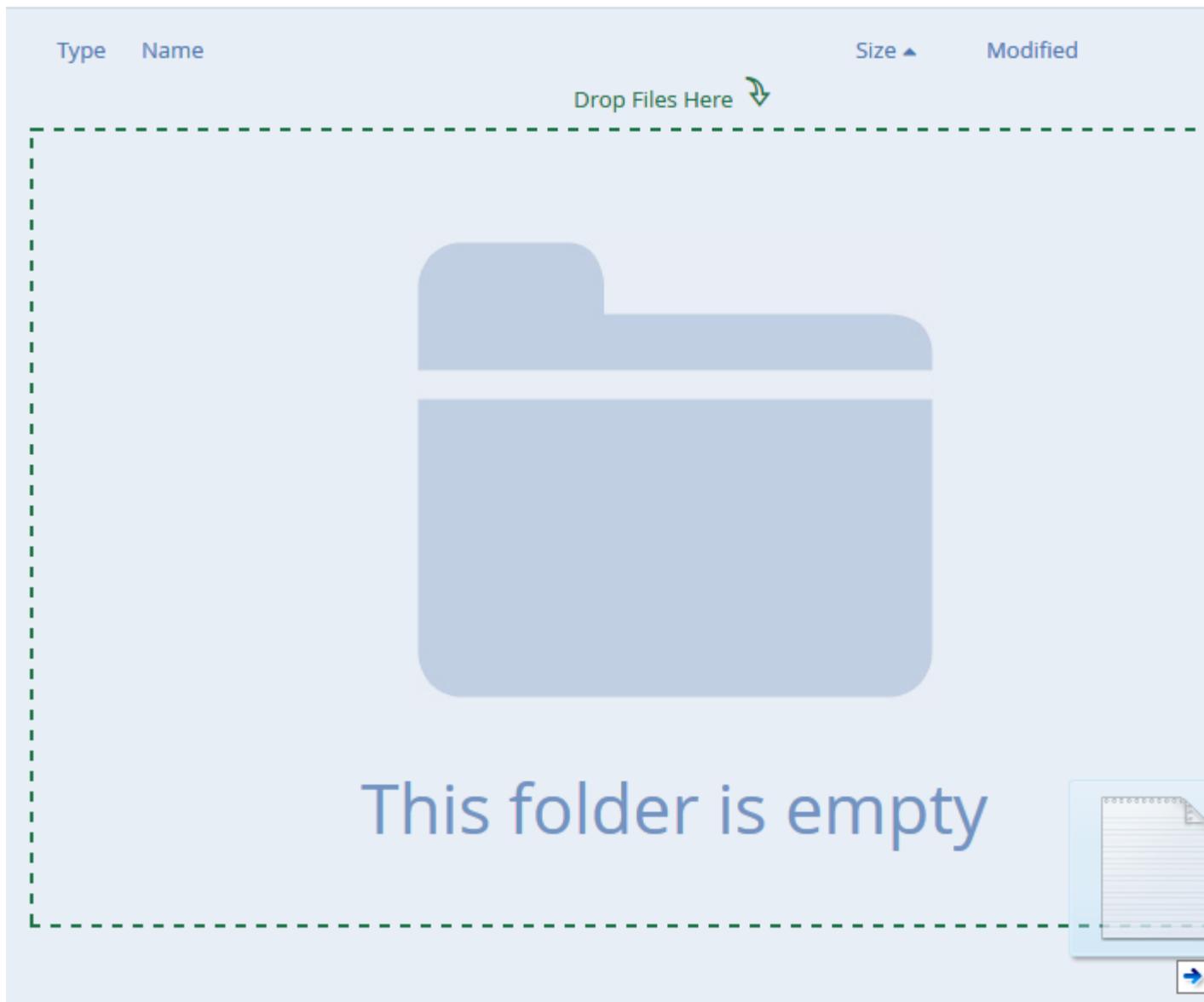
1. Navigate into the new folder by clicking its name.
2. Click the **Upload Files** button, click the **Add Files...** button and select a file or files from your computer.



3. The file(s) will be uploaded to the folder you are in. Press **Done**.

Another way of uploading files is simply dragging and dropping them to the web page:

Sync & Share > Marketing Project



Clicking on a file or folder shows the available actions in the right sidebar.



Download



Revisions



Rename



Copy



Move



Email Link



Get Link



Delete

Downloading a file

If you want to download a file, simply click on its name. You can also click on the row to the right of the file or folder name and press **Download** from the sidebar.

Note: When using Internet Explorer you have to make sure that **Do not save encrypted pages to disk** is unchecked in order to be able to download files. This setting is found under **Internet Options** -> **Advanced** -> **Security**.

Copying a file or folder

If you want to copy a file or folder, do the following:

1. Click on the row to the right of the file or folder name and select **Copy**.
2. In the new lightbox, navigate to the folder where you want to paste the file and press **Copy**.

Moving a file or folder

1. Click on the row to the right of the file or folder name and select **Move**.
2. In the new lightbox, navigate to the folder where you want to move the file and press **Move**.

Sharing a Folder

Note: If you want to share a file or folder that was shared with you by another user, you need to have the permissions to invite other users to that share. If you do not have the permissions to invite other users, you will not be able to share the files and folders with another user. The option **Sharing** in the right sidebar will not be visible as well.

To share a folder with a colleague or business partner, do the following:

1. Click on **Sync&Share**.
2. Click on the folder you want to share and select **Sharing** from the sidebar.



Download



Revisions



Rename



Copy



Move



Share



Delete

3. In the **Sharing** lightbox, enter an email address and an appropriate text message. An email containing your information and access instructions will be generated and sent to the recipient.

Invite to Marketing Project ✕

Invite members to this folder

Message (optional)

Allow editing and deletion
 Allow to invite other members
 Allow to view other members of this share

Invitation Language **English** ▾ **Share Folder**

Note: If the **Allow editing and deletion** check box is disabled, invited users can only download and read documents included in the shared folder.

Sharing a single file

Note: If you want to share a file or folder that was shared with you by another user, you need to have the permissions to invite other users to that share. If you do not have the permissions to invite other users, you will not be able to share the files and folders with another user. The option **Sharing** in the right sidebar will not be visible as well.

1. Open the Acronis Access Web Interface.
2. If you've logged in with an administrator account, press **Leave Administration** in the upper right corner.
3. Locate the desired file and click on the row next to its name.
 - a) **Sending a link via email**
 - a. Select **Send Link** from the sidebar.
 - b. Enter the desired expiration time and language for the invitation.
 - c. Enter the email address(es) of the user(s) you want to receive the download link.
 - d. Press **Send**.
 - b) **Sending a link via other methods**
 - a. Select **Get Link** from the sidebar.
 - b. Enter the desired expiration time and language for the invitation.

- c. Press **Copy Link**.
- d. Share the link via whatever method you prefer.

Subscribing to email notifications

You can subscribe to email notification alerts for folders shared with you.

1. To do so, simply enter the shared folder and click on **Notifications** in the sidebar.
2. Select the conditions you want to be notified for and press **Save**.

Manage Notifications ✕

Default Notifications

Emails Frequency minutes

- Notify when files are downloaded
- Notify when files and folders are added
- Notify when files and folders are updated
- Notify when files and folders are deleted
- Notify when users are invited or removed
- Notify when errors occur

You can look at the history of events by opening the **Log** tab. Search and filter options are available. Event importance is marked with different colors.

Log

Timestamp ▲	Type	User	Message	Filter
2014-11-11 18:07:53	Info		Removed share 'Marketing Project' because there were no members.	Type All
2014-11-11 18:07:52	Info	John Price <john.price@glilabs.com>	Added new share 'Marketing Project'.	Search Te
2014-11-11 18:06:39	Info	John Price <john.price@glilabs.com>	Added new file 'ExtremeZ-IP README.txt'.	
2014-11-11 18:05:28	Info	John Price <john.price@glilabs.com>	Added new folder 'Marketing Project'.	
2014-11-11 18:04:55	Info	John Price <john.price@glilabs.com>	Added new file 'Acronis Access 6.0.doc'.	
2014-11-11 18:03:04	Info	John Price <john.price@glilabs.com>	Deleted file "Access 7 Thumbnails.docx".	
2014-11-11 18:02:58	Info	John Price <john.price@glilabs.com>	Restored file 'Access 7 Thumbnails.docx' => 'Access 7 Thumbnails.docx'.	

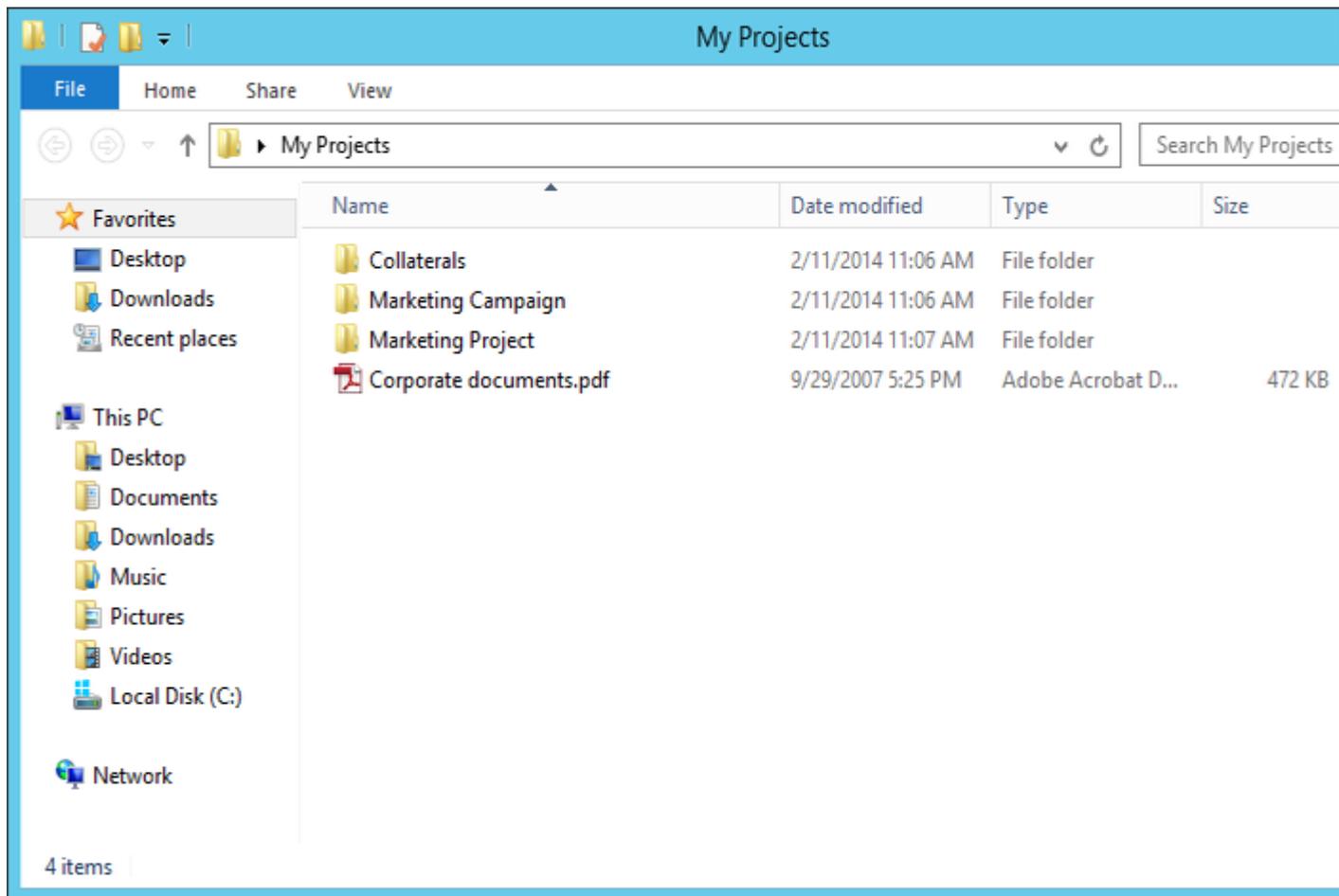
8.1 Using the desktop client

First Steps

Note: If you haven't installed your Acronis Access Desktop Client yet, you can do so by following the *Client Installation and Configuration guide*.

1. Open the folder you selected for syncing during the configuration process. This is just a normal folder, so instead of calling it Sync Folder you should use more regular names. In this example we named it **My Projects**.
2. Create a folder named **Marketing Campaign** inside **My Projects**.
3. Create a text document inside **My Projects**, fill it with text, and then save and close it.

4. Create another folder inside **My Projects** with a name **Collaterals**.

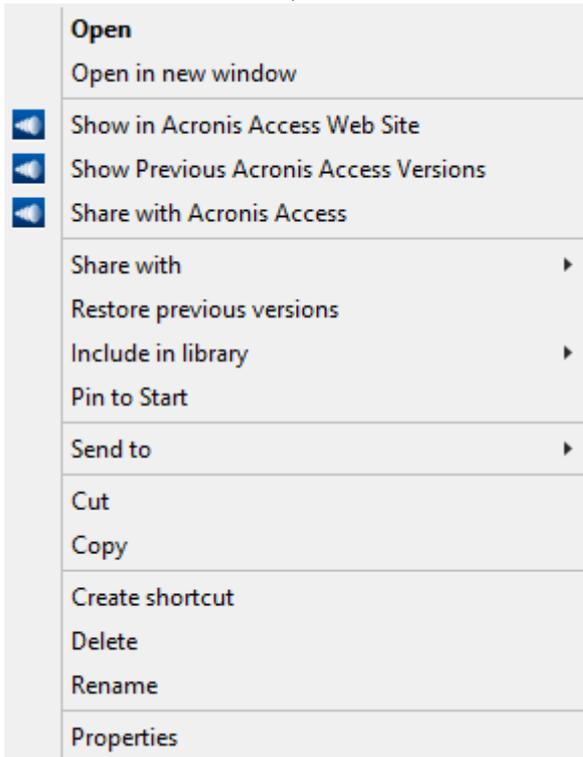


5. Place some files into it by copying them from your computer.
6. Now it's time to share a folder with a colleague. You can do this in two different ways: directly from Windows Explorer or using your web browser. Follow step 7 to share content from your desktop using Windows Explorer, or follow step 8 to share content using your preferred web browser.

Note: You can also share just a single file as described at the bottom of this article.

7. If you want to do it right from your desktop, select the **Marketing Campaign** folder

- a. Right Click on it.
- b. From the context menu, select **Share with Acronis Access**



- c. This will launch a web browser and show you the invite dialog.
- d. In the **Invite others** dialog enter an email address and an appropriate text message.

Invite to Marketing Project ✕

Invite members to this folder

Message (optional)

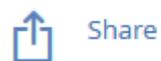
Allow editing and deletion
 Allow to invite other members
 Allow to view other members of this share

Invitation Language **English** ▾

Share Folder

If you prefer to use your web browser instead:

1. Open <https://server.com/> <https://server.com/>, where **server.com** is the Acronis Access server address, and log in using your username and password credentials.
2. Click on **Sync&Share**.
3. Click on the folder you want to share and select **Sharing** from the sidebar.



4. In the **Sharing** lightbox, enter an email address and an appropriate text message. An email containing your information and access instructions will be generated and sent to the recipient.

Invite to Marketing Project ✕

Invite members to this folder

✕

Message (optional)

John, this is the project we are working on. Please make any changes to the documents included as needed.

Allow editing and deletion
 Allow to invite other members
 Allow to view other members of this share

Invitation Language **English** ▾

Share Folder

Note: If the **Allow editing and deletion** check box is disabled, invited users can only download and read documents included in the shared folder.

Regardless of the method used to invite a person, the recipient will then receive one or two emails, depending on whether he is an internal (Active Directory) or external user.

- a. For an external user, the first email with subject **You have been invited to Acronis Access** contains a link to set a personalized password.
- b. The second email with subject **You have been given access to Marketing Campaign** contains your message and a link for accessing the shared files.

Once the invited user clicks on the link to access the system (and set his password if needed) you and your colleague will share access over the files in the **Marketing Campaign** folder.

Make sure you tell your colleague about the Access Desktop Client, so you can synchronize files automatically among your computers.

1. **Note:** The maximum path length is different between Mac OS X and Windows which can lead to syncing errors in cross platform deployments. On Windows there is an OS limitation of 260 characters (MAX_PATH) total for the entire path, including the "**C:\mysharefolder**" part. So on Windows the max filename length will be $260 - [\text{share folder path length}] - 1$ (for NULL terminator).

e.g. The user is sharing C:\my_shared_documents and is trying to download a file into C:\my_shared_documents\this_is_a_folder\ the max file name length of that subdirectory would be $260 - 40 - 1 = 219$ characters. The Mac OS X limit is 1024 characters.

9 Server Administration

In this section

Administering a Server.....	94
Administrators and Privileges	95
Audit Log	97
Server	99
SMTP	101
LDAP	102
Email Templates.....	104
Licensing.....	106
Debug Logging.....	107
Monitoring	108

9.1 Administering a Server

If you are an administrator logging in to the web interface takes you directly to into **Administration** mode. After you log in you can switch between **Administration** and **User** modes.



To switch between modes, do the following:

1. Open the web interface and log in as an administrator.
 - To exit administration, press the **Leave Administration** button at the top-right. This takes you to the user side of the web interface.
 - To go back into administration, press the **Administration** button at the top-right. This will take you back into administration mode.

Note: Administrators have access to the API documentation. You can find the link in the footer of the Access web interface.

9.2 Administrators and Privileges

Provisioned LDAP Administrator Groups

Provisioned LDAP Administrator Groups

Add Pr

Members of groups listed here will have their user accounts automatically created at first login and will be given administrative access for as long as they are members of a provisioned administrator group.

LDAP Group	Full Rights	Manage Users	Manage Mobile Data Sources	Manage Mobile Policies	View Audit Log
CN=Administrators,CN=Builtin,DC=t-soft,DC=biz	✓	✓	✓	✓	✓
CN=Users,CN=Builtin,DC=t-soft,DC=biz	✓	✓	✓	✓	✓

50 per page ▾

Show



This section allows you to manage your administrative groups. Users in these groups will automatically receive administrative privileges.

Using the **Actions** button you can delete or edit the group.

To add a provisioned LDAP administrator group:

Add Provisioned LDAP Administrator Group ×

Selected group:

Administrative Rights

- Full administrative rights?
- Can manage users?
- Can manage mobile data sources?
- Can manage mobile policies?
- Can view audit log?

Search for an LDAP group and click on the Common Name to select it as a Provisioned Administrators LDAP Group.

Find group that

Add

Cancel

1. Press the **Add Provisioned Group**.
2. Mark if the group should have Sync & Share functionality.
3. Find the group.
4. Click on the group name.
5. Press **Save**.

Administrative Users

This section lists all your Users with administrative rights, their authentication type (Ad-Hoc or LDAP), whether they have Sync & Share rights and their status (Disabled or Enabled).

You can invite a new user with full 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 Access Web Interface.
2. Log in with an administrator account.
3. Expand the **General Settings** tab and open the **Administrators** page.

4. Press the **Add Administrator** button under **Administrative Users**.
 5. Select either the Active Directory/LDAP or Invite by Email tab depending on what type of user you are inviting and what you want them to administer. LDAP users without emails cannot be given Sync & Share functionality.
- a) **To invite via Active Directory/LDAP do the following:**
1. Search for the user you want to add in the Active Directory and then click on their Common Name to select a user.
-
- Note:** *The LDAP User and Email fields will fill in automatically.*
-
2. Enable/Disable the Sync & Share functionality.
 3. Select which administrative rights the user should have.
 4. Press Add.
- b) **To invite by Email do the following:**
1. Enter the email address of the user you want to add as an administrator.
-
- Note:** *Ad-hoc users invited by email will always have Sync & Share functionality.*
-
2. Select whether this user should be licensed.
 3. Select the language of the Invitation email.
 4. Press Add.

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 **Full Administrative Rights?**
6. 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.

- **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.

To enable Audit Logging for a specific gateway server:

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

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

9.3.2 Settings

Acronis Access 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.
 - **Export file path** - Sets the folder where the exported logs will go.

9.4 Server

Server Settings

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://192.168.1.72:3000"/>
Color Scheme	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="Dark Blue"/> ▼
Audit Log Language	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="English"/> ▼
Session Timeout in Minutes	<input type="text" value="15"/>
Enable Sync and Share Support	<input checked="" type="checkbox"/>

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 and Japanese**. The default is **English**.
- **Session timeout in minutes** – sets the length of the user session.
- **Enable Sync and Share Support** - this checkbox enables/disables the Sync and Share features.

Notifications

If enabled, notifications will be sent using the configured **SMTP settings**.

Email administrator a summary of errors?

Email Addresses

Notification Frequency mins

Notification Settings

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

9.5 SMTP

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

SMTP

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

SMTP Server Address

SMTP Server Port

Use secure connection?

From Name

From Email Address

Use SMTP authentication?

Save

Send Test Email

- **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?** - enable the option to use a secure SSL connection to your SMTP server. This setting is enabled by default. Uncheck the box to disable secure SMTP.
- **From Name** - this is the username that appears in the "From" line in emails sent by the server.
- **Use SMTP authentication?** - enable to connect with a SMTP username and password or disable 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

9.6 LDAP

Microsoft Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Other Active Directory products (i.e. Open Directory) are not supported at this time.

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication
 Require exact match

LDAP information caching interval

Proactively Resolve LDAP Email Addresses

Use LDAP lookup for type-ahead suggestions for invites and download links.

Include nested distribution group membership

- **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.
- **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. (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 Access 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 Access is caching the Active Directory structure.
- **Proactively resolve LDAP email addresses** - When this setting is enabled, Acronis Access 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.

9.7 Email Templates

Acronis Access 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 Access 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 ERB, embedded Ruby. Please review the default templates to determine how best to customize your templates.

- **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).

- **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.

Email Templates

All emails sent by the Acronis Access server can be customized to meet your needs. For each email, you will need to provide HTML and text-formatted email templates. Template bodies must be written in **ERB, embedded Ruby**. Please review the available templates to determine how best to customize your templates.

Select Language:

Select Email Template:

Available Parameters

- @invitation.email - User's email address
- @invitation.pin - User's PIN
- @invitation.display_name - User's display name
- @management_server_address - Acronis Access server address
- @expiration - PIN expiration date
- @url - Acronis Access URL
- @invitation.user - Username (User principal name)
- @app_name - App name ("Acronis Access" or "Acronis Access for Good Dynamics")
- @is_good - True if application is for Good Dynamics
- @send_ios_instructions - True if invitation should contain iOS instructions
- @send_android_instructions - True if invitation should contain Android instructions
- @locale - Locale code for this template

Email Subject

[View Default](#)

To use parameters in the subject, surround the parameter name with # {}, e.g. #{parameter_name}

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.

Select Email Template: 

Available Parameters

- @user** - User whose password is being reset
- @passkey** - Passkey to take user to password reset page
- @passkey_expiration** - Number of days after which the passkey will expire (or nil if n
- @root_web_address** - The URL to reach the Acronis Access server
- @locale** - Locale code for this template

Note: Pressing the **View Default** button will show you the default template.

Make sure you click the **Save Templates** button when you finished modifying your templates.

9.8 Licensing

Licensing

Licensing

License:	Trial
Clients:	500
Current Licensed Client Count:	0
Current Free Client Count:	1
Expiration Date:	2014-03-04

I understand the details and scope of my license may be found on my invoice and at <http://www.acronis.com/compan>

You will see a list of all your licenses.

- **License** - Type of the license (Trial, subscription etc).
- **Clients** - Maximum number of allowed licensed users.
- **Current Licensed Client Count** - Number of currently used user licenses.
- **Current Free Client Count** - Number of free users currently in the system.

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: The supported licensed client counts are 50 and 100. If you've bought a 50 user license, you can upgrade it to a 100.

Note: You can upgrade your instance of Acronis Access to Acronis Access Advanced by using a Acronis Access Advanced license key. All your current settings and configurations will be saved.

9.9 Debug Logging

Settings in this page are designed to enable extended logging information that might be useful when configuring and troubleshooting Acronis Access. 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 [Server Details \(p. 50\)](#) article.

Debug Logging

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

Please consult the [documentation](#) for more information on where log files are located.

General Debug Logging Level

Enabled debug modules always log at the debug level, regardless of the general debug logging level above.

Available Debug Modules

active_record
cluster
comet
exceptions
expiration
invitations
ldap
ldap_caching

Add +

- Remove

- Remove All

Enabled Debug Modules

authentication
encryption

Save

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 Access, the log files will be in **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.42\logs**

9.10 Monitoring

The performance of this server can be monitored using New Relic. If you would like to monitor this server, please enable monitoring and provide the path to your New Relic YML file. To obtain a New Relic YML file, you will need to create an account with New Relic.

Monitoring

The performance of this server can be monitored using [New Relic](#). If you would like to monitor this server, please enable monitoring and provide the path to your New Relic YML file. To obtain a New Relic YML file, you will need to create an account with [New Relic](#).

It is highly recommended not to put your New Relic YML file into the Acronis Access server directories to avoid having your file accidentally removed or altered on upgrade or uninstall.

If you make changes to your New Relic YML file, or change New Relic YML files, you will need to restart the Acronis Access Tomcat service for the changes to take effect.

Enable New Relic monitoring?

New Relic YML Path

E.g., c:\path to file\newrelic.yml. Make sure the user Tomcat is running as has read access to this file.

Note: It is highly recommended not to put your New Relic YML file into the Acronis Access 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 Access Tomcat service for the changes to take effect.

Enable New Relic monitoring? - If enabled, you are required to provide a path to the **New Relic** configuration file (newrelic.yml)

Installing New Relic

This type of installation will let you monitor your Acronis Access Server application, not the actual computer on which it is installed.

1. Open <http://newrelic.com/> and create a New Relic account.
2. For Application type select Mobile app.
3. For Platform mark Ruby.
4. Finish creating your account and log in.
5. Go to Applications, leave the **ruby bundle**(step 1) as is and continue to the next step.
6. Download the New Relic script - newrelic.yml.
7. Open your Acronis Access web UI.
8. Go to Settings and click on Monitoring.

9. 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 Access folder so that it will not be removed or altered on upgrade or uninstall.
10. Click Save and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
11. If more than 10 minutes pass, restart your Acronis Access Tomcat service and wait a couple of minutes. The button should be active now.
12. You should be able to monitor you Acronis Access server via the New Relic website.

*All the information the Acronis Access 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.*

There is frequently a warning/error that starts like this:

WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which

That's a side effect of the code used to patch another New Relic bug and is innocuous.

If you want to monitor the actual computer as well

1. Open <http://newrelic.com/> and log in with your account.
2. Press Servers and download the New Relic installer for your operating system.
3. Install the New Relic monitor on your server.
4. The New Relic server monitor requires Microsoft .NET Framework 4. The link the New Relic installer takes you to is only for the Microsoft .NET Framework 4 Client Profile. You will need to go to the Microsoft Download Center and download the entire .NET 4 Framework from the internet and install it before running the New Relic Server Monitor installer.
 - Wait until New Relic detects your server.

10 Supplemental Material

In this section

Conflicting Software	110
Using trusted server certificates with Acronis Access	110
Changing the Acronis Access Tomcat SSL Ciphers	112
How to support different Access Desktop Client versions.....	113
Customizing the web interface	113
Creating a Drop Folder.....	114
Monitoring Acronis Access with New Relic.....	115
Third-party Software for Acronis Access.....	116

10.1 Conflicting Software

There are some software products that may cause problems with Acronis Access. The currently known conflicts are listed below:

- **VMware View™ Persona Management** - This application will cause issues with the Acronis Access desktop client syncing process and issues with deleting files. Placing the Acronis Access sync folder outside of the **Persona Management user profile** should avoid the known conflicts.

10.2 Using trusted server certificates with Acronis Access

This section explains how to configure Acronis Access with trusted server certificates. By default, Acronis Access will use a self-generated SSL certificate. Using a certificate signed by a trusted Certificate Authority will establish the identity of the server and allow browsers to connect without displaying a warning message that the server is untrusted.

Note: *Acronis Access 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 recommended.*

Creating a certificate request

Note: *Creating certificates is not and will never be a function of Acronis Access. This certificate request is in no way necessary for the operation of Acronis Access but it is required by Certificate vendors.*

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](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
```

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 OPENSSE_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 your 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.

Installing your certificate to your Windows certificate store

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 Access Configuration Utility.

Configure Acronis Access to use your certificate

After you've successfully installed your certificate to your certificate store, you have to configure Acronis Access to use that certificate.

1. Launch the Acronis Access Configuration Utility.

Note: Located in **C:\Program Files (x86)\Acronis\Access\Configuration Utility** by default.

2. Select your certificate from the Certificate selector on the **Gateway Server** and **Access Server** tabs.
3. Click **Apply**.

The web services will restart and after about a minute they should be running with your certificate.

10.3 Changing the Acronis Access Tomcat SSL Ciphers

Changing the ciphers:

This procedure is necessary only if you wish to use a custom set of SSL ciphers. You might want to do so to support the web interface on Internet Explorer 8 or the Acronis Access Desktop client on Windows XP but It is not recommended. Changing the ciphers might expose your server to vulnerabilities and is generally unsecure.

1. Navigate to your Acronis Access Tomcat installation folder (e.g. **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.55\conf**).
2. Make a copy of your **server.xml** file before editing it.
3. Open the **server.xml** file.
4. Find this line: **SSLCipherSuite=""**
5. Replace the contents between the two quotation marks with the ciphers you wish to use.

Note: If you wish to support an unsecure version of Internet Explorer 8 or the Acronis Access Desktop client on Windows XP, enter the following:

ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

e.g.:

SSLCipherSuite="ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"

6. Save the changes made to the **server.xml** file and restart the Acronis Access Tomcat service.

10.4 How to support different Access Desktop Client versions

If you want to use a version of Access Desktop Client which is different from the latest, follow these steps:

1. Download the version of Access Desktop Client which you want to use. Make sure you have these 4 files:
 - AcronisAccessMac.zip
 - AAClientInstaller.msi
 - AcronisAccessInstaller.dmg
 - AcronisAccessClientInstaller.exe
2. Copy the files.
3. On the server, open the Access Desktop Clients folder (**C:\Program Files (x86)\Acronis\Access\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. **2.7.0x167**, **2.6.0.x140**, **2.7.1x145**).
5. Paste the 4 files in the sub-folder you just created.
6. Next, open the **Web User Interface** of your Acronis Access server.
7. Log-in as an **administrator** and go to the **Sync & Share** tab and open the **Acronis Access 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 Access Desktop Client version. If you do not want the users to download the latest version, go to the **\Acronis\Access\Access Server\Web Application\clients** folder and rename the latest client version (e.g. **3.0.3x102**) folder to "**do not use version number**" (e.g. "**do not use 3.0.3x102**").

10.5 Customizing the web interface

Acronis Access allows for the web based user interface to be modified to satisfy branding and look and feel requirements. The logo can be changed to permit customers to better integrate the solution with their corporate standards.

To add a custom logo:

1. Open the web interface and navigate to **General Settings -> Server**.
2. Select **Use Custom Logo** and select the desired image. The file must be a JPEG or PNG, with a minimum width of 160 pixels. To select another image, click on Custom Logo, pick **New...** from the drop down menu and select a new image file.
3. Press **Save**.

Note: Custom Logo images are stored in the **Web Application\customizations** folder, generally found at: **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\customizations**. These files are retained on Acronis Access upgrades.

Note: Copyright notices, logos and elements at the bottom (footer) of each web page must not be modified or eliminated without Acronis's explicit consent.

10.6 Creating a Drop Folder

This guide will cover setting up a Drop Folder using Acronis Access and Windows Active Directory. A Drop Folder is a folder in which certain users can only add new files and folders (without the ability to edit or delete any of the files) while other users have full control.

In the Active Directory, do the following:

1. Either select two existing LDAP groups or create two new groups. One will be used for the superusers (e.g. Group A is for Administrators, Teachers, Doctors) while the other will be for the drop-only users (e.g. Group B is for Clients, Students, Patients).
2. For each group add the desired members.

On the machine where the Drop Folder will reside, do the following:

Creating the Drop Folder

1. Create a new folder. This will be your Drop Folder.
2. Right-click on the folder and select **Properties**.
3. Click on the security tab and press **Edit**.
4. On the new window press **Add**, enter the name of the group you want to add and press **OK**. Do this for both LDAP groups and for the **Creator Owner** group.
5. Press **OK** to close the new window and return to the **Security** tab.

Setting the permissions

On the **Security** tab, press **Advanced** and on the **Advanced Security Settings** window press **Change Permissions...**

For the superuser group

Press **Edit** and under **Allow**, mark the following permissions:

- **Traverse Folder/Execute File**
- **List Folder/Read Data**
- **Read Attributes**
- **Read Extended Attributes**
- **Create Files/Write Data**
- **Create Folders/Append Data**
- **Write Attributes**
- **Write Extended Attributes**
- **Delete**
- **Read Permissions**

For the drop-only users

Press **Edit** and under **Allow**, mark the following permissions:

- **List Folder/Read Data**
- **Create Files/Write Data**
- **Read Permissions**

For the Creator Owner group

Press **Edit** and under **Allow**, mark the following permissions:

- **Delete**

In the Acronis Access Server web interface, do the following:

1. Expand the **Mobile Access** tab and open the **Policies** page.
2. Press **Add Group Policy**.
3. For the superuser group (Group A), fill out all policy tabs per your company's requirements. For more information visit the Policies (p. 33) section.
4. For the drop-only group (Group B), fill out all policy tabs per your company's requirements. On the **Application Policy** tab, select only the following actions:
 - **File Copies / Creation**
 - **File Deletes**
 - **Folder Copies**
 - **Sending Files to Acronis Access from Other Apps**
 - **Sending Files to Acronis Access Using Quickoffice 'Save Back'**

Done! Your Drop Folder is now configured and ready for use.

10.7 Monitoring Acronis Access with New Relic

This type of installation will let you monitor your Acronis Access Server application, not the actual computer on which it is installed.

1. Open <http://newrelic.com/> and create a New Relic account.
2. For Application type select Mobile app.
3. For Platform mark Ruby.
4. Finish creating your account and log in.
5. Go to Applications, leave the **ruby bundle**(step 1) as is and continue to the next step.
6. Download the New Relic script - newrelic.yml.
7. Open your Acronis Access web UI.
8. Go to Settings and click on Monitoring.
9. 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 Access folder so that it will not be removed or altered on upgrade or uninstall.
10. Click Save and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.

11. If more than 10 minutes pass, restart your Acronis Access Tomcat service and wait a couple of minutes. The button should be active now.
12. You should be able to monitor you Acronis Access server via the New Relic website.

All the information the Acronis Access 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.

There is frequently a warning/error that starts like this:

WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which

That's a side effect of the code used to patch another New Relic bug and is innocuous.

If you want to monitor the actual computer as well

1. Open <http://newrelic.com/> and log in with your account.
2. Press Servers and download the New Relic installer for your operating system.
3. Install the New Relic monitor on your server.
4. The New Relic server monitor requires Microsoft .NET Framework 4. The link the New Relic installer takes you to is only for the Microsoft .NET Framework 4 Client Profile. You will need to go to the Microsoft Download Center and download the entire .NET 4 Framework from the internet and install it before running the New Relic Server Monitor installer.
5. Wait until New Relic detects your server.

10.8 Third-party Software for Acronis Access

In this section

PostgreSQL	116
Apache Tomcat	117
New Relic.....	117

10.8.1 PostgreSQL

Acronis Access Server uses PostgreSQL as it's database storage.

Documentation on the latest PostgreSQL <http://www.postgresql.org/docs/9.2/interactive/index.html> (for other versions visit this site <http://www.postgresql.org/docs/manuals/>).

List of error codes <http://www.postgresql.org/docs/9.2/interactive/errcodes-appendix.html>.

When installing Acronis Access server, by default you also install pgAdmin. It provides a graphical user interface to PostgreSQL. For documentation on all versions of pgAdmin visit this site <http://www.pgadmin.org/docs/>.

Useful information can be found at the PostgreSQL Wiki http://wiki.postgresql.org/wiki/Main_Page, including a troubleshooting guide http://wiki.postgresql.org/wiki/Troubleshooting_Installation.

For anti-virus related problems check this article

http://wiki.postgresql.org/wiki/Running_&_Installing_PostgreSQL_On_Native_Windows#Antivirus_software.

For information on backing up a PostgreSQL database: PostgreSQL backup.

10.8.2 Apache Tomcat

Acronis Access Server uses ApacheTomcat for its web server. Acronis Access 2.7 and later installs its own version of Tomcat into the Group Logic\Common or Acronis\Common folder.

Troubleshooting Tomcat Wiki <https://wiki.openmrs.org/display/docs/Troubleshooting+Tomcat>.

Troubleshooting from the Apache website

<http://commons.apache.org/logging/troubleshooting.html>.

10.8.3 New Relic

New Relic is an on-demand application monitoring and optimization solution that can identify and resolve performance issues for Ruby, JRuby, Java, PHP and .NET applications. Monitor, troubleshoot and tune production web apps 24x7. New Relic includes Real User Monitoring (RUM) to analyze user requests in real time, offering insights about user experience including page load times, time in request queue, how long a page takes to render, and Apdex score. In addition, New Relic includes dashboard to visualize performance metrics by geography, by longest time in queue, throughput, and so on.

By using New Relic, you can monitor your Acronis Access server's activity in real time in an easy and user friendly way.

For more information visit <http://newrelic.com/> <http://newrelic.com/>

For information on installing New Relic for your Acronis Access server, visit the Monitoring Acronis Access with New Relic (p. 115) section.

11 Sync & Share

In this section

Sharing Restrictions	118
LDAP Provisioning	118
Quotas.....	119
File Purging Policies.....	119
User Expiration Policies.....	121
File Repository.....	122
Acronis Access Client.....	123

11.1 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.

Single File Sharing Expiration

Prevent User from Sharing Files with Infinite Expiration - If this setting is disabled, user will be able to share single files and the link will never expire. If enabled, users sharing single files must set expiration days for each link.

- **Minimum Expiration Time** - Controls the minimum amount of time (in days) that the users can set.
- **Maximum Expiration Time** - Controls the maximum amount of time (in days) that the users can set.

11.2 LDAP Provisioning

LDAP Provisioning

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

LDAP Group

CN=Administrators,CN=Builtin,DC=gililabs,DC=com

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

Find group that begins with Search

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

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.

11.3 Quotas

Administrators can set the amount of space dedicated to each user in the system.

Quotas

Enable Quotas?

Ad-hoc User Quota GB

LDAP User Quota GB

Enable admin-specific quotas?

Admin Quota GB

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.
 - **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.

11.4 File Purging Policies

In Acronis Access, 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 Access 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.

File Purging Policies

Acronis Access 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 Access. 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 months

Purge previous revisions older than months

Keep at least revisions per file, regardless of age

Only keep revisions per file

Save

Purge scans run automatically every 60 minutes. However, you may [click here](#) to save your settings and run a purge scan immediately.

Acronis Access 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 Access. 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.

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

11.5 User Expiration Policies

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

User Expiration Policies

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

Delete passkeys after days

Delete pending invitations after days

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

Delete adhoc users who have not logged in for days

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

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

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

Save

- **Delete passkeys after X days** - If enabled, deletes all passkeys after a set number of days.
- **Delete pending invitations after X days** - If enabled, deletes all pending invitations 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 adhoc users who have not logged in for X days** - If enabled, deletes adhoc 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.

11.6 File Repository

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

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 Access Server. The Acronis Access Configuration utility is used to set the file repository address, port and file store location. The store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the [documentation](#).

File Store Repository
Endpoint

Encryption Level

File Store Low Disk
Space Warning
Threshold

File Store Status: Free space for
file store <http://127.0.0.1:5787> =
52 GB (52055752704 bytes)

Please go to **Server Settings** to configure admin notifications.

Save

- **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-128.
- **File Store Low Disk Space Warning Threshold** - After the free space goes below this threshold, the administrator will receive notifications of low disk space.

11.7 Acronis Access Client

These settings are for the Access Desktop Client.

Access Desktop Client

Force Legacy Polling Mode	<input type="checkbox"/>
Minimum Client Update Interval	<input type="text" value="60"/>
Client Notification Rate Limit	<input type="text" value="250"/>
Show Client Download Link	<input checked="" type="checkbox"/>
Minimum Client Version	<input type="text" value="Any"/>
Prevent Clients from Connecting	<input type="checkbox"/>
Allow Client Auto-update to Version	<input type="text" value="Latest"/>

- **Force Legacy Polling Mode** - Forces the clients to poll the server instead of being asynchronously notified by the server. You should only enable this option if instructed to do so by Acronis support.
 - **Client Polling Time** - Sets the time intervals in which the client will poll the server. This option is available only when **Force Legacy Polling Mode** is enabled.
- **Minimum Client Update Interval** - Sets the minimum time (in seconds) the server will wait before re-notifying a client that updated content is available.
- **Client Notification Rate Limit** - Sets the maximum number of client update notifications the server will send per minute.
- **Show Client Download Link** - If enabled, web users will be shown a link to download the desktop client.

- **Minimum Client Version** - Sets the minimum client version that can connect to the server.
- **Prevent Clients from Connecting** - If enabled, Access 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 Access Desktop Client version that will be deployed to all Access Desktop Clients via auto-update checks. Select **Do not allow updates** to prevent clients from auto-updating at all.

12 Upgrading

In this section

Upgrading from Acronis Access to a newer version125

12.1 Upgrading from Acronis Access to a newer version

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

Note: This procedure can be used only for versions newer than Acronis Access 7.0.

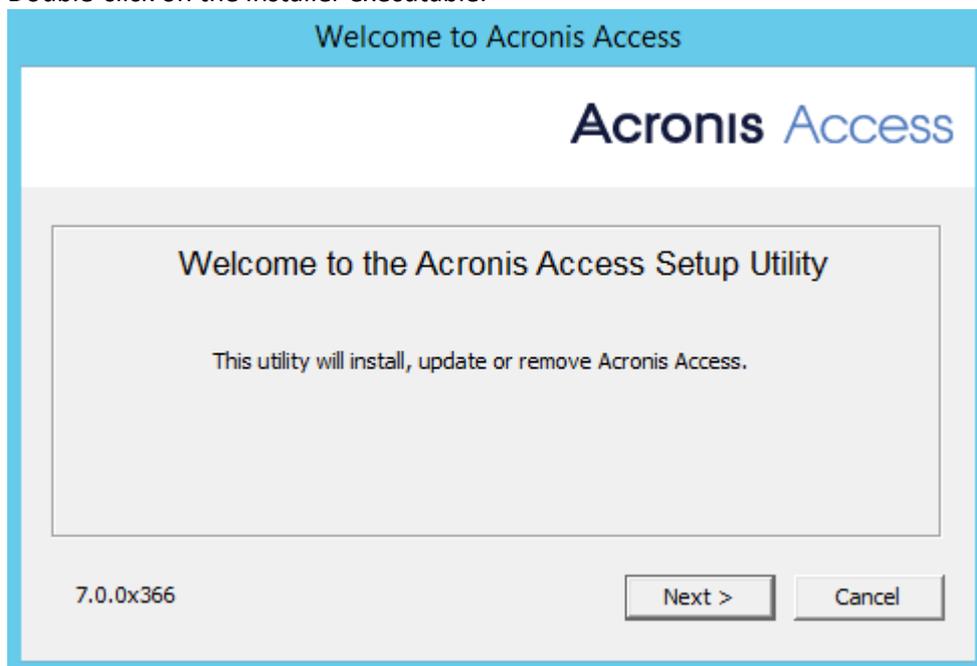
Users upgrading from versions older than Acronis Access 7.0 should upgrade to Acronis Access Advanced. For more information please consult the Acronis Access Advanced documentation.

Backup the Apache Tomcat folder

On upgrade the Apache Tomcat may be upgraded and all of the current Tomcat configuration files and 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\Access\Common**.

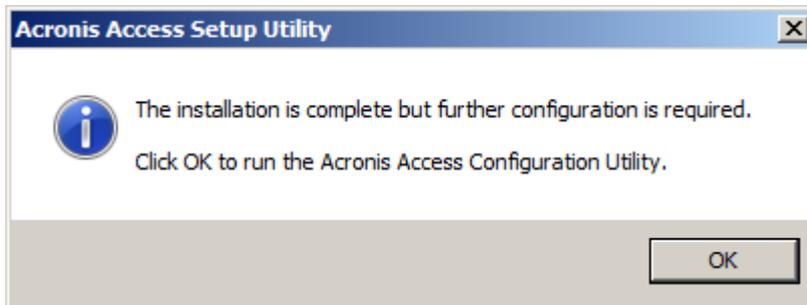
Upgrade

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. Review the installed components and close the installer.
8. You will be prompted to open the Configuration Utility, press **OK**.



9. Verify that none of the settings in the Configuration Utility have changed. After you have verified all of your settings are as expected, press **OK** to close the Configuration Utility and start the Acronis Access services.

13 Users&Devices

In this section

Managing Mobile Devices.....127

Managing Users130

13.1 Managing Mobile Devices

Once an Access Mobile Client has enrolled with the Acronis Access Server, their device will appear on the **Devices** list. This list gives detailed status information for each device that is managed. You can also wipe mobile devices or change their app password.

Users & Devices

Users

Devices

Reassign Delete

Acronis Access tracks each device that has been enrolled in client management. Use this page to invite users to enroll a device, check device status, and issue remote password resets and remote wipes of the mobile app.

Filters

Select None

Actions

Send Enrollment Invite

	Name / Email	Device Name	Model	OS	Version	Status	Last Contact	Policy
<input type="checkbox"/>	Pam	iPod touch 5G	iPod Touch 5G	iOS 7.1.1	6.1.3.107	Managed	2014-11-11 17:35:42	Default
<input type="checkbox"/>	Frank Burton	iPod touch 5G	iPod Touch 5G	iOS 7.1.1	7.0.0.458	Managed	2014-11-11 17:33:01	Default
<input type="checkbox"/>	John Price	Pam's iPod touch	iPod Touch 5G	iOS 8.1	6.1.3.107	Managed	2014-11-11 17:31:14	Default

- **Select**
 - **All** - Selects all entries.
 - **None** - Deselects all entries.
 - **Actions** - Performs the selected action on all selected entries. The available actions are **Remote Wipe**, **Cancel Remote Wipe** (These have no effect on Sync&Share users) and **Remove From List**.
- **Name / Email** – the user's Display name or email address.

- **Device name** – the device name set by the user.
- **Model** – type/model of the device.
- **OS** – version of the operating system of the device.
- **Version** – version of the Acronis Access Mobile app on the device.
- **Status** – the status of the enrollment of the Acronis Access Mobile app on the device.
- **Last Contact** – the date and time of the last connection between the management server and the client.
- **Policy** – name and link of the management policy of the user.
- **Actions**
 - **More Info** - Shows additional details about the device, including device unique ID and editable device Notes field.
 - **App password reset** - Remotely reset the Acronis Access Mobile application lock password on that device. Here, you enter the code you get from your Acronis Access Mobile app, generate a confirmation code and enter the confirmation code in the app on your device.
 - **Remote wipe** – The next time the device connects to the management server, all of the files in the Acronis Access Mobile app (and it's settings), will be deleted. No other apps or OS data is effected.
- **Remove from list** – This will remove the device from the **Device** list and it will un-manage mobile devices without wiping them. This is typically used to remove a device that you do not expect to ever contact the Acronis Access Access server again. If you have enabled "**Allow mobile clients restored to new devices to auto-enroll without PIN**", a device removed from the list will automatically reappear and become managed again if it ever makes contact with the server in the future.

In this section

Performing Remote Application Password Resets	128
Performing Remote Wipes.....	129

13.1.1 Performing Remote Application Password Resets

The Access Mobile Client can be secured with an Application Lock Password that must be entered when Acronis Access is launched. If a user forgets this password, they will not be able to access Acronis Access. The Access Mobile Client app password is independent of the user's Active Directory account password.

When a password is lost, the only recourse a user has is to uninstall Acronis Access from their device and reinstall it. This deletes any existing data and settings, which maintains security but will likely leave them with no access to Acronis Access servers until they are sent a new management invitation.

To avoid these issues, the Acronis Access Server can perform a remote application password reset.

Resetting an application password

Acronis Access 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 Access app. One aspect of this encryption is that Acronis Access clients can not have their application lock password reset over the air. Instead, a password reset code and confirmation code must be exchanged between the

device user and the Acronis Access IT administrator, in order to enable Acronis Access to decrypt its settings database and allow the user to set a new app password.

To reset a Acronis Access for iOS or Android application password:

1. An end user will contact you requesting to have their Acronis Access app password reset, they will give you their **Password Reset Code**.
2. Open the **Users & Devices** tab.
3. Open the **Devices** tab.
4. Find the device you'd like to issue an app password reset for and click the **Actions** button.
5. Press **App password reset...**
6. Enter the **Password Reset Code** given to you by the user, then click **Generate Confirmation**
7. Tell or email the user the **Confirmation Code** that is displayed
8. The user will enter this code into the app's password reset dialog and will then be prompted to set a new password. If they abort this process without setting a proper app password, they will continue to be denied access to Access Mobile Client and will have to repeat the app password reset process.

Reset App Password ×

Enter the password reset code displayed in this device's Acronis Access app, then click "Generate Confirmation". A confirmation code will be displayed that can be entered into the Acronis Access app to authorize a password reset.

Password Reset Code:

<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------------	----------------------	----------------------

Generate Confirmation

Close

13.1.2 Performing Remote Wipes

Acronis Access allows an Access Mobile Client application to be remotely wiped. This selective remote wipe removes all files that are locally stored or cached within the Acronis Access app. All app settings are reset to previous default settings and any servers that have been configured in the app are removed.

Queuing a Remote wipe

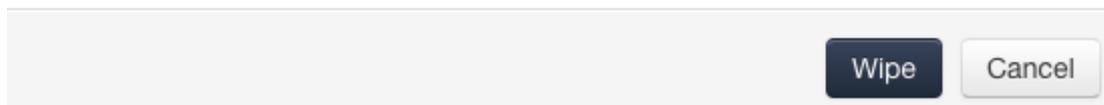
1. Open the **Mobile Access** tab.
2. Open the **Users & Devices** tab.
3. Find the device you'd like to issue a remote wipe for and press the **Actions** button.

4. Press **Remote wipe...**
5. Confirm the remote wipe by pressing **Queue remote wipe**.
6. A '**Pending remote**' status will appear in the **Status** column for that device. When the remote wipe has been accepted by the device, its **Status** will reflect this.

***Note:** Remote wipes can be canceled at any time before the client next connects to the management server. This option appears in the **Actions** menu after a remote wipe has been issued.*

Remote Wipe ×

All Acronis Access files and settings will be erased the next time this device connects.



Connectivity requirements

Acronis Access clients must have network access to the Acronis Access 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 Access, they will also need to connect to the VPN before management commands will be accepted.

13.2 Managing Users

From this section you can manage all your users. You can invite new users from the **Add Sync&Share User** button or edit/delete current users from the **Actions** button. While editing a user, you can give him administrative rights (if you have the right to do so), change his email, change his password or disable/enable his account. If quotas are enabled, you can set a custom quota for the user.

There are 2 types of Sync & Share users - Ad-hoc and LDAP

- Ad-hoc users can be created in several ways - via email invitation or via an invitation to a shared folder. These users are not licensed by default and the administrator must convert them to licensed manually. If a user is not licensed, he can only create, edit, delete, and upload folders and files in the folders shared with him by other users. Non-licensed users cannot create or upload their own content and they cannot use the desktop client.

- LDAP users and users with administrative rights are automatically licensed at creation. They are able to create and upload files and folders as well as share those files and folders with other users. They can use the desktop client as well. Unless you have setup a Provisioned LDAP group (p. 118) you will have to create your LDAP users the same way as the Ad-hoc users, but you won't have to license them manually. Administrators without Sync & Share allowed do not need to have an email address set - they can simply log in with their LDAP credentials. These administrators can be added without having setting up SMTP for your Acronis Access Server. For more information visit the Administrators and Privileges (p. 95) article.

Users & Devices

Users
Devices
Reassign Deleted User

Add Sync & Share User
Send Mobile Enrollment Invitation

Filters

Name ▲	Email	Sync & Share		Last Logged in	
		Status	Usage		
John Price	john.price@glilabs.com	Licensed	26.44 kB	2014-11-11 17:07:32	A
Frank Burton	frank.burton@glilabs.com	Licensed	279.92 MB	2014-11-11 16:59:59	A
administrator	administrator	No access	0 bytes	2014-11-11 17:14:52	A

- Name** – shows the name used to login to the server.
- Email** - shows the email address of the user.
- Policy** - displays the mobile policy currently used by the user. If the user has not enrolled in client management, the **Policy** tab will state **Unresolved**.
- Sync & Share**
 - Status** - displays the type of license used by the user.
 - Usage** - shows the number of folders, files and the total size of the user's content.
- Last Logged in** – time and date of last log in.
- Actions**
 - More Info** - Displays additional information about the user.
 - Show Devices** - Displays information about the devices used by this user.
 - Reset Sync & Share Password** - Sends a password resetting email.
 - Convert to Licensed** - Converts a free user to a licensed user. This will use 1 license.
 - Edit User** - Allows you to edit this user.
 - Delete** - Deletes the user.

Adding an Ad-Hoc user

1. Open the Acronis Access Web Interface.
2. Log in with an administrator account.
3. Open the **Sync & Share** tab.
4. Open the **Users** tab.
5. Press the **Add User** button.
6. Write the email of the user.
7. Select whether the user should have administrative rights or not.
8. Select the language of the invitation.
9. Press the **Add** button.

The user will receive an email with a link. Once he opens the link, he will be asked to set a name and password and his account will be complete. These can be changed after the user logs in successfully.

Adding an LDAP user

1. Open the Acronis Access Web Interface.
2. Log in with an administrator account.
3. Open the **Sync & Share** tab.
4. Open the **Users** tab.
5. Press the **Add User** button.
6. Write the email of the user.
7. Select whether the user should have administrative rights or not.
8. Select the language of the invitation.
9. Press the **Add** button.

The user will now be able to log in with his LDAP credentials. His account will be complete once he logs in.

Note: *If you have LDAP enabled, and have a provisioned LDAP Administrator Group, users in that LDAP group will be able to log in directly with their LDAP credentials and will have full administrative rights.*

Reassign Content

Deleted users without any content are completely removed. Users which had content (files, folders) remain in the system and will be moved to this section. Administrators can access the list of deleted users with content still in the system. This content can be reassigned to another user or left alone to be purged automatically by the system according to the purging policies in effect.

Active Users Deleted Users

Only deleted users with content are shown on this page. Deleted users without any content are removed from the system.

0 LDAP Users, 1 Ad-hoc User

▼ Filters

Name	Authentication	Deleted at	Owned Content
john@gillabs.com	Ad-hoc	2014-02-12 11:39:02	Reassign Content (1 Folder / 8 Files / 3.7

When deleting a user, a window will ask you if you want to reassign this user's content to another user. If you select another user, the deleted user's content is moved to the target person's owned space and that user will not appear in the **Deleted Users** tab.

14 What's New

In this section

What's New in Acronis Access Server	134
What's New in the Acronis Access app	148
Previous Releases.....	149

14.1 What's New in Acronis Access Server

Note: Numbers such as "[DE1013, US552, #2717]" refer to Acronis' internal change tracking system.

Note: Numbers such as "[7.0.1x18]" indicate the specific build in which a change was introduced.

Acronis Access 7.0

ENHANCEMENTS

- Redesigned and enhanced Access web client user interface.
- **Acronis Access** is now named **Acronis Access Advanced** and is the upgrade path for existing users of Acronis Access 6 or earlier. A new version tailored for small/medium businesses with simpler requirements has been also introduced. This new version is named Acronis Access.
- During new installations, the configuration wizard now attempts to detect and system configuration options, such as SMTP server and Active Directory (LDAP) server.
- During installation, Acronis Access and Acronis Access Advanced can now be configured to operate using a single open port for client connections. In this configuration, all Access clients (mobile app, desktop sync client, web client interface) use the same network address and port to connect to the Access server.
- Folders and files residing on file servers, NAS and SharePoint Servers can now be browsed and accessed from within the Access web client interface. This capability can be enabled or disabled on a user or group basis.
- Updated graphic design of default email templates. Redesigned notification and invitation email templates.
- The Users administration page and Devices administration page are now unified into a single admin console page.
- Access now provides conflict resolution for Sync & Share files and folders. If users' file modifications overlap and cause conflicts, the conflicting files will be renamed with the users name and the current date, so that the conflicting file is obvious and can be handled as needed. Previous to Access 7.0, these conflicting files would have been saved as new versions.
- Sync & Share files can now be copied between Sync & Share folders using the web client interface.
- Sync & Share file download links can be now be generated and copied for use, without requiring an email to be sent by the Access server. The file download links feature can be enabled or disabled.
- Usernames can now be assigned to 'Ad-hoc' external users. All Sync & Share users are generally referred to by user names instead of just email addresses.
- Access Client Version is now displayed in the Users and Devices section of Access Server administration page. (US8696)

- Java version 7 U71 is used in this release. (US9486)
- Improved audit logging when files are downloaded from direct download link. (DE10961)
- Sorting files by type is now allowed in the web client interface. (US6836)
- Postgres can now be removed using the 'Add/Remove Programs' control panel. (US8270)
- There is now a global setting to disable the ability to share files using direct download links. (US8347)
- The default threshold and interval for user notification as they approach their quota for Sync & Share can now be configured. (US8605)
- Apache Tomcat 7.0.56 is used in this release. (US9801)
- OpenSSL version 1.0.1i is used in this release. (DE11653)
- Added support for batch operations in the Devices table (remote wipe, cancel remote wipe, etc.). (US8875)

BUG FIXES

- Fixed a PostgreSQL installer failure that could occur if a local users group does not have enough privileges.
- Fixed issue with querying LDAP when debug logging is enabled that could occasionally result in an error for some UTF-8 usernames.
- Fixed usage of @display_name variable for Acronis Access enrollment emails.

KNOWN ISSUES

- Internet Explorer 8 is not supported in the initial version of the Acronis Access 7.0 Web client. IE8 users will not be able to log into the Acronis Access Web client. Support for IE8 is anticipated to return in a followup release, though in this followup release IE8 users will be presented with the previous Access 6 web UI and will not be able to use the new Access 7 features. If you have end-users running Internet Explorer 8, please consider upgrading to a more secure browser or waiting until support is added in the upcoming Access Server update. (DE12649)
- Windows XP users will not be able to use the Acronis Desktop Sync Client or Web Client after an Access Server is upgraded to 7.0 or later. This is due to an incompatibility of XP and IE8 with the secure SSL bindings the Access Server now uses. Administrators can change the SSL bindings to support XP users. Details here: [Changing the Acronis Access Tomcat SSL Ciphers \(p. 112\)](#). Please note that changing these ciphers might expose your server to vulnerabilities and is generally unsecure.
- Windows Server 2003 is no longer supported. (US9572)
- 'Mobile Access' Network Home Folders configured for users on the Access Server are not displayed in the Web client interface. This will be supported in a followup release. (US9733)
- If user select several files for upload they will be uploaded one after the other, not simultaneously. (DE12512)
- SharePoint check-in / check-out is not yet supported in the web client interface. This will be supported in a followup release. (US8282)

Upgrade from mobilEcho 4.5 is not supported in the initial version of the Acronis Access 7.0. Support for upgrade from mobilEcho 4.5 is anticipated to return in a followup release. (DE12971)

Acronis Access 6.1.3

ENHANCEMENTS

- The default SSL bindings of Acronis Access no longer support Internet Explorer 8 client connections. To enable unsecure Internet Explorer 8 connections on a new installation, please see this article: [Changing the Acronis Access Tomcat SSL Ciphers \(p. 112\)](#). (US8460)
- New Relic agent updated to the version 3.9.0.229. Please note that New Relic will stop working until it is upgraded to this release.
- Performance Optimizations in Access Server for handling large numbers of self-provisioned folders. (DE11452)
- Enhanced Web UI login to provide a link to knowledge base article in case Java Cryptography Extensions are not installed properly. See <https://kb.acronis.com/content/47618> for details. (US9226)
- Acronis Access Client for Mac has been updated to support Mac OS X 10.9.5. (US9249)
- Installer includes Java Version 7 Update 51.
- Apache Tomcat updated to 7.0.55. (US9392)

BUG FIXES

- Fixed issue with querying LDAP if debug logging is enabled that could result in an error when provisioning users. (DE11545)
- On install or upgrade the installer will always install the Java Cryptography Extension files regardless of the Java version. This is done to ensure that the correct JCE libraries are used even if Java version > 7.0.51 is installed on the system. (DE11219)

Acronis Access 6.1.2

ENHANCEMENTS

- Fixed a potential issue with uploading large files via Access web client interface.
- "**Require exact match**" option has been added to "**Domains for LDAP authentication**". When Access sharing invitation emails are sent to users whose email address domain matches the domains listed in '**Domains for LDAP authentication**' setting, they will be instructed to log in with their internal LDAP (Active Directory) credentials. Users who do not match '**Domains for LDAP authentication**' will be invited to create an Acronis Access external user account. Users whose email domain is a subdomain of an entry in '**Domains for LDAP Authentication**' will receive emails with internal user LDAP instructions, unless this '**Require exact match**' checkbox is **checked**. This checkbox is unchecked by default and for upgrades.
- Adjusted the **Application Policy** administration page to reflect changes in the Acronis Access for Android 3.2.3 application.
- In addition to being denied access and redirected, an error message will now be displayed when trying to access a Sync & Share folder you do not have access to via a URL.
- The audit log now allows the owner of a shared folder to see when a member of the shared folder sends download links to others.
- Configuration utility updated to use OpenSSL 1.0.1h.
- Tomcat version updated to 7.0.54.

- Java 7 Update 51 is used in this release.

BUG FIXES

- Fixed an issue with downloading **Sync & Share** files from an Amazon S3 repository.
- Fixed an issue with distinguishing multiple ad-hoc Access Server administrators that do not have associated email addresses.
- Fixed an issue with populating the **owner_name** value in the exported logs.
- Fixed an issue where some provisioned administrator groups were unable to log in after an upgrade.
- Fixed possible request timeout issue when enrolling a mobile client in a large Active Directory.
- Fixed an automatic service startup issue when installed on a Windows Server that is not a member of a domain.
- Fixed a licensing message issue with running multiple Gateway servers on the same network using the same serial number.
- Fixed intermittent SSL errors in the mobile Acronis Access app when accessing **Sync & Share** folders.
- Fixed some Java detection issues in the installer.
- Fixed the issue with the client reporting a python exception instead of an error indicting the actual problem.

KNOWN ISSUES

- When upgrading from Access Server 6.1 if "**redirect for port 80 on Apache Tomcat**" option was set it will not be preserved. Please enable this option in the Configuration Utility manually after the upgrade.

Acronis Access 6.1.1

ENHANCEMENTS

- Improved authentication speed for users in large Active Directory catalogs logging into the Acronis Access web interface.
- Configuring user Sync & Share quotas via the Access API is now done in units of gigabytes (GB).
- Improved error-handling on Gateway Server interactions with Microsoft SharePoint.
- Organizational Units and Domains are no longer displayed when creating Mobile Access group policies since they are not supported.

BUG FIXES

- Users with the reserved string "data" in their username are now able to complete mobile app enrollment.
- Fixed an issue where an Acronis Access Gateway Server could be listed multiple times in the Access mobile app if the Gateway Server was configured to be visible and multiple data source folders were also assigned.
- Fixed enabling/disabling logging for an Access Server cluster group.

- Addressed a dependency issue that could prevent the Access Gateway service from starting automatically after a reboot on Windows Server 2008R2.

Acronis Access 6.1

ENHANCEMENTS

- Web Services API for the Acronis Access Server administration. The API documentation is packaged within the Access server and is accessible by administrators. The link can be found in the footer.
- The Acronis Access audit log can now be configured to automatically export and purge old log entries. Preferences for export and purge settings can be set on the Audit Log => Settings page.
- New Acronis Access configuration summary tool to collect relevant server configuration details for sending to Acronis support.
- Improved login performance, through general performance improvements and by caching Active Directory group membership information.
- There is now an option for administrators to preview custom email templates before saving them.
- The Acronis Access server logo and color scheme can now be easily customized. Please consult the documentation here on how to customize your server: Customizing the web interface (p. 113).
- A new email template exists to customize the email that will be sent to newly invited administrators who do not have sync and share access.
- The Gateway Server logging tab can now be found under the “Edit” menu item instead of “Details”.
- When adding enrollment invitations, the search results will now show whether there are already enrolled devices for that user.
- Acronis Access will now email the original sender if emails sent on their behalf cannot be delivered because the recipient's email was invalid.
- Whitelists and blacklists can now be assigned to the default profile from the “Allowed Apps” page.
- Administrators can click a link on the LDAP settings page to force all cached LDAP information to be refreshed.
- Provisioned LDAP administrator groups can now be configured to allow sync and share access.
- Cluster group members can now be added via the cluster group’s menu.
- Support for Windows 8.1.
- Installer support for installations where PostgreSQL is located on a different server.
- Improved PostgreSQL installation process.
- Improved uninstallation process.
- Improved error reporting in web interface.

BUG FIXES

- The active session count will be refreshed when the Gateway Servers page is reloaded.
- Type-ahead search for selecting users to invite to shared files and folders is now supported on Internet Explorer 8.

- The Acronis Gateway Server service is now dependent on other key services so it should be assured to start properly when the server starts up.
- When a Cluster Group is disbanded, any policies that were using that Cluster Group as the Gateway Server used to access “My Network Folders” (locations added by the user) will be updated to instead use the last Gateway Server that was a member of the Cluster Group.
- Fixed an issue with email address filtering for enrolled users.
- Administrators should no longer get a fatal error page when changing the language setting after receiving an error message.
- Administrators should no longer encounter problems applying trial extensions after upgrading an expired server.
- LDAP sync and share users should now always be listed as LDAP once they have successfully authenticated, even if their email domain does not match the domains for LDAP authentication. Administrators can be added from LDAP even if the email domain is not included in domains from LDAP authentication.
- When administrators add new users or administrators, they will receive an immediate error message if adding a user with an invalid email address.
- Pending invitations will now be properly resolved to grant sync and share access to existing administrative users.
- Exports of the users table will now include the the “Licensed” field.
- Sending a download link will now respect the blacklist and whitelist restrictions.
- Searching for new LDAP users to enroll should be much faster.
- New users who are in both a LDAP provisioned administrators group and a LDAP provisioned sync and share group will get the combined permissions.
- Mapping a home directory to an existing data source now works properly if the available data source uses the %USERNAME% wildcard.
- LDAP searches no longer display built-in groups which are not valid choices for group memberships.
- Slow home directory lookups will no longer cause mobile users to fail to enroll.
- Fixed an issue which could cause authenticating and accessing assigned sources with certificates on Windows 2003 R2 to fail.
- Unlicensed adhoc users are now properly restricted from connecting with the client to the server.
- Information in the Gateway Servers table is now updated immediately, instead of when you open the details tab for the server.
- The cosmetic “from” address in emails sent by Acronis Access now appears as the actual sender’s email address.
- Old Acronis Access serial numbers are now removed when a new base serial number is applied.
- The installer will no longer create multiple Gateway server entries in Programs and Features on upgrade.
- Fixed memory leak in Gateway server.

Acronis Access 6.0.2

BUG FIXES

- Includes upgraded OpenSSL DLL to address **HeartBleed** vulnerability.

Acronis Access 6.0.1

ENHANCEMENTS

- Added a new policy to specify which gateway or cluster group will be used to share users' Active Directory assigned home folders. Active Directory assigned home folders will now automatically be shared by a gateway without the need to manually create a data source or enable the "Allow User to Add Network Folders by UNC path or URL" policy setting.
- A new setting, "LDAP information caching interval", is now available on the LDAP Settings page to allow administrators to specify how often the Acronis Access server will update its cached information about LDAP users and groups.
- A new setting, "Use user principal name (UPN) for authentication to Gateway Servers", exists on the Mobile Access Settings page. If enabled, users will authenticate to gateway servers with their UPN regardless of what format of username they used to enroll. If disabled, users will be authenticated with whatever format username they used to enroll.
- Performance improvements have been made when determining LDAP group memberships, which will improve the speed of enrollment and authentication. To improve performance, we no longer by default include nested LDAP distribution groups when determining group membership. If your configuration requires members of nested distribution groups to be included, please enable the new setting, "Include nested distribution group membership" on the LDAP settings page.

BUG FIXES

- The Access Desktop Client on Windows will no longer crash if the client downloads or uploads a huge number of files.
- Gateway servers will now be automatically contacted after they are added on fresh installations, so they can immediately be added to a cluster group or have self-provisioning enabled.
- Sync & Share functionality and data sources will now continue to work during the grace period after the license expires.
- Audit log licensing warning messages are now properly localized in all cases.
- Volumes will no longer become inaccessible if their parameters included the pipe ('|') symbol.
- Sending links or invitations from the Acronis Access mobile application will no longer fail when the device is configured for languages other than English, French, German or Japanese.
- The installer will no longer create multiple Gateway server entries in Programs and Features on upgrade for non-English installations.
- Fixed a bug where the Acronis Access Tomcat service would periodically fail to startup correctly and would need to be restarted in order to allow clients to connect.
- Fixed a bug where clients that are configured to require credentials "once per session" could prompt the user for a password when connecting to the management server after the server was upgraded from 4.x.
- Self-provisioned folders now can be added and removed successfully when the profile is configured to use either a gateway server or a cluster group, regardless of whether or not the server or cluster group is online.
- Policy priority order will be respected, so users will receive the highest priority group policy to which they are entitled.

- Clients who do not have sync and share enabled will no longer be incorrectly reported as “unmanaged” in the audit log.
- Files with Japanese or other characters in their filenames should no longer have the filenames changed when downloaded with Internet Explorer.
- Administrators should no longer see unresolvable errors when subscription licenses expire.
- The Access Desktop Client minimum version list now correctly includes 3.0 client versions, and will be honored for both old and new desktop clients.
- Home directories should no longer be inaccessible after upgrades from pre-5.0 versions of mobilEcho.
- Miscellaneous localization bug fixes.

Acronis Access 6.0.0

ENHANCEMENTS

- 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**.
- Active Directory-based Administrator users are no longer required to have an email address assigned. Administrator users can also be added without configuring the Acronis Access Server for SMTP.
- A new checkbox is provided on the Server Settings that allows Sync & Share functionality to be turned on or off. By default when upgrading from mobilEcho to Acronis Access Server Sync & Share (formerly known as activEcho) is disabled.
- Active Directory distribution groups can now be invited to Sync & Share folders.
- Inviting many users to Sync & Share folders is now significantly faster.
- The Configuration Utility now includes more status / progress messages when it is setting up the server.
- The Configuration Utility will now generate an error if the repository is located on a remote network volume but the Repository Service is configured to run under the Local System account. The Repository Service needs to run under an account with permissions to the remote network volume.
- The Configuration Utility will now present an error if an SSL certificate is selected that does not have an embedded private key.
- Java has been upgraded to Version 7 Update 51.
- The Server Settings "Server Name" is now used as the title of the web site that appears to end users.
- The LDAP Cache refresh interval has been changed from 60 to 15 minutes.
- A new Advanced Setting for Gateway Servers has been added that, if enabled, users will authenticate with their UPN (example: username@domain.com). Otherwise, users will authenticate with their separate domain and usernames (example: domain\username). This is sometimes needed when authenticating to some federated scenarios, i.e., SharePoint 365.

BUG FIXES

- The Default Language setting in Server Settings has been renamed to be clear that it is the default audit log language.
- If a data source for an Active Directory home folder cannot be resolved, the Mobile Clients will no longer see the home folder, instead of getting an error accessing the !HOME_DIR_SERVER.
- Miscellaneous bug fixes in the Acronis Access Desktop Client.
- Miscellaneous localization improvements.

Acronis Access 5.1.0

ENHANCEMENTS

- The Configuration Utility now provides the ability to control whether the Access Server should bind to HTTP port 80 and redirect automatically to the configured HTTPS port. Previously this was enabled by default, but now the administrator must enable it on clean installations.
- When editing email templates a new option allows the administrator to view the default value for the email subject.
- 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

- Exporting a large set of records from the audit log now completes significantly faster.
- Error messages from some dialogs are now properly cleared when the error condition is resolved.
- Only one instance of the Configuration Utility can now be run at a time.

- On Windows Server 2003, the uninstall process no longer reports that PostgreSQL was not installed by the Acronis Access Server installer.
- The Configuration Utility now generates an error if the Gateway Service is configured to bind to all address on a port and the Access Server on a specific address with the same port.
- By default on clean installs Tomcat is now configured to not listen for shutdown requests on port 8005. This prevents conflicts with other instances of Tomcat on a server. Because the Access Server Tomcat instance runs as a service, shutdown requests over network ports are not needed.
- Miscellaneous localization improvements.
- Improved performance displaying the log for non-administrative users
- Expired license notifications will no longer appear when activEcho is disabled via the Access 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
- 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.

Acronis Access 5.0.3

ENHANCEMENTS

- Acronis Access Server can now be installed on a Windows Failover Cluster, for Windows Server 2003 SP2, 2008/2008R2 and 2012/2012R2. Please see *Installing Acronis Access on a cluster and Upgrading Acronis Access on a cluster* for instructions on how to install or upgrade in this configuration.

BUG FIXES

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

Acronis Access 5.0.2

ENHANCEMENTS

- Acronis Access Server has been certified on Windows Server 2012 R2.
- LDAP administrators can now be added even if SMTP is not configured.
- The Configuration Utility no longer creates duplicate firewall rules when applying changes.
- Authentication performance for large multi-domain LDAP trees is significantly improved.
- Improved performance of the activEcho client when there are a large number of updates.
- The Folder list in Data Sources now shows the assigned Gateway Server using its Display Name instead of its IP Address.

BUG FIXES

- Localization improvements.
- Choosing to uninstall from the installer application now works on Windows Server 2003.
- Installer will now enforce that a minimum of 1GB of free disk space is available before installing.
- Upgrades from activEcho 2.7 now work properly on non-English PostgreSQL installations.
- 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")

Acronis Access 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.

Acronis Access 5.0.0

ENHANCEMENTS

- Acronis Access Server is a new shared server platform used by both mobilEcho and activEcho. Both products now use the same shared backend infrastructure. Functionality for each product is determined and enabled based on licensing.
- New integrated platform installer. Acronis Access server, mobilEcho and activEcho are included in the installer. Installer run time installation options allow administrator to determine what elements are deployed.
- Acronis Access Server automatically installs Java JRE and the required Java Cryptographic Engine policy files.
- New Server Configuration Utility allows administrators to set base configuration options like binding to specific IP addresses and ports, handling local machine firewall rules, installation of SSL certificates.
- Acronis Access Server is localized in English, German, Japanese and French.
- New startup wizard simplifies initial configuration of the server
- Redesigned, updated user and management web interfaces, including responsive design with support for mobile devices.
- New paging tables support display, sorting and filtering of much larger sets of data. The log filtering has been improved, including filtering by typing partial user names, by message type, etc.
- 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 responsiveness 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.
- The mobilEcho Client Management Server is integrated with Acronis Access 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 Acronis Access 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 Acronis Access 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 Acronis Access 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 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

- Improved support for exporting Unicode characters to TXT or CSV files.
- 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.
- 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.

14.2 What's New in the Acronis Access app

Access Mobile Client 6.1

ENHANCEMENTS

- Added support for iOS 7 managed app configuration.
- Updated MobileIron AppConnect integration to version 1.7.
- Addressed an issue where iWork files might appear as zip files.
- Added new mobilecho:// link variables (action=edit & action=preview) that can be used to automatically open the linked file.
- Miscellaneous fixes and improvements.

Access Mobile Client 6.0.1

BUG FIXES

- Fixed crash that could occur when annotating PDF documents with the stamp tool.

Access Mobile Client 6.0

ENHANCEMENTS

- The mobilEcho mobile app is now named 'Acronis Access'.
- Miscellaneous fixes and improvements.

mobilEcho 5.1

ENHANCEMENTS

- Implemented new iOS 7 style interface.
- Network shares and SharePoint locations can now be added from within the app, if allowed by your mobilEcho profile.
- Support for Kerberos Constrained Delegation authentication to mobilEcho Servers.
- Miscellaneous fixes and improvements.

mobilEcho 5.0

ENHANCEMENTS

- Optional policy-based expiration of on-device files in 'My Files' and 'File Inbox'.
- Font size options when previewing or editing text files.
- Multiple file attachments can now be included in one email.
- Support for sending invitations to activEcho shared files and folders.
- Miscellaneous fixes and improvements.

mobilEcho 4.5.2

ENHANCEMENTS

- Added support for using smart cards to unlock the mobilEcho app and to authenticate with mobilEcho servers. This feature utilizes the Thursby PKard Reader app and the smart cards (CAC, PIV, etc) and card readers the Thursby app supports.
- Miscellaneous fixes and improvements.

mobilEcho 4.5.1

- mobilEcho now supports iOS 7, both when operating as a standalone app and when MobileIron AppConnect-enabled.
- Miscellaneous fixes and improvements.

mobilEcho 4.5

ENHANCEMENTS

- In-app Office document editing (Supports: DOC, DOCX, XLS, XLSX, PPT, PPTX).
- In-app text file editing.
- Added support for SharePoint 365.
- The encryption module used by mobilEcho is now FIPS 140-2 certified.
- Alternative grid view for browsing files, with thumbnail previews of on-device files.
- Multiple files can now be opened simultaneously.
- If file synchronization is occurring when leaving the mobilEcho app, it will now continue in the background until the file transfer completes or the process is stopped by iOS.
- The interval at which mobilEcho will perform file syncs while the app is open can now be set.
- Syncing can now be configured, from within the app, to automatically occur only when the device has a WiFi connection.
- Improvements to sync progress and error indication.
- mobilEcho links to SharePoint locations in site collections can now be opened, as long as the user has access to a higher-level location on the SharePoint server where the site collection resides.
- Text search and table of contents are now available when viewing a PDF file while your IT administrator has disabled PDF annotation.
- Support for user certificate authentication with mobilEcho servers.
- Miscellaneous fixes and improvements.

14.3 Previous Releases

14.3.1 activEcho

Acronis Access 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 Acronis Access Server (p. 134) 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 Access 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 responsiveness 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 if 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-RedirectingHTTPPrequeststoHTTPS>

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

14.3.2 mobilEcho

Acronis Access 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 Acronis Access Server (p. 134) 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 Acronis Access 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 Acronis Access 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 Acronis Access 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 Acronis Access 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 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.

mobileEcho 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.

mobileEcho 4.5.1 (Released: September 2013)

ENHANCEMENTS:

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

BUG FIXES:

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

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

mobileEcho 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 mobileEcho 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.