Acronis

Acronis Access

Administration Guide

Copyright Statement

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

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

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

Linux is a registered trademark of Linus Torvalds.

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

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

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

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

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

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

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

Acronis patented technologies

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

Table of contents

1 Mobile Access 6

1.1 Concepts 6

1.2 Policies 8

1.2.1 User & Group Policies 8

1.2.2 Allowed Apps 22

1.2.3 Default Access Restrictions 24

1.3 On-boarding Mobile Devices 26

1.3.1 Server-side Management Enrollment Process 26

1.3.2 User-side Management Enrollment Process 29

1.4 Managing Mobile Devices 32

1.4.1 Performing Remote Application Password Resets 34

1.4.2 Performing Remote Wipes 35

1.5 Managing Gateway Servers 36

1.5.1 Registering new Gateway Servers 37

1.5.2 Server Details 38

1.5.3 Editing Gateway Servers 40

1.5.4 Licensing Gateway Servers 47

1.5.5 Cluster Groups 47

1.6 Managing Data Sources 49

1.6.1 Folders 50

1.6.2 Assigned Sources 53

1.6.3 Gateway Servers Visible on Clients 54

1.6.4 Legacy Data Sources 55

1.7 Settings 56

2 Sync & Share 58

2.1 Managing Users 58

2.2 Sharing Restrictions 60

2.3 LDAP Provisioning 61

2.4 Quotas 62

2.5 File Purging Policies 63

2.6 User Expiration Policies 64

2.7 File Repository 65

2.8 Acronis Access Client 66

3 Server Administration 67

3.1 Administering a Server 67

3.2 Administrators and Privileges 67

3.3 Audit Log 70

3.3.1 Log 70

3.3.2 Settings 71

3.4 Server 72

3.5 SMTP 73

3.6 LDAP 74

Copyright © Acronis International GmbH, 2002-2014

3.7 Email Templates 75
3.8 Licensing 77
3.9 Debug Logging 78
3.10 Monitoring 80
4 Maintenance Tasks 82
4.1 Disaster Recovery guidelines 82
4.2 Backing up and Restoring Acronis Access 84
4.3 Tomcat Log Management on Windows 86
5 Supplemental Material 91
5.1 Conflicting Software 91
5.2 Load balancing Acronis Access 91
5.3 Third-party Software for Acronis Access 97
5.3.1 PostgreSQL 97
5.3.2 Apache Tomcat 97
5.3.3 New Relic 97
5.4 Using Acronis Access with Microsoft Forefront Threat Management Gateway (TMG) 98
5.4.1 Overview 98
5.4.2 Introduction 99
5.4.3 Install the SSL Server Certificate 101
5.4.4 Create a New Web Listener 102
5.4.5 Create a New Web Site Publishing Rule 106
5.4.6 Configure an External DNS Entry for the Acronis Access Gateway Server 112
5.4.7 Using the Access Mobile Client with a TMG reverse proxy server 112
5.4.8 Using the Access Desktop Client with a TMG reverse proxy server. 113
5.5 Unattended desktop client configuration 113
5.6 Monitoring Acronis Access with New Relic 114
5.7 Using trusted server certificates with Acronis Access 115
5.8 Creating a Drop Folder 117
5.9 Customizing the web interface 118
5.10 How to support different Access Desktop Client versions 119
5.11 How to move the FileStore to a non-default location. 119
5.12 Acronis Access for Good Dynamics 120
5.12.1 Introduction 120
5.12.2 Testing a trial version of Acronis Access for Good Dynamics 121
5.12.3 Requesting and configuring Acronis Access within Good Control 122
5.12.4 Good Dynamics Policy Sets and Acronis Access 126
5.12.5 Granting Acronis Access access to a Good Dynamics User or Group 127
5.12.6 Enrolling the Acronis Access client app in Good Dynamics 129
5.13 MobileIron AppConnect support 131
5.13.1 Introduction 132
5.13.2 Testing a trial version of Acronis Access with AppConnect 132
5.13.3 Creating an AppConnect configuration and policy for Acronis Access on your MobileIron VSP 132
5.13.4 Activating the Acronis Access iOS client with AppConnect 136
5.13.5 Ongoing AppConnect management of Access Mobile Clients 137
5.13.6 Using AppConnect with Kerberos Constrained Delegation 137

Copyright © Acronis International GmbH, 2002-2014

6 Configuring an AppConnect tunnel between the Access Mobile client and the Access server via username/password authentication 140

7 Adding Kerberos Constrained Delegation Authentication 151

7.1.1 Advanced Delegation Configurations 159

7.2 Installing Acronis Access on a Microsoft Failover Cluster 160

7.2.1 Installing Acronis Access on a Windows 2003 Microsoft Failover Cluster 160

7.2.2 Installing Acronis Access on a Windows 2008 Microsoft Failover Cluster 174

7.2.3 Installing Acronis Access on a Windows 2012 Microsoft Failover Cluster 185

7.3 Upgrading from mobilEcho 4.5 on a Microsoft Failover Cluster 196

7.3.1 Upgrading a mobilEcho server on a Windows 2003 Failover Cluster to Acronis Access 196

7.3.2 Upgrading a mobilEcho server on a Windows 2008 Failover Cluster to Acronis Access 206

7.3.3 Upgrading a mobilEcho server on a Windows 2012 Failover Cluster to Acronis Access 215

7.4 Upgrading Acronis Access on a Microsoft Failover Cluster 225

8 What's New 228

8.1 What's New in Acronis Access Server 228

8.2 What's New in the Acronis Access app 238

8.3 Previous Releases 239

8.3.1 activEcho 239

8.3.2 mobilEcho 250

Copyright © Acronis International GmbH, 2002-2014

1 Mobile Access

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

In this section

Concepts....6
Policies....8
On-boarding Mobile Devices....26
Managing Mobile Devices....32
Managing Gateway Servers....36
Managing Data Sources....49
Settings....56

1.1 Concepts

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

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

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

Fig 1. Single Gateway server, many Access Mobile Clients

Copyright © Acronis International GmbH, 2002-2014

Any number of Gateway Servers can later be added to the network and configured for access from the client app.

Note: *Details on installing Acronis Access are included in the Installing section of this guide. Configuration of Gateway Servers and Data Sources is explained in the Mobile Access (p. 6) section.*

If you wish to remotely manage your Access Mobile Clients, Acronis Access Client Management allows you to create policies per Active Directory user or group. These policies can:

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

Only one Acronis Access Server is required.

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

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

Note: *Details on enabling and configuring the client management are included in the Policies (p. 8) and Managing Mobile Devices (p. 32) section of this guide.*

Copyright © Acronis International GmbH, 2002-2014

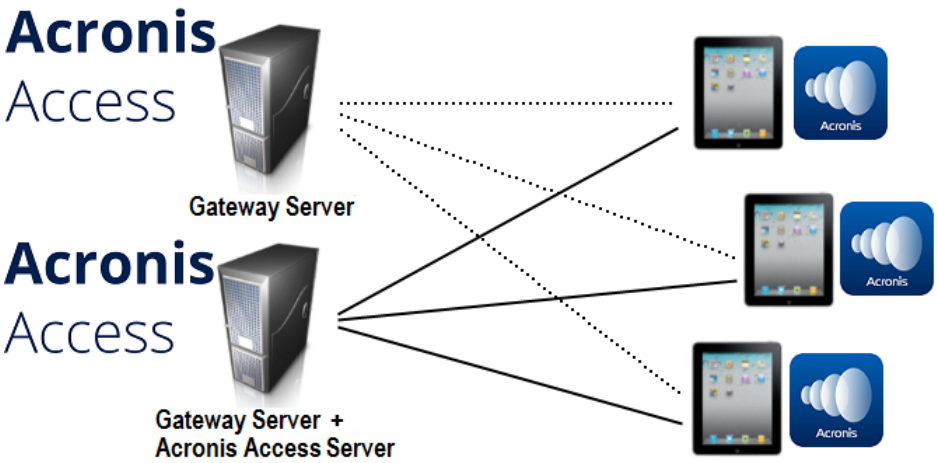


Fig 2. One Gateway Server, one Gateway Server + Acronis Access Server, many clients

1.2 Policies

In this section

User & Group Policies 8
Allowed Apps 22
Default Access Restrictions 24

1.2.1 User & Group Policies

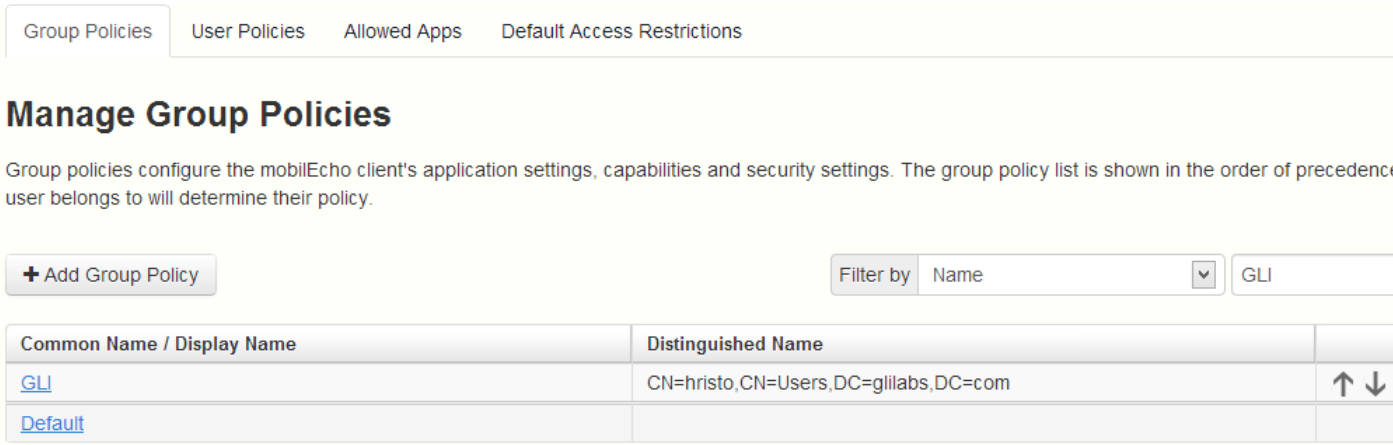
Acronis Access Client Management allows policies to be assigned to Active Directory groups. Group policies will usually address most or all of your client management requirements. The group policies list is displayed in order of precedence, with the first group in the list having the highest priority.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

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

Group Management Tips

Copyright © Acronis International GmbH, 2002-2014

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



In this section

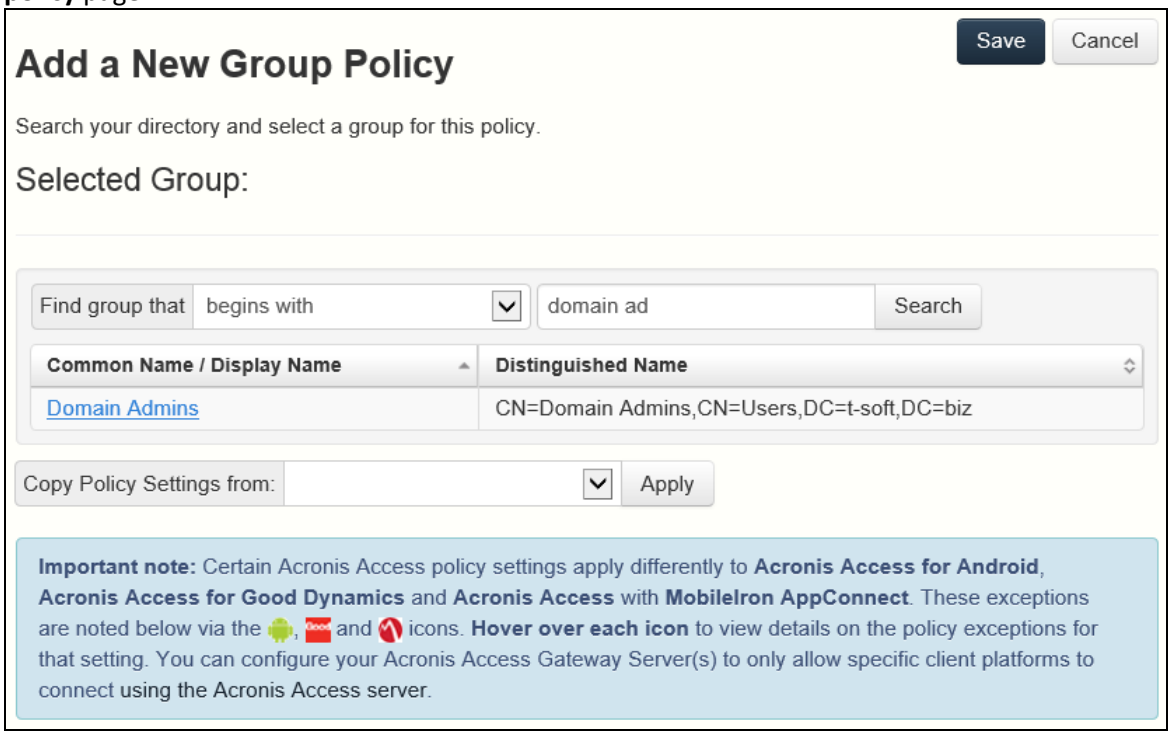
Adding a New Policy....9
Exceptions for policy settings....11
Modifying Policies....12
Creating a Blocked Path list....12
Security Policy....14
Application Policy....16
Synced Folder....19
Home Folders....20
Server Policy....21

1.2.1.1 Adding a New Policy

To add a new group policy:

Copyright © Acronis International GmbH, 2002-2014

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

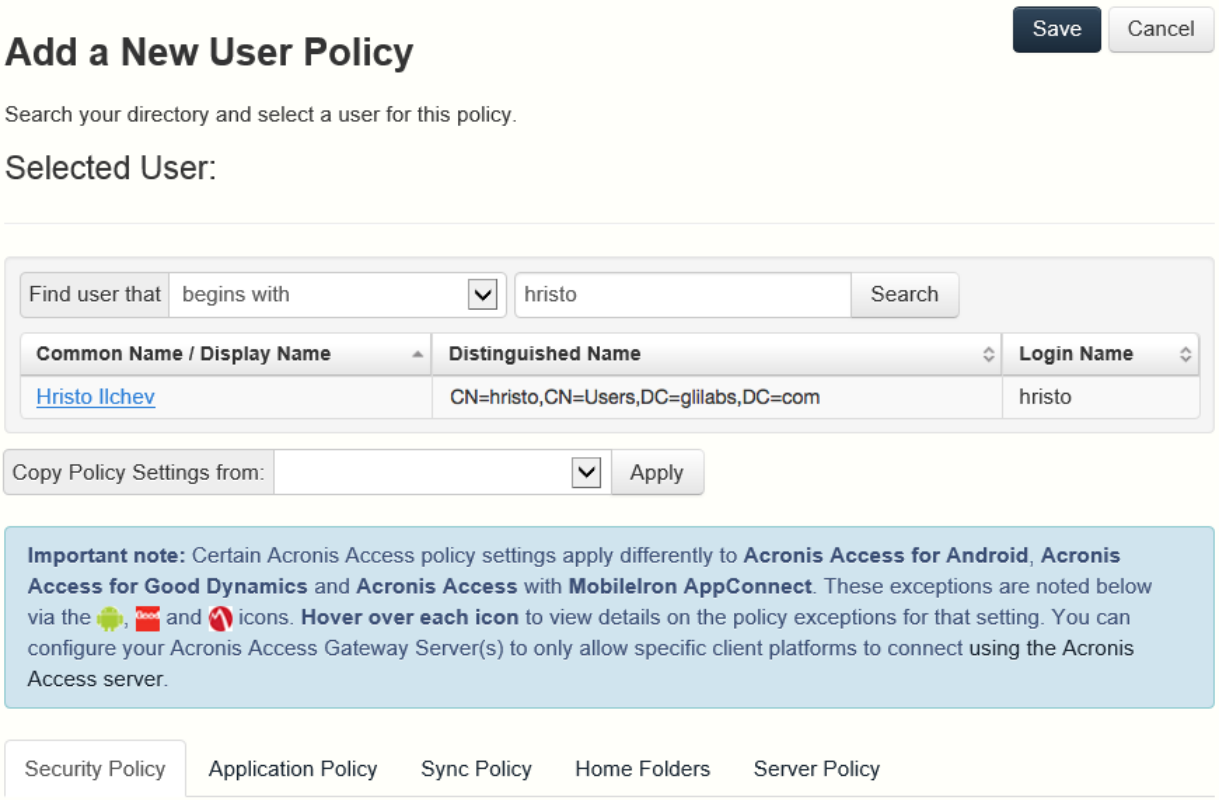


3. In the **Find group** field, enter the partial or complete Active Directory group name for which you'd like to create a policy. You can perform '**begins with**' or '**contains**' searches for Active Directory groups. Begins with search will complete much faster than contains searches.
4. Click **Search** and then find and click the group name in the listed results.
5. Make the necessary configurations in each of the tabs (Security (p. 14), Application (p. 16), Sync (p. 19), Home Folders (p. 20) and Server (p. 21)) and press **Save**.

To add a new user policy:

Copyright © Acronis International GmbH, 2002-2014

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



3. In the **Find user** field, enter the partial or complete Active Directory user name for which you'd like to create a policy. You can perform '**begins with**' or '**contains**' searches for Active Directory users. Begins with search will complete much faster than contains searches.
4. Click **Search** and then find and click the user name in the listed results.
5. Make the necessary configurations in each of the tabs (Security (p. 14), Application (p. 16), Sync (p. 19), Home Folders (p. 20) and Server (p. 21)) and press **Save**.

1.2.1.2 Exceptions for policy settings

For users running the **Access Mobile Client for Android, Access Mobile Client for Good Dynamics** (iOS) and **Access Mobile Client with Mobile Iron AppConenct** apps, there are some exceptions to the way Acronis Access management policies are applied to the Access Mobile Client app. In the case of Android, a few of the features of the iOS client are not yet supported, so the related policies do not apply. In the case of Good Dynamics, a few of the standard Access Mobile Client policy features are deferred to the Good Dynamics system and the Good Dynamics policy set that you have configured on your Good Control server. With MobileIron, a few of the standard Acronis Access policy features are deferred to the MobileIron AppConnect platform. These exceptions are noted on the Acronis Access policy configuration pages. Hover over the Good, Android and MobileIron logos for more details on the individual policy exceptions.

Copyright © Acronis International GmbH, 2002-2014

1.2.1.3 Modifying Policies

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

Client management connectivity requirements

Access Mobile Clients must have network access to the management server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access Acronis Access Gateway servers they will also need to VPN before management commands will be accepted.

To modify a group policy

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

To modify a user policy:

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

1.2.1.4 Creating a Blocked Path list

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

To create a list:

1. Open the web interface as an administrator.
2. Open the Policies (p. 8) page.
3. Click on the desired User policy or Group policy.
4. Open the Server Policy (p. 21) tab.
5. Select the **Block access to specific network paths** check box.

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

6. Press **Add/Edit lists**.

Copyright © Acronis International GmbH, 2002-2014

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

To enable the blacklist for a User or Group policy:

1. Open the web interface as an administrator.
2. Open the Policies (p. 8) page.
3. Click on the desired User policy or Group policy.
4. Open the Server Policy (p. 21) tab.
5. Select the **Block access to specific network paths** check box.

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

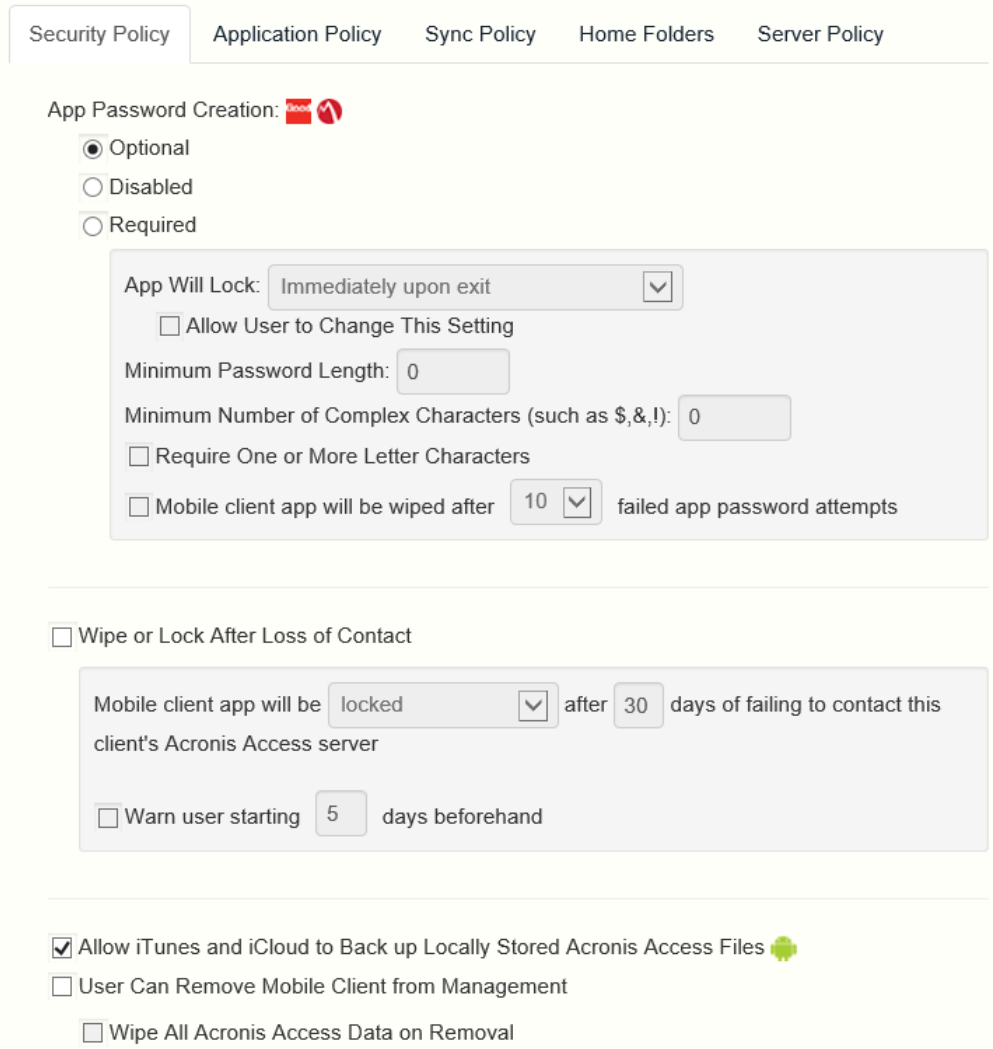
6. Select the desired list from the drop-down menu.

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

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

Copyright © Acronis International GmbH, 2002-2014

1.2.1.5 Security Policy



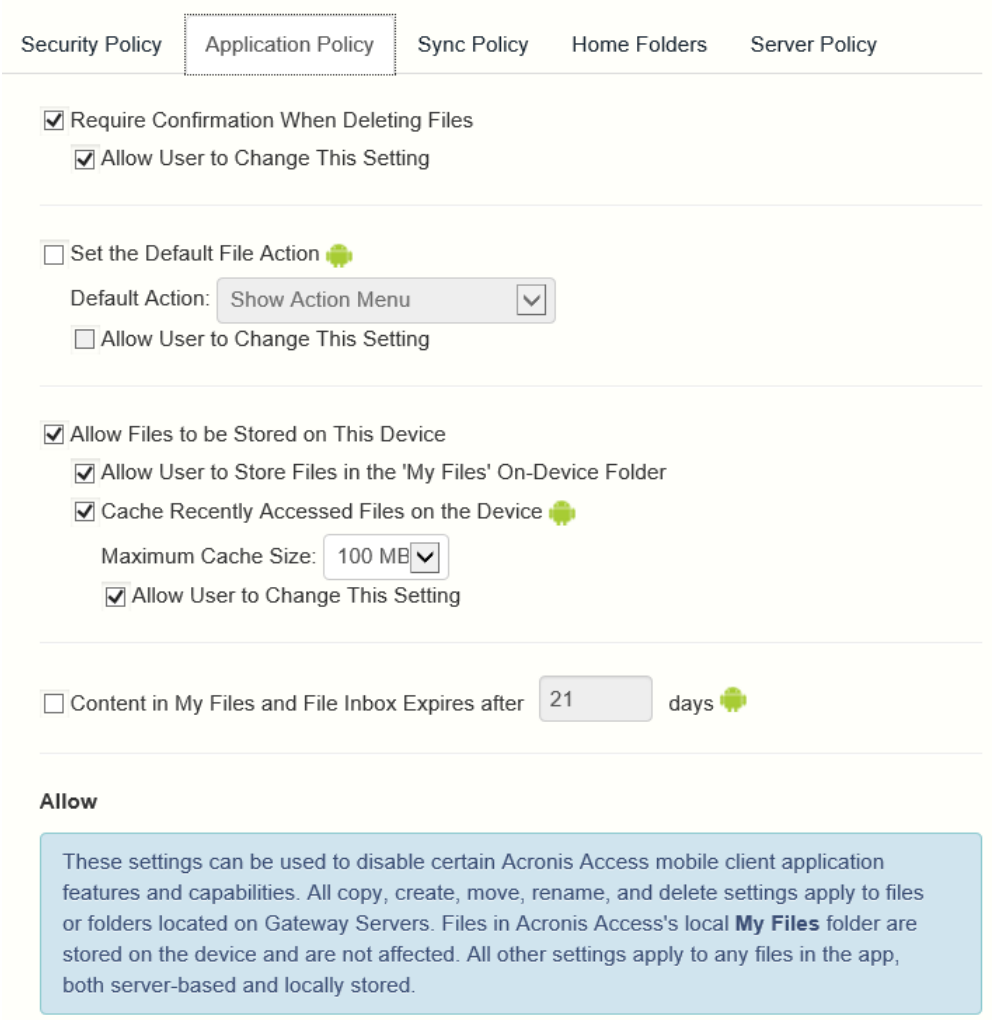
- **App password creation** - The Access Mobile Client application can be set with a lock password that must be first entered when launching the application.
  - **Optional** - This setting will not force the user to configure an application lock password, but they will be able to set one from the **Settings** menu within the app if they desire.
  - **Disabled** - This setting will disable the ability to configure an application lock password from the **Settings** menu within the app. This might be useful in the case of shared mobile devices where you prefer that a user cannot set an app password and will lock other users out of the Access Mobile Client.
  - **Required** - This setting will force the user to configure an application lock password if they do not already have one. The optional application password complexity requirements and failed password attempt wipe setting only apply when **App password creation** is set to **Required**.
    - **App will lock** - This setting configures the application password grace period. When a user switches from the Access Mobile Client to another application on their device, if they return to the Access Mobile Client before this grace period has elapsed, they will not be required to enter their application lock password. To require that the password is entered every time, choose **Immediately upon exit**. If you would like the user to be able to modify their **App will lock** setting from within the Access Mobile Client settings, select **Allow user to change this setting**.

Copyright © Acronis International GmbH, 2002-2014

    - **Minimum password length** - The minimum allowed length of the application lock password.
    - **Minimum number of complex characters** - The minimum number of non-letter, non-number characters required in the application lock password.
    - **Require one or more letter characters** - Ensures that there is at least one letter character in the application password.
    - **Mobile Client app will be wiped after X failed app password attempts** - When this option is enabled, the settings and data in the Access Mobile Client app will be wiped after the specified number of consecutive failed app password attempts.
- **Wipe or lock after loss of contact**- Enable this setting if you would like the Access Mobile Client app to automatically wipe or lock in the case that it has not made contact with this Acronis Access server in a certain number of days. Locked clients will automatically unlock in the event that they later contact the server successfully. Wiped clients immediately have all the local files stored in the Mobile Client app deleted, their client management policy removed, and all settings reset to defaults. Wiped clients will have to be re-enrolled in management to gain access to gateway servers.
    - **Mobile Client app will be locked/wiped after X days of failing to contact this client's Acronis Access server -** Set the default action after the client fails to contact this Acronis Access server for a number of days.
    - **Warn user starting [ ] days beforehand** - The Access Mobile Client app can optionally warn the user when a 'loss of contact' wipe or lock is going to happen in the near future. This gives them the opportunity to reestablish a network connection that allows the Access Mobile Client app to contact its Acronis Access Server and prevent the lock or wipe.
- **User can remove Mobile Client from management**- Enable this setting if you would like your Acronis Access users to be able to uninstall their management policy from within Acronis Access. Doing so will return the application to full functionality and restore any configuration that was changed by their policy.
    - **Wipe all Acronis Access data on removal** - When user removal of policies is enabled, this option can be selected. If enabled, all data stored locally within the Access Mobile Client application will be erased if it is removed from management, ensuring that corporate data does not exist on a client not under management controls.
- **Allow iTunes to back up locally stored Acronis Access files** - When this setting is disabled, the Access Mobile Client will not allow iTunes to back up its files. This will ensure that no files within Acronis Access' secure on-device storage are copied into iTunes backups.

Copyright © Acronis International GmbH, 2002-2014

1.2.1.6 Application Policy



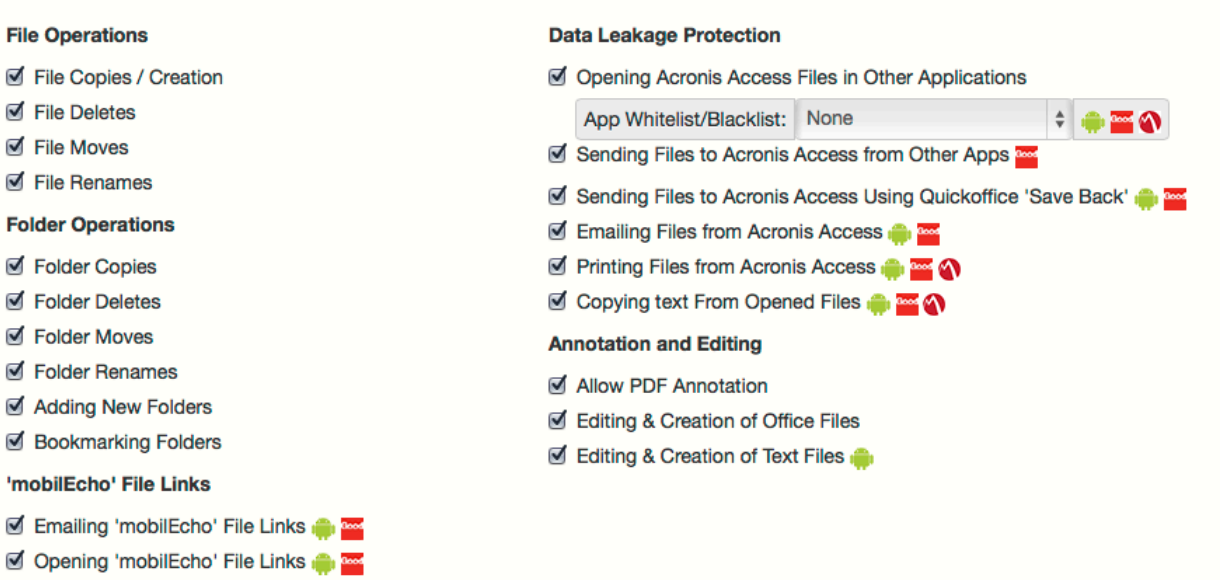
- **Require Confirmation When Deleting Files** - When enabled, the user will be asked for confirmation each time they delete a file. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Set the Default File Action** - This option determines what will happen when a user taps a file in the Access Mobile Client application. If this is not set, the client application defaults to **Action Menu**. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Allow Files to be Stored on the Device** - This setting is enabled by default. When enabled, files will be permitted to remain on the device, within Acronis Access' sandboxed storage. Individual features that store files locally (My Files folder, sync folders, recently accessed file caching) can be enabled or disabled using additional policy settings. If this option is disabled, no files will be stored on the device, ensuring that no corporate data is on the device if it is lost or stolen. If this setting is disabled, the user will not be able to save or sync files for offline use, cache files for improved performance, or send files from other applications to the Access Mobile Client using the "Open In" function.
  - **Allow User to Store Files in the 'My Files' On-Device Folder** - If enabled, files can be copied into the 'My Files' folder for offline access and editing. This is a general purpose storage area within Acronis Access' on-device storage sandbox.
  - **Cache Recently Accessed Files on the Device** - If enabled, server-based files that have been recently access will be saved in a local cache on the device, for use if they are accessed again

Copyright © Acronis International GmbH, 2002-2014

and have not changed, providing performance and bandwidth conservation benefits. **Maximum Cache Size** can be specified and the user can optionally be allowed to change this setting.

- **Content in My Files and File Inbox Expires after X days** - If this option is enabled, files in the File Inbox and in My Files will be deleted from the device after the set number of days.

Allow



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

File Operations

- **File Copies / Creation** - If this option is disabled, the user will not be able to save files from other applications or from the iPad Photos library to a Gateway Server. They will also be unable to copy or create new files or folders on the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file creation.
- **File Deletes** - If this option is disabled, the user will not be able to delete files from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file deletion.
- **File Moves** - If this option is disabled, the user will not be able to move files from one location to another on the Gateway Server, or from the server to the Access Mobile Client application's local My Files storage. This setting supersedes any NTFS permissions that client may have that allow file or folder moves.
- **File Renames** - If this option is disabled, the user will not be able to rename files from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file renames.

Copyright © Acronis International GmbH, 2002-2014

Folder Operations

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

'mobilEcho' File Links

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

Data Leakage Protection

- **Opening Acronis Access Files in Other Applications** - If this option is disabled, the Access Mobile Client application will omit the **Open In** button and not allow files in Acronis Access to be opened in other applications. Opening a file in another application results in the file being copied to that application's data storage area and outside of Acronis Access control.
  - **App Whitelist/Blacklist** - Select a predefined whitelist or blacklist that restricts that third party apps that Acronis Access files can be opened into on the device. To create a whitelist or blacklist, click **Allowed Apps** in the top menu bar.
- **Sending Files to Acronis Access from Other Apps** - If this option is disabled, the Access Mobile Client application will not accept files sent to it from other applications' **Open In** feature.
- **Sending Files to Acronis Access Using Quickoffice 'Save Back'** - If this option is disabled, the Acronis Access application will not accept files sent to it from the Quickoffice app's **Save Back** feature.

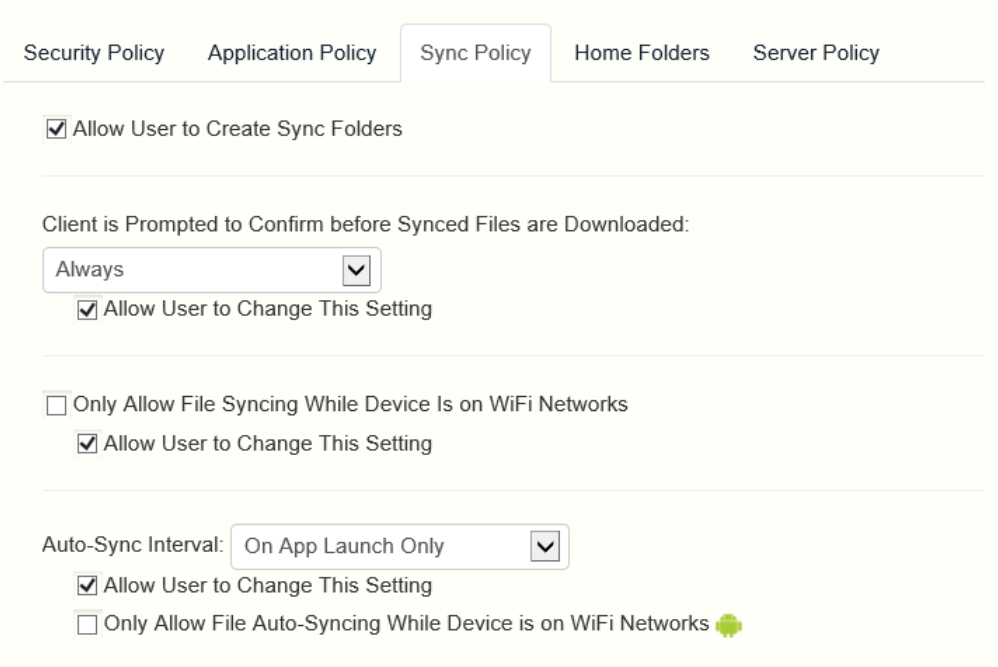
Copyright © Acronis International GmbH, 2002-2014

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

Annotation and Editing

- **Allow PDF annotation** - If this option is disabled, the Access Mobile Client will not be allowed to annotate PDFs.
- **Editing & Creation of Office files** - If this option is disabled, users will not be allowed to edit documents using the integrated SmartOffice editor.
- **Editing & Creation of Text files** - If this option is disabled, users will not be allowed to edit .txt files using the built-in text editor.

1.2.1.7 Synced Folder

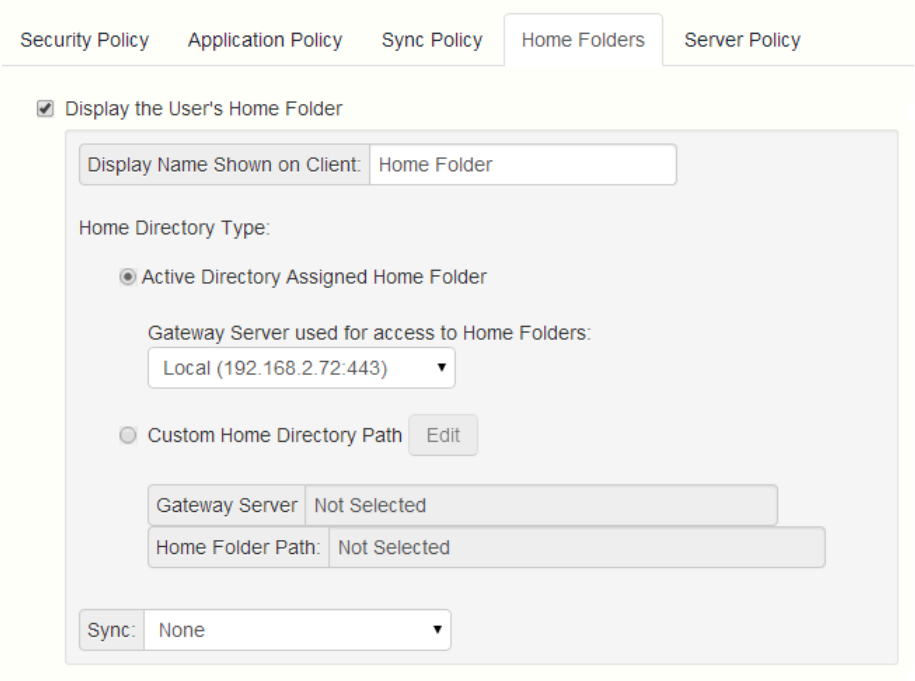


- **Allow User to Create Sync Folders -** Allows the user to create their own sync folders.
- **Client is Prompted to Confirm Before Synced Files are Downloaded** - Select the conditions under which the user must confirm before files in synced folders are downloaded. Options are: **Always**, **While on cellular networks only,** and **Never**. If **Allow User to Change This Setting** is enabled, clients will be able to change the confirmation options.
- **Only Allow File Syncing While Device is on WiFi Networks** - When this option is enabled, Acronis Access will not allow files to be synced over cellular connections. If **Allow User to Change This Setting** is enabled, clients will be able to enable or disable automatic file syncing while on WiFi networks.

Copyright © Acronis International GmbH, 2002-2014

- **Auto-Sync Interval** - When this option is enabled, Acronis Access will automatically sync **never**, **on app launch only** or on several **time intervals**.
  - **Allow User to Change This Setting** - When this option is enabled, the users will be able to change the time interval from the Access Mobile Client app.
  - **Only Allow File Auto-Syncing While Device is on WiFi Networks** - When this option is enabled the auto-sync will not occur unless the user is connected via WiFi.

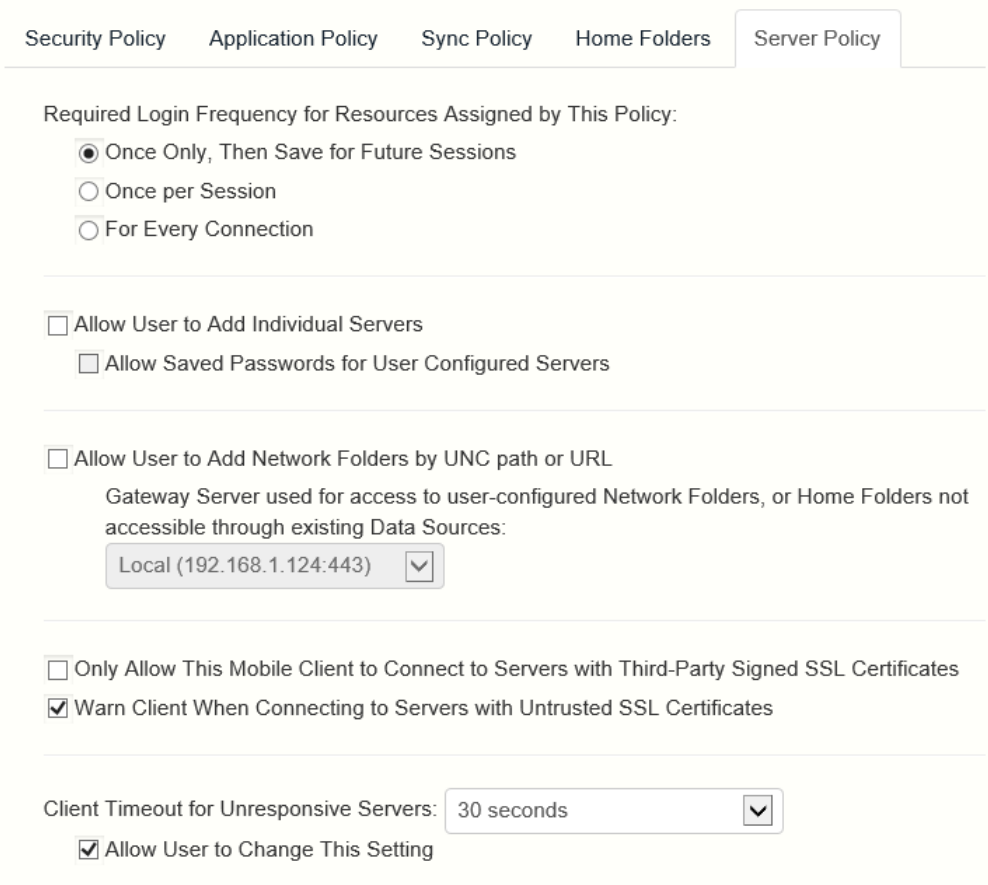
1.2.1.8 Home Folders



- **Display the user's home folder**- This option causes a user's personal home directory to appear in the Access Mobile Client app.
  - **Display name shown on client** - Sets the display name of the home folder item in the Access Mobile Client app.
  - **Active Directory assigned home folder** - The home folder shown in the Access Mobile Client app will connect the user to the server/folder path defined in their AD account profile. The Home Folder will be accessible via the selected Gateway.
  - **Custom home directory path** - The home folder shown in the Access Mobile Client app will connect the user to the server and path defined in this setting. The %USERNAME% wildcard can be used to include the user's username in the home folder path. %USERNAME% must be capitalized.
  - **Sync –** This option selects the type of sync of your Home Directory.

Copyright © Acronis International GmbH, 2002-2014

1.2.1.9 Server Policy



- **Required login frequency for resources assigned by this policy**- sets the frequency that a user must log into the servers that are assigned to them by their policy.
  - **Once only, then save for future sessions** - The user enters their password when they are initially enrolled in management. This password is then saved and used for any file server connections they later initiate.
  - **Once per session** - After launching the Access Mobile Client, the user is required to enter their password at the time they connect to the first server. Until they leave the Access Mobile Client application, they can then connect to additional servers without having to reenter their password. If they leave the Access Mobile Client for any period of time and then return, they will be required to enter their password again to connect to the first server.
  - **For every connection** - The user is required to enter their password each time they connect to a server.
- **Allow user to add individual servers** - If this option is enabled, users will be able to manually add servers from within the Access Mobile Client application, as long as they have the server's DNS name or IP address. If you want the user to only have their policy **Assigned Servers** available, leave this option disabled.
  - **Allow saved passwords for user configured servers** - If a user is allowed to add individual servers, this sub-option determines whether they are allowed to save their password for those server.
- **Allow User to Add Network Folders by UNC path or URL** - When enabled, the mobile client users will be able to add and access network folders and SharePoint sites not assigned to them or not accessible through the existing Data Sources. The selected Gateway Server must have access to those SMB shares or SharePoint sites.

Copyright © Acronis International GmbH, 2002-2014

- **Block access to specific network paths** - When enabled, allows the administrator to create and use blacklists of network paths which the users shouldn't be allowed to self-provision.

- **Only allow this Mobile Client to connect to servers with third-party signed SSL certificates** - If this option is enabled, the Access Mobile Client will only be permitted to connect to servers with third-party signed SSL certificates.

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

- **Warn client when connecting to servers with untrusted SSL certificates** - If your users are routinely connecting to servers that will be using self-signed certificates, you may choose to disable the client-side warning dialog message they will receive when connecting to these servers.
- **Client timeout for unresponsive servers** - This option sets the client login connection timeout for unresponsive servers. If your clients are on especially slow data connections, or if they rely on a VPN-on-demand solution to first establish a connection before a Gateway Server is reachable, this timeout can be set to a value greater than the 30 second default. If you want the client to be able to change this through the Access Mobile Client app, check **Allow user to change this setting.**

1.2.2 Allowed Apps

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

Whitelists - allow you to specify a list of apps that Acronis Access files are allowed to be opened into. All other apps are denied access.

Blacklists - allow you to specify a list of apps that Acronis Access files are not allowed to be opened into. All other apps are allowed access.

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

Note: *App whitelisting and blacklisting are not currently supported by the Access Mobile Client for Android.*

Lists

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

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

In this section

Copyright © Acronis International GmbH, 2002-2014

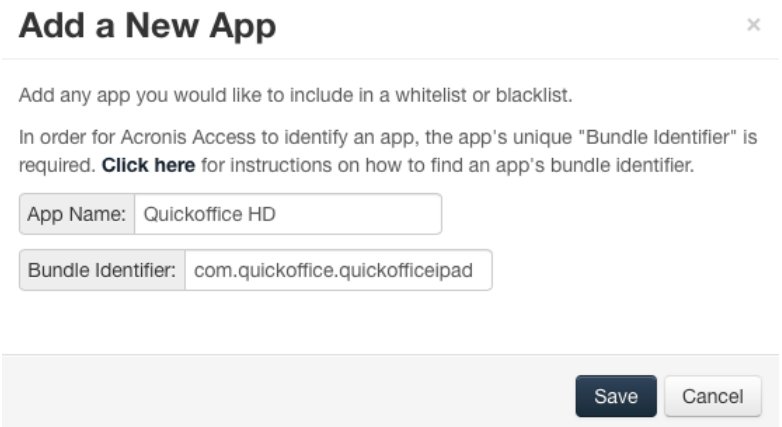
Adding Apps Available for Lists 23
Finding an app's bundle identifier by browsing the files on your device 23
Finding an app's bundle identifier in an iTunes Library 23

1.2.2.1 Adding Apps Available for Lists

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

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

There is unfortunately no way to look these **Bundle Identifiers** up in the App Store or elsewhere at this time. To find a bundle identifier, you will need to look at a file inside the app.



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

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

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

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

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

1. Navigate to your iTunes Library and open the **Mobile Applications** folder.

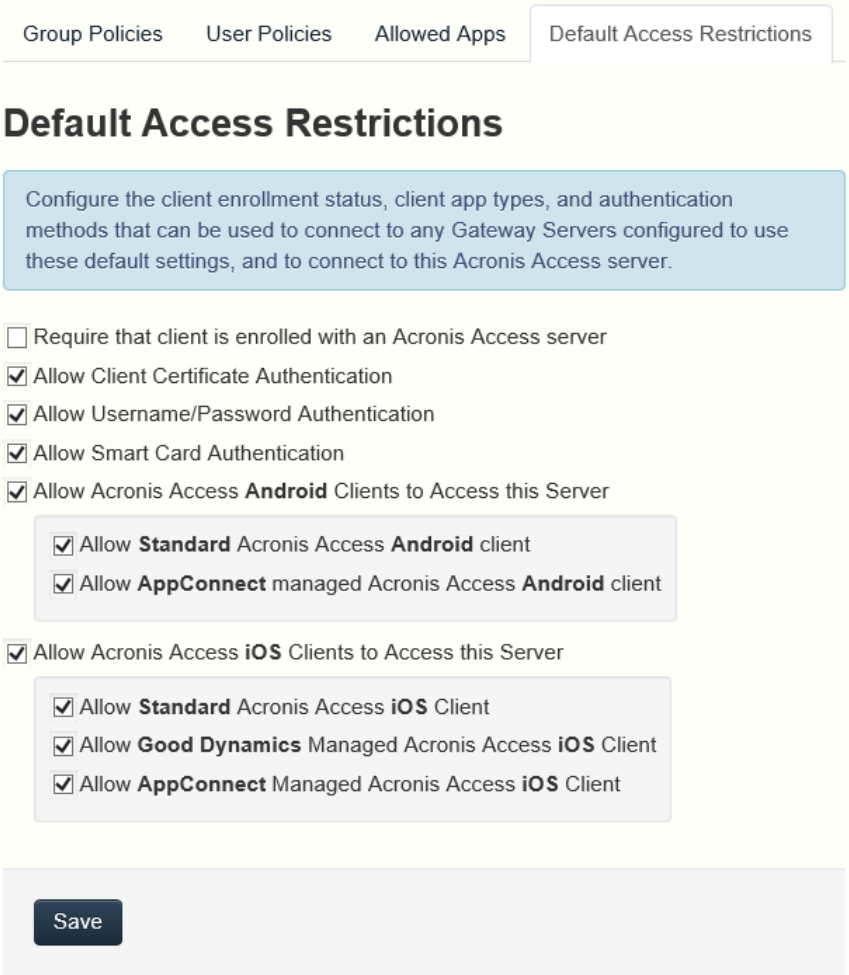
Copyright © Acronis International GmbH, 2002-2014

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

1.2.3 Default Access Restrictions

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

Note: *For information on setting custom access restrictions for your Gateway Servers visit the Editing Gateway Servers (p. 40) article in the Managing Gateway Servers section.*



Copyright © Acronis International GmbH, 2002-2014

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

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

Copyright © Acronis International GmbH, 2002-2014

1.3 On-boarding Mobile Devices

To get started with the Acronis Access mobile client, users need to install the Access Mobile Client application through the Apple App Store. If your company is using client management, the users also need to enroll the Access Mobile Client app on their device with the Acronis Access Server. Once enrolled, their mobile client configuration, security settings, and capabilities are controlled by their Acronis Access user or group policy.

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

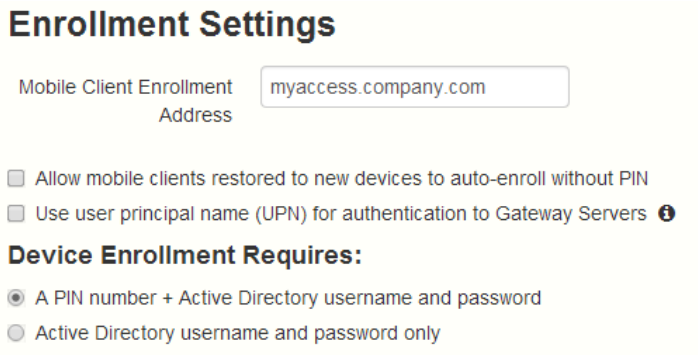
- Requiring a Access Mobile Client application lock password
- App password complexity requirements
- Ability to remove the Access Mobile Client app from management
- Allow emailing and printing files from the Access Mobile Client
- Allow storing files on the device
- Allow Access Mobile Client on-device files to be included in iTunes backups
- Allow sending files to the Access Mobile Client from other applications
- Allow opening Access Mobile Client files in other applications
- Restrict the other applications that Access Mobile Client files are allowed to be opened into
- Allow PDF annotation
- Allow file and folder creation, renames and deletes
- Allow moving files
- Require confirmation when deleting
- Servers, folders, and home directories can be assigned so they automatically appear in the Access Mobile Client app
- Assigned folders can be configured to perform 1-way to 2-way syncing with the server

In this section

Server-side Management Enrollment Process.....26
User-side Management Enrollment Process 29

1.3.1 Server-side Management Enrollment Process

Selecting an enrollment mode



1. Open the Acronis Access web interface.

Copyright © Acronis International GmbH, 2002-2014

2. Log in as an administrator.
3. Open the **Mobile Access** tab.
4. Open the **Settings** tab.
5. Select the desired device enrollment requirements

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

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

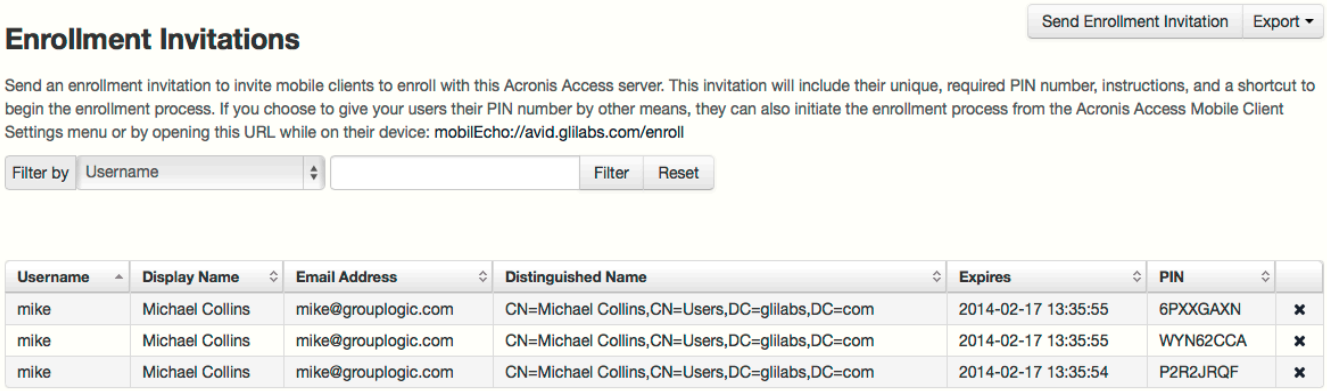
Inviting a user to enroll

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

- Once an enrollment invitation is generated, the invited users are displayed on the **Enrollment Invitations** page. Each user's PIN number is listed, in the case that you need to communicate it by a means other than the automatic email.
- Once a user successfully enrolls their Access Mobile Client using their one-time use PIN number, they will no longer appear in this list.
- To revoke a user's invitation PIN number, press delete to remove them from the list.
- **Filter by** - The invitations list can be filtered by Username, Display Name, or Email Address.

Copyright © Acronis International GmbH, 2002-2014

- Download enrollment invitations as CSV - The entire or filtered invitations list can be exported to a CSV file and opened in Excel or imported into a custom process.



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

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

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

Note: *For more information on the two modes, visit the Settings (p. 56) section.*

To generate an Acronis Access enrollment invitation:

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

   Note: *If you prefer to manually communicate enrollment PIN numbers to the users, you can uncheck the* ***Send an enrollment invitation email to each user with a specified address*** *option. Each PIN number will be visible on the* ***Enrollment Invitations*** *page.*
7. Choose the number of days you'd like the invitation to be valid for in the Number of days until invitation expires field.

Copyright © Acronis International GmbH, 2002-2014

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

   ***Note**: Acronis Access licensing allows each licensed user to activate up to 3 devices, each additional device beyond 3 is counted as a new user for licensing purposes.*

9. Choose the version or versions of the Access Mobile Client that you would like your users to download and install on their device. You may choose iOS, Android, or Both. If you are using Acronis Access for Good Dynamics, you can select that option and your users will only be directed to download the Good Dynamics version of the Access Mobile Client.
10. Press Send.

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

Inviting users previously enrolled by mobilEcho 4.5 or earlier

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

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

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

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

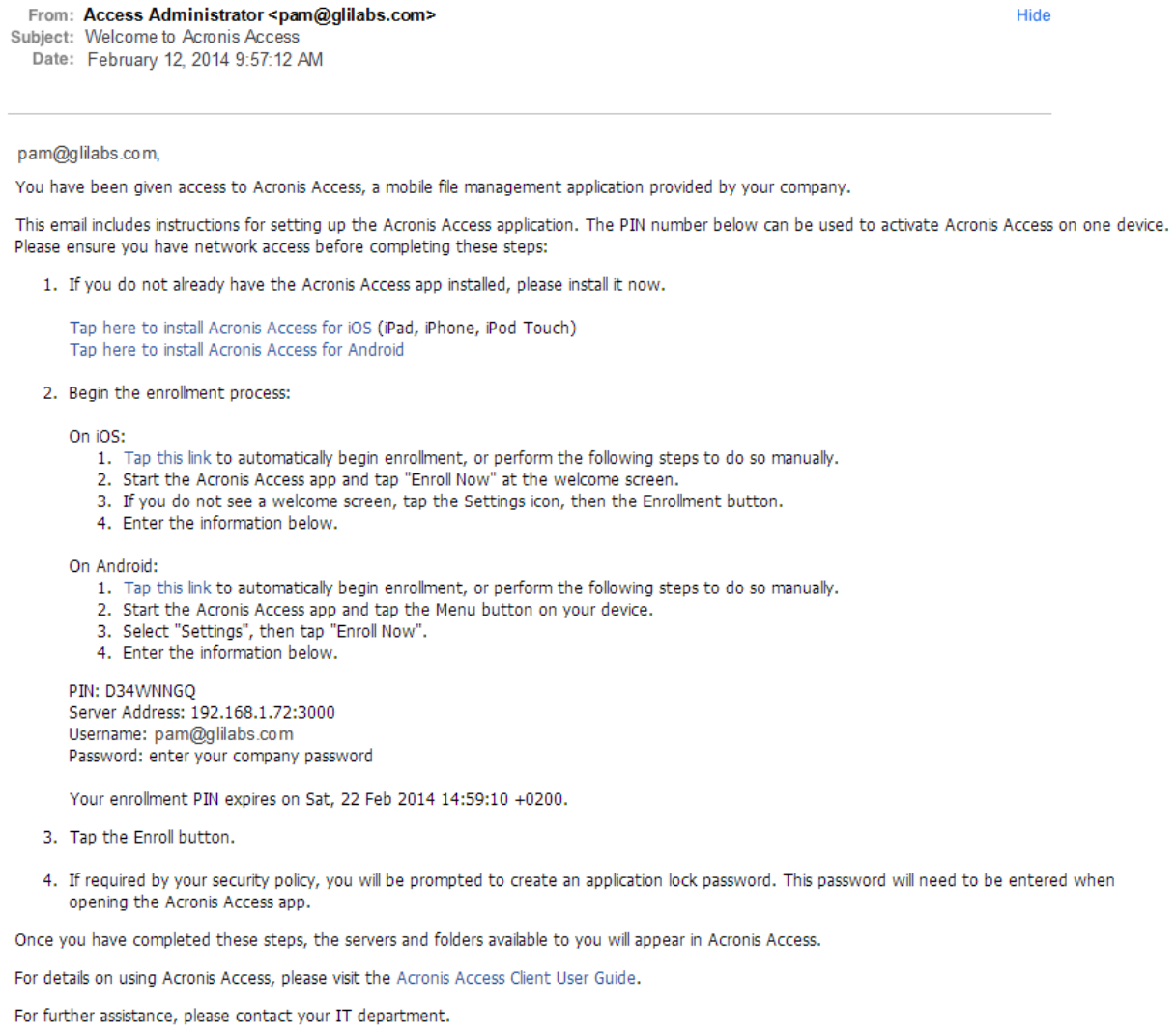
1.3.2 User-side Management Enrollment Process

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

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

Copyright © Acronis International GmbH, 2002-2014

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



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

pam@glilabs.com,

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

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

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

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

2. Begin the enrollment process:

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

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

   PIN: D34WNNGQ
   Server Address: 192.168.1.72:3000
   Username: pam@glilabs.com
   Password: enter your company password

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

3. Tap the Enroll button.

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

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

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

For further assistance, please contact your IT department.

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

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

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

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

Copyright © Acronis International GmbH, 2002-2014

To enroll in management

Enroll automatically via enrollment email

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

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

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

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

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

Manual enrollment

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

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

Copyright © Acronis International GmbH, 2002-2014

Ongoing Management Updates

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

Client management connectivity requirements

Access Mobile Clients must have network access to the management server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access Acronis Access Gateway servers they will also need to VPN before management commands will be accepted.

Removing Management

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

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

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

To unmanage your device follow the steps below:

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

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

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

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

1.4 Managing Mobile Devices

Once a Access Mobile Client has enrolled with the Acronis Access Server, their mobile device will appear on the **Devices** list. This list gives detailed status information for each device that has been activated with a PIN number, or previously managed by a mobilEcho 2.1 or earlier server, if that option is enabled.

Copyright © Acronis International GmbH, 2002-2014

Here you can view every managed device and information about them. You can also wipe the device or change it's app password.

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

In this section

Performing Remote Application Password Resets 34
Performing Remote Wipes.....35

Copyright © Acronis International GmbH, 2002-2014

1.4.1 Performing Remote Application Password Resets

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

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

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

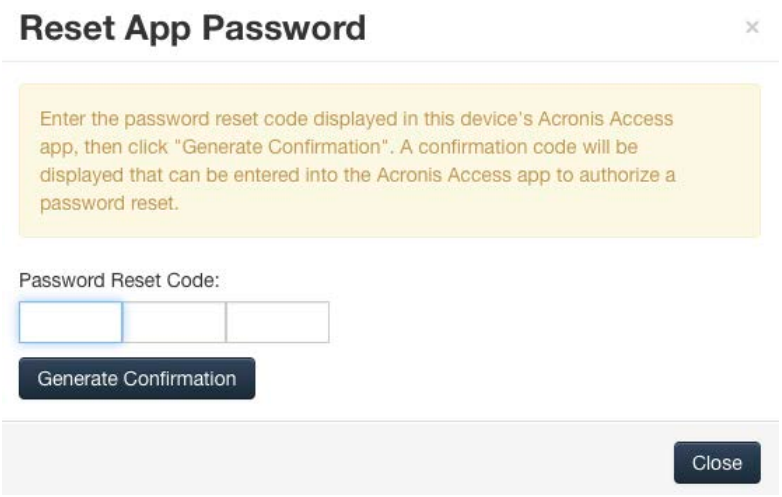
Resetting an application password

Acronis Access on-device files have always been protected using Apple Data Protection (ADP) file encryption. To further protect files on devices being backed up into iTunes and iCloud, devices without device-level lock codes enabled, and as a general security enhancement, we introduced a second layer of full-time custom encryption applied directly by the Acronis Access app. One aspect of this encryption is that Acronis Access 5.0 and later can no longer have their application lock password reset over the air. Instead, a password reset code and confirmation code must be exchanged between the device user and the Acronis Access IT administrator, in order to enable Acronis Access to decrypt its settings database and allow the user to set a new app password.

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

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

Copyright © Acronis International GmbH, 2002-2014



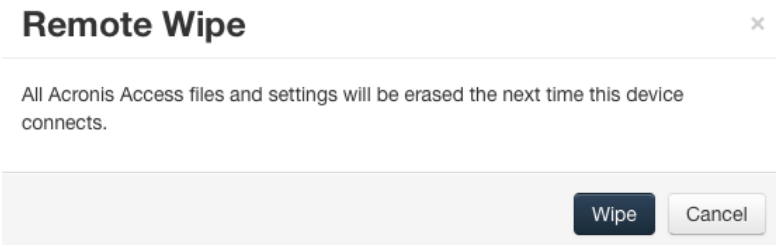
1.4.2 Performing Remote Wipes

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

Queuing a Remote wipe

1. Open the **Mobile Access** tab.
2. Open the **Devices** tab.
3. On the **Manage Devices** page, find the device you'd like to issue a remote wipe for and press the **Actions** button.
4. Press **Remote wipe...**
5. Confirm the remote wipe by pressing **Queue remote wipe**.
6. A '**Pending remote**' status will appear in the **Status** column for that device. When the remote wipe has been accepted by the device, its **Status** will reflect this.

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



Client management connectivity requirements

Access Mobile Clients must have network access to the management server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access Acronis Access Gateway servers they will also need to VPN before management commands will be accepted.

Copyright © Acronis International GmbH, 2002-2014

1.5 Managing Gateway Servers

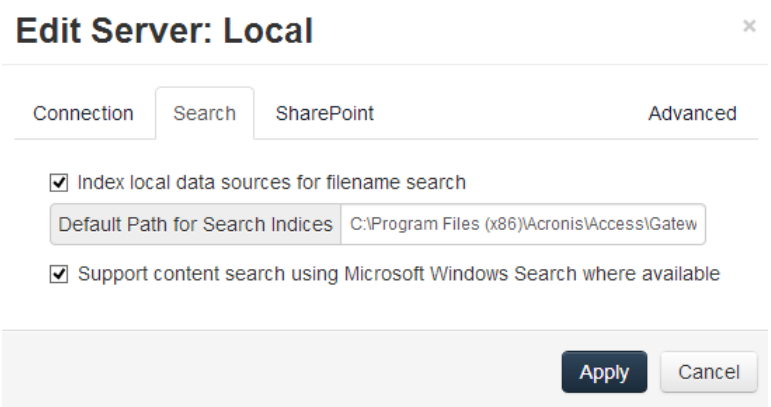
The Acronis Access Gateway Server is the server contacted by the Access Mobile Clients that handles accessing and manipulating files and folders in file servers, SharePoint repositories, and/or Sync & Share volumes. The Gateway Server is the "gateway" for mobile clients to their files.

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

- **Type** - Shows the type of the gateway, at the moment it can only be of the Server type.
- **Name** - Cosmetic name given to the gateway when you create it.
- **Address** - DNS name or IP address of the gateway.
- **Version** - Shows the version of the Acronis Access Gateway Server.
- **Status** - Shows whether the server is Online or Offline.
- **Active Sessions** - Number of currently active sessions to this Gateway Server.
- **Licenses Used** - Number of licenses used and the number of available licenses.
- **License** - Shows the current type(s) of license(s) used by the Gateway Server.

You can register new Gateway Servers using the **Add new Gateway Server** button. From the actions menu for each Gateway Server the administrator can get more details on a server and its performance, edit its configuration, change the access restrictions for the server, change licensing for the server, or remove the Gateway Server.

Search



Index local data sources for filename search

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

Default path

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

Support content search using Microsoft Windows Search where available

Copyright © Acronis International GmbH, 2002-2014

Support for content search of shared is enabled by default, and can be enabled or disabled by checking this option. You can enable or disable content searching for each Gateway Server in the Edit Server dialog.

In addition to enabling this setting, content search requires that the Microsoft Windows Search application be installed on the Acronis Access Gateway server and be configured to index any data source where content search is enabled. Windows Search is built into Windows Vista and no additional installation is required. It is also built into Windows Server 2008, but it is not enabled by default. To enable it add the Role called File Services in the Server Manager, and have the Windows Search Service enabled. Windows Search can be installed on Windows 2003 Server and Windows XP by running Windows Update. It is listed as an optional install. Once installed, Windows Search can be configured to index the necessary data sources by right clicking the Windows Search icon in the Start bar and selecting Windows Search Options. You can do Windows content searches on Windows reshares but the remote machine(s) must be in the same domain as the Gateway Server.

SharePoint

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

In this section

Registering new Gateway Servers....37
Server Details....38
Editing Gateway Servers....40
Licensing Gateway Servers....47
Cluster Groups....47

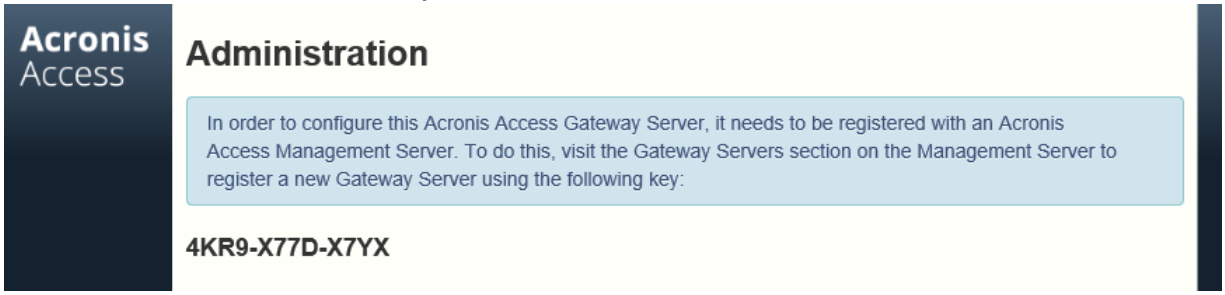
1.5.1 Registering new Gateway Servers

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

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

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

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



Copyright © Acronis International GmbH, 2002-2014

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

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

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

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

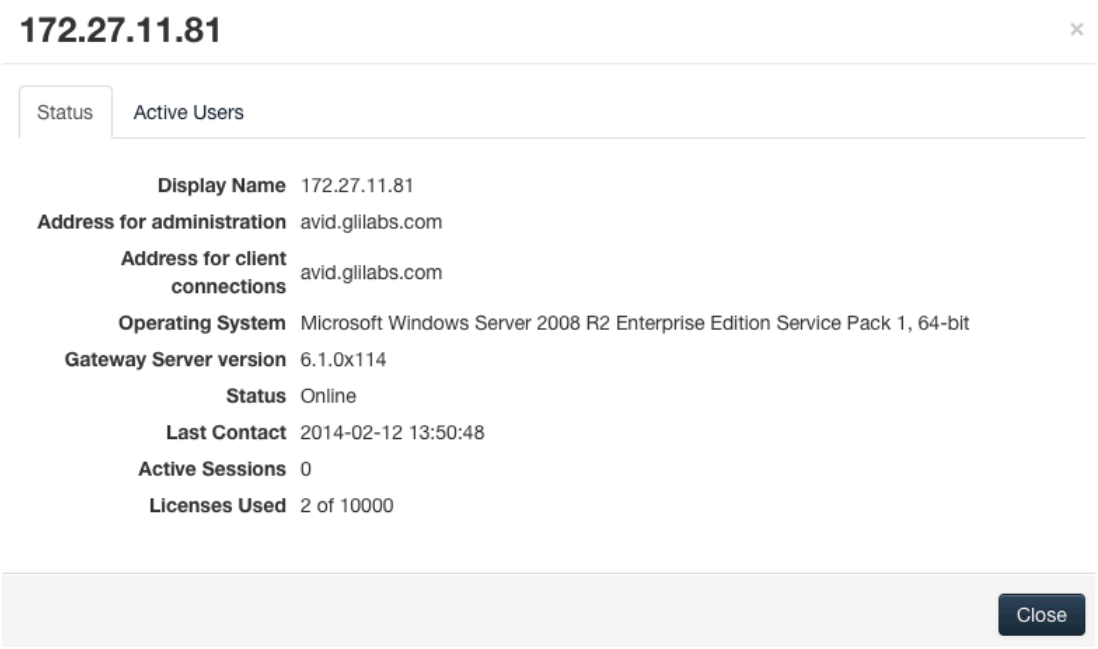
After you've registered your Gateway Server, you may want to configure custom access restrictions for this Gateway Server. For more information on this, visit the Editing Gateway Servers (p. 40) section.

1.5.2 Server Details

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

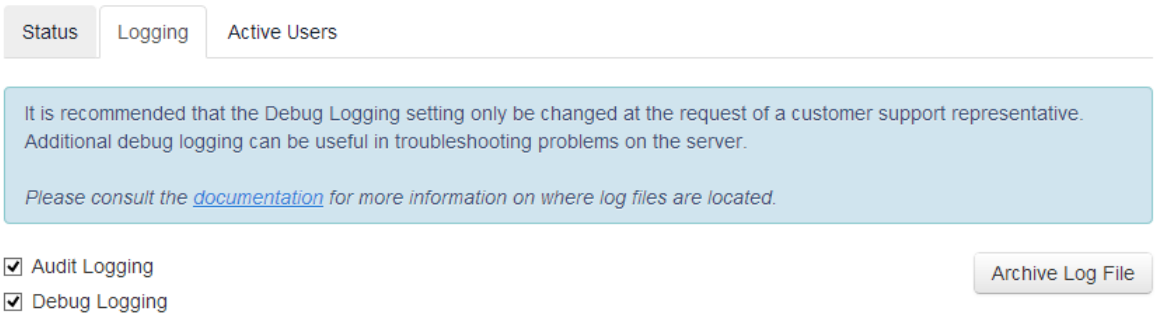
Copyright © Acronis International GmbH, 2002-2014

Status



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

Logging



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

To enable Audit Logging for a specific gateway server:

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

Copyright © Acronis International GmbH, 2002-2014

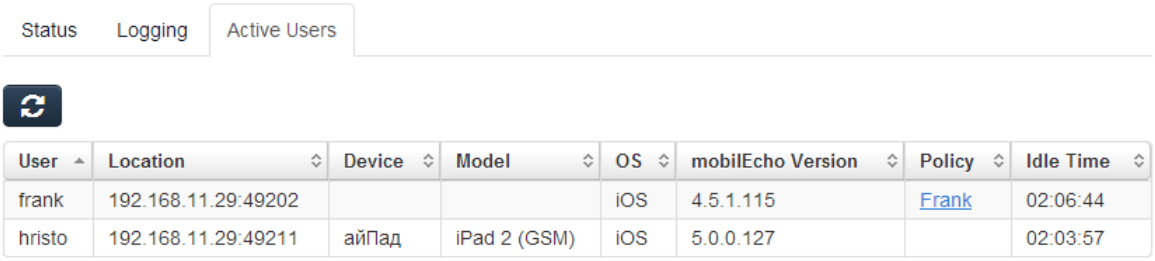
8. Press the **Save** button.

To enable Debug Logging for a specific gateway server:

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

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

Active Users



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

- **User** - Shows the user's Active Directory (full) name.
- **Location** - Shows the IP address of the device.
- **Device** - Shows the name given to the device by the user.
- **Model** - Shows the type/model of the device.
- **OS** - Shows the operating system of the device.
- **Client Version** - Shows the version of the Acronis Access app installed on the device.
- **Policy** - Shows the policy for the account used by the device.
- **Idle Time** - Shows the time the user has spent connected to the gateway.

1.5.3 Editing Gateway Servers

Access Restrictions

You can use the default access restrictions set in the Policies (p. 8) section or you can set custom access restrictions for each Gateway Server.

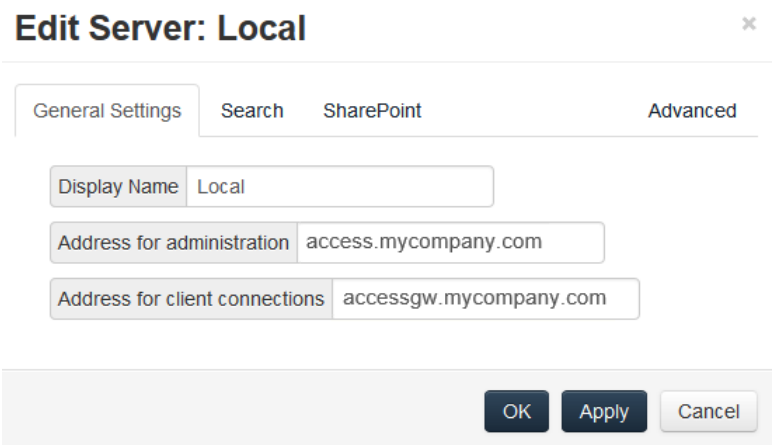
Setting custom access restrictions for this Gateway Server

1. Press the Down arrow next to the **Details** button.
2. Select **Access Restrictions**.

Copyright © Acronis International GmbH, 2002-2014

3. Open the **Use Custom settings** tab.
4. Select the specific access restrictions you want for this Gateway Server.
5. Press **Apply**.

General Settings

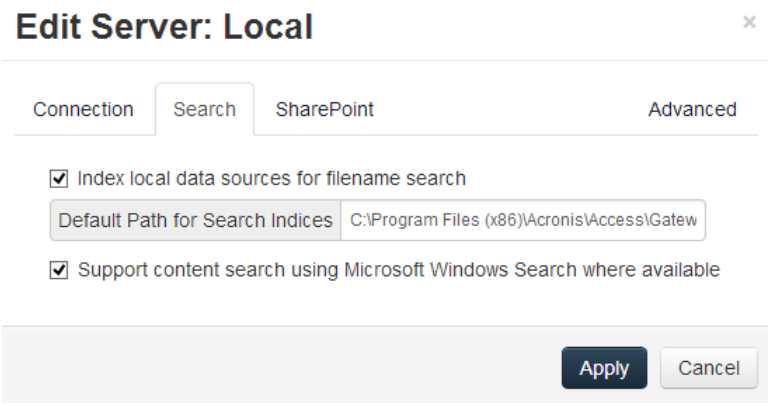


Display Name - Sets the display name of the Gateway Server.

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

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

Search



Index local data sources for filename search

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

Default path

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

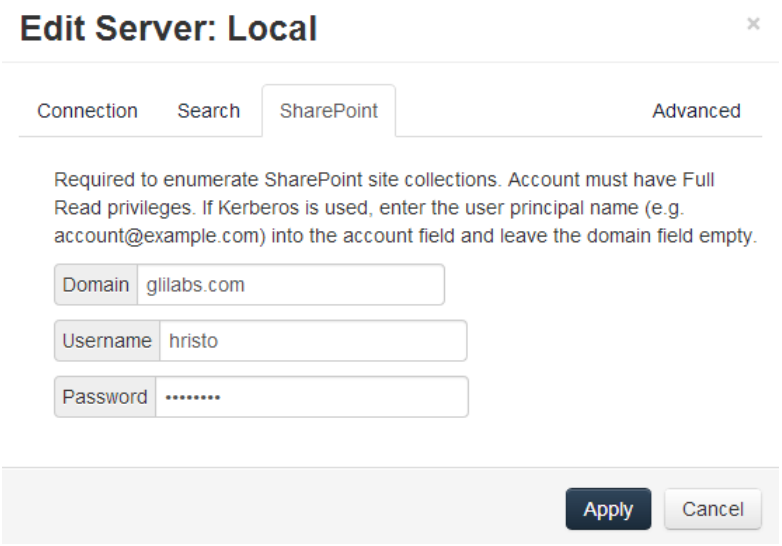
Copyright © Acronis International GmbH, 2002-2014

Support content search using Microsoft Windows Search where available

Support for content search of shared is enabled by default, and can be enabled or disabled by checking this option. You can enable or disable content searching for each Gateway Server in the Edit Server dialog.

In addition to enabling this setting, content search requires that the Microsoft Windows Search application be installed on the Acronis Access Gateway server and be configured to index any data source where content search is enabled. Windows Search is built into Windows Vista and no additional installation is required. It is also built into Windows Server 2008, but it is not enabled by default. To enable it add the Role called File Services in the Server Manager, and have the Windows Search Service enabled. Windows Search can be installed on Windows 2003 Server and Windows XP by running Windows Update. It is listed as an optional install. Once installed, Windows Search can be configured to index the necessary data sources by right clicking the Windows Search icon in the Start bar and selecting Windows Search Options. You can do Windows content searches on Windows reshares but the remote machine(s) must be in the same domain as the Gateway Server.

SharePoint

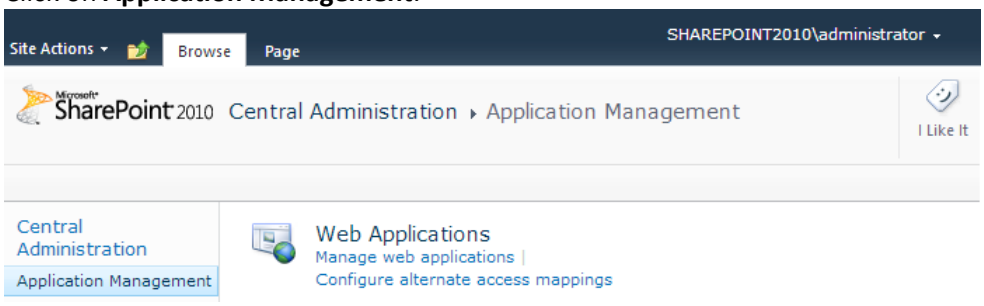


Entering these credentials is optional for general SharePoint support, but required to enumerate site collections. For example, say you have two site collections: http://sharepoint.example.com and http://sharepoint.example.com/SeparateCollection. Without entering credentials, if you create a volume pointing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

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

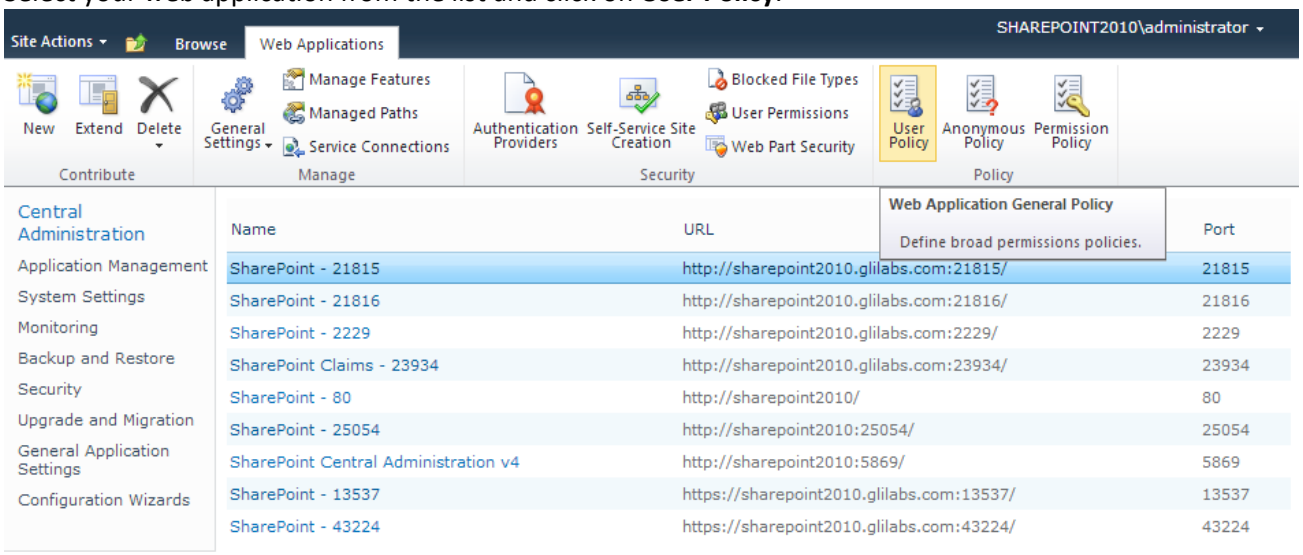
Copyright © Acronis International GmbH, 2002-2014

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

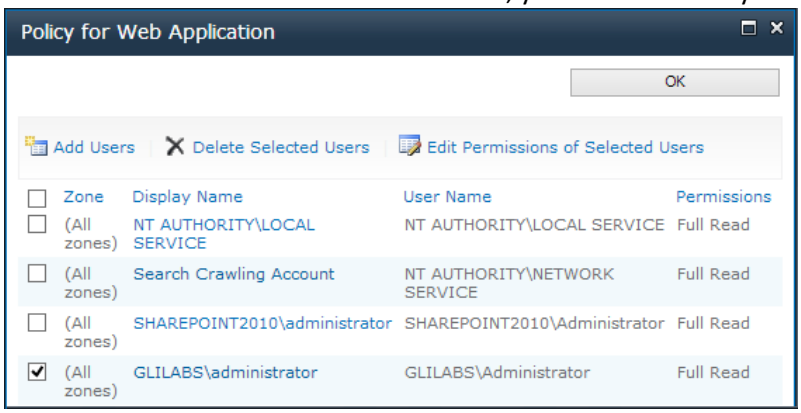


Copyright © Acronis International GmbH, 2002-2014

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

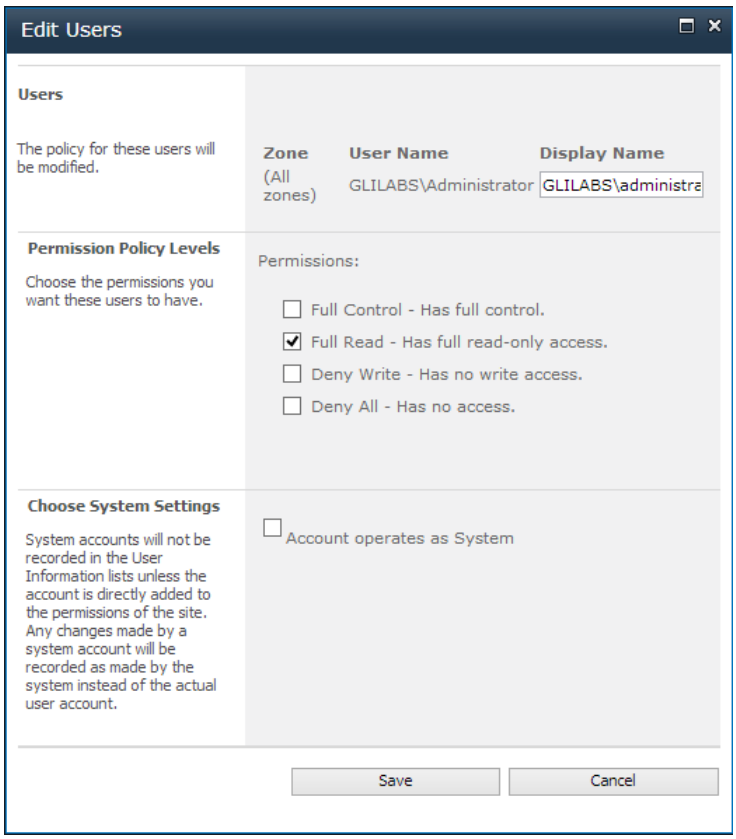


5. Select the checkbox of the user you want to give permissions to and click on **Edit Permissions of Selected Users**. If the user is not in the list, you can add him by clicking on **Add Users**.



Copyright © Acronis International GmbH, 2002-2014

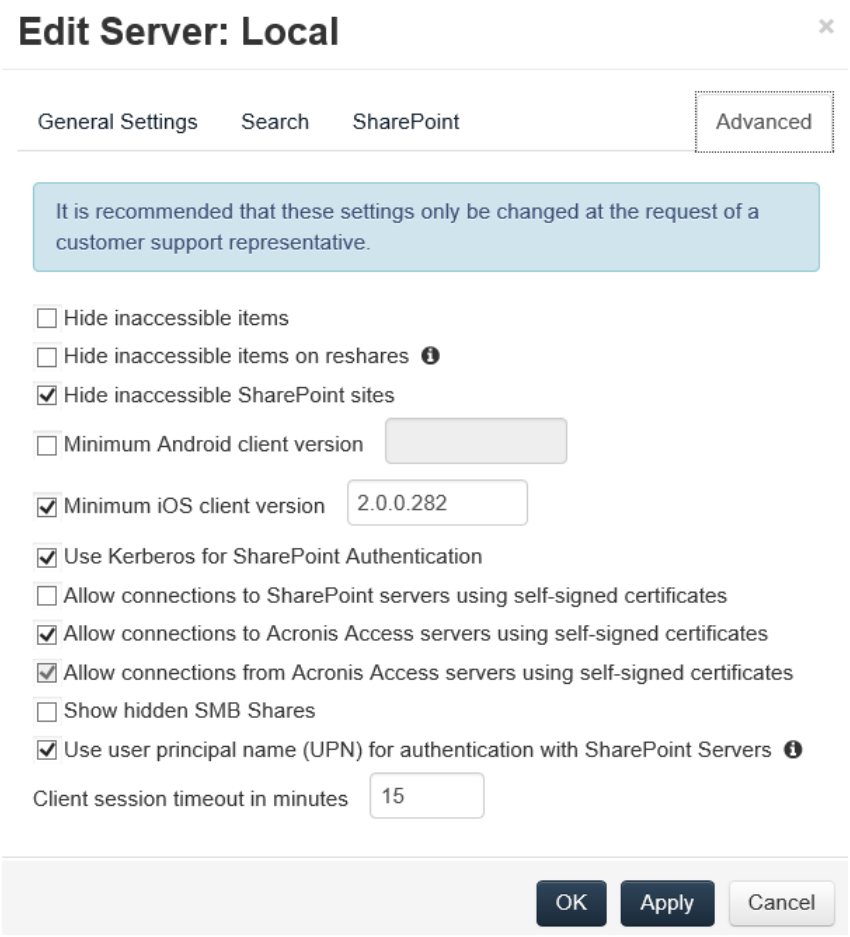
6. From the **Permission Policy** Levels section, select the checkbox for **Full Read - Has Full read-only access**.



7. Press the **Save** button.

Copyright © Acronis International GmbH, 2002-2014

Advanced



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

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

  ***Note**: Enabling this feature can have a significant negative impact while browsing folders.*
- **Hide inaccessible SharePoint sites** - When enabled, SharePoint sites for which the user does not have the necessary permissions will not be shown.
- **Minimum Android client version** - When enabled, users connecting to this Gateway will be required to have this or a later version of the Acronis Access Android client app.
- **Minimum iOS client version** - When enabled, users connecting to this Gateway will be required to have this or a later version of the Acronis Access iOS client app..
- **Use Kerberos for SharePoint Authentication** - If your SharePoint server requires Kerberos authentication, you should enable this setting. You will also need to make an update to the Active Directory computer object for the Windows server or servers that are running the Gateway server software. The Acronis Access Windows server needs to be given permission to present delegated credentials to your SharePoint server on behalf of you users. Enabling the Acronis Access Windows server to perform Kerberos Delegation:

Copyright © Acronis International GmbH, 2002-2014

1. In **Active Directory Users and Computers**, locate the Windows server or servers that you have the Gateway Server installed on. They are commonly in the **Computers** folder.
2. Open the **Properties** window for the Windows server and select the **Delegation** tab.
3. Select **Trust this computer for delegation to specified services only**
4. Select **Use any authentication protocol**, this is required for negotiation with the SharePoint server.
5. You must now add any SharePoint servers that you would like your users to be able to access using Acronis Access. If your SharePoint implementation consists of multiple load balanced nodes, you will need to add each SharePoint/Windows node to this list of permitted computers. Click **Add...** to search for these Windows computers in AD and add them. For each, you will need to select the "http" service type only.

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

- **Allow connections to SharePoint servers using self-signed certificates** - When enabled, allows connections from this Gateway to SharePoint servers using self-signed certificates.
- **Allow connections to Acronis Access servers with self-signed certificates** - When enabled, allows connections from this Gateway to Acronis Access servers using self-signed certificates.
- **Allow connections from Acronis Access servers with self-signed certificates** - When enabled, allows connections to this Gateway from Acronis Access servers using self-signed certificates.
- **Show hidden SMB Shares** - When enabled, shows hidden system SMB shares to the users.
- **Client session timeout in minutes** - Sets the time before an inactive user is kicked out of the Gateway Server.
- **Use user principal name (UPN) for authentication with SharePoint Servers** - When enabled, users will authenticate to SharePoint servers via their user principal name (e.g. hristo@glilabs.com), otherwise they will authenticate with domain/username (e.g. glilabs/hristo).

1.5.4 Licensing Gateway Servers

For more information on licensing your Gateway Servers, visit the Licensing (p. 77) section.

1.5.5 Cluster Groups

In Acronis Access version 5.1 or newer, you have the ability to create a cluster group of Gateway Servers.

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

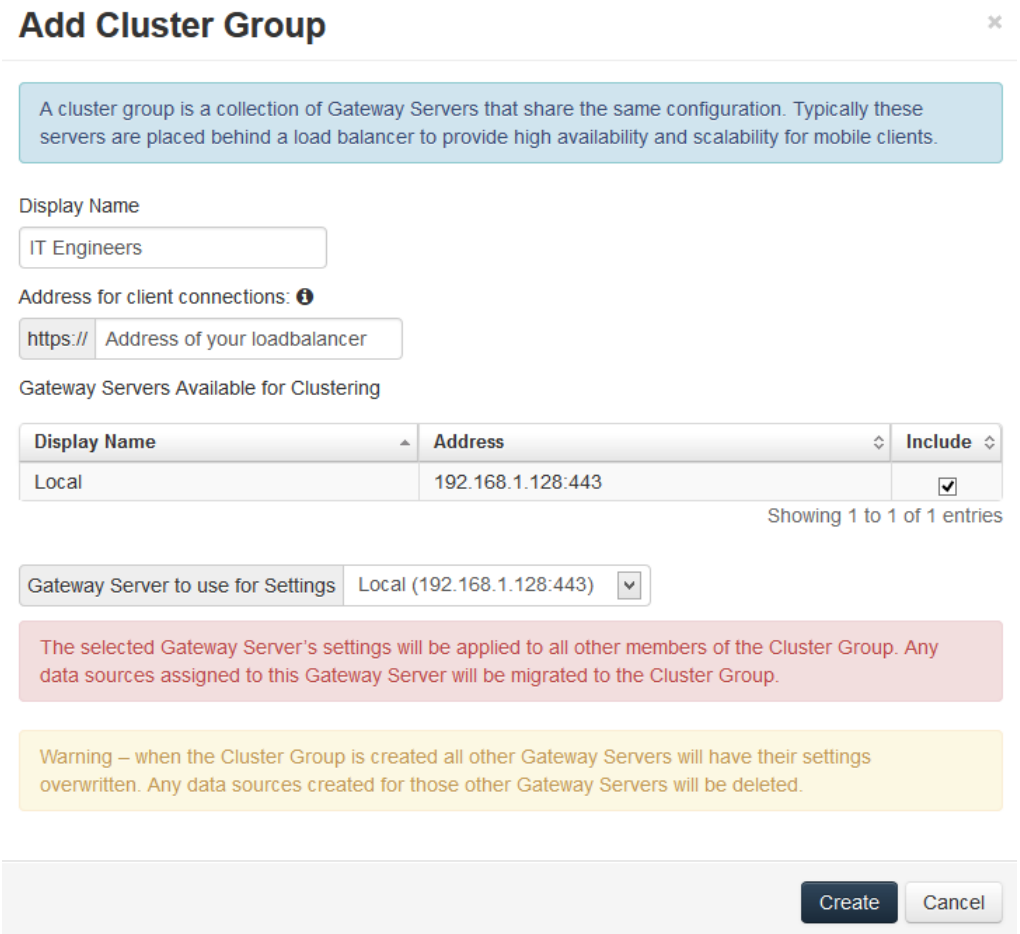
For a clustered gateway setup, you need a load balancer, two or more gateways and an Acronis Access Server. All of your Gateway Servers should be added to a Cluster Group in the Acronis Access web interface and placed behind the load balancer. Your Acronis Access Server acts as both your management server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

Copyright © Acronis International GmbH, 2002-2014

To create a cluster group:

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

1. Open the Acronis Access Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Gateway Servers** page.
4. Press the **Add Cluster Group** button.
5. Enter a display name for the group.
6. Enter the DNS name or IP address of the load balancer.
7. Mark the checkbox for each Gateway you want to be in the group.
8. Select the Gateway which will control the group's settings. All of the existing settings on that Gateway (including assigned Data Sources and excluding the address for administration) will be copied to every Gateway in the group.



9. Press **Create**.

Editing a cluster group:

Editing cluster groups does not differ from editing regular Gateways. For more information visit the Editing Gateway Servers (p. 40) article.

Copyright © Acronis International GmbH, 2002-2014

Adding members to an existing cluster group:

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

1.6 Managing Data Sources

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

Access to SharePoint 2007, 2010, 2013, 365 content

Acronis Access can provide access to files residing in document libraries on SharePoint 2007, 2010, 2013 and 365 servers. An Acronis Access SharePoint data source can point to an entire SharePoint server, a specific SharePoint site or sub-site, or a specific document library. These files can be opened, PDF annotated, edited, and synced, just like files that reside in traditional file server or NAS storage. Acronis Access also supports Check Out and Check In of SharePoint files.

SharePoint authentication methods supported

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

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

Changing Permissions for Shared Files and Folders

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

Copyright © Acronis International GmbH, 2002-2014

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

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

In this section

Folders.....50
Assigned Sources.....53
Gateway Servers Visible on Clients.....54
Legacy Data Sources.....55

1.6.1 Folders

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

Folders can point to any type of content that Acronis Access is providing access to. They simply refer to locations in Gateway Servers that have already been configured within the Acronis Access management. This can be a local file share volume, a "network reshare" volume providing access to files on another file server or NAS, a DFS share or a SharePoint volume.

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

\\company.com\namespace\share

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

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

Require Salesforce activity logging

Copyright © Acronis International GmbH, 2002-2014

Acronis has partnered with Salesforce to offer an option for logging access to files shown to customers using Acronis Access. Enabling this option will require any user who has this folder assigned to their management policy to log a customer activity in Saleforce before they can open any file in the folder. This is done completely within the Access Mobile Client app.

- All items in this folder will be restricted from being emailed, printed, copied or moved outside this folder, or opened in other apps on the device.
- This feature requires an Acronis Access client and server of version 5.0 or later.
- Acronis Access for Android clients does not support this Salesforce integration.

SharePoint Sites and Libraries

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

- Creating a Data Source for a whole SharePoint site or subsite

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

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

- Creating a Data Source for **a SharePoint Library**

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

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

- Creating a Data Source for **a specific folder within a SharePoint Library**

When creating a Data Source for a specific folder within a SharePoint Library, you will have to fill in all fields. In the URL field you enter the address of your SharePoint site or subsite, for the Document Library Name field you enter the name of your Library and for the Subpath field you enter the name of the desired folder.

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

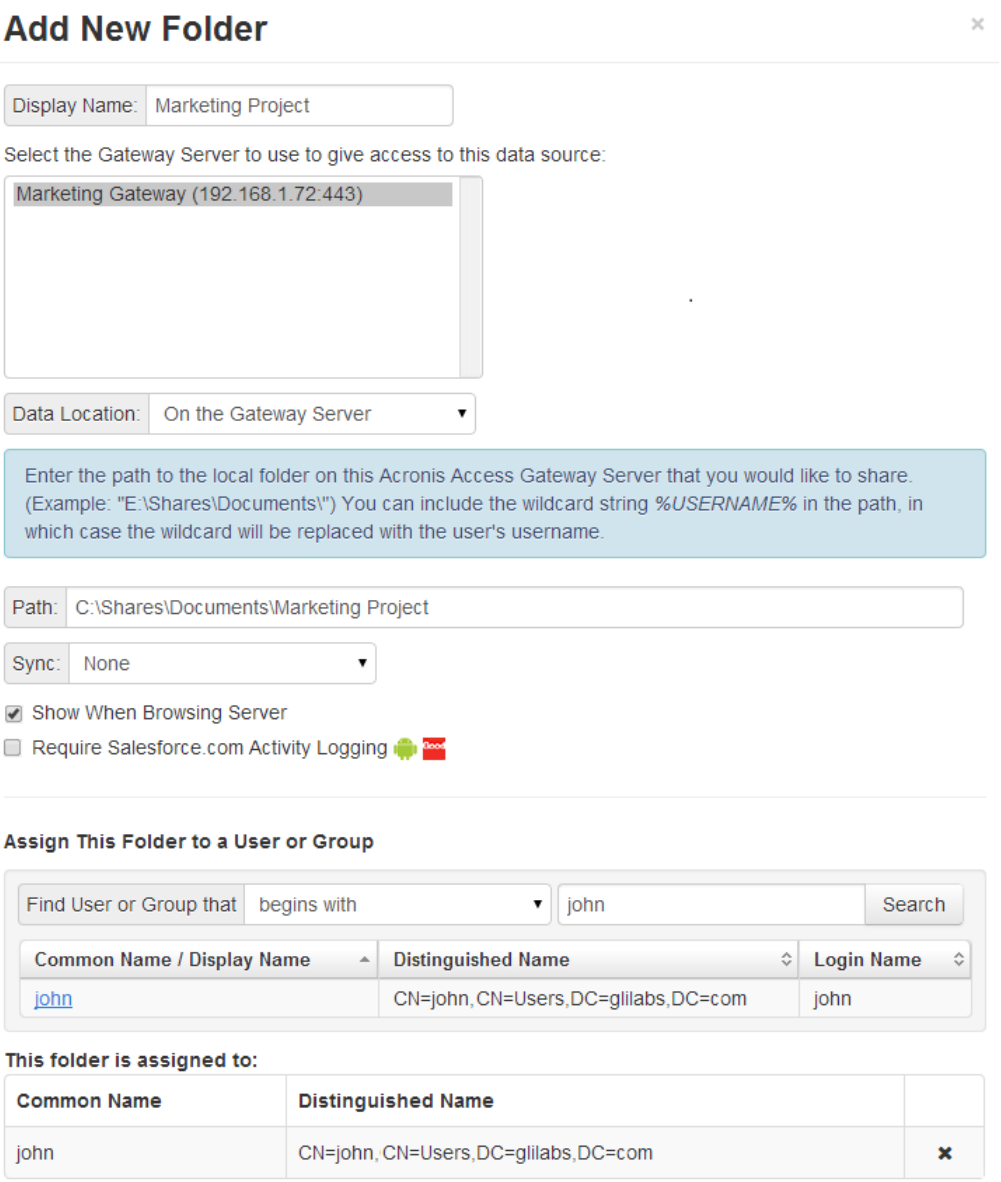
Note: *When creating a Data Source pointing to a SharePoint resource using a Subpath, you cannot enable the* ***Show When Browsing Server*** *option.*

The Access Mobile Client supports NTLM, Kerberos Constrained Delegation, Claims based and SharePoint 365 authentication. Depending on your SharePoint setup, you may need to make some additional configurations to the Gateway Server used to connect to these Data Sources. For more information visit the Editing Gateway Servers (p. 40) article.

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

Copyright © Acronis International GmbH, 2002-2014

Creating a Data Source



To create a Data source:

1. Open the Acronis Access Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Data Sources** tab.
4. Go to **Folders**.
5. Press the **Add New Folder** button.
6. Enter a display name for the folder.
7. Select the Gateway Server which will give access to this folder.
8. Select the location of the data. This can be on the actual Gateway Server, on another SMB server, on a SharePoint Site or Library or on a Sync & Share server.

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

9. Based on your choice of location, enter the path to that folder, server, site or library.

Copyright © Acronis International GmbH, 2002-2014

10. Select the **Sync** type of this folder.
11. Enable **Show When Browsing Server** if you want this Data Source to be visible when Acronis Access mobile clients browse the Gateway Server.
12. Select if the folder should require Salesforce activity logging.
13. Find and select the User or Group the folder will be assigned to.
14. Press the Save button.

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

1.6.2 Assigned Sources

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

The Servers table lists the Gateway Server's display name, DNS name or IP address and the policies to which this server is assigned.

Servers

Display Name	Address	Assigned to
Local	192.168.1.128:443	Michael Collins

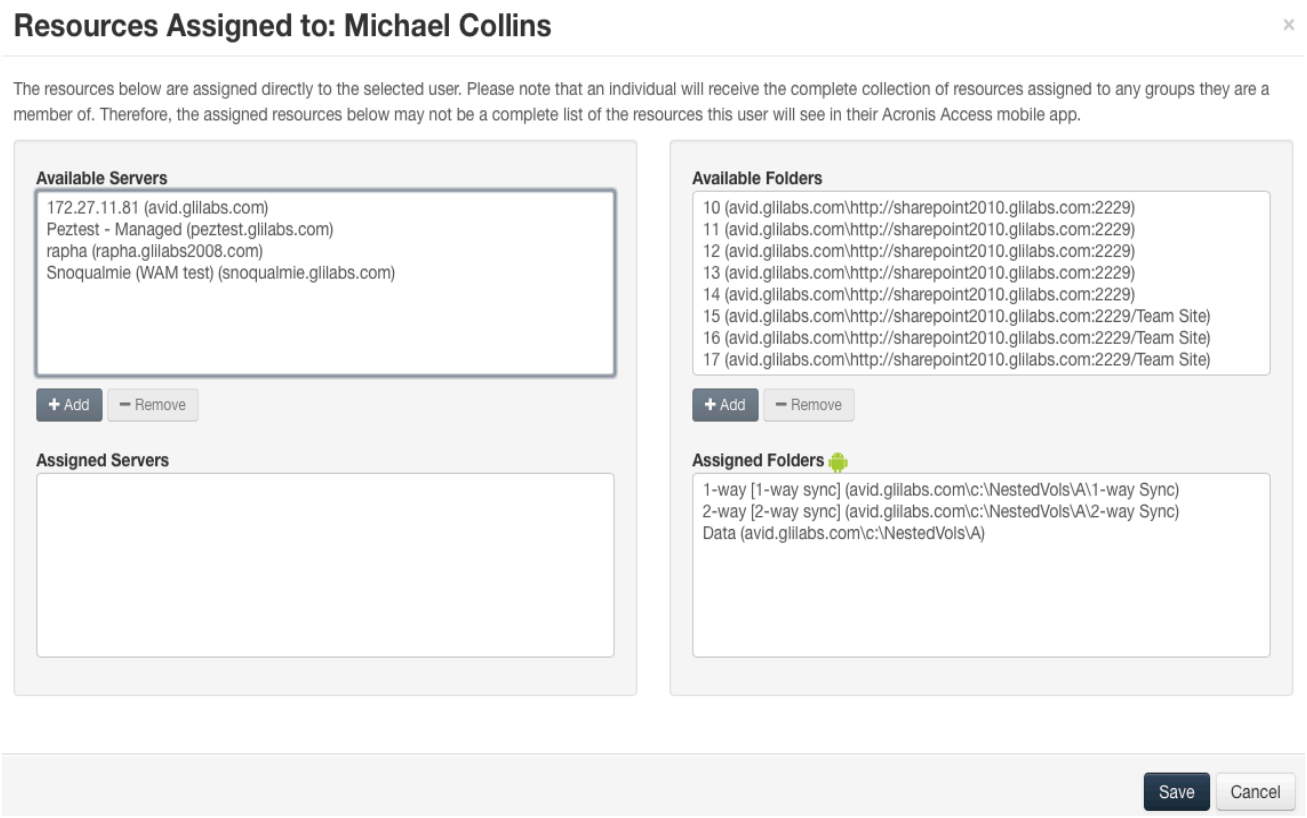
The Folders table lists the Data Source's display name, Gateway Server, sync type, path and the policies to which this Data Source is assigned.

Folders

Display Name	Server	Sync	Path	Assigned to
Data	172.27.11.81	None	c:\NestedVols\A	Michael Collins
2-way	172.27.11.81	2-way	c:\NestedVols\A\2-way Sync	Michael Collins
1-way	172.27.11.81	1-way	c:\NestedVols\A\1-way Sync	Michael Collins

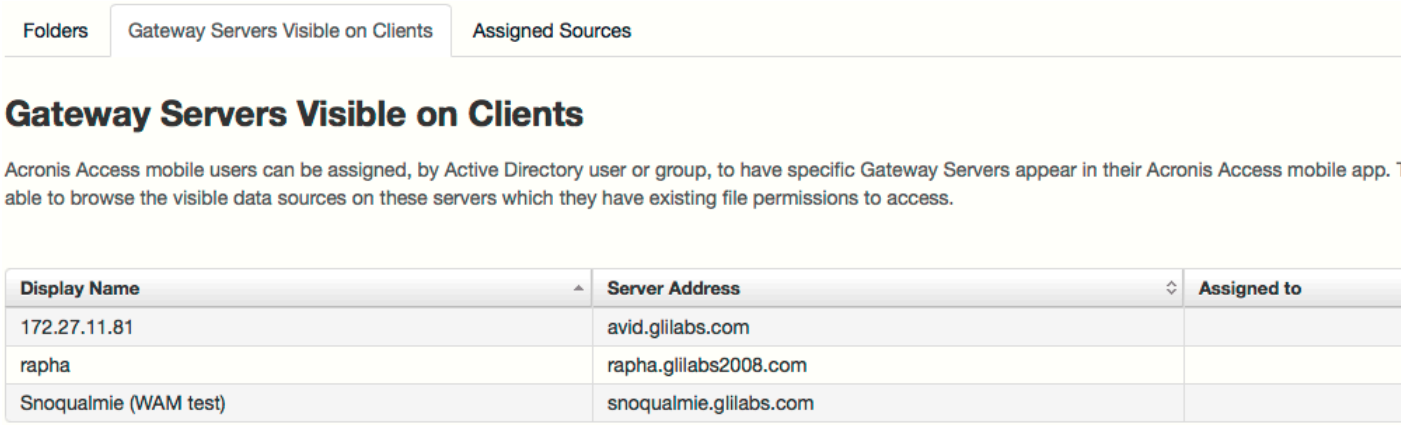
Copyright © Acronis International GmbH, 2002-2014

By pressing the **Edit resources assigned to** button, the administrator can quickly edit the assignments for this policy.



1.6.3 Gateway Servers Visible on Clients

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



To edit the current assignment of a server:

1. Press the **Edit** button on that server.
   - If you want to unassign this server from a user, press the **X** for that user.

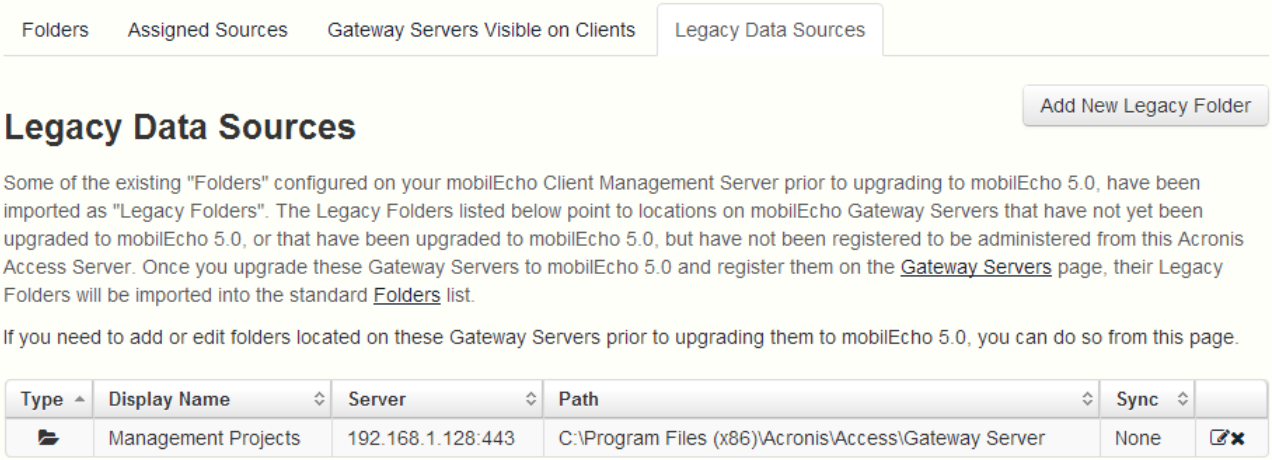
Copyright © Acronis International GmbH, 2002-2014

- If you want to assign a new User or Group to this server, find the User/Group name and press it.

2. Press the **Save** button.

1.6.4 Legacy Data Sources

If you have updated to Acronis Access from a previous mobilEcho installation, all of your assigned folders will carry over automatically and will be put in this section. If you're still using a mobilEcho 4.5 server or older, you can also create a volume in the mobilEcho Administrator, and add it to the Legacy Data Sources from this page.



Adding a new legacy folder

1. Press the **Add New Legacy Folder** button.
2. Enter a **Display Name**. This name will be shown in the mobilEcho client application.
3. Select the mobilEcho server that contains the mobilEcho volume where the folder is located.
4. Enter the folder's Path. The path must begin with the mobilEcho shared volume name. If the path of the folder specific doesn't start with a mobilEcho volume name, the folder will not function when users try to access it. If you would like to give access to a subfolder in that shared volume, include the full path to that subfolder in the Path field.
   - You can include the wildcard string %USERNAME% in the path. This wildcard will be replaced with the user's account username.
   - SharePoint sites and document libraries are displayed when browsing in the mobilEcho app using their "Title". It is possible for a site's title to be different from the site's URL name. For example, http://sharepoint.company.com/testsite might have a title of "Test Site". You may use either the URL path or the Title when configuring Folders that point to SharePoint locations. The entire path that you specify must use either the titles or URL names of any sites, subsites, and document libraries referenced in the path.
5. Choose a Sync option. **None**, **1-way**, or **2-way**.
6. Optionally, enable **Require Salesforce activity logging**.
7. Search for an Active Directory User and Group you'd like to assign this new folder to, and click the user or group name. This will result in the folder automatically appearing in that user's or group's mobilEcho app.
8. Press the **Save** button.

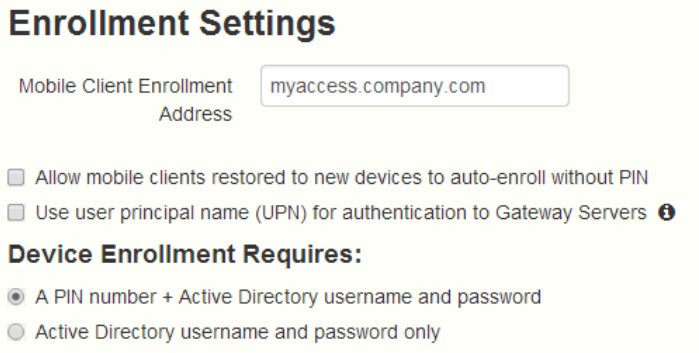
Copyright © Acronis International GmbH, 2002-2014

To move your Legacy Data Sources to the new system:

1. Find the mobilEcho File Server on which the Data Source resides.
2. Upgrade the mobilEcho File Server to the Acronis Access Gateway server.
3. Open the Acronis Access web interface and log in as an administrator.
4. Open the **Gateway Servers** tab.
5. Add your server to the list of Gateway Servers. For more information on this process, visit the Managing Gateway Servers (p. 36) section.
6. Add a license for the Gateway Server.
7. Repeat this process for every Legacy data source.

After these steps, the Legacy Data Sources tab will disappear and all of your Legacy Data Sources will be moved to the Folders section.

1.7 Settings



Enrollment Settings

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

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

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

Device Enrollment Requires:

- **PIN number + Active Directory username and password** - In order to activate their Acronis Access app and gain access to Acronis Access servers, a user is required to enter an expiring, one-time use PIN number and a valid Active Directory username and password. This option ensures that a user can only enroll one device, and only after receiving a PIN number issued by their IT administrator. This option is recommended when the enhanced security of two-factor device enrollment is required.

Copyright © Acronis International GmbH, 2002-2014

- **Active Directory username and password only** - A user can activate their Acronis Access app using only their Active Directory username and password. This option allows a user to enroll one or more devices at any point in the future. Users just need to be given the name of their Acronis Access Client Management server, or a URL pointing to their Acronis Access Client Management server, which can be posted on a web site or emailed, simplifying the rollout of Acronis Access to large numbers of users. This option is preferred in environments where two-factor enrollment is not required and many users may need access to Acronis Access at any time, such as student deployments.

Copyright © Acronis International GmbH, 2002-2014

2 Sync & Share

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

In this section

Managing Users 58
Sharing Restrictions 60
LDAP Provisioning 61
Quotas.....62
File Purging Policies.....63
User Expiration Policies.....64
File Repository.....65
Acronis Access Client.....66

2.1 Managing Users

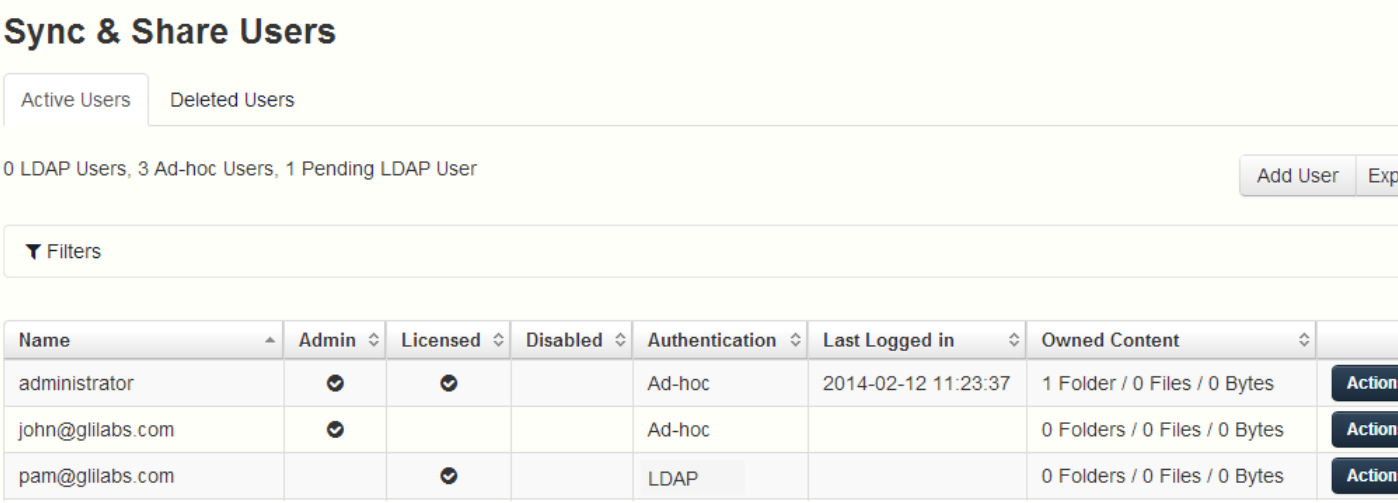
Active Users

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

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

- Ad-hoc users can be created in several ways - via email invitation or via an invitation to a shared folder. These users are not licensed by default and the administrator must convert them to licensed manually. If a user is not licensed, he cannot create, share or upload folders and files or use the desktop client but he can still access files and folders shared with him by other users.
- LDAP users and users with administrative rights are automatically licensed at creation. They are able to create and upload files and folders as well as share those files and folders with other users. They can use the desktop client as well. Unless you have setup a Provisioned LDAP group (p. 61) you will have to create your LDAP users the same way as the Ad-hoc users, but you won't have to license them manually. Administrators without Sync & Share allowed do not need to have an email address set - they can simply log in with their LDAP credentials. These administrators can be added without having setting up SMTP for your Acronis Access Server. For more information visit the Administrators and Privileges (p. 67) article.

Copyright © Acronis International GmbH, 2002-2014



- **Name** – shows the name used to login to the server.
- **Admin** – if the user has administrator privileges there will be a check mark.
- **Licensed** - if the user is licensed there will be a check mark.
- **Disabled** – if this account is disabled there will be a check mark.
- **Authentication** – shows whether the user authenticates using his LDAP credentials or through Ad-hoc.
- **Last Logged in** – time and date of last log in.
- **Owned Content** – shows the number of folders, files and the total size of the user's content.
- **Actions**
  - **Edit** - Allows you to edit this user.
  - **Delete** - Deletes the user.

Adding an Ad-Hoc user

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

The user will receive an email with a link. Once he opens the link, he will be asked to set a password and his account will be complete.

Adding an LDAP user

1. Open the Acronis Access Web Interface.

Copyright © Acronis International GmbH, 2002-2014

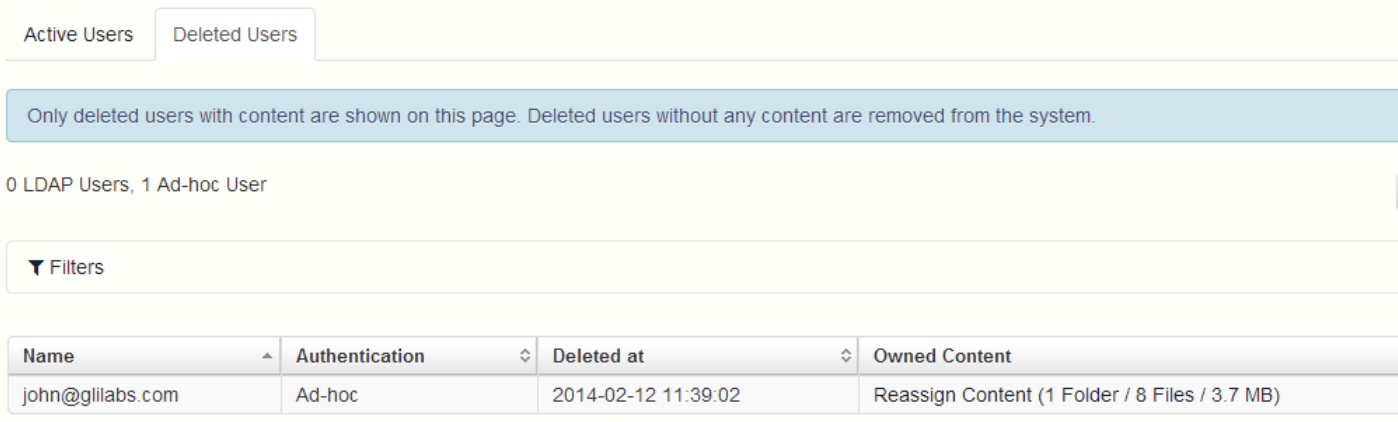
2. Log in with an administrator account. An account with the **Manage Users** rights can be used as well.
3. Open the **Sync & Share** tab.
4. Open the **Users** tab.
5. Press the **Add User** button.
6. Write the email of the user.
7. Select whether the user should have administrative rights or not.
8. Select the language of the invitation.
9. Press the **Add** button.

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

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

Deleted Users

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



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

2.2 Sharing Restrictions

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

Single File Sharing Expiration

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

Copyright © Acronis International GmbH, 2002-2014

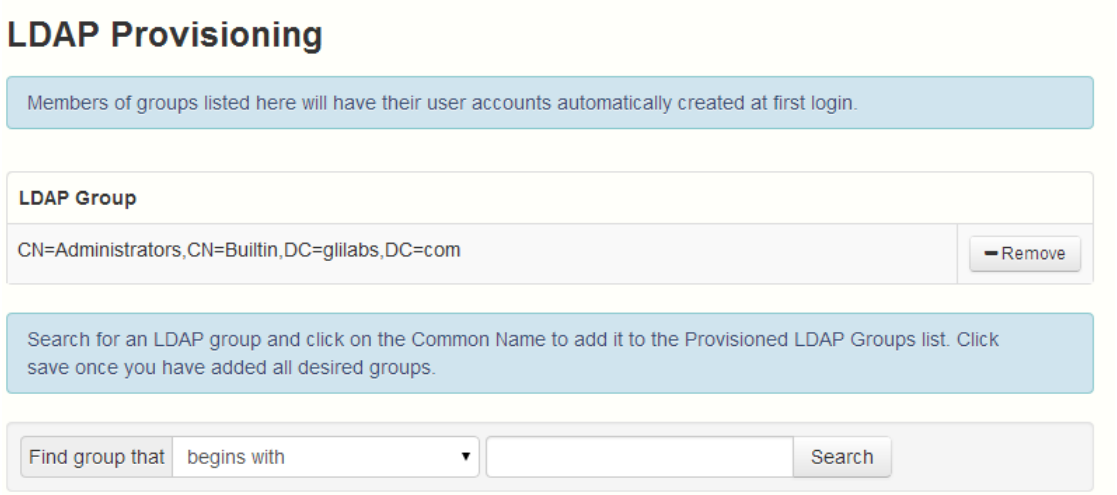
- **Minimum Expiration Time** - Controls the minimum amount of time (in days) that the users can set.
- **Maximum Expiration Time** - Controls the maximum amount of time (in days) that the users can set.

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

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

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

2.3 LDAP Provisioning



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

LDAP Group

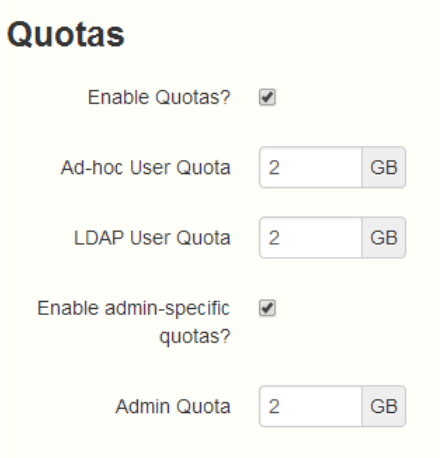
This is the list of currently selected groups.

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

Copyright © Acronis International GmbH, 2002-2014

2.4 Quotas

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



There are distinct default settings for external (ad-hoc) and internal (Active Directory - LDAP) users. Administrators can also assign different quota values based on individual users or Active Directory group membership.

- **Enable Quotas?** - If enabled, limits the maximum space a user has by a quota.
  - **Ad-hoc User Quota** - Sets the quota for Ad-Hoc users.
  - **LDAP User Quota** - Sets the quota for LDAP users.
  - **Enable admin-specific quotas?** - If enabled, administrators will have a separate quota applied to them.
    - **Admin Quota** - Sets the quota for administrators.

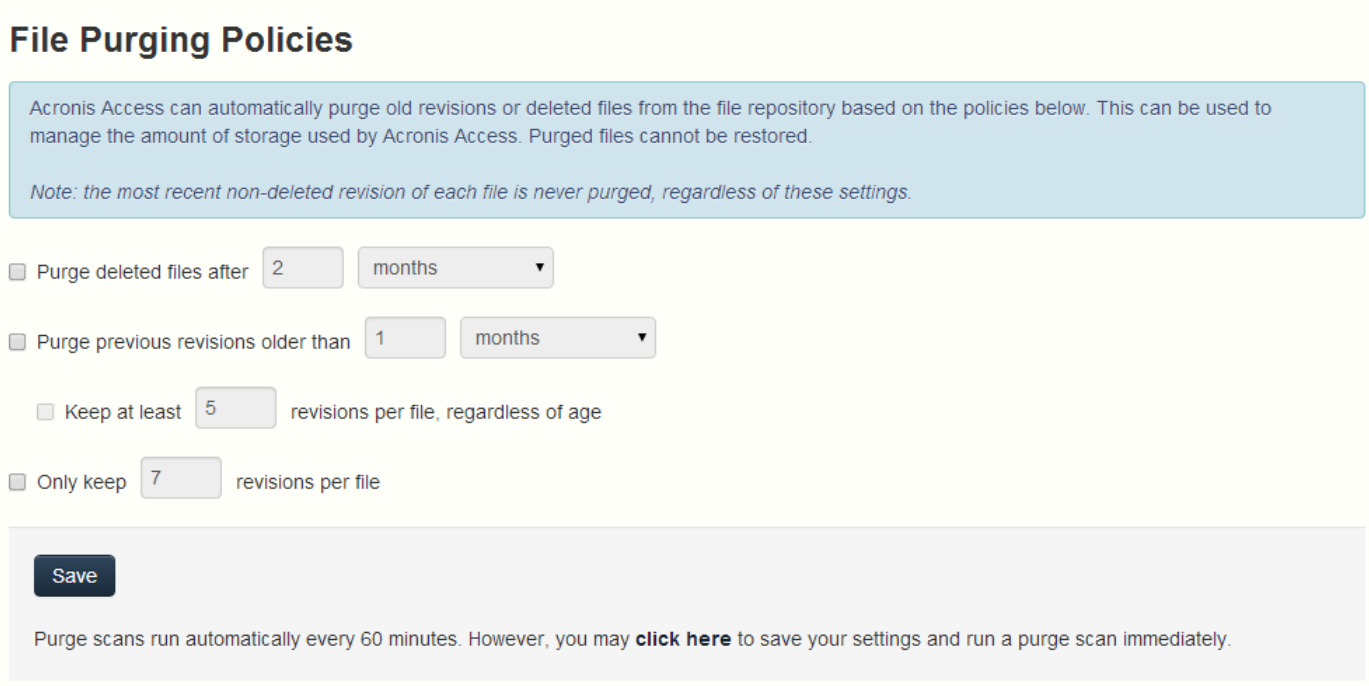
Note: *If a user is a member of multiple groups, only the biggest quota is applied.*

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

Copyright © Acronis International GmbH, 2002-2014

2.5 File Purging Policies

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



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

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

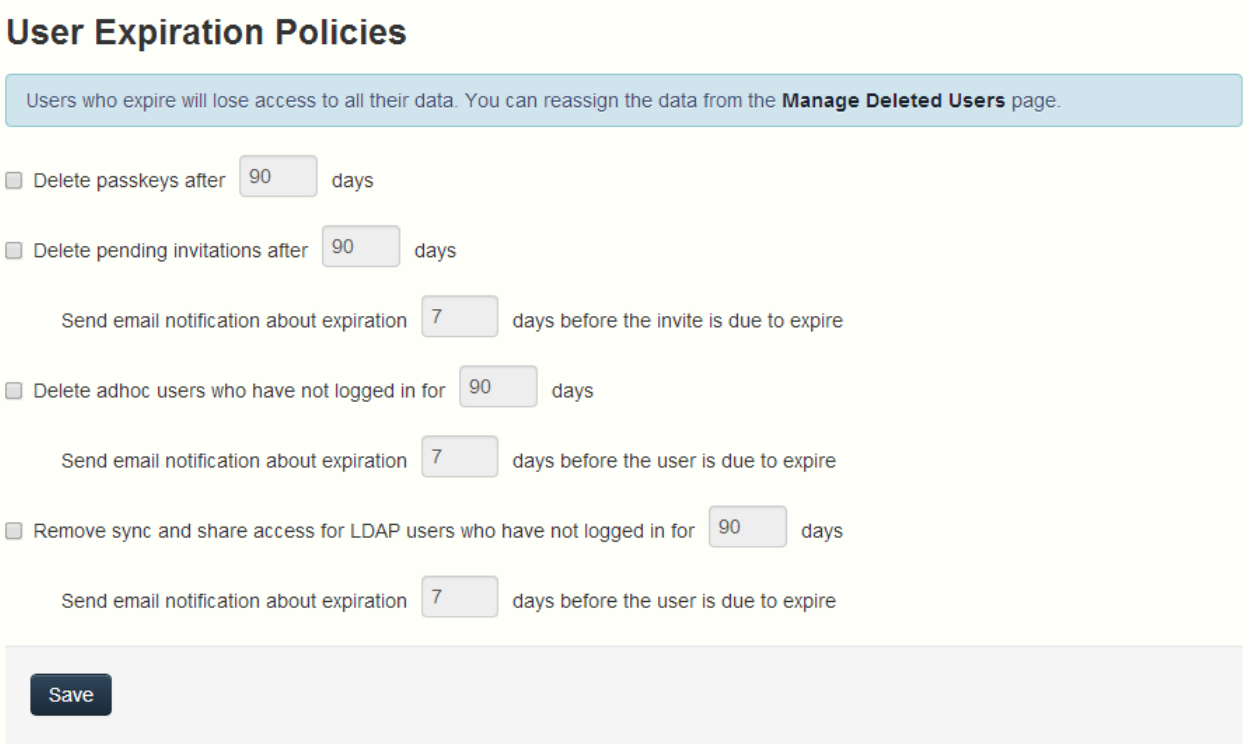
- **Purge deleted files after** - If enabled, files older than this setting will be purged.
- **Purge previous revisions older than** - If enabled, file revisions older than this setting will be purged.
  - **Keep at least X revisions per file, regardless** - If enabled, keeps a minimum number of revisions per file, regardless of their age.
- **Only keep X revisions per file** - If enabled, limits the maximum number of revisions per file.

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

Copyright © Acronis International GmbH, 2002-2014

2.6 User Expiration Policies

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

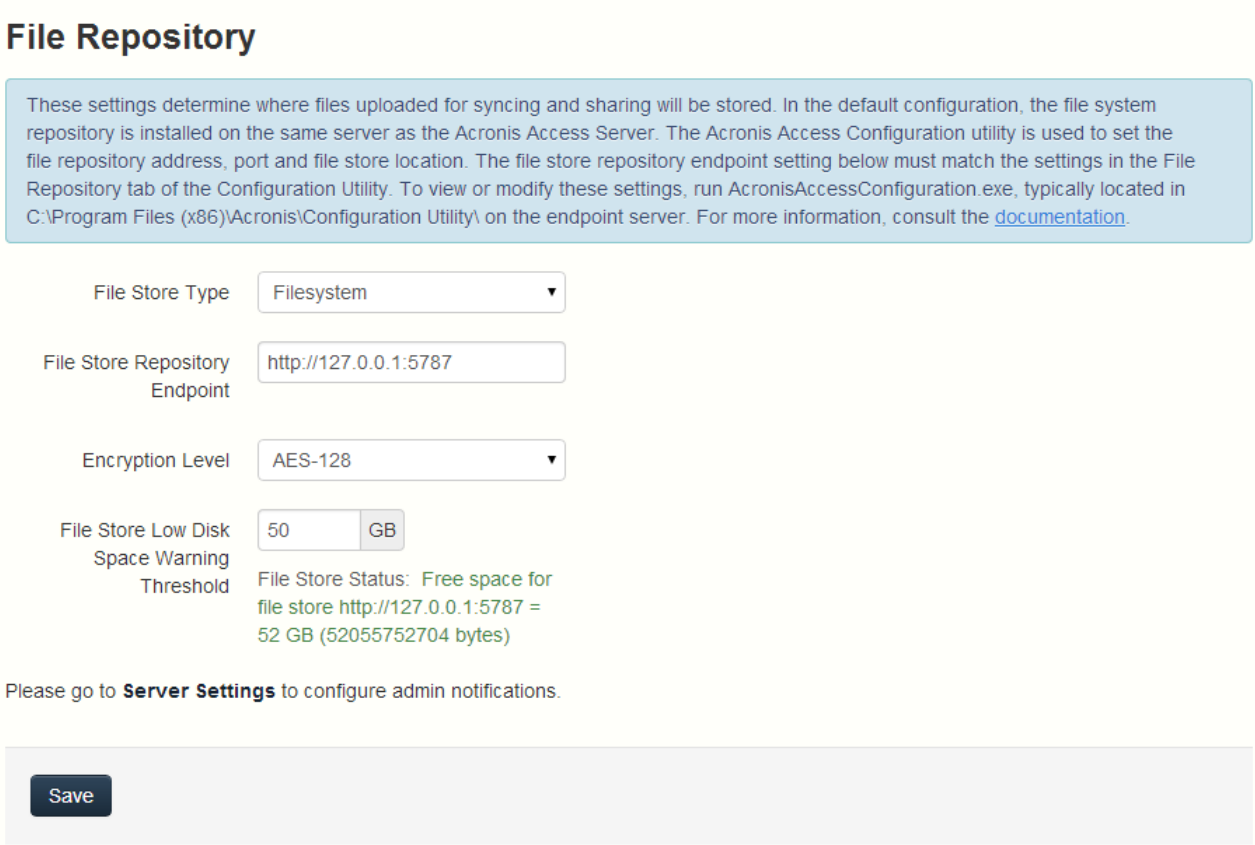


- **Delete passkeys after X days** - If enabled, deletes all passkeys after a set number of days.
- **Delete pending invitations after X days** - If enabled, deletes all pending invitations after a set number of days.
  - **Send email notification about expiration X days before the invite is due to expire**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

Copyright © Acronis International GmbH, 2002-2014

2.7 File Repository

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

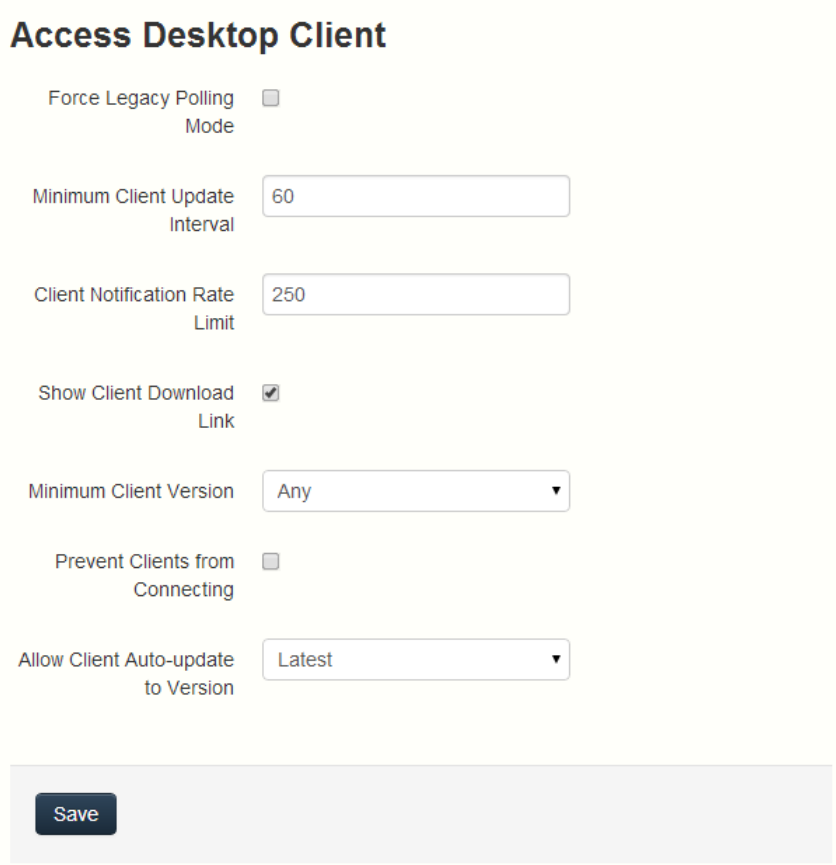


- **File Store Type** - Select the storage location you would like to use for the virtual file system's repository. The options are File System and Amazon S3.
- **File Store Repository Endpoint** - Set the URL address of the file system repository endpoint.
- **Encryption Level** - Specify the type of encryption that should be used to encrypt files stored in the virtual file system's repository. The options are None, AES-128 and AES-256. The default is AES-128.
- **File Store Low Disk Space Warning Threshold** - After the free space goes below this threshold, the administrator will receive notifications of low disk space.

Copyright © Acronis International GmbH, 2002-2014

2.8 Acronis Access Client

These settings are for the Access Desktop Client.



- **Force Legacy Polling Mode** - Forces the clients to poll the server instead of being asynchronously notified by the server. You should only enable this option if instructed to do so by Acronis support.
  - **Client Polling Time** - Sets the time intervals in which the client will poll the server. This option is available only when **Force Legacy Polling Mode** is enabled.
- **Minimum Client Update Interval** - Sets the minimum time (in seconds) the server will wait before re-notifying a client that updated content is available.
- **Client Notification Rate Limit** - Sets the maximum number of client update notifications the server will send per minute.
- **Show Client Download Link** - If enabled, web users will be shown a link to download the desktop client.
- **Minimum Client Version** - Sets the minimum client version that can connect to the server.
- **Prevent Clients from Connecting** - If enabled, Access Desktop Clients will not be able to connect to the server. In general, this should be enabled only for administrative purposes. This does not prevent connections to the web interface.
- **Allow Client Auto-update to Version** - Sets the Access Desktop Client version that will be deployed to all Access Desktop Clients via auto-update checks. Select **Do not allow updates** to prevent clients from auto-updating at all.

Copyright © Acronis International GmbH, 2002-2014

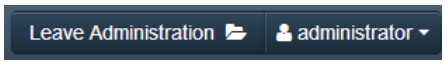
3 Server Administration

In this section

Administering a Server 67
Administrators and Privileges 67
Audit Log 70
Server 72
SMTP 73
LDAP 74
Email Templates 75
Licensing 77
Debug Logging 78
Monitoring 80

3.1 Administering a Server

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



To switch between modes, do the following:

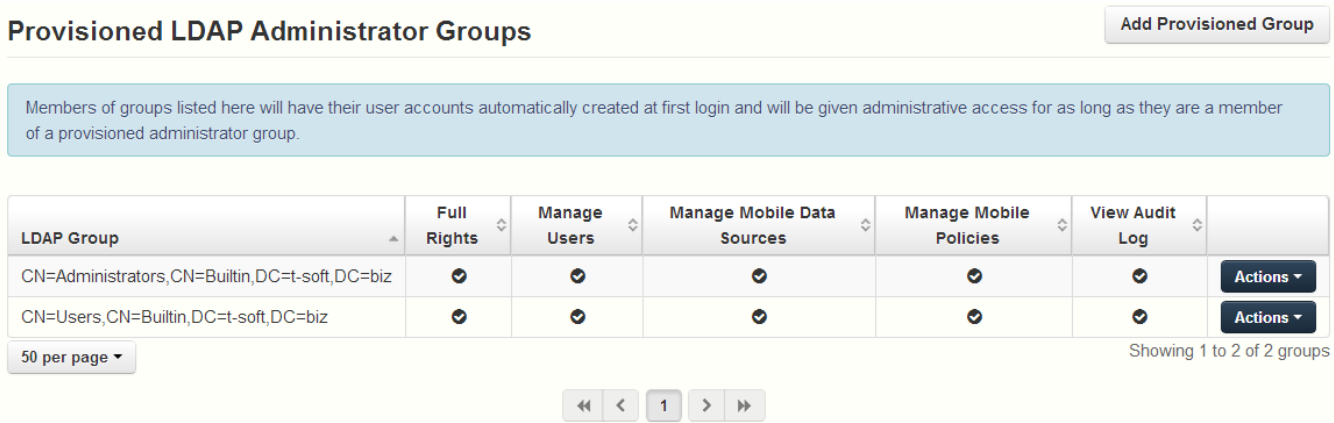
1. Open the web interface and log in as an administrator.

- To exit administration, press the **Leave Administration** button at the top-right. This takes you to the user side of the web interface.
- To go back into administration, press the **Administration** button at the top-right. This will take you back into administration mode.

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

3.2 Administrators and Privileges

Provisioned LDAP Administrator Groups

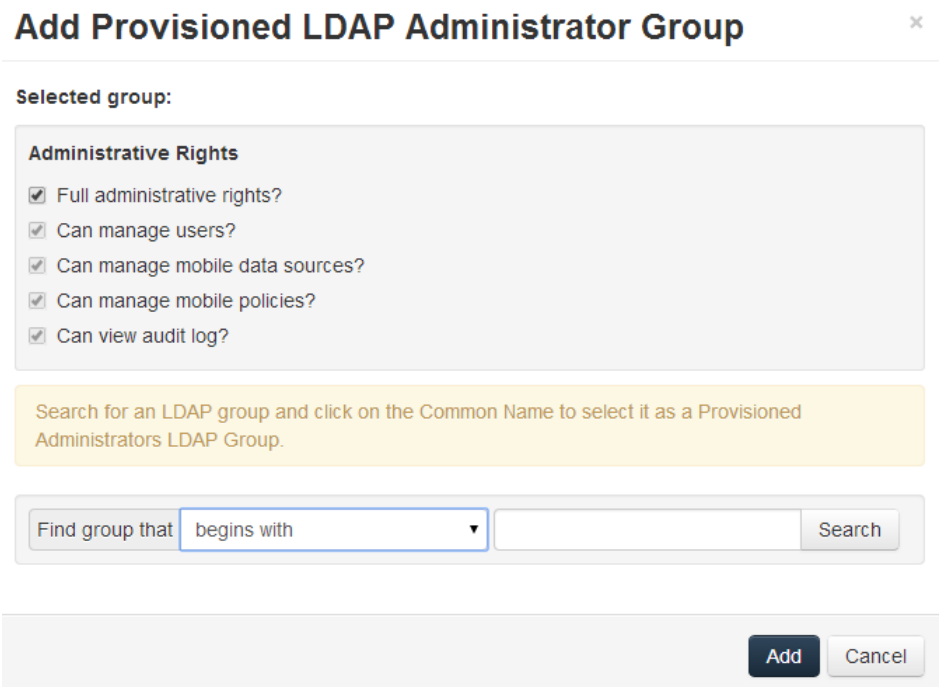


Copyright © Acronis International GmbH, 2002-2014

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

Using the **Actions** button you can delete or edit the group. You can edit the group's administrative rights.

To add a provisioned LDAP administrator group:



1. Press the **Add Provisioned Group**.
2. Mark if the group should have Sync & Share functionality.
3. Mark all of the administrative rights you want your group users to have.
4. Find the group.
5. Click on the group name.
6. Press **Save**.

Administrative Users

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

You can invite a new user with full or partial administrative rights using the **Add Administrator** button. Using the **Actions** button you can delete or edit the user. You can edit his administrative rights, status, email address and password.

Inviting a single administrator

1. Open the Acronis Access Web Interface.
2. Log in with an administrator account.
3. Expand the **General Settings** tab and open the **Administrators** page.

Copyright © Acronis International GmbH, 2002-2014

4. Press the **Add Administrator** button under **Administrative Users**.
5. Select either the Active Directory/LDAP or Invite by Email tab depending on what type of user you are inviting and what you want them to administer. LDAP users without emails cannot be given Sync & Share functionality.

a) **To invite via Active Directory/LDAP do the following:**

1. Search for the user you want to add in the Active Directory and then click on their Common Name to select a user.

Note: *The LDAP User and Email fields will fill in automatically.*

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

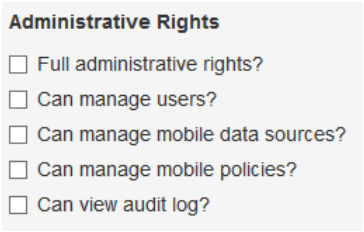
b) **To invite by Email do the following:**

1. Enter the email address of the user you want to add as an administrator.

Note: *Ad-hoc users invited by email will always have Sync & Share functionality.*

2. Select whether this user should be licensed.
3. Select which administrative rights the user should have.
4. Select the language of the Invitation email.
5. Press Add.

Administrative rights



- **Full administrative rights** - Gives the user full administrative rights.
- **Can manage users** - Gives the user the right to manage users. This includes inviting new users, LDAP group provisioning, sending Acronis Access enrollment invitations and managing the connected mobile devices.
- **Can manage mobile Data Sources** - Gives the user the right to manage the mobile Data Sources. This includes adding new Gateway Servers and Data Sources, managing the assigned sources, gateways visible on clients and legacy Data Sources.
- **Can manage mobile policies** - Gives the user the right to manage the mobile policies. This includes managing user and group policies, allowed apps and default access restrictions.
- **Can view audit log** - Gives the user the right to view the audit log.

Note: *New users who are in both a LDAP provisioned administrators group and a LDAP provisioned sync & share group will get the combined permissions.*

To give a user administrative rights:

1. Open the **Sync & Share** tab

Copyright © Acronis International GmbH, 2002-2014

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

To give an administrator specific rights:

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

3.3 Audit Log

3.3.1 Log

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

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

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

If you have enabled Audit logging on a Gateway Server, you will also see the activity of your mobile clients.

- **Device Name** – name of the connected device.
- **Device IP** – shows the IP address of the connected device.
- **Gateway Server** – shows the name of the Gateway Server to which the device is connected.
- **Gateway Server Path** – shows the path to the data source on that Gateway Server.

Copyright © Acronis International GmbH, 2002-2014

To enable Audit Logging for a specific gateway server:

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

To enable Debug Logging for a specific gateway server:

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

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

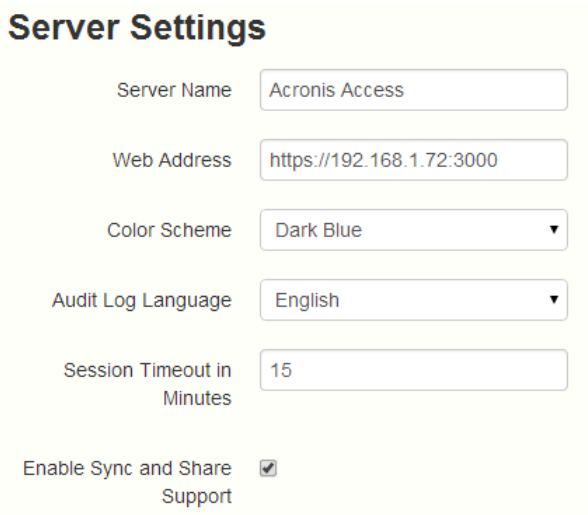
3.3.2 Settings

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

- **Automatically purge log entries more than X Y old** - When enabled, logs older than a number of days/weeks/months will be automatically purged.
  - **Export log entries to file as X before purging** - When enabled, exports a copy of the logs before purging them in either CSV, TXT or XML.
    - **Export file path** - Sets the folder where the exported logs will go.

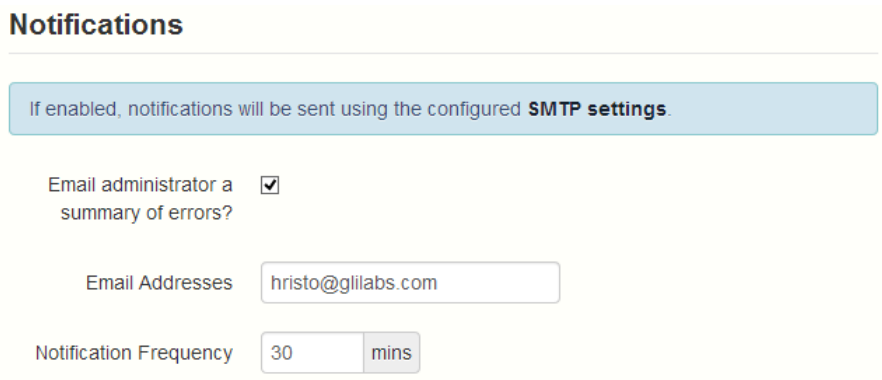
Copyright © Acronis International GmbH, 2002-2014

3.4 Server



Server Settings

- **Server Name** – cosmetic server name used as the title of the web site as well as identifying this server in admin notification email messages.
- **Web Address** – specify the root DNS name or IP address where users can access the website (starting with http:// or https://). Do not use 'localhost' here; this address will also be used in email invitation links.
- **Color Scheme** – select the color scheme for the website. Current options are **Gray, Purple, Cappucino, Blue, Dark Blue** and **Orange**. The default is **Dark Blue**.
- **Audit Log Language** – select the default language for the Audit Log. The current options are **English, German, French and Japanese**. The default is **English**.
- **Session timeout in minutes** – sets the length of the user session.
- **Enable Sync and Share Support** - this checkbox enables/disables the Sync and Share features.



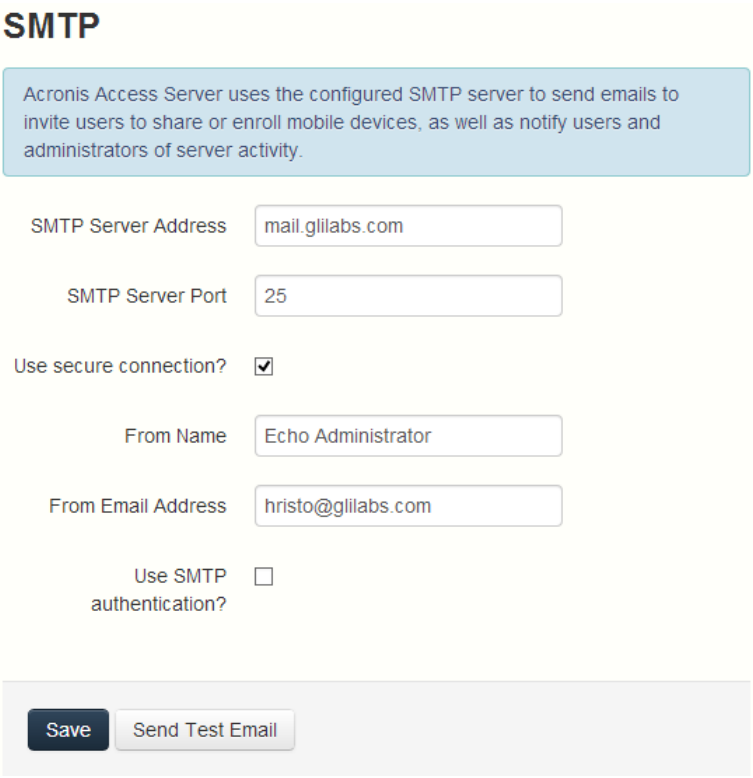
Notification Settings

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

Copyright © Acronis International GmbH, 2002-2014

3.5 SMTP

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

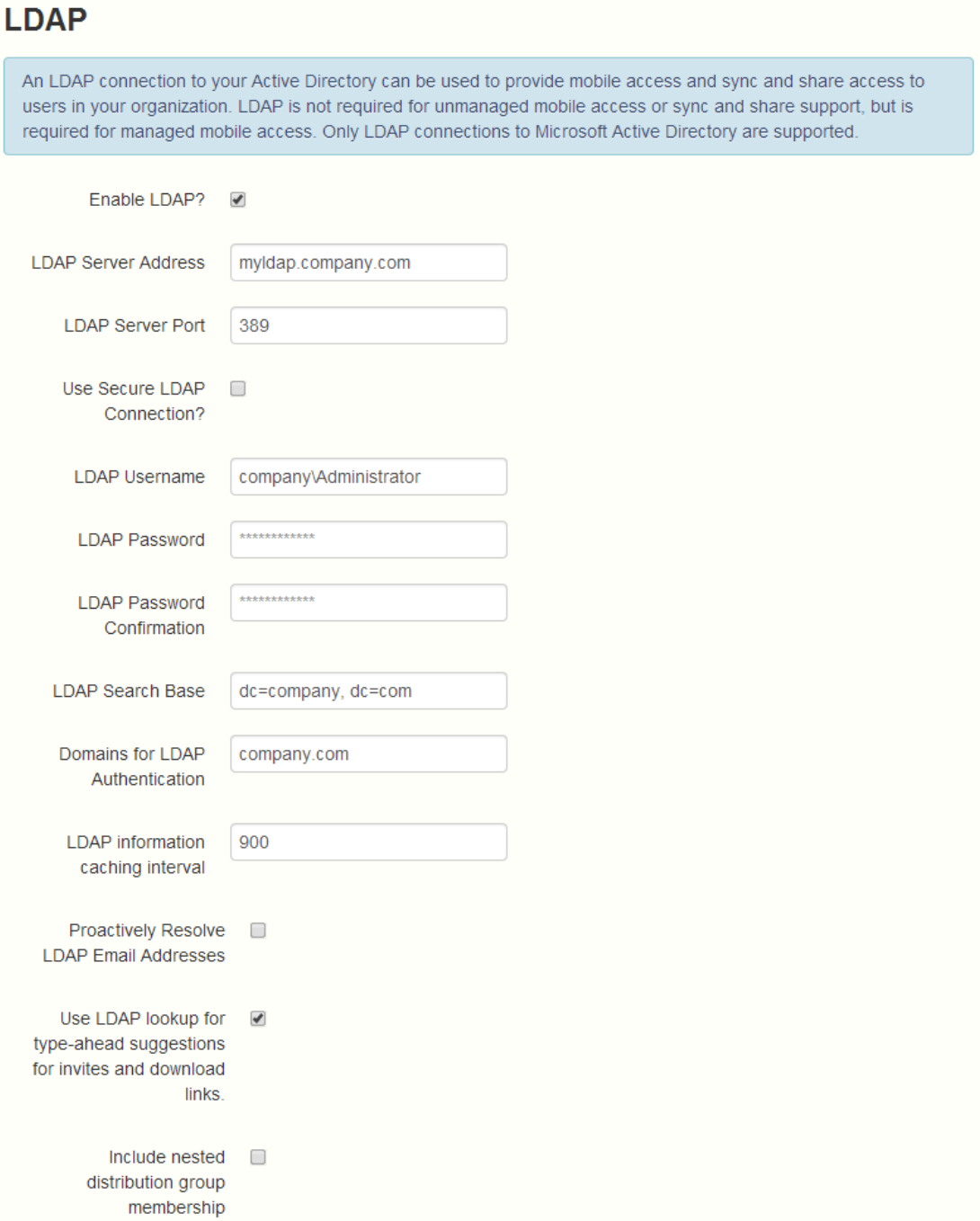


- **SMTP server address** - enter the DNS name of an SMTP server that will be used to send email invitations to your users.
- **SMTP server port** - enter your SMTP server port. This setting defaults to port 587.
- **Use secure connection?** - enable the option to use a secure SSL connection to your SMTP server. This setting is enabled by default. Uncheck the box to disable secure SMTP.
- **From Name** - this is the username that appears in the "From" line in emails sent by the server.
- **Use SMTP authentication?** - enable to connect with a SMTP username and password or disable to connect without them.
  - **SMTP username** - enter a username for SMTP authentication.
  - **SMTP password** - enter a password for SMTP authentication.
  - **SMTP password confirmation** - re-enter the SMTP password to confirm it.
- **Send Test Email** - sends an email to ensure all configurations are working as expected

Copyright © Acronis International GmbH, 2002-2014

3.6 LDAP

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



- **Enable LDAP?** - If enabled, you will be able to configure LDAP.
  - **LDAP server address** - enter the DNS name or IP address of the Active Directory server you would like to use for regulating access.
  - **LDAP server port** - the default Active Directory port is 389. This will likely not need to be modified.

Copyright © Acronis International GmbH, 2002-2014

Note: *If you're supporting multiple domains you should probably use the global catalog port.*

- **Use LDAP secure connection?** - disabled by default. Check the box to connect to Active Directory using secure LDAP.
- **LDAP username / password** - this login credentials will be used for all LDAP queries. Ask your AD administrator to find out if you have designated service accounts that should be used.
- **LDAP Search Base** - enter the root level you would like searches for users and groups to begin. If you would like to search your entire domain, enter "dc=domainname, dc=domainsuffix".
- **Domains for LDAP authentication** - users with email addresses whose domains are in this comma-delimited list must authenticate against LDAP. (i.e. to enable LDAP authentication for an account with the email **joe@glilabs.com**, you would enter **glilabs.com**). Users in other domains will authenticate against the Acronis Access database.
- **LDAP information caching interval** - sets the interval in which Acronis Access is caching the Active Directory structure.
- **Proactively resolve LDAP email addresses** - When this setting is enabled, Acronis Access will search Active Directory for the user with the matching email address on login and invite events. This allows users to log in with their email addresses and get immediate feedback on invitations, but may be slow to execute if the LDAP catalog is very large. If you encounter any performance problems or slow response on authentication or invite, uncheck this setting.
- **Use LDAP lookup for type-ahead suggestions for invites and download links -** LDAP lookup for type-ahead will search LDAP for users with matching email addresses. This lookup may be slow against large LDAP catalogs. If you encounter performance problems with type-ahead, uncheck this setting
- **Include nested distribution group membership** - When enabled, when inviting a distribution group to a share, will invite all members of that group as well as members of any subgroups.

3.7 Email Templates

Acronis Access makes extensive use of email messages to provide dynamic information to users and administrators. Each event has an HTML and text associated template. You can click the Email Template pull down menu to select an event and edit both templates.

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

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

- **Select Language** - Select the default language of the invitation emails.

  Note*: When sending an enrollment invitation or an invitation to a share or sharing a single file, you can select another language in the invitation dialog.*

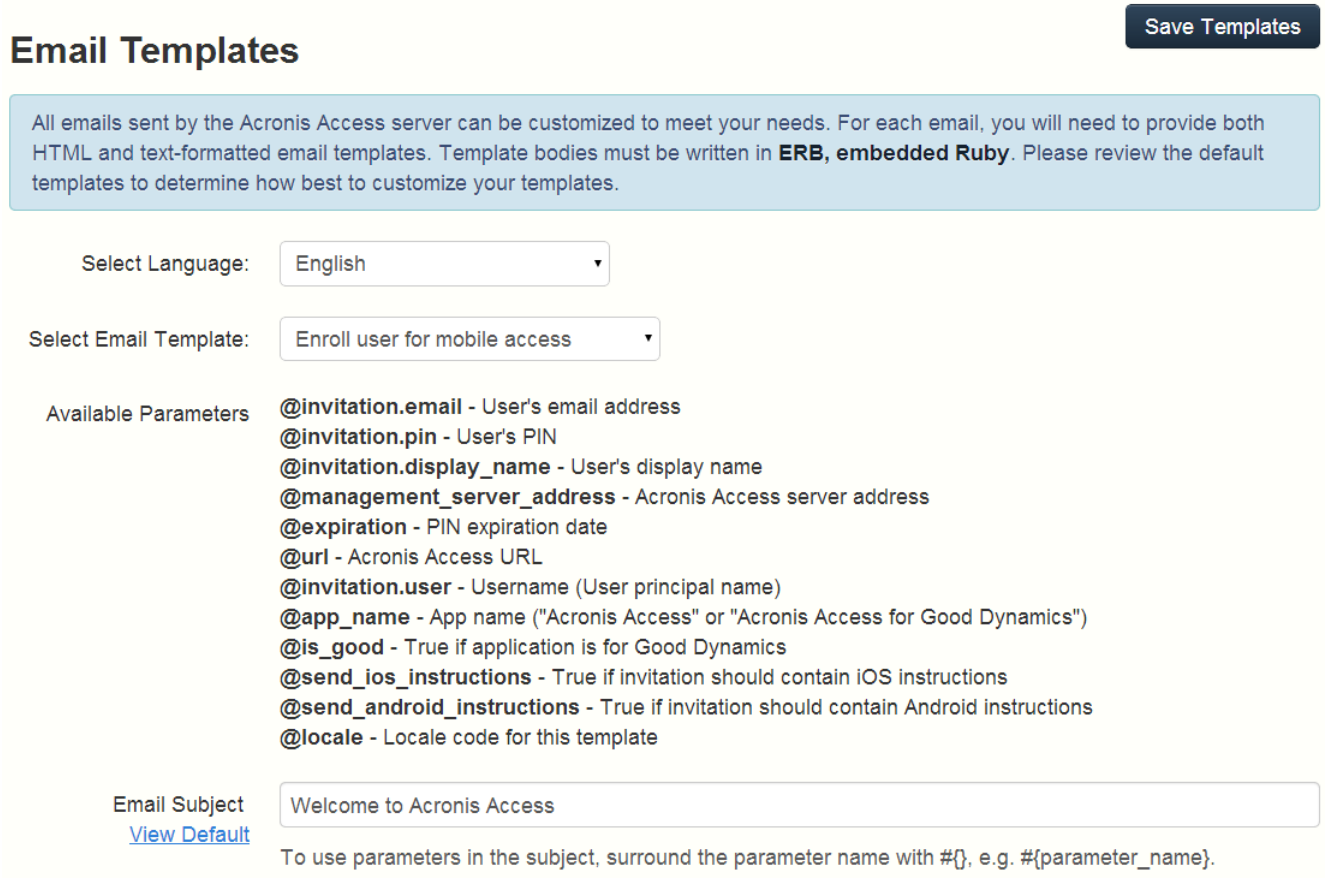
- **Select Email Template** - Select the template you want to view or edit. Each template is used for a specific event (e.g. Enrolling a user for mobile access, resetting a user's password).

Copyright © Acronis International GmbH, 2002-2014

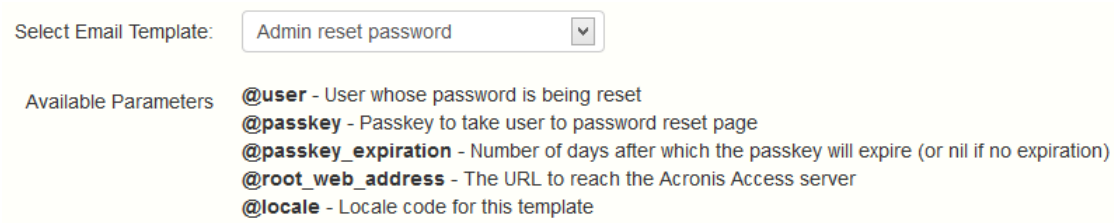
- **Available Parameters** - The available parameters are different for each template and will change based on the template you've selected.
- **Email Subject** - The subject of the invitation email. Pressing the **View Default** link will show you the default subject for that language and email template.
- **HTML Email template** - Shows the HTML-coded email template. If you enter valid HTML code, it will be displayed. Pressing the **Preview** button will show you a preview of how your current template looks.
- **Text Email template** - Shows the text-based email template. Pressing the **Preview** button will show you a preview of how your current template looks.

Note: *Always remember to click the* ***Save Templates*** *button when you finished modifying your templates.*

Note: *Editing a template in English does not edit the other languages. You need to edit each template separately for each language.*



Notice that templates allow you to include dynamic information by including parameters. When a message is delivered these parameters are replaced with the appropriate data. Different events have different available parameters.



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

Copyright © Acronis International GmbH, 2002-2014

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

3.8 Licensing

Licensing

You will see a list of all your licenses.

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

Adding a new license

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

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

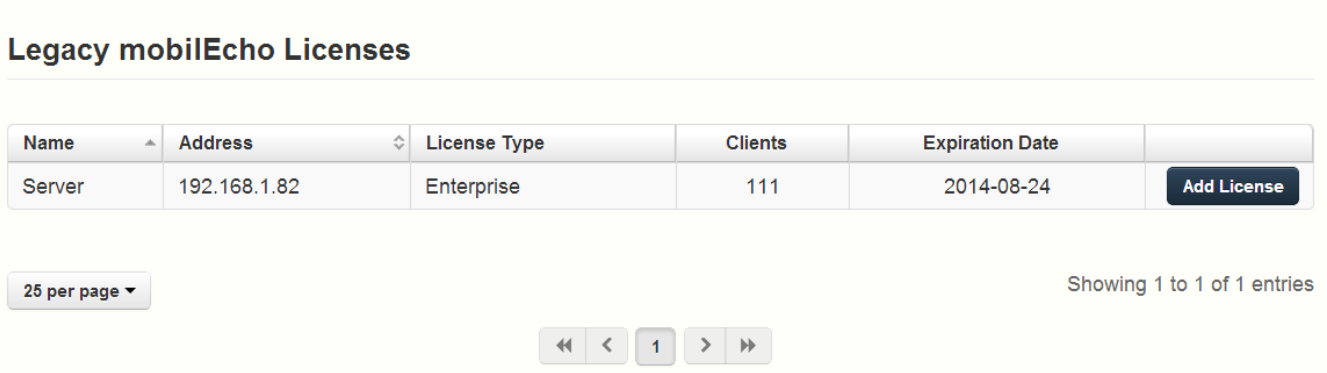
Adding a new license for a Gateway Server

In Acronis Access version 6.0, the Acronis Access server and the Gateway servers share the same license. This means that you will not have to manually add licenses to your Gateway servers.

If you are still using Gateway servers with an older version, you will also see the Legacy mobilEcho Licenses section

Copyright © Acronis International GmbH, 2002-2014

To license them, you will need a mobilEcho license. Follow the steps below:



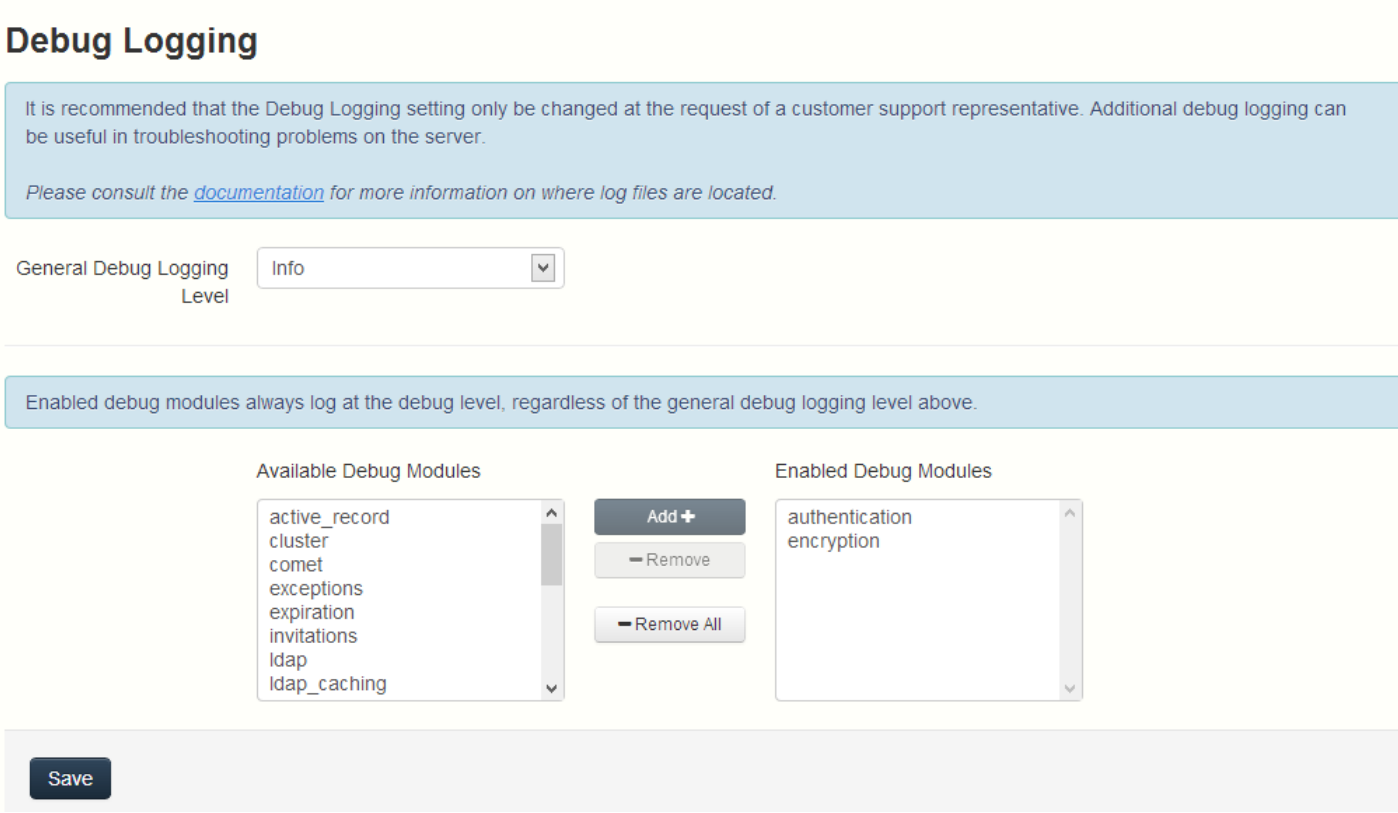
1. Open the web interface and log in as an administrator.
2. Open the **General Settings** tab and open the **Licensing** page.
3. In the **Legacy mobilEcho Licenses** section you have a list of all Gateway servers using the old licensing.
4. Press **Add License** for the desired Gateway and enter your license key.
5. Press **Save**.

3.9 Debug Logging

Settings in this page are designed to enable extended logging information that might be useful when configuring and troubleshooting Acronis Access. It is recommended that these settings only be changed at the request of a customer support representative. Additional debug logging can be useful in troubleshooting problems on the server.

Copyright © Acronis International GmbH, 2002-2014

Note: *For information on enabling/disabling debug logging for a specific Gateway Server visit the Server Details (p. 38) article.*



Warning: *These settings should not be used during normal operation and production conditions.*

- **General Debug Logging Level** - Sets the main level you want to be logged (Info, Warnings, Fatal errors etc.)

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

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

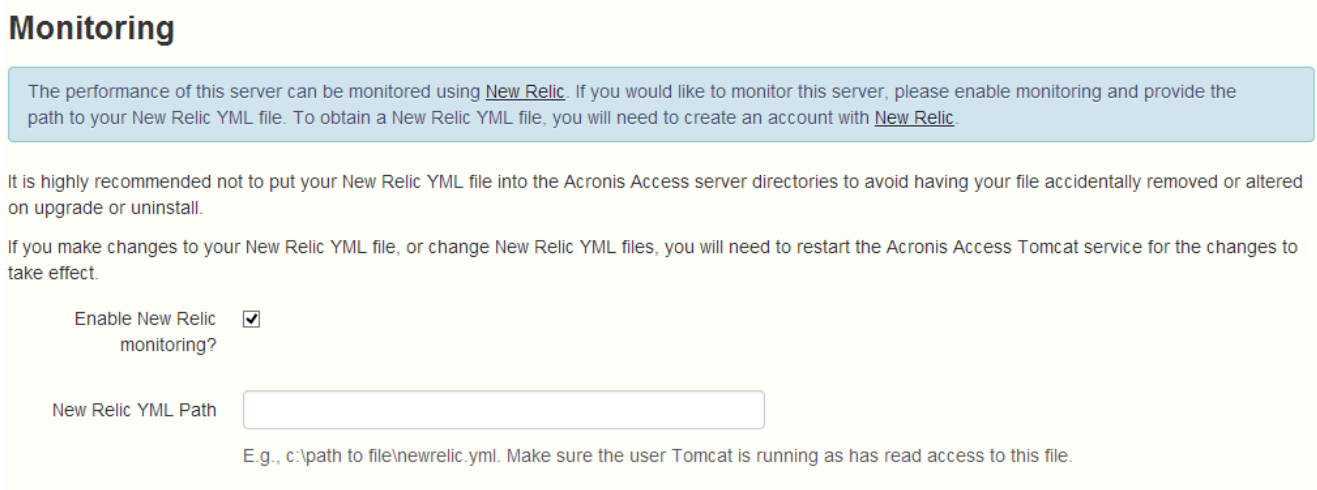
Note: *In the cases where the product was updated and not a new installation, the log files will be in* ***C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs****.*

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

Copyright © Acronis International GmbH, 2002-2014

3.10 Monitoring

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



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

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

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

Installing New Relic

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

1. Open http://newrelic.com/ http://newrelic.com/ and create a New Relic account.
2. For Application type select Mobile app.
3. For Platform mark Ruby.
4. Finish creating your account and log in.
5. Go to Applications, leave the **ruby bundle**(step 1) as is and continue to the next step.
6. Download the New Relic script - newrelic.yml.
7. Open your Acronis Access web UI.
8. Go to Settings and click on Monitoring.
9. Enter the path to the newrelic.yml including the extension (e.g. **`C:\software\newrelic.yml`**). We recommend you put this file in a folder outside of the Acronis Access folder so that it will not be removed or altered on upgrade or uninstall.
10. Click Save and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
11. If more than 10 minutes pass, restart your Acronis Access Tomcat service and wait a couple of minutes. The button should be active now.
12. You should be able to monitor you Acronis Access server via the New Relic website.

Copyright © Acronis International GmbH, 2002-2014

All the information the Acronis Access server logs about trying to connect to New Relic and set up monitoring is in a file called ***newrelic_agent.log*** *found here -* ***C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs****. If you have any problems, you can find information in the log file.*

There is frequently a warning/error that starts like this:
WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which

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

If you want to monitor the actual computer as well

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

- Wait until New Relic detects your server.

Copyright © Acronis International GmbH, 2002-2014

4 Maintenance Tasks

To backup all of Acronis Access's elements and as part of your best practices and backup procedures, you may want to read the Disaster Recovery guidelines (p. 82) article.

In this section

Disaster Recovery guidelines 82
Backing up and Restoring Acronis Access 84
Tomcat Log Management on Windows 86

4.1 Disaster Recovery guidelines

High availability and fast recovery is of extreme importance for mission critical applications like Acronis Access. Due to planned or unplanned circumstances ranging from local hardware failures to network disruptions to maintenance tasks, it may be required to provision the means for restoring Acronis Access to a working state in a very short period of time.

Introduction:

For mission critical applications like Acronis Access, high availability is of extreme importance. Due to various circumstances ranging from local hardware failures to network disruptions to maintenance tasks, it may be required to provision the means for restoring Acronis Access to a working state in a very short period of time.

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

Description of the Acronis Access elements:

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

Acronis Access Gateway Server

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

Acronis Access Server

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

Acronis Access Configuration Utility

Note: *Normally located here:* ***`C:\Program Files (x86)\Acronis\Access\Configuration Utility`***

File Store

The location of the **File Store** is set during the installation when you first use the **Configuration Utility.**

Note: *The FileStore structure contains user files and folders in encrypted form. This structure can be copied or backed up using any standard file copy tool (robocopy, xtree). Normally this structure should be located in a high availability network volume or NAS so the location may differ from the default.*

Copyright © Acronis International GmbH, 2002-2014

PostgreSQL database. This is a discrete element running as a Windows service, installed and used by Acronis Access. The Acronis Access database is one of the most critical elements because it maintains all configurations, relationships between users and files, and file metadata.

All those components are needed in order to build a working instance of Acronis Access.

Resources needed to implement a fast recovery process

The resources needed to fulfill the disaster recovery process are:

- Appropriate hardware to host the operating system, application and its data. The hardware must meet the system and software requirements for the application.
- A backup and restore process in place to ensure all software and data elements are available at the time the switch is needed.
- Network connectivity, including internal and external firewall and routing rules that permit users to access the new node with no or minimal need to change client side settings.
- Network access for Acronis Access to contact an Active Directory domain controller and SMTP server.
- Fast or automated DNS switching ability to redirect incoming request to the secondary node.

The process

Backup Setup

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

1. Have an installation of Acronis Access, including all elements in the secondary, restore, node. If this is not possible, a full (source) machine backup or image is a good alternative. In virtualized environments, periodic snapshots prove to be effective and inexpensive.
2. Backup the Acronis Access server software suite (all elements mentioned above, including the entire Apache Software branch) regularly. Use any standard, corporate class backup solution for the task.
3. Backup the FileStore as frequently as possible. A standard backup solution can be used, but an automated differential copy tool is a good and sometimes preferred alternative due to the amount of data involved. A differential copy minimizes the time this operation takes by updating what is different between the source and target FileStores.
4. Backup the Acronis Access database as frequently as possible. This is performed by an automated database dump script triggered by Windows Task Scheduler. The database dump should then be backed up by a standard backup tool.

Recovery

Provided the conditions described in the section above have been met and implemented, the process to bring online the backup resources is relatively simple:

1. Boot up the recovery node. Adjust any network configuration like IP Address, Host Name if needed. Test Active Directory connectivity and SMTP access,
2. If needed restore the most recent Acronis Access software suite backup.
3. Verify that Tomcat is not running (Windows Control Panel/Services).

Copyright © Acronis International GmbH, 2002-2014

4. If needed, restore the FileStore. Make sure the relative location of the FileStore is the same as it was in the source computer. If this is not the case, the location will need to be adjusted by using the Configuration Utility.
5. Verify that the PostgreSQL service is running (Windows Control Panel/Services).
6. Restore the Acronis Access database.
7. Start the Acronis Access Tomcat service.
8. Migrate DNS to point to the new node.
9. Verify Active Directory and SMTP are working

4.2 Backing up and Restoring Acronis Access

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

Backing up your databases

Backing up your Acronis Access's database

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

1. Open a Command Prompt window and navigate to the **`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

Backing up your Gateway Server's database

Copyright © Acronis International GmbH, 2002-2014

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.

Restoring Acronis Access

Restoring your Acronis Access's database

The database restore process is similar to the backup process.

1. Prior to executing the command to restore your database, make sure the source backup file is located in a directory or location where it can be accessed by the logged in user.
2. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.
   cd "**C:\PostgreSQL\9.2\bin**"

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

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

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

   dropdb -U postgres acronisaccess_production

   A "p*assword for user* **postgres***:* " message may appear. If that happens, enter the **postgres** password that you set during the Acronis Access installation process.
   acronisaccess_production must be entered exactly as shown. This is the **Acronis Access** database name.
4. Once the operation finishes, enter the following line:
   createdb -U postgres acronisaccess_production

   A "p*assword for user* **postgres***:* " message may appear. If that happens, enter the **postgres** password that you set during the Acronis Access installation process.
   acronisaccess_production must be entered exactly as shown. This is the **Acronis Access** database name.
5. To fill the newly created database with the information from your backup, enter the following line:
   psql -U postgres -d acronisaccess_production -W -f mybackup.sql

   Replace **mybackup.sql** with the fully qualified name of the backup file, for instance:
   D:\Backups\mybackup.sql
   A "p*assword for user* **postgres***:* " message may appear. If that happens, enter the **postgres** password that you set during the Acronis Access installation process.
   acronisaccess_production must be entered exactly as shown. This is the **Acronis Access** database name.
6. Once the process has completed successfully, restart the postgres service and start the Acronis Access Tomcat service.

Copyright © Acronis International GmbH, 2002-2014

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

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

Restoring your Gateway Server's database

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

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

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

4.3 Tomcat Log Management on Windows

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

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

Introduction:

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

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

Acronis Access's log files are named ***acronisaccess_date****.*

There are many tools capable of automating the task of deleting unneeded log files. For our example, we will use a built-in Windows command called ForFiles.

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

A sample process:

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

Info: *The sample script (batch) file is designed to work on Windows 2003 and Windows 2008. Click here to download the script.*
Optionally you could copy and paste the script code into an empty text document and save it as "AASTomcatLogPurge.bat"

Click here for the full batch script code...

Copyright © Acronis International GmbH, 2002-2014

```
ECHO OFF
 REM Script: aETomcatLogsPurge.bat
 REM 2012-05-12: Version: 1.0: MEA: Created
ECHO This script will delete files older than a number of days from a directory
 ECHO Run it from the command line or from a scheduler
 ECHO Make sure the process has permissions to delete files in the target folder
REM ===== CONFIGURATIONS ==================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"


REM NumDays - Log files older than NumDays will be processed
 set NumDays=14
REM ===== END OF CONFIGURATIONS ======================
ECHO
ECHO ===== START ============
REM ForFiles options:
 REM       "/p": the path where you want to delete files.
 REM       "/s": recursively look inside other subfolders present in the folder
mentioned in the batch file path
 REM       "/d": days for deleting the files older than the present date. For instance
"/d -7" means older than 7 days
 REM       "/c": command to execute to actually delete files: "cmd /c del @file".
forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"
:End
ECHO ===== BATCH FILE COMPLETED ============================================
```

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

Steps:

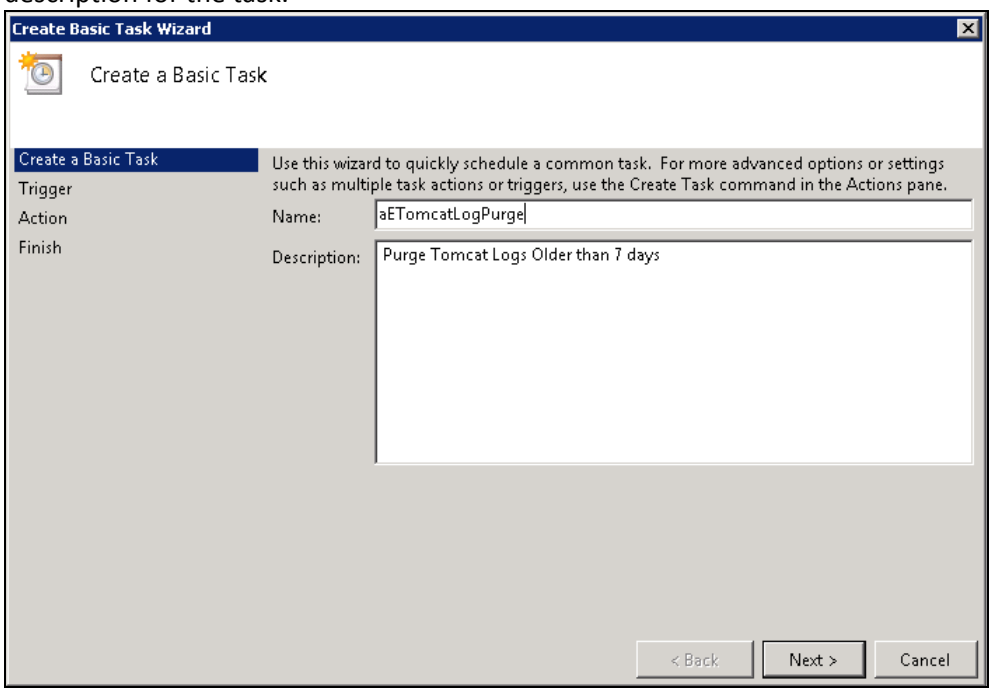
1. Copy the script to the computer running Acronis Access (Tomcat) and open it with Notepad or a suitable plain text editor.
2. Locate the section illustrated in the picture below and edit the LogPath and NumDays variables with your specific paths and retention settings:

Copyright © Acronis International GmbH, 2002-2014

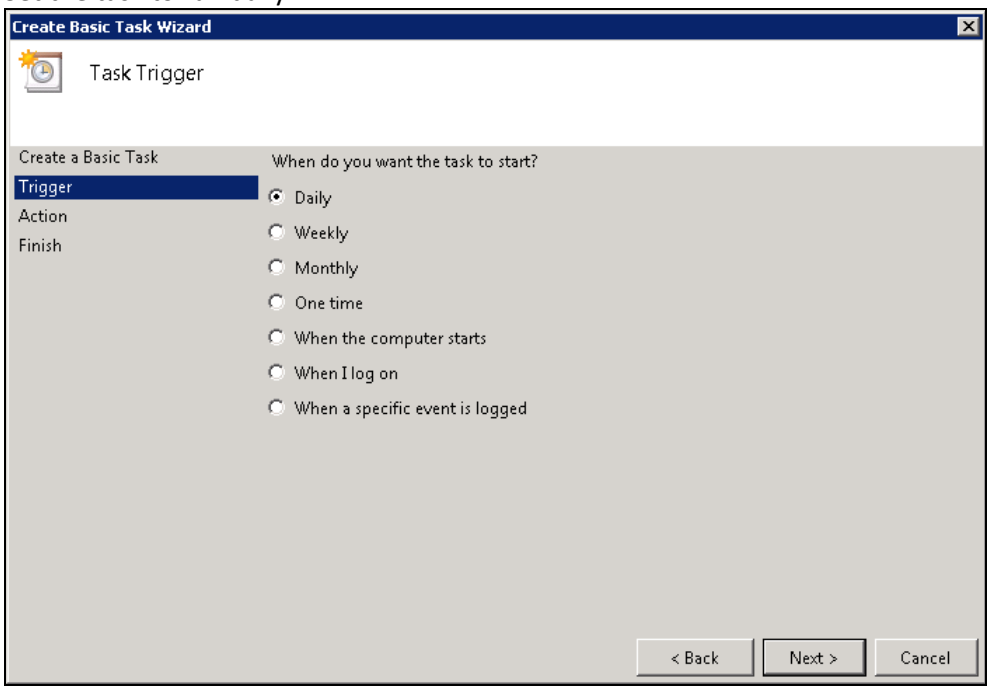
```
REM ===== CONFIGURATIONS ================================================
REM Note: all paths containing spaces must be enclosed in double quotes
 REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
 set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

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

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

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

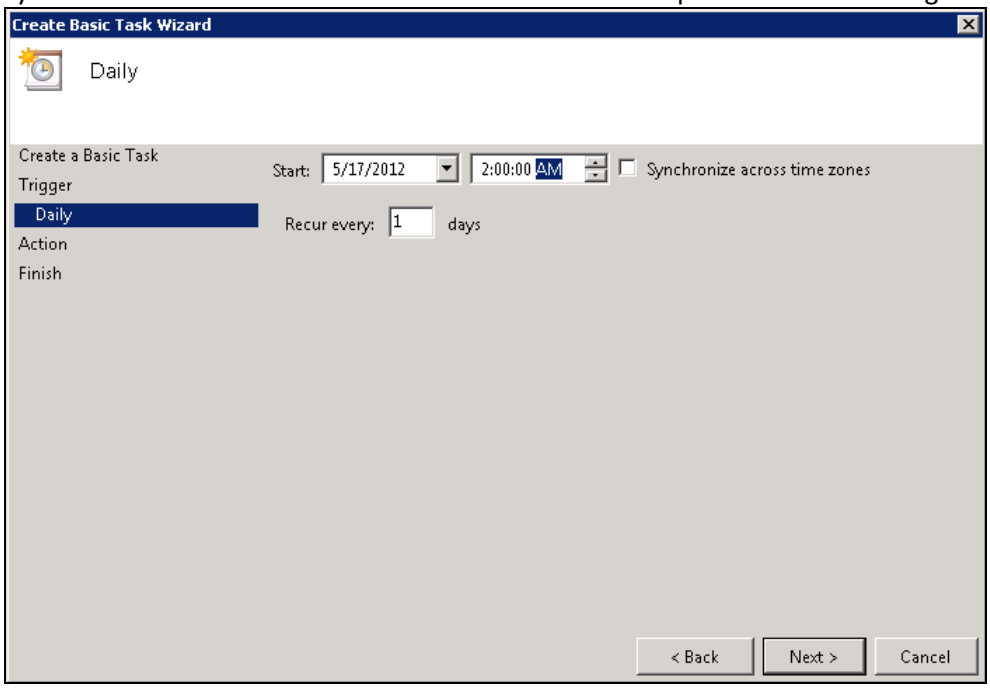


5. Set the task to run daily.

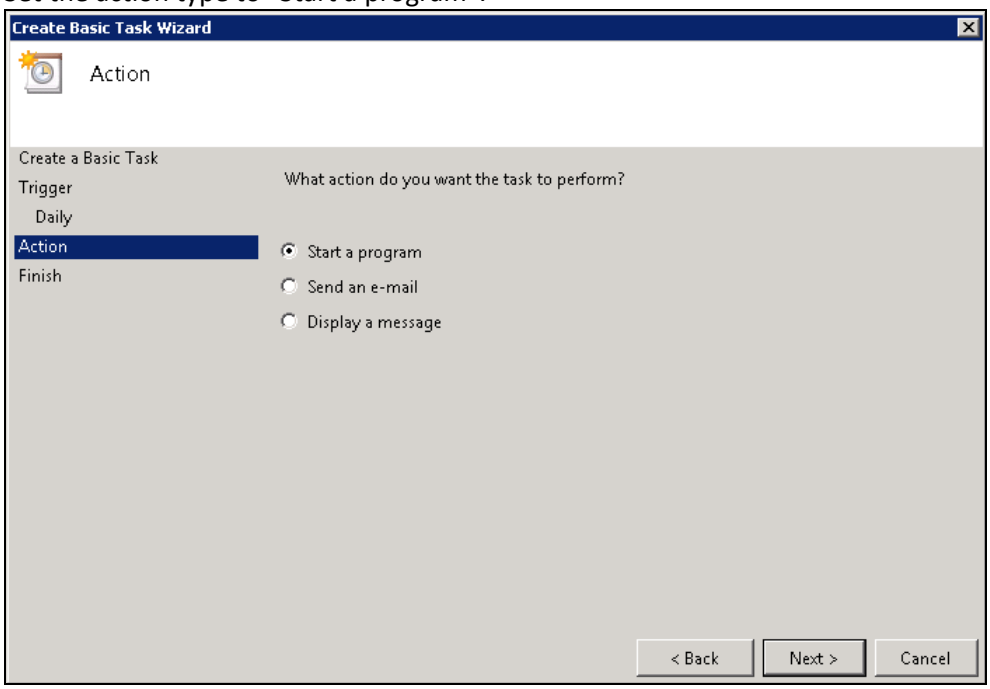


Copyright © Acronis International GmbH, 2002-2014

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

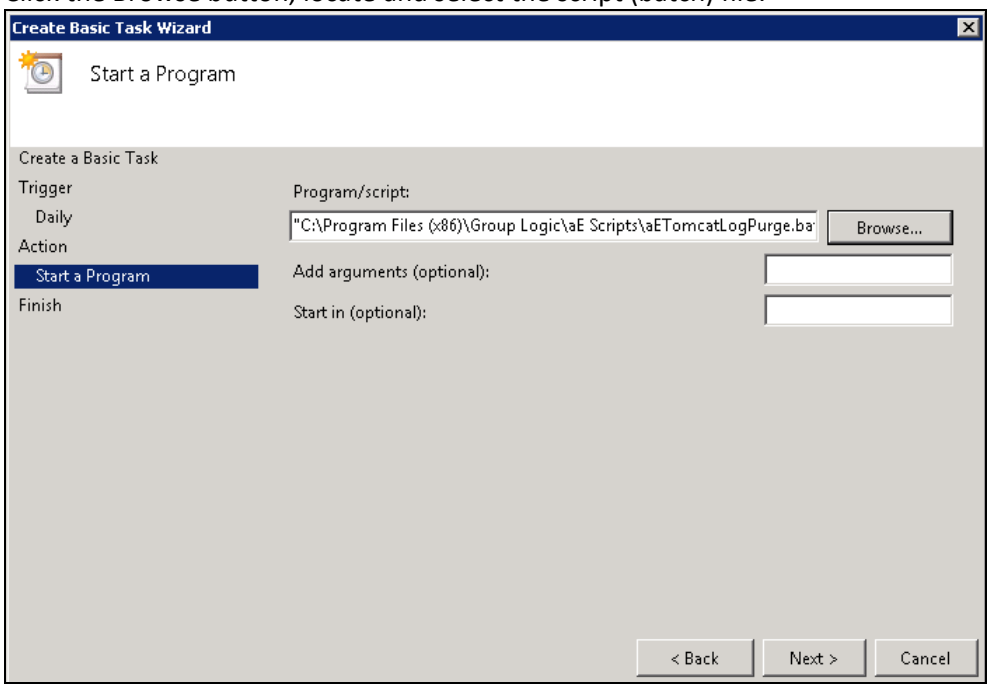


7. Set the action type to “Start a program”.

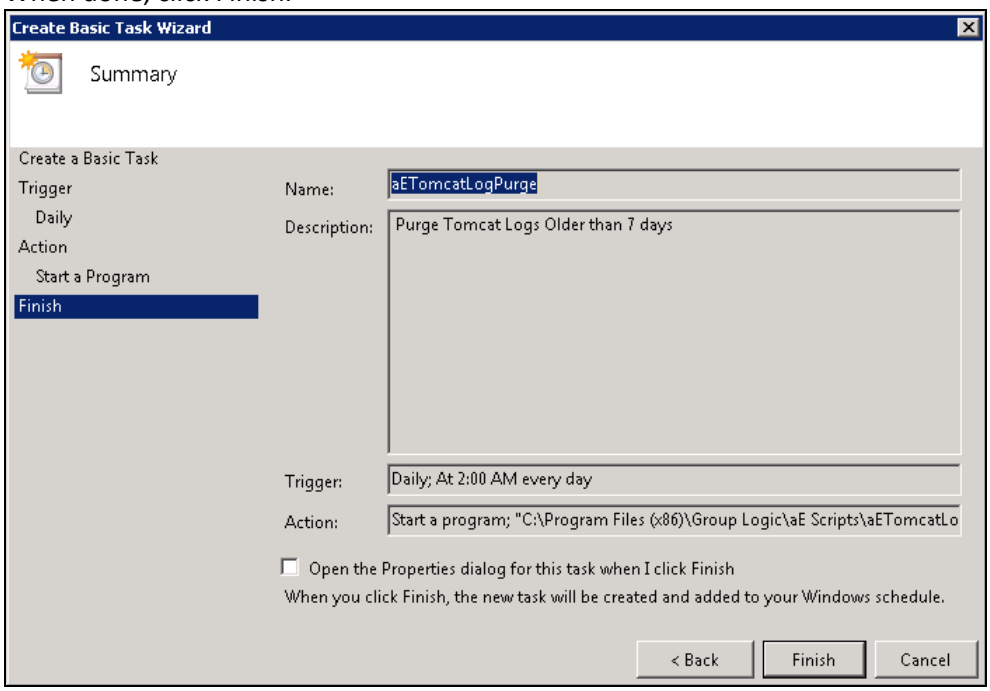


Copyright © Acronis International GmbH, 2002-2014

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



9. When done, click Finish.



10. In the tasks list you may want to right click on the task, select properties and verify the task will run whether a user is logged on or not, for unattended operation.
11. You can verify the task is properly configured and running properly by selecting the task, right clicking on it and selecting “Run”. The scheduler’s log should report start, stop and any errors.

Copyright © Acronis International GmbH, 2002-2014

5 Supplemental Material

In this section

Conflicting Software....91
Load balancing Acronis Access....91
Third-party Software for Acronis Access....97
Using Acronis Access with Microsoft Forefront Threat Management Gateway (TMG) 98
Unattended desktop client configuration....113
Monitoring Acronis Access with New Relic....114
Using trusted server certificates with Acronis Access....115
Creating a Drop Folder....117
Customizing the web interface....118
How to support different Access Desktop Client versions....119
How to move the FileStore to a non-default location. 119
Acronis Access for Good Dynamics....120
MobileIron AppConnect support....131
Installing Acronis Access on a Microsoft Failover Cluster....160
Upgrading from mobilEcho 4.5 on a Microsoft Failover Cluster 196
Upgrading Acronis Access on a Microsoft Failover Cluster....225

5.1 Conflicting Software

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

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

5.2 Load balancing Acronis Access

There are two main ways you can load balance Acronis Access:

Load balancing only the Gateway Servers

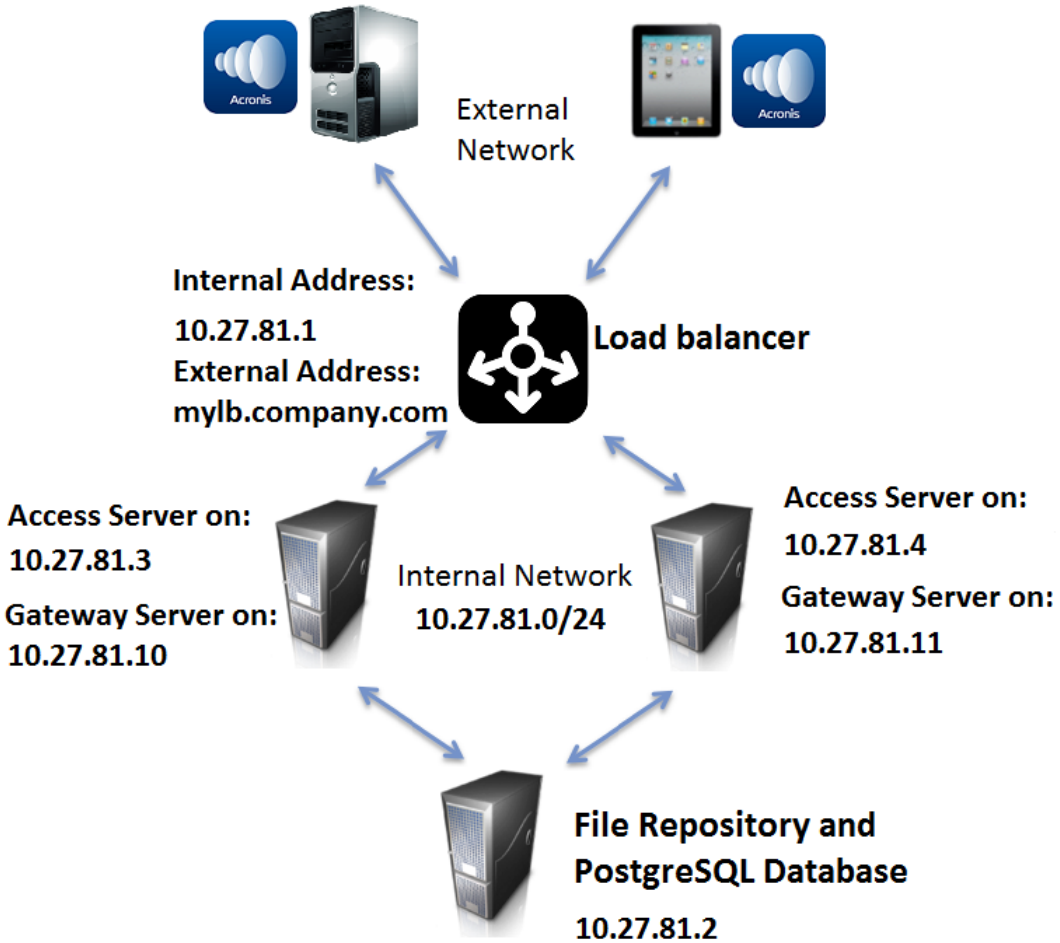
This configuration ensures that the components under the heaviest loads, the Gateway Servers, are load balanced and always accessible for your mobile clients. The Access Server is not behind the load balancer as it is not required in order to connect to the Gateway Servers for unmanaged access. For more information visit the Cluster Groups (p. 47) article.

Load balancing all of Acronis Access

This configuration load balances all of Acronis Access' components and ensures high-availability for all users. You will need at least two separate machines in order to test this setup. Many of the settings when configuring load balancing differ between different software and hardware so they will not be covered in this guide.

Copyright © Acronis International GmbH, 2002-2014

In the setup example we will use three separate machines. One of them will act as our File Repository and Database and the other two as both Access and Gateway servers. Below you can see a guide on how to configure this setup.



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

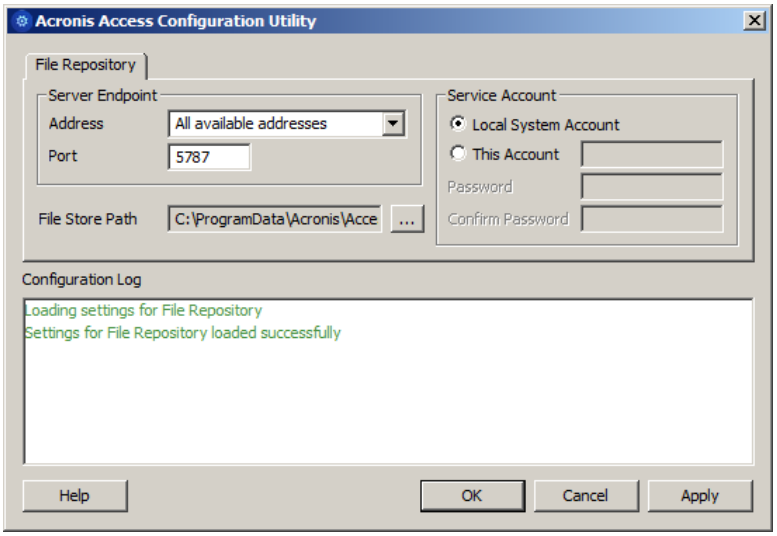
On the server that will be hosting your PostgreSQL database and File Repository, perform the following steps:

1. Start the Acronis Access installer and press **Next**. Read and accept the license agreement.
2. In the Access installer, choose **Custom**, and select **Acronis Access File Repository** and **PostgreSQL Database Server** and press **Next**.
3. Select where the File Repository and Configuration Utility will be installed.
4. Select where PostgreSQL should be installed and enter a password for the superuser **postgres**.
5. Open TCP port 5432. You will be using it to access the PostgreSQL database from the remote machines.
6. After finishing the installation procedure, proceed with going through the Configuration Utility.
   a. You will be prompted to open the Configuration Utility. Press **OK**.
   b. Select the address and port, on which your File Repository will be accessible.

Copyright © Acronis International GmbH, 2002-2014

Note: *You will need to set the same address and port in the Acronis Access web interface. For more information visit the Using the Configuration Utility and File Repository (p. 65) articles.*

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



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

7. Navigate to the PostgreSQL installation directory (e.g. C:\Program Files\PostgreSQL\9.2\data\ ) and edit **pg_hba.conf** with a text editor.
8. Include host entries for each of your Access servers using their internal addresses and save the file. The **pg_hba.conf** (HBA stands for host-based authentication) file controls client authentication and is stored in the database cluster's data directory. In it you specify which servers will be allowed to connect and what privileges they will have. e.g.:

```
# TYPE  DATABASE  USER  ADDRESS              METHOD
# Loadbalancer1 (First Acronis Access & Gateway server)
host      all       all   10.27.81.3/32      md5
# Loadbalancer2 (Second Acronis Access & Gateway server)
host      all       all   10.27.81.4/32      md5
```

In these examples all users connecting from 10.27.81.3/32 and 10.27.81.4/32 can access the database with full privileges (except the replication privilege) via a md5 encrypted connection.

9. Open the **pgAdmin** tool, connect to your local server, select **Databases**, and either right-click or select **New Database** from the **Edit** -> **New Object** menu to create a new database. Name it **acronisaccess_production**.

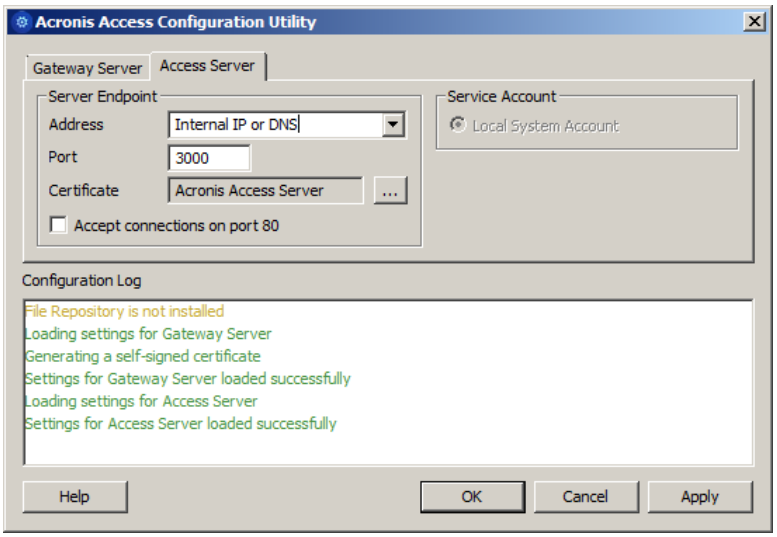
On the two servers that will be acting as both Access and Gateway servers, perform the following steps:

1. Start the Acronis Access installer and press **Next**. Read and accept the license agreement.
2. In the Access installer, choose **Custom**, and select only **Acronis Access Server** and **Acronis Access Gateway Server** and continue with the installation procedure.
3. After finishing the installation procedure, proceed with going through the Configuration Utility.
   a. You will be prompted to open the Configuration Utility. Press **OK**.
   b. **On the Access Server tab:**

Copyright © Acronis International GmbH, 2002-2014

- Enter the address and port on which your Acronis Access management server will be reachable (i.e. 10.27.81.3 and 10.27.81.4).
- Select your certificate. This should be the same SSL certificate that is tied to the DNS address of the load balancer.
- Press **Apply**.

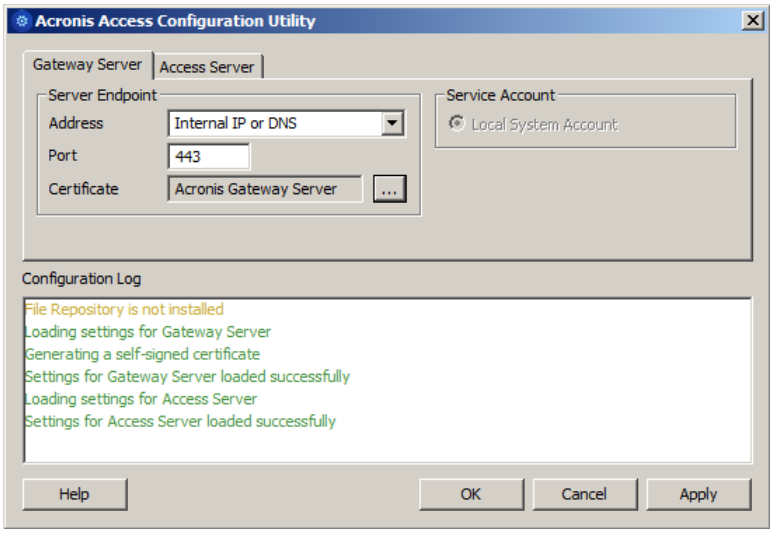
Note: *If you don't have a certificate, a self-signed certificate will be created by Acronis Access. This certificate should NOT be used in production environments.*



c. **On the Gateway Server tab:**

- Enter the address and port on which your Gateway Server will be reachable (i.e. 10.27.81.10 and 10.27.81.11).
- Select your certificate. This should be the same SSL certificate that is tied to the DNS address of the load balancer.
- Press **Apply**.

Note: *If you don't have a certificate, a self-signed certificate will be created by Acronis Access. This certificate should NOT be used in production environments.*



4. Navigate to the Acronis Access installation directory (e.g. C:\Program Files (x86)\Acronis\Access\Access Server\ ) and edit **acronisaccess.cfg** with a text editor.

Copyright © Acronis International GmbH, 2002-2014

5. Set the username, password, and internal address of the server that will be running the PostgreSQL database and save the file. This will configure your Access Server to connect to your remote PostgreSQL database. e.g.:

```
DB_DATABASE =acronisaccess_production
DB_USERNAME =postgres
DB_PASSWORD =password123
DB_HOSTNAME =10.27.81.2
DB_PORT =5432
```

6. Open Services.msc and restart the Acronis Access services.

On one of your Access and Gateway servers, perform the following steps:

This is the server which you will configure first and it's settings will be replicated across all other servers. After the settings get replicated, all servers will be identical. It does not matter which server you choose.

1. Open Services.msc and restart the **Acronis Access Tomcat** service. This will populate the database you have created.
2. Visit https://myaccess (i.e. https://10.27.81.3 or https://10.27.81.4) in your web browser and complete the Setup Wizard.
   a. **Under the Licensing tab:**
      - Enter your license key, mark the checkbox and press **Continue**.
   b. **Under the General Settings tab:**
      - Enter a Server Name.
      - The Web Address should be the external address of your load balancer (i.e. mylb.company.com). If you are not using port 443 you will have to write the port as well.
      - The Client Enrollment Address should be the external address of your load balancer (i.e. mylb.company.com).
      - Select your Color Scheme.
      - Select the language for the Audit Log messages.
   c. **Under the SMTP tab:**
      - Enter the DNS name or IP address of your SMTP server
      - Enter the port of your SMTP server.
      - If you do not use certificates for your SMTP server, unmark **Use secure connection?.**
      - Enter the name which will appear in the "From" line in emails sent by the server.
      - Enter the address which will send the emails sent by the server.
      - If you use username/password authentication for your SMTP server, mark **Use SMTP authentication?** and enter your credentials.
      - Press **Save**.
   d. **Under the LDAP tab:**
      - Mark **Enable LDAP**.
      - Enter the DNS name or IP address of your LDAP server.
      - Enter the port of your LDAP server.
      - If you use a certificate for connections with your LDAP server, mark **Use Secure LDAP Connection**.

Copyright © Acronis International GmbH, 2002-2014

- Enter your LDAP credentials, with the domain. (e.g. acronis\joe).
- Enter your LDAP search base.
- Enter the desired domain(s) for LDAP authentication. (i.e.to enable LDAP authentication for an account with the email joe@glilabs.com, you would enter glilabs.com)
- Press **Save**.

e. **Under the Local Gateway tab:**

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.*

- Set a DNS name or IP address for the local Gateway Server. This is an internal address behind the load balancer (i.e. 10.27.81.10).
- Press **Save**.

f. **Under the File Repository tab:**

- The File Repository Address should be the internal address of the server you have created for the file repository role (i.e. 10.27.81.2).

3. Once you've completed the Setup Wizard, press **Finish** and navigate to **Mobile Access** -> **Gateway Servers**.
4. It is time to register your second Gateway server:
   a. Enter a Display name for the second Gateway.
   b. The **Address For Administration** should be an internal address behind the load balancer (i.e. 10.27.81.11).
   c. Enter the **Administration Key**. You can obtain it by going to the machine on which the Gateway you are adding is installed, navigating to https://mygateway:443 (i.e. https://10.27.81.10 or https://10.27.81.11) and the key will be displayed there. For more information visit the Registering new Gateway Servers (p. 37) article.
   d. Press **Save**.
5. Create a Cluster Group and add all of your Gateway servers to it. Your primary server should be the one you have already gone through the Setup Wizard on. For more information visit the Cluster Groups (p. 47) article.

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

   a. Expand the **Mobile Access** tab.
   b. Open the **Gateway Servers** page.
   c. Press the **Add Cluster Group** button.
   d. Enter a display name for the group.
   e. Enter the internal DNS name or IP address of the load balancer (i.e. 10.27.81.1).
   f. Mark the checkbox for each Gateway you want to be in the group.
   g. Select the Gateway which will control the group's settings. This should be the Gateway which you configured first. All of the existing settings on that Gateway (including assigned Data Sources and excluding the address for administration) will be copied to every Gateway in the group.

On the load balancer:

1. Enable duration-based session stickiness (or your load balancer's equivalent) on your load balancer and configure it to not expire.

Copyright © Acronis International GmbH, 2002-2014

2. If a health-check is required (looking for an HTTP status of 200 to be returned), a ping to https://INTERNALSERVERNAME:MANAGEMENTPORT/signin will satisfy it (i.e. https://myaccessserver1.company.com/signin and https://myaccessserver2.company.com/signin).

Using a browser, open https://mylb.company.com to verify the configuration is working.

5.3 Third-party Software for Acronis Access

In this section

PostgreSQL 97
Apache Tomcat 97
New Relic 97

5.3.1 PostgreSQL

Acronis Access Server uses PostgreSQL as its database storage.

Documentation on the latest PostgreSQL http://www.postgresql.org/docs/9.2/interactive/index.html (for other versions visit this site http://www.postgresql.org/docs/manuals/).
List of error codes http://www.postgresql.org/docs/9.2/interactive/errcodes-appendix.html.
When installing Acronis Access server, by default you also install pgAdmin. It provides a graphical user interface to PostgreSQL. For documentation on all versions of pgAdmin visit this site http://www.pgadmin.org/docs/.
Useful information can be found at the PostgreSQL Wiki http://wiki.postgresql.org/wiki/Main_Page, including a troubleshooting guide http://wiki.postgresql.org/wiki/Troubleshooting_Installation.
For anti-virus related problems check this article http://wiki.postgresql.org/wiki/Running_&_Installing_PostgreSQL_On_Native_Windows#Antivirus_software.
For information on backing up a PostgreSQL database: PostgreSQL backup.

5.3.2 Apache Tomcat

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

Troubleshooting Tomcat Wiki https://wiki.openmrs.org/display/docs/Troubleshooting+Tomcat.
Troubleshooting from the Apache website http://commons.apache.org/logging/troubleshooting.html.

5.3.3 New Relic

New Relic is an on-demand application monitoring and optimization solution that can identify and resolve performance issues for Ruby, JRuby, Java, PHP and .NET applications. Monitor, troubleshoot and tune production web apps 24×7. New Relic includes Real User Monitoring (RUM) to analyze user requests in real time, offering insights about user experience including page load times, time in request queue, how long a page takes to render, and Apdex score. In addition, New Relic includes dashboard to visualize performance metrics by geography, by longest time in queue, throughput, and so on.

Copyright © Acronis International GmbH, 2002-2014

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

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

For information on installing New Relic for your Acronis Access server, visit the Monitoring Acronis Access with New Relic (p. 114) section.

5.4 Using Acronis Access with Microsoft Forefront Threat Management Gateway (TMG)

In this section

Overview 98
Introduction 99
Install the SSL Server Certificate 101
Create a New Web Listener 102
Create a New Web Site Publishing Rule.....106
Configure an External DNS Entry for the Acronis Access Gateway Server112
Using the Access Mobile Client with a TMG reverse proxy server 112
Using the Access Desktop Client with a TMG reverse proxy server. 113

5.4.1 Overview

Info: *This document covers the case when TMG is used as an Edge Firewall. If your organization uses TMG in a different network topology please contact Acronis for specific instructions.*

If you are using Microsoft Forefront Threat Management Gateway (TMG) to dedicate and protect your internal network from Internet threats and viruses, you need to make certain configurations to your TMG server to get it working with Acronis Access. To use TMG as reverse proxy and firewall for your Acronis Access server you need to create two separate networks on your TMG computer: internal and external. The two TMG network adapters should be properly configured, one with a private (internal IP address) and one with a public (external IP address). The Acronis Access server should be part of the internal network.

To use Acronis Access with TMG you need to complete the steps described in this document:

- Obtain an SSL server certificate and install it to your Acronis Access server and to the TMG server computer.
- Create a web listener in TMG.
- Create new web site publishing rule for the Acronis Access Gateway server, so that the clients from outside your network can connect to Acronis Access.
- Create an external DNS record in your DNS server.

The Access Mobile Client app supports these forms of authentication with a reverse proxy server:

- Pass-through authentication
- HTTP authentication (username & password)
- Certificate authentication

Copyright © Acronis International GmbH, 2002-2014

5.4.2 Introduction

Acronis Access clients connect to the Acronis Access server running inside your firewall securely via HTTPS and need to traverse your firewall via either VPN, HTTP reverse proxy or an open HTTPS port. This article provides step by step instructions that enable connections by your user running the Acronis Access desktop or mobile client from outside your network using the "reverse proxy" functions of the Microsoft Forefront Threat Management Gateway (TMG) software, which is the successor to ISA Server 2006.

Forefront Threat Management Gateway (TMG) is a secure web gateway that enables safe employee web use through comprehensive protection against malware, malicious web sites and vulnerabilities. Building on its predecessor, ISA Server 2006, TMG provides new URL filtering, anti-malware, and intrusion-prevention technologies to protect businesses against the latest web-based threats. These technologies are integrated with core network protection features such as firewall and VPN to create a unified, easy-to-manage gateway.

The Forefront TMG solution includes two separately licensed components:

- Forefront TMG server that provides URL filtering, antimalware inspection, intrusion prevention, application- and network-layer firewall and HTTP/HTTPS inspection in a single solution.
- Forefront TMG Web Protection Service that provides the continuous updates for malware filtering and access to cloud-based URL filtering technologies aggregated from multiple Web security vendors to protect against the latest Web-based threats.

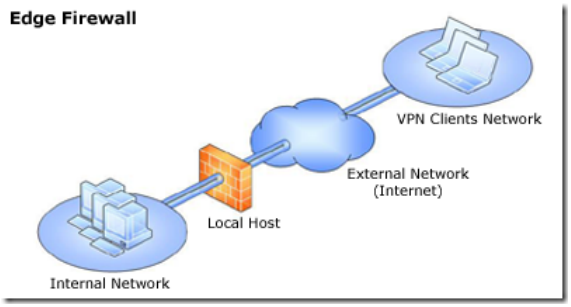
In this section

Understanding Forefront Threat Management Gateway (TMG) Network Topology 99
Understanding Forefront Threat Management Gateway authentication 101

5.4.2.1 Understanding Forefront Threat Management Gateway (TMG) Network Topology

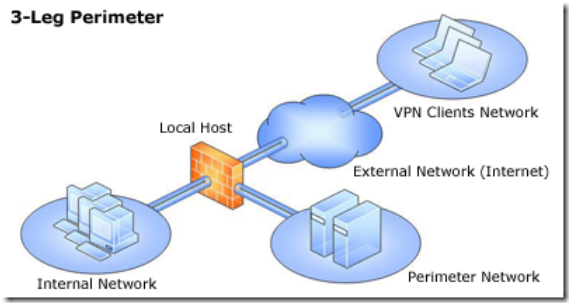
Forefront TMG includes four different network templates, that can fit in your existing network topology. It is important to choose the most appropriate for your organization option. After installing TMG, the **Getting Started Wizard** will appear, where you need to make initial configuration to your TMG. The first menu of the **Getting Started Wizard** is **Configure Network Setting**, where you need to make your choice about what network template to use. See below the available options.

- **Edge Firewall** - In this topology, Forefront TMG is located at the network edge, where it serves as the organization's edge firewall, and is connected to two networks: the internal network and the external network (usually the Internet).

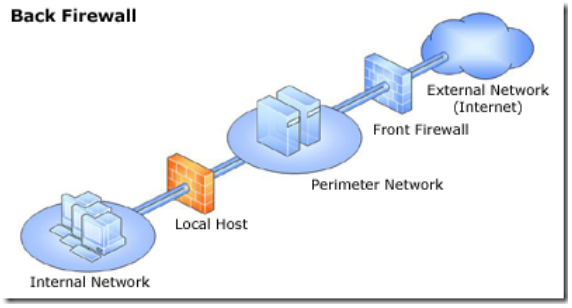


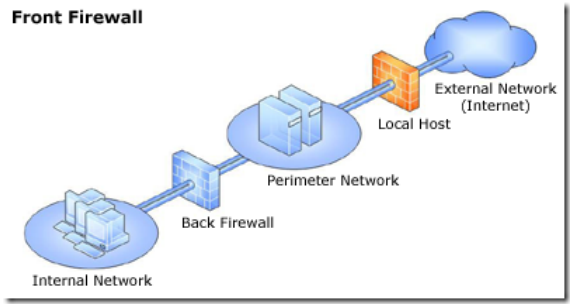
Copyright © Acronis International GmbH, 2002-2014

- **3-Leg Perimeter** - This topology implements a perimeter (DMZ) network. Forefront TMG is connected to at least three physical networks: the internal network, one or more perimeter networks and the external network.

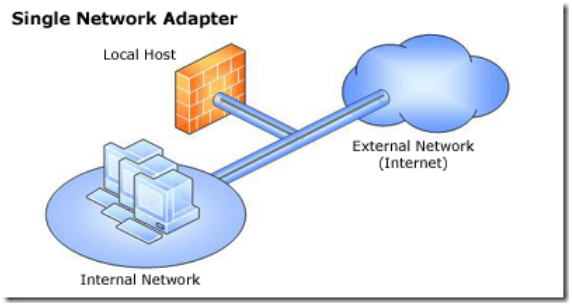


- **Back/Front Firewall** - In this topology, Forefront TMG is located at the network's back-end. Use this topology when another network element, such as a perimeter network or an edge security device, is located between Forefront TMG and the external network. Forefront TMG is connected to the internal network and to the network element in front of it.





- **Single Network Adapter** - This topology enables limited Forefront TMG functionality. In this topology, Forefront TMG is connected to one network only, either the internal network or a perimeter network. Typically, you would use this configuration when Forefront TMG is located in the internal corporate network or in a perimeter network, and another firewall is located at the edge, protecting corporate resources from the Internet.



Info:

For more information about how to install and configure TMG visit:
http://technet.microsoft.com/en-us/library/cc441445.aspx
http://technet.microsoft.com/en-us/library/cc441445.aspx.

For TMG minimum systems requirements visit:
http://www.microsoft.com/forefront/threat-management-gateway/en/us/system-requirements.aspx
http://www.microsoft.com/forefront/threat-management-gateway/en/us/system-requirements.aspx.

For pricing details visit:
http://www.microsoft.com/forefront/threat-management-gateway/en/us/pricing-licensing.aspx
http://www.microsoft.com/forefront/threat-management-gateway/en/us/pricing-licensing.aspx.

Copyright © Acronis International GmbH, 2002-2014

5.4.2.2 Understanding Forefront Threat Management Gateway authentication

TMG provides 3 general methods of authenticating users and they are:

HTTP authentication:

- Basic authentication - The user enters a username and password which the TMG server validates against the specified authentication server.
- Digest and WDigest authentication - Has the same features as the Basic authentication but provides a more secure way of transmitting the authentication credentials.
- Integrated windows authentication - Uses the NTLM, Kerberos, and Negotiate authentication mechanisms. These are more secure forms of authentication because the user name and password are hashed before being sent across the network.

Forms-based authentication:

- Password form - Prompts the user to enter a username and a password.
- Passcode form - Prompts the user to enter a username and a passcode.
- Passcode and Password form - Prompts the user to enter a username/password combination and a username/passcode combination.

Client certificate authentication

When users make a request for published resources, the client certificate sent to Forefront TMG is passed to a domain controller, which determines the mapping between certificates and accounts. The certificate must be matched to a user account.

Note: *Client certificate authentication is not supported for authenticating outbound Web requests.*

Info: *For more information on TMG authentication, please visit these sites:*
http://technet.microsoft.com/en-us/library/cc441695.aspx
http://technet.microsoft.com/en-us/library/cc441695.aspx

http://technet.microsoft.com/en-us/library/cc441713.aspx
http://technet.microsoft.com/en-us/library/cc441713.aspx

5.4.3 Install the SSL Server Certificate

Request and install an SSL certificate using the FQDN for each mobilEcho file server you want to publish via TMG in order to prevent DNS spoofing. You need to install the root SSL certificates on the TMG computer. These certificates should match the FQDN of each published server.

Follow the steps bellow to import a certificate to the TMG computer:

1. On the TMG computer, click **Start**, type **mmc**, and then press **Enter** or click **OK**.
2. 2. Click the **File** menu and then click **Add/Remove Snap-in** or press **Ctrl+M**. Under **Available Snap-ins**, click **Certificates** and then click **Add**.
3. Select Computer Account and then click **Next**, click **Local Computer** and then click **Finish**.
4. Click **OK** in the **Add Or Remove Snap-ins** dialog box.
5. Expand **Certificates (Local Computer)**, then expand **Personal**, and then expand **Certificates**.
6. Right-click the **Certificates** node, select **All Tasks**, and then select **Import...** .
7. The **Welcome To The Certificate Import Wizard** page appears. Click **Next**.
8. On the **File To Import** page, type the certificate location.

Copyright © Acronis International GmbH, 2002-2014

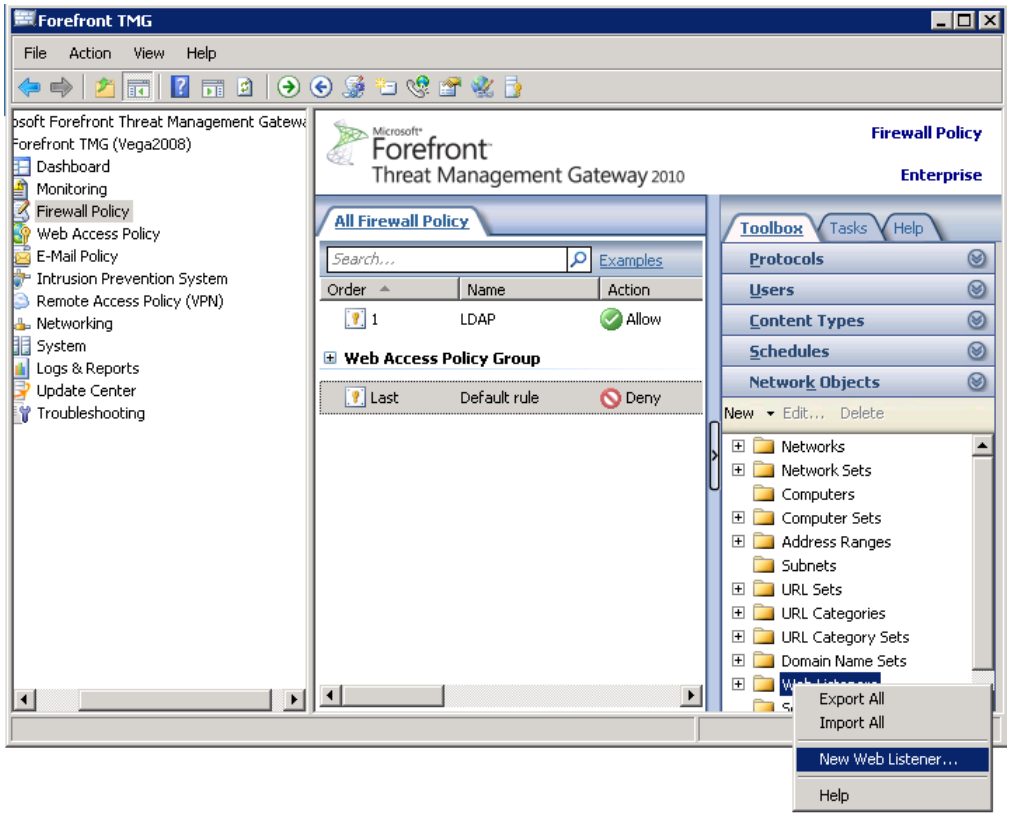
9. On the **Password** page, type the password provided by the entity that issued this certificate.
10. On the **Certificate Store** page confirm that the location is **Personal**.
11. The **Completing The Certificate Import Wizard** page should appear with a summary of your selections. Review the page and click **Finish**.

Verify that your CA is in the list of trusted root CAs:

1. On each edge server, click **Start**, and then click **Run**. In the Open box, type **mmc**, and then click **OK**. This opens an **MMC console**.
2. On the **File** menu, click **Add/Remove Snap-in.**
3. In the **Add Standalone Snap-ins** box, click **Certificates**, and then click **Add**.
4. In the **Certificate snap-in** dialog box, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, ensure that the **Local computer**: (the computer this console is running on) check box is selected, and then click **Finish**.
6. Click **OK**. In the console tree, expand **Certificates (Local Computer)**, expand **Personal**, and then click **Certificates**.
7. In the **details** pane, verify that your CA is on the list of trusted CAs. Repeat this procedure on each server.

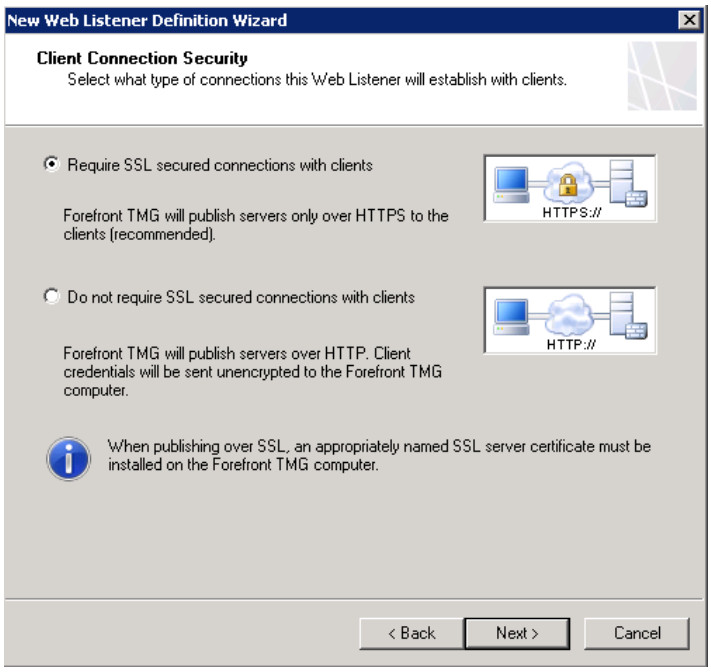
5.4.4 Create a New Web Listener

1. Open the Forefront TMG Management Console.
2. Expand Forefront TMG (Array Name or Computer Name) in the left pane and click **Firewall Policy**.
3. In the right pane click the **Toolbox** tab, click **Network Objects**, right-click **Web Listener** and select **New Web Listener** from the menu.

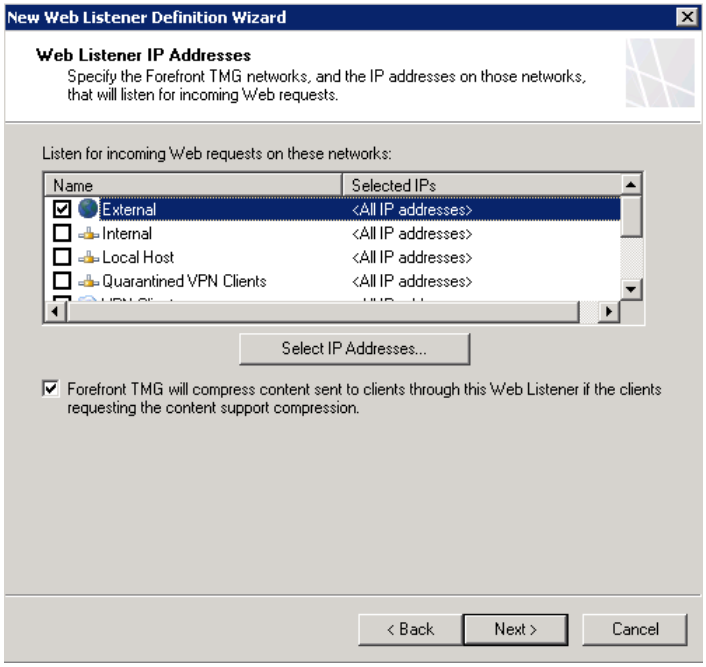


Copyright © Acronis International GmbH, 2002-2014

4. The **Welcome to the New Web Listener Wizard** page appears. Give a name to the **Web Listener** (e.g. Access WL) and click **Next**.
5. On the **Client Connection Security** page select **Require SSL secured connections with clients** and click **Next**.

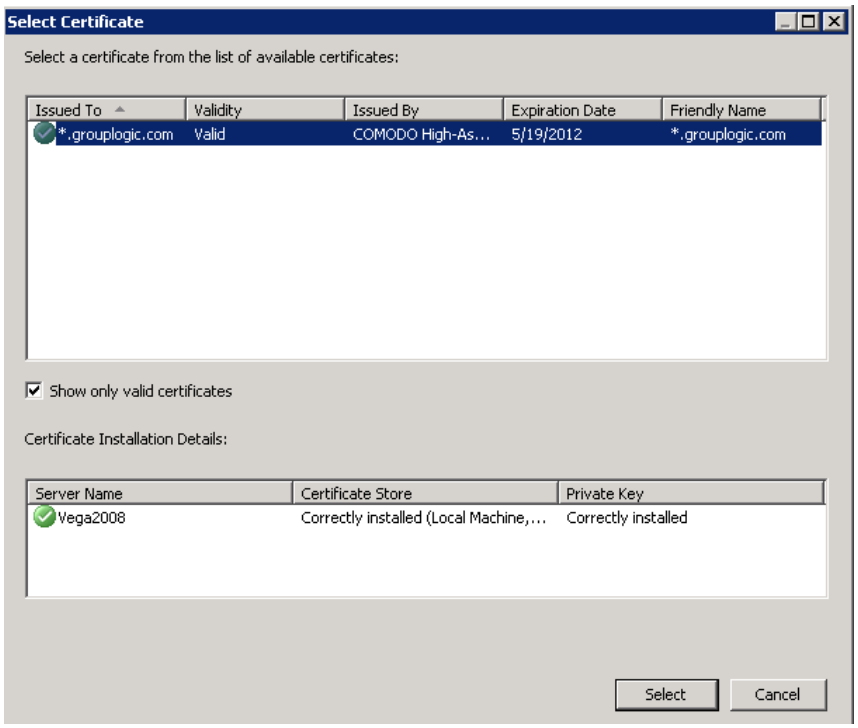


6. On the **Web Listener IP Addresses** page select **External** and click **Next**.



Copyright © Acronis International GmbH, 2002-2014

7. On the **Listener SSL Certificates** page select **Use a single certificate for this Web Listener** and click the **Select Certificate** button. Select the appropriate certificate and click the **Select** button to confirm your choice.



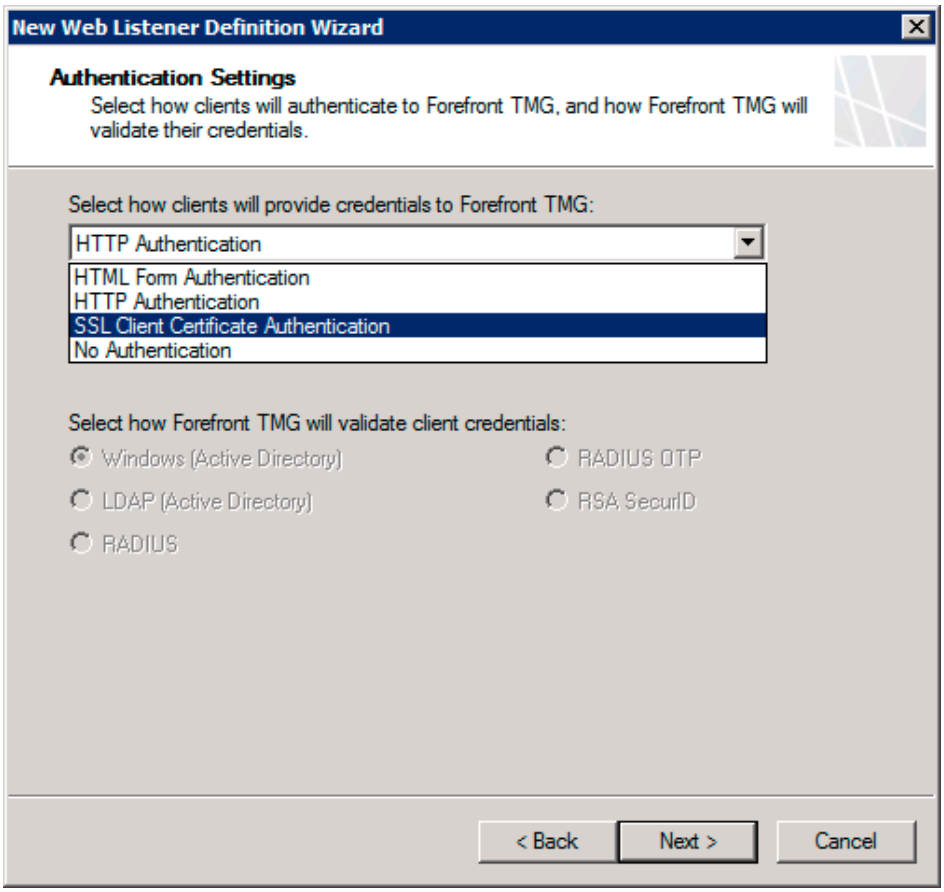
8. Confirm that the correct certificate appears on the **Listener SSL Certificates** page and click **Next**.
9. On the **Authentication Settings** page choose the type of authentication you'd like Acronis Access to use when it contacts the TMG reverse proxy server, and click **Next**.

   Acronis Access mobile client supports:

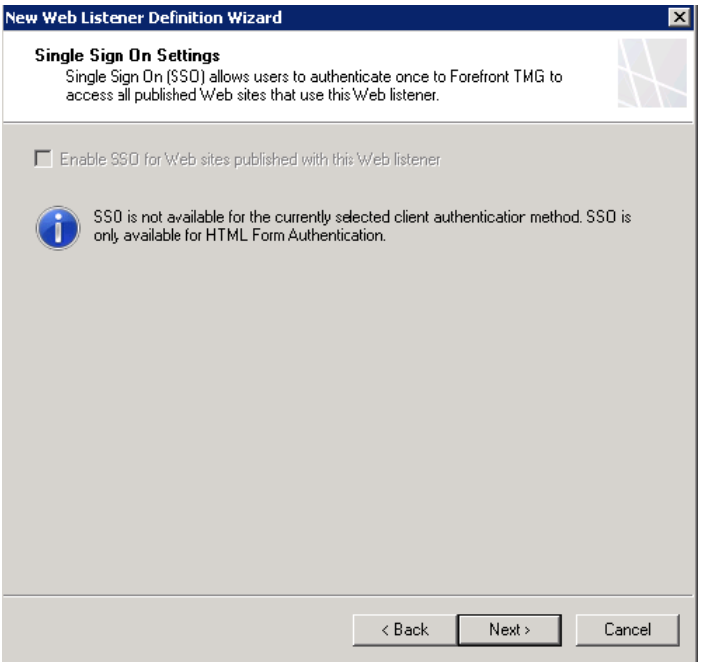
   - **No Authentication** - Use this option if you'd like the Access Mobile Client requests to pass through the TMG reverse proxy server without needing to authenticate.
   - **HTTP Authentication** - Use this option if you'd like the Access Mobile Client app to authenticate with the TMG reverse proxy using the user's username and password. This is typically the user's Active Directory credentials. If the Access Mobile Client app is configured to require authentication "Once per session" or "Once per server", the user will be prompted for their credentials when they initially contact the TMG reverse proxy server.

Copyright © Acronis International GmbH, 2002-2014

- **SSL Client Certificate Authentication** - Use this option if you'd like the Access Mobile Client app to authenticate with the TMG reverse proxy with an SSL user identity certificate. This certificate must be added to the Access Mobile Client app before the user can authenticate with the TMG reverse proxy server. Additional instructions can be found here. http://support.grouplogic.com/?p=3830

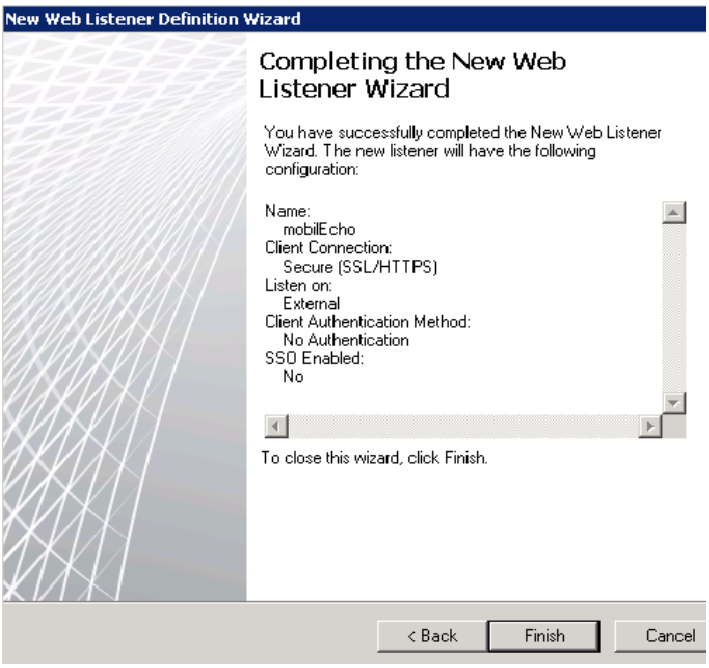


10. On the **Single Sign On Settings** page verify that the **SSO** setting is disabled and click **Next**.



Copyright © Acronis International GmbH, 2002-2014

11. Review your selections on the **Completing The New Web Listener Wizard** page and click **Finish**.



12. Click the **Apply** button to commit the changes.

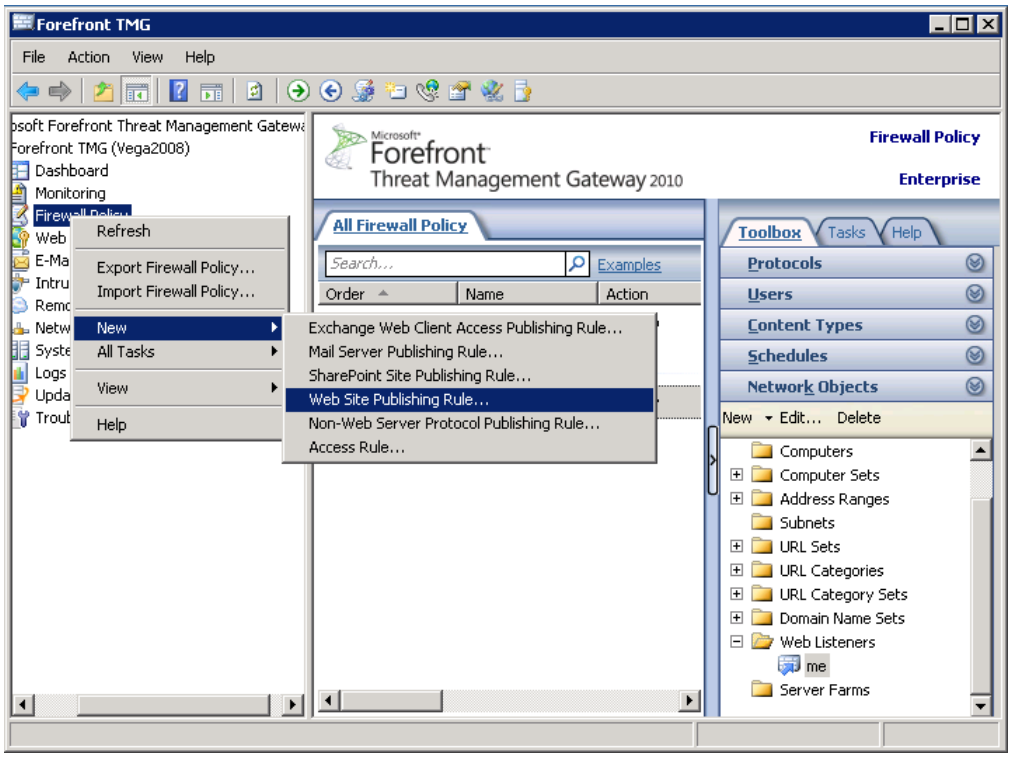
13. In the left pane of the Forefront TMG Management Console click **Monitoring**, then click on the **Configuration** tab in the middle pane. Keep clicking on the **Refresh Now** link in the right pane (**Tasks** tab) until there is a green icon with the checkbox in front of the TMG computer name (array name).

5.4.5 Create a New Web Site Publishing Rule

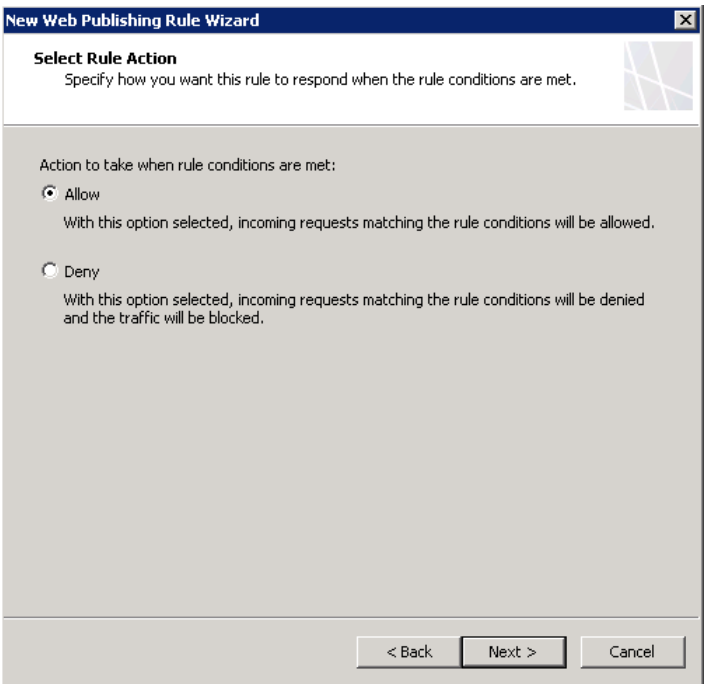
1. In the Forefront TMG Management Console expand Forefront TMG (Array Name or Computer Name) in the left pane.

Copyright © Acronis International GmbH, 2002-2014

2. Right-click **Firewall Policy**, select **New**, and click **Web Site Publishing Rule**.

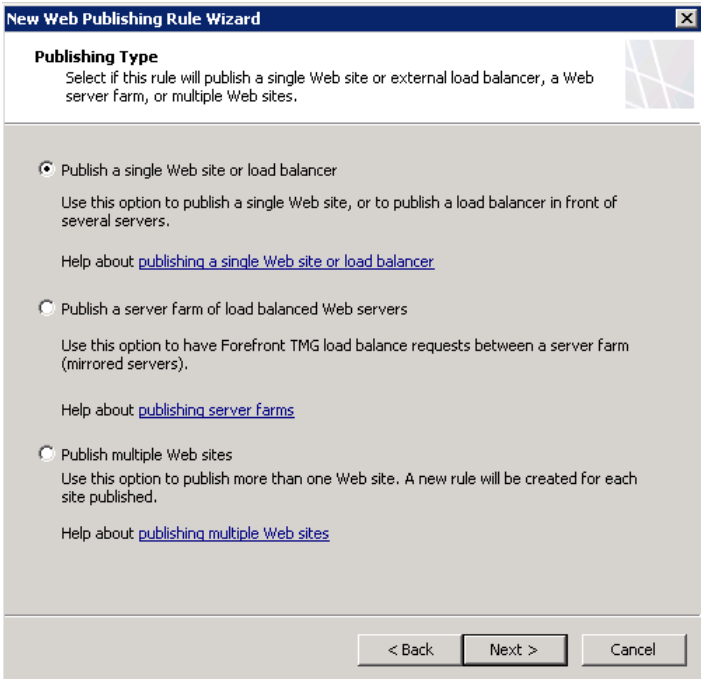


3. The **Welcome to the New Web Publishing Rule Wizard** page appears. Enter a name for the Web publishing rule (e.g. Access WP) and click **Next**.
4. On the **Select Rule Action** page verify that the **Allow** option is selected and click **Next**.

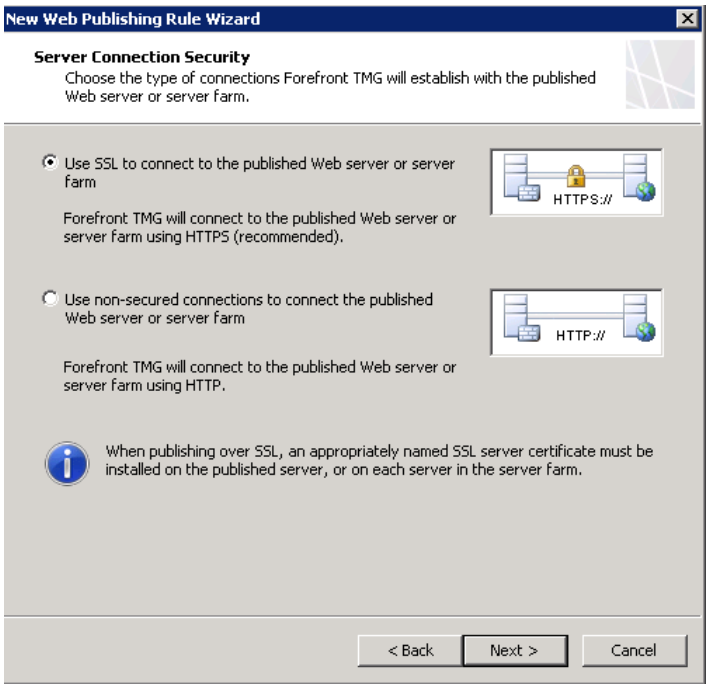


Copyright © Acronis International GmbH, 2002-2014

5. On the **Publishing Type** page choose the applicable option for your case and click **Next**.



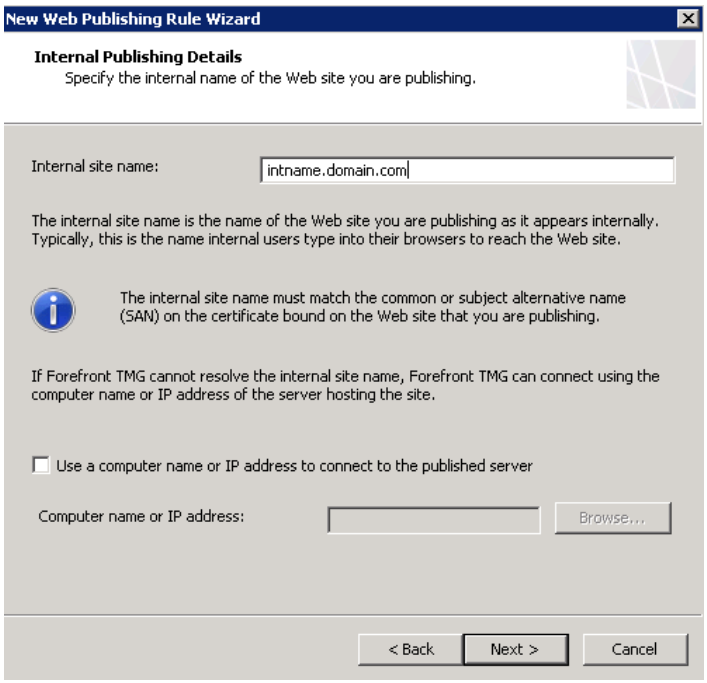
6. On the **Server Connection Security** page choose the **Use SSL to connect to the published Web server or server farm** option and click **Next**.



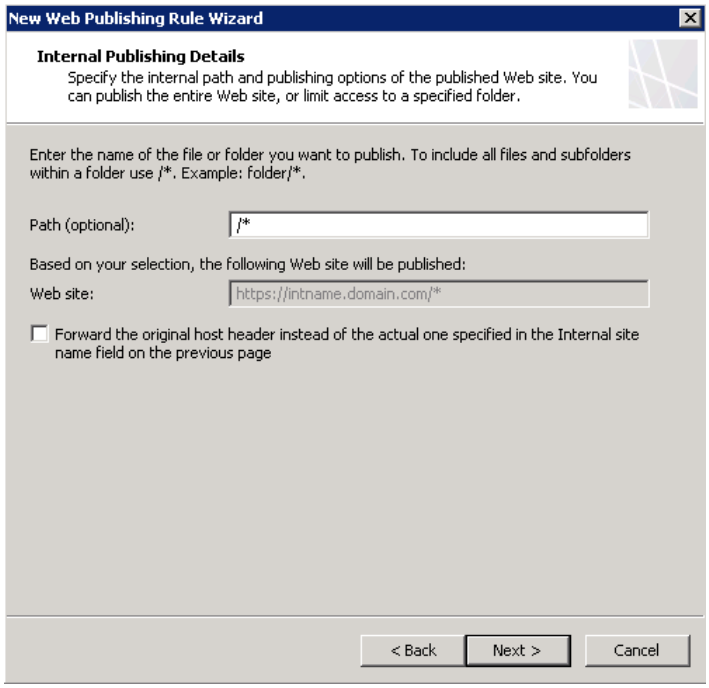
7. On the **Internal Publishing Details** page type "intname.domain.com" in the **Internal site name** field, where **domain** is a placeholder for the domain name the server you want to publish belongs to, and **intname** is a name you give to this server, which should be different than the external name in order to prevent routing loop. Click **Next** to commit the changes.

Copyright © Acronis International GmbH, 2002-2014

Note: *Create a DNS entry in the internal DNS server of your organization for "intname.domain.com".*

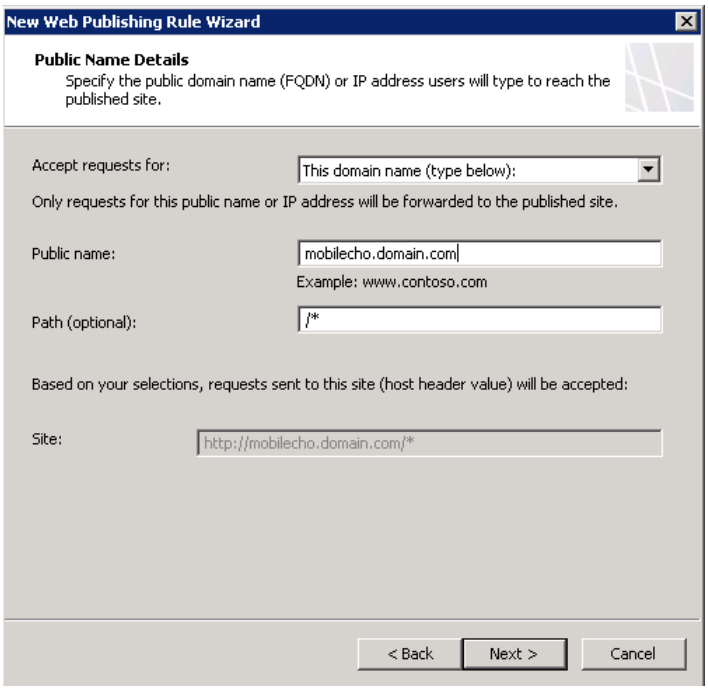


8. On the **Internal Publishing Details** page enter "**/***" in the **Path (optional)** field to allow access to the entire content of the Acronis Access Gateway server. Click **Next**.

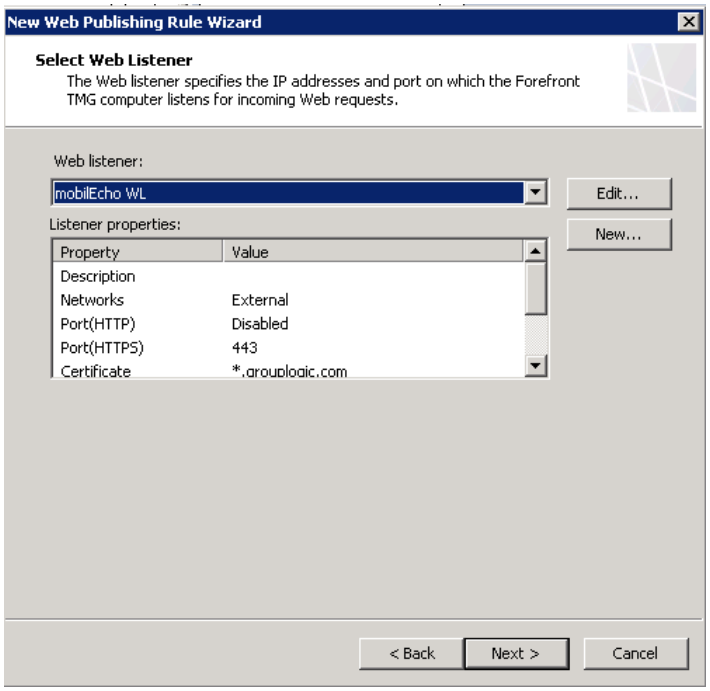


Copyright © Acronis International GmbH, 2002-2014

9. On the **Public Name Details** page you need to specify the name that the remote clients will use to connect to the published server. Enter "access.domain.com" in the **Public name** field, where **domain** is a placeholder for the domain name of the server you want to publish. Leave the other options the way they are by default and click **Next**.

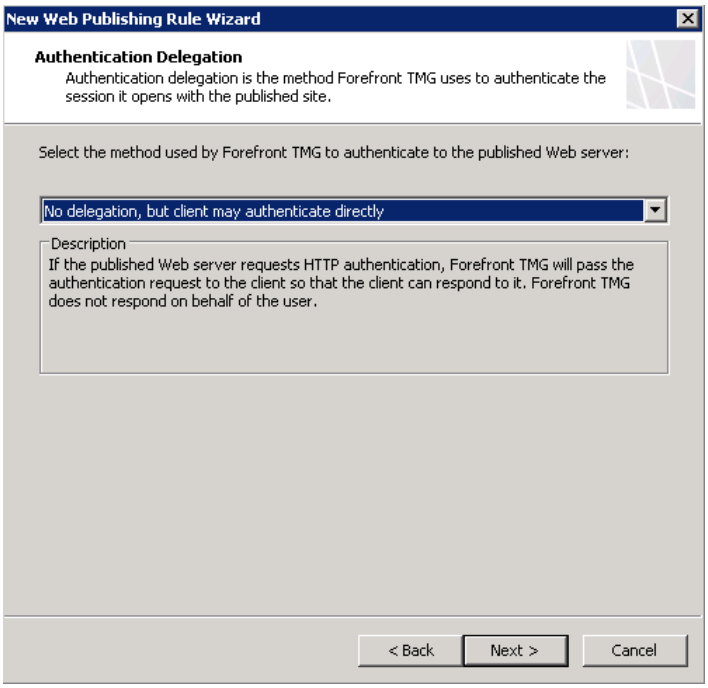


10. On the **Select Web Listener** page select the web listener that you have created for Acronis Access from the drop-down menu and click **Next**.

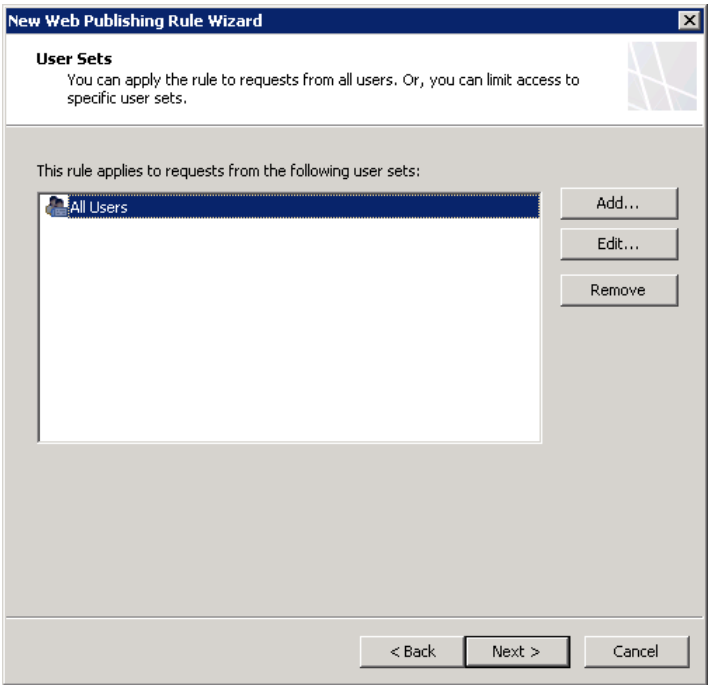


Copyright © Acronis International GmbH, 2002-2014

11. On the **Authentication Delegation** page select the **No delegation, but client may authenticate directly** option from the drop-down menu and click **Next**.

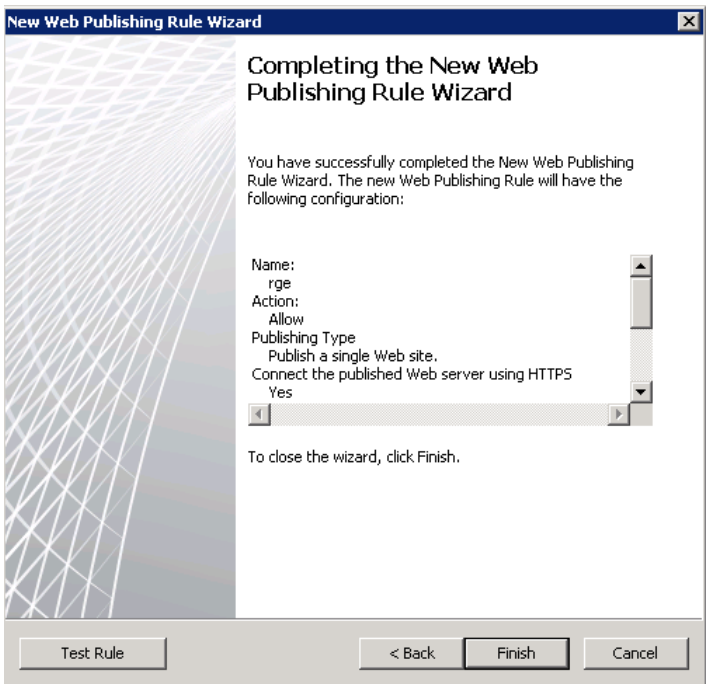


12. On the **User Sets** page verify that the default **All Users** option is present and click **Next** to continue.

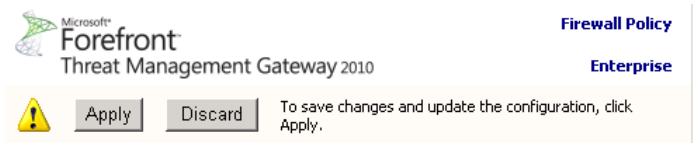


Copyright © Acronis International GmbH, 2002-2014

13. On the **Completing The New Web Publishing Rule Wizard** page review the summary of your selections. Click **Test Rule** to confirm that the publishing rule is working properly. Click **Finish** to complete the process.



14. Click the **Apply** button to commit the changes.



15. In the left pane of the Forefront TMG Management Console click **Monitoring**, then click on the **Configuration** tab in the middle pane. Keep clicking on the **Refresh Now** link in the right pane (**Tasks** tab) until there is a green icon with the checkbox in front of the TMG computer name (array name).

5.4.6 Configure an External DNS Entry for the Acronis Access Gateway Server

After the TMG configuration process has been completed, you need to create a DNS record in the external DNS servers in order to redirect all Acronis Access desktop/mobile connections to the external network adapter of the TMG. The DNS entry should resolve the name of your server (e.g. access.domain.com) to the external IP address of the TMG server. All client requests will be sent to and managed by TMG. In this configuration scenario, TMG does not require clients to authenticate, and all users will access the Acronis Access server without any knowledge that the response is coming from the Microsoft Forefront TMG instead.

5.4.7 Using the Access Mobile Client with a TMG reverse proxy server

This feature is built-in and requires little to no configuration.

In the Access Mobile Client app you manually add the server by doing the following:

1. Press the **+** button located in the left corner. This button allows you to add a new server.

Copyright © Acronis International GmbH, 2002-2014

2. In the **Server Name or IP Address** field, write the path to your server (e.g. yourserver.companyname.com/a http://yourserver.companyname.com/mobilechoccess).
3. Fill in your **credentials** (username / password).
4. Tap **Save.**

5.4.8 Using the Access Desktop Client with a TMG reverse proxy server.

This feature is built-in and requires little to no configuration.

For the desktop client:

1. RIght click on the tray Acronis Access icon. Select **Preferences**.
2. In the **Server URL** field, write the path to your server (e.g. access.companyname.com http://yourserver.companyname.com/activecho).
3. Fill in your **credentials** (username / password).
4. Press **Apply.**
5. Done!

5.5 Unattended desktop client configuration

With the use of Microsoft's Group Policy Management, you can easily configure the Acronis Access Desktop client on multiple machines remotely. The only thing end users will have to do is install, start the client and enter their password. The Group Policy Management also ensures that users cannot change/replace the correct settings by accident. If this happens, they can simply log off and when they log in, the correct settings will be re-applied.

Creating and configuring the Group Policy Management object:

1. On your domain controller, open the **Group Policy Management** console.
2. Right-click on your desired domain and select **Create a GPO in this domain, and Link it here...**.
3. Give it a name and press **OK**.
4. Expand the **Group Policy Objects** section and select your new policy.
5. Under the **Scope** tab select the desired sites, domains, OUs, groups, users and/or computers.

Creating the folder and registry entries:

In this example we will create entries for the Username, Sync-Folder, Server URL, the Auto-Update checkbox and if the client should connect to servers with self-signed certificates.

1. Expand the **Group Policy Objects** section and right click on your new Policy Object.
2. Select **Edit** and expand **User Configuration** -> **Preferences** -> **Windows Settings**.

Creating the sync folder:

1. Right-click on **Folders** and select **New** -> **Folder**.

Copyright © Acronis International GmbH, 2002-2014

2. Set the **Action** to **Create**.
3. For the path, enter the following token: **%USERPROFILE%\Desktop\AAS Data Folder**

Creating the registry:

1. Right-click on **Registry** and select **New** -> **Registry Item**.
2. Set the **Action** to **Create**.
3. For **Hive**, select **HKEY_CURRENT_USER**.
4. For the path, enter the following: **Software\Group Logic, Inc.\activEcho Client**
5. Now do the following for the desired entries:
6. For the Username:
   a. For **Value name** enter "**Username**".
   b. For **Value type** select **REG_SZ**.
   c. For **Value data** enter the following token: **%USERNAME%@%USERDOMAIN%**
7. For the Server URL:
   a. For **Value name** enter "**Server URL**".
   b. For **Value type** select **REG_SZ**.
   c. For **Value data** enter the address of your Access Server. e.g. **https://myaccess.com**
8. For the Sync-Folder:
   a. For **Value name** enter "**activEcho Folder**".
   b. For **Value type** select **REG_SZ**.
   c. For **Value data** enter the following token and path: **%USERPROFILE%\Desktop\AAS Data Folder**
9. For the Auto-Update:
   a. For **Value name** enter "**AutoCheckForUpdates**".
   b. For **Value type** select **DWORD**.
   c. For **Value data** enter "**00000001**". The value "**1**" enables this setting and the client will automatically check for updates. Setting the value to "**0**" will disable the setting.
10. For the Certificates:
    a. For **Value name** enter "**AllowInvalidCertificates**".
    b. For **Value type** select **DWORD**.
    c. For **Value data** enter "**00000000**". The value "**0**" disables this setting and the client will not be able to connect to Acronis Access servers with invalid certificates. Setting the value to "**1**" will enable the setting.

5.6 Monitoring Acronis Access with New Relic

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

1. Open http://newrelic.com/ http://newrelic.com/ and create a New Relic account.
2. For Application type select Mobile app.
3. For Platform mark Ruby.
4. Finish creating your account and log in.
5. Go to Applications, leave the **ruby bundle**(step 1) as is and continue to the next step.

Copyright © Acronis International GmbH, 2002-2014

6. Download the New Relic script - newrelic.yml.
7. Open your Acronis Access web UI.
8. Go to Settings and click on Monitoring.
9. Enter the path to the newrelic.yml including the extension (e.g. **`C:\software\newrelic.yml`**). We recommend you put this file in a folder outside of the Acronis Access folder so that it will not be removed or altered on upgrade or uninstall.
10. Click Save and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
11. If more than 10 minutes pass, restart your Acronis Access Tomcat service and wait a couple of minutes. The button should be active now.
12. You should be able to monitor you Acronis Access server via the New Relic website.

All the information the Acronis Access server logs about trying to connect to New Relic and set up monitoring is in a file called ***newrelic_agent.log*** *found here -* ***`C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs`****. If you have any problems, you can find information in the log file.*

There is frequently a warning/error that starts like this:
WARN : DNS Error caching IP address: Errno::ENOENT: No such file or directory - C:/etc/hosts which

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

If you want to monitor the actual computer as well

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

5.7 Using trusted server certificates with Acronis Access

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

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

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

Requirements

The certificate you are using must contain its private key. PFX certificates are highly recommended but other types (CRT, CER) will work too, as long as they have their private key.

Copyright © Acronis International GmbH, 2002-2014

Installing your certificate to your Windows certificate store

1. On the server, click **Start**, and then click **Run**.
2. In the **Open box**, type **mmc**, and then click **OK**.
3. On the **File menu** click **Add/Remove snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, click **Computer account** (this is not selected by default), and then click **Next**.
7. In the **Select Computer** dialog box, click **Local computer**: (the computer this console is running on), and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the left pane of the console, double-click **Certificates** (**Local Computer**).
11. Right-click **Personal**, point to **All Tasks**, and then click **Import**.
12. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
13. On the **File to Import page**, click **Browse**, locate your certificate file, and then click **Next**.

    Note: *If you are importing a PFX file, you will need to change the file filter to* ***"Personal Information Exchange (*.pfx, *.p12)****" to display it.*

14. If the certificate has a password, type the password on the **Password** page, and then click **Next**.
15. Check the following boxes:
    a. **Mark this key as exportable**
    b. **Include all extended properties**
16. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.
17. Click **Finish**, and then click **OK** to confirm that the import was successful.

All of the certificates successfully installed in the Windows Certificate Store will be available when using the Acronis Access Configuration Utility.

Configure Acronis Access **to use your certificate**

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

1. Launch the Acronis Access Configuration Utility.

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

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

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

Copyright © Acronis International GmbH, 2002-2014

5.8 Creating a Drop Folder

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

In the Active Directory, do the following:

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

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

Creating the Drop Folder

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

Setting the permissions

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

For the superuser group

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

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

For the drop-only users

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

Copyright © Acronis International GmbH, 2002-2014

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

For the Creator Owner group

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

- **Delete**

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

1. Expand the **Mobile Access** tab and open the **Policies** page.
2. Press **Add Group Policy**.
3. For the superuser group (Group A), fill out all policy tabs per your company's requirements. For more information visit the Policies (p. 8) section.
4. For the drop-only group (Group B), fill out all policy tabs per your company's requirements. On the **Application Policy** tab, select only the following actions:
   - **File Copies / Creation**
   - **File Deletes**
   - **Folder Copies**
   - **Sending Files to Acronis Access from Other Apps**
   - **Sending Files to Acronis Access Using Quickoffice 'Save Back'**

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

5.9 Customizing the web interface

Acronis Access allows for the web based user interface to be modified to satisfy branding and look and feel requirements. Color schemes, logos and other elements can be changed to permit customers to better integrate the solution with their corporate standards.

To add a custom logo:

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

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

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

To add custom style sheets:

Copyright © Acronis International GmbH, 2002-2014

1. Make a copy of one of the default style sheets in the **\stylesheets** directory. They are generally located at: **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\stylesheets**.
2. Place it in the **customizations** folder. This folder is generally located at: **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\customizations**.
3. Edit the style sheet and change colors and settings based on your preference and save the changes.
4. Give the file a new name starting with **color_scheme_*.css**. (e.g. **color_scheme_My_Color.css**). This file will appear in the **Color Scheme** drop-down on the Server Settings (p. 72) page.
5. Open the web interface and navigate to **General Settings** -> **Server**.
6. Click on **Color Scheme** and select your custom scheme (**My Color**) from the drop-down menu.
7. Press **Save**.

5.10 How to support different Access Desktop Client versions

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

1. Download the version of Access Desktop Client which you want to use. Make sure you have these 4 files:
   - AcronisAccessMac.zip
   - AAClientInstaller.msi
   - AcronisAccessInstaller.dmg
   - AcronisAccessClientInstaller.exe
2. Copy the files.
3. On the server, open the Access Desktop Clients folder (**C:\Program Files (x86)\Acronis\Access Server\Web Application\clients**).
4. Create a sub-folder for this version of the client. It should be named with the **client version number** (e.g. **2.7.0x167**, **2.6.0.x140**, **2.7.1x145**).
5. Paste the 4 files in the sub-folder you just created.
6. Next, open the **Web User Interface** of your Acronis Access server.
7. Log-in as an **administrator** and go to the **Sync & Share** tab and open the **Acronis Access Client** page.
8. Find this setting: **Allow client auto-update to version**.
9. From the drop-down menu select your desired version.

Note: *The download link in the* ***Action menu*** *for your account, will still download the latest available Acronis Access Desktop Client version. If you do not want the users to download the latest version, go to the* ***\Access Server\Web Application\clients*** *folder and rename the latest client version (e.g.* ***3.0.3x102****) folder to "****do not use version number****" (e.g. "****do not use 3.0.3x102****").*

5.11 How to move the FileStore to a non-default location.

Note: *Before proceeding, please log-in as an administrator, go to the* ***Server Settings*** *page and from the* ***File Store Repository Service*** *field take note of the port being used. This port is normally 5787 but your setup may be different. You will need this port in the following steps.*

Copyright © Acronis International GmbH, 2002-2014

1. Go to the machine on which Acronis Access is installed.
2. Stop the **Acronis Access File Repository Server** service.
3. Stop the **Acronis Access Tomcat** service.
4. You will find the current FileStore in the folder which you selected with the **Configuration Utility**.
5. Copy or move the entire FileStore folder with all its contents to the target point, like so: **`D:\MyCustom Folder\FileStore`**
6. Open the **Configuration Utility**.
7. In the **File Repository** tab, change the path of the **FileStore** to the new path where you've moved the **FileStore.**
8. Change the FileStore port if needed. If you change the FileStore port, you must also change the File Store Repository Endpoint in the Sync & Share File Repository (p. 65) settings.
9. If the file storage for the File Repository is on a remote network share, configure the service account 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.
10. Start **Acronis Access File Repository Server** service
11. Start the **Acronis Access Tomcat** service.
12. Done.

5.12 Acronis Access for Good Dynamics

In this section

Introduction 120
Testing a trial version of Acronis Access for Good Dynamics 121
Requesting and configuring Acronis Access within Good Control.....122
Good Dynamics Policy Sets and Acronis Access.....126
Granting Acronis Access access to a Good Dynamics User or Group 127
Enrolling the Acronis Access client app in Good Dynamics 129

5.12.1 Introduction

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

The components of the Good Dynamics platform include:

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

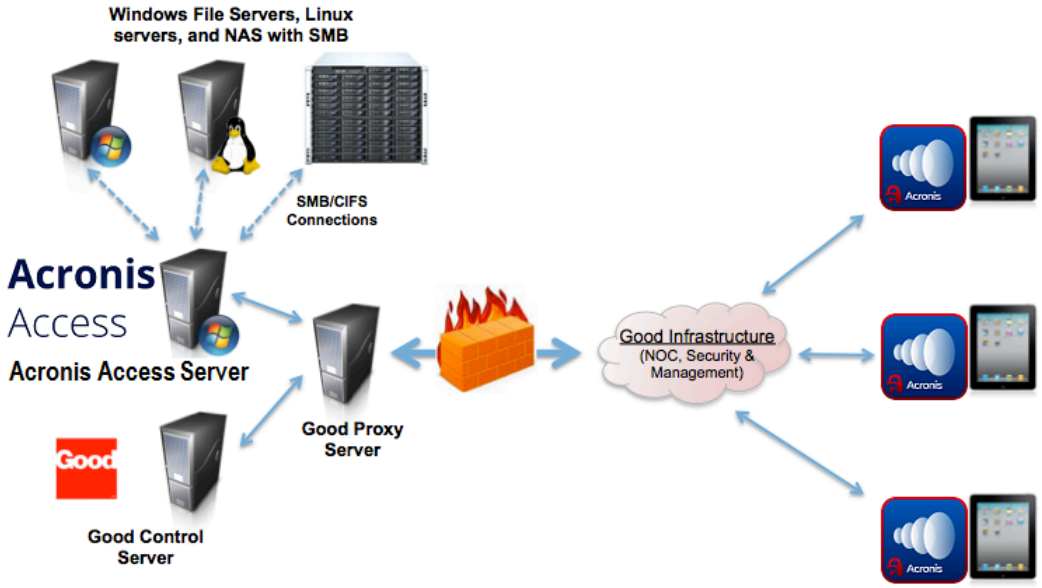
 Copyright © Acronis International GmbH, 2002-2014

managed using the Good Dynamics platform and also provide the app with FIPS 140-2 certified on-device encrypted secure storage and Good secure communication.

Acronis Access for Good Dynamics requires:

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

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



5.12.2 Testing a trial version of Acronis Access for Good Dynamics

The process of trialing Acronis Access for Good Dynamics is very much the same as a regular Acronis Access trial.

1. A trial version of the server-side software can be requested by visiting the Trial page. Once this request form has been submitted, you will receive an email with links to download the Acronis Access server trial installer and to the Quick Start Guide to assist in initial setup.
2. The Acronis Access for Good Dynamics client app is a free download from the Apple App Store http://www.grouplogic.com/web/megoodappstore.
   http://www.grouplogic.com/web/meappstore

Acronis Access for Good Dynamics client apps need to be activated in your Good Dynamics system before they can be configured for access to Gateway Servers. When you are ready to enroll Acronis Access in Good Dynamics, please proceed to the following sections of this document.

Copyright © Acronis International GmbH, 2002-2014

5.12.3 Requesting and configuring Acronis Access within Good Control

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

In this section

Requesting access to Acronis Access for Good Dynamics 122
Configuring Good Proxy access to your Acronis Access Gateway server(s)124
Allowing access to multiple Acronis Access Gateway servers 125

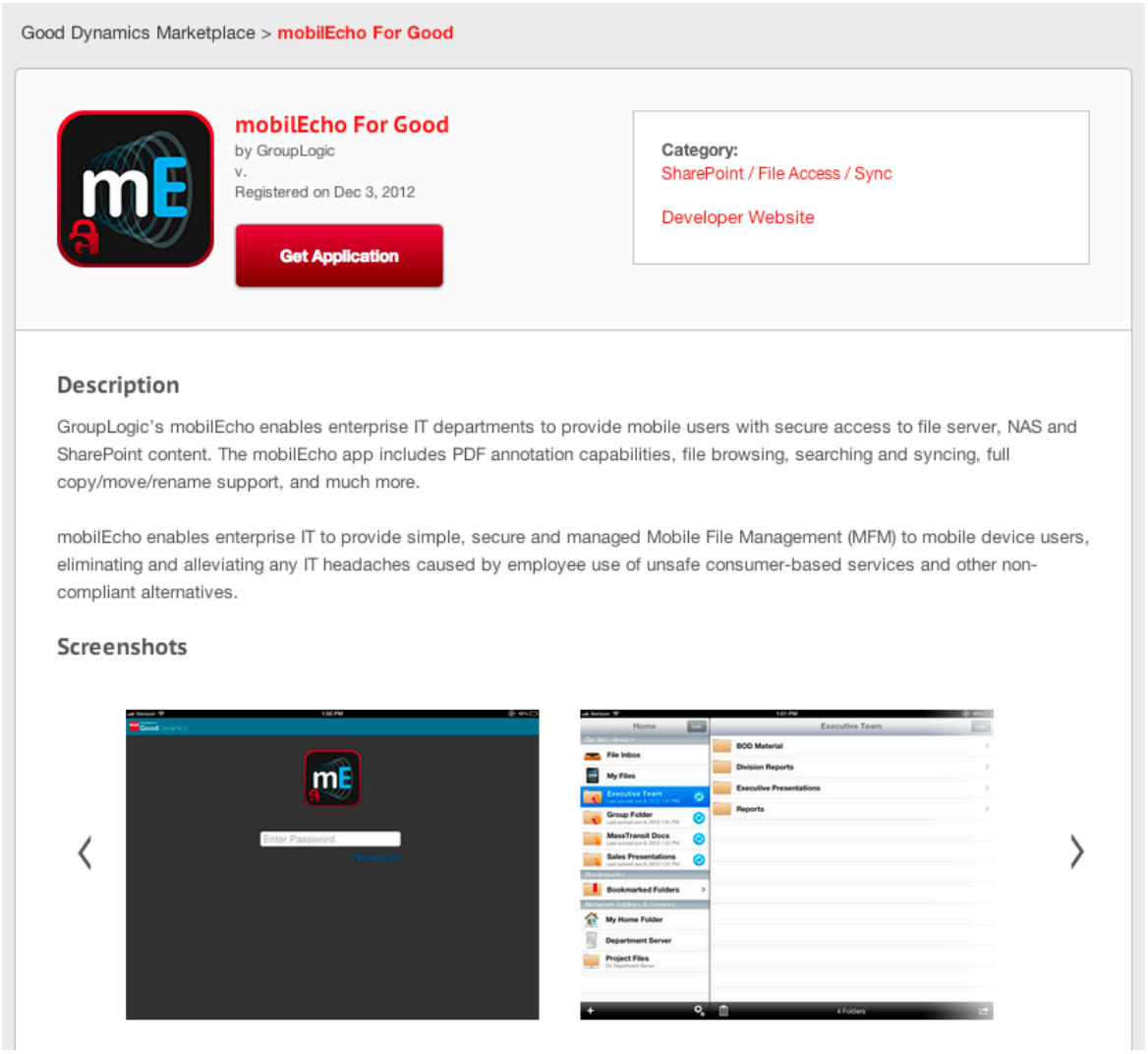
5.12.3.1 Requesting access to Acronis Access for Good Dynamics

To request access to **Acronis Access for Good**, visit this URL:
https://begood.good.com/gd-app-details.jspa?ID=248978
https://begood.good.com/gd-app-details.jspa?ID=248978

That link should take you directly to the app. If it does not, visit
https://begood.good.com/marketplace.jspa https://begood.good.com/marketplace.jspa and locate **Acronis Access for Good** in the list of available **Good Dynamics** apps.

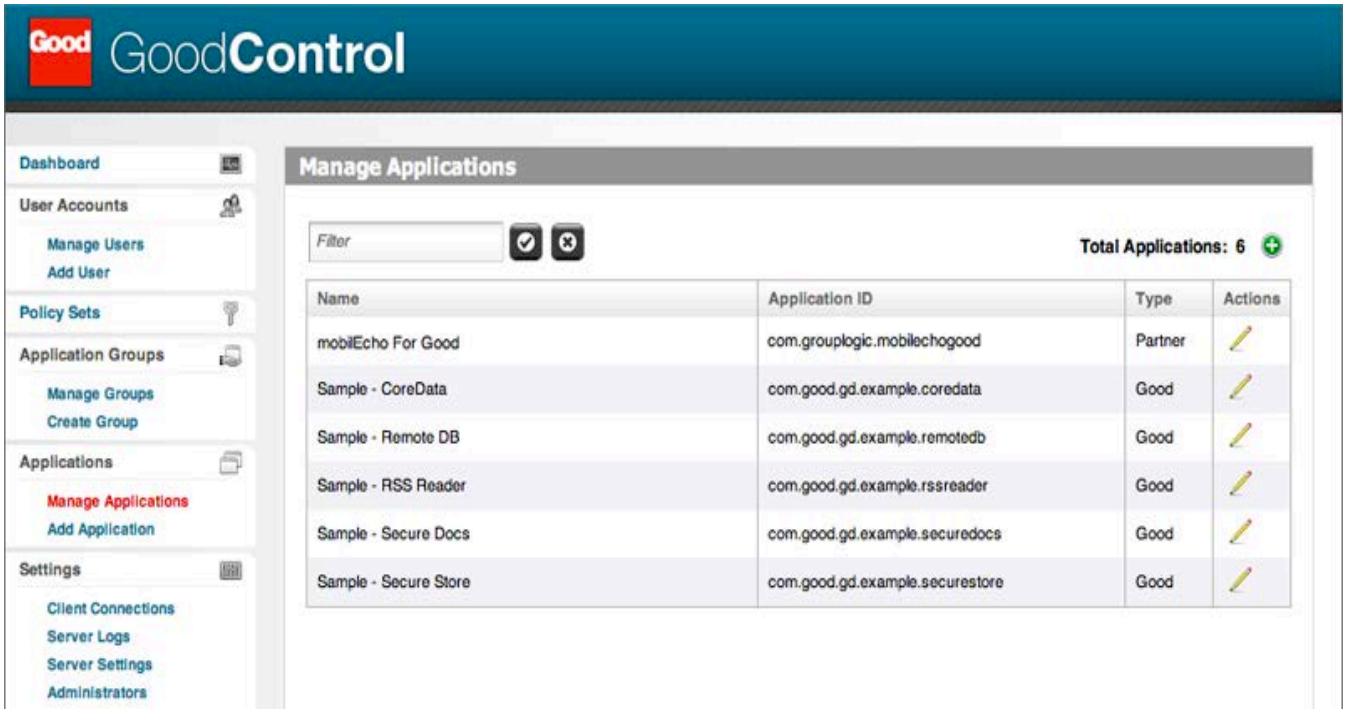
Copyright © Acronis International GmbH, 2002-2014

On the Acronis Access for Good app page, click the Get Application button to request a trial or licensed version of the app. https://begood.good.com/gd-app-details.jspa?ID=248978



Copyright © Acronis International GmbH, 2002-2014

If you select a trial version of the app, your access should be granted within a few minutes. You should receive a notification from the beGood site when your request has been accepted and notifying you that the **Acronis Access for Good** app as been published to your Good Control server. Once this has happened, log into your Good Control server and click Manage Applications in the lefthand menu. Acronis Access should now be listed as a Partner app in your managed applications list. If it's not listed, give it 15 minutes or so and check again. This will allow the change time to propagate to your server.



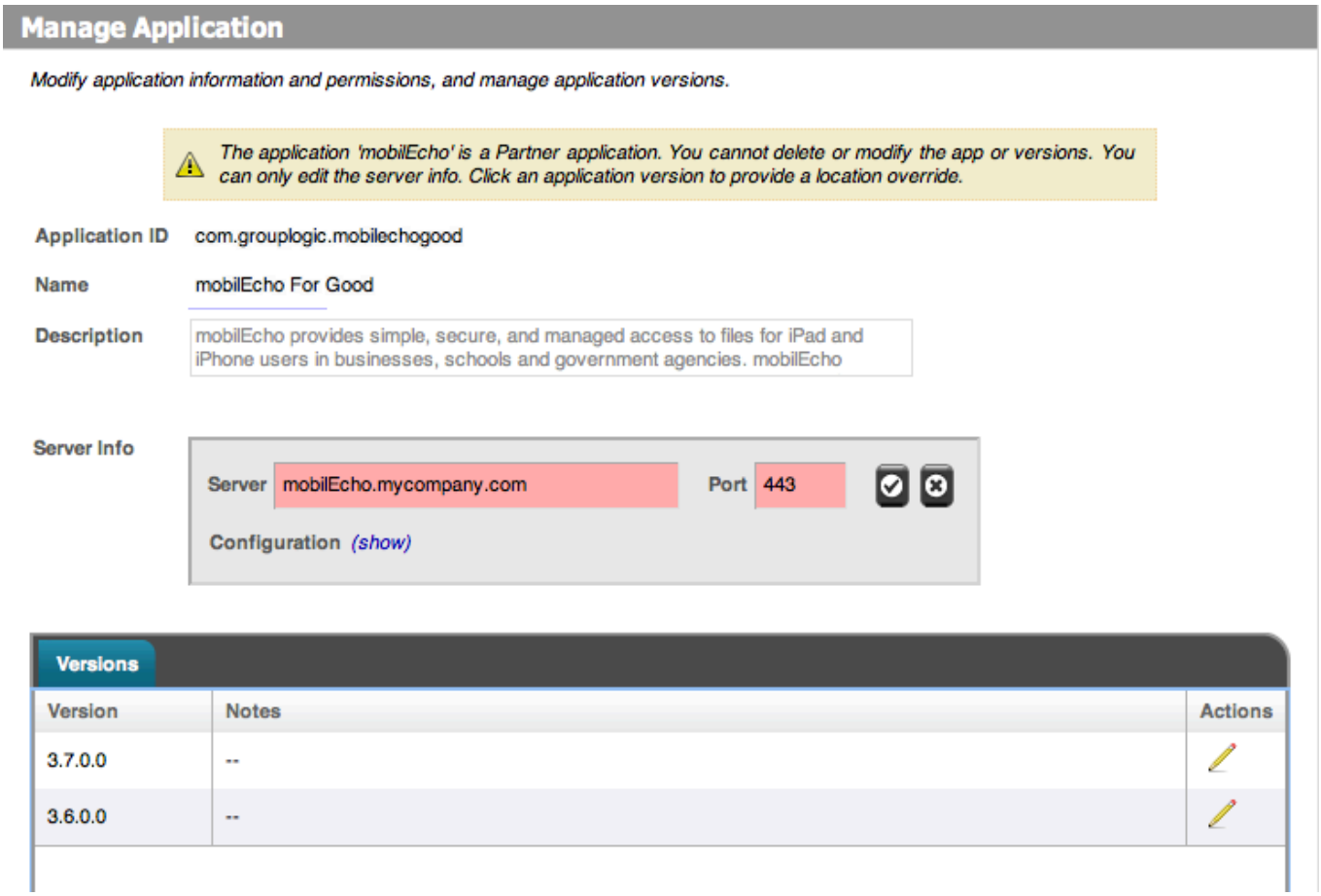
5.12.3.2 Configuring Good Proxy access to your Acronis Access Gateway server(s)

In order for Access Mobile Clients to be able to access your Acronis Access Gateway server through the Good Proxy server, you will need to enter the address of your Acronis Access Gateway server in the application's configuration. If you have more than one Acronis Access Gateway server, configure access to one Acronis Access Gateway server here and additional servers can be added on the Client Connections page in the Good Control console. Details on doing so are included below.

Click the **Acronis Access** app in the **Manage Applications** list to open its settings.

Copyright © Acronis International GmbH, 2002-2014

In the **Server Info** box, enter the DNS name or IP address of your Acronis Access Gateway server. The **Port** number is usually **443**, unless you've configured Acronis Access to run on a non-standard port. All communication between Acronis Access clients and the Gateway servers occurs on port 443 by default. Click the 'Check' button to save this change.



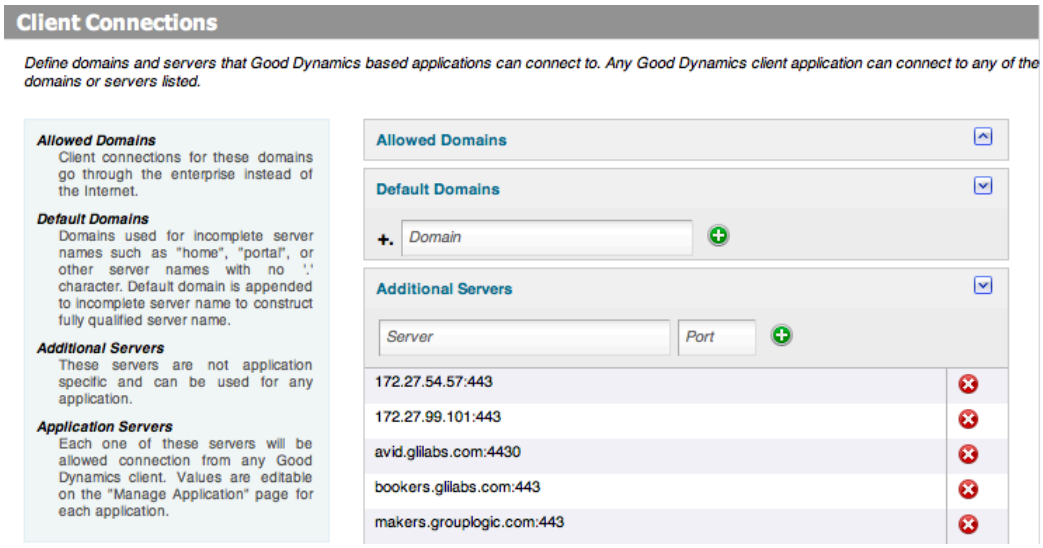
5.12.3.3 Allowing access to multiple Acronis Access Gateway servers

If you have more than one Acronis Access Gateway server on your network, you will have to allow additional server addresses in the Good Control console. If you do not so this, the Access Mobile Client will only be able to connect to the single server you configured in the previous step.

To permit access to additional Gateway servers, select the **Client Connections** item in the lefthand menu in the Good Control console.

Copyright © Acronis International GmbH, 2002-2014

In the **Additional Servers** box, enter the Gateway server's DNS name or IP address and it's port, then click the "+" icon to add it to the list. The default Gateway server port is 443.



5.12.4 Good Dynamics Policy Sets and Acronis Access

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

These settings include:

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

Data Leakage Protection effects and limitations

If **Data Leakage Protection** is enabled in a policy set, the Access Mobile Client app will not be permitted to:

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

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

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

Copyright © Acronis International GmbH, 2002-2014

An upcoming version of Acronis Access for Good Dynamics will add the ability to transfer files directly between the Acronis Access for Good Dynamics app and other 3rd party Good Dynamics apps. This capability requires changes to Acronis Access for Good Dynamics and to the 3rd party apps involved, so any app that you need to transfer files to will also need to be updated by its vendor.

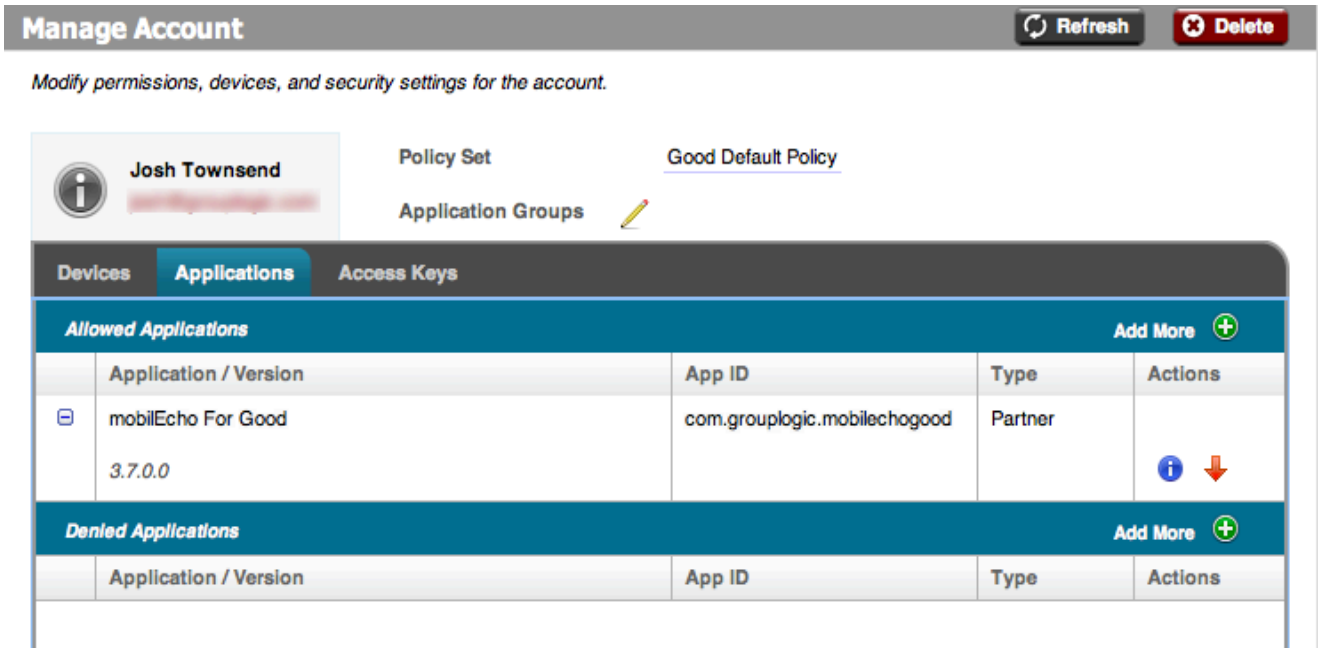
5.12.5 Granting Acronis Access access to a Good Dynamics User or Group

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

IMPORTANT DEPLOYMENT NOTE: *When you assign access to Good Dynamics applications to individual users, you are required to select specific version numbers of the app to allow. If you managed access on the user level, when new versions of Acronis Access for Good are released, you will need to return to the users' Good Control configuration and add the new version before they are allowed to run that version. We **highly recommend** that you allow access to Good Dynamics apps using the **Manage Groups** functionality in the Good Control console. Good Control allows you to give a group access to ALL versions of an app, so that future versions will be allowed without IT admin intervention.*

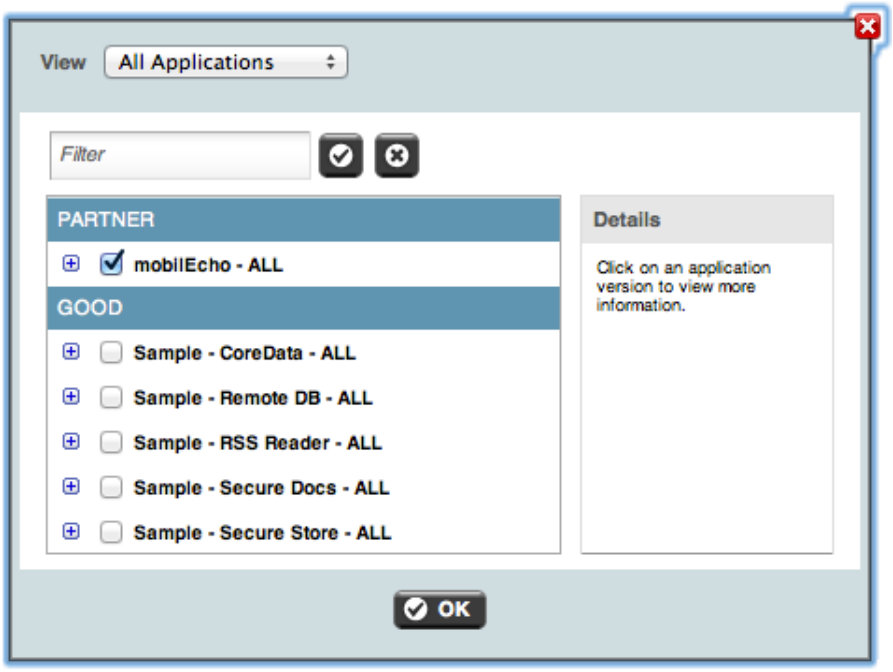
To add the Acronis Access **app to an Allowed Applications list in a User Account or Application Group:**

1. Select **Manage Groups** or **Manage Users** from the lefthand menu in the Good Control console.
2. Select the group or user you'd like to give access to Acronis Access for Good.
3. On the **Applications** tab, click the **Allowed Applications** "**Add More**" button.



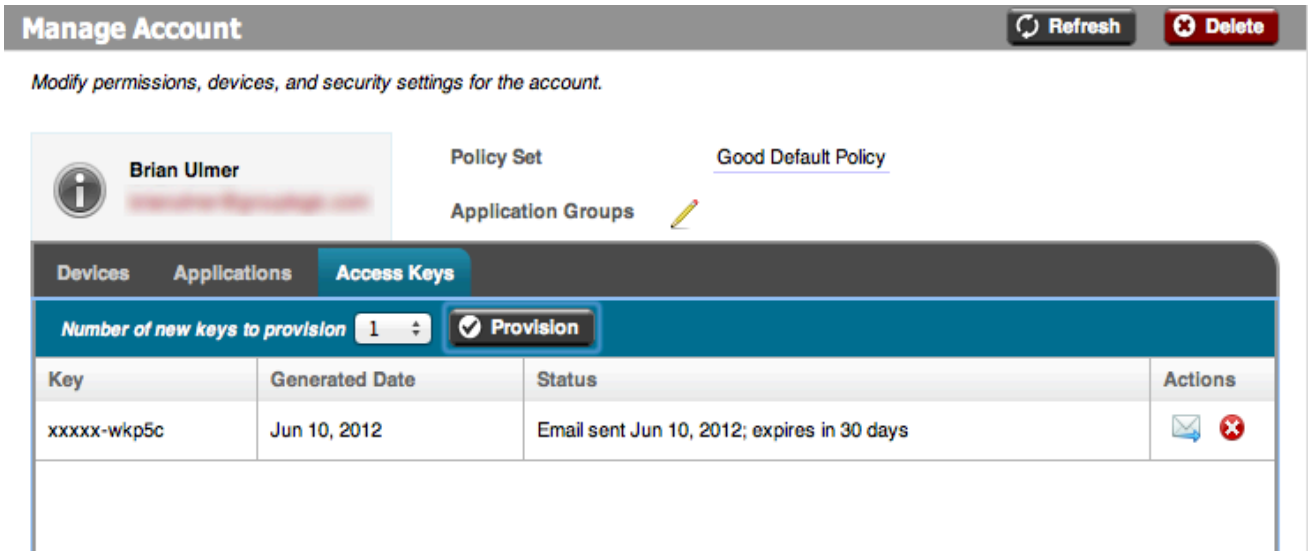
Copyright © Acronis International GmbH, 2002-2014

4. Select **Acronis Access for Good** from the list of available applications and click **OK**.



To generate an Access Key that will allow a user to enroll their Acronis Access for Good app with Good Dynamics:

1. Select **Manage Users** from the lefthand menu in the Good Control console.
2. Select the user you'd like to create an **Access Key** for.
3. On the **Access Keys** tab, select the number of keys you'd like to send and click the **Provision** button.



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

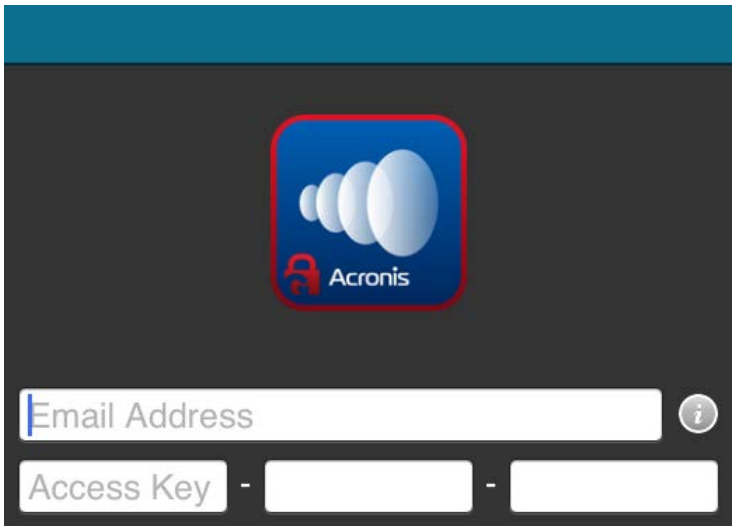
Copyright © Acronis International GmbH, 2002-2014

5.12.6 Enrolling the Acronis Access client app in Good Dynamics

The Acronis Access for Good client app available on the Apple App Store http://www.grouplogic.com/web/megoodappstore is purpose build as a Good Dynamics integrated application. When first installed on a device, the Acronis Access app starts and required the user to activate it in your Good Dynamics system.

To enroll a Acronis Access **client app in Good Dynamics:**

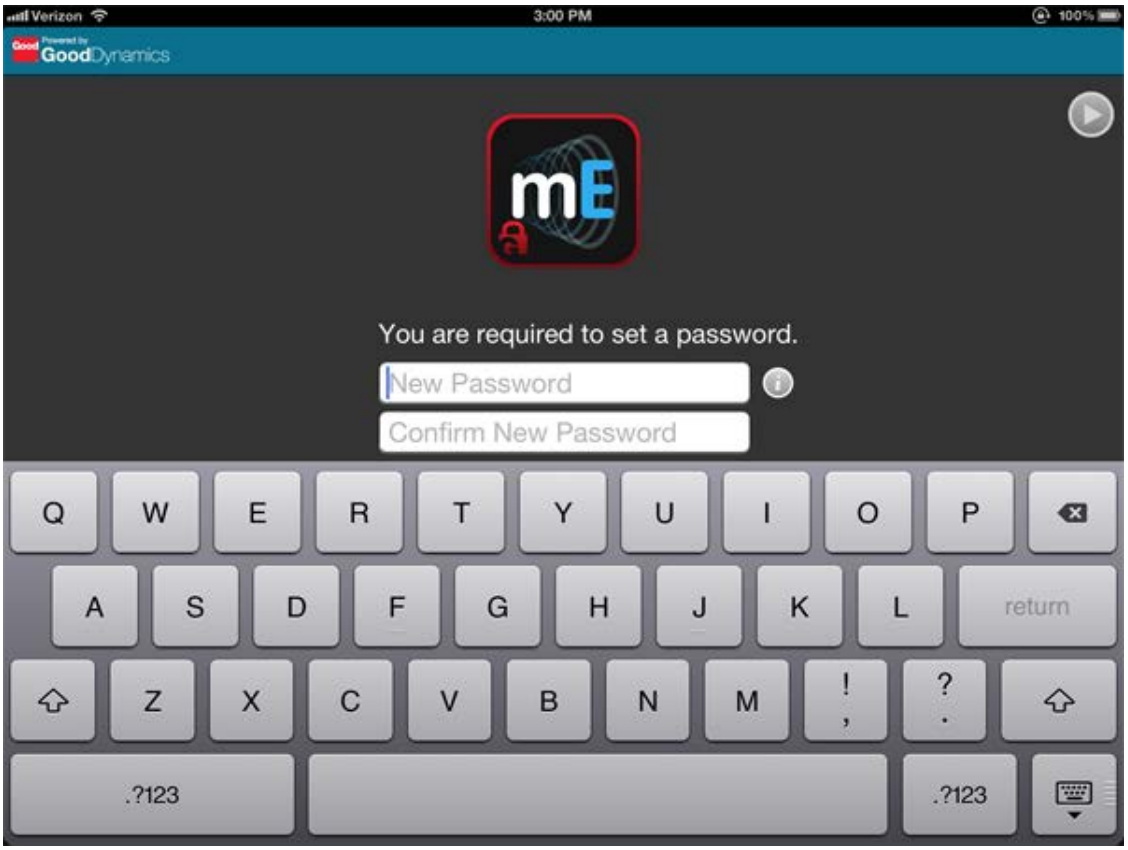
1. Launch **Acronis Access for Good Dynamics** on your device.
2. Enter your **Email Address** and the **Access Key** that was emailed to you by your IT administrator.



3. Progress will be displayed as your app is enrolled with Good Dynamics.

Copyright © Acronis International GmbH, 2002-2014

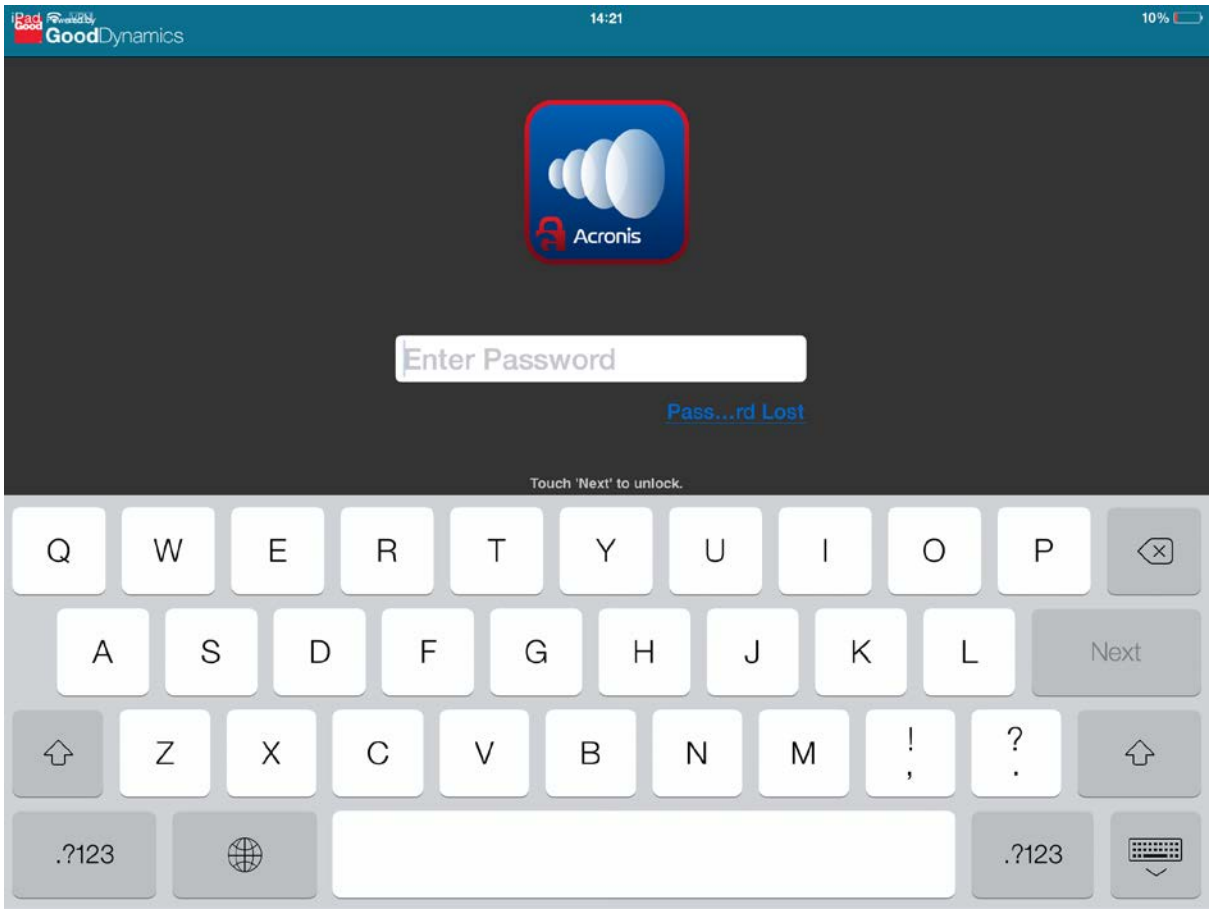
4. If required by your Good Dynamics policy, you will be asked to set an application lock password. If you are also using Good for Enterprise, Acronis Access may require that you log into Good for Enterprise in order to gain access to the Acronis Access app.



5. Once this process is completed, you will be taken to the Acronis Access application's home screen.

Copyright © Acronis International GmbH, 2002-2014

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



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

Once the Acronis Access for Good Dynamics app has been activated in Good Dynamics, it is not possible to deactivate. If you need to switch to a standard version of Acronis Access , you will need to delete the Acronis Access for Good Dynamics app and reinstall the standard Access Mobile Client app by visiting the Apple App Store http://www.grouplogic.com/web/meappstore.

5.13 MobileIron AppConnect support

In this section

Introduction 132
Testing a trial version of Acronis Access with AppConnect 132
Creating an AppConnect configuration and policy for Acronis Access on your MobileIron VSP 132
Activating the Acronis Access iOS client with AppConnect 136
Ongoing AppConnect management of Access Mobile Clients.....137
Using AppConnect with Kerberos Constrained Delegation 137
Advanced Delegation Configurations 159

Copyright © Acronis International GmbH, 2002-2014

5.13.1 Introduction

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

The components of Acronis Access with MobileIron AppConnect include:

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

5.13.2 Testing a trial version of Acronis Access with AppConnect

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

1. A trial version of the server-side software can be requested by visiting the Trial page. Once this request form has been submitted, you will receive an email with links to download the Acronis Access server trial installer and to the Quick Start Guide to assist in initial setup.
2. The Acronis Access iOS client app is a free download from the Apple App Store. http://www.grouplogic.com/web/meappstore

The Acronis Access iOS app needs to have an AppConnect configuration and policy created on your MobileIron Virtual Smartphone platform (VSP) before it can be auto-configured for access to your Acronis Access Gateway server(s).

The iOS device also needs to have the MobileIron Mobile@Work app https://itunes.apple.com/app/mobilecho/id320659794 installed before any AppConnect-enabled apps can be activated.

When you are ready to activate Access Mobile Clients with AppConnect, please proceed to the following sections of this document.

5.13.3 Creating an AppConnect configuration and policy for Acronis Access on your MobileIron VSP

Before you can start on-boarding Acronis Access users (p. 26). You will need to create two items on your MobileIron VSP:

Copyright © Acronis International GmbH, 2002-2014

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

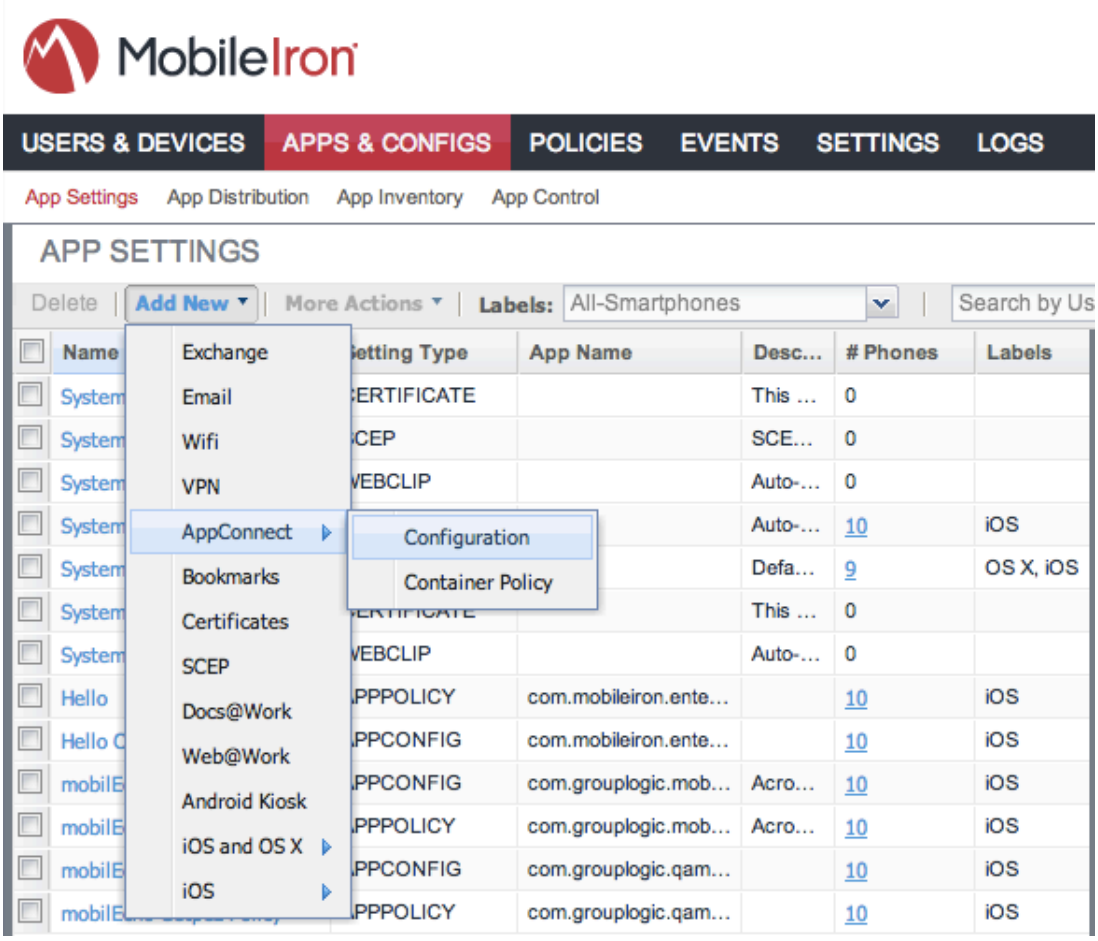
In this section

Creating a Access Mobile Client app Configuration.....133
Creating a Acronis Access app Container Policy 135
Assign labels to the new Configuration and Container Policy 136

5.13.3.1 Creating a Access Mobile Client app Configuration

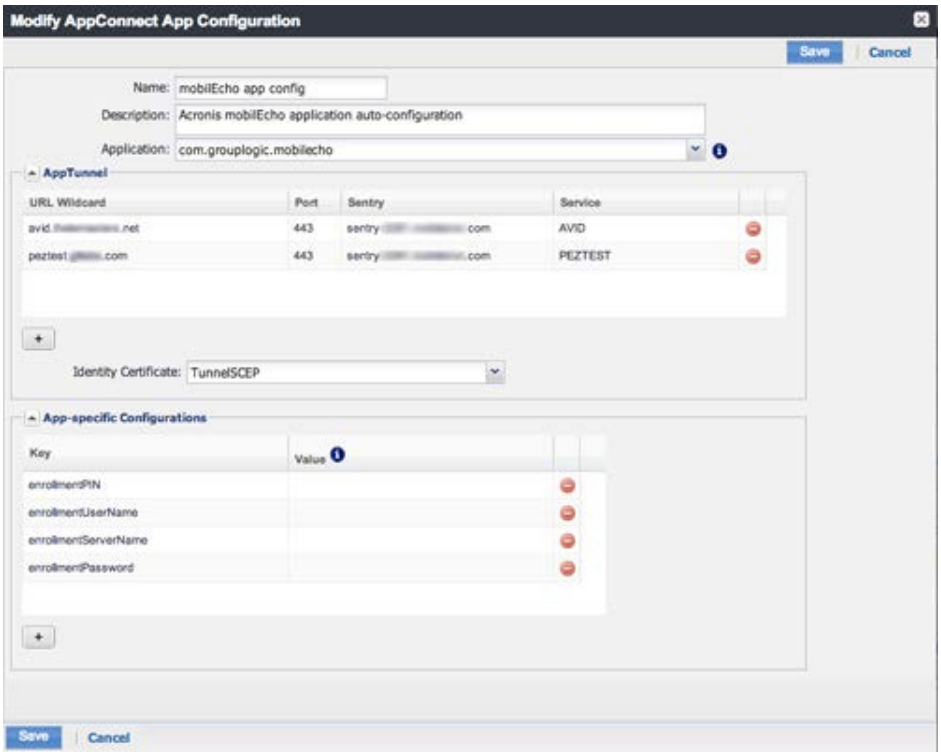
Log into your MobileIron VSP web console and select the **APPS & CONFIGS** tab.

Within **App Settings**, click **Add New** and select **Configuration** in the **AppConnect** menu item.



Copyright © Acronis International GmbH, 2002-2014

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



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

Description – This can be any description you like.

Application – This must be set to the *Bundle Identifier* of the Access Mobile Client app, which is: **com.grouplogic.mobilecho**

AppTunnel – The AppTunnel settings are optional and only needed if you are using AppTunnel to provide access to your Acronis Access Gateway server(s). **URL Wildcard** = the DNS address of your Gateway server(s) or your domain as a whole. Acronis Accesss use port 443 by default. **Sentry** = the DNS address of your MobileIron Sentry server.

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

- **enrollmentServerName** – This key field is required. The value of this key should be set to the DNS address of the Acronis Access Server that the user should enroll with.
- **enrollmentPIN** – This key is optional. If your Acronis Access Server requires a PIN number for client enrollment, you can auto-complete the PIN number field in the Acronis Access enrollment form with this value. It is typical that the PIN requirement on the Acronis Access Server is disabled, since AppConnect can serve as the 2nd factor of authentication before a user has access, rather than the one-time-use PIN number. This PIN requirement is configured on the **Settings** page (p. 56) of the **Acronis Access** web console.
- **enrollmentAutoSubmit** - This key is optional. This will cause the enrollment form to be submitted automatically, so that they user does not have to tap the "Enroll Now" button to proceed. To enable this key, set its value to: **Yes**

Copyright © Acronis International GmbH, 2002-2014

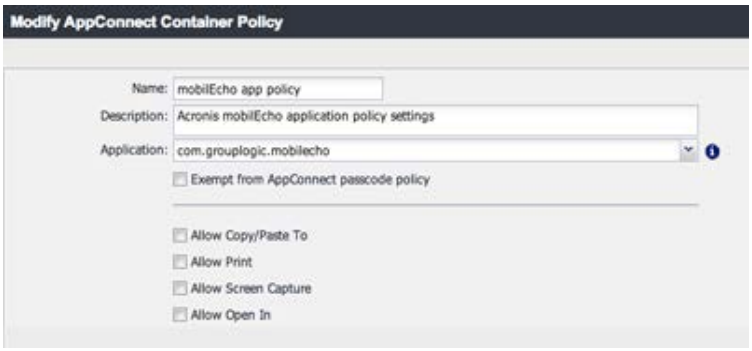
- **requirePIN** – This key is optional. If you are distributing a PIN to Acronis Access mobile users that they will need to manually enter into the Acronis Access enrollment form, you can specify that the PIN field is immediately shown in the form by setting this key's value to: **Yes**
- **enrollmentUserName** – This key is optional. The value of this key will be inserted into the Username field in the Acronis Access enrollment form. You can use a MobileIron variable to autocomplete this value with the specific user's username.
- **enrollmentPassword** – This key is optional. The value of this key will be inserted into the Password field in the Acronis Access enrollment form. You can use a MobileIron variable to autocomplete this value with the specific user's password.

5.13.3.2 Creating a Acronis Access app Container Policy

Log into, or return to, your MobileIron VSP web console's **APPS & CONFIGS** tab.

Within **App Settings**, click **Add New** and select **Container Policy** in the **AppConnect** menu item.

Within this new Container Policy, enter the following information:



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

Description – This can be any description you like.

Application – This must be set to the *Bundle Identifier* of the Access Mobile Client app, which is: **com.grouplogic.mobilecho**

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

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

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

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

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

Copyright © Acronis International GmbH, 2002-2014

5.13.3.3 Assign labels to the new Configuration and Container Policy

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

5.13.4 Activating the Acronis Access iOS client with AppConnect

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

Ensure Mobile@Work is installed and configured

Before installing or activating the Access Mobile Client, ensure that you have installed the MobileIron Mobile@Work iOS app https://itunes.apple.com/app/mobileiron-mobile-work-client/id320659794 on your device. This app serves as the conduit through which Acronis Access communicates with the MobileIron VSP and receives AppConnect configuration and commands.

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

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

In this section

Acronis Access has already been installed on the device, and has already been enrolled with a Acronis Access Server
Acronis Access has already been installed on the device, but has not yet been enrolled with a Acronis Access Server
Acronis Access has not yet been installed on the device 137

5.13.4.1 Acronis Access has already been installed on the device, and has already been enrolled with a Acronis Access Server

This scenario, is similar to the previous scenario, the only difference being that the AppConnect Acronis Access Configuration will not be used to auto-enroll the Access Mobile Client app. If the Access Mobile Client app is already enrolled with a Acronis Access Server, it will maintain that original configuration. Acronis Access will become managed by AppConnect and will begin using the AppConnect passcode and permissions Container Policies. If you require a user to enroll with a different Acronis Access Server, you will need to have them uninstall Acronis Access and reinstall the app before they can be configured by AppConnect.

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

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

Copyright © Acronis International GmbH, 2002-2014

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

5.13.4.3 Acronis Access has not yet been installed on the device

In this scenario, you will need to install Acronis Access for the first time from the Apple App Store http://www.grouplogic.com/web/meappstore.

Once installed, start Acronis Access.

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

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

5.13.5 Ongoing AppConnect management of Access Mobile Clients

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

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

5.13.6 Using AppConnect with Kerberos Constrained Delegation

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

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

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

Copyright © Acronis International GmbH, 2002-2014

username/password authentication before moving on to Kerberos to eliminate steps in problem determination.

Before you begin

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

  Note: *All of the configuration related to KCD is done through MobileIron and Windows. There are no special changes to make in Acronis Access itself.*

- Key Distribution Center, abbreviated KDC, is a network service that supplies session tickets and temporary session keys to users and computers within an Active Directory domain.
- Only the Gateway Server accepts Kerberos authentication. The Access Server does not.
  - The Access client app must be enrolled in client management with a Gateway Server. If the client is enrolled with the Access Server, their login will fail.
  - Mobile clients using Kerberos authentication will only be able to authenticate to network shares and SharePoint sites. They cannot use KCD to access Acronis Access Sync & Share folders, since the Access service does not allow Kerberos authentication.

Prerequisites

The following software is should already be installed and configured:

- MobileIron VSP (5.9 used in this document)
- For Kerberos to work properly the user accounts on the VSP should come from the Active Directory that will be configured to support Kerberos
- MobileIron Sentry (4.8 used in this document)
- Access server installed (6.0.2 used in this document)
- Servers interoperability
  - The time on the VSP, Sentry, Domain Controller, and Access servers must all be synchronized (NTP recommended)
  - Domain name resolution (DNS). The Sentry will ask for a ticket from the KDC using the DNS name it has been configured to contact. This name must match the computer name set up for Kerberos delegation or the KDC will refuse to grant a ticket.
  - The VSP must be able to reach the Sentry (ports 9090 and 443 by defaults – others based on your configuration).
  - The Sentry must be able to reach the Active Directory and Access server (ports 88, 389, 636).
  - Ports 88 (UDP and TCP) and 389 (TCP) between Active Directory and Sentry (or port 636 (TCP) if you are using SSL-enabled Active Directory) need to be opened to allow communication. Port 88 is used for Kerberos protocol communication. Port 389 (or 636) is used for the LDAP ping between Sentry and the KDC to verify that the KDC IP is the same as the Active Directory IP.
  - If Windows Server 2003 is being used, the KDC may listen for requests on port 88 using UDP instead of TCP. You can force Kerberos to use TCP instead of UDP by changing the

Copyright © Acronis International GmbH, 2002-2014

MaxPacketSize from 0 to 1 in the registry editor. For information about how to do this, refer to the following Microsoft KB article: http://support.microsoft.com/kb/244474 http://support.microsoft.com/kb/244474.

- The iOS device must be able to reach the VSP and the Sentry.
- iOS Device registered on VSP.
- Mobile@Work installed on the device and registered in the VSP. The MDM profiles properly installed during the registration.

In this section

Configuring an AppConnect tunnel between the Access Mobile client and the Access server via username/password a
Adding Kerberos Constrained Delegation Authentication.....151

Copyright © Acronis International GmbH, 2002-2014

6 Configuring an AppConnect tunnel between the Access Mobile client and the Access server via username/password authentication

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

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

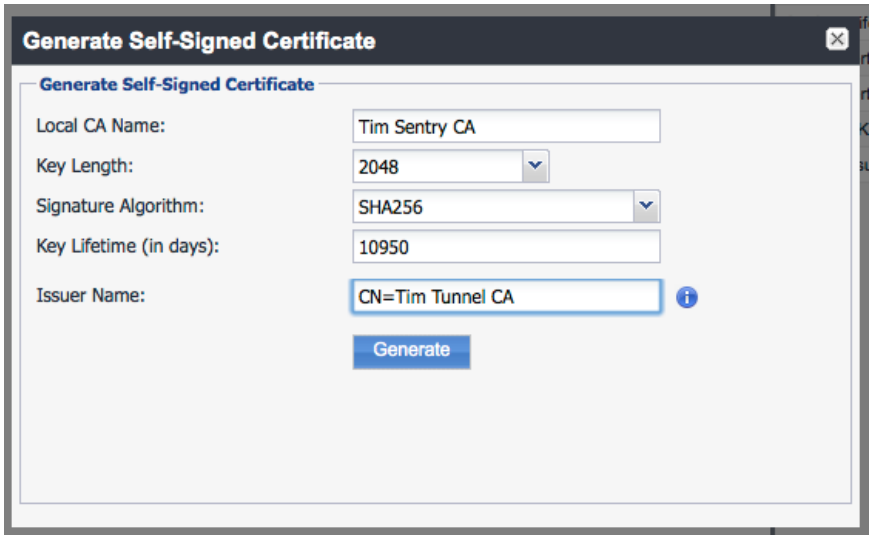
You may have an alternate Certificate Authority (CA) and Simple Certificate Enrollment Protocol (SCEP) provider but this guide assumes you do not for completeness sake. Please consult MobileIron documentation for configuring a third party CA and SCEP provider.

In this section

Configuring Acronis Access on the VSP.....143
Verify AppTunnel usage 149

3.

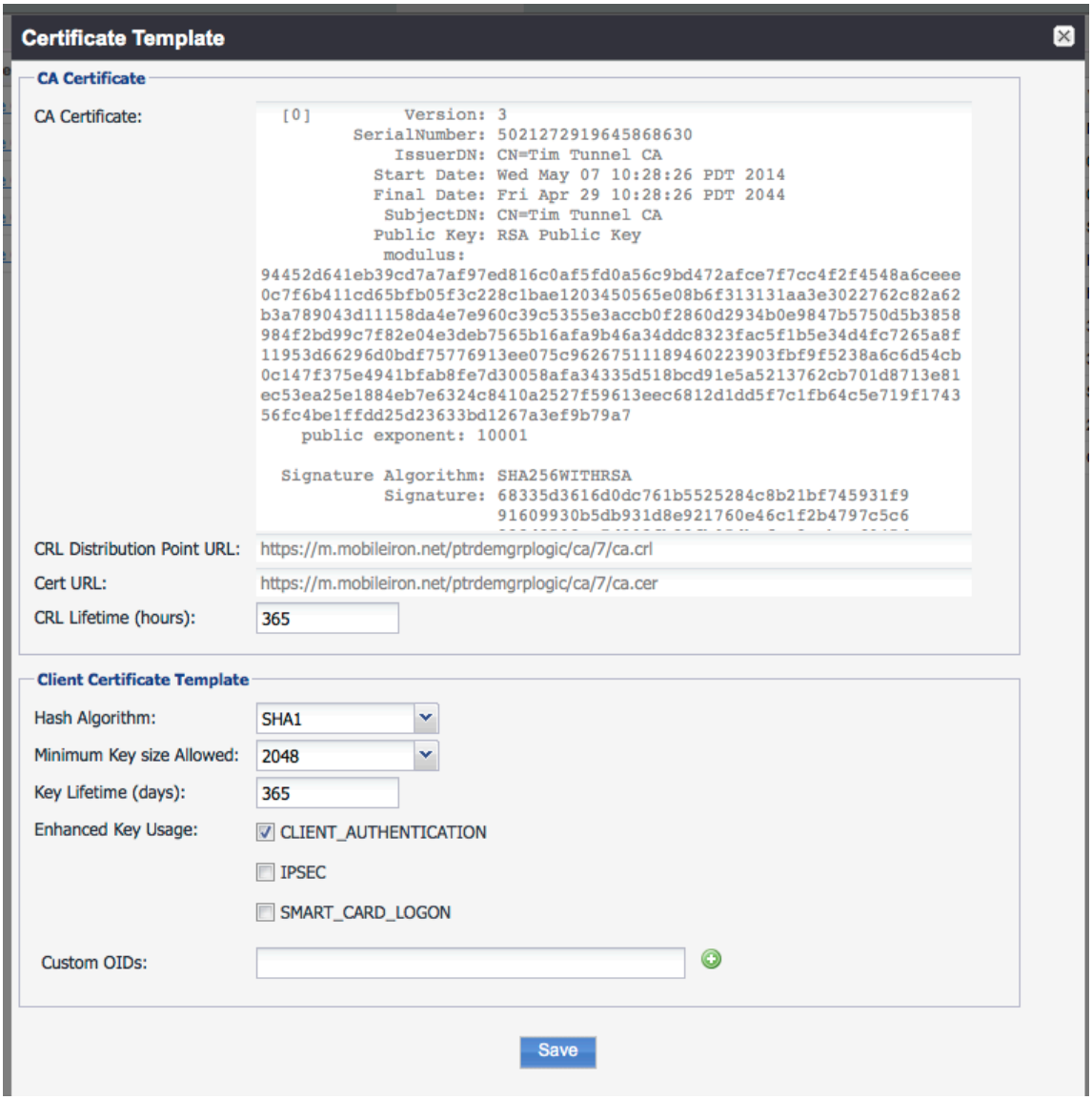
1. Open the MobileIron VSP Admin Portal.
2. Select **Settings** and open **Local CA**.
3. Press **Add New** and select **Generate Self-Signed Cert**.



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

Copyright © Acronis International GmbH, 2002-2014

4. Click **Generate**.

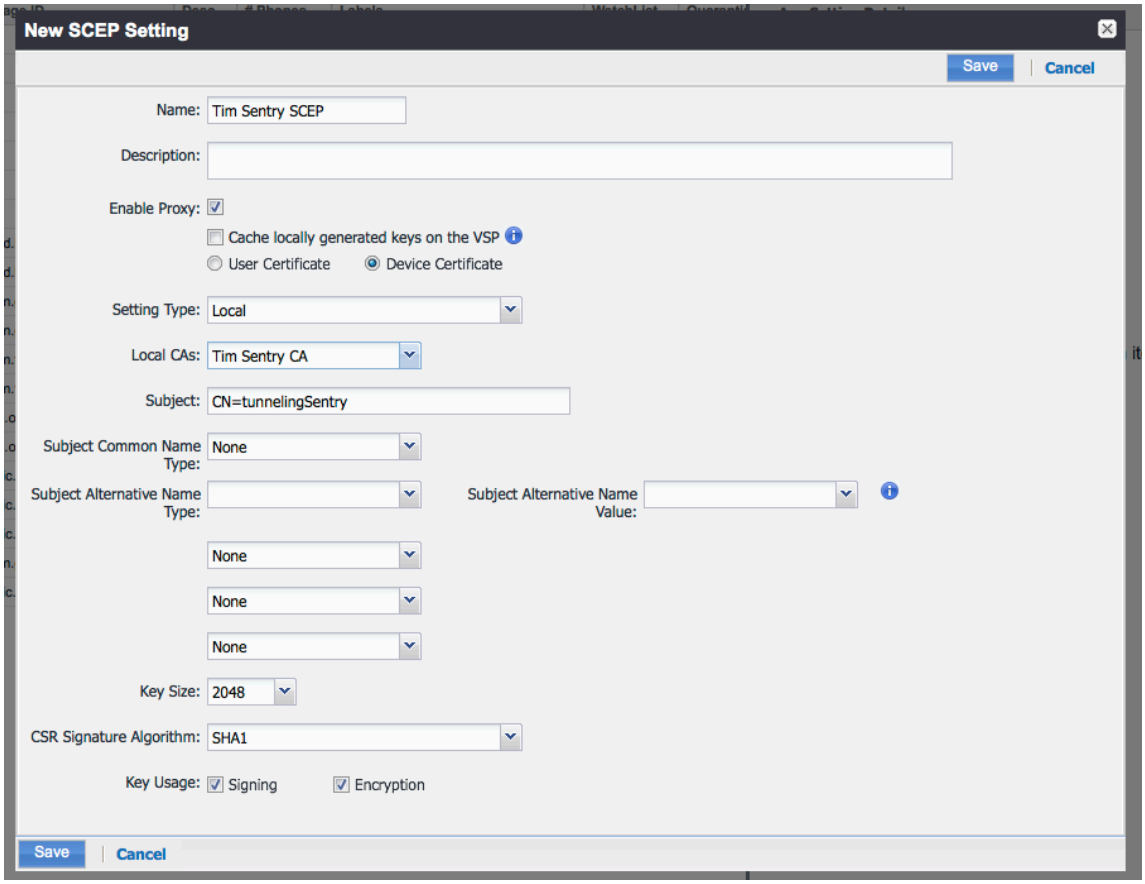


5. Then click **Save**.
6. Click **View Certificate** on the new CA.
7. Copy the certificate to a new text file and save to the desktop.

1. Open the MobileIron VSP Admin Portal.
2. Select **Policies & Configs** and open **Configuration**.

Copyright © Acronis International GmbH, 2002-2014

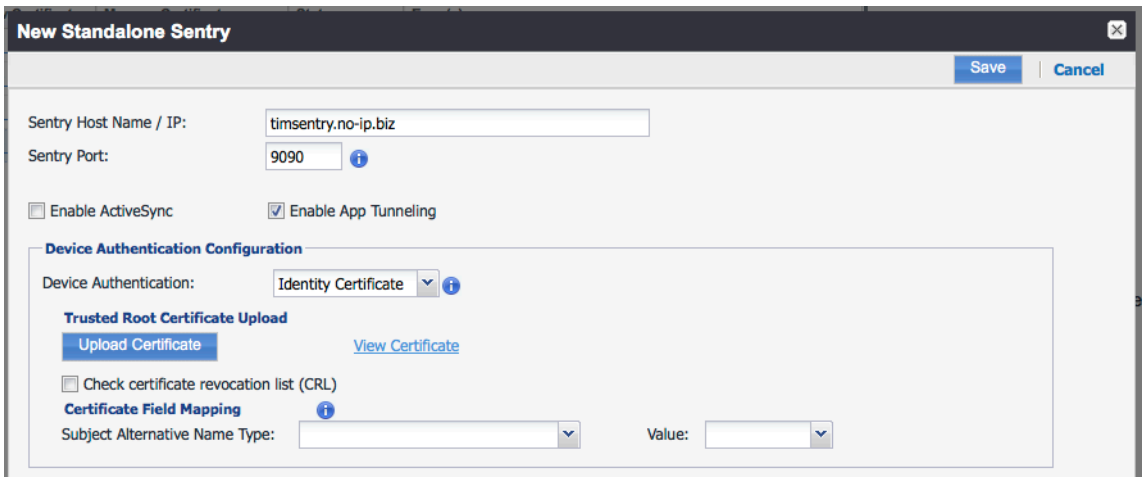
3. Press **Add New** and select **SCEP**.



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

4. Click **Save**.

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

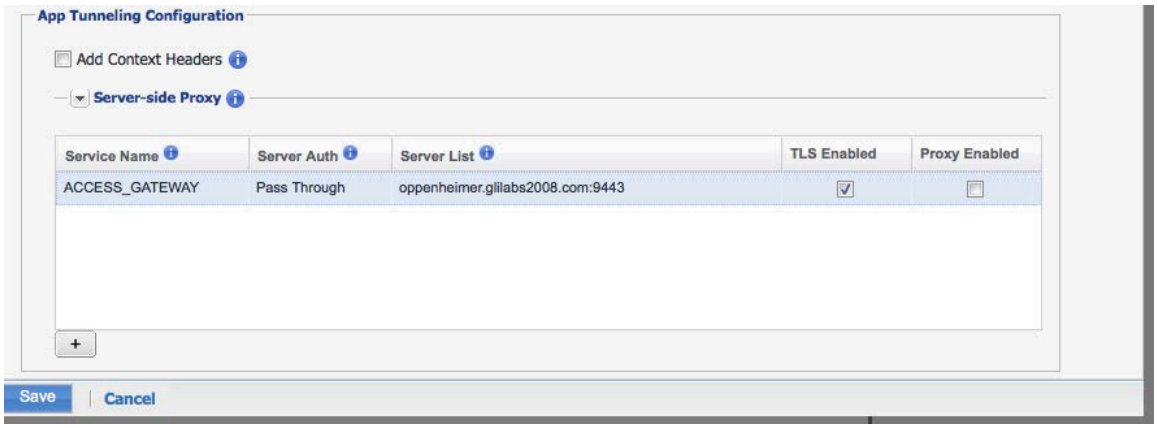


Copyright © Acronis International GmbH, 2002-2014

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

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

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



- **Service Name**: Enter a name based on your preference.
- **Server Auth**: Select **Pass Through**. This will be changed in a later part of this guide.
- **Server List**: Semi-colon separated list of servers. For this document we will use a single server. That will be the DNS address of the Access Gateway server and the port it is listening on.
- **TLS Enabled**: Mark the checkbox.

Click **Save**.

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

Configuring Acronis Access on the VSP

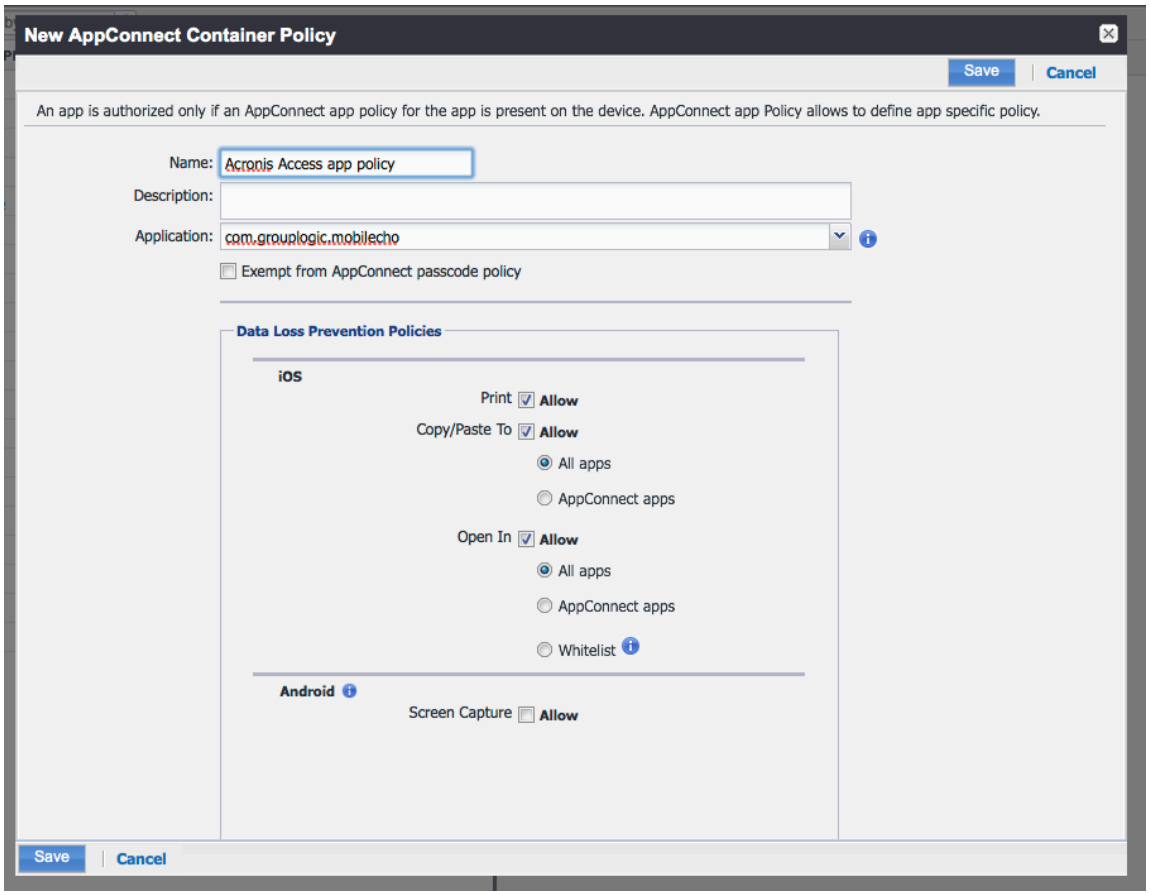
Once the Sentry is setup, the App Policy and App Configuration needs to be created for Acronis Access. This is a multi-step process that will include the following steps.

In this section

Copyright © Acronis International GmbH, 2002-2014

6.

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



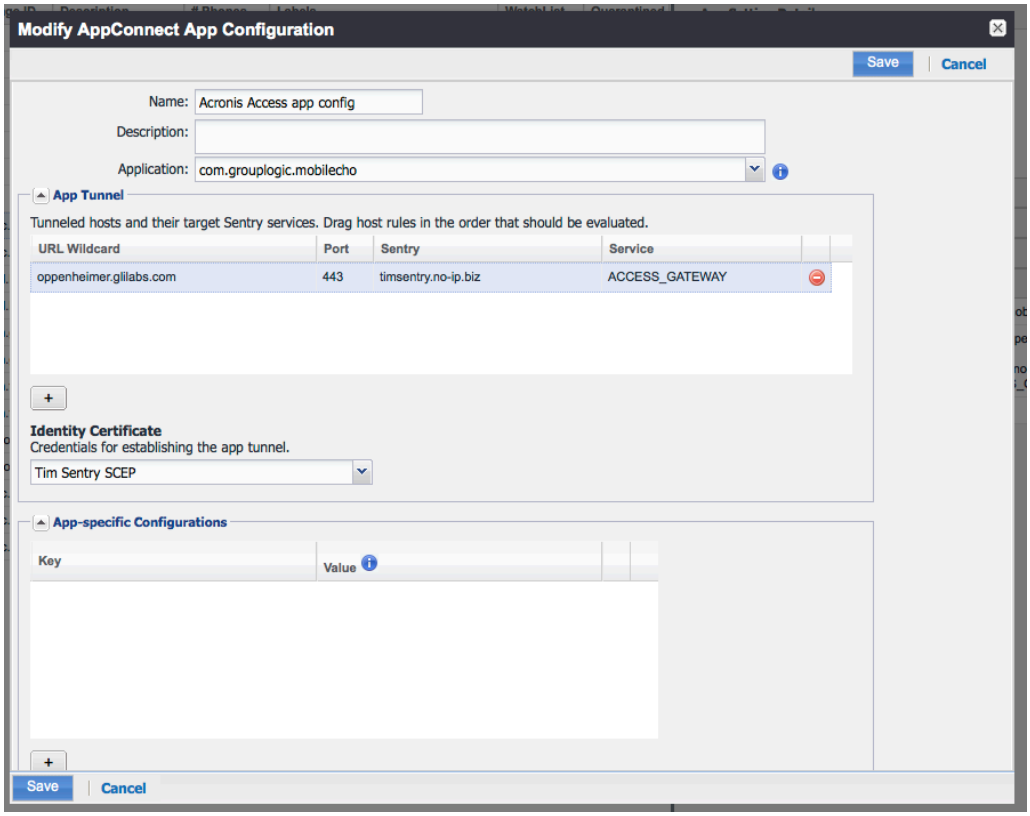
- **Name**: Enter a name based on your preference.
- **Application**: Enter **com.grouplogic.mobilecho**. This is a Bundle ID from the iOS App Store.
- **Policies**: Set whatever MobileIron policies you want to use for managing Acronis Access.

3. Click **Save**.

1. Still within the MobileIron VSP Admin Portal, select **Policies & Configs** and open **Configurations**.

Copyright © Acronis International GmbH, 2002-2014

2. Press **Add New**, select **AppConnect** and select **Configuration**.

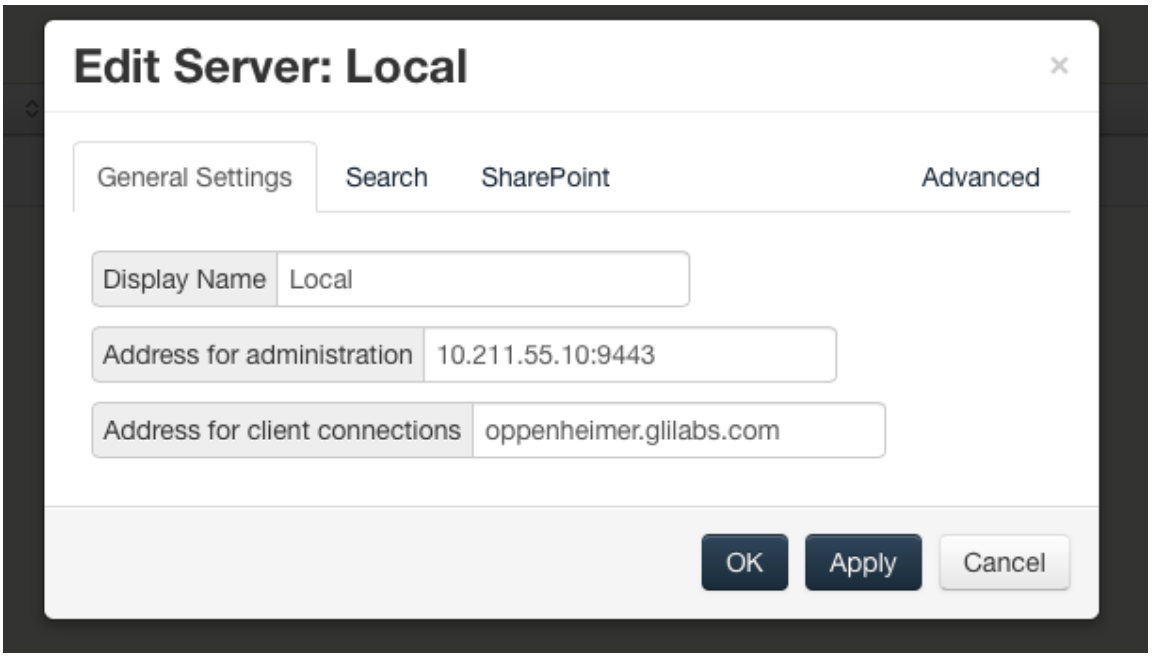


- **Name**: Enter a name based on your preference.
- **Application**: Enter com.grouplogic.mobilecho. This is the Bundle ID as seen in the Apple store.
- **App Tunnel**
  - **URL Wildcard**: The URL that the client will try to contact the Acronis Access gateway server on. This must match the "Address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

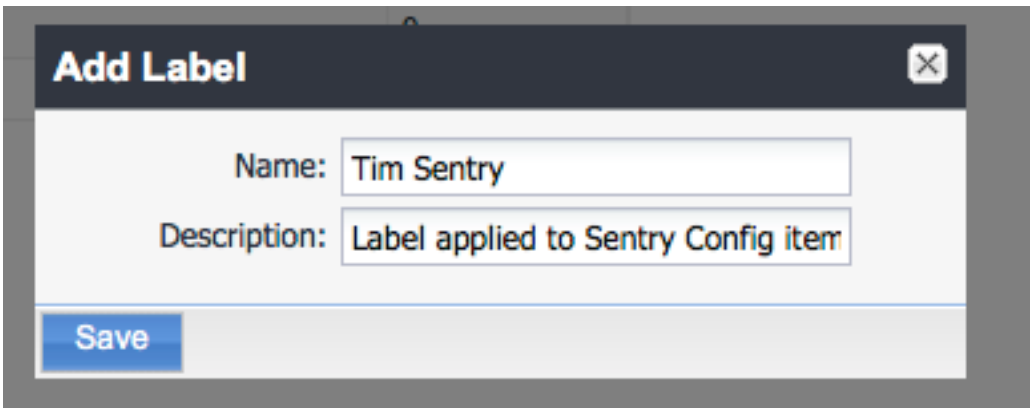
3. Click **Save**.

Copyright © Acronis International GmbH, 2002-2014

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



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

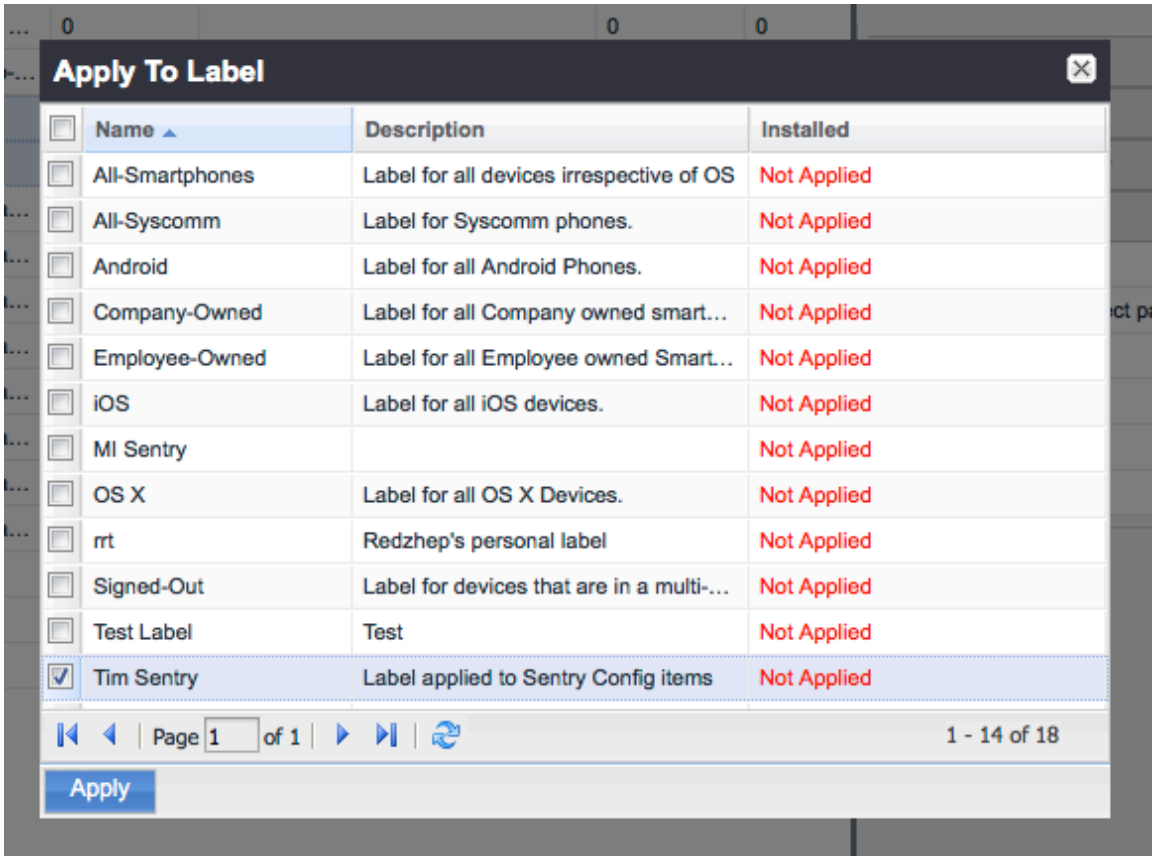


   - **Name**: Enter a name based on your preference.
   - **Description**: Enter a description based on your preference.
3. Click **Save**.

1. Still within the MobileIron VSP Admin Portal, select **Policies & Configs**.

Copyright © Acronis International GmbH, 2002-2014

2. Mark the SCEP, AppConnect policies, and AppConnection configurations you created while following this document. Open **Configurations** to view them listed.

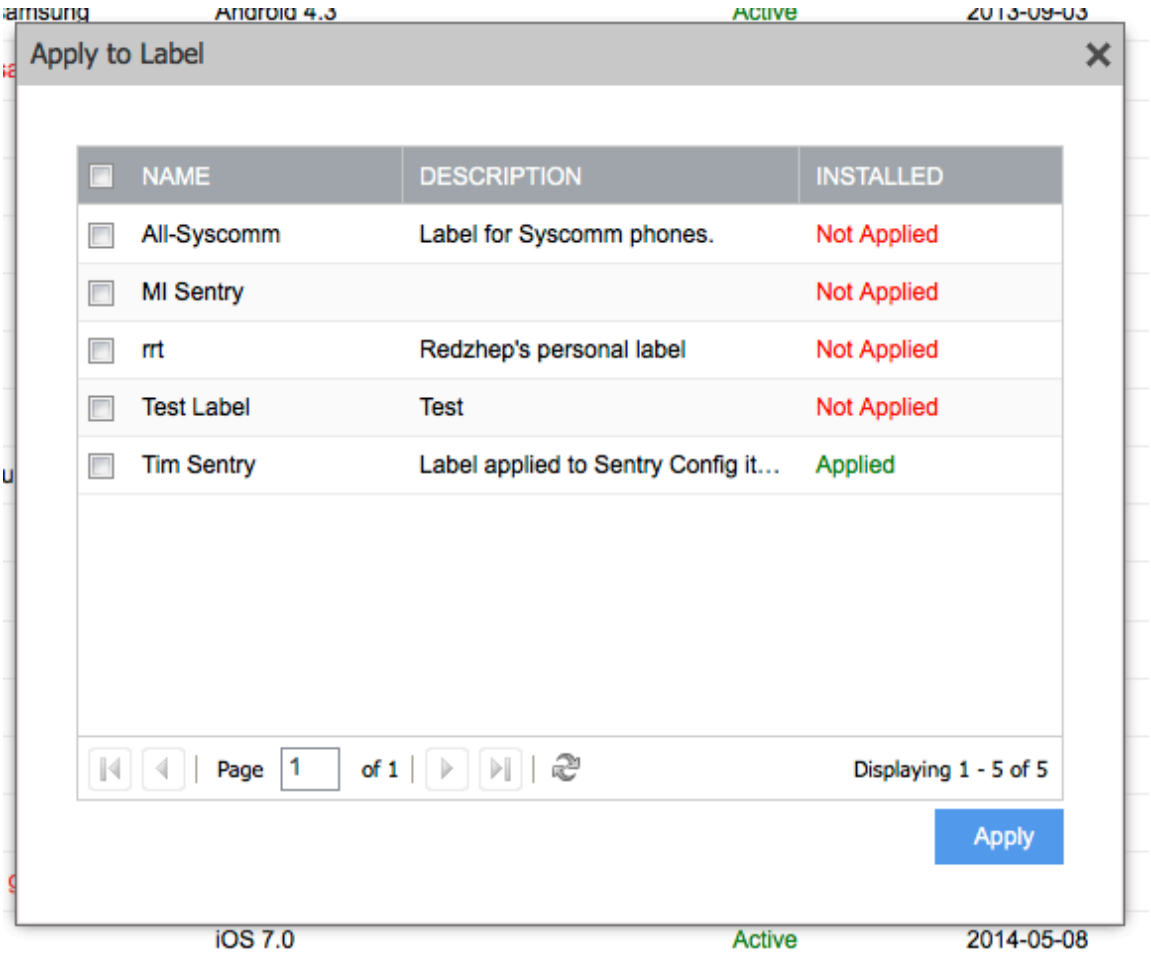


3. Press **More Actions** and select **Apply to Label**.
4. Mark the Label created in "Create a new label".
5. Click **Apply**.

1. Still within the MobileIron VSP Admin Portal, Select **Users & Devices** and open **Devices**.

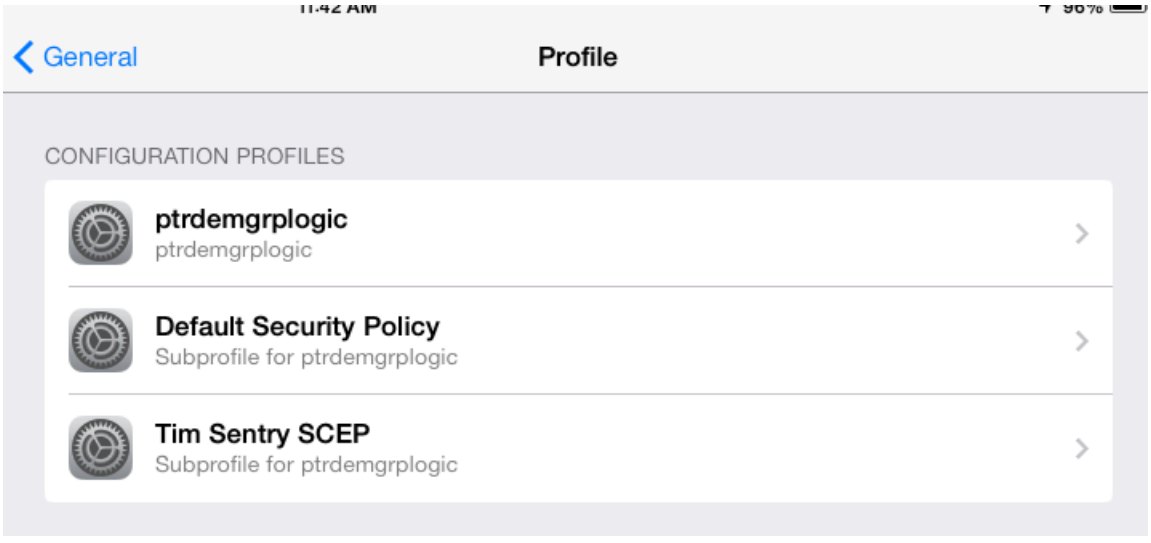
Copyright © Acronis International GmbH, 2002-2014

2. Mark the iOS device to be used for Sentry testing.



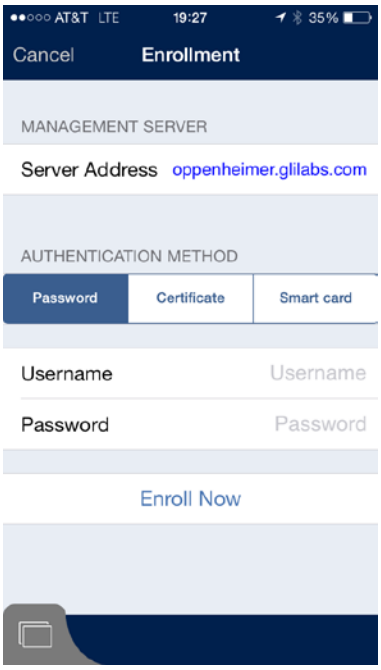
3. Select **Actions** -> **Apply to Label**.
4. Check Label created in "Create a new label".
5. Click **Apply**.

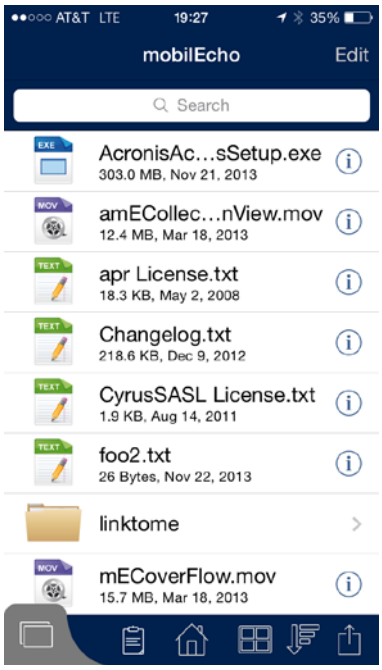
1. Open the Mobile@Work app and open the **Settings**.
2. Tap on Check for Updates.
3. Tap on **Force Device Check-In**. If this is successful the SCEP configured in this document should show up in the device settings at **Settings** -> **General** -> **Profiles**.



Copyright © Acronis International GmbH, 2002-2014

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





6. Enter the address used for client connections to the Acronis Access Gateway and configured in the **AppConnection Configuration**. For a true test this URL should not be reachable by the mobile client (use celluar or an external network).
7. Tap **continue**.
8. Enter **Username** and **Password** and tap **Enroll Now**.

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

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

Verify AppTunnel usage

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

1. Select Troubleshooting and open **Logs**.
2. Check **Sentry**, **To/From Device**, **To/From Service**, and **Level 4**.
3. Select **Apply**.
4. Under "**View Module Logs**" select **Sentry**.

Copyright © Acronis International GmbH, 2002-2014

5. When traffic comes from the mobile device you should see the sentry log scroll with entries related to the hostname configured.

Copyright © Acronis International GmbH, 2002-2014

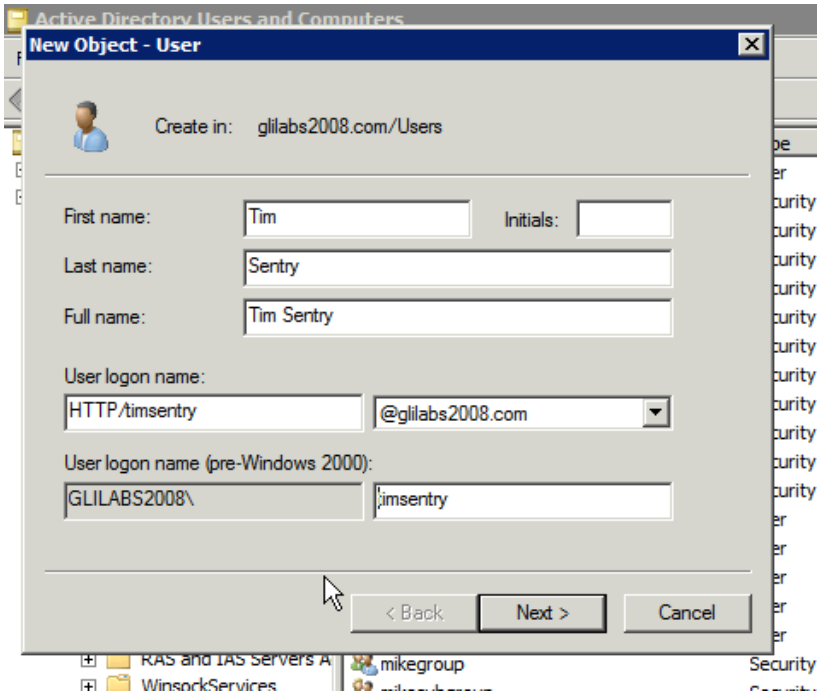
7 Adding Kerberos Constrained Delegation Authentication

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

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

If you are going to use the same iOS device to test the Kerberos Constrained Delegation it is recommended you uninstall the Acronis Access Mobile client at this time.

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

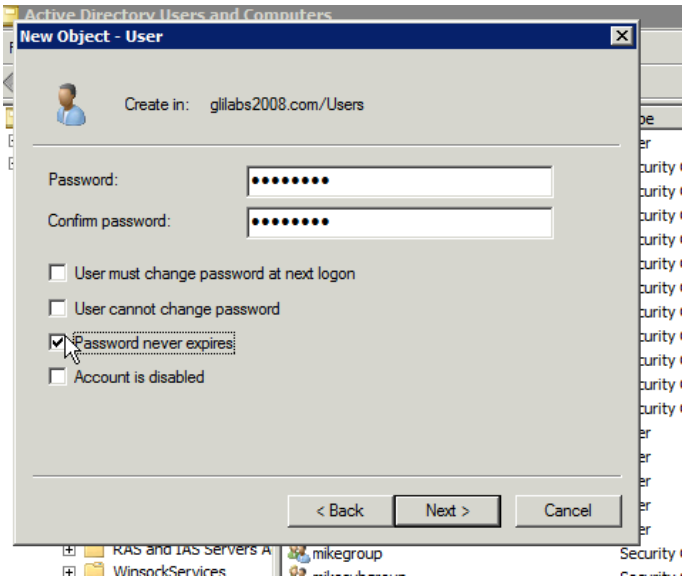


- Enter a **Name** and a **User Logon Name** for the Kerberos service account. The name must start with **HTTP/**. Use standard alphanumeric characters with no whitespace for the **User Logon Name**, as it is entered in a command prompt later in the guide. If **HTTP/** automatically appears next to the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

Copyright © Acronis International GmbH, 2002-2014

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

5. Click **Next**.



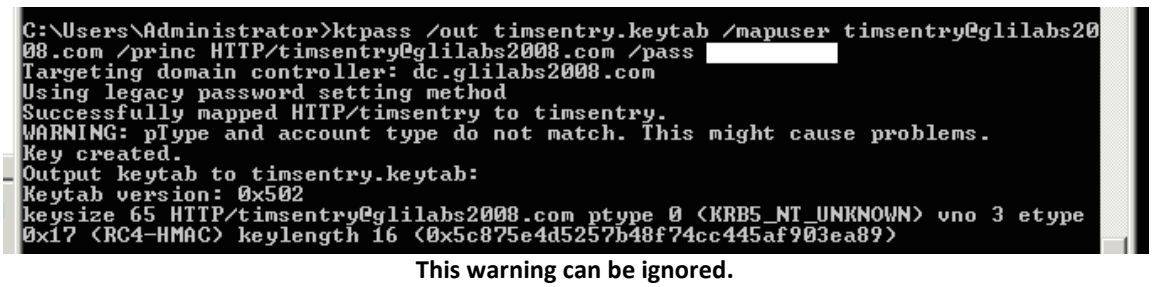
- **Password**: Enter a password.
- **Password never expires**: Ensure that User must change password at next logon is not selected. Typically, in the enterprise, the **User cannot change password** and **Password Never Expires** fields should be selected.

6. Click **Next**.
7. Click **Finish**.

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

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

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

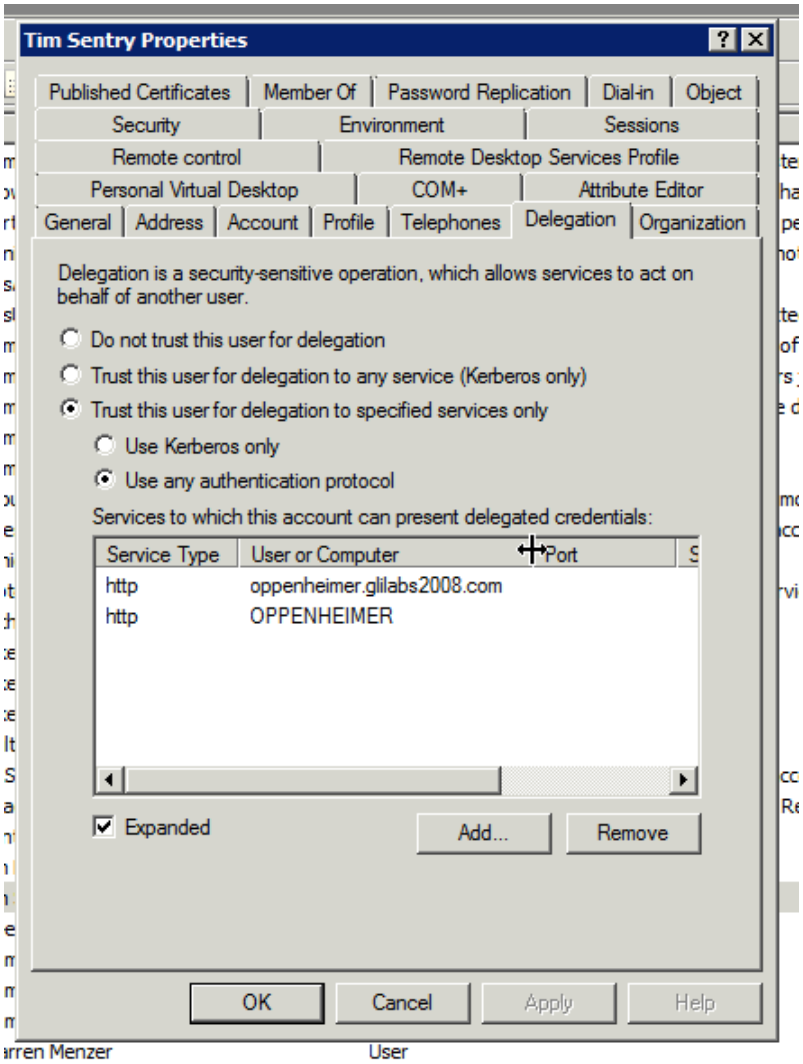


This warning can be ignored.

1. From the Windows Start menu, select **All Programs** and open **Administrative Tools** > **Active Directory Users and Computers**.
2. In the newly opened console, expand the realm (domain).
3. Click on **Users**.

Copyright © Acronis International GmbH, 2002-2014

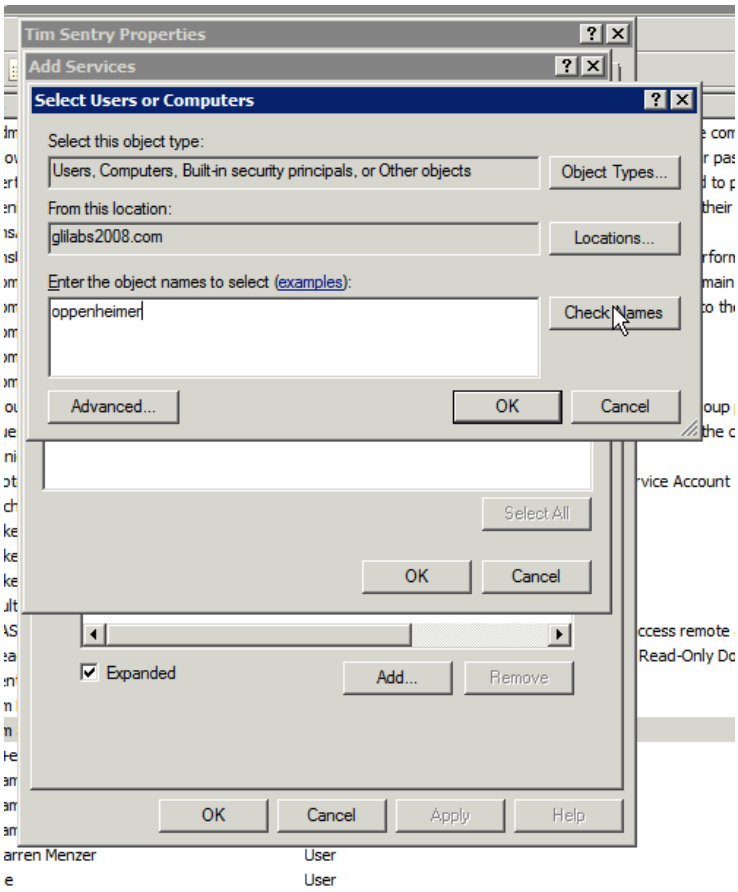
4. Find and select the Kerberos user account that you created in "Create a Kerberos Service Account".
5. Right-click on the account and select **Properties**.
   - Click on the **Delegation** tab.
   - Select **Trust This User For Delegation To Specified Services Only**.
   - Select **Use Any Authentication Protocol**.



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

Copyright © Acronis International GmbH, 2002-2014

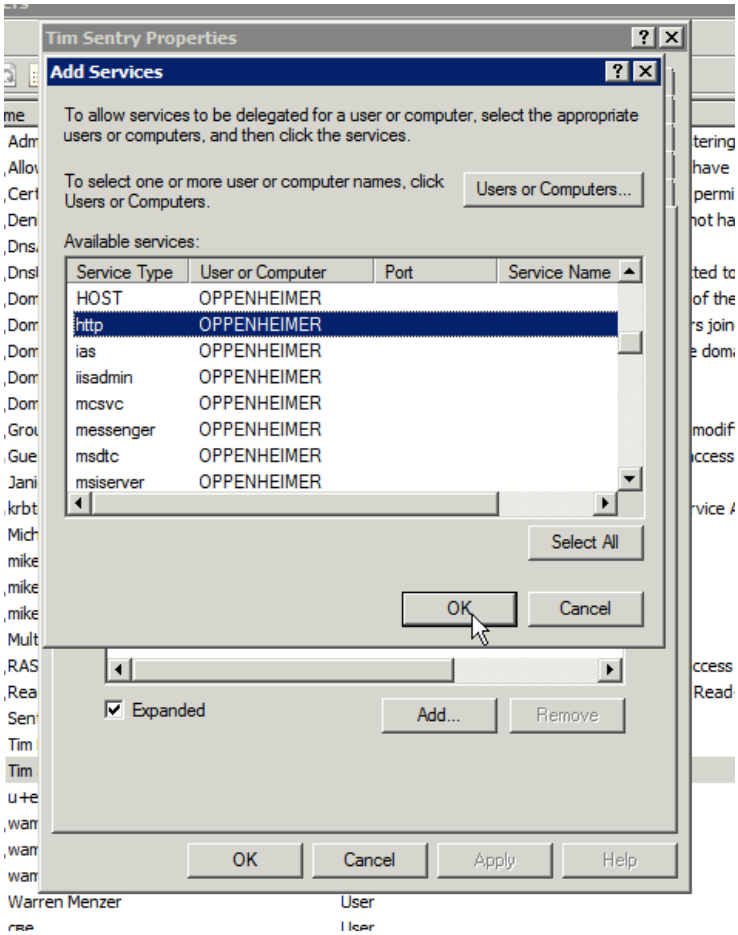
- The correct computer name should appear in the object name box.



8. Click **OK**.

Copyright © Acronis International GmbH, 2002-2014

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



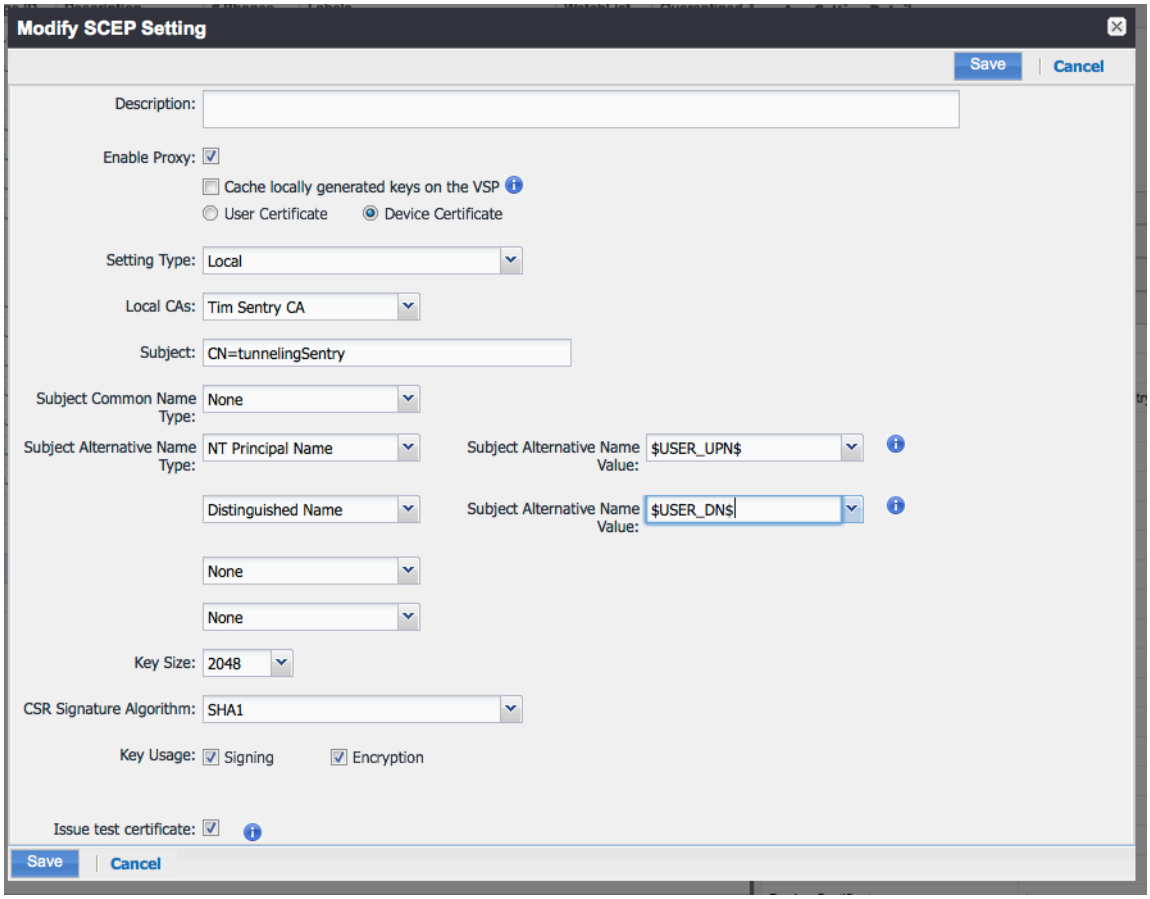
10. Click **OK**.

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

1. Open the MobileIron VSP Admin Portal.
2. Select **Policies & Configs** and open **Configurations**.
3. Find the SCEP created in "Create a new SCEP".

Copyright © Acronis International GmbH, 2002-2014

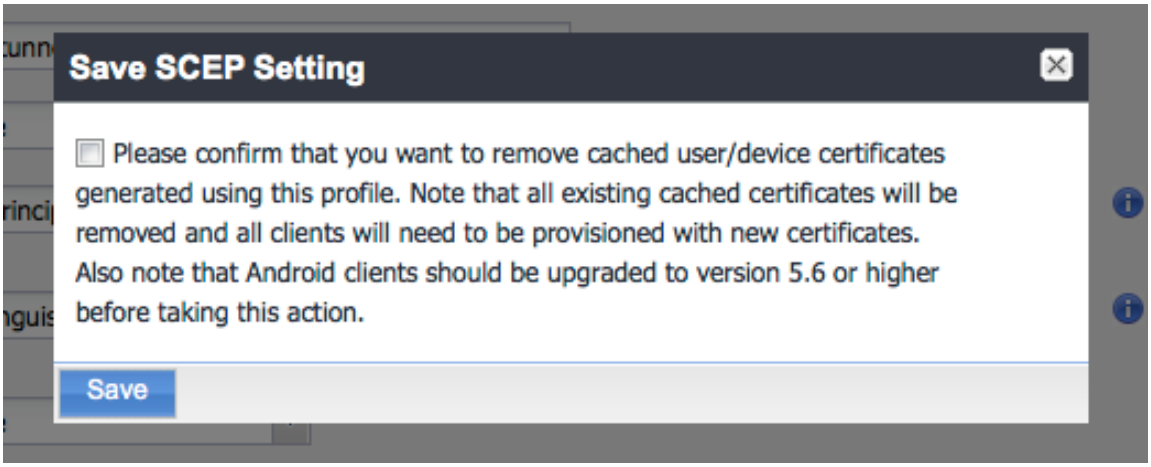
4. Click on its name and click **Edit** in the panel on the right.



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

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

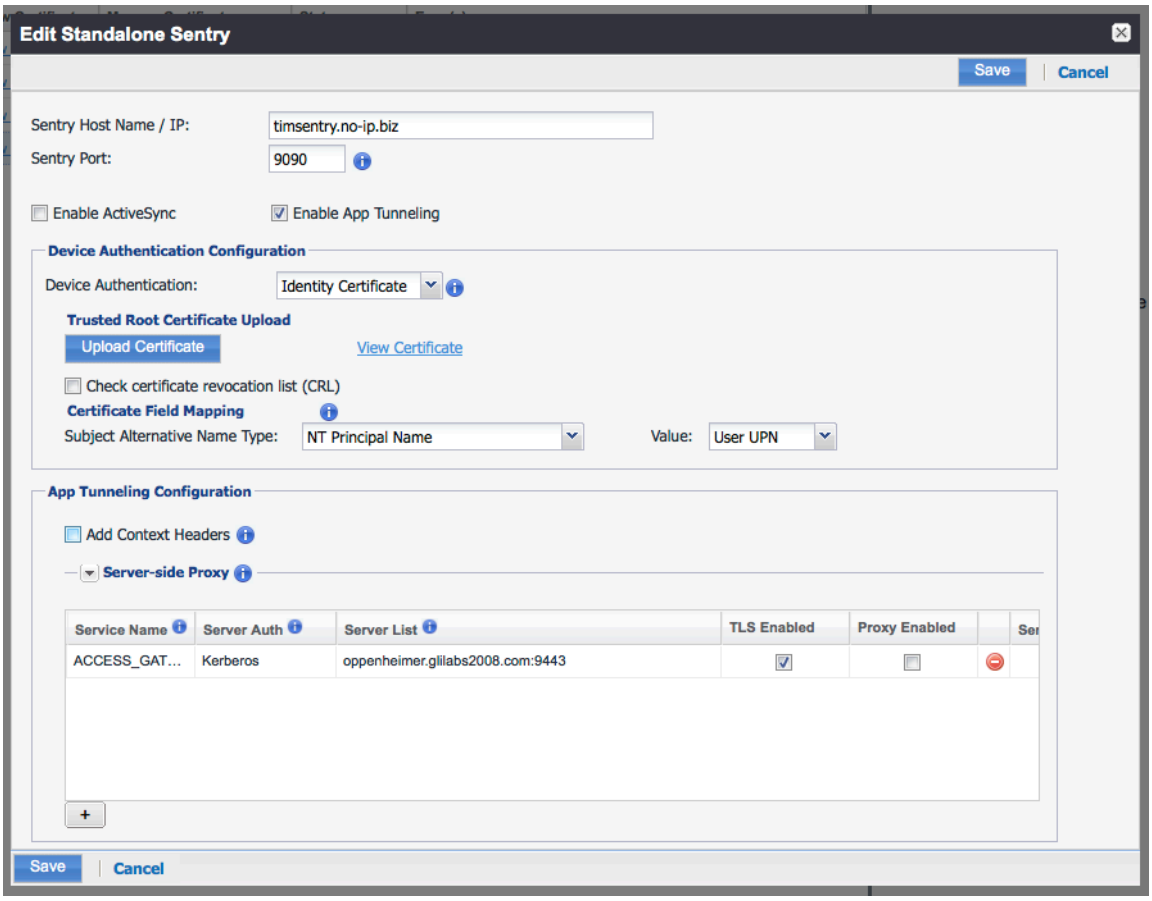
5. Click **Save**.



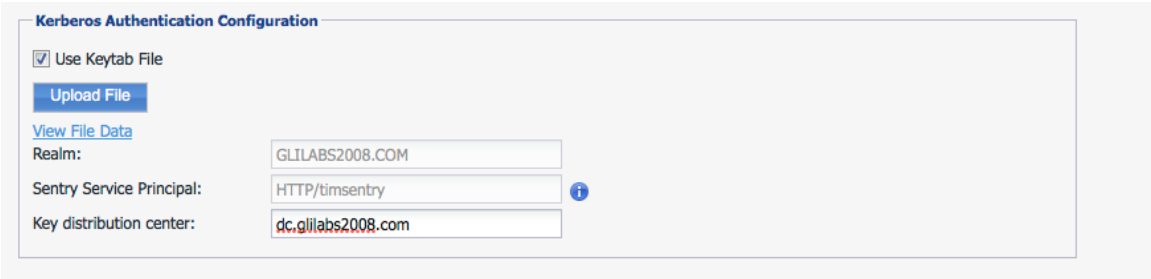
6. Since you have modified the SCEP, you will have to re-provision the device in Mobile@Work before testing the iOS client.

Copyright © Acronis International GmbH, 2002-2014

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



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



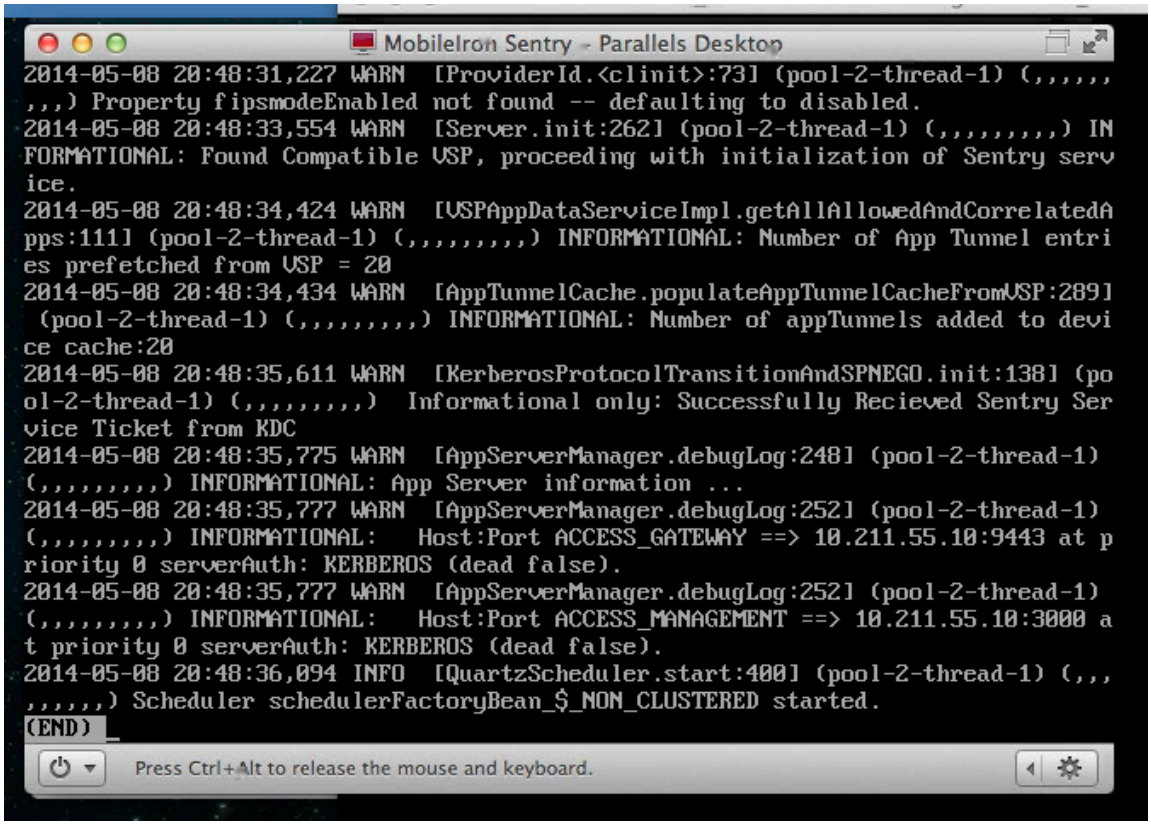
- In the **Kerberos Authenication Configuration** section.
  - Check **Use Keytab File**.
  - Click **Upload File**.
  - Upload the keytab file created in "Create a keytab for the Kerberos Service Account".
  - Put the domain controller in the Key distribution center.

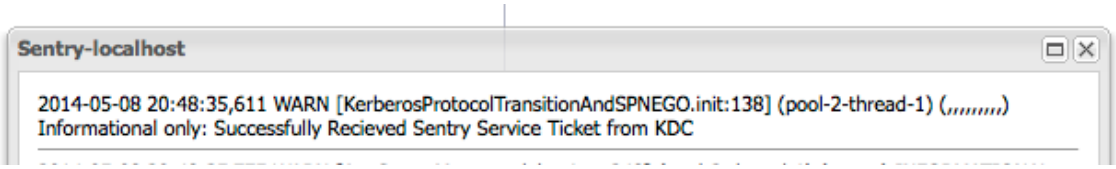
4. Click **Save**.

Copyright © Acronis International GmbH, 2002-2014

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

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



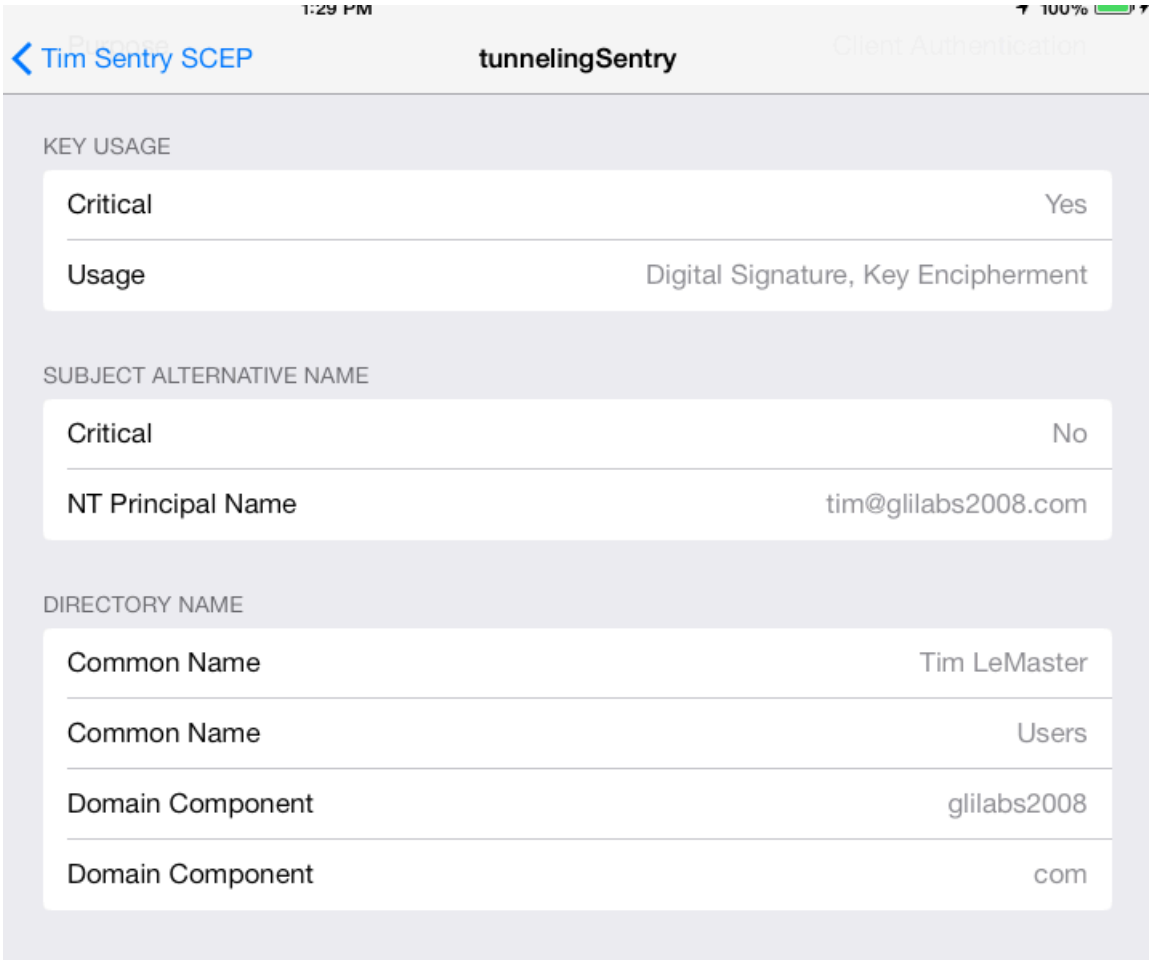


The changes we made to the SCEP must be pushed down to the iOS device. The changes we made to the Sentry can take several minutes to be pushed down to it.

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

Copyright © Acronis International GmbH, 2002-2014

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



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

7.1.1 Advanced Delegation Configurations

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

For network shares and SharePoint servers, do the following:

Following these steps, you will enable delegation from the Gateway server to the target server(s).

1. Open **Active Directory Users and Computers**.

Copyright © Acronis International GmbH, 2002-2014

2. Find the computer object corresponding to the Gateway server.
3. Right-click on the user and select Properties.
4. Open the **Delegation** tab.
5. Select **Trust this computer for delegation to specified services only**.
6. Under that select **Use any authentication protocol**.
7. Click **Add**.
8. Click **Users or Computers**.
9. Search for the sever object for the SMB share or SharePoint server and click **OK**.
   - For SMB shares, select the **cifs** service.
   - For SharePoint, select the **http** service.
10. Repeat these steps for each server that the Acronis Access Gateway server will need to access.
11. Repeat this process for each Gateway server.

These delegation changes, can take a few minutes to propagate depending on the size of the domain forest. You may need to wait up to 15 minutes (possibly more) for the changes to take effect. If it's still not working after 15 minutes, try restarting the Acronis Access Gateway service.

7.2 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 Cluster160
Installing Acronis Access on a Windows 2008 Microsoft Failover Cluster174
Installing Acronis Access on a Windows 2012 Microsoft Failover Cluster185

7.2.1 Installing Acronis Access on a Windows 2003 Microsoft Failover Cluster

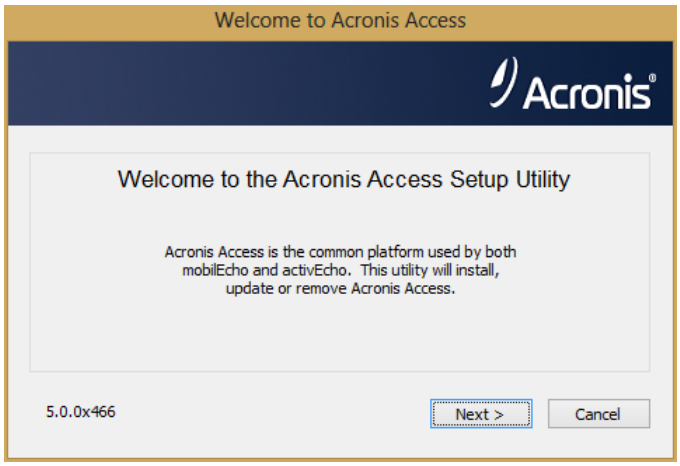
Installing Acronis Access

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

1. Download the Acronis Access installer.

Copyright © Acronis International GmbH, 2002-2014

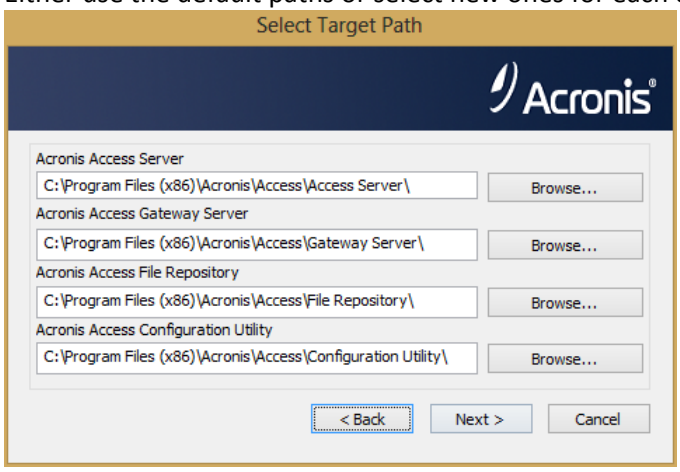
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



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

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

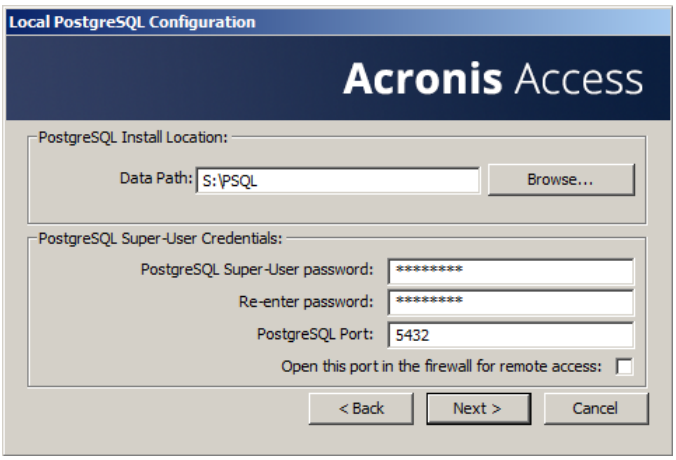
7. Either use the default paths or select new ones for each component and press OK.



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

Copyright © Acronis International GmbH, 2002-2014

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

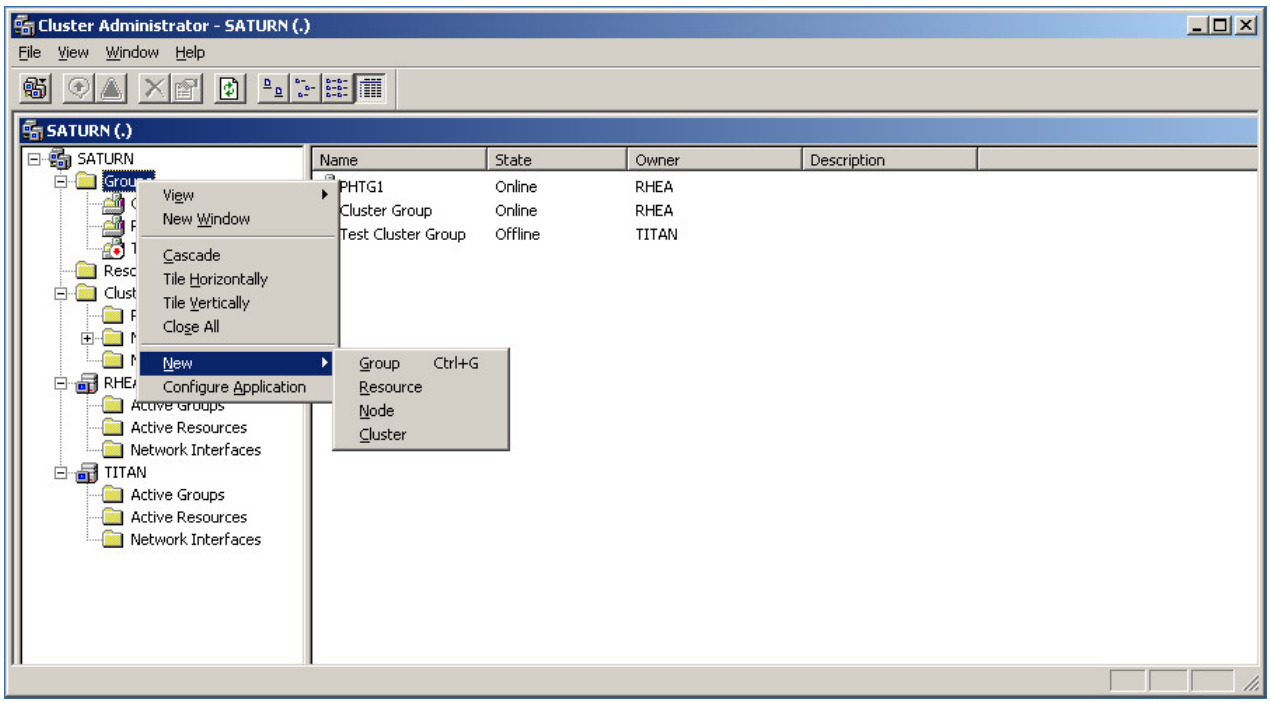


10. A window displaying all the components which will be installed appears. Press **OK** to continue.

When the Acronis Access installer finishes, press Exit**.**

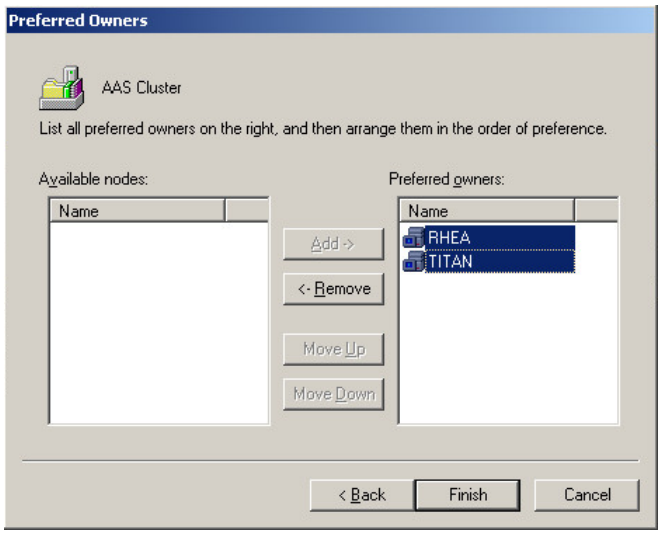
Creating the cluster group

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



Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_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.*

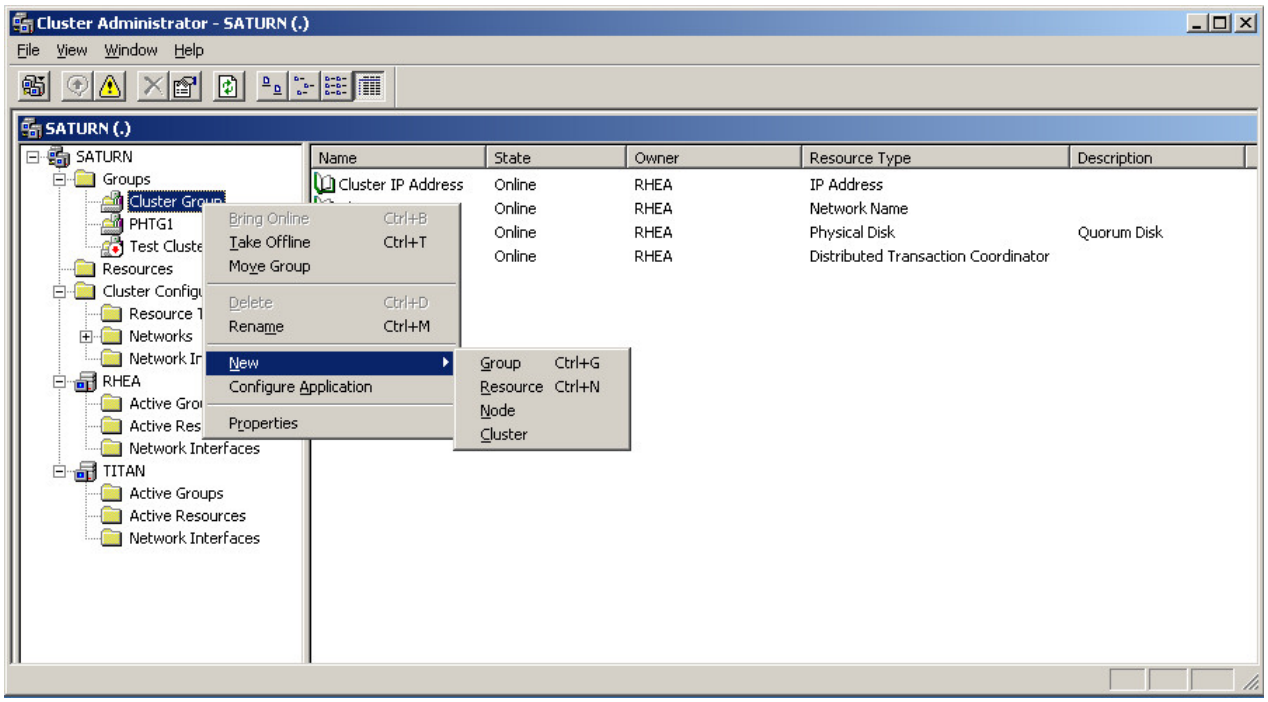
Adding all of the necessary services to the Acronis Access cluster group

Complete the following procedure for each of the following services: AcronisAccessGateway, postgresql-x64-9.2 (this may be different depending on the version of PostgreSQL), AcronisAccessRepository and AcronisAccessTomcat

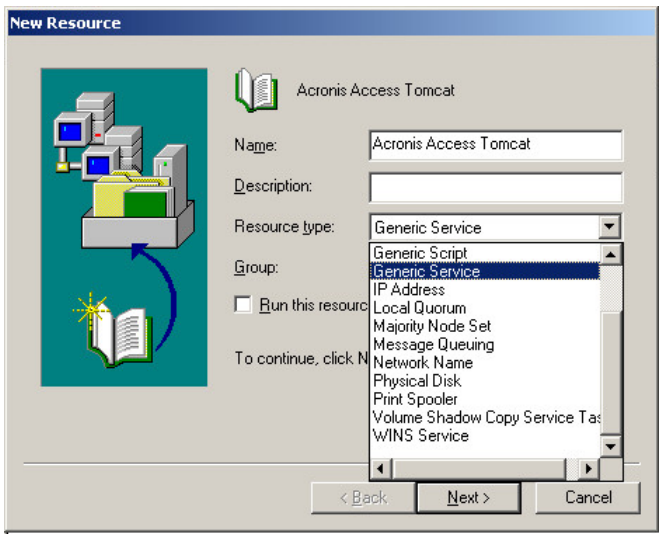
1. Right-click on the Acronis Access cluster group.

Copyright © Acronis International GmbH, 2002-2014

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

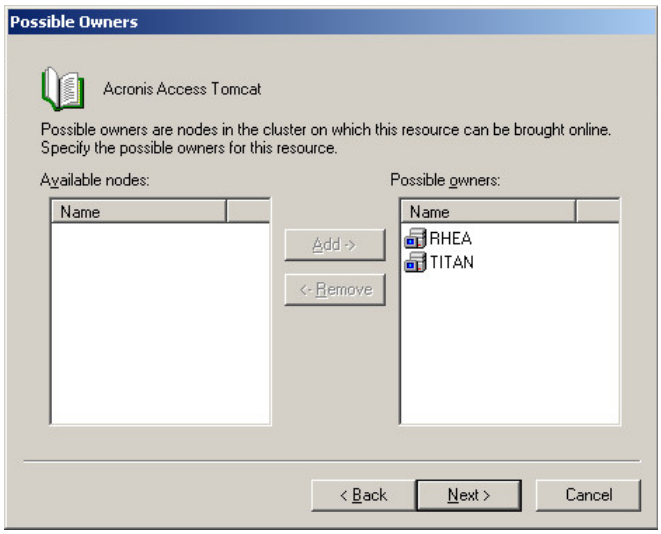


3. Enter a name for the service and select the correct cluster group.
4. From the **Resource Type** drop down menu select **Generic Service** and press **Next**.



Copyright © Acronis International GmbH, 2002-2014

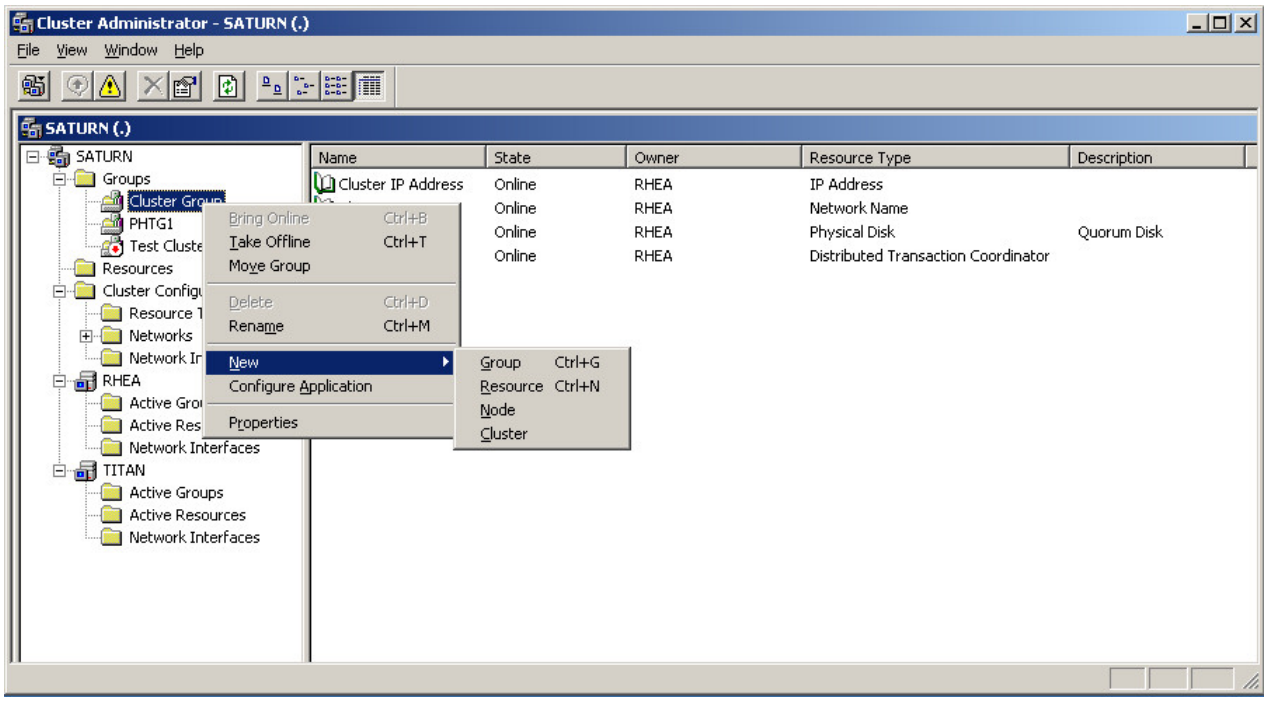
5. Make sure both of your nodes are listed as **Possible owners** and press **Next**.



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.

Setting an IP address for the cluster group

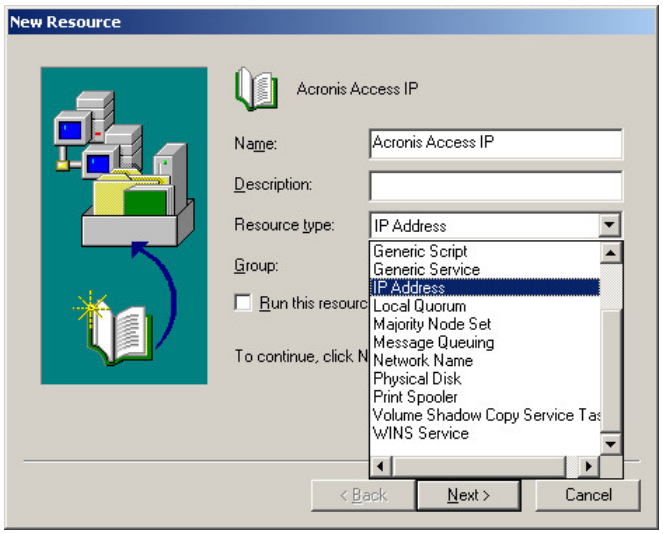
1. Right-click on the Acronis Access cluster group.
2. Open **New** and select **Resource**.



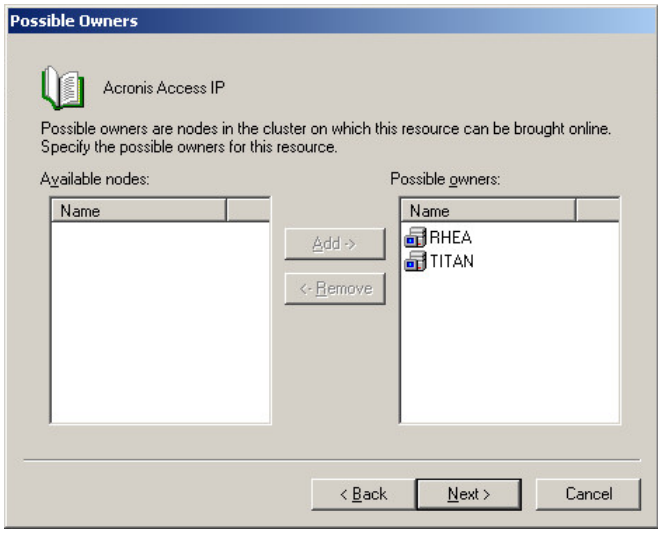
3. Enter a name for the resource and select the correct cluster group.

Copyright © Acronis International GmbH, 2002-2014

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**.



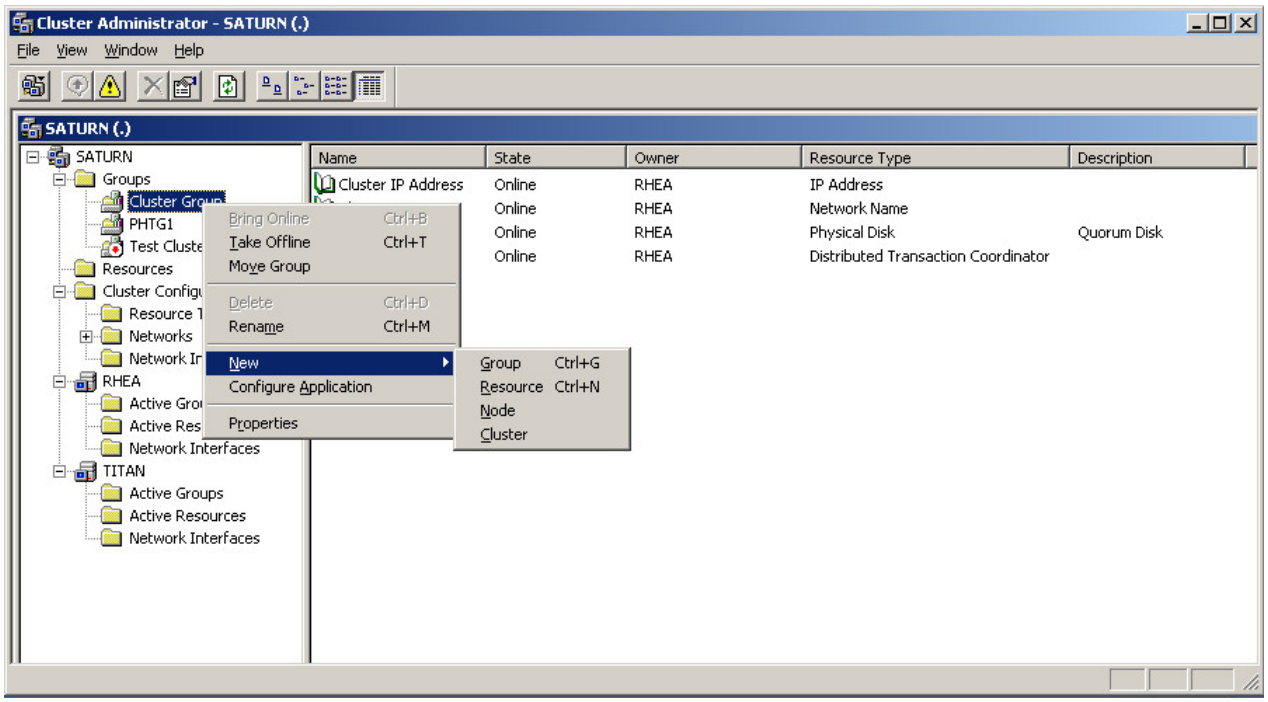
6. Skip the dependencies for now by pressing **Next**.
7. Enter the IP address you will use for this cluster group.
8. Enter the subnet mask and press **Finish**.

Adding a shared disk

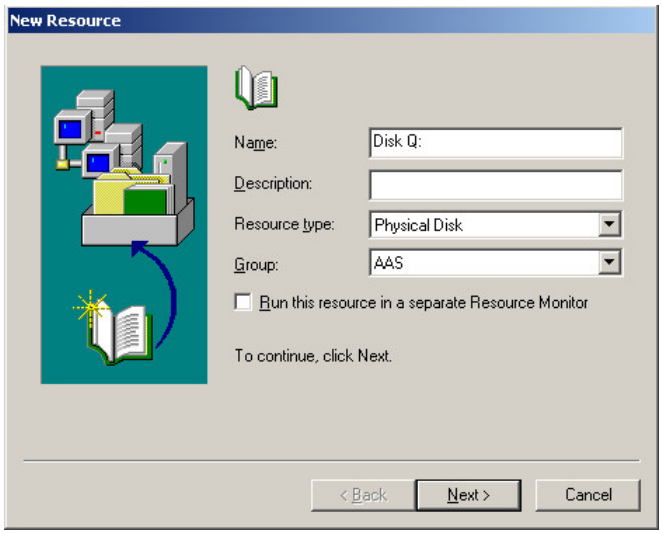
1. Right-click on the Acronis Access cluster group.

Copyright © Acronis International GmbH, 2002-2014

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

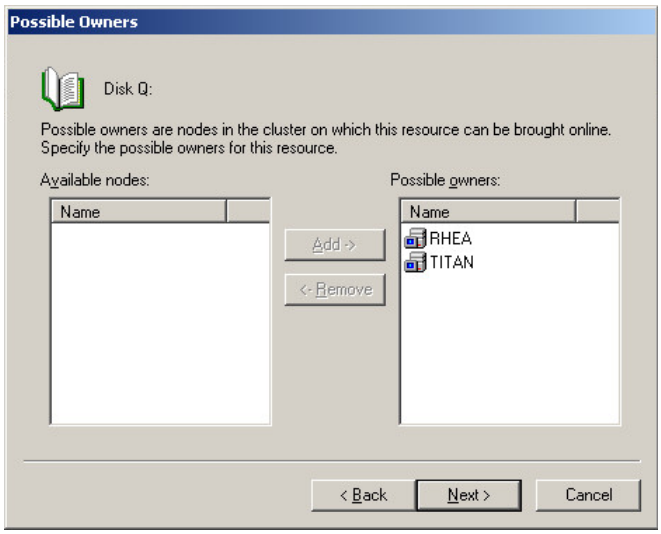


3. Enter a name for the resource and select the correct cluster group.
4. From the **Resource Type** drop down menu select **Physical Disk** and press **Next**.



Copyright © Acronis International GmbH, 2002-2014

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

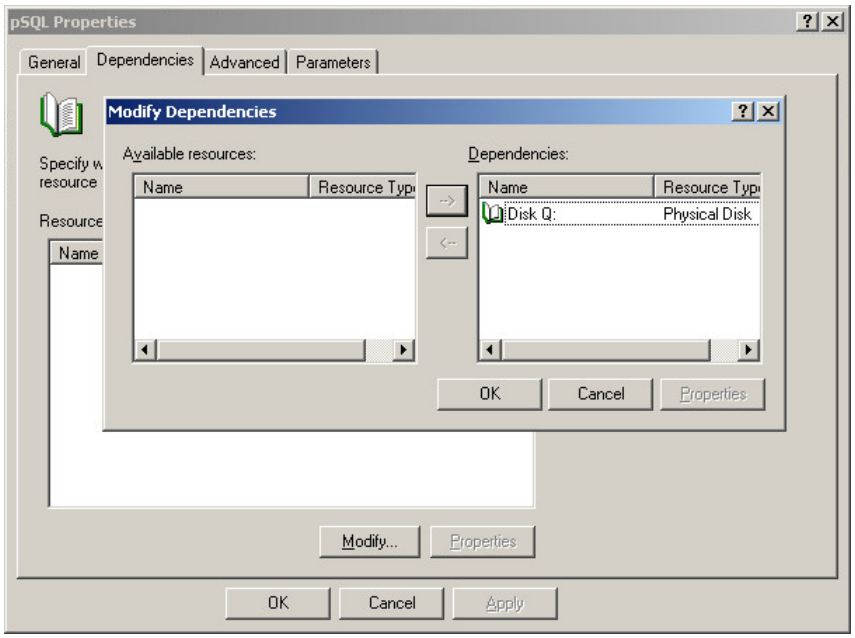


6. Skip the dependencies for now by pressing **Next**.
7. Select an available disk from the drop down menu and press **Finish**.

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.



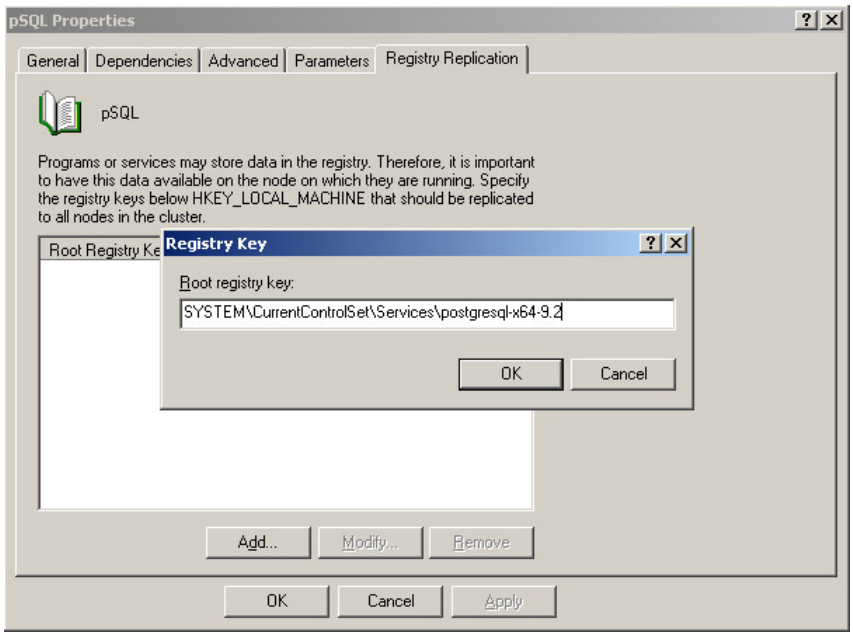
5. Press **OK**.

For PostgreSQL also do the following:

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

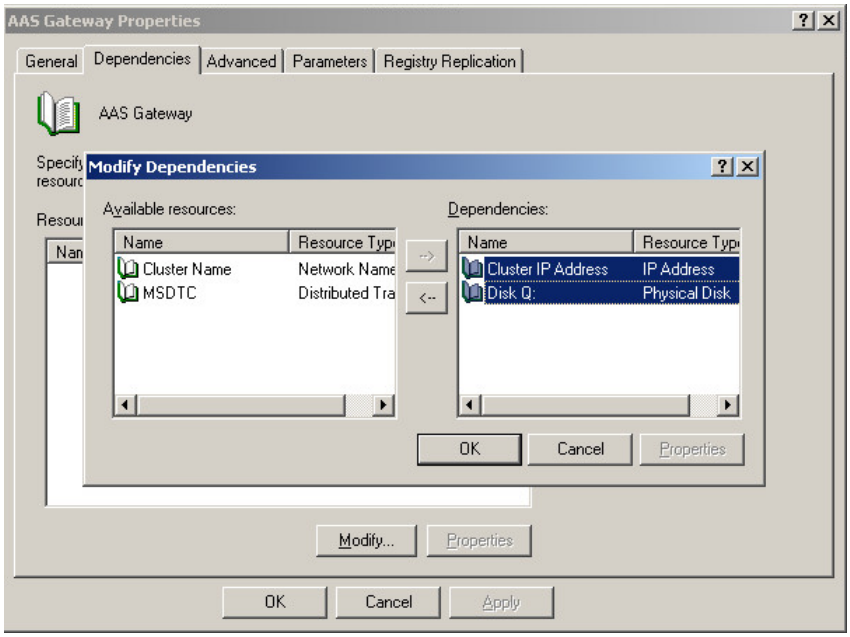
Copyright © Acronis International GmbH, 2002-2014

2. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\postgresql-some version (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.

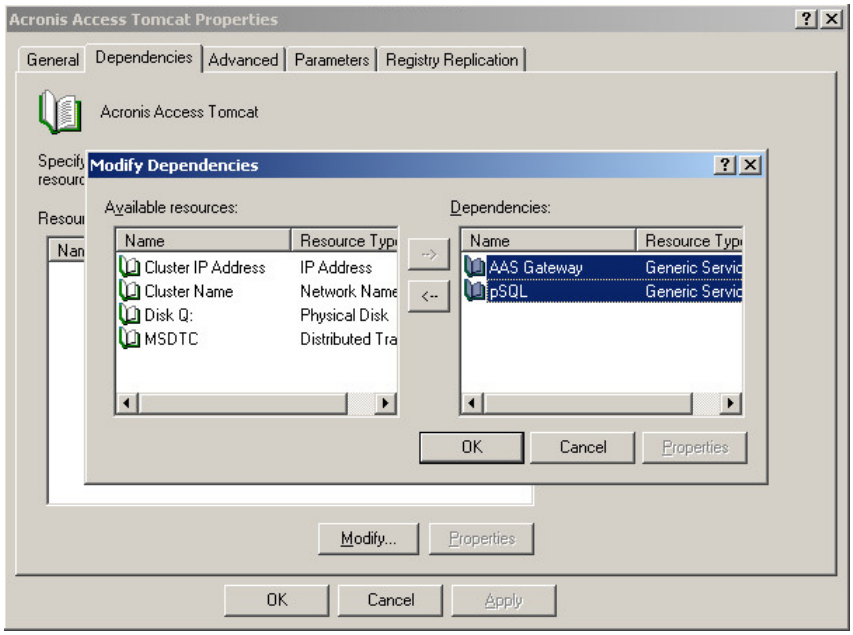


5. Press **OK**.

Copyright © Acronis International GmbH, 2002-2014

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.



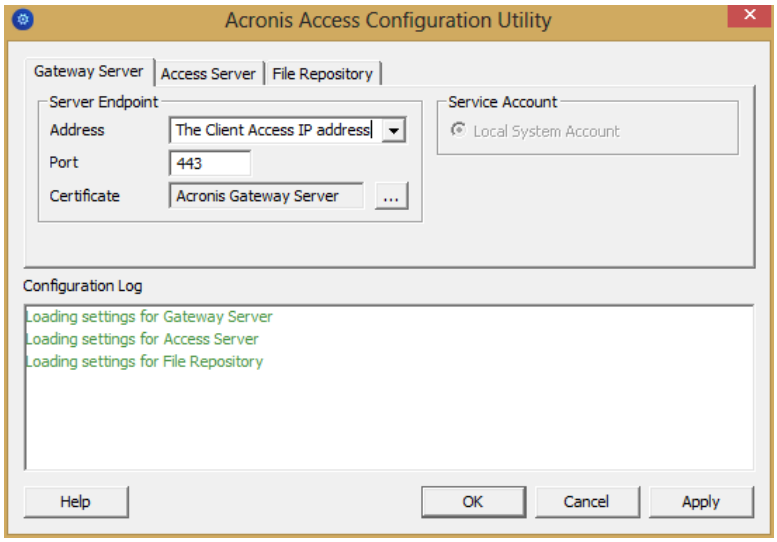
5. Press **OK**.

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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

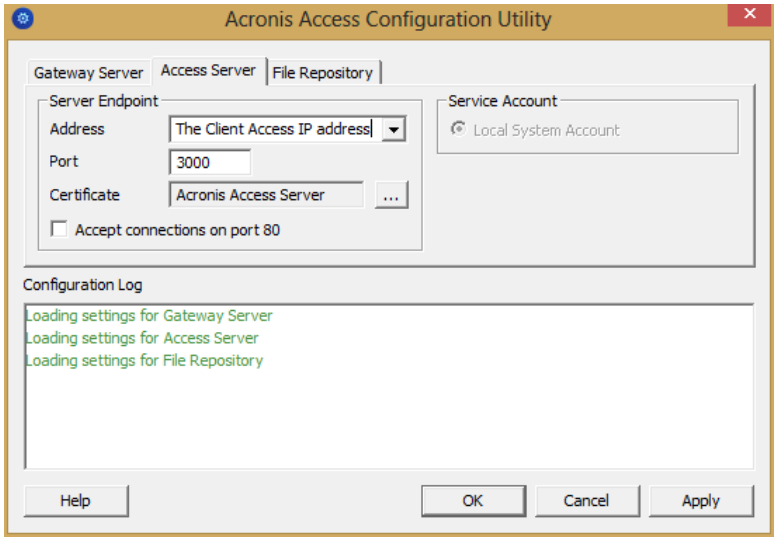
Copyright © Acronis International GmbH, 2002-2014

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



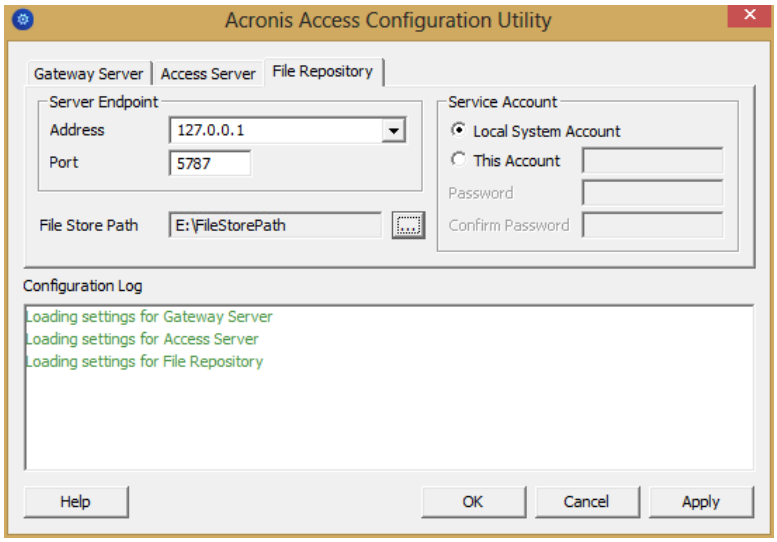
4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

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

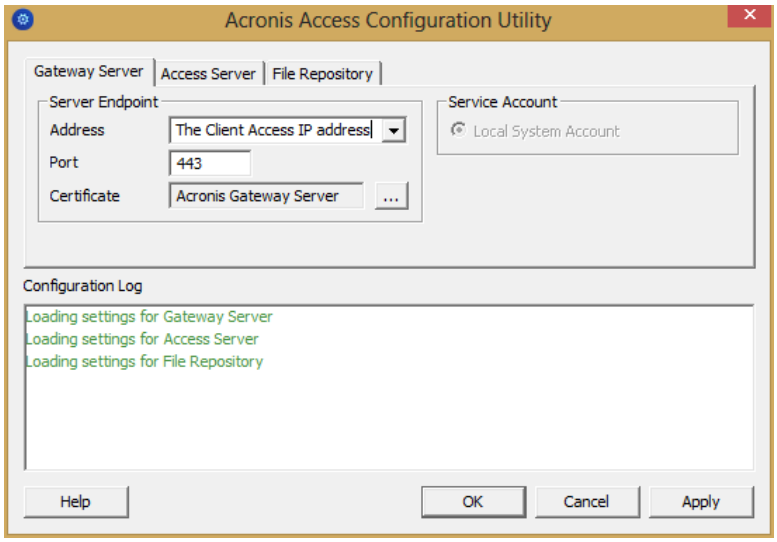
   Note: *You can copy the configured database.yml from the first node and paste it to the second node.*

   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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

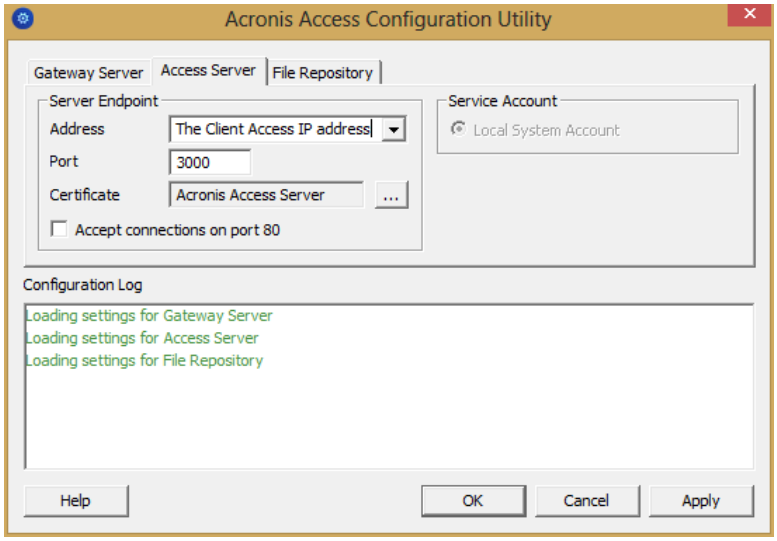
Copyright © Acronis International GmbH, 2002-2014

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



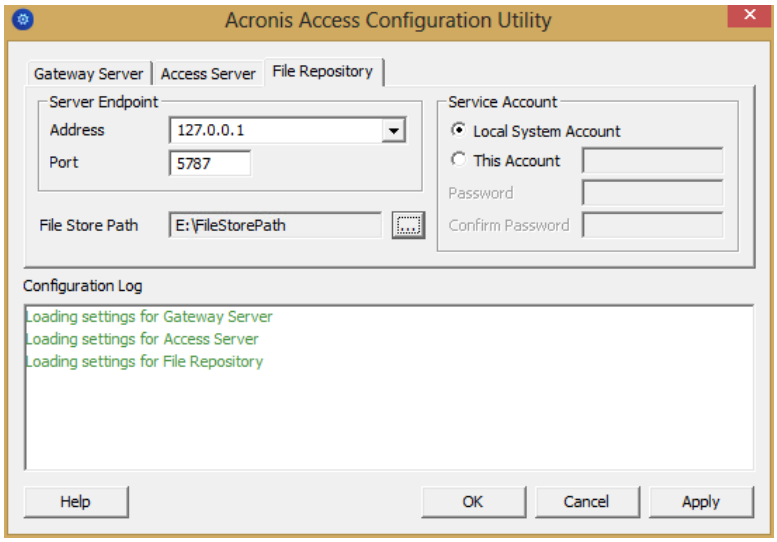
8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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.



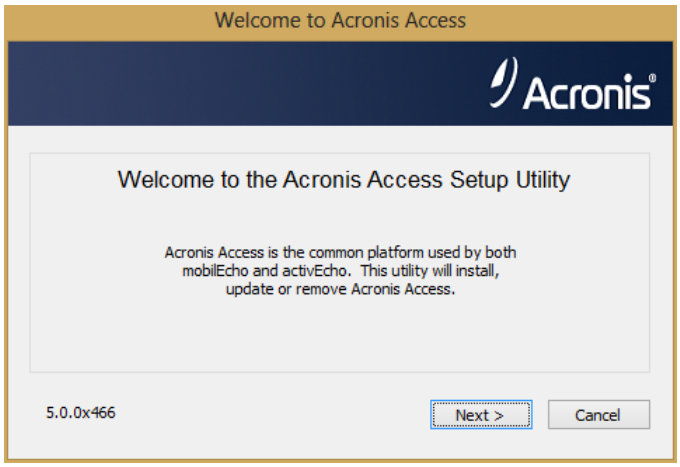
10. Click **OK** to complete the configuration and restart the services.

7.2.2 Installing Acronis Access on a Windows 2008 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.

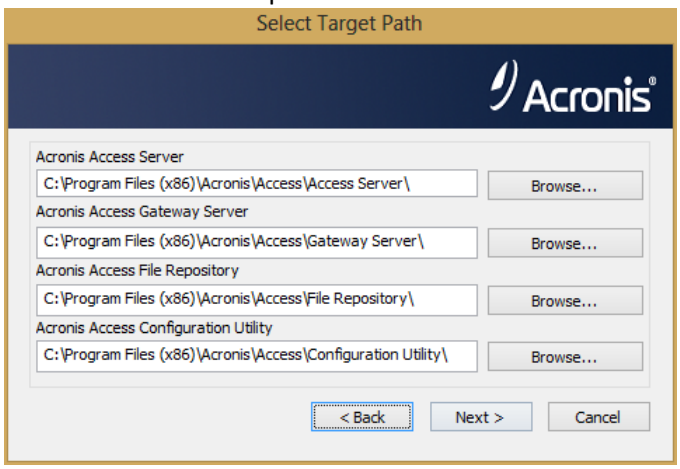


4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.

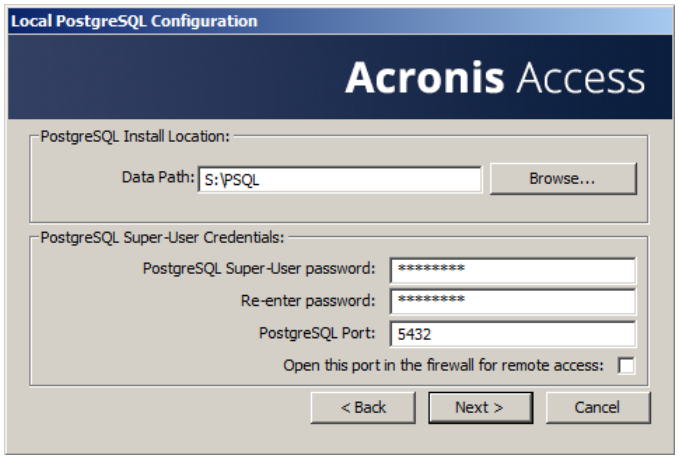
Copyright © Acronis International GmbH, 2002-2014

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

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



8. Set a password for the user Postgres and write it down. This password will be needed for database backup and recovery.
9. 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.

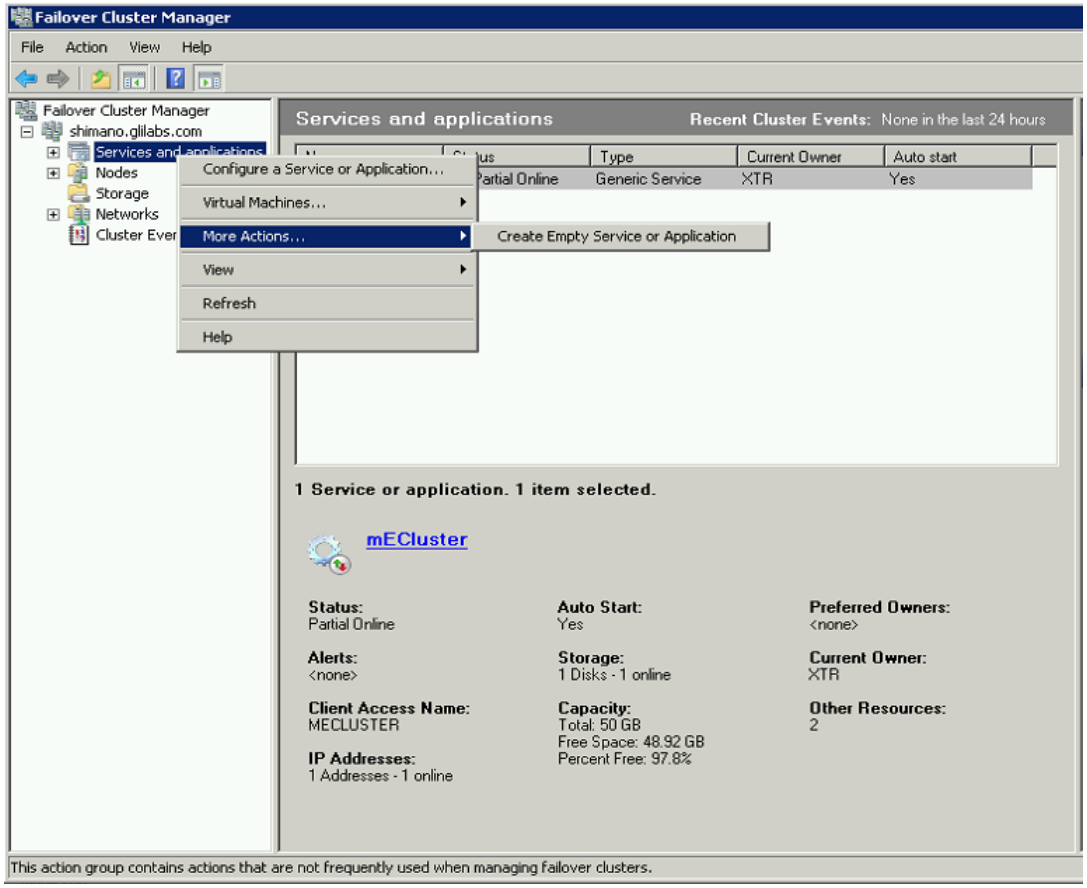
When the Acronis Access installer finishes, press Exit.

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**.

Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_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.*

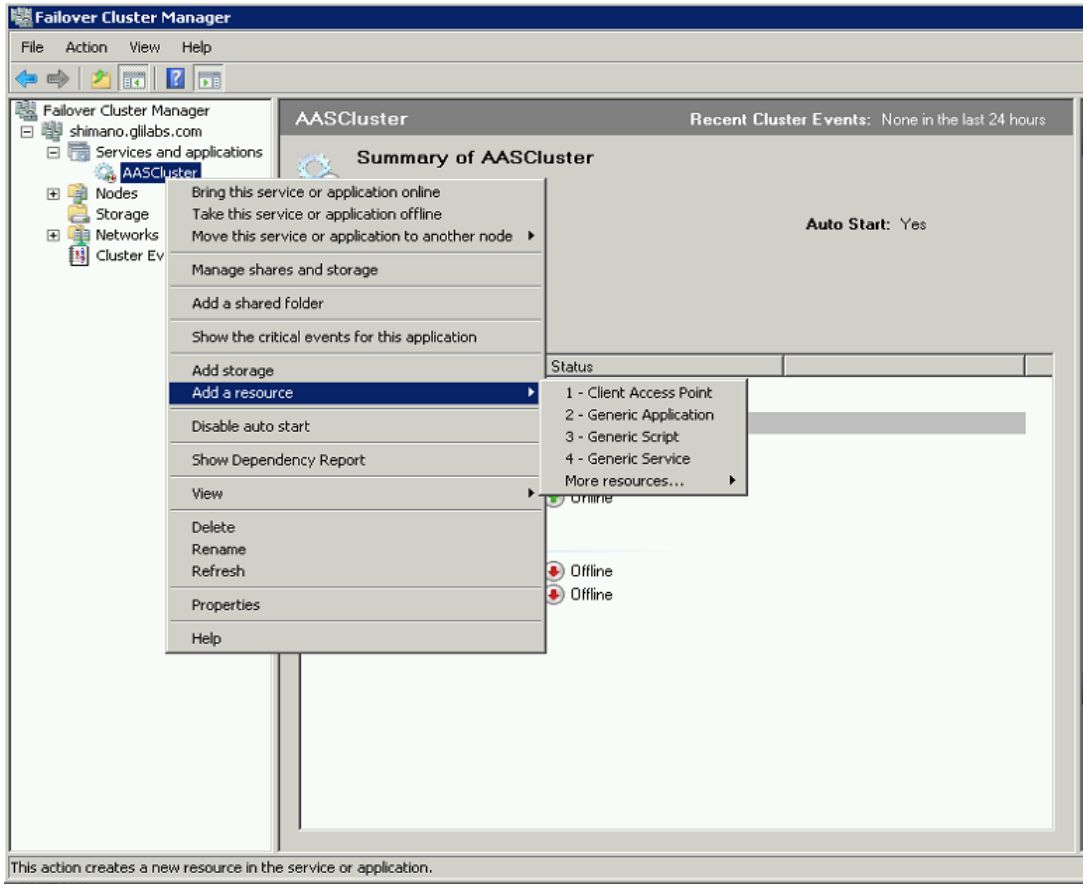
Adding all of the necessary services to the Acronis Access Service group

Complete the following procedure for each of the following services: AcronisAccessGateway, postgresql-x64-9.2 (this may be different depending on the version of PostgreSQL), AcronisAccessRepository and AcronisAccessTomcat

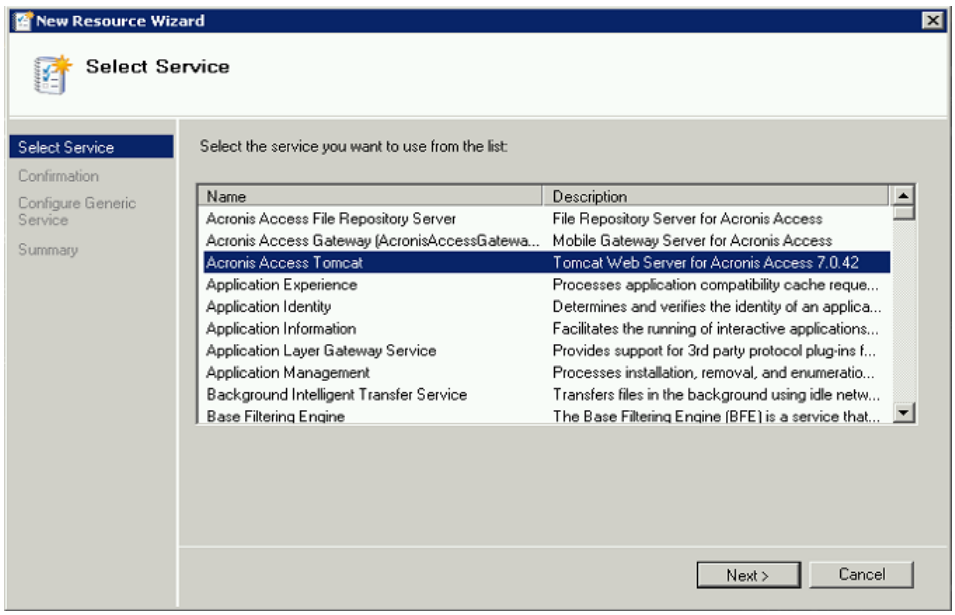
1. Right-click on the Acronis Access service group and select **Add a resource**.

Copyright © Acronis International GmbH, 2002-2014

2. Select **Generic Service**.



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



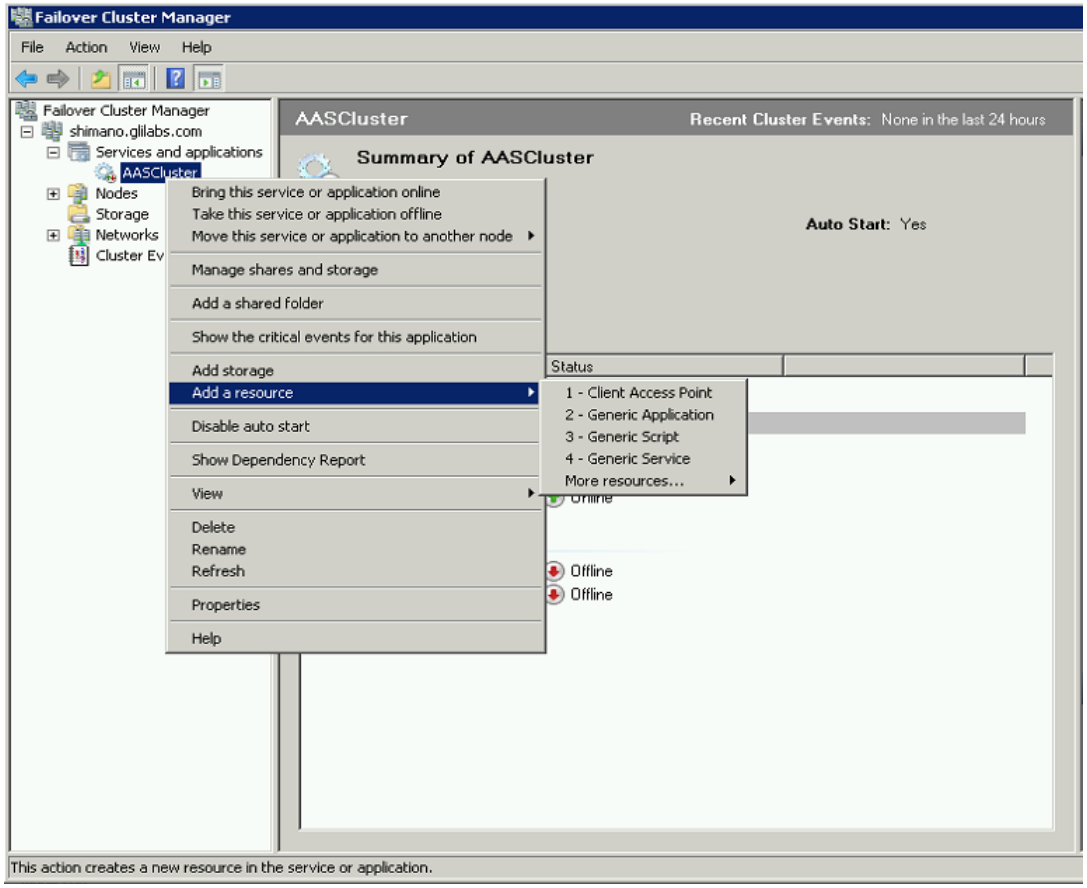
4. On the confirmation window press **Next**.
5. Press **Next** on the **Replicate Registry Settings** window.
6. On the summary window press **Finish**.

Setting a Client Access Point

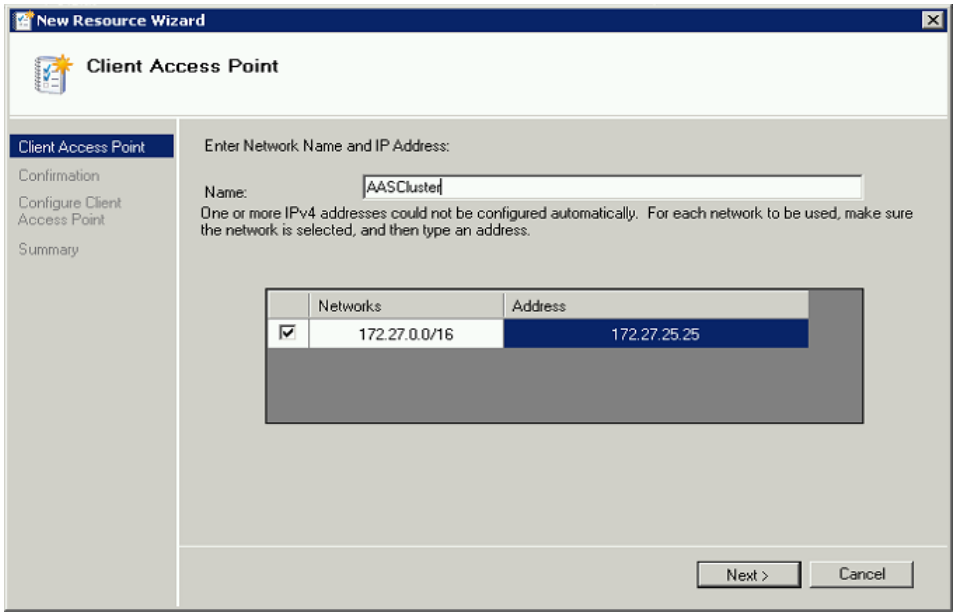
1. Right-click on the Acronis Access service group and select **Add a resource**.

Copyright © Acronis International GmbH, 2002-2014

2. Select **Client Access Point**.



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



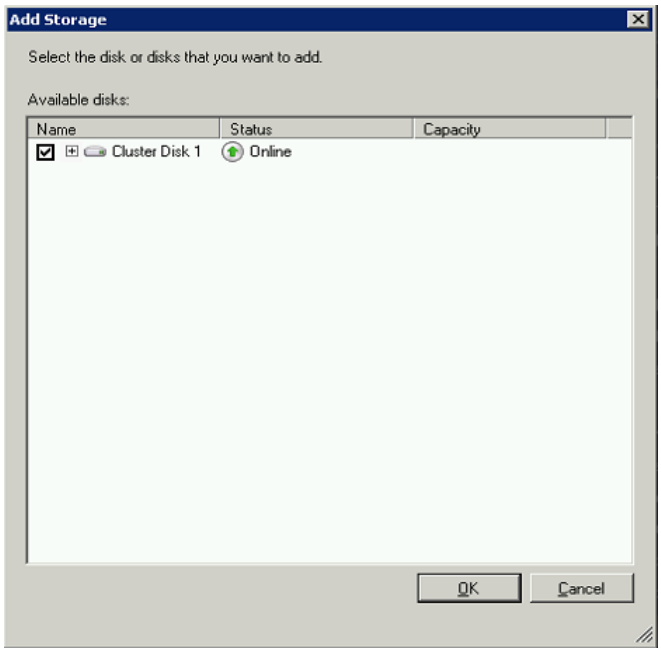
5. Enter the IP address and press **Next**.
6. On the Confirmation window press **Next**.
7. On the summary window press **Finish**.

Adding a shared disk

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

Copyright © Acronis International GmbH, 2002-2014

2. Select the desired shared drive.



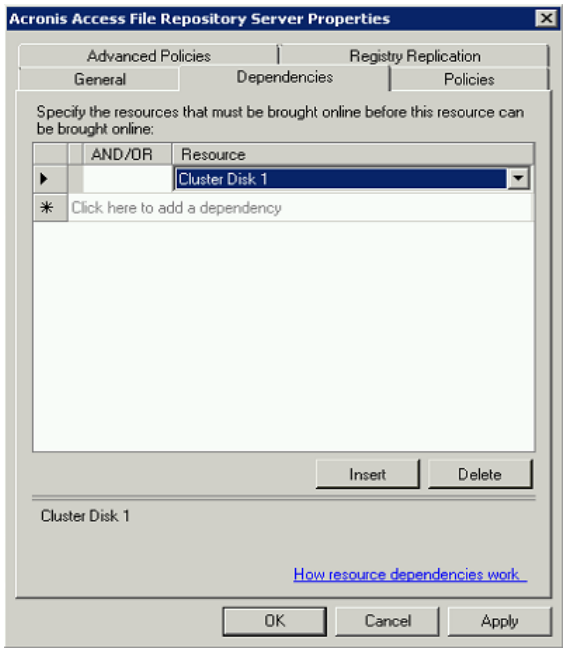
3. On the Confirmation window press **Next**.
4. On the summary window press **Finish**.

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.

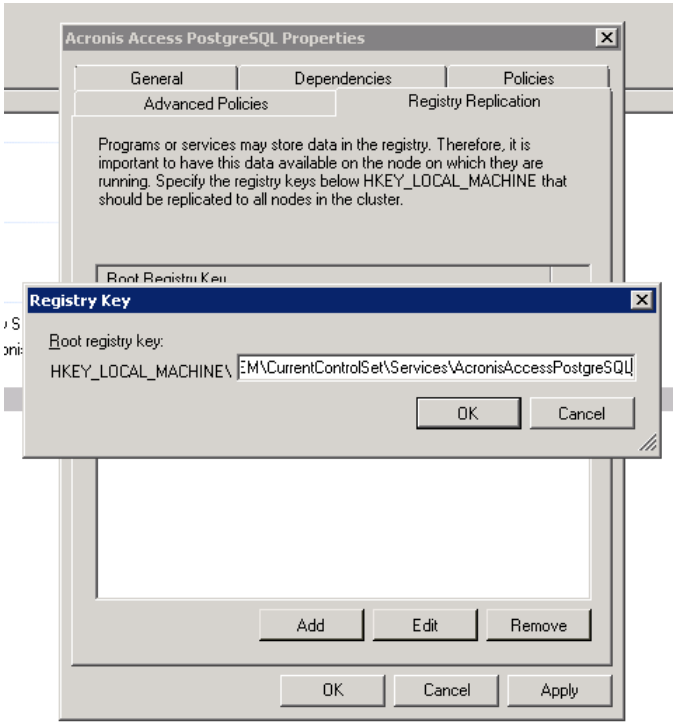


4. Press **Apply** and close the window.

For PostgreSQL also do the following:

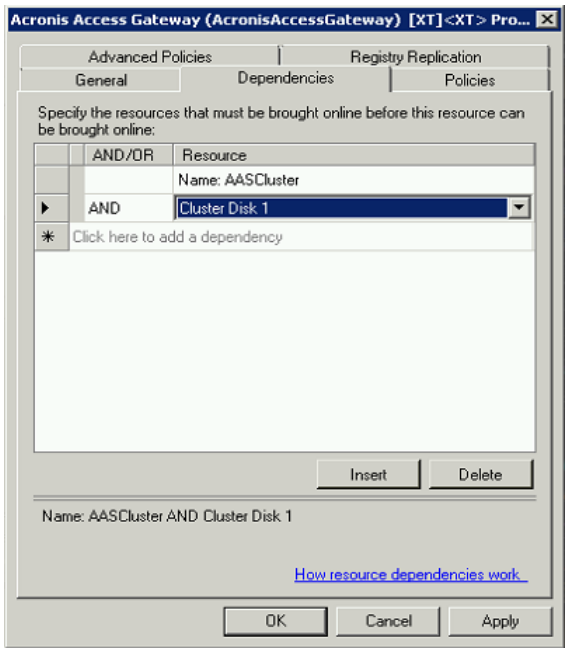
Copyright © Acronis International GmbH, 2002-2014

1. Click on the **Registry Replication** tab.
2. Press **Add** and enter the following:
   `SYSTEM\CurrentControlSet\Services\postgresql-some version` (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).

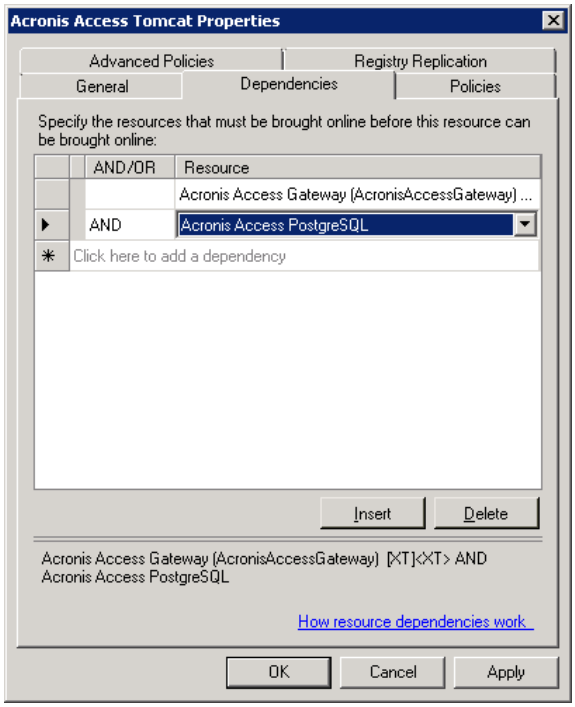


Copyright © Acronis International GmbH, 2002-2014

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.



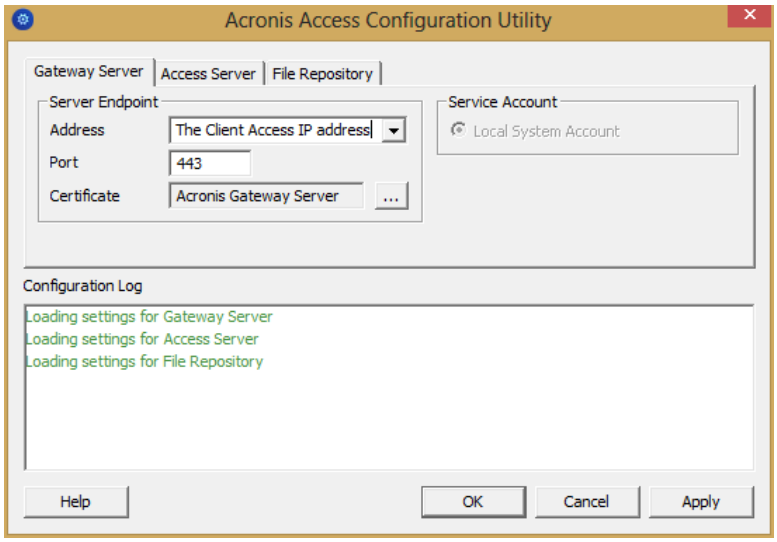
Note: *If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access Service group and set it as a dependency for the network name.*

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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

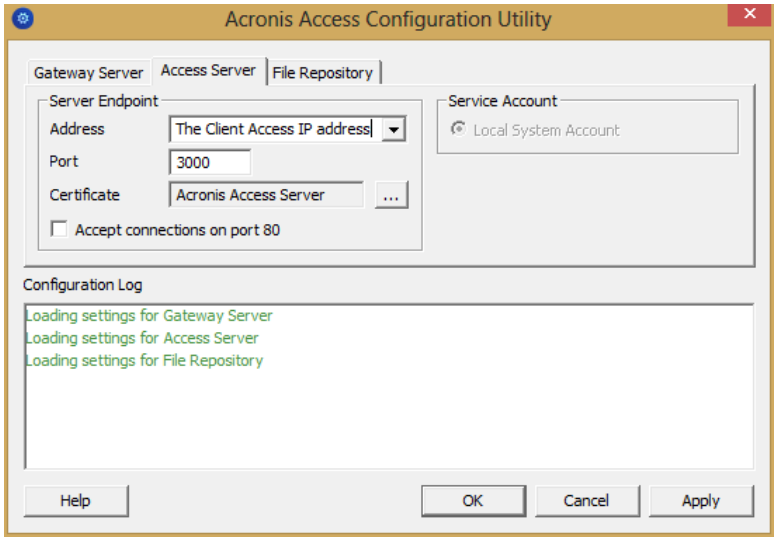
Copyright © Acronis International GmbH, 2002-2014

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



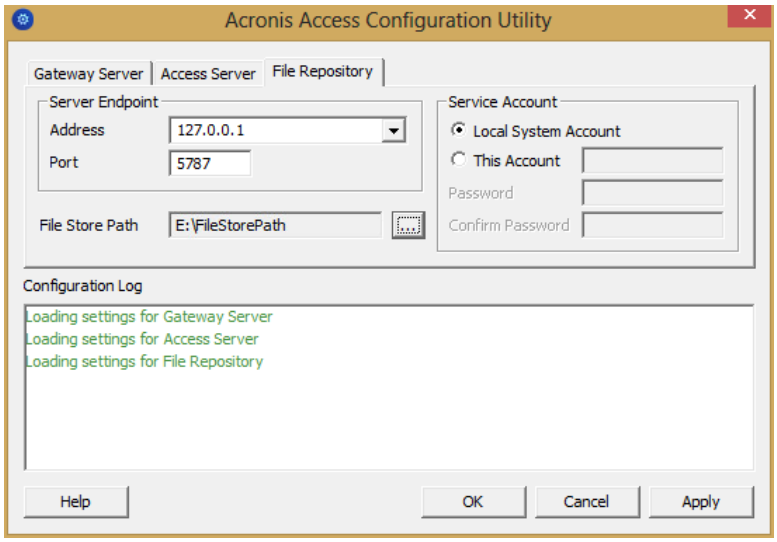
4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

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

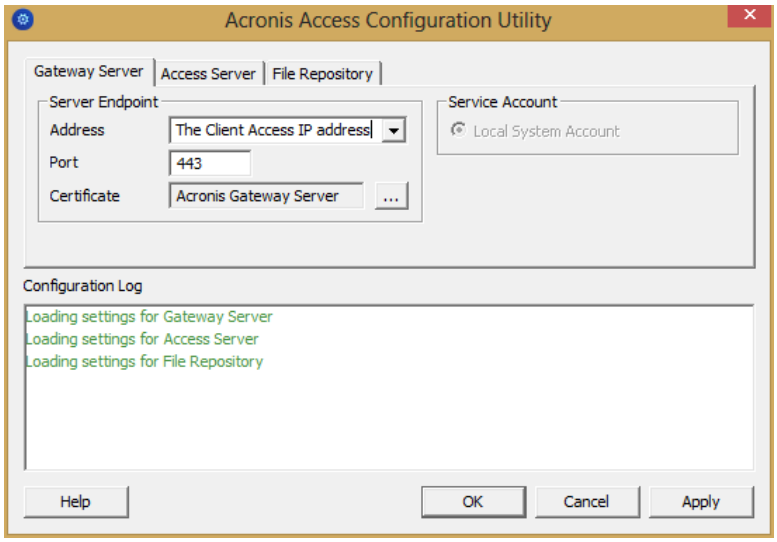
   Note: *You can copy the configured database.yml from the first node and paste it to the second node.*

   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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

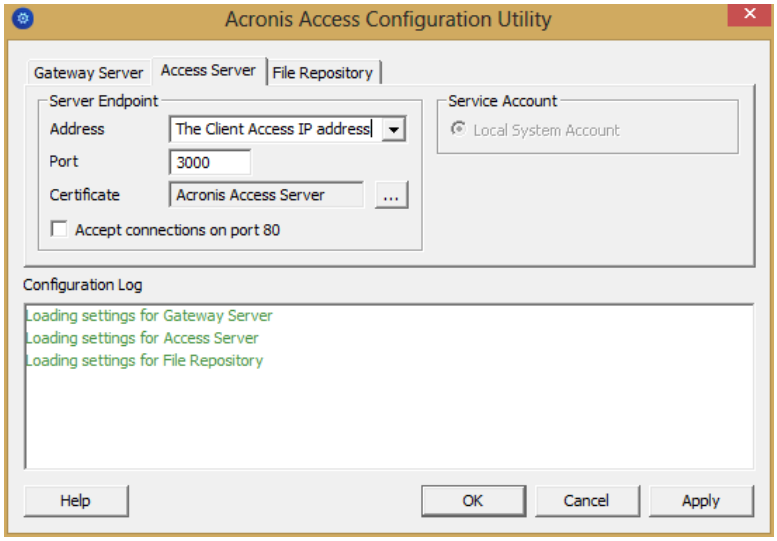
Copyright © Acronis International GmbH, 2002-2014

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



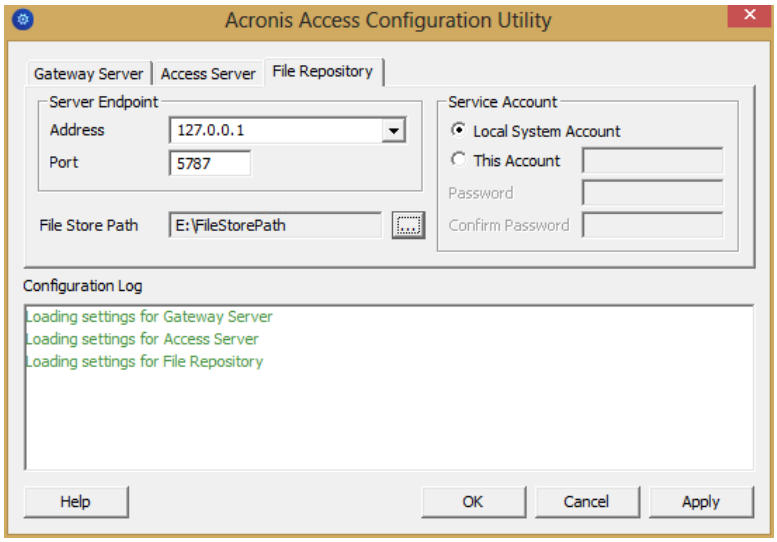
8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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.



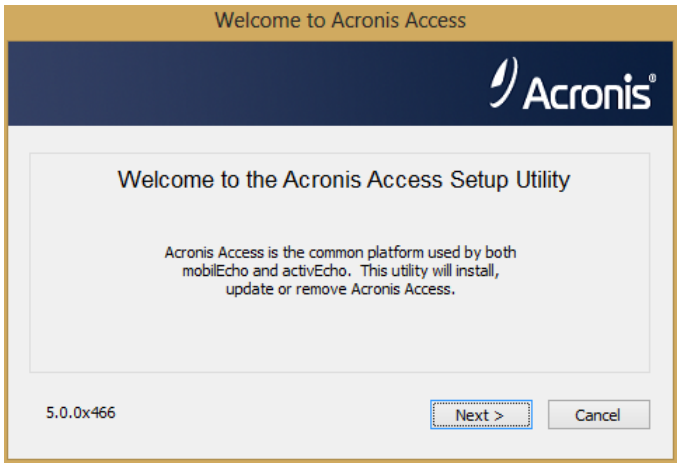
10. Click **OK** to complete the configuration and restart the services.

7.2.3 Installing Acronis Access on a Windows 2012 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.

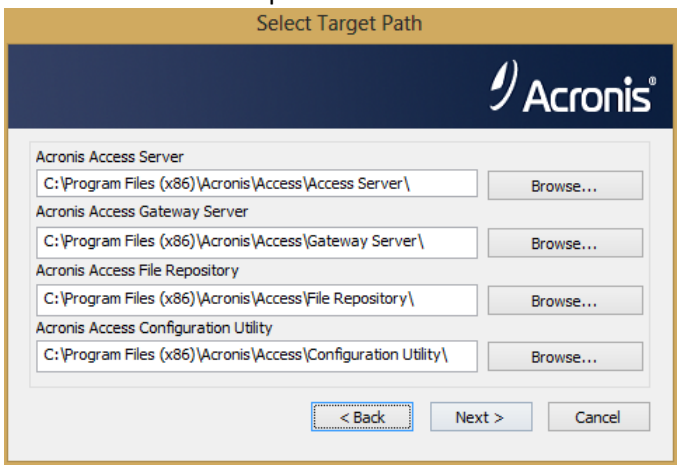


4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.

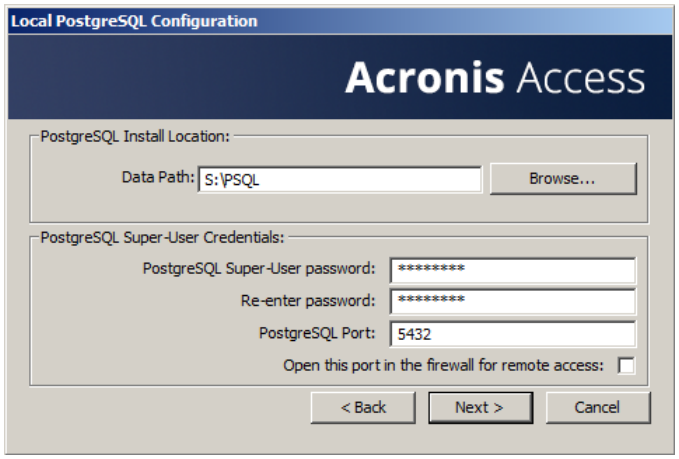
Copyright © Acronis International GmbH, 2002-2014

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

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



8. Set a password for the user Postgres and write it down. This password will be needed for database backup and recovery.
9. 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.

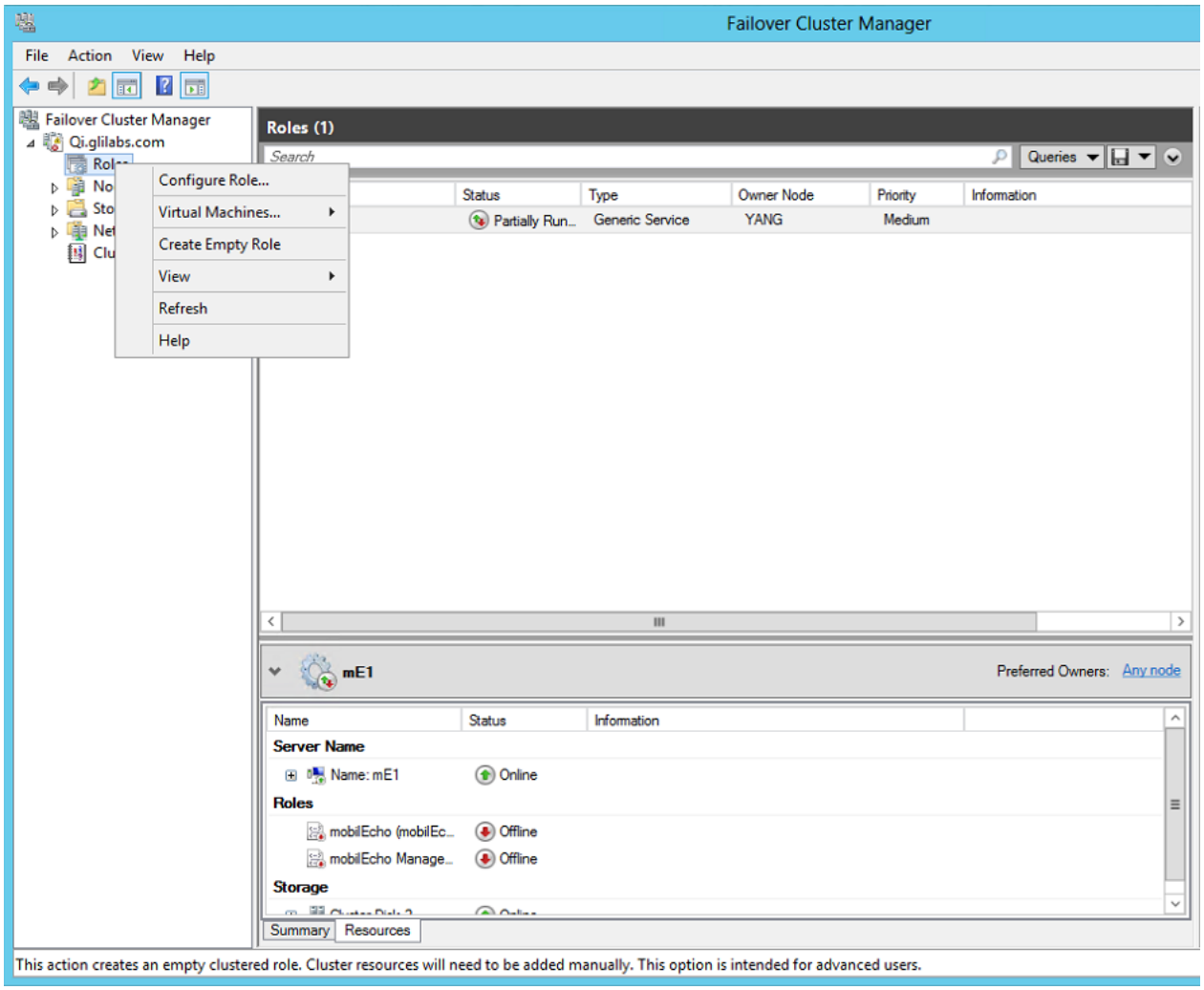
When the Acronis Access installer finishes, press **Exit**.

Creating the role

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

Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

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

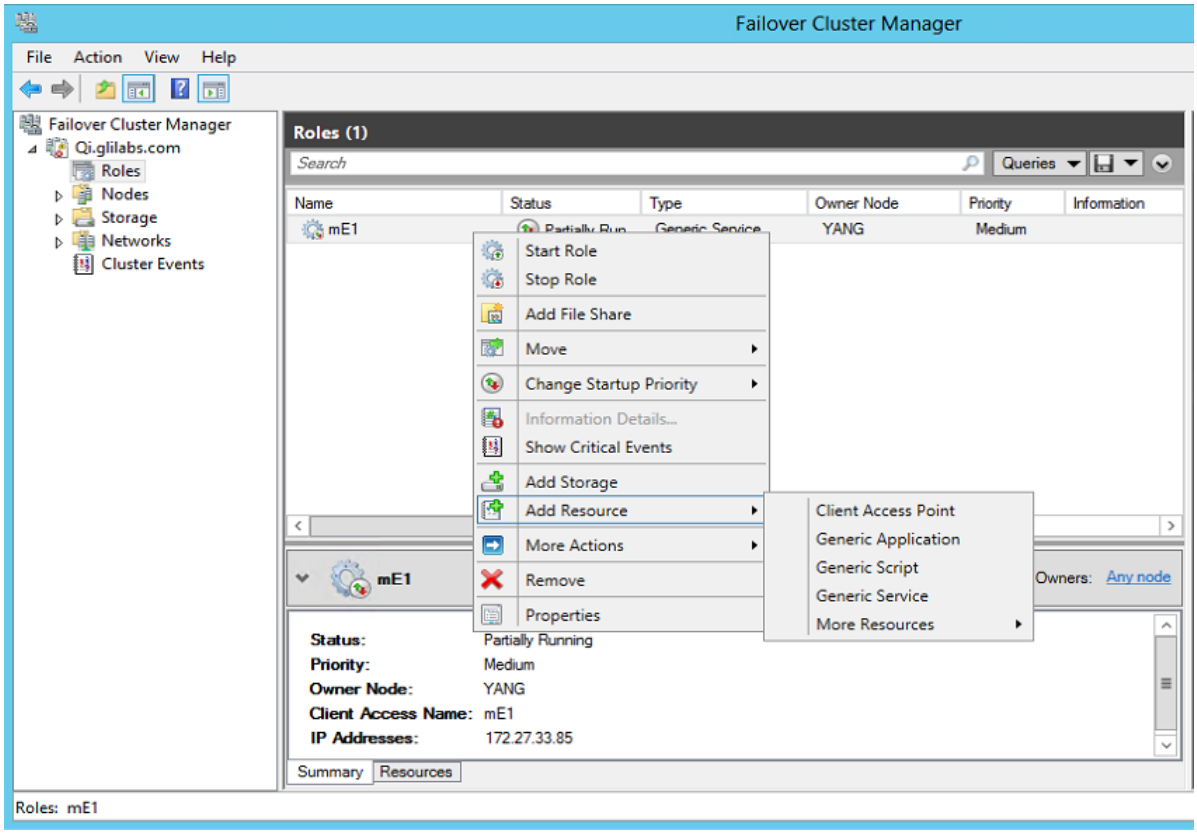
   Note: *You can copy the configured database.yml from the first node and paste it to the second node.*

Adding all of the necessary services to the Acronis Access role

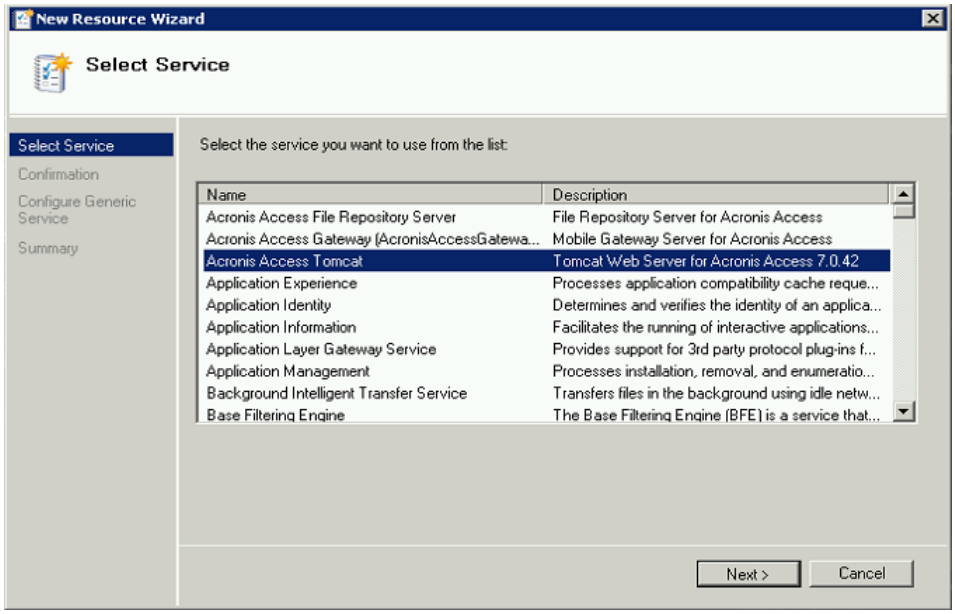
Complete the following procedure for each of the following services: AcronisAccessGateway, postgresql-x64-9.2 (this may be different depending on the version of PostgreSQL), AcronisAccessRepository and AcronisAccessTomcat

Copyright © Acronis International GmbH, 2002-2014

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**.



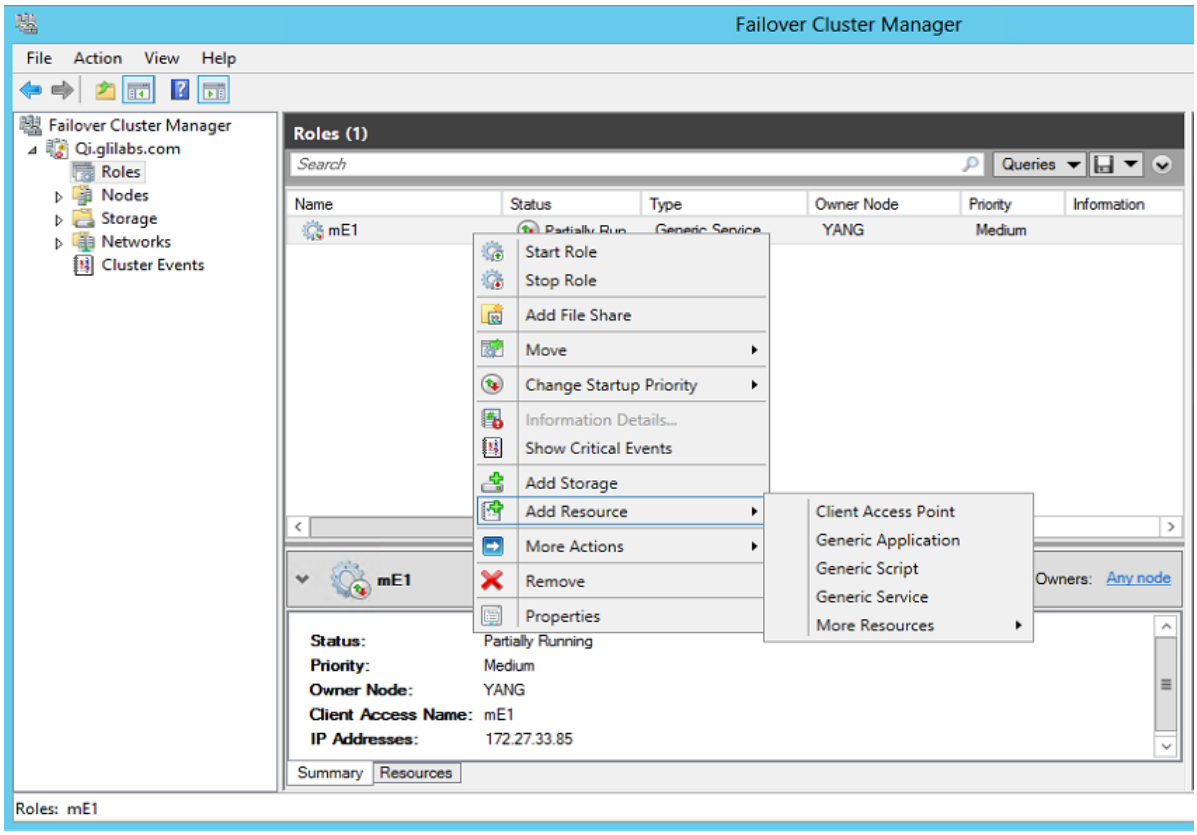
4. On the Confirmation window press **Next**.
5. On the summary window press **Finish**.

Setting an Access Point

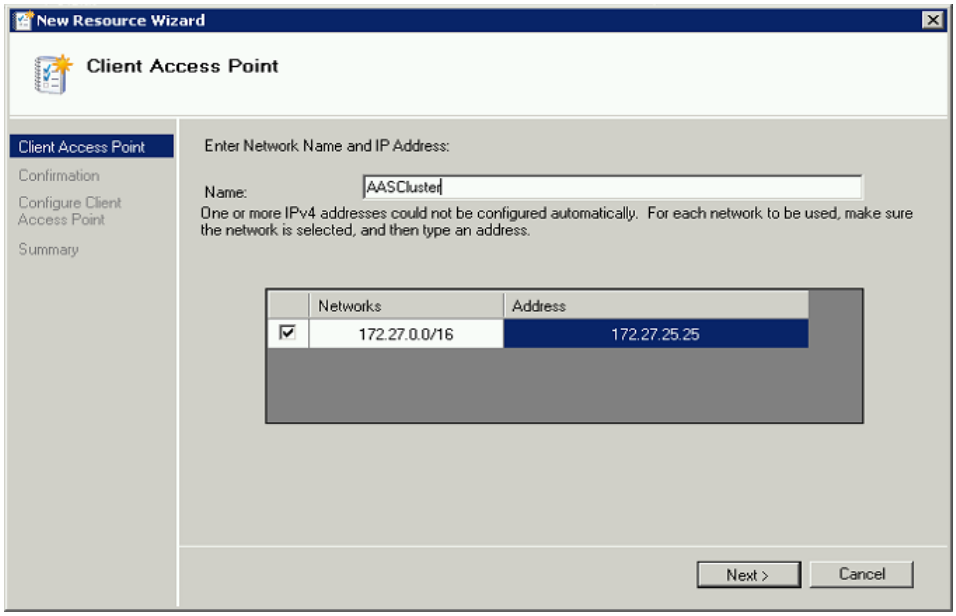
1. Right-click on the Acronis Access role and select **Add a resource**.

Copyright © Acronis International GmbH, 2002-2014

2. Select **Client Access Point**.



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



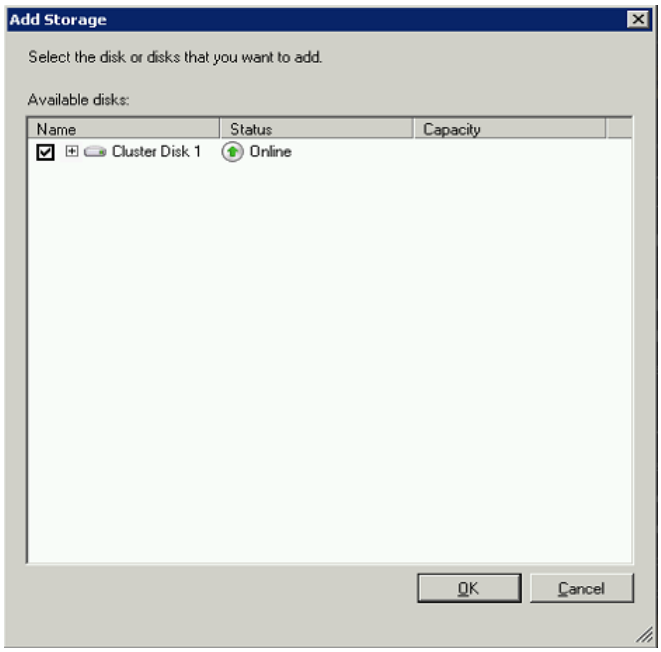
5. Enter the IP address and press **Next**.
6. On the Confirmation window press **Next**.
7. On the summary window press **Finish**.

Adding a shared disk

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

Copyright © Acronis International GmbH, 2002-2014

2. Select the desired shared drive.

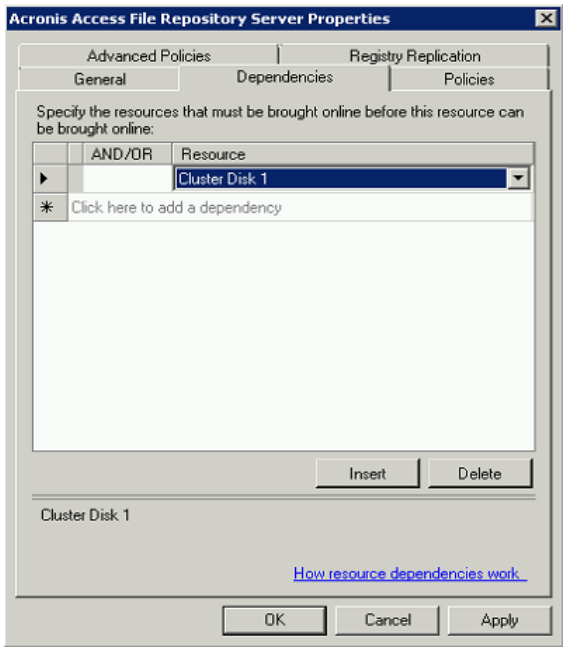


Configuring dependencies

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.

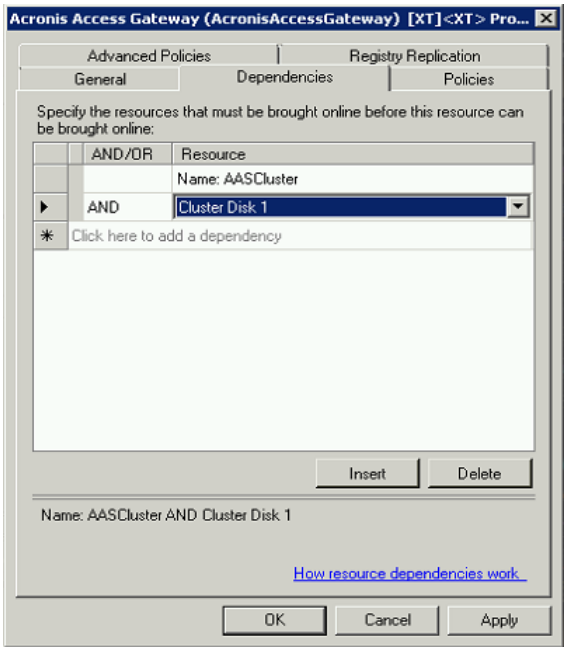


4. Press **Apply** and close the window.

For the Acronis Access Gateway Server service do the following:

Copyright © Acronis International GmbH, 2002-2014

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).



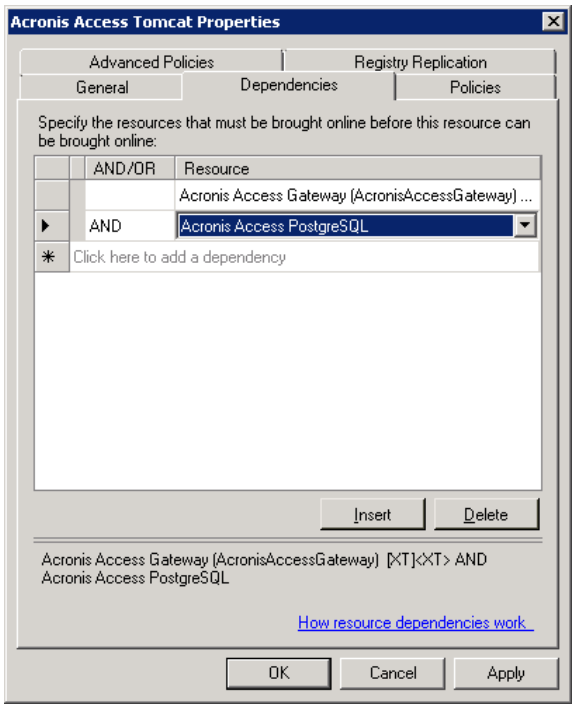
4. Press **Apply** and close the window.

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.

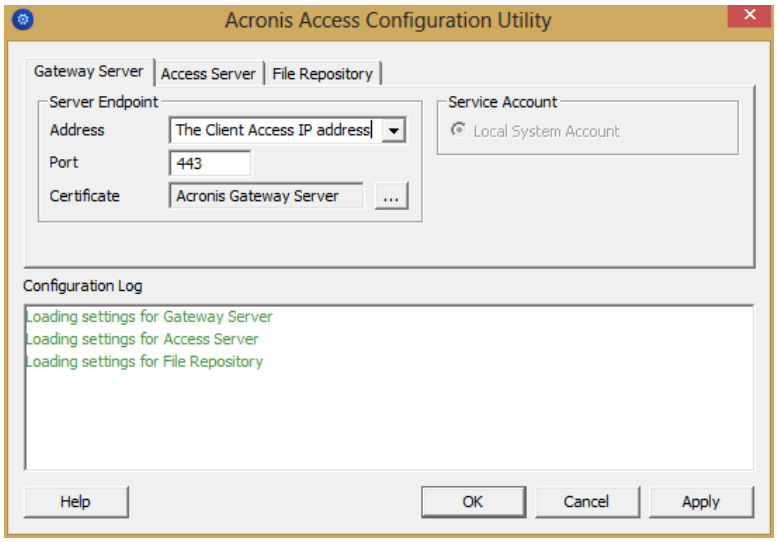
Copyright © Acronis International GmbH, 2002-2014

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

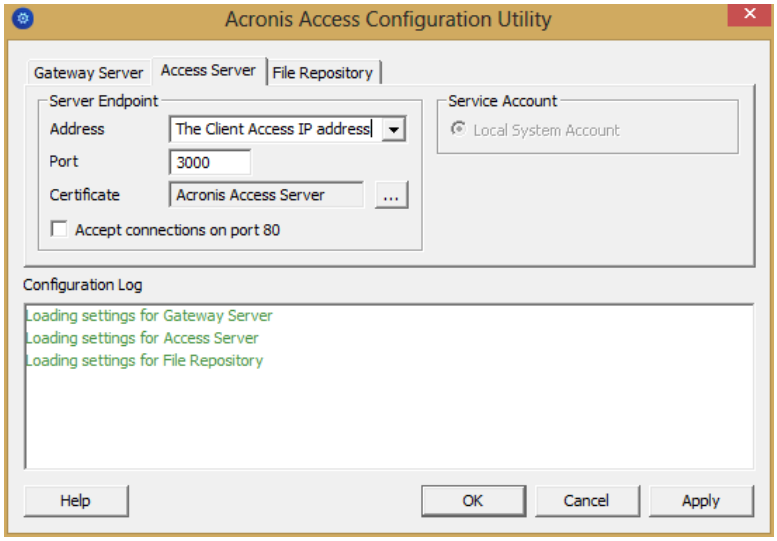
1. Right-click on the Acronis Access role and press **Start role**.
2. Launch the Configuration Utility.
   - On a clean install, this is generally located at **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program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



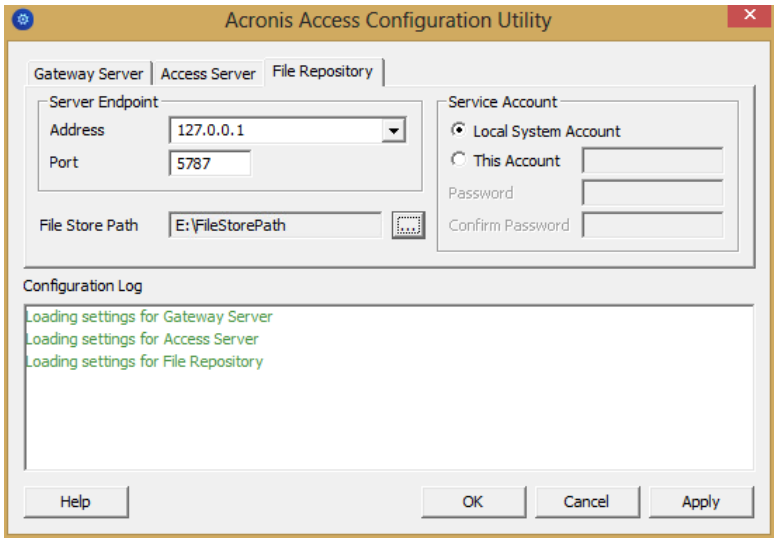
4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Copyright © Acronis International GmbH, 2002-2014

***Note:** If **Accept connections on 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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho Server\`**
   b. Find the **database.yml** file and open it with a text editor.

Copyright © Acronis International GmbH, 2002-2014

c. Find this line: **`database_path: './database/'`** and replace **./database/** with the path you want to use (e.g. **`database_path: 'S:/mobilEcho_cluster/database/'`**).

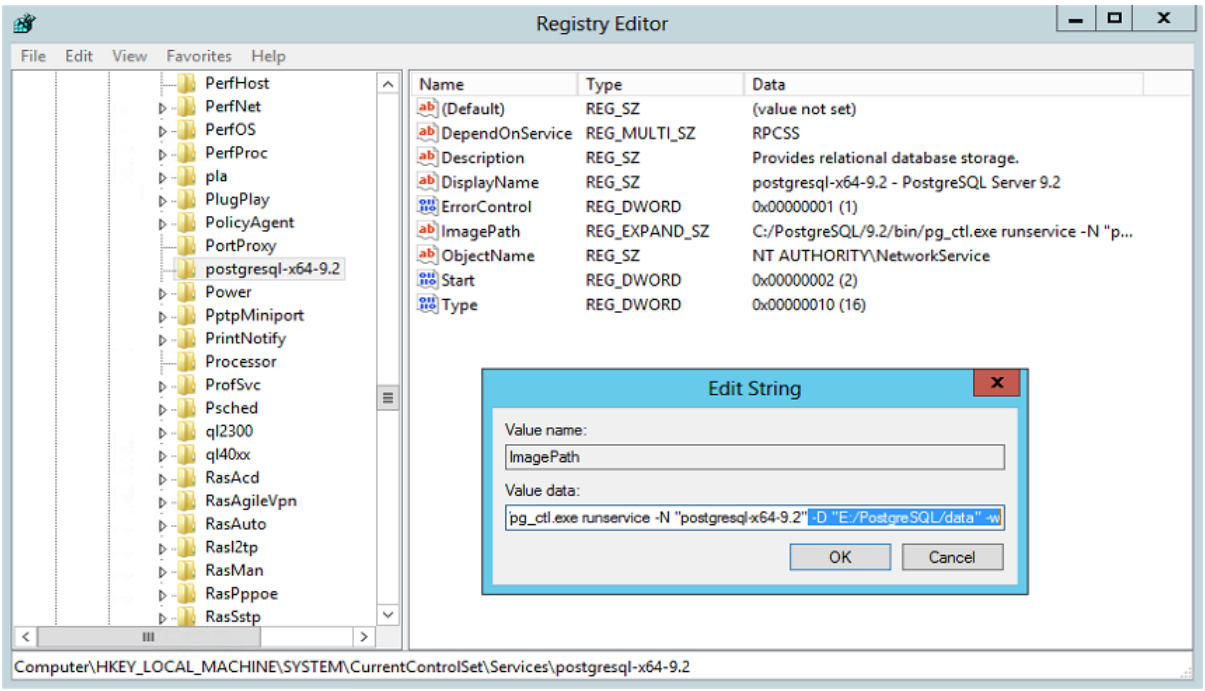
Note: *Use slashes(/) as a path separator.*

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 you will need to manually replicate the registry:

1. Open **Regedit**.
2. Navigate to **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-some version\`** and open this key: **ImagePath**
3. Change the value of the key to this: **`-D "The path you selected for the PostgreSQL data location" -w`** (e.g. **`-D "E:/PostgreSQL/data" -w`**)



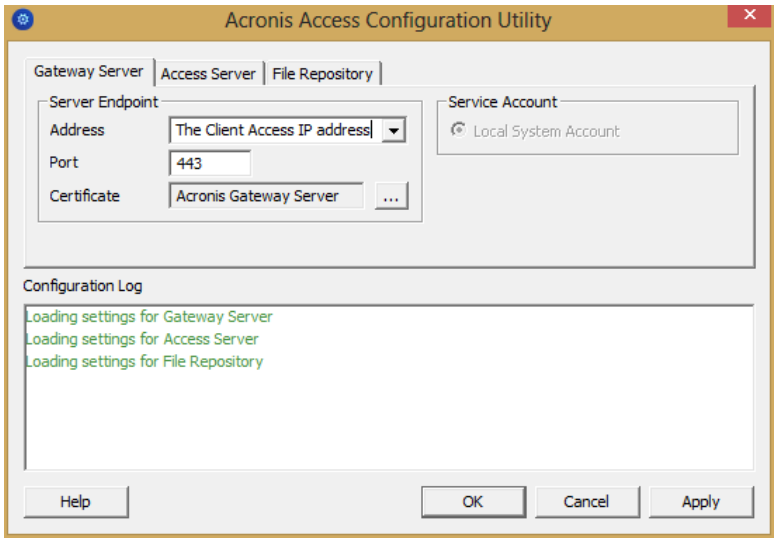
4. Close **Regedit** and continue with the steps below.
5. Move the Acronis Access role to the second node.

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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

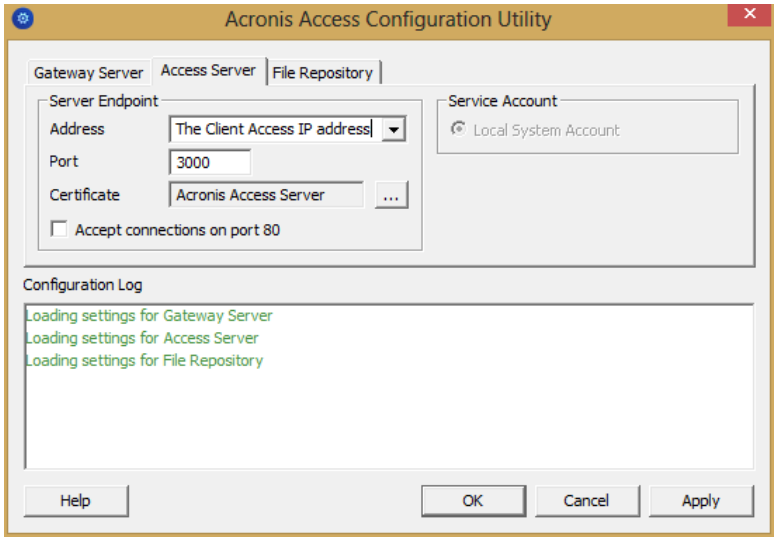
Copyright © Acronis International GmbH, 2002-2014

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



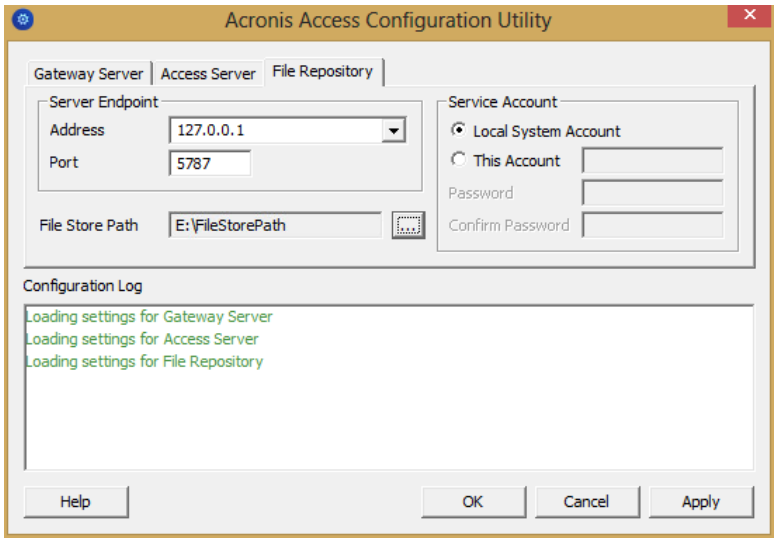
3. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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.

7.3 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 196
Upgrading a mobilEcho server on a Windows 2008 Failover Cluster to Acronis Access 206
Upgrading a mobilEcho server on a Windows 2012 Failover Cluster to Acronis Access 215

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

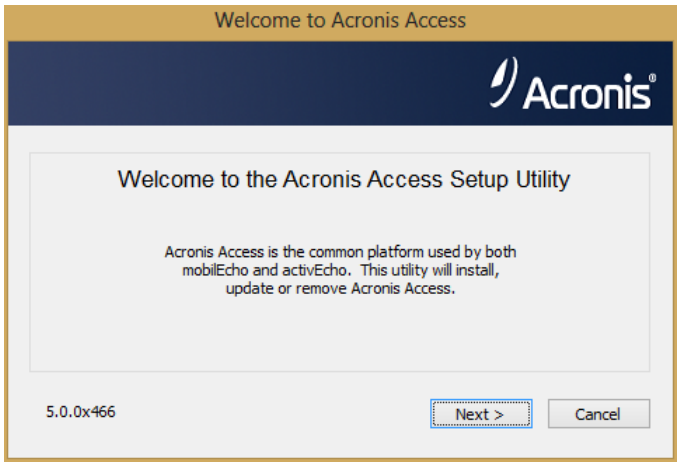
1. Open the **Cluster Administrator** and double-click on your service group.
2. Delete the mobilEcho service resources.

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

3. Launch the installer on the active node.

Copyright © Acronis International GmbH, 2002-2014

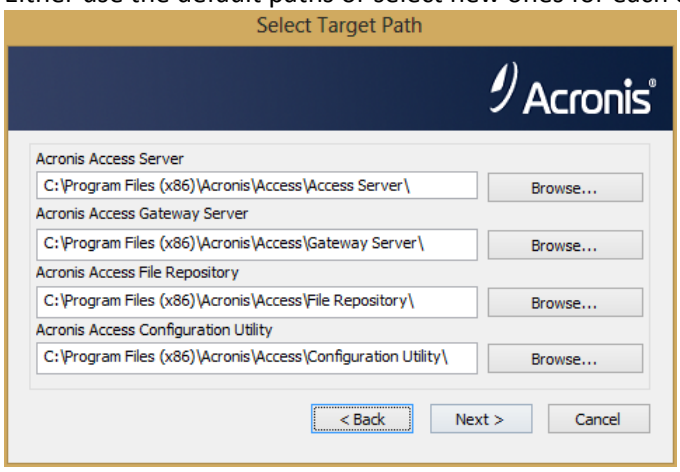
4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
5. Double-click on the installer executable.



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.*

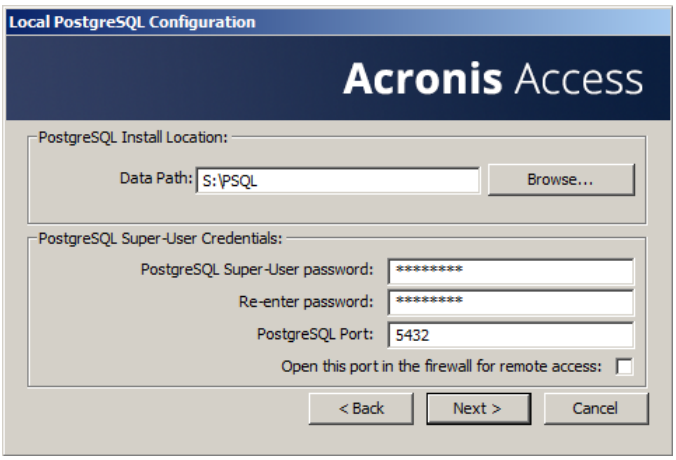
9. Either use the default paths or select new ones for each component and press OK.



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

Copyright © Acronis International GmbH, 2002-2014

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**, **mobilEcho_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\mobilEcho Server\ManagementUI\db\production.sqlite3

C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg

C:\Program Files (x86)\Group Logic\mobilEcho 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)\Acronis\Access\Gateway Server\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_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.*

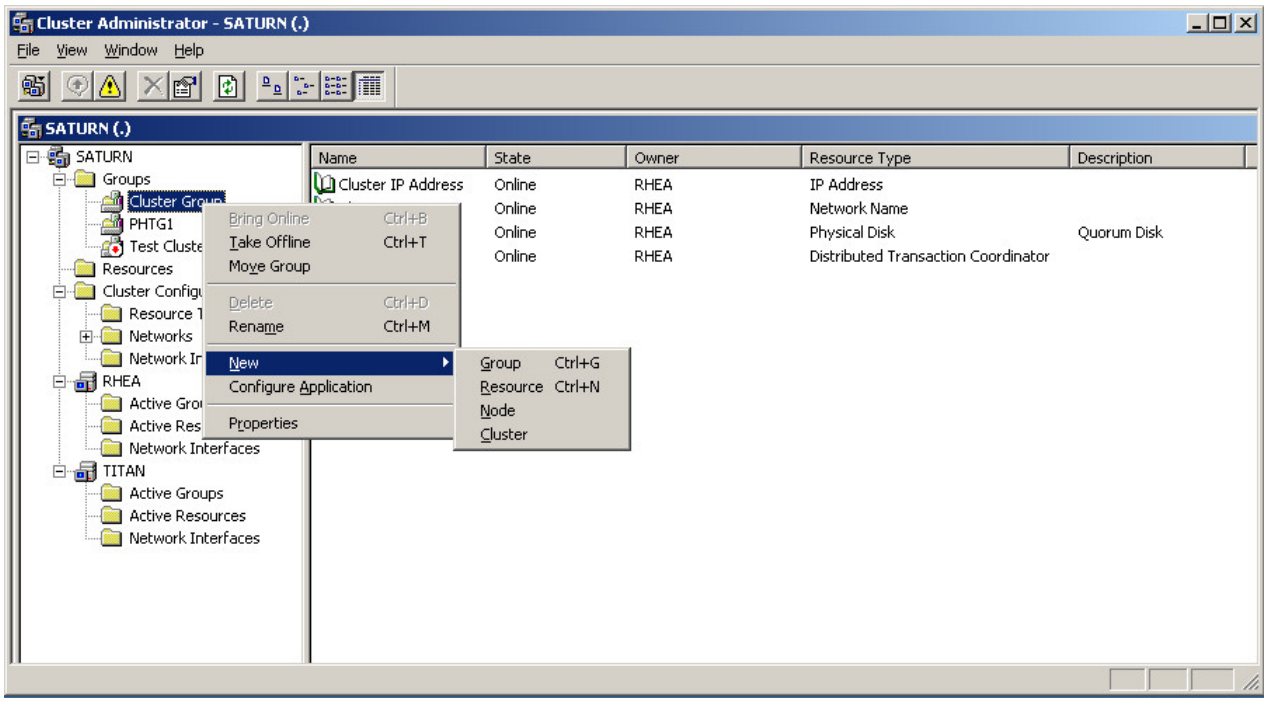
Adding all of the necessary services to the Acronis Access cluster group

Complete the following procedure for each of the following services: AcronisAccessGateway, postgresql-x64-9.2 (this may be different depending on the version of PostgreSQL), AcronisAccessRepository and AcronisAccessTomcat

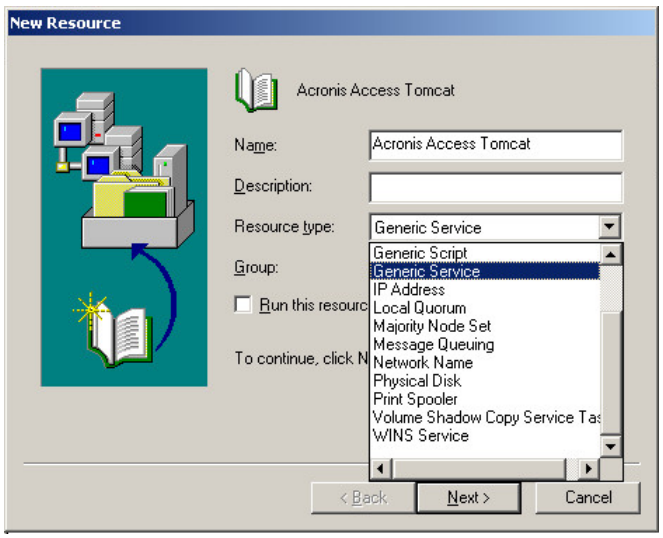
1. Right-click on the Acronis Access cluster group.

Copyright © Acronis International GmbH, 2002-2014

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

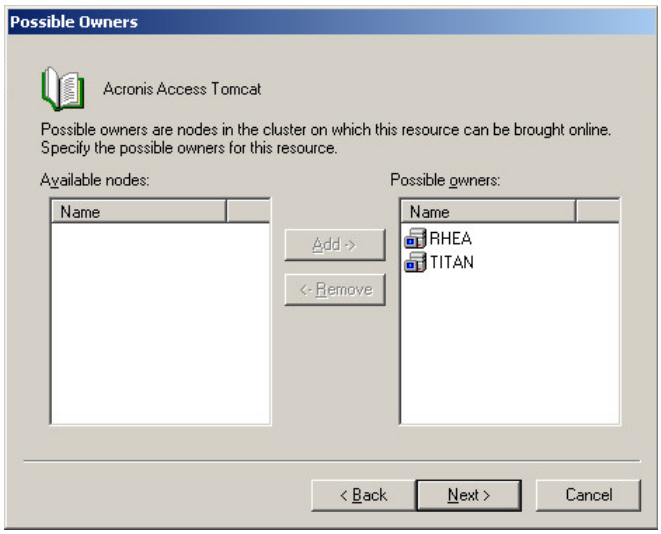


3. Enter a name for the service and select the correct cluster group.
4. From the **Resource Type** drop down menu select **Generic Service** and press **Next**.



Copyright © Acronis International GmbH, 2002-2014

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

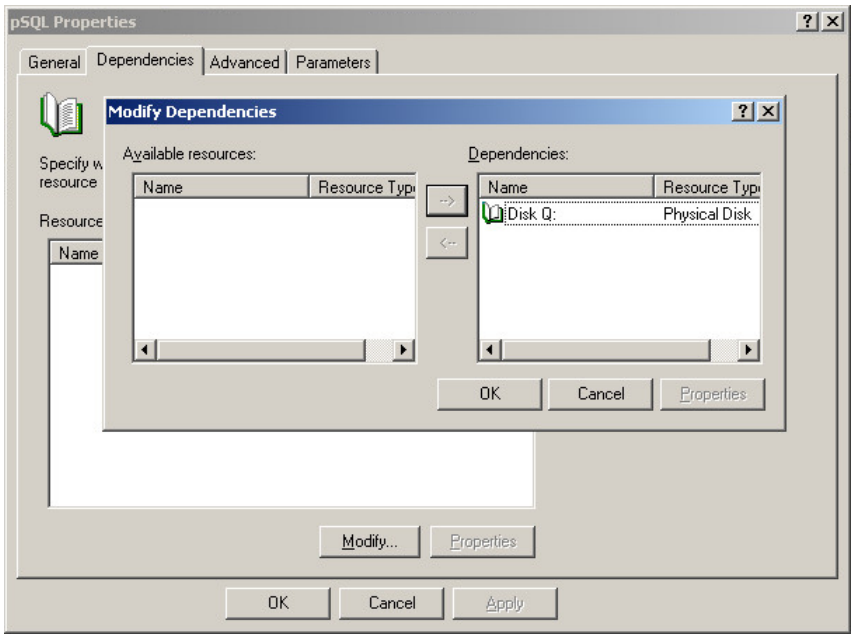


6. Skip the dependencies for now by pressing **Next**.
7. Enter the correct service name of the service you are adding (e.g. postgresql-x64-9.2) and press **Next**.
8. Skip the **Registry Replication** window for now by pressing **Next**.
9. Press **Finish** to complete the procedure.

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.

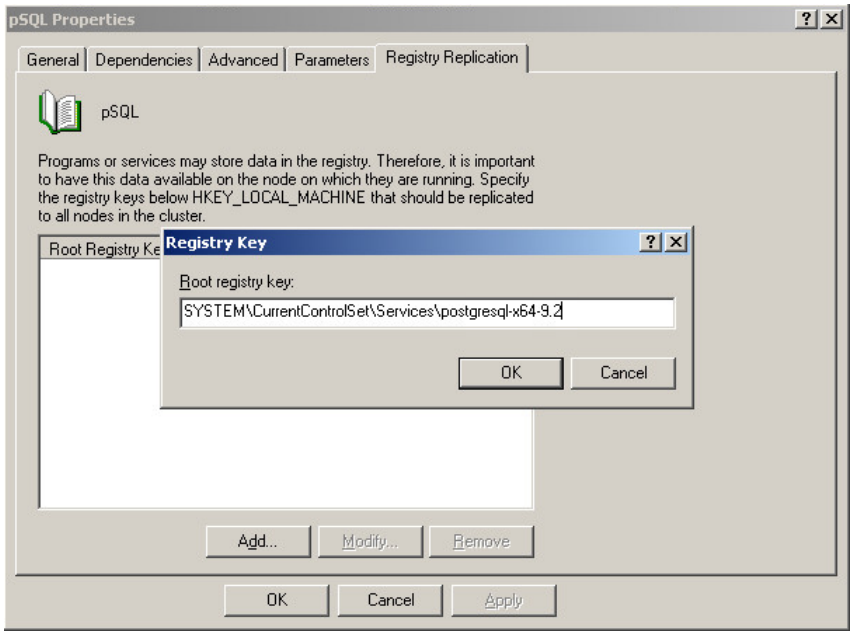


5. Press **OK**.

Copyright © Acronis International GmbH, 2002-2014

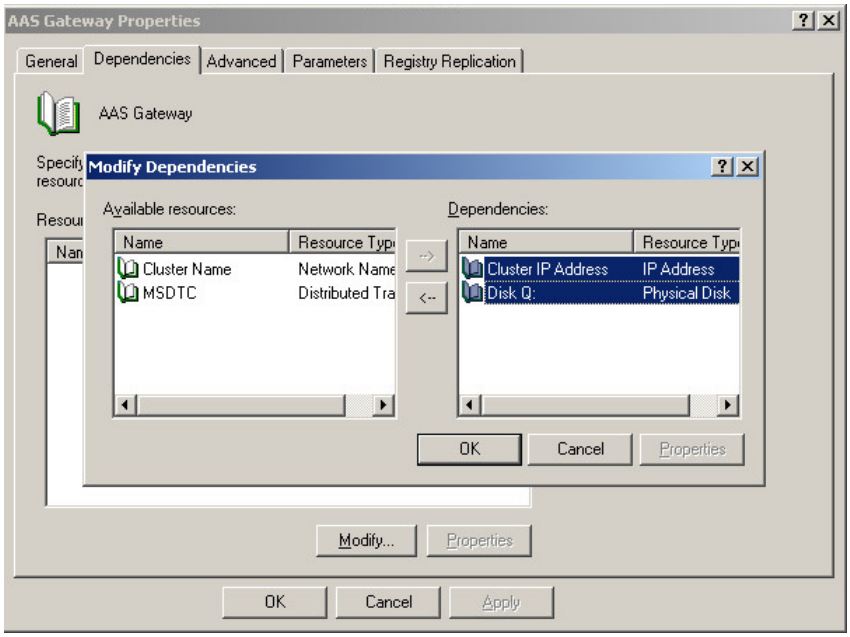
For PostgreSQL also do the following:

1. Click on the **Registry Replication** tab.
2. Press **Add** and enter the following:
   SYSTEM\CurrentControlSet\Services\postgresql-some version (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.

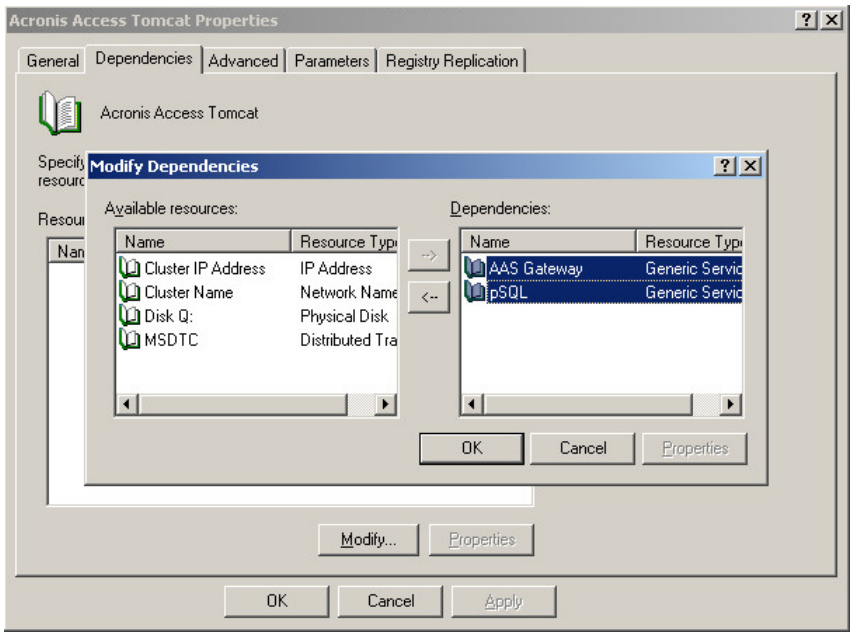


Copyright © Acronis International GmbH, 2002-2014

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.



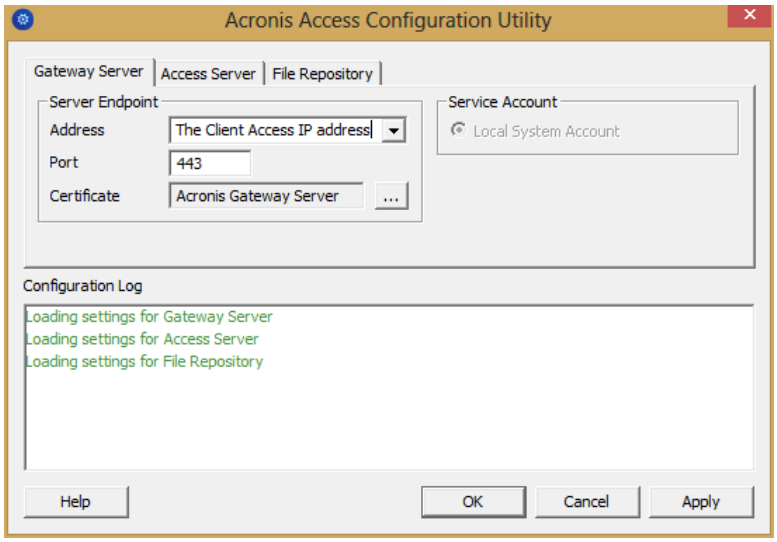
5. Press **OK**.

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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

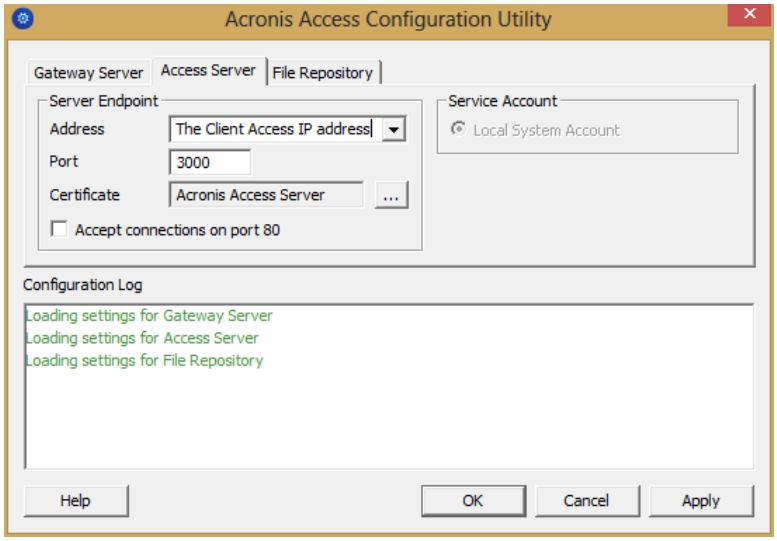
Copyright © Acronis International GmbH, 2002-2014

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



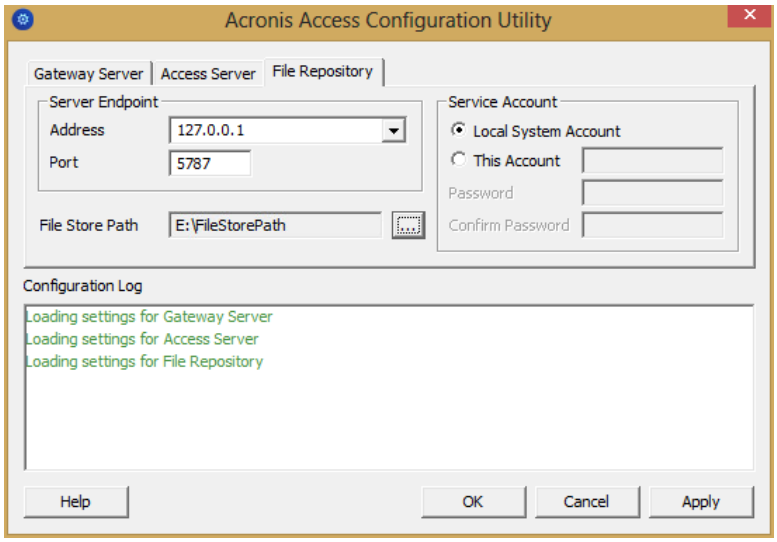
4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

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

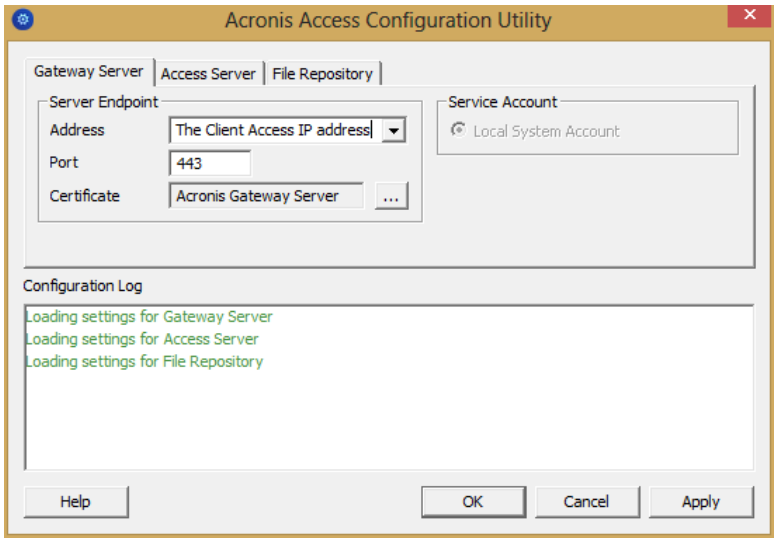
   Note: *You can copy the configured database.yml from the first node and paste it to the second node.*

   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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

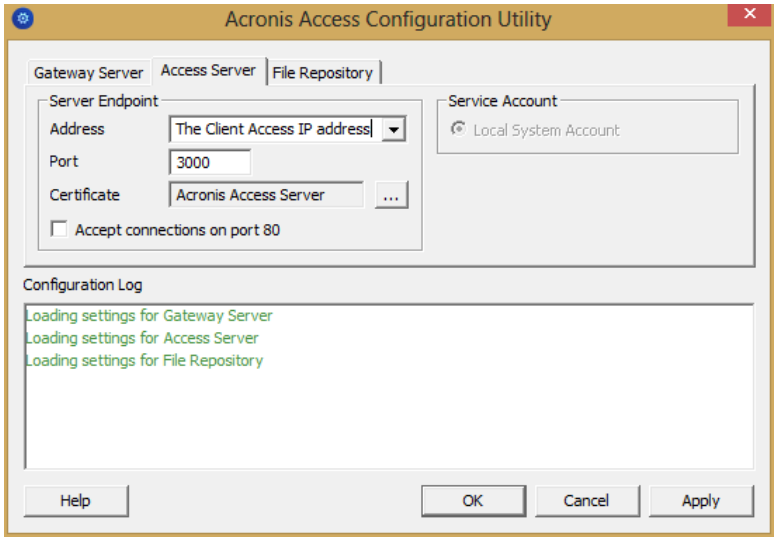
Copyright © Acronis International GmbH, 2002-2014

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



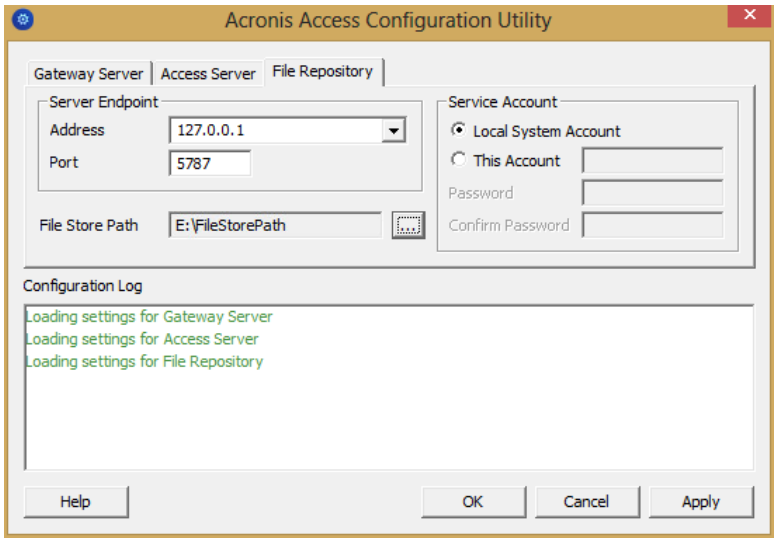
8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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.



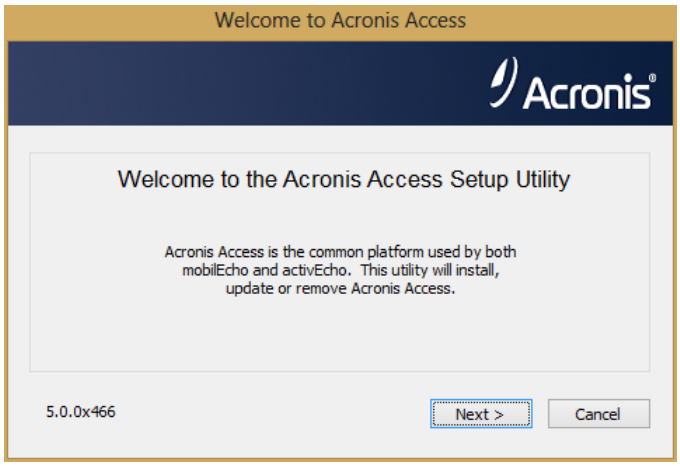
10. Click **OK** to complete the configuration and restart the services.

7.3.2 Upgrading a mobilEcho server on a Windows 2008 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.

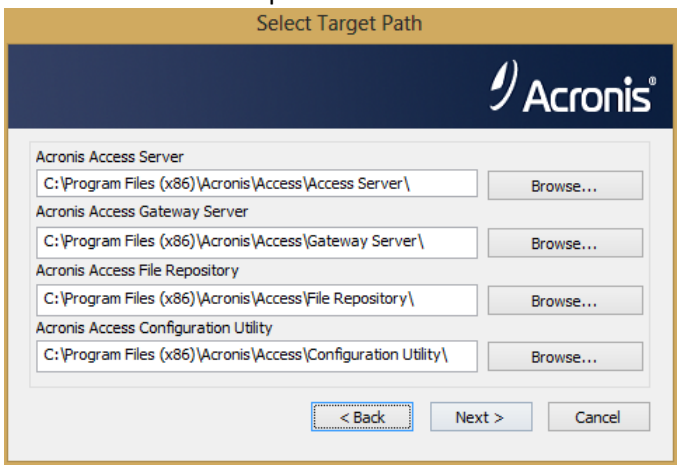


6. Press **Next** to begin.
7. Read and accept the license agreement.
8. Press **Install**.

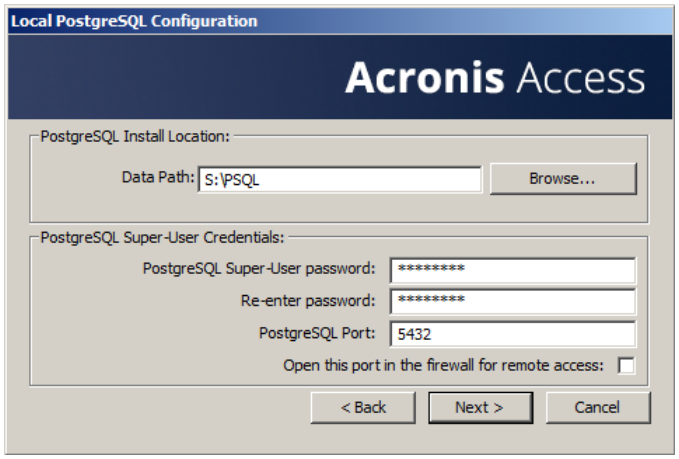
Copyright © Acronis International GmbH, 2002-2014

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 paths or select new ones for each component 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**, **mobilEcho_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\mobilEcho Server\ManagementUI\db\production.sqlite3

C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg

C:\Program Files (x86)\Group Logic\mobilEcho 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)\Acronis\Access\Gateway Server**

Copyright © Acronis International GmbH, 2002-2014

- If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

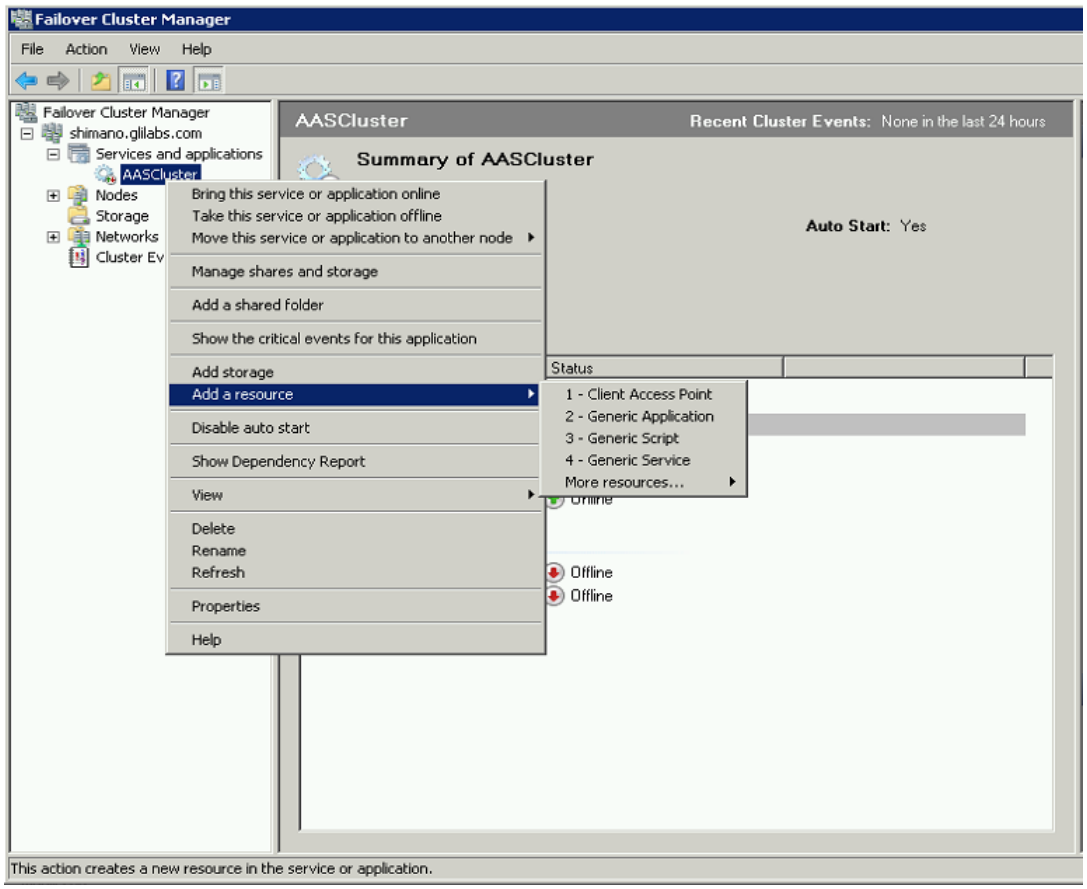
Note: *Use slashes(/) as a path separator.*

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

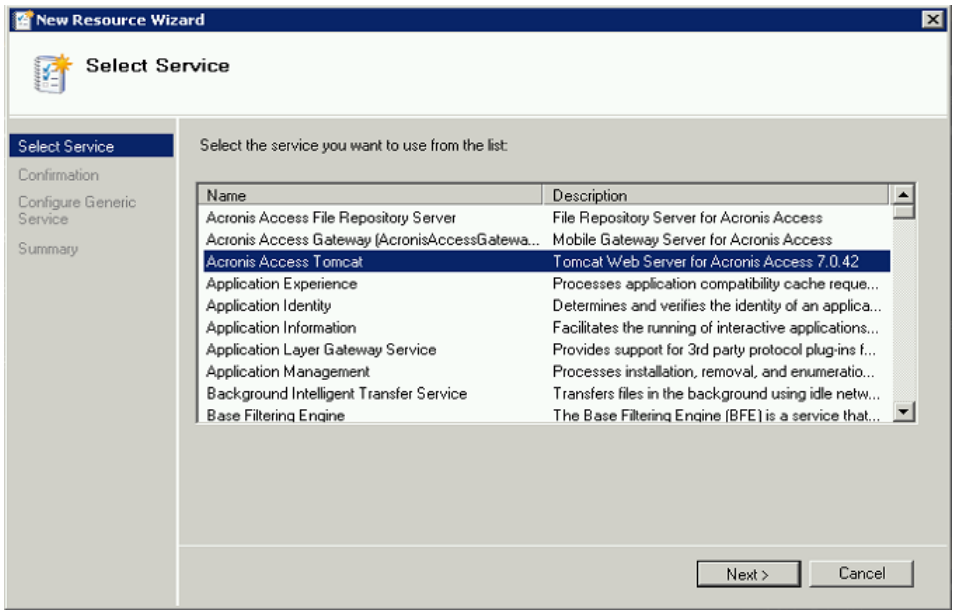
Complete the following procedure for each of the following services: AcronisAccessGateway, postgresql-x64-9.2 (this may be different depending on the version of PostgreSQL), AcronisAccessRepository and AcronisAccessTomcat

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



Copyright © Acronis International GmbH, 2002-2014

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



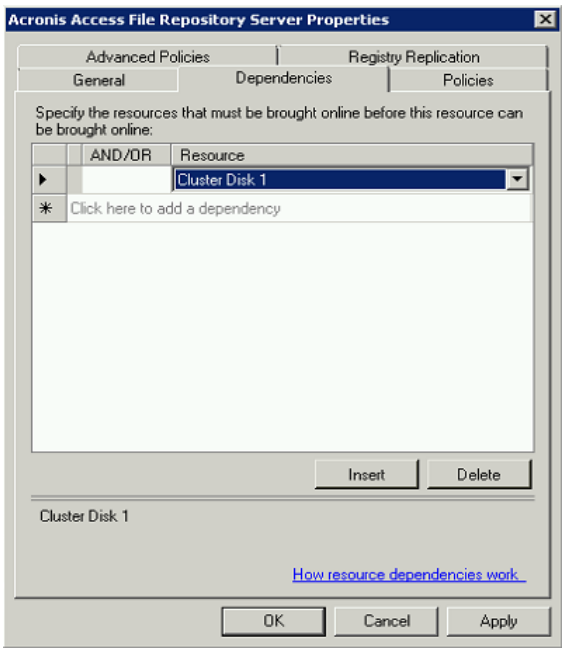
4. On the confirmation window press **Next**.
5. Press **Next** on the **Replicate Registry Settings** window.
6. On the summary window press **Finish**.

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.

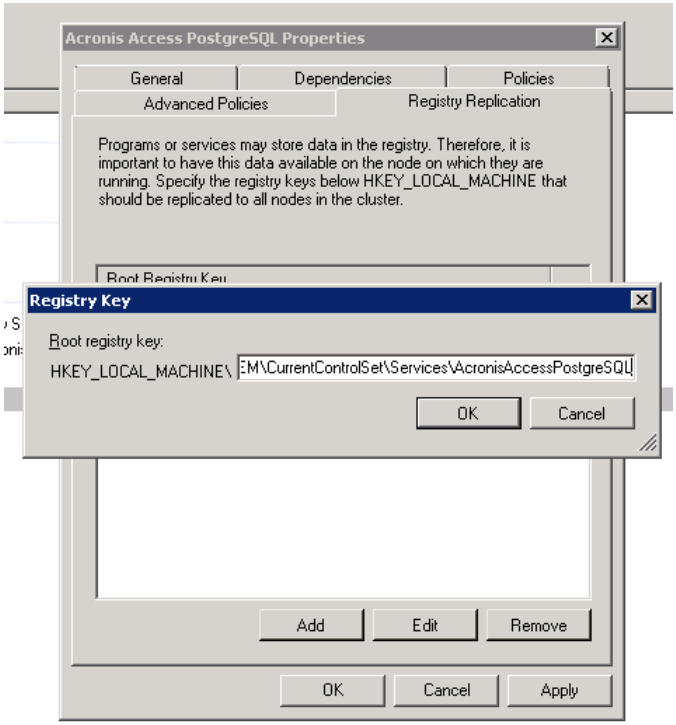


4. Press **Apply** and close the window.

Copyright © Acronis International GmbH, 2002-2014

For PostgreSQL also do the following:

1. Click on the **Registry Replication** tab.
2. Press **Add** and enter the following:
   `SYSTEM\CurrentControlSet\Services\postgresql-some version` (e.g. **postgresql-x64-9.2**)

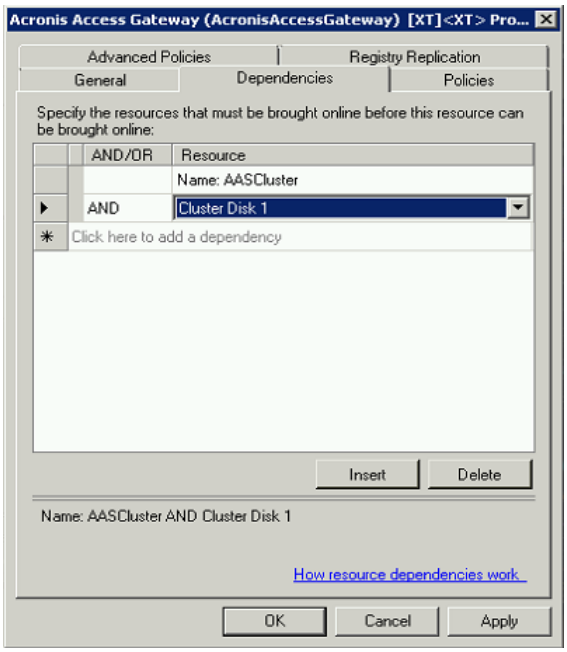


For the Acronis Access Gateway Server service do the following:

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

Copyright © Acronis International GmbH, 2002-2014

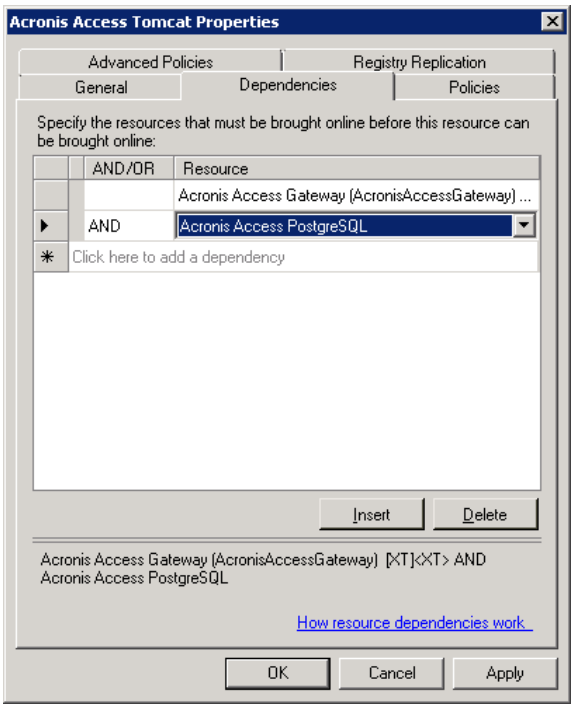
3. Click on **Resource** and select the shared disk you have added and the **Network Name** (this is the name of the Client access point).



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.

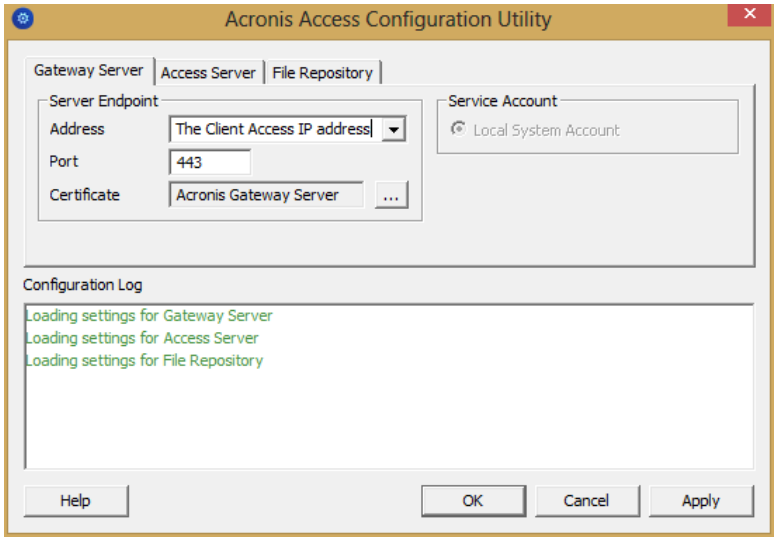


Note: *If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access Service group and set it as a dependency for the network name.*

Copyright © Acronis International GmbH, 2002-2014

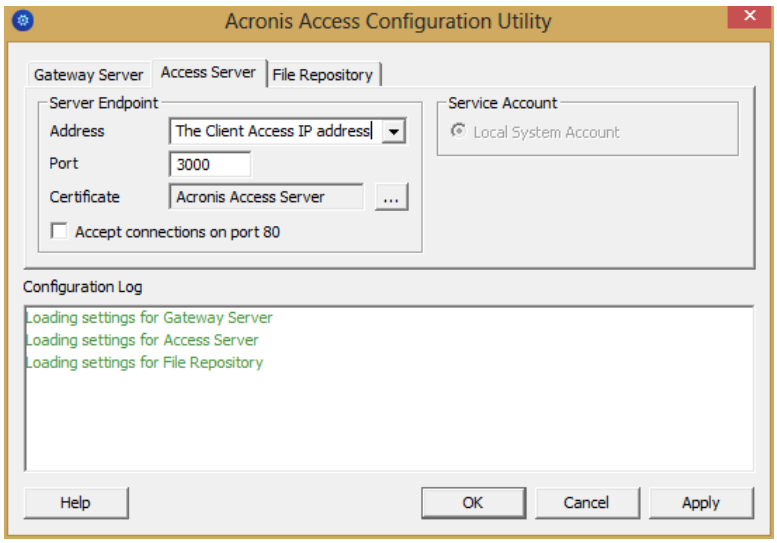
Bringing the service group online and using the Configuration Utility

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`**
   - 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.



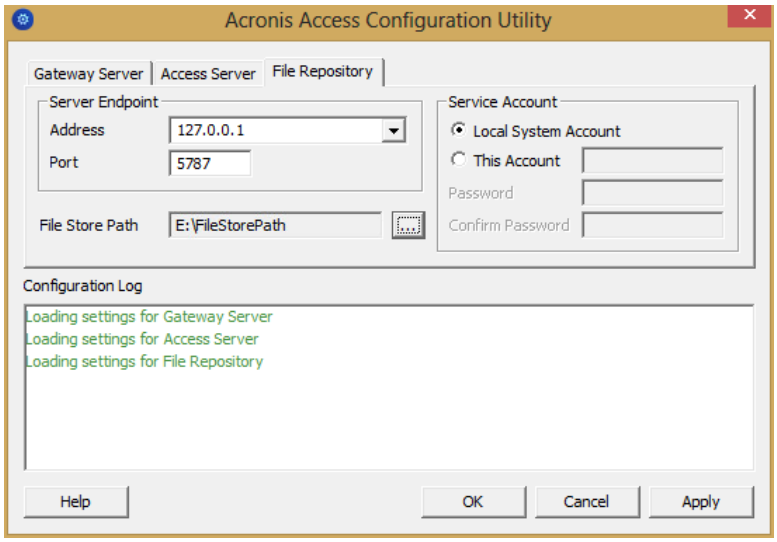
4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

***Note:** If **Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

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

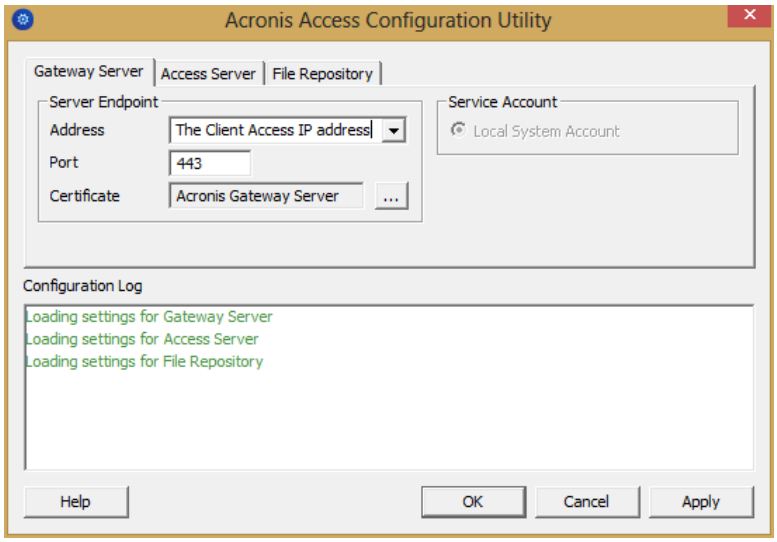
   Note: *You can copy the configured database.yml from the first node and paste it to the second node.*

   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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

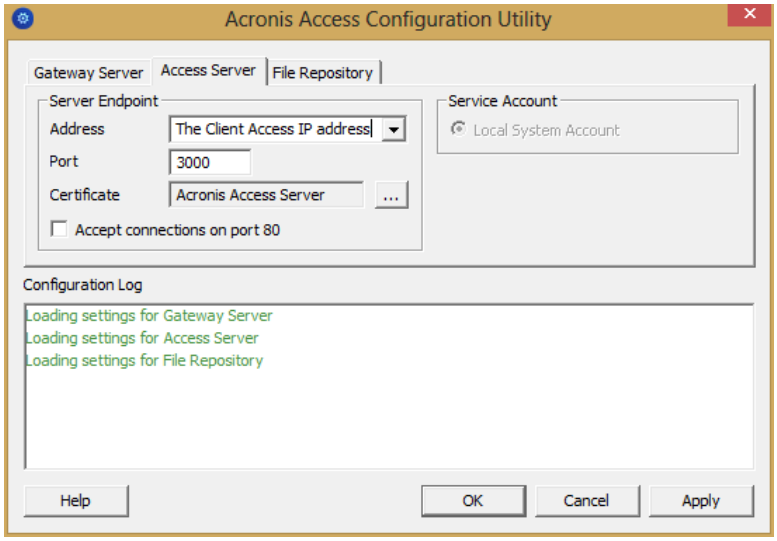
Copyright © Acronis International GmbH, 2002-2014

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



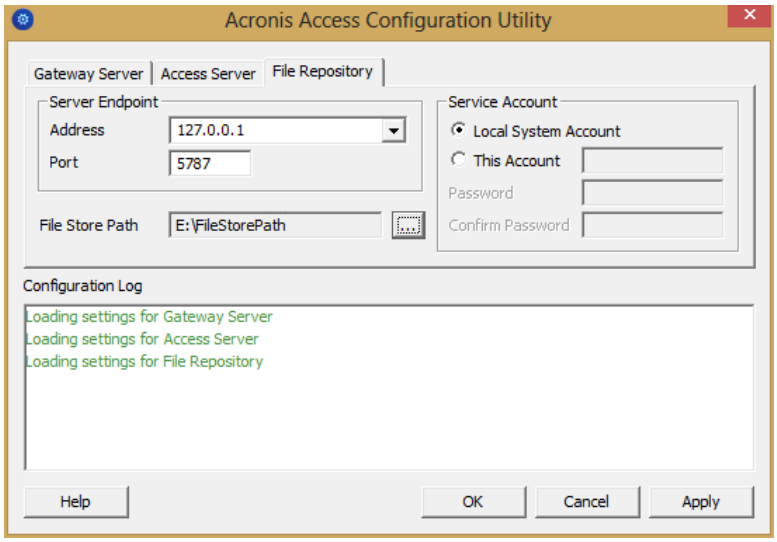
8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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.



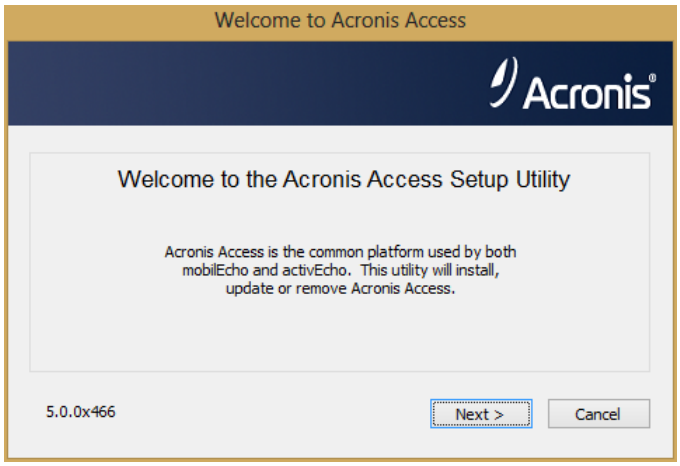
10. Click **OK** to complete the configuration and restart the services.

7.3.3 Upgrading a mobilEcho server on a Windows 2012 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.

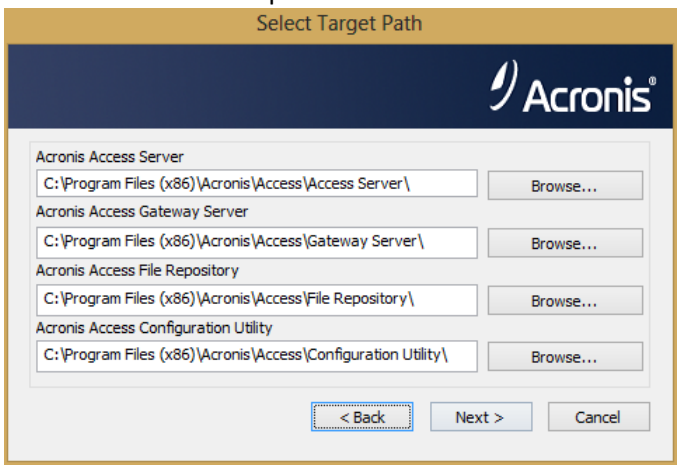


6. Press **Next** to begin.
7. Read and accept the license agreement.
8. Press **Install**.

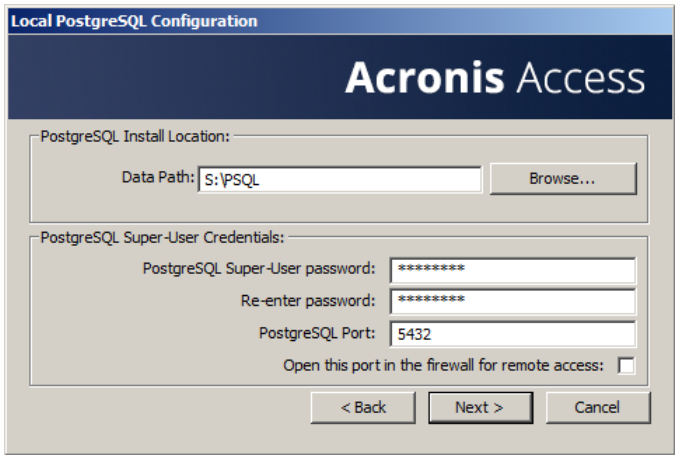
Copyright © Acronis International GmbH, 2002-2014

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 paths or select new ones for each component 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**, **mobilEcho_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\mobilEcho Server\ManagementUI\db\production.sqlite3

C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg

C:\Program Files (x86)\Group Logic\mobilEcho 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)\Acronis\Access\Gateway Server**

Copyright © Acronis International GmbH, 2002-2014

- If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_cluster/database/'`**).

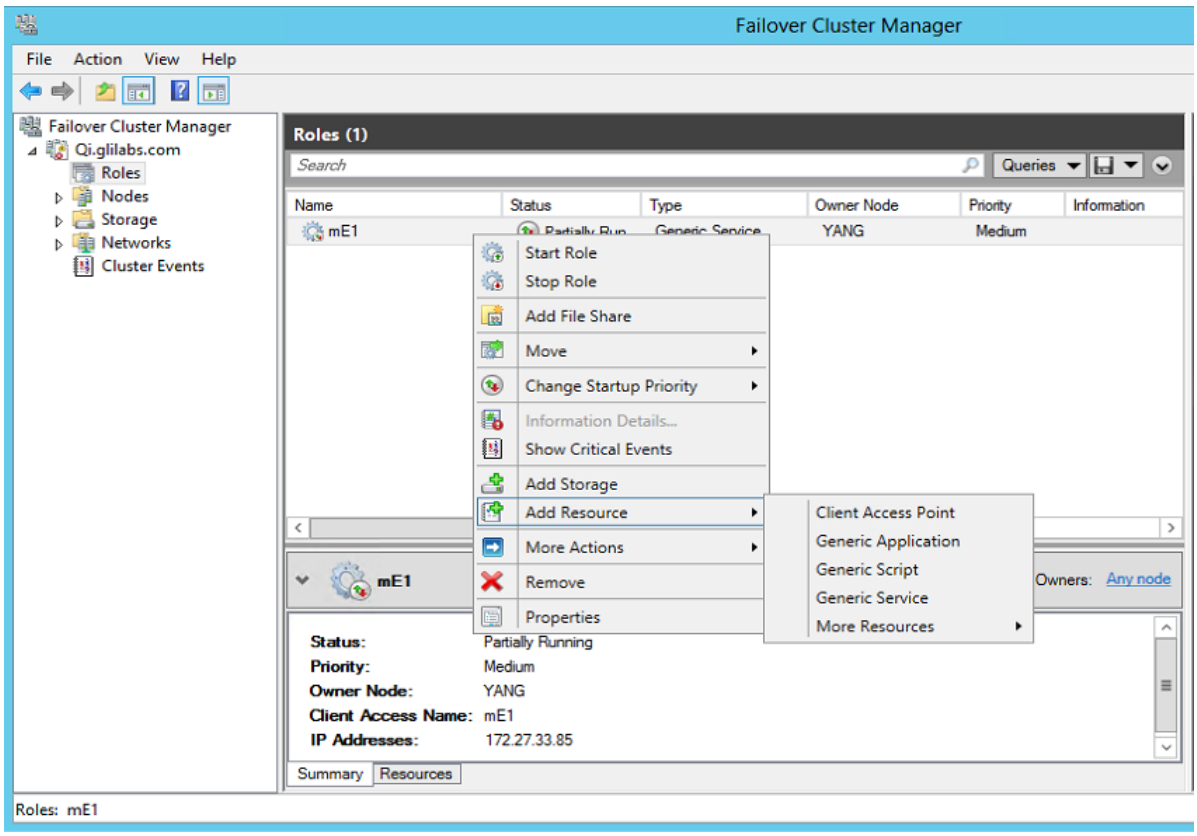
Note: *Use slashes(/) as a path separator.*

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

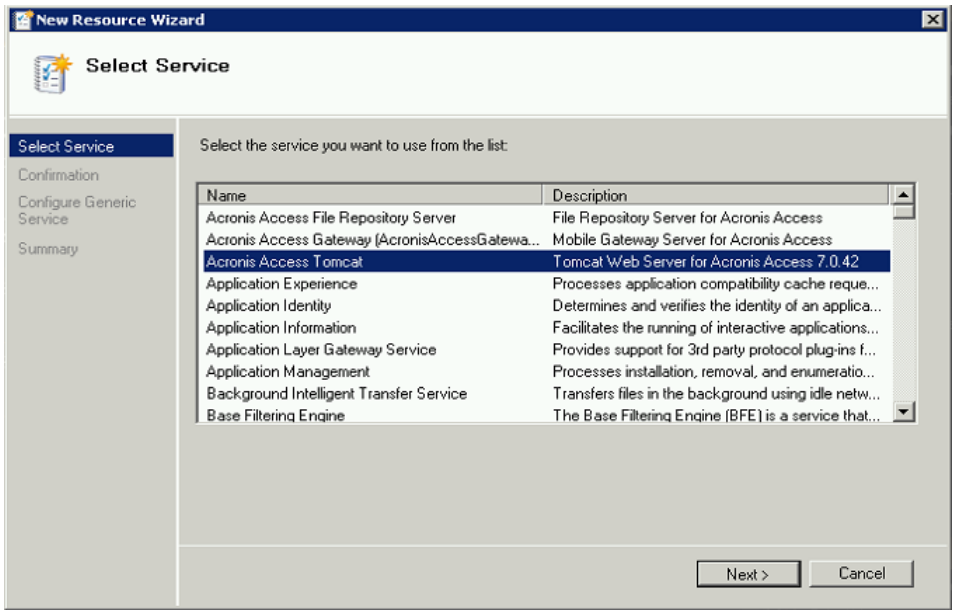
Complete the following procedure for each of the following services: AcronisAccessGateway, postgresql-x64-9.2 (this may be different depending on the version of PostgreSQL), AcronisAccessRepository and AcronisAccessTomcat

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



Copyright © Acronis International GmbH, 2002-2014

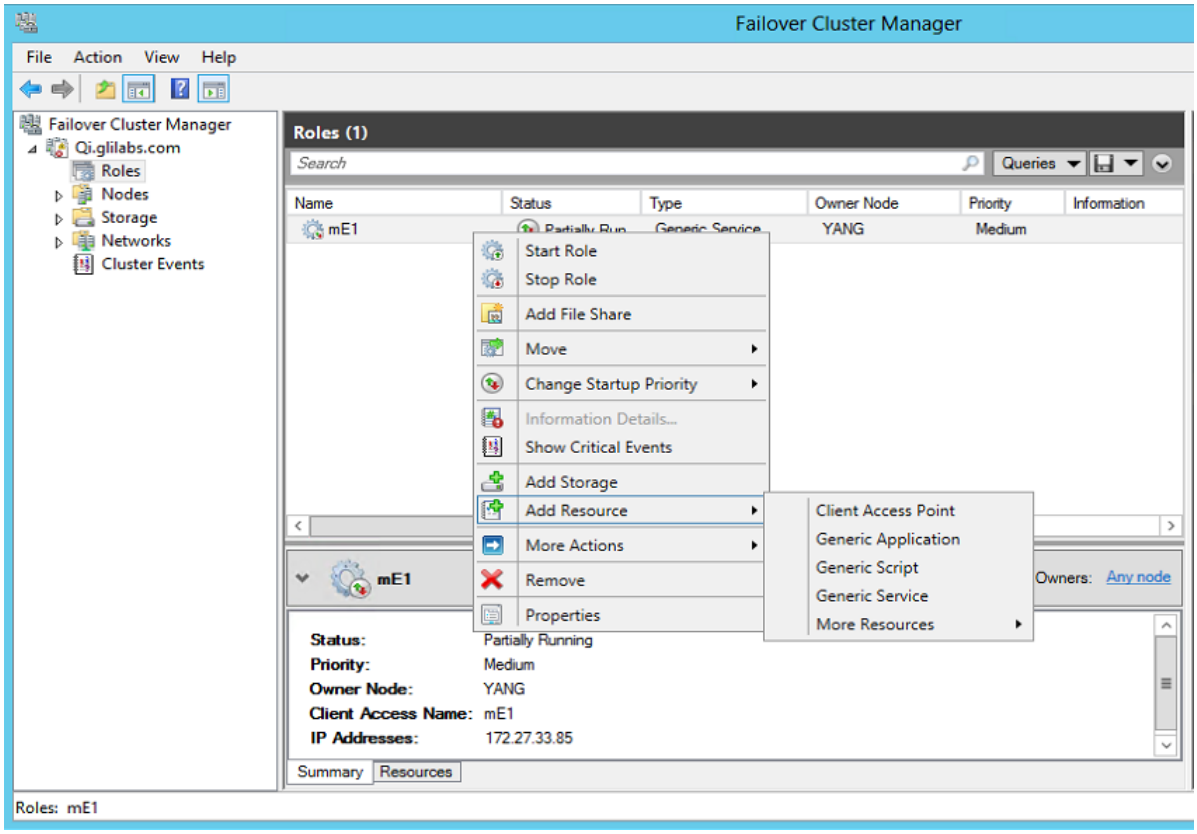
3. Select the proper service and press **Next**.



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

Setting an Access Point

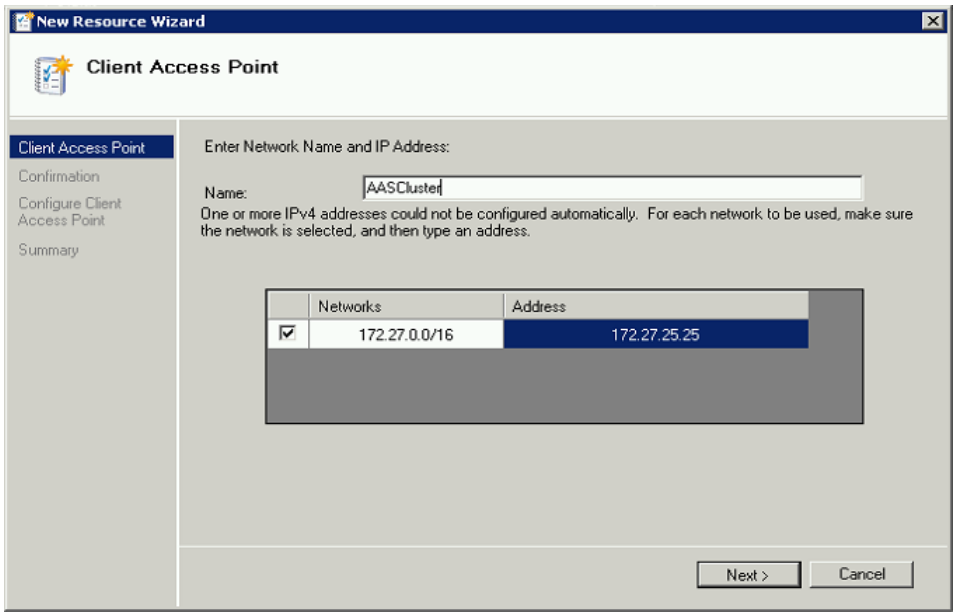
1. Right-click on the Acronis Access role and select **Add a resource**.
2. Select **Client Access Point**.



3. Enter a name for this access point.

Copyright © Acronis International GmbH, 2002-2014

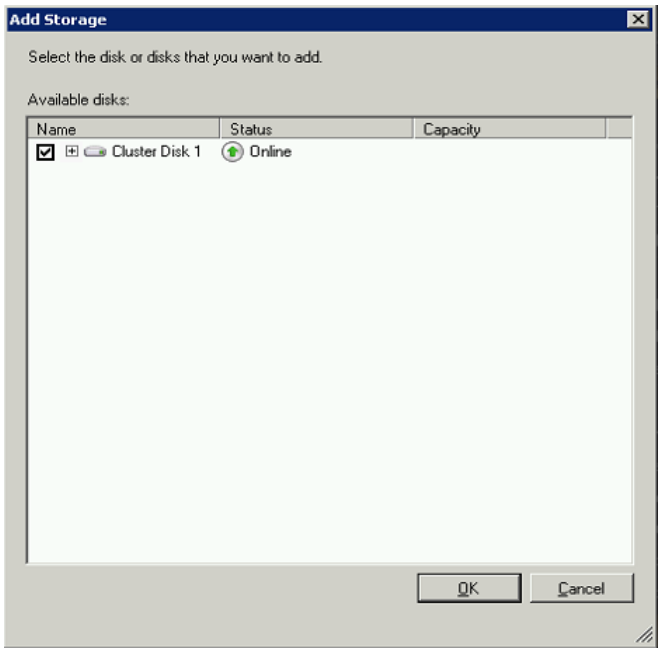
4. Select a network.



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

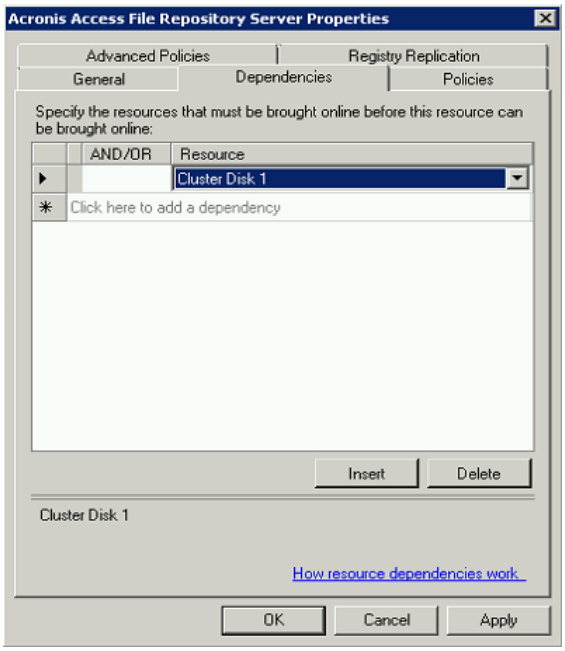
1. Select the Acronis Access role and click on the **Resources** tab

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

1. Right-click on the appropriate service and select **Properties**.

Copyright © Acronis International GmbH, 2002-2014

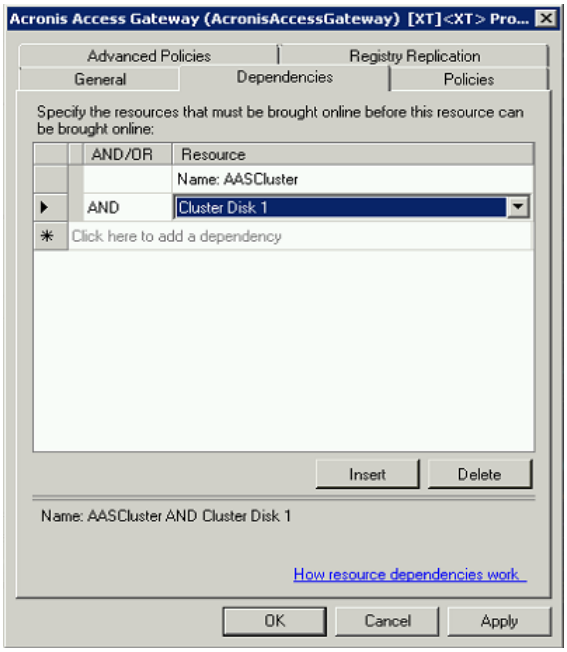
2. Click on the **Dependencies** tab.
3. Click on **Resource** and select the shared disk you have added.



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).



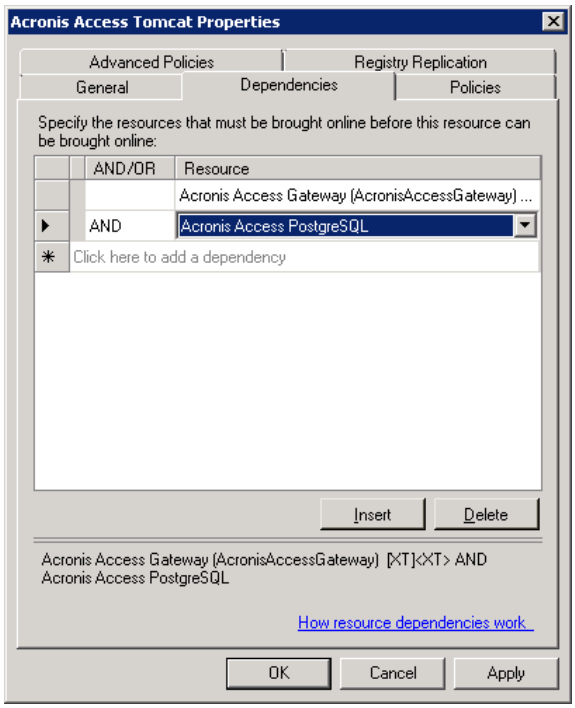
4. Press **Apply** and close the window.

Copyright © Acronis International GmbH, 2002-2014

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.*

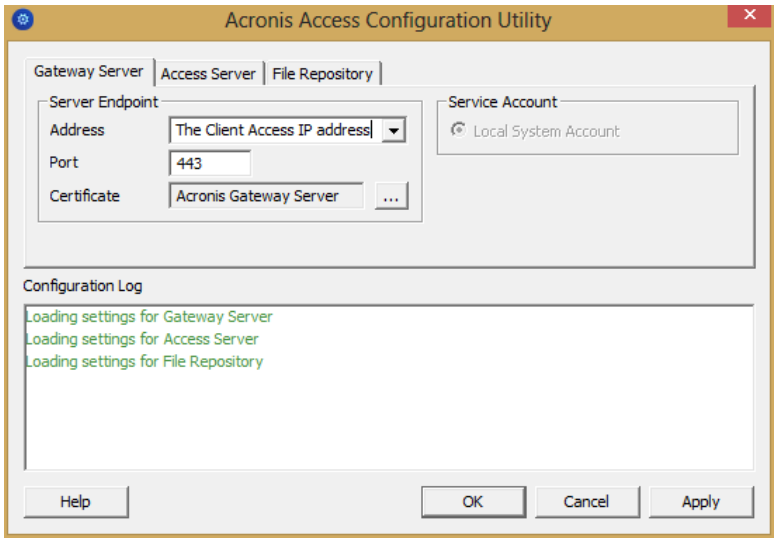


Starting the role and using the Configuration Utility

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`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**

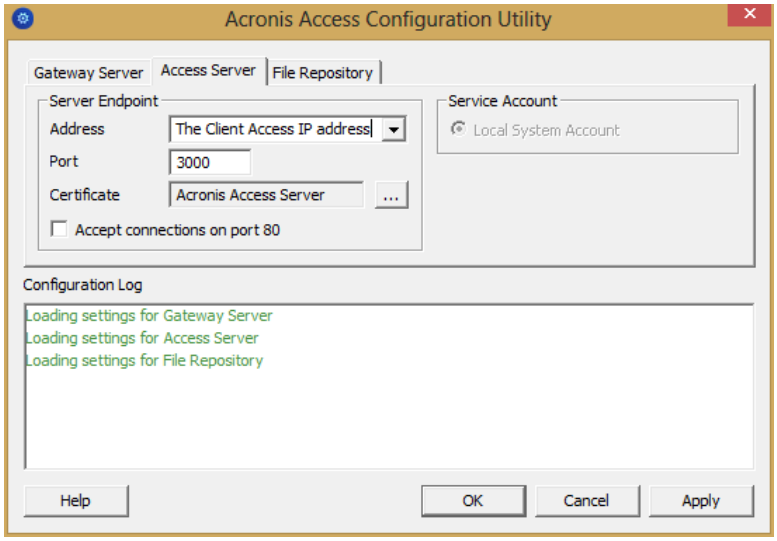
Copyright © Acronis International GmbH, 2002-2014

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



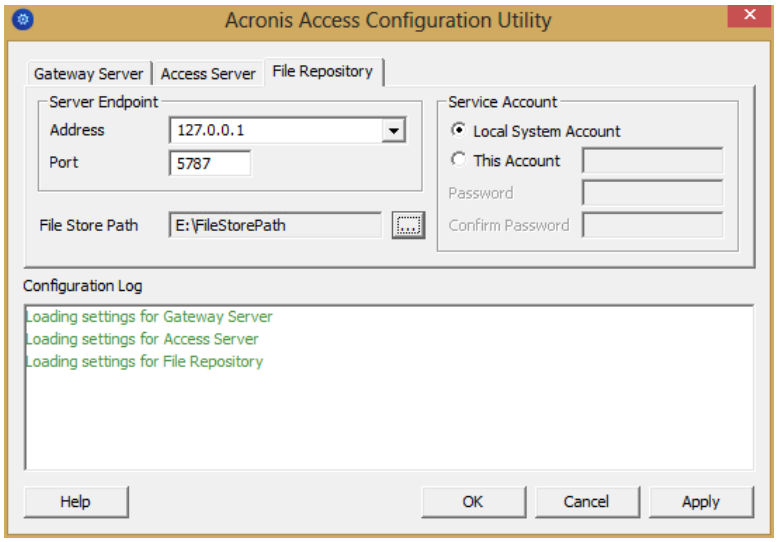
4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: *If* ***Accept connections on 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.*



Copyright © Acronis International GmbH, 2002-2014

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\`**
      - If you're upgrading, the path will be **`C:\Program Files (x86)\GroupLogic\mobilEcho 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:/mobilEcho_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.*

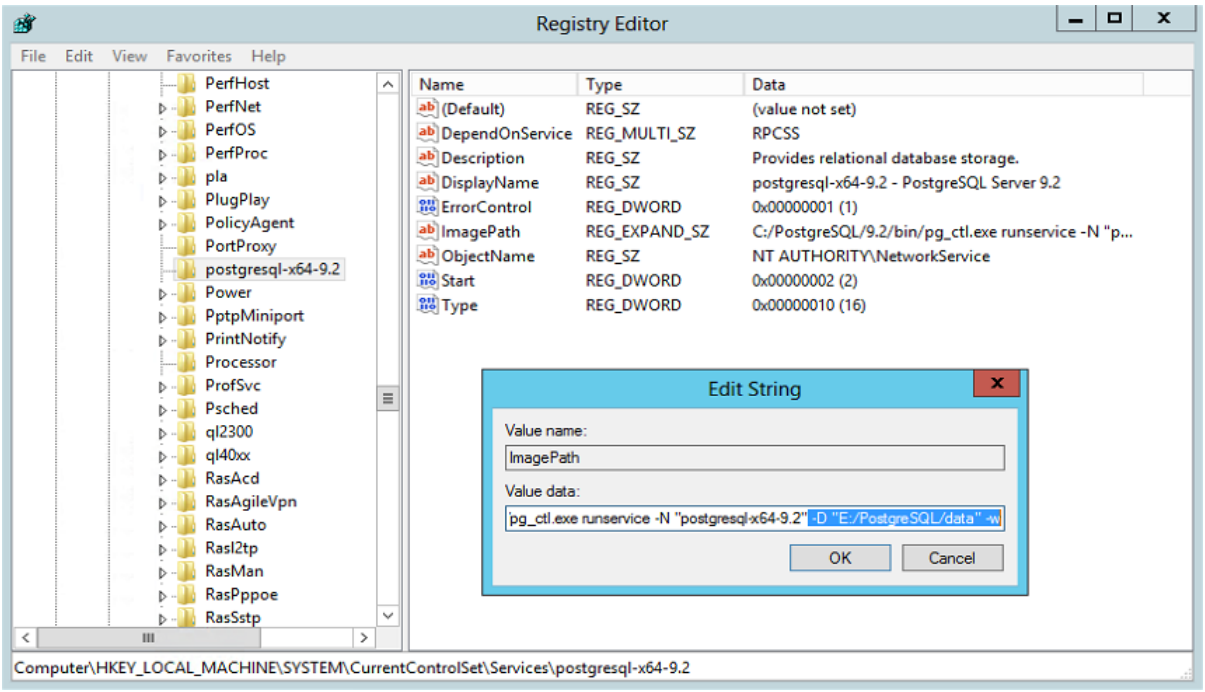
   Note: *The path should match the path set on the first node.*

For PostgreSQL you will need to manually replicate the registry:

1. Open **Regedit**.
2. Navigate to **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-some version\`** and open this key: **ImagePath**

Copyright © Acronis International GmbH, 2002-2014

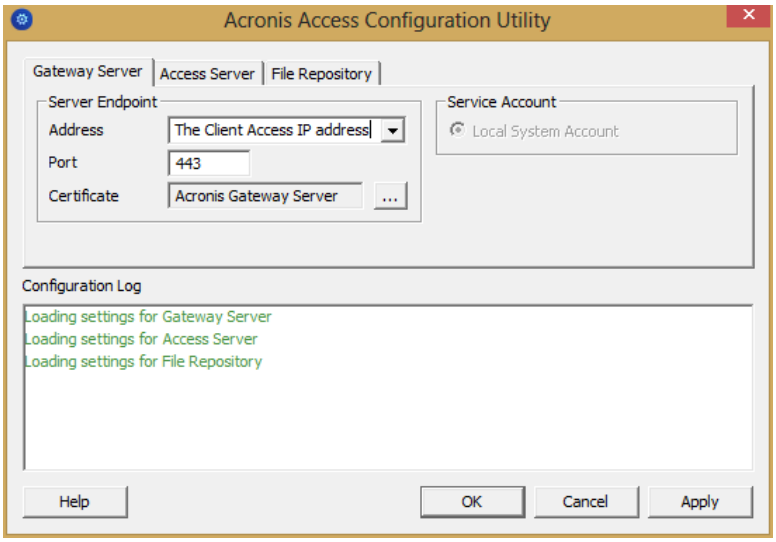
3. Change the value of the key to this: **`-D "The path you selected for the PostgreSQL data location" -w`** (e.g. **`-D "E:/PostgreSQL/data" -w`**)



4. Close **Regedit** and continue with the steps below.
5. Move the Acronis Access role to the second node.

Using the Configuration Utility on the second node

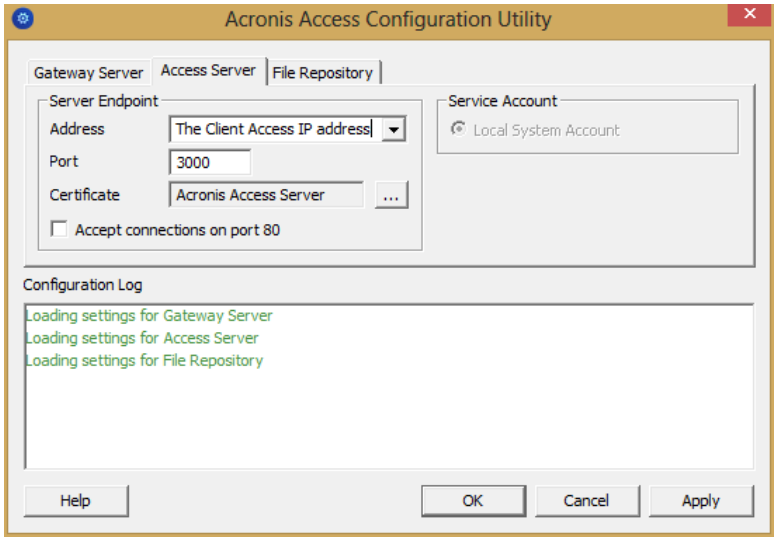
1. Launch the Configuration Utility.
   - On a clean install, this is generally located at **`C:\Program Files (x86)\Acronis\Access\Configuration Utility`**
   - On an upgrade from mobilEcho, this is generally located at **`C:\Program Files (x86)\GroupLogic\Configuration Utility`**
2. Configure the Acronis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



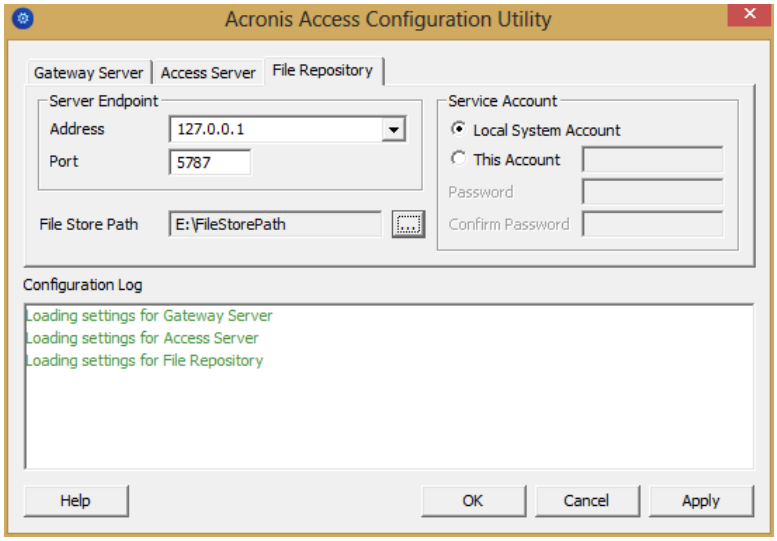
Copyright © Acronis International GmbH, 2002-2014

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

Note: *If* ***Accept connections on 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.

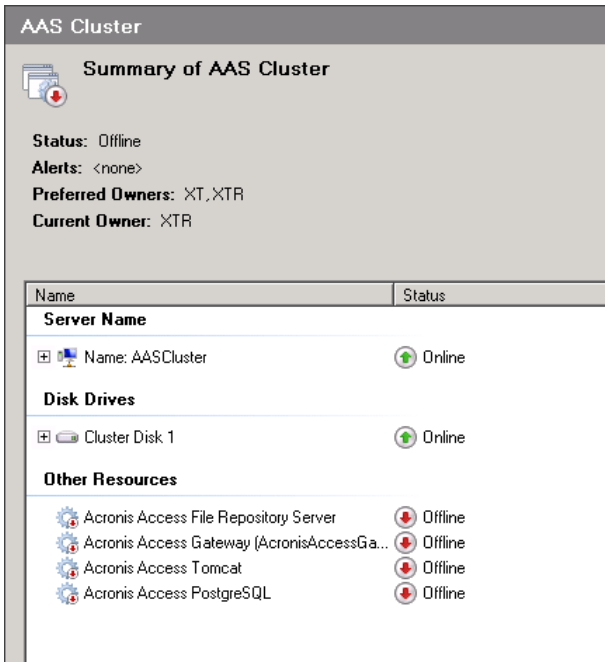
7.4 Upgrading Acronis Access on a Microsoft Failover Cluster

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

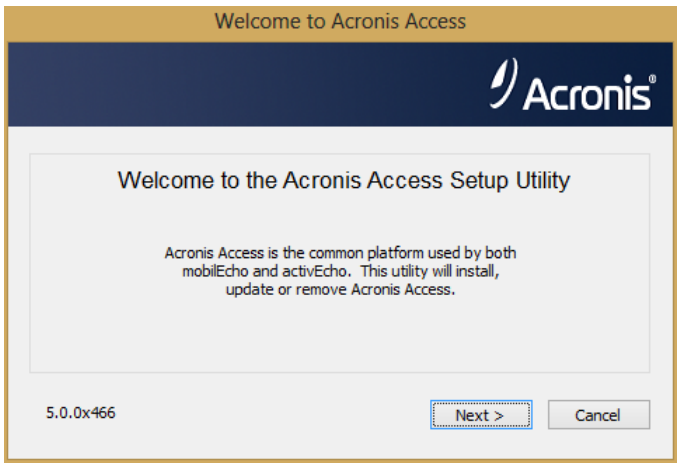
1. Go to the active node.
2. Open the **Cluster Administrator**/**Failover Cluster Manager**.

Copyright © Acronis International GmbH, 2002-2014

3. Stop all of the Acronis Access services (including **postgres-some-version**). The shared disk must be online.



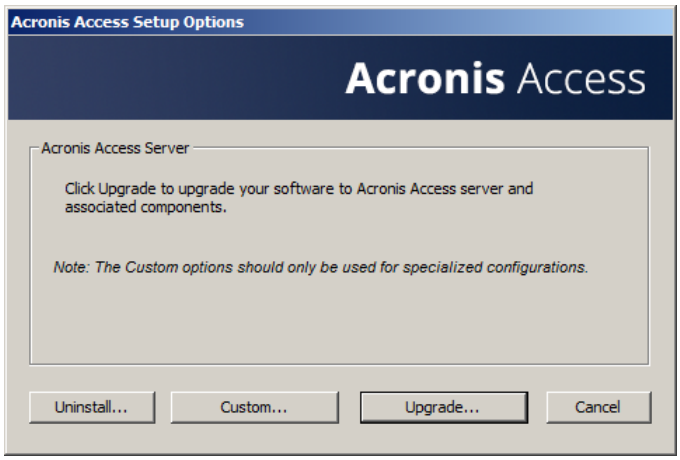
4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
5. Double-click on the installer executable.



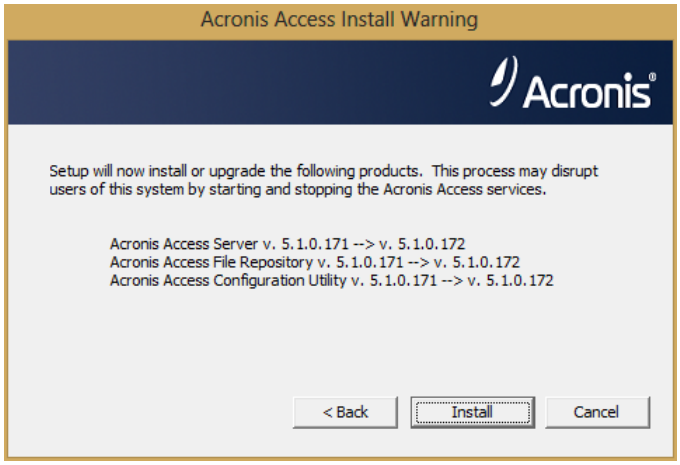
6. Press **Next** to begin.
7. Read and accept the license agreement.

Copyright © Acronis International GmbH, 2002-2014

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.

Copyright © Acronis International GmbH, 2002-2014

8 What's New

In this section

What's New in Acronis Access Server 228
What's New in the Acronis Access app 238
Previous Releases.....239

8.1 What's New in Acronis Access Server

Acronis Access 6.1

ENHANCEMENTS

- Web Services API for the Acronis Access Server administration.
- The Acronis Access audit log can now be configured to automatically export and purge old log entries. Preferences for export and purge settings can be set on the Audit Log => Settings page.
- New Acronis Access configuration summary tool to collect relevant server configuration details for sending to Acronis support.
- Improved login performance, through general performance improvements and by caching Active Directory group membership information.
- There is now an option for administrators to preview custom email templates before saving them.
- The Acronis Access server logo and color scheme can now be easily customized. Please consult the documentation here on how to customize your server: Customizing the web interface (p. 118).
- A new email template exists to customize the email that will be sent to newly invited administrators who do not have sync and share access.
- The Gateway Server logging tab can now be found under the “Edit” menu item instead of “Details”.
- When adding enrollment invitations, the search results will now show whether there are already enrolled devices for that user.
- Acronis Access will now email the original sender if emails sent on their behalf cannot be delivered because the recipient's email was invalid.
- Whitelists and blacklists can now be assigned to the default profile from the “Allowed Apps” page.
- Administrators can click a link on the LDAP settings page to force all cached LDAP information to be refreshed.
- Provisioned LDAP administrator groups can now be configured to allow sync and share access.
- Cluster group members can now be added via the cluster group’s menu.
- Support for Windows 8.1.
- Installer support for installations where PostgreSQL is located on a different server.
- Improved PostgreSQL installation process.
- Improved uninstallation process.
- Improved error reporting in web interface.

Copyright © Acronis International GmbH, 2002-2014

BUG FIXES

- The active session count will be refreshed when the Gateway Servers page is reloaded.
- Type-ahead search for selecting users to invite to shared files and folders is now supported on Internet Explorer 8.
- The Acronis Gateway Server service is now dependent on other key services so it should be assured to start properly when the server starts up.
- When a Cluster Group is disbanded, any policies that were using that Cluster Group as the Gateway Server used to access “My Network Folders” (locations added by the user) will be updated to instead use the last Gateway Server that was a member of the Cluster Group.
- Fixed an issue with email address filtering for enrolled users.
- Administrators should no longer get a fatal error page when changing the language setting after receiving an error message.
- Administrators should no longer encounter problems applying trial extensions after upgrading an expired server.
- LDAP sync and share users should now always be listed as LDAP once they have successfully authenticated, even if their email domain does not match the domains for LDAP authentication. Administrators can be added from LDAP even if the email domain is not included in domains from LDAP authentication.
- When administrators add new users or administrators, they will receive an immediate error message if adding a user with an invalid email address.
- Pending invitations will now be properly resolved to grant sync and share access to existing administrative users.
- Exports of the users table will now include the “Licensed" field.
- Sending a download link will now respect the blacklist and whitelist restrictions.
- Searching for new LDAP users to enroll should be much faster.
- New users who are in both a LDAP provisioned administrators group and a LDAP provisioned sync and share group will get the combined permissions.
- Mapping a home directory to an existing data source now works properly if the available data source uses the %USERNAME% wildcard.
- LDAP searches no longer display built-in groups which are not valid choices for group memberships.
- Slow home directory lookups will no longer cause mobile users to fail to enroll.
- Fixed an issue which could cause authenticating and accessing assigned sources with certificates on Windows 2003 R2 to fail.
- Unlicensed adhoc users are now properly restricted from connecting with the client to the server.
- Information in the Gateway Servers table is now updated immediately, instead of when you open the details tab for the server.
- The cosmetic “from" address in emails sent by Acronis Access now appears as the actual sender’s email address.
- Old Acronis Access serial numbers are now removed when a new base serial number is applied.
- The installer will no longer create multiple Gateway server entries in Programs and Features on upgrade.

Copyright © Acronis International GmbH, 2002-2014

Acronis Access 6.0.2

BUG FIXES

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

Acronis Access 6.0.1

ENHANCEMENTS

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

BUG FIXES

- The Access Desktop Client on Windows will no longer crash if the client downloads or uploads a huge number of files.
- Gateway servers will now be automatically contacted after they are added on fresh installations, so they can immediately be added to a cluster group or have self-provisioning enabled.
- Sync & Share functionality and data sources will now continue to work during the grace period after the license expires.
- Audit log licensing warning messages are now properly localized in all cases.
- Volumes will no longer become inaccessible if their parameters included the pipe ('|') symbol.
- Sending links or invitations from the Acronis Access mobile application will no longer fail when the device is configured for languages other than English, French, German or Japanese.
- The installer will no longer create multiple Gateway server entries in Programs and Features on upgrade for non-English installations.
- Fixed a bug where the Acronis Access Tomcat service would periodically fail to startup correctly and would need to be restarted in order to allow clients to connect.
- Fixed a bug where clients that are configured to require credentials "once per session" could prompt the user for a password when connecting to the management server after the server was upgraded from 4.x.

Copyright © Acronis International GmbH, 2002-2014

- Self-provisioned folders now can be added and removed successfully when the profile is configured to use either a gateway server or a cluster group, regardless of whether or not the server or cluster group is online.
- Policy priority order will be respected, so users will receive the highest priority group policy to which they are entitled.
- Clients who do not have sync and share enabled will no longer be incorrectly reported as “unmanaged” in the audit log.
- Files with Japanese or other characters in their filenames should no longer have the filenames changed when downloaded with Internet Explorer.
- Administrators should no longer see unresolvable errors when subscription licenses expire.
- The Access Desktop Client minimum version list now correctly includes 3.0 client versions, and will be honored for both old and new desktop clients.
- Home directories should no longer be inaccessible after upgrades from pre-5.0 versions of mobilEcho.
- Miscellaneous localization bug fixes.

Acronis Access 6.0.0

ENHANCEMENTS

- The mobilEcho and activEcho products have been combined into a single new product called Acronis Access Server. This changes the branding and product names in the mobile and desktop clients as well as the web application. Acronis Access Server 6.0 can be installed as an upgrade to mobilEcho and/or activEcho and existing licenses will continue to work. Customers are entitled to exchange their existing mobilEcho and/or activEcho license(s) for a new Acronis Access license that will enable the full functionality of the combined product. To request this upgrade, please **submit this web form**.
- Active Directory-based Administrator users are no longer required to have an email address assigned. Administrator users can also be added without configuring the Acronis Access Server for SMTP.
- A new checkbox is provided on the Server Settings that allows Sync & Share functionality to be turned on or off. By default when upgrading from mobilEcho to Acronis Access Server Sync & Share (formerly known as activEcho) is disabled.
- Active Directory distribution groups can now be invited to Sync & Share folders.
- Inviting many users to Sync & Share folders is now significantly faster.
- The Configuration Utility now includes more status / progress messages when it is setting up the server.
- The Configuration Utility will now generate an error if the repository is located on a remote network volume but the Repository Service is configured to run under the Local System account. The Repository Service needs to run under an account with permissions to the remote network volume.
- The Configuration Utility will now present an error if an SSL certificate is selected that does not have an embedded private key.
- Java has been upgraded to Version 7 Update 51.
- The Server Settings "Server Name" is now used as the title of the web site that appears to end users.
- The LDAP Cache refresh interval has been changed from 60 to 15 minutes.

Copyright © Acronis International GmbH, 2002-2014

- A new Advanced Setting for Gateway Servers has been added that, if enabled, users will authenticate with their UPN (example: username@domain.com). Otherwise, users will authenticate with their separate domain and usernames (example: domain\username). This is sometimes needed when authenticating to some federated scenarios, i.e., SharePoint 365.

BUG FIXES

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

Acronis Access 5.1.0

ENHANCEMENTS

- The Configuration Utility now provides the ability to control whether the Access Server should bind to HTTP port 80 and redirect automatically to the configured HTTPS port. Previously this was enabled by default, but now the administrator must enable it on clean installations.
- When editing email templates a new option allows the administrator to view the default value for the email subject.
- Users with mobilEcho 5.1 or later on iOS can now create their data sources directly from the application to access any file share or SharePoint location. Users enter UNC paths or SharePoint URLs from the client. New policy settings have been introduced on the management server to control whether clients are allowed to create these data sources, and which Gateway Servers are used for these requests.
- Multiple Gateway Servers can now share a common configuration via a Cluster Group. Changes to the settings and policies assigned to the Cluster Group are automatically pushed to all members of the Group. This will typically be used when multiple Gateway Servers are placed behind a load balancer for high availability.
- Gateway Servers now support authentication using Kerberos. This can be used to in scenarios using Kerberos Constrained Delegation to authenticate mobilEcho iOS clients through a reverse proxy using client certificates. It also can be used to authenticate mobile devices with client certificates using MobileIron AppTunnel. Note that when using this form of authentication, mobile clients cannot access activEcho shares.
- The required data sources are now automatically created when assigning home folders to a user or group policy. Previously administrators needed to manually create a data source for the server hosting the home directory.
- The address of a legacy Gateway Server can now be modified
- The policy exceptions for Android have been updated to reflect the functionality of the mobilEcho Android 3.1 client

BUG FIXES

- Exporting a large set of records from the audit log now completes significantly faster.

Copyright © Acronis International GmbH, 2002-2014

- Error messages from some dialogs are now properly cleared when the error condition is resolved.
- Only one instance of the Configuration Utility can now be run at a time.
- On Windows Server 2003, the uninstall process no longer reports that PostgreSQL was not installed by the Acronis Access Server installer.
- The Configuration Utility now generates an error if the Gateway Service is configured to bind to all address on a port and the Access Server on a specific address with the same port.
- By default on clean installs Tomcat is now configured to not listen for shutdown requests on port 8005. This prevents conflicts with other instances of Tomcat on a server. Because the Access Server Tomcat instance runs as a service, shutdown requests over network ports are not needed.
- Miscellaneous localization improvements.
- Improved performance displaying the log for non-administrative users
- Expired license notifications will no longer appear when activEcho is disabled via the Access Server administrator
- New users that receive an invite email now receive a message to set their initial password instead of changing the password
- The Upload New Files dialog no longer shows an extra field when using Internet Explorer 8 or 9
- The Windows Desktop Client will no longer re-upload content in some situations when the user's password expires and is re-entered
- Miscellaneous fixes to the file sync logic in the Desktop Client
- Removing a user or group policy with a custom home folder now properly removes the volume on the Gateway Server.
- Displaying Assigned Sources for a user now displays sources assigned to that user through their group memberships.
- Improved the ordering of the tabs in the Data Sources administration page.
- Changing a Gateway Server administration address no longer dismisses the edit dialog when clicking Apply.
- mobilEcho clients enrolling for management using client certificates will no longer fail periodically if the user was not already in the server's LDAP cache.
- Adding white space to Gateway Server addresses no longer prevents the Gateway Server from being properly managed.
- Notes in the Device Information dialog are now saved properly.
- When policies are disabled, they now appear grayed out in the policy list.
- On upgrade from mobilEcho Server 4.5 the mobilEcho users are now imported properly even if the wrong LDAP search base is entered in the configuration wizard.
- License keys starting with YD1 are now displayed properly as trials with an expiration date on the licensing page, instead of perpetual licenses.
- Enrollment email invitations now have proper links for Android clients.
- Editing SharePoint credentials for a Gateway Server is now disabled if the Gateway Server does not have a license supporting SharePoint connectivity.

Acronis Access 5.0.3

ENHANCEMENTS

Copyright © Acronis International GmbH, 2002-2014

- Acronis Access Server can now be installed on a Windows Failover Cluster, for Windows Server 2003 SP2, 2008/2008R2 and 2012/2012R2. Please see Installing Acronis Access on a cluster (p. 160) and Upgrading Acronis Access on a cluster (p. 196) for instructions on how to install or upgrade in this configuration.

BUG FIXES

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

Acronis Access 5.0.2

ENHANCEMENTS

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

BUG FIXES

- Localization improvements.
- Choosing to uninstall from the installer application now works on Windows Server 2003.
- Installer will now enforce that a minimum of 1GB of free disk space is available before installing.
- Upgrades from activEcho 2.7 now work properly on non-English PostgreSQL installations.
- Clients can now access data sources with a colon in their name.
- Upgrades from mobilEcho 4.5 now properly handle migrating SharePoint data sources.
- After an upgrade, the Assigned Sources tab in Data Sources now properly displays resources assigned to a user.
- Sorting the Active Users table by Policy or Idle Time no longer generates an error.
- Clients can now access Gateway Servers that are provisioned to be visible on clients and that have different addresses for client connections.
- Fixed a bug where home folders could fail to open in the mobilEcho client if the Access Server contained data sources with similar paths (for example "\\homes" and "\\homes2")

Acronis Access 5.0.1

Copyright © Acronis International GmbH, 2002-2014

BUG FIXES

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

  ActiveRecord::JDBCError: ERROR: value too long for type character varying(255): INSERT INTO "password_resets" ....
  Customers that have this condition can upgrade to this new version of the server and the problem will be resolved automatically.
- Fixed an issue that could cause some clients to go into restricted mode after the upgrade to mobilEcho 5.0.
- The management server data sources table now shows the Gateway Server's display name instead of IP address.

Acronis Access 5.0.0

ENHANCEMENTS

- Acronis Access Server is a new shared server platform used by both mobilEcho and activEcho. Both products now use the same shared backend infrastructure. Functionality for each product is determined and enabled based on licensing.
- New integrated platform installer. Acronis Access server, mobilEcho and activEcho are included in the installer. Installer run time installation options allow administrator to determine what elements are deployed.
- Acronis Access Server automatically installs Java JRE and the required Java Cryptographic Engine policy files.
- New Server Configuration Utility allows administrators to set base configuration options like binding to specific IP addresses and ports, handling local machine firewall rules,installation of SSL certificates.
- Acronis Access Server is localized in English, German, Japanese and French.
- New startup wizard simplifies initial configuration of the server
- Redesigned, updated user and management web interfaces, including responsive design withsupport for mobile devices.
- New paging tables support display, sorting and filtering of much larger sets of data.The log filtering has been improved, including filtering by typing partial user names, bymessage type, etc.
- Redesigned, easier to use Projects view for end users.
- activEcho Clients (Mac/Windows) have been localized in German, Japanese and French.
- Support for HTML5 drag and drop file uploading directly to the web interface. One or many files can be uploaded via Drag and Drop in a single operation.
- Improved file upload handling, including progress indicators in the web interface and the ability to cancel uploads.
- Folders can be downloaded as a ZIP file from the Projects view in the Web UI.
- Individual files can be shared with other users. Those users will get a link to download the files, which can be configured to expire.
- Sharing invitation dialogs now support type-ahead against both local users and users in Active Directory / LDAP.

Copyright © Acronis International GmbH, 2002-2014

- The previous revisions feature for finding / downloading / restoring previous versions of files has been redesigned and is more flexible. Previous revisions can be selected to be "made current".
- activEcho desktop clients (Mac/Windows) now show progress indicators files being synchronized.
- New "unsubscribe" button is available in folders shared to you.
- Sorting criteria chosen by the end user is now saved when browsing project folders.
- Event Notifications can now be configured globally as default settings for all shares. Users can override the defaults for individual shares.
- Notifications can now be configured to be sent when a file is downloaded / synced.
- activEcho clients on Windows now perform validation of SSL certificates using the built-in Windows certificate store. This improves compatibility with 3rd party certificate authorities.
- Improved user interface responsiveness for re-assigning content when there are 1000s of users in the system.
- The Amazon S3 access key no longer displayed in plain text on the administration pages.
- Improved page load times when there are many users and/or files, especially when quotas are in use.
- Improved support for email invitations using different formats of email addresses.
- Wildcards can now be used in domains for sharing black and whitelists.
- Administrators can now globally hide the checkbox "Allow collaborators to invite other collaborators".
- New Administration mode toggles between a user's individual project / log views and the administration console.
- mobilEcho client management has been fully integrated into a common web administration interface. This can be used for managing mobile clients for activEcho, or if a mobilEcho license is provided the single console can manage all mobilEcho and activEcho functions.
- Users list can now be exported.
- The mobilEcho Client Management Server is integrated with Acronis Access Server and built on Apache Tomcat and PostgreSQL database for improved scalability and resilience.
- The mobilEcho Administrator previously used to manage individual mobilEcho servers has been removed; Access Gateway Servers (formerly mobilEcho File Access Servers) are now managed directly within the Acronis Access Server web administration user interface.
- mobilEcho Client Management Server configuration file has been removed; configuration settings previously in the configuration file are automatically migrated and are now managed through the Acronis Access Server web administration user interface.
- Configuration of data sources (formerly assigned "Folders") to be shared to mobile devices has been redesigned.
- New "Assigned Sources" capability allows administrators to get a report of all of the assigned resources that a particular Active Directory user or group will receive.
- Audit logging can be enabled to report on mobile user activity across multiple Acronis Access Gateway Servers.
- Administrators can now be granted different permissions for administrative activity, including managing users, data sources, mobile policies or viewing the audit log. This can be based on individual users and/or membership in Active Directory groups.
- Devices operations such as remote wipe or removing devices from the device list can now be performed in batches.
- A catch-all "default" policy can be configured which applies to all users that don't match configured Active Directory user or group policies.

Copyright © Acronis International GmbH, 2002-2014

- New policy options allow specification that content on the device within the "My Files" and "File Inbox" folders expires and is removed after a certain amount of time.
- When sending an enrollment invitation to an Active Directory group, users who are already enrolled through another group can be filtered out.
- A warning is presented if a user is invited for enrollment but does not match any existing user/group policy.
- The devices table now lists the user or group policy in use for each device.
- Cached Active Directory / LDAP information about users is now updated periodically in the background.
- Content searching is now available against remote Windows file shares running Windows Search.
- A policy cannot be be deleted if a device is being managed by it
- mobilEcho enrollment invitation templates can be modified directly from within the web administration console. Multiple languages for each template are supported.
- A new token is available in the enrollment invitation templates to include the Active Directory user's Display Name.
- Devices list and device details screen now show whether devices are managed by Good Dynamics or MobileIron AppConnect.
- Support for authenticating to the web administration console using SSLv2 has been deprecated by the transition to the Apache Tomcat web server.
- Support for trace logging and performance monitoring via New Relic.

BUG FIXES

- Improved support for exporting Unicode characters to TXT or CSV files.
- Folders that cannot be shared no longer have the Invite... option.
- Users can now remove themselves from the share even if they do not have permission to invite other users to the share.
- If a file or folder cannot be downloaded to a Windows client because the name is too long, unchecking the Sync to devices option in the web interface now resolves the error on the client by removing the entire shared folder.
- activEcho clients properly handle error when uploading files and user is out of quota space.
- Users can now be deleted even if they are listed on the black list.
- Files can be uploaded to the repository when encryption is disabled.
- Home directory configuration is now retrieved properly when LDAP is configured to use the global catalog.
- Improved handling of Active Directory lookups when trailing spaces are used.
- The "Enrolled at" date is now formatted properly when exporting to .CSV file.
- Improved support for displaying Unicode via the web administration user interface.
- SharePoint folders ending with a space can now be enumerated by clients.
- SharePoint libraries that have extra slashes now support file deletion and copy properly.

Copyright © Acronis International GmbH, 2002-2014

8.2 What's New in the Acronis Access app

Access Mobile Client 6.1

ENHANCEMENTS

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

Access Mobile Client 6.0.1

BUG FIXES

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

Access Mobile Client 6.0

ENHANCEMENTS

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

mobilEcho 5.1

ENHANCEMENTS

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

mobilEcho 5.0

ENHANCEMENTS

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

Copyright © Acronis International GmbH, 2002-2014

mobilEcho 4.5.2

ENHANCEMENTS

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

mobilEcho 4.5.1

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

mobilEcho 4.5

ENHANCEMENTS

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

8.3 Previous Releases

8.3.1 activEcho

Acronis Access Server 6.0

The mobilEcho and activEcho products have been combined into a single new product called Acronis Access Server. This changes the branding and product names in the mobile and desktop clients as

Copyright © Acronis International GmbH, 2002-2014

well as the web application. Acronis Access Server 6.0 can be installed as an upgrade to mobilEcho and/or activEcho and existing licenses will continue to work. Customers are entitled to exchange their existing mobilEcho and/or activEcho license(s) for a new Acronis Access license that will enable the full functionality of the combined product. To request this upgrade, please **submit this web form**. For the latest information, please visit the What' New in Acronis Access Server (p. 228) article.

activEcho 5.1.0

BUG FIXES

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

activEcho 5.0.3

BUG FIXES

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

activEcho 5.0.2

ENHANCEMENTS

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

BUG FIXES

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

activEcho 5.0.1

- No changes.

activEcho 5.0.0

ENHANCEMENTS

- Redesigned, easier to use Projects view for end users.
- activEcho Clients (Mac/Windows) have been localized in German, Japanese and French.
- Support for HTML5 drag and drop file uploading directly to the web interface. One or many files can be uploaded via Drag and Drop in a single operation.

Copyright © Acronis International GmbH, 2002-2014

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

BUG FIXES

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

Copyright © Acronis International GmbH, 2002-2014

activEcho 2.7.3 (Released: June 2013)

ENHANCEMENTS:

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

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

BUG FIXES:

Pending users can now be deleted without error.

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

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

activEcho 2.7.2 (Released: May 2013)

BUG FIXES:

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

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

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

activEcho 2.7.1 (Released: April 2013)

ENHANCEMENTS:

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

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

Improved load speed of users page by caching content usage.

BUG FIXES:

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

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

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

Copyright © Acronis International GmbH, 2002-2014

activEcho 2.7.0 (Released: February 2013)

ENHANCEMENTS:

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

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

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

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

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

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

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

The Projects tab now supports pagination, sorting, filtering.

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

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

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

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

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

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

User proxy AD objects can now successfully authenticate to activEcho.

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

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

```
<%= @root_web_address %>

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

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


Copyright © Acronis International GmbH, 2002-2014

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

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

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

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

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

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

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

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

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

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

Customers not needing redirection refer to the online documentation:

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

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

Filtering options have been added to projects page sidebar.

Improved shutdown speed of the Mac and Windows sync clients.

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

Upgraded default version of PostgreSQL to 9.2.1.

Validation of support for Windows 2012 Server.

Validation of support for Java 7 update 15.

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

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

BUG FIXES:

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

error and could no longer sync.

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

 Copyright © Acronis International GmbH, 2002-2014

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

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

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

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

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

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

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

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

Fixed various case-sensitivity bugs with LDAP authentication.

Adding trial server licenses will no longer occasionally fail.

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

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

Users can no longer share deleted folders.

Improved error handling for SMTP errors.

Miscellaneous other bug fixes.

activEcho 2.6.1 (Released: October 2012)

BUG FIXES:

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

activEcho 2.6.0 (Released: October 2012)

ENHANCEMENTS:

Log and Users tabs support pagination, sorting, filtering.

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

Log tab provides new start and end date display filters.

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

Copyright © Acronis International GmbH, 2002-2014

Quotas can now be defined specifically for administrative users.

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

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

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

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

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

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

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

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

Improved diagnostic logging provided in the file repository service.

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

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

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

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

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

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

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

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

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

to

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

Validation of support for Java 7 update 7.

BUG FIXES:

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

Copyright © Acronis International GmbH, 2002-2014

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

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

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

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

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

Miscellaneous other bug fixes.

activEcho 2.5.1 (Released: July 2012)

ENHANCEMENTS:

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

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

Uploading and downloading of files via mobile devices is faster.

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

Support for Mac OS X 10.8 "Mountain Lion"

BUG FIXES:

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

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

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

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

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

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

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

Miscellaneous other bug fixes

activEcho 2.5.0 (Released: July 2012)

Copyright © Acronis International GmbH, 2002-2014

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

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

ENHANCEMENTS:

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

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

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

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

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

activEcho clients support pausing / resuming syncing.

Syncing files to Mac OS X clients is significantly faster.

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

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

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

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

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

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

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

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

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

Web log view now has a reset filters button.

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

BUG FIXES:

Copyright © Acronis International GmbH, 2002-2014

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

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

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

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

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

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

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

Miscellaneous bug fixing in desktop syncing.

activEcho 2.1.1 (Released: June 2012)

ENHANCEMENTS:

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

Improved LDAP performance.

BUG FIXES:

Improved authentication against LDAP to avoid timeouts against large catalogs.

activEcho 2.1.0 (Released: May 2012)

ENHANCEMENTS:

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

Customizeable email templates.

Export log to TXT, CSV, or XML files.

Improved, administrator configurable trace logging for diagnostics.

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

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

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

More than one email address can be provided for notifications.

Support for 64-bit Java installations.

Improved LDAP performance.

Copyright © Acronis International GmbH, 2002-2014

Miscellaneous usability enhancements.

BUG FIXES:

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

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

Miscellaneous bug fixes in desktop syncing.

activEcho 2.0.2 (Released: March 2012)

BUG FIXES:

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

Various bug fixes in desktop syncing.

Bug fixes in activEcho server installer to fix future upgrades.

activEcho 2.0.1 (Released: March 2012)

BUG FIXES:

Improvements to the server administration user experience.

Various bug fixes in desktop syncing.

Improvements to the client installer upgrade process.

activEcho 2.0.0 (Released: February 2012)

Initial release

8.3.2 mobilEcho

Acronis Access Server 6.0

The mobilEcho and activEcho products have been combined into a single new product called Acronis Access Server. This changes the branding and product names in the mobile and desktop clients as well as the web application. Acronis Access Server 6.0 can be installed as an upgrade to mobilEcho and/or activEcho and existing licenses will continue to work. Customers are entitled to exchange their existing mobilEcho and/or activEcho license(s) for a new Acronis Access license that will enable the full functionality of the combined product. To request this upgrade, please **submit this web form**. For the latest information, please visit the What' New in Acronis Access Server (p. 228) article.

mobilEcho 5.1.0

 Copyright © Acronis International GmbH, 2002-2014

ENHANCEMENTS

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

BUG FIXES

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

Copyright © Acronis International GmbH, 2002-2014

mobilEcho 5.0.3

BUG FIXES

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

mobilEcho 5.0.2

ENHANCEMENTS

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

BUG FIXES

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

mobilEcho 5.0.1

BUG FIXES

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

  ActiveRecord::JDBCError: ERROR: value too long for type character varying(255): INSERT INTO "password_resets" ....
  Customers that have this condition can upgrade to this new version of the server and the problem will be resolved automatically.
- Fixed an issue that could cause some clients to go into restricted mode after the upgrade to mobilEcho 5.0.
- The management server data sources table now shows the Gateway Server's display name instead of IP address.

Copyright © Acronis International GmbH, 2002-2014

mobilEcho 5.0

ENHANCEMENTS

- The mobilEcho Client Management Server is integrated with Acronis Access Server and built on Apache Tomcat and PostgreSQL database for improved scalability and resilience.
- The mobilEcho Administrator previously used to manage individual mobilEcho servers has been removed; Access Gateway Servers (formerly mobilEcho File Access Servers) are now managed directly within the Acronis Access Server web administration user interface.
- mobilEcho Client Management Server configuration file has been removed; configuration settings previously in the configuration file are automatically migrated and are now managed through the Acronis Access Server web administration user interface.
- Configuration of data sources (formerly assigned "Folders") to be shared to mobile devices has been redesigned.
- New "Assigned Sources" capability allows administrators to get a report of all of the assigned resources that a particular Active Directory user or group will receive.
- Audit logging can be enabled to report on mobile user activity across multiple Acronis Access Gateway Servers.
- Administrators can now be granted different permissions for administrative activity, including managing users, data sources, mobile policies or viewing the audit log. This can be based on individual users and/or membership in Active Directory groups.
- Devices operations such as remote wipe or removing devices from the device list can now be performed in batches.
- A catch-all "default" policy can be configured which applies to all users that don't match configured Active Directory user or group policies.
- New policy options allow specification that content on the device within the "My Files" and "File Inbox" folders expires and is removed after a certain amount of time.
- When sending an enrollment invitation to an Active Directory group, users who are already enrolled through another group can be filtered out.
- A warning is presented if a user is invited for enrollment but does not match any existing user/group policy.
- The devices table now lists the user or group policy in use for each device.
- Cached Active Directory / LDAP information about users is now updated periodically in the background.
- Content searching is now available against remote Windows file shares running Windows Search.
- A policy cannot be be deleted if a device is being managed by it
- mobilEcho enrollment invitation templates can be modified directly from within the web administration console. Multiple languages for each template are supported.
- A new token is available in the enrollment invitation templates to include the Active Directory user's Display Name.
- Devices list and device details screen now show whether devices are managed by Good Dynamics or MobileIron AppConnect.
- Support for authenticating to the web administration console using SSLv2 has been deprecated by the transition to the Apache Tomcat web server.
- Support for trace logging and performance monitoring via New Relic.

Copyright © Acronis International GmbH, 2002-2014

BUG FIXES

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

mobilEcho 4.5.2 (Released: October 2013)

ENHANCEMENTS:

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

mobilEcho 4.5.1 (Released: September 2013)

ENHANCEMENTS:

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

BUG FIXES:

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

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

mobilEcho 4.5 (Released: August 2013)

ENHANCEMENTS:

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

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

Added support for client certificate authentication to mobilEcho file servers.

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

Copyright © Acronis International GmbH, 2002-2014

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

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

BUG FIXES:

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

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

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

mobilEcho 4.3.2 (Released: April 2013)

BUG FIXES:

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

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

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

mobilEcho 4.3.1 (Released: April 2013)

ENHANCEMENTS:

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

BUG FIXES:

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

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

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

Copyright © Acronis International GmbH, 2002-2014

mobilEcho 4.3 (Released: March 2013)

ENHANCEMENTS:

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

BUG FIXES:

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

Fixed an issue where the mobilEcho server's memory usage could increase if the "mobilEcho Administrator" was left open for a long period of time.

Fixed an issue where the client would fail to show an error or would show an incorrect error message if the user's AD account password had expired, or the account was locked out or disabled.

Fixed an issue where the server upgrade process could fail if mobilEcho had been installed to a non-system drive.

Fixed an issue where a JavaScript error would occur each time a user or group profile was added via the mobilEcho Client Management web console when using IE8.

mobilEcho 4.2 (Released: February 2013)

ENHANCEMENTS:

mobilEcho 4.2 servers now support mobilEcho 4.2 clients localized in German, French and Japanese. The 4.2 server will ensure that these clients receive server error messages in their local language. In addition, the mobilecho_manager_intl.cfg file contains settings to configure the client enrollment invitation email subjects in these three languages.

The mobilEcho Client Management service will now automatically detect crashes in the client management web application and stop the service so that administrators can properly detect these errors. Additional error information will be written to the ManagementUI\log folder.

BUG FIXES:

Fixed a problem where the user could repeatedly be asked to enter proxy credentials when accessing the mobilEcho server through an HTTPS reverse proxy server.

Fixed a problem where the mobilEcho Client Management Server web UI could fail to restart because the client management database schema was not updated properly on upgrade. This would occur if the database was configured to be stored on a disk that was not available at upgrade time.

Sorting devices by "Last Contact" now sorts newest to oldest by default.

Copyright © Acronis International GmbH, 2002-2014

Fixed a problem where whitelists and blacklists could not be assigned when adding or editing a user or group profile.

Fixed a problem where files that were already on the device could sync again unnecessarily if the sync source was within an activEcho volume.

The password field on the login page of the client management web UI now has auto-complete disabled.

Removing a user or group profile now causes the name information for that user/group to be removed from cache. This ensures that re-adding a profile for that user/group will always force the management UI to retrieve the latest name from Active Directory.

Fixed a problem where "set the default file action" and "cache recently accessed files on this device" could be enabled in profiles after upgrading mobilEcho server.

Fixed a problem where the app password reset functionality in the management server UI might not work properly in Firefox.

Fixed a problem on the Invitations page of the client management server web UI where users within distribution subgroups could fail to be found in LDAP searches.

Fixed a problem where the server check for free disk space in a folder would incorrectly check the free space at the root of the mobilEcho volume.

Fixed a problem where open file handles would not be closed for 24 hours if a client disconnected in the middle of a file transfer. These handles will now be closed when the session times out, after 15 minutes.

Fixed a problem where the "Allow iTunes and iCloud to back up locally stored mobilEcho files" profile setting would always revert to enabled after saving management profile.

mobilEcho 4.1 (Released: December 2012)

ENHANCEMENTS:

Added an alternative client management server authentication mechanism so that mobilEcho clients that are configured to not save credentials for assigned servers and folders can authenticate to the management server to retrieve their profile without requiring their Active Directory password be stored on the device.

Modified the app password reset process. This was necessary to support the new custom on-device encryption that is included in the mobilEcho 4.1 client app. If a managed client forgets their app password, they now provide their administrator with a code generated by the app. The administrator enters this code into the mobilEcho Client Management web console and receives a second code that they give back to the client. This code allows the user to reset their app password and get into the app.

Enhanced the way resources (servers and folders) are provisioned to clients. Provisioned resources are no longer assigned directly to user/group profiles. Users or groups are now assigned directly to individual assigned resources and each user receives the full collection of resources assigned to their user account or a group they are a member of.

Added the ability to send up to three enrollment invitations to the same email address automatically for users with multiple devices.

Copyright © Acronis International GmbH, 2002-2014

Added a column to the LDAP search table for Distinguished Name so that users with the same name in different subdomains can be distinguished.

Added new management profile setting to allow or disallow users from opening and/or sending links to files.

Added client Good Dynamics status in the management server Devices list. Devices enrolled with Good Dynamics will no longer have the "Reset App Password" option available. The app password is managed within the Good Control console in this scenario.

BUG FIXES:

Fixed a problem where hiding inaccessible files on reshares when one of the volumes was a SharePoint volume could cause some of the volumes to fail to appear on the client.

Fixed a problem where the Client Management Administrator could fail to filter the devices or invitations tables, or could take a very long time to complete the filter. Filtering is now done without the need to perform additional LDAP requests.

Fixed a problem where attempting to read a file on an activEcho volume that no longer exists would result in a corrupted file being read rather than an error being returned.

Fixed a problem where the presence of a misconfigured or unavailable activEcho volume could cause clients to time out when attempting to retrieve the volume list.

Fixed a misleading message in the Client Management Administrator if a profile was configured to have 'App password must contain complex characters' greater than the 'Minimum password length'.

Fixed a problem when the client management server was configured to use a non-default port (i.e. not port 3000) and the server was upgraded. The first time the management server would run after upgrade it would attempt to use port 3000 rather than the configured port.

Modified the message in the Client Management Administrator when removing a currently managed client from the devices list to indicate that the client may automatically reenroll at a later time if enrollment PINs are not being used.

Fixed a problem where the Client Management Administrator could display an error if a profile was configured to use a home folder with an empty custom path.

Fixed a problem where 0-byte files would fail to download or sync with a "device not ready" error.

Content search is now automatically disabled on activEcho and SharePoint volumes since content search is not available.

Fixed a problem where users with email address beginning with underscore (e.g. "_user@example.com") could fail to receive enrollment invitations.

Client Management Administrator now returns a better error message than "unknown result" if the LDAP server requires SSL.

Fixed a problem where sessions could time out while downloading very large files.

Fixed a problem where configuring an assigned folder with an invalid path (e.g. "C:\foo\bar") could cause the Users page to show the error "can't modify frozen string".

Copyright © Acronis International GmbH, 2002-2014

Fixed a problem where selecting the "Reindex all volumes" button in the mobilEcho Administrator would generate an invalid error message.

Fixed a problem where filtering on a Unicode string in the Client Management Administrator could generate an "incompatible character encodings" error.

SharePoint "Wiki Page Gallery" libraries are now removed from site enumerations because they are not supported by mobilEcho.

Fixed a problem where new profile settings could become corrupted on upgrade.

Fixed a problem where a SharePoint document library volume would fail to work if the document library name was URL encoded, e.g. "My%20Library".

mobilEcho 4.0.3 (Release: October 2012)

ENHANCEMENTS:

Added support for SharePoint custom document libraries.

BUG FIXES:

Fixed a problem accessing SharePoint sites and document libraries whose paths are multiple levels below their parent site.

Fixed a problem accessing SharePoint sites that use Claims Based Authentication.

mobilEcho 4.0.2 (Released: September 2012)

ENHANCEMENTS:

Added support for Android clients.

Added settings to the mobilEcho Administrator for restricting access by iOS and/or Android clients.

Added support for sending enrollment instructions for iOS, Android and Good clients.

BUG FIXES:

Fixed a problem where exporting the devices list to a .csv file could result in a server error, or could result in some fields displaying as "Not found in AD".

Fixed a problem where non-Good clients could enroll with a management server that was configured to require clients be enrolled with Good Dynamics. Previously, clients could enroll, but would receive an error when contacting the server to access data. Clients are now disallowed from enrolling in the first place.

mobilEcho 4.0.1 (Released: August 2012)

Copyright © Acronis International GmbH, 2002-2014

ENHANCEMENTS:

Added profile settings for "Number of days to warn of pending lock" and "Number of days to warn of pending wipe". These settings relate to existing settings that can wipe or lock the mobilEcho app if the device does not contact the management server for a specified period of time.

Added pagination, filtering and sorting to the Users and Groups pages within the mobilEcho Client Management server.

BUG FIXES:

Fixed a crash that could occur when attempting to authenticate with SharePoint volumes using Kerberos authentication.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their user principal name (UPN) had a different domain than their Windows 2000 domain.

Fixed a problem where users could fail to authenticate with SharePoint volumes if their username contained Unicode characters and authentication was performed using NTLM.

Fixed a problem where users could fail to authenticate with SharePoint volumes if the user was a member of a subdomain and authentication was performed using NTLM.

SharePoint document libraries will now display all items, regardless of the settings of the library's default view.

The "Last Contact Time" column on the Devices page of the mobilEcho Client Management server now properly sorts by date.

Filters in the mobilEcho Client Management server now work properly with Unicode characters.

Filters in the mobilEcho Client Management server now "stick" after pagination settings are changed.

Disabled the "Indexed Search" and "Content Search" checkboxes when adding or editing reshare volumes in the mobilEcho Administrator, since search is not supported on those volumes.

The mobilEcho Administrator now automatically fills in the existing path when editing a SharePoint, activEcho or reshare volume path.

The mobilEcho server now returns a better error code if the user attempts to overwrite a file via Save Back that is checked out to another user.

mobilEcho 4.0 (Released: July 2012)

ENHANCEMENTS:

Added support for accessing data in SharePoint 2007 and 2010 document libraries.

The mobilEcho server can now simultaneously support activEcho and other volume types. Previous versions required switching into activEcho-only mode to access activEcho data.

Improved performance of the mobilEcho Client Management server by making LDAP queries "begins with" rather than "contains" by default. Administrators may choose "contains" when searching to obtain the previous behavior.

Copyright © Acronis International GmbH, 2002-2014

The mobilEcho Client Management server can now filter the invitations tables by username.

The mobilEcho Client Management server can now export the devices list to a .csv file.

The mobilEcho Client Management server now sorts and paginates the devices, users, groups and invitations tables.

Added a profile setting to allow/disallow users from creating bookmarks.

Added a profile setting to disable My Files while still allowing sync folders.

Added a profile setting to automatically lock the mobilEcho app or wipe all mobilEcho data if the device does not contact the management server for a specified period of time.

Added a profile setting to prevent users from setting an app password.

Files can now be copied within activEcho volumes by transferring data through the client.

Improved performance reading and writing to activEcho volumes.

BUG FIXES:

Fixed a problem where files and folders ending in a period or space could fail to be accessible on activEcho volumes.

Fixed a problem where the Devices page could fail to load in mobilEcho Client Management server after Japanese and Chinese users have enrolled.

mobilEcho 3.7 (Released: June 2012)

ENHANCEMENTS:

Improved performance of the mobilEcho Client Management server by caching user information to minimize the number of LDAP queries.

BUG FIXES:

Active Directory distribution groups are no longer found when searching for groups on the group profile page.

Fixed a problem when the path of a provisioned folder ends with a backslash.

mobilEcho 3.6.1 (Released: May 2012)

BUG FIXES:

Fixed a problem where files on an activEcho server could fail to preview, copy or sync.

Fixed a problem where users could fail to preview, copy or sync files in a home directory if the home directory was set up with a network reshare path mapping in the mobilEcho Client Management server.

Copyright © Acronis International GmbH, 2002-2014

Fixed a problem where users could fail to see their home directories if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

Fixed a problem where the "%USERNAME%" wildcard would fail to use the correct username if the client authenticated to the management server with a user principal name (UPN) such as user@domain.com.

mobilEcho 3.6 (Released: April 2012)

ENHANCEMENTS:

Improved performance of Active Directory lookups for users and groups.

Searches of Active Directory in the mobilEcho Client Management server now search on both common names and display names.

Add profile settings for allowing/denying the ability of users to create sync folders, and to perform a Quickoffice® "Save Back".

The mobilEcho Client Management server can now be configured to store database and profile information in a different location than the application directory, allowing for the management server service to be failed over to other cluster nodes.

The mobilEcho Administrator now displays the number of licenses currently being occupied, and will only display a single session for each user/device if the user has reconnected to the mobilEcho server multiple times.

The mobilEcho Administrator now automatically runs with elevated privileges.

The enrollment email subject can now be customized in the 'mobilEcho_management.cfg' file.

BUG FIXES:

mobilEcho no longer permits Active Directory "Distribution" groups to be used to create mobilEcho Client Management group policies. Distribution groups are provided by Microsoft for email purposes only. If you are using AD "Distribution" groups for any of your mobilEcho Client Management policies, please use the "Active Directory Users and Computers" control panel to convert these groups to "Security" groups.

Fixed a problem where a user that used different username formats to enroll with multiple devices would occupy multiple licenses. For example, if one device was enrolled as "user@example.com" and a second device was enrolled as "example\user", the licensing logic would treat those as two separate user accounts for licensing purposes.

Fixed a problem where a user could fail to get the appropriate group profile if the user's Active Directory primary group was not set to the default of "Domain Users".

Fixed a problem where a user could fail to get the appropriate group profile if the user's group was a "universal" Active Directory group.

Fixed a problem where users with Unicode characters in their usernames would not have their credentials saved after enrolling with mobilEcho Client Management.

Copyright © Acronis International GmbH, 2002-2014

Fixed a problem where the server could allow mobilEcho clients to overwrite files that were flagged as read-only.

Fixed some mobilEcho Client Management display issues on Mac Safari.

Fixed a problem where Verizon iPad 3 devices were displayed as "AT&T" (and vice versa) in the mobilEcho Client Management devices page.

Fixed a problem where the mobilEcho Administrator could crash when viewing the list of connected users.

Fixed a problem where the invitation email would fail to show the username.

mobilEcho 3.5 (Released: February 2012)

ENHANCEMENTS:

Added support for 2-way sync folders. Client-side changes made in 2-way sync enabled folders will be synced back to the server automatically. These 2-way sync folders can be provisioned through the mobilEcho Client Management server.

Added support for reverse proxy authentication. Reverse proxy servers, such as Microsoft Forefront Threat Management Gateway (TMG), can be configured to require authentication before granting access to internal network resources. The mobilEcho client now supports both HTTP username/password and SSL Client Certificate authentication methods. To use SSL Client Certificate authentication, a certificate must be installed in the mobilEcho keychain. See this Knowledge Base article for more information: http://support.grouplogic.com/?p=3830

Added additional options for configuring mobilEcho device enrollment requirements. mobilEcho can now be optionally configured to accept enrollment requests from devices without the need for a one-time PIN. In addition, when mobilEcho is configured to require such PINs, these PINs can be viewed within the management interface.

Added support for client app whitelisting and blacklisting. A managed mobilEcho client can be configured so that files can only be opened into a restricted whitelist or blacklist of third-party iOS apps.

Improved browsing performance of network reshare volumes by disabling the filtering of inaccessible file and folders by default on such volumes.

Added support for network reshare to SMB/CIFS volumes on NetApp storage.

Added the ability to configure mobilEcho provisioned folder paths that include a username wildcard.

Added the ability to configure mobilEcho home folders with custom paths. These paths may include a username wildcard.

mobilEcho no longer requires that users have "list folder" permissions at the root of a share containing their home folder.

Added a new registry setting to control whether or not hidden shares on a network reshare are visible to mobilEcho clients. To enable this feature, set the following registry setting to 1:

Copyright © Acronis International GmbH, 2002-2014

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\GetShowHiddenSMBShares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would appear to allow access without a proper username and password.

Fixed a problem where files would incorrectly require a sync after a change in daylight savings time.

Fixed a problem where renamed files would continue to be returned in search results when searching under the old filename. This problem would only occur for volume that were configured to use "indexed search" (not Windows Search).

Fixed a problem where mobilEcho could fail to install or run on systems missing a system DLL (normaliz.dll).

Fixed a problem where the client could fail to copy a file to the server if the user account did not have permission to calculate the amount of free space on the volume. The client would report an error about there not being enough free space on the volume.

Removed extraneous logging from the mobilEcho LOG.TXT file.

Fixed a problem where folders could not be provisioned for servers whose display name contained parentheses.

mobilEcho 3.1 (Released: November 2011)

ENHANCEMENTS:

Client management profiles can now be configured with the following new settings:

- The number of incorrect app password attempts that can be made before the local data within the mobilEcho app is automatically wiped. This feature is disabled by default.
- Whether the user is required to confirm before syncing occurs (options are: "Always", "Never", and "Only on 3G").
- Whether syncing is allowed any time, or only while on WiFi networks.
- Client timeout for unresponsive servers now accepts additional values of 90, 120 and 180 seconds.

The mobilEcho Client Management server can now be configured to communicate with Active Directory via secure LDAP.

Profiles now default to allow files to be cached on the local device. If caching is disabled or if the "Allow files to be stored on this device" setting is disabled, no files will be cached.

Copyright © Acronis International GmbH, 2002-2014

The text of enrollment invitation emails can be customized. Please visit the GroupLogic Knowledge Base for more information: http://support.grouplogic.com/?p=3749

Added a setting to the management configuration file to control the name that enrollment invitation emails appear from (e.g. "mobilEcho Invitation <mobilEcho_invitation@example.com>". Version 3.0 only allowed an address to be specified (e.g. "mobilEcho_invitation@example.com").

The VALID_LOGIN_NAMES field of the management configuration file now supports Active Directory groups in addition to specific users that can administer the mobilEcho Client Management service.

Changing SMTP settings within the management configuration file no longer requires a restart of the mobilEcho Client Management service.

Profiles for users and groups that no longer exist in Active Directory are now marked as such in the mobilEcho Client Management service.

Added the ability to show inaccessible items only on reshare volumes. This can be useful in cases where determining file and folder accessibility is causing performance problems. This behavior can be adjusted by modifying the following registry setting and restarting the service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\HideInaccessibleItemsOnReshares

BUG FIXES:

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path if the associated 'Network reshare path mapping' included a trailing backslash.

Fixed a problem where the mobilEcho Client Management server would not properly calculate an Active Directory home directory path that only included a server and share name. (i.e. \\servername\sharename)

Fixed a problem that could prevent network reshare volumes configured with paths to the root of a server (i.e. \\servername) from appearing properly in the mobilEcho client.

mobilEcho clients now always log into provisioned servers using fully qualified domain accounts. In previous versions of mobilEcho, the credentials entered at enrollment time would be used to authenticate with file servers, even if these credentials did not include a domain name (e.g. domain\user). This could cause problems if the provisioned server was on a different domain than the management server and access to the server in the secondary domain relied on a domain trust with the primary domain. This behavior can be reverted to the previous default by setting the following registry value to 0 and restarting the service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\DomainAndUsernameShouldBeSentToClient

Fixed a problem where the mobilEcho Client Management server did not properly sort "Last contact date" properly on the Devices page.

Copyright © Acronis International GmbH, 2002-2014

Fixed a problem in the mobilEcho Administrator where the Help button would not adjust properly as the Users window was resized.

mobilEcho 3.0 (Released: October 2011)

ENHANCEMENTS:

Centrally managed device enrollment. Client enrollment invitations are now generated and emailed to the user from the mobilEcho Client Management Administrator. These invitations include a one-time use PIN number required for client enrollment.

Remote wipe and remote reset of app passwords is now performed on a per-device basis.

Individual device status is now displayed in the mobilEcho Client Management Administrator. This includes device user name, device name, device type, iOS version, mobilEcho version, mobilEcho status, last contact time.

Users' Active Directory assigned network home folders can now be automatically displayed in the mobilEcho client app.

Specific mobilEcho shared volumes or folders within shared volumes can now be assigned to user or group profiles. These shared volumes or folders are then automatically displayed in the mobilEcho client app.

Shared volumes or folders assigned to user or group profiles can be configured to automatically one-way sync from server to mobilEcho client, making the contained files available for online or offline use.

BUG FIXES:

Fixed a problem where the mobilEcho server would not properly report free space for server-to-server copies.

Improved error messages and processing if a user attempts to copy or move files into the root of a network reshare.

Fixed a problem where a user could be authenticated with AD by contacting mobilEcho via a web browser. This could cause a user account to become locked.

Improved the speed of installation, particularly for upgrades.

Fixed a problem where files and folders ending a period or space could fail to copy properly.

Fixed a problem logging into the management UI with a username containing numbers, e.g. "e12345".

Updated OpenSSL library to latest version. OpenSSL libraries are used for encryption.

mobilEcho 2.1.1 (Released: July 2011)

BUG FIXES:

Copyright © Acronis International GmbH, 2002-2014

Fixed a bug when listing the contents of folders which may have resulted in slow performance or client timeouts if many of the folders were not accessible to the client.

mobilEcho 2.1.0 (Released: July 2011)

ENHANCEMENTS:

Added the ability to create mobilEcho shares that reshare data on a remote system. The mobilEcho reshare feature is only available for customers with an enterprise license. Reshares can be a particular share (e.g. "\\server\share") or an entire server ("\\server\").

The mobilEcho client can now perform copy and move operations on folders when connected to a server running mobilEcho Server 2.1 or later, and the management UI now has settings to allow or disallows these operations.

The management UI now has the ability to add a new group or user using settings from an existing user or group.

Management profiles can now be disabled so that the corresponding user or group cannot receive their profile.

Added the ability to prevent clients from connecting to servers with self-signed certificates.

Added a management setting to enable or disable copying text from a previewed document.

Added a management setting that tells the client to store files so that they are not backed up by iTunes.

mobilEcho 2.0.0 (Released: May 2011)

ENHANCEMENTS:

Added the ability to manage mobilEcho clients using server-defined profiles using mobilEcho Client Management.

Added the ability to reset mobilEcho app passwords from the server.

Added the ability to force a remote wipe for a particular mobilEcho user.

mobilEcho will now use an internal filename index for satisfying search requests if Windows Search is not installed or available.

The mobilEcho administrator now allows for volumes to be seamlessly replicated from SMB and/or ExtremeZ-IP shares.

mobilEcho 1.0.0 (Released: January 2011)

Initial release.

Copyright © Acronis International GmbH, 2002-2014