

# Acronis



# Acronis Access

Installation and Upgrade Guide

## 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

<b>1</b>	<b>Installing.....</b>	<b>4</b>
1.1	Requirements .....	4
1.1.1	Operating System Requirements .....	4
1.1.2	Mobile Client requirements .....	4
1.1.3	Minimum Hardware Recommendation .....	5
1.1.4	Network Requirements .....	5
1.1.5	Desktop Client Requirements .....	6
1.2	Installing Acronis Access on your server.....	7
1.3	Using the Configuration Utility .....	8
1.4	Using the Setup wizard .....	11
1.5	Clustering Acronis Access .....	15
1.6	Load balancing Acronis Access .....	16
<b>2</b>	<b>Upgrading.....</b>	<b>17</b>
2.1	Upgrading from Acronis Access to a newer version .....	17
2.2	Upgrading from mobilEcho 4.5 or earlier .....	18
2.2.1	Before You Begin .....	18
2.2.2	The Upgrade Process .....	26
2.2.3	Downgrading to mobilEcho 4.5.....	59
2.3	Upgrading from activEcho 2.7 or earlier.....	60
2.3.1	Before You Begin .....	60
2.3.2	The Upgrade Process .....	61
2.4	Upgrading Clustered Configurations .....	79
<b>3</b>	<b>Quick Start: Mobile Access .....</b>	<b>81</b>
3.1	First Run .....	81
3.2	Configuring Your First Gateway Server and Data Source .....	84
3.3	Setting up a Policy.....	87
3.4	Installing the Access Mobile Client application .....	88
3.5	Enrolling in client management.....	89
<b>4</b>	<b>Quick Start: Sync &amp; Share .....</b>	<b>93</b>
4.1	First Run .....	93
4.2	Using the web interface to access files.....	96
4.3	Using the desktop client .....	101

# 1 Installing

## In this section

Requirements.....	4
Installing Acronis Access on your server.....	7
Using the Configuration Utility .....	8
Using the Setup wizard .....	11
Clustering Acronis Access.....	15
Load balancing Acronis Access.....	16

## 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.....	4
Mobile Client requirements.....	4
Minimum Hardware Recommendation .....	5
Network Requirements.....	5
Desktop Client Requirements .....	6

### 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  
Windows 2003, SP2 or later

---

**Note:** When installing on a machine with a Windows Server 2003 operating system, you must have **Microsoft Core XML Services (MSXML) 6.0** installed, otherwise the Configuration Utility will not work.

**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:

#### Access Mobile Client Application Supported devices:

- Apple iPad 2nd, 3rd, 4th generation
- Apple iPad Mini 1st, 2nd generation
- Apple iPhone 3GS, 4, 4S, 5, 5s, 5c
- Apple iPod Touch 4th, 5th generation

- Android Smartphones and Tablets (Devices with x86 processor architecture are not supported)

#### **Access Mobile Client Application Supported OS's:**

- iOS 6 or later
- Android 2.2 or later (Devices with x86 processor architecture are not supported)

#### **The Access Mobile Client Application 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 Network Requirements

- 1 Static IP Address. 2 IP addresses may be needed for certain configurations.
- Optional but recommended: DNS names matching the above IP addresses.
- Network access to 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 - VPN, MobileIron, Good Dynamics and etc.
- All machines running the Access Server or the Gateway Server need to be bound to the Windows Active Directory.

There are two components that handle HTTPS traffic, the Gateway Server and the Acronis Access Server. The Gateway Server is used by mobile clients to access both files and shares from the Data Sources. The Access Server provides the web user interface for Sync & Share clients, and is also the administration console for both Mobile Access and Sync & Share. It is recommended that two IP addresses be assigned to the server along with two separate DNS entries for those addresses. However, the server can be configured to use only one IP address with different ports for each

component. This one IP address configuration is sufficient for most Mobile Access-only installations but two IP addresses is recommended when using Sync & Share as well.

**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 Mobile Device Management (MDM) systems or the Apple iPhone Configuration Utility to configure the certificate-based iOS “VPN-on-demand” feature, giving seamless access to Acronis 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, username / password authentication, Kerberos constrained authentication delegation and certificate authentication. For details on adding certificates to the Access Mobile Client app, visit the Using client certificates article.
- **Good Dynamics enabled Access Mobile Client app:** The Access Mobile Client app includes the ability to be enrolled in and managed by the Good Dynamics platform. In this configuration, all network communication between Access Mobile Clients and Gateway Servers is routed through the Good Dynamics secure communication channel and Good Proxy Server. For more details, see the Access Mobile Client for Good Dynamics manual page.
- **MobileIron AppConnect enrolled Access Mobile Client app:** If the Access Mobile Client application is enrolled with MobileIron's AppConnect platform, then all network communication between Access Mobile Client clients and Gateway Servers can be routed through the MobileIron Sentry. For more information see the MobileIron AppConnect manual page.

**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.

## 1.1.5 Desktop Client Requirements

**Supported operating systems:**

- Windows XP, Windows Vista, Windows 7, Windows 8 and 8.1
- 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](#).

---

**Supported web browsers:**

- Mozilla Firefox 6 and later
- Internet Explorer 8 and later (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

## 1.2 Installing Acronis Access on your server

The following steps will allow you to perform a fresh install and test Acronis Access with HTTPS using the provided Self Signed certificate.

---

**Note:** For upgrade instructions visit the *Upgrading (p. 17)* section.

**Note:** For instructions on installing on a cluster visit the *Installing Acronis Access on a cluster* section.

---

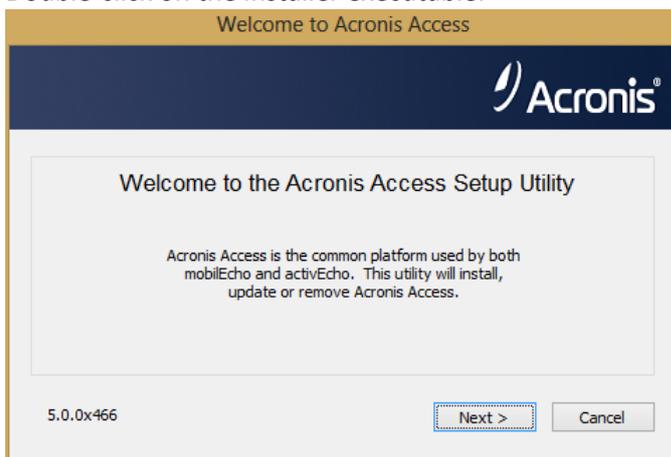
The installation of Acronis Access involves three steps:

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

### 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.



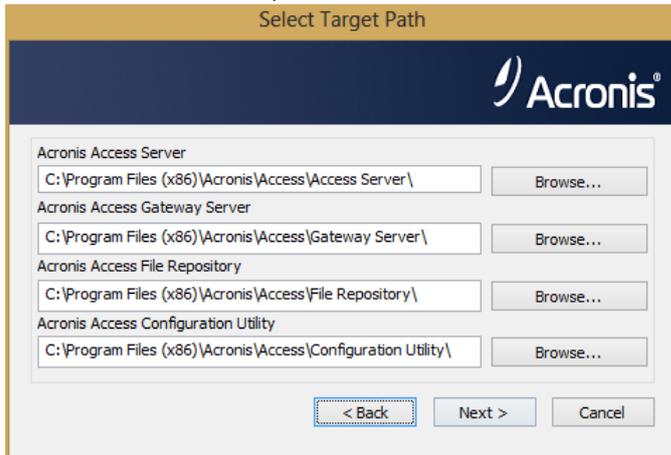
4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.

---

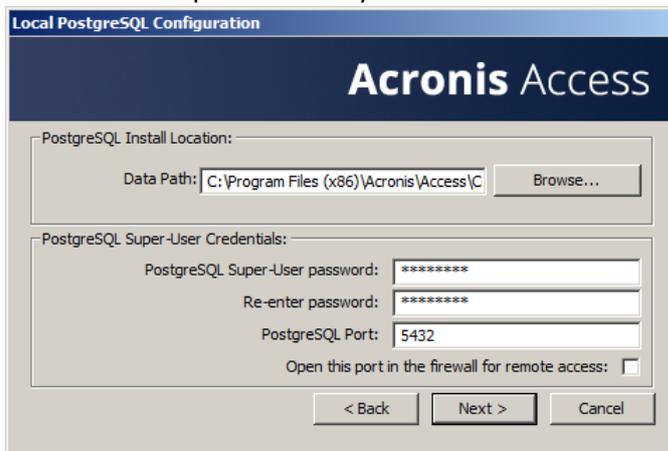
**Note:** If you're deploying multiple Acronis Access servers, or you are installing a non-standard configuration, you can select which components to install from the **Custom Install** button.

---

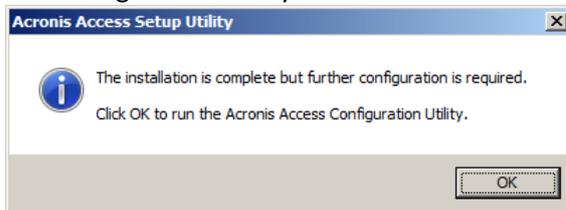
7. Either use the default paths or select new ones for each component and press OK.



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



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



For instructions on using the Configuration utility, visit the Using the Configuration Utility (p. 8) page.

## 1.3 Using the Configuration Utility

The Acronis Access installer comes with 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. The Gateway Server is used by mobile clients to access both files and shares. The Access Server provides the web user interface for Acronis Access clients, and is also the administration console for both Mobile Access and Sync & Share.

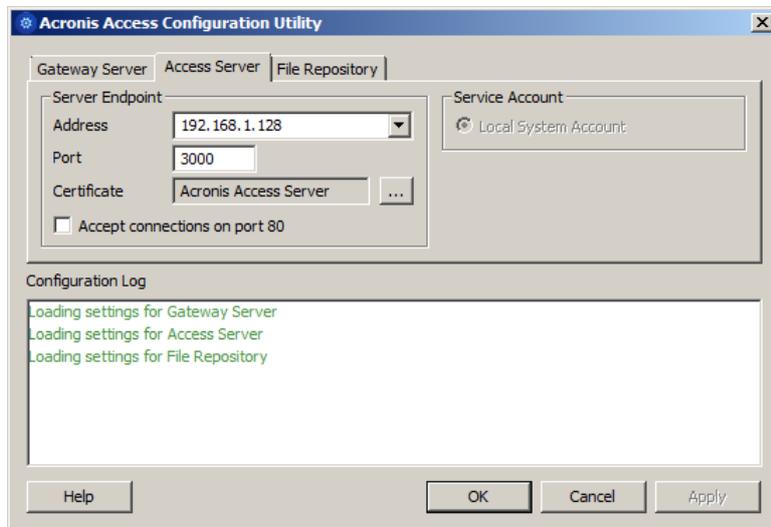
---

**Note:** See the Network Requirements (p. 5) 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 article.

---

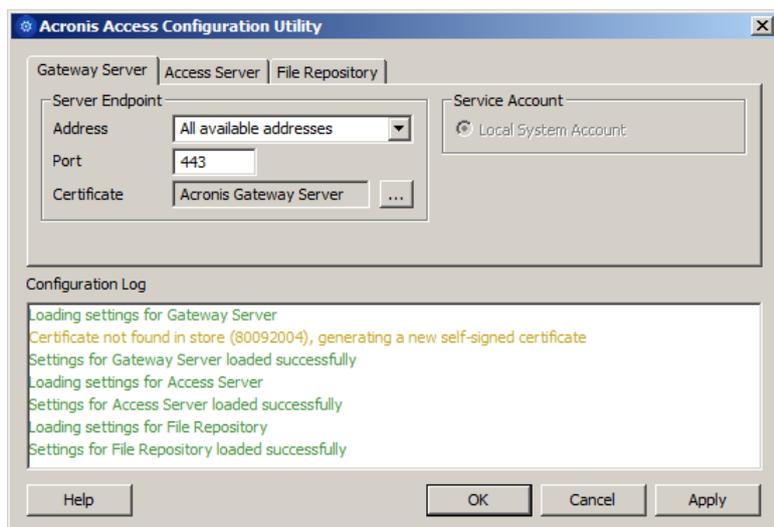
## Access Server Overview



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

- **Address** - The DNS name or IP address of your Web Interface or pick **All Addresses** to listen on all interfaces.
- **Port** - The port of your Web Interface.
- **Certificate** - Path to the certificate for your Web Interface. You can choose a certificate from the Microsoft Windows Certificate Store.
- **Accept connections on port 80** - When selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.
- **Service Account** - This allows the Acronis Access Server service to run in the context of another account. This is normally not required in typical installations.

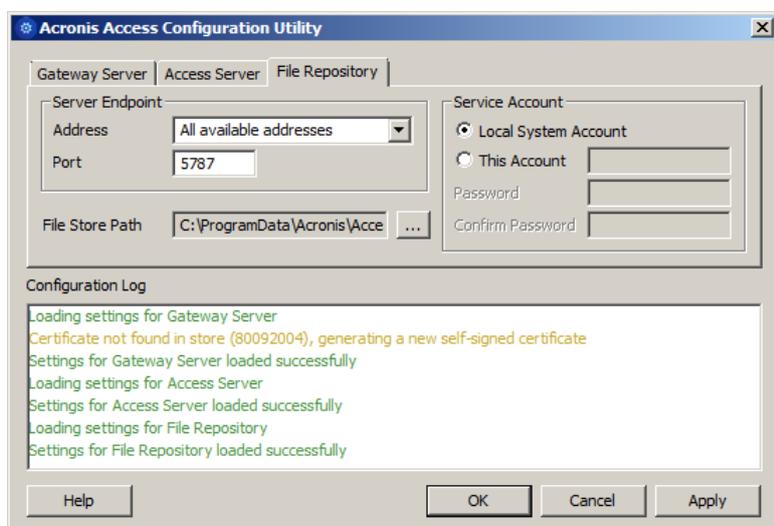
## Gateway Server Overview



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

- **Address** - The DNS name or IP address of your Gateway Server or pick **All Addresses** to listen on all interfaces.
- **Port** - The port of your Gateway Server.
- **Certificate** - Path to the certificate for your Gateway Server. You can choose a certificate from the Microsoft Windows Certificate Store.
- **Service Account** - This allows the Gateway Server service to run in the context of another account. This is normally not required in typical installations.

## File Repository Overview



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

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

---

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

---

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

After you have filled in all the necessary fields, pressing Apply or OK will restart the services you have made changes to. It will take 30-45 seconds after the services have started before the Acronis Access Server is available. At this point, a web browser will automatically launch and connect to the Acronis Access's IP address and port. On the login page, set the administrator password and then the Setup Wizard (p. 11) will guide you through the setup process.

---

**Note:** *Write down the administrator password, as it cannot be recovered if forgotten.*

**Note:** *If you need to change any of the network IP addresses/ports or certificates used by the Acronis Access components, you can run the Configuration Utility again at any time to make these changes. It will automatically adjust the necessary configuration files and restart the services for you.*

---

## 1.4 Using the Setup wizard

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

---

**Note:** *If you are upgrading from activEcho or mobilEcho, please read the Upgrading (p. 17) section before continuing.*

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

---

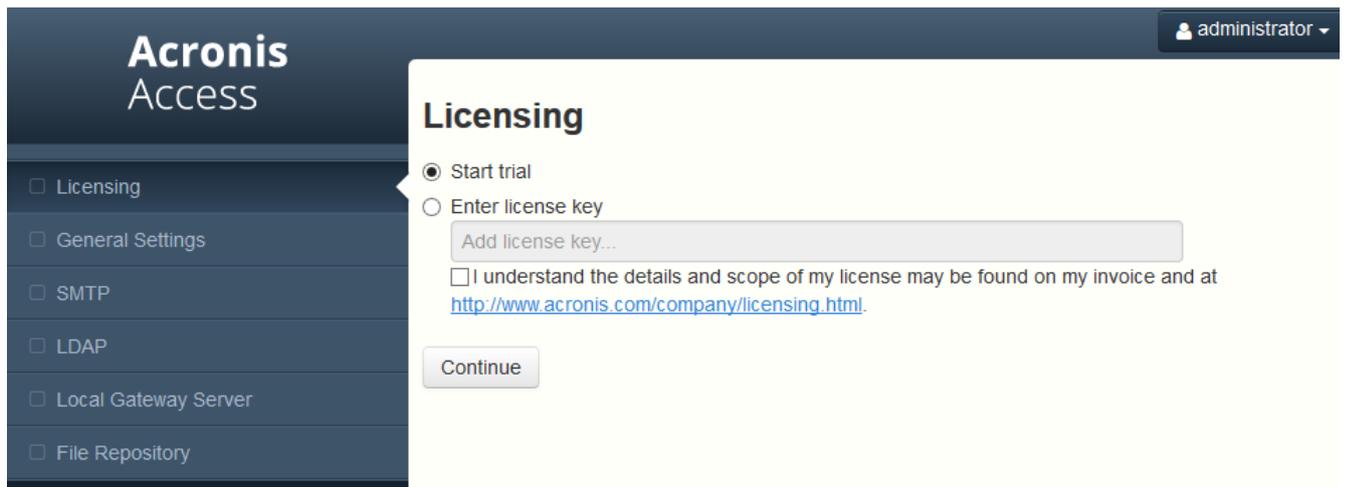
Navigate to the Acronis Access's web interface using the IP address and port specified in the configuration utility. You will be prompted to set the password for the default administrator account.

---

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

---

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

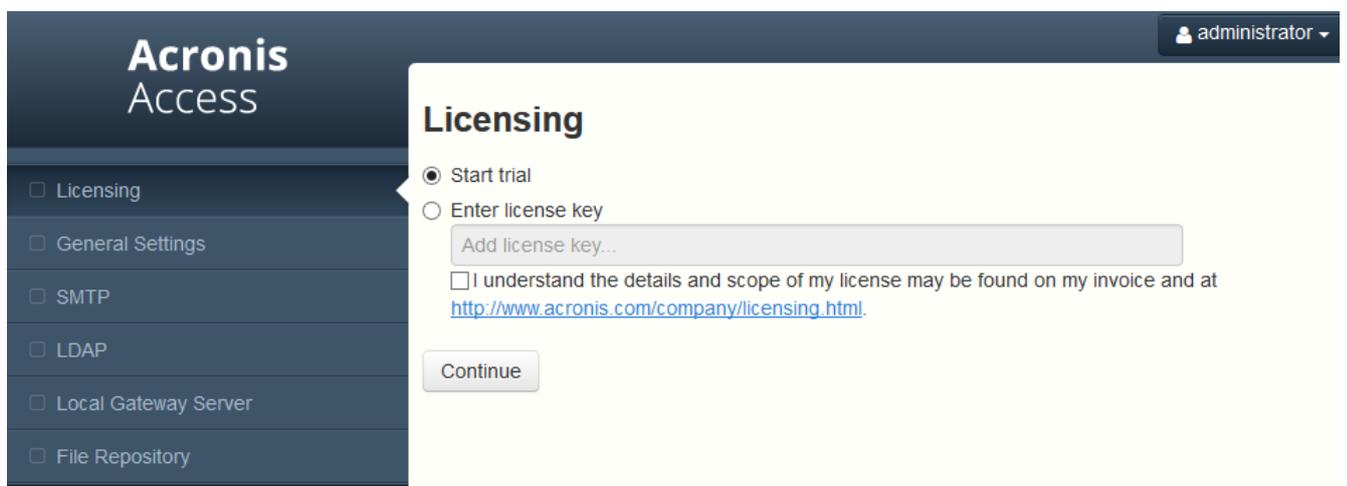


- General Settings cover settings of the web interface itself, like the language, the color scheme, the server name used in admin notifications, licensing and administrators.
- LDAP settings allow you to use Active Directory credentials, rules and policies with our product.
- SMTP settings cover functionality in both Mobile Access features and Sync & Share features. For Mobile Access, the SMTP server is used when sending enrollment invitations. Sync & Share features use the SMTP server to send folder invitations, warnings, summaries of errors.

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

## Going through the initial configuration process

### Licensing



#### 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="access.mycompany.com"/>
Mobile Client Enrollment Address	<input type="text" value="192.168.1.72:3000"/>
Color Scheme	<input type="text" value="Dark Blue"/>
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 a Color Scheme. Current options are Gray, Purple, Cappuccino, Blue, Dark Blue and Orange.
5. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
6. 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.gililabs.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="pam@gililabs.com"/>
Use SMTP authentication?	<input type="checkbox"/>

---

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

---

Enter the DNS name or IP address of your SMTP server

Enter the SMTP port of your server.

If you do not use certificates for your SMTP server, unmark **Use secure connection?**.

Enter the name which will appear in the "From" line in emails sent by the server.

Enter the address which will send the emails sent by the server.

If you use username/password authentication for your SMTP server, mark **Use SMTP authentication?** and enter your credentials.

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

1. Press **Save**.

## LDAP

### LDAP

Directory Services, like 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.

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

---

**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**.

## Local Gateway Server

### Local Gateway Server

Your local Gateway Server is being administered via address 192.168.1.72:443.  
What address should client connections use to contact the Gateway Server? For example: gateway.example.com

---

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

---

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

## File Repository

1. Select a file store type. Use **Filesystem** for a file store on your computers or **Amazon S3** for a file store in the cloud.
2. Enter the DNS name or IP address for the file repository service.

---

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

---

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

For further instructions on using activEcho, visit the Quick Start Guide for activEcho (p. 93).

## 1.5 Clustering Acronis Access

Acronis Access allows the configuration of high-availability setups without needing third-party clustering software. This is configured through the new Cluster Groups feature introduced in Acronis Access 5.1. The setup procedure is simple, but provides high-availability for the Acronis Access

Gateway Servers as they are the component under the heaviest load. All of these configurations are managed through the Acronis Access Server.

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

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

## 1.6 Load balancing Acronis Access

Acronis Access supports load balancing. For more information please visit the Load Balancing Acronis Access and Cluster Groups articles.

## 2 Upgrading

### In this section

Upgrading from Acronis Access to a newer version .....	17
Upgrading from mobilEcho 4.5 or earlier .....	18
Upgrading from activEcho 2.7 or earlier .....	60
Upgrading Clustered Configurations.....	79

### 2.1 Upgrading from Acronis Access to a newer version

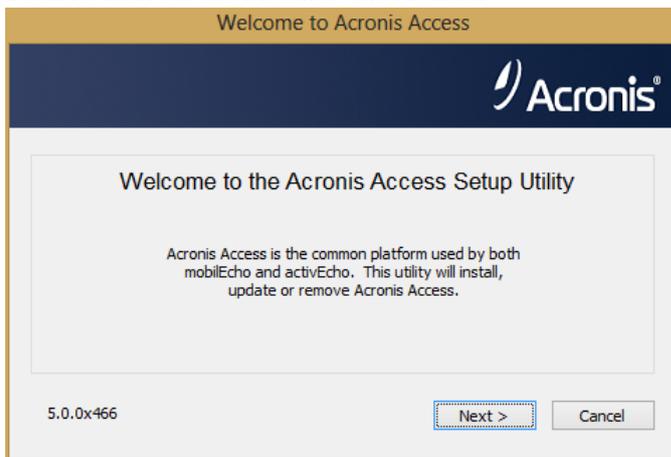
The upgrade procedure from a previous version of Acronis Access is a simplified process and requires almost no configuration.

#### 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\**.

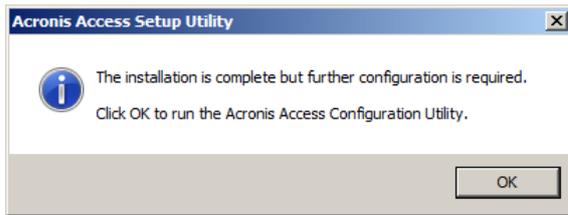
#### Upgrade

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.

## 2.2 Upgrading from mobilEcho 4.5 or earlier

### In this section

Before You Begin.....	18
The Upgrade Process .....	26
Downgrading to mobilEcho 4.5.....	59

### 2.2.1 Before You Begin

#### Back up mobilEcho before upgrading

Please back up the data files used by your existing mobilEcho server. The Acronis Access installer backs up these files, but to be safe, it is recommended that you have your own backup copy before you begin the upgrade.

The process for backing up and restoring a mobilEcho 4.5 or earlier server can be found here: <http://docs.grouplogics.com/display/MobilEcho/mobilEcho+Server+Backup+and+Restoration>

**Upgrade your version of mobilEcho to version 4.5 before proceeding with the upgrade to Acronis Access.**

#### Know your configuration

Before you proceed with the upgrade make sure you know the following:

- Do you have both mobilEcho and activEcho installed?
- Are they on the same computer or on separate machines?
- Which ports is mobilEcho using? On which port is the File Server and on which port is the Management server?
- Which port is activEcho using? Is the File Repository on the same machine?

#### Enhancements

Acronis Access includes a number of enhancements that improve the configuration and management of mobilEcho servers, as well as consolidate management of both the mobilEcho and activEcho products into a single console. This guide will describe the architectural and functional changes you'll need to consider as you upgrade to Acronis Access.

In Acronis Access, you don't need to setup Network Reshare Path Mapping, because we're doing it automatically, but you have to have a "Folder" Data Source created that points to each server hosting home directories.

### **You must carefully plan for your upgrade**

Acronis Access introduces extensive architectural and functional changes to mobilEcho's software services, database/settings locations, and administration. While these changes introduce powerful new features and integration, the upgrade to Acronis Access requires careful consideration.

For single server deployments of mobilEcho, the process is fairly straightforward. If you are using a reverse proxy server, a load balancer, have multiple mobilEcho servers, or are using Microsoft Failover Clustering, it is essential that you understand the upgrade considerations in this document for your specific scenario.

This document includes the details you need to plan for and safely upgrade to Acronis Access. It is highly recommended that you perform this upgrade on a test environment that simulates your unique mobilEcho deployment, before you upgrade your production mobilEcho server(s).

### **Load balanced mobilEcho servers and Microsoft Failover Clusters**

If you have deployed multiple mobilEcho servers front-ended by a load balancer or if you are running mobilEcho on a Microsoft Failover Cluster, you will need to upgrade to Acronis Access 5.1 or newer. A new feature has been introduced in 5.1 that allows groups of load balanced Gateway servers to be automatically administered from within the Acronis Access Server console. This feature eliminates the need to replicate registry settings and script updates to your servers. Adding a new data source (volume) to your servers is a one step process that is handled automatically by the management console. For more information, visit the Cluster Groups article.

---

*Installing and upgrading mobilEcho on a Windows Failover Cluster is a complicated process. The architecture changes introduced in mobilEcho 5.0 require change to the way mobilEcho works on Windows Failover Clusters.*

*For instructions on installing Acronis Access on a cluster, visit the [Installing Acronis Access on a cluster](#) article.*

*For instructions on upgrading a mobilEcho cluster to an Acronis Access cluster, visit the [Upgrading Acronis Access on a cluster](#) article.*

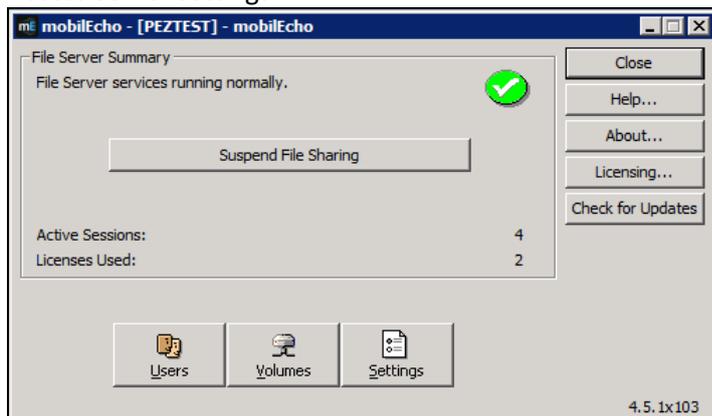
---

### **Architectural and Terminology Changes**

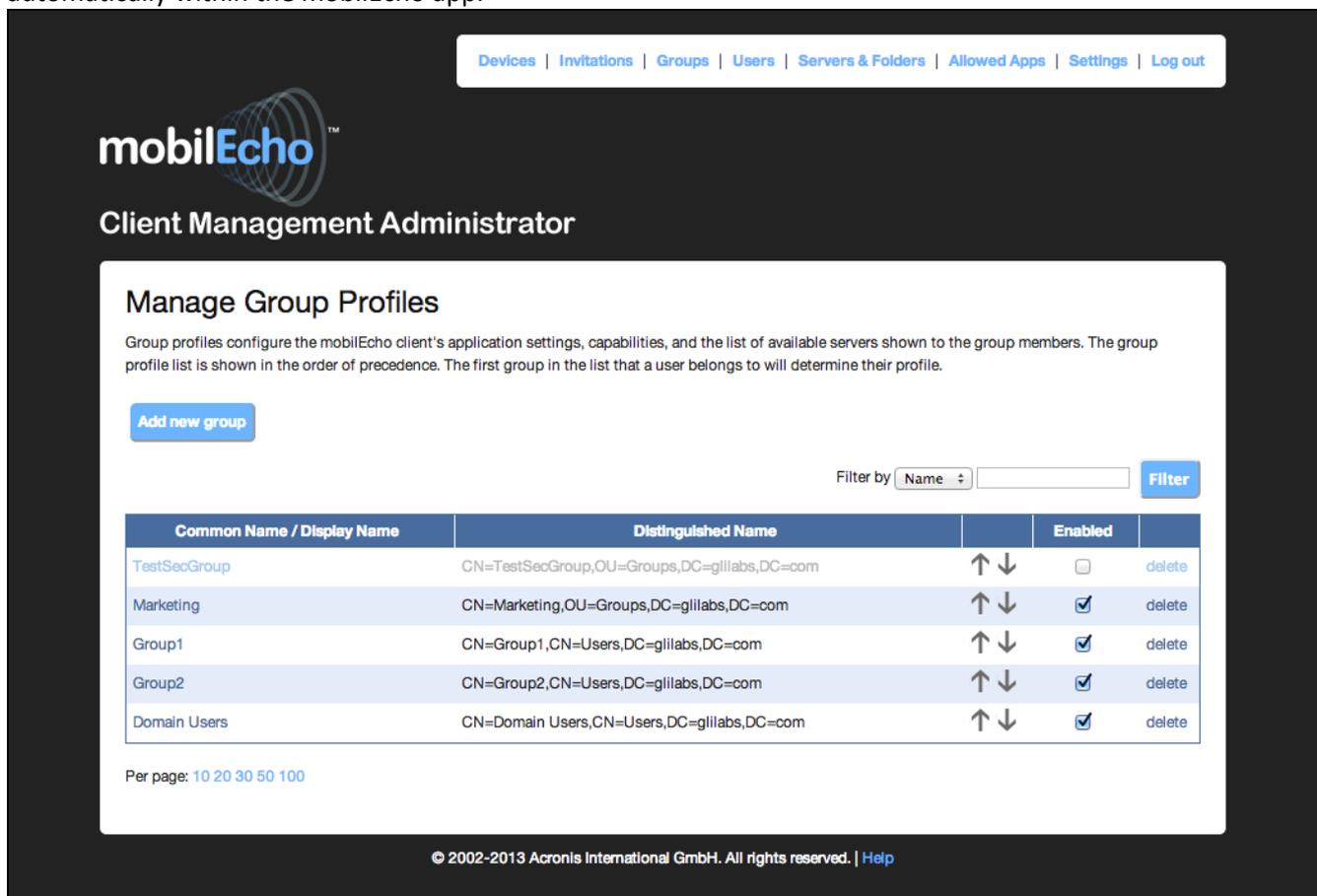
Acronis has consolidated the mobilEcho and activEcho products into a common software platform. These two products continue to be licensed separately and can be used separately or together, but they now share a common installer and administration console. This common web-based console is called the Acronis Access Server.

### **mobilEcho 4.5 and earlier included two management consoles:**

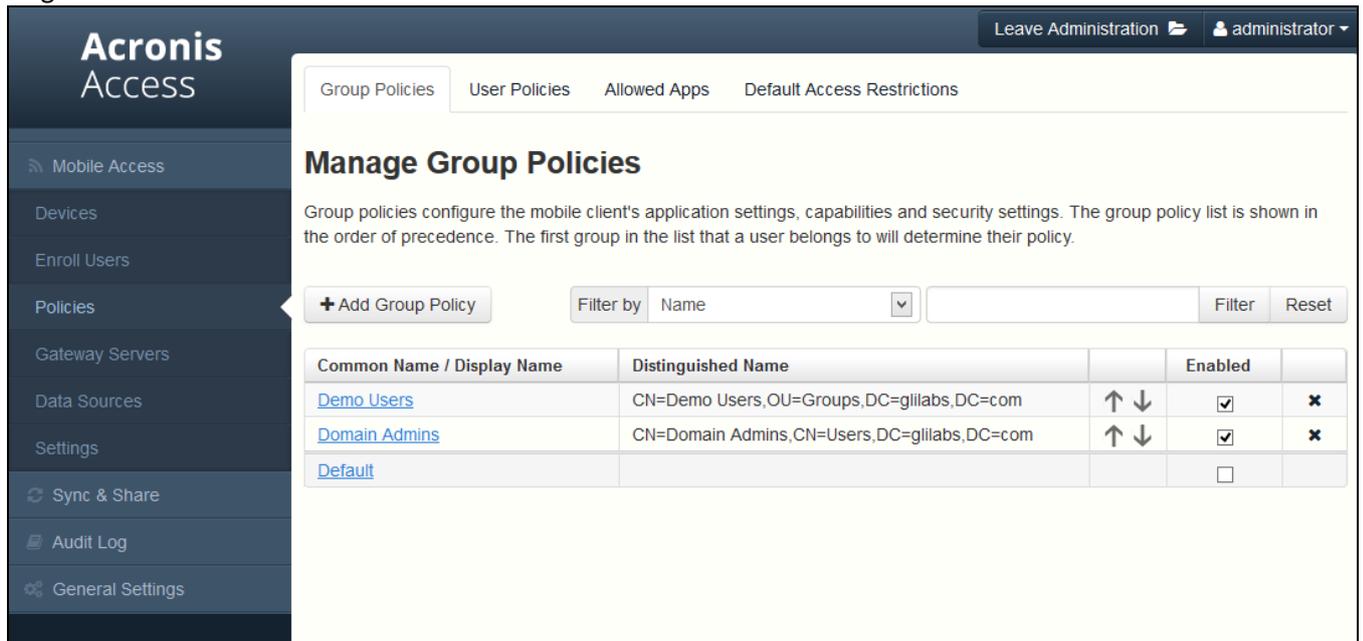
**mobilEcho Administrator** – This Windows program was used to define the file share “Volumes” that were available to mobilEcho clients, to monitor active users, and to configure general mobilEcho File Access Server settings.



**mobilEcho Client Management Administrator** – This web-based console was used to onboard, monitor and remote wipe mobilEcho client users, to define client security and configuration policies, and to assign the mobilEcho servers, network folder shortcuts, and synchronized folders that appear automatically within the mobilEcho app.



With the release of Acronis Access, these two management consoles have been combined into a single web-based console called Acronis Access Server.



The Acronis Access Server is a web application that fills the following roles:

- mobilEcho administration console
- activEcho administration console
- activEcho client web interface

If you are only using the mobilEcho product, your existing mobilEcho Client Management Administrator web console (typically running on port 3000 of your mobilEcho server) will be upgraded to an Acronis Access Server web console when you upgrade to Acronis Access.

The functions within the mobilEcho Administrator Windows program are now handled by the Acronis Access Server web console. Upon upgrading to Acronis Access, you will no longer use the mobilEcho Administrator to configure your mobilEcho File Access Server service and it will be removed from your mobilEcho server.

### Settings are no longer stored in the Windows Registry

Earlier versions of mobilEcho stored mobilEcho File Access Server settings and configured Volumes in the Windows Registry. When upgrading to Acronis Access, these settings are moved to an internal SQL database. If you have any automated processes that add mobilEcho Volumes directly to the Windows Registry, or that back up mobilEcho's registry settings, these processes will need to be modified to act on the SQL database instead.

On an upgraded server, this SQL database is located here by default:

`C:\Program Files (x86)\Group Logic\mobilEcho Server\database\mobilEcho.sqlite3`

If you are managing Volumes for a set of load balanced mobilEcho servers by directly editing the registry, a new clustered mobilEcho server management feature is being introduced that will alleviate the need to make Volume changes in the registry.

## Administering your Acronis Access server

### Existing settings

All existing mobilEcho 4.5 or earlier volumes, enrolled users, policies, assigned servers and folders, and allowed apps are migrated to your Acronis Access Server during the upgrade process. Existing mobilEcho client users will continue to connect to the server without any client side changes necessary, and will receive the same policies and data sources. While it is recommended they upgrade to the Acronis Access iOS client app or Acronis Access Android client app, older versions of the client app are compatible with the Acronis Access server.

### Configuring server administrators

Any existing users or groups configured as mobilEcho administrators before your upgrade to Acronis Access continue to have full admin rights to the Acronis Access Server web console. Acronis Access introduces new role-based admin rights that can be used to limit admin capabilities for specific users or groups. To add or edit administrators, visit the Administrators page on the General Settings menu.

**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 begins with

## Email Templates

If you have customized the email template used for the mobilEcho Enrollment Invitation email that is sent to your users, this email template is not migrated when upgrading to Acronis Access. There is a new interface for editing email templates. In the Acronis Access Console, you will need to open the Email Templates page in the General Settings menu and modify the email template as required. For more information, visit the Email Template Settings article.

**Note:** A copy of your previous mobilEcho templates can be found in the **Legacy mobilEcho files** folder by default located here: **C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files**. The files are named **invitation.html.erb** and **invitation.txt.erb**. These files can be used as a reference when customizing the new templates.

## Data Source / Volume management

Acronis Access consolidates the server administration features of the mobilEcho Administrator Windows program and the mobilEcho Client Management Administrator web console into a single web interface. By doing so, the concept of Volumes is no longer required.

Giving users access to a new file share or SharePoint location is now a one step process. To do so, click Add New Folder on the Folders tab of the Data Sources page. In this single step, you will:

1. Give the Folder a Display Name that your users will see
2. Select the Gateway Server you would like to use to provide access to this data file
3. Select the type of data source: Local folder on the Gateway Server, SMB/CIFS share, SharePoint Site or Document Library, or activEcho server.
4. Select whether this folder is automatically synchronized to the users is it assigned to.
5. Select whether this folder is displayed in the root of the mobilEcho server, assuming your users are configured to allow browsing the root of the server.

- Assign this folder to a collection of Active Directory (AD) users or groups so that it automatically appears in their mobilEcho app.

**Edit Folder**

Display Name: Demo Share

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

Local (192.168.1.141:443)

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: D:\Demo Share

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 Search

**This folder is assigned to:**

Common Name	Distinguished Name

Save Cancel

To configure a Gateway Server to automatically appear in the mobilEcho client app, use the Gateway Servers Visible on Clients tab. On this page you can assign AD users or groups to your Gateway Server(s) and these users will see these servers listed in their mobilEcho app. They will be able to view and browse into any Folders that have the “Show when browsing server” property enabled AND

that they have file permissions to access.

Folders Gateway Servers Visible on Clients Assigned Sources

### Gateway Servers Visible on Clients

Acronis Access mobile users can be assigned, by Active Directory user or group, to have specific Gateway Servers appear in their Acronis Access mobile app. These users will then be able to browse the visible data sources on these servers which they have existing file permissions to access.

Display Name	Server Address	Assigned to	
Local	192.168.1.141:443	Domain Admins	
Main Server	192.168.1.140:443	Demo Users	

### Start using advanced mobilEcho Client Management features

If your existing mobilEcho server did not have the mobilEcho Client Management features configured, the Acronis Access install process will guide you through the basic configuration that will allow you to start using these advanced features.

To get started you will be asked for LDAP settings to allow Acronis Access Server to enumerate your Active Directory users and groups and for SMTP settings so that enrollment email invitations can be sent to your users.

Once this configuration is performed, you can take advantage of user and group policies, per-device tracking and many additional features.

### New Audit Logging option

Acronis Access includes a new Audit Logging feature that allows Acronis Access Gateway servers to report all file activities back to the Acronis Access web console. These activities are stored in a consolidated Audit Log that can be used to audit all file operations being performed by users.

Audit Logging is disabled by default on Gateway Servers. To enable audit logging on a Gateway Server, visit the Gateway Servers page, click the Details button for the desired server, then select the Audit Logging option on the Logging tab.

### Main Server

Status Logging Active Users

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

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

Audit Logging  Debug Logging

Archive Log File

Close

Events will then be logged into the Audit Log, accessible from the main menu of the Acronis Access Server.

## 2.2.2 The Upgrade Process

### Acronis Access Upgrade Process

First, please identify the type of mobilEcho deployment you will be upgrading. The instructions for these scenarios are detailed in the next section of this document. The most common scenarios are:

- 1. Single mobilEcho Server without Client Management configured**
  - A single Windows server, running the mobilEcho File Access Server service only
- 2. Single mobilEcho Server with Client Management**
  - A single Windows server, running both the mobilEcho File Access Server service and the mobilEcho Client Management service
- 3. Multiple mobilEcho Servers with Client Management**
  - Multiple Windows servers running the mobilEcho File Access Server service, with one of those Windows servers also running the mobilEcho Client Management service
- 4. Multiple mobilEcho Servers front-ended by a load balancer**
  - One standalone Windows server running the mobilEcho Client Management service, and two or more Windows servers running the mobilEcho File Access Server service only, front-ended by a load-balancer.
- 5. Windows Failover Cluster**
  - Supported in version 5.0.3 or newer.
  - A multi-node Windows Failover Cluster running mobilEcho on 1 or more active/active or active/passive virtual servers.

#### Important notes on Scenario 4 – Load Balanced mobilEcho File Access Servers

---

*If you are running multiple mobilEcho File Access Servers front-ended by a load balancer, each of these mobilEcho servers must be kept configured with identical mobilEcho Volumes, so that users can connect to any node to access their files. The most common way to maintain identical Volumes on these sets of load balanced servers is to replicate the mobilEcho Volumes settings, which are stored in the registry in mobilEcho 4.5 or earlier.*

*In Acronis Access, the Volumes settings have been moved into a SQL database. If you upgrade to Acronis Access, your existing scripted registry updates used when adding new volumes to your mobilEcho servers will cease to work. A new feature has been introduced in 5.1 that allows groups of load balanced Gateway servers to be automatically administered from within the Acronis Access Server console. This feature eliminates the need to replicate registry settings and script updates to your servers. Adding a new data source (volume) to your servers is a one step process that is handled automatically by the management console. For more information, visit the [Cluster Groups](#) article.*

---

#### Important notes on Scenario 5 – Windows Failover Cluster

---

*Installing and upgrading mobilEcho on a Windows Failover Cluster is a complicated process. The architecture changes introduced in mobilEcho 5.0 require change to the way mobilEcho works on Windows Failover Clusters.*

*For instructions on installing Acronis Access on a cluster, visit the [Installing Acronis Access on a cluster](#) article.*

*For instructions on upgrading a mobilEcho cluster to an Acronis Access cluster, visit the [Upgrading Acronis Access on a cluster](#) article.*

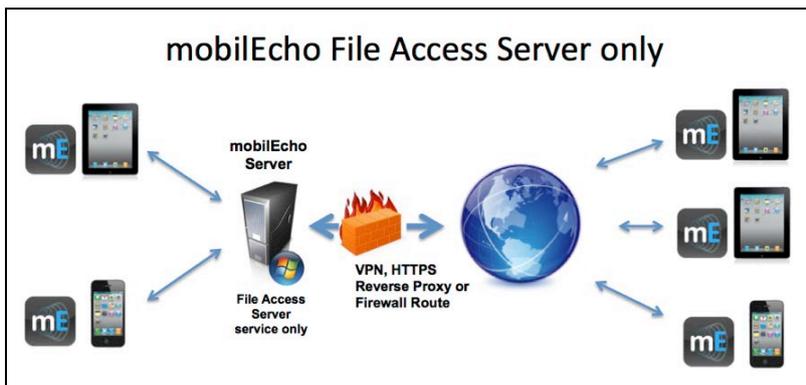
---

## In this section

- Upgrading a single mobilEcho server without Client Management configured 27
- Upgrading a single mobilEcho server with Client Management enabled 39
- Upgrading multiple mobilEcho servers with Client Management.....54
- Upgrading a single mobilEcho server with Client Management enabled and an activEcho server 59

### 2.2.2.1 Upgrading a single mobilEcho server without Client Management configured

#### Scenario 1 - Upgrading a single mobilEcho server without Client Management configured



In this scenario, you have a single Windows Server running just the mobilEcho File Access Server service. With this architecture, you have not enabled the optional mobilEcho Client Management Administrator web console and are not using mobilEcho’s policy and remote management features. When your users set up mobilEcho, they manually enter their server name, username, and password into the mobilEcho app.

When upgrading to Acronis Access, your mobilEcho File Access Server is upgraded to an Acronis Access Gateway Server. This service will continue to accept connections from mobilEcho clients and to act as the gateway to any file server, NAS or SharePoint data sources your users are accessing.

The upgrade will also install the Acronis Access Server web console. This new console replaces the mobilEcho Administrator Windows program previously used to administer your mobilEcho server. The Acronis Access Server web console allows you to administer your mobilEcho servers from one unified web interface and will allow you to take advantage of additional client management features if you desire.

#### To perform an upgrade to Acronis Access:

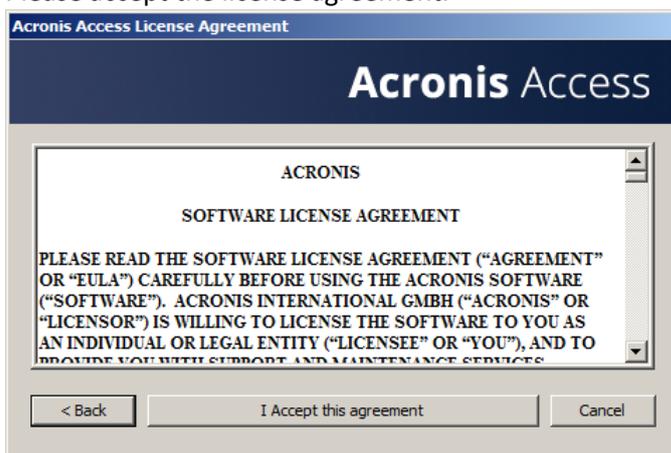
1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Download the Acronis Access Server installer to your mobilEcho server and run the installer.
  - a. To access the latest installer, please visit: [http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598)
  - b. You will need to enter your product serial number for verification before downloading the installer.

c. The installer file is named: AcronisAccessSetup.exe

4. Click **Next** on the Welcome Screen.



5. Please accept the license agreement.



6. Click the **Upgrade** option to automatically upgrade your mobilEcho File Access Server service to an Acronis Access Gateway Server. In the upgrade process, the Acronis Access Server and its required services will also be installed.

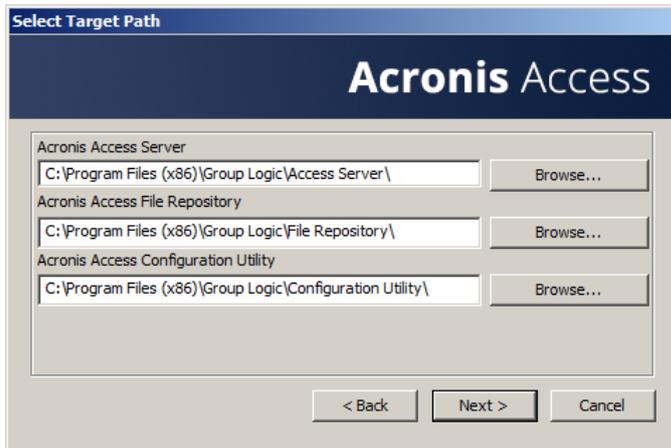
---

**Note:** Do not choose **Custom** and install only the Acronis Access Gateway Server. The Acronis Access Server is the new web console that replaces the mobilEcho Administrator Windows program. It is required to administer your mobilEcho server. If you do not install it, you will have no means to change your mobilEcho settings or to give access to new file shares.

---



7. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing mobilEcho server, these paths will default to your existing installation location. We recommend you do not change these installation paths.



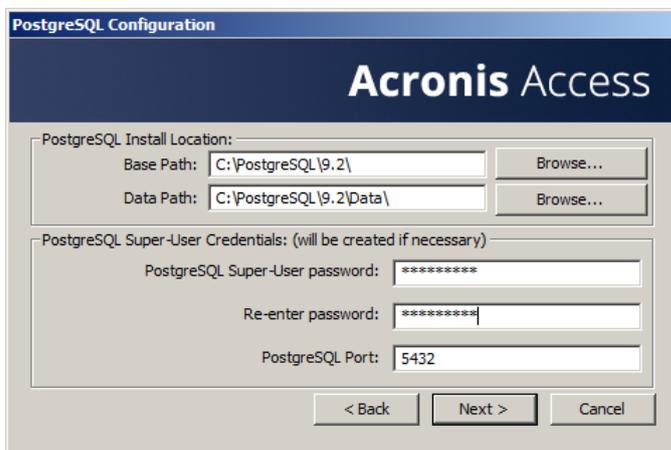
8. The Acronis Access Server uses a PostgreSQL database to store its settings. This database is required and is installed automatically.

---

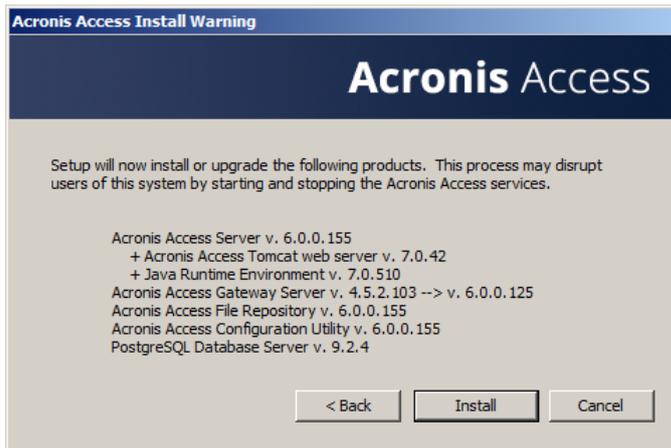
**Note:** Please enter and confirm a Super-User password for the “postgres” administrative account. Be sure to record this password in a safe place.

**Note:** It is not recommended that you alter the PostgreSQL install location or port.

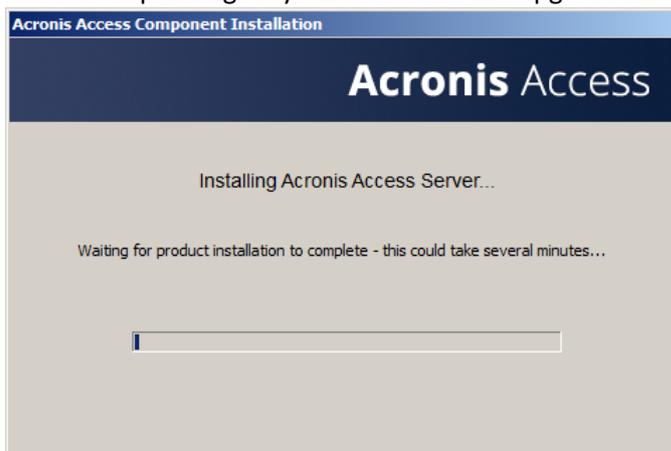
---



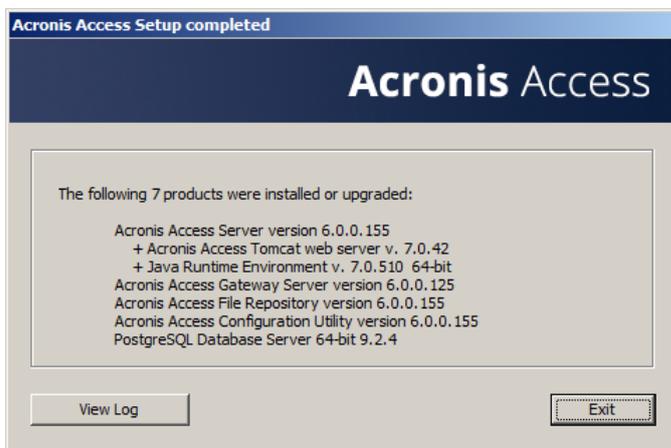
9. Please review the services being installed and upgraded. Then click **Install** to begin the upgrade.



**Note:** All required components will be automatically installed in sequence. This may take 5 to 15 minutes depending on your server. Future upgrade installs will be quicker.



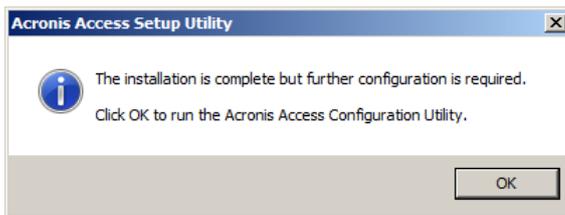
10. Once installation has completed, a summary of the components installed is shown. Click **Exit** to continue.



11. At this point in the upgrade process, all necessary software has been installed, but you must now configure the network interfaces, ports, and certificates that will be used.

**IMPORTANT NOTE:** *If you do not proceed with this configuration step, your mobilEcho server will not be functional. This step is mandatory.*

When exiting the installer, you will be prompted to run the Acronis Access Configuration Utility. Click **OK** to continue.



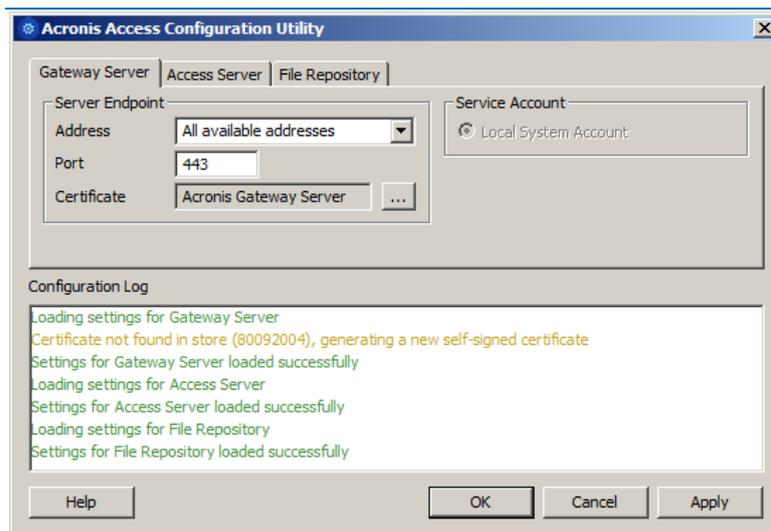
If you accidentally skip this step or need to change your network interfaces, ports, or certificates in the future. You can manually run the configuration utility at any time.

On upgraded mobilEcho servers, the utility's default location is:

**C:\Program Files (x86)\Group Logic\Configuration Utility\AcronisAccessConfiguration.exe**

12. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core mobilEcho service that your mobilEcho clients connect to and that gives access to your file servers, NAS, and SharePoint servers. This service was called the mobilEcho File Access Server prior to Acronis Access.

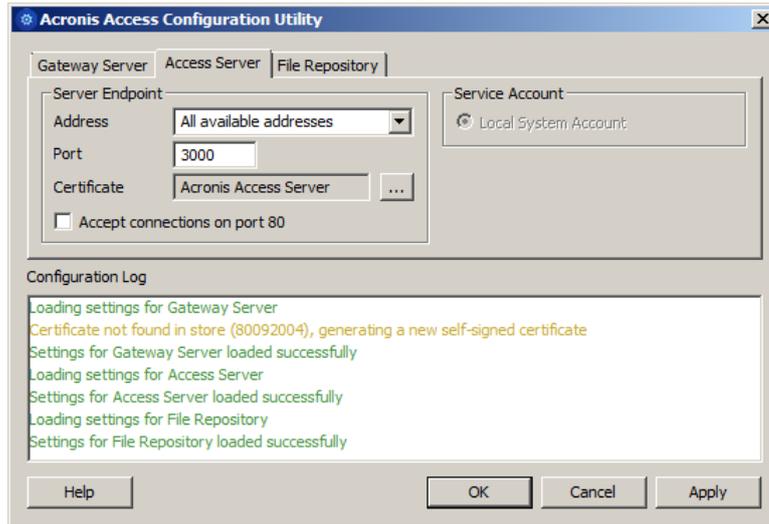
**Note:** You existing settings are retained. Please confirm that these settings match your existing mobilEcho File Access Server settings. This service typically runs on all available network addresses on port 443. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.



13. The Access Server tab is used to configure your Acronis Access Server's network address, port, and certificate. The Acronis Access Server is the web console that is used to perform all server administration and remote client management. This console replaces the mobilEcho Administrator Windows program and is required.

**Note:** Please review the settings for the Access Server. The default settings are recommended. This web console typically runs on all available network addresses on port 3000. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be

generated.



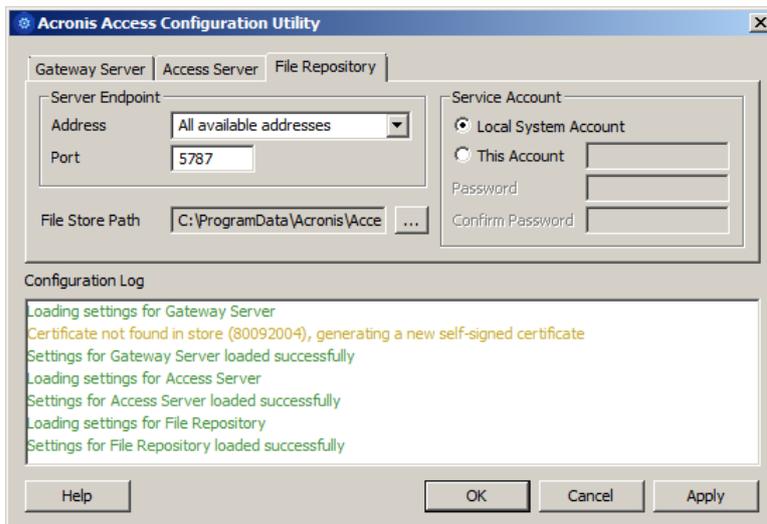
14. Acronis Access Server requires that a File Repository location be selected. If you are using mobilEcho only, this File Repository will not be used to store anything, but setting a location is still required.

*This repository is used by Acronis' activEcho file sync and share features. These features will not be enabled if you are upgrading a server that does not already have them installed, but you can chose to enable them at a later time, if desired.*

*The default location for the File Repository is:*

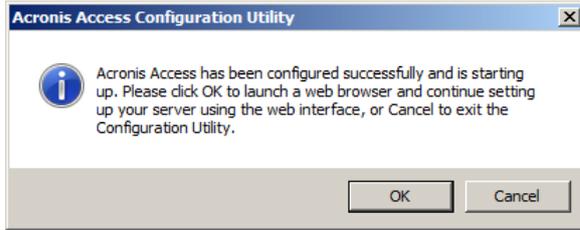
**C:\ProgramData\Acronis\Access\FileStore**

*If you would like to try out activEcho in the future, you may want to select a location on a data drive instead of the C: drive. This location can be modified post-install, too.*



15. Click **OK** to exit the Configuration Utility and apply these settings.
16. You will now log into the Acronis Access Server web console for the first time to complete your configuration. You will be prompted to click OK to launch a web browser and complete this

configuration.



### Required initial configuration of Acronis Access:

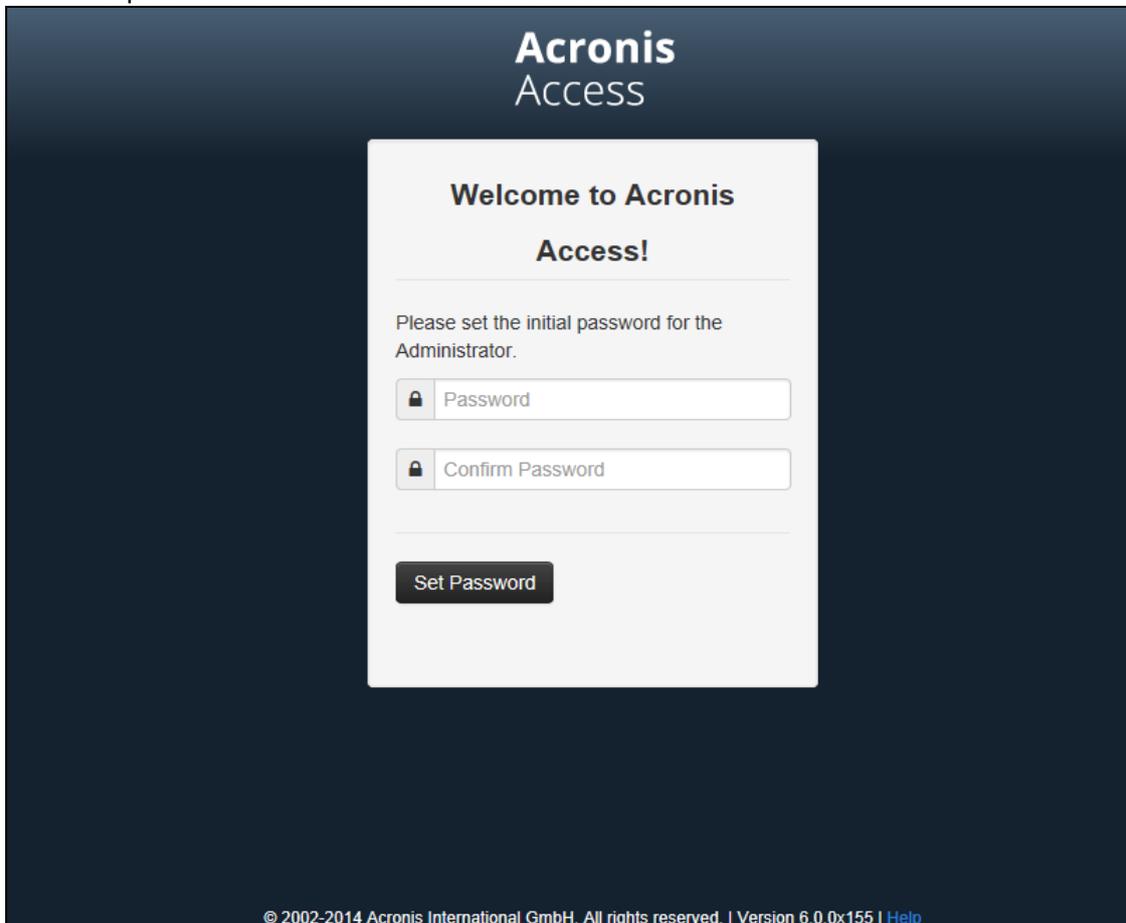
1. The Acronis Access Server web console should open automatically after completing the steps above. It may take 30 seconds or so for the services to start up and the web page to load for the first time.
2. If the web page does not load automatically, open a web browser and navigate to the Access Server HTTPS address and port you selected in the Configuration Utility.
  - a. For example: <https://mobilecho.mycompany.com:3000> or <https://localhost:3000>

---

**Note:** Most of the settings in the SMTP, General Settings and LDAP pages should already be present from your mobilEcho installation.

---

3. Acronis Access Server requires that a local administrator account be created. Please enter and confirm a password for this local administrator account.



- a. The username for this local administrator account is: administrator
- b. Keep this local administrator password in a safe place. It will be needed to log in as an administrator, until you configure additional administrative users.

- c. Once your server is configured, you will be able to designate additional Active Directory users or groups to act as administrators of the server.
- 4. You will now be presented with a setup wizard that will guide you through the remainder of the configuration process.
- 5. Licensing
- a) You will be prompted to enter the new type of license or continue using your old mobilEcho license.
- 6. SMTP settings

The screenshot displays the Acronis Access web interface for configuring SMTP settings. The left sidebar shows navigation options: Licensing, General Settings, SMTP (selected), and LDAP. The main content area is titled 'SMTP' and includes a descriptive text box: '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.' Below this, the configuration fields are as follows:

- SMTP Server Address:
- SMTP Server Port:
- Use secure connection?:
- From Name:
- From Email Address:
- Use SMTP authentication?:

At the bottom of the form, there are three buttons: 'Save', 'Send Test Email', and 'Skip SMTP Setup'.

- a. You will be prompted to configure the SMTP settings used by the Access Server to send email alerts and client enrollment invitations.

b. There is an option to send a test email to confirm these settings.

## 7. LDAP settings

**Acronis Access** administrator

### LDAP

Directory Services can be used to provide mobile access to users in your organization. LDAP is required for managed mobile access.

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

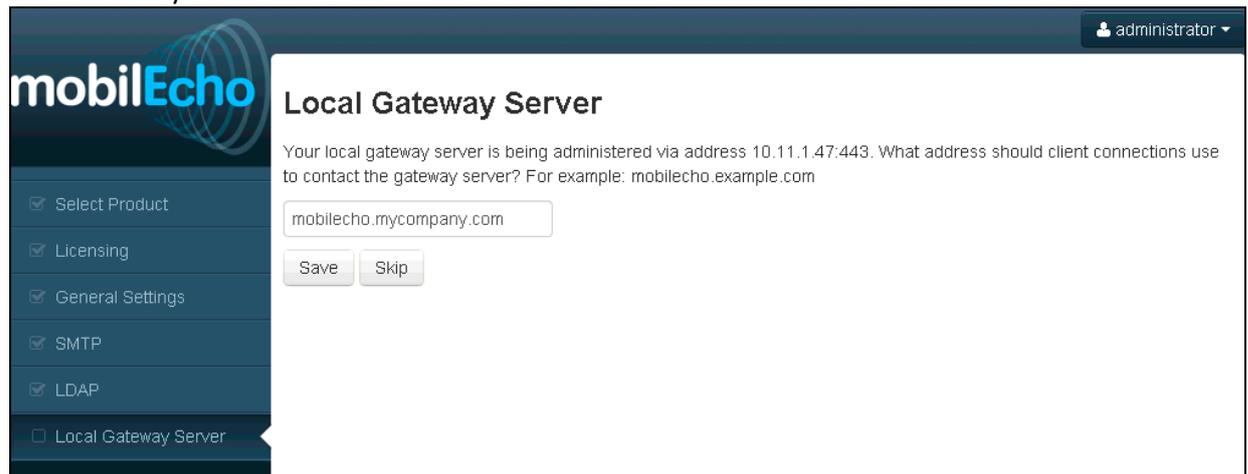
LDAP Search Base

Domains for LDAP Authentication

- The Acronis Access Server needs an LDAP connection to search your Active Directory for the users and groups you would like to assign policies and data sources to.
- Please enter the LDAP information for an Active Directory server on your network. If you have a multi domain network this will need to be a Global Catalog Server on port 3268 or 3269 (for SSL connections). Tool tips are provided for each field for more detail.
- You are required to configure an LDAP username and password to be used when the server makes request to LDAP.

d. The LDAP settings you enter will be tested when you save them.

8. Local Gateway Server – Client connection address



- a. Your mobilEcho Gateway Server has been automatically paired for administration by your Acronis Access Server web console. This connection is made by IP address by default, and can be modified later.
- b. In this step, you will need to enter the network address that your mobilEcho clients use to connect to this mobilEcho server. This is typically a DNS address and may be the DNS address of this server, but could be the address of a proxy server used to gain access to this server.

9. Your initial configuration is now complete.

- a. Click **Finish** Configuration to continue.

**Working with your mobilEcho Gateway Server**

Your Gateway Server is automatically registered during the setup process and will appear in the Gateway Servers list, where you can adjust its settings and view its details and status.

Display Name	Server Address	Assigned to	
Local	192.168.1.141	TG, Demo Users	
Main Server	rrt.gllilabs.com	Domain Admins	

When it was registered, the Volumes that existed on the mobilEcho Gateway Server prior to being upgraded to Acronis Access were imported into the Data Sources – Folders list.

[Folders](#) | [Gateway Servers Visible on Clients](#) | [Legacy Data Sources](#) | [Assigned Sources](#)

[Add New Folder](#)

## Folders

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

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

Type ^	Display Name	Server	🗑️	Path	Sync	✎ ✕
📁	test folder	Local	✔️	D:\testfolder	None	✎ ✕
🌐	Access	Local	✔️	https://192.168.1.141:3000	None	✎ ✕
📁	Thousand Files	Local	✔️	\\vega\test files\10000 files	None	✎ ✕
📁	SharePoint	Local	✔️	http://sharepoint2010.gllilabs.com:2229	None	✎ ✕

There are no longer “Volumes” in mobilEcho 5.0. Instead of using Volumes to share data sources, you will now create Folders. These Folders have an optional “Show when browsing server” property. When this option is enabled, the Folder will appear when a user browses the root of the Gateway Server in their mobilEcho app, just as Volumes were displayed in mobilEcho 4.5 or earlier.

### Edit Folder

Display Name:

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

- Local (192.168.1.141)

Data Location:

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:

Sync:

Show When Browsing Server

Require Salesforce.com Activity Logging

**Assign This Folder to a User or Group**

Find User or Group that begins with

**This folder is assigned to:**

Common Name	Distinguished Name

All the Volumes from your mobilEcho 4.5 or earlier server were imported into to the Acronis Access console as Folders with the “Show when browsing server” property enabled. So, they will continue to appear when your users browse the root of a mobilEcho Gateway Server. Any Folders added later can be configured to act like Volumes by enabling this setting. You can also begin using advanced client management features, such as the ability to add Folders that automatically appear in the mobilEcho client app for the list of Active Directory user or groups you assign them to.

As shown below, the 4 existing Volumes from this mobilEcho 4.5 server were imported into the Folders list after Gateway Server registration, and they continue to appear when browsing the server from the mobilEcho app.

**Folders**

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

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

Type	Display Name	Server	Path	Sync
	test folder	Local	D:\testfolder	None
	Access	Local	https://192.168.1.141:3000	None
	Thousand Files	Local	\\vega\test files\10000 files	None
	SharePoint	Local	http://sharepoint2010.gllilabs.com:2229	None

You can also begin to create and use client policies and officially enroll users with your server so that they are managed by these policies. A Default policy that applies to all users can be enabled and configured, or you can add custom policies based on Active Directory users and groups.

Once policies have been configured, you can use the Enroll Users page to send enrollment invitation emails to your users so that they can enroll as managed users.

## 2.2.2.2 Upgrading a single mobilEcho server with Client Management enabled

### Scenario 2 - Upgrading a single mobilEcho server with Client Management enabled



In this scenario, you have a single Windows server that is running mobilEcho 4.5 or earlier. This server has both the required mobilEcho File Access Server service running and the optional mobilEcho Client Management Server service enabled.

When upgrading to Acronis Access, your mobilEcho File Access Server is upgraded to an Acronis Access Gateway Server. This service will continue to accept connections from mobilEcho clients and to act as the gateway to any file server, NAS or SharePoint data sources your users are accessing.

Your mobilEcho Client Management Administrator web console will be upgraded to an Acronis Access Server web console. This new web console allows you to administer your mobilEcho servers and clients from one unified web interface.

#### To perform an upgrade of Acronis Access:

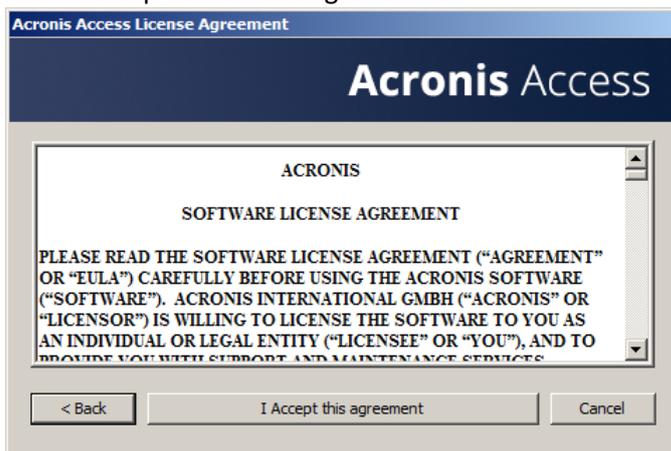
1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Download the Acronis Access Server installer to your mobilEcho server and run the installer.
  - a. To access the latest installer, please visit: [http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598)
  - b. You will need to enter your product serial number for verification before downloading the installer.

c. The installer file is named: AcronisAccessSetup.exe

4. Click **Next** on the Welcome Screen.



5. Please accept the license agreement.

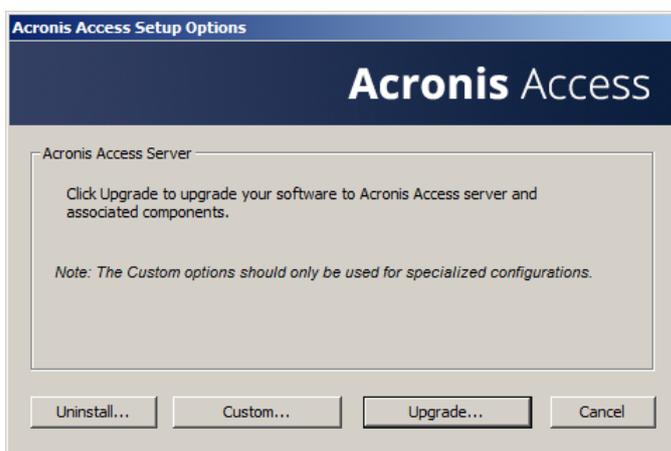


6. Click the **Upgrade** option to automatically upgrade your mobilEcho File Access Server service to an Acronis Access Gateway Server. In the upgrade process, the Acronis Access Server and its required services will also be installed.

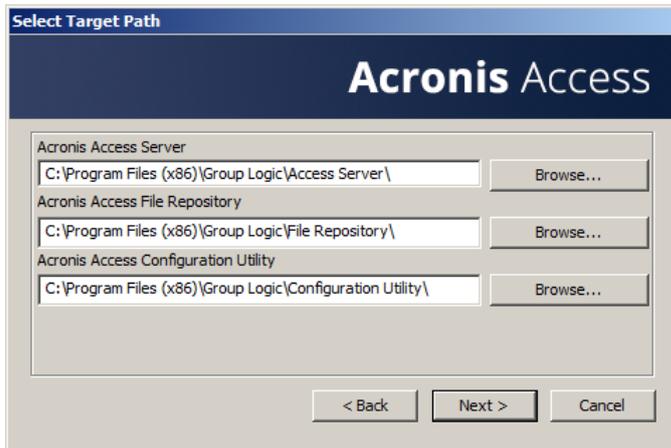
---

**Note:** Do not choose **Custom** and install only the Acronis Access Gateway Server. The Acronis Access Server is the new web console that replaces the mobilEcho Administrator Windows program. It is required to administer your mobilEcho server. If you do not install it, you will have no means to change your mobilEcho settings or to give access to new file shares.

---



7. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing mobilEcho server, these paths will default to your existing installation location. We recommend you do not change these installation paths.



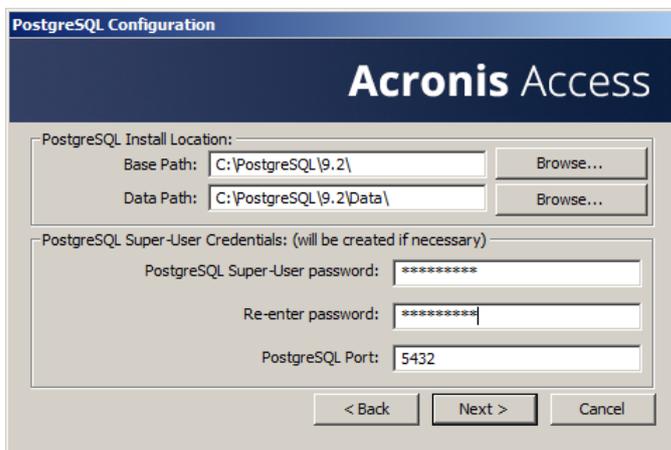
8. The Acronis Access Server uses a PostgreSQL database to store its settings. This database is required and is installed automatically.

---

**Note:** Please enter and confirm a Super-User password for the “postgres” administrative account. Be sure to record this password in a safe place.

**Note:** It is not recommended that you alter the PostgreSQL install location or port.

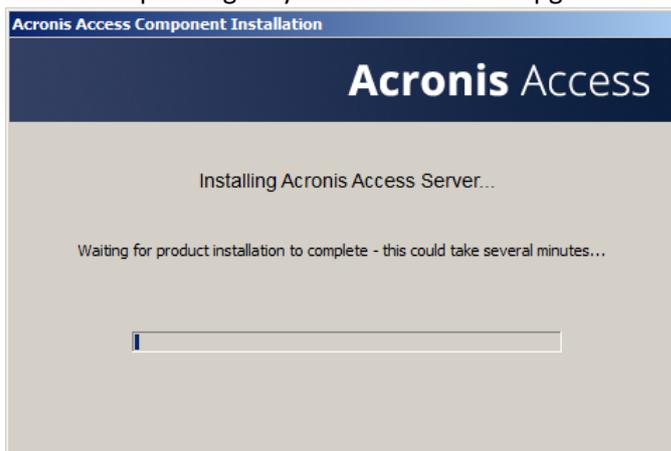
---



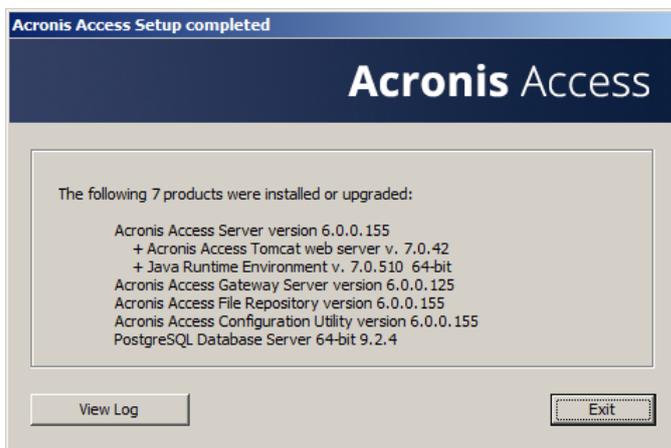
9. Please review the services being installed and upgraded. Then click **Install** to begin the upgrade.



**Note:** All required components will be automatically installed in sequence. This may take 5 to 15 minutes depending on your server. Future upgrade installs will be quicker.



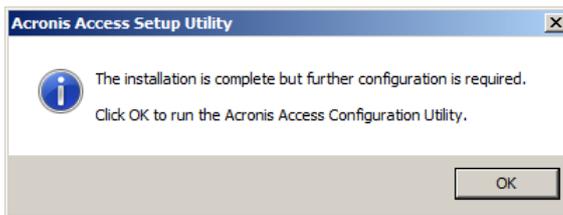
10. Once installation has completed, a summary of the components installed is shown. Click **Exit** to continue.



11. At this point in the upgrade process, all necessary software has been installed, but you must now configure the network interfaces, ports, and certificates that will be used.

**IMPORTANT NOTE:** *If you do not proceed with this configuration step, your mobilEcho server will not be functional. This step is mandatory.*

When exiting the installer, you will be prompted to run the Acronis Access Configuration Utility. Click **OK** to continue.



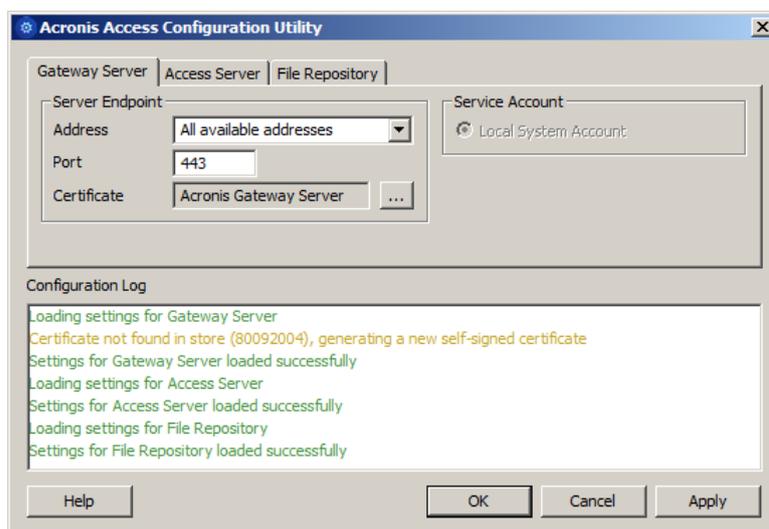
If you accidentally skip this step or need to change your network interfaces, ports, or certificates in the future. You can manually run the configuration utility at any time.

On upgraded mobilEcho servers, the utility's default location is:

**C:\Program Files (x86)\Group Logic\Configuration Utility\AcronisAccessConfiguration.exe**

12. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core mobilEcho service that your mobilEcho clients connect to and that gives access to your file servers, NAS, and SharePoint servers. This service was called the mobilEcho File Access Server prior to Acronis Access.

**Note:** You existing settings are retained. Please confirm that these settings match your existing mobilEcho File Access Server settings. This service typically runs on all available network addresses on port 443. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.

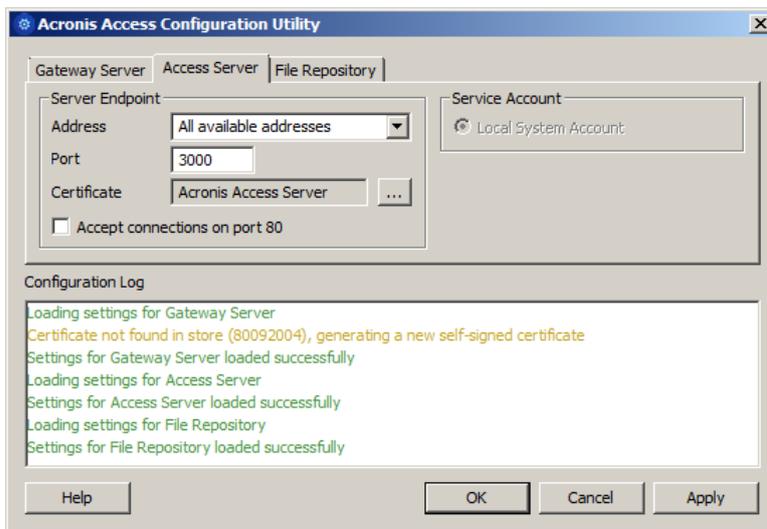


13. The Access Server tab is used to configure your Acronis Access Server's network address, port, and certificate. The Acronis Access Server is the web console that takes the place of your mobilEcho Client Management Server web console.

---

**Note:** Please confirm the settings match your existing mobilEcho Client Management Server settings. This web console typically runs on all available network addresses on port 3000. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.

---



14. Acronis Access Server requires that a File Repository location be selected. If you are using mobilEcho only, this File Repository will not be used to store anything, but setting a location is still required.

---

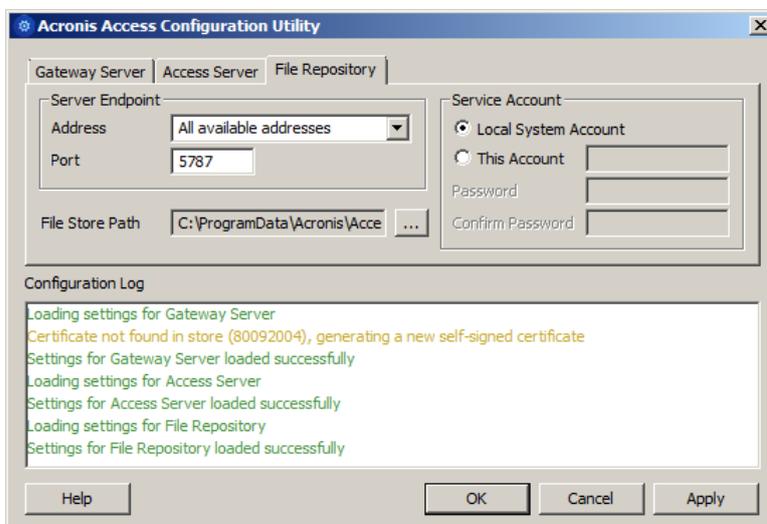
*This repository is used by Acronis' activEcho file sync and share features. These features will not be enabled if you are upgrading a server that does not already have them installed, but you can choose to enable them at a later time, if desired.*

The default location for the File Repository is:

**C:\ProgramData\Acronis\Access\FileStore**

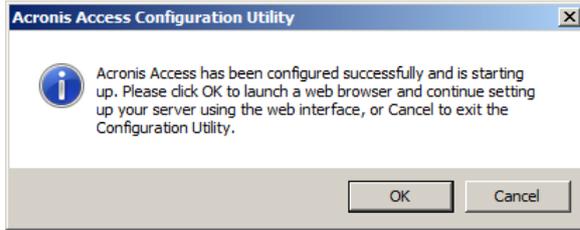
*If you would like to try out activEcho in the future, you may want to select a location on a data drive instead of the C: drive. This location can be modified post-install, too.*

---



15. Click **OK** to exit the Configuration Utility and apply these settings.
16. You will now log into the Acronis Access Server web console for the first time to complete your configuration. You will be prompted to click OK to launch a web browser and complete this

configuration.



**Required initial configuration of Acronis Access:**

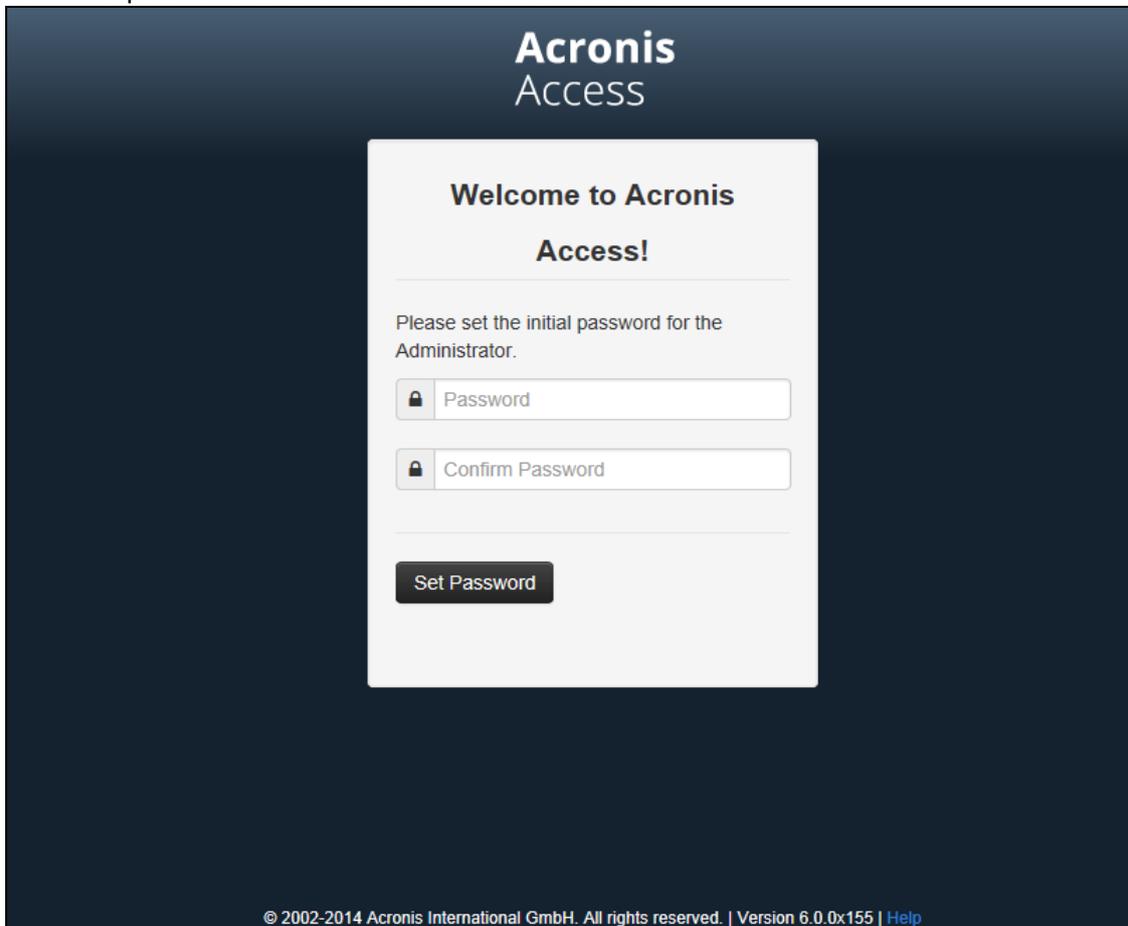
1. The Acronis Access Server web console should open automatically after completing the steps above. It may take 30 seconds or so for the services to start up and the web page to load for the first time.
2. If the web page does not load automatically, open a web browser and navigate to the Access Server HTTPS address and port you selected in the Configuration Utility.
  - a. For example: <https://mobilecho.mycompany.com:3000> or <https://localhost:3000>

---

**Note:** Most of the settings in the SMTP, General Settings and LDAP pages should already be present from your mobilEcho installation.

---

3. Acronis Access Server requires that a local administrator account be created. Please enter and confirm a password for this local administrator account.



- a. The username for this local administrator account is: administrator
- b. Keep this local administrator password in a safe place. It will be needed to log in as an administrator, until you configure additional administrative users.

- c. Once your server is configured, you will be able to designate additional Active Directory users or groups to act as administrators of the server.
4. You will now be presented with a setup wizard that will guide you through the remainder of the configuration process.
5. Licensing
- a) You will be prompted to enter the new type of license or continue using your old mobilEcho license.
6. SMTP settings

The screenshot displays the Acronis Access web interface for configuring SMTP settings. The left sidebar shows navigation options: Licensing, General Settings, SMTP (selected), and LDAP. The main content area is titled 'SMTP' and includes a descriptive text box: '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.' Below this, the configuration fields are as follows:

- SMTP Server Address:
- SMTP Server Port:
- Use secure connection?:
- From Name:
- From Email Address:
- Use SMTP authentication?:

At the bottom of the form, there are three buttons: 'Save', 'Send Test Email', and 'Skip SMTP Setup'.

- a. You will be prompted to configure the SMTP settings used by the Access Server to send email alerts and client enrollment invitations.

b. There is an option to send a test email to confirm these settings.

## 7. LDAP settings

**Acronis Access** administrator

### LDAP

Directory Services can be used to provide mobile access to users in your organization. LDAP is required for managed mobile access.

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

a. The Acronis Access Server needs an LDAP connection to search your Active Directory for the users and groups you would like to assign policies and data sources to.

b. Please enter the LDAP information for an Active Directory server on your network. If you have a multi domain network this will need to be a Global Catalog Server on port 3268 or 3269 (for SSL connections). Tool tips are provided for each field for more detail.

c. You are required to configure an LDAP username and password to be used when the server makes request to LDAP.

d. The LDAP settings you enter will be tested when you save them.

## 8. Your initial configuration is now complete.

a. Click **Finish** Configuration to continue.

### Registering your mobilEcho Gateway Server(s)

When upgrading an existing mobilEcho 4.5 or earlier server, where the mobilEcho Client Management service was configured, all the Servers that were configured on the Servers & Folders page are imported into the Acronis Access Gateway Servers list.

These Gateway Servers are initially imported as Legacy gateway servers. This means they have not yet been registered to be controlled and administered by the Acronis Access web console. This

registration is required to manage these Gateway servers once they have been upgraded to Acronis Access.

In order to be registered for administration, these servers must first be upgraded to Acronis Access. Until they are upgraded, you will continue to use the mobilEcho Administrator Windows program to administer those servers.

As shown in the example below, the two servers in the Servers & Folder page in mobilEcho 4.5 now appear on the Gateway Servers page.

The screenshot shows the mobilEcho Client Management Administrator interface. At the top, there is a navigation bar with links: Devices | Invitations | Groups | Users | Servers & Folders | Allowed Apps | Settings | Log out. The mobilEcho logo is on the left. The main heading is "Client Management Administrator". Below this is a section titled "Servers and Folders" with a descriptive paragraph. Underneath is a sub-section "Assign by user or group" with a "Find user or group" button. The "Servers" section includes an "Add new server" button and a table of existing servers.

mobilEcho Server	Display Name	
192.168.1.141	Local	delete
rrt.gllilabs.com	Main Server	delete

The screenshot shows the Acronis Access Gateway Servers page. On the left is a navigation sidebar with "Gateway Servers" selected. The main content area is titled "Gateway Servers" and features a table with a "+ Add Gateway Se" button. The table lists two gateway servers.

Type	Name	Address	Version	Status	Active S
🗑️	Local	192.168.1.141		Legacy	0
🗑️	Main Server	rrt.gllilabs.com		Legacy	0

All the existing Folders configured in the mobilEcho 4.5 Client Management Administrator are first migrated into the Legacy Data Sources tab on the Data Sources page. You can continue to add and modify the folders on this page until you upgrade their associated Gateway Server to Acronis Access. Once a Gateway Server is upgraded to Acronis Access and registered to be administered by this Acronis Access server, the folders associated with that Gateway Server will be moved to the main Folders tab on the Data Sources page.

**Note:** Each mobilEcho Gateway Server can only be administered by one Acronis Access console. If your organization maintains multiple mobilEcho Client Management Servers (now called Acronis Access Servers), you will need to deploy unique Gateway Servers for each Acronis Access Server.

The screenshot shows the Acronis Access web interface. The left sidebar contains navigation options: Mobile Access, Devices, Enroll Users, Policies, Gateway Servers, Data Sources (selected), Settings, Sync & Share, Audit Log, and General Settings. The main content area is titled 'Legacy Data Sources' and contains a table of folders. The table has columns for Type, Display Name, Server, Path, and Sync. The data in the table is as follows:

Type	Display Name	Server	Path	Sync	
Folder	Access	Local	VEGA AE	None	✎ ✕
Folder	Management	Main Server	sp2010\Management	None	✎ ✕
Folder	Presentations	Main Server	localfiles\Presentations	None	✎ ✕
Folder	Reports	Main Server	localfiles\Reports	None	✎ ✕
Folder	SharePoint	Local	sp	None	✎ ✕
Folder	SharePoint 2010	Main Server	sp2010	None	✎ ✕
Folder	SharePoint 2013	Main Server	sp2013	None	✎ ✕
Folder	Team Docs	Main Server	localfiles\Team Docs	None	✎ ✕
Folder	test folder	Local	test	None	✎ ✕
Folder	Thousand Files	Local	test files\10000 files	None	✎ ✕

In this scenario, you should only have one Windows Server running the Acronis Access console and the Gateway Server, so you will have just one server listed on the Gateway Servers page. This server needs to be registered so that you can administer it.

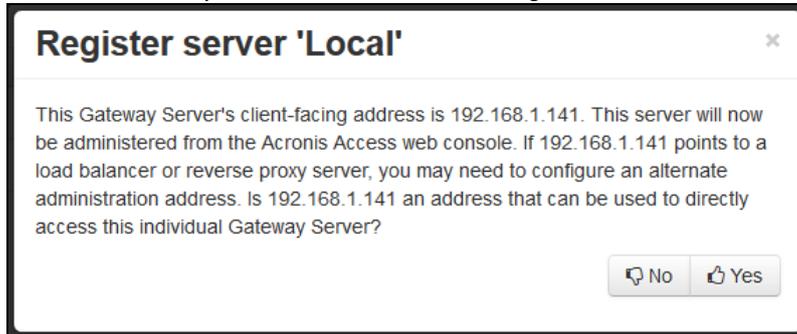
1. Click the menu button for the Gateway Server on your Acronis Access server and select **Register**.

The screenshot shows a table row for a Gateway Server. The row contains the following information: a folder icon, the text 'Local', the IP address '192.168.1.141', the text 'Legacy', and the number '0'. To the right of the row is a 'Details' button. A context menu is open over the row, showing three options: 'Edit Address', 'Register' (which is highlighted in blue), and 'Remove'.

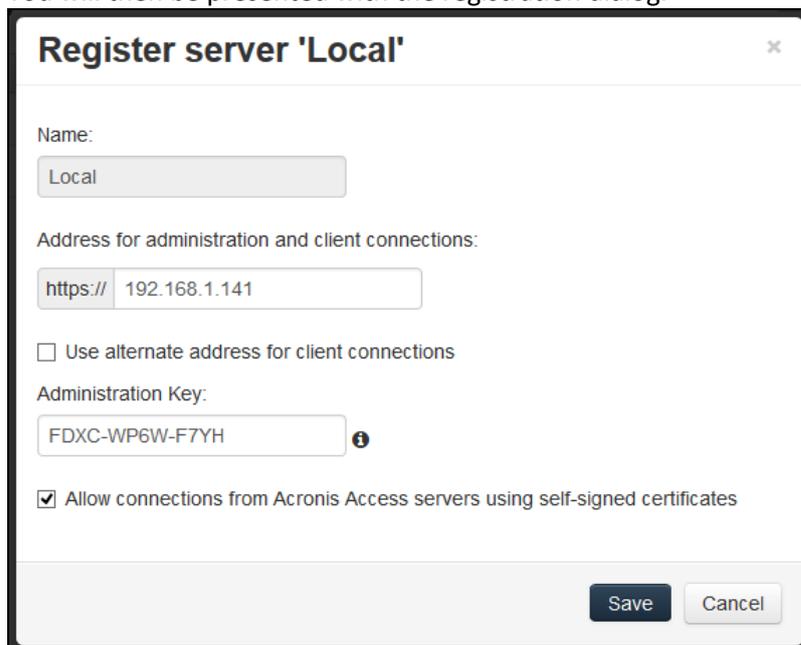
2. You will be asked if the existing network address for the server you are registering can be used to directly access the server. The existing address is typically the network address that your mobile device users must use to access the Gateway Server, so it's possible this address points to a proxy server or load balancer.

---

**Note:** If this is the case, you need to select “No” at this dialog and enter an alternate network address that will be used by the Acronis Access server to gain direct network access to this Gateway Server



3. You will then be presented with the registration dialog.



---

**Note:** If your Gateway Server is using a self-signed SSL certificate, you will need to enable “Allow connections from Acronis Access servers using self-signed certificates”.

**Note:** You will also need to enter an Administration Key, to enable the pairing with this remote server. This is done to validate and secure the administrative relationship.

4. To obtain an Administration Key from your Gateway Server, open a new browser window or tab and navigate to the Gateway Server’s HTTPS address. This should be the same address that is

listed in the “Address for administration and client connections” field.

**Acronis Access Administration**

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

**XVPX-JKTW-KTZ2**

**Note:** For security purposes, this must be done from a web browser running on the actual Windows Server that the Gateway Server is running on. You will not be able to view your Administration Key from a remote web browser.

5. Enter the 12 digit Administration Key (including dashes) into the registration form and click **Save**.

**Note:** Once the server has been registered it will appear in the Gateway Servers list as registered and you can adjust its settings and view its details and status.

**Gateway Servers** + Add Gateway Server + Add Cluster Group

Type	Name	Address	Version	Status	Active Sessions	
☰	Main Server	rrt.gllabs.com		Legacy	0	Details
☰	Local	192.168.1.141		✔	0	Details

- Details
- Edit
- Access Restrictions
- Remove

When registered, the Volumes that existed on the mobilEcho Gateway Server prior to being upgraded to Acronis Access are imported into the Data Sources – Folders list.

**Acronis Access** administrator

Folders Gateway Servers Visible on Clients Legacy Data Sources Assigned Sources

**Folders** Add New Folder

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

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

Type	Display Name	Server	☰	Path	Sync	
📁	test folder	Local	✔	D:\testfolder	None	✎ ✕
🌐	Access	Local	✔	https://192.168.1.141:3000	None	✎ ✕
📁	Thousand Files	Local	✔	\\vega\test files\10000 files	None	✎ ✕
📁	SharePoint	Local	✔	http://sharepoint2010.gllabs.com:2229	None	✎ ✕

There are no longer “Volumes” in mobilEcho 5.0. Instead of using Volumes to share data sources, you will now create Folders. These Folders have an optional “Show when browsing server” property. When this option is enabled, the Folder will appear when a user browses the root of the Gateway Server in their mobilEcho app, just as Volumes were displayed in mobilEcho 4.5 or earlier.

The screenshot shows the 'Edit Folder' configuration window. At the top, the title is 'Edit Folder' with a close button (x). Below the title, there is a text input field for 'Display Name' containing 'test folder'. A section titled 'Select the Gateway Server to use to give access to this data source:' contains a dropdown menu with 'Local (192.168.1.141)' selected. Below this is a 'Data Location' dropdown menu set to 'On the Gateway Server'. A light blue informational box contains the text: '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.' Below this is a 'Path' text input field containing 'D:\testfolder'. A 'Sync' dropdown menu is set to 'None'. There are two checkboxes: 'Show When Browsing Server' (checked) and 'Require Salesforce.com Activity Logging' (unchecked). Below these is a section titled 'Assign This Folder to a User or Group' with a search bar containing 'Find User or Group that begins with' and a 'Search' button. At the bottom, there is a table with the header 'This folder is assigned to:' and two columns: 'Common Name' and 'Distinguished Name'. The table is currently empty. At the bottom right, there are 'Save' and 'Cancel' buttons.

All the Volumes from your mobilEcho 4.5 or earlier server were imported into to the Acronis Access console as Folders with the “Show when browsing server” property enabled. So, they will continue to appear when your users browse the root of a mobilEcho Gateway Server. Any Folders added later can be configured to act like Volumes by enabling this setting. You can also begin using advanced client management features, such as the ability to add Folders that automatically appear in the mobilEcho client app for the list of Active Directory user or groups you assign them to.

As shown below, the 4 existing Volumes from this mobilEcho 4.5 server were imported into the Folders list after Gateway Server registration, and they continue to appear when browsing the server from the mobilEcho app.

[Folders](#)
[Gateway Servers Visible on Clients](#)
[Legacy Data Sources](#)
[Assigned Sources](#)

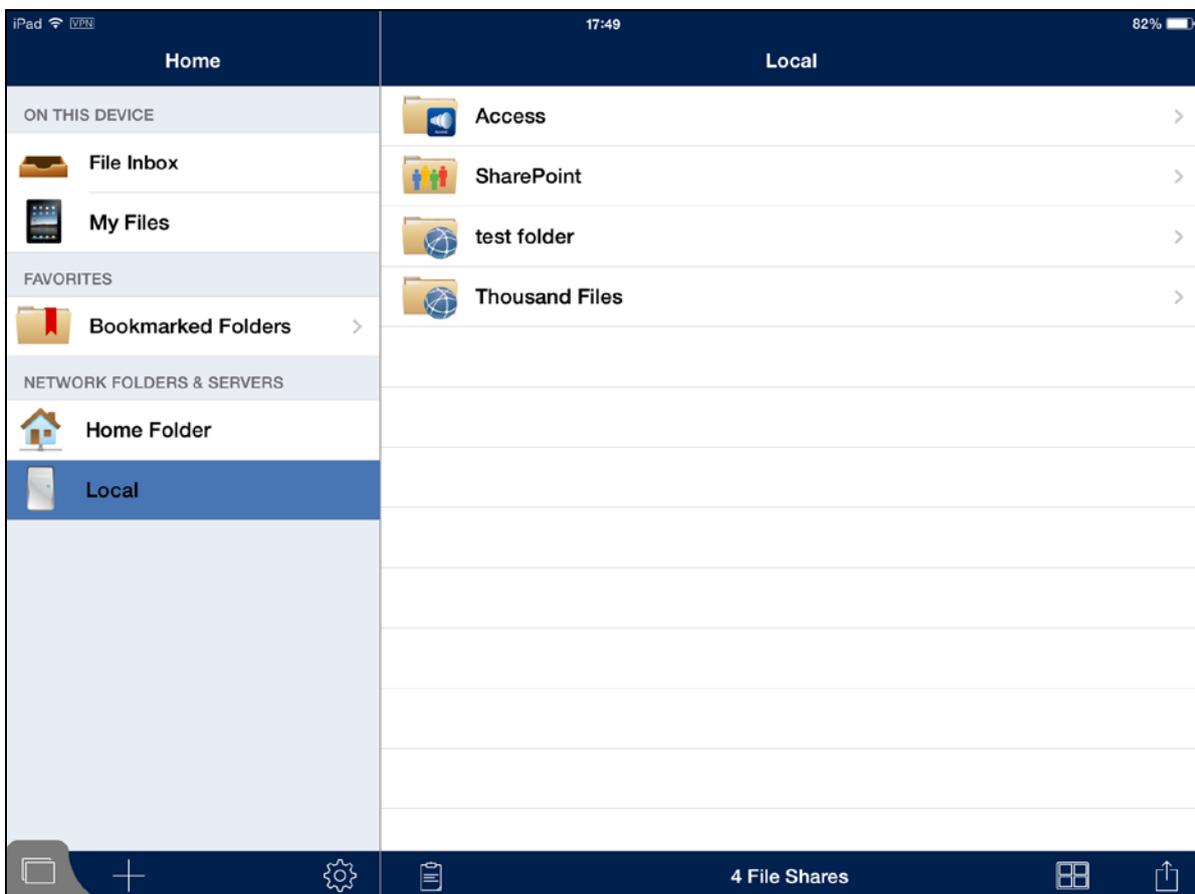
[Add New Folder](#)

## Folders

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

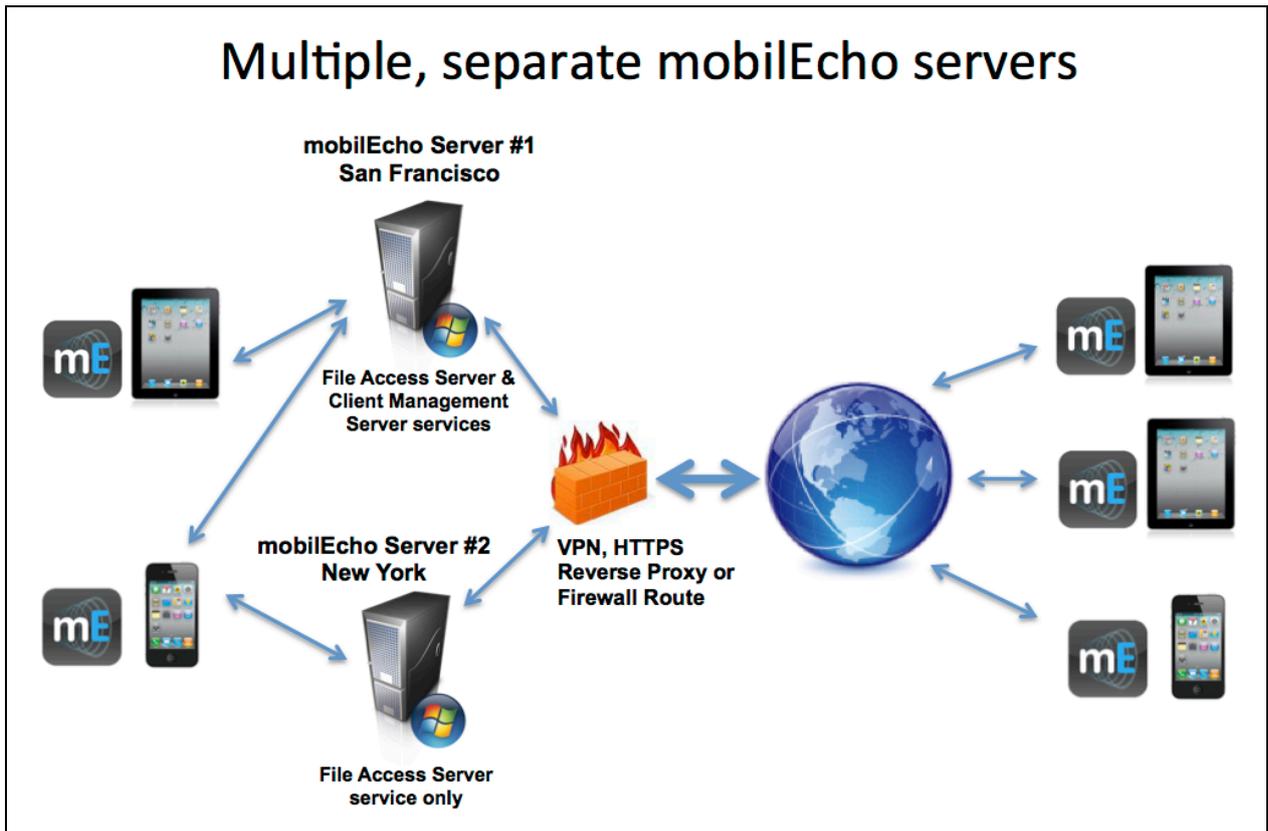
Add specific folder locations on your Gateway Servers and assign these folders to users or groups.

Type	Display Name	Server	🔒	Path	Sync	
📁	test folder	Local	✔️	D:\testfolder	None	✎ ✕
🌐	Access	Local	✔️	https://192.168.1.141:3000	None	✎ ✕
📁	Thousand Files	Local	✔️	\\vega\test files\10000 files	None	✎ ✕
🌐	SharePoint	Local	✔️	http://sharepoint2010.gililabs.com:2229	None	✎ ✕



### 2.2.2.3 Upgrading multiple mobilEcho servers with Client Management

#### Scenario 3 - Upgrading multiple mobilEcho servers with Client Management



In this scenario, you have a multiple Windows servers running mobilEcho 4.5 or earlier. One server has both the required mobilEcho File Access Server service running and the optional mobilEcho Client Management Server service enabled. The other servers are just acting as mobilEcho File Access Servers.

When upgrading to Acronis Access, your mobilEcho File Access Servers will be upgraded to Acronis Access Gateway Servers. This service will continue to accept connections from mobilEcho clients and to act as the gateway to any file server, NAS or SharePoint data sources your users are accessing.

The mobilEcho Client Management Administrator web console on your server acting as your mobilEcho Client Management Server will be upgraded to an Acronis Access Server web console. After upgrade, you will no longer use the mobilEcho Administrator Windows program on each mobilEcho File Access Servers to administer those servers. This new web console will be used to administer all of your mobilEcho servers and clients from one unified web interface.

#### To perform an upgrade of Acronis Access:

##### On the Windows Server acting as your mobilEcho Client Management Server:

1. Follow the instructions in Scenario 2 to upgrade the Windows Server that is acting as your mobilEcho Client Management Server. This is the server that you connect to when you log into the mobilEcho Client Management Administrator web console.
2. Once you complete that upgrade, you will have a functional Acronis Access Server web console with the mobilEcho File Access Server (now called an Acronis Access Gateway Server) residing on

that Windows server registered for administration. You will also see your additional servers listed on the Acronis Access Gateway Servers page as “Legacy” servers. In the example below, your upgraded server “BGU2008” is registered and your yet to be upgraded server “Department Server” has not yet been registered.

3. Next, you will upgrade each additional server that is acting as a mobilEcho File Access Server only. Please follow the steps bellow.

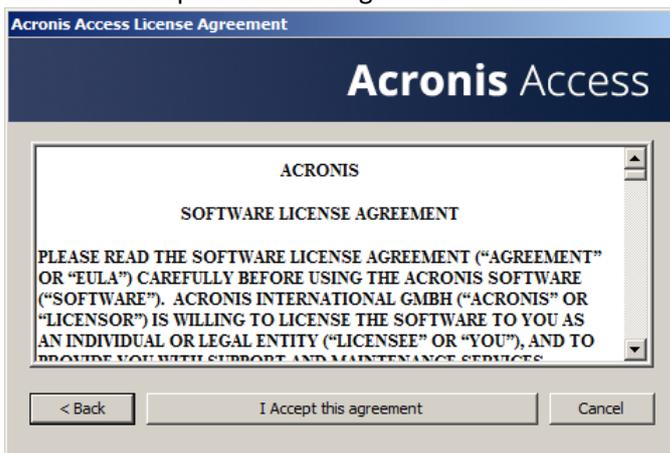
**On every Windows Server acting as a mobilEcho File Access Server only:**

1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.

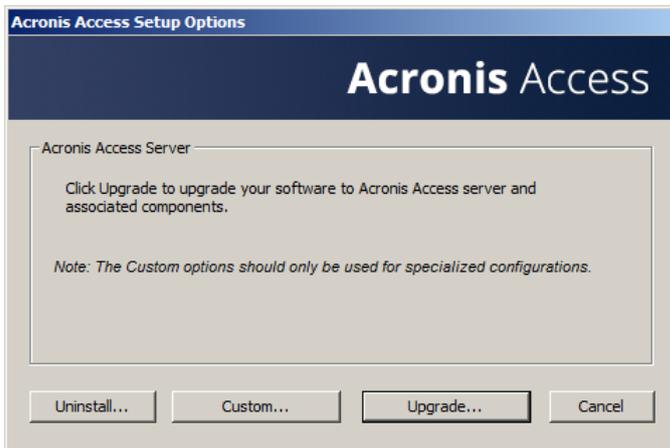
2. Run the Acronis Access installer on the desired server.
3. Press **Next** on the Welcome screen.



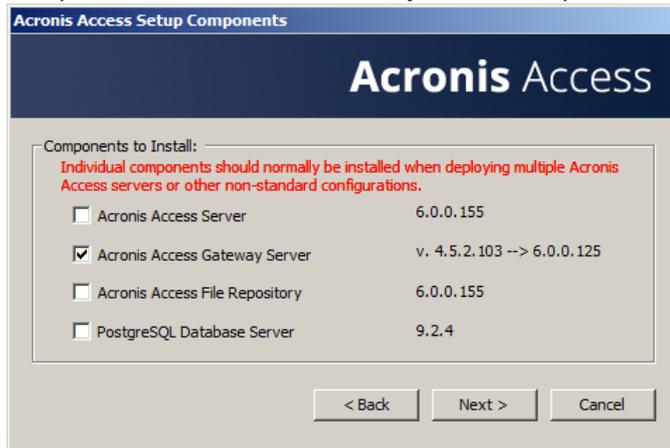
4. Read and accept the license agreement.



5. Click **Custom**.



6. Select only the **Acronis Access Gateway Server** component and press



**Next.**

7. The rest of the installation and Configuration Utility steps follow what is outlined in the earlier scenarios, with the exception that you will not need to configure the Access Server and File Repository in the Configuration Utility.
8. When you complete the Configuration Utility process, there will be no additional web console configuration, as the Acronis Access Server console was not installed.
9. Return to the Acronis Access Server console on the first server you performed the full installation on. Open the Gateway Servers page and click the menu button for the additional Gateway Server that you just upgraded to Acronis Access, and select **Register**.

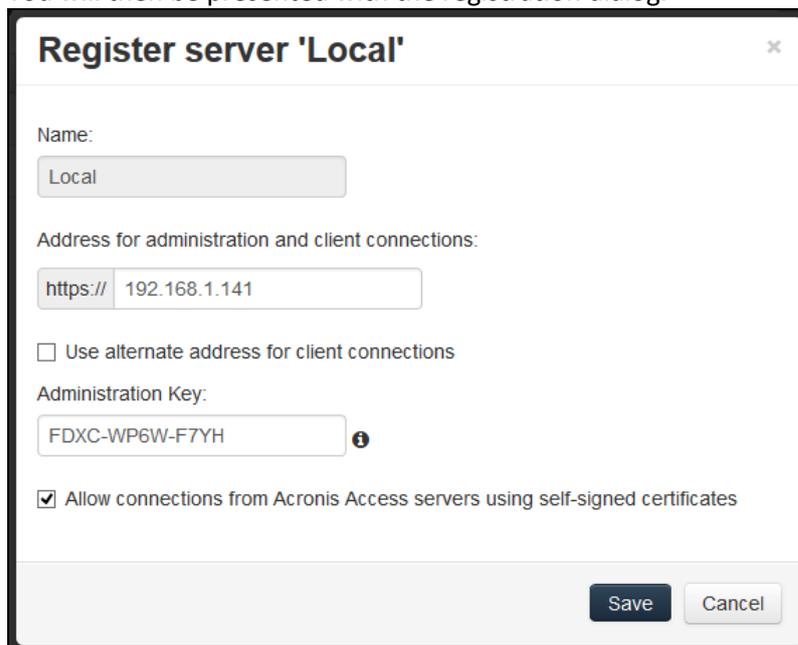
- You will be asked if the existing network address for the server you are registering can be used to directly access the server. The existing address is typically the network address that your mobile device users must use to access the Gateway Server, so it's possible this address points to a proxy server or load balancer.

---

**Note:** If this is the case, you need to select "No" at this dialog and enter an alternate network address that will be used by the Acronis Access server to gain direct network access to this Gateway Server.



- You will then be presented with the registration dialog.



---

**Note:** If your Gateway Server is using a self-signed SSL certificate, you will need to enable "Allow connections from Acronis Access servers using self-signed certificates".

**Note:** You will also need to enter an Administration Key, to enable the pairing with this remote server. This is done to validate and secure the administrative relationship.

- To obtain an Administration Key from this Gateway Server, open a new browser window or tab on the actual Windows Server that you are registering, and navigate to the Gateway Server's HTTPS address. This should be the same address that is listed in the "Address for administration and client connections" field.

---

**Note:** For security purposes, this must be done from a web browser running on the actual Windows Server that the Gateway Server is running on. You will not be able to view your Administration Key from a remote web browser.

- Enter the 12 digit Administration Key (including dashes) into the registration form and click **Save**.

---

**Note:** Once the server has been registered it will appear in the Gateway Servers list as registered and you can adjust its settings and view its details and status.

**Note:** When registered, the Volumes that existed on this mobilEcho Gateway Server prior to being upgraded to Acronis Access are imported into the Data Sources – Folders list. They will behave just as explained in the prior upgrade scenarios.

<b>Acronis Access</b>	<b>Administration</b>
	<p>In order to configure this Acronis Access Gateway Server, it needs to be registered with an Acronis Access Management Server. To do this, visit the Gateway Servers section on the Management Server to register a new Gateway Server using the following key:</p> <p><b>XVPX-JKTW-KTZ2</b></p>

14. All management of this Gateway Server is now done from within Acronis Access Server web console. When creating new Folders on the Data Sources page, this Gateway Server will now appear in the list of Gateway Servers available to give access to the new Folder.
15. If you have any additional Gateway Servers to upgrade and register, please follow the same procedure as above.

#### 2.2.2.4 Upgrading a single mobilEcho server with Client Management enabled and an activEcho server

For this procedure, please visit the Upgrading an activEcho server with a mobilEcho Client Management Server (p. 65) article.

### 2.2.3 Downgrading to mobilEcho 4.5

Downgrading Acronis Access to mobilEcho 4.5 is a complicated procedure and should not be attempted unless absolutely necessary. Make sure you make proper backups and place them in safe locations.

#### To downgrade Acronis Access to mobilEcho 4.5:

---

**Warning:** Do not add any licenses to the mobilEcho Administrator until you've completed the whole procedure. Do not edit the registry while performing this procedure!

---

In order for this procedure to work you need to have made a successful upgrade to Acronis Access.

1. Before you begin, make a backup of the file **settings\_backup** and the folder **Legacy mobilEcho files**.

---

**Note:** The file is located here: **C:\Program Files (x86)\Group Logic\mobilEcho Server**

and the folder here: **C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files**

---

2. Download the mobilEcho 4.5 installer and the Acronis Access installer.
3. Run the Acronis Access installer.
4. Press **Next** on the Welcome screen.
5. Accept the license agreement.
6. Click **Uninstall** to begin the downgrade procedure.
7. Press **OK** on the warning popup.

8. Select **Uninstall all Acronis Access components**.
9. Review the selected components and press **Uninstall**.
10. On the PostgreSQL Uninstallation popup press **Yes**. Some files and settings will remain.
11. Review everything uninstalled and press **Exit**.
12. Run the mobilEcho 4.5 installer.
13. Read and accept the license agreement and press **Next**.
14. Select the folders where mobilEcho was installed previously. If they were the defaults, you can use these defaults as well.
15. Press **Install** to begin the mobilEcho 4.5 installation. Once the installation is complete unselect Launch the File Server Administrator and press **Finish**.
16. Run the **settings\_backup** file you backed up.
17. Open the **Legacy mobilEcho files** folder you backed up.
  - a. Copy the **invitation.html.erb** and **invitation.txt.erb** files to: **C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\app\views\user\_mailer**
  - b. Copy the **mobilEcho\_manager** file to: **C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI**
  - c. Copy the **production.sqlite3** file to: **C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db**
  - d. There may be a 4th file called **priority.txt**, if present, copy it to **C:\Program Files (x86)\Group Logic\mobilEcho Server\Management**. You will have to create the **Management** folder manually.

---

**Note:** It is highly recommended to delete the old file first, and then place the new one.

---

18. Start the **mobilEcho File Access** service and start the **mobilEcho Management** service.

---

**Note:** You will have to manually re-enable all of your user and group profiles.

---

## 2.3 Upgrading from activEcho 2.7 or earlier

### In this section

Before You Begin.....	60
The Upgrade Process .....	61

### 2.3.1 Before You Begin

#### Back up activEcho before upgrading

Please back up the data files used by your existing activEcho server.

The process for backing up and restoring an activEcho 2.7 or earlier server can be found here:  
<http://docs.grouplogic.com/display/ActivEcho/Maintenance+Tasks>

---

**Note:** All customizations of the activEcho web interface will be lost on upgrade.

---

**Update your version of activEcho to version 2.7 before upgrading to Acronis Access.**

#### Backup Tomcat before upgrading

On upgrade the Apache Tomcat may be upgraded and all of the current Tomcat configuration files, certificates 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)\Group Logic\Common\**.

### **Know your configuration**

Before you proceed with the upgrade make sure you know the following:

- Do you have both mobilEcho and activEcho installed?
- Are they on the same computer or on separate machines?
- Which ports is mobilEcho using? On which port is the File Server and on which port is the Management server?
- Which port is activEcho using? Is the File Repository on the same machine?

## **2.3.2 The Upgrade Process**

### **activEcho 5.0 Upgrade Process**

First, please identify the type of activEcho deployment you will be upgrading. The instructions for these scenarios are detailed in the next section of this document. The most common scenarios are:

1. **Single activEcho Server without a mobilEcho Client Management Server**
  - A single Windows server, running the activEcho Server only.
2. **Single activEcho Server with a mobilEcho Client Management Server**
  - A single Windows server, running both the activEcho Server and the mobilEcho Client Management and File Server services.
3. **An activEcho Server and a mobilEcho Client Management Server on another server**
  - One Windows server running the activEcho Server and another server running the mobilEcho Client Management service.

### **In this section**

Upgrading a single activEcho server without a mobilEcho Client Management Server	61
Upgrading an activEcho server with a mobilEcho Client Management Server	65
Upgrading an activEcho server with a mobilEcho Client Management Server on another server	71

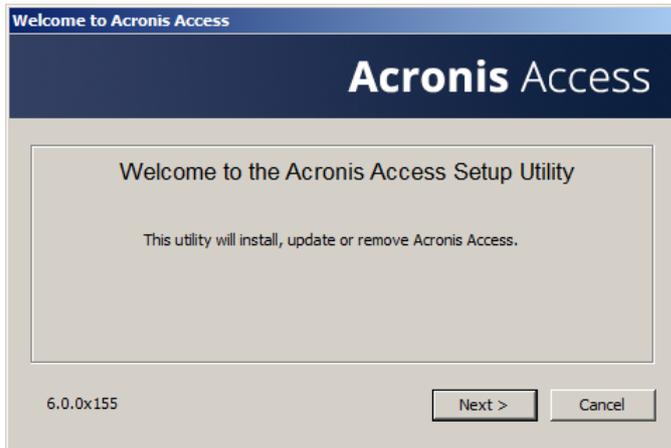
### **2.3.2.1 Upgrading a single activEcho server without a mobilEcho Client Management Server**

#### **Scenario 1 - Upgrading a single activEcho server without a mobilEcho Client Management Server**

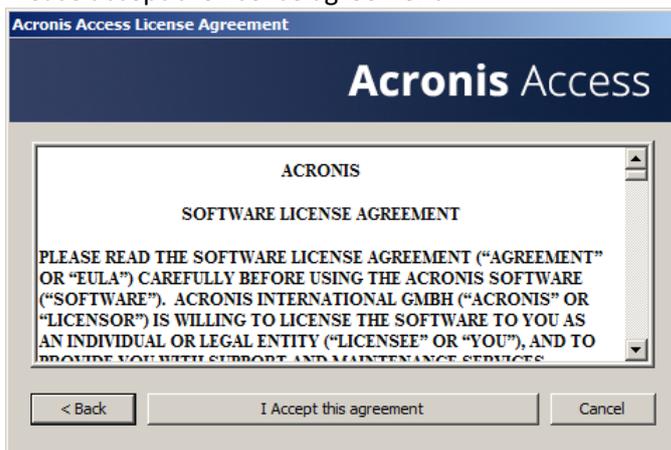
In this scenario, you have a single Windows Server running just the activEcho Server. This procedure will upgrade your activEcho server to the Acronis Access Server web console. This new console retains all of activEcho's functionality with some added features. The Acronis Access Server web console allows you to administer both activEcho and mobilEcho from one unified web interface.

#### **To perform an upgrade of activEcho:**

1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Download the Acronis Access Server installer to your activEcho server and run the installer.
  - a. To access the latest installer, please visit: [http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598)
  - b. You will need to enter your product serial number for verification before downloading the installer.
  - c. The installer file is named: AcronisAccessSetup.exe
4. Click **Next** on the Welcome Screen.

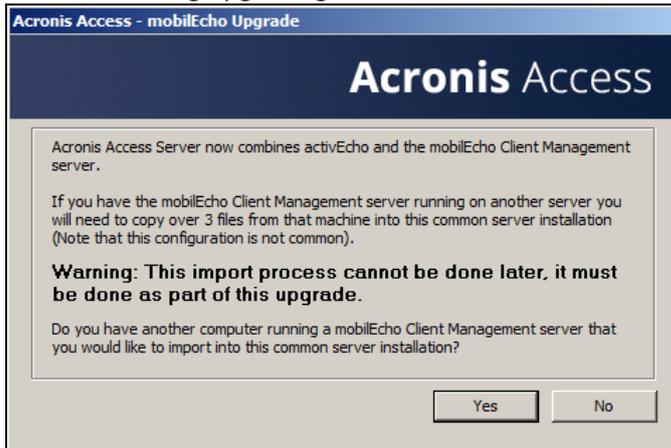


5. Please accept the license agreement.

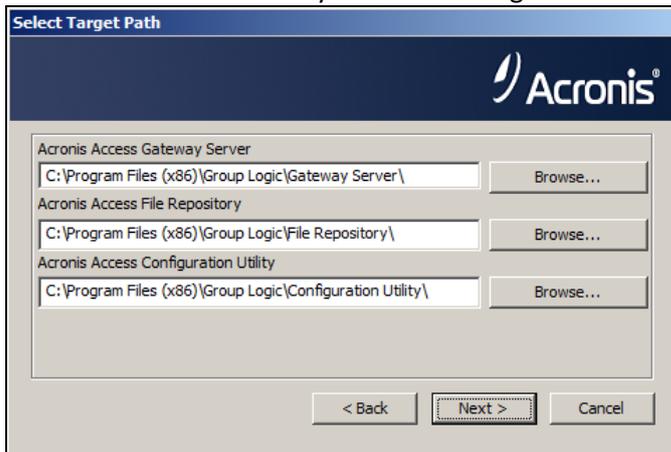


6. Click **Upgrade** to automatically upgrade your activEcho Server to the new Acronis Access Server. In the upgrade process, a Gateway Server and it's required services will also be installed.
7. A prompt for remote mobilEcho Servers will be shown. If you don't have a mobilEcho Client Management Server, press **No**. If you have a mobilEcho Client Management Server, go to the Upgrading an activEcho server with a mobilEcho Client Management Server (p. 65) or Upgrading an activEcho server with a mobilEcho Client Management Server on another server (p. 71)

articles covering upgrading with a mobilEcho installation present.



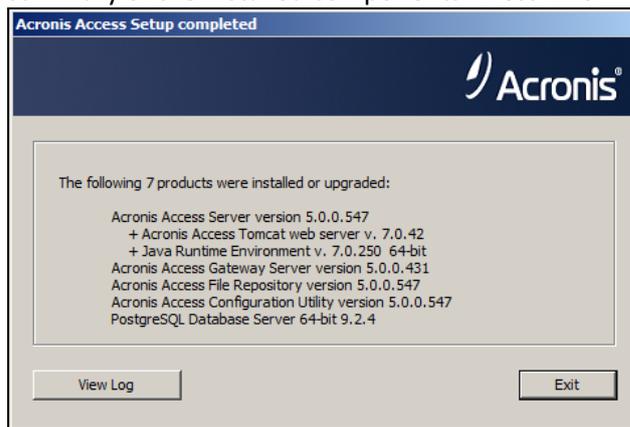
8. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing activEcho server, these paths will default to your existing installation location. We recommend you do not change these installation paths. Click **Next**.



9. Please review the services being installed and upgraded.



10. Press **Install** to begin the upgrade. Once the installation is complete, you will be shown a summary of the installed components. Press **Exit**.

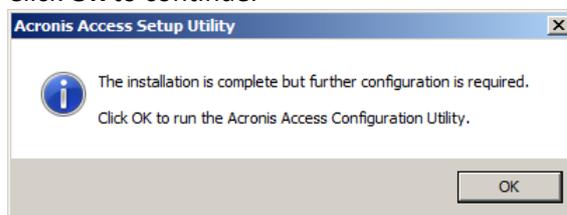


---

**Note:** All required components will be automatically installed in sequence. This may take 5 to 15 minutes depending on your server. Future upgrades will be quicker.

---

11. At this point in the upgrade process, all necessary software has been installed, but you must now configure the network interfaces, ports, and certificates that will be used. This step is mandatory. When exiting the installer, you will be prompted to run the Acronis Access Configuration Utility. Click **OK** to continue.



12. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core Acronis Access service that your mobilEcho clients connect to and that gives access to your file servers, NAS, and SharePoint servers.

---

**Note:** Your existing settings are retained. Please confirm that these settings match your existing mobilEcho File Access Server settings. This service typically runs on all available network addresses on port 443. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.

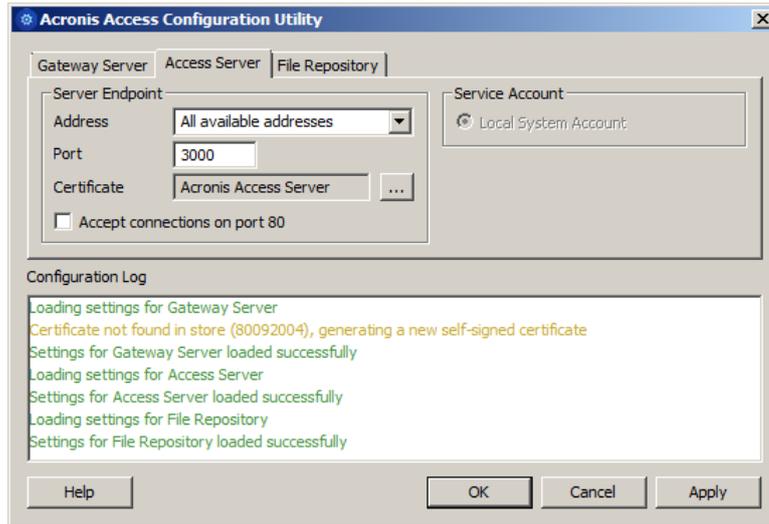
---

13. The Access Server tab is used to configure your Acronis Access Server's network address, port, and certificate. The Acronis Access Server is the web console that is used to configure all Sync & Share features and your activEcho users as well as perform all server administration and remote client management. This is also the console the users will use to access the web client.

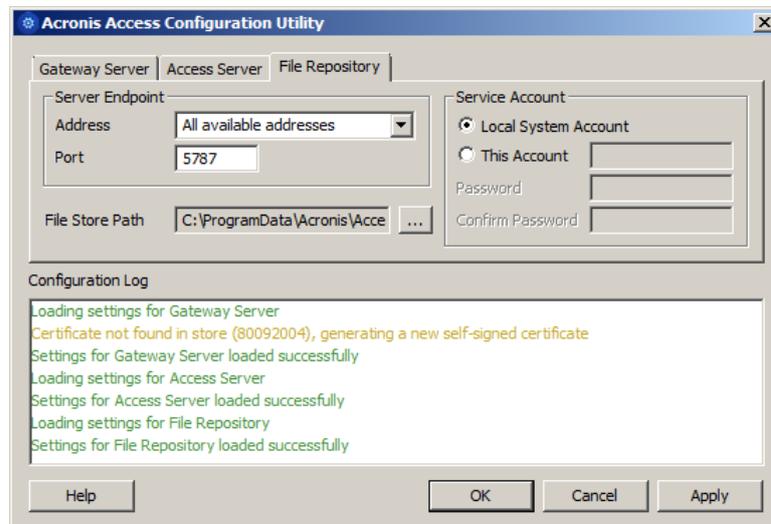
---

**Note:** Please review the settings for the Access Server. The default settings are recommended. This web console typically runs on all available network addresses on port 3000. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be

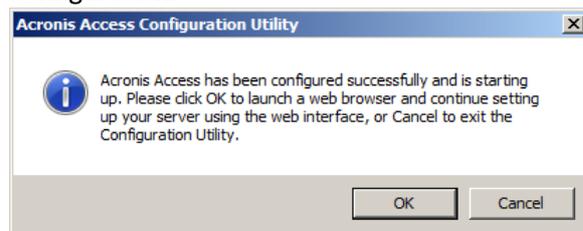
generated.



**Note:** Acronis Access Server requires that a File Repository location be selected. This repository is used by Acronis' activEcho file sync and share features.



14. Click **OK** to exit the Configuration Utility and apply these settings.
15. You will now log into the Acronis Access Server web console for the first time to complete your configuration. You will be prompted to click OK to launch a web browser and complete this configuration.



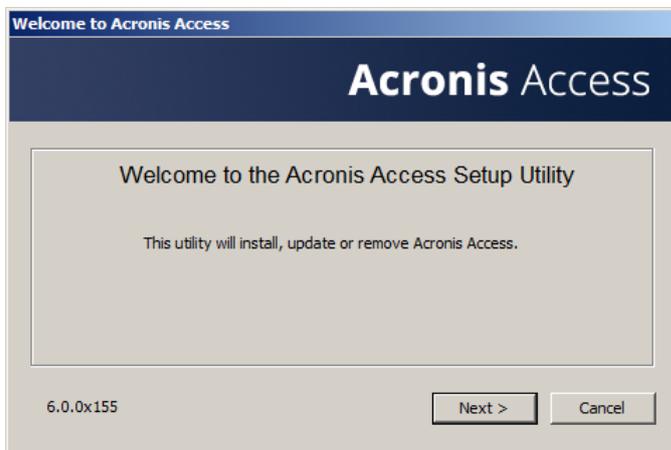
### 2.3.2.2 Upgrading an activEcho server with a mobilEcho Client Management Server

#### Scenario 2 - Upgrading an activEcho server with a mobilEcho Client Management Server

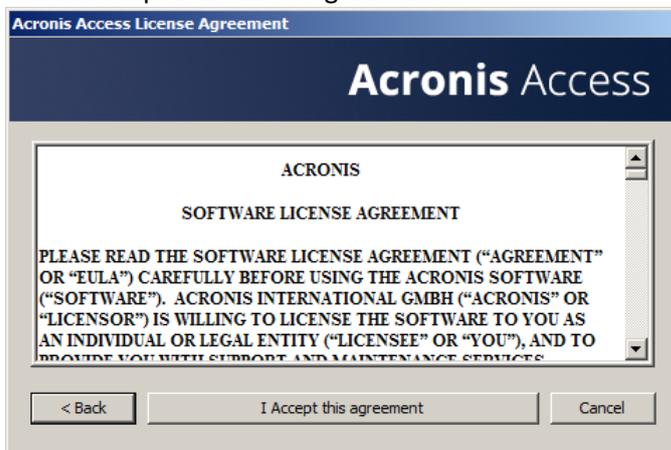
In this scenario, you have one Windows Server running the activEcho Server and the mobilEcho File Server and Management Server. This procedure will upgrade your activEcho server and mobilEcho Client Management Server to the unified Acronis Access Server web console. The new console also replaces the mobilEcho Administrator Windows program previously used to administer mobilEcho servers. The Acronis Access Server web console allows you to administer both activEcho and mobilEcho from one unified web interface.

**To perform an upgrade of activEcho:**

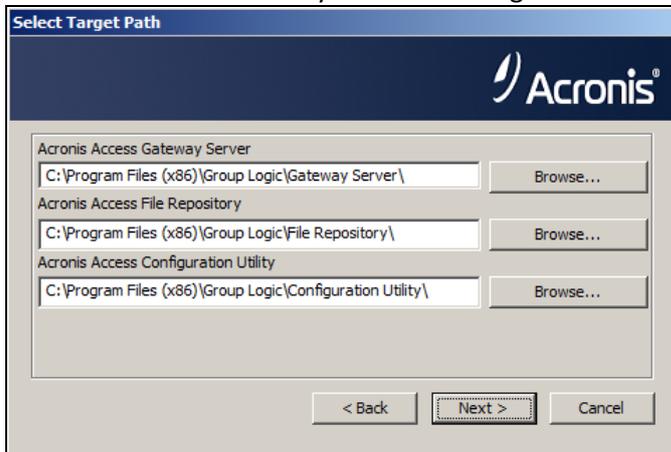
1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Download the Acronis Access Server installer to your activEcho server and run the installer.
  - a. To access the latest installer, please visit: [http://support.grouplogics.com/?page\\_id=3598](http://support.grouplogics.com/?page_id=3598)
  - b. You will need to enter your product serial number for verification before downloading the installer.
  - c. The installer file is named: AcronisAccessSetup.exe
4. Click **Next** on the Welcome Screen.



5. Please accept the license agreement.



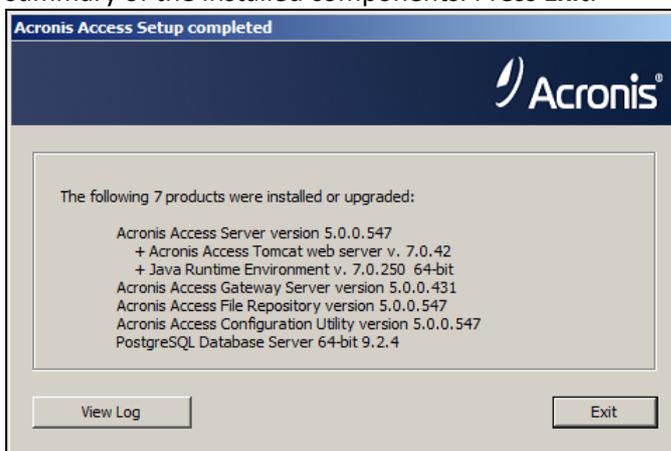
6. Click **Upgrade** to automatically upgrade your activEcho Server and mobilEcho Client Management Server to the new Acronis Access Server. In the upgrade process, a Gateway Server and it's required services will also be installed. If a File Server is present, the installer will upgrade the File Server to the new Gateway Server instead of installing a new one.
7. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing activEcho server, these paths will default to your existing installation location. We recommend you do not change these installation paths. Click **Next**.



8. Please review the services being installed and upgraded.



9. Press **Install** to begin the upgrade. Once the installation is complete, you will be shown a summary of the installed components. Press **Exit**.

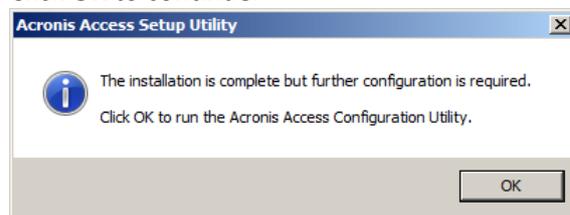


---

**Note:** All required components will be automatically installed in sequence. This may take 5 to 15 minutes depending on your server. Future upgrades will be quicker.

---

10. At this point in the upgrade process, all necessary software has been installed, but you must now configure the network interfaces, ports, and certificates that will be used. This step is mandatory. When exiting the installer, you will be prompted to run the Acronis Access Configuration Utility. Click **OK** to continue.



11. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core Acronis Access service that your mobilEcho clients connect to and that gives access to your file servers, NAS, and SharePoint servers.

---

**Note:** Your existing settings are retained. Please confirm that these settings match your existing mobilEcho File Access Server settings. This service typically runs on all available network addresses on port 443. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.

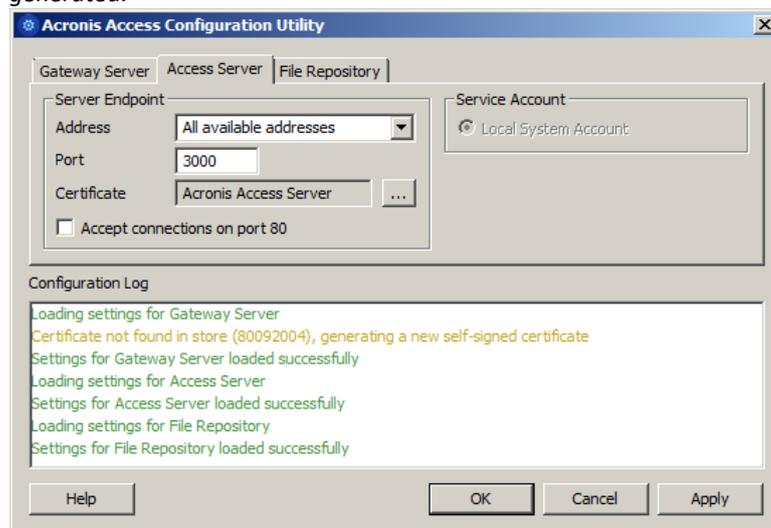
---

12. The Access Server tab is used to configure your Acronis Access Server's network address, port, and certificate. The Acronis Access Server is the web console that is used to configure all Sync & Share features and your activEcho users as well as perform all server administration and remote client management. This is also the console the users will use to access the web client.

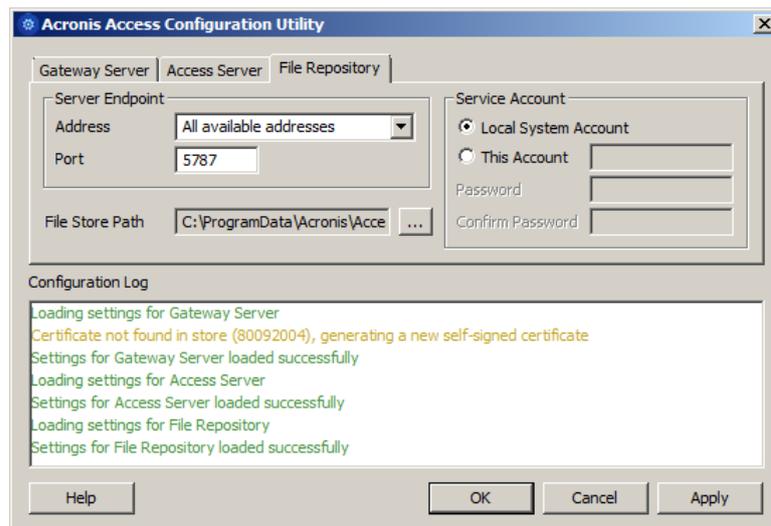
---

**Note:** Please review the settings for the Access Server. The default settings are recommended. This web console typically runs on all available network addresses on port 3000. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.

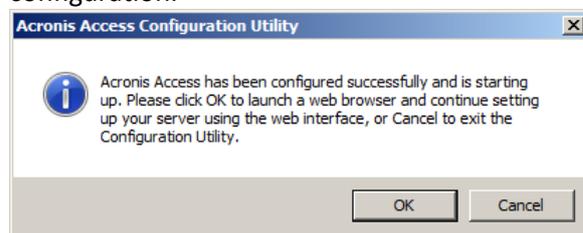
---



**Note:** Acronis Access Server requires that a File Repository location be selected. This repository is used by Acronis' activEcho file sync and share features.



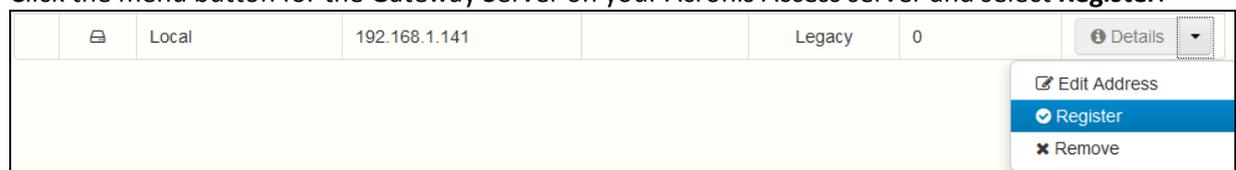
13. Click **OK** to exit the Configuration Utility and apply these settings.
14. You will now log into the Acronis Access Server web console for the first time to complete your configuration. You will be prompted to click OK to launch a web browser and complete this configuration.



## Registering the Gateway

In this scenario, you should only have one Windows Server running the Acronis Access console and the Gateway Server, so you will have just one server listed on the Gateway Servers page. This server needs to be registered so that you can administer it.

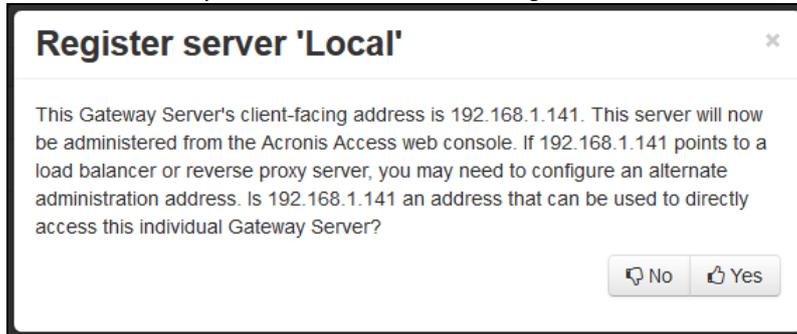
1. Click the menu button for the Gateway Server on your Acronis Access server and select **Register**.



2. You will be asked if the existing network address for the server you are registering can be used to directly access the server. The existing address is typically the network address that your mobile device users must use to access the Gateway Server, so it's possible this address points to a proxy server or load balancer.

---

**Note:** If this is the case, you need to select “No” at this dialog and enter an alternate network address that will be used by the Acronis Access server to gain direct network access to this Gateway Server



3. You will then be presented with the registration dialog.



---

**Note:** If your Gateway Server is using a self-signed SSL certificate, you will need to enable “Allow connections from Acronis Access servers using self-signed certificates”.

**Note:** You will also need to enter an Administration Key, to enable the pairing with this remote server. This is done to validate and secure the administrative relationship.

4. To obtain an Administration Key from your Gateway Server, open a new browser window or tab and navigate to the Gateway Server’s HTTPS address. This should be the same address that is

listed in the “Address for administration and client connections” field.

**Acronis Access Administration**

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

**XVPX-JKTW-KT2**

**Note:** For security purposes, this must be done from a web browser running on the actual Windows Server that the Gateway Server is running on. You will not be able to view your Administration Key from a remote web browser.

5. Enter the 12 digit Administration Key (including dashes) into the registration form and click **Save**.

**Note:** Once the server has been registered it will appear in the Gateway Servers list as registered and you can adjust its settings and view its details and status.

**Gateway Servers** + Add Gateway Server + Add Cluster Group

Type	Name	Address	Version	Status	Active Sessions	
🔒	Main Server	rrt.gililabs.com		Legacy	0	Details
🔒	Local	192.168.1.141		🟢	0	Details

- Details
- Edit
- Access Restrictions
- Remove

### 2.3.2.3 Upgrading an activEcho server with a mobilEcho Client Management Server on another server

#### Scenario 3 - Upgrading an activEcho server with a mobilEcho Client Management Server on another server

**Warning!** For this scenario, we recommend that you keep your activEcho and mobilEcho servers separate and upgrade each one individually. For instructions on upgrading your activEcho server, follow the *Upgrading a single activEcho server without a mobilEcho Client Management Server (p. 61)* guide and for instructions on upgrading your mobilEcho server, follow the *Upgrading a single mobilEcho server with Client Management enabled (p. 39)* guide.

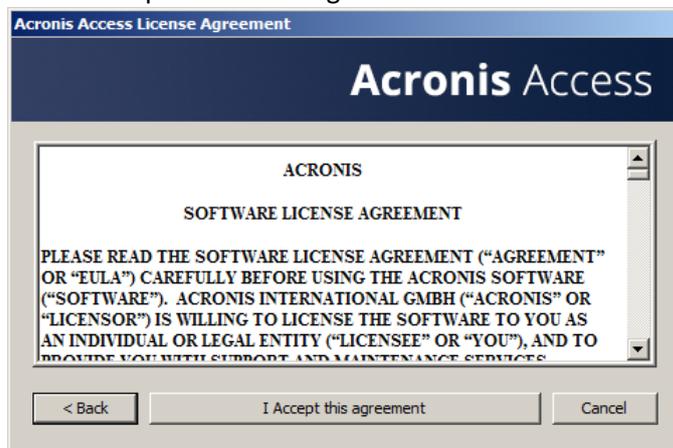
In this scenario, you have two (or more) Windows Servers with one running just the activEcho Server and another running the mobilEcho File Server and Management Server. This procedure will upgrade your activEcho server and mobilEcho Client Management Server to the unified Acronis Access Server web console. The new console also replaces the mobilEcho Administrator Windows program previously used to administer mobilEcho servers. The Acronis Access Server web console allows you to administer both activEcho and mobilEcho from one unified web interface.

To perform an upgrade to Acronis Access Server:

1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Write down the current IP Address of your server running mobilEcho and give the computer a different IP address (You will need the new one as well).
3. Go to the server running activEcho and add the IP address of your server running mobilEcho to a separate network adapter.
4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
5. Download the Acronis Access Server installer to your activEcho server and run the installer.
  - a. To access the latest installer, please visit: [http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598)
  - b. You will need to enter your product serial number for verification before downloading the installer.
  - c. The installer file is named: AcronisAccessSetup.exe
6. Click **Next** on the Welcome Screen.

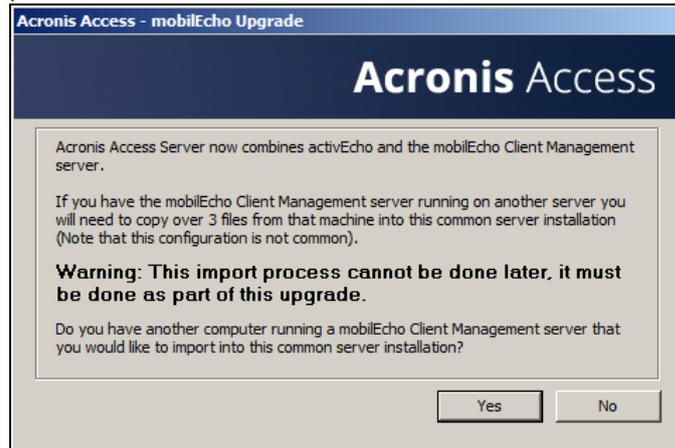


7. Please accept the license agreement.

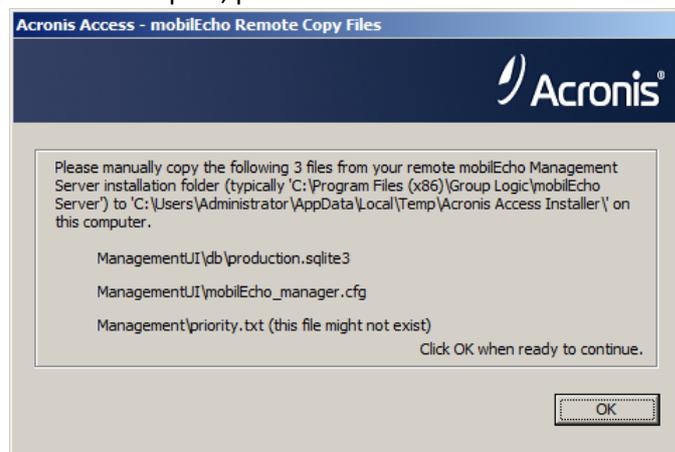


8. Click **Upgrade** to automatically upgrade your activEcho Server to the new Acronis Access Server. In the upgrade process, a Gateway Server and it's required services will also be installed.
9. If you have a mobilEcho Client Management Server, press **Yes**. If you don't have a mobilEcho Client Management Server, go to the first article on upgrading without a mobilEcho installation

present.



10. Go to the server on which you have the mobilEcho Client Management server running and locate these 3 files: **production.sqlite3**, **mobilEcho\_manager.cfg**, **priority.txt** (this file might not exist) and copy them to the machine on which you've started the upgrade to the folder location shown to you on the dialog on your computer. This path is custom for each installation. (i.e. C:\Users\Administrator\AppData\Local\Temp\Acronis Access Installer\). When all of the files have been copied, press **OK** to continue.



**Note:** These files are generally located at:

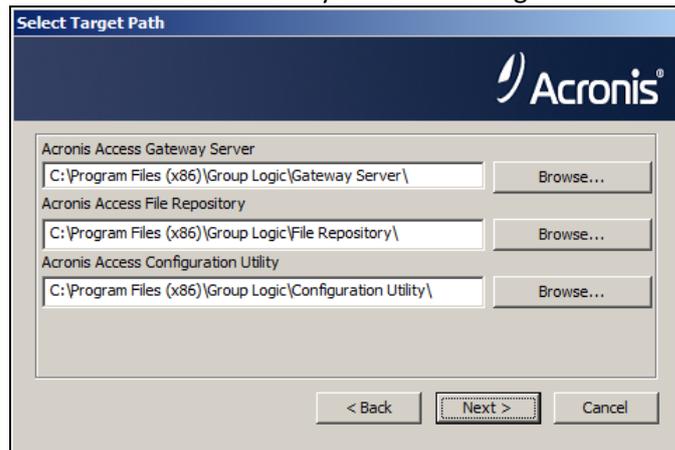
**C:\Program Files (x86)\Group Logic\mobileEcho Server\ManagementUI\db\production.sqlite3**

**C:\Program Files (x86)\Group Logic\mobileEcho Server\ManagementUI\mobileEcho\_manager.cfg**

**C:\Program Files (x86)\Group Logic\mobileEcho Server\Management\priority.txt**

11. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing activEcho server, these paths will default to your existing installation

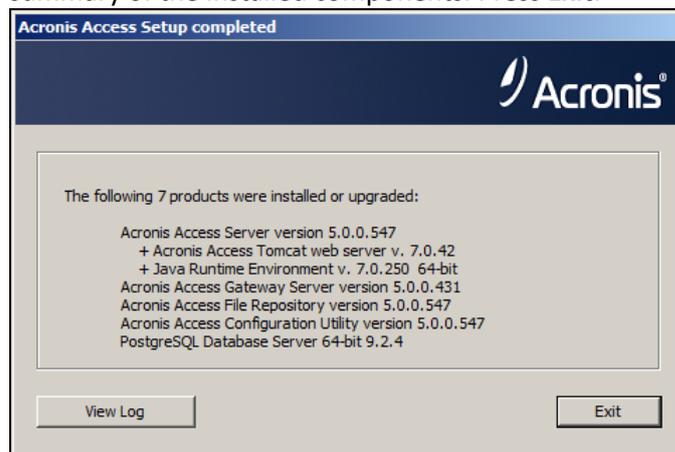
location. We recommend you do not change these installation paths. Click **Next**.



12. Please review the services being installed and upgraded.



13. Press **Install** to begin the upgrade. Once the installation is complete, you will be shown a summary of the installed components. Press **Exit**.



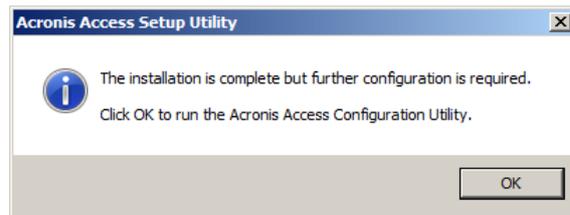
---

**Note:** All required components will be automatically installed in sequence. This may take 5 to 15 minutes depending on your server. Future upgrades will be quicker.

---

14. At this point in the upgrade process, all necessary software has been installed, but you must now configure the network interfaces, ports, and certificates that will be used. This step is mandatory. When exiting the installer, you will be prompted to run the Acronis Access Configuration Utility.

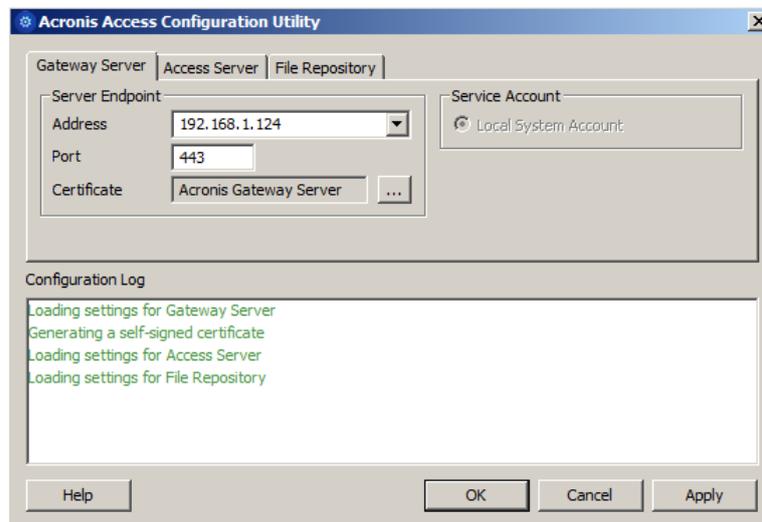
Click **OK** to continue.



## Using the Configuration Utility

### On the Gateway Server tab

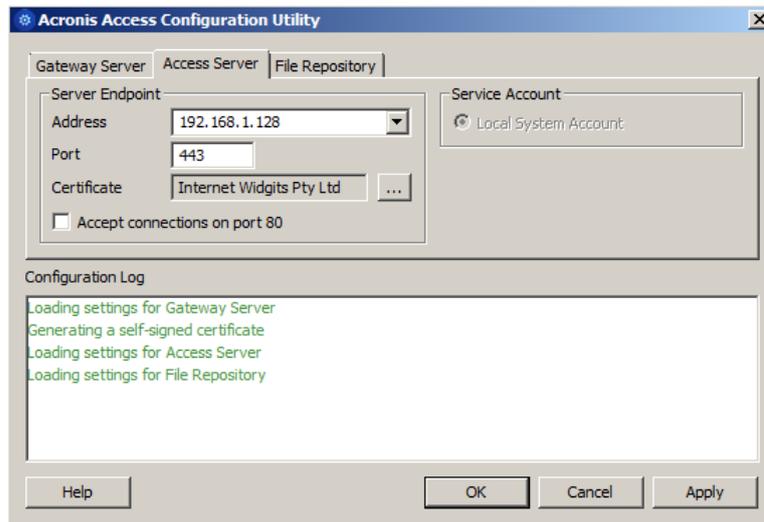
1. For the **Address** field, enter the IP address of your server that was running mobilEcho. This is the address you wrote down at the beginning.
2. For the **Port** field, enter the port number that your mobilEcho File Server used.
3. Add the certificate you have been using for the mobilEcho File Server.



### On the Access Server

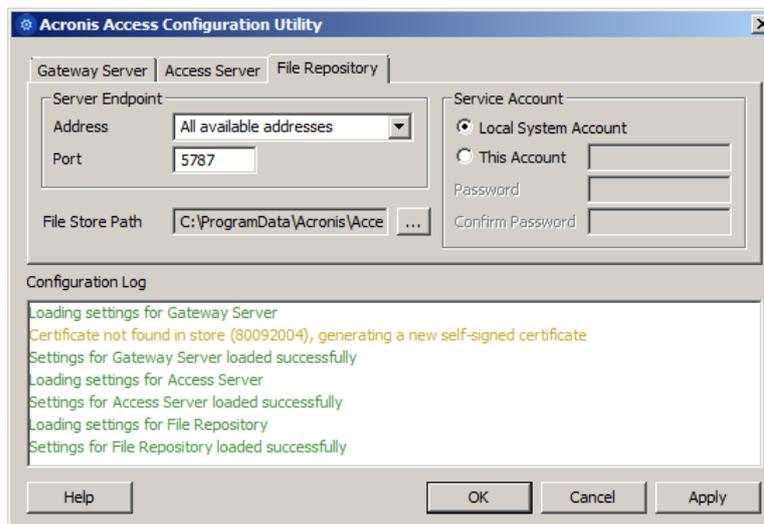
1. For the **Address** field, enter the IP address you've been using for your activEcho server until now. This should be the default.
2. For the **Port** field, enter the port number you've been using for your activEcho server until now. This should be the default.

3. Add the certificate you have been using for your activEcho server.



### On the File Repository tab

1. For the **Address** field, enter the IP address or DNS name of your Repository Service. This should be the default.
2. For the **Port** field, enter the port number for your Repository Service. This should be the default.
3. Select the path to your FileStore folder. This should be the default.

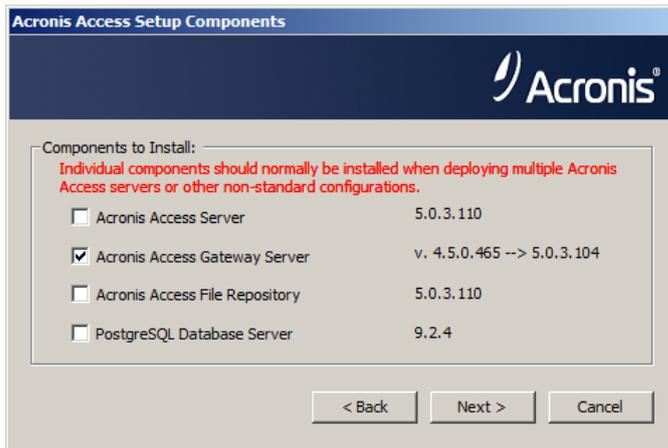


After you have made all the necessary configurations, press OK to exit the Configuration Utility.

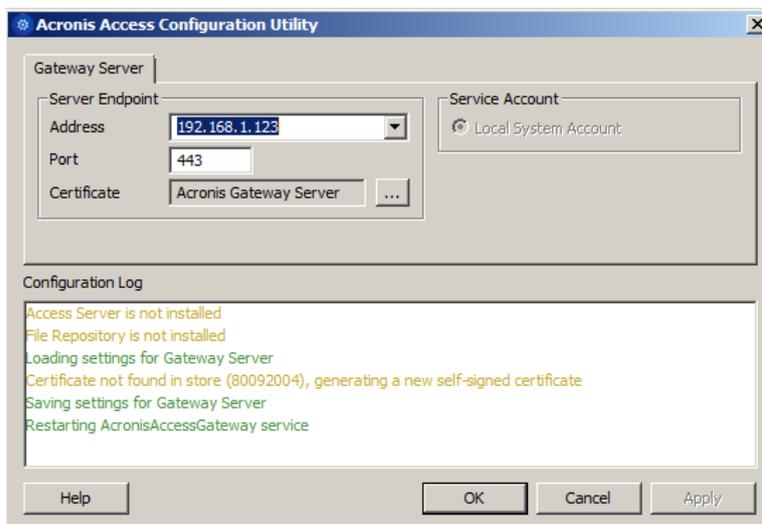
### Configuring your local Gateway Server

1. Copy the Acronis Access Installer and place it on the server with mobilEcho.
2. Stop the mobilEcho Management Server service.
3. Run the installer and press **Next** on the Welcome Screen.
4. Read and accept the license agreement.
5. Press **Custom**.

6. Select only the **Gateway Server** component and press **Next**.



7. Review the installation path and press **Next**. This should be the default.
8. Review the components which will be installed and press **Install**.
9. After the installation finishes, close the installer and start the configuration utility (if it doesn't start automatically, it can generally be found at: **C:\Program Files (x86)\Group Logic\Configuration Utility**).
10. For the **Address** field, specify the new IP you gave to your machine hosting mobilEcho.
11. For the **Port** field, specify the port number your mobilEcho File Server previously used (this should be the default).



12. Press **OK** to complete the configuration and close the utility.
13. Open the Acronis Access web interface and login.
14. Expand the **Mobile Access** tab and open the **Gateway Servers** page.

- Locate the Gateway Server with a **Legacy** status, open the drop down menu for that gateway and select **Register**.

**Acronis Access Gateway Servers** + Add New Gateway Server

Type ^	Name ^	Address ^	Version ^	Status ^	Active Sessions ^	Licenses Used	License	
	Local	192.168.1.128:443	5.0.2x104	Legacy	0	1 of Unlimited	activEcho	Details ▾ <input checked="" type="checkbox"/> Register <input checked="" type="checkbox"/> Remove

- A dialog will appear, press **Yes**.

**Register server 'Local'** ×

This gateway server's client-facing address is 192.168.1.128:443. This server will now be administered from the Acronis Access web console. If 192.168.1.128:443 points to a load balancer or reverse proxy server, you may need to configure an alternate administration address. Is 192.168.1.128:443 an address that can be used to directly access this individual gateway server?

No
  Yes

- In the **Address for administration and client connections** field, enter the IP address of your upgraded Gateway Server. This is the new IP address you gave to the machine previously hosting mobilEcho.

**Register server 'AWR'** ×

Name:

Address for administration and client connections:

Use alternate address for client connections

Administration Key:

Allow connections from Acronis Access servers using self-signed certificates

- In the **Administration Key** field, enter the key of your Gateway Server. To obtain it, open the IP address of the Gateway in a browser. (e.g. https://192.168.1.1). This should be done on the machine which previously had mobilEcho installed.
- Register your Gateway by pressing **Save**.

## Registering your local Gateway server

While on the Gateway Servers page:

1. Press the **Add Gateway Server** button.
2. Enter a display name for your new Gateway Server.
3. Enter the IP address of the Gateway. This is the IP address that was previously used by your mobilEcho server (this is the IP you wrote down at the beginning).
4. Enter the administration key for that Gateway. To obtain it, open the IP address of the Gateway in a browser. (e.g. https://192.168.1.1). This should be done on the machine that is now hosting your Acronis Access Server.

### Add New Gateway Server ×

Display Name:

Address for administration: ⓘ

Use alternate address for client connections ⓘ

Administration Key: ⓘ

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

5. Register your Gateway by pressing **Save**.

## 2.4 Upgrading Clustered Configurations

To upgrade an Acronis Access clustered configuration, you need to upgrade both the Acronis Access Server and the Gateway Servers in your Cluster Group. For instructions on upgrading the Access Server, visit the [Upgrading from Acronis Access to a newer version \(p. 17\)](#) article and for each Gateway, you will need to do the following procedure.

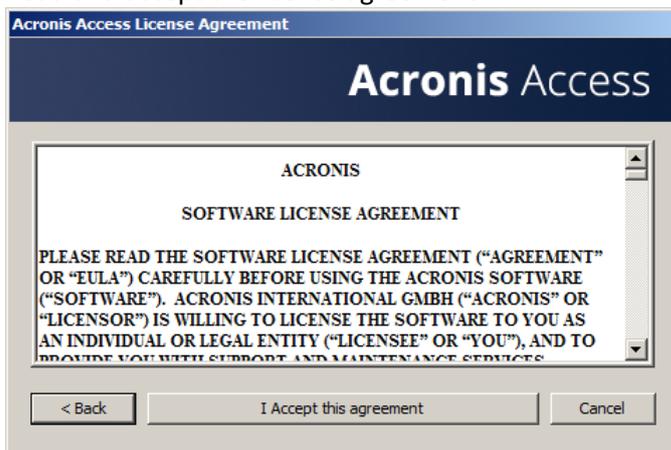
For information on upgrading a Microsoft Failover Clustering configuration, visit the [Supplemental Material](#) section.

## Upgrading a Gateway Server

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



3. Read and accept the license agreement.



4. Click **Custom**.



5. Select only the **Acronis Access Gateway Server** component and press **Next**.
6. Review the components and press **Install**.
7. Once the installation finish, review the Summary, and close the installer. You will be prompted to open the Configuration Utility. Open it to review that all of your previous Gateway Server settings are in place. Make any changes if necessary and press OK.

## 3 Quick Start: Mobile Access

This guide provides the essential steps for setting up a Gateway Server, adding a Data Source and installing the Access Mobile Client app. For more detailed instructions on configuring the Acronis Access Gateway Server and the Client Management components, see the Managing Gateway Servers and Mobile Access sections.

### In this section

First Run .....	81
Configuring Your First Gateway Server and Data Source .....	84
Setting up a Policy .....	87
Installing the Access Mobile Client application .....	88
Enrolling in client management .....	89

### 3.1 First Run

If you haven't done so already, install and configure Acronis Access. For more information on doing so, check the Installing (p. 4) and Configuration Utility (p. 8) 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="access.mycompany.com"/>
Mobile Client Enrollment Address	<input type="text" value="192.168.1.72:3000"/>
Color Scheme	<input type="text" value="Dark Blue"/>
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 a Color Scheme. Current options are Gray, Purple, Cappuccino, Blue, Dark Blue and Orange.
5. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
6. 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.gllilabs.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="pam@gllilabs.com"/>
Use SMTP authentication?	<input type="checkbox"/>

---

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

---

Enter the DNS name or IP address of your SMTP server

Enter the SMTP port of your server.

If you do not use certificates for your SMTP server, unmark **Use secure connection?**

Enter the name which will appear in the "From" line in emails sent by the server.

Enter the address which will send the emails sent by the server.

If you use username/password authentication for your SMTP server, mark **Use SMTP authentication?** and enter your credentials.

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

1. Press **Save**.

## LDAP

### LDAP

Directory Services, like 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.

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

---

**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**.

## Local Gateway Server

### Local Gateway Server

Your local Gateway Server is being administered via address 192.168.1.72:443.  
What address should client connections use to contact the Gateway Server? For example: gateway.example.com

---

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

---

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

## 3.2 Configuring Your First Gateway Server and Data Source

### Registering a new Gateway Server:

1. Go to the computer on which you have the Gateway Server installed.
2. Open <https://localhost/>.

---

**Note:** The port 443 is the default port. If you have changed the default port, add your port number after localhost.

---

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



The screenshot shows the Acronis Access Administration interface. On the left, there is a dark blue sidebar with the Acronis Access logo. The main content area has a white background with the heading "Administration". Below the heading, there is a light blue box containing the text: "In order to configure this Acronis Access Gateway Server, it needs to be registered with an Acronis Access Management Server. To do this, visit the Gateway Servers section on the Management Server to register a new Gateway Server using the following key:". Below this box, the Administration Key "4KR9-X77D-X7YX" is displayed in a bold, black font.

4. Open the Acronis Access Web Interface.
5. Open the **Mobile Access** tab.

6. Open the **Gateway Servers** page.
7. Press the **Add New Gateway Server** button.

## Add New Gateway Server

Display Name:

Marketing Gateway

Address for administration: ⓘ

https:// 192.168.1.72

Use alternate address for client connections ⓘ

Administration Key: ⓘ

4KR9-X77D-X7YX

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

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

---

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

---

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

---

**Note:** Make sure you have at least 1 Gateway Server available.

---

## Creating a Data Source

### Add New Folder ×

Display Name:

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

Data Location:

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:

Sync:

Show When Browsing Server

Require Salesforce.com Activity Logging 

#### Assign This Folder to a User or Group

Find User or Group that

Common Name / Display Name	Distinguished Name	Login Name
<a href="#">john</a>	CN=john,CN=Users,DC=gllilabs,DC=com	john

This folder is assigned to:

Common Name	Distinguished Name	
john	CN=john,CN=Users,DC=gllilabs,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. Select if the folder should require Salesforce activity logging.
13. Find and select the User or Group the folder will be assigned to.
14. Press the Save button.

### 3.3 Setting up a Policy

In order to enroll users in client management, you must configure a user or group policy. For more information on policies, visit the User & Group Policies article.

#### To add a new group policy:

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

## Add a New Group Policy

Search your directory and select a group for this policy.

**Selected Group:**

---

Find group that

Common Name / Display Name	Distinguished Name
<a href="#">Domain Admins</a>	CN=Domain Admins,CN=Users,DC=t-soft,DC=biz

Copy Policy Settings from:

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

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

#### To add a new user policy:

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

## Add a New User Policy

Search your directory and select a user for this policy.

**Selected User:**

---

Find user that

Common Name / Display Name	Distinguished Name	Login Name
<a href="#">Hristo Ilchev</a>	CN=hristo,CN=Users,DC=gllilabs,DC=com	hristo

Copy Policy Settings from:

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

Security Policy
Application Policy
Sync Policy
Home Folders
Server Policy

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

## 3.4 Installing the Access Mobile Client application

1. Browse to Acronis Access in the Apple or Android app store
  - From your iOS device, visit the Apple App Store and search for Acronis Access, or follow this link: <http://www.grouplogic.com/web/meappstore>
  - 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 Access Mobile Client 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 the Acronis Access Server or Gateway Server 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. <RPRODUCT\_NAME> 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.

## 3.5 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.
- A one-time use PIN number.
- 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 on one device. 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, PIN number, and username are also encoded in this URL, so these fields are auto-completed in the enrollment form. At this point, the user simply has enters their password to complete the enrollment process.

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

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

## To enroll in management

### Enroll automatically via enrollment email

1. Open the email sent to you by your IT administrator and tap the **click here to install the Acronis 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, PIN, and Username will be automatically filled out.

---

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

---

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

---

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

---

5. After completing the entire form, tap the **Enroll** button.
6. Depending on the configuration of your company's server, you may be warned that your management server's security certificate is not trusted. To accept this warning and proceed, you can click **Proceed Always**.
7. If 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.
8. A confirmation window may appear if your management policy restricts the storage of files in Acronis Access or disables your ability to add individual servers from within the Access Mobile Client app. If you have files stored locally in the Access Mobile Client app, you will be asked to confirm that any files in your **My Files** local file storage will be deleted. If you select No, the management enrollment process will be canceled and your files will remain unchanged.

### Manual enrollment

1. Open the Acronis Access app.
2. Open **Settings**.
3. Tap **Enroll**
4. Fill in your server's address, your PIN (if required), username and password.
5. After completing the entire form, tap the **Enroll** button.
6. Depending on the configuration of your company's server, you may be warned that your management server's security certificate is not trusted. To accept this warning and proceed, you can click **Proceed Always**.
7. If 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.

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

## Ongoing Management Updates

After the initial management setup, 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.

---

### **Client management connectivity requirements**

*Access Mobile Clients must have network access to the management 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 Gateway servers they will also need to 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>

## 4 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 .....	93
Using the web interface to access files .....	96
Using the desktop client .....	101

### 4.1 First Run

If you haven't done so already, install and configure Acronis Access. For more information on doing so, check the Installing (p. 4) and Configuration Utility (p. 8) 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="access.mycompany.com"/>
Mobile Client Enrollment Address	<input type="text" value="192.168.1.72:3000"/>
Color Scheme	<input type="text" value="Dark Blue"/>
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 a Color Scheme. Current options are Gray, Purple, Cappuccino, Blue, Dark Blue and Orange.

5. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
6. 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.gllilabs.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="pam@gllilabs.com"/>
Use SMTP authentication?	<input type="checkbox"/>

---

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

---

Enter the DNS name or IP address of your SMTP server

Enter the SMTP port of your server.

If you do not use certificates for your SMTP server, unmark **Use secure connection?**

Enter the name which will appear in the "From" line in emails sent by the server.

Enter the address which will send the emails sent by the server.

If you use username/password authentication for your SMTP server, mark **Use SMTP authentication?** and enter your credentials.

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

1. Press **Save**.

## LDAP

### LDAP

Directory Services, like 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.

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

---

**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\joe).
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**.

## Local Gateway Server

### Local Gateway Server

Your local Gateway Server is being administered via address 192.168.1.72:443.  
What address should client connections use to contact the Gateway Server? For example: gateway.example.com

---

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

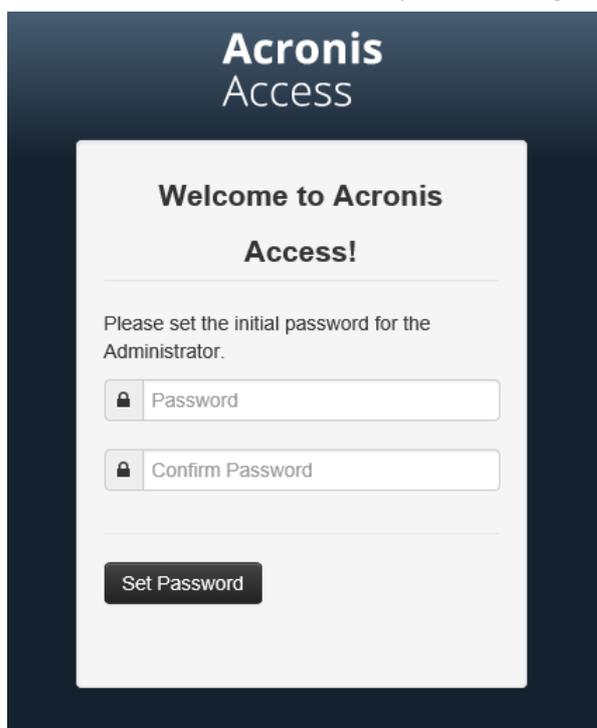
---

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

## 4.2 Using the web interface to access files

### Opening the Acronis Access 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.

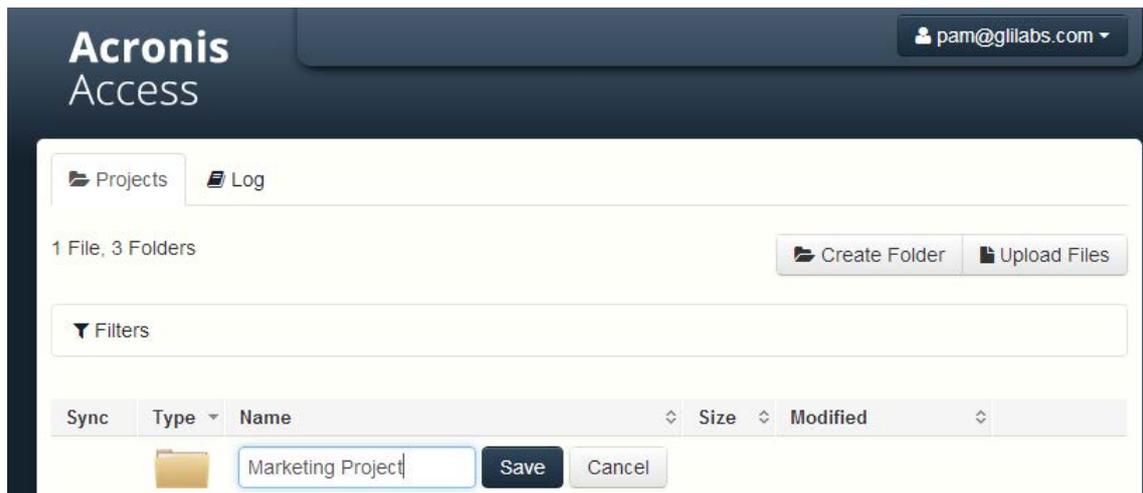


2. Login with your credentials.
  - a. If you have just installed the Acronis Access server, login as **administrator** with the password you set after the installation process. If this is the first time you open the web interface, you will be asked to set the password now.

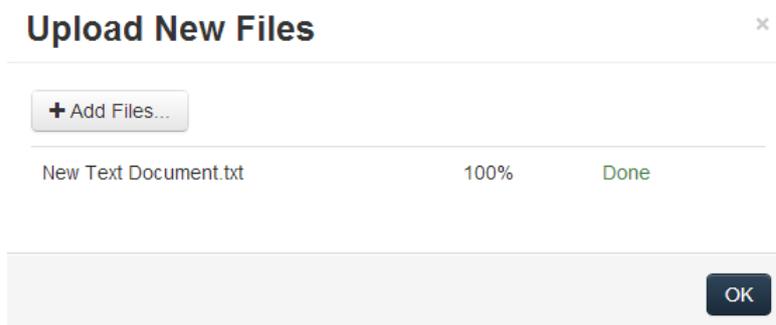
- b. If you received an email inviting you to Acronis Access you may need to **set your own personal password** at this point or log in using your Active Directory credentials.
  - c. If your Acronis Access server has been configured to use Active Directory for authentication and user account provisioning you should be able to login using valid network credentials.
3. If you are logged in as an administrator, you have to leave administrative mode to use the web client.
    - To do so, simply press the **Leave Administration** button at the top-right.

## Creating folders and uploading files

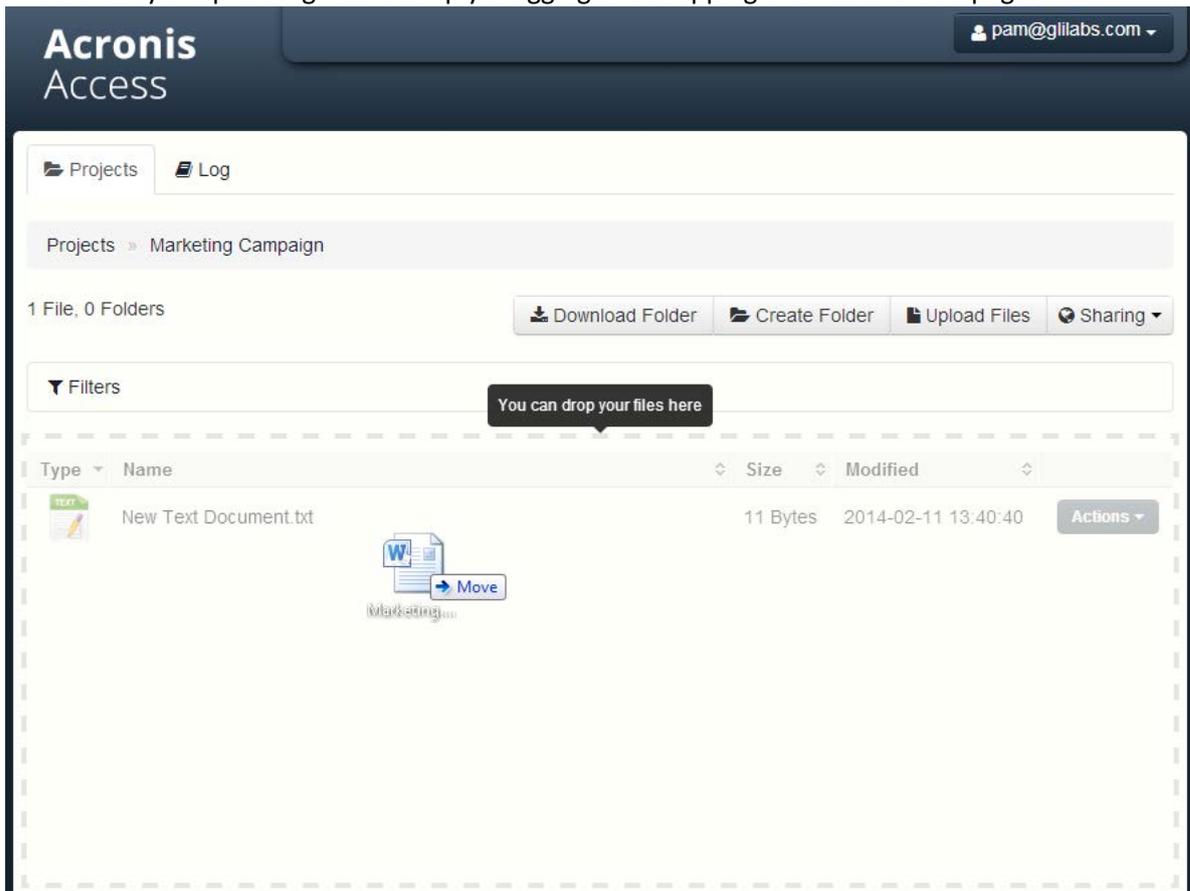
1. Click the **Create Folder** button and enter a name for the new folder. In this example we will use **Marketing Project**. Press the **Save** button.



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

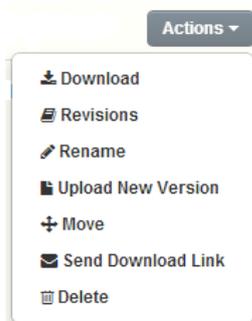


- The file(s) will be uploaded to the folder you are in. Press **Ok**.
- Another way of uploading files is simply dragging and dropping them to the web page.



## File and folder actions

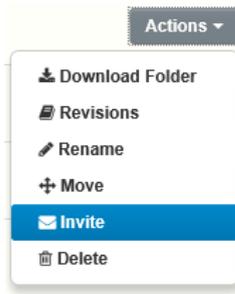
- Notice there is an **Actions** button next to every file or folder. Clicking on it shows what actions you can perform and information on the item, including access to previous versions of the same file.



- If you want to download this or any other file, just click on its name. Alternatively, you can press the **Actions** button and press **Download**.

**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**.

3. Now it's time to share a folder with a colleague or business partner. Click on **Projects**, click on the **Actions** button for the folder you want to share and click **Invite**.



4. In the **Invite others** dialog 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 Others to "Marketing Project" ×

Invite collaborators to this folder using a list of email addresses

Send a message with your invitation

Invite collaborators to share with read-only access

Allow collaborators to invite other collaborators

Allow collaborators to view other members of this share

Invitation Language

▼

**Note:** If the **Invite collaborators to share with read-only access** check box is enabled, invited users can only download and access for reading documents included in the shared folder

5. You can subscribe to email notification alerts for folders shared with you. To do so, simply press the **Actions** button for that shared folder and click on **Notifications**.

### Notifications for 'Collaterals' ×

Use Your Defaults | Customize Your Notifications

Specify how often you would like to be emailed about changes to this share and which events you would like to be notified about.

Frequency (in 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

Change My Defaults

Save Cancel

## Audit logging

You can also look at the history of events by clicking the **Log** tab. Search and filter options are available. You can export the results as XML, CSV or text files.

Projects | Log

### Recent Events Export ▾

Filters

Timestamp	Type	User	Message
2014-02-11 13:54:12	Info	pam@gllilabs.com	Invited plamena@t-soft.biz to share 'Collaterals'.
2014-02-11 13:54:12	Info	pam@gllilabs.com	Added new share 'Collaterals'.
2014-02-11 13:45:35	Info	pam@gllilabs.com	Downloaded file 'Marketing.docx'.
2014-02-11 13:45:34	Info	pam@gllilabs.com	Downloaded file 'Marketing.docx'.
2014-02-11 13:44:41	Info	pam@gllilabs.com	Updated file 'Marketing.docx'.
2014-02-11 13:44:26	Info	pam@gllilabs.com	Deleted file "Marketing.docx".
2014-02-11 13:42:41	Info	pam@gllilabs.com	Downloaded file 'Marketing.docx'.

## Sharing a Single file

### Send Download Link

Send download link for **Corporate documents.pdf** using a semicolon-separated list of email addresses

Send a message with your invitation

Link expiration days must be set between 30 and 365 days.

Number of Days Until Link Expires

Invitation Language

**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 **Send Download Link** under the Actions menu 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. Press the **Actions** button for the file you want to share.
4. Press **Send Download Link**.
5. Enter the email address(es) of the user(s) you want to receive the download link.
6. Set link expiration.
7. Select the language of the email.
8. Press the **Send** button.

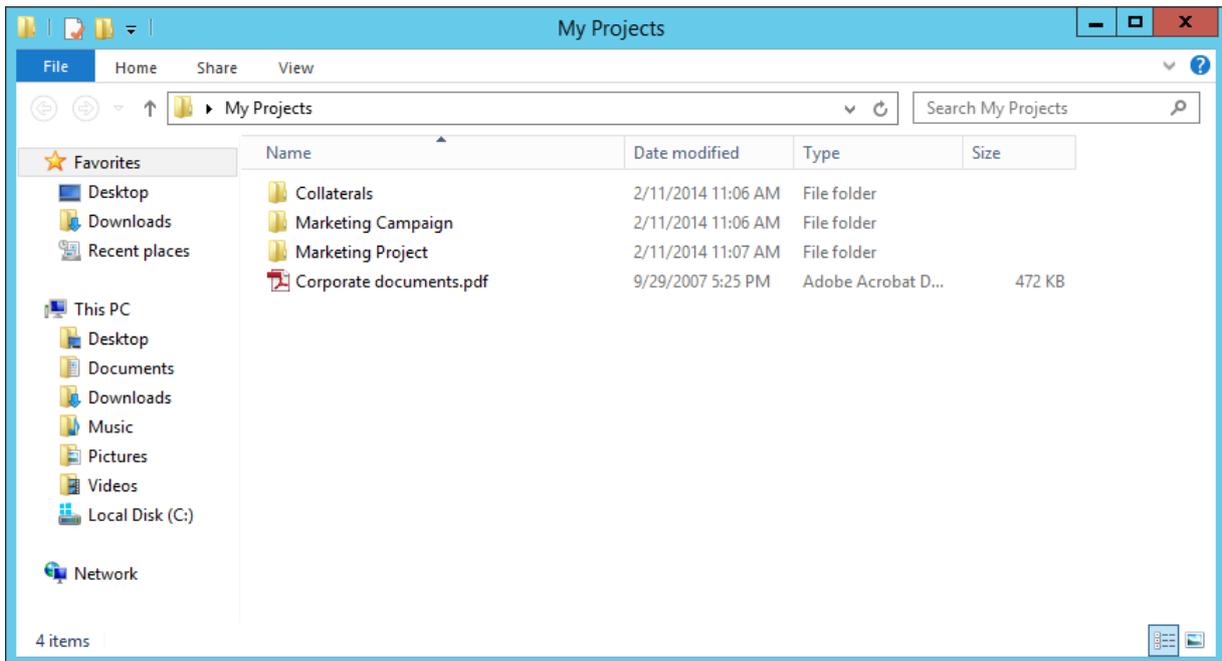
## 4.3 Using the desktop client

### 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**.



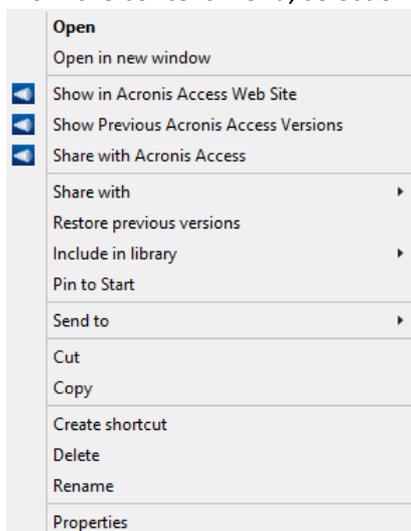
5. Place some files into it by copying them from your computer.
6. Now it's time to share a folder with a colleague. You can do this in two different ways: directly from Windows Explorer or using your web browser. Follow step 7 to share content from your desktop using Windows Explorer, or follow step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

Invite collaborators to this folder using a list of email addresses

Send a message with your invitation

Invite collaborators to share with read-only access

Allow collaborators to invite other collaborators

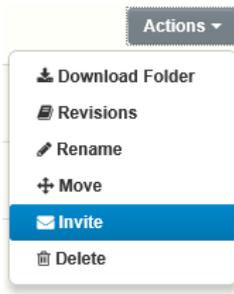
Allow collaborators to view other members of this share

Invitation Language

▼

8. If you prefer to use your web browser instead, 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.

- a. Go to the **Projects** page and locate the **Marketing Campaign** folder.
- b. Click on the **Actions** button sign near the **Marketing Campaign** folder, and then click **Invite**.



- c. In the **Invite others** dialog enter an email address and an appropriate text message.

### Invite Others to "Marketing Project" ×

Invite collaborators to this folder using a list of email addresses

✕ john <john@glilabs.com>

Send a message with your invitation

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

Invite collaborators to share with read-only access

Allow collaborators to invite other collaborators

Allow collaborators to view other members of this share

Invitation Language

English ▼

Share Folder
Cancel

9. 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.
  1. For an external user, the first email with subject **You have been invited to Acronis Access** contains a link to set a personalized password.
  2. The second email with subject **You have been given access to Marketing Campaign** contains your message and a link for accessing the shared files.
10. 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 desktop client, so you can synchronize files automatically among your computers.

---

**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 - [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.

---

## Sharing a single file

### Send Download Link

Send download link for **Corporate documents.pdf** using a semicolon-separated list of email addresses

Send a message with your invitation

Link expiration days must be set between 30 and 365 days.

Number of Days Until Link Expires

Invitation Language

**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 **Send Download Link** under the Actions menu 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. Press the **Actions** button for the file you want to share.
4. Press **Send Download Link**.
5. Enter the email address(es) of the user(s) you want to receive the download link.
6. Set link expiration.
7. Select the language of the email.
8. Press the **Send** button.