

Acronis Access Advanced

Installation & Upgrade Guide

Copyright Statement

Copyright © Acronis International GmbH, 2002-2016. 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.

1 Installing

In this section

Requirements.....	3
Installing Acronis Access Advanced on your server	7
Using the Configuration Utility	8
Using the Setup wizard	12
Clustering Acronis Access.....	17
Load balancing Acronis Access.....	17

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.....	3
Mobile Client Requirements	4
Minimum Hardware Recommendation	4
Network Requirements.....	5
Desktop Client Requirements	6

1.1.1 Operating System Requirements

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

Recommended:

- Windows Server 2016 Standard
- Windows Server 2012 R2 Standard & Datacenter
- Windows Server 2008 R2 Standard, Enterprise & Datacenter, with Service Pack 1

Supported:

- Windows Server 2016 Standard
- Windows Server 2012 R2 Standard & Datacenter
- Windows Server 2012 Standard & Datacenter
- Windows Server 2008 R2 Standard, Enterprise & Datacenter, with Service Pack 1
- Windows Server 2008 Standard, Enterprise & Datacenter, 32 & 64 bit editions, with Service Pack 2

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

Supported devices:

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

Note: Windows devices will work with Acronis Access servers version 6.0 and newer.

Supported OS's:

- iOS 8 or later.
- Android 4.1 or later (devices with x86 processor architecture are not supported).
- Windows 8.1 or later (Windows RT is not supported).

Note: Windows devices will work with Acronis Access servers version 6.0 and newer.

The Acronis Access app can be downloaded from:

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

1.1.3 Minimum Hardware Recommendation

Example deployments

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

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

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

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

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

Note: These values are our recommendations for a production environment. If you plan on starting a trial or installing Acronis Access for testing purposes, you can step-down the hardware depending on your test load.

Small Deployments

- Up to 25 users
- CPU: Intel i7 Xeon class with 4 cores or AMD equivalent.

- RAM: 16 GB
- Disk Space: 100 GB

Medium Deployments

- Up to 500 users
- CPU: Intel i7 Xeon class with 8 cores or AMD equivalent.
- RAM: 40 GB
- Disk Space: 2 TB RAID

Large Deployments

- Up to 2500 users.
- CPU: Intel i7 Xeon class with 16 cores or AMD equivalent.
- RAM: 64 GB
- Disk Space: 10 TB RAID

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

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 your Domain Controller if you plan on using Active Directory (LDAP).
- Network access to an SMTP server for email notifications and invitation messages.
- The address **127.0.0.1** is used internally by the 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.

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

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

- **Port 443 access:** Acronis 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, Windows 10

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

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

Note: The Access desktop client version 7.1.2 is the last version that is compatible with Mac OS X 10.6 and 10.7. If you want to use a newer version of the Acronis Access desktop client, you will have to update your Mac OS.

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 9 and later

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**.

Note: Internet Explorer 11 and earlier do not support uploads of files larger than 4GBs.

- Google Chrome
- Safari 5.1.10 or later

1.2 Installing Acronis Access Advanced on your server

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

Note: For upgrade instructions visit the *Upgrading (p. 58)* section.

Note: For instructions on installing on a cluster visit the *Installing Acronis Access on a cluster (p. 17)* section.

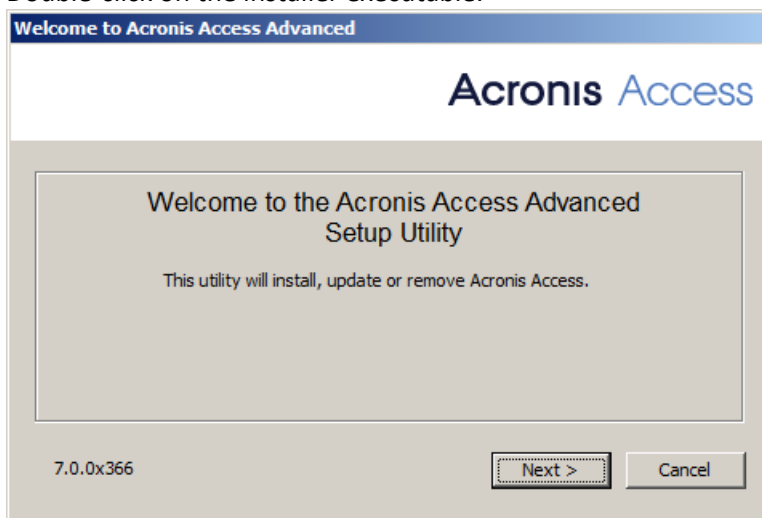
The installation of Acronis Access involves three steps:

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.

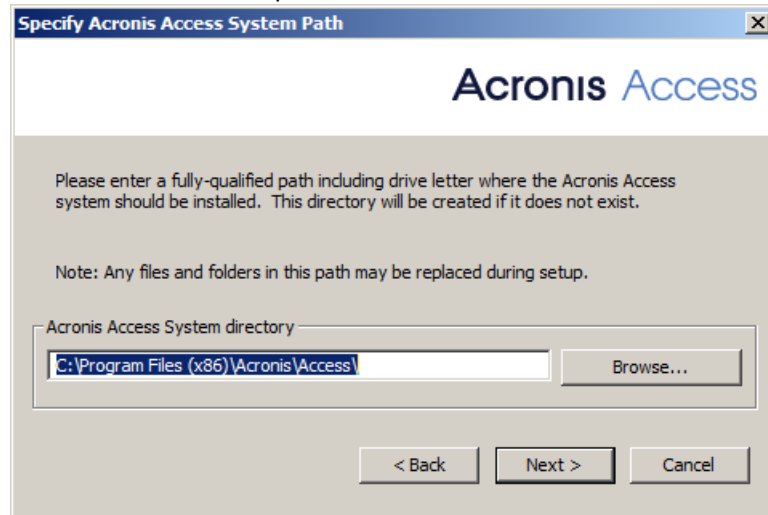
1. Download the Acronis Access installer.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



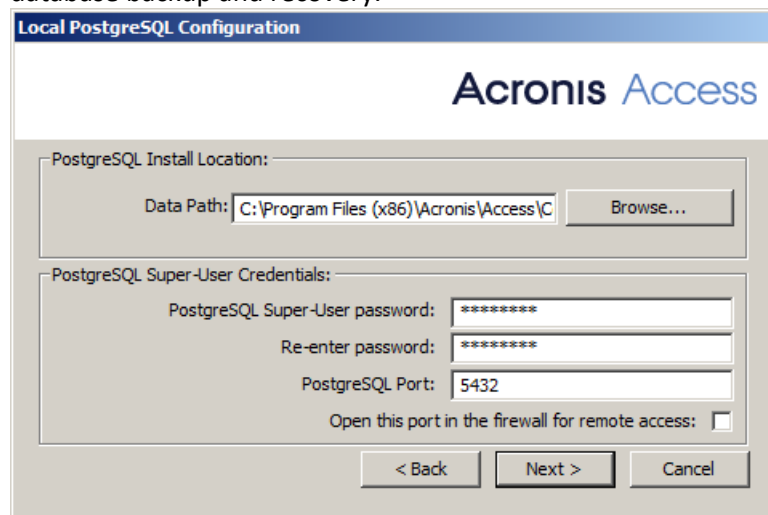
4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.

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.

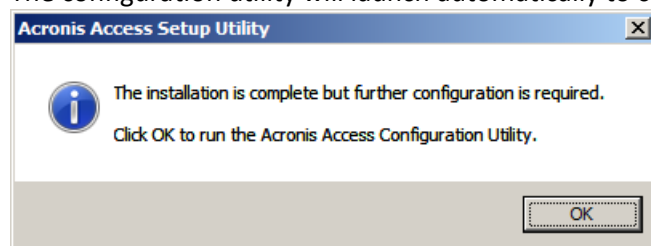
7. Either use the default path or select a new one for the Acronis Access main folder and press OK.



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

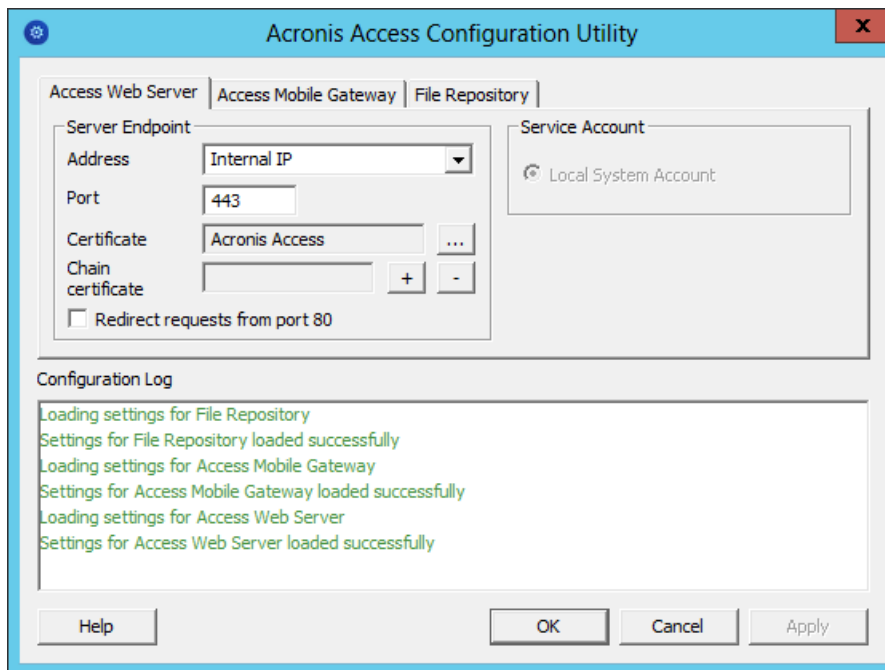
The Acronis Access installer comes with configuration utility, which allows you to quickly and easily set up the access to your Acronis Access Gateway server, File Repository and Acronis Access Server.

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.

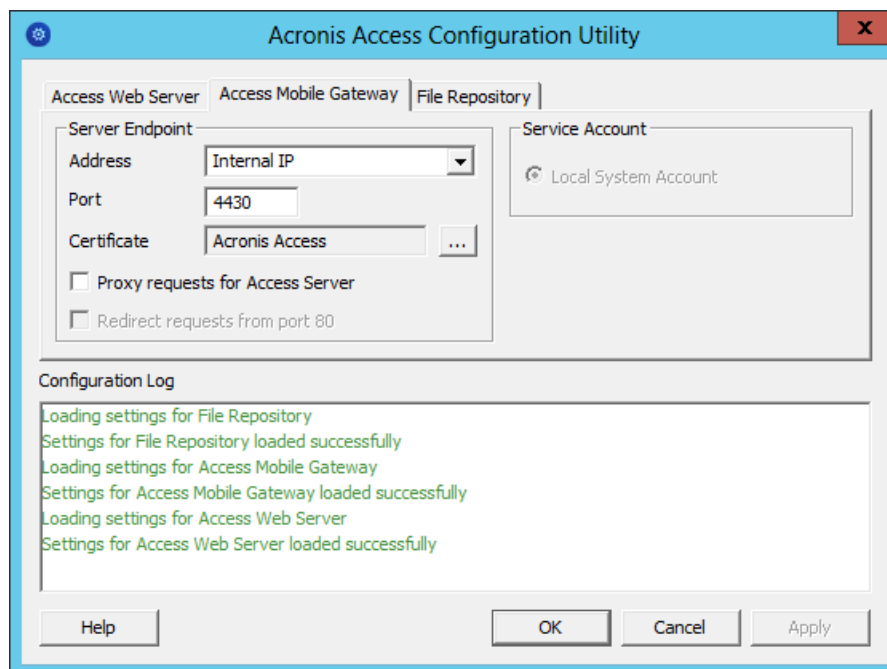
Access Server Overview



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 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.
- **Chain Certificate** - Path to the Intermediate certificate for your Web Interface. You can choose one from the Microsoft Windows Certificate Store. This certificate is only required if your Certificate Authority has also issued you an Intermediate certificate.
- **Redirect requests from port 80** - When selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.
- **Service Account** - This allows the Acronis Access Server service to run in the context of another account. This is normally not required in typical installations.

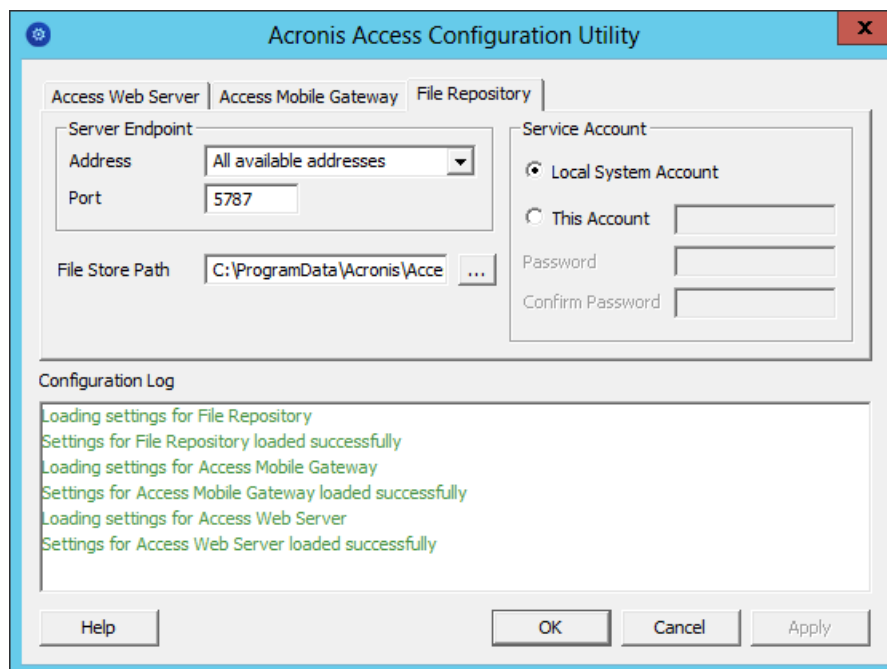
Gateway Server Overview



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

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

File Repository 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 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.

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

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. 12) 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. 58) 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

Acronis Access administrator

Licensing

☒ Start trial

☐ Enter license key

Add license key...

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

Continue

To start a trial:

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

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: Acronis Access

Web Address: https://www.access.domain.com

Mobile Client Enrollment Address: www.access.domain.com

Use Custom Logo: ☐

Audit Log Language: English

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

3. Specify the DNS name or IP address to which the mobile users will enroll to.
4. Select the default language for the **Audit Log**. The current options are English, German, French and Japanese.
5. Press **Save**.

SMTP

SMTP

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

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

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

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

LDAP

LDAP

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

Enable LDAP? ☒

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection? ☐

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

☐ Require exact match

LDAP information caching interval

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

1. Mark **Enable LDAP**.

2. Enter the DNS name or IP address of your LDAP server.
3. Enter the port of your LDAP server.
4. If you use a certificate for connections with your LDAP server, mark **Use Secure LDAP Connection**.
5. Enter your LDAP credentials, with the domain. (e.g. acronis\hristo).
6. Enter your LDAP search base.
7. Enter the desired domain(s) for LDAP authentication. (i.e. to enable LDAP authentication for an account with the email **joe@glilabs.com**, you would enter **glilabs.com**)
8. Press **Save**.

Local Gateway Server

Local Gateway Server

Acronis Access mobile app clients connect to the Access server using its Gateway Server address. Depending on your server configuration, your desktop sync clients and web clients may also connect here. Your Gateway Server is currently running on 192.168.2.129:443. It is recommended that you configure your clients to connect using a DNS address that is reachable from all networks they will be connecting from. If your clients connect through a proxy server, this address may actually be the DNS address of your proxy server. An example: gateway.mycompany.com

Address clients use to connect to the server:

gateway.mycompany.com

Save

Skip

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**.

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 Installing Acronis Access on a Microsoft Failover Cluster

Warning! Acronis Access failover clustering is not supported by versions older than 5.0.3. If you're using an older version, you will have to upgrade to version 5.0.3 or newer before proceeding with any kind of cluster configurations.

The guides listed below will help you install Acronis Access on your cluster.

In this section

Installing Acronis Access on a Windows 2003 Microsoft Failover Cluster	17
Installing Acronis Access on a Windows 2008 (R2) Microsoft Failover Cluster	31
Installing Acronis Access on a Windows 2012 (R2) Microsoft Failover Cluster	45

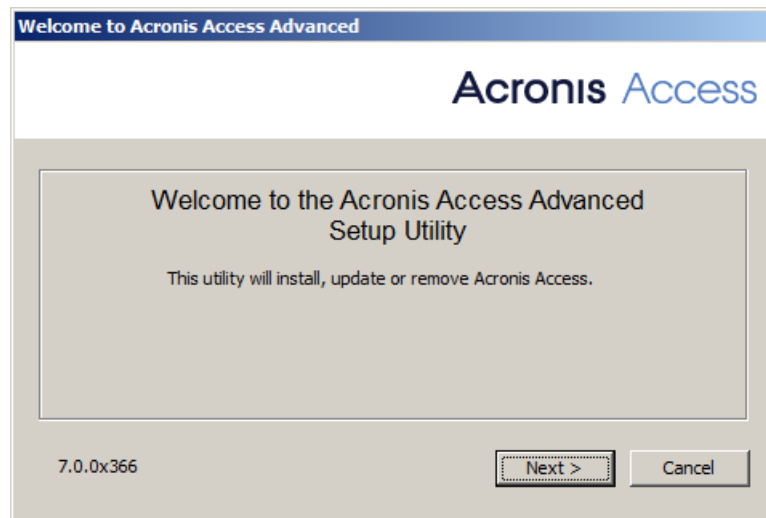
2.1 Installing Acronis Access on a Windows 2003 Microsoft Failover Cluster

Installing Acronis Access

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

1. Download the Acronis Access installer.

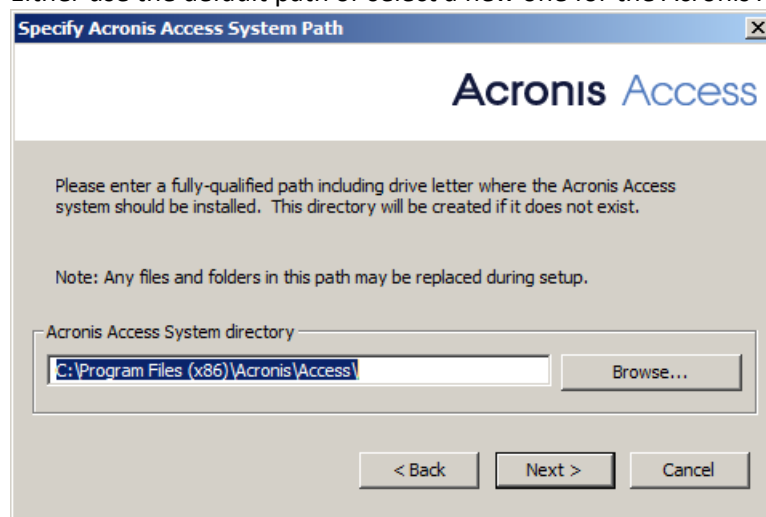
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



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 path or select a new one for the Acronis Access main folder 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.

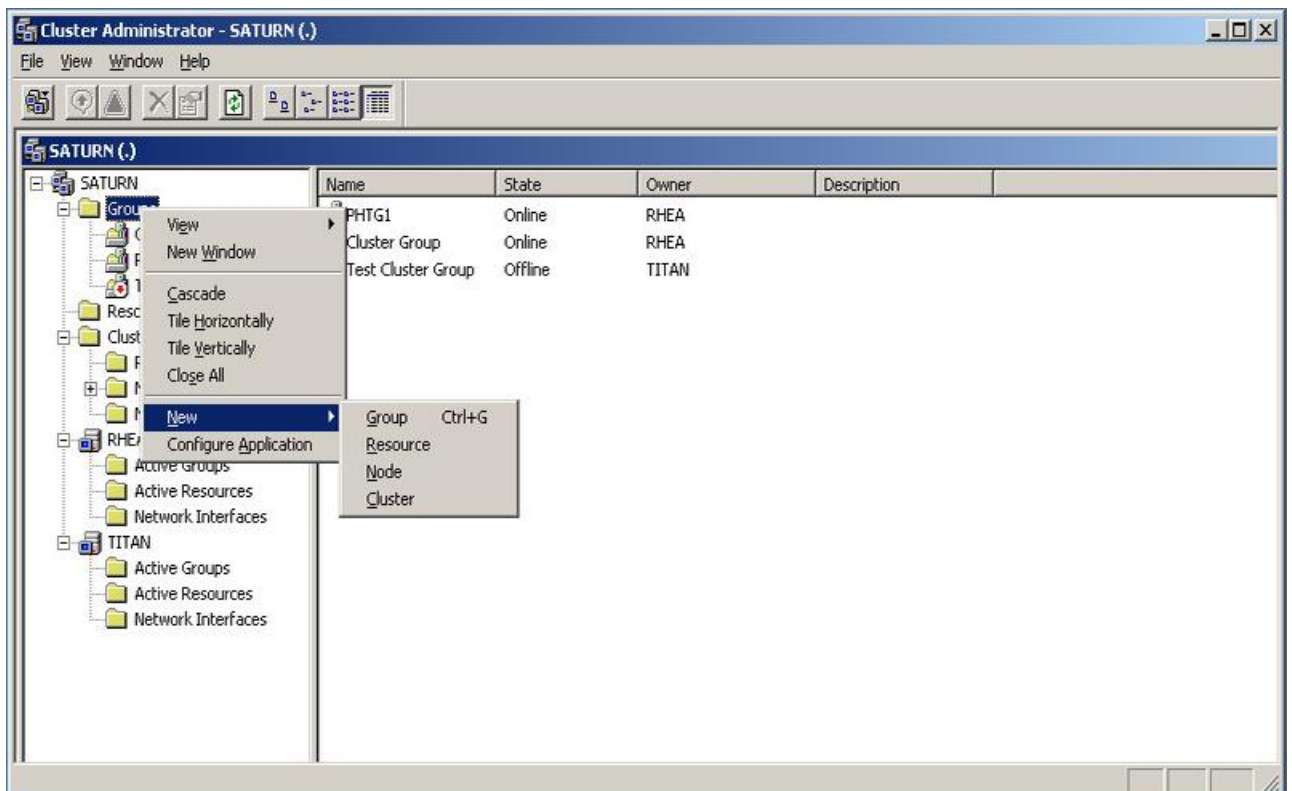
- Choose a location on a shared disk for the **Postgres Data** folder and press **Next**.

- A window displaying all the components which will be installed appears. Press **OK** to continue.

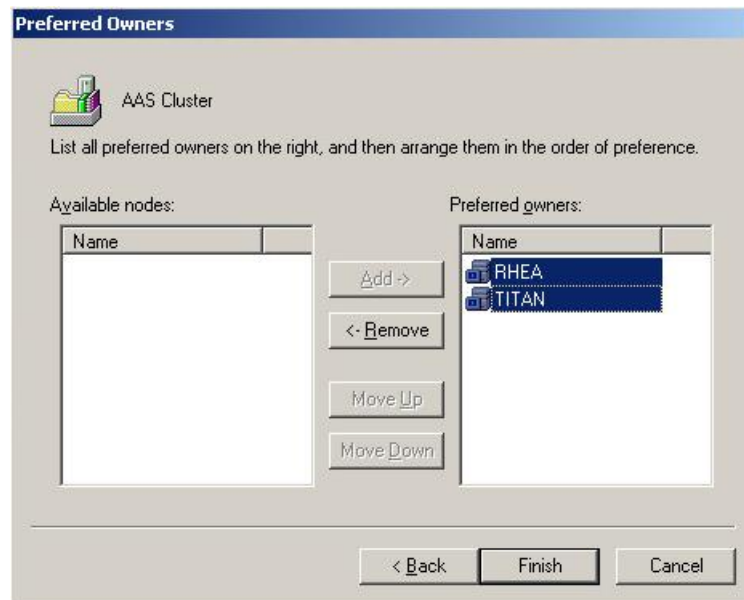
When the Acronis Access installer finishes, press Exit.

Creating the cluster group

- Open the **Cluster Administrator** and open **Groups**.
- Right-click on **Groups** and select **New** and then **Group**. Give the cluster group a proper name. (e.g. Acronis Access, AAS Cluster)



3. Select the machines which will be a part of this cluster group and press **Finish**.



Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\Acronis\Access\Gateway Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/access_cluster/database/'**).

Note: Use slashes(/) as a path separator.

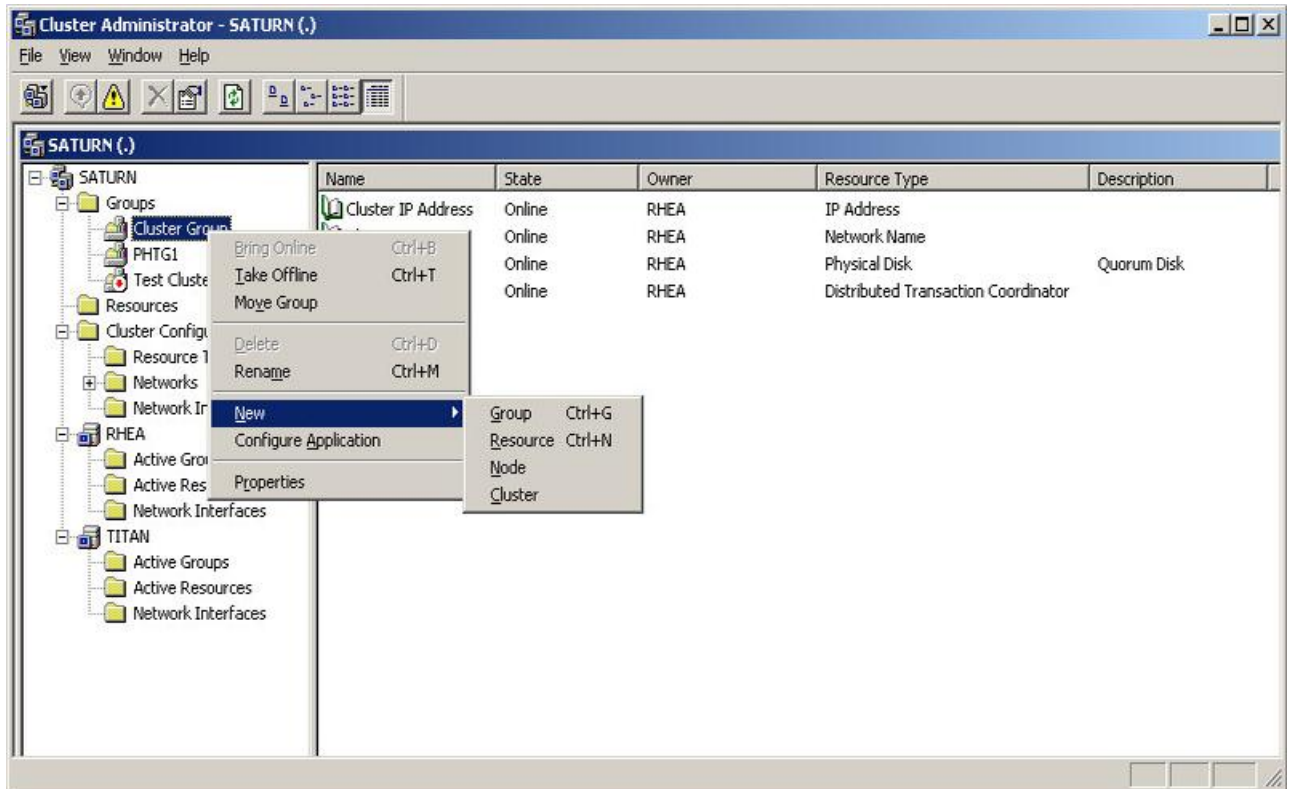
Note: You can copy the configured **database.yml** from the first node and paste it to the second node.

Adding all of the necessary services to the Acronis Access cluster group

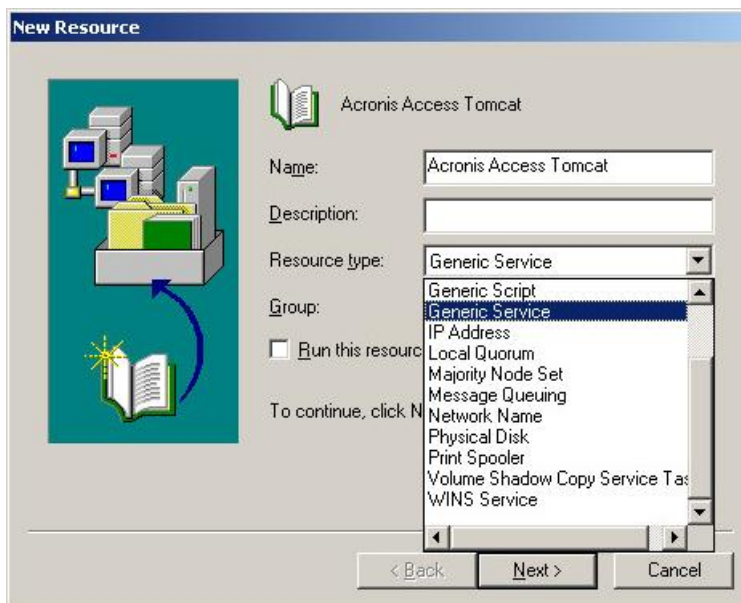
Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

1. Right-click on the Acronis Access cluster group.

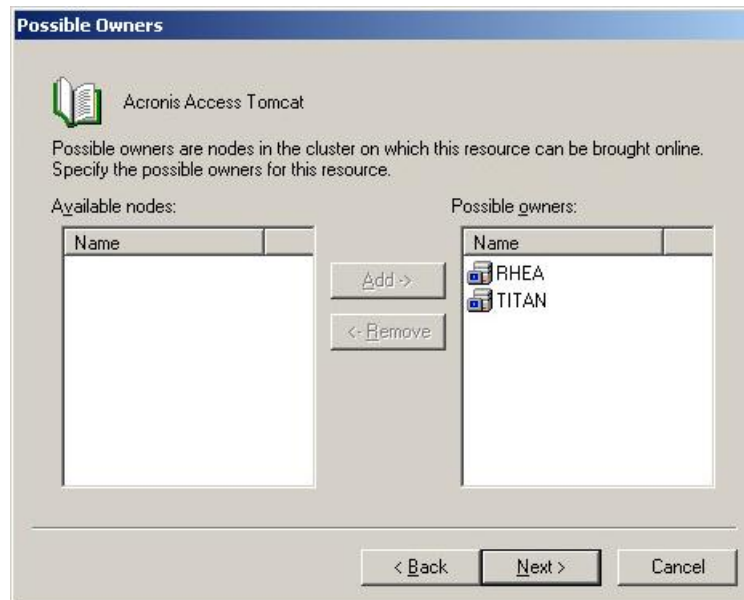
2. Open **New** and select **Resource**.



3. Enter a name for the service and select the correct cluster group.
4. From the **Resource Type** drop down menu select **Generic Service** and press **Next**.



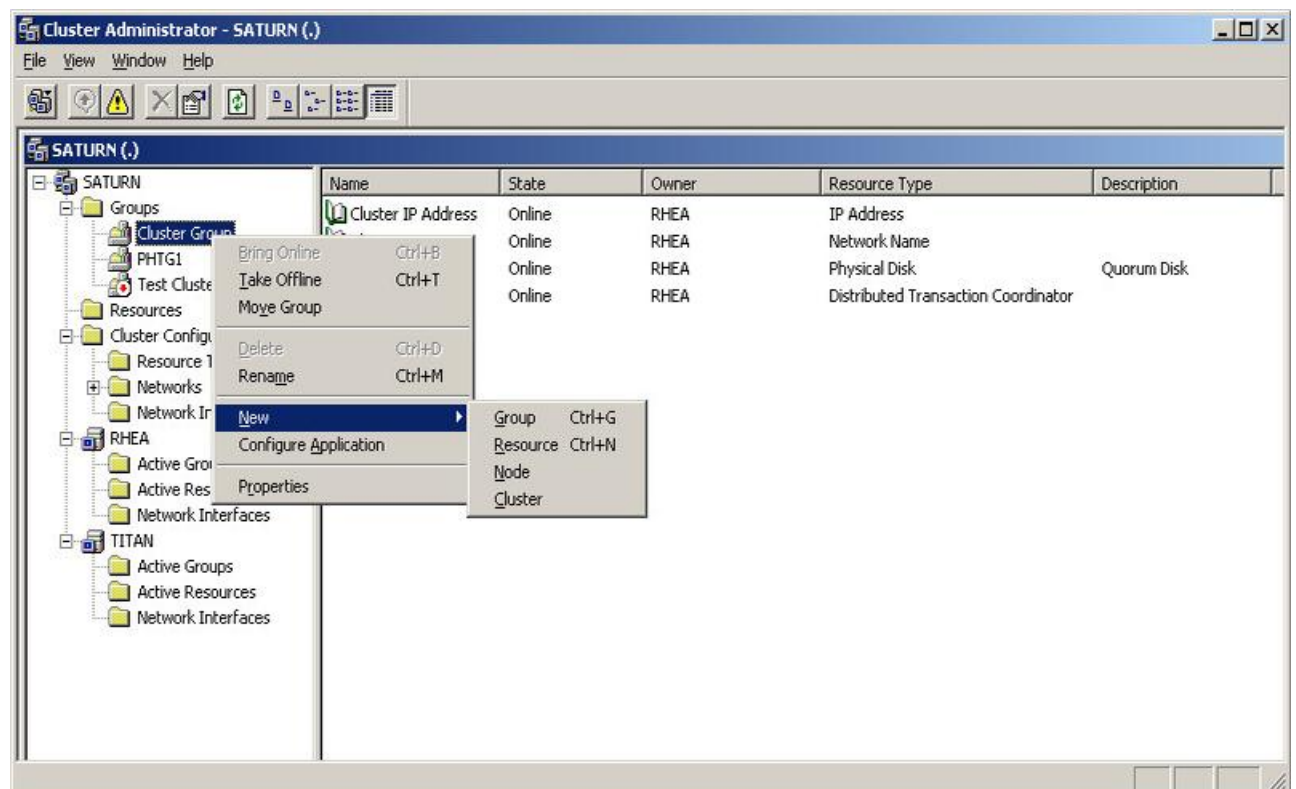
- Make sure both of your nodes are listed as **Possible owners** and press **Next**.



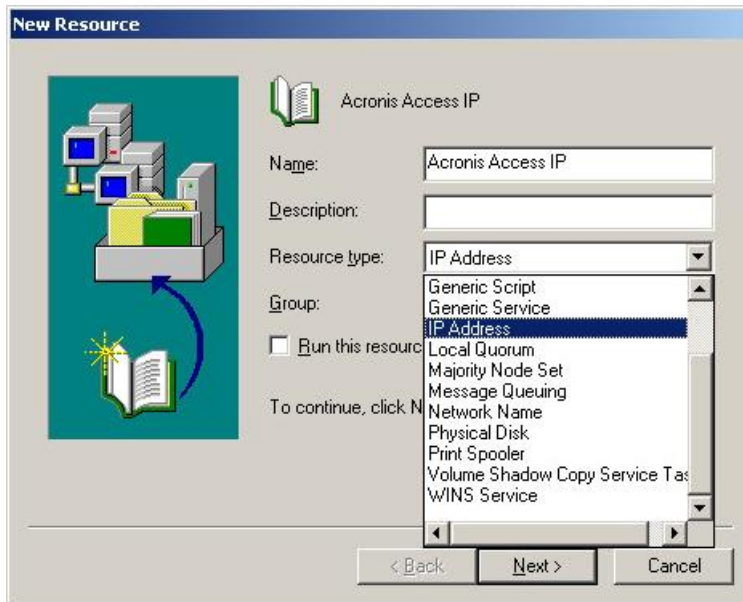
- Skip the dependencies for now by pressing **Next**.
- Enter the correct service name of the service you are adding (e.g. postgresql-x64-9.2) and press **Next**.
- Skip the **Registry Replication** window for now by pressing **Next**.
- Press **Finish** to complete the procedure.

Setting an IP address for the cluster group

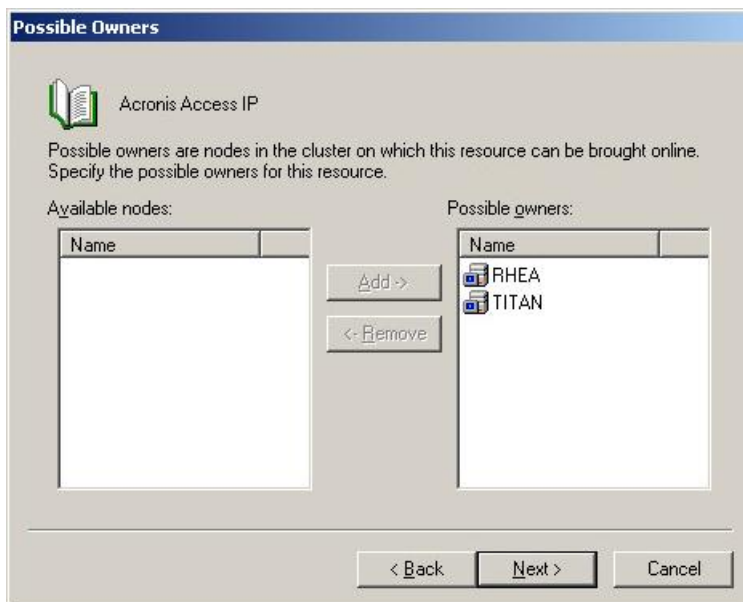
- Right-click on the Acronis Access cluster group.
- Open **New** and select **Resource**.



3. Enter a name for the resource and select the correct cluster group.
4. From the **Resource Type** drop down menu select **IP Address** and press **Next**.



5. Make sure both of your nodes are listed as **Possible owners** and press **Next**.

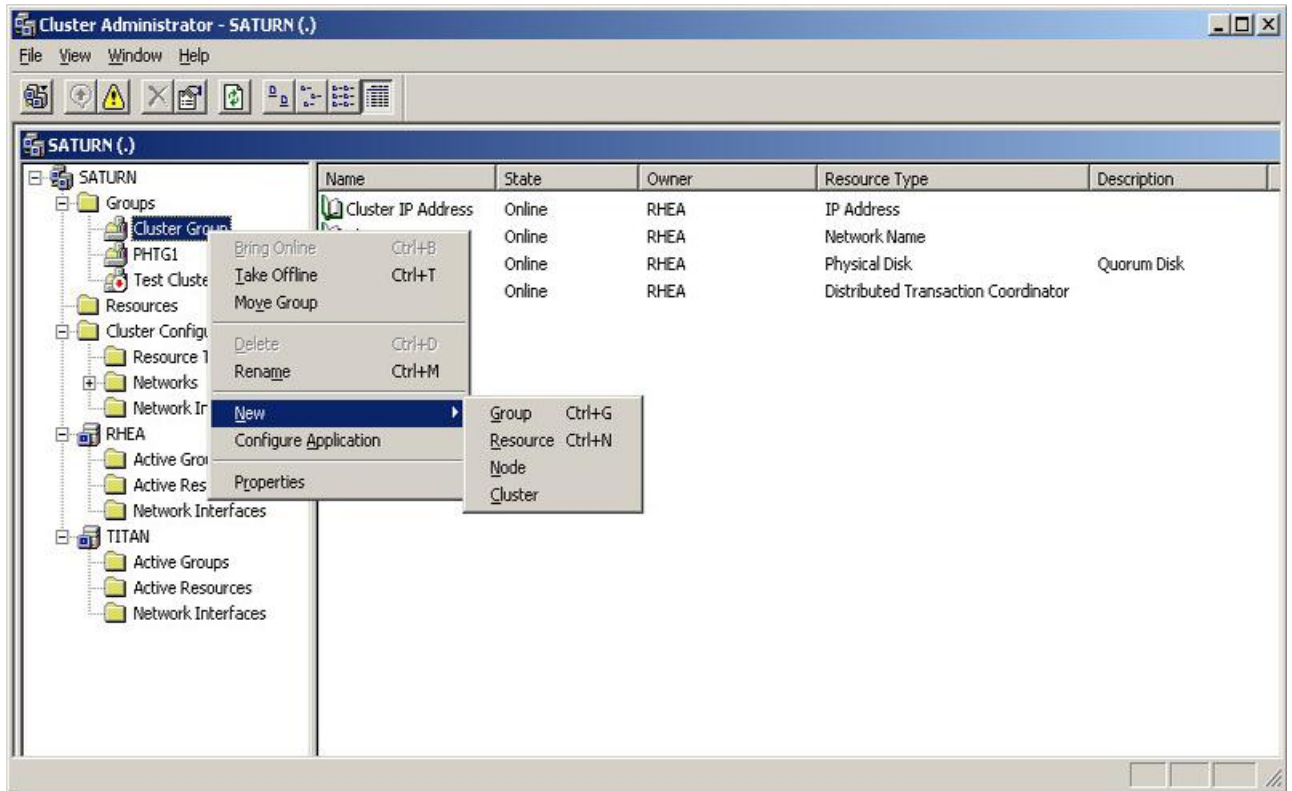


6. Skip the dependencies for now by pressing **Next**.
7. Enter the IP address you will use for this cluster group.
8. Enter the subnet mask and press **Finish**.

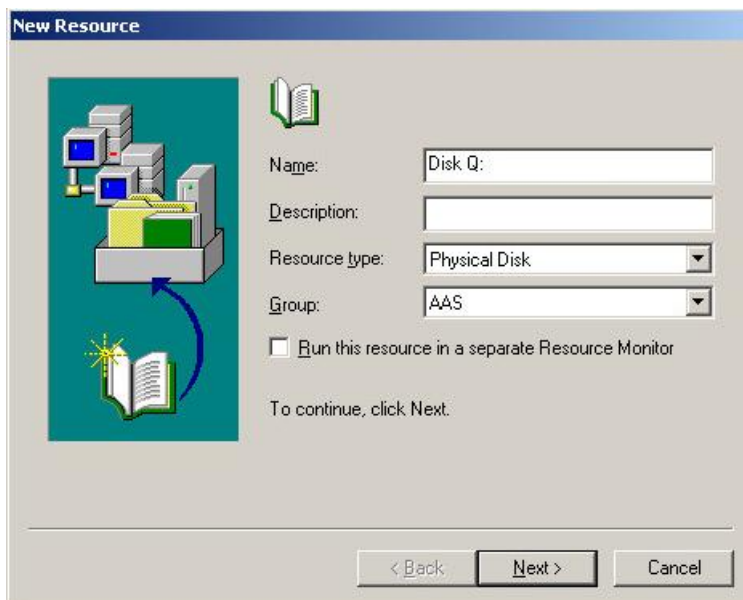
Adding a shared disk

1. Right-click on the Acronis Access cluster group.

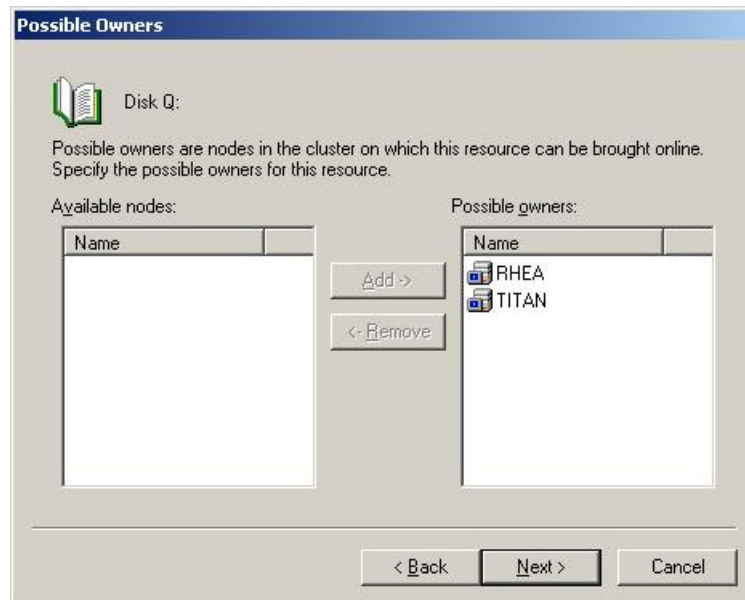
2. Open **New** and select **Resource**.



3. Enter a name for the resource and select the correct cluster group.
4. From the **Resource Type** drop down menu select **Physical Disk** and press **Next**.



5. Make sure both of your nodes are listed as **Possible owners** and press **Next**.

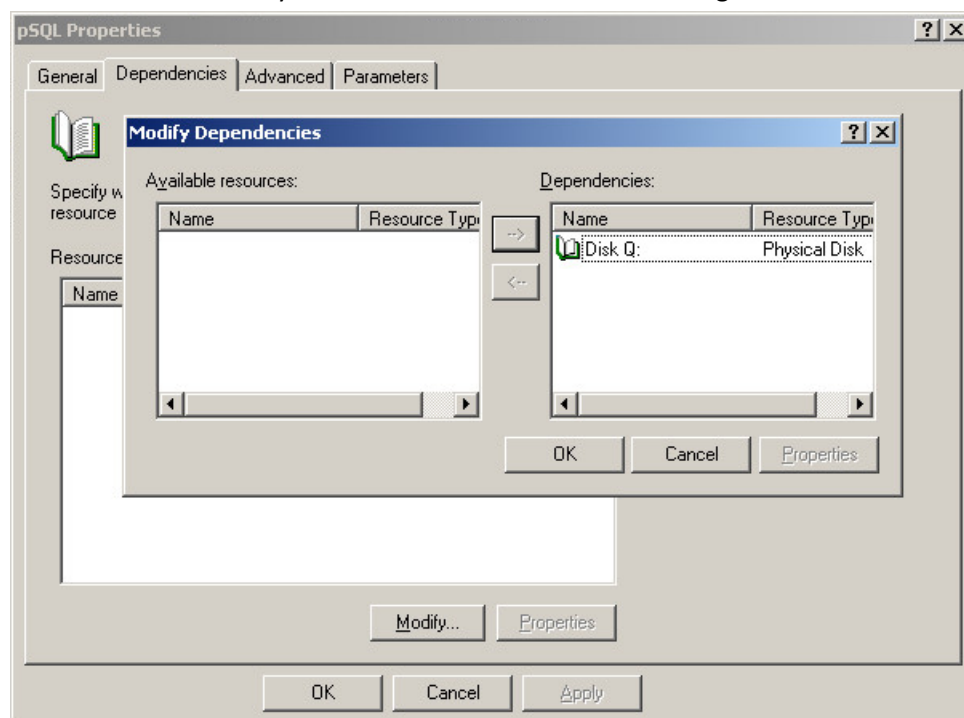


6. Skip the dependencies for now by pressing **Next**.
7. Select an available disk from the drop down menu and press **Finish**.

Configuring dependencies

For PostgreSQL and Acronis Access File Repository do the following:

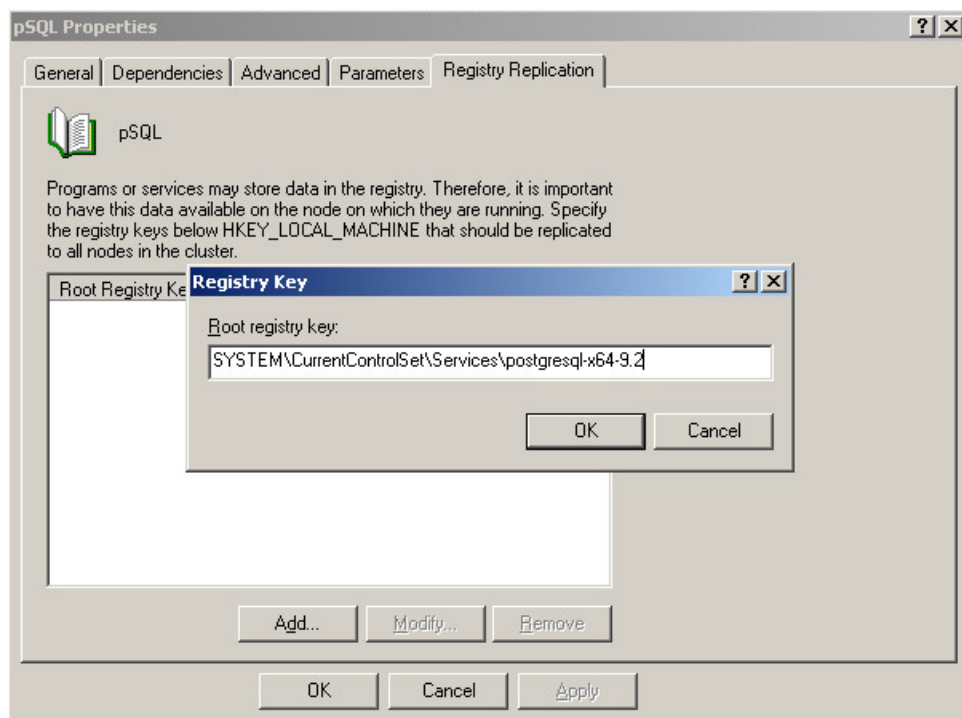
1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Modify**.
4. Select the shared disk you have added and move it to the right side.



5. Press **OK**.

For PostgreSQL also do the following:

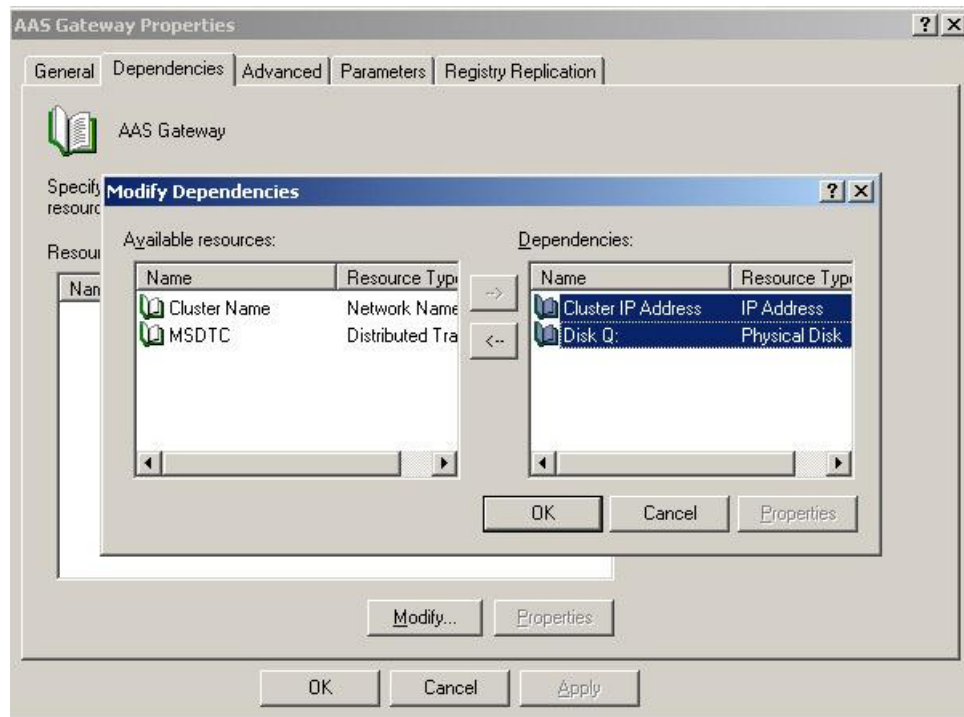
1. Click on the **Registry Replication** tab.
2. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL (For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)



For the Acronis Access Gateway Server service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Modify**.

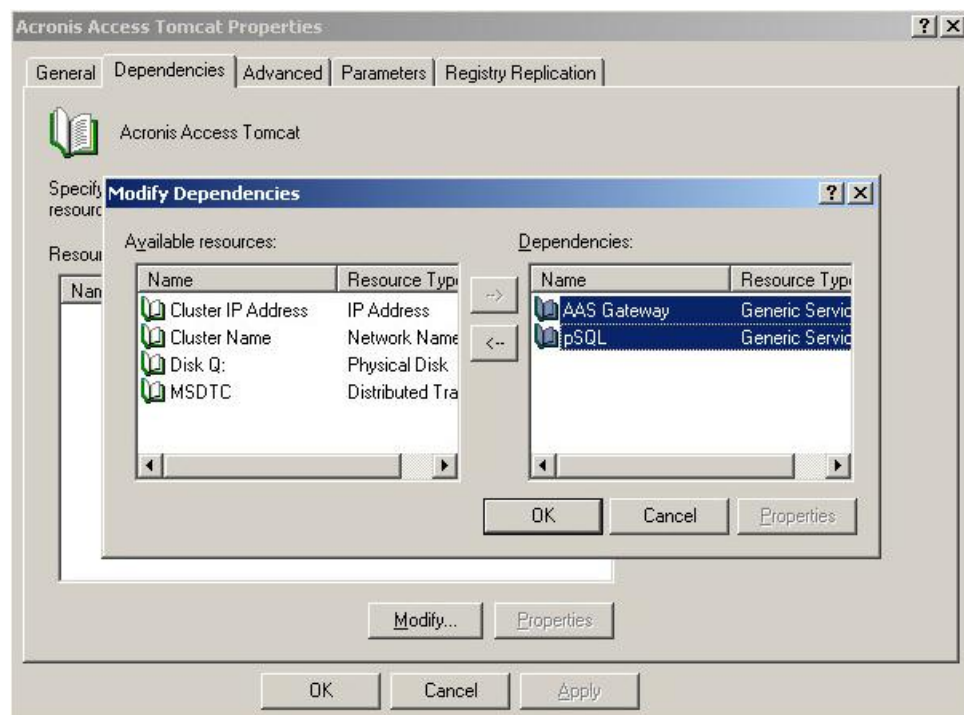
4. Select the **IP Address** and **Physical disk** and move them to the right side.



5. Press **OK**.

For the Acronis Access Tomcat service do the following:

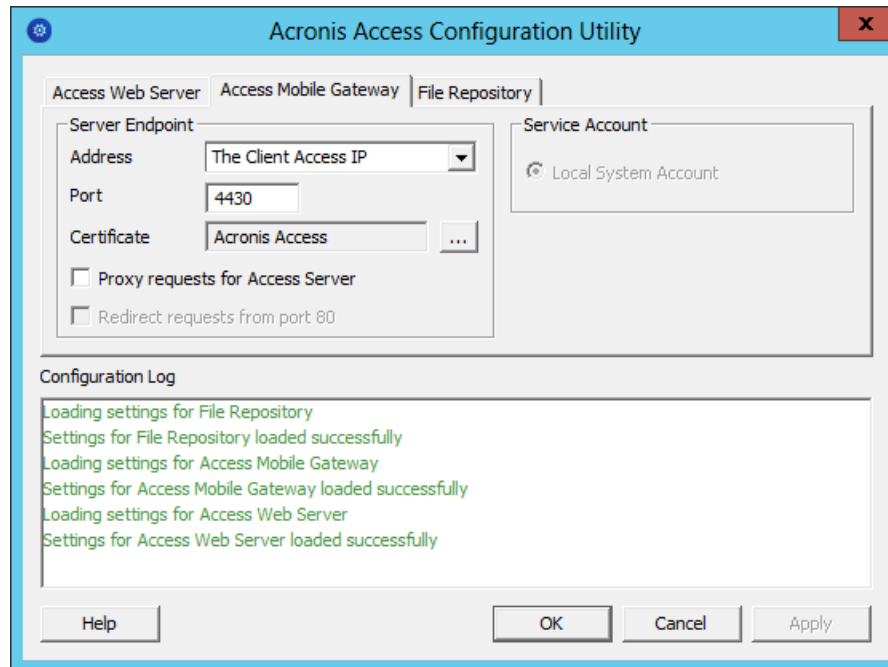
1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Modify**.
4. Select the PostgreSQL and Acronis Access Gateway Server services and move them to the right side.



5. Press **OK**.

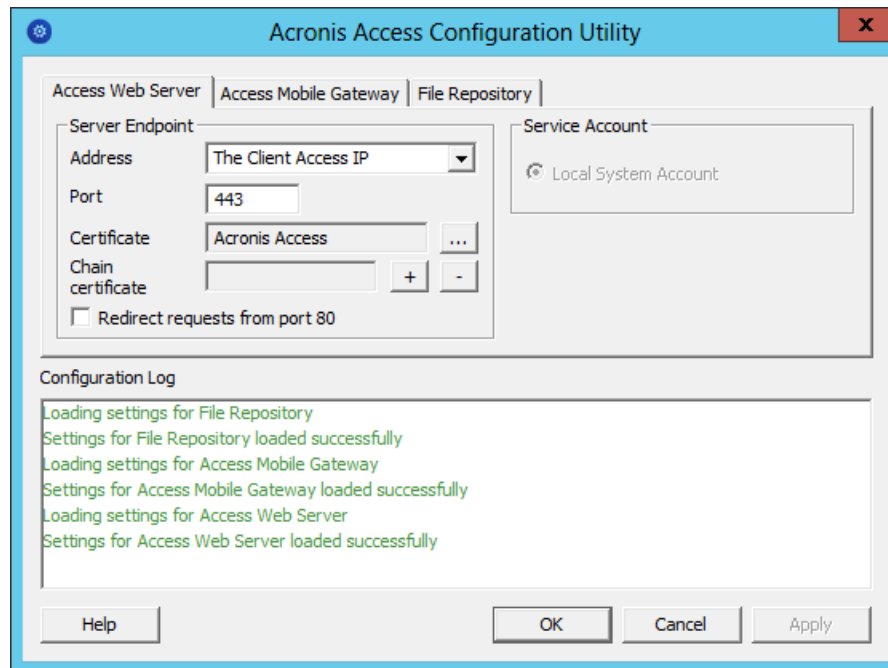
Bringing the cluster group online and using the Configuration Utility

1. Right-click on the cluster group and press **Bring online**.
2. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**
3. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

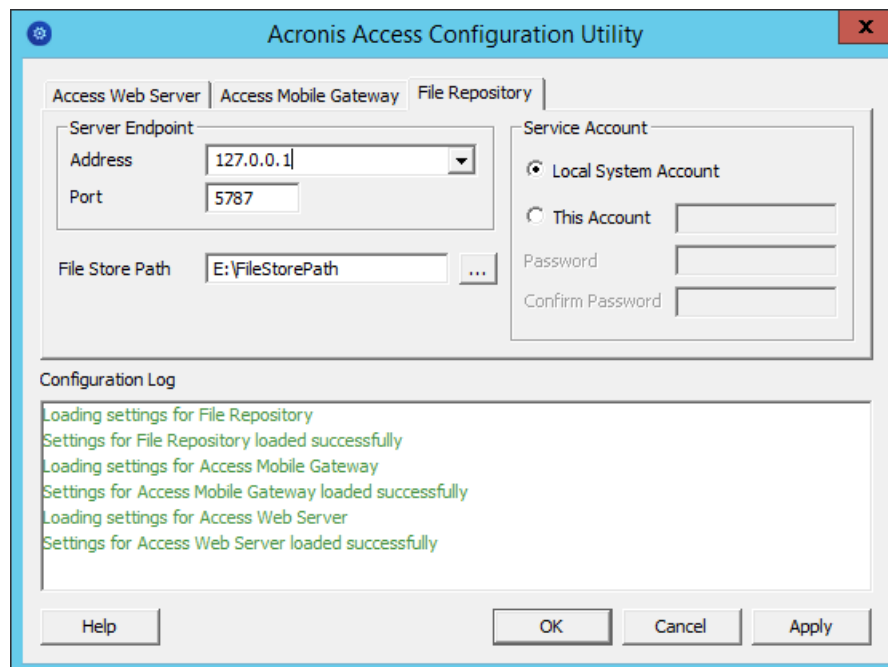


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



5. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

Installation and configuration on the second node

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

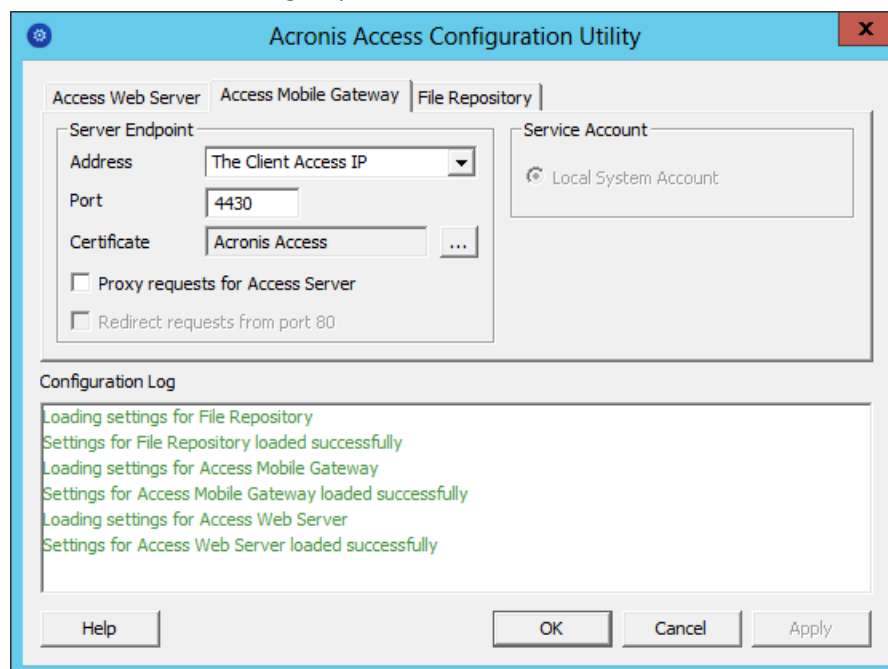
2. Install Acronis Access on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.
3. Complete the installation.
4. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\Acronis\Access\Gateway Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/access_cluster/database/'**).

Note: Use slashes(/) as a path separator.

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

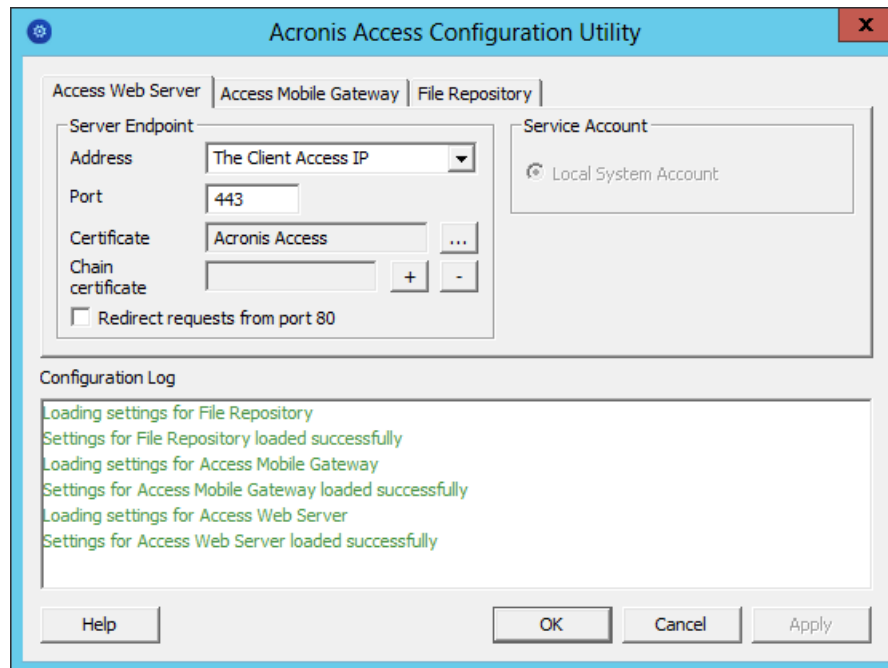
Note: The path should match the path set on the first node.

5. Move the cluster group to the second node. To do so, right-click on the cluster group and click on **Move Group**.
6. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**
7. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

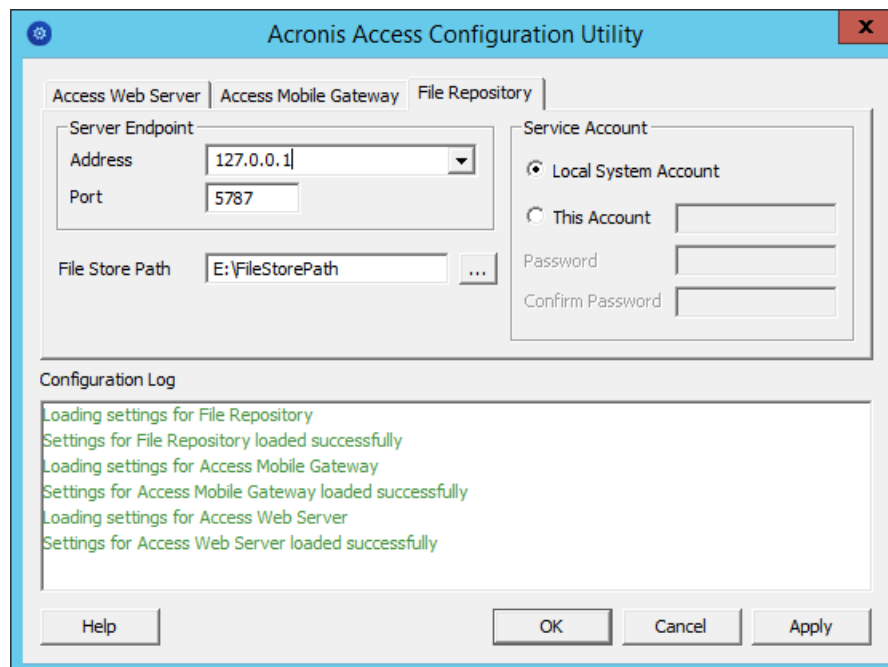


8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



9. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



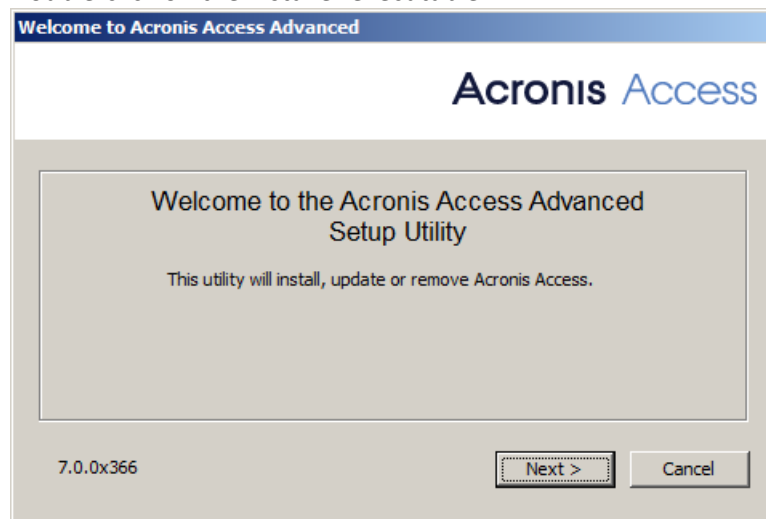
10. Click **OK** to complete the configuration and restart the services.

2.2 Installing Acronis Access on a Windows 2008 (R2) Microsoft Failover Cluster

Installing Acronis Access

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

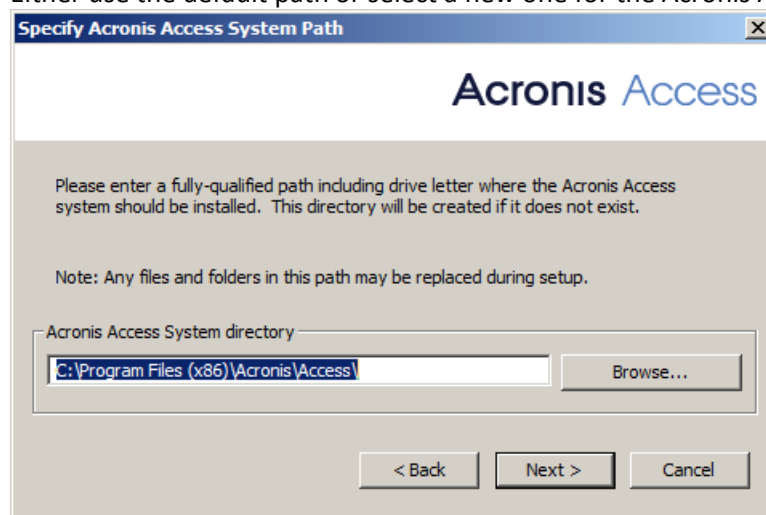
1. Download the Acronis Access installer.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



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

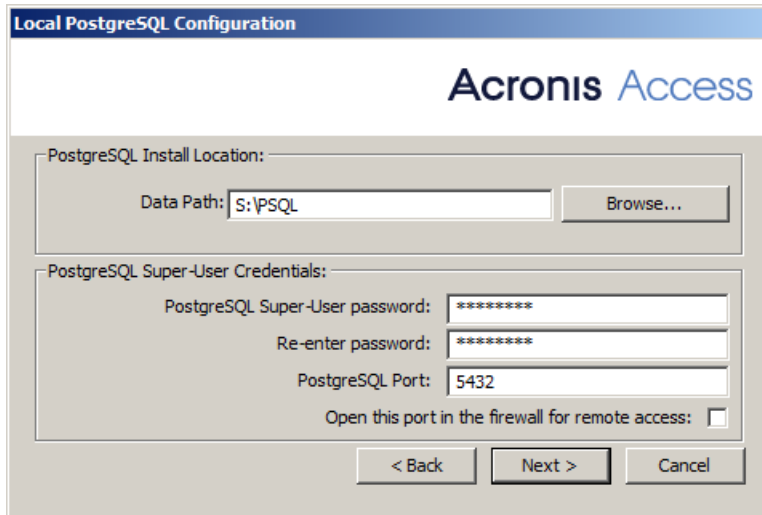
Note: If you're deploying multiple Acronis Access servers, or you are installing a non-standard configuration, you can select which components to install from the **Custom Install** button.

7. Either use the default path or select a new one for the Acronis Access main folder 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. Choose a location on a shared disk for the **Postgres Data** folder and press **Next**.



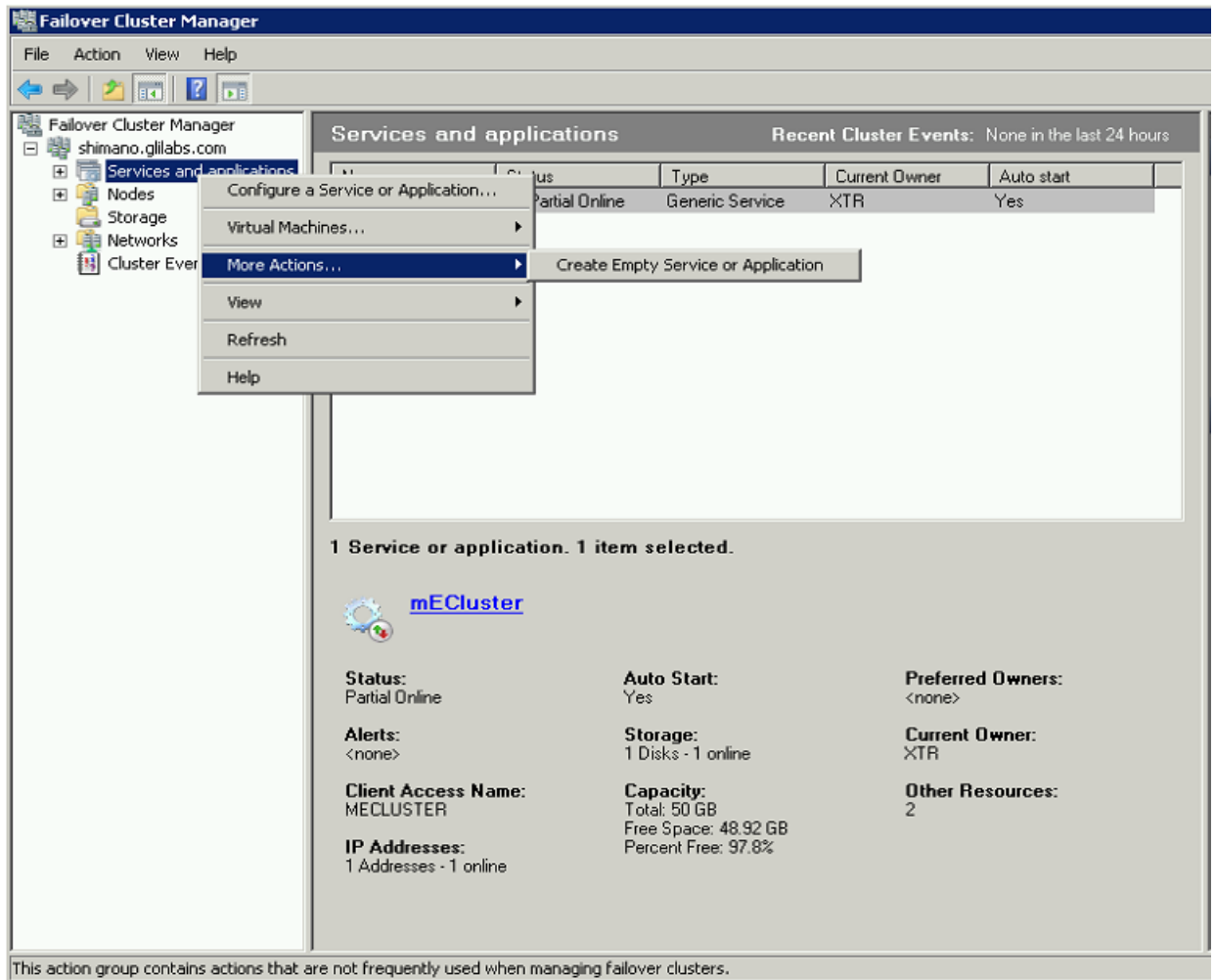
10. A window displaying all the components which will be installed appears. Press **OK** to continue.

When the Acronis Access installer finishes, press Exit.

Creating the Service group

1. Open the **Failover Cluster Manager** and expand your cluster.
2. Right-click on **Services and Applications** and select **More Actions**.

3. Select the **Create Empty Service or Application** and press **Next**. Give the service group a proper name. (e.g. Acronis Access, AAS Cluster).



Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\Acronis\Access\Gateway Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/access_cluster/database/'**).

Note: Use slashes(/) as a path separator.

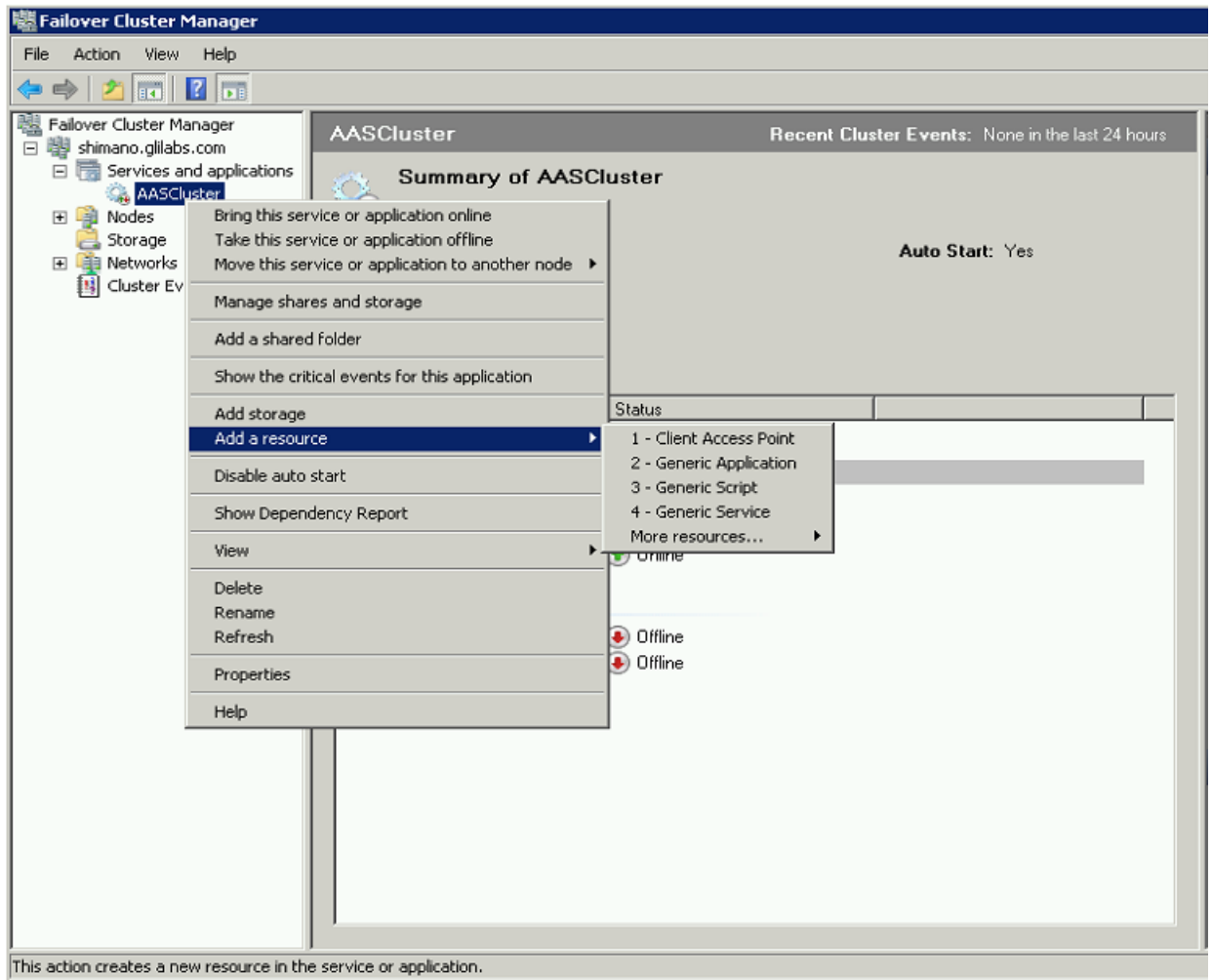
Note: You can copy the configured database.yml from the first node and paste it to the second node.

Adding all of the necessary services to the Acronis Access Service group

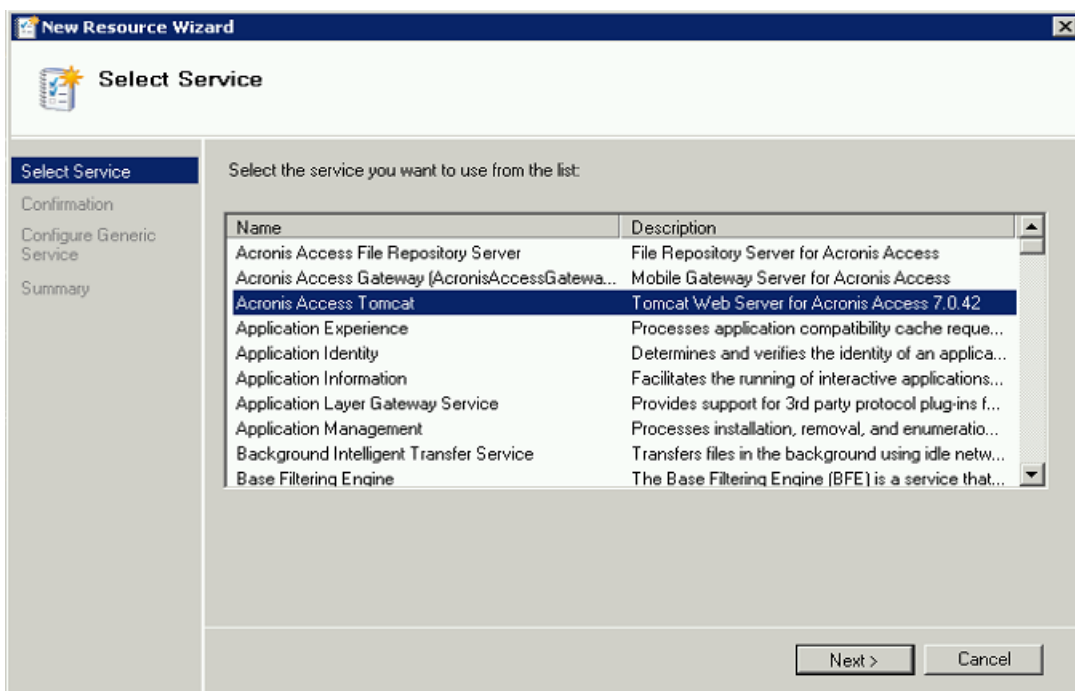
Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

1. Right-click on the Acronis Access service group and select **Add a resource**.

2. Select **Generic Service**.



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

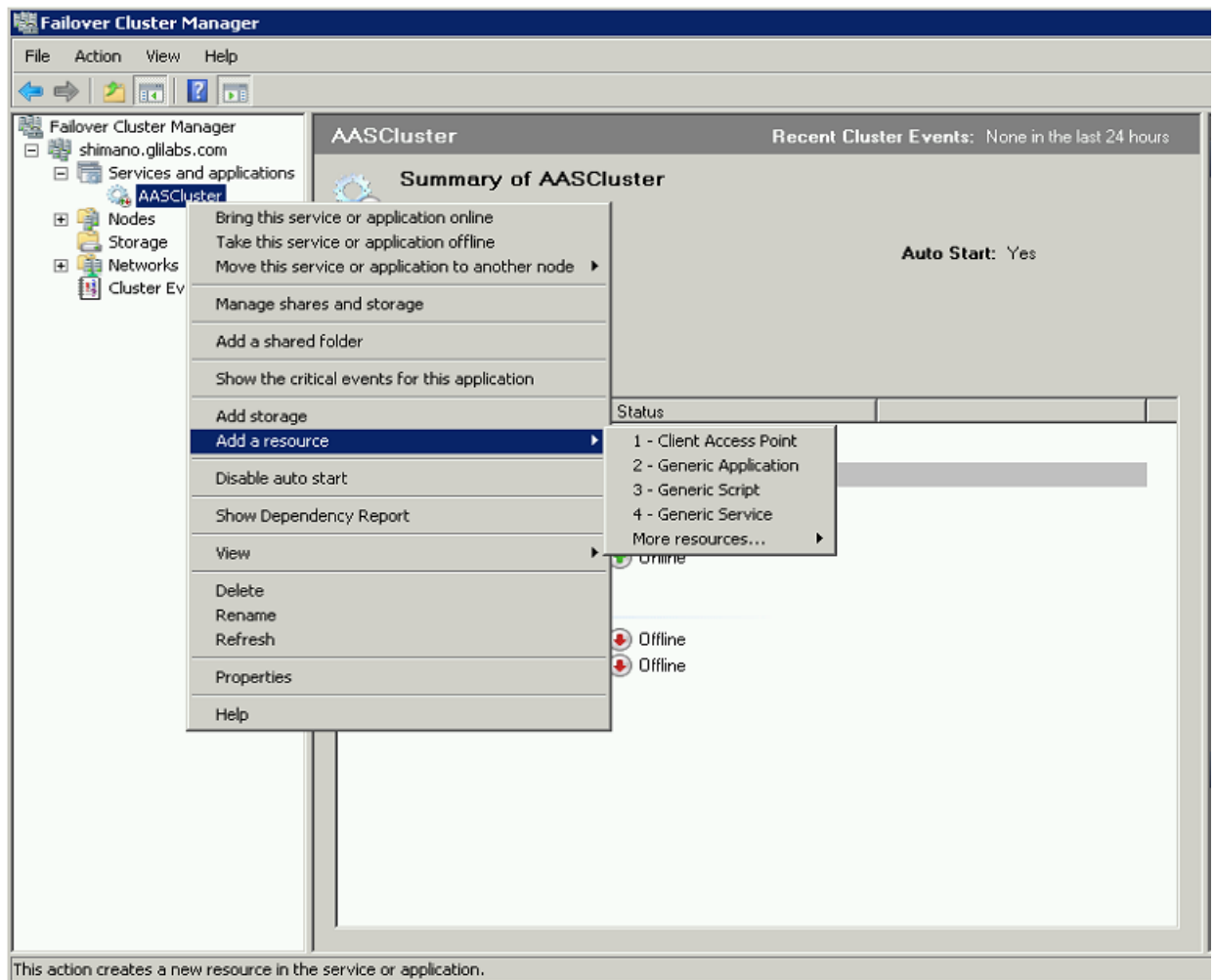


4. On the confirmation window press **Next**.

5. Press **Next** on the **Replicate Registry Settings** window.
6. On the summary window press **Finish**.

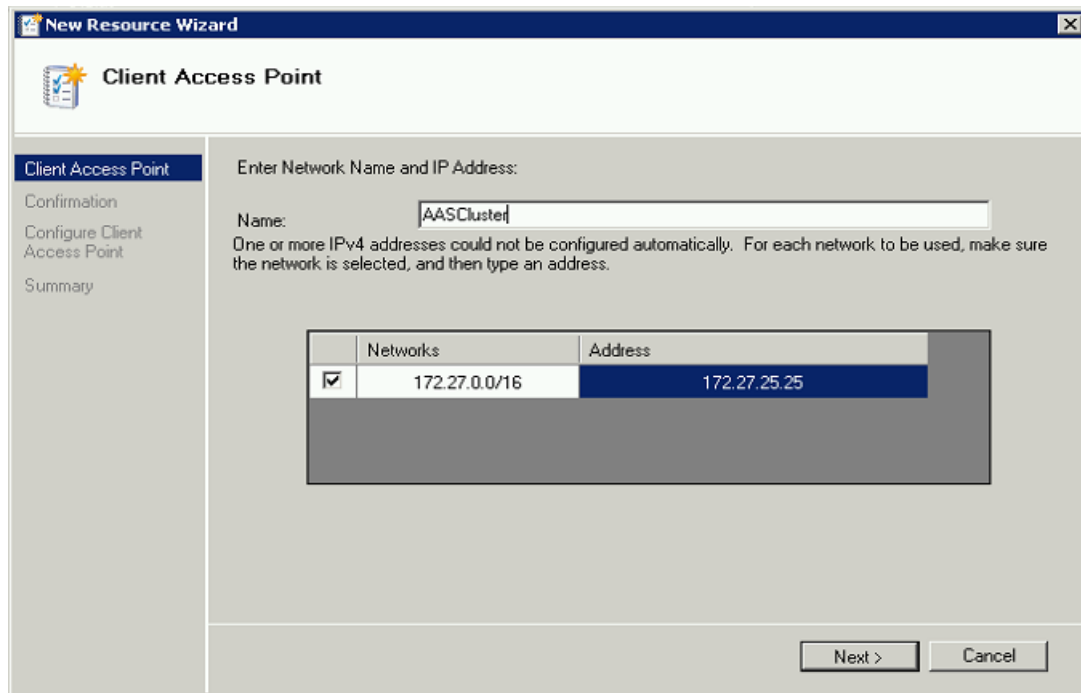
Setting a Client Access Point

1. Right-click on the Acronis Access service group and select **Add a resource**.
2. Select **Client Access Point**.



3. Enter a name for this access point.

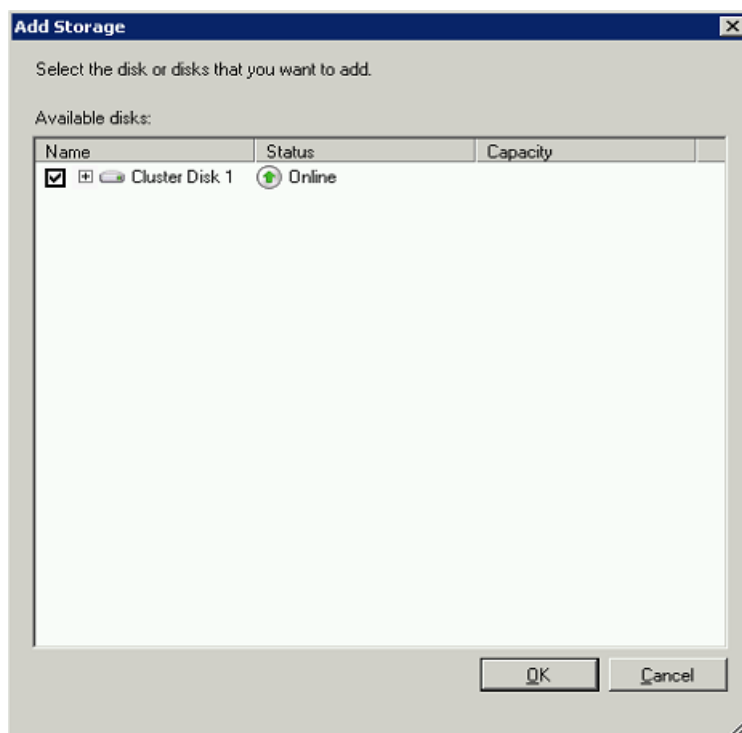
4. Select a network.



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

Adding a shared disk

1. Right-click on the Acronis Access service group and select **Add Storage**.
2. Select the desired shared drive.



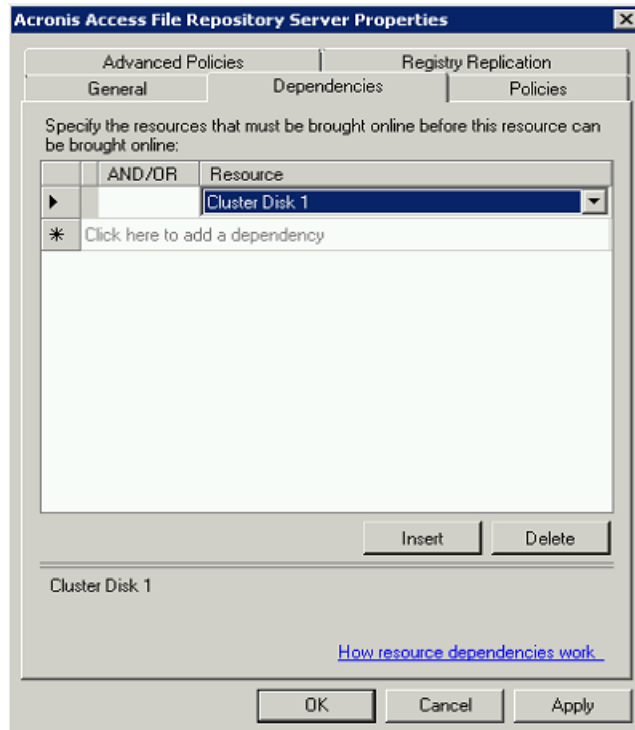
3. On the Confirmation window press **Next**.
4. On the summary window press **Finish**.

Configuring dependencies

1. Double click on the Acronis Access Service group.

For PostgreSQL and Acronis Access File Repository services do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the shared disk you have added.

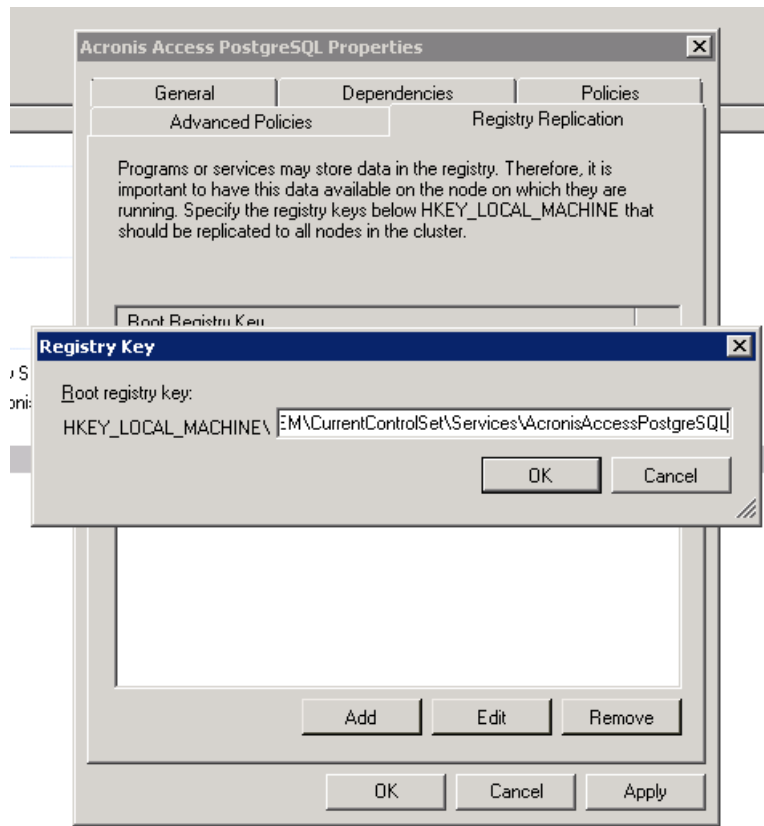


4. Press **Apply** and close the window.

For PostgreSQL also do the following:

1. Click on the **Registry Replication** tab.

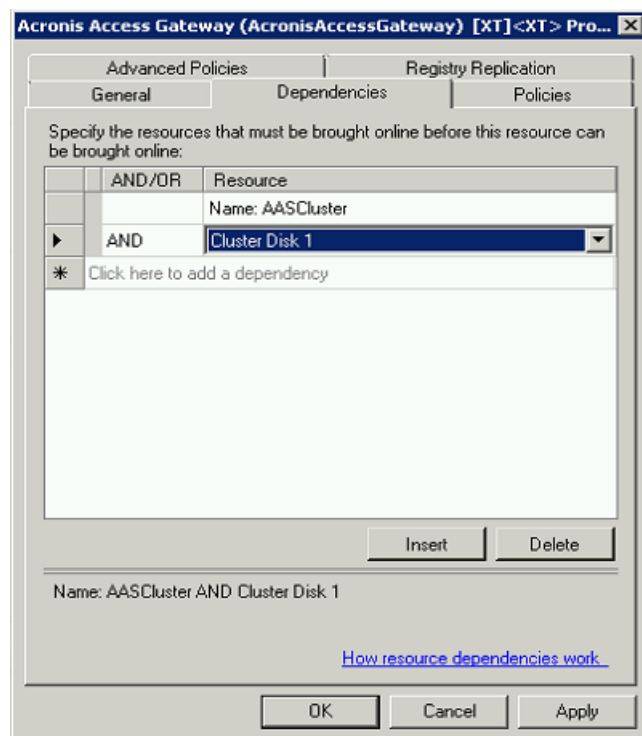
2. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL (For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)



For the Acronis Access Gateway Server service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.

3. Click on **Resource** and select the shared disk you have added and the **Network Name** (this is the name of the Client access point).

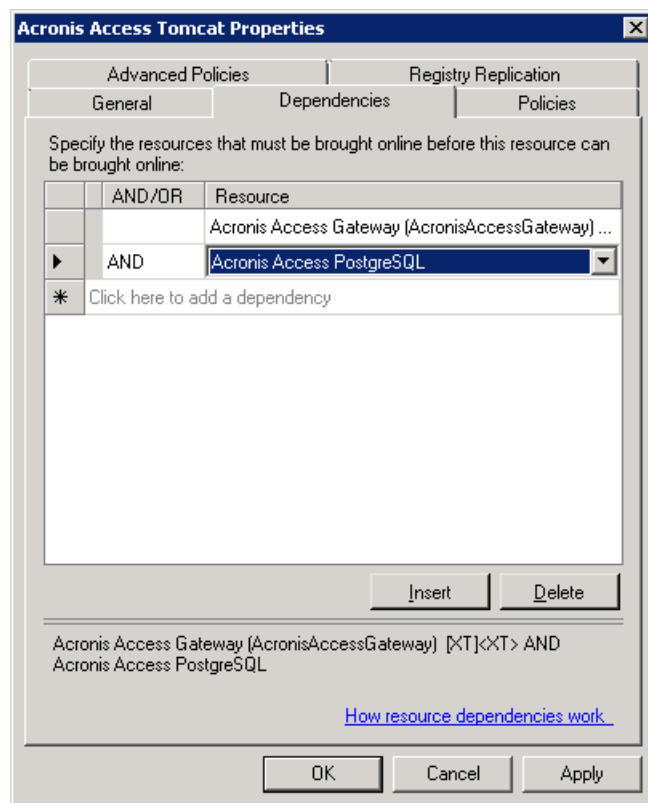


4. Press **Apply** and close the window.

For the Acronis Access Tomcat service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.

3. Click on **Resource** and select the PostgreSQL and Acronis Access Gateway Server services as dependencies. Press **Apply** and close the window.

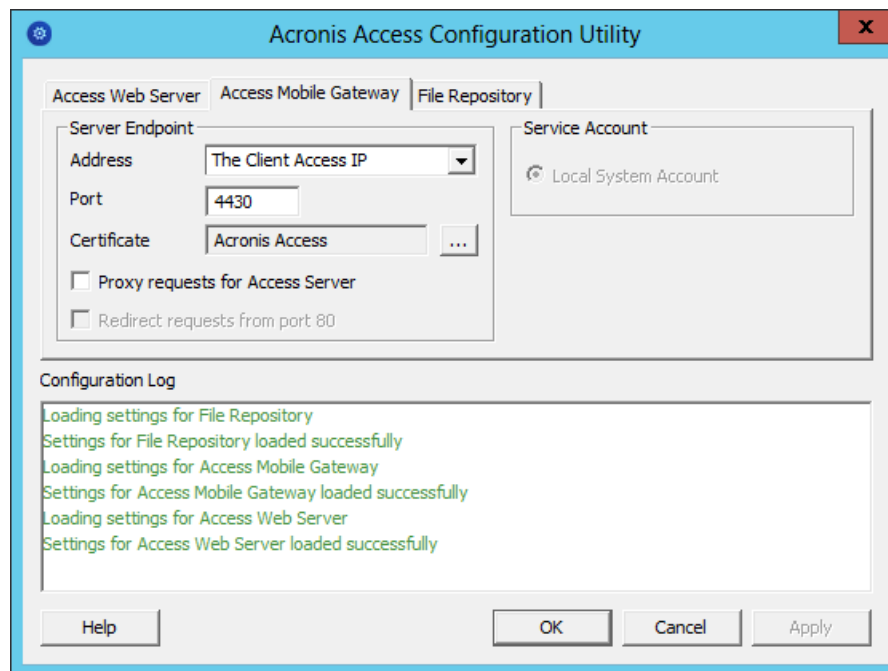


Note: If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access Service group and set it as a dependency for the network name.

Bringing the service group online and using the Configuration Utility

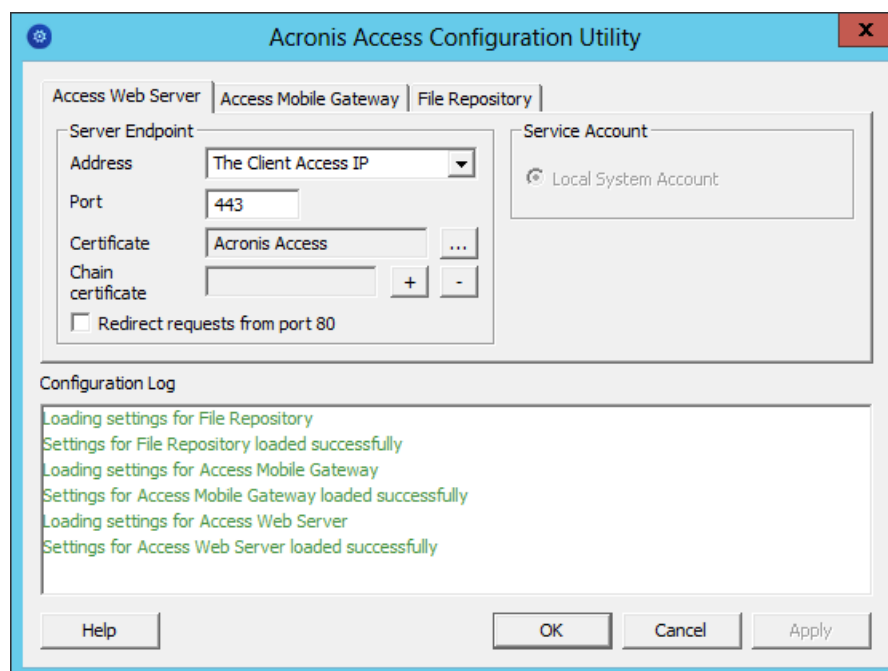
1. Right-click on the Acronis Access service group and press **Bring this application or service group online**.
2. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**

3. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

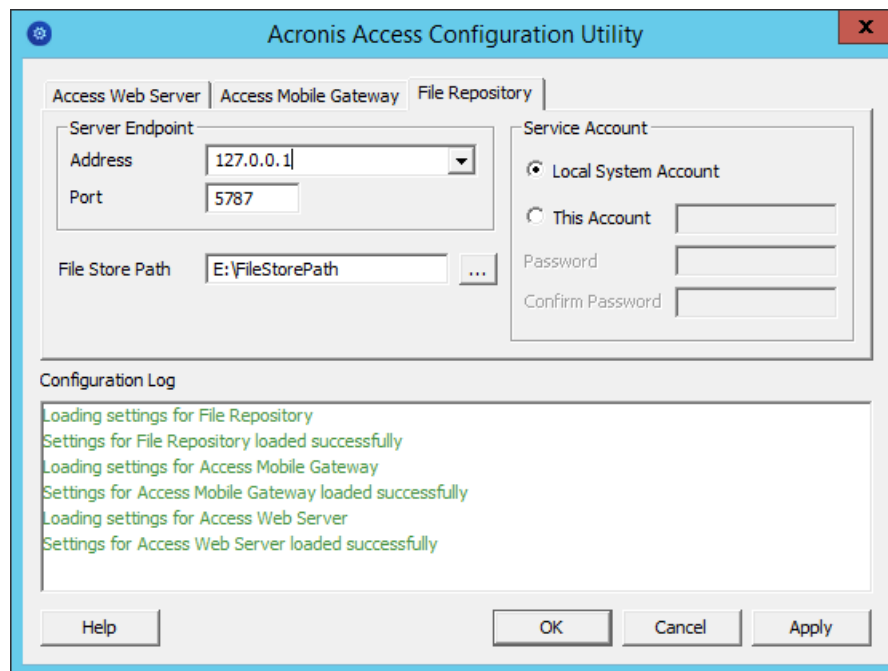


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



5. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

Installation and configuration on the second node

1. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
2. Install Acronis Access on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.
3. Complete the installation.
4. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\Acronis\Access\Gateway Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/access_cluster/database/'**).

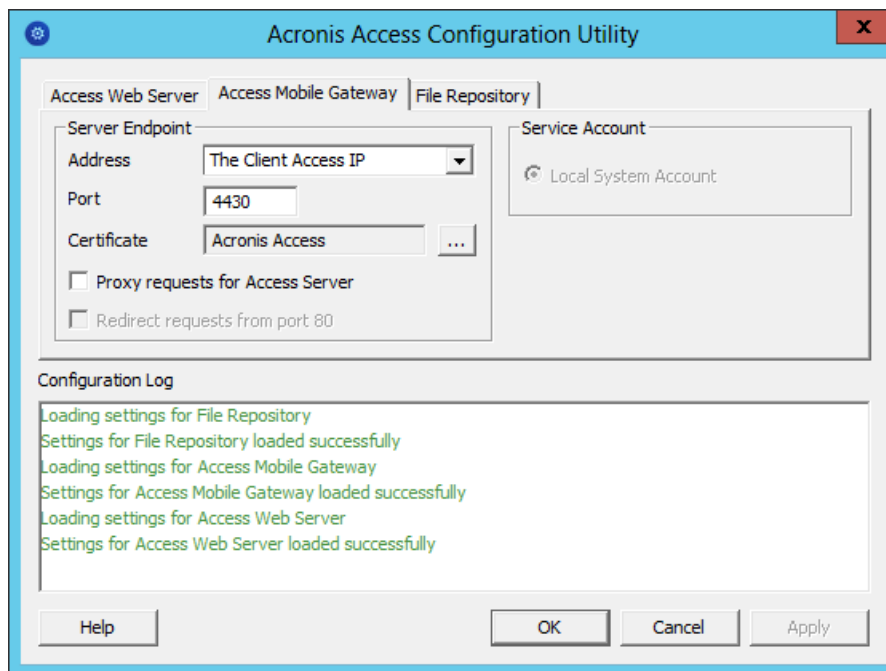
Note: Use slashes(/) as a path separator.

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

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

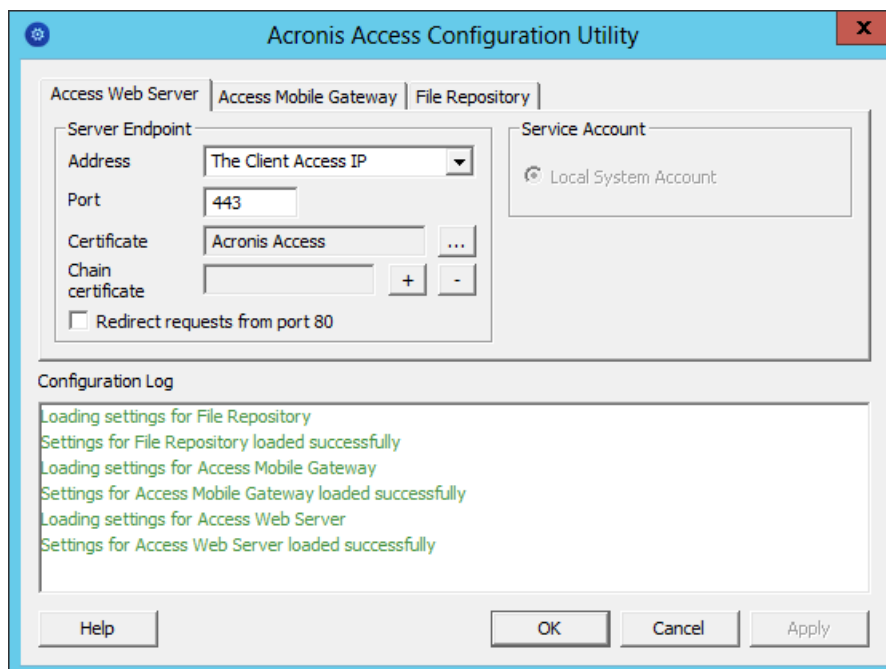
5. Move the Acronis Access service group to the second node. To do so, right-click on the service group and click on **Move to the second node**.
6. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**

7. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

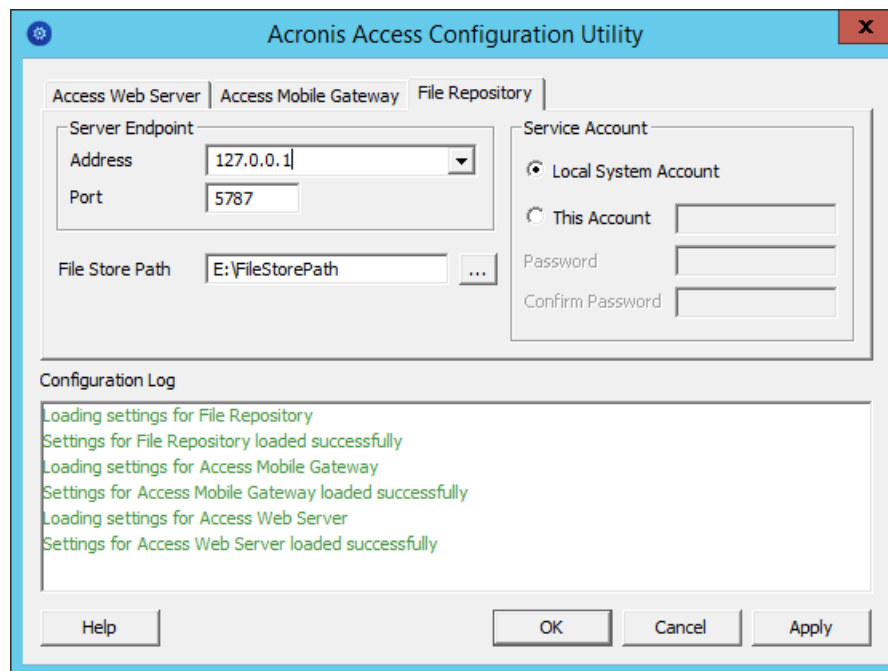


8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



- Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



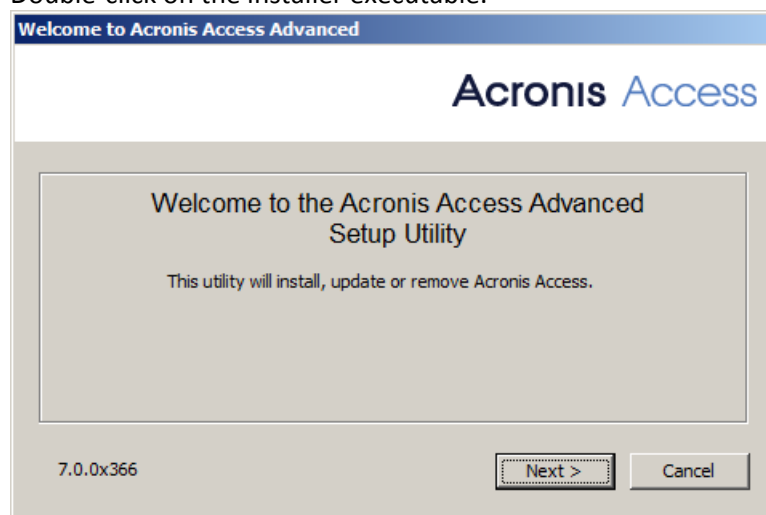
- Click **OK** to complete the configuration and restart the services.

2.3 Installing Acronis Access on a Windows 2012 (R2) Microsoft Failover Cluster

Installing Acronis Access

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

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

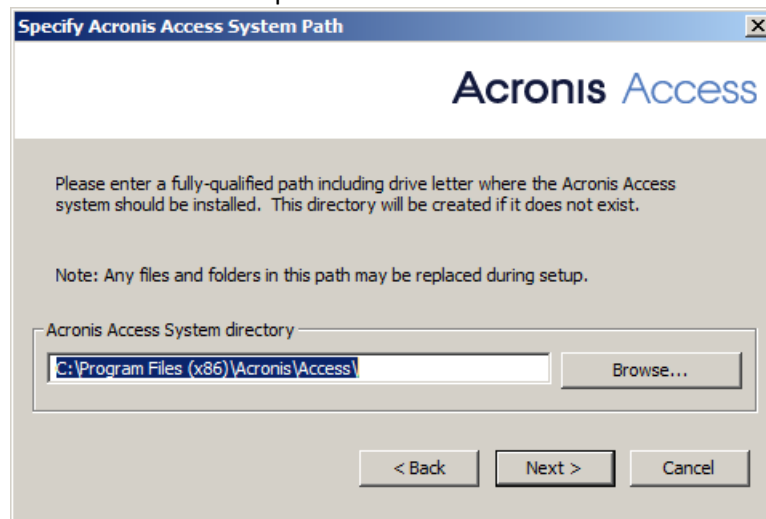


- Press **Next** to begin.
- Read and accept the license agreement.

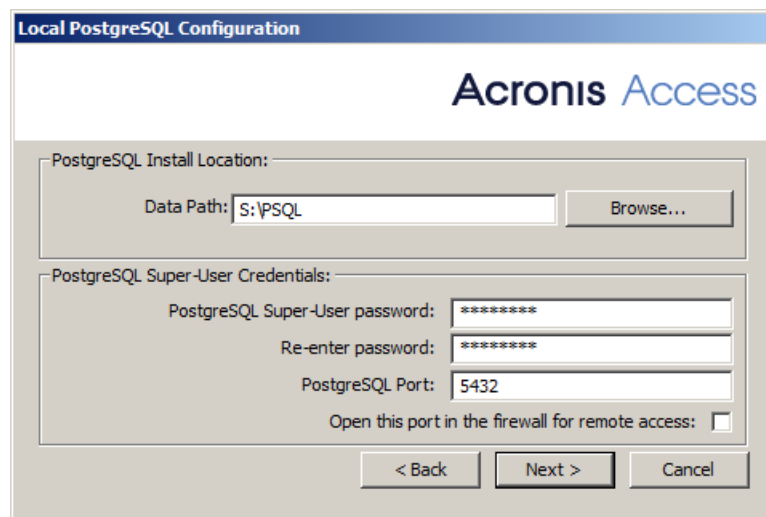
6. Press **Install**.

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 path or select a new one for the Acronis Access main folder 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. Choose a location on a shared disk for the **Postgres Data** folder and press **Next**.

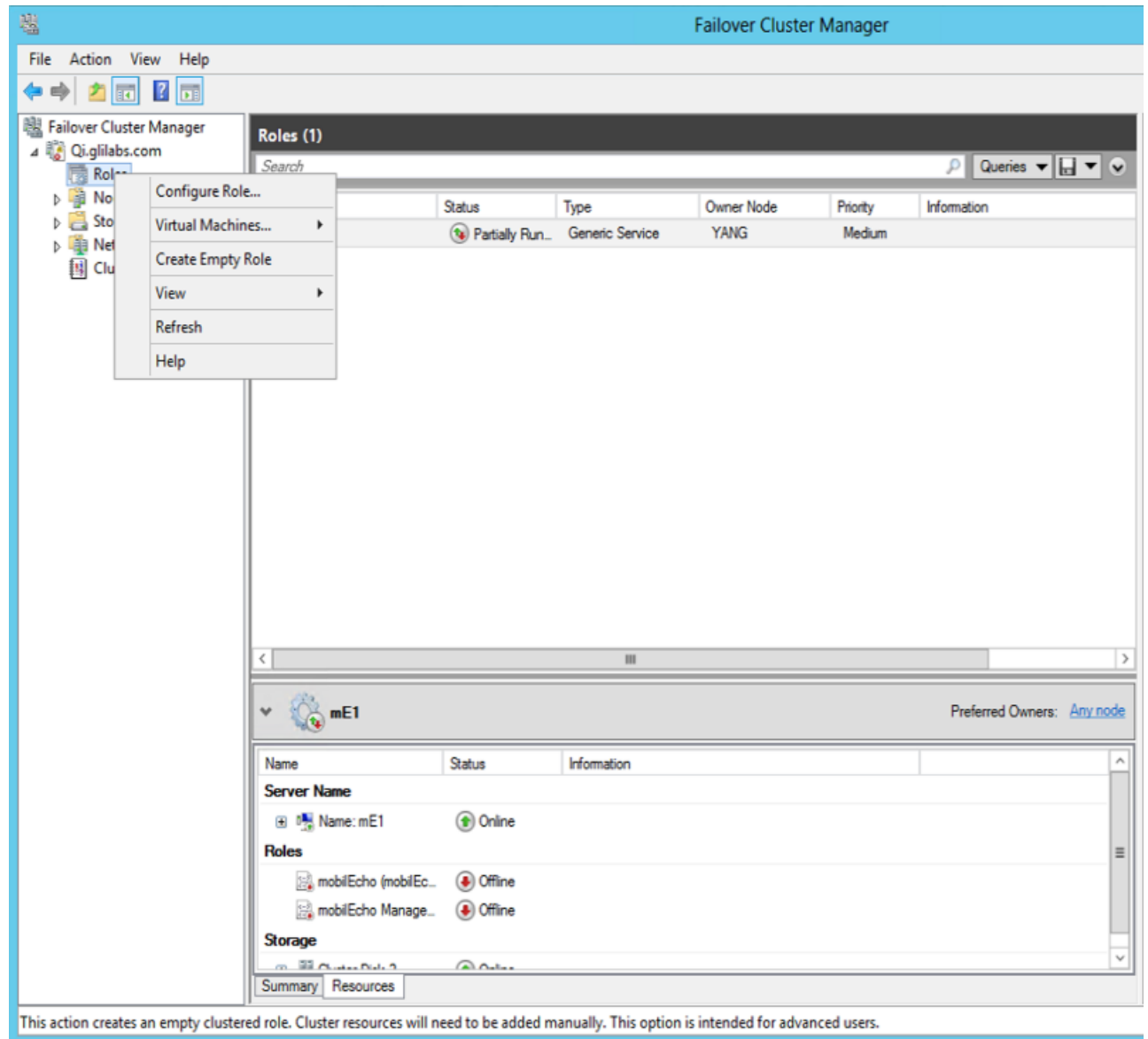


10. A window displaying all the components which will be installed appears. Press **OK** to continue.
- When the Acronis Access installer finishes, press **Exit**.

Creating the role

1. Open the **Failover Cluster Manager** and right-click on **Roles**.

2. Select **Create empty role**. Give the role a proper name. (e.g. Acronis Access, AAS Cluster)



Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\Acronis\Access\Gateway Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/access_cluster/database/'**).

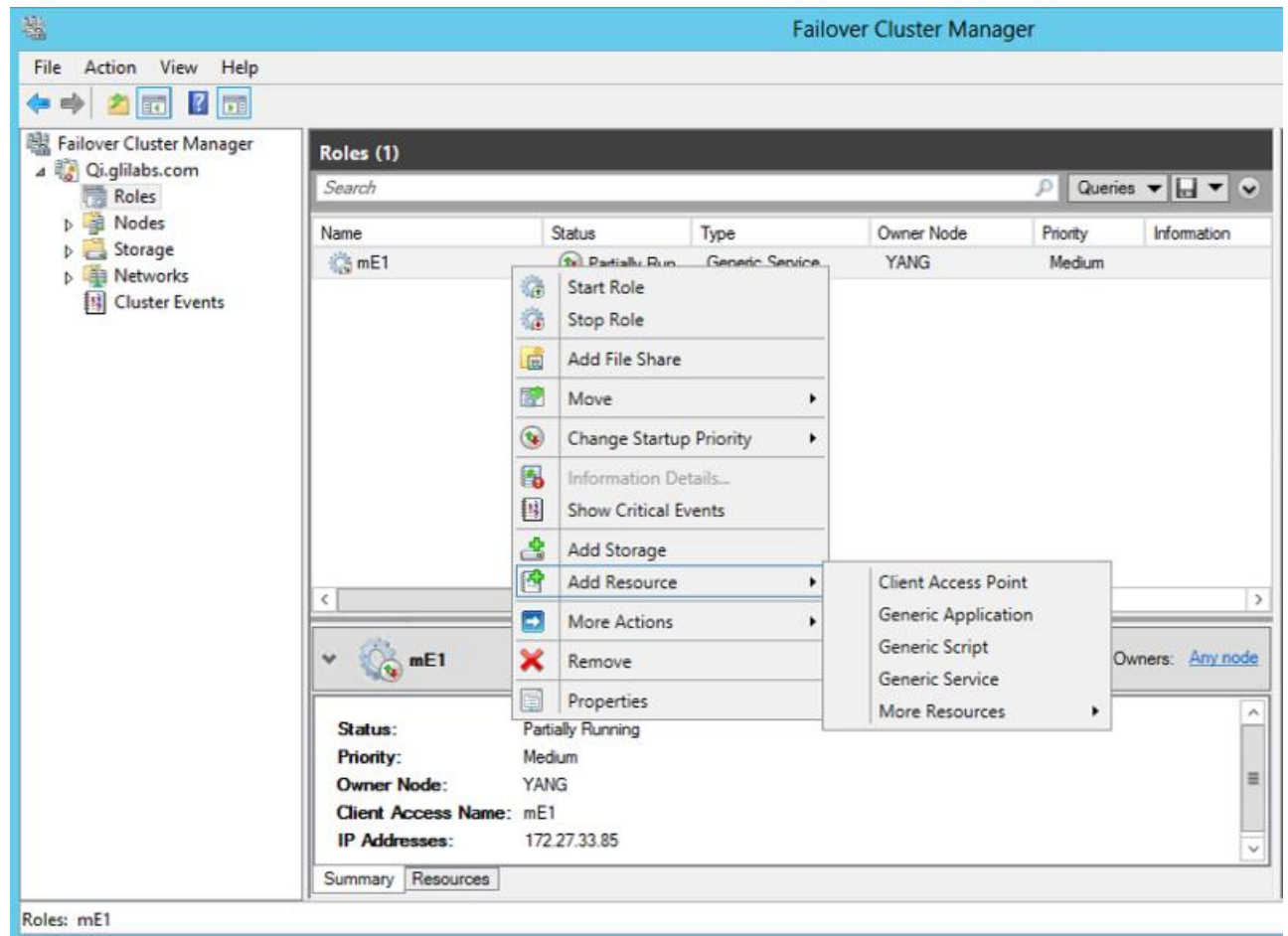
Note: Use slashes(/) as a path separator.

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

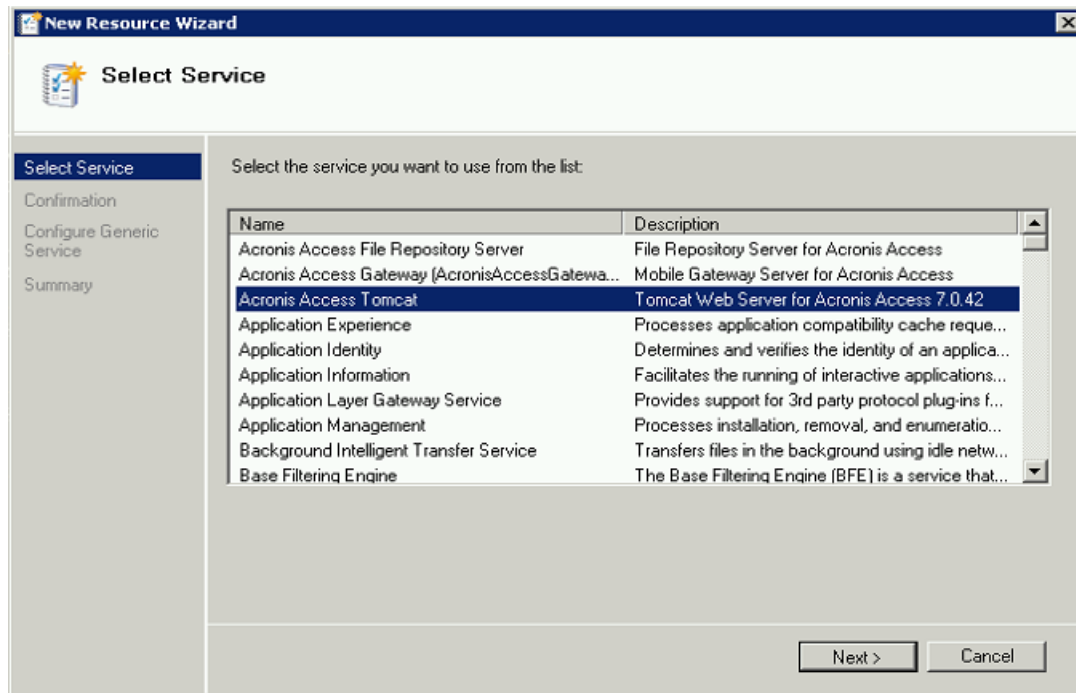
Adding all of the necessary services to the Acronis Access role

Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

1. Right-click on the Acronis Access role and select **Add a resource**.
2. Select **Generic Service**.



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

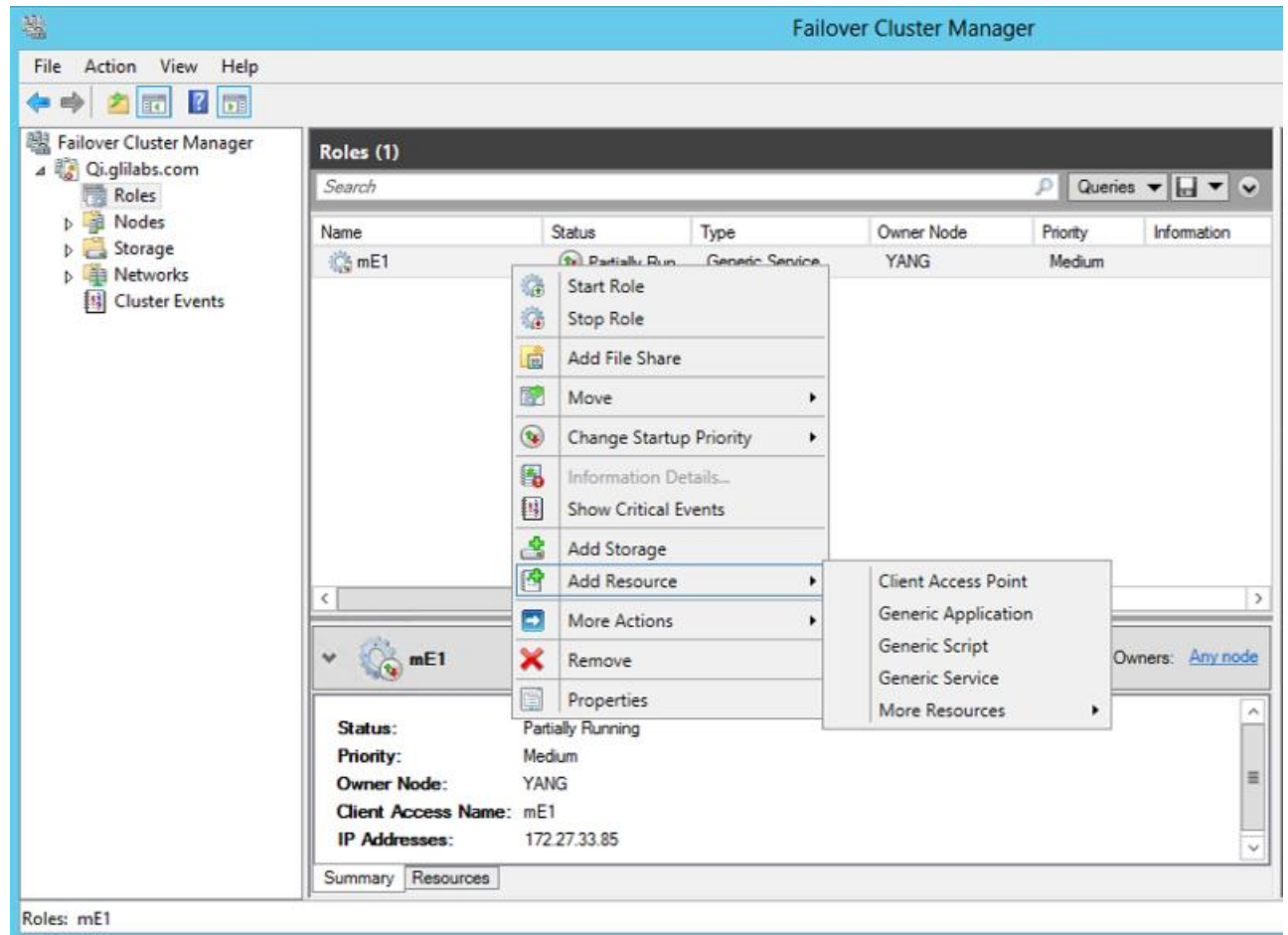


4. On the Confirmation window press **Next**.
5. On the summary window press **Finish**.

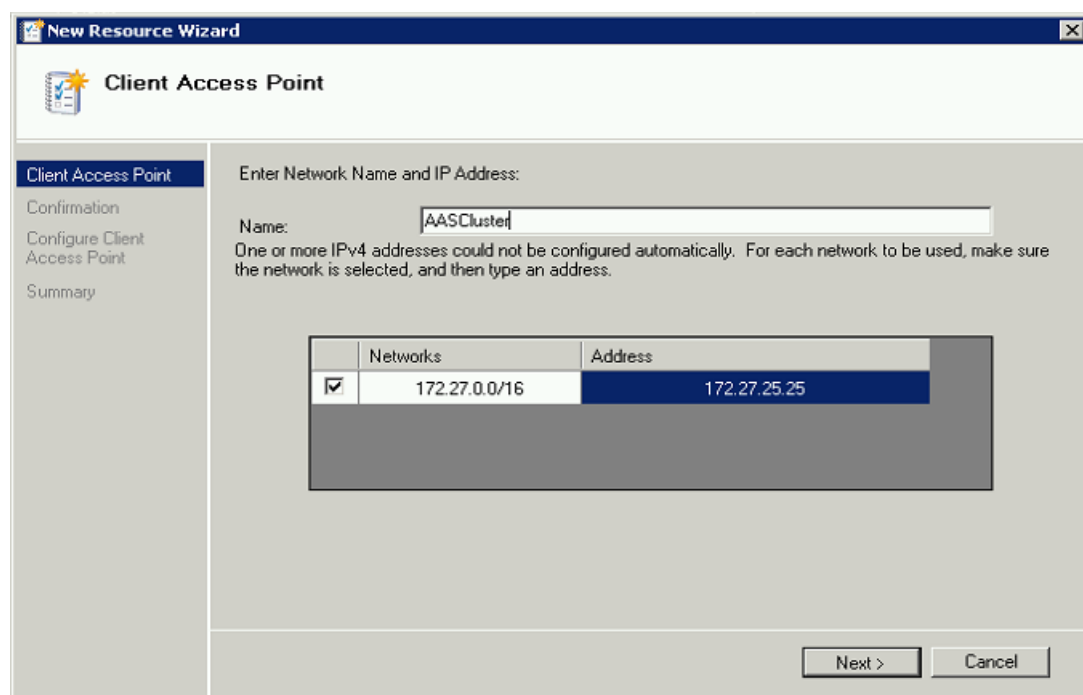
Setting an Access Point

1. Right-click on the Acronis Access role and select **Add a resource**.

2. Select **Client Access Point**.



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

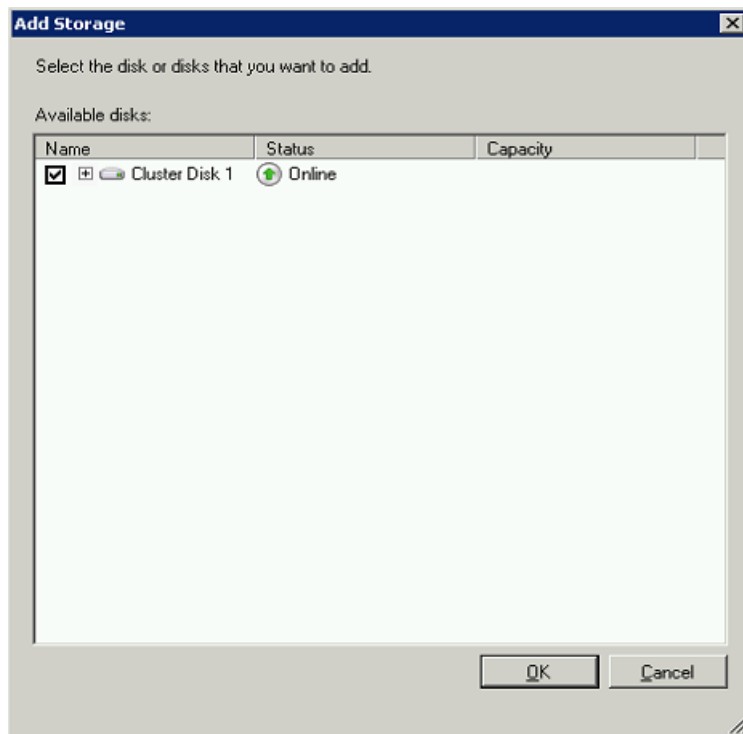


5. Enter the IP address and press **Next**.
6. On the Confirmation window press **Next**.

7. On the summary window press **Finish**.

Adding a shared disk

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



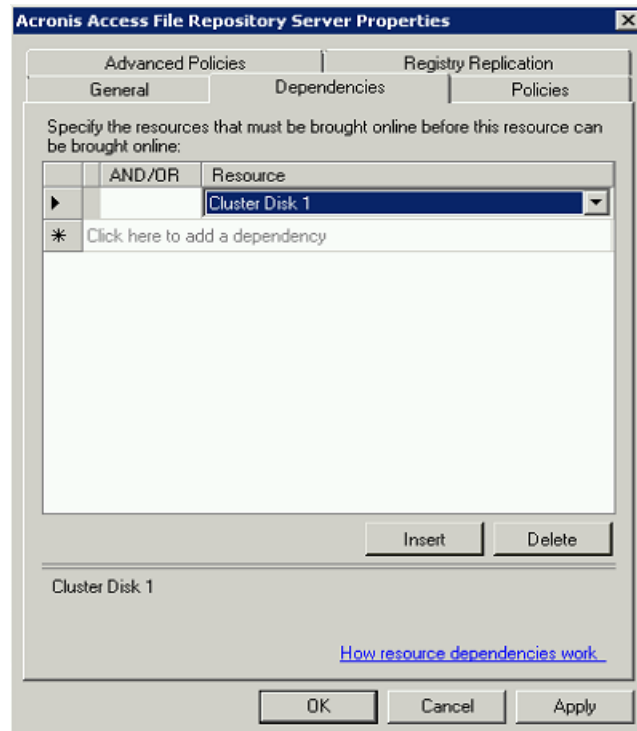
Configuring dependencies

1. Select the Acronis Access role and click on the **Resources** tab

For PostgreSQL and Acronis Access File Repository services do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.

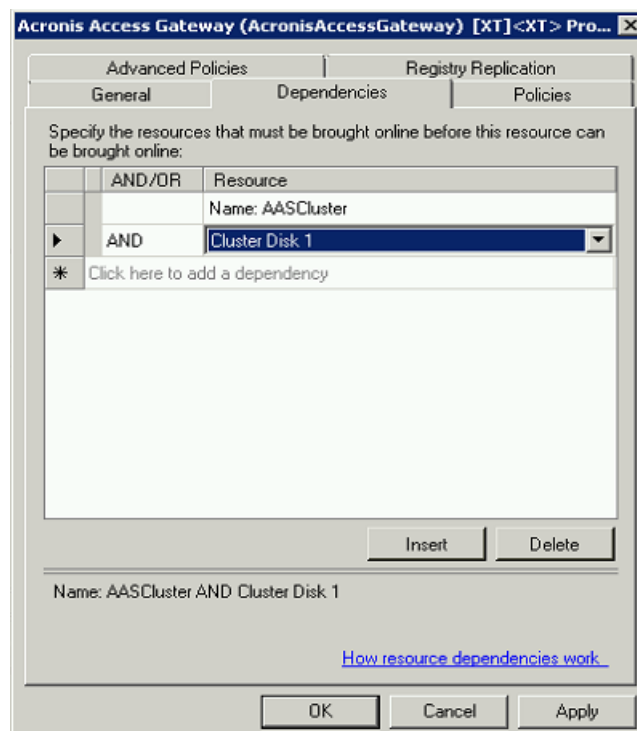
3. Click on **Resource** and select the shared disk you have added.



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

For the Acronis Access Gateway Server service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the shared disk you have added and the **Network Name** (this is the name of the Client access point).

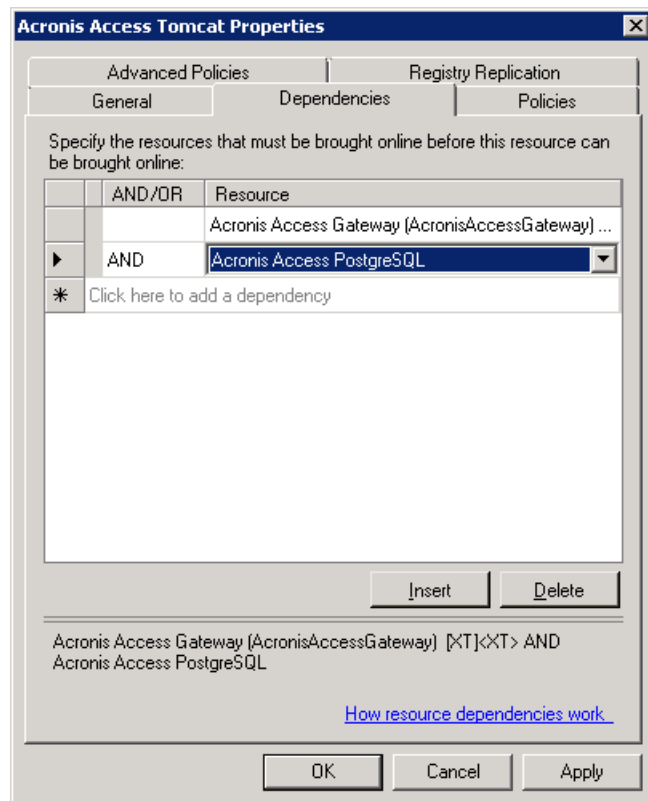


4. Press **Apply** and close the window.

For the Acronis Access Tomcat service do the following:

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

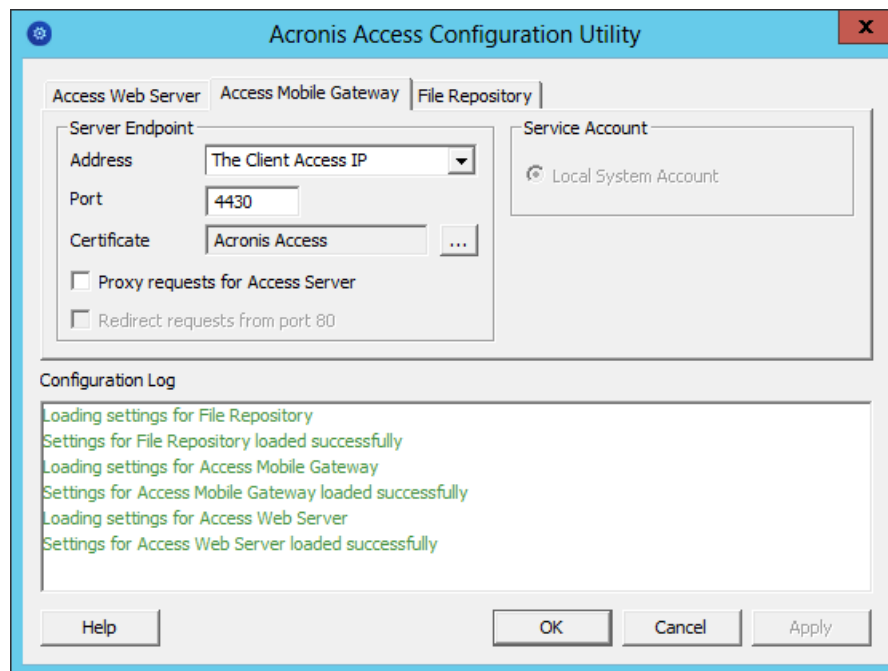
Note: If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access role and set it as a dependency for the network name.



Starting the role and using the Configuration Utility

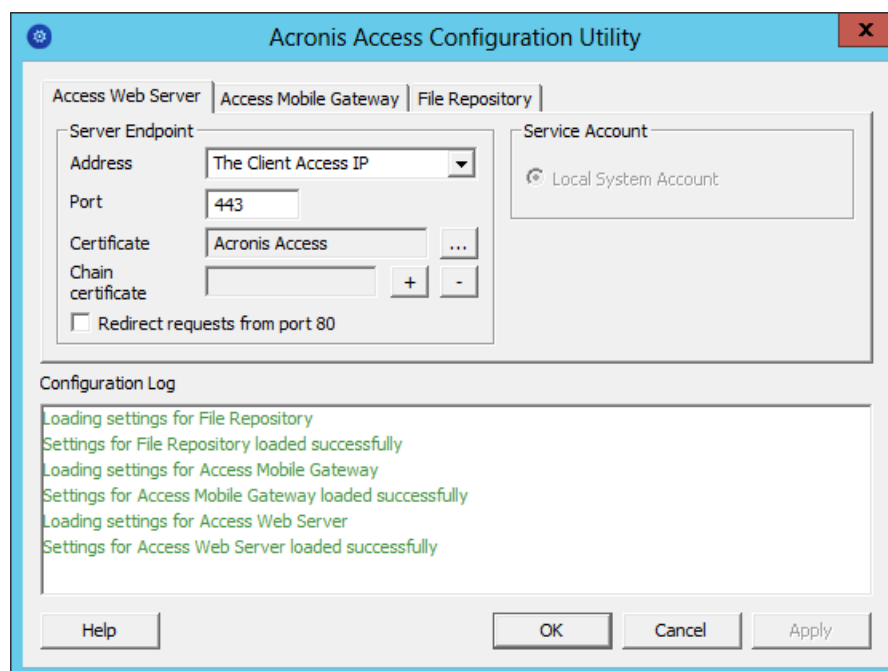
1. Right-click on the Acronis Access role and press **Start role**.
2. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**

3. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

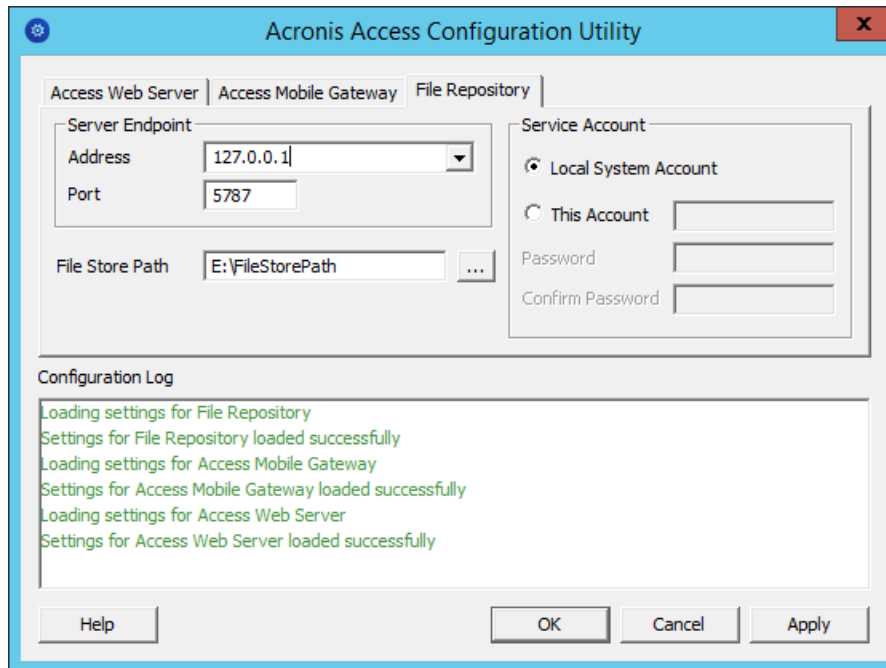


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



- Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

Installation and configuration on the second node

- Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
- Install Acronis Access on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.
- Complete the installation.
- Configure your Gateway Server's database to be on a location on a shared disk.
 - Navigate to **C:\Program Files (x86)\Acronis\Access\Gateway Server**
 - Find the **database.yml** file and open it with a text editor.
 - Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/access_cluster/database/'**).

Note: Use slashes(/) as a path separator.

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

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

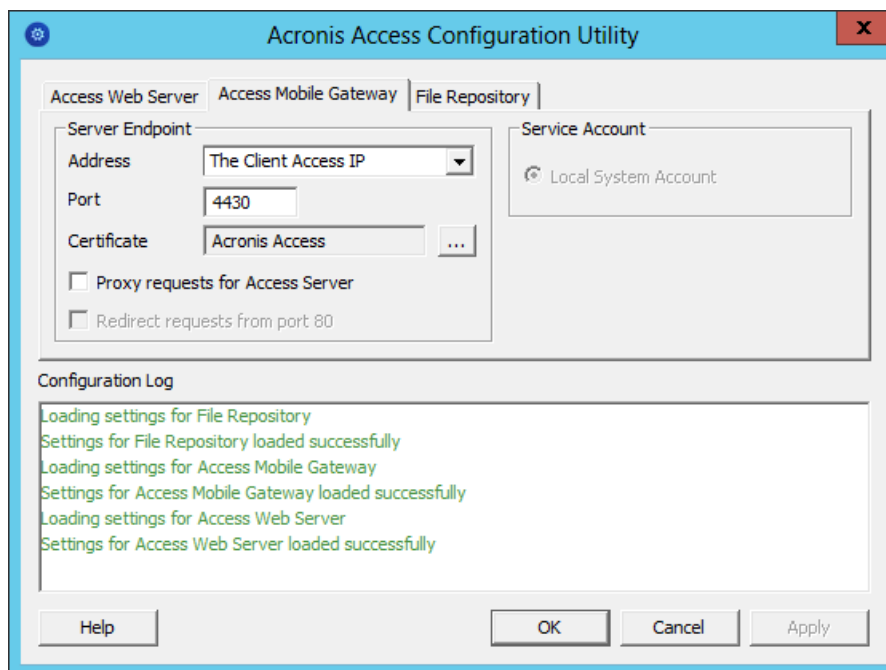
For PostgreSQL do the following:

- Open the **Failover Cluster Manager**.
- Find and select the PostgreSQL Generic Service resource.
- Right-click on it and select **Properties**.
- Click on the **Registry Replication** tab.

5. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL (For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)
6. Move the Acronis Access role to the second node.

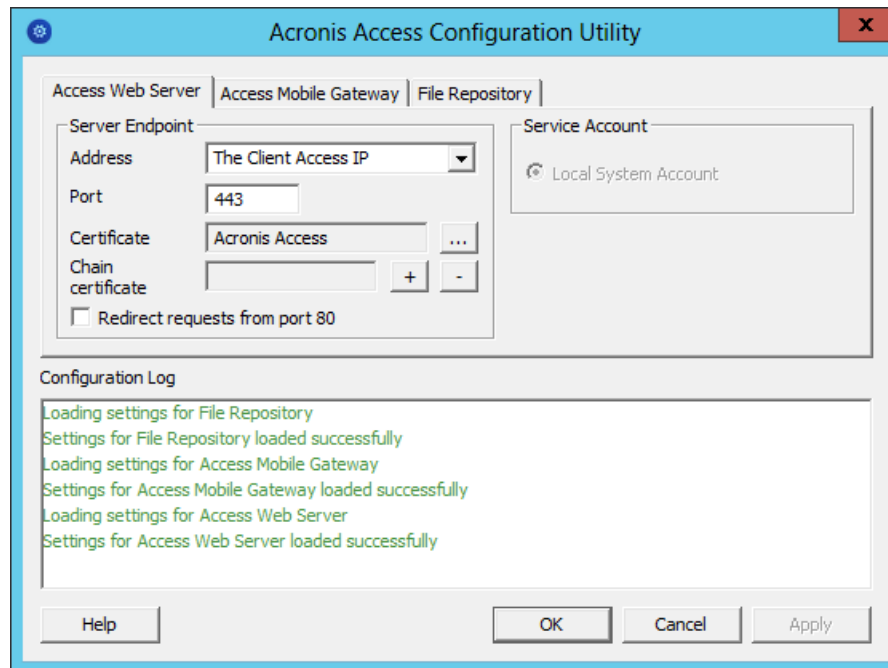
Using the Configuration Utility on the second node

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

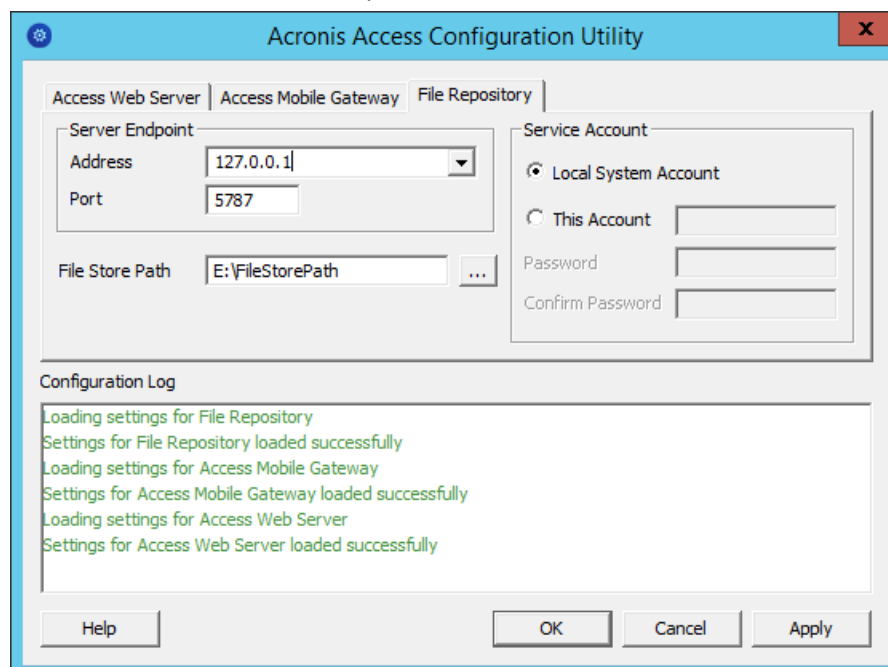


3. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



4. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

3 Upgrading

In this section

Upgrading from Acronis Access to a newer version	58
Upgrading to Acronis Access Advanced	60
Upgrading from mobilEcho 4.5 or earlier	61
Upgrading from activEcho 2.7 or earlier	106
Upgrading Gateway Clusters	132
Upgrading Load-balanced configurations	134

3.1 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 vital components:

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**.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

The PostgreSQL database

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

1. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
e.g. **cd "C:\PostgreSQL\9.2\bin"**
2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

```
D:\Backups\mybackup.sql
```

Note: *acronisaccess_production must be entered exactly as shown as it is the name of the Acronis Access database*

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access installation process.

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

4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

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

pg_dumpall -U postgres > alldbs.sql

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

For full syntax on this command see: <http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html>
<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

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

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

1. Navigate to the Acronis Access installation folder containing the configuration file.

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

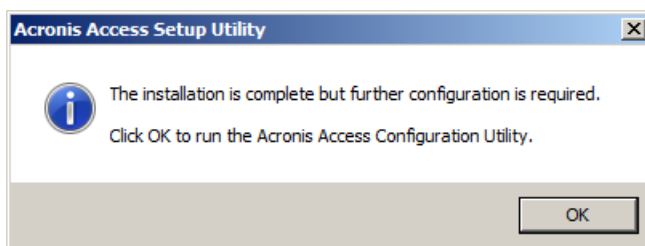
2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

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.

3.2 Upgrading to Acronis Access Advanced

In order to upgrade your Acronis Access Server to the Advanced version, all you need is a Acronis Access Advanced license key.

To do so:

1. Open the Acronis Access Web interface as an administrator.

2. Open the **General Settings** tab and click on **Licensing**.
3. Add your license.

Adding a new license

1. Copy your license key.
2. Paste it in the **Add license key** field.
3. Read and accept the licensing agreement by selecting the checkbox.
4. Press **Add License**.

3.3 Upgrading from mobilEcho 4.5 or earlier

In this section

Before You Begin.....	61
The Upgrade Process	67
Downgrading to mobilEcho 4.5.....	105

3.3.1 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.grouplogix.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 \(p. 17\)](#) article.

For instructions on upgrading a mobilEcho cluster to a Acronis Access cluster, visit the [Upgrading Acronis Access on a cluster \(p. 138\)](#) article.

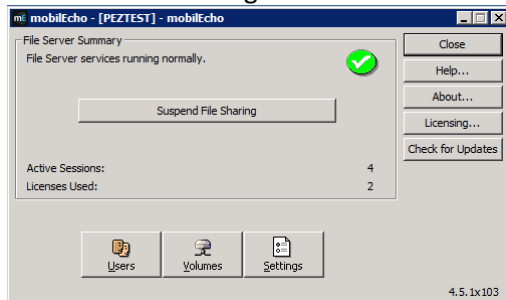
Architectural and Terminology Changes

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.

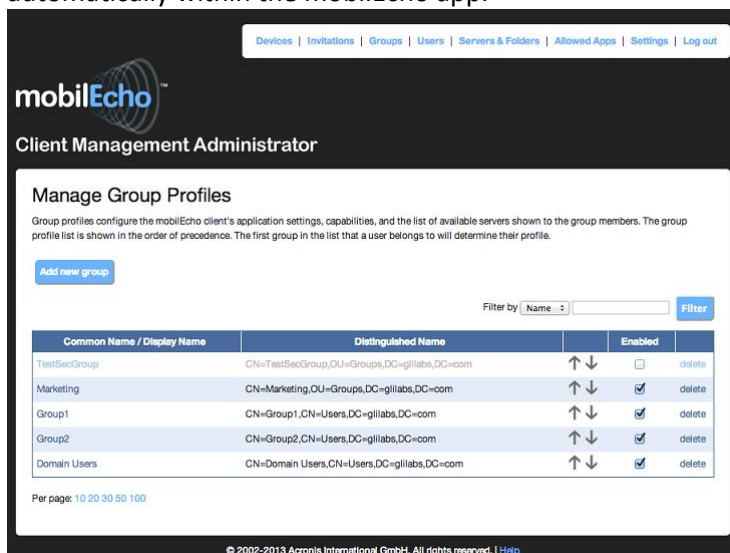
mobilEcho 4.5 and earlier included two management consoles:

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

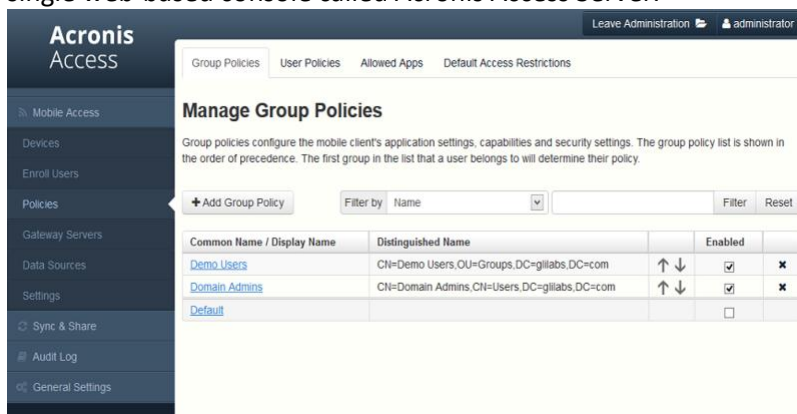
Access Server settings.



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

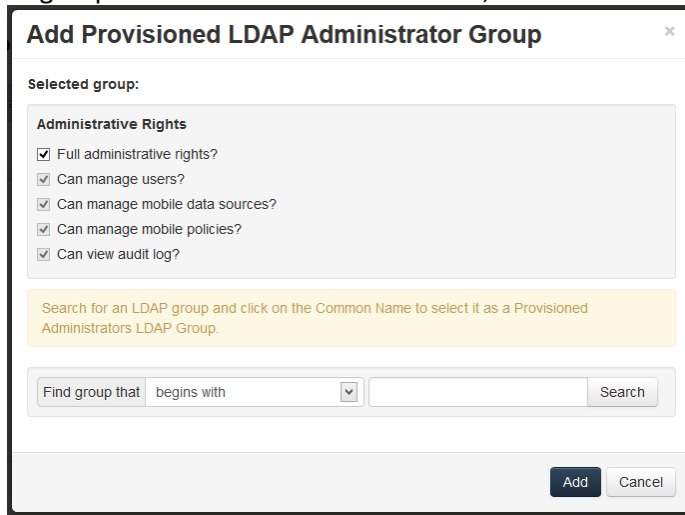
Existing settings

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

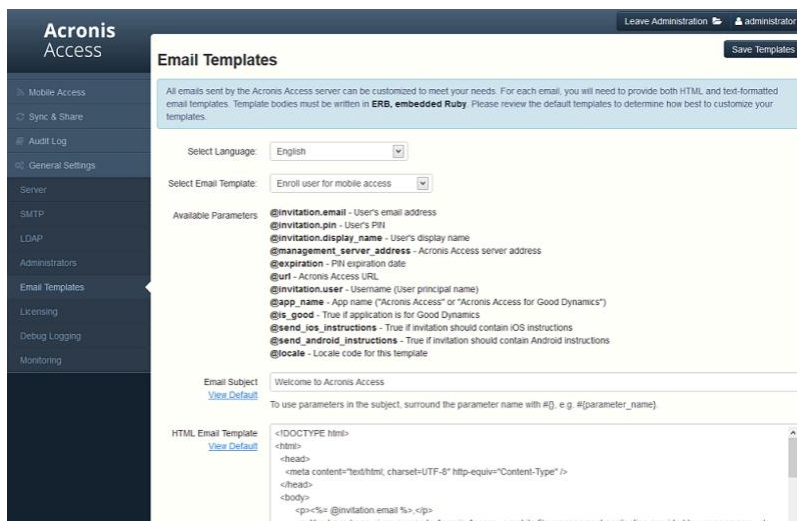
or groups. To add or edit administrators, visit the Administrators page on the General Settings menu.



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 source
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.
6. 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:

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 begins with

This folder is assigned to:

Common Name	Distinguished Name
Domain Admins	
Demo Users	

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	<input checked="" type="checkbox"/>
Main Server	192.168.1.140:443	Demo Users	<input checked="" type="checkbox"/>

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.

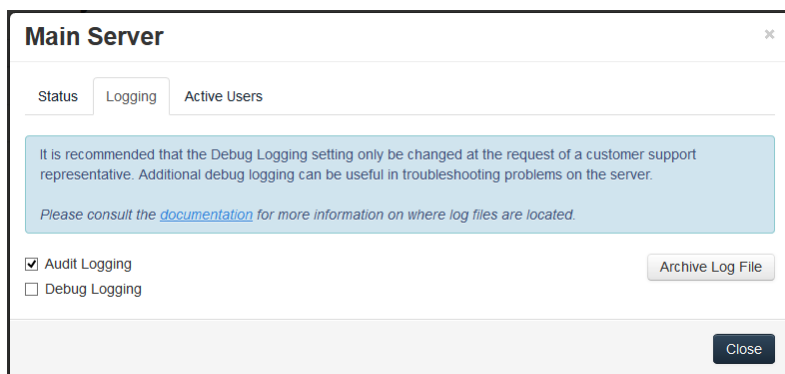
To get started you will be asked for LDAP settings to allow Acronis Access Server to enumerate your Active Directory users and groups and for SMTP settings so that enrollment email invitations can be sent to your users.

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.



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

3.3.2 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 \(p. 17\)](#) article.

For instructions on upgrading a mobilEcho cluster to a Acronis Access cluster, visit the [Upgrading Acronis Access on a cluster \(p. 138\)](#) article.

In this section

Upgrading a single mobilEcho server without Client Management configured	69
Upgrading a single mobilEcho server with Client Management enabled	83
Upgrading multiple mobilEcho servers with Client Management.....	100
Upgrading a single mobilEcho server with Client Management enabled and an activEcho server	105

3.3.2.1 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.

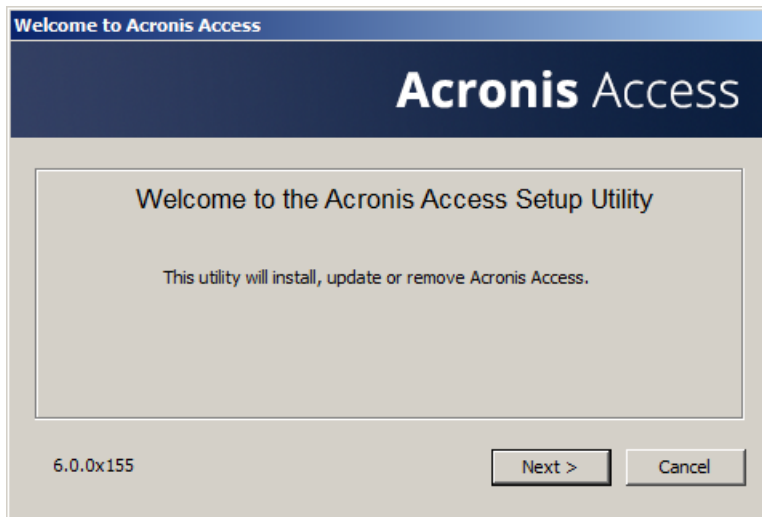
When upgrading to Acronis Access, your mobilEcho File Access Server is upgraded to an Acronis Access Gateway Server. This service will continue to accept connections from mobilEcho clients and to act as the gateway to any file server, NAS or SharePoint data sources your users are accessing.

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.

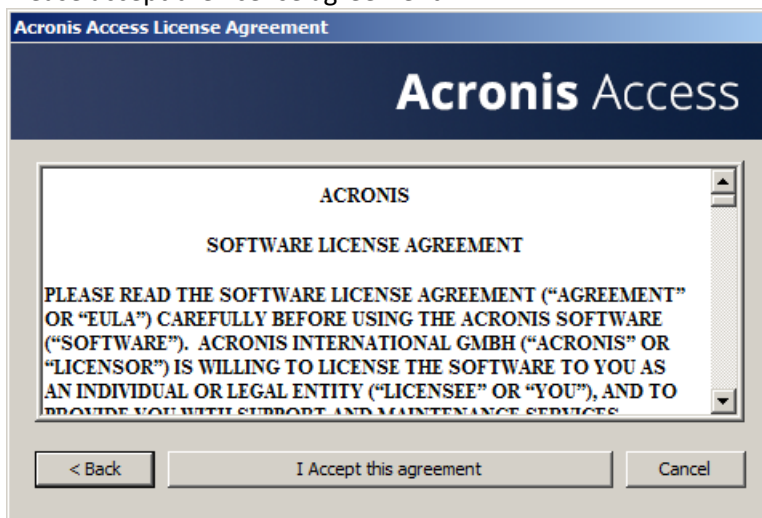
To perform an upgrade to Acronis Access:

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://www.grouplogic.com/web/aalatest>
 - b. You will need to enter your product serial number for verification before downloading the installer.

- c. The installer file is named: AcronisAccessAdvancedSetup.exe
4. Click **Next** on the Welcome Screen.

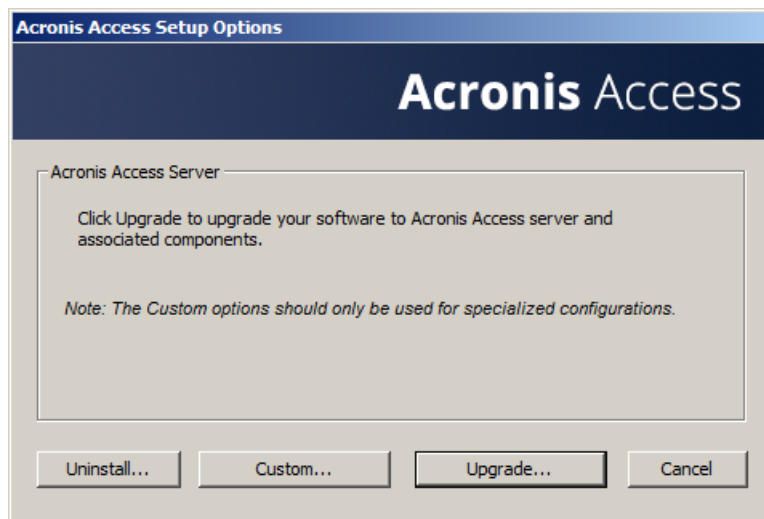


5. Please accept the license agreement.

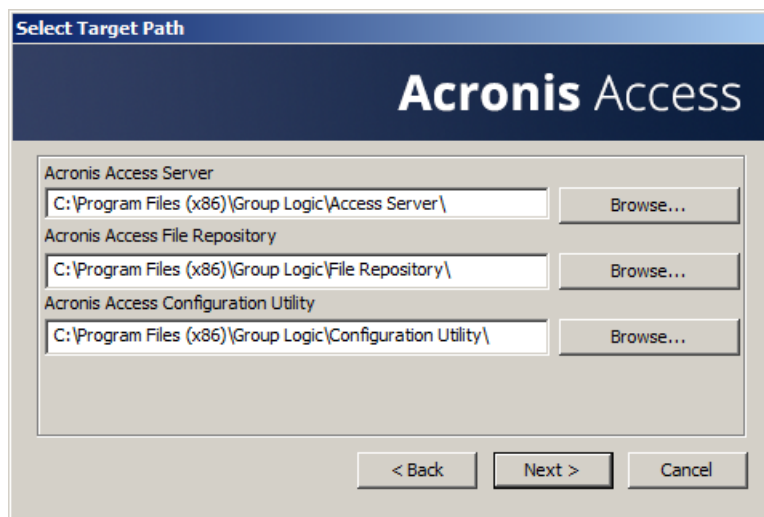


6. Click the **Upgrade** option to automatically upgrade your mobilEcho File Access Server service to an Acronis Access Gateway Server. In the upgrade process, the Acronis Access Server and its required services will also be installed.

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.

The dialog box is titled "PostgreSQL Configuration" and "Acronis Access". It contains two main sections. The first section, "PostgreSQL Install Location:", has two rows: "Base Path:" with a text field containing "C:\PostgreSQL\9.2\" and a "Browse..." button, and "Data Path:" with a text field containing "C:\PostgreSQL\9.2\Data\" and a "Browse..." button. The second section, "PostgreSQL Super-User Credentials: (will be created if necessary)", has three rows: "PostgreSQL Super-User password:" with a masked text field (asterisks), "Re-enter password:" with another masked text field, and "PostgreSQL Port:" with a text field containing "5432". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

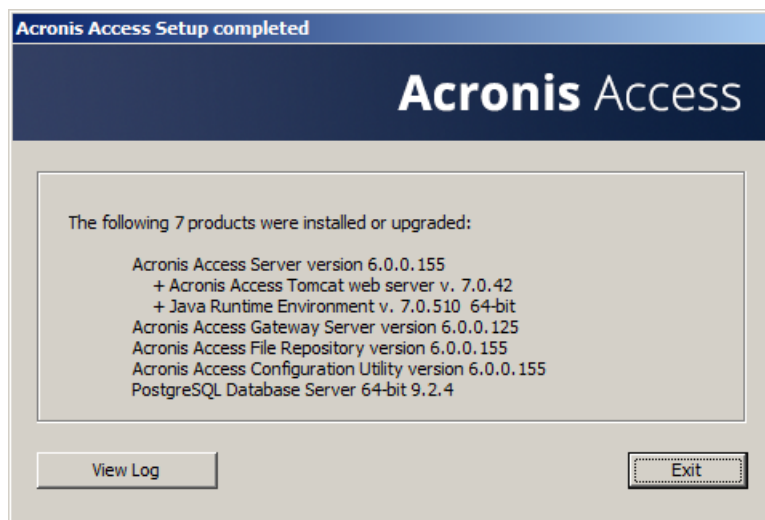
9. Please review the services being installed and upgraded. Then click **Install** to begin the upgrade.

The dialog box is titled "Acronis Access Install Warning" and "Acronis Access". It contains a warning message: "Setup will now install or upgrade the following products. This process may disrupt users of this system by starting and stopping the Acronis Access services." Below this is a list of products and versions: "Acronis Access Server v. 6.0.0.155", "+ Acronis Access Tomcat web server v. 7.0.42", "+ Java Runtime Environment v. 7.0.510", "Acronis Access Gateway Server v. 4.5.2.103 --> v. 6.0.0.125", "Acronis Access File Repository v. 6.0.0.155", "Acronis Access Configuration Utility v. 6.0.0.155", and "PostgreSQL Database Server v. 9.2.4". At the bottom are three buttons: "< Back", "Install", and "Cancel".

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.

The dialog box is titled "Acronis Access Component Installation" and "Acronis Access". It contains the text "Installing Acronis Access Server..." and "Waiting for product installation to complete - this could take several minutes...". Below this is a progress bar with a small blue segment on the left.

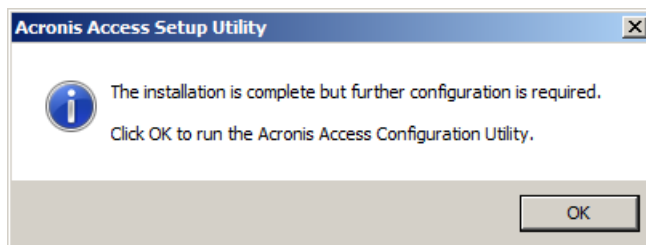
10. Once installation has completed, a summary of the components installed is shown. Click **Exit** to continue.



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.



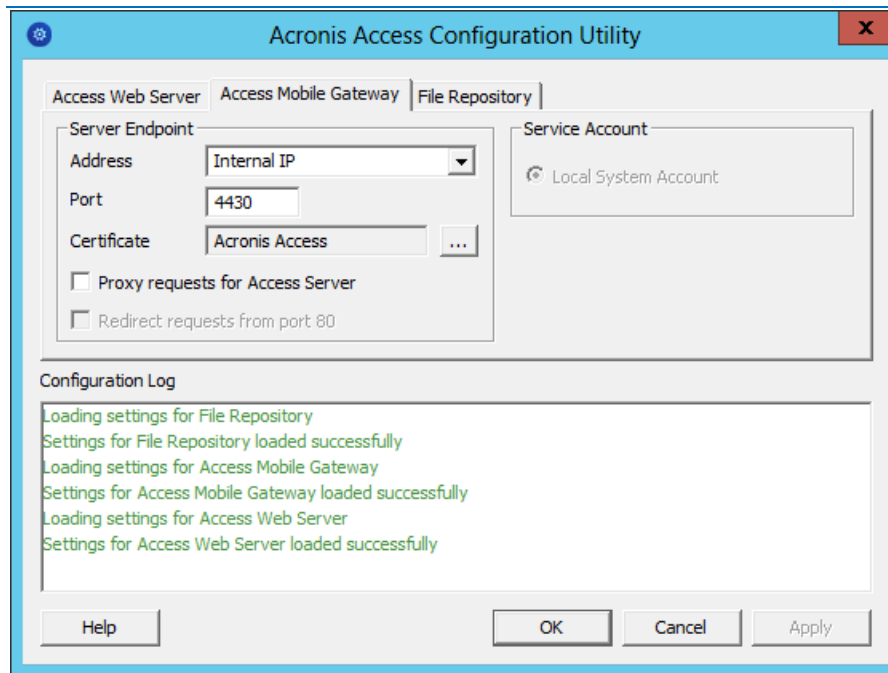
If you accidentally skip this step or need to change your network interfaces, ports, or certificates in the future. You can manually run the configuration utility at any time.

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

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

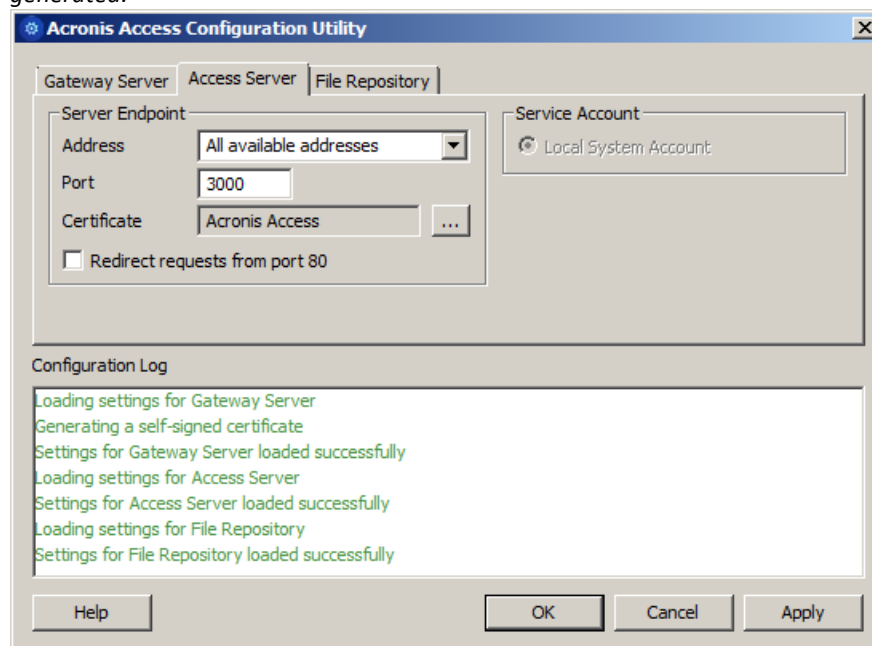
12. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core mobilEcho service that your mobilEcho clients connect to and that gives access to your file servers,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

Note: 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 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.



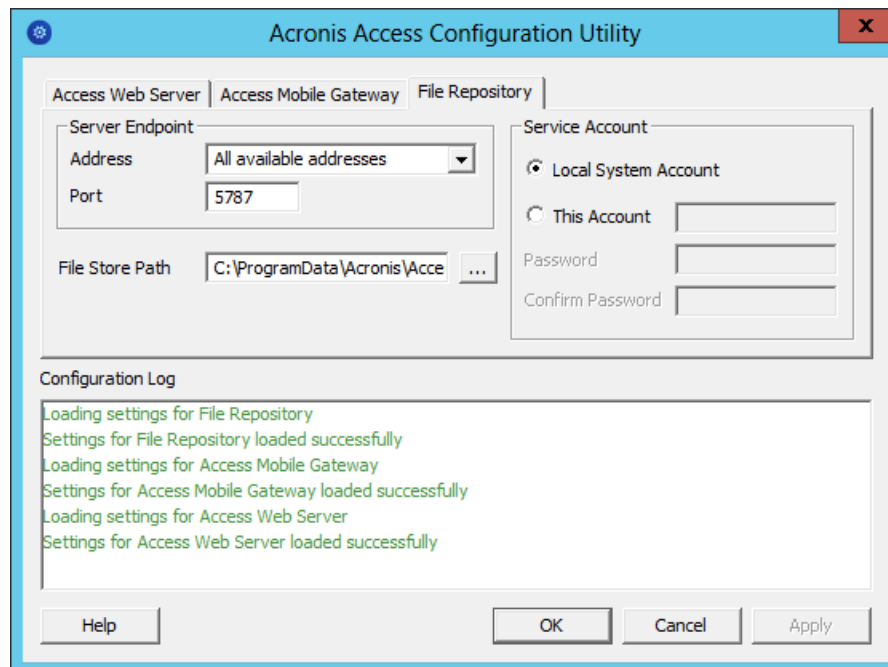
14. Acronis Access Server requires that a File Repository location be selected. If you are using mobilEcho only, this File Repository will not be used to store anything, but setting a location is still required.

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 choose to enable them at a later time, if desired.

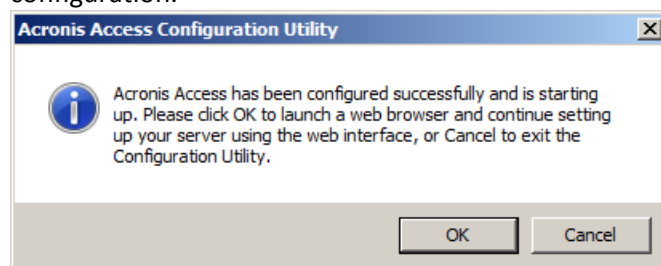
The default location for the File Repository is:

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.



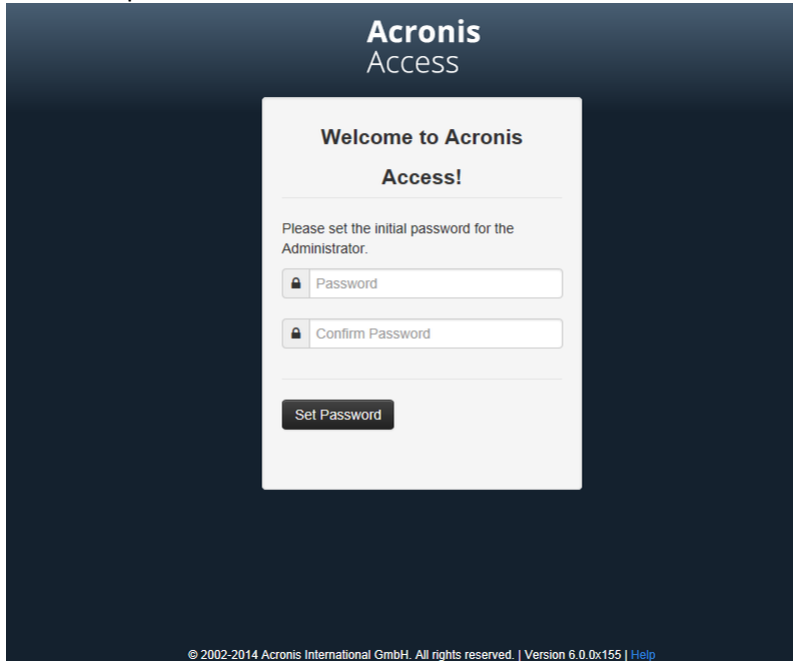
Required initial configuration of Acronis Access:

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

Acronis Access administrator

SMTP

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

SMTP Server Address:

SMTP Server Port:

Use secure connection? ☒

From Name:

From Email Address:

Use SMTP authentication? ☐

- 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:

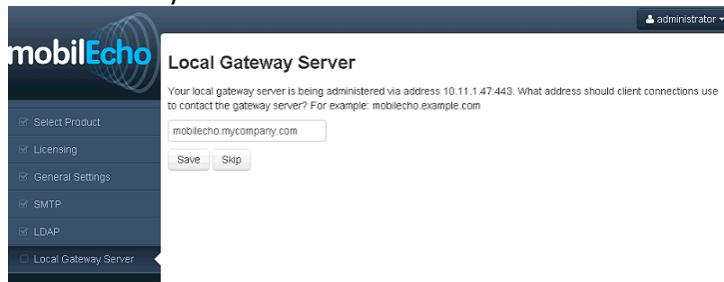
LDAP Search Base:

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. Local Gateway Server – Client connection address



- 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.
- 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.

- Click **Finish** Configuration to continue.

Upgrading Acronis Access 6.0 to 7.x or newer:

Once you have confirmed that the upgrade is successful, you can continue the upgrade to the latest version by following the steps below. The upgrade procedure from a previous version of Acronis Access is a simplified process and requires almost no configuration.

Backup the vital components:

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**.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

The PostgreSQL database

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

- Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
e.g. **cd "C:\PostgreSQL\9.2\bin"**
- Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

D:\Backups\mybackup.sql

Note: *acronisaccess_production* must be entered exactly as shown as it is the name of the Acronis Access database

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access installation process.

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

4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

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

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

Where **alldbs.sql** will be the generated backup file. It can include a full path specification, for instance

D:\Backups\alldbs.sql

For full syntax on this command see: <http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html>
<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

Info: *For more information on PostgreSQL backup procedures and command syntax please read this:*

<http://www.postgresql.org/docs/9.2/static/backup.html>

<http://www.postgresql.org/docs/9.1/static/backup.html>

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

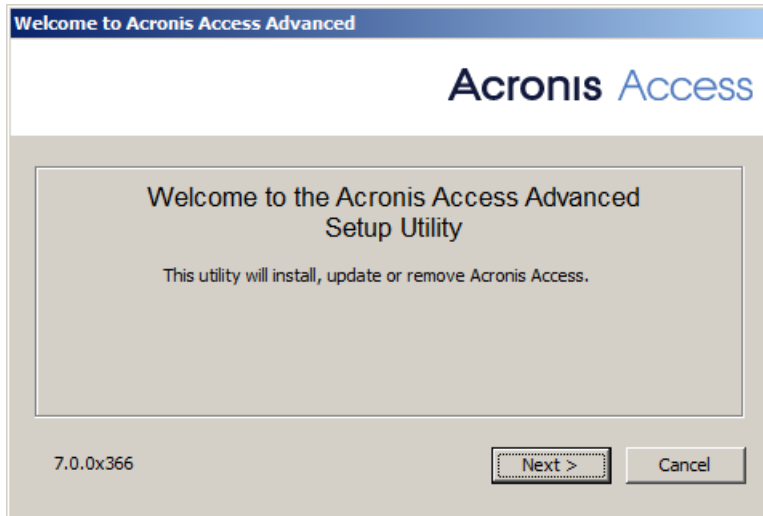
1. Navigate to the Acronis Access installation folder containing the configuration file.

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

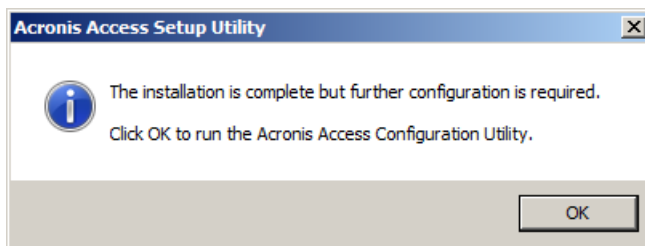
2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

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**.



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.

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.

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	TG, Demo Users	
Main Server	rt.gillabs.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.gillabs.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: test folder

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

Local (192.168.1.141)

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:\testfolder

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

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	
Folder	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.gillabs.com:2229	None	

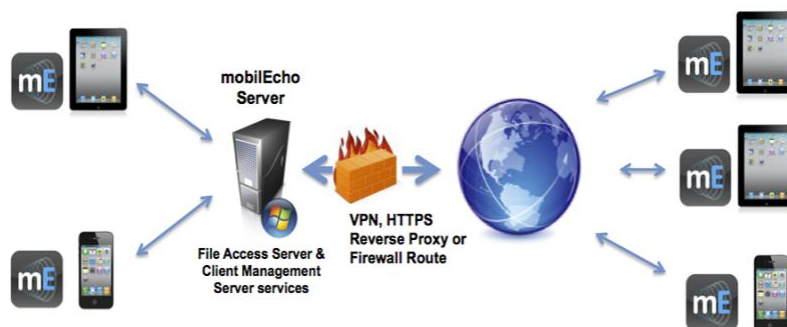
You can also begin to create and use client policies and officially enroll users with your server so that they are managed by these policies. A Default policy that applies to all users can be enabled and configured, or you can add custom policies based on Active Directory users and groups.

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.

3.3.2.2 Upgrading a single mobilEcho server with Client Management enabled

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

File Access Server & Client Management Server



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.

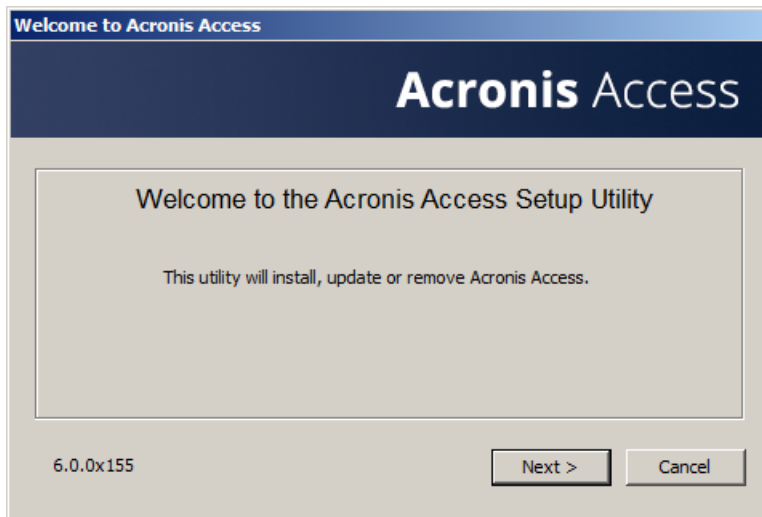
When upgrading to Acronis Access, your mobilEcho File Access Server is upgraded to an Acronis Access Gateway Server. This service will continue to accept connections from mobilEcho clients and to act as the gateway to any file server, NAS or SharePoint data sources your users are accessing.

Your mobilEcho Client Management Administrator web console will be upgrade 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.

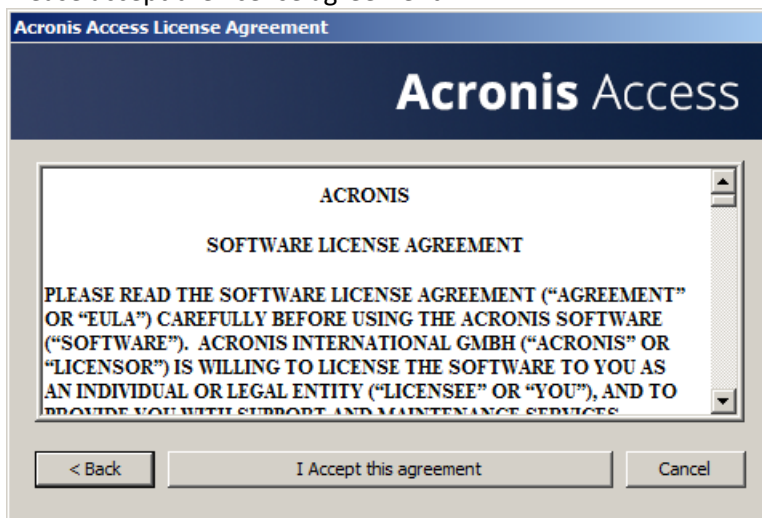
To perform an upgrade of Acronis Access:

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://www.grouplogic.com/web/aalatest>
 - b. You will need to enter your product serial number for verification before downloading the installer.

- c. The installer file is named: AcronisAccessAdvancedSetup.exe
4. Click **Next** on the Welcome Screen.

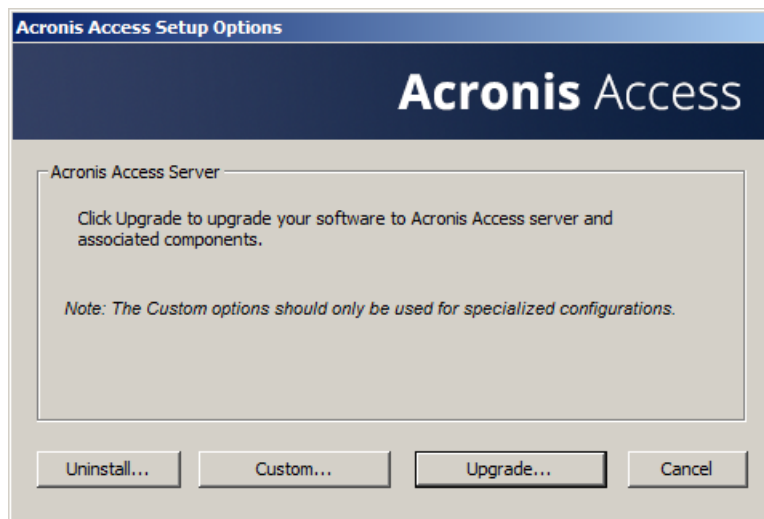


5. Please accept the license agreement.

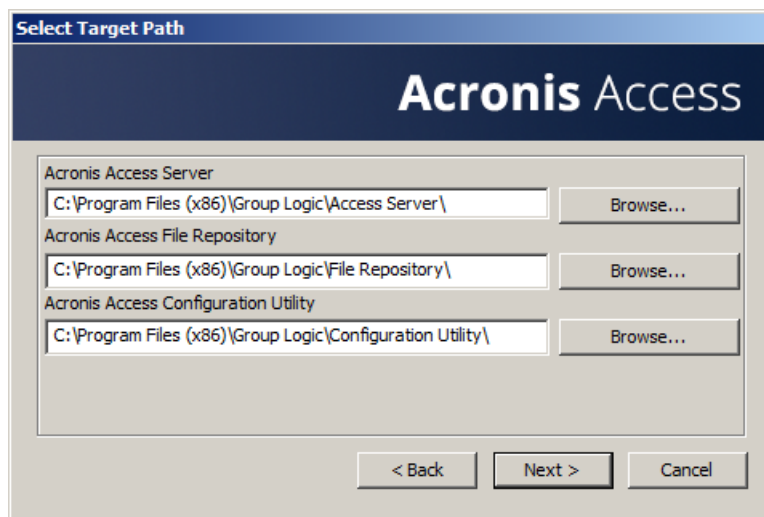


6. Click the **Upgrade** option to automatically upgrade your mobilEcho File Access Server service to an Acronis Access Gateway Server. In the upgrade process, the Acronis Access Server and its required services will also be installed.

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.

The dialog box is titled "PostgreSQL Configuration" and "Acronis Access". It contains two main sections. The first section, "PostgreSQL Install Location:", has two rows: "Base Path:" with a text field containing "C:\PostgreSQL\9.2\" and a "Browse..." button, and "Data Path:" with a text field containing "C:\PostgreSQL\9.2\Data\" and a "Browse..." button. The second section, "PostgreSQL Super-User Credentials: (will be created if necessary)", has three rows: "PostgreSQL Super-User password:" with a masked text field (asterisks), "Re-enter password:" with another masked text field, and "PostgreSQL Port:" with a text field containing "5432". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

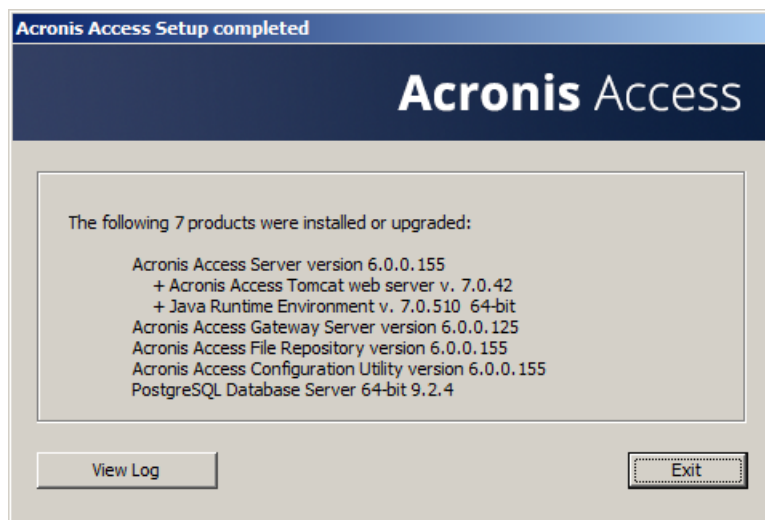
9. Please review the services being installed and upgraded. Then click **Install** to begin the upgrade.

The dialog box is titled "Acronis Access Install Warning" and "Acronis Access". It contains a warning message: "Setup will now install or upgrade the following products. This process may disrupt users of this system by starting and stopping the Acronis Access services." Below this is a list of components: "Acronis Access Server v. 6.0.0.155", "+ Acronis Access Tomcat web server v. 7.0.42", "+ Java Runtime Environment v. 7.0.510", "Acronis Access Gateway Server v. 4.5.2.103 --> v. 6.0.0.125", "Acronis Access File Repository v. 6.0.0.155", "Acronis Access Configuration Utility v. 6.0.0.155", and "PostgreSQL Database Server v. 9.2.4". At the bottom are three buttons: "< Back", "Install", and "Cancel".

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.

The dialog box is titled "Acronis Access Component Installation" and "Acronis Access". It contains the text "Installing Acronis Access Server..." and "Waiting for product installation to complete - this could take several minutes...". Below this is a progress bar with a small blue segment on the left.

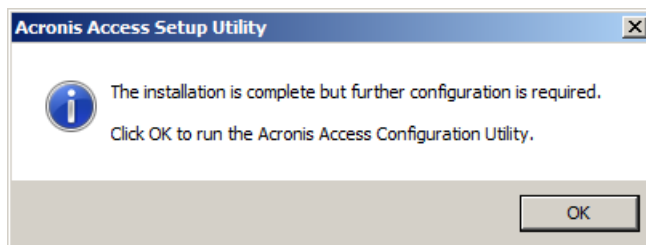
10. Once installation has completed, a summary of the components installed is shown. Click **Exit** to continue.



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.



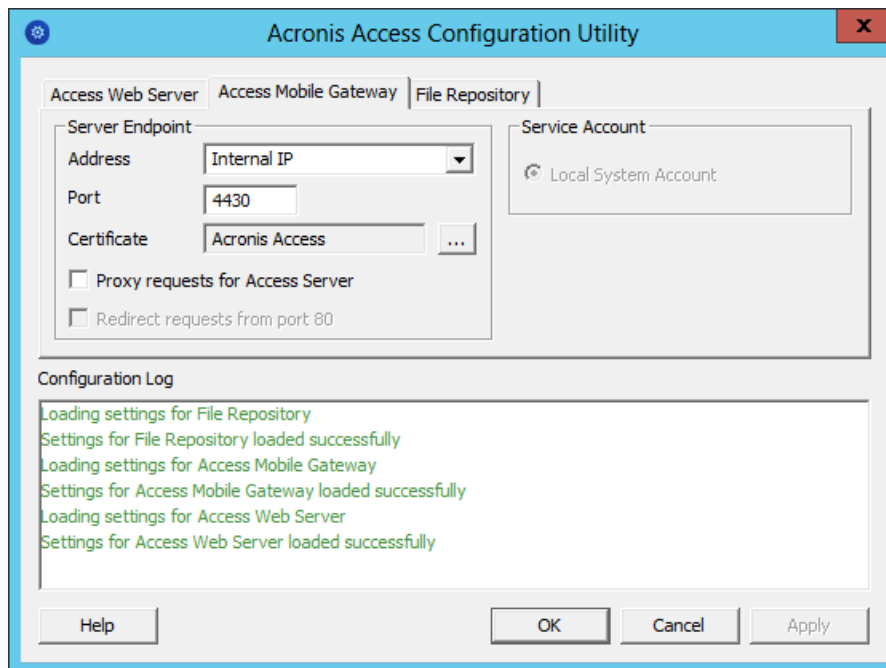
If you accidentally skip this step or need to change your network interfaces, ports, or certificates in the future. You can manually run the configuration utility at any time.

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

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

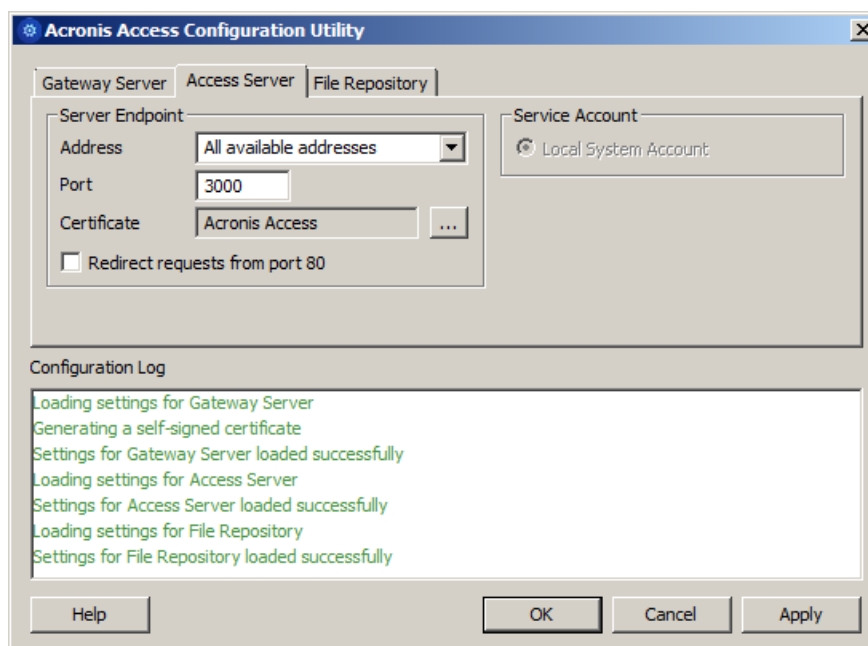
12. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core mobilEcho service that your mobilEcho clients connect to and that gives access to your file servers,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

Note: 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 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.



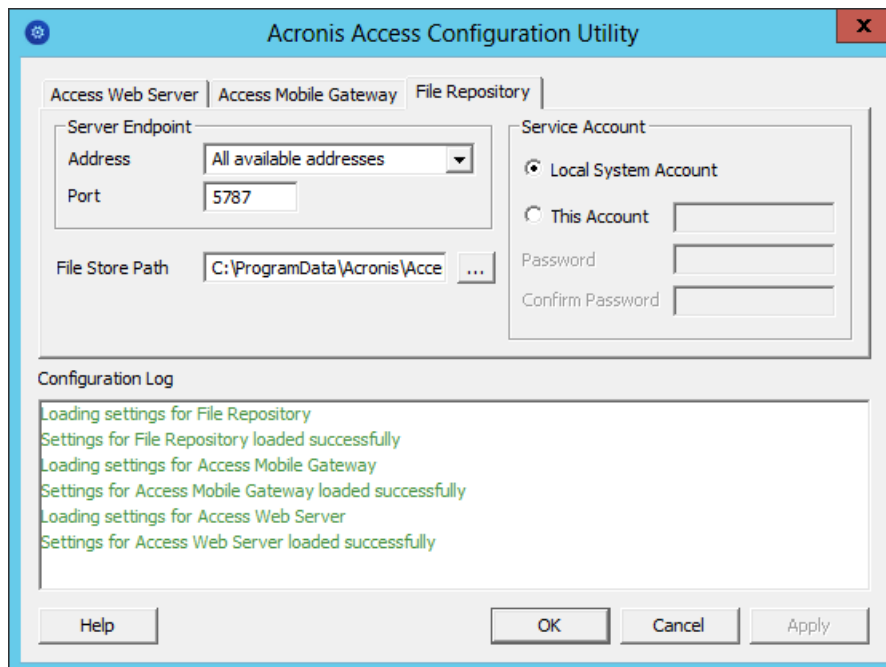
14. Acronis Access Server requires that a File Repository location be selected. If you are using mobilEcho only, this File Repository will not be used to store anything, but setting a location is still required.

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 chose to enable them at a later time, if desired.

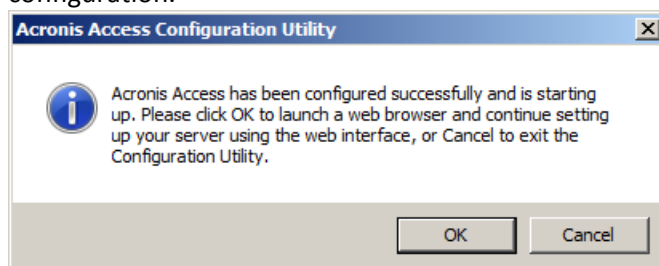
The default location for the File Repository is:

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.



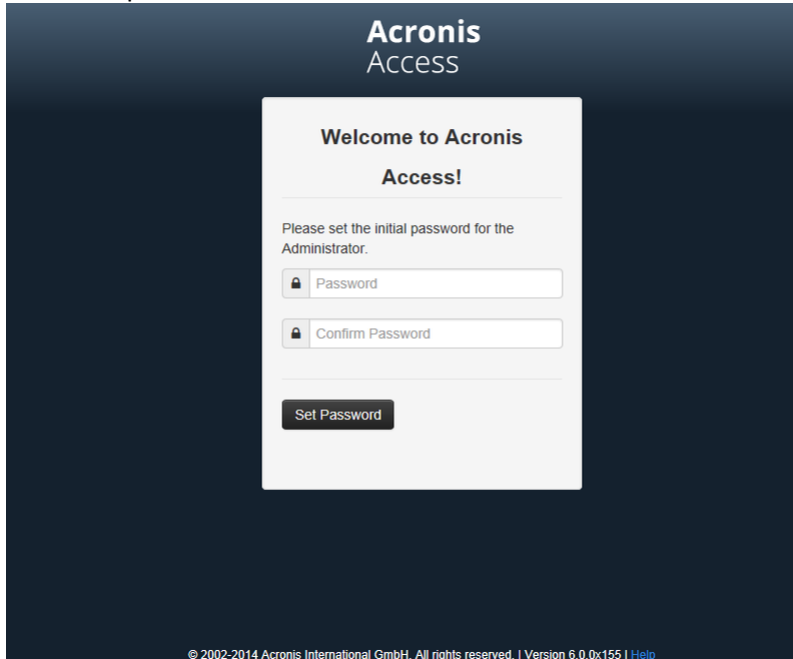
Required initial configuration of Acronis Access:

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

Acronis Access administrator

SMTP

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

SMTP Server Address:

SMTP Server Port:

Use secure connection? ☒

From Name:

From Email Address:

Use SMTP authentication? ☐

- 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 image shows two screenshots. The top screenshot is from the 'mobilEcho Client Management Administrator' web interface. It has a navigation bar with links: Devices, Invitations, Groups, Users, Servers & Folders, Allowed Apps, Settings, and Log out. The main content area is titled 'Servers and Folders' and includes a description, an 'Assign by user or group' section with a 'Find user or group' button, and a 'Servers' section with an 'Add new server' button. Below this is a table with two servers:

mobilEcho Server	Display Name	
192.168.1.141	Local	delete
rtt.gillabs.com	Main Server	delete

The bottom screenshot is from the 'Acronis Access' web console. It has a sidebar with navigation links: Mobile Access, Devices, Enroll Users, Policies, Gateway Servers, Data Sources, Settings, Sync & Share, Audit Log, and General Settings. The main content area is titled 'Gateway Servers' and has buttons for '+ Add Gateway Server' and '+ Add Cluster Group'. It contains a table with the same two servers as the top screenshot:

Type	Name	Address	Version	Status	Active Sessions	
Local	Local	192.168.1.141		Legacy	0	Details
Main Server	Main Server	rtt.gillabs.com		Legacy	0	Details

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.



Acronis Access administrator

Folders Gateway Servers Visible on Clients Legacy Data Sources Assigned Sources

Legacy Data Sources Add New Legacy Folder

Some of the existing "Folders" configured on your mobilEcho Client Management Server prior to upgrading to Acronis Access, have been imported as "Legacy Folders". The Legacy Folders listed below point to locations on Gateway Servers that have not yet been upgraded to Acronis Access, or that have been upgraded to Acronis Access but have not been registered to be administered from this Acronis Access Server. Once you upgrade these Gateway Servers to Acronis Access and register them on the [Gateway Servers](#) page, their Legacy Folders will be imported into the standard [Folders](#) list. If you need to add or edit folders located on these Gateway Servers prior to upgrading them to Acronis Access, you can do so from this page.

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

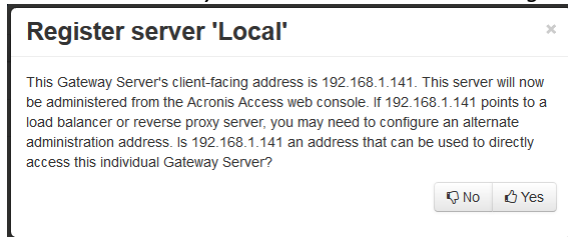


Type	Display Name	Server	Path	Sync	
Local	192.168.1.141		Legacy	0	Details

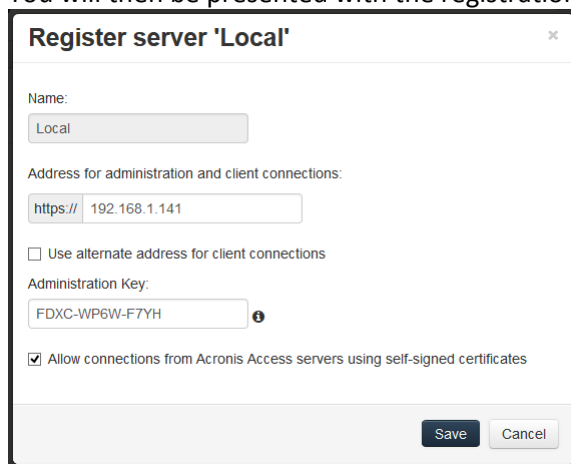
- ✎ Edit Address
- Register**
- ✕ Remove

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



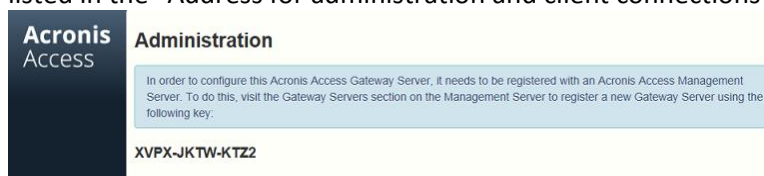
3. You will then be presented with the registration dialog.



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.



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.giliabs.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	Edit Remove
🌐	Access	Local	https://192.168.1.141:3000	None	Edit Remove
📁	Thousand Files	Local	\\vegaritest\files\10000 files	None	Edit Remove
🌐	SharePoint	Local	http://sharepoint2010.giliabs.com:2229	None	Edit Remove

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: test folder

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

Local (192.168.1.141)

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:\testfolder

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

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

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	
Folder	test folder	Local	D:\testfolder	None	
Folder	Access	Local	https://192.168.1.141:3000	None	
Folder	Thousand Files	Local	\\vega\test files\10000 files	None	
Folder	SharePoint	Local	http://sharepoint2010.gilllabs.com:2229	None	

Home

ON THIS DEVICE

File Inbox

My Files

FAVORITES

Bookmarked Folders

NETWORK FOLDERS & SERVERS

Home Folder

Local

Local

Access

SharePoint

test folder

Thousand Files

4 File Shares

Upgrading Acronis Access 6.0 to 7.x or newer:

Once you have confirmed that the upgrade is successful, you can continue the upgrade to the latest version by following the steps below. The upgrade procedure from a previous version of Acronis Access is a simplified process and requires almost no configuration.

Backup the vital components:

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**.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

The PostgreSQL database

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

1. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
e.g. `cd "C:\PostgreSQL\9.2\bin"`
2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

```
D:\Backups\mybackup.sql
```

Note: *acronisaccess_production must be entered exactly as shown as it is the name of the Acronis Access database*

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access installation process.

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

4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

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

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

Where **alldbs.sql** will be the generated backup file. It can include a full path specification, for instance

```
D:\Backups\alldbs.sql
```

For full syntax on this command see: <http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html>

<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

Info: *For more information on PostgreSQL backup procedures and command syntax please read this:*

<http://www.postgresql.org/docs/9.2/static/backup.html>

<http://www.postgresql.org/docs/9.1/static/backup.html>

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

1. Navigate to the Acronis Access installation folder containing the configuration file.

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

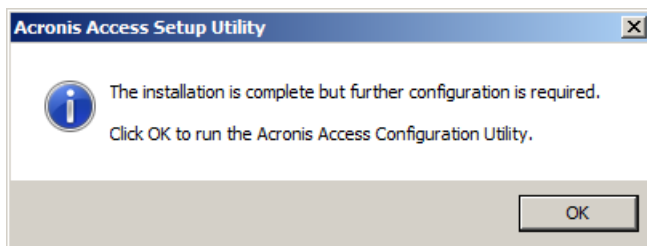
2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

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**.

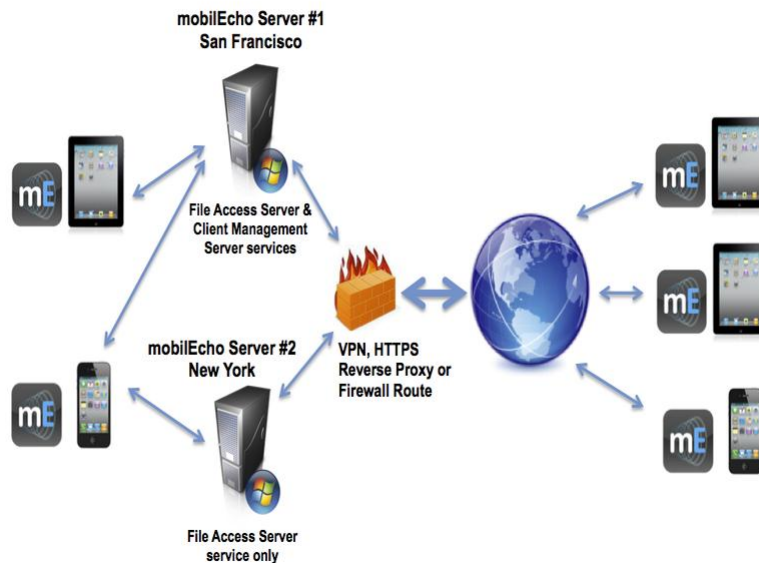


Verify that none of the settings in the Configuration Utility have changed. After you have verified all of your settings are as expected, press **OK** to close the Configuration Utility and start the Acronis Access services.

3.3.2.3 Upgrading multiple mobilEcho servers with Client Management

Scenario 3 - Upgrading multiple mobilEcho servers with Client Management

Multiple, separate mobilEcho servers



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:

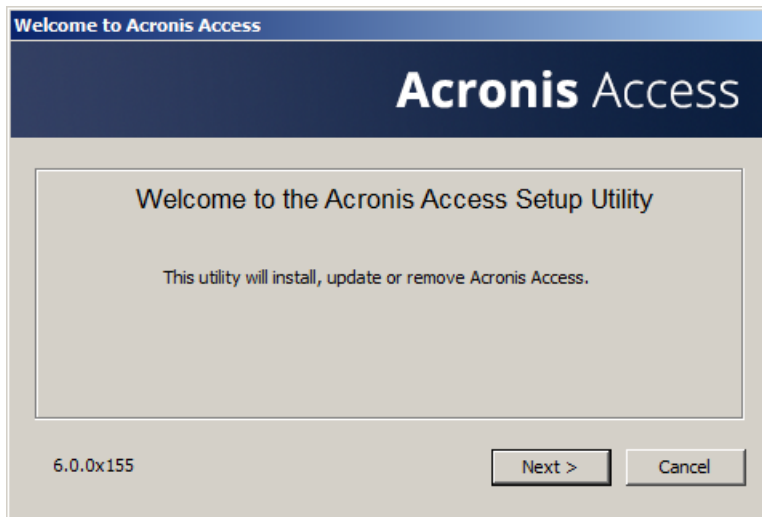
1. Follow the instructions in Scenario 2 to upgrade the Windows Server that is acting as your mobilEcho Client Management Server. This is the server that you connect to when you log into the mobilEcho Client Management Administrator web console.
2. Once you complete that upgrade, you will have a functional 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.

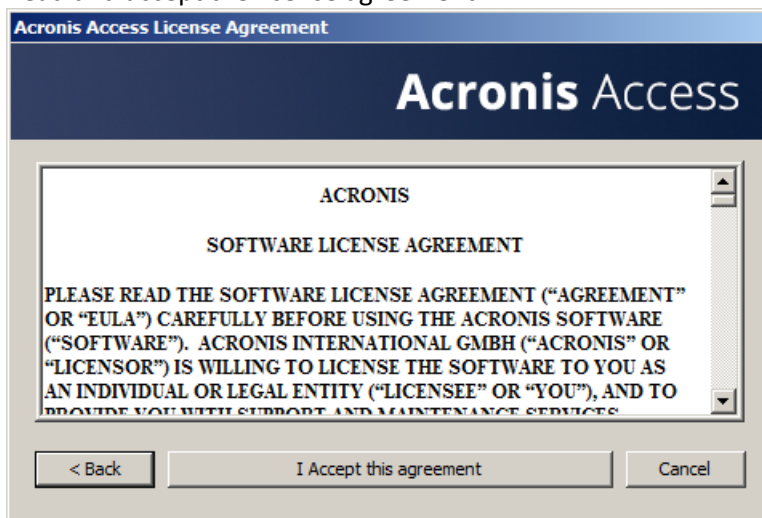
On every Windows Server acting as a mobilEcho File Access Server only:

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

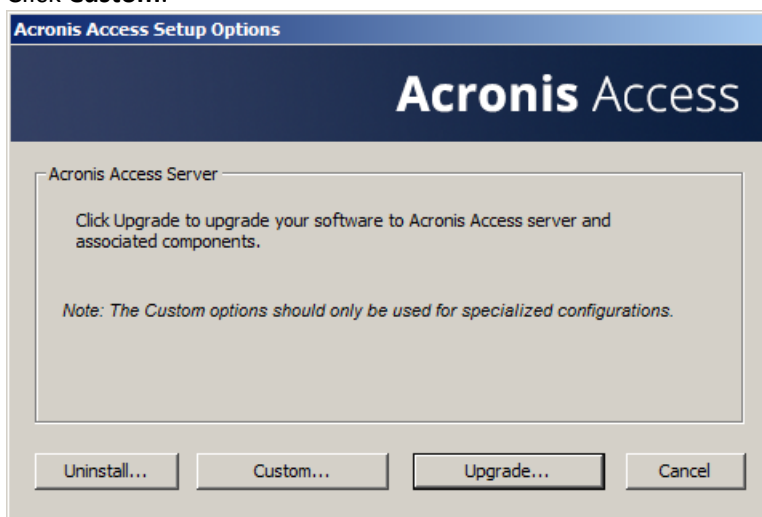
2. Run the Acronis Access installer on the desired server.
3. Press **Next** on the Welcome screen.



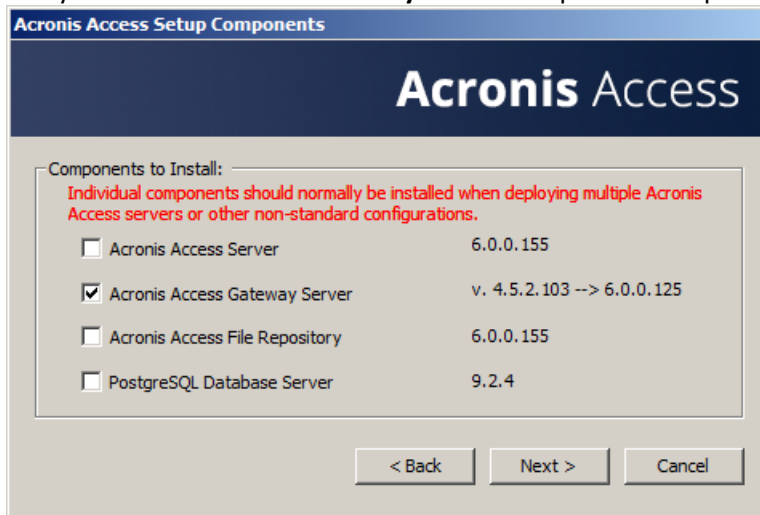
4. Read and accept the license agreement.



5. Click **Custom**.



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

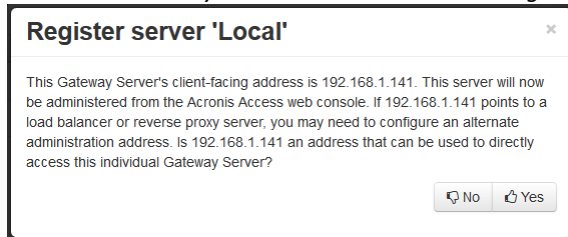


Next.

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**.

10. 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.



11. 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.

12. 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.

13. 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.



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.

3.3.2.4 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. 113) article.

3.3.3 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 a 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.*

3.4 Upgrading from activEcho 2.7 or earlier

In this section

Before You Begin.....	106
The Upgrade Process	107

3.4.1 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?

3.4.2 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	107
Upgrading an activEcho server with a mobilEcho Client Management Server	113
Upgrading an activEcho server with a mobilEcho Client Management Server on another server	121

3.4.2.1 Upgrading a single activEcho server without a mobilEcho Client Management Server

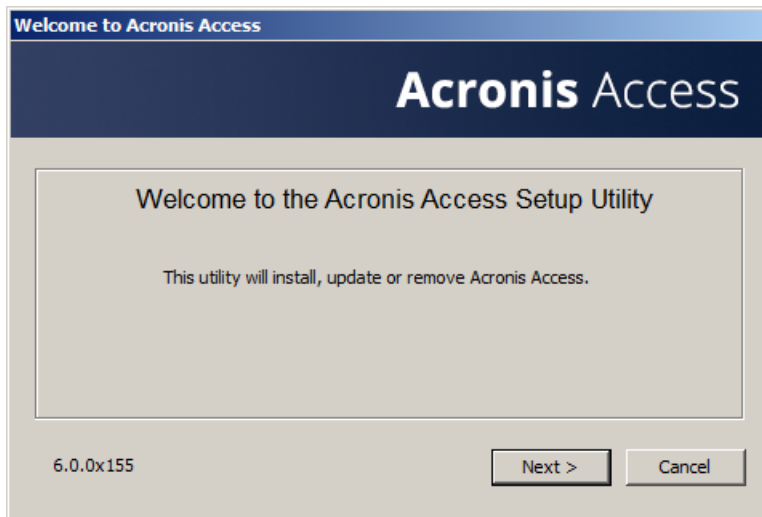
Scenario 1 - Upgrading a single activEcho server without a mobilEcho Client Management Server

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.

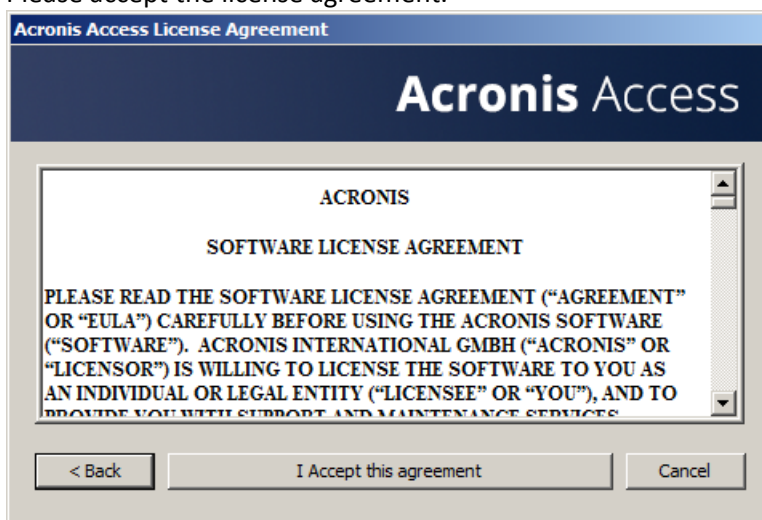
To perform an upgrade of activEcho:

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://www.grouplogic.com/web/aalatest>
 - b. You will need to enter your product serial number for verification before downloading the installer.

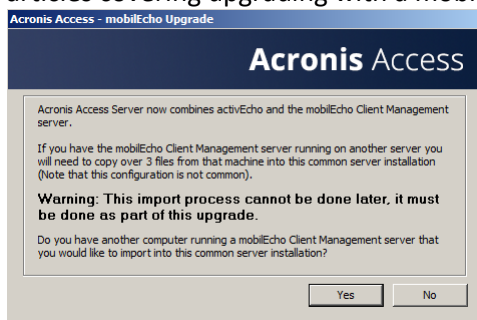
- c. The installer file is named: AcronisAccessAdvancedSetup.exe
4. Click **Next** on the Welcome Screen.



5. Please accept the license agreement.

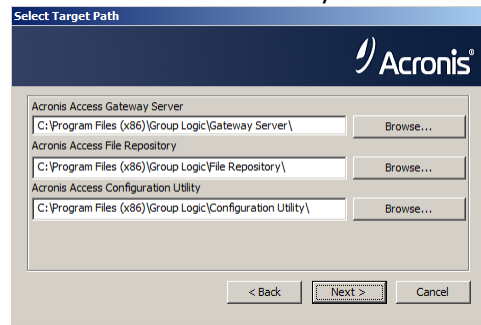


6. Click **Upgrade** to automatically upgrade your activEcho Server to the new Acronis Access Server. In the upgrade process, a Gateway Server and it's required services will also be installed.
7. A prompt for remote mobilEcho Servers will be shown. If you don't have a mobilEcho Client Management Server, press **No**. If you have a mobilEcho Client Management Server, go to the Upgrading an activEcho server with a mobilEcho Client Management Server (p. 113) or Upgrading an activEcho server with a mobilEcho Client Management Server on another server (p. 121) articles covering upgrading with a mobilEcho installation present.

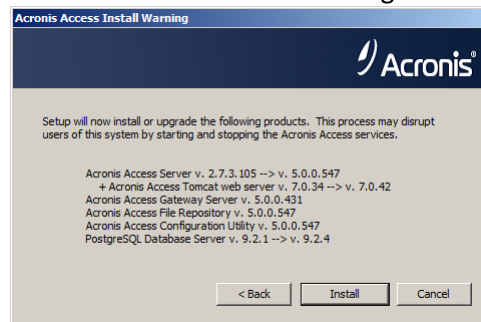


8. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing activEcho server, these paths will default to your existing installation

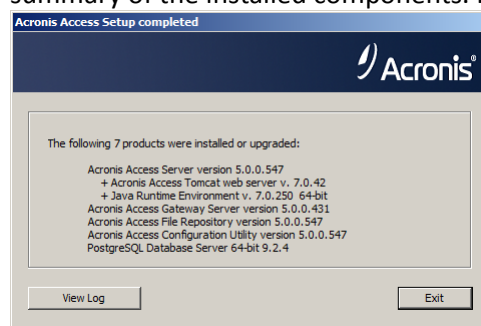
location. We recommend you do not change these installation paths. Click **Next**.



9. Please review the services being installed and upgraded.

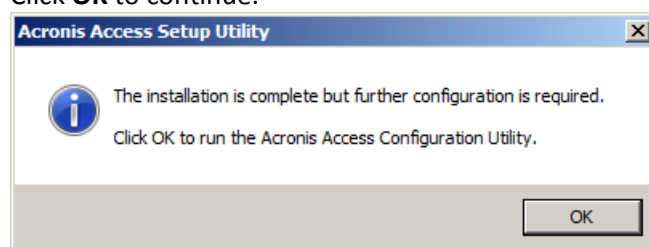


10. Press **Install** to begin the upgrade. Once the installation is complete, you will be shown a summary of the installed components. Press **Exit**.



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.



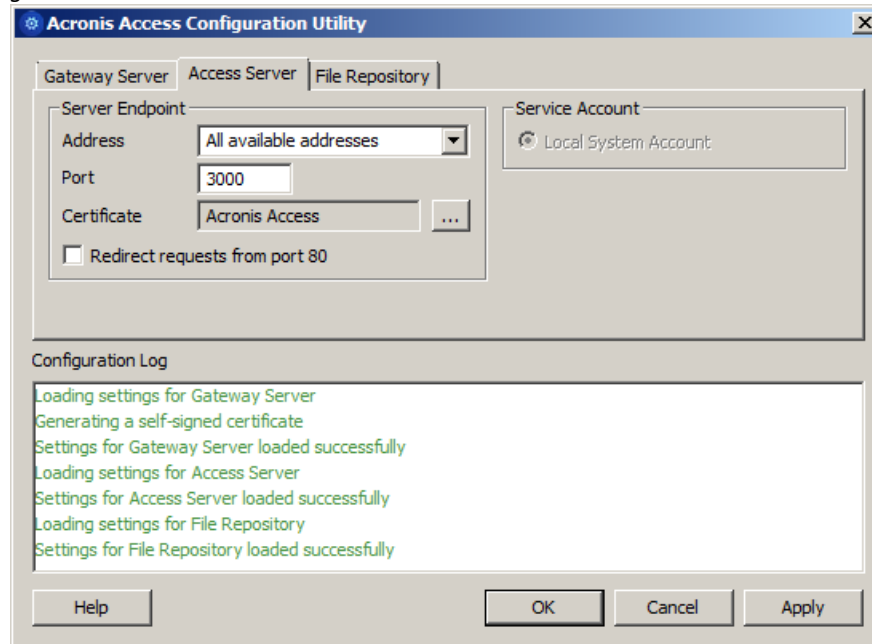
12. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core Acronis Access service that your mobilEcho clients connect to and that gives access to your file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

Note: 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

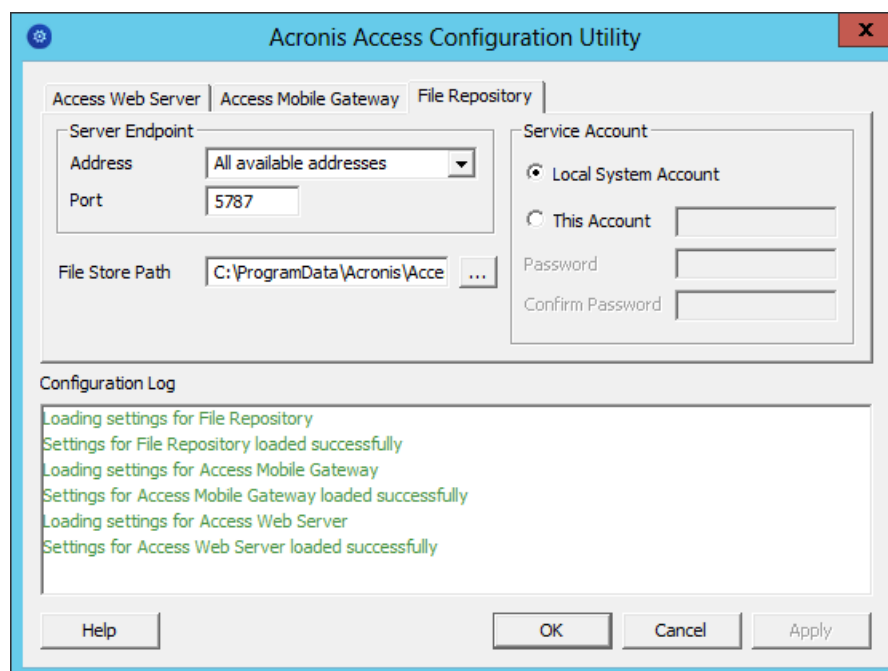
have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate will be generated.

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 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.

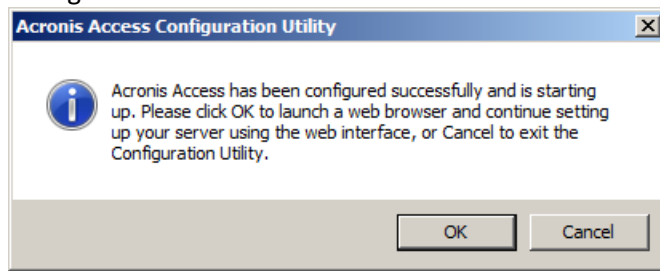
Note: Please review the settings for the Access Server. The default settings are recommended. This web console typically runs on all available network addresses on port 3000. If you have an existing SSL server identity certificate, it will be automatically selected. If you do not, a self-signed certificate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



Upgrading Acronis Access 6.0 to 7.x or newer:

Once you have confirmed that the upgrade is successful, you can continue the upgrade to the latest version by following the steps below. The upgrade procedure from a previous version of Acronis Access is a simplified process and requires almost no configuration.

Backup the vital components:

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**.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

The PostgreSQL database

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

1. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
e.g. **cd "C:\PostgreSQL\9.2\bin"**
2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

```
D:\Backups\mybackup.sql
```

Note: *acronisaccess_production* must be entered exactly as shown as it is the name of the Acronis Access database

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access installation process.

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

4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

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

pg_dumpall -U postgres > alldbs.sql

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

For full syntax on this command see: <http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html>

<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

Info: For more information on PostgreSQL backup procedures and command syntax please read this:

<http://www.postgresql.org/docs/9.2/static/backup.html>

<http://www.postgresql.org/docs/9.1/static/backup.html>

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

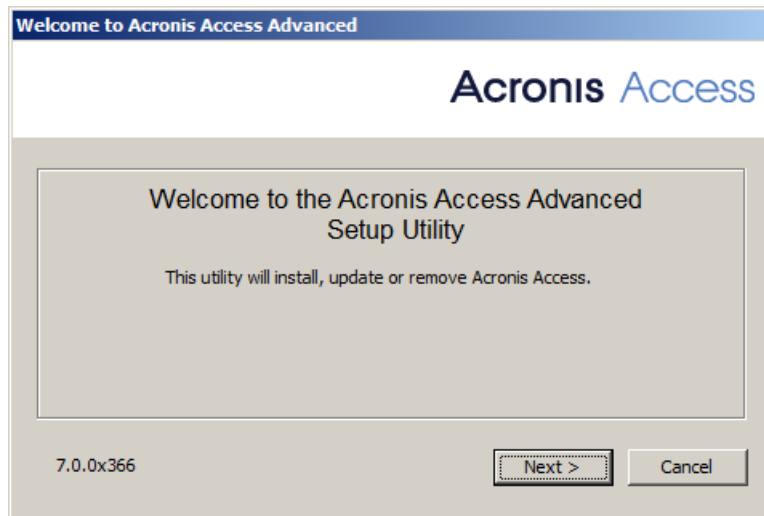
1. Navigate to the Acronis Access installation folder containing the configuration file.

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

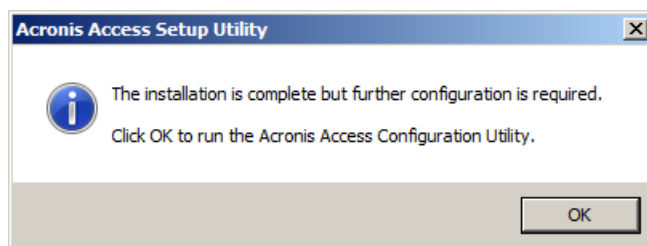
2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

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**.



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.

3.4.2.2 Upgrading an activEcho server with a mobilEcho Client Management Server

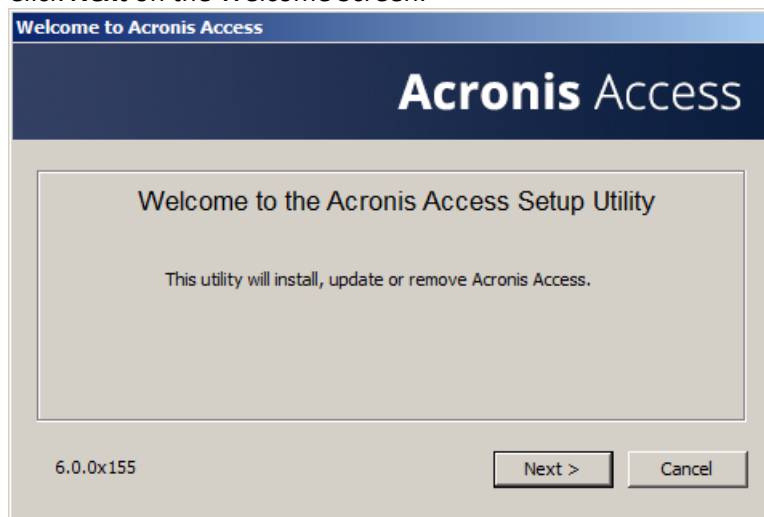
Scenario 2 - Upgrading an activEcho server with a mobilEcho Client Management Server

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

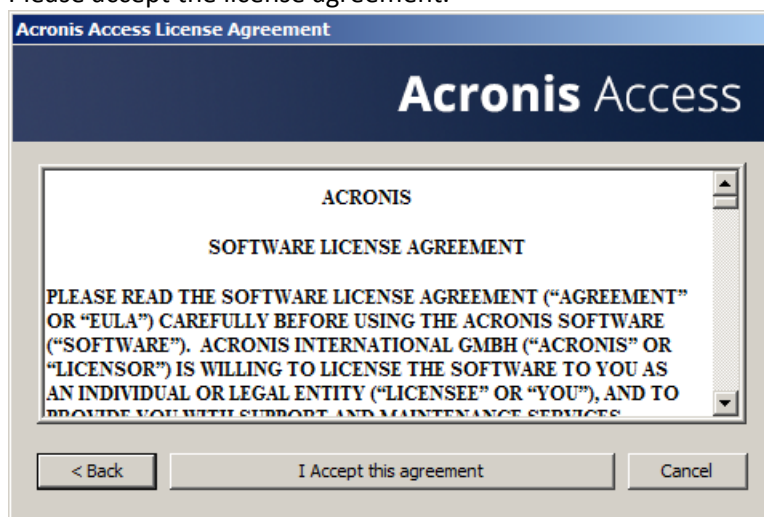
servers. The Acronis Access Server web console allows you to administer both activEcho and mobilEcho from one unified web interface.

To perform an upgrade of activEcho:

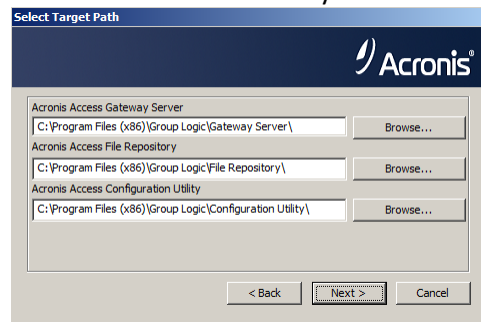
1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Download the Acronis Access Server installer to your activEcho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



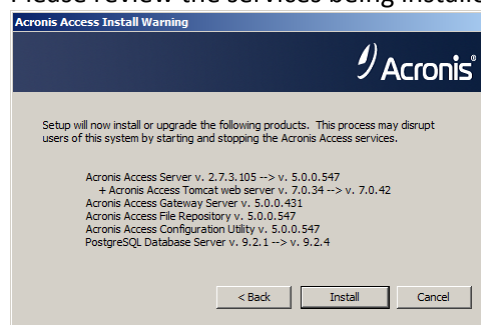
5. Please accept the license agreement.



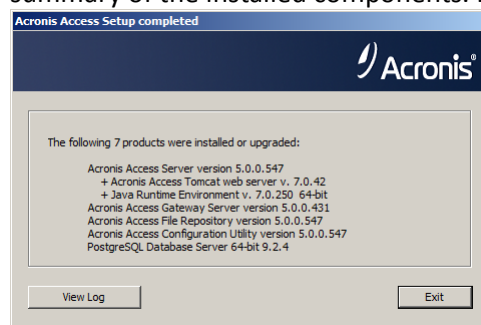
6. Click **Upgrade** to automatically upgrade your activEcho Server and mobilEcho Client Management Server to the new Acronis Access Server. In the upgrade process, a Gateway Server and it's required services will also be installed. If a File Server is present, the installer will upgrade the File Server 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.

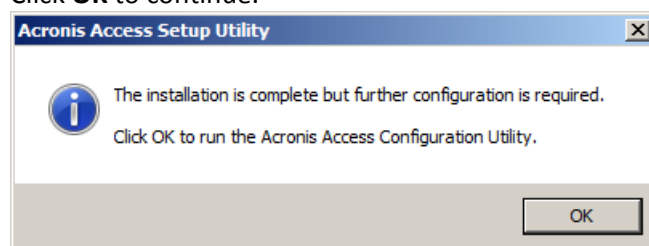


9. Press **Install** to begin the upgrade. Once the installation is complete, you will be shown a summary of the installed components. Press **Exit**.



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.

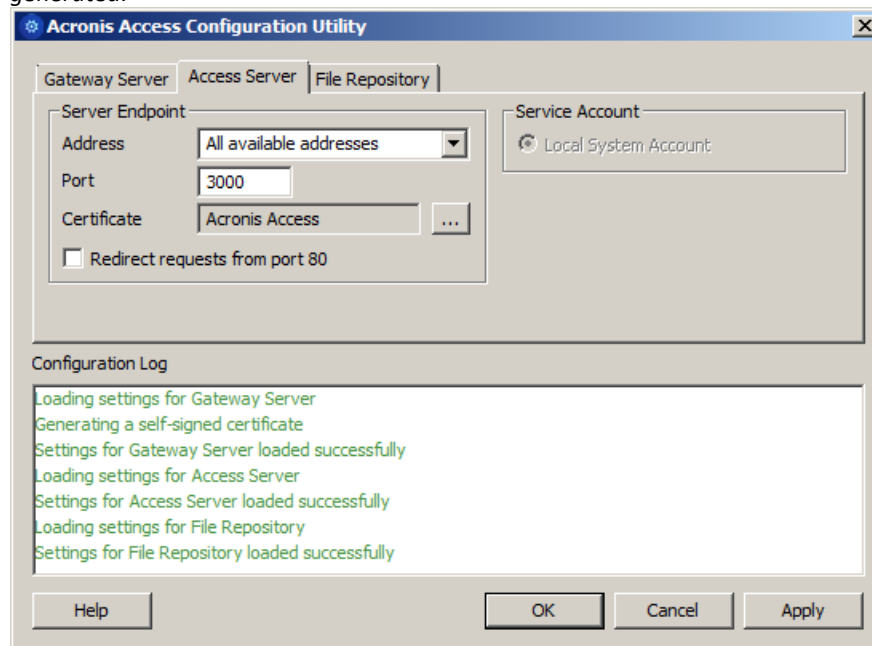


11. Within the Configuration Utility, the Gateway Server tab is used to configure your Acronis Access Gateway Server's network address, port, and certificate. The Acronis Access Gateway Server is the core Acronis Access service that your mobilEcho clients connect to and that gives access to your file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

Acronis Access Configuration Utility

Access Web Server | Access Mobile Gateway | **File Repository**

Server Endpoint
Address: All available addresses
Port: 5787

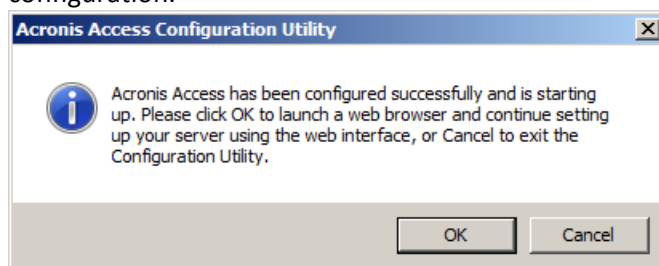
File Store Path: C:\ProgramData\Acronis\Acce

Service Account
☒ Local System Account
☐ This Account
Password:
Confirm Password:

Configuration Log
Loading settings for File Repository
Settings for File Repository loaded successfully
Loading settings for Access Mobile Gateway
Settings for Access Mobile Gateway loaded successfully
Loading settings for Access Web Server
Settings for Access Web Server loaded successfully

Help OK Cancel Apply

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

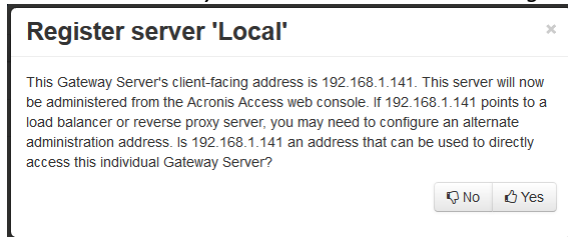
In this scenario, you should only have one Windows Server running the Acronis Access console and the Gateway Server, so you will have just one server listed on the Gateway Servers page. This server needs to be registered so that you can administer it.

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

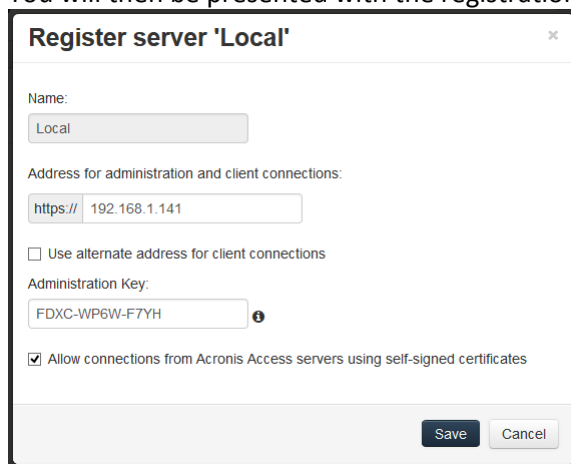


-
2. You will be asked if the existing network address for the server you are registering can be used to directly access the server. The existing address is typically the network address that your mobile device users must use to access the Gateway Server, so it's possible this address points to a proxy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



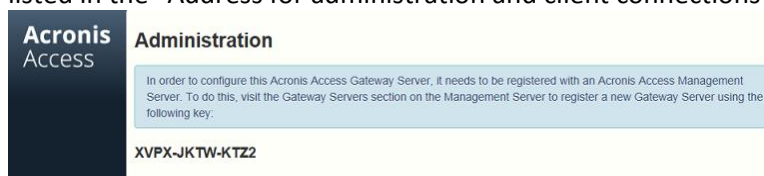
-
-
3. You will then be presented with the registration dialog.



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.



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.giliabs.com		Legacy	0	Details
☰	Local	192.168.1.141		🟢	0	Details

Details
 Edit
 Access Restrictions
 Remove

Upgrading Acronis Access 6.0 to 7.x or newer:

Once you have confirmed that the upgrade is successful, you can continue the upgrade to the latest version by following the steps below. The upgrade procedure from a previous version of Acronis Access is a simplified process and requires almost no configuration.

Backup the vital components:

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**.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

The PostgreSQL database

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

1. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
e.g. `cd "C:\PostgreSQL\9.2\bin"`
2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

Note: **acronisaccess_production** must be entered exactly as shown as it is the name of the Acronis Access database

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access installation process.

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

4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

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

pg_dumpall -U postgres > alldbs.sql

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

For full syntax on this command see: <http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html>
<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

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

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

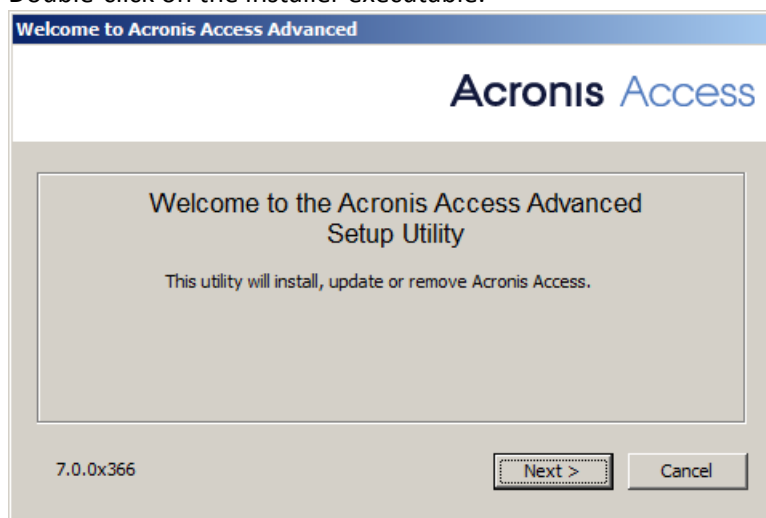
1. Navigate to the Acronis Access installation folder containing the configuration file.

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

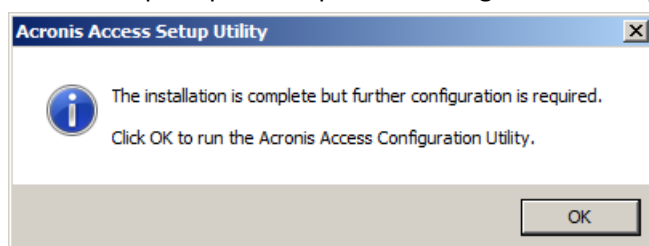
2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

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**.



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.

3.4.2.3 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

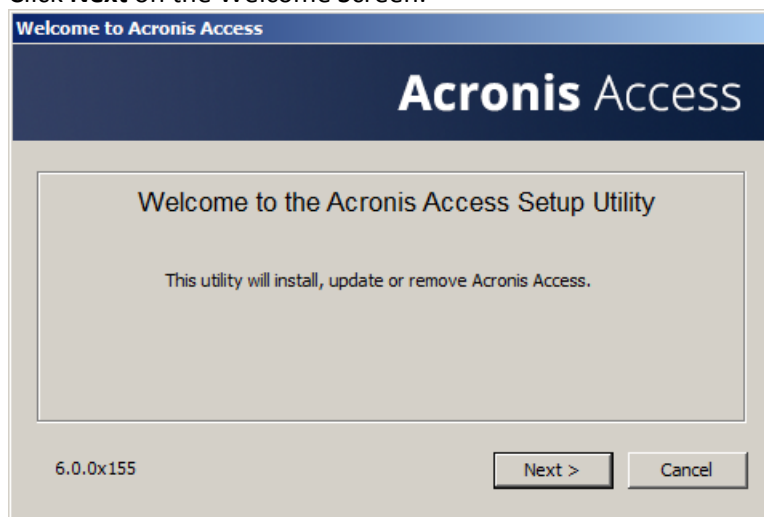
Warning! For this scenario, we recommend that you keep your activEcho and mobilEcho servers separate and upgrade each one individually. For instructions on upgrading your activEcho server, follow the *Upgrading a single activEcho server without a mobilEcho Client Management Server (p. 107)* guide and for instructions on

upgrading your mobilEcho server, follow the Upgrading a single mobilEcho server with Client Management enabled (p. 83) guide.

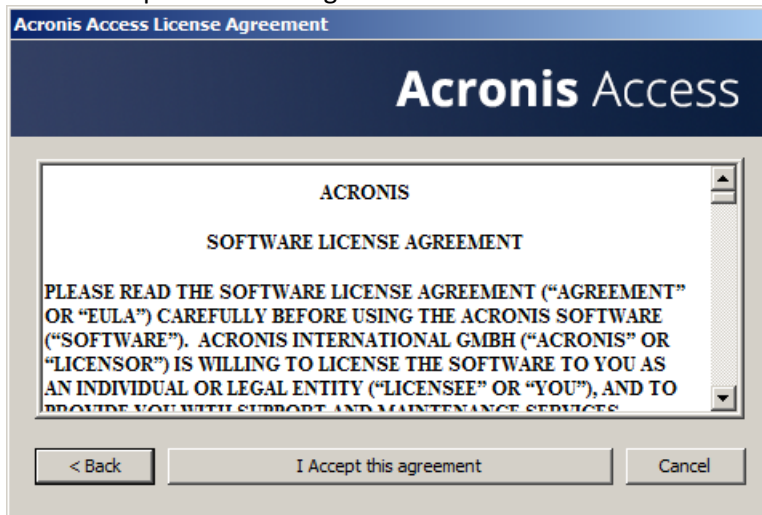
In this scenario, you have two (or more) Windows Servers with one running just the activEcho Server and another running the mobilEcho File Server and Management Server. This procedure will upgrade your activEcho server and mobilEcho Client Management Server to the unified Acronis Access Server web console. 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:

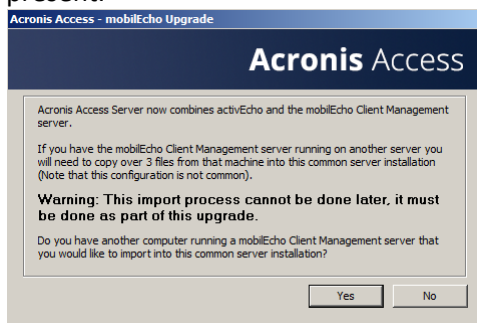
1. Backup all of the necessary files following these guides: mobilEcho 4.5 Backup and/or activEcho 2.7 backup.
2. Write down the current IP Address of your server running mobilEcho and give the computer a different IP address (You will need the new one as well).
3. Go to the server running activEcho 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://www.grouplogic.com/web/aalatest>
 - b. You will need to enter your product serial number for verification before downloading the installer.
 - c. The installer file is named: AcronisAccessAdvancedSetup.exe
6. Click **Next** on the Welcome Screen.



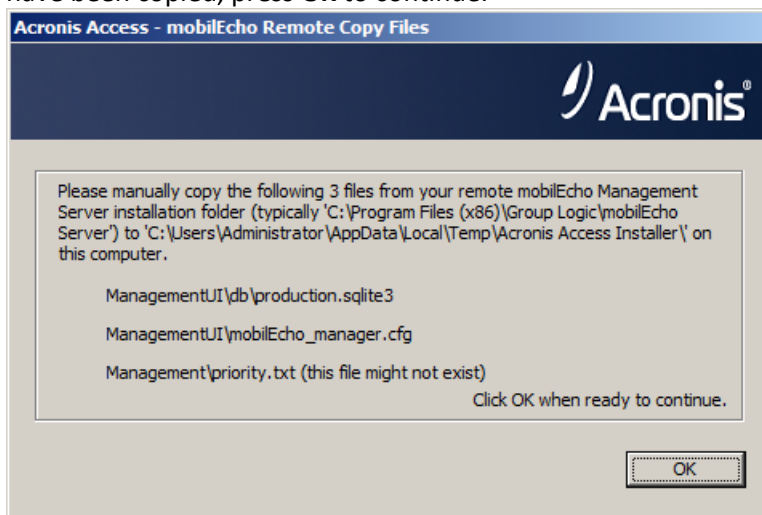
7. Please accept the license agreement.



8. Click **Upgrade** to automatically upgrade your activEcho Server to the new Acronis Access Server. In the upgrade process, a Gateway Server and its 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.



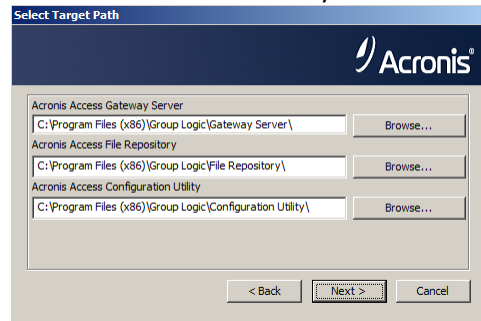
Note: These files are generally located at:

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

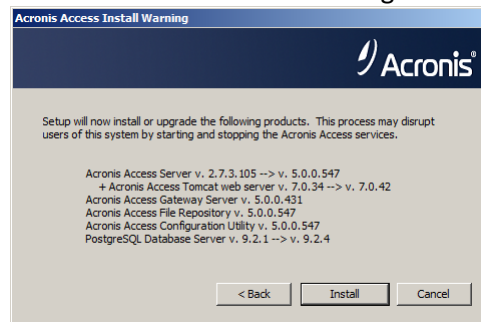
C:\Program Files (x86)\Group Logic\mobileEcho Server\ManagementUI\mobileEcho_manager.cfg

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

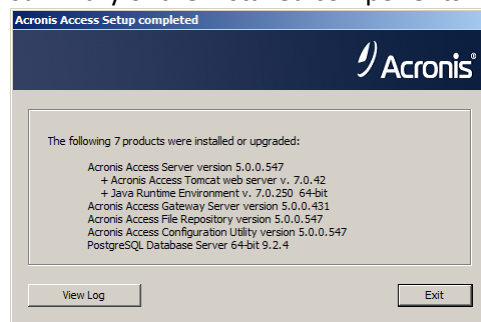
11. Select an installation location for the Acronis Access components being installed. If you are upgrading an existing activEcho server, these paths will default to your existing installation location. We recommend you do not change these installation paths. Click **Next**.



12. Please review the services being installed and upgraded.



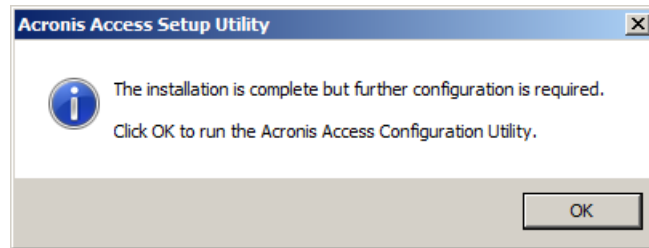
13. Press **Install** to begin the upgrade. Once the installation is complete, you will be shown a summary of the installed components. Press **Exit**.



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.

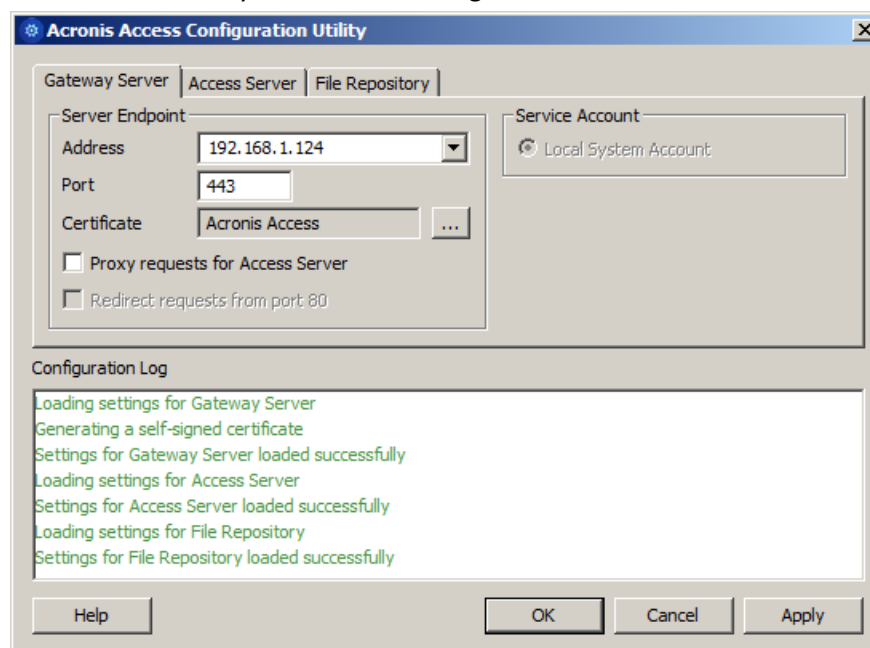
Click **OK** to continue.



Using the Configuration Utility

On the Gateway Server tab

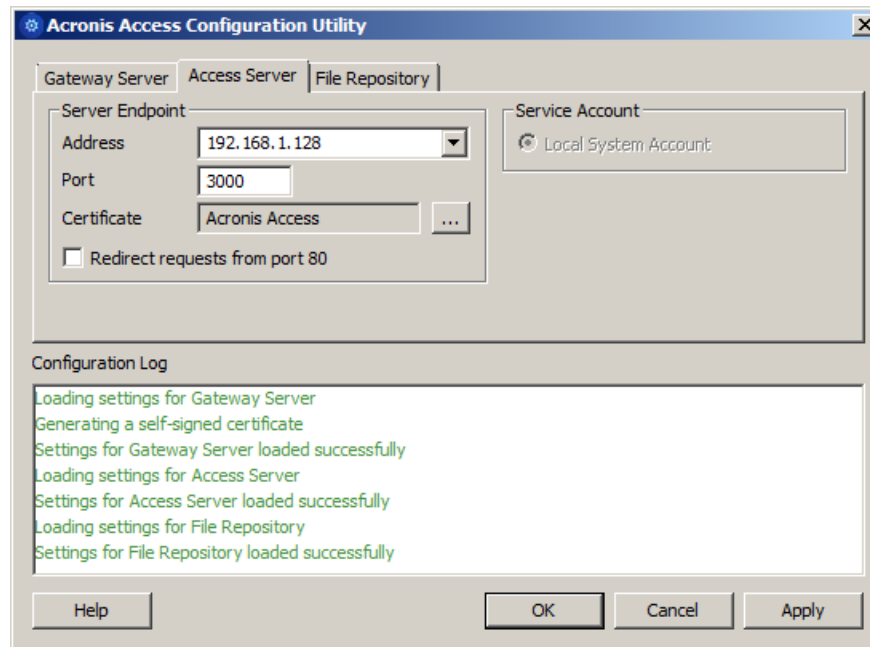
1. For the **Address** field, enter the IP address of your server that was running mobilEcho. This is the address you wrote down at the beginning.
2. For the **Port** field, enter the port number that your mobilEcho File Server used.
3. Add the certificate you have been using for the mobilEcho File Server.



On the Access Server

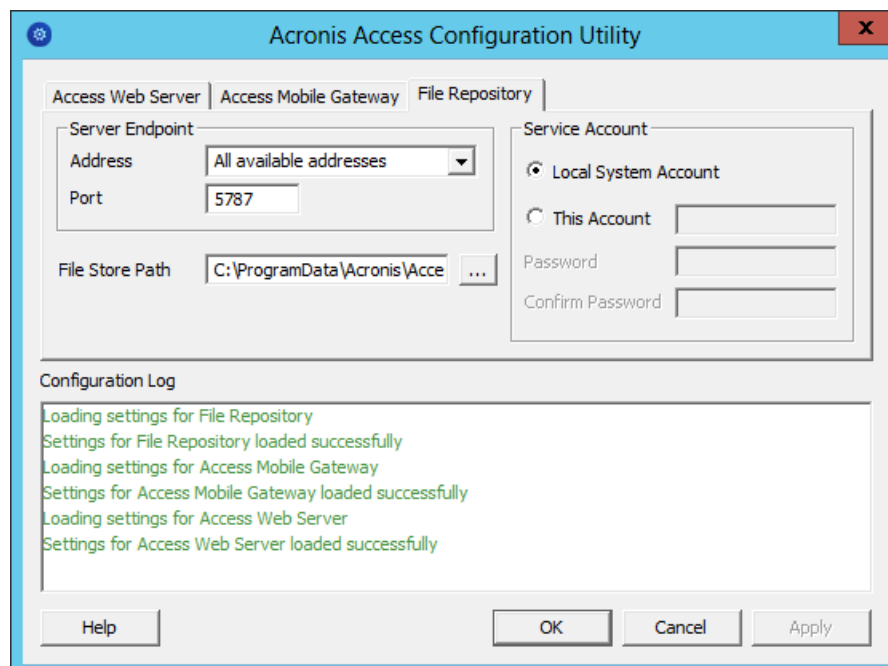
1. For the **Address** field, enter the IP address you've been using for your activEcho server until now. This should be the default.
2. For the **Port** field, enter the port number you've been using for your activEcho server until now. This should be the default.

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



On the File Repository tab

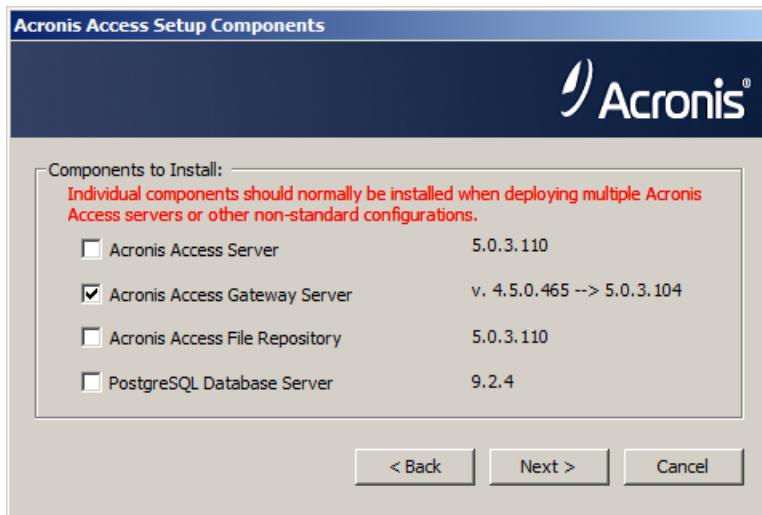
1. For the **Address** field, enter the IP address or DNS name of your Repository Service. This should be the default.
2. For the **Port** field, enter the port number for your Repository Service. This should be the default.
3. Select the path to your FileStore folder. This should be the default.



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

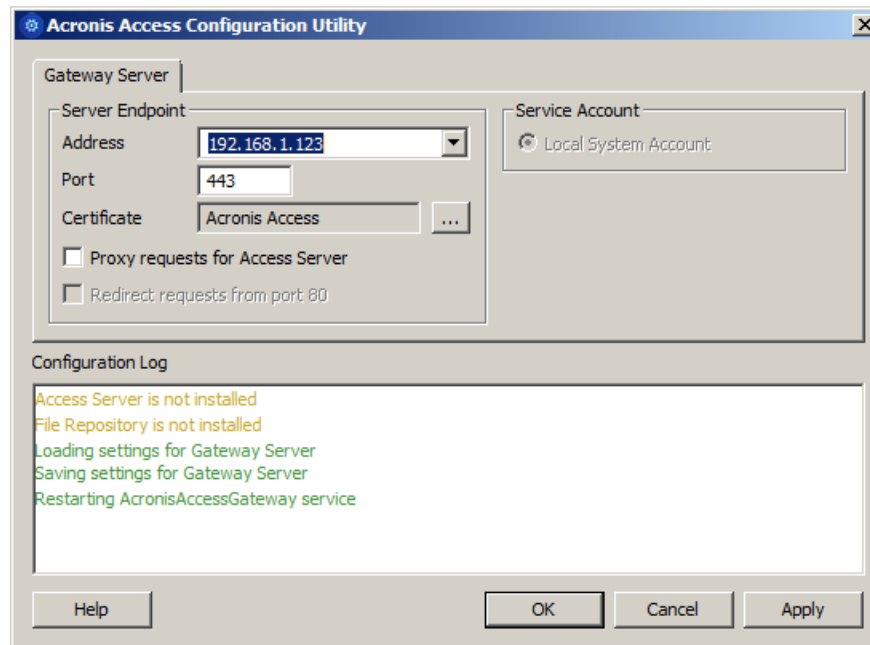
Configuring your local Gateway Server

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**.

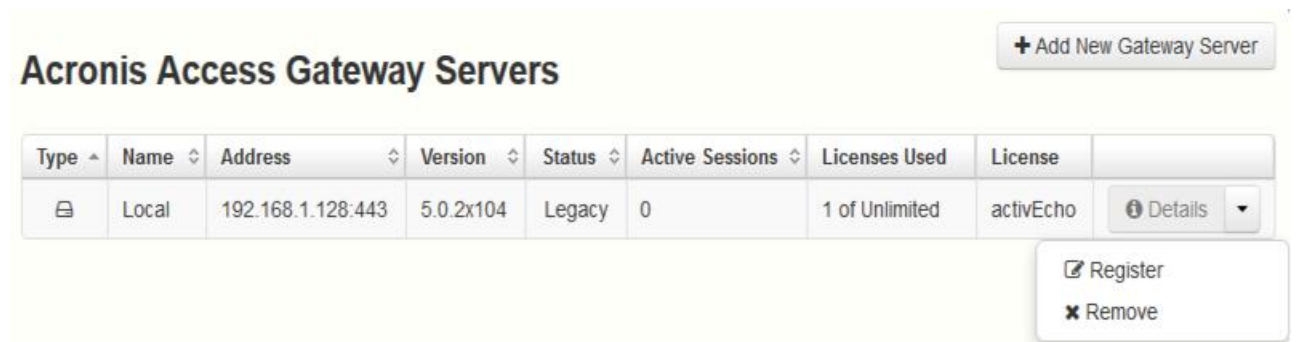


7. Review the installation path and press **Next**. This should be the default.
8. Review the components which will be installed and press **Install**.
9. After the installation finishes, close the installer and start the configuration utility (if it doesn't start automatically, it can generally be found 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.

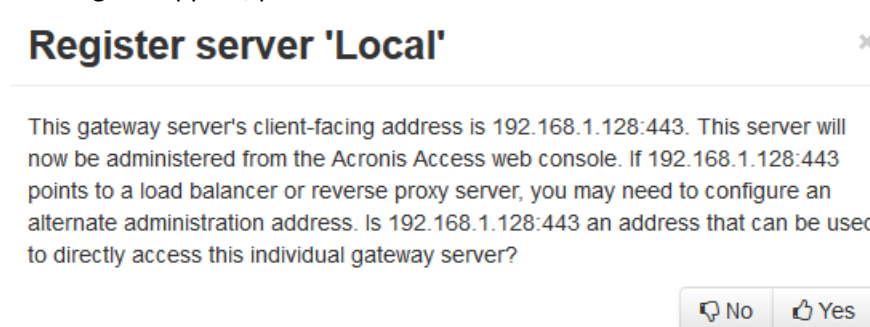
11. For the **Port** field, specify the port number your mobilEcho File Server previously used (this should be the default).



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



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



17. 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:

AWR

Address for administration and client connections:

https:// 192.168.1.123

☐ Use alternate address for client connections

Administration Key:

MZWZ-9HRV-ZT3V ⓘ

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

Save

Cancel

18. 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.
19. 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:

Local Gateway

Address for administration: ⓘ

[https://](#) 192.168.1.124

☐ Use alternate address for client connections ⓘ

Administration Key: ⓘ

RAA3-J7F8-Z13A

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

Save

Cancel

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

Upgrading Acronis Access 6.0 to 7.x or newer:

Once you have confirmed that the upgrade is successful, you can continue the upgrade to the latest version by following the steps below. The upgrade procedure from a previous version of Acronis Access is a simplified process and requires almost no configuration.

Backup the vital components:

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**.

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On, those changes are preserved), you will have to manually copy and paste your changes from the old file.

The PostgreSQL database

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

1. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
e.g. `cd "C:\PostgreSQL\9.2\bin"`
2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

Note: *acronisaccess_production* must be entered exactly as shown as it is the name of the Acronis Access database

3. A "Password: " line appears. Enter the postgres password that you set during the Acronis Access installation process.

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

4. Your backup file will appear in the **bin** folder by default unless the output file specification contains a full path to a different directory.

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

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

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

For full syntax on this command see: <http://www.postgresql.org/docs/9.2/static/app-pg-dumpall.html>
<http://www.postgresql.org/docs/9.1/static/app-pg-dumpall.html>

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

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

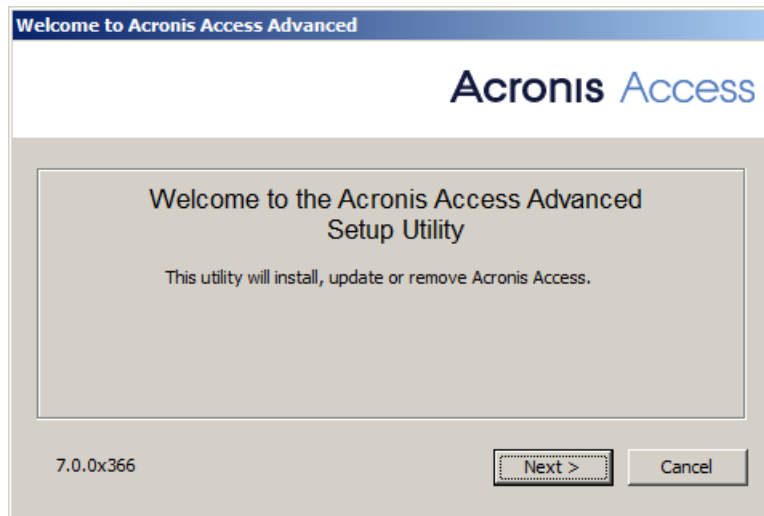
1. Navigate to the Acronis Access installation folder containing the configuration file.

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

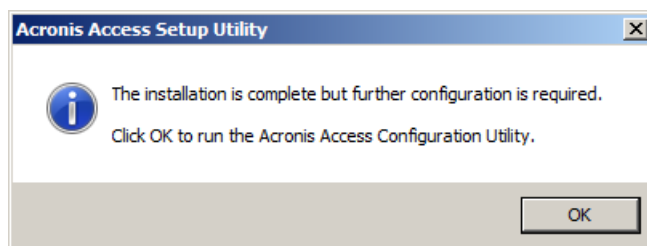
2. Copy the **acronisaccess.cfg** file and paste it in a safe location.

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**.



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.

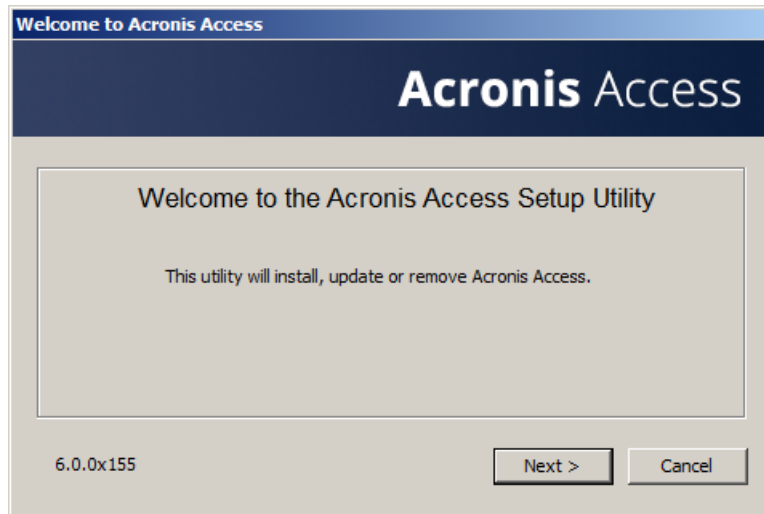
3.5 Upgrading Gateway Clusters

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. 58) article and for each Gateway, you will need to do the following procedure.

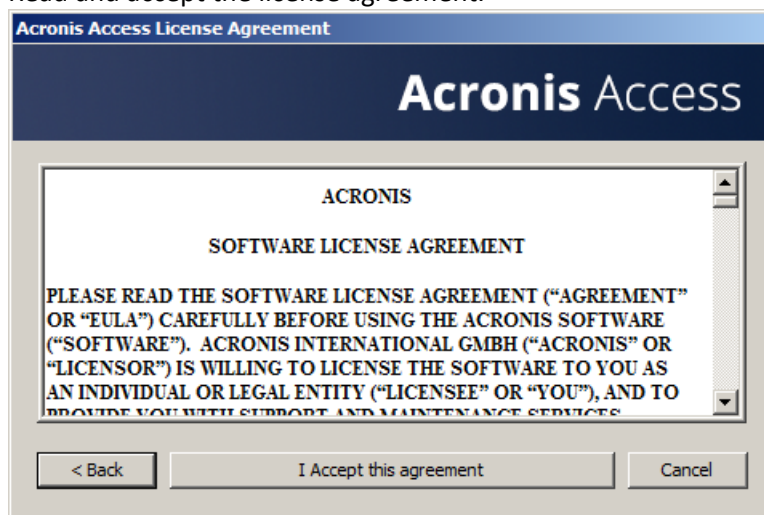
For information on upgrading a Microsoft Failover Clustering configuration, visit the Supplemental Material section.

Upgrading a Gateway Server

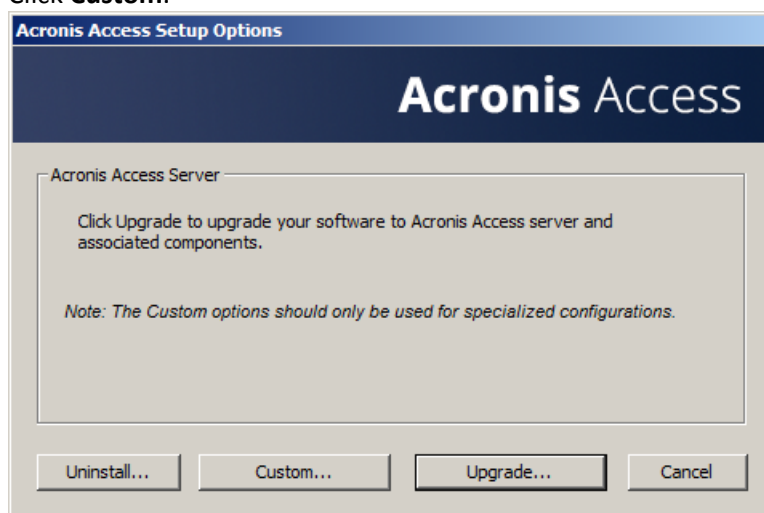
1. Run the Acronis Access installer on the desired server.
2. Press **Next** on the Welcome screen.



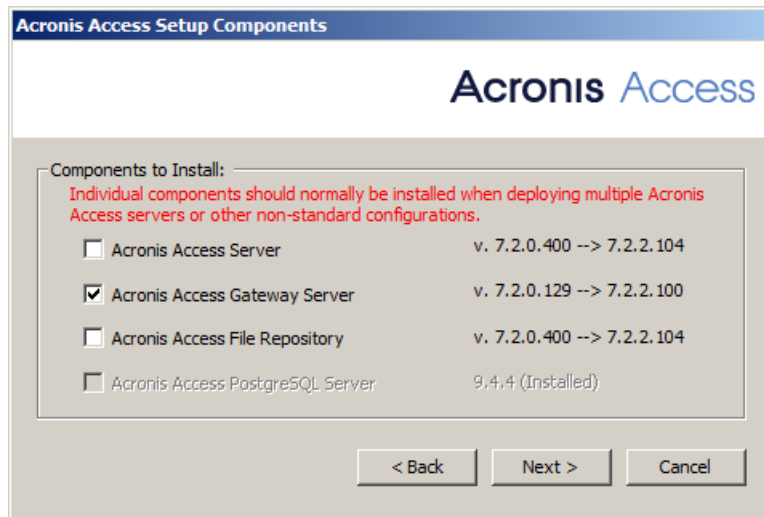
3. Read and accept the license agreement.



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.

3.6 Upgrading Load-balanced configurations

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

Stop all Acronis Access services on all nodes

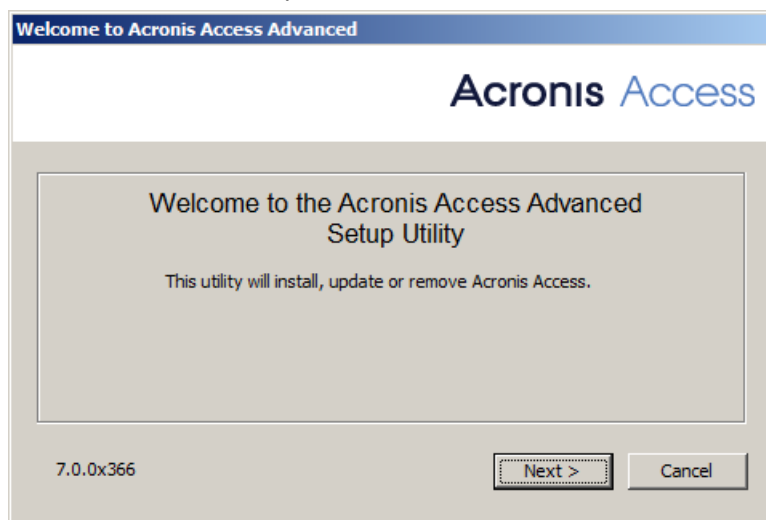
1. Stop all Acronis Access services on all nodes. This includes the Access Tomcat service, the Access Gateway Service, the Access PostgreSQL service and the File Repository service, depending on what you have installed on each machine.

It is vital that all Access Tomcat services are stopped before you upgrade. We recommend stopping the other services as well as a precaution.

2. Pick a node that will act as the primary and copy to it the installer for the new version of Acronis Access that you wish to upgrade to. This node is Primary only in the sense that it will be upgraded first and it will migrate any changes/settings to the other servers.

Upgrade the Primary node of Acronis Access services and verify they work

1. On the selected Primary node, start the Acronis Access installer.



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

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

4. Press Install and let the installer finish and launch the the Configuration Utility.

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

5. Once the Configuration Utility starts all the necessary services, verify that Acronis Access on this node works as expected.
6. Leave this instance of Acronis Access running while you update all other nodes.

Upgrading all other nodes

Once you have successfully updated the Primary Acronis Access node, continue by upgrading the rest of the nodes.

1. Copy the Acronis Access installer to the desired node and start it.
2. Press Next on the Welcome screen and then Custom. This will allow you to upgrade only the necessary services that are already installed on the machine, without installing others.
3. Select any Acronis Access services that you wish to upgrade. Choose only the ones that are already present on the machine.

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

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

4. Press Install and let the installer finish and launch the the Configuration Utility.

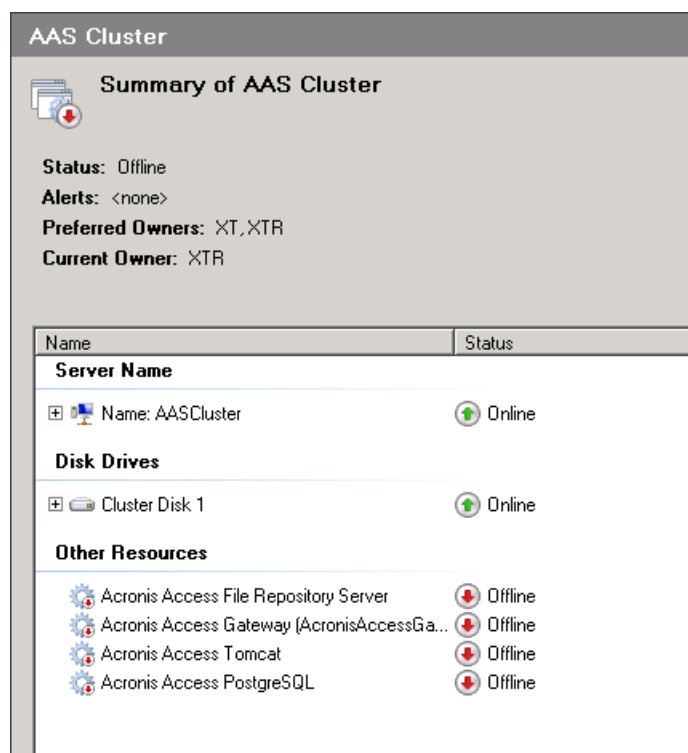
Note: Do not change any settings in the Configuration Utility! Changing settings can cause issues with your configuration.

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

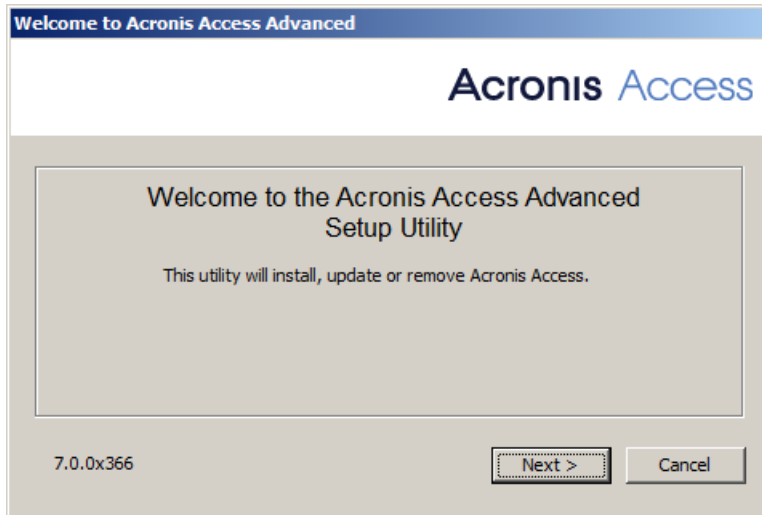
4 Upgrading Acronis Access on a Microsoft Failover Cluster

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

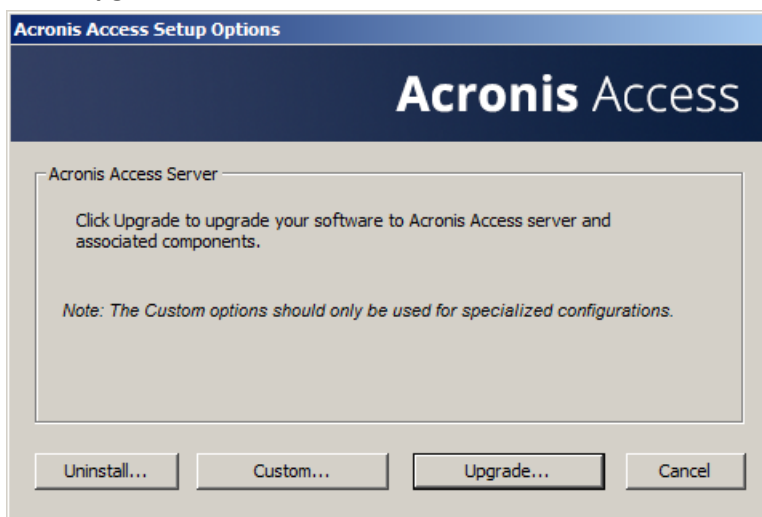
1. Go to the the active node.
2. Open the **Cluster Administrator/Failover Cluster Manager**.
3. Stop all of the Acronis Access services (including **postgres-some-version**). The shared disk must be online.



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



6. Press **Next** to begin.
7. Read and accept the license agreement.
8. Press **Upgrade**.



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



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

Warning! Do not bring the cluster group online!

12. Move the cluster group to the second node.
13. Complete the same installation procedure on the second node.
14. Bring all of the Acronis Access services online.

5 Upgrading from mobilEcho 4.5 on a Microsoft Failover Cluster

Warning! Acronis Access failover clustering is not supported by versions older than 5.0.3. If you're using an older version, you will have to upgrade to version 5.0.3 or newer before proceeding with any kind of cluster configurations.

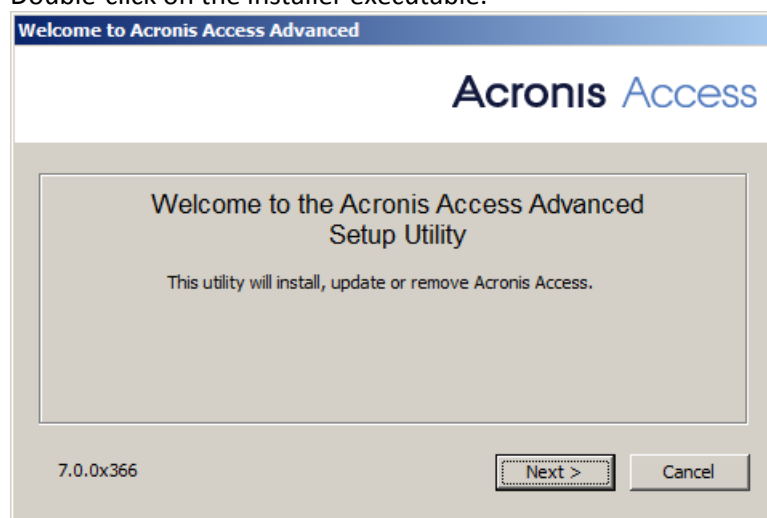
The guides listed below will help you upgrade your cluster from mobilEcho to Acronis Access.

In this section

Upgrading a mobilEcho server on a Windows 2003 Failover Cluster to Acronis Access	138
Upgrading a mobilEcho server on a Windows 2008 (R2) Failover Cluster to Acronis Access	147
Upgrading a mobilEcho server on a Windows 2012 (R2) Failover Cluster to Acronis Access	158

5.1 Upgrading a mobilEcho server on a Windows 2003 Failover Cluster to Acronis Access

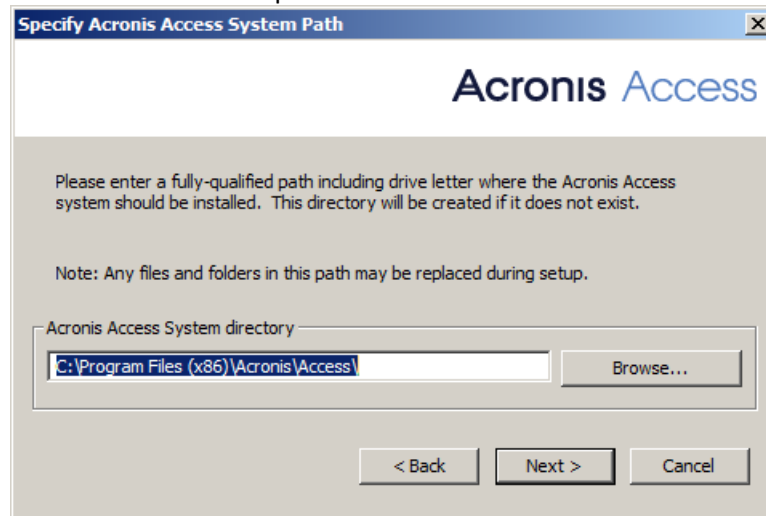
1. Open the **Cluster Administrator** and double-click on your service group.
 2. Delete the mobilEcho service resources.
-
- Note:** Do not bring the entire cluster group offline, just delete the mobilEcho service resources.
-
3. Launch the installer on the active node.
 4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
 5. Double-click on the installer executable.



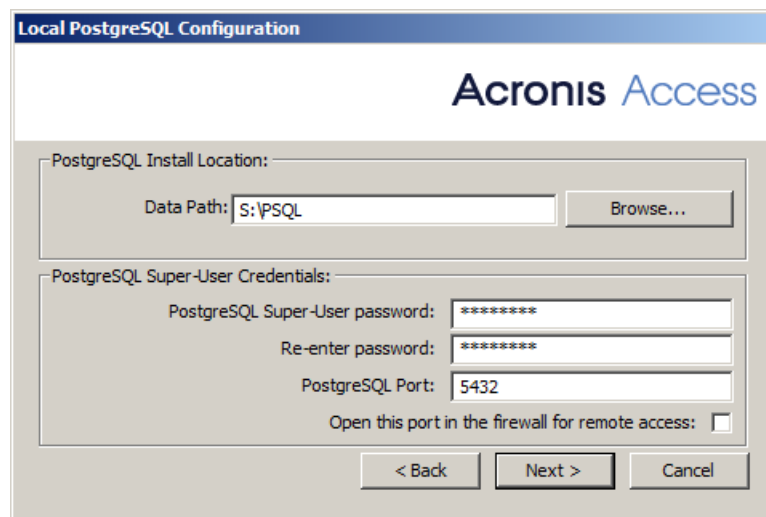
6. Press **Next** to begin.
7. Read and accept the license agreement.
8. Press **Install**.

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.

9. Either use the default path or select a new one for the Acronis Access main folder and press OK.



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



12. A window displaying all the components which will be installed appears. Press **OK** to continue.
13. When the Acronis Access installer finishes, press **Exit**. Navigate to your shared disk, locate and copy these 3 files: **production.sqlite3**, **mobileEcho_manager.cfg** and **priority.txt** (this one might not exist) and paste them to the Acronis Access installation directory, replacing the existing files.

Note: These files you should replace 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

Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\GroupLogic\mobileEcho Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/mobileEcho_cluster/database/'**).

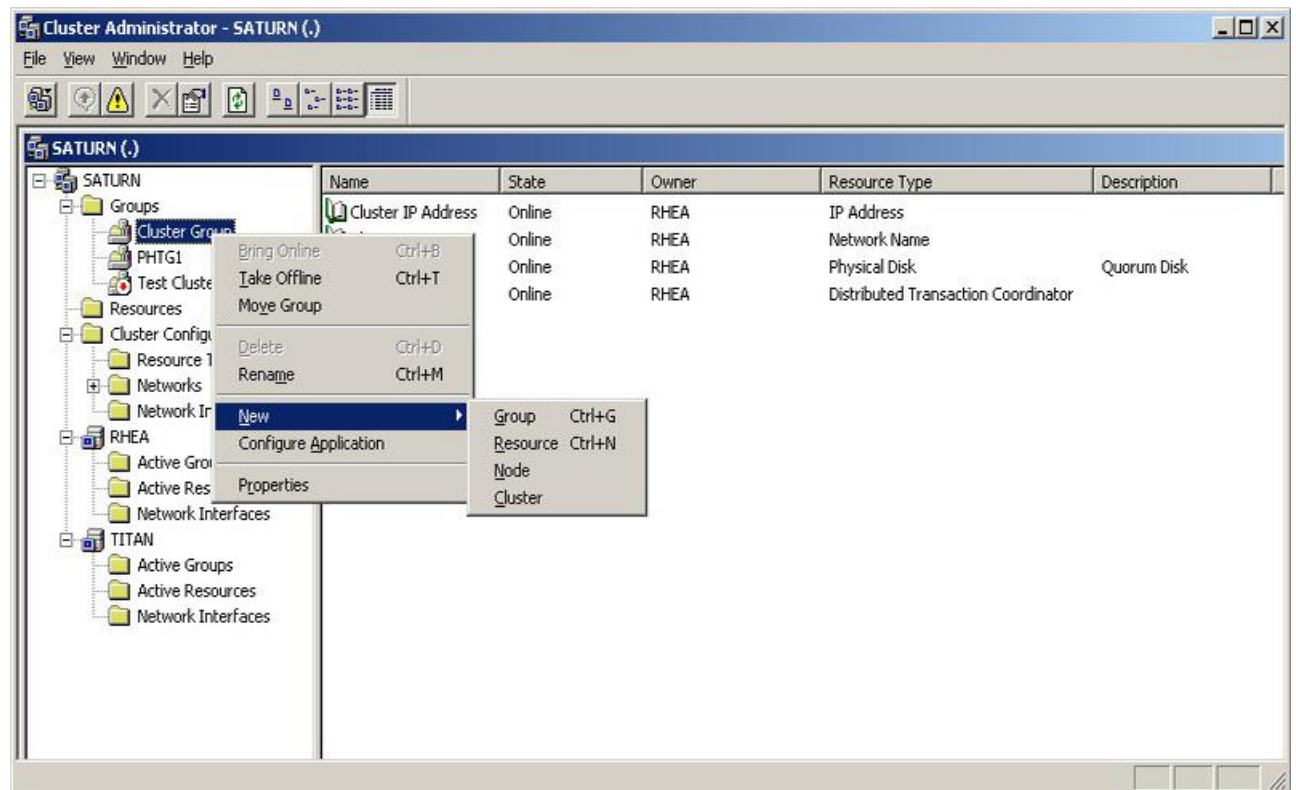
Note: Use slashes(/) as a path separator.

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

Adding all of the necessary services to the Acronis Access cluster group

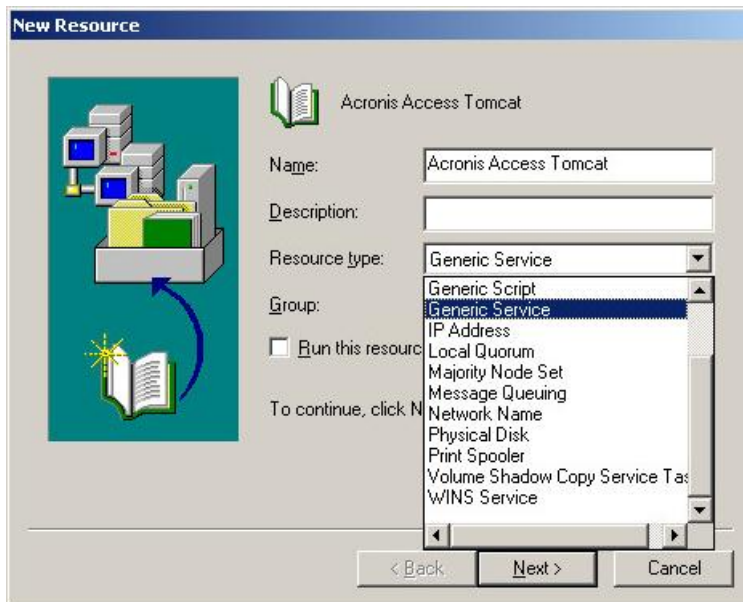
Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

1. Right-click on the Acronis Access cluster group.
2. Open **New** and select **Resource**.

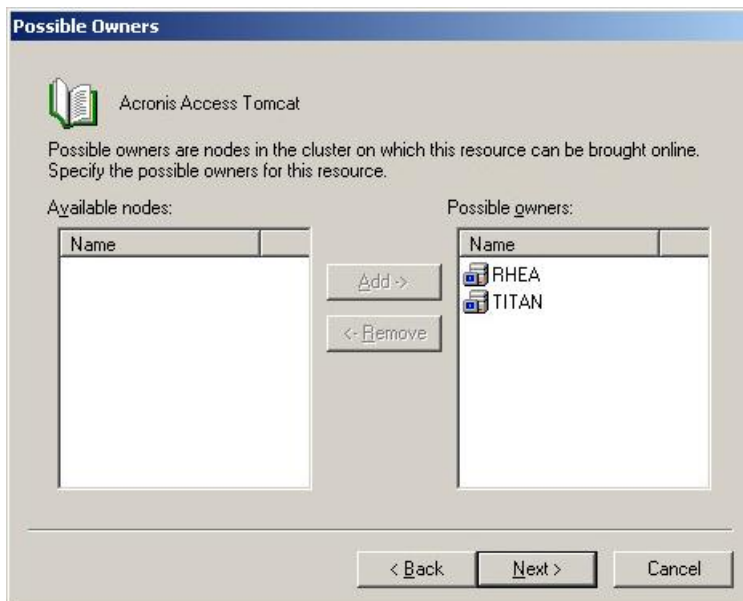


3. Enter a name for the service and select the correct cluster group.

4. From the **Resource Type** drop down menu select **Generic Service** and press **Next**.



5. Make sure both of your nodes are listed as **Possible owners** and press **Next**.



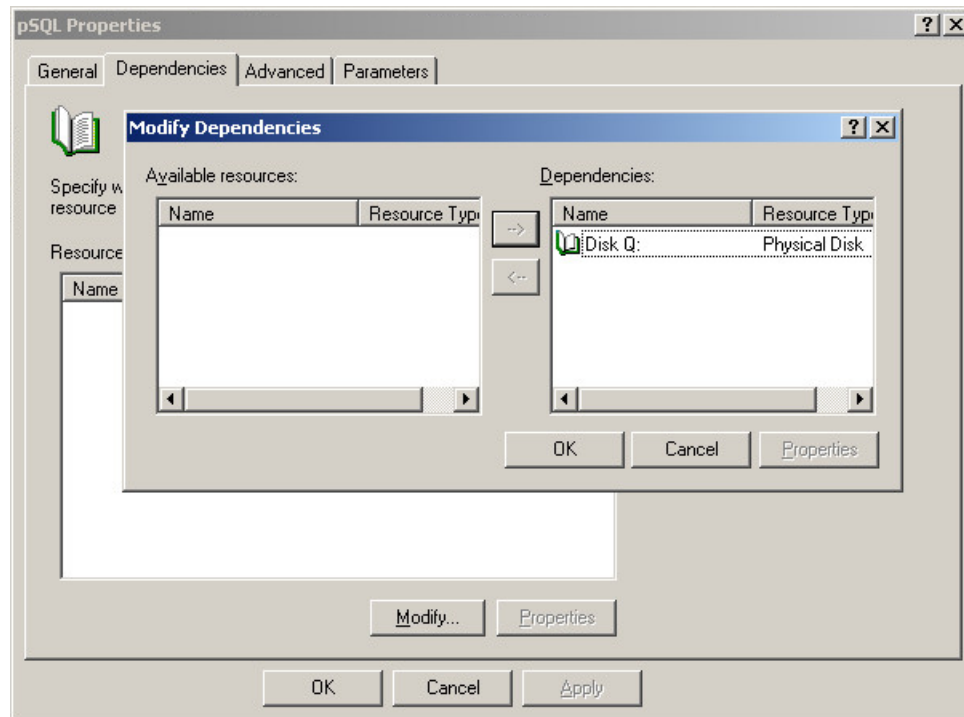
6. Skip the dependencies for now by pressing **Next**.
7. Enter the correct service name of the service you are adding (e.g. postgresql-x64-9.2) and press **Next**.
8. Skip the **Registry Replication** window for now by pressing **Next**.
9. Press **Finish** to complete the procedure.

Configuring dependencies

For PostgreSQL and Acronis Access File Repository do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Modify**.

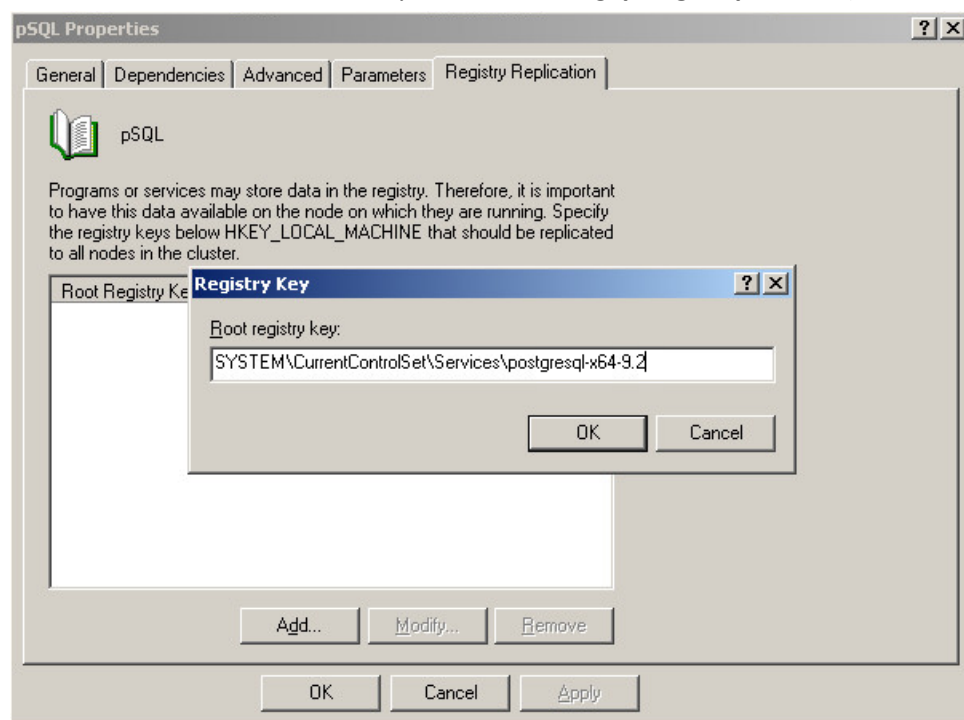
4. Select the shared disk you have added and move it to the right side.



5. Press **OK**.

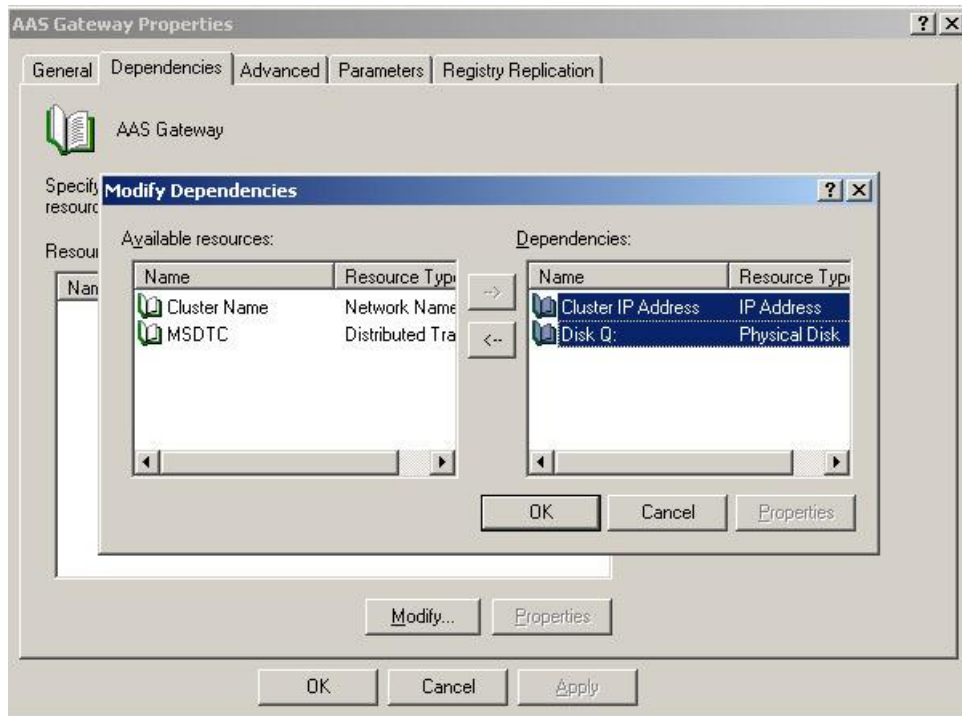
For PostgreSQL also do the following:

1. Click on the **Registry Replication** tab.
2. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL (For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)



For the Acronis Access Gateway Server service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Modify**.
4. Select the **IP Address** and **Physical disk** and move them to the right side.

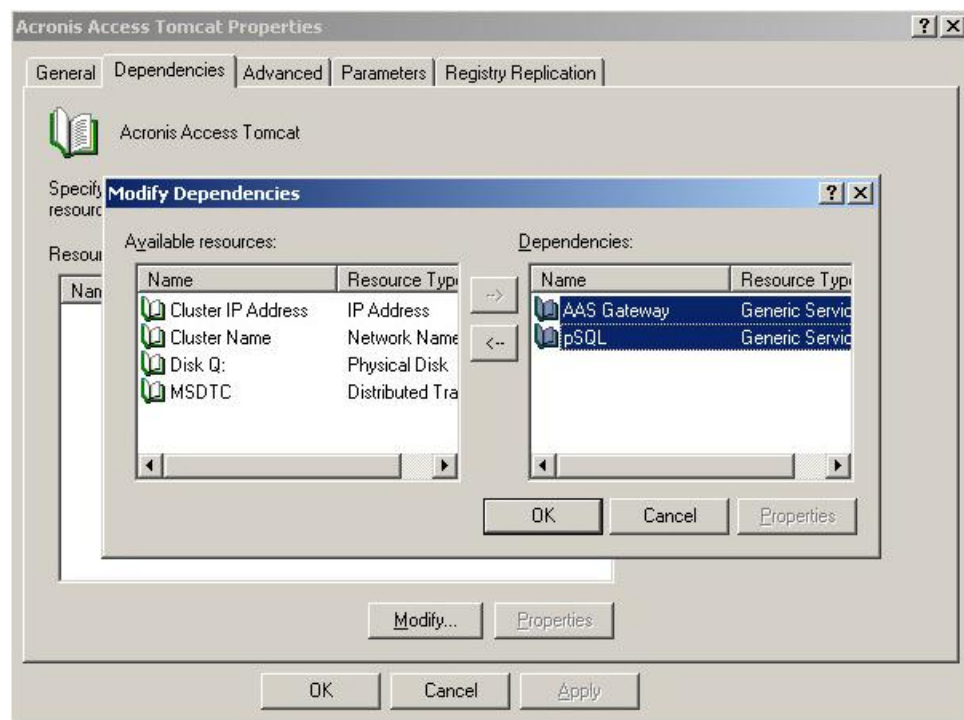


5. Press **OK**.

For the Acronis Access Tomcat service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Modify**.

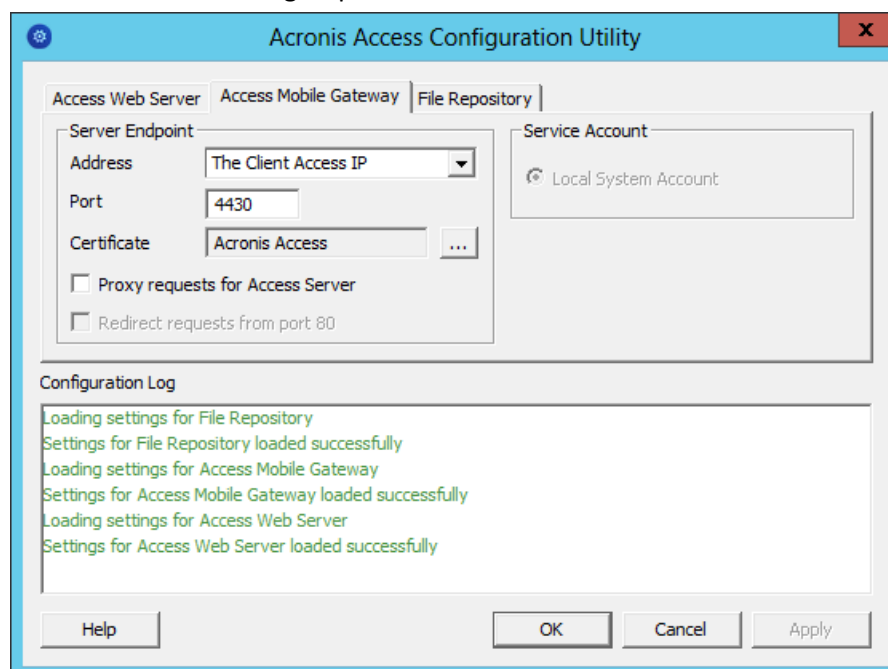
4. Select the PostgreSQL and Acronis Access Gateway Server services and move them to the right side.



5. Press **OK**.

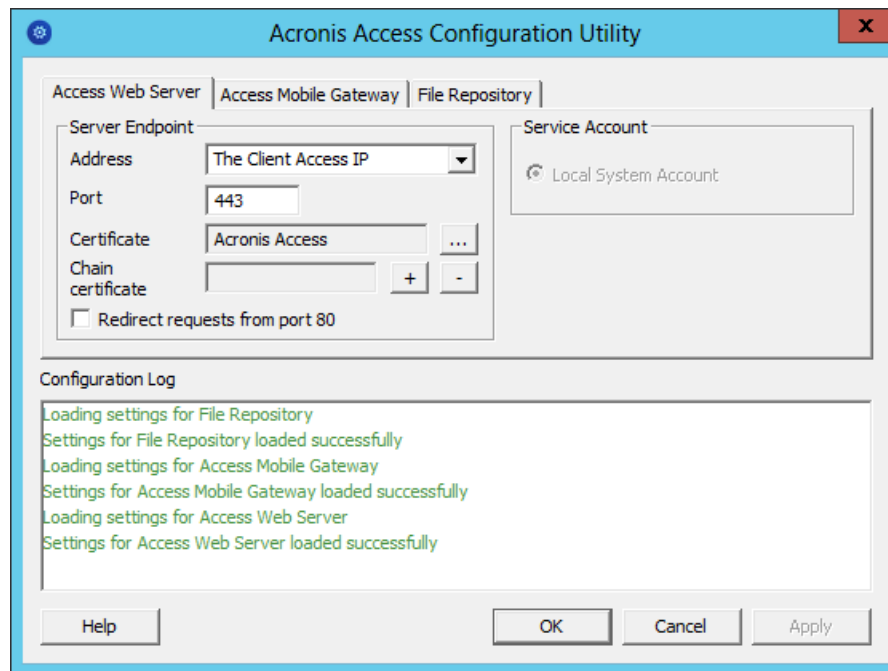
Bringing the cluster group online and using the Configuration Utility

1. Right-click on the cluster group and press **Bring online**.
2. Launch the Configuration Utility. On an upgrade from mobilEcho, this is generally located at **C:\Program Files (x86)\GroupLogic\Configuration Utility**
3. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

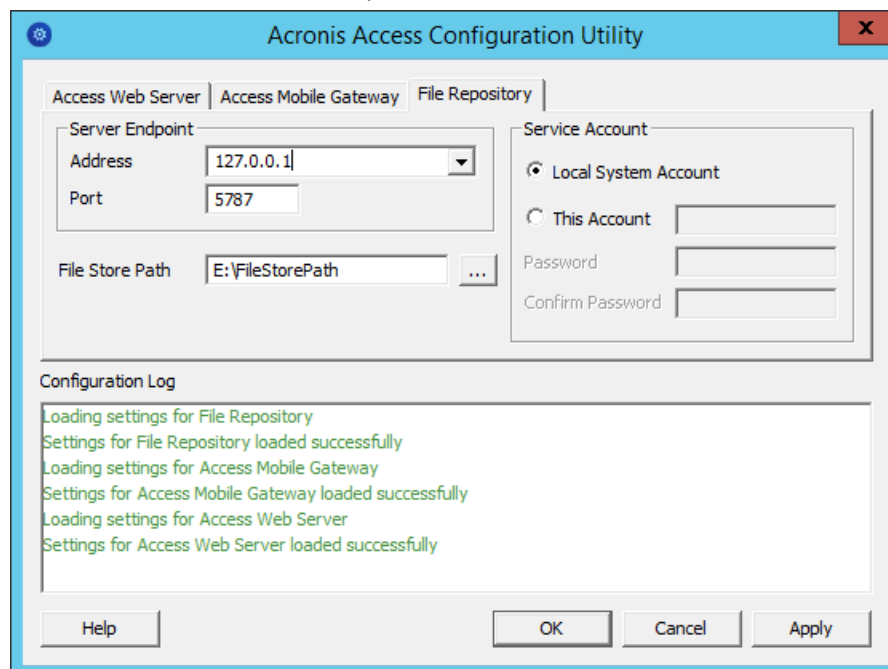


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



5. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

Installation and configuration on the second node

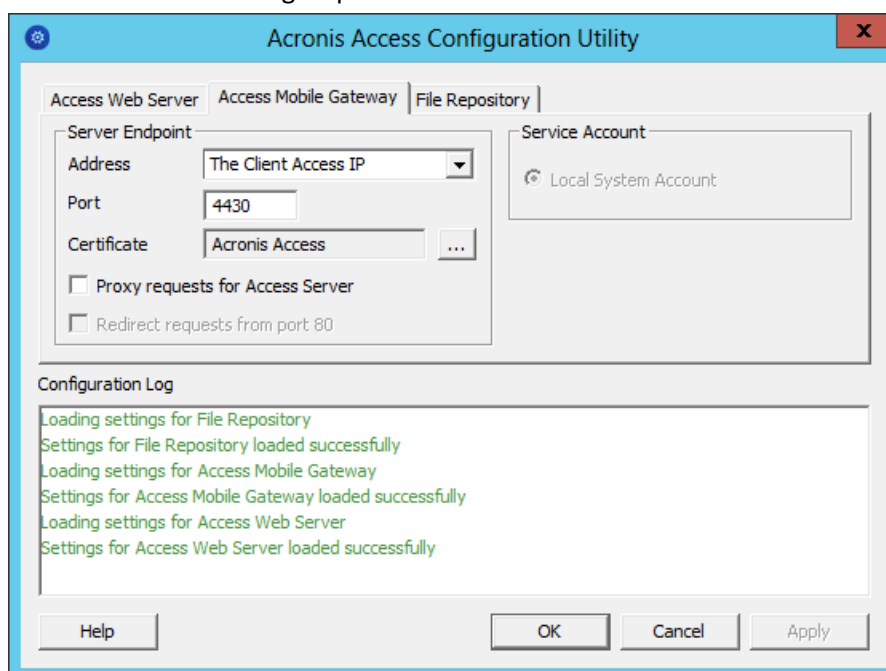
1. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
2. Install Acronis Access on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.
3. Complete the installation.
4. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\GroupLogic\mobileEcho Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/mobileEcho_cluster/database/'**).

Note: Use slashes(/) as a path separator.

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

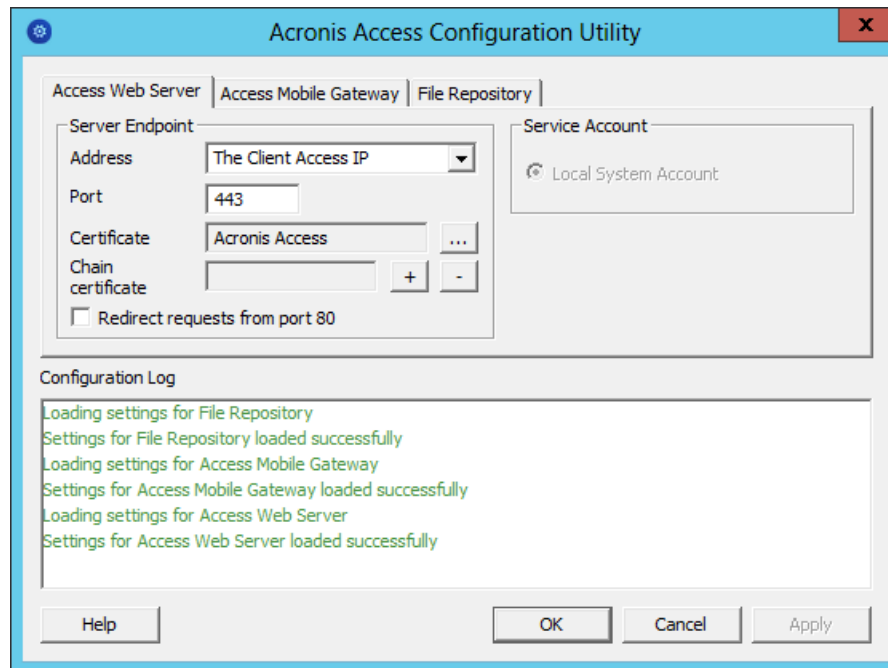
Note: The path should match the path set on the first node.

5. Move the cluster group to the second node. To do so, right-click on the cluster group and click on **Move Group**.
6. Launch the Configuration Utility. On an upgrade from mobileEcho, this is generally located at **C:\Program Files (x86)\GroupLogic\Configuration Utility**
7. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

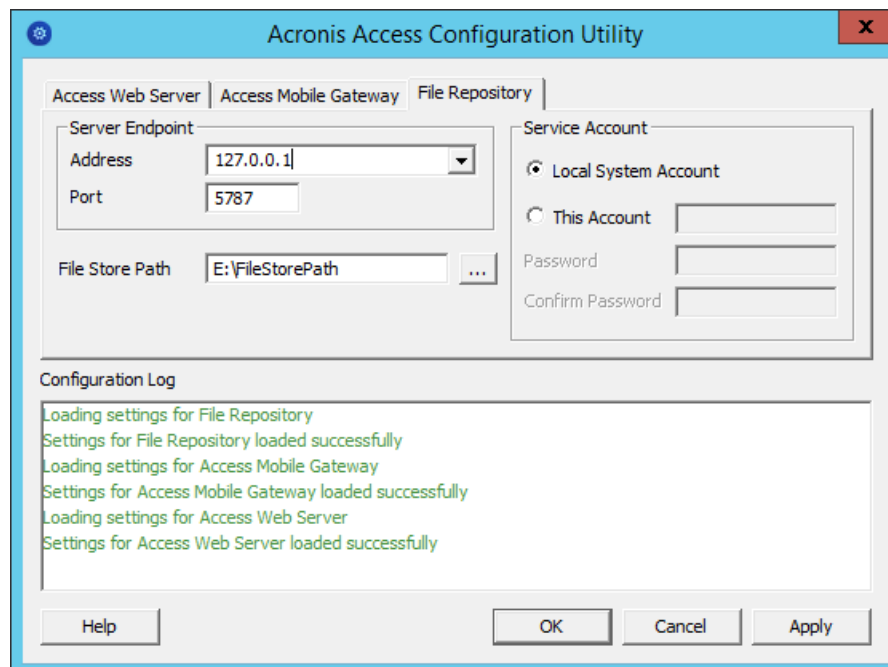


8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



9. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



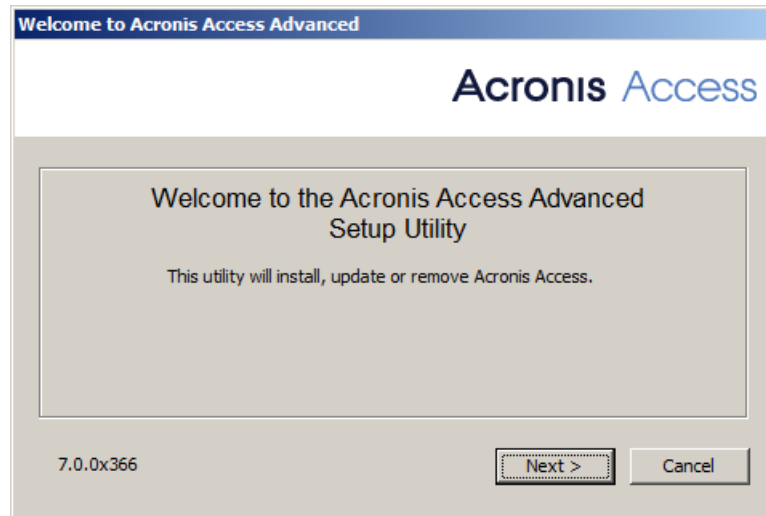
10. Click **OK** to complete the configuration and restart the services.

5.2 Upgrading a mobilEcho server on a Windows 2008 (R2) Failover Cluster to Acronis Access

1. Open the **Failover Cluster Manager** and double-click on your service group.
2. Delete the mobilEcho service resources.

Note: Do not bring the entire cluster group offline, just delete the mobilEcho service resources.

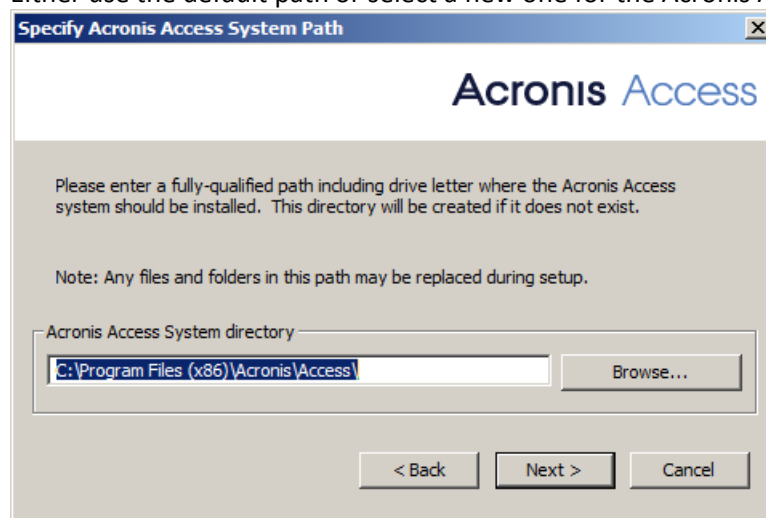
3. Launch the installer on the active node.
4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
5. Double-click on the installer executable.



6. Press **Next** to begin.
7. Read and accept the license agreement.
8. Press **Install**.

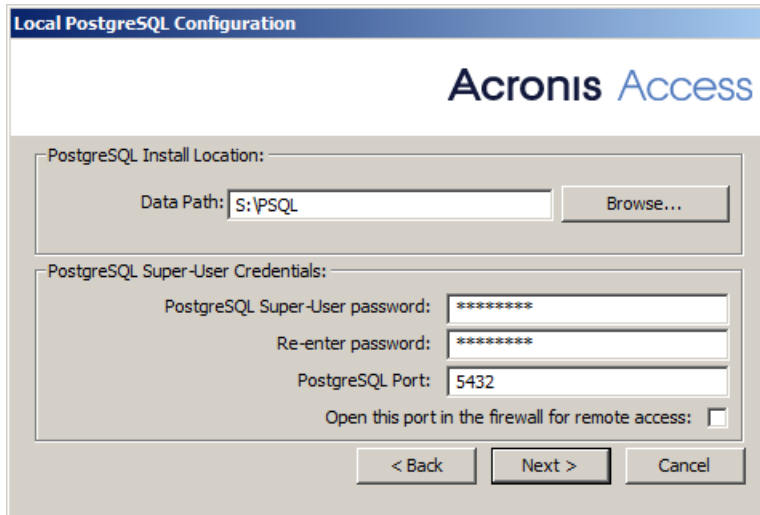
Note: If you're deploying multiple Acronis Access servers, or you are installing a non-standard configuration, you can select which components to install from the **Custom Install** button.

9. Either use the default path or select a new one for the Acronis Access main folder and press OK.



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

11. Choose a location on a shared disk for the **Postgres Data** folder and press **Next**.



12. A window displaying all the components which will be installed appears. Press **OK** to continue.
13. When the Acronis Access installer finishes, press **Exit**. Navigate to your shared disk, locate and copy these 3 files: **production.sqlite3**, **mobileEcho_manager.cfg** and **priority.txt** (this one might not exist) and paste them to the Acronis Access installation directory, replacing the existing files.

Note: These files you should replace 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

Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\GroupLogic\mobileEcho Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/mobileEcho_cluster/database/'**).

Note: Use slashes(/) as a path separator.

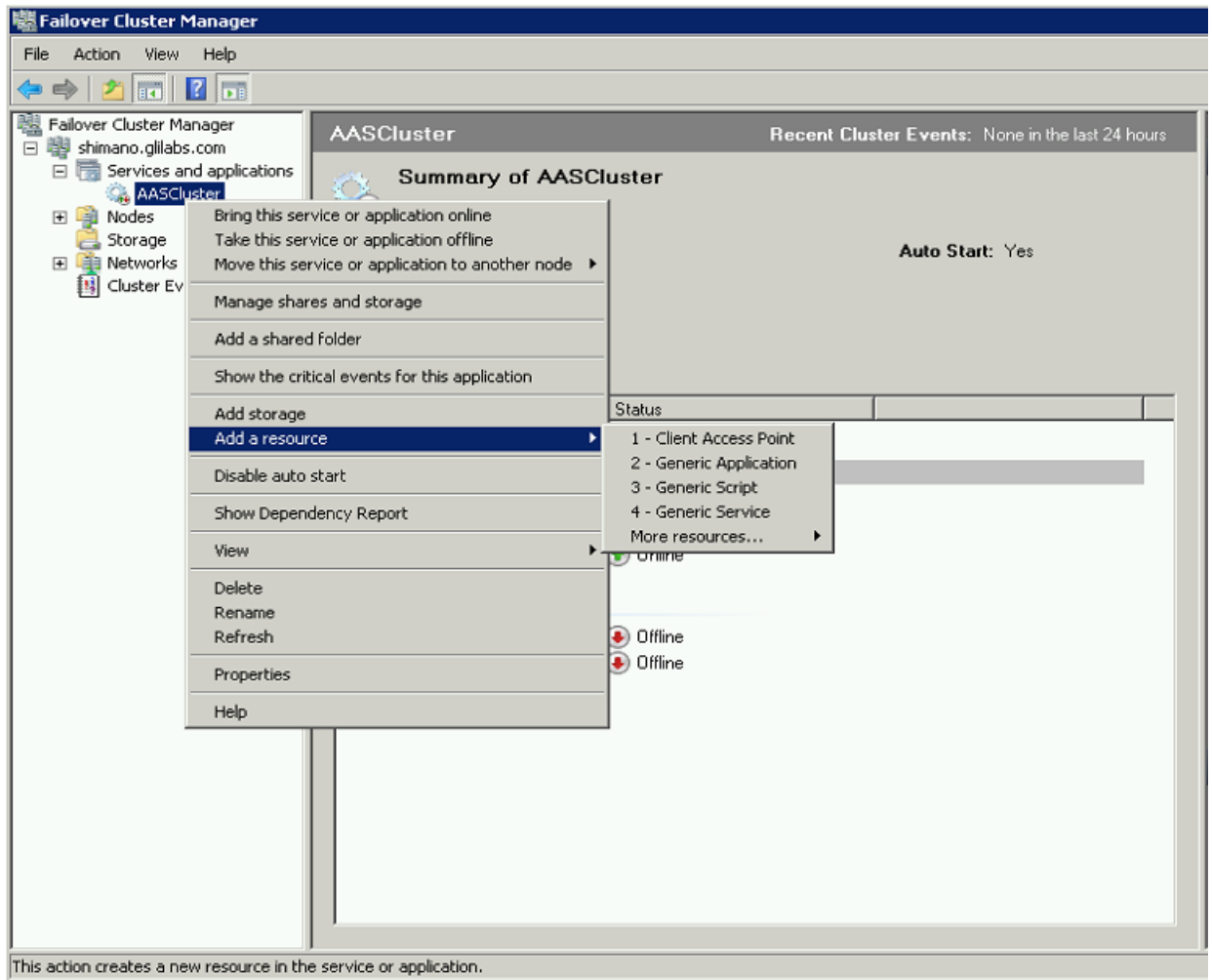
Note: You can copy the configured database.yml from the first node and paste it to the second node.

Adding all of the necessary services to the Acronis Access Service group

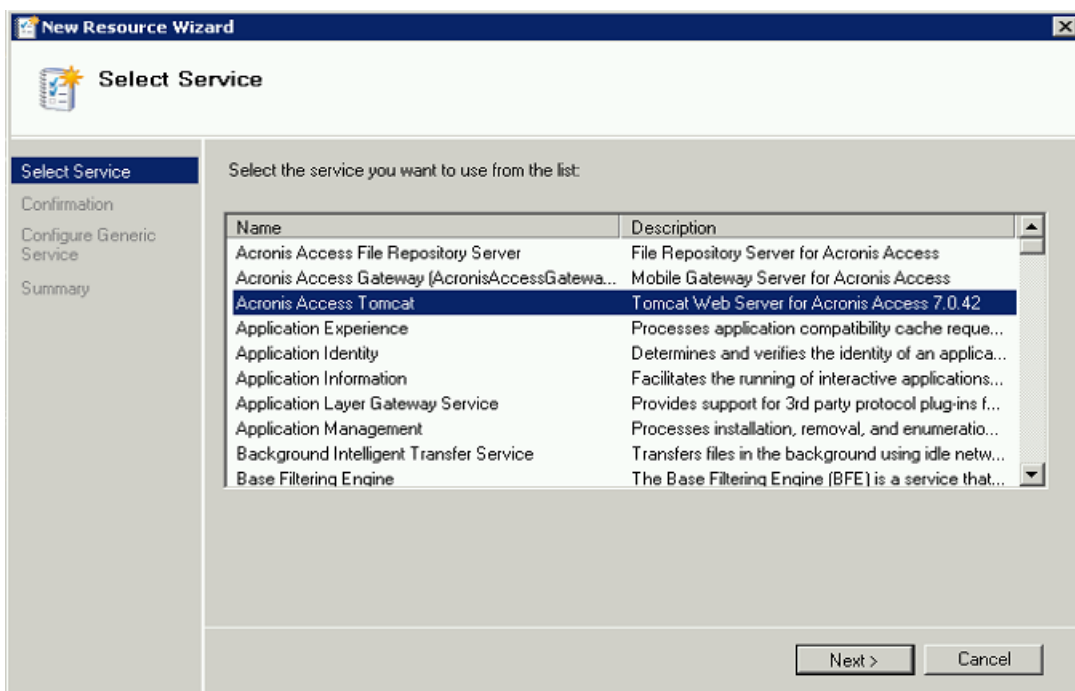
Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

1. Right-click on the Acronis Access service group and select **Add a resource**.

2. Select **Generic Service**.



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



4. On the confirmation window press **Next**.

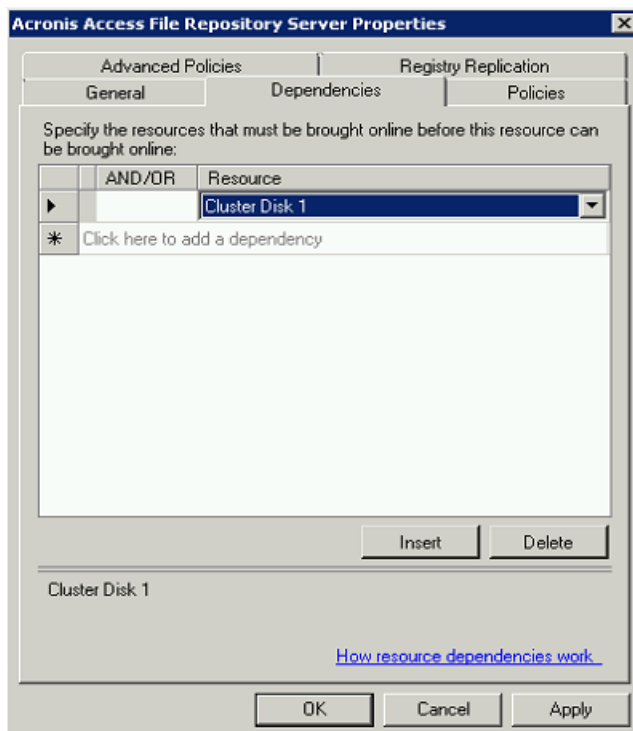
5. Press **Next** on the **Replicate Registry Settings** window.
6. On the summary window press **Finish**.

Configuring dependencies

1. Double click on the Acronis Access Service group.

For PostgreSQL and Acronis Access File Repository services do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the shared disk you have added.

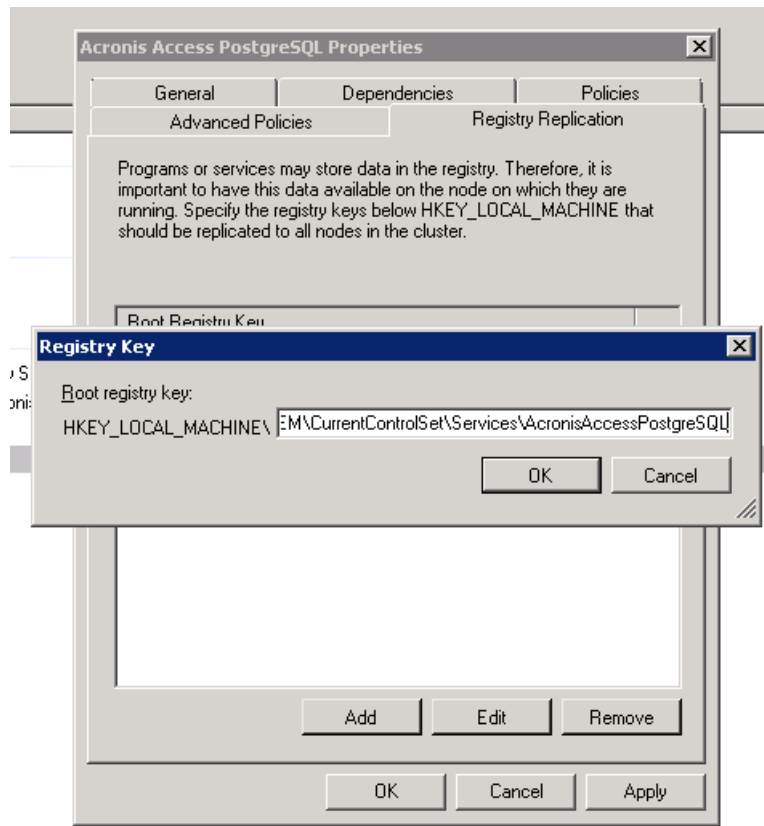


4. Press **Apply** and close the window.

For PostgreSQL also do the following:

1. Click on the **Registry Replication** tab.

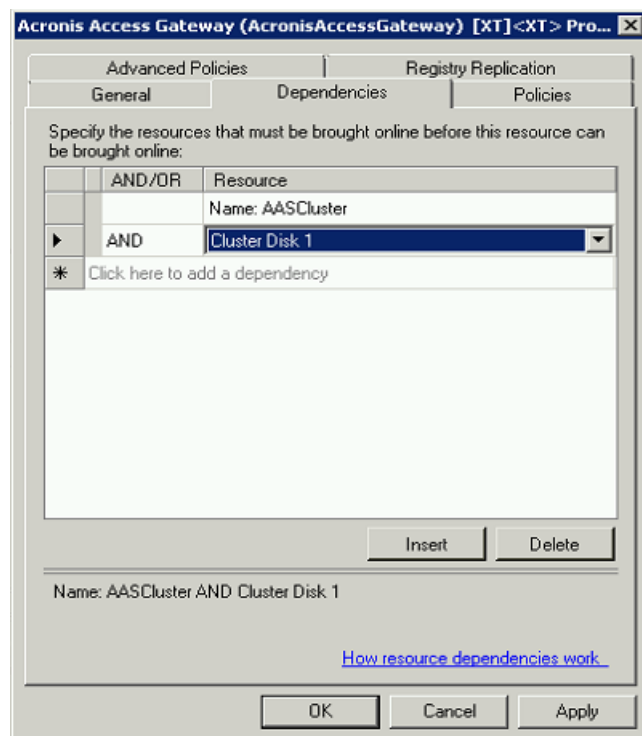
2. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL (For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)



For the Acronis Access Gateway Server service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.

- Click on **Resource** and select the shared disk you have added and the **Network Name** (this is the name of the Client access point).

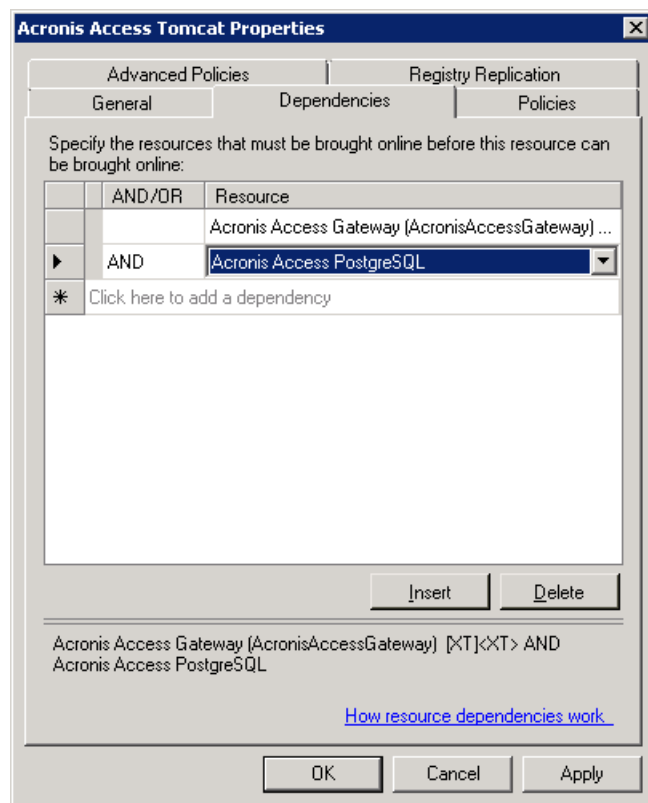


- Press **Apply** and close the window.

For the Acronis Access Tomcat service do the following:

- Right-click on the appropriate service and select **Properties**.
- Click on the **Dependencies** tab.

3. Click on **Resource** and select the PostgreSQL and Acronis Access Gateway Server services as dependencies. Press **Apply** and close the window.

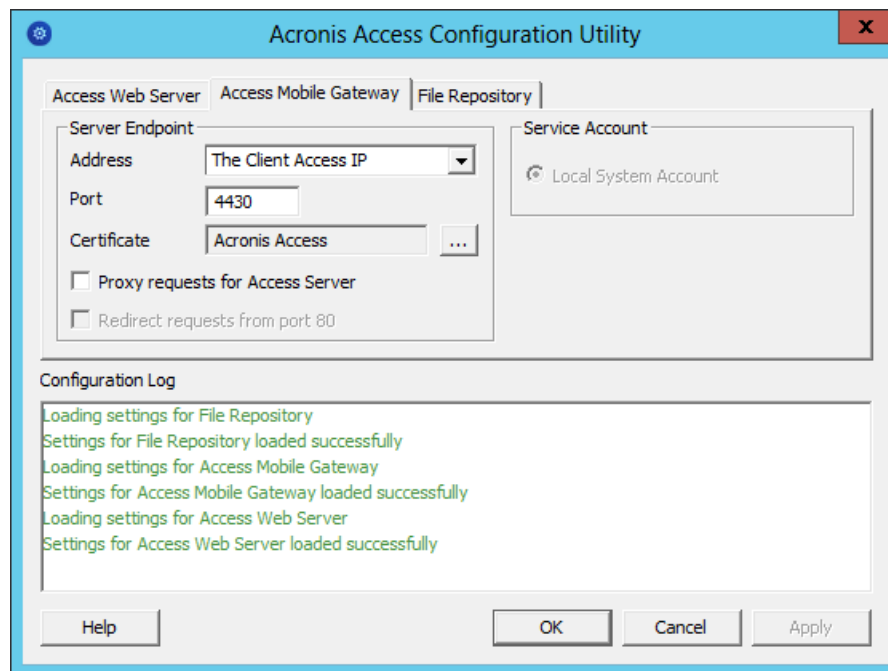


Note: If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access Service group and set it as a dependency for the network name.

Bringing the service group online and using the Configuration Utility

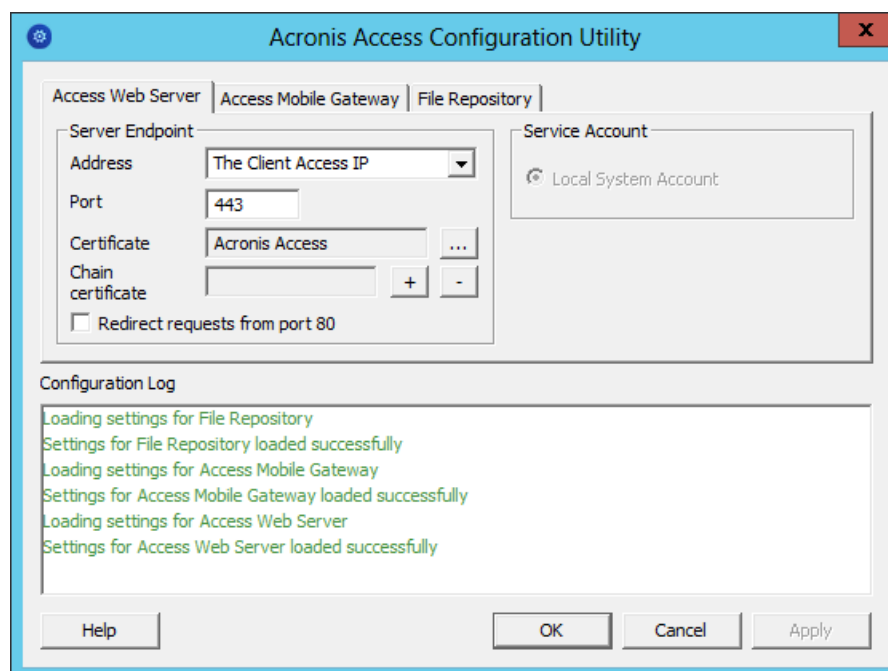
1. Right-click on the Acronis Access service group and press **Bring this application or service group online**.
2. Launch the Configuration Utility. On an upgrade from mobilEcho, this is generally located at **C:\Program Files (x86)\GroupLogic\Configuration Utility**

3. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

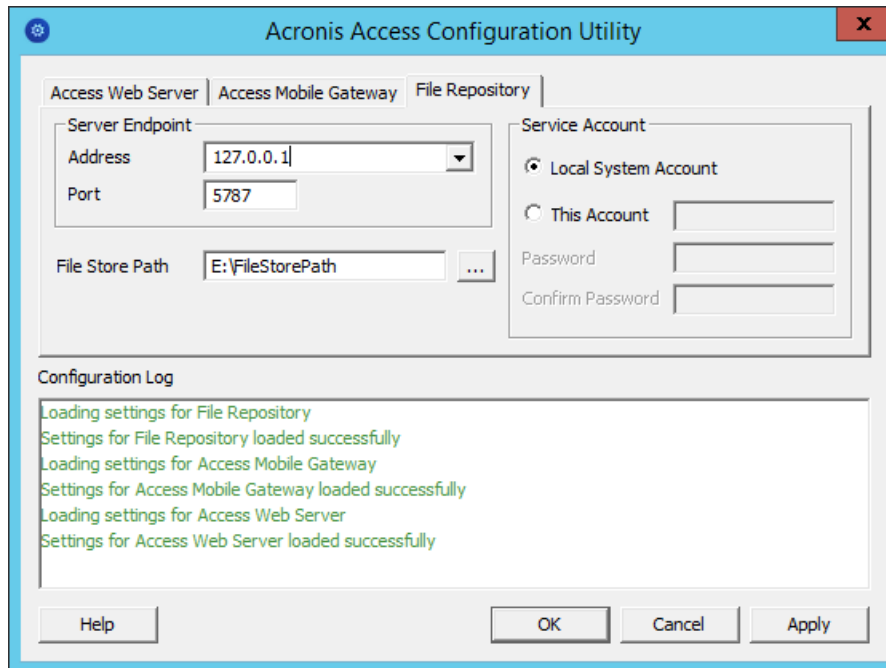


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



- Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

Installation and configuration on the second node

- Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
- Install Acronis Access on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.
- Complete the installation.
- Configure your Gateway Server's database to be on a location on a shared disk.
 - Navigate to **C:\Program Files (x86)\GroupLogic\mobileEcho Server**
 - Find the **database.yml** file and open it with a text editor.
 - Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/mobileEcho_cluster/database/'**).

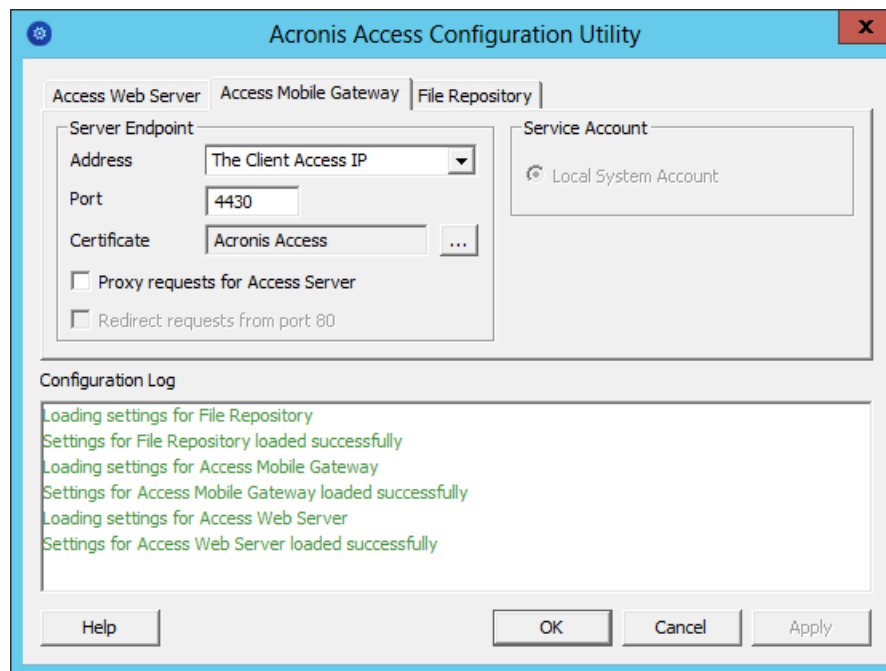
Note: Use slashes(/) as a path separator.

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

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

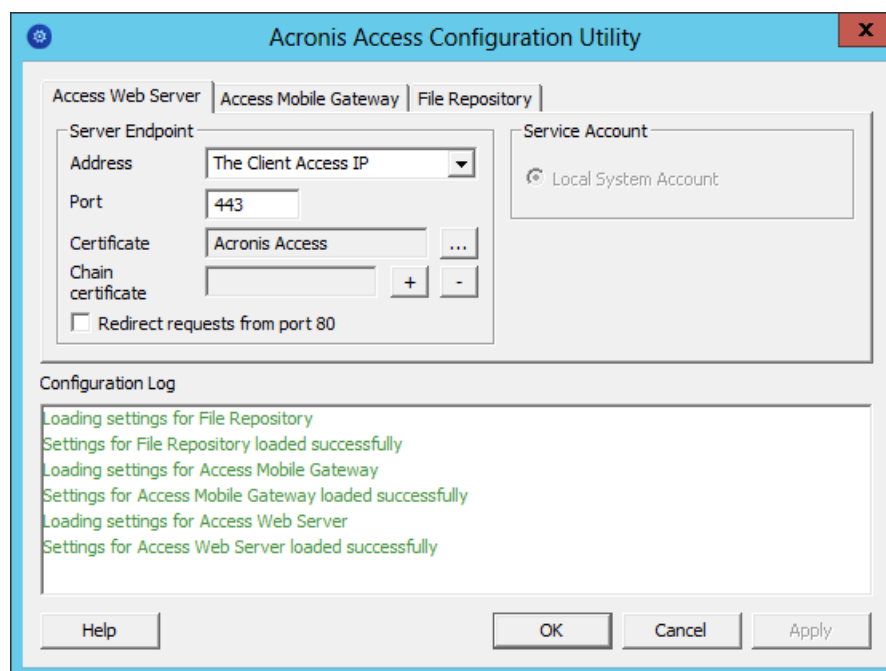
- Move the Acronis Access service group to the second node. To do so, right-click on the service group and click on **Move to the second node**.
- Launch the Configuration Utility. On an upgrade from mobileEcho, this is generally located at **C:\Program Files (x86)\GroupLogic\Configuration Utility**

7. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

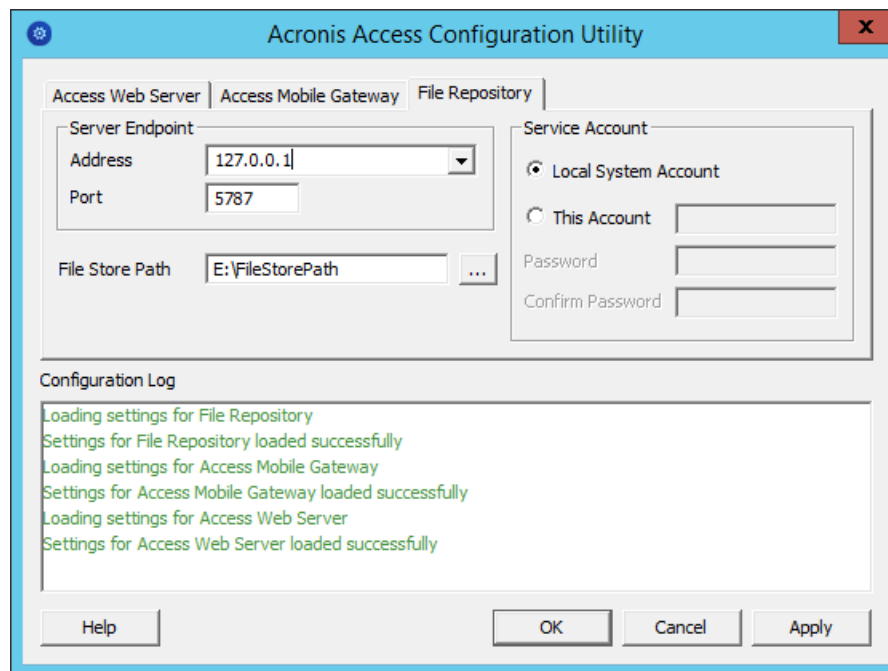


8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



- Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



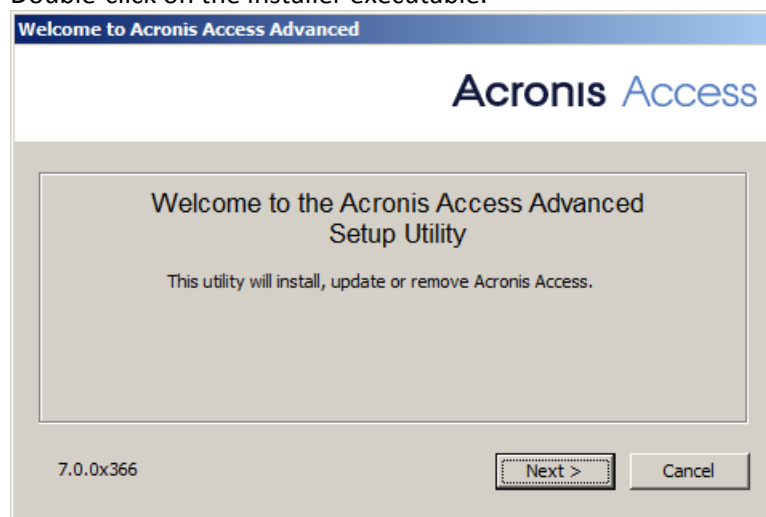
- Click **OK** to complete the configuration and restart the services.

5.3 Upgrading a mobilEcho server on a Windows 2012 (R2) Failover Cluster to Acronis Access

- Open the **Failover Cluster Manager** and double-click on your service group.
- Delete the mobilEcho service resources.

Note: Do not bring the entire cluster group offline, just delete the mobilEcho service resources.

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

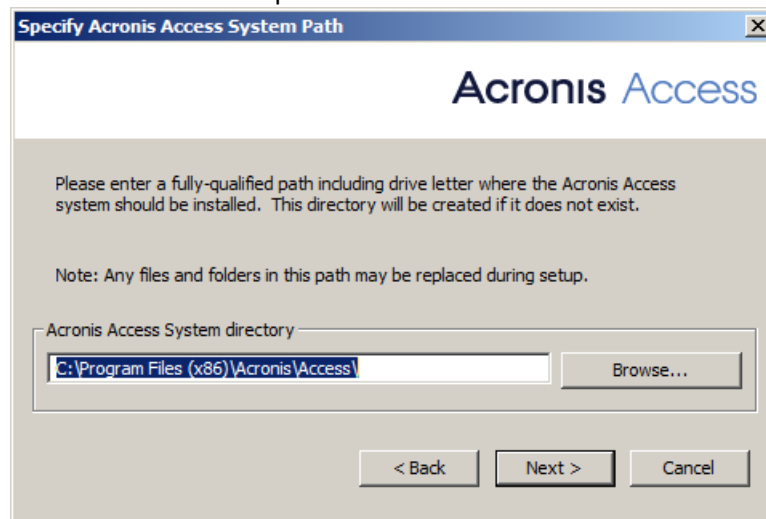


- Press **Next** to begin.
- Read and accept the license agreement.

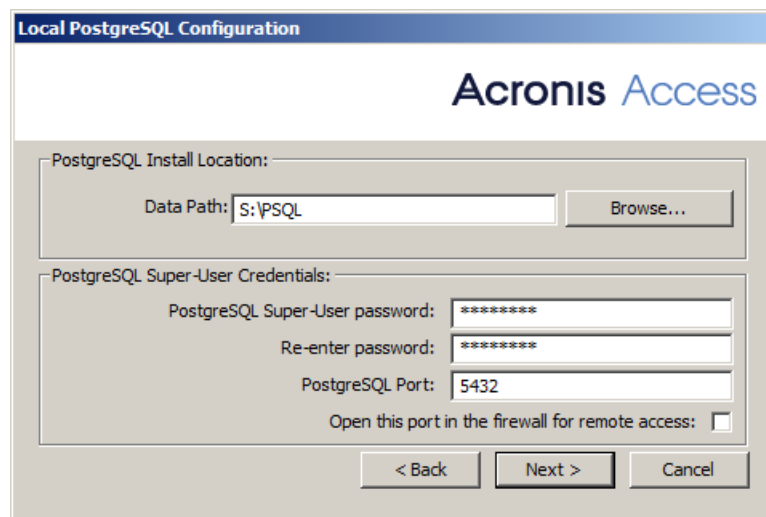
8. Press **Install**.

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.

9. Either use the default path or select a new one for the Acronis Access main folder and press OK.



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



12. A window displaying all the components which will be installed appears. Press **OK** to continue.
13. When the Acronis Access installer finishes, press **Exit**. Navigate to your shared disk, locate and copy these 3 files: **production.sqlite3**, **mobileEcho_manager.cfg** and **priority.txt** (this one might not exist) and paste them to the Acronis Access installation directory, replacing the existing files.

Note: These files you should replace 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

Configurations on the Active node

1. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\GroupLogic\mobileEcho Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/mobileEcho_cluster/database/'**).

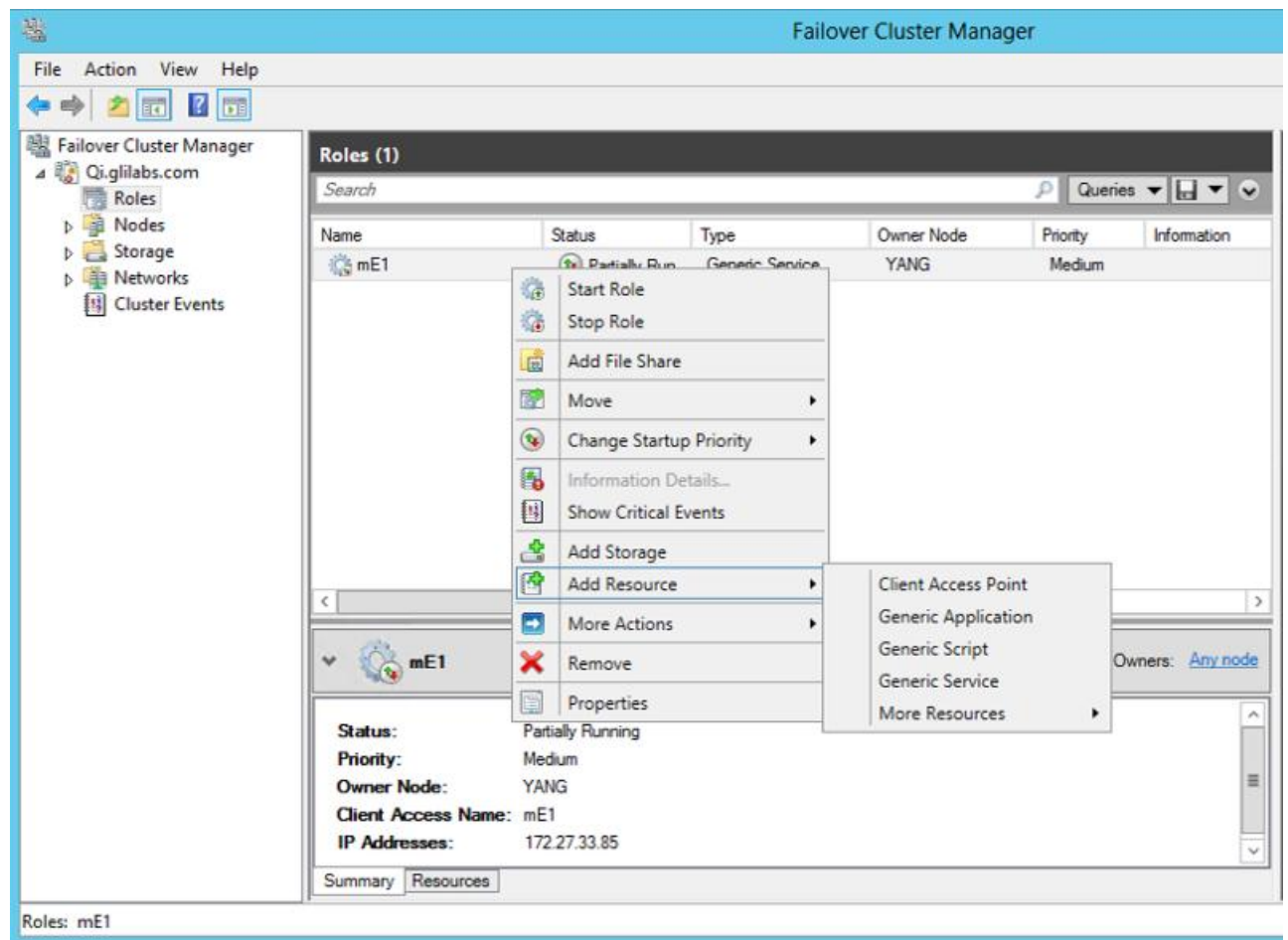
Note: Use slashes(/) as a path separator.

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

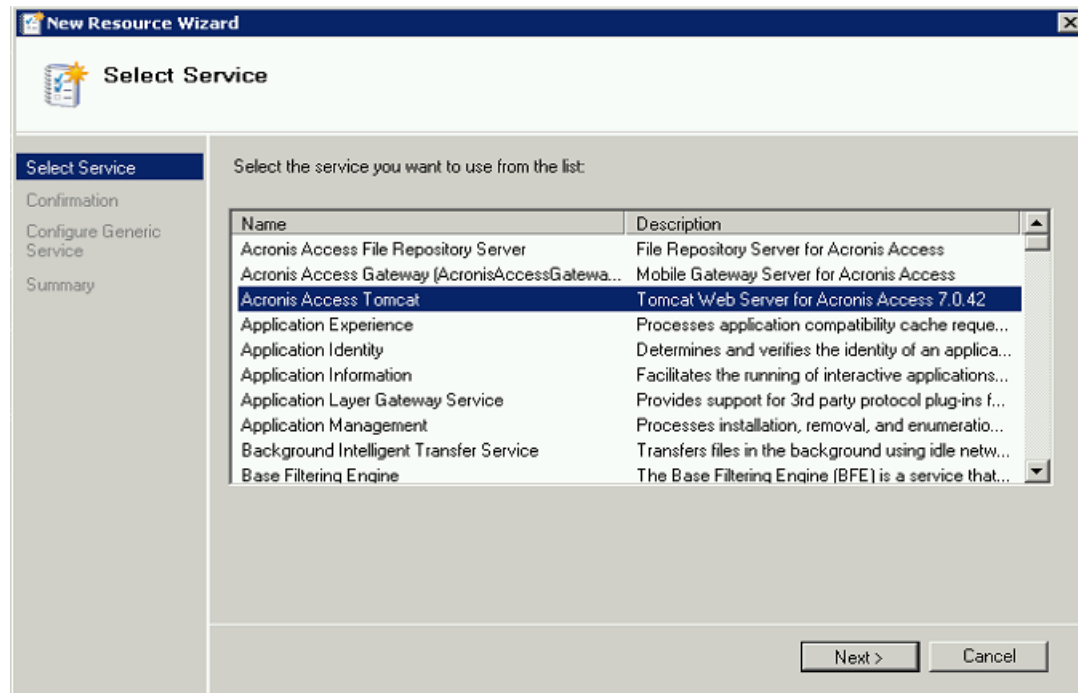
Adding all of the necessary services to the Acronis Access role

Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

1. Right-click on the Acronis Access role and select **Add a resource**.
2. Select **Generic Service**.



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

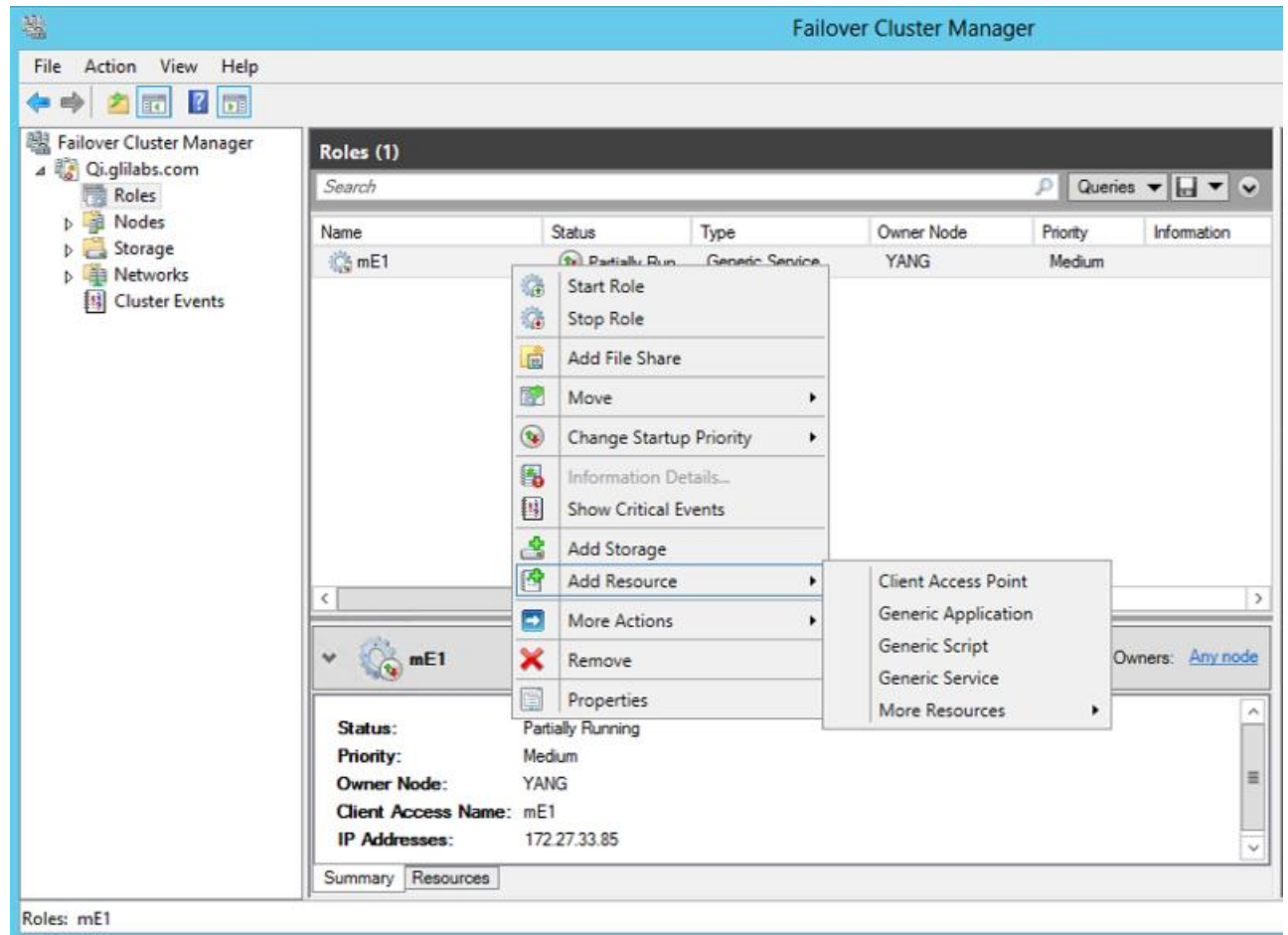


4. On the Confirmation window press **Next**.
5. On the summary window press **Finish**.

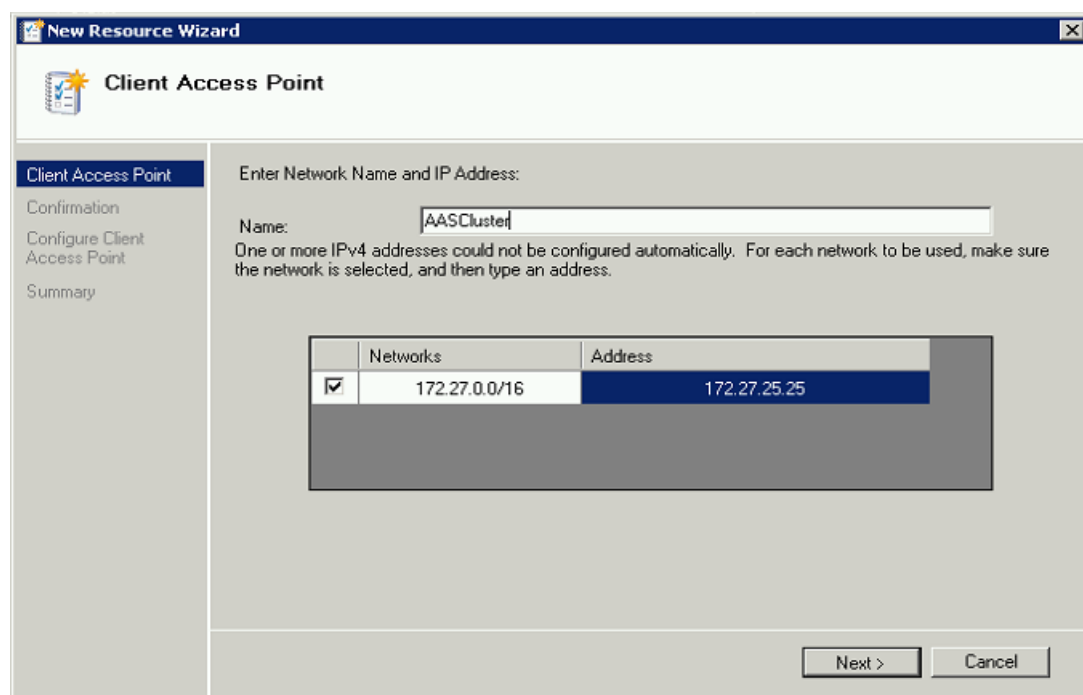
Setting an Access Point

1. Right-click on the Acronis Access role and select **Add a resource**.

2. Select **Client Access Point**.



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

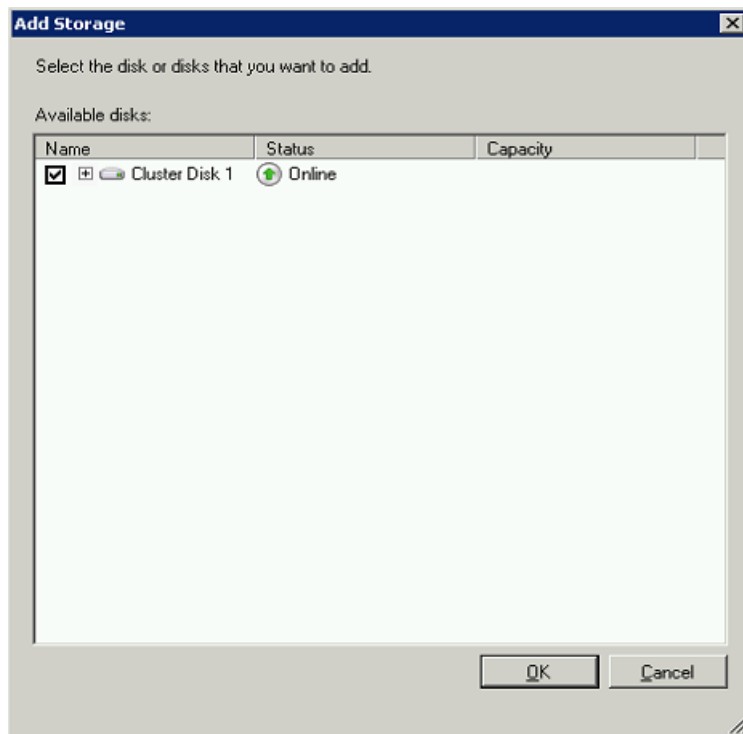


5. Enter the IP address and press **Next**.
6. On the Confirmation window press **Next**.

7. On the summary window press **Finish**.

Adding a shared disk

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



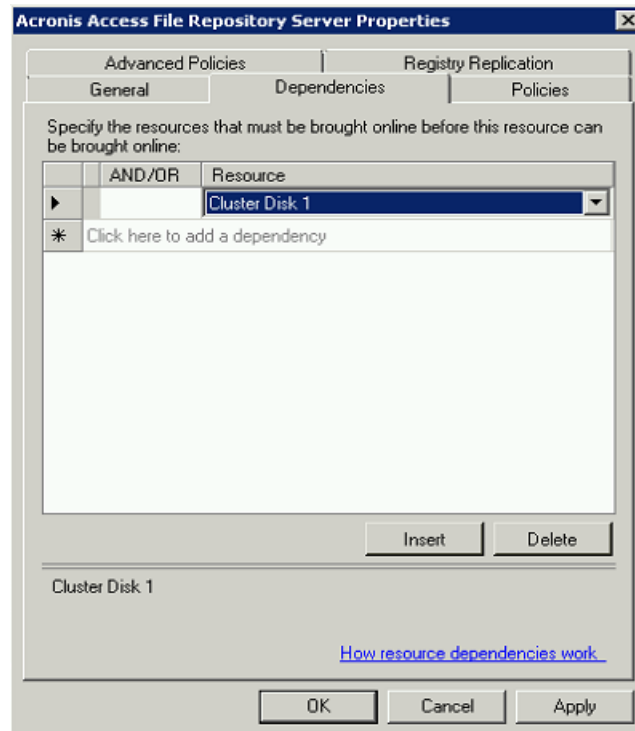
Configuring dependencies

1. Select the Acronis Access role and click on the **Resources** tab

For PostgreSQL and Acronis Access File Repository services do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.

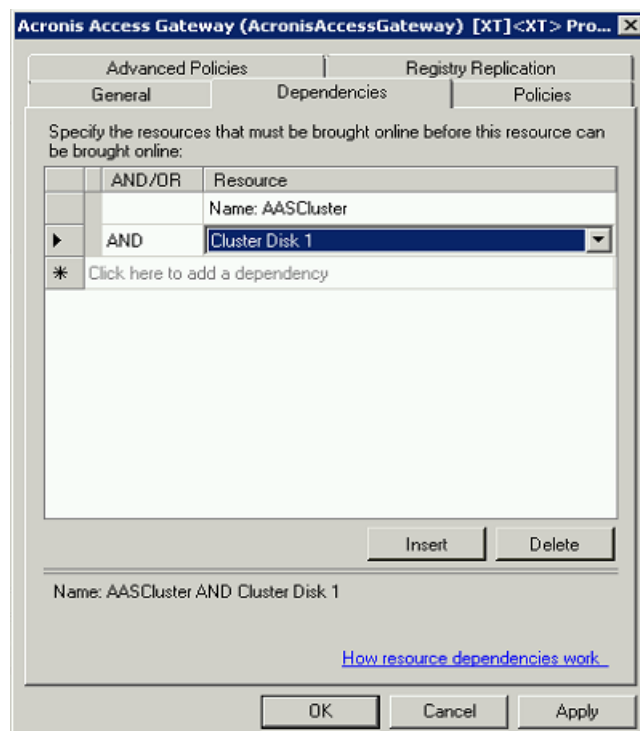
3. Click on **Resource** and select the shared disk you have added.



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

For the Acronis Access Gateway Server service do the following:

1. Right-click on the appropriate service and select **Properties**.
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the shared disk you have added and the **Network Name** (this is the name of the Client access point).

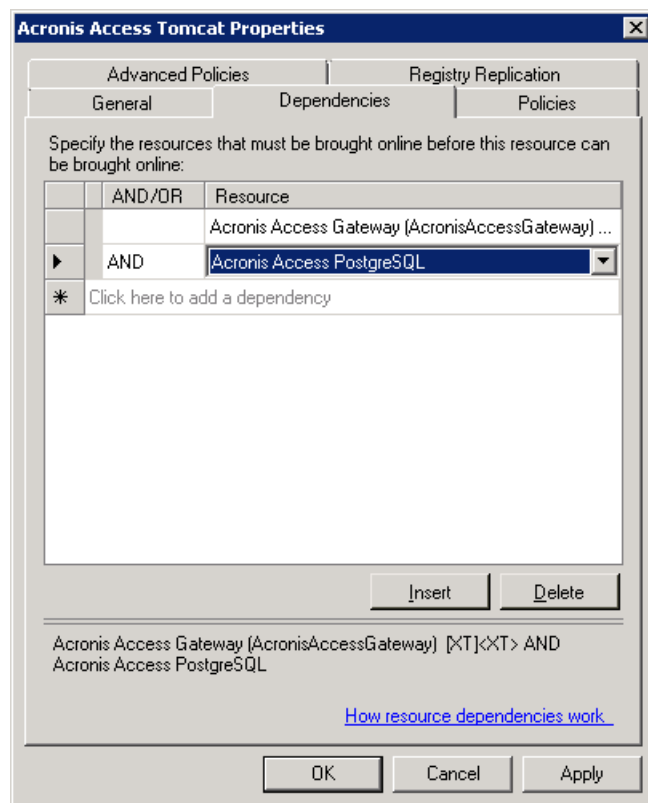


4. Press **Apply** and close the window.

For the Acronis Access Tomcat service do the following:

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

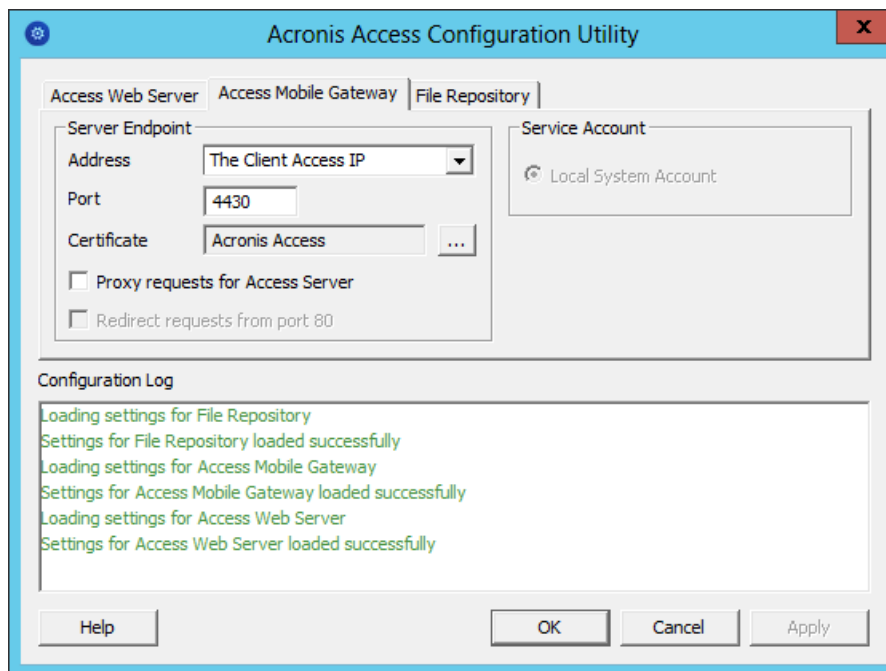
Note: If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access role and set it as a dependency for the network name.



Starting the role and using the Configuration Utility

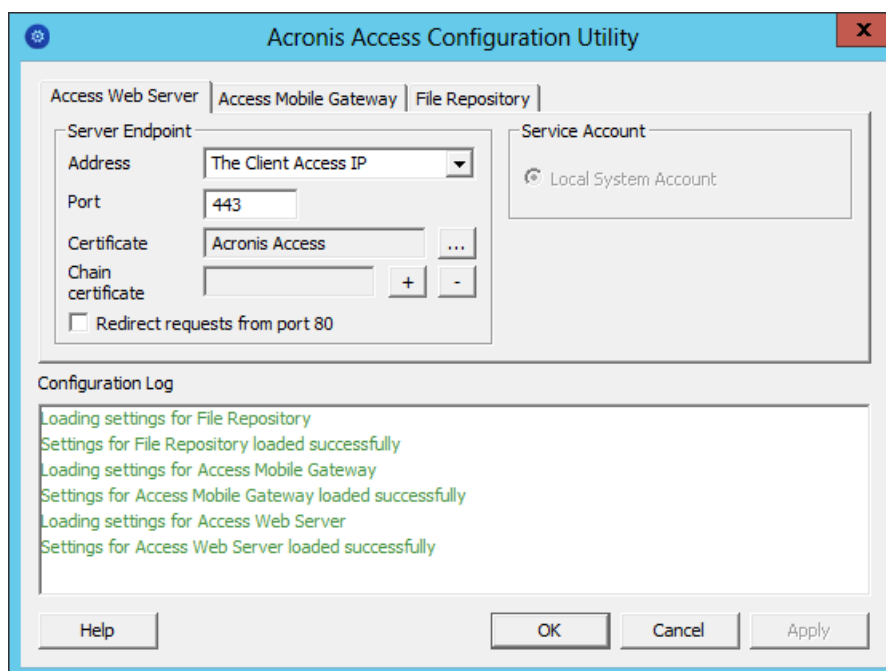
1. Right-click on the Acronis Access role and press **Start role**.
2. Launch the Configuration Utility. On an upgrade from mobilEcho, this is generally located at **C:\Program Files (x86)\GroupLogic\Configuration Utility**

3. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

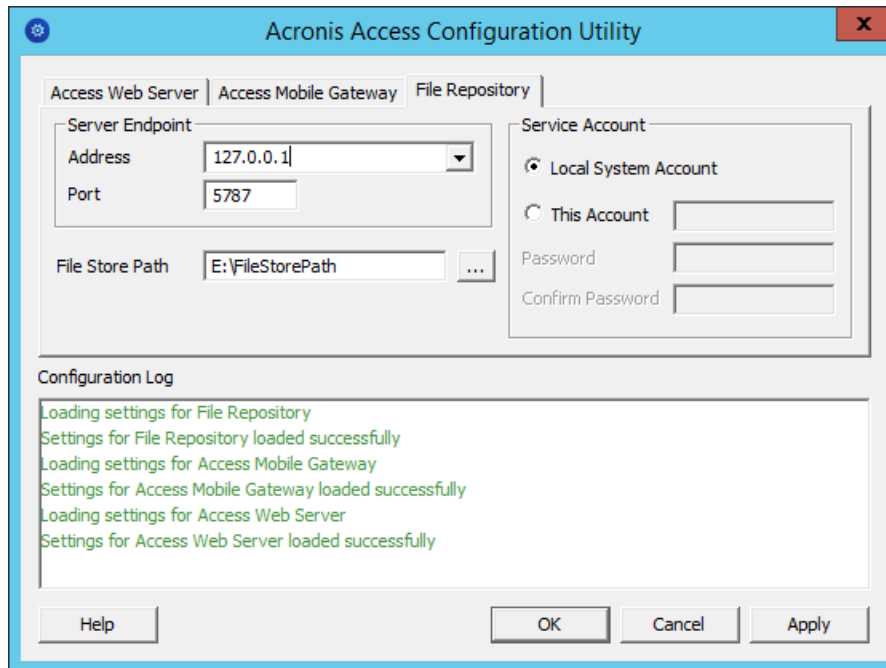


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



5. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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

Installation and configuration on the second node

1. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
2. Install Acronis Access on the second node, but this time use the default **Postgres Data** location and the same postgres user password as for the first node.
3. Complete the installation.
4. Configure your Gateway Server's database to be on a location on a shared disk.
 - a. Navigate to **C:\Program Files (x86)\GroupLogic\mobileEcho Server**
 - b. Find the **database.yml** file and open it with a text editor.
 - c. Find this line: **database_path: './database/'** and replace **./database/** with the path you want to use (e.g. **database_path: 'S:/mobileEcho_cluster/database/'**).

Note: Use slashes(/) as a path separator.

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

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

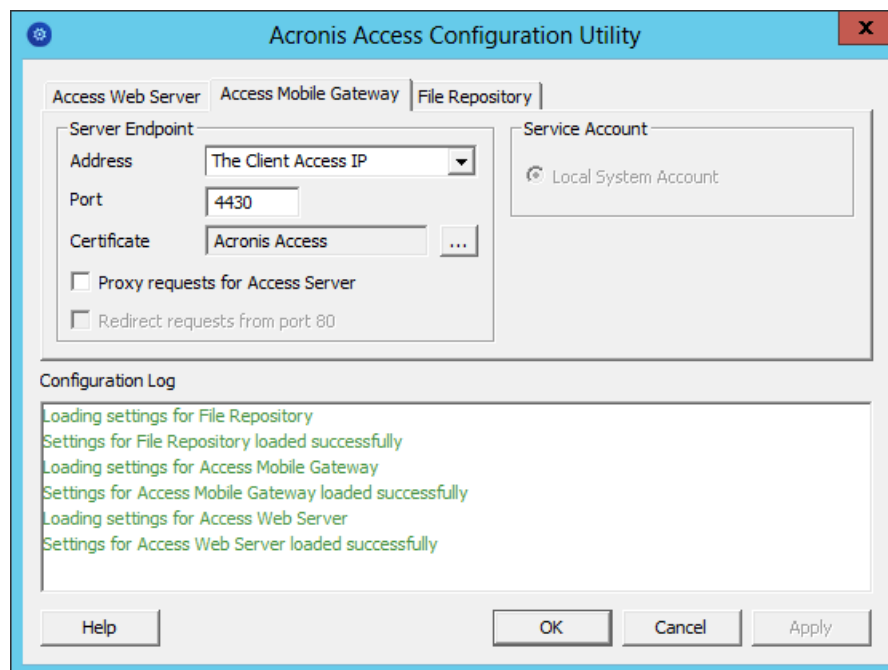
For PostgreSQL do the following:

1. Open the **Failover Cluster Manager**.
2. Find and select the PostgreSQL Generic Service resource.
3. Right-click on it and select **Properties**.
4. Click on the **Registry Replication** tab.

5. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL (For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)
6. Move the Acronis Access role to the second node.

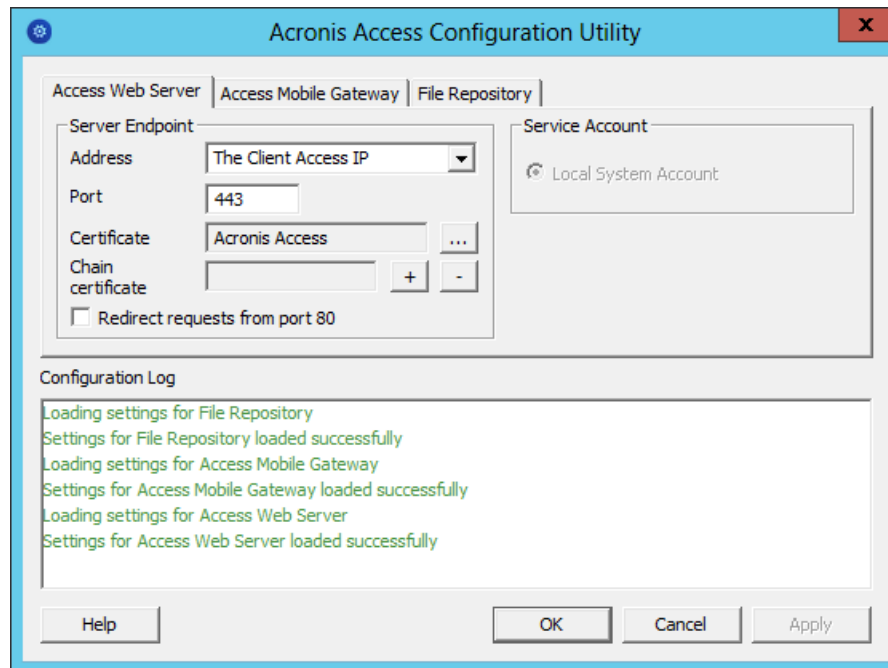
Using the Configuration Utility on the second node

1. Launch the Configuration Utility. On an upgrade from mobilEcho, this is generally located at **C:\Program Files (x86)\GroupLogic\Configuration Utility**
2. Configure the Acronis Access Gateway Server service to listen on the IP address(es) for the Acronis Access Service group.

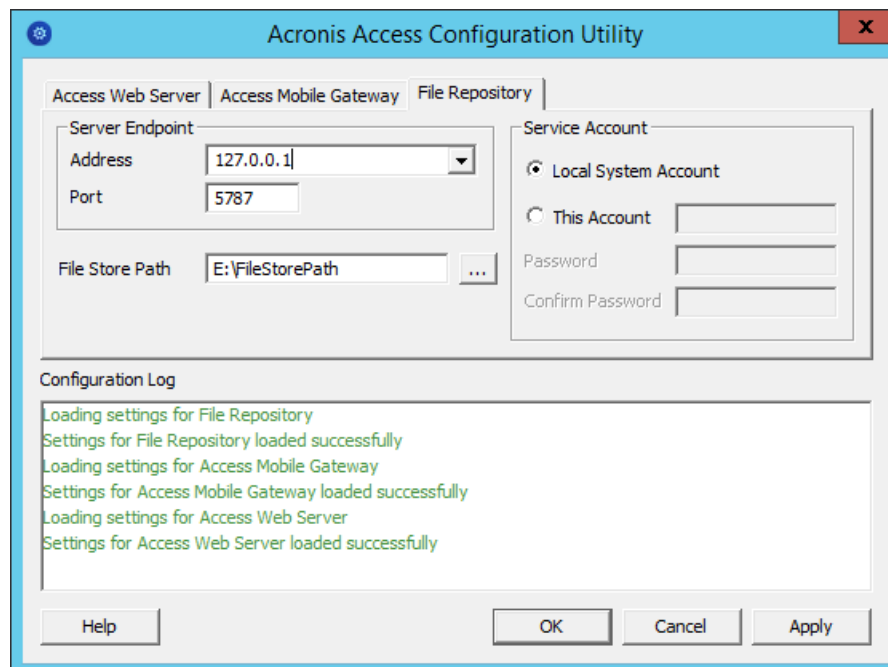


3. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is 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.



4. Configure the Acronis Access File Repository to listen on localhost and change the Filestore path to be on the shared disk. This path should be the same for both nodes.



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